MODELING FANCY BEAR CYBER ATTACKS

Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks

Author:	Mr. drs. Paul Pols
Student ID:	S1806084
Date:	December 7, 2017
Supervisor:	Dr. ir. Pieter Burghouwt
Second Reader:	Prof. dr. ir. Jan van den Berg
Institution:	Cyber Security Academy (CSA)

[1]

FOX IT
FOR A MORE SECURE SOCIETY

CYBERSECURITYACADEMYUNIVERSITEIT LEIDENCAMPUSDENHAAGTECHNISCHEUNIVERSITEITDELFTDEHAAGSEHOGESCHOOL

Abstract

Organizations increasingly rely on Information and Communication Technology (ICT), exposing them to increasing risks from cyber attacks from a range of threat actors. The term Advanced Persistent Threats (APTs) is used to refer to particularly capable threat actors, that are typically backed by nation-states. To raise their resilience, organizations can model APT cyber attacks using Lockheed Martin's Cyber Kill Chain® (CKC) or ethical hacking assessments by Red Teams. The modus operandi (MO) of APTs does not necessarily coincide with these models, which can limit their predictive value and lead to misaligned defensive capabilities and investments.

In this thesis, a Unified Kill Chain (UKC) model is developed that focuses on the tactics that form the consecutive phases of cyber attacks (Table 1). A hybrid research approach is used to develop the UKC, combining design science with qualitative research methods. The UKC is first developed through literature study, extending the CKC by uniting improvements that were previously proposed by other authors with the tactics of MITRE's ATT&CK™ model. The UKC is subsequently iteratively evaluated and improved through case studies of attacks by Fox-IT's Red Team and APT28 (alias Fancy Bear). The resulting UKC is a meta model that supports the development of end-to-end attack specific kill chains and actor specific kill chains, that can subsequently be analyzed, compared and defended against.

Table 1 - Overview of the development of the Unified Kill Chain (UKC)

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Laliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	Reconnaissance	1	1	1	1	1		1	1	1	1	1	1
2	Weaponization	2	3	3	3	2		2	2	2	2	2	2
3	Delivery	3	5	5	6	3		7	7	3	3	3	3
4	Social Engineering	5	6	6	11	5		3	3	4	4	4	4
5	Exploitation	6	8	8	14	6		5	4	5	5	5	5
6	Persistence	8	14	9	18	8	6	6	5	6	6	6	6
7	Defense Evasion	18	18	14	16	10	11	8	6	7	7	7	7
8	Command & Control			18		5	7	9	8	8	8	8	8
9	Pivoting					11	13	11	9	9	9	9	9
10	Discovery					14	10	10	11	11	11	10	10
11	Privilege Escalation					17	14	14	10	10	10	11	11
12	Execution					18	12	12	14	14	14	12	12
13	Credential Access						15	13	12	12	12	13	13
14	Lateral Movement						16	17	13	13	13	14	14
15	Collection						8	15	17	17	17	17	15
16	Exfiltration							16	15	15	15	15	16
17	Target Manipulation								16	16	16	16	17
18	Objectives												18

The literature and case studies show that the traditional CKC is perimeter- and malware-focused and as such fails to cover other attack vectors and internal attacks paths. The case studies falsify a crucial assumption underlying the CKC model, namely that attackers must progress successfully through each phase of the deterministic sequence of the CKC. The observation that attack phases can be bypassed affects defensive strategies fundamentally, as an attacker may also bypass the security controls that apply to that phase in doing so. Instead of focusing on thwarting attacks at the earliest point in time, layered defense strategies that focus on phases that are vital for the attack path or that occur with a higher frequency are thus expected to be more successful.

The UKC provides insights into the ordered arrangement of phases in end-to-end cyber attacks and covers diverse attack vectors, by uniting and extending existing models. The UKC offers a significant improvement over the scope limitations of the CKC and the time-agnostic nature of the ATT&CK™ model. Other improvements over the existing CKC and ATT&CK™ models include: explicating the role of users by modeling social engineering, recognizing the crucial role of choke points in attacks by modeling pivoting, covering the compromise of integrity and availability in addition to confidentiality and elucidating the socio-technical objectives of threat actors. These insights support the development (or realignment) of layered defense strategies that adopt the *assume breach* and *defense in depth* principles.

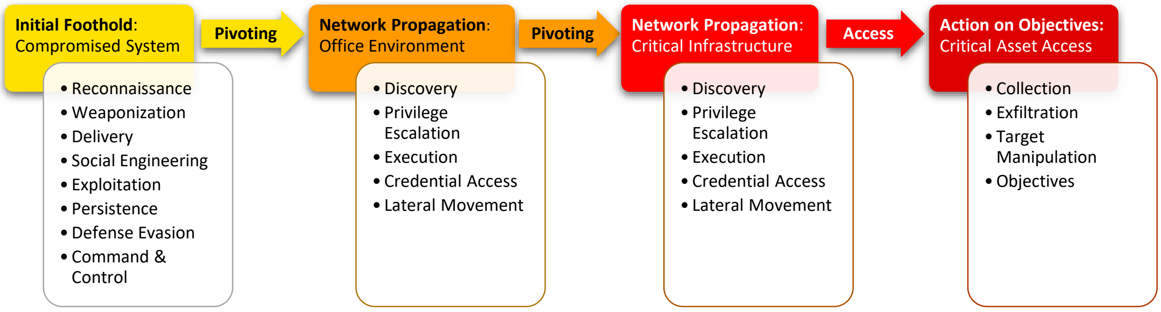


Figure 1 – A further attack path abstraction supported by the Unified Kill Chain

The UKC is utilized to analyze and compare attacks by Fox-IT's Red Team and APT28 to improve threat emulation and to raise organizational resilience against APT28 attacks. The comparison shows that the tactical MO of these actors converge in their attack paths within internal networks of targeted organizations. Red Team assessments are thus thought to be particularly well suited to test the resilience of organizations against this part of APT28's potential attack path. Notable divergences were also identified, which signify the potential to improve the predictive value of Red Team assessments, for example by performing action on objectives (Figure 1).

As the reliance of organizations on ICT continues to grow, and APT cyber attacks continue to rise in number and in force, the risks for organizations and societies as a whole increase at an accelerating pace. The UKC attack model can be used by Red Teams to improve their threat emulations and by defenders to develop and realign their defense strategies in their attempts to decelerate this dangerous trend.

Keywords — Attack Modeling, Attack Simulation, Threat Emulation, Cyber Kill Chain®, MITRE ATT&CK™, CORAS, APT28, Fancy Bear, Pawn Storm, Sednit, Sofacy, Strontium, Red Team, Tactics, Techniques, Procedures, Design Science, Assume Breach, Defense in Depth, Unified Kill Chain.

Table of Contents

1 Introduction

In the last decades, the dependence throughout modern societies on information and communication technology (ICT) has continued to rise. Vulnerabilities in the supporting ICT assets threaten the cyber activities that are performed within modern societies. Organizations need to protect their assets against a variety of threat actors that range from cyber criminals to nation states. At the more advanced and persistent end of this threat actor spectrum, actors are often described as Advanced Persistent Threats (APTs).

To assess their security posture and improve their resilience against APT attacks, many organizations hire Red Teams that are comprised of ethical hackers. Red Teams take an attacker-like approach to compromising critical supporting ICT assets. The predictive value of the threat emulations offered by Red Teams relies on the alignment of the modus operandi (MO) of the Red Team with the relevant threat actors. However, the tactics and operational techniques and procedures (TTPs) that are used by these actors do not necessarily coincide.

To perform a structured analysis of the MO of Red Teams and APTs, threat modeling is required. The Cyber Kill Chain® by Lockheed Martin (hereafter CKC) is frequently regarded as the industry standard model for defending against APTs. The CKC models the consecutive phases that APTs go through in compromising assets. Despite (or because of) its prominent status, the CKC has been widely criticized. The most damaging criticisms argue that the CKC is perimeter- and malware-focused [2]. To accurately model and compare Red Team and APT attacks beyond the organizational perimeter and beyond malware attacks, the CKC may thus require modifications.

The aim of this thesis is to (re)design a kill chain artefact that can serve to model and compare end-to-end attacks by both Red Teams and relevant APTs. The term “kill chain” describes an *end-to-end* process [3, p. 4], or the entire chain of events, that is required to perform a successful attack. The (re)designed kill chain model is iteratively developed, evaluated and refined through literature research and case studies. The scope of the case studies is limited to two threat actors, namely Fox-IT’s Red Team, and APT28 (alias Fancy Bear). The resulting Unified Kill Chain (UKC) is expected to offer a substantiated basis for realigning defensive capabilities and investments within organizations and to allow for the improvement of the predictive value of Red Team threat emulations.

1.1 Conceptualization and Contextualization

In this section, the foundational concepts underlying this thesis are conceptualized and contextualized first, to allow for a deeper and broader level of understanding of the research topic.

1.1.1 Societal Dependence on Cyberspace

The realm of cyberspace can be regarded as consisting of three interdependent layers (Figure 2). The primary object of study for this thesis is the technological layer, which comprises the hardware and software of ICT systems and data contained therein. The technical layer supports a so-termed socio-technical layer, where ICT enables a variety of cyber activities. The socio-technical layer comprises the interactions that take place between people and systems that are often referred to with the term “cyber”. The final layer is the governance layer, which as the name suggests, governs the technical and socio-technical layers [4, p. 2].

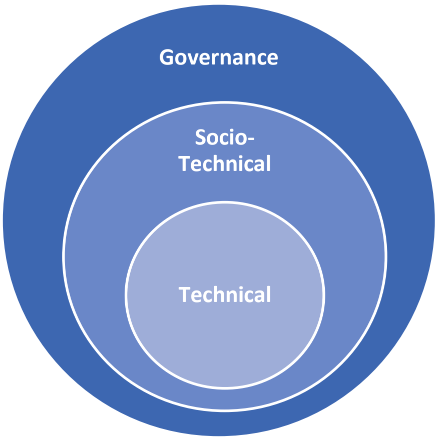


Figure 2 – Layered Cyberspace Model [4]

The dependence of cyber activities on the technical layer is inescapable in modern societies. These cyber activities include critical organizational processes that may range from information exchange within and between organizations to the remote control of Information Control Systems (ICS) in critical infrastructures [4, p. 2]. The socio-technical dependence of society on supporting ICT assets, combined with the inevitable vulnerability of complex systems, entails that vulnerabilities in ICT systems can pose risks to critical cyber activities and societies as a whole. The fact that many of these systems are (in)directly connected to the internet creates the possibility that cyber activities can be threatened from anywhere in the world at any point in time. The diffuse global governance structure of cyberspace has not been able to mitigate these risks to an acceptable level and is not expected to do so in the foreseeable future.

1.1.2 Constructs of Technical and Cyber Risk

Risks can exist on multiple layers of the layered cyberspace model. Risks on the technical layer can be deconstructed into a predefined set of risk components, namely the threat actor, threat, vulnerabilities, controls, impact and the supporting ICT asset that can be compromised. Threat actors (or agents) act with intent towards an asset. A threat is the potential cause of an unwanted event that can affect an asset, as a result from (un)intentional acts or contingencies. Vulnerabilities are weaknesses in assets, that can be exploited by threats with a certain likelihood. Controls are measures that are intended to modify risks. Impact refers to the consequence of an event in which a threat materializes through the exploitation of a vulnerability in an asset [5].

Technical risks thus describe the potential that threat actors cause threats to materialize by exploiting vulnerabilities, in lieu of appropriate controls, that result in an undesirable impact for a supporting ICT asset. Socio-technical or “cyber” risks can arise when supporting assets are compromised on the technical layer, with the potential to pose a threat on the socio-technical layer for vulnerable cyber activities that can have an undesirable organizational impact (in lieu of appropriate controls) [6].

1.1.3 Mitigation of Technical and Cyber Risk

Traditionally, efforts to mitigate risks focused on mitigating technical *vulnerabilities* in supporting ICT assets. This approach is thought to be particularly useful in reducing the technical risks associated with relatively static threats such as self-propagating code (virii and worms) [3, p. 1]. More recently, efforts have shifted towards the *threat* component of risk, to reduce risks by increasing the organizational resilience against foreseeable actions by dynamic threat actors. The shift is necessitated by the rise of Advanced Persistent Threats (APTs) and the frequency and the size of the socio-technical impact of their attacks [3, p. 2].

1.1.4 Advanced Persistent Threats (APTs)

The acronym APT is used to describe a variety of threat actors in cyberspace. The acronym was purportedly first used within the United States intelligence community to describe *Asia-Pacific Threats* (cyber threats originating from China). Since then, the term has been used to describe various (relatively) advanced attackers who are (particularly) persistent in their attacks on their targets. Currently, the term Advanced Persistent Threat is defined by NIST as:

> *“An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The*

> *advanced persistent threat:*
> *(i) pursues its objectives repeatedly over an extended period of time;*
> *(ii) adapts to defenders' efforts to resist it; and*
> *(iii) is determined to maintain the level of interaction needed to execute its objectives*" [7]

1.1.5 APT Threat Modeling

Attacks by APTs typically extend beyond exploiting one vulnerability in an internet-connected system. Depending on the security posture of the target, APT attacks may require an attack path during which multiple correlated vulnerabilities are exploited before assets can be targeted and objectives can be achieved. Within the attack path, discrete phases can be discerned that are captured by Lockheed Martin's CKC in a linear and sequential model. The CKC, as well as other attack lifecycle models, can help defenders understand the increasingly complex attacks that they are facing. Without understanding how modern attacks take place, it is very difficult to properly defend against them.

1.1.6 Ethical Hacking and Red Teams

Many organizations assess their security posture and resilience against attacks using ethical hackers. Penetration testing typically occurs within a limited scope according to pre-approved testing guidelines and aims to identify as many vulnerabilities as possible with the allotted timeframe [8, p. 11]. In contrast to classical penetration testing, Red Teams take an attacker-like approach and typically focus on obtaining access to critical supporting assets rather than identifying the most vulnerabilities [8, p. 1]. Within the cyber security context, it is said that "Red Team [efforts] should simulate an attack from a potential attacker" [8, p. 11]. The more advanced the attacker whose threat should be emulated, the more advanced Tactics, Techniques and Procedures (TTP) should be used by a Red Team [8, pp. 16–17]. Red Teams may thus serve to model threats by simulating or emulating their attacks in a transparent manner, which provides insights into complex attack paths.

1.2 Problem Description

1.2.1 High Profile and Impactful APT Attacks

Cyber security firms are keen to publicize forensic reports following (un)successful APT attacks, which allows organizations to reassess their security posture and raise their resilience against similar attacks. An APT that has performed particularly high profile and impactful attacks over the last few years is APT28. Attacks that have been linked to this group include (attempted) hacks of Dutch ministries and the Dutch Safety Board ('Onderzoeksraad Voor Veiligheid'), as well as the Ukrainian Central Election Commission (CEC), TV5Monde, the U.S. Democratic National Committee (DNC), the World Anti-Doping Agency (WADA), the Polish government and power exchanges, the German Bundestag and political parties, the North Atlantic Treaty Organization (NATO) and the Organization for Security and Co-operating in Europe (OSCE) [9].

Perhaps the highest profile and the most impactful APT28 attack targeted the Democratic National Committee (DNC) in the United States [10]. In the aftermath of the attack, compromised DNC data was publicized by Wikileaks [11]. The DNC hack was reportedly part of a larger "active measures" campaign by the Russian state, to sway the presidential elections using "a combination of cyber, of propaganda [and] social media" [12]. A narrow margin, of less than 1% of the voters in three crucial states, ultimately decided the outcome of the elections [13]. Evidence has been uncovered that voters in at least two of these states were specifically targeted by the active measures campaign [12]. This raises the question if the active measures may have swayed at least 1 in every 200 voters in these states, thereby potentially swayed the outcome of the presidential election [14]. This question, and many other related questions regarding the active measures campaign, are currently being investigated post-mortem by multiple committees and investigators in the United States.

1.2.2 Attribution and Relevance

The cyber attacks performed by APT28 have been attributed to the Russian military intelligence service (‘Main Intelligence Directorate of the General Staff of the Russian Armed Forces‘ or GRU for short) with a “high” level of confidence by a collection of intelligence agencies of the United States of America [10]. Others have described APT28 as a group that reportedly “works for the Russian state or the Russian state intelligence services, but [that] the state keeps the actual attacks at a certain distance” [15, p. 13].

The variety of the previous victims of APT28 suggests that a wide variety of organizations may be targeted by this group in the future. The attribution of APT28 attacks to the Russian state makes raising resilience against their attacks a top priority for many of Fox-IT’s customers, given the current geopolitical climate. According to the Dutch secret service, Russia actively targets Dutch actors in sectors such as economics, science, politics and defense to gather intelligence, influence decision making processes as well as the public opinion [16, pp. 3–7]. Attacks by APT28 thus factor into the threat model of many private and public organizations, ranging from large corporations to critical infrastructure and government entities. The advanced and persistent nature of this threat actor, in combination with the pervasive, widely publicized and impactful nature of its successful attacks, underlines the importance of increasing resilience against APT28 attacks.

The MO of threat actors such as APT28 may be studied to improve the resilience of organizations against similar attacks, even if attribution is impossible or highly uncertain. When Fox-IT’s clients express the desire to defend themselves against “the Russians”, they generally aim to protect themselves against the types of attacks that have been attributed to the Russians, particularly those by APT28 (and APT29). Consequently, even if the attribution of APT28 to the Russian military intelligence service is inaccurate, at the core many of Fox-IT’s clients aim to defend themselves against the attacks of threat actors such as APT28.

1.2.3 Red Team Threat Emulation and Attack Simulation

One of the methods to assess and improve the resilience of organizations against APT attacks is threat emulation and attack simulation through Red Team assessments. In theory, Red Teams assessments provide insight into the organizational security posture and resilience against actual attacks by the relevant threat actors. The added value of Red Team attack simulations for organizations relies in a large part on the assumption that the default MO of a Red Team and relevant threat actors coincide. In practice, the MO of Red Teams does not necessarily coincide with the MO of the threats they implicitly or explicitly aim to emulate. If differences do exist between the MO of APTs and Red Teams, the predictive value of these threat emulations may be limited.

1.2.4 Limitations of APT Threat Modeling

The Cyber Kill Chain® by Lockheed Martin (CKC) is frequently regarded as the industry standard model for defending against APTs. This highly influential model describes the MO of APTs, but largely relies on untested assumptions. The CKC posits the consecutive phases that APTs go through in compromising cyber assets. Furthermore, the researchers posit that attacks by APTs may be thwarted by disrupting any one of the phases in this chain of events. As such, the CKC provides defenders with a model to stop APTs from compromising cyber assets beyond remediating vulnerabilities. By helping to find the most effective way to stop APTs during one of the consecutive phases of the attack, the CKC can also be beneficial in allocating defensive efforts.

If the idealized MO underlying the CKC is inaccurate however, defensive capabilities and investments are likely to be ineffectively distributed over the attack surface of organizations. Moreover, if reference models such as the CKC idealize an inaccurate MO, Red Teams are prone to develop an inaccurate MO in APT emulations, thereby adding to this problem.

1.3 Research Question(s)

1.3.1 Research Goal

The desire to raise the organizational and societal resilience against cyber attacks through the improvement of Red Team threat emulations of APTs is the primary driver of this thesis. To assess and improve the predictive value of Red Team assessments, a thorough comparison between the MO of Red Teams and relevant APTs is required. The comparison of the MO in Red Team and APT attacks is expected to be hindered by the absence of an accurate and comprehensive modeling framework. To overcome this challenge, the CKC is expected to require improvements and amendments to enable the sought for comparison. This research thesis proposes improvements and amendments to the CKC that result in a comprehensive kill chain based model, that covers end-to-end attacks, which is named the Unified Kill Chain (UKC).

1.3.2 Levels of Abstraction

The identified problem (section 1.2) can be examined at different levels of abstraction, in accordance with the three levels of abstraction of offensive and defensive actions [17, p. 97]:

- The *operational* level deals with the specific techniques that comprise attacks (or: *how* actions are performed in an attack). An analysis on the operational level of abstraction could in theory be very useful, to reproduce the MO of an attacker exactly. However, an operational analysis can become redundant quickly given the high pace of development of vulnerabilities, exploits and techniques. Furthermore, APTs may have access to resources and techniques that are beyond the reach of Red Teams, such as the use of zero-day exploits.
- At the *tactical* level, activities are directed to achieve the objectives of an attack [18, p. 1] (or: *which* actions are performed in an attack). The representation of actions as phases (or tactics), that can be discerned within an attack, occurs on the tactical level. These phases can remain similar across multiple attacks, even if specific techniques and procedures are changed on the operational level.
- At the *strategic* level, the objectives are set which attacks are intended to accomplish to achieve a goal [18, p. 3] (or: *why* actions are performed in an attack). The limitations regarding attribution of attacks in cyberspace, combined with the inability to reliably gain insight into the overall plans and intentions of threat actors, make scientific analysis on this level particularly difficult.

The term Tactics, Techniques and Procedures (TTPs) can be mapped to the three levels of abstraction. Tactics occur on the tactical level and describe “the employment and ordered arrangement of forces in relation to each other”. Techniques and procedures occur on the operation level and entail “non-prescriptive ways or methods used to perform missions, functions or tasks” and “standard, detailed steps that prescribe how to perform specific tasks” respectively [19].

Given the previously described goal of this thesis, the analysis of the identified problem and the construction of solutions primarily takes place on the tactical level of abstraction and thus focuses on *tactics*. However, taking the operational techniques and procedures and the strategic objectives into account may be enlightening to discern and understand the interconnection and the ultimate goal of the tactics.

When the sequence within which tactics occur is considered (their “ordered arrangement” [19]), tactics can be regarded as the phases of an attack. The end-to-end sequence of all phases of an attack forms the kill chain of that attack (or an *attack specific kill chain*). When multiple attacks from the same actor are analyzed and compared, they can be used to develop a *threat actor kill chain*, which describes the tactics in an actors’ repertoire as phases that may occur in their attacks. These threat actor specific kill chains are developed for Fox-IT’s Red Team and APT28, to facilitate a comparison of their MO and to test and refine the UKC.

1.3.3 Primary and Sub Questions

To achieve the research goal, the following primary research question is answered in this thesis:

> *Which kill chain model supports the comprehensive analysis, comparison and defense against the tactical modus operandi in Fox-IT’s Red Team and APT28 attacks?*

The research question can be further divided into the following sub research questions:

1. To what extent does the CKC allow for a comprehensive tactical comparison of attacker MOs? (sections 2.1 and 2.2)
2. What modifications to the CKC are expected to be required to allow for a comprehensive tactical comparison? (sections 2.2 to 2.5.2)
3. To what extent can the tactical MO of Fox-IT’s Red Team be modeled using the UKC? (chapter 3)
4. To what extent can the tactical MO of APT28 be modeled using the UKC? (chapter 4)
5. What are notable convergences or divergences between the CKC, UKC and the tactical MO of Fox-IT’s Red Team and APT28? (chapter 5)
6. How can the CKC and Red Team modeling of APT28 attacks be improved? (chapters 5 and 6)

1.4 Research Methodology

This thesis aims to raise the resilience against cyber attacks through the development of a (re)designed kill chain that allows for the comprehensive tactical comparison of Red Team and APT28 attacks. For this purpose, research questions have been defined in section 1.3. In this section, the design of and approach to this research study is detailed in the light of the research questions and the available data sources.

1.4.1 Availability of Research Data

Performing scientific research into the MO of APTs is difficult given the level of secrecy that applies to both (TTPs employed by) attackers and (breaches experienced by) defenders. Data regarding APT attacks is limited to public reports into isolated malware samples and acknowledged breaches, which frequently lack details regarding (internal) systems that were breached. Furthermore, definitive attribution often remains elusive. As a result, it is difficult to gain robust data regarding the attack paths of specific APTs, especially if the industry standard CKC model for defenders is lacking in this regard. Nonetheless, actors such as APT28 pose very real risks to organizations. Therefore, despite these intrinsic difficulties, scientific methods are used with the available data to perform research into this area as described in the subsequent section.

In contrast, the modus operandi of Fox-IT's Red Team is transparent as unfiltered access is available to reports, all supporting data and team members during this research. If Red Teams are successful in emulating APTs, their attacker-like approach to compromising networks and assets can generate more robust data and can be useful to gain further insights into expected attacker behavior. There are reasons to presume a priori that the MO of Red Teams may be similar to APTs. Both types of actors typically start from the perspective of an unauthorized outsider. Both may have comparable objectives that need to be achieved, for which a finite number of attack paths of correlated vulnerabilities are possible. Both types of actors presumably attempt to effectively and efficiently pave their way towards their targets, while remaining undetected. Both APTs and Red Teams may leverage TTPs that are available in the public domain, in addition to potential private TTPs.

1.4.2 Research Design and Approach

To answer the research questions, a hybrid approach was developed that combines design science with qualitative research methods. Figure 3 provides a schematic overview of the research approach. A schematic overview of the results of the research approach is provided in Table 25 (on page 69).

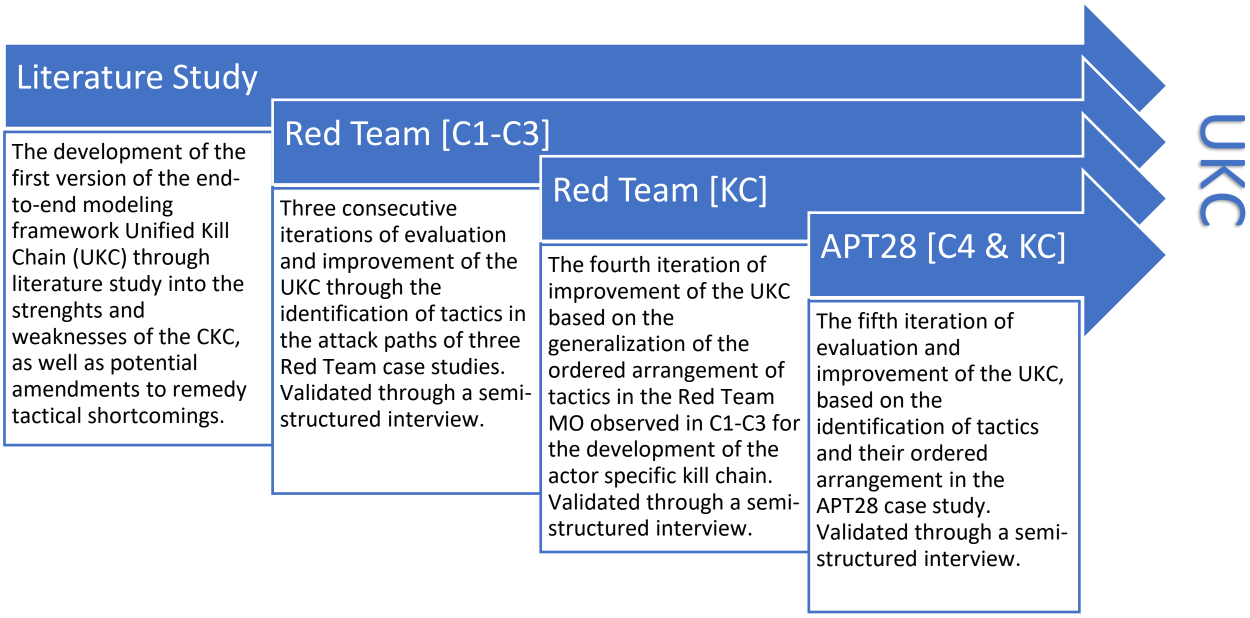

Literature Study
The development of the first version of the end-to-end modeling framework Unified Kill Chain (UKC) through literature study into the strenghts and weaknesses of the CKC, as well as potential amendments to remedy tactical shortcomings.
Red Team [C1-C3]
Three consecutive iterations of evaluation and improvement of the UKC through the identification of tactics in the attack paths of three Red Team case studies. Validated through a semi-structured interview.
Red Team [KC]
The fourth iteration of improvement of the UKC based on the generalization of the ordered arrangement of tactics in the Red Team MO observed in C1-C3 for the development of the actor specific kill chain. Validated through a semi-structured interview.
APT28 [C4 & KC]
The fifth iteration of evaluation and improvement of the UKC, based on the identification of tactics and their ordered arrangement in the APT28 case study. Validated through a semi-structured interview.
UKC

Figure 3 - Schematic overview of the research approach

In this research thesis, the appropriate modeling framework is first developed through literature study. Lockheed Martin's CKC model serves as the starting point to analyze APT and Red Team attacks. The need to improve and amend the CKC model is assessed based on the critiques on the model from experts. Phases from the various previously proposed modifications are combined with the tactics described in MITRE's ATT&CK™ model in the area where the CKC falls short. In this manner, a first version of an all-inclusive "*Unified Kill Chain*" (UKC) is developed through literature research, which unites all relevant phases of the various models to retain their collective explanatory power.

Secondly, the validity and explanatory value of the Unified Kill Chain is evaluated using observational methods through case studies of transparent attacks by Fox-IT's Red Team. In these case studies, the chain of events of each attack is first derived from reports and is visualized on the operational level (using CORAS diagrams [20, p. 1]). Subsequently, phases are discerned based on the correlation of actions within the chain of events using the building blocks offered by the previously identified phases (or tactics). The sequences of phases observed in actual attacks form the *attack specific kill* *chains* for each attack path in the Red Team case studies. This method to develop attack specific kill chains not only allows the UKC to be evaluated thoroughly, but also to be improved iteratively through each application of the model to each of the three Red Team case studies. Collectively, the attack specific kill chains are used to formulate a "*Red Team Kill Chain*", which displays the tactics in the Red Team repertoire in their ordered arrangement, and to realign and improve the UKC.

Thirdly, public forensic reports are studied to model the phases in the attacks of APT28, using the building blocks offered by the previously identified phases (or tactics). Given the limited availability of technical details regarding compromised systems and attacks paths in individual attacks, the available data is used to develop and select likely *attack specific kill chains* and to develop a *threat actor specific kill chain*. These kill chains are used to evaluate and refine the UKC, that was first developed through literature research and improved through the Red Team case studies.

The developed Red Team and APT28 kill chains are validated using semi-structured interviews. In the case of attacks by Fox-IT's Red Team, validation takes place through semi-structured interviews with Fox-IT's Red Team lead, who performs attacks and drives the Red Team forward by incorporating new TTPs into its MO. In the case of APT28, the validation takes place through a semi-structured interview with an intelligence analyst of Fox-IT who has persistently tracked, analyzed and documented the MO of this specific threat actor.

After the case studies have been performed and the Red Team and APT28 attacks have been analyzed and modeled using kill chains, the existing and developed kill chains are compared to identify notable convergences and divergences. The presence or absence of an identified Unified Kill Chain (UKC) phase in the Cyber Kill Chain (CKC), Red Team Kill Chain (RT KC) and the APT28 Kill Chain (APT28 KC) respectively may lead to different conclusions for this research study:

Table 2 - Conclusions or "Truth" Matrix

Presence of UKC Phase	In RT KC & In APT28 KC	In RT KC & Not in APT28 KC	Not in RT KC & In APT28 KC	Not in RT & Not in APT28 KC
In the Cyber Kill Chain	Phase may be sufficiently modeled by CKC and sufficiently emulated by RT	Phase may be superfluously modeled by CKC and superfluously emulated by RT	Phase may be sufficiently modeled by CKC but is not sufficiently emulated by RT	Phase may be superfluously modeled by CKC
Not in the Cyber Kill Chain	Phase is not sufficiently modeled by CKC but may be sufficiently emulated by RT	Phase may be superfluously emulated by RT	Phase is not sufficiently modeled by CKC and is not sufficiently emulated by RT	Phase may not be required to model attacks

Insights into points of convergence and divergence between the UKC, CKC, RT KC and APT28 KC are relevant to improve threat modeling (using the CKC) and threat emulation (by Red Teams). This allows organizations to prioritize and (re)align their defensive efforts to improve their security posture and resilience against APT28 attacks. The research that is performed in this thesis is based on a limited sample of one Red Team and one APT. Nevertheless, the case studies in this thesis may prove sufficient to falsify the claim that every phase of the CKC must be executed in the strict posited sequence in a successful attack. Furthermore, the results from this limited sample of threat actors may also be indicative for the MO of other Red Teams, APTs and even other categories of threat actors, which is reflected upon (section 6.5) and could be the subject of follow-up research.

1.4.3 Incorporating the Guidelines for Design Science

The kill chain models that are developed as part of this research thesis are abstractions and representations of the MO of various real-world attackers [21, p. 77]. The construction of models aids in "problem and solution understanding and [...] represents the connection between problem and solution components" [21, pp. 78–79]. Within the context of this thesis, the kill chain models represent the connection between advanced attacks by APTs (the problem) and the defensive actions and controls (the solution components) that may be available to strengthen the security posture and resilience of organizations.

The development of these kill chains occurs within the design-science paradigm and is therefore guided by Hevner's guidelines for design science in information systems research [21, p. 83]:

1. **Design as an Artifact**: this research study aims to (re)design purposeful artifacts, namely kill chain models that can represent the end-to-end modus operandi of various real-world attackers to support analysis, comparisons and defense, as described in section 1.3;
2. **Problem Relevance**: the goal for the (re)design of the kill chain artifacts is utility, in the form of a strengthened security posture and resilience against the high-profile and impactful attacks of APTs, as described in section 1.2;
3. **Design Evaluation**: the UKC that is first (re)designed through a literature study is evaluated and improved iteratively through observational case studies [21, p. 86], in which attack and threat actor specific kill chains are developed. The validity of the resulting kill chain models is validated through semi-structured interviews, as described in section 1.4.2;
4. **Research Contributions**: the (re)designed kill chain models enable the solution of a heretofore unsolved problem [21, p. 87], that is preventing, detecting and responding to end-to-end attacks by APTs. The (re)designed models also enable the comparison between attacks from different actors, which allows for the comparison between APT and Red Team attacks and consequently the improvement for threat emulations;
5. **Research Vigor**: to approach the (re)design rigorously, the (re)design process is approached from multiple perspectives. The UKC is first developed through literature research. Subsequently, the UKC is evaluated and improved by developing attack and actor specific kill chains, which are developed through the chain of events of attacks, as described in section 1.4.2.
6. **Design as a Search Process**: the research design allows for the iterative improvement of the kill chain models. The first proposal for a kill chain is developed through literature study, which is iteratively improved through case studies that start with transparent attacks by Fox-IT's Red Team and work towards the attacks of APT28, as described in section 1.4.2;
7. **Communication of Research**: this thesis aims to describe the search process for (re)designed kill chains in a way that allows both technology- and management-orientated readers to grasp its concepts. For this reason, this thesis starts with a conceptualization and contextualization of its foundational concepts in section 1.1 and a glossary is included in Appendix E. The search process, as well as the significance of the kill chain artefacts in which this thesis culminates, will be the subject of a course day within the ICT Systems class of the Cyber Security executive master's degree at the Cyber Security Academy.

1.5 Thesis Structure

In this first chapter the topic of the thesis was introduced. Firstly, the foundational concepts underlying this thesis were conceptualized and contextualized. Secondly, the problem space was described, in which existing models and ethical hackers may fall short of modeling and emulating APTs attacks that threaten the cyber activities on which organizations and societies depend. Thirdly, the research goal and research questions were defined, which seek to address the described problem. Fourthly, the research methodology was detailed, which guides the search process to answer the research questions through a hybrid research approach.

The remainder of the thesis is structured as follows:

- In chapter 2, the attack modeling framework is developed through literature study;
- In chapter 3, case studies are performed based on attacks by Fox-IT’s Red Team;
- In chapter 4, a case study is performed of APT28 attacks;
- In chapter 5, the UKC, CKC, RT KC and APT28 KC are compared;
- In chapter 6, the results of the research and their wider applicability are reflected upon;
- In chapter 7, the conclusions of the research thesis are described;
- In Appendix A, the final (re)designed Unified Kill Chain (UKC) is included;
- In Appendix B, the attack specific kill chains from the Red Team case studies are included;
- In Appendix C, the tactics of APT28 that were identified in forensic reports are referenced;
- In Appendix D, the questions of the semi-structured interviews are detailed;
- In Appendix E, a glossary explains the specialized terminology that is used in the thesis.

2 Modeling Framework

In the previous chapter, it was argued how traditional defensive approaches that focus on the *vulnerability* element of risk do not suffice in the protection against attacks by APTs (section 1.1.3). By better understanding the way that intrusions are performed by APTs, thereby focusing on the *threat (actor)* element of risk, the resilience of organizations against APT attacks may be strengthened. Attack models could prove beneficial to better understand how attacks are performed by APTs on a tactical level.

A variety of models may be employed to analyze attacks by APTs. For this thesis, the primary modeling tool that is used is Lockheed Martin's Cyber Kill Chain® (CKC) [3]. The CKC is often cited as the original cyber kill-chain model and has arguably attained the status of industry standard in defending against APTs [22, p. 4]. For example, the CKC is currently used by the National Institute of Standards and Technology (NIST) as a component of its Cyber Security Framework.

Despite the CKC's explicit aim to focus on APT attacks, the model has been criticized as reinforcing traditional perimeter-focused and malware-prevention thinking [2]. If the criticism is well founded, making modifications to the model may prove necessary to properly analyze end-to-end APT attacks. Since the publication of the model in 2011, various modifications have been proposed by scientific authors and cyber security professionals. In the section Cyber Kill Chain Variants (section 2.2), a concise overview of proposed modifications to the CKC is provided.

The reinforcement of perimeter-focused thinking by the CKC model may be overcome by combining the CKC with proposed variants and/or MITRE's Adversarial Tactics, Techniques & Common Knowledge for Enterprise (hereafter: ATT&CK) model. The ATT&CK model focuses specifically on the attack path that can be identified after the network perimeter of an organization has been breached. The ten tactics that are identified in the ATT&CK model, which may partially overlap with proposed modifications, could provide well defined and organized building blocks in analyzing APT attacks within internal networks.

Lastly, the findings of the research performed in this chapter are used to design a Unified Kill Chain (UKC), which includes the end-to-end phases that may be identified in attacks on a tactical level. The resulting model is subsequently evaluated and improved iteratively, by applying it to several cases studies, that differ in the amount of information that is available. These include Red Team attacks (chapter 3), as well as attacks by APT28 (chapter 4).

2.1 The Cyber Kill Chain (CKC)

2.1.1 The Origin of the Cyber Kill Chain

In 2011, researchers from the Lockheed Martin Corporation developed an intelligence-driven computer network defense strategy, which has been popularized under the name The Kill Chain®. According to the Lockheed Martin researchers, conventional incident response methods are inadequate when dealing with APTs, because these methods generally rely on two flawed assumptions:

- Firstly, incident response traditionally assumes that response should happen after the point of compromise [3, p. 1]. The idealized incident response methodology [23] consists of the phases preparation, identification, containment, eradication, recovery and follow-up [24, p. 355]. The follow-up phase primarily consisted of gathering forensic artifacts for evidentiary purposes and incorporating lessons learned into policies, procedures and guidelines [24, p. 362]. While these phases may suffice to remedy common attacks, the damage inflicted by a successful APT attack may be irreversible before traditional incident response methodology commences.

- Secondly, incident response methodology traditionally assumes that incidents are the result of fixable flaws [3, p. 1]. Based on this assumption, traditional incident response methodology aims to prevent future incidents by mitigating the vulnerabilities that cause incidents [24, p. 358]. The attacks that are performed by APTs, however, frequently leverage "zero-day"[1] exploits for previously unknown vulnerabilities. Even if these vulnerabilities are subsequently mitigated by organizations, for example through patching, future attacks that abuse other zero days will typically be unaffected. Similarly, APTs frequently use advanced custom tools, that anti-virus products cannot detect or mitigate [3, p. 2].

To heed attacks by APTs, the Lockheed Martin researchers argue that an evolution in analysis, process and technology is required to anticipate and mitigate future intrusions based on knowledge of the threat [3, p. 2]. For this purpose, an intelligence-driven and threat-focused risk management strategy was developed, which analyzes attacks from the perspective of the attacker, to drive the selection of defensive courses of action [3, p. 3]. The model posits the discrete consecutive phases that APTs go through in compromising cyber assets, which can be mapped against defensive measures.

The CKC builds on existing kill chain models that are used for military purposes. Within the military context, the term "kill chain" describes an *end-to-end* process [3, p. 4], or a chain of events, that is required to perform a successful attack. Breaking a chain in this course of events would result in the failure of the attack and is thus the objective of defenders [3, p. 2]. The United States Department of Defense (DoD) Joint Staff publication 3-60, which is regarded by Lockheed Martin as its reference kill chain model, defines an attack kill chain that consists of the phases find, fix, track, target, engage and assess (F2T2EA) [25, Sec. II-21]. The DoD model describes what each step entails, defines relevant terminology, explains what the inputs and outputs of the step are and illuminates how a step relates to the other steps where necessary.

[1] The term "zero-days" refers to the amount of time that defenders have had to fix a vulnerability since it became known, for example by patching or by applying other mitigation measures. Zero-day vulnerabilities are thus by their very definition regarded as previously unknown by defenders when they are first used.

2.1.2 The Cyber Kill Chain Phases

The essence of an attack, according to the Lockheed Martin researchers, is that an “aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives” [3, p. 4]. The chain of events, or kill chain, which an external attacker must go through is defined in the CKC on a tactical level as shown in Table 3:

Table 3 - The discrete phases of the Cyber Kill Chain (CKC) [3]

Reconnaissance	• Researching, identifying and selecting targets. This may consist of *passive* reconnaisance of open source intelligence or *active* reconnaisance where internet facing systems are probed for potential weaknesses.
Weaponization	• Coupling a remote access trojan with an exploit into a deliverable payload. Typically PDF or Microsoft Office documents can serve as the weaponized deliverable for the malicious payload.
Delivery	• Transmitting the payload to the targeted environment. Prevalent delivery vectors include e-mail attachments, malicious websites and removable media such as USB.
Exploitation	• Exploitation triggers the intruders' payload. Exploitation may target vulnerability or feature in an application or the operating system. Exploitation can also involve social engineering to target a user directly.
Installation	• Installing a remote access trojan or backdoor on the system allows an attacker to maintain their presence in the target environment even if the compromised system is rebooted.
Command & Control	• Beaconing outbound to an Internet controller server to establish a Command & Control (C2) channel. The channel provides attackers with direct remote access to the compromised system in the target environment.
Action on Objectives	• Taking actions on the original objectives, such as exilftration of confidential data, the violation of data integrity or availability, or compromising additional systems and moving laterally inside the network.

2.1.3 The Attacker-Defender Balance

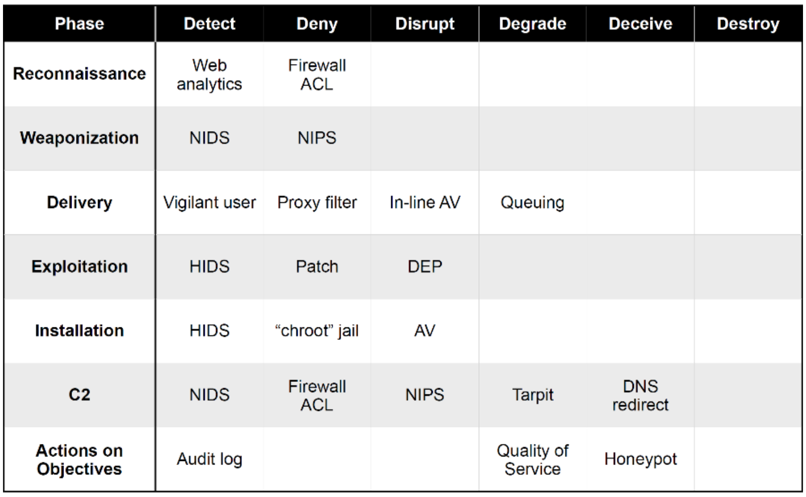
A conventional belief in cyber security is that attackers fundamentally have the upper hand [26, p. 1]. Attackers only need to find one flaw to succeed, while defenders need to do everything right to prevail, according to this often-heard defeatist adage. The CKC challenges this assumption and provides defenders with a model to stop APTs from compromising cyber assets beyond remediating all possible vulnerabilities. In contrast to the widely held belief, APT attacks are not singular events but phased progressions [3, p. 3]. These attacks thus consist of discrete phases, during which a multitude of correlated vulnerabilities must be exploited to pave a path towards a target. Defenders may prevail by disrupting just one of the consecutive phases in this chain of events [3, p. 2]:

> “*the adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary*”

Consequently, the CKC model suggests a fundamentally different balance between attackers and defenders, where one successful mitigation by defenders can thwart a complex and multi-phased attack. The model can even be leveraged to use the persistent nature of APTs against them, overturning persistence from a strength into a potential weakness. More specifically, if APTs show any observable repetition during any of the phases of their attacks, this may lead to their detection in future attacks. The application of the CKC has shown that repetition in the MO of attackers can lead to detection, even when a zero-day exploit is used in an attack [3, p. 11]. Response can then take place before critical cyber assets are compromised and the APT reaches its objective(s).

2.1.4 Defensive Courses of Action

Using the CKC, defensive courses of action can be mapped to each of the attack phases (Figure 4). By helping to find (the most) effective ways to stop APTs during one of the phases of an attack, the CKC can be beneficial in allocating defensive efforts. For this purpose, the CKC refers to the Department of Defense information operations doctrine, which defines the defensive options as a detect, deny, disrupt, degrade, deceive or destroy [27].



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Figure 4 – Courses of defensive action matrix for the CKC phases [3]

Alternatively, a defensive approach may be formulated along the lines of NIST's Cyber Security Framework, which is more tailored to the cyber context. The options that are available to defenders could then be defined as know, prevent, detect, respond and recover [28], which may be more familiar to cyber security professionals.

2.2 Cyber Kill Chain variants

2.2.1 Critiques of the Cyber Kill Chain

Since the publication of the CKC, it has been widely adopted. Organizations base their security and resilience efforts against APT attacks on the model, while the cyber security industry aligns its products and services with the phases of the model. Even though the CKC has arguably attained the status of industry standard in defending against APTs, the model has also been criticized and various modifications have been proposed.

The most damaging critiques of the CKC are that it reinforces traditional perimeter-focused and malware-prevention thinking, because that is precisely what the model aims to overcome. The first 6 phases of the 7-phased model describe the steps that lead to the compromise of one endpoint within a network, which may take hours or days. The 7th phase (*Action on Objectives*), encompasses all the further steps that may be required by an APT to achieve their objectives within the target network, which could take months [2]. Furthermore, the first 6 phases accurately describe the steps that are required in a malware-based attack, but may not be suited for attacks that leverage remote access, social engineering or those performed by insiders.

> "*The Intrusion Kill Chain is excellent for attacks, but doesn't exactly work for insider threats*" [29]

The criticisms that the CKC is too focused on the perimeter and on the malware attack vector are complementary. The malware-focus critique points out that other attack vectors may also provide attackers with initial access to the target network. The perimeter-focus critique points out that the CKC does not explicitly model the distinctive phases that subsequently occur within the target networks, namely after the initial compromise of one endpoint and before the achievement of the APT's objectives. The application of the CKC on case studies may thus show that the CKC phases does not cover all available attack vectors and insufficiently models what occurs within internal networks of targeted organizations.

2.2.2 Proposed Improvements and Amendments

Both scholars and cyber security professionals have proposed improvements and amendments to the CKC to remedy the identified shortcomings. The proposed modifications may support the expansion of the model to cover the perspective of an insider. This extension is thought to be crucial, given the plethora of attack vectors that can result in an insider-equivalent level of access to the internal network. This includes (spear) phishing attacks, but also a range of other attacks vectors that for example target physical security, BYOD (Bring Your Own Device) or the integrity of supply chains:

> "*Given the inevitability of a successful attack that breaches the internal network [perimeter], corporations need to develop a strategy for dealing with attackers inside the firewall. They need to think of every attacker as [a] potential insider*" [30]

Hereafter, four prominent revisions of the CKC are discussed, to discern what improvements and amendments their authors propose[2].

2.2.2.1 Laliberte's Kill Chain

A variant of the CKC was proposed by Laliberte (Figure 5), that aims to model the attack vector "drive-by downloads". These types of attacks leverage infected websites (or malicious advertisements) to target outdated software on systems of its visitors, typically to deploy malware. Watering hole attacks similarly use this technique against a more targeted group of users [31, p. 17].

Laliberte argues that the *Weaponization* phase of the CKC is superfluous, because it cannot be defended against. Instead, the addition of a Lateral Movement phase is proposed, which occurs between the phases Command & Control and Action on Objectives. According to Laliberte, Lateral Movement entails moving on to bigger targets on the target network after initially compromising one system in the network [32].

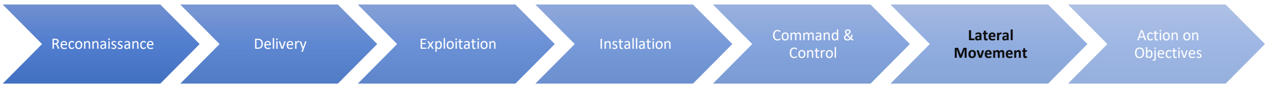


Figure 5 – Laliberte's Kill Chain

2.2.2.2 Nachreiner's Kill Chain

Nachreiner also opts to remove the *Weaponization* phase from the CKC in his kill chain (Figure 6), because he argues that phases should be actionable by defenders. The phase Installation is replaced by *Infection* without an explicit argument, but may underline the variety of persistence methods that are available to attackers.

To cover how APTs can leverage their initial access to a target network to spread within that network, Nachreiner proposes to explicitly add Lateral Movement as well as Pivoting to the Action on Objectives phase [33]. Pivoting describes the act of tunneling traffic through one system to connect to other internal systems that may otherwise be inaccessible. One could argue that some of the benefit of the addition of Lateral Movement and Pivoting is lost when these phases collapse into Command & Control, similarly to how Action on Objectives in the CKC already encompasses all

[2] To demarcate the proposed modifications in this section more clearly, proposed improvements or the removal of existing Cyber Kill Chain phases are identified with *italics*, while phases that are added to the Cyber Kill Chain are underlined in text sections and use a black font in figures.

actions that occur within internal networks.

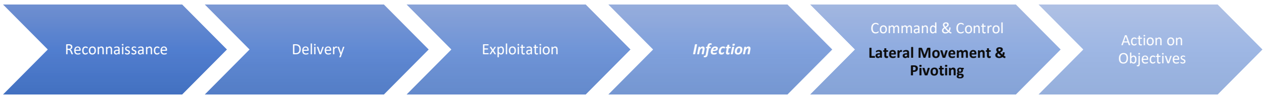


Figure 6 – Nachreiner's Kill Chain

2.2.2.3 Bryant's Kill Chain

In line with Laliberte and Nachreiner, Bryant proposes a kill chain model (Figure 7) that omits the *Weaponization* phase, because it "occurs outside the victim's network and is not likely to be observed with sensor data" [34]. According to Bryant, *Exploitation* occurs throughout the phases Delivery, Installation and Privilege Escalation and does not warrant a dedicated phase. Similarly, the *Command & Control* phase is removed, as the phases Delivery, Installation, Lateral Movement or Exfiltration may already exhibit evidence of remote command and control.

Bryant proposes to amend the CKC with the phases Privilege Escalation and Lateral Movement. During the Privilege Escalation phase, the segregation between the routine user environment and privileged account data is breached. In Bryant's terminology, the Lateral Movement phase is introduced to differentiate between "activity originating from an external network [reconnaissance] and reconnaissance activity from an internal network" [34], which notably differs from Laliberte's use of the same term (section 2.2.2.1). Lastly, the phase Exfiltration is added to emphasize the possibility to detect anomalous data transfers originating from the internal network to an external network.

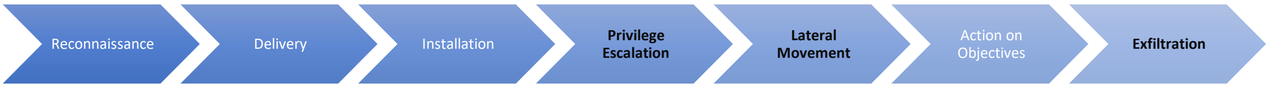


Figure 7 - Bryant's Kill Chain

2.2.2.4 Malone's Kill Chain

The most extensive expansion of the CKC is proposed by Malone, who leaves the initial model intact but expands it with two additional chains. Malone describes the CKC as appropriate to describe the breach of the enterprise network perimeter (Figure 8), after which an internal kill chain is executed to gain access to target systems that is common to most objectives (Figure 9). Malone posits that the internal kill chain consists of the phases Internal Reconnaissance, Internal Exploitation, Enterprise Privilege Escalation, Lateral Movement and Target Manipulation [35].

Subsequently, a target manipulation kill chain is described by Malone (Figure 10), which is objective-specific and allows an attacker to manipulate the target systems to achieve their objectives. Since these phases are objective-specific and occur within a single system, they may be less useful for defenders than the commonly shared phases that are described in Malone's internal kill chain (Figure 9).

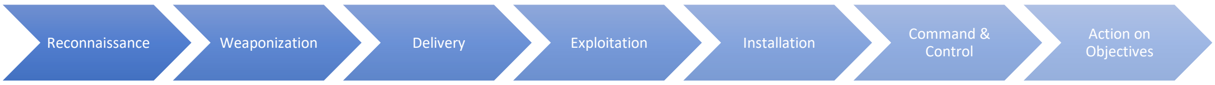


Figure 8 – Lockheed Martin's Cyber Kill Chain (CKC)

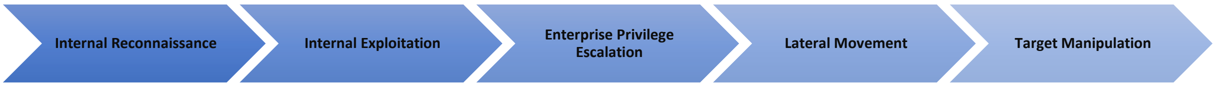


Figure 9 – Malone's Internal Kill Chain

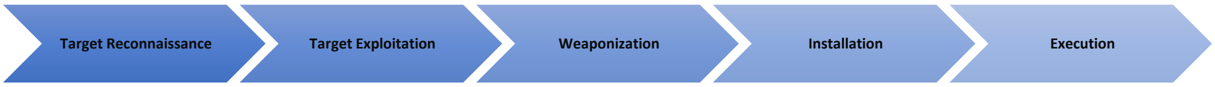


Figure 10 - Malone's Target Manipulation Kill Chain

2.2.3 Convergences and Divergences Between Models

The revised kill chain models that are proposed by Laliberte, Nachreiner, Bryant and Malone show notable convergences and divergences. For example, three of the four authors propose to remove the *Weaponization* phase from the CKC, because they argue it occurs outside the locus of control of defenders. Based on the previously discussed literature, requirements can be posited for activities to be regarded as a phase of an attack in a kill chain model:

- The attack phase should describe a *tactic* in its ordered arrangement (section 1.3.2);
- The attack phase should be *logically distinct* from other attack phases;
- An attack phase should be *relevant*, *observable* and *actionable* for defenders (section 2.2).

An attack phase is thus regarded as the execution of tactic that is logically distinct within the chain of events of an attack, which is relevant for defenders because it is observable and actionable.

All four authors attempt to expand the CKC to include the phases that occur within internal networks after the initial compromise of a system, addressing the perimeter-focus critique. Their models all include a form of internal Lateral Movement by attackers. However, the descriptions and place in the model of the Lateral Movement phase diverge. None of the models appear to address the malware-focus critique, which would presumably require modifying rather than extending the original phases of the CKC.

In addition to Lateral Movement, the models of Nachreiner, Bryant and Malone also discern other phases of attacks that occur within internal networks. These phases are Internal Reconnaissance, Internal Exploitation, Privilege Escalation, Pivoting, Target Manipulation and Exfiltration. The phases are visualized in Figure 11. As these phases originate from the different models that were discussed previously, they may overlap or occur in a different order. However, each of these phases may (or may not) occur within the internal networks of targeted organizations and could thus prove useful to analyze activities and demarcate phases in the case studies.

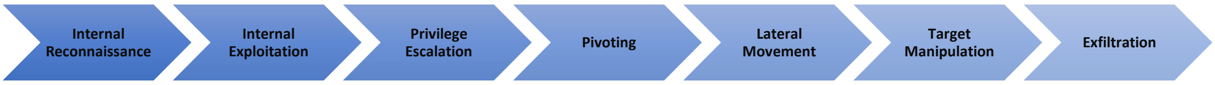


Figure 11 – Overview of All Proposed Phases

2.3 MITRE ATT&CK™

The CKC provides defenders with insight into APT attacks and allows them to align their defenses accordingly (section 2.1). However, the CKC appears to be lacking in its description of the actions that APTs perform after breaching the network perimeter within targeted organizations (section 2.2.1). The variants of the CKC that were analyzed all aim to address this deficiency, by expanding the model to cover attacker activity within internal networks of targeted organizations (section 2.2.2). The proposed models diverge in terms of the phases that are demarcated, the definition of these phases and their place in each of the models (section 2.2.3).

To facilitate the analysis of cyber attacks, such as those by Red Teams and APTs, developing a more structured approach towards and a shared terminology for these phases is needed. The Adversarial Tactics, Techniques & Common Knowledge for Enterprise (ATT&CK) framework from the non-profit research center MITRE appears particularly well suited for this purpose. The ATT&CK model "consolidates and provides concise, more complete descriptions of what cyber attackers do once inside and embedded in a computer network" [36]. The common behaviors that are included in the model are based on observed APT intrusions from public reporting and are characterized at the level of abstraction that allows for effectively prioritizing defense capabilities and investments [37, p. 4].

2.3.1 The ATT&CK™ Tactics

Within the ATT&CK model, tactics represent the highest level of abstraction and correspond with the tactical goals that an attacker has during an operation [37, p. 10]. These tactics perform a comparable function in the ATT&CK model as phases do in the CKC. The ATT&CK model defines the tactics as summarized in Table 4:

Table 4 - The MITRE ATT&CK™ Tactics [37]

Persistence	• Any access, action or change to a system that provides an attacker with a persistent presence.
Privilege Escalation	• Techniques that provide an attacker with higher permissions on a system or network.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Credential Access	• Techniques resulting in the access of, or control over, system, domain or service credentials.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Lateral Movement	• Techniques that enable an attacker to access and control remote systems on a network.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Collection	• Techniques used to identify and gather information from a target network prior to exfiltration.
Exfiltration	• Techniques that result or aid in an attacker removing files and information from a target network.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.

In contrast with the CKC, the outlined description of the tactics in the ATT&CK model is not sequential. For example, Command & Control is described lastly, but will typically be required to access other internal systems and thus to execute the other tactics. The order is not reversed either, as the objective-specific tactics Collection and Exfiltration are described just after (or before) Command & Control. To move from tactics (ATT&CK) to phases of an attack (kill chain), the dimension *time* thus needs to be added. The ATT&CK tactics could be regarded as building blocks that can be used to describe the phases that occur in an attack. Once the building blocks (tactics) are assembled in their ordered arrangement to accurately model the phases of an attack, they form the kill chain of that attack (or: an attack specific kill chain).

2.3.2 Comparison with Kill Chain Models

The tactics in the ATT&CK model can be regarded as a deconstruction of the tactical attack activities that occur within internal networks during the Action on Objectives phase of the CKC. Interestingly, the tactics in the ATT&CK model notably overlap with two of the phases that are already present in the CKC, namely Persistence (*Installation* in the CKC) and Command & Control.

When the ATT&CK model is compared[3] with the Kill Chain variants (section 2.2), it shows that four of the additional phases that were suggested (section 2.2.3) are also covered and defined by the ATT&CK model. More specifically, this applies to Internal Reconnaissance (*Discovery* in the ATT&CK model), Privilege Escalation, Lateral Movement and Exfiltration. The identified overlap strengthens the presumption that the ATT&CK tactics can serve to provide a well-structured framework to describe additional kill chain phases.

Table 5 - MITRE ATT&CK™ compared with the CKC and proposed variants

Persistence	• Any access, action or change to a system that provides an attacker with a persistent presence.
Privilege Escalation	• Techniques that provide an attacker with higher permissions on a system or network.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Credential Access	• Techniques resulting in the access of, or control over, system, domain or service credentials.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Lateral Movement	• Techniques that enable an attacker to access and control remote systems on a network.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Collection	• Techniques used to identify and gather information from a target network prior to exfiltration.
Exfiltration	• Techniques that result or aid in an attacker removing files and information from a target network.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.

The Pivoting phase however, as suggested by Nachreiner, is not explicitly demarcated in the ATT&CK model. Pivoting may be regarded as an implicit technique that is enabled by (and part of) Command & Control and is required to perform further actions such as Discovery and Lateral Movement. Target Manipulation, as proposed by Malone, is also not included as such in the ATT&CK model. Instead, the ATT&CK model includes two other tactics to describe objective-specific phases in an attack, namely Collection and Exfiltration. However, Target Manipulation may be broader than Collection and Exfiltration however, and include tactics towards other objectives such as Denial of Service. The application of the ATT&CK model to case studies can show if the Collection and Exfiltration tactics are sufficient to cover the objective-specific activities within APT attacks.

[3] In the comparison visualized in Table 5, a white font is used to mark tactics that occur as phases in the original CKC. A black font is used to mark tactics that overlap with additional phases that have previously been proposed as amendments to the CKC. A red font is used for the remaining tactics of the ATT&CK framework.

2.4 CORAS

The CORAS framework consist of a methodology, a language and a tool to perform security risk analysis [20, p. 1] using the Unified Modelling Language (UML). As such, CORAS allows for security threat and risk modeling to take place in a structured way. Intermediate results and conclusions can be represented using CORAS diagrams, that visually represent a chain of events that ultimately leads to the compromise of an asset [38].

The intermediate results within the CORAS method can be used to visualize the chain of events in attacks. The visualization of the attack using CORAS is expected to facilitate the process of discerning and mapping ATT&CK tactics to a kill chain representation of the analyzed attacks. Consequently, an adaptation of the CORAS notation is used to visualize the chain of events of Red Team attacks, so that tactics can be discerned and their sequence in the attack can be identified. In this way, attack specific kill chains can developed, using the CORAS building blocks of Figure 12 below [39].

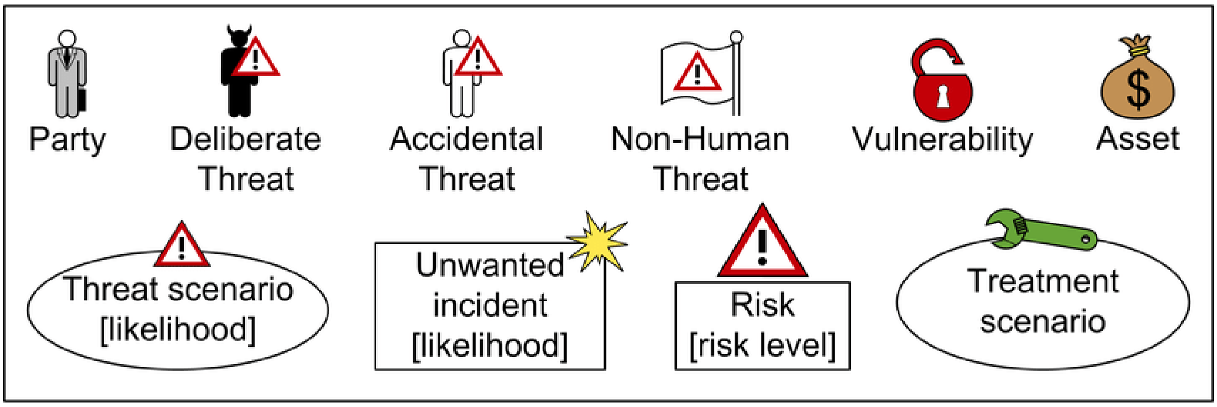


Figure 12 - Basic Building Blocks of CORAS Diagrams [39]

2.5 Uniting the Kill Chain Models

In this chapter, the strengths of the CKC were detailed first in combination with the attack phases that it identifies (section 2.1). Subsequently, the main critiques of the CKC were described, in combination with the various proposals to extend the original model to cover attack phases that occur within internal networks (section 2.2). The ATT&CK model may provide a structured and well-defined framework to extend the CKC to model attacker activities within internal networks (section 2.3).

2.5.1 Description of Formation Process

In this section, the before-mentioned models are conjoined by uniting the phases and tactics from all the examined models. The CKC serves as the primary basis to describe how attacks breach the organizational network perimeter. The ATT&CK model and the Kill Chain variants are used to describe the path within internal networks that is followed to ultimately achieve the objectives. Collectively, they form the first version of the Unified Kill Chain (UKC) in Table 6 in the next section. The UKC is evaluated and iteratively improved through the application of the model to case studies in the following chapters.

In light of the preliminary findings of the examinations of the CKC, the kill chain variants and the ATT&CK model, some further design decisions are made which are not trivial and are hence described sequentially hereafter:

- The UKC incorporates all previously identified phases from the different models insofar as possible to retain the maximum explanatory power for the case studies. However, evident overlap between phases is prevented where necessary;
- While the tactics of the ATT&CK model serve a comparable purpose to the phases of the CKC, they are not presented in a sequential order. Based on personal experience in performing attacks as an ethical hacker, the tactics of the ATT&CK model are placed in the sequence within which they are presumed to occur, which is tested in the case studies;
- The description of all phases was rephrased to one-liners, to be as concise as possible without losing relevant information;
- The Weaponization phase of the CKC was retained despite the identified criticism on this stage, to allow its (lack of) added value to be tested during the case studies;
- Defense Evasion may occur throughout the attack, but becomes particularly important behind the network perimeter. From that point onwards, an attacker stands to lose the access that was acquired, which raises the stakes. Consequently, the Defense Evasion phase has been added between Weaponization and Delivery;
- The description of the Exploitation phase of the CKC was rephrased to emphasize that exploitation of a vulnerability (or feature) may, amongst others, result in code execution;
- The Installation phase of the CKC may also be described as Infection (Nachreiner) or Persistence. The last term, and its definition by MITRE, is phrased in the broadest sense and are therefore expected to cover the most techniques to acquire persistence.
- The Command & Control phase (CKC) and tactic (ATT&CK) were conjoined into one phase, which serves as a linking pin between models and the external and internal parts of the UKC;
- The Pivoting phase from Nachreiner is included as a building block to describe actions specifically aimed at tunneling traffic towards systems that are not directly accessible, which could also apply later in kill chains (to access segmented objective-specific systems);
- The Target Manipulation phase from Malone is included in addition to the Collection and Exfiltration phases, as it may cover a broader range of objectives (such as Denial of Service).

2.5.2 Description of initial Unified Kill Chain

Table 6 provides an overview of the initial Unified Kill Chain, as developed in section 2.5.1, which unites the Cyber Kill Chain® (CKC) and proposed kill chain variants with MITRE's ATT&CK™ model.

Table 6 – The first Unified Kill Chain developed through literature study

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Coupling a remote access trojan with an exploit into a deliverable payload.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on a system or network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Credential Access	• Techniques resulting in the access of, or control over, system, service or domain credentials.
Target Manipulation	• Techniques aimed at manipulation of the target system to achieve the objective of the attack.
Collection	• Techniques used to identify and gather information from a target network prior to exfiltration.
Exfiltration	• Techniques that result or aid in an attacker removing files and information from a target network.

3 Case Study: Fox-IT's Red Team

In this chapter, the MO of Fox-IT's Red Team is analyzed to evaluate and improve the Unified Kill Chain (UKC). A brief description of the actor is included first, that outlines the objectives and incentives that apply to the Red Team. These objectives and incentives drive the formation of the attack strategy and may affect the applicability and sequence of phases within the kill chain.

The MO of the Red Team is analyzed in three different ethical hacks. The MO covers end-to-end attacks, in the sense that they start from the perspective of an unauthorized outsider and result in the compromise of critical supporting ICT assets. The MO in the attacks is visualized using CORAS, to facilitate the demarcation of phases within attacks. Afterwards, the attack specific kill chains are compared and combined into an actor specific kill chain, which is used to realign the UKC. The chapter concludes with a validation of the developed kill chains through a semi-structured interview.

3.1 Actor Description

Red Teams can operate as dedicated teams within large organizations, or may be offered as a service by the security industry. Fox-IT is part of the security industry and provides products and services to a variety of organizations. The company helps to protect its customers, in accordance with its mission "For a more secure society". The services offered include penetration testing and Red Team assessments, which are operated by the Audits & Readiness department. The department consists of over a dozen ethical hackers, who are teamed up for Red Team assignments based on their availability. Internal knowledge sharing systems and procedures aim to ensure a constant MO and quality of threat emulations. The Red Team assessment is intended to provide customers with [40]:

1. A threat simulation using Tactics, Techniques and Procedures (TTPs) of real-world attackers;
2. A maturity assessment of an organization's security posture to improve resilience;
3. A detectability analysis of actions that were detectable on hosts or the network level;
4. A risk analysis of identified vulnerabilities with detailed recommendations for improvements.

The success of Fox-IT's Audits & Readiness department and of individual employees is measured using Key Performance Indicators (KPIs). One of the main KPIs is the Net Promoter Score (NPS), which indicates how likely a customer is to recommend Fox-IT's services to a colleague or third party[4]. The NPS may be incorporated in both departmental and individual performance evaluations. The more pleased a customer is with a Red Team assignment, the higher the NPS is expected to be. Similar incentives are expected to apply to other Red Teams. Consequently, Red Teams are incentivized to satisfy the desires of their clients with their assessment, while they are also expected to strive for objectivity in the assessment.

One way for a Red Team to meet the desires of clients while striving for objectivity is to execute more thorough tests, to deliver more comprehensive reports. Clients expect value for their money, which they may measure in terms of the amount and severity of vulnerabilities identified, which incentivizes the Red Teams to perform more thorough testing and to identify multiple attacks paths. However, performing more thorough testing generally entails performing more potentially detectable actions. Furthermore, clients generally want to minimize the risks of disturbance to production systems resulting from the test. As a result, a Red Team may be less inclined to perform actions that could potentially affect critical production systems. These incentives can inadvertently negatively affect the predictive value of Red Team assessments.

[4] The NPS is based on answers to the survey question: "*How likely is it that you would recommend Fox-IT's services to a colleague or a third party?*"

3.2 Case Study 1 (C1)

The attack visualization in Figure 13 below shows how the Red Team compromised a critical supporting ICT asset from an unauthorized and external perspective in an assessment. The attack visualization is directly based on the Attack Path section of the corresponding Red Team report, that describes the chain of events of the attack on a tactical level. The attack visualization is typical for attacks that use the *(spear) phishing* attack vector to breach the network perimeter.

3.2.1 Attack Visualization

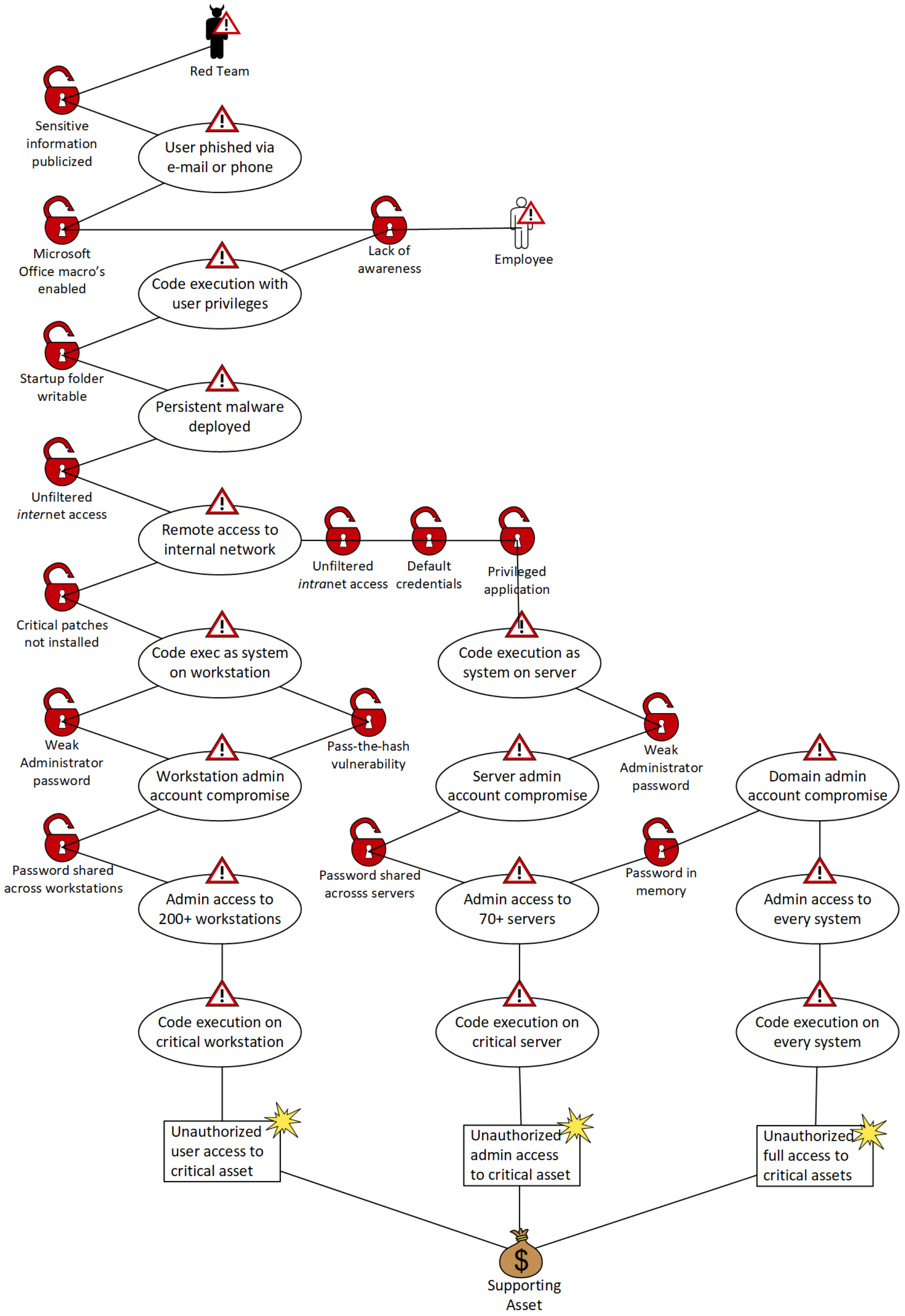

Red Team
Sensitive information publicized
User phished via e-mail or phone
Microsoft Office macro's enabled
Lack of awareness
Employee
Code execution with user privileges
Startup folder writable
Persistent malware deployed
Unfiltered internet access
Remote access to internal network
Unfiltered intranet access
Default credentials
Privileged application
Critical patches not installed
Code exec as system on workstation
Code execution as system on server
Weak Administrator password
Pass-the-hash vulnerability
Workstation admin account compromise
Server admin account compromise
Weak Administrator password
Domain admin account compromise
Password shared across workstations
Password shared acrosss servers
Password in memory
Admin access to 200+ workstations
Admin access to 70+ servers
Admin access to every system
Code execution on critical workstation
Code execution on critical server
Code execution on every system
Unauthorized user access to critical asset
Unauthorized admin access to critical asset
Unauthorized full access to critical assets
$
Supporting Asset

Figure 13 - Attack visualization of a (spear) phishing approach to breach the network perimeter

3.2.2 Attack Analysis

In the Attack Analysis section, the tactics, techniques and procedures (TTPs) that were used in this attack are described in more detail sequentially, based on the customer report and the supporting technical data. Supporting technical data includes full packet captures, console logs and screenshots from the Red Team systems. When the description of a TTP can be linked directly to a description in the Unified Kill Chain (UKC), the name of the relevant phase is underlined. This allows for the identification and demarcation of the phases of the attack, to form attack specific kill chains.

Attack preparation: open source intelligence & setting up the infrastructure

1. First, the target organization was passively researched through open source intelligence (OSINT). Information was gathered in preparation of further attacks, including the domains used by the target organization and contact information of employees (*Reconnaissance*).
2. The customer specific attack infrastructure was set-up, which included:
   - Registering domain names that were notably similar to the primary domains of the customer, but which contained typing errors (a technique known as *typo squatting*).
   - Setting up a mail server to send phishing e-mails and a command & control server to receive so-termed back-connects from shells on compromised systems using the registered domains.
   - Preparing a trojan horse, which appeared to be a legitimate document but resulted in execution of a payload once it was opened and Microsoft Office macros were enabled (*Weaponization*). The lightweight first stage of the payload (also known as the *dropper*) was specifically designed to download a second stage: a Remote Access Trojan (RAT). The RAT connected back to a command and control server and allowed pivoting, the remote execution of commands and additional code. Creating a multi-staged delivery method limited the probability and the exposure of the malicious code to defenders (*Defense Evasion*).

Phishing foothold: remotely compromising an employee workstation

3. Previously identified employees were targeted via e-mail (a technique known as *phishing*) and by phone (a technique known as *vishing*). A document was attached to an e-mail (phishing) or available on a typo squatted domain (vishing) and contained the first stage of the payload (*Delivery*).
4. The targeted employees were enticed to open and enable macro's in a document that functioned as a trojan horse, which resulted in the execution of the first stage of the payload (*Social Engineering*).
5. The first stage of the payload consisted of a dropper, which downloaded the second stage which consisted of a Remote Access Trojan (*Delivery*).
6. The RAT was dropped into the Startup folder of the affected user, to ensure that the RAT was executed as part of the startup procedure (*Persistence*).
7. Once the RAT was executed, it connected back to the command and control server and provided remote access to the compromised machine with the privileges of the affected user (*Command & Control*).

Internal attack path 1: internally compromising critical workstations

8. Remote access to the compromised workstation allowed the Red Team to actively investigate the system itself and passively monitor regular traffic to other systems within the internal network. Furthermore, information was actively obtained from the Active Directory, and internal wiki and individual systems, which provided information about the users and

groups within the organization, the roles of individual employees and where active users were logged in (*Discovery*).

9. The RAT was initially running with the privileges of a regular user. Through the discovery techniques, it was established that critical security patches had not been applied to the system. One of these vulnerabilities was exploited to escalate to the privileges of a local system administrator (*Privilege Escalation*).
10. As a local system administrator on a Windows machine, it was possible to extract password hashes of local users. The password hash could be used directly for authentication purposes (using a technique known as *pass-the-hash*), which makes the hash a password equivalent. This was not necessary, as the original password could be retrieved through an offline brute force attack on the password hash, which revealed a weak password (*Credential Access*).
11. The compromised workstation was used to tunnel traffic towards other workstations in the internal network (*Pivoting*).
12. The compromised local administrator credentials were used to authenticate to other workstations, which revealed that the credentials provided administrative access to at least 200 workstations (*Lateral Movement*).
13. Using the information obtained in step 8, the workstation of a specific employee was identified who had user level access to one of the critical supporting ICT assets. On the workstation of this specific employee, a RAT was deployed (*Execution*).
14. The plain text user level credentials to the supporting asset were extracted from memory on the workstation of the specific employee (*Credential Access*).
15. The credentials provided the Red Team with remote user level access to the critical supporting asset, of which a screenshot was made (*Action on Objectives*). Since the objective was ambiguously defined and it was unclear if user level access to the supporting asset sufficed to obtain the 'flag', further access was sought.

Internal attack path 2: internally compromising critical servers

16. Command and control of the initially compromised workstation, as obtained in step 7, allowed the system to be used as a pivot point for traffic that was relayed to other internal systems (*Pivoting*).
17. Network segments that contained servers were scanned for open TCP ports, which indicated the presence of accessible network services. Subsequently, the specific services were probed for the presence of potential vulnerabilities (*Discovery*).
18. After the discovery of an administrative web interface of a JBoss application server, factory default credentials were used to gain administrative access to the application (*Privilege Escalation*).
19. Standard functionality in the JBoss application was used to deploy a Web Application Resource (WAR) file, which allowed the execution of custom Java code, to obtain a command shell on the targeted server with administrative privileges (*Execution*).
20. As a local system administrator on a Windows machine, it was possible to extract password hashes of local users. The password hash could be used directly for authentication purposes (using a technique known as *pass-the-hash*). This was not necessary, as the original password could be retrieved through an offline brute force attack on the password hash, which revealed a weak password (*Credential Access*).
21. The compromised local administrator credentials were used to authenticate to other servers. The authentication scan revealed that the credentials provided administrative access to at least 70 servers (*Lateral Movement*).

22. Based on the descriptive hostnames of the affected servers, it could be determined that at least one server was used as a supporting asset for one of the critical organizational processes. To evidence that administrative access had been obtained to the supporting asset, a screenshot was made of a Remote Desktop session (*Action on Objectives*).

Internal attack path 3: internally compromising practically every workstation and server

23. The administrative access to at least 70 servers, as obtained in step 21, was also used in an attempt to compromise a Domain Administrator account. For this purpose, all 70 servers were probed to determine which users were currently logged in to these affected servers (*Lateral Movement*).
24. A Domain Administrator was logged into at least one of the affected servers. Using the local server administrator privileges, a RAT was deployed on the affected server (*Execution*).
25. The RAT was leveraged to obtain passwords from system memory using the built in *mimikatz* tool, which included the plain text password of a Domain Administrator (*Credential Access*).
26. The acquired domain administrator privileges provided administrative access to any workstation, server and account that is part of the Active Directory, which was used for the organizational identity and access management (IAM). As a result, most of the flags could be obtained (*Action on Objectives*).

3.2.3 Attack Specific Kill Chain Formation

In the formation of the attack specific kill chains some non-trivial design decisions are made, which are described subsequently. These design decisions are also incorporated into the UKC (Appendix A) and are applied to all attack and actor specific kill chains that are formed subsequently.

Kill chains represent successful attack paths

The visualization and analysis of sections 3.2.1 and 3.2.2 only describe successful branches within the attack tree. During the attack, other paths were also explored, which ultimately did not lead to access to the supporting asset(s). Additional opportunities for detection and response of attacks may also exist in these unsuccessful branches of the attack tree. However, implementing further preventive controls in unsuccessful attack branches are expected to be less effective than preventive controls implemented in successful branches. The primary focus therefore remains on representing successful branches, as these are expected to offer better defensive opportunities to stop attackers from succeeding in achieving their objectives.

Definition and demarcation of phases

The attack specific kill chains could be formed with relative ease, because the building blocks offered by the phases in the UKC covered almost all the relevant activities in the analyzed attack(s). In some cases, an expanded interpretation of the description of these phases was required or a phase could benefit from a further subdivision:

- The *Weaponization* phase of the UKC is narrowly described as coupling a RAT with an exploit (based on the CKC). However, other preparatory activities that are aimed at setting up the broader attack infrastructure can also be regarded as part of Weaponization, such as typo squatting domain names for phishing purposes and setting up a command and control server. The phase is thus redefined as:

  “*Preparatory activities aimed at setting up the infrastructure required for the attack*”

- The *Exploitation* phase was defined as "*techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution*", which includes social engineering in the original definition of the CKC.

  Through social engineering techniques, in which users were enticed to perform unsafe actions by e-mail (*phishing*) and phone (*vishing*), the users were enticed to compromise their systems through vulnerable software features (rather than by exploiting security bugs). These social engineering activities occur on a different level of the cyberspace model and are logically distinct from the technical delivery and exploitation of vulnerabilities from the attacker's perspective. Raising resilience against social engineering is expected to require different controls from the perspective of defenders, such as raising user awareness of their role in securing the assets of the organization rather than hardening endpoint controls. As such the tactic is relevant, observable and actionable. This warrants the addition of a separate *Social Engineering* phase:

  "*Techniques aimed at the manipulation of people to perform unsafe actions*"

- The *Delivery* phase of the UKC was defined as "*techniques resulting in the transmission of the payload to the targeted environment*" (based on the CKC).

  In the analyzed attack, a common multi-staged Delivery tactic was used, to prevent the unnecessary exposure of code to anti-virus software. The first stage of Delivery consisted of transmission of a dropper and occurred before Social Engineering took place. The second stage of Delivery, only took place after users had successfully been socially engineered. Since the Delivery phase was intermittent and conditional on the success of the social engineering attempt, Delivery is modeled to occur both before and after Social Engineering. The definition of the Delivery phase is also refined to reflect that it is not necessarily limited to a "payload" [3], but may also include other weaponized objects such as a dropper or a link:

  "*Techniques resulting in the transmission of a weaponized object to the targeted environment*"

Tempus specialis derogat tempori generali

The building blocks that are offered by the phases in the UKC vary in their specificity and show a degree of overlap. For example, Exploitation of a vulnerability may result in code Execution that is specifically aimed at attaining Privilege Escalation. As a result, every step that involves the abuse of a bug could be labelled Exploitation of a vulnerability, which would have occurred up to 10 times in an attack specific kill chain. While performing an analysis at this level of detail could be beneficial on the operational level of abstraction, this research thesis aims to perform an analysis at the tactical level of abstraction, which focuses on how operational activities are directed to achieve the (intermediate) objectives on an attack.

Considering the above, phases were demarcated similarly to the legal maxim *lex specialis derogat legi generali*, which entails that in the interpretation of law, specific laws trump general laws. In attack modeling, the application of the maxim entails that attack activities were described using the most specific description of a phase (*tempus*) that was available. The application of the maxim focuses on what an attacker aims to accomplish tactically with the operational activities during a phase of the attack. For example, the Exploitation of a vulnerability can be used for code Execution solely to obtain Privilege Escalation, which can collectively occur within a split second in a way that is transparent for the attacker. In this thesis, these entwined activities would thus only be tactically labelled as Privilege Escalation, to simplify the resulting kill chain.

Addition of Action on Objectives

The objective of the Red Team attack is typically to provide evidence that strategically placed "flags" can be obtained. In the analyzed Red Team assignment, the level of access to the flags was not specified, which can vary from user-level access or admin-level access to specific flags to admin-level access to practically all systems (including the flags). To evidence access to the flags, while preventing the risk of disturbing production systems, regular user- and system functionalities were used to obtain access to these systems.

The phases in the UKC that model objective-specific activities, namely Target Manipulation, Collection and Exfiltration are all too invasive to properly describe the Red Team's activities. Consequently, the phase Action on Objectives from the CKC was re-introduced to replace these final phases in the three attack specific kill chains. The original description of Action on Objectives is technically oriented and describes the objectives in terms of Confidentiality, Integrity and Availability. These generalized descriptions depict the potential consequences of the level of access that was evidenced.

3.2.4 Attack Specific Kill Chains

A kill chain representation of an attack is both linear and sequential, but the attack visualization in section 3.2.1 shows that the Red Team attack has a tree-like structure. Every branch within the attack tree represents a viable attack path towards a supporting asset, each of which can be represented using a linear kill chain. A kill chain can thus be thought of as a (successful and) unique end-to-end attack path within the attack tree structure. Kill chains can be formed by chaining the phases that were described for each of the viable attack paths in section 3.2.2. On this basis, three kill chains are outlined in Appendix B, that align with the three unique successful attack paths within the attack tree:

1. Phishing foothold – paving a path for user-level access to supporting asset (C1-1)
2. Phishing foothold – paving a path for admin-level access to supporting asset (C1-2)
3. Phishing foothold – paving a path for Domain Administrator access (C1-3)

A comparison and generalization of the Red Team attack specific kill chains is included in section 3.5.1.

3.3 Case Study 2 (C2)

The attack visualization in Figure 14 below shows how the Red Team compromised a supporting asset from an unauthorized and external perspective. The attack visualization is directly based on the Attack Path section of the corresponding Red Team report, that describes the chain of events of the attack on a tactical level. The attack visualization is typical for attacks that use the *physical social engineering* attack vector to breach the network perimeter.

3.3.1 Attack Visualization

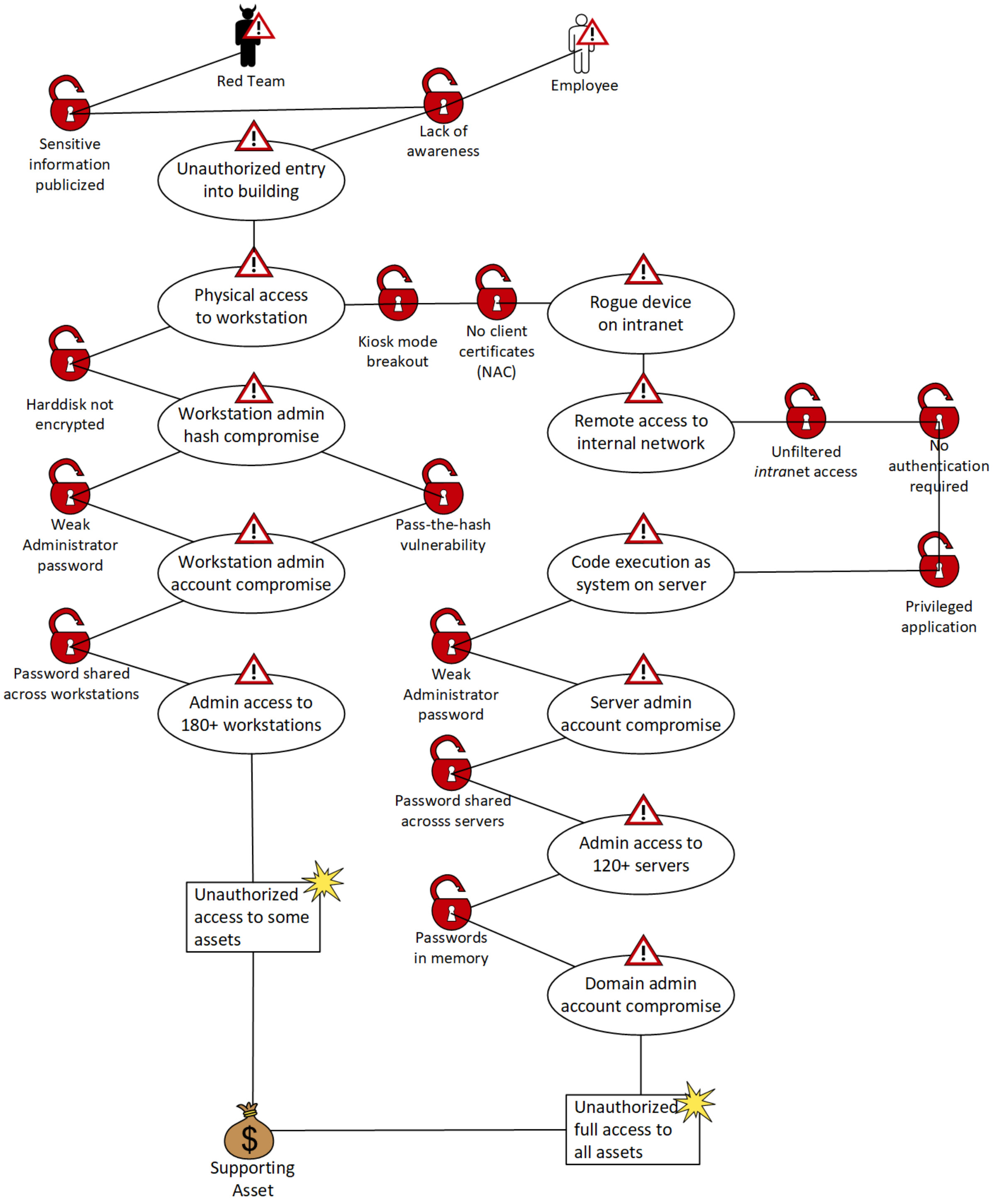

Red Team
Employee
Sensitive information publicized
Lack of awareness
Unauthorized entry into building
Physical access to workstation
Kiosk mode breakout
No client certificates (NAC)
Rogue device on intranet
Harddisk not encrypted
Workstation admin hash compromise
Remote access to internal network
Unfiltered intranet access
No authentication required
Weak Administrator password
Pass-the-hash vulnerability
Workstation admin account compromise
Code execution as system on server
Privileged application
Password shared across workstations
Weak Administrator password
Admin access to 180+ workstations
Server admin account compromise
Password shared acrosss servers
Admin access to 120+ servers
Unauthorized access to some assets
Passwords in memory
Domain admin account compromise
Unauthorized full access to all assets
$
Supporting Asset

Figure 14 - Attack visualization of physical social engineering approach to breach the network perimeter

3.3.2 Attack Analysis

In the Attack Analysis section, the TTPs that were used in this attack are described in more detail sequentially. When the description of a TTP can be linked directly to a description in the UKC, the name of the relevant phase is underlined. This allows for the identification and demarcation of the phases of the attack, to form attack specific kill chains.

Attack preparation: open source intelligence

1. First, the target organization was passively researched through open source intelligence (OSINT). Information was gathered in preparation of further attacks, which included scouting the physical locations of the organization through Google Maps and gathering potentially sensitive documents online (*Reconnaissance*).
2. Preparatory activities were performed to set up the attack infrastructure (*Weaponization*):
   - Preparing a forged document, which seemingly authorized a fictitious third party to execute an assignment on the premises of the targeted organization, using a signature from an executive that was gathered during Reconnaissance.
   - Preparing so-termed drop devices, consisting of two Raspberry Pi's with two network interfaces. The first interface could be connected to the targeted internal network. The second interface provided remote over-the-air Virtual Private Network (VPN) based access to the drop device using a 4G-dongle.

Physical foothold: tailgating for physical access to the network

3. Social engineering and *tailgating* techniques enabled unauthorized physical access to the premises of the targeted organization and to breach its network perimeter (*Social Engineering*).
4. Since Network Access Control (NAC) was enabled based on Media Access Control (MAC) addresses authentication, an Internet Protocol (IP) address could not be assigned directly to the drop devices. A vulnerability in the kiosk mode of a workstation in a meeting room was exploited to acquire its MAC-address (*Exploitation*).
5. The MAC-address of one of the drop devices was spoofed to clone the MAC-address of the meeting room workstation, which was sufficient to bypass the MAC-based authentication for the Network Access Control (NAC) (*Defense Evasion*).[5]
6. The drop devices were connected to the internal network to bridge the internal network to a remote command and control server (*Command &* Control).[6]

Internal attack path 1: leveraging physical access to compromise workstations

7. Physical access to the unencrypted hard drive of a workstation in a meeting room was exploited to acquire the password hash of a local administrator. The password hash could be used directly for authentication purposes (using a technique known as *pass-the-hash*), which makes the hash a password equivalent. This was not necessary, as the original password could be retrieved through an offline brute force attack on the password hash, which revealed a weak password (*Credential Access*).
8. A drop device was used to tunnel traffic towards systems in the internal network (*Pivoting*).

[5] Spoofing can be regarded as a (collection of) technique(s) rather than as a separate tactic. The technique may be used to execute the tactics Exploitation, Credential Access or Defense Evasion. This aligns with the interpretation of MITRE, when asked to contextualize "spoofing" within its ATT&CK framework [41].

[6] One of the drop devices was detected and removed within hours, because it had been connected to an outlet before a legitimate MAC-address was spoofed.

9. The compromised local administrator credentials were used to authenticate to other workstations, which revealed that the credentials provided administrative access to at least 180 workstations (*Lateral Movement*). Only the local subnet was scanned limit detectability.
10. This presumably provided the Red Team with remote user level access to supporting assets, which could affect the confidentiality, integrity and availability of data (*Action on Objectives*). Since the objectives were not clearly defined, further access was sought.

Internal attack path 2: internally compromising practically every workstation and server

11. Command and control, as established using the drop device in step 6, allowed the drop device to be used as a pivot point for traffic that was relayed to other internal systems (*Pivoting*).
12. One specific network segment that contained servers was scanned for open TCP ports, which indicated the presence of accessible network services. Subsequently, the specific services were probed specifically for vulnerable web services, as the resulting HTTP traffic was less prone to detection (*Discovery*).
13. An administrative web interface of a Tomcat application server was discovered, which was accessible without authentication and provided administrative access to the application (*Privilege Escalation*).
14. Standard functionality in the Tomcat application was used to deploy a custom Web Application Resource (WAR) file, which allowed the execution of custom Java code, to obtain a command shell on the targeted server (*Execution*). Since the application server was running with the highest privileges on the system, no further Privilege Escalation was required.
15. As a local system administrator on a Windows machine, it was possible to extract password hashes of local users. The password hash could be used directly for authentication purposes (using a technique known as *pass-the-hash*). This was not necessary, as the original password could be retrieved through an offline brute force attack on the password hash, which revealed a weak password (*Credential Access*).
16. The compromised local administrator credentials were used to authenticate to other servers in the same subnet as the initially compromised server. The authentication scan revealed that the credentials provided administrative access to at least 120 servers (*Lateral Movement*).
17. The administrative access to the 120 servers was used to execute a *mimikatz* script in memory remotely, which was directly and solely used to extract the plain text passwords from logged in users from memory. In this way, the credentials of over 1500 unique accounts were compromised, which included 3 Domain Administrators (*Credential Access*).
18. The acquired Domain Administrator privileges provided administrative access to any workstation, server and account that is part of the Active Directory, was used for the organizational identity and access management (IAM). As a result, it was presumed that the confidentiality, integrity and availability of supporting assets could be compromised (*Action on Objectives*).

3.3.3 Attack Specific Kill Chain Formation

In the formation of the attack specific kill chains, that are described in section 3.3.4 and included in Appendix B, some non-trivial design decisions are made which are described subsequently. The design decisions that were previously made, namely in sections 2.5.1 and 3.2.3, are applied in this section. The design decisions made in this section are also applied to all kill chains that are formed subsequently and to iteratively improve the UKC (Appendix A).

Defense evasion: general and specific occurrence

The evasion of defenses occurred throughout the attack in the second case study, as suggested in section 2.5.1. For example, port scans were executed in a more targeted way, in terms of the amount of systems and the amount of ports that were scanned, to prevent detection. The authentication scan only occurred in the same subnet as the compromised system, to avoid potential detection. A custom WAR-file was uploaded to a vulnerable application server, to avoid triggering anti-virus software. Likewise, the password extraction tool was executed in memory without ever touching the hard disk, to avoid triggering anti-virus software.

The evasion of defenses was presumably more apparent in the second case study, because the Red Team stood to lose the access that was acquired physically. Acquiring access through physical means is riskier for the Red Team, as team members can personally be apprehended and identified, in contrast to the relative anonymity provided by the phishing e-mail attack vector. After the first drop device had been detected (following step 6), the precautions that were taken to evade defenses to avoid detection were increased, to prevent losing the valuable physical access that had been acquired.

The second case study shows that defense evasion can occur continuously throughout the execution of multiple phases of attack. For this reason, the Defense Evasion phase was not described as a separate phase each time that defense evasion and particularly avoiding detection is considered in executing activities in the chain of events in the second case study. It is expected that the analysis of APT28 attacks of high profile targets will similarly show that the evasion of defenses occurs continuously in the execution of the phases of the attacks. This may particularly apply after an initial foothold has been established and the attackers stand to lose the level of access that they have acquired. Consequently, Defense Evasion is only modeled subsequently to describe specific activities for which the *sole* purpose is to evade defenses.

To acquire access to the internal network, it was necessary to *spoof* the MAC-address of a legitimate device. The term spoofing describes a collection of techniques in which an attacker falsifies data to illegitimately masquerade as a legitimate system or other entity [42, p. 202]. Spoofing is frequently executed to abuse weaknesses in the authentication of protocols, such as Address Resolution Protocol (ARP), NetBIOS Name Service (NBNS) and Link-Local Multicast Name Resolution (LLMNR). In the context of case study C2, the technique was used for the sole purpose of evading the protection offered by Network Authentication Control (NAC). As such, evading NAC was an end in itself and not merely a consideration in the execution of another tactic. Consequently, the spoofing technique is modeled in C2 as Defense Evasion, which occurred before Command & Control was established.

Action on Objectives phase modeled in lieu of actions on objectives

In preparation of the Red Team attack, very abstract socio-technical risks had been identified by the client. For example, one of the primary socio-technical risks was described as “intentional sabotage by an attacker that prevents [organization] from achieving its mission”. No explicit flags had been identified for the Red Team. Because of the lack of specificity of actionable objectives, the Red Team expressed risks in terms of the level of access that was acquired to general supporting assets such as workstations and servers. Further actions on the objectives were not specifically performed, as an unguided quest for high value sabotageable production systems could have had unnecessary adverse effects. Nonetheless, the Action on Objectives phase is modeled in the kill chains of case study 2, because these actions were described in the report as possible and are expected to be relevant for modeling APT attacks.

3.3.4 Attack Specific Kill Chains

Every branch within the attack tree in section 3.3.1 represents a viable attack path towards a supporting asset. Each unique end-to-end attack path is represented using a chain, by chaining the phases that were described for each of the attack paths in section 3.3.2. On this basis, two kill chains are outlined in Appendix B, that align with the two unique successful attack paths within the attack tree:

1. Physical foothold – paving a path for user-level access (C2-1)
2. Physical foothold – paving a path for Domain Administrator access (C2-2)

A comparison and generalization of the Red Team attack specific kill chains is included in section 3.5.1.

3.4 Case Study 3 (C3)

The attack visualization in Figure 15 below shows how the Red Team compromised a supporting asset from an unauthorized and external perspective. The attack visualization is directly based on the Attack Path section of the corresponding Red Team report that describes the chain of events of the attack on a tactical level. The attack visualization describes an attack that uses a *multi attack vector approach* to breach the network perimeter.

3.4.1 Attack Visualization

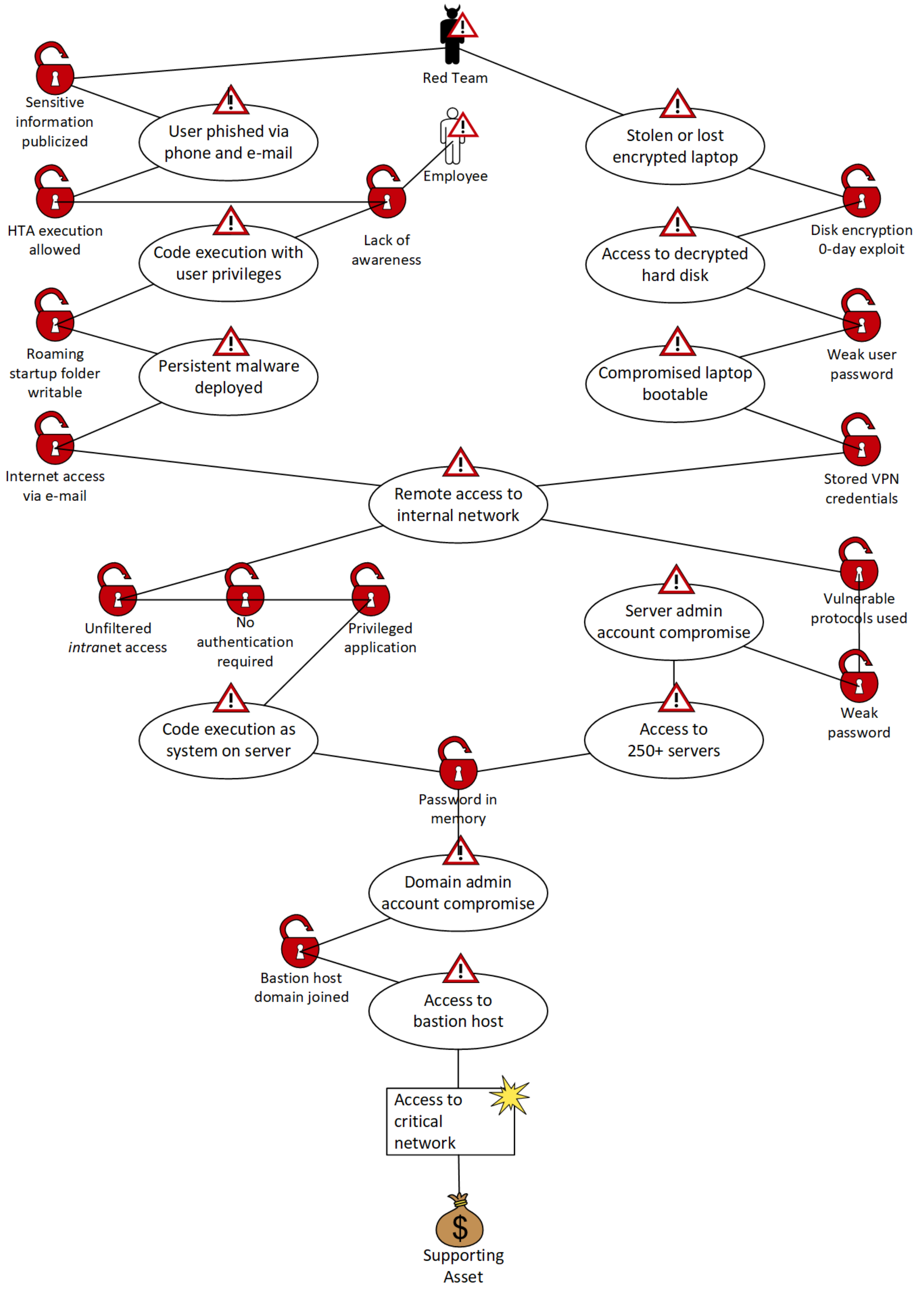

Red Team
Sensitive information publicized
User phished via phone and e-mail
Employee
Stolen or lost encrypted laptop
HTA execution allowed
Lack of awareness
Disk encryption 0-day exploit
Code execution with user privileges
Access to decrypted hard disk
Roaming startup folder writable
Weak user password
Persistent malware deployed
Compromised laptop bootable
Internet access via e-mail
Stored VPN credentials
Remote access to internal network
Unfiltered *intranet* access
No authentication required
Privileged application
Server admin account compromise
Vulnerable protocols used
Weak password
Code execution as system on server
Access to 250+ servers
Password in memory
Domain admin account compromise
Bastion host domain joined
Access to bastion host
Access to critical network
Supporting Asset

Figure 15 – Attack visualization of a multi attack vector approach to breach the network perimeter

3.4.2 Attack Analysis

In the Attack Analysis section, the TTPs that were used in this attack are described in more detail sequentially. When the description of a TTP can be linked directly to a description in the UKC, the name of the relevant phase is underlined. This allows for the identification and demarcation of the phases of the attack, to form attack specific kill chains.

Attack preparation: open source intelligence

1. First, the target organization was passively researched through open source intelligence (OSINT). Information was gathered in preparation of further attacks, which included scouting the physical locations of the organization through Google Maps and on foot, and performing digital reconnaissance through social platforms such as LinkedIn (*Reconnaissance*).
2. Preparatory activities were performed to set up the attack infrastructure (*Weaponization*):
   - Setting up a mail server to send phishing e-mails and a command & control server to receive so-termed back-connects from shells on compromised systems using the registered domains.
   - Preparing a HTML Application (HTA) file, which contained executable code, in preparation of a variant of a so-termed “Microsoft phone scam” [43]. The HTA provided a graphical user interface that emulated the interface of a virus scanner and showed the messages ‘scanning’, ‘cleaning’ and ‘success’. Meanwhile, a custom Remote Access Trojan (RAT) was deployed in the background, which was also included in the HTA.

Phishing foothold: remotely compromising an employee workstation

3. Two employees that were identified in the Reconnaissance phase received a phone call that their computer had been infected by a virus. After their initial startled reaction, they were reassured that the virus could easily be removed with a specialized tool (*Social Engineering*).
4. An e-mail was subsequently sent to the employees who had been social engineered, which supposedly contained a removal tool, but contained the custom RAT instead (*Delivery*).
5. Both employees that were targeted through social engineering proceeded to execute the HTA file on the basis of the instructions in the e-mail (*Social Engineering*).
6. To maintain persistence on the compromised workstation, a user run key was added to the Windows registry, which executed malicious code at the start of Windows (*Persistence*).
7. Since user workstations were expected not to allow direct outbound connections to the internet, e-mails that were hidden from the users were employed as a command and control channel, which provided a slow but sure way to enable remote access to the compromised machines with the privileges of the affected users (*Command & Control*).

Physical foothold: physically compromising an employee workstation

8. A laptop was received from the targeted organization to assess the risk if an encrypted and powered down laptop of an employee would be stolen or lost. Stealing a laptop is expected to require additional attack phases, namely *Reconnaissance* and *Social Engineering*, but a lost laptop could be stumbled upon without going through any preparatory attack phases.

9. The software that was used to apply full disk encryption (FDE) was analyzed, which identified a previously unknown vulnerability in its implementation of the encryption scheme. An exploit was developed to decrypt the contents of the hard disk (*Exploitation*).[7]
10. Access to the unencrypted contents of the hard disk allowed for the extraction of a cached password hashes of a domain user with administrative privileges, who had previously logged into the system, which could be cracked to reveal the password (*Credential Access*).
11. The laptop could then be booted using the acquired credentials. The affected user had access to a Virtual Private Network (VPN) application, for which credentials were stored and no second factor was required, which provided physical command and control over a client in the targeted network (*Command & Control*).

Internal attack path 1: compromising the office environment through a vulnerable server

12. Command and control, as established using the drop device in steps 7 and 11, allowed the compromised workstations (or laptop) to be used as a pivot point for traffic that was relayed to other internal systems (*Pivoting*).
13. Specific network segments that contained servers were scanned for open TCP ports, which indicated the presence of accessible network services. Subsequently, the specific services were probed specifically for vulnerable web services, as the resulting HTTP traffic is less prone to detection (*Discovery*).
14. An administrative web interface of an Apache Tomcat application server was discovered, which was accessible without authentication and provided administrative access to the Tomcat application server (*Privilege Escalation*).
15. Standard functionality in the Tomcat application was used to deploy a custom Web Application Resource (WAR) file, which allows the execution of custom Java code, to obtain a command shell on the targeted server (*Execution*).
16. The administrative access to the server was used to execute a *mimikatz* script in memory remotely, which was directly and solely used to extract the plain text passwords from logged in users from memory. In this way, the credentials of an administrator were acquired with privileges equivalent to a Domain Administrator (*Credential Access*).

Internal attack path 2: compromising the office environment through vulnerable protocols

17. Command and control, as established using the drop device in steps 7 and 11, allowed the compromised workstations or laptop to be used as a pivot point for traffic to other internal systems (*Pivoting*).
18. The internal network traffic showed multicast broadcast network traffic from systems in the local subnet using vulnerable protocols such as NetBIOS Name Server (NBNS) and Link-Local Multicast Name Resolution (LLMNR) (*Discovery*).
19. Forged NBNS and LLMNR responses were spoofed using the *Responder* tool. Consequently, the affected internal systems attempted to authenticate to the compromised system, which resulted in a challenge-response password hash for a server administrator that could be cracked (*Credential Access*).
20. The compromised administrator credentials were used to authenticate to servers in the office network segments, which provided access to at least 250 servers (*Lateral Movement*).

[7] In the execution of the third Red Team study, two previously unidentified vulnerabilities were discovered and “zero day” exploits were developed for these vulnerabilities. One of the vulnerabilities was superfluous for the formation of the attack paths towards the assets. Both “zero day” vulnerabilities were reported to the client and the product vendor in accordance with Fox-IT’s Corporate Social Responsibility policy [44].

21. The administrative access to the servers was used to execute a *mimikatz* script in memory remotely, which was directly and solely used to extract the plain text passwords from logged in users from memory. In this way, the credentials of an administrator were acquired with privileges equivalent to a Domain Administrator (*Credential Access*).

Action on Objectives: pivoting towards the critical infrastructure segment

22. The privileges acquired in steps 16 and 21 provided administrative access to any workstation, server and account that is part of the segregated office domain in the Active Directory. This included a bastion host [45] (*Lateral Movement*).
23. The bastion host was used by the client to bridge the office network to a production network for critical infrastructure. Access to the bastion host thus provided a pivot point towards this environment that was not directly connected to the internet (*Pivoting*).
24. Discovery methods were used to ascertain if unauthorized network access had been acquired to other systems in the critical infrastructure network segment through the bastion host (*Discovery*).
25. Remote access to the critical infrastructure was defined as one of the objectives of the attack. No further actions within the critical infrastructure were performed, to prevent unintended disturbances (*Action on Objectives*).

3.4.3 Attack Specific Kill Chain Formation

The phases offered by the UKC, in combination with the design decisions previously made in 3.2.3 and 3.3.3, were sufficient to model all tactics that were identified in the four unique successful kill chains in case study C3. In the formation of the attack specific kill chains, that are described in section 3.4.4 and included in Appendix B, some other non-trivial design decisions are made, which are detailed subsequently. Design decisions made in this section are also applied to all kill chains that are formed subsequently to iteratively improve the UKC (Appendix A).

Phases modeled in lieu of their occurrence

For the scenario that a laptop was stolen or lost, a laptop was provided directly to the Red Team by the targeted organization. A description of a kill chain from that point onwards only emulates the scenario where a laptop is inadvertently lost and is incidentally recovered by a skillful bystander. According to the NIST definition, APTs may use multiple attack vectors including cyber, physical and deception [7]. The stolen laptop scenario is thus thought to be more relevant than the lost stolen scenario in defending against APTs, who act with intent rather than merely rely on happenstance. Stealing a laptop is expected to require additional attack phases, namely *Reconnaissance* and *Social Engineering*, which have consequently been modelled as they are expected to be relevant for modeling APT attacks.

The relation between Command & Control, Pivoting, Discovery and Lateral Movement

The phases Command & Control, Pivoting, Discovery and Lateral Movement originate from different models and may (appear to) show a degree of overlap. The third case study pertains to a target network that is relatively well segmented and isolated, which offers an opportunity to evaluate the relation and position of these four tactics in the attack specific kill chains. It is subsequently argued that these four phases do not necessarily overlap and can in fact add explanatory power when used in conjunction. In the UKC and the previous two case studies, the phases were used as defined in Table 7.

Table 7 – Attack Phases: Origins and Definitions

Phase	Source	Definition
Command & Control	ATT&CK and CKC	Techniques that allow attackers to communicate with controlled systems within a target network
Pivoting	Nachreiner	Tunneling traffic through a controlled system to other systems that are not directly accessible.
Discovery	ATT&CK	Techniques that allow an attacker to gain knowledge about a system and its internal network.
Lateral Movement	ATT&CK	Techniques that enable an attacker to access and control remote systems on a network.

In the case studies, it was shown that the initial foothold results in command and control of a system in the internal network of a targeted organization (*Command & Control*). This level of access can be used to gain knowledge about the system and the network on a compromised system itself (Local *Discovery*). The access can also be used to gain knowledge about the system and (other systems in) the network, by performing activities that actively query other systems (Network *Discovery*). Techniques that actively query other internal systems are explicitly included in the ATT&CK framework within the Discovery tactic (such as *Network Service Scanning*) [46]. Discovery thus describes a similar activity from an internal perspective as Reconnaissance does from an external perspective.

The term pivoting was used by Nachreiner to specifically describe techniques that are used to tunnel traffic through a controlled system towards other systems in the network (*Pivoting*). Command & Control of a compromised system enables pivoting, but does not encompass pivoting. More specifically, Command & Control refers to techniques that an attacker uses to “communicate with systems under their control”[37, p. 10], while pivoting refers to network traffic directed at any reachable system (which typically is not yet under the attacker’s control). When *Network* Discovery is performed through a compromised system however, this also results in tunneled traffic which can be used to merely access other systems. It could thus be argued that Pivoting is not required as a separate phase and that Discovery should be further divided to distinguish between Local Discovery and Network Discovery.

As the third case study shows however, an attack may require multiple pivot points if networks are strictly segmented. In the third case study, a compromised workstation (or laptop) provided the first pivot point into the office environment of the targeted organization. A second pivot point, consisting of a compromised bastion host, was required to tunnel traffic towards the critical infrastructure environment. Even more strictly segmented networks could require additional pivot points. These pivot points form *choke points*, that an attacker is forced through, and can thus be crucial for the success or failure of an attack. Consequently, modeling Pivoting as a separate phase is expected to be highly beneficial to understand where these choke points occur in an attack.

Furthermore, when a separate Pivoting phase is explicitly modeled, it allows for the implicit distinction between local and network variants of the Discovery phase. More specifically, if Discovery is modeled before Pivoting occurs, it entails that local discovery methods are used that do not result in traffic towards other internal systems. If Discovery is modeled after Pivoting, the Discovery activities can result in tunneled network traffic towards internal systems[8]. As a result, it is not necessary to explicitly further divide Discovery into a local and a network variant if Pivoting is modelled separately.

The term lateral movement is frequently abused to describe all activities that attackers perform within internal networks after they obtain their initial foothold, as evidenced by Lockheed Martin's Cyber Kill Chain and (in part by) the kill chain revisions of Laliberte, Nachreiner and Bryant. Within the ATT&CK framework, the definition of the Lateral Movement phase describes techniques that enable an attacker to *access and control* other systems on a network. The use of the AND operator as a logical conjunction in this definition distinguishes Lateral Movement from Pivoting and Network Discovery, since a level of control of the targeted system is required for Lateral Movement.

To underline the *control*-requirement of Lateral Movement, and in accordance with the literal meaning of the phrase, activities are regarded in the UKC as Lateral Movement if an attacker moves through the network horizontally. More specifically, the phase describes the activities of an attacker where previously acquired privileges are used to obtain the same level of control over other systems in the network. For example, if local administrator account credentials are compromised on one system, Lateral Movement describes the phase in which these credentials are used to access and control other systems that use the same password for this account. As such, the *horizontal* escalation of privileges in the Lateral Movement phase can just be juxtaposed against the *vertical* escalation of privileges in the Privilege Escalation phase. In other words, Lateral Movement can be regarded as horizontal movement while Privilege Escalation entails vertical movement of the attacker[9].

3.4.4 Attack Specific Kill Chains

Every branch within the attack tree in section 3.4.1 represents a viable attack path towards a supporting asset. Each unique end-to-end attack path is represented using a kill chain, by chaining the phases that were described for each of the attack paths in section 3.4.2. On this basis, four kill chains are outlined in Appendix B, that align with the four unique successful attack paths within the attack tree:

1. Phishing for foothold and a vulnerable server for access to critical infrastructure (C3-1)
2. Phishing for foothold and vulnerable protocols for access to critical infrastructure (C3-2)
3. Physical foothold and a vulnerable server for access to critical infrastructure (C3-3)
4. Physical foothold and vulnerable protocols for access to critical infrastructure (C3-4)

A comparison and generalization of the Red Team attack specific kill chains is included in section 3.5.1.

[8] Similarly, the placement of the Pivoting phase can be used to distinguish between local Privilege Escalation (on the initially compromised system) and remote Privilege Escalation. For example, kill chain C1-2 describes an attack that moves from Command & Control to Pivoting to Discovery to Privilege Escalation (and thus refers to a remote form of Privilege Escalation).

[9] In special cases, the use of privileges obtained on system A may result in a higher level of privileges on system B. This case is within the realm of possibilities, but was not encountered in the case studies. Such a situation could be modelled as Lateral Movement followed by Privilege Escalation (or as Diagonal Movement).

3.5 Red Team Actor Specific Kill Chain

In chapter 2, the Unified Kill Chain (UKC) model was first developed through literature study. In this chapter, the UKC was tested against 3 Red Team based case studies (C1, C2 and C3). For all 3 case studies, attack specific kill chains were developed for each of the identified successful attack paths using the building blocks offered by the phases of the UKC. Where the explanatory power of the UKC did not suffice to analyze and demarcate phases in the attack paths, modifications were made to refine the model. The resulting meta kill chain model is included in Appendix A.

3.5.1 Red Team Kill Chain Formation

In this section an actor specific kill chain is developed, that encompasses all phases that were identified in the 3 case studies and which is included in section 3.5.2. The actor specific kill chain provides an overview of the repertoire of tactics that an attacker may employ during an attack in their expected order. When this *actor* specific kill chain is applied to a specific environment, this results in an *attack* specific kill chain, which is context dependent. In contrast to the actor specific kill chain, attack phases may occur more than once in an attack specific kill chain depending on the target environment. To better understand the relationship of phases and attack patterns within the attack paths, a sequential overview of the 9 attack paths that were identified in the Red Team case studies is included in Table 8.[10]

Table 8 – Heatmap of occurrence and sequence of UKC phases in Red Team attack paths

		Red Team Kill Chains								
#	***Unified Kill Chain***	**C1-1**	**C1-2**	**C1-3**	**C2-1**	**C2-2**	**C3-1**	**C3-2**	**C3-3**	**C3-4**
1	*Reconnaissance*	1	1	1	1	1	1	1	~~1~~	~~1~~
2	*Weaponization*	2	2	2	2	2	2	2	4	4
3	*Defense Evasion*	5	5	5	4	4	4	4	6	6
4	*Social Engineering*	4	4	4	6	6	5	5	14	14
5	*Delivery*	5	5	5	3	3	4	4	8	8
6	*Exploitation*	7	7	7	8	8	7	7	9	9
7	*Persistence*	8	8	8	14	9	8	8	11	11
8	*Command & Control*	11	9	11	9	11	9	9	13	14
9	*Pivoting*	10	11	10	12	10	11	11	10	12
10	*Privilege Escalation*	14	10	14	~~15~~	13	13	14	14	14
11	*Discovery*	9	13	9		14	10	12	12	12
12	*Lateral Movement*	12	14	12		12	14	14	9	9
13	*Execution*	13	12	13		14	12	12	11	11
14	*Credential Access*	14	15	14		~~15~~	9	9	~~15~~	~~15~~
15	*Action on Objectives*	15		15			11	11		
16	*Target Manipulation*						~~15~~	~~15~~		
17	*Collection*									
18	*Exfiltration*									

[10] The phases of the UKC progress from green before the perimeter is breached to red as critical supporting assets are breached. A black line is used to distinguish phases that occur after the initial compromise of one system behind the network perimeter (Command & Control). Phases that are modelled in lieu of their occurrence, as explained in sections 3.3.3 and 3.4.3, are ~~struck through~~. In section 3.5 and further, the more specific definition of Defense Evasion was retro-actively applied to the kill chains C1-1, C1-2 and C1-3, which do not meet the standard for Defense Evasion as introduced in section 3.3.3 of C2, to enable a more straight forward comparison.

Attack Specific Kill Chains: Length, Sequence and Patterns

In the case studies, the length of an attack specific kill chain depends on the amount of different tactics that an attacker uses to reach their objective. As such, the length of the attack specific kill chains is determined in large part by the defensive posture of the targeted organizations. The stronger the security posture, the longer the kill chain is expected to be[11]. Based on the available data including the attack visualizations, attack descriptions, attack specific kill chains and Table 8, the pattern in the modus operandi of the Red Team can be generalized as follows:

1. Firstly, the attack is prepared from an external perspective:
   - To enhance the chance of success the target is researched (*Reconnaissance*)
   - Preparatory activities are performed such as setting up the attack infrastructure (*Weaponization*)
2. Secondly, the attacker must acquire command and control of a system in the target network:
   - Users are targeted to infect a system within the perimeter (*Social Engineering*)
     - Which may require the transmission of a weaponized object to a system (*Delivery*)
     - Which may require the exploitation of a vulnerability (*Exploitation*)
     - Which may be used to acquire persistent access (*Persistence*)
   - Alternatively, physical access is acquired through social engineering to get control over a system within the perimeter (*Social Engineering*)
     - Which may require the exploitation of a vulnerability (*Exploitation*)
     - Which may result in acquiring access to credentials (*Credential Access*)
   - The systems provide remote access to the target network (*Command & Control*)
3. Thirdly, the attacker may first focus on the initially compromised system. This can consist of:
   - Gathering information about the local system (local *Discovery*)
   - Locally escalating privileges vertically to a higher level (local *Privilege Escalation*)
   - Acquiring credentials from the local system through the extraction of credentials from the hard disk or from memory (*Credential Access*)
4. Fourthly, an attacker may first or subsequently focus on compromising other systems:
   - Using the initially compromised system as a pivot point (*Pivoting*)
   - Using techniques aimed at identifying potential vulnerabilities (network *Discovery*)
   - Which may lead to the vertical escalation of privileges (remote *Privilege Escalation*)
   - Which may allow for remote code execution with the acquired privileges (*Execution*)
   - Which may allow for the extraction of credentials from the hard disk or from memory (*Credential Access*)
5. Fifthly, acquired privileges may be *iteratively* leveraged to gain further access to systems:
   - Once credentials have been acquired that provide control over other systems an attacker may horizontally escalate privileges to these systems (*Lateral Movement*)
   - Control over these systems may allow for credential extraction (*Credential Access*)
   - Credential Access and Lateral Movement may be iterated until access to supporting assets is acquired (*Action on Objectives*)

[11] This particularly applies to heavily segmented network environments, as shown in C3. In each of the C3 kill chains, the Red Team was required to go through a pivot point (or choke point) to reach a critical infrastructure segment. If the Identity and Access Management (IAM) is strictly separated along the same lines as the network infrastructure, this forces an attacker to start anew in this environment without any relevant authorizations after *Pivoting* with *Discovery*.

Actor Specific Kill Chain and Refining the Unified Kill Chain

The generalized Red Team MO is represented using an actor specific kill chain in section 3.5.2. The Red Team Kill Chain (RT KC) encompasses the unique phases that comprise the tactical repertoire of the attacker in their expected sequence, as first explained in section 1.4.2 as well as previously in this section. The RT KC is a linear kill chain representation of the tactics employed by Fox-IT's Red Team and their presumable ordered arrangement when compromise of critical assets. As Table 8 (on page 47) shows, the sequence of phases is amongst others influenced by the attack vectors and paths that are used to achieve the objectives.

The Unified Kill Chain (UKC) is iteratively refined throughout the thesis. Following the Red Team case studies, the ordered arrangement of the phases in the UKC can be similarly rearranged to the RT KC. More specifically the following changes are made to model the RT KC and to realign the UKC:

- The *Defense Evasion* phase is modelled after Exploitation and before Command & Control, based on the place where this activity occurred as an end itself, namely in C2-1 and C2-2.
- The *Delivery* phase occurred before and after Social Engineering in C1-1, C1-2 and C1-3 (spear phishing). In contrast, the Social Engineering phase occurred before and after Delivery in C3-1 and C3-2 (vishing followed by spear phishing). On this basis, Delivery is modeled before Social Engineering in the RT KC and UKC to reflect the most prevalent attack vector.
- The local *Discovery* phase occurred before local and/or remote Privilege Escalation in C1-1, C1-2, C1-3, C2-2, C3-1 and C3-3. Consequently, the Discovery phase is modelled before Privilege Escalation.
- The phase *Credential Access*, occurred before (to obtain a physical foothold) and behind the perimeter (after obtaining an initial phishing foothold) in the case studies. The most frequent occurrence of Credential Access was behind the perimeter, which corresponds with the most prevalent attack vector, so this phase is modelled to occur behind the perimeter.
- Acquiring plain text credentials from memory typically requires code execution with the highest privileges on the system. Once credentials have been obtained, these may be used to authenticate and move laterally to other systems. In accordance with the majority of the attack specific kill chains, these phases are thus modelled to occur in the order *Privilege Escalation*, *Execution*, *Credential Access* and *Lateral Movement*.

3.5.2 The Red Team Kill Chain

The Red Team Kill Chain (RT KC) encompasses the unique phases that comprise the tactical repertoire of Fox-IT's Red Team in their expected sequence, as first explained in section 1.4.2. As such, the RT KC is a threat actor specific instance of the UKC. The RT KC was formed in accordance with the generalized Red Team MO and the considerations described in section 3.5.1.

Table 9 - The Red Team Actor Specific Kill Chain (RT KC)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Delivery	• Techniques resulting in the transmission of the weaponized obejct to the targeted environment.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on a system or network.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Credential Access	• Techniques resulting in the access of, or control over, system, service or domain credentials.
Lateral Movement	• Techniques that enable an adversary to horizontally access and control other remote systems.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

3.6 Validation of Red Team Case Studies

The data, analysis and results of this chapter were validated through a semi-structured interview with Francisco Dominguez Santos, Fox-IT's Red Team Lead. The interviewee was first concisely briefed on the research question, the methodology and the specific Red Team assignments which were sampled. The interview was conducted based on 9 open ended questions (detailed in Appendix D), which left room for follow-up questions.

Dominguez exhibited knowledge of multiple attack lifecycle models, including but not limited to Lockheed Martin's Cyber Kill Chain (CKC). Dominguez stated that a kill chain model should provide decision makers with insight into the overall process and steps of an attack, which would allow them to better prioritize their investments in security capabilities. More specifically, Dominguez explained that some risks in the preventive controls could be accepted, because every organization should expect the compromise of individual systems at some point. Instead, Dominguez argued that investments should be focused on detection and response capabilities, to limit the risks that one compromised system can be leveraged to expand the compromise to other systems in the network.

The interviewee affirmed that the attack visualizations, attack analysis and the identification of tactics, the formulation of attack specific kill chains and the generalization of the Red Team MO generally provided accurate representations of the Red Team assignments. The following remarks were chronologically made regarding these elements by Dominguez:

- The attack visualization, which is represented using an interpretation of the CORAS methodology, could prove very useful to provide insight into attacks in future customer reports.
- The presence of multiple attack paths in the visualization shows that the Red Team aims to provide additional value to its customers. However, executing phases in attack paths that are redundant to achieve the objectives can inadvertently and unnecessarily raise the detectability of the attack. However, most customers struggle to detect attacks even in the face of multiple attack paths, so this downside may also provide organizations with more opportunities to practice detection and response. As such, raising detectability by identifying multiple attack paths in the execution of the attack, may be the appropriate choice in some assignments.
- In contrast to APT attacks, the Red Team attacks typically end after a certain level of access has been obtained and do not perform malicious actions towards the attacker's objectives, such as the exfiltrating objective-specific sensitive data.
- The use of zero-days is sensationalized and rarely necessary to compromise organizations.
- Access to the target network and pivoting points form bottlenecks in the attack paths, which are most clearly visualized by the attack visualization in section 3.4.1.

When asked if Dominguez regards Red Team attacks as an accurate emulation of APT attacks, Dominguez pointed out there are many relevant differences between Red Teams and APTs. Elements that differ include their strategic objectives, available resources, attacker mindset, time available, level of persistence and ethical and legal restrictions that affect the scope and possible attack vectors. Dominguez argues that it is important to retain the essence of APT attacks, namely a creative approach with as little restrictions of the scope as possible to achieve representative objectives. Given the applicable limitations, Red Team assignments are thought to be particularly useful to identify potential bottlenecks in the execution of attacks; certain points that an attacker must go through or tactics that are hard to replace in the execution of an attack.

The limitations that apply to Red Team emulations may in part be overcome if organizations provide active support in the execution of attacks. For example, legal and ethical restrictions in performing supply chain based attacks may emulated by providing a Red Team with a Virtual Private Network (VPN) connection to the targeted network, similar to the level of access that is provided to suppliers. Furthermore, an organization may provide support regarding the function and normal use of critical assets, to overcome restrictions in resources and the time available to perform an attack. As such, active support from a targeted organization could make a Red Team attack more predictive for actual APT attacks.

According to Dominguez, a kill chain model should encompass all activities starting from external reconnaissance up to the exfiltration of sensitive data or other objective-specific actions. From a technical perspective, a lot of intermediate phases are missing from Lockheed Martin's Kill Chain. As a result, organizations that rely on kill chain approaches in marketing materials from the security industry may misalign their investments by focusing primarily on preventing the compromise of individual systems and blocking Command & Control traffic. For the previously mentioned objective of a kill chain model however, Dominguez nonetheless regards the Cyber Kill Chain as a valuable tool to provide decision makers with relevant insights. A more technically correct approach, such as the UKC, may benefit from further abstraction to allow decision makers on a management level to comprehend the attack lifecycle and to realign their security investments.

4 Case Study: APT28 - Fancy Bear (C4)

4.1 Actor Description

APT28 is a threat actor that has reportedly been operating since at least 2004 [47]. APT28 (FireEye's initial designation of the actor) is also known as Fancy Bear (CrowdStrike), Pawn Storm (TrendMicro), Sednit (ESET), Sofacy Group (F-Secure), Strontium (Microsoft), Threat Group-4127 (SecureWorks), Tsar Team (Trustwave) and one of the two Grizzly Steppe threat actors (Department of Homeland Security of the United States). The actor appears to have (re)claimed the battle name (Dutch: 'geuzennaam') Fancy Bear(s) in its self-publications of collected confidential information [1]. Over the last years, the attacks by APT28 have increased tenfold, making APT28 one of the most prolific, agile and dynamic threat actors in cyberspace [48]. The advanced and persistent attacks by APT28 are consistent with nation-state level capabilities [49].

Through the years, APT28 has engaged extensively in espionage [49] with a common objective: securing outcomes that are beneficial to the Russian Federation [9]. In recent years, the operations of APT28 have grown beyond espionage to execute covert influence campaigns (or "active measures") [50]. These campaigns aim to manipulate the public opinion and the domestic politics of foreign nations through the collection and controlled release of (mis)information. The current (geo)political climate and the prevalence of fake news (accusations) has in part been attributed to intentional leaks and manipulations by threat actors such as APT28 [51].

Publications regarding APT28 attacks show that there are commonalities in the actor's MO across multiple attacks, which may be used to identify likely attack paths and thus to develop kill chains. The attacks by APT28 are not particularly stealthy and have been described as *brazen* (a shameless or disrespectful boldness). This indicates that hiding its activities is not a high priority for the APT28, in contrast to many other threat actors in cyberspace. If APT28 is caught after achieving its objectives, this can result in free mass media coverage, which can further damage the targeted organization(s) and set the scene for the release of (mis)information. Even though much has been written about APT28 attacks in recent years and its DNC hack is at the center of multiple investigations in the United States, the activities by APT28 have grown in number and aggressiveness [51].

The attacks of APT28 have been publicly attributed to the Russian (military) intelligence services by the United States intelligence community, the DHS, the FBI, organizations in the security industry and other entities [52]. The attribution of APT28's attacks to Russia's military intelligence service (GRU) aligns with the agency's main role in collecting military intelligence, performing active measures to subvert and destabilize Western governments and its general aggressive and risk-taking culture. The GRU also has a subsidiary role in collecting political, economic and counter-intelligence. The GRU is one of Russia's four main intelligence agencies, which have been characterized as a powerful, feral and obedient multi-headed hydra. These agencies are reportedly granted a considerable latitude in their methods and operate in a cut-throat competitive environment with overlapping objectives [53].

Research into APT28 is typically based on the analysis of the capabilities in malware samples, that have been submitted to VirusTotal [54] or have otherwise been acquired by anti-virus telemetry or researchers [47]. The multi-staged malware ecosystem that is used by APT28, where reconnaissance malware can be deployed first, further limits the exposure of more valuable components to defenders and researchers. APT28 can also use a tunnel component and/or a VPN connection to join a Kali Linux based system to a targeted network, which allows the actor to only ephemerally expose its tools that are used to compromise assets internally [55]. In most cases, forensic investigations into APT28 compromises take place under confidentiality clauses, which limit the publicly available information regarding how APT28's capabilities are used for its activities [49]. Consequently, the reports tend to focus on static capabilities of the APT28 specific malware ecosystem rather than dynamic activities of the APT28 threat actor. As a result, it is expected that attack phases to initially compromise a system behind the perimeter with malware (which can be represented with the traditional CKC) are overrepresented in the forensic reports in comparison with attack phases that occur in the attack paths behind the organizational perimeter of compromised organizations.

4.2 APT28 Tactics Analysis

To gain insights into the tactics that are used by APT28, 17 forensic reports were analyzed that detail APT28's malware ecosystem and its attacks. The reports were published between October 2014 and October 2017, but some reports also cover prior activities of APT28. The TTPs that have been developed and employed by APT28, that could be identified in these reports, were mapped to the UKC through the interpretive analysis of their contents. The raw results are included in Appendix C, which includes a comprehensive but not necessarily exhaustive collection of relevant citations and references. Citations regarding similar or even identical TTPs from multiple sources are included, to corroborate the statements in these reports.

Based on Appendix C, an overview of the occurrence of APT28 tactics is provided in Table 10. The names of the tactic(s) that could not be identified in the analysis of APT28's MO in the reports are ~~struck through~~ in Table 10. The initial order of the tactics is based on the UKC as developed through literature analysis and the Red Team case studies. In section 4.3, APT28 attack patterns and sequences of tactics are used to transform these tactics into phases of attacks to form kill chains.

Table 10 - Overview of identified APT28 tactics

Tactic	Occurrence
Reconnaissance	Reconnaissance has been performed by APT28 through a variety of techniques. IP-ranges assigned to countries or used by targeted organizations have been scanned for vulnerabilities. In one of the analyzed attacks, APT28 may have identified a Remote Desktop Protocol (RDP) interface that was exposed to the internet with default credentials. Open source intelligence (OSINT) has been performed to identify targets for spear phishing campaigns. Previously exfiltrated and analyzed intelligence is also used to craft highly targeted spear phishing campaigns.
Weaponization	Typo squatted domains are frequently registered by APT28 for phishing purposes, which can include the name of the targeted organization. The group tends to re-use service providers and components across multiple attacks. Spear phishing e-mails can contain links to spoofed webmail portals or malicious documents and may rely on social engineering or exploit(kit)s for execution. Links can be obfuscated using URL shorteners. Compromised e-mail or VPN accounts have been used to mount further attacks. APT28 has had access to a multitude of zero-day exploits for previously unknown vulnerabilities, but has also rapidly implemented exploits that became publicly available. APT28 can leverage an extensive malware ecosystem, that includes multi-staged droppers and RATs for various platforms. The malware ecosystem has been actively maintained and has been extended as required.
Social Engineering	APT28 frequently uses social engineering lures to manipulate users into performing unsafe actions. Social engineering lures can be very targeted, based on reconnaissance and previously acquired intelligence. Social engineering can be used to entice users to click on links to malicious URLs or to open malicious documents, which has been combined with the use of exploits. Social engineering techniques have been used to trick users into exposing credentials for e-mail and VPNs, or to deploy the first stage of the malware ecosystem. Advanced social engineering techniques, such as *tabnabbing*, have been used by APT28 to acquire credentials. Alternatively, OAuth based social engineering attacks have been used to obtain persistent access to e-mail through supposed add-ons or apps. These attacks have been performed against users of common cloud e-mail providers, but also against corporate webmail users.
Delivery	Two primary initial delivery methods (attack vectors) have been used by APT28, namely spear phishing e-mails and watering hole attacks. Spear phishing e-mails can contain a malicious payload in the form of a weaponized document or a link to a weaponized website. In the watering hole attacks, APT28 compromised and injected malicious code into legitimate websites, which its targets were likely to

	visit. When potential targets visited APT28 (controlled) websites, fingerprinting techniques were used to determine if the user was a valuable target. Depending on their apparent value, users could be presented with the legitimate website, a social engineering lure, an old exploit or even (a) zero-day exploit(s) to deploy APT28's malware ecosystem. The malware ecosystem that is used by APT28 is typically delivered in multiple stages. During the first delivery stage, a dropper is used to deploy a payload consisting of a relatively simple Remote Access Trojan (RAT) that provides command and control and is primarily used for reconnaissance purposes. If a high value target has been infected, a second delivery stage can be initiated, in which the first stage malware receives a dropper and subsequently deploys the second stage malware. The multi-stage setup limits the exposure of the more advanced malware ecosystem components to anti-virus.
Exploitation	APT28 is known for its frequent use of zero-day exploits in its attacks. In 2015 alone, the group used at least 6 zero-day exploits for previously unknown vulnerabilities. APT28 is also known to quickly repurpose and extend exploitation techniques and Proof of Concept (PoC) code once it has become part of the public domain. These exploits have been embedded in malicious documents, have been served as a chain of exploits as required by the command & control server and have been combined in an exploit pack (in the case of watering hole attacks). Software that has been exploited by APT28 includes Adobe Flash, Internet Explorer, Java, Microsoft Word and Microsoft Windows. In addition to using exploits for security bugs, APT28 has exploited software features such as the ability to execute untrusted code through Microsoft Word macro's. The exploits are typically used to deploy first-stage malware (Flash, Internet Explorer, Java and Microsoft Word) and/or to escalate privileges on the compromised system (Microsoft Windows). The public Browser Exploitation Framework (BeEF) has also been injected into legitimate websites in watering hole attacks, which allowed reconnaissance through the website's visitors' browser.
Persistence	Persistence has been realized by APT28 through different techniques depending on the attack vector. To make components of the malware ecosystem persistent, techniques such as registry Run keys or AutoStart extensibility points (ASEP) registry entries, shell icon overlay handlers and a so termed Office Test method have been used. The group has also persisted its malware through a kernel mode rootkit installed as a Windows service and by infecting the Master Boot Record (MBR) with a bootkit. Moreover, a higher level of persistence has been obtained by deploying multiple malware components on a single system, each of which can individually provide command and control over the compromised system. To gain persistent access to the e-mail of spear phishing targets, APT28 has used different techniques. In OAuth-based spear phishing attacks, the OAuth token remains valid and provides full access until it is explicitly revoked, even if the password of the affected user is changed. In other spear phishing attacks on e-mail accounts, an e-mail forwarding address has been setup to gain persistent access to the contents of e-mails even after the password of the affected user has been changed.
Defense Evasion	The modus operandi of APT28 has not been particularly stealthy, which indicates that hiding its activities is not always the group's highest priority. This is amongst others shown by the tendency to re-use the same service providers for its attack infrastructure. Nonetheless, APT28's first stage malware checks for the presence of specific endpoint security products. The malware also disables the creation of and/or removes potential forensic artefacts such as crash reporting, event logging and debugging. Some of the malware components have specific functions to delete files, and the collected data is removed after it is uploaded. Timestamps of files have been altered to avoid detection. APT28 is also known to have used a User Account Control (UAC) bypass technique.
Command & Control	The malware ecosystem components of APT28 can use different methods to establish command and control after a system has initially been compromised. The malware will generally first attempt to determine if a direct connection to the internet is possible via HTTP(S). If a direct connection is not possible, the malware attempts to connect to the internet via the proxy server that is configured on the system or by injecting into a running browser. Alternatively, the malware uses e-mail (SMTP and POP3) as a covert communication channel with the Command & Control server(s). In one of the analyzed attacks, APT28 appears to have acquired remote access to a targeted network through third-party VPN credentials.
Pivoting	The malware ecosystem of APT28 contains at least two components that can be used to pivot to systems that are otherwise not directly accessible to the attackers. The Xagent component can infect USB drives that are connected to a compromised system to create an ad-hoc pseudo-network that routes messages between the filesystems and the registry. The component can notably spread laterally to air-gapped networks via the autorun invocation of infected USB drives. As such, the component can be used to transfer information from the air-gapped network when the drive is connected back to the internet connected network.

	The Xtunnel component, which was named as such by its developers, is typically deployed as a second (or even third) stage malware. The component serves as a network pivot to other systems in the network. TCP and UDP traffic can be tunneled at will to other internal systems through the compromised system from a command & control server. APT28 has also used VPN connections to virtually join Kali (a Linux distribution created for penetration testers) based systems to targeted networks, which presumably used the Xtunnel component. The Xtunnel is thought to be of high importance to APT28, as it is the only known component that is heavily obfuscated and is subject to continuous development efforts to add new features.
Discovery	The first stage malware that is deployed to systems infected by APT28 serves as discovery malware. These components can gather detailed information regarding the compromised system, including the physical location of the computer and a list of running processes. If the compromised system is deemed interesting, further stages of the malware ecosystem can be deployed. The group has also used the BeEF exploit framework to perform discovery through the browser of users that visit a malicious website.
Execution	Various techniques have been used to execute attacker-controlled code on local or remote systems. The deployed malware components can be used to download and execute additional components. Some components, such as Xagent contain built in capabilities for remote command execution. Executable files have also been generated from Python scripts using py2exe. Other methods used to execute code locally include the use of NSTask:launch, rundll32.exe and lesser known techniques such as kernel asynchronous procedure call (APC) injection. Tools that have specifically been used to execute code on other (remote) internal systems includes RemCOM, which is an open-source replacement for the widely used PsExec tool from the Windows Sysinternals suite.
Privilege Escalation	Before or during the deployment of the first-stage malware component, local privilege escalation exploits have been used to gain system privileges if required. Similarly, Windows features have been abused by malware components to auto-elevate privileges. The local escalation of privileges typically takes place before the malware is made persistent on the system, which enables the malware to use more intrusive methods to obtain persistence. APT28 has also used the leaked EternalBlue SMB exploit to remotely escalate privileges on other internal systems, which provides an unauthenticated attacker with system-privileges.
Credential Access	Acquiring credentials has played a key role in APT28 attacks. Spear phishing attacks have been used to specifically acquire credentials for externally accessible webmail environments and VPN access. Access to the externally accessible webmail and management interfaces can be used to collect and exfiltrate confidential information directly or to identify additional targets. Acquired VPN credentials have provided APT28 with remote access to a target network. On compromised systems, different techniques have been used to acquire access to plain text credentials. These include the use of a custom variant of the publicly available tool mimikatz to extract Windows single sign-on passwords from memory, which requires system-level access. Credentials that have been stored by applications, such as browsers and e-mail clients, can also be collected by some of the malware components. A built-in keylogging functionality can serve to acquire credentials that are not stored. On targeted networks, the publicly available Responder tool has been used to spoof NetBios Name Service (NBNS) responses to acquire usernames and password hashes.
Lateral Movement	Lateral movement techniques have been used by APT28 to move through targeted organizations in search of access to more data and high(er) value targets. Techniques employed by APT28 to perform lateral movement notably include pass-the-hash (PtH), in which the LM or NTLM password hash of a user is leveraged for authentication to other internal systems, in combination with tools such as WinExe (which provides remote command-line execution). The spread of the Xagent component to other systems in air-gapped environments through infected USB drives can also be regarded as a form of lateral movement.
~~Action on Objectives~~	All the identified objective-specific activities of APT28 that occur within the locus of control of targeted organization could be described with the tactics Target Manipulation, Collection and Exfiltration.
Target Manipulation	The Department of Homeland Security of the United States of America has alleged that Russian civilian and military intelligence services (APT28 and APT29) have conducted disruptive or even damaging attacks on amongst others critical infrastructure networks. Only one attack that has specifically and publicly been attributed to APT28 corroborates the use of this tactic by APT28. In the TV5Monde hack, the firmware of routers and switches was erased to sabotage the broadcasting of TV channels.
Collection	Espionage appears to be one of APT28's primary objectives. A variety of data has been collected from targeted e-mail accounts and networks. Access to externally accessible e-mail accounts allows APT28 to silently gather data over extended periods of time. Malware components contain functionality such as key logging, e-mail address harvesting, capturing periodic screenshots, tracking window focus and scraping window contents and checking for the presence of backups of iOS devices. Files can also be harvested from local and USB drive, a process for which rules can be defined. The collected data is

	typically stored on disk in hidden files and/or folders, which prevents the loss of acquired data if a system is rebooted.
Exfiltration	Data that has been collected by APT28 malware components can be automatically and periodically exfiltrated in bulk, by uploading the hidden files to the Command & Control server(s). APT28 can also exfiltrate data manually. The visible Command & Control servers may simply function as an intermediate proxy in the exfiltration of collected data, which creates an extra hop that makes investigations more difficult. Access to externally accessible e-mail environments of spear phishing targets has been leveraged to persistently exfiltrate data by setting up an e-mail forwarding address. The exfiltrated data is reportedly analyzed for intelligence purposes and has been leaked to third parties to further Russian interests.

4.3 APT28 Attack Patterns and Sequences

In the attacks of APT28, common patterns and sequences can be derived from the analyzed reports and Table 10, which are detailed in the tables in the subsequent sections. Two attack vectors are typically used by APT28 to initially target organizations. Firstly, (spear) phishing can be used to initially send links to malicious URLs or to deliver malicious documents to specific targets. Secondly, legitimate websites that are visited by potential targets can be compromised to deliver malicious code in watering hole attacks. The initial attack vectors can be leveraged followed by three attack paths: acquiring credentials through social engineering, infecting systems with first stage malware through social engineering or infecting systems through exploits [56].

Once APT28 has deployed its malware to one system of a targeted organization, other (in)directly reachable internal systems of the organization may be targeted. The attack paths that were identified in the reports that could lead to successful attack paths are: using credentials from the initially compromised (local) system to move towards targets on the network, using the exploits to move towards targets on the network (EternalBlue), using (NBNS) spoofing techniques to acquire credentials to move towards targets on the network and infecting USB drives to move towards air-gapped targets. In all identified cases, the level of access that is acquired is typically used by APT28 to perform actions on their objectives by collecting and exfiltrating data.

4.3.1 Attack vector: spear phishing e-mails

Table 11 - Attack vector: spear phishing e-mails

Phase	Description
Reconnaissance	Open source intelligence (OSINT) and previously exfiltrated and analyzed intelligence can be used to craft highly targeted spear phishing campaigns.
Weaponization	APT28 has invested in an extensive malware ecosystem and exploits, which can be leveraged in attacks. The infrastructure can be extended with additional components, exploits, social engineering methods, spoofed (web) interfaces and command and control servers as required.
Delivery	Weaponized objects, such as links or documents, are frequently delivered to APT28 targets through spear phishing e-mails.

4.3.2 Attack vector: watering hole websites

Table 12 - Attack vector: watering hole websites

Phase	Description
Weaponization	Vulnerabilities in third party infrastructure are (or have been) exploited to weaponize that infrastructure in preparation for watering hole attacks on targeted organizations.

Delivery	APT28 injects malicious code into legitimate websites, which its targets are likely to visit. When potential targets visit APT28 (controlled) websites, fingerprinting techniques are used to determine the appropriate payload for the potential target.

4.3.3 Attack path: social engineering for credentials

Table 13 - Attack path: social engineering for credentials

Phase	Description
Social Engineering	Social engineering is used to present users with spoofed (web) interfaces.
Credential Access	When users enter e-mail or VPNs credentials into the spoofed (web) interfaces, the credentials are exposed to APT28.
Persistence	To gain persistent access to the e-mail of spear phishing targets, techniques such as approving OAuth tokens or setting up e-mail forwarding addresses are used.

4.3.4 Attack path: social engineering for infection

Table 14 - Attach method: social engineering for infection

Phase	Description
Social Engineering	Social engineering can be used to entice users to click on links to malicious URLs, to open malicious documents, or to allow the use of features such as Word macro’s.
Delivery	Code execution is used to deploy the first-stage malware. More specifically, a dropper is initiated that deploys a payload consisting of a Remote Access Trojan.
Privilege Escalation	If the malware is executed with limited privileges, a local privilege escalation exploit can be used to escalate to SYSTEM privileges.
Persistence	A variety of techniques can be used to make the first-stage malware persistent. These may result in persistence in user-land, or through a rootkit or bootkit. Persistence can be strengthened by deploying further malware components.
Defense Evasion	APT28 first stage malware checks for the presence of specific endpoint security products. The first stage malware also disables the creation of and/or removes potential forensic artefacts such as crash reporting, event logging and debugging.
Command & Control	The malware ecosystem components of APT28 can use different methods to establish command and control after a system has initially been compromised.

4.3.5 Attack path: exploitation for infection

Table 15 - Attack path: exploitation for infection

Phase	Description
Social Engineering	Social engineering can be used to entice users to click on links to malicious URLs or to open malicious documents, which can include the use of exploits.
Exploitation	Exploits can be embedded in malicious documents, can be served as a chain of exploits by the command & control server or can be combined into an exploit pack.
Delivery	Code execution is used to deploy the first-stage malware. More specifically, a dropper is initiated that deploys a payload consisting of a Remote Access Trojan.
Privilege Escalation	If the malware is executed with limited privileges, a local privilege escalation exploit can be used to escalate to SYSTEM privileges.
Persistence	A variety of techniques can be used to make the first-stage malware persistent. These may result in persistence in user-land, or through a rootkit or bootkit. Persistence can be strengthened by deploying further malware components.

Defense Evasion	APT28 first stage malware checks for the presence of specific endpoint security products. The first stage malware also disables the creation of and/or removes potential forensic artefacts such as crash reporting, event logging and debugging.
Command & Control	The malware ecosystem components of APT28 can use different methods to establish command and control after a system has initially been compromised.

4.3.6 Attack path: using local credentials to move towards targets on the network

Table 16 - Attack path: using local credentials to move towards targets on the network

Phase	Description
Discovery	The first stage malware that is typically deployed to systems infected by APT28 serves as discovery malware (Seduploader). This component can gather detailed information regarding the compromised system.
Delivery	If a high value target has been infected, a second delivery stage can be delivered, in which case the first stage malware receives a dropper and subsequently deploys the second stage malware (Xtunnel).
Execution	The malware components can be used to execute arbitrary code such as mimikatz.
Credential Access	On compromised systems, different techniques can be used to acquire plain text credentials from disk, keylogging and/or from memory. If credentials are acquired, APT28 can move to Pivoting and Lateral Movement.
Pivoting	Remote access to the compromised system can be leveraged to target other internal systems. The Xtunnel component can be used as a network pivot towards other reachable internal systems on the same network.
Lateral Movement	Lateral movement techniques have been used by APT28 to move through targeted organization in search of access to more data and high(er) value targets, through techniques such as pass-the-hash.

4.3.7 Attack path: using exploits to move towards targets on the network

Table 17 - Attack path: using exploits to move towards targets on the network

Phase	Description
Discovery	The first stage malware that is typically deployed to systems infected by APT28 serves as discovery malware (Seduploader). This component can gather detailed information regarding the compromised system.
Delivery	If a high value target has been infected, a second delivery stage can be delivered, in which case the first stage malware receives a dropper and subsequently deploys the second stage malware (Xtunnel).
Pivoting	Remote access to the compromised system can be leveraged to target other internal systems. The Xtunnel component can be used as a network pivot towards other reachable internal systems on the same network.
Privilege Escalation	APT28 may perform remote privilege escalation on the other reachable internal systems through exploits such as EternalBlue, which provides an unauthenticated attacker with system-privileges on the targeted system.
Execution	The acquired privileges on remote systems can be used to execute arbitrary code.
Credential Access	If remote code execution has been obtained, different techniques can be used to acquire plain text credentials from the system from disk, keylogging and/or from memory.
Lateral Movement	Lateral movement techniques have been used by APT28 to move through targeted organization in search of access to more data and high(er) value targets, through techniques such as pass-the-hash.

4.3.8 Attack path: using spoofing to move towards targets on the network

Table 18 - Attack path: using spoofing to move towards targets on the network

Phase	Description
Discovery	The first stage malware that is typically deployed to systems infected by APT28 serves as discovery malware (Seduploader). This component can gather detailed information regarding the compromised system.
Delivery	If a high value target has been infected, a second delivery stage can be delivered, in which case the first stage malware receives a dropper and subsequently deploys the second stage malware (Xtunnel).
Pivoting	Remote access to the compromised system can be leveraged to target other internal systems. The Xtunnel component can be used as a network pivot towards other reachable internal systems on the same network.
Credential Access	The publicly available Responder tool can be used to spoof NetBios Name Service (NBNS) responses from systems in the same network to acquire usernames and password hashes.
Lateral Movement	Lateral movement techniques have been used by APT28 to move through targeted organization in search of access to more data and high(er) value targets, through techniques such as pass-the-hash.

4.3.9 Attack path: infecting USB drives to move towards air-gapped targets

Table 19 - Attack path: infecting USB drives to move towards air-gapped targets

Phase	Description
Discovery	The first stage malware that is typically deployed to systems infected by APT28 serves as discovery malware (Seduploader). This component can gather detailed information regarding the compromised system.
Delivery	If a high value target has been infected, a second delivery stage can be delivered, in which case the first stage malware receives a dropper and can deploy the Xagent component.
Pivoting	The Xagent component can be used to pivot towards systems in air-gapped networks.
Lateral Movement	Xagent can spread to other systems in air-gapped environments through infected USB drives.

4.3.10 Action on Objectives: acquiring data and/or target manipulation

Table 20 - Action on Objectives: acquiring data

Phase	Description
Collection	Data can be collected from targeted e-mail accounts and/or from systems on targeted networks. Access to externally accessible e-mail accounts allows APT28 to silently gather data over extended periods of time. Malware components can also be used to collect and store data.
Exfiltration	Access to externally accessible e-mail environments can be leveraged to persistently exfiltrate data, for example by retaining access or by setting up an e-mail forwarding address. Data that has been collected by APT28 malware components can be automatically or manually exfiltrated.
Target Manipulation	After collecting and exfiltrating data, APT28 has allegedly manipulated supporting ICT assets that resulted in the sabotage of critical organizational processes.

4.4 APT28 Attack Paths and Attack Specific Kill Chains

The previously described attack vectors and attack paths of APT28 can be logically combined to form 22 unique attack paths, which all position the threat actor to acquire data and/or manipulate targets:

1. Spear phishing e-mails + social engineering for credentials
2. Spear phishing e-mails + social engineering for infection
3. Spear phishing e-mails + exploitation for infection
4. Spear phishing e-mails + social engineering for infection + using local credentials to move towards targets on the network
5. Spear phishing e-mails + social engineering for infection + using exploits to move towards targets on the network
6. Spear phishing e-mails + social engineering for infection + using spoofing to move towards targets on the network
7. Spear phishing e-mails + social engineering for infection + infecting USB drives to move towards air-gapped targets
8. Spear phishing e-mails + exploitation for infection + using local credentials to move towards targets on the network
9. Spear phishing e-mails + exploitation for infection + using exploits to move towards targets on the network
10. Spear phishing e-mails + exploitation for infection + using spoofing to move towards targets on the network
11. Spear phishing e-mails + exploitation for infection + infecting USB drives to move towards air-gapped targets
12. Watering hole websites + social engineering for credentials
13. Watering hole websites + social engineering for infection
14. Watering hole websites + exploitation for infection
15. Watering hole websites + social engineering for infection + using local credentials to move towards targets on the network
16. Watering hole websites + social engineering for infection + using exploits to move towards targets on the network
17. Watering hole websites + social engineering for infection + using spoofing to move towards targets on the network
18. Watering hole websites + social engineering for infection + infecting USB drives to move towards air-gapped targets
19. Watering hole websites + exploitation for infection + using local credentials to move towards targets on the network
20. Watering hole websites + exploitation for infection + using exploits to move towards targets on the network
21. Watering hole websites + exploitation for infection + using spoofing to move towards targets on the network
22. Watering hole websites + exploitation for infection + infecting USB drives to move towards air-gapped targets

As section 4.3 shows however, the attack paths “social engineering for infection” (4.3.4) and “exploitation for infection” (4.3.5) are very similar. Both attack paths include Social Engineering and lead to the same intermediary result (an initial infection behind the internal network perimeter). The “exploitation for infection” path also includes an Exploitation phase in contrast to the “social engineering for infection” path. The amount of unique attack paths can be reduced by only modeling the “exploitation for infection” based internal attack paths, while still retaining insight into the role of users in raising resilience against social engineering. The base path “spear phishing e-mails + social engineering for infection”, is still modeled so that it can be included in later comparisons.

Furthermore, in recent years social engineering has been the attack vector of choice of APT28 to acquire an initial infection [47, p. 20]. The amount of attack paths to be modeled can be reduced further by only modeling the internal attack paths for the spear phishing attack vector. The base path “watering hole websites + exploitation for infection”, is still modeled so that it can be included in later comparisons. These two reductions result in 9 unique attack paths, which is incidentally the same number of attack paths that were modelled for the Red Team case study. Consequently, the following unique attack paths, which all position APT28 to acquire data and/or manipulate targets, are modeled:

1. Watering hole websites + social engineering for credentials (C4-1)
2. Watering hole websites + exploitation for infection (C4-2)
3. Spear phishing e-mails + social engineering for credentials (C4-3)
4. Spear phishing e-mails + social engineering for infection (C4-4)
5. Spear phishing e-mails + exploitation for infection (C4-5)
6. Spear phishing e-mails + exploitation for infection + using local credentials to move towards targets on the network (C4-6)
7. Spear phishing e-mails + exploitation for infection + using exploits to move towards targets on the network (C4-7)
8. Spear phishing e-mails + exploitation for infection + using spoofing to move towards targets on the network (C4-8)
9. Spear phishing e-mails + exploitation for infection + infecting USB drives to move towards air-gapped targets (C4-9)

To visualize the relationship of phases within the attack paths, a sequential overview of these 9 attack paths are included in Table 21 as kill chains. The phases of the UKC progress from green to red as critical organizational assets are breached. A black line is used to distinguish phases that occur after the initial compromise of one system behind the network perimeter (*Command & Control*). Target Manipulation was only performed on switches and routers, which requires an internal attack path beyond the initial compromise of a workstation and is therefore only modeled in C4-6 to C4-9.

Table 21 – Heatmap of occurrence and sequence of UKC phases in APT28 attack paths

		APT28 Attack Paths								
#	Unified Kill Chain	C4-1	C4-2	C4-3	C4-4	C4-5	C4-6	C4-7	C4-8	C4-9
1	Reconnaissance	2	2	1	1	1	1	1	1	1
2	Weaponization	3	3	2	2	2	2	2	2	2
3	Delivery	4	4	3	3	3	3	3	3	3
4	Social Engineering	13	5	4	4	4	4	4	4	4
5	Exploitation	6	3	13	3	5	5	5	5	5
6	Persistence	17	11	6	11	3	3	3	3	3
7	Defense Evasion	18	6	17	6	11	11	11	11	11
8	Command & Control		7	18	7	6	6	6	6	6
9	Pivoting		8		8	7	7	7	7	7
10	Discovery		17		17	8	8	8	8	8
11	Privilege Escalation		18		18	17	10	10	10	10
12	Execution					18	3	3	3	3
13	Credential Access						12	9	9	9
14	Lateral Movement						13	11	13	14
15	Action on Objectives						9	12	14	17
16	Target Manipulation						14	13	17	18
17	Collection						17	14	18	16
18	Exfiltration						18	17	16	
							16	18		
								16		

The 9 attack paths described in Table 21 do not necessarily occur with the same frequency in APT28 attacks. The three most common base attack paths for APT28 are thought to be spear phishing to social engineer for credentials (C4-3) [47, p. 12], spear phishing with malicious documents containing exploits to initially infect systems (C4-5) [47, p. 18] and using watering hole websites in combination with an exploit kit to initially infect systems (C4-2) [47, p. 20]. Since most reports are based on analysis of static capabilities of the malware ecosystem rather than the dynamic activities of the threat actor, it is not evident which path APT28 most frequently follows within internal networks (out of the identified attack paths C4-6, C4-7, C4-8 and C4-9).

4.5 APT28 Actor Specific Kill Chain Formation

The actor specific kill chains are intended to provide a linear representation of the entire repertoire of the tactics that an attacker may employ during an attack in their expected order. When this *actor* specific kill chain is applied to a specific environment, this results in an *attack* specific kill chain, which is context dependent. In contrast to the actor specific kill chain, attack phases may occur more than once in an attack specific kill chain depending on the target environment. In the actor specific kill chain, phases that may occur more than once in an attack are generally modeled in the position in the sequence where they first occur.

Kill chain C4-7 provides the most comprehensive overview of the phases that may be employed by APT28. The internal attack path was observed in APT28 attacks in August 2017 by FireEye [57]. The

C4-7 kill chain notably includes all the phases that occur in the other APT28 attack specific kill chains. As such, every other APT28 attack specific kill chain can be built using the attack phases that are encompassed by kill chain C4-7. None of the other APT28 attack specific kill chains have this property. Consequently, C4-7 serves as the basis for the APT28 actor specific kill chain in the following section. Phases that occur multiple times in C4-7 will be modeled based on their first occurrence, except for Privilege Escalation because the first instance is optional, while the second instance was required.

In the clear majority of APT28's analyzed attacks, the primary objective appears to be espionage as evidenced by the prevalence of the attack phases Collection and Exfiltration. However, at least one attack that resulted in sabotage has also been attributed to APT28, which involved Target Manipulation after the phases Collection and Exfiltration were completed. This re-arranged order of the objective-specific tactics is also reflected in the threat actor specific kill chain and in the final UKC in Appendix A. Given the *tempus specialis derogat tempore generali* rule that was applied from section 3.2.3 onwards, which entails that phases are described with the most specific description of the activities that is available, the Action on Objectives phase as such was not necessary to model APT28's objective-specific activities on the technical layer of cyberspace.

The term Action on Objectives has been used as an abstract term that encompasses multiple objective-specific phases on the technical layer in the Red Team case studies. More specifically, Collection and Exfiltration typically refer to activities that compromise the confidentiality of data. Target Manipulation can describe the compromise of the integrity and availability of systems or data. Collectively the phases Collection, Exfiltration and Target Manipulation suffice to describe all compromises of the Confidentiality, Integrity and Availability (CIA) triad. The term Action on Objectives can be used to refer to these collective objective-specific phases on a more abstract level regarding the activities on the technical layer of cyberspace (as used subsequently in section 6.4), which aligns with how the term has been used from the Red Team case study C1 onwards.

The Action on Objective phases (Collection, Exfiltration and Target Manipulation) are technically oriented and describe tactical *actions*. It is thought to be valuable to bridge the gap between these tactical actions of APTs on the technical layer of cyberspace and the strategic goals on the socio-technical layer of cyberspace. The term *Objectives* could be detached from the original "Action on Objectives" CKC phase, to refer to the socio-technical objectives of the attack that are intended to achieve a strategic goal. For the threat actor APT28, this interpretation of the Objectives element could cover the post-compromise use of acquired data for the controlled release of (mis)information with the strategic goal to manipulate the public opinion and the domestic politics of foreign nations.

This explicit inclusion of Objectives forces defenders to take the socio-technical objectives and strategic goals of attackers into account in their application of the kill chains whenever possible, which is expected to be beneficial for a deeper level of understanding of the attacker activities. For example, when the Objectives of a threat actor are known, it may be possible to predict which assets are more likely to be targeted. The Objectives are logically distinct from other attack phases, are highly relevant and may be observable (in accordance with the requirements for a phase described in section 2.2.3). While it may not be easy to counteract the Objectives specifically, relevant measures can be prepared after a technical compromise. For example, a proactive incident management communication strategy can be adopted to pre-empt the release of (mis)information following a compromise. Consequently, the threat actor's Objectives will be made explicit in the APT28 threat actor specific kill chain and the final UKC in Appendix A.

4.6 APT28 Actor Specific Kill Chain

The APT28 Kill Chain (APT28 KC) encompasses the unique phases that comprise the tactical repertoire of APT28 in their expected sequence, as first explained in section 1.4.2. As such, the APT28 KC is a threat actor specific instance of the UKC. The APT28 KC was based on the attack specific kill chain C4-7, as described in section 4.5.

Table 22 - The APT28 Actor Specific Kill Chain (APT28 KC)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Delivery	• Techniques resulting in the transmission of a weaponized object to the targeted environment.
Social Engineering	• Techniques aimed at the manipulation of people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on a system or network.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Credential Access	• Techniques resulting in the access of, or control over, system, service or domain credentials.
Lateral Movement	• Techniques that enable an adversary to horizontally access and control other remote systems.
Collection	• Techniques used to identify and gather information from a target network prior to exfiltration.
Exfiltration	• Techniques that result or aid in an attacker removing files and information from a target network.
Target Manipulation	• Techniques aimed at manipulation of the target system to achieve the objective of the attack.
Objectives	• Socio-technical objectives of an attack that are intended to achieve a strategic goal.

4.7 Validation of APT28 Case Study

The data, analysis and results of this chapter were validated through a semi-structured interview with an intelligence analyst of Fox-IT. The intelligence analyst has tracked, analyzed and documented the MO of APT28 for an amount of time that was sufficient to acquire a thorough overview of the MO of this threat actor. The focus of Fox-IT's intelligence research into APT28 is to improve the detection of APT28 attacks in Fox-IT's Cyber Threat Management platform (CTMp) and Managed Intelligence Service (MIS). For reasons of operational security, some details have been omitted, such as the exact period for which APT28 has been investigated. The interviewee has requested to remain anonymous. The interview was conducted based on 10 open ended questions (detailed in Appendix D), which left room for follow-up questions.

The intelligence analyst was familiar with Lockheed Cyber Kill Chain (CKC), but did not specifically use the model for his activities. Instead, the analyst has familiarized himself with the MO of APT's such as APT28 and how their phases progressions occur on a tactical level. The logical place of malware samples in the chain of events of attacks is derived in practice by the analyst from the context and the capabilities of the malware. For example, first-stage malware is identified as such because it is dropped using weaponized documents and exploits and includes limited discovery capabilities to gather information from the infected system. Second-stage malware, in contrast, is modular and notably includes tunneling capabilities to attack other systems within the internal network. The analysts regarded the CKC as more suitable for incident response investigations, to track an actor during multiple phases and to reconstruct the chain of events.

The source of the data that is available to researchers influences their ability to gain insights into certain parts of the attack paths. For example, data from VirusTotal is frequently used for intelligence purposes by various security organizations. The analyst stated that VirusTotal can be a valuable source for exploit- and malware samples, which can provide insights into the first part of the kill chain, namely Delivery, Social Engineering, Exploitation and Persistence. Even if second-stage malware samples are uploaded to VirusTotal, they do not provide insight into how the malware capabilities are used in an attack. To gain insights into later parts of the kill chain, such as the attack paths within targeted networks, a security services provider will have to perform incident response cases into APT28 breaches at impacted organizations.

When asked specifically regarding the applicability of the CKC phases to APT28 attacks, the phases of the kill chain were thought to correspond with the initial infection of a system with APT28's first-stage malware. The analyst noted that in such an infection, multiple CKC phases occur almost instantaneously (particularly Exploitation, Installation and Command & Control). Table 10 - Overview of identified APT28 tactics was explained and discussed, which included various tactics in addition to the phases of the original CKC based on the UKC, which were all familiar to the analyst. For most of these tactics additional details regarding relevant TTPs could be provided by the analyst.

The steps to reduce the total number of possible combinations APT28 attack specific kill chains in section 4.4 was explained and did not meet objections. The limited prevalence of watering hole attacks in the resulting kill chains was deemed appropriate, because no cases of the use by APT28 of the exploit kit for watering hole attacks have been publicly documented in the last year. However, the analyst noted that watering hole attacks can be more difficult to detect, which could provide an alternative explanation for their relatively low occurrence in public reports. The primary initial attack vector of APT28 nonetheless currently appears to be (spear) phishing. Credential phishing occurs continuously by APT28 and may be highly automated. Phishing for infections also occurs frequently, but tends to take place in intervallic campaigns.

On an abstract level, 3 generalized distinct APT28 attack paths were discussed based on the 9 kill chains in Table 21 (on page 62). The kill chains C4-1 and C4-3, which leverage credential theft to acquire data, may be sufficient for APT28 to achieve its objectives. If the acquired access is not sufficient to achieve APT28's objectives, accessible data such as the targeted user's contacts may be extracted and weaponized for further attacks. Further attacks may consist of infecting a system to acquire data that could allow APT28 to achieve its objectives, as modeled by C4-2, C4-4 and C3-5. If the infected system still does not allow APT28 to achieve its objectives directly, internal attack paths may be required, as modeled by C4-6 to C4-9. As such, multiple kill chains may be executed by APT28 in the attacks against a single targeted organization to ultimately achieve its objectives.

The amount of time that is required for APT28 to achieve its objectives differs for the 3 generalized attack paths. When APT28 targets externally accessible webmail interfaces, the time between Weaponization (setting up the attack infrastructure) and Exfiltration (of data) may be a day or less. If the objectives require APT28 to successfully complete an internal attack paths however, the amount of time required may be raised significantly, depending on the level of security of the targeted organization. Correspondingly, both the amount of time and the number of possibilities to detect and respond to an APT28 attack are expected to be higher for those attack paths.

The ordered arrangement of the phases within the UKC was thought to be appropriate by the analyst. He noted that defense evasion can occur throughout an attack or may not be required at all. Some phases in the UKC may be optional, depending on the security posture of an organization and the objectives on an attacker. The analyst stated that the UKC definitely resembles what one would expect from APT28, but also from threat actors in general. He noted that some relevant different may exist within the Action on Objectives part of the kill chain, between APTs that focus on acquiring intelligence and cybercrime groups or script kiddies. The analyst also noted that for the latter two types of threat actors, an additional Clean-up phase may occur in which traces of the attack are removed.

The design choice to make the Objectives explicit at the end of the kill chain was also discussed. The analyst expressed that it may be difficult to ascertain what the objectives of a threat actor are, unless the process is supported by capabilities similar to an intelligence service. However, the analyst deemed it valuable to make objectives explicit, especially if the actor's objectives are different from what is typically sought by other attackers. As such, making objectives explicit can be valuable to identify which critical assets are likely to be targeted. Nonetheless, the analyst pointed out that it is unclear if the same people that are behind APT28's hacks are responsible for its (mis)information campaigns, or if APT28's hackers only pass the data on to other entities for this purpose.

The intelligence analyst deemed the UKC valuable for organizations in defending against APT28 attacks. For example, he commented that the UKC can be used to determine against which phases of the attacks IT vendors' products and services aim to provide protection. The UKC was also deemed to be valuable to make strategic choices in (re)aligning defenses against APT28 attacks, for example by focusing on the first or the latter part of the kill chain, depending on the requirements and attack surface of the targeted organization. Even though organizations may want to stop APT28 attack as soon as possible, the UKC was thought to support the development of defense in depth strategies.

Following the semi-structured interview, the intelligence analyst was provided with the full contents of chapter 4 (the APT28 case study) and the corresponding appendices. The analyst concluded that most of the relevant publicly available sources regarding APT28 had been used to perform the analysis. Overall, he concluded that the content of the chapter looked good and that there was little need for critical remarks.

5 Results

In this chapter, the results of the research are detailed. Firstly, the applicability of the CKC in the case studies is assessed through a comparison with the attack specific kill chains. Secondly, an overview of the development of the UKC is provided. Thirdly, the applicability of the UKC phases is assessed through a non-sequential comparison with the CKC and the Red Team and APT28 actor specific kill chains. Thirdly, the sequence and composition of the attack specific kill chains from the case studies are compared in detail, to identify convergences and divergences between the MO of the Red Team and APT28 and to formulate recommendations for improvements of Red Team assessments.

5.1 Applicability of the Cyber Kill Chain (CKC)

To assess the applicability of the CKC, it is first analyzed to what extent the phases of the CKC occur in the case studies. The original CKC definitions of the phases are used as the basis for the comparison, as defined in Table 3 (on page 19). As a result, Weaponization is limited to coupling a remote access trojan with a deliverable payload. Delivery refers to the transmission of the weapon to the target. In the CKC, Exploitation is thought to include Social Engineering. Installation is more restrictive than Persistence and describes the installation of a remote access trojan on a system.

The subsequent Table 23 (Red Team) and Table 24 (APT28) provide *non-sequential* visualizations of the occurrence CKC phases that progress from green to red as the perimeter is breached. Phases represented using a ~~strikethrough~~ of phase numbers are modelled in lieu of their occurrence, as previously explained. A red font is used to designate phases that can only be said to occur when expanded interpretations of the CKC phases are used. Both these choices are favorable for the CKC in the comparison with the kill chains from the case studies.

Table 23 – Overview of the occurrence of CKC phases in the Red Team case studies

		Red Team Attack Paths								
#	***Cyber Kill Chain***	**C1-1**	**C1-2**	**C1-3**	**C2-1**	**C2-2**	**C3-1**	**C3-2**	**C3-3**	**C3-4**
1	*Reconnaissance*	1	1	1	1	1	1	1	~~1~~	~~1~~
2	*Weaponization*	2	2	2	2	2	2	2		
3	*Delivery*	3	3	3	3	3	3	3	3	3
4	*Exploitation*	4	4	4	4	4	4	4	4	4
5	*Installation*	5	5	5			5	5		
6	*Command & Control*	6	6	6	6	6	6	6	6	6
7	*Action on Objectives*	7	7	7	~~7~~	~~7~~	~~7~~	~~7~~	~~7~~	~~7~~

As Table 23 shows, when attacks involve other attack vectors than phishing, such as in C2 and C3, phases of the CKC do not formally apply or can be bypassed altogether in the Red Team case studies:

- *Weaponization* is not required to get access to a stolen laptop, as in C3-3 and C3-4. In C2-1 and C2-2 a physical drop device was prepared, which does not meet the definition "coupling a remote access trojan with an exploit into a deliverable payload" [3].
- *Delivery* does not formally apply to C2-1, C2-2, C3-3 and C3-4, as no *transmission* of a weapon is required when the organizational perimeter is physically breached.
- The *Exploitation* phase in C2-1 and C2-2 was only required to circumvent the optional control Network Authentication Control (NAC). In its absence, the same attack could have been executed without going through an Exploitation phase.
- *Installation* was not performed in C2-1, C2-2, C3-3 and C3-4, as these kill chains involved the use of rogue (that is: attacker controlled) devices.

Table 24 - Overview of the occurrence of CKC phases in the APT28 case study

		APT28 Attack Paths								
#	*Cyber Kill Chain*	C4-1	C4-2	C4-3	C4-4	C4-5	C4-6	C4-7	C4-8	C4-9
1	*Reconnaissance*			1	1	1	1	1	1	1
2	*Weaponization*	2	2	2	2	2	2	2	2	2
3	*Delivery*	3	3	3	3	3	3	3	3	3
4	*Exploitation*	4	4	4	4	4	4	4	4	4
5	*Installation*	5	5	5	5	5	5	5	5	5
6	*Command & Control*		6		6	6	6	6	6	6
7	*Action on Objectives*	7	7	7	7	7	7	7	7	7

Table 24 again shows limitations of the CKC. When attack vectors other than phishing are used by APT28, CKC phases may be bypassed. Even when phishing is used as the initial attack vector, the application of the CKC to APT28 attacks that do not use malware shows that phases can be bypassed or that the application of the CKC to the case is strained:

- The *Reconnaissance* phase is not required in APT28's watering hole attacks, as shown in C4-1 and C4-2. These types of attacks can target all users that visit compromised websites.
- The *Weaponization* phase of the CKC does not formally apply to C4-1 and C4-3, as no remote access trojan is used when APT28 socially engineers directly for credentials. The phase only applies when other preparatory activities to weaponize an infrastructure are included.
- The *Installation* phase of the CKC does not formally apply to C4-1 and C4-3, as no remote access trojan or backdoor is installed on a victim system. Only when relevant activities are more broadly understood as Persistence, the phase can be thought to occur.
- The *Command & Control* phase does not occur at all in attacks where APT28 directly socially engineers users for credentials, without infecting their system with malware (C4-1 and C4-3).

The findings in this section, regarding the absence of one or more CKC phases in 7 out of the 18 attack paths, **falsify** a crucial assumption underlying the CKC, namely that an attacker "***must progress successfully through each stage of the chain*** *before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary*" [3, p. 2]. The CKC accurately models the phases that are required to gain an initial foothold in the target network when specific attack vectors are used to do so. More specifically, the CKC appears to be particularly useful to model the initial malware infection of a system within the network perimeter through phishing and vishing based attacks. The critique that the CKC is *malware focused* (described in section 2.2), thus appear to be correct.

Furthermore, the case studies have shown that the phases of the CKC do not occur in the strict sequence that was posited by Lockheed Martin's researchers (in C1-1 to C4-9). Other relevant phases such as Privilege Escalation and Credential Access may occur before Command & Control is established (C3-3 to C4-9), which are not currently modeled by the CKC. All steps that occur after Command & Control has been obtained over a system within the network perimeter are grouped using the term *Action on Objectives* in the CKC. As the next two sections show, many additional phases may occur after the organizational perimeter has been breached (C1-1 to C3-4 and C4-6 to C4-9). The critique that the CKC is *perimeter focused* (described in section 2.2), thus appear to be correct. Additional phases have been modeled in the UKC, because they can offer additional opportunities for raising resilience against APT attacks.

5.2 The Development of the Unified Kill Chain (UKC)

In this thesis, the UKC was developed from multiple sources. Firstly, literature research was performed into the CKC (section 2.1.2), its shortcomings (section 2.2.1) and potential improvements (section 2.2.2). The CKC and the identified potential improvements were combined with MITRE's ATT&CK framework of time-agnostic tactics to form a first version of the UKC in Table 6 (on page 28). The phases of the first version of the UKC provided a promising starting point for modeling the attack paths in the case studies, which allowed for the iterative evaluation, improvement and rearrangement of the phases in the UKC based on the phases in Red Team (in sections 3.2.3, 3.3.3, 3.4.3 and 3.5.1) and APT28 attack paths (in section 4.5) as shown in Table 25 below.

Table 25 - Overview of the development of the UKC throughout the thesis

#	Unified Kill Chain	Cyber Kill Chain® (CKC)	Laliberte	Nachreiner	Bryant	Malone	MITRE ATT&CK™	UKC after literature study	UKC after Red Team C1	UKC after Red Team C2	UKC after Red Team C3	UKC after Red Team KC	UKC after APT28 C4 & KC
1	*Reconnaissance*	1	1	1	1	1		1	1	1	1	1	1
2	*Weaponization*	2	3	3	3	2		2	2	2	2	2	2
3	*Delivery*	3	5	5	6	3		7	7	3	3	3	3
4	*Social Engineering*	5	6	6	11	5		3	3	4	4	4	4
5	*Exploitation*	6	8	8	14	6		5	4	5	5	5	5
6	*Persistence*	8	14	9	18	8	6	6	5	6	6	6	6
7	*Defense Evasion*	18	18	14	16	10	11	8	6	7	7	7	7
8	*Command & Control*			18		5	7	9	8	8	8	8	8
9	*Pivoting*					11	13	11	9	9	9	9	9
10	*Discovery*					14	10	10	11	11	11	10	10
11	*Privilege Escalation*					17	14	14	10	10	10	11	11
12	*Execution*					18	12	12	14	14	14	12	12
13	*Credential Access*						15	13	12	12	12	13	13
14	*Lateral Movement*						16	17	13	13	13	14	14
15	*Collection*						8	15	17	17	17	17	15
16	*Exfiltration*							16	15	15	15	15	16
17	*Target Manipulation*								16	16	16	16	17
18	*Objectives*												18

The first version of the UKC described the phases that lead to the initial compromise of a system behind the perimeter with the CKC and used MITRE's ATT&CK framework to describe the phases behind the organizational perimeter. Two further additions were made to the model based on the literature study, namely the addition of the phases Pivoting (Nachreiner) and Target Manipulation (Malone). Pivoting describes actions specifically aimed at tunneling traffic towards systems that are not directly accessible. Modeling this phase explicitly can be used to identify choke points in attacks, which may be crucial for the success or failure of an attack. Target Manipulation covers a broader range of objectives than the phases Collection and Exfiltration of MITRE's ATT&CK framework.

Through the Red Team case studies, the Social Engineering phase was added to the UKC, which can be modeled to make the role of users in raising organizational resilience explicit. Furthermore, the definition of the phases Weaponization and Delivery were extended while Exploitation and Defense Evasion were restricted, to develop a coherent set of tactics that covered all the identified attack phases. Maxims were developed regarding the application of the UKC in this thesis, such as modeling only successful attack paths and preferring the descriptions of actions with specialized phases over generic phases (*tempus specialis derogat tempori generali*). The Red Team case studies also allowed the arrangement of the UKC to be realigned up to the Lateral Movement phase, in accordance with the sequence observed in actual attacks.

In the APT28 case study, the UKC could be used to model all phases that were identified in APT28's attacks from the initial Reconnaissance up to the Exfiltration of confidential data. All phases of the UKC were identified at least once in the APT28 case study, with the notable exception of the generic phase Action on Objectives. The APT28 case study could also be used to test and realign the order up to but also from the Lateral Movement phase onwards, which covered the phases Collection, Exfiltration and Target Manipulation. Furthermore, it was proposed to detach and explicitly describe the Objectives, which refer to a threat actor's socio-technical objectives towards a strategical goal. On a more abstract level, these phases can collectively be described as Action on Objectives.

The development of the UKC resulted in an increasingly robust attack model. Overall, the UKC adds 11 unique attack phases to the CKC, of which 2 typically occur before the perimeter and 7 typically occur behind the perimeter. Another 2 phases have been observed to occur both before and behind the organization perimeter, namely Privilege Escalation and Credential Access. These numbers exclude the Objectives phase, because it is in part based on the original Action on Objectives phase from the CKC. 8 out of the 11 additional phases originate from MITRE's ATT&CK framework, which consists of 10 unique tactics (the phases Installation/Persistence and Command & Control are present in both the CKC and ATT&CK). The 3 further additions to the UKC are Social Engineering, Pivoting and Target Manipulation. Each of the 11 additional phases represents an additional opportunity to strengthen the resilience against APT attacks.

5.3 Applicability of the Unified Kill Chain (UKC)

Subsequently, an overview is provided of all phases that occurred in the case studies and have been assembled into the Unified Kill Chain (UKC) in comparison with the Cyber Kill Chain (CKC) and the actor specific Red Team (RT KC) and the APT28 (APT28 KC) kill chains. The presence or absence of these phases in the CKC, RT KC and APT28 KC respectively may lead to different conclusions for this research study, as previously detailed in Table 2 (on page 14).

Table 26 - Applied Conclusions Matrix

Unified Kill Chain	Cyber Kill Chain	Red Team Kill Chain	APT28 Kill Chain
Reconnaissance	✓	✓	✓
Weaponization	✓	✓	✓
Delivery	✓	✓	✓
Social Engineering	!	✓	✓
Exploitation	✓	✓	✓
Persistence	✓	✓	✓
Defense Evasion	✗	✓	✓
Command & Control	✓	✓	✓
Pivoting	✗	✓	✓
Discovery	✗	✓	✓
Privilege Escalation	✗	✓	✓
Execution	✗	✓	✓
Credential Access	✗	✓	✓
Lateral Movement	✗	✓	✓
Collection	!	✗	✓
Exfiltration	!	✗	✓
Target Manipulation	!	✗	✓
Objectives	!	!	✓

As Table 26 shows, 7 phases that can typically occur before the perimeter may be sufficiently modeled by the CKC (✓) and sufficiently emulated by the Red Team (✓). However, 1 phase that is counted is Social Engineering, which is only implicitly included as part of Exploitation in the CKC (!). In contrast, 7 phases that can typically occur behind the perimeter are not sufficiently modeled by the CKC (✗), but may be sufficiently emulated by the Red Team (✓).

The 3 phases that are objective-specific, namely Collection and Exfiltration, are not explicitly modeled by the CKC (!) and are not sufficiently emulated by the Red Team (✗). Instead, these tactics are collectively modeled as 1 phase by the CKC, namely Action on Objectives (!). Action on Objectives is only performed in a very limited form by the Red Team (!). In its generalized form, the Action on Objectives phase was not necessary to model APT28's attacks. The Objectives element of the phase was detached from the Action on Objectives phase, to make the socio-technical objectives towards achieving a strategic goal explicit (✓).

5.4 Comparison of Red Team and APT28 Attack Specific Kill Chains

The MO of Fox-IT’s Red Team and APT28 can be compared in more detail by comparing the composition of the attack specific kill chains rather than the actor specific kill chains (as performed in the previous section).

In Table 27 an overview is provided of the phases of the UKC and the attack specific kill chains C1-1 to C4-9. The overview is used in this section to identify notable convergences or divergences between these kill chains. In Table 27, a black line is used to demarcate phases that occur before and after *Command & Control* is established over an initially compromised system. Phases that are ~~struck through~~ are modeled in lieu of their actual occurrence. As previously argued for in section 3.3.3, this choice enables a more straight forward comparison between complete attack paths by including all phases that are thought to be required to an end-to-end attack.

The attack specific kill chains are qualitatively compared subsequently, since the sample size for the Red Team case studies is small, insufficient data is available regarding the frequency that the APT28 attack specific kill chains occur and because steps have been taken to reduce the number of unique attack specific kill chains which would skew quantitative approaches.

#	*Unified Kill Chain*
1	*Reconnaissance*
2	*Weaponization*
3	*Delivery*
4	*Social Engineering*
5	*Exploitation*
6	*Persistence*
7	*Defense Evasion*
8	*Command & Control*
9	*Pivoting*
10	*Discovery*
11	*Privilege Escalation*
12	*Execution*
13	*Credential Access*
14	*Lateral Movement*
15	*Collection*
16	*Exfiltration*
17	*Target Manipulation*
18	*Objectives*

Table 27 – Heatmap of UKC phases in CKC, RT and APT28 attack paths

UKC	*Red Team Attack Paths*									*APT28 Attack Paths*								
	C1-1	**C1-2**	**C1-3**	**C2-1**	**C-2**	**C3-1**	**C3-2**	**C3-3**	**C3-4**	**C4-1**	**C4-2**	**C4-3**	**C4-4**	**C4-5**	**C4-6**	**C4-7**	**C4-8**	**C4-9**
1	1	1	1	1	1	1	1	~~1~~	~~1~~	2	2	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	4	4	3	3	2	2	2	2	2	2	2
3	3	3	3	4	4	4	4	5	5	4	4	3	3	3	3	3	3	3
4	4	4	4	5	5	3	3	13	13	13	5	4	4	4	4	4	4	4
5	3	3	3	7	7	4	4	8	8	6	3	13	3	5	5	5	5	5
6	6	6	6	8	8	6	6	9	9	15	11	6	11	3	3	3	3	3
7	8	8	8	13	9	8	8	10	10	16	6	15	6	11	11	11	11	11
8	10	9	10	9	10	9	9	12	13	18	7	16	7	6	6	6	6	6
9	11	10	11	14	11	10	10	11	14		8	18	8	7	7	7	7	7
10	13	11	13	~~15~~	12	12	13	13	13		15		15	8	8	8	8	8
11	9	12	9	~~16~~	13	11	14	14	14		16		16	15	10	10	10	10
12	14	13	14	~~18~~	14	13	13	9	9		18		18	16	3	3	3	3
13	12	14	12		13	14	14	10	10					18	12	9	9	9
14	13	~~15~~	13		~~15~~	9	9	~~15~~	~~15~~						13	11	13	14
15	~~15~~	~~16~~	~~15~~		~~16~~	10	10	~~16~~	~~16~~						9	12	14	15
16	~~16~~	~~18~~	~~16~~		~~18~~	~~15~~	~~15~~	~~18~~	~~18~~						14	13	15	16
17	~~18~~		~~18~~			~~16~~	~~16~~								15	14	16	17
18						~~18~~	~~18~~								16	15	17	18
															17	16	18	
															18	17		
																18		

Generalized APT28 Attack Paths

The attack visualizations in sections 3.2.1, 3.3.1 and 3.4.1, as well as the attack paths and techniques detailed in Appendix C, show that attack paths vary significantly on an operational level. These differences are still noticeable but more limited at the tactical level of abstraction. Because this research study is aimed to raise resilience against the attacks of APT28, its attack specific kill chains serves as the basis for the following comparison. At the tactical level of abstraction, APT28's MO can be further generalized to three distinct APT28 attack paths (in accordance with the semi-structured interview of section 4.7):

- Spear phishing or watering hole attacks for credential theft to acquire data (C4-1 and C4-3);
- Spear phishing or watering hole attacks for infections to acquire data (C4-2, C4-4 and C4-5);
- Spear phishing or watering hole attacks for infections that require diagonal movement to manipulate targets and/or acquire data (C4-6 to C4-9).

Reconnaissance, Information Position and Targeting

The only tactical difference between the attack vectors phishing (C1, C3-1, C3-2, C4-3 to C4-9) and watering hole websites (C4-1 and C4-2) is the presence or absence of a Reconnaissance phase that is specific to the attack. The capability of a Red Team to perform watering hole attacks is limited, because these attacks typically involve weaponizing legitimate third-party infrastructure. The attacks by intelligence-driven actors such as APT28 can be regarded as a continuous cycle of attacking organizations to acquire data and leveraging the acquired data to prepare further attacks on the same or other organization(s). In contrast, Red Team assignments are typically one-off assignments that perform Reconnaissance by gathering intelligence from open sources on the target at the start of an assignment (OSINT), which puts the Red Team at a disadvantage from the start.

APT28 can leverage its information position to target very specific targets for credential theft or malware infections. When the information position is leveraged to steal credentials directly (C4-1 and C4-3), it is not necessary for the threat actor to perform Delivery, Installation or Command & Control in the CKC sense of these phases, because the use of a Remote Access Trojan (RAT) is not required when (web)mail is exposed to the internet. In the broader interpretation of the UKC, Delivery occurs through spear phishing e-mails and other techniques may be used to acquire Persistent access to the data. When APT28's information position is leveraged to infect the systems of high value targets directly (C4-2 and C4-4), data can be acquired without requiring further internal diagonal movements.

Weaponization and Delivery: the Malware Ecosystem

The malware ecosystem (part of the attack infrastructure as forged in the Weaponization) that can be leveraged by APT28 in Delivery is more extensive and modular than that of Fox-IT's Red Team. As a result, the Delivery of the components is more intermittent in APT28's attacks than in the attacks of the Red Team. The basis for the Delivery of the components is similar however, which consists of deploying a dropper and a payload. The deployment may be intermitted by other phases, such as Social Engineering (C1-1 to C1-3 and C4-3 to C4-9), Exploitation (C4-2 and C4-6 to C4-9), Privilege Escalation, Defense Evasion, Command & Control and local Discovery (C4-5 to C4-9). The capabilities offered by the ecosystems are also very similar, in that they enable data gathering and internal attacks paths consisting of phases such as Pivoting, Discovery, Credential Access and Lateral Movement.

Exploitation: zero-days and/or Social Engineering

Exploitation of vulnerabilities, which may or may not be used in combination with Social Engineering, is typically used by APT28 to Deliver its malware components to targeted systems. This frequently includes the use of exploits for previously unknown vulnerabilities (zero-days) in widely used third party software. The zero-day exploits may be used in broad campaigns, that target multiple organizations at once when these exploits become available. In contrast, the Red team typically exclusively relies on Social Engineering for Delivery of its malware components to the targeted systems. If previously unknown vulnerabilities are identified and zero-day exploits are developed during an assignment, these vulnerabilities are reported to the client and the vendor in accordance with Fox-IT's Corporate Social Responsibility (CSR) policy [44], which diminishes their value across multiple assignments.

Internal Attack Paths and Diagonal Movement

In contrast to APT28's MO, all attacks paths that were identified in the Red Team case studies focused on obtaining Command & Control over a system in the targeted network. After access to the targeted network is obtained, remote Discovery methods (that occur after Pivoting) are used by the Red Team to identify high value targets (for instance by enumerating users and groups in the Active Directory IAM). In the APT28 case study, the actor mostly appears to perform local Discovery, which may be due to their strong pre-existing information position.

Within the target network, the Red Team typically aims to perform Privilege Escalation to the highest privileges within the Identity and Access Management (IAM) infrastructure, as this generally allows Lateral Movement towards any asset. The case study of APT28's MO shows that the threat actor may also pave an internal attack path towards critical assets to achieve its objectives. These attack paths may be required if (web)mail is not directly exposed to the internet, if insufficient prior intelligence is available to select high value targets during Reconnaissance, if the less targeted watering hole attacks serve as the initial attack vector for Delivery of the malware components or if the objective is Target Manipulation.

The phases that APT28 goes through within target networks (C4-6 to C4-9) generally includes Privilege Escalation, Execution, Credential Access, Pivoting and Lateral Movement at some point in the attack path. The composition and even the sequence within which these internal attack phases occur notably converges between APT28 and Red Team attacks. For example, the internal attack paths of Red Team kill chains C1-2 and C2-2 converge with APT28 kill chain C4-7, in that Privilege Escalation, Execution, Credential Access and Lateral Movement occur in that specific sequence after Pivoting and before actions can be taken on the original objectives.

Action(s) on Objectives

In the Red Team assignments, the impact of attacks was typically shown by proving that access had been obtained to a supporting ICT asset (a "flag"). In the Red Team case studies, this activity was abstractly modeled as Action on Objectives. The phase was included in the Red Team attack specific kill chains, even though proving access may not entail taking any other actions towards the objectives (C2-1 to C3-4). As described in section 3.1, this limitation follows from the (purported) risks of disturbance to production systems resulting from the tests. In contrast, the presence of the phases Collection and Exfiltration is typical in APT28's attacks, which may be supplemented with Target Manipulation, that are intended to achieve Objectives on the socio-technical layer towards a strategic goal.

Comparison of Red Team Kill Chains with the Generalized APT28 Attacks Paths

Overall the Red Team kill chains (C1-1 to C3-4) contain the most similarities with APT28's attacks that use spear phishing or watering hole attacks to obtain infections that are followed by further diagonal movement to manipulate targets and/or acquire data (C4-6 to C4-9). Given the prevalence of the internal attack phases in all of the Red Team's attack paths (C1-1 to C3-4), the Red Team assessments are thought to be particularly well suited to assess the organizational resilience against the internal attack paths of APT28.

As workstations of low and high value targets were similarly configured in the Red Team case studies, the Red Team attacks are also thought to provide relevant insights into the organizational resilience against spear phishing or watering hole attacks that aim to obtain infections to acquire data (C4-2, C4-4 and C4-5). The spear phishing or watering hole attacks that directly aim to steal credentials to acquire data (C4-1 and C4-3) show the most divergence with the attacks paths of the Red Team. However, even for these cases a relevant part of the attack path is assessed, namely the resilience of users against social engineering based initial attack vectors.

Improving Threat Emulation of APT28 Attacks

The emulation of APT28 attacks by Fox-IT's Red Team can be improved to remedy some of the identified differences through the qualitative comparison in this section. Subsequently, a non-exhaustive list of potential improvements is suggested. Potential improvements that are thought to be outside the realm of realistic possibilities, such as increasing the resources of the Red Team to a nation state level, are not included. The following measures could be taken to improve Red Team assessments and their predictive value for APT28 attacks:

- The disadvantaged information position of the Red Team may be offset if clients provide more detailed information that a threat actor may acquire through nonpublic means:
  - This can include details regarding high value targets such as e-mail addresses;
  - This can include details regarding high value assets such as IP-addresses;
  - This can include details regarding the normal use of critical assets;
  - This can include credentials for third party level access to the targeted network.
- The disadvantaged information position of the Red Team can be further offset if assignments are occasionally repeated and information that was previously acquired, for example regarding high value targets, assets, privileges and credentials, can be re-used.
- The threat emulation of APT28 can be further improved by specifically targeting high value targets with credential theft attacks through social engineering (similar to C4-1 and C4-3).
- The assessment of the resilience of organizations against objective-specific tactics, such as Collection, Exfiltration and Target Manipulation, can be improved by explicitly performing activities towards presumable threat actor Objectives. To minimize the risk of disturbing critical production assets, clients could provide support regarding the use of these assets.
- Atomic Red Team testing strategies can be adopted, which aim to repeatedly perform small detection tests of techniques that map back to particular MITRE ATT&CK tactics [58]. After executing the test, evidence can be collected and improvements in (prevention and) detection can be developed to raise resilience. This strategy can be performed in a cyclic manner, which also allows progress to be measured over time. Specific atomic Red Team tests can also be performed after measures have been implemented following an end-to-end Red Team test, to assess the improvements. Furthermore, atomic Red Team tests may be performed to specifically test tactics and techniques that cannot be incorporated into the end-to-end tests because of legal, ethical, resource, budget or efficiency limitations.

6 Reflection

6.1 Methodology used to develop the UKC

Without a thorough understanding of how modern attacks take place, investments in defensive capabilities are expected to be inefficiently distributed over the attack surface of organizations. In this thesis, the Unified Kill Chain (UKC) was developed iteratively in search of a kill chain model that could be used to analyze, compare and defend against attacks by APTs such as APT28. The search process showed that the end-to-end attacks by APTs do not necessarily align with the sequence of attack phases posited by the Cyber Kill Chain (CKC). A crucial hypothesis in the CKC, namely that all attacks follow a deterministic sequential pattern, was falsified in the case studies. Instead, the search process for the UKC resulted in a meta-model that can be used to develop attack specific and actor specific kill chains.

A first version of the UKC model was developed through literature study and by uniting existing models. Subsequently, attack specific kill chains were developed from transparent attack paths as executed by Fox-IT's Red Team. In this step, the attack specific kill chains were developed using the building blocks in the first version of the UKC, which were extended and realigned where necessary. This process, in which observed activities in the Red Team case study were matched with tactics in the UKC in their ordered arrangement, resulted in the description and sequence of the phases of the analyzed attacks and a revised UKC.

Since this process in the Red Team case study was performed using the building blocks of the first version of the UKC, this step is not thought to be a fully independent validation of the correctness and completeness of the tactics in the UKC. The fact that the tactics in the developed UKC sufficed to model all phases of the attacks in the subsequent APT28 case study, however, shows that the tactics in the UKC model *can* be adequate to describe end-to-end APT attacks on a tactical level. Furthermore, both case studies are thought to be reasonable validations of the *ordered arrangement* of these tactics, which distinguishes the time-agnostic tactics from the phases of attacks.

6.2 Added value of the UKC

The UKC meta-model can be used to develop attack specific and actor specific kill chains. The attack specific kill chains can be used to analyze the intricacies of individual attacks. Multiple attack specific kill chains can be compared to show how these attacks converge or diverge on a tactical level and to realign defenses accordingly. The actor specific kill chains demonstrate the tactics that are in a specific actor's repertoire in their presumable ordered arrangement. As such, an actor specific kill chain encompasses all tactics that have been observed in the attacks by that threat actor and forms the relevant subset of the UKC for that threat actor. In defending against the threat actor, a defense strategy can be created with the relevant tactics (which are potential attack phases) in mind.

The incorporation of both the CKC phases and MITRE's ATT&CK tactics into one UKC, means that the (re)designed kill chain model can hit the ground running by combining and extending the established models' explanatory power to model attacks end-to-end. Additionally, the following improvements to the pre-existing models are thought to be particularly noteworthy:

- The insights into the ordered arrangement of tactics, or how they occur as phases in actual attacks, offer a significant improvement over MITRE's existing time-agnostic ATT&CK model. Understanding how and why tactics occur in distinct sequences as phases within attacks is valuable in developing an adequate defense-in-depth strategy.
- Recognizing the critical role of choke points in attacks by explicitly modeling Pivoting is expected to be highly beneficial for developing defense strategies. If segmentation is strictly

applied, encompassing both the network and Identity and Access Management layers, each pivot point is expected to force an attacker to start anew in the targeted environment from the first ATT&CK phase(s). As such, the UKC provides the relevant context for the applicability of the ATT&CK framework, which can occur in its entirety between every two Pivoting phases or between a Pivoting phase and the objective-specific tactics (see Figure 16 on page 78).

- The broader interpretation of the Weaponization phase overcomes previous criticisms, as it makes logically distinct, relevant and observable preparatory attacker activities actionable. In both the Red Team and APT28 case studies, this could have led to the early detection of imminent attacks in which typo-squatted phishing domains were used.
- By separating Social Engineering in the UKC from the Exploitation phase in the CKC, the role of users in the execution of attacks can be made explicit in modeling attacks. These insights can be incorporated into security awareness training to secure the assets of an organization.
- The objective-specific tactics of the CKC and ATT&CK models were extended and redefined. The addition of Target Manipulation allows the UKC to model a broader range of APT objectives, that for example includes sabotage in addition to espionage and now covers the Confidentiality, Integrity and Availability (CIA) triad in full. Making Objectives explicit forces defenders to take the socio-technical objectives of attackers into account in the application and interpretation of kill chains, which is expected to be beneficial for a deeper level of understanding of the interconnection and targets of attacker activities.

6.3 Potential difficulties for the UKC

Two potential difficulties for modeling attacks through linear models such as the UKC (and the CKC) were identified in the case studies. Firstly, successful attacks may materialize in the form of a tree structure, in which some branches fail and (at least) one branch successfully leads to the objective, as discussed in section 3.2.2. Secondly, some phases of an attack may occur in a loop until a condition or an objective is met, as shown in section 3.5.1. The UKC is thought to be able to sufficiently accommodate these potential difficulties:

- Each branch of the attack tree can be modeled using the UKC as a unique attack path. In this research study, modeling was restricted to successful attack paths because these are believed to offer the most value. Most real-life attacks are presumably based on one successful attack path (in addition to the potential unsuccessful paths), which could be modeled with one attack specific kill chain. Further research into unsuccessful attack paths may be beneficial however, as this could show why and how other attack paths are thwarted.
- The loops of phases that may occur in the MO of an attacker are not expected to pose a significant hurdle for the UKC, as the linear representation of such these sequence as longer chains sufficed in the case studies. Nonetheless, variants and visualizations of the UKC could be developed that incorporate one or more loops into the otherwise linear chain of events, which limit the length of the chain that is required to model the relevant phases. Identifying loops may be beneficial, as phases that are repeated in a single attack path are expected to offer a higher return on security investment.

6.4 Level of abstraction of the UKC

In the development of the UKC, the choice was made to model phases in accordance with the maxim *tempus specialis derogat tempori generali* (section 3.2.3). The application of this maxim resulted in shorter kill chains that focus on what the attacker aims to accomplish tactically, at the expense of the technical completeness of the kill chain's description of the chain of events. However, the UKC could also be used to model the complete chain of events for a less abstract but technically more complete model of the chain of events as required.

Alternatively, further abstraction of the UKC is possible to explain the tactical chain of events to a management-orientated audience. For example, in the UKC and the kill chains C1-1 to C3-4 and C4-6 to C4-9, the collective phases of the CKC could be described as “initial compromise” or “initial foothold”. The relevant ATT&CK phases could be described with terms such as “diagonal movement” or “network propagation”. Collections of relevant ATT&CK phases may be separated by “choke points” (Pivoting). Ultimately, successful diagonal movement or network propagation results in sufficient privileges and access to allow an actor to perform “action on objectives”. Figure 16 shows an abstraction of the UKC, based on an infrastructure as encountered in Red Team case study C3.

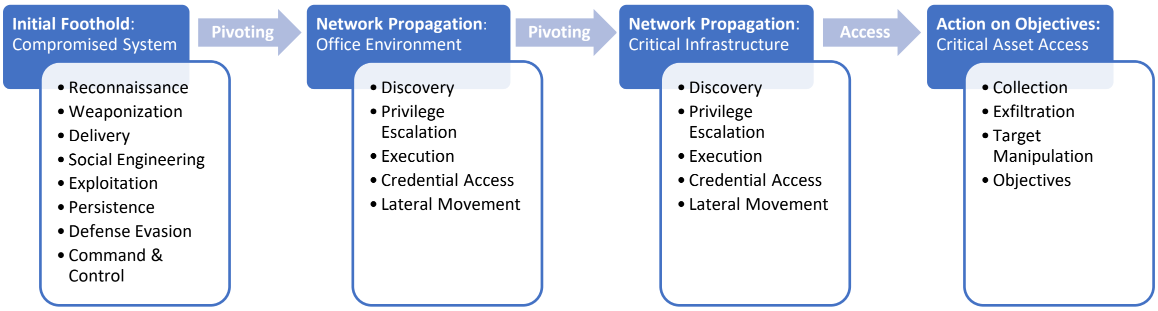


Figure 16 – A further abstraction of the UKC for a management-orientated audience

6.5 Broader applicability of the UKC

The scope of the cases studies was limited to one Red Team and one APT, for reasons that were previously outlined. The limited scope naturally raises the question if the value of the UKC may extend beyond these initial case studies. To touch upon an answer on this question, the applicability of the UKC on the attacks of APT29 was briefly examined.

APT29 is also known as Cozy Bear and its attacks have been attributed to the Russian civilian intelligence service FSB [49]. The tactical end-to-end attack paths of APT29 appear to be similar to those of APT28, even though operational techniques are only partially shared and the prior is generally stealthier than the latter [59]. APT29 has also used tactics in its attacks that extend beyond the CKC, such as Privilege Escalation [60], Credential Access [61] and Lateral Movement [62] within targeted networks. Furthermore, APT29 has also used Pivoting in its internal attacks paths [62], which is not explicitly modeled by ATT&CK.

The applicability of the UKC may even extend beyond targeted attacks by APTs and be relevant for the prevention of modern malware attacks. In 2017, at least three major ransomware worms surfaced that infected many hundreds of thousands of computers worldwide[12] [64]. The ransomware worms crippled critical assets at hospitals [64], banks, power companies, metro stations and airports [65]. The reported losses amounted to approximately a billion (10^9) USD at three multinationals alone from just one of these worms [66] [67] [68]. These unprecedented attacks have been attributed to North Korean [69] and Russian APTs [70] [71].

[12] Both the NotPetya and the BadRabbit worms were specifically restricted to spread only within targeted networks, but incidentally infected systems globally. This demonstrates that “*there is a Shadow Internet of linked networks that provides pathways to compromise targets globally without targeting public facing Internet systems*” [63]. The interconnectedness of modern internal networks is accompanied with transitive risks that provide further support for the argument that defensive efforts should extend beyond protecting the perimeter between internal networks and the Internet.

The ransomware worms implemented tactics that were previously primarily seen in targeted attacks:

- The *WannaCry* worm exploited a Privilege Escalation vulnerability with the EternalBlue exploit within internal networks, after Pivoting from an internet facing system, to perform Target Manipulation (file encryption) [72].
- The *NotPetya* worm relied a range of tactics in addition to Privilege Escalation via EternalBlue to propagate through networks. The worm also used the tactics Pivoting (to reserved IP spaces), (local and network) Discovery, Execution (via PsExec and WMI), Credential Access (via a *mimikatz* variant), Lateral Movement (via the acquired credentials) and Target Manipulation (file and disk encryption) [73].
- The BadRabbit worm relied on similar tactics as NotPetya. BadRabbit used the tactics Social Engineering (enticing users to install a fake Flash player), Pivoting (to reserved IP spaces), (network) Discovery (for SMB shares), Privilege Escalation (via EternalRomance), Execution (via RunDLL32, scheduled tasks and WMI), Credential Access (via a *mimikatz* variant and brute force attempts), Lateral Movement (via the acquired credentials) and Target Manipulation (file and disk encryption) [74].

The tactics that were used by these worms, namely Pivoting, Discovery, Privilege Escalation, Execution, Credential Access, Lateral Movement and Target Manipulation were also identified in the Red Team and the APT28 case studies. The similarities with the case studies even exist on the level of operational techniques (such as the use of EternalBlue, mimikatz, RunDLL32 and PsExec). Each of these tactics extends beyond the traditional CKC, while Social Engineering, Pivoting and Target Manipulation also extend beyond the ATT&CK framework. All identified tactics are modeled as phases in the UKC, which largely aligns with the hard-coded sequence within which these tactics are executed. As such, the UKC may not only prove useful to raise the resilience of targeted organizations against targeted APT attacks but also of (un)targeted organizations against other APT cyber attacks such as modern ransomware worms.

6.6 Realigning defense strategies with the UKC

The evidence that attack phases may be bypassed by APTs challenges the foundational assumption of the CKC that APT attacks can by thwarted by disrupting any one of the phases in the chain of events (section 5.1). Based on this assumption in the traditional CKC, defenders may naturally focus their efforts on disrupting APT attacks at the earliest attack phases. The fact that attack phases can be bypassed however affects defensive strategies fundamentally. In bypassing an attack phase, an attacker may also bypass the security controls that apply specifically to that phase. Instead of focusing on thwarting attacks at the earliest point in time, defensive strategies that focus on phases that either occur with a higher frequently or that are vital for the attack path are expected to be more successful. This notably includes creating, securing and monitoring choke points that force attackers to pivot before they can act on their original objectives.

In the case studies, multiple attack phases were identified that are not explicitly modelled as separate phases in the CKC, but which may be necessary for APTs to act on their original objectives. These additional phases typically occur after one system in the internal network has initially been compromised and before the critical supporting ICT assets can be compromised. These attack phases are executed within the confines of an organization’s internal network and thus occur within the locus of control of defenders. It is challenging to prevent the compromise of every single internet connected system in a large network, while the number of critical supporting assets is typically far more limited. Strategies that aim to defend a limited amount of critical supporting assets may thus be more likely to succeed than strategies that aim to defend all internet connected systems.

Organizations can therefore potentially significantly increase their resilience, by focusing their efforts on the attack phases that occur within the confines of their internal network that pave the path for APTs to act on their objectives.

The APT28 case study showed that the threat actor can leverage zero-day exploits in their attacks. All zero-days that were identified in the APT28 case study targeted the system that was initially compromised, which can provide an initial foothold to the target network. APT28 has also gained access to targeted networks via compromised third party VPN access [75]. Both facts provide further support for the argument that defenders should not just focus their efforts on protecting all internet connected systems. In defending against attacks such as those by APT28, defenders should adopt the principles Assume Breach [76, p. 20] and Defense in Depth [77] to develop layered defense strategies that assume that every control could fail. With these principles in mind, defense strategies can be developed or realigned after mapping existing capabilities in the areas know, prevent, detect, respond and recover of NIST's Cyber Security Framework [28] to the relevant UKC phases given the organization's threat model.

7 Conclusion

The primary driver for this thesis was to raise the resilience of organizations and societies against cyber attacks by improving attack modeling through kill chains and Red Team assessments. The improvement was shown to be required, as the industry standard Cyber Kill Chain® (CKC) model fails to accurately and comprehensively model cyber attacks by Advanced Persistent Threats (APTs), despite its explicit aim to do so. The CKC is limited to modeling the initial compromise of systems behind the organizational perimeter with malware through specific attack vectors such as phishing. As such, the CKC reinforces perimeter-focused and malware-prevention defensive strategies.

To overcome the deficiencies of the CKC, a Unified Kill Chain (UKC) was iteratively developed through literature study and case studies. The UKC amongst others unites the CKC with MITRE's ATT&CK™ framework to cover attack phases in additional attack vectors and attack paths that occur behind the perimeter and within the locus of control of targeted organizations. The resulting UKC is a meta-model that can be employed to develop attack specific and actor specific kill chains to support the analysis, comparison and defense against the (un)targeted end-to-end attacks of APTs. The UKC supported the analysis and comparison of the attacks of Fox-IT's Red Team and APT28 in the identified attack paths. The comparison showed that both actors may use a similar range of tactics that occur in similar sequences to form attacks paths to achieve their objectives within internal networks of targeted organizations. Notable differences were also identified in the MO of these actors, signifying the potential to improve the predictive value of the Red Team assessments.

A conventional belief within cyber security is that attackers have the upper hand, because they only need to exploit one defensive flaw. The CKC promised a fundamentally reversed balance, by claiming that defenders could prevail by disrupting attackers at any point in their deterministically phased progression. The claim of the UKC is more limited than that of the CKC. Advanced attacks can be regarded as phased progressions, but phases of the UKC may be bypassed, occur more than once or out of sequence. The balance between attackers and defenders suggested by the UKC is thus more delicate than is assumed by the defeatist adage or promised by the CKC. Raising resilience against the phased progressions of APTs is possible by developing threat actor specific kill chains using the UKC, that align with an organization's threat model, and developing a layered defense strategy that adopts the assume breach and defense in depth principles.

In future research, the UKC could be evaluated and potentially further refined through the study of a broader range of (un)targeted end-to-end cyber attacks by various threat actors. Additional case studies could validate the UKC or potentially identify additional tactics that could be incorporated. This applies in particular to the objective-specific phases, as the relevant data in this thesis primarily originates from the APT28 case study. Empirical research into the prevalence of UKC phases could identify which phases are more likely to occur. Similarly, research into the occurrence of loops in attack paths could help to identify phases that offer a higher return on security investment. The UKC was used to linearly represent successful branches of tree shaped attacks paths. Further research into failed branches could help to gain insights into how attack paths are thwarted in practice.

Organizations and societies as a whole are becoming increasingly dependent on Information and Communication Technology (ICT). In lieu of an effective global cyber governance structure or effective deterrents, cyber attacks can be highly effective methods for APTs to achieve their socio-technical objectives towards strategic goals and are thus expected to increase in number and in force. The UKC and improved Red Team assessments could be valuable to decelerate this trend, by allowing the structured analysis and comparison of past cyber attacks and by providing a solid basis to develop (or realign) defensive strategies to raise resilience against cyber attacks in the future.

8 References

[1] Fancy Bear, “Fancy Bears’ HT (@FancyBears),” *Twitter*. [Online]. Available: https://twitter.com/FancyBears/. [Accessed: 26-Oct-2017].

[2] G. Engel, “Deconstructing The Cyber Kill Chain,” *Dark Reading*. [Online]. Available: http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542. [Accessed: 27-Apr-2017].

[3] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” *Lead. Issues Inf. Warf. Secur. Res.*, vol. 1, p. 80, 2011.

[4] J. van den Berg *et al.*, “On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education,” in *Proc. NATO STO/IST-122 symposium*, Talinn, 2014.

[5] International Electrotechnical and International Organization for Standardization, “ISO/IEC 27005:2011.”

[6] E. van Luit, P. Pols, and V. de Vries, “Enhancing the Bowtie Model for Security Risk Assessments [S1M2A3].” Cyber Security Academy.

[7] “CSRC - Glossary.” [Online]. Available: https://beta.csrc.nist.gov/Glossary/?term=2856. [Accessed: 05-Jul-2017].

[8] C. Peake, “Red Teaming: The Art of Ethical Hacking.” SANS Institute InfoSec Reading Room, 16-Jul-2003.

[9] FireEye iSight Intelligence, “FireEye | APT28: At The Center Of The Storm,” Jan-2017. [Online]. Available: https://www2.fireeye.com/WEB-2017-RPT-APT28.html. [Accessed: 24-Oct-2017].

[10] Department of Homeland Security, “Joint Statement on Election Security,” 07-Oct-2016. [Online]. Available: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national. [Accessed: 31-Jul-2017].

[11] “WikiLeaks - Search the DNC email database.” [Online]. Available: https://wikileaks.org/dnc-emails/. [Accessed: 05-Oct-2017].

[12] CNN, “Exclusive: Russian-linked Facebook ads targeted Michigan, Wisconsin,” *CNN*. [Online]. Available: http://www.cnn.com/2017/10/03/politics/russian-facebook-ads-michigan-wisconsin/index.html. [Accessed: 05-Oct-2017].

[13] New York Times, “Live Presidential Forecast,” *The New York Times*, 09-Nov-2016. [Online]. Available: http://www.nytimes.com/elections/forecast/president. [Accessed: 05-Oct-2017].

[14] H. Enten, “How Much Did WikiLeaks Hurt Hillary Clinton?,” *FiveThirtyEight*, 23-Dec-2016. [Online]. Available: https://fivethirtyeight.com/features/wikileaks-hillary-clinton/. [Accessed: 05-Oct-2017].

[15] M. de Bruijne, M. van Eeten, C. Hernández Gañán, and W. Pieters, “Towards a new cyber threat actor typology,” Delft University of Technology, Jun. 2017.

[16] Algemene Inlichtingen- en Veiligheidsdienst [AIVD], “Jaarverslag 2016,” 04-Apr-2017. [Online]. Available: https://www.aivd.nl/publicaties/jaarverslagen/2017/04/04/jaarverslag-2016. [Accessed: 29-Sep-2017].

[17] K. Lieber, “The Offense-Defense Balance and Cyber Warfare,” 2014. [Online]. Available: http://calhoun.nps.edu/handle/10945/40037. [Accessed: 01-Sep-2017].

[18] C. J. Rogers, “Strategy, Operational Design, and Tactics.” [Online]. Available: https://www.academia.edu/13085191/Strategy_Operational_Design_and_Tactics. [Accessed: 22-Sep-2017].

[19] Defense Technical Information Center (DTIC), “Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, As Amended Through 15 June 2015,” Jun. 2015.

[20] F. Vraalsen, F. den Braber, M. S. Lund, and K. Stølen, “The CORAS Tool for Security Risk Analysis,” in *Trust Management*, 2005, pp. 402–405.

[21] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Q*, vol. 28, no. 1, pp. 75–105, Mar. 2004.

[22] Gartner, "Defending against Advanced Threats: Addressing the Cyber Kill Chain," 15-Aug-2014. [Online]. Available: http://informationsecurity.report/Resources/Whitepapers/20cb712c-870f-4686-8769-968e399137cd_Addressing%20the%20Cyber%20Kill%20Chain%20-%20Are%20you%20prepared.pdf. [Accessed: 08-May-2017].

[23] National Institute of Standards and Technology, "SP 800-61 - Computer Security Incident Handling Guide," *Spec. Publ. NIST SP - 800-61*, Jan. 2004.

[24] S. Mitropoulos, D. Patsos, and C. Douligeris, "On Incident Handling and Response: A state-of-the-art approach," *Comput. Secur.*, vol. 25, no. 5, pp. 351–370, Jul. 2006.

[25] U.S. Department of Defense, "Joint Publication 3-60 Joint Targeting." Apr-2007.

[26] R. Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *Int. Secur.*, vol. 41, no. 3, pp. 72–109, Feb. 2017.

[27] U.S. Department of Defense, "Joint Publication 3-13 Information Operations." Feb-2006.

[28] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[29] Patrick Reidy, "Combating the Insider Threat at the FBI," presented at the Blackhat USA 2013.

[30] Matt Devost, "Every Cyber Attacker is an Insider," *OODA Loop*, 19-Feb-2015. [Online]. Available: https://www.oodaloop.com/osint/cyber/2015/02/19/every-cyber-attacker-insider/. [Accessed: 18-Sep-2017].

[31] ISACA, *Advanced Persistent Threats: How to Manage the Risk to your Business*. Isaca, 2013.

[32] M. Laliberte, "A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack," *Dark Reading*. [Online]. Available: http://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952. [Accessed: 09-May-2017].

[33] C. Nachreiner, "Kill Chain 3.0: Update the cyber kill chain for better defense," *Help Net Security*, 10-Feb-2015. [Online]. Available: https://www.helpnetsecurity.com/2015/02/10/kill-chain-30-update-the-cyber-kill-chain-for-better-defense/. [Accessed: 10-May-2017].

[34] B. D. Bryant and H. Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software," *Comput. Secur.*, vol. 67, pp. 198–210, Jun. 2017.

[35] S. Malone, "Using an expanded cyber kill chain model to increase attack resiliency," *BlackHat USA*, 09-Mar-2016. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf. [Accessed: 10-May-2017].

[36] MITRE, "MITRE Research Opens Window into Cyber Attacker Behavior," *The MITRE Corporation*, 16-Jun-2015. [Online]. Available: https://www.mitre.org/news/press-releases/mitre-research-opens-window-into-cyber-attacker-behavior. [Accessed: 19-Sep-2017].

[37] B. E. Strom *et al.*, "Finding Cyber Threats with ATT&CK^{TM}-Based Analytics," 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att&ck-based-analytics.pdf. [Accessed: 19-Sep-2017].

[38] Ketil Stølen, "The CORAS Method." [Online]. Available: http://coras.sourceforge.net/. [Accessed: 19-Sep-2017].

[39] H. Dahl, I. Hogganvik, and K. Stølen, *Semantics for the CORAS Security Risk Modelling Language*. 2007.

[40] "Red Teaming - Fox-IT (ENG)," *Fox-IT (ENG)*. [Online]. Available: https://www.fox-it.com/en/our-technology-services/product/red-teaming/. [Accessed: 05-Jul-2017].

[41] MITRE ATT&CK, "MITRE ATT&CK Twitter," *@MITREattack*, 03-Oct-2017. [Online]. Available: https://twitter.com/MITREattack/status/921371131281633280. [Accessed: 22-Oct-2017].

[42] U. Nayak and U. H. Rao, *The InfoSec Handbook: An Introduction to Information Security*. Apress, 2014.

[43] "Avoid Phone Scams | Cybercriminal Tech Support Scam | Security Threats." [Online]. Available: https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx. [Accessed: 12-Oct-2017].

[44] Fox-IT, B. Slob, and P. Pols, “Corporate Social Responsibility policy,” *Fox-IT (ENG)*, 02-Mar-2015. [Online]. Available: https://www.fox-it.com/en/about-fox-it/corporate-social-responsibility/. [Accessed: 29-Nov-2017].

[45] M. J. Ranum, “Thinking about firewalls V2.0: Beyond perimeter security,” *Inf. Secur. Tech. Rep.*, vol. 2, no. 3, pp. 33–45, Jan. 1997.

[46] “ATT&CK Matrix - enterprise.” [Online]. Available: https://attack.mitre.org/wiki/ATT%26CK_Matrix. [Accessed: 14-Oct-2017].

[47] ESET, “En Route with Sednit,” Oct-2016. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-full.pdf. [Accessed: 25-Oct-2017].

[48] Securelist, “Sofacy APT hits high profile targets with updated toolset,” *Securelist - Information about Viruses, Hackers and Spam*, 04-Dec-2015. [Online]. Available: https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/. [Accessed: 24-Oct-2017].

[49] CrowdStrike, “Bears in the Midst: Intrusion into the Democratic National Committee,” 15-Jun-2016. [Online]. Available: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/. [Accessed: 24-Oct-2017].

[50] U.S. Senate Select Committee on Intelligence and E. Rumer, “Russian Active Measures and Influence Campaigns,” *Carnegie Endowment for International Peace*. [Online]. Available: http://carnegieendowment.org/2017/03/30/russian-active-measures-and-influence-campaigns-pub-68438. [Accessed: 27-Oct-2017].

[51] TrendMicro and F. Hacquebord, “Two Years of Pawn Storm,” 2017. [Online]. Available: https://resources.trendmicro.com/rs/945-CXD-062/images/2017-Q2-EMEA-EN-wp-two-years-of-pawn-storm.pdf. [Accessed: 25-Oct-2017].

[52] The Department of Homeland Security (DHS), “GRIZZLY STEPPE – Russian Malicious Cyber Activity,” 29-Dec-2016. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf. [Accessed: 24-Oct-2017].

[53] M. Galeotti, *Putin’s hydra: inside Russia’s intelligence services*. European Council on Foreign Relations, 2016.

[54] Google Security Team, “Peering Into the Aquarium: Analysis of a Sophisticated Multi-Stage Malware Family,” 05-Sep-2014. [Online]. Available: https://assets.documentcloud.org/documents/3461560/Google-Aquarium-Clean.pdf. [Accessed: 24-Oct-2017].

[55] Microsoft, “Microsoft Security Intelligence Report,” Volume 19, Jun. 2015.

[56] Bitdefender, “APT28 Under the Scope: A Journey into Exfiltrating Intelligence and Government Information,” 17-Dec-2015. [Online]. Available: https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf. [Accessed: 25-Oct-2017].

[57] FireEye Threat Research Blog, “APT28 Targets Hospitality Sector, Presents Threat to Travelers,” *FireEye*, 11-Aug-2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html. [Accessed: 24-Oct-2017].

[58] Red Canary, “atomic-red-team: Small and highly portable detection tests.,” 01-Nov-2017. [Online]. Available: https://github.com/redcanaryco/atomic-red-team. [Accessed: 01-Nov-2017].

[59] F-Secure, “The Dukes: 7 Years Of Russian Cyber-Espionage,” *News from the Lab*, 17-Sep-2015. [Online]. Available: https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/. [Accessed: 05-Nov-2017].

[60] M. Dunwoody and FireEye, “APT29 Domain Fronting With TOR,” *FireEye*, 27-Mar-2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html. [Accessed: 05-Nov-2017].

[61] Symantec, "'Forkmeiamfamous': Seaduke, latest weapon in the Duke armory," *Symantec Security Response*, 13-Jul-2015. [Online]. Available: http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory. [Accessed: 05-Nov-2017].

[62] M. Dunwoody, N. Carr, and FireEye, "No Easy Breach: Challenges and Lessons from an Epic Investigation," presented at the DerbyCon 2016, Mar-2016.

[63] the grugq, "The Shadow Internet," *Comae Technologies*, 27-Oct-2017. [Online]. Available: https://blog.comae.io/the-shadow-internet-d42b7195a118. [Accessed: 06-Nov-2017].

[64] Department of Health - National Audit Office (UK), "Investigation: WannaCry cyber attack and the NHS," Oct. 2017.

[65] T. Fox-Brewster, "Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry," 27-Jun-2017. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/. [Accessed: 05-Nov-2017].

[66] MAERSK, "Interim Report Q2 2017 (OMX:MAERSKA)." [Online]. Available: http://investor.maersk.com/releasedetail.cfm?ReleaseID=1037421. [Accessed: 05-Nov-2017].

[67] FedEx TNT, "FedEx Corp. Reports First Quarter Earnings," *About FedEx*, 17-Sep-2017. [Online]. Available: http://about.van.fedex.com/newsroom/fedex-corp-reports-first-quarter-earnings-2/. [Accessed: 05-Nov-2017].

[68] Saint-Gobain, "First-half 2017 results," 27-Jul-2017. [Online]. Available: https://www.saint-gobain.com/sites/sgcom.master/files/cp_va_resultats_s1_2017_t.pdf. [Accessed: 05-Nov-2017].

[69] Reuters, "Britain believes North Korea was behind 'WannaCry' NHS cyber attack," *Reuters*, 27-Oct-2017. [Online]. Available: https://www.reuters.com/article/us-britain-security-northkorea/britain-believes-north-korea-was-behind-wannacry-nhs-cyber-attack-idUSKBN1CW153. [Accessed: 06-Nov-2017].

[70] P. Polityuk, "Ukraine points finger at Russian security services in recent cyber attack," *Reuters*, 01-Jul-2017. [Online]. Available: https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-says-russian-security-services-involved-in-recent-cyber-attack-idUSKBN19M39P. [Accessed: 06-Nov-2017].

[71] P. Polityuk and M. Williams, "Ukraine says NotPetya hackers likely behind BadRabbit malware," *Reuters*, 31-Oct-2017. [Online]. Available: https://www.reuters.com/article/us-cyber-summit-ukraine/ukraine-says-notpetya-hackers-likely-behind-badrabbit-malware-idUSKBN1D02D1. [Accessed: 06-Nov-2017].

[72] M. van Dantzig, "Massive outbreak of ransomware variant infects large amounts of computers around the world," *Fox-IT International blog*, 12-May-2017. [Online]. Available: https://blog.fox-it.com/2017/05/12/massive-outbreak-of-ransomware-variant-infects-large-amounts-of-computers-around-the-world/. [Accessed: 05-Nov-2017].

[73] K. de Mik, "FAQ about PETYA/GOLDENEYE/PETR outbreak," *Fox-IT International blog*, 28-Jun-2017. [Online]. Available: https://blog.fox-it.com/2017/06/28/faq-about-petya-outbreak/. [Accessed: 05-Nov-2017].

[74] N. Biasini and Talos, "Threat Spotlight: Follow the Bad Rabbit," 24-Oct-2017. [Online]. Available: http://blog.talosintelligence.com/2017/10/bad-rabbit.html. [Accessed: 06-Nov-2017].

[75] M. Suiche, "Lessons from TV5Monde 2015 Hack," *Comae Technologies*, 10-Jun-2017. [Online]. Available: https://blog.comae.io/lessons-from-tv5monde-2015-hack-c4d62f07849d. [Accessed: 31-Oct-2017].

[76] R. Pompon, *IT Security Risk Control Management: An Audit Preparation Plan*. Apress, 2016.

[77] D. of H. Security, *Control Systems Cyber Security: Defense in Depth Strategies*. CreateSpace Independent Publishing Platform, 2014.

[78] FireEye, "APT28 - A Window Into Russia's Cyber Espionage Operations?," 27-Oct-2014. [Online]. Available: https://www2.fireeye.com/apt28.html. [Accessed: 24-Oct-2017].

[79] SecureWorks, “Hillary Clinton Email Targeted by Threat Group-4127,” 16-Jun-2016. [Online]. Available: https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign. [Accessed: 24-Oct-2017].

[80] Palo Alto Networks, “New Sofacy Attacks Against US Government Agency,” *Palo Alto Networks Blog*, 14-Jun-2016. [Online]. Available: https://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/. [Accessed: 24-Oct-2017].

[81] Palo Alto Networks and R. Falcone, “XAgentOSX: Sofacy’s XAgent macOS Tool,” *Palo Alto Networks Blog*, 14-Feb-2017. [Online]. Available: https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/. [Accessed: 25-Oct-2017].

[82] FireEye Threat Research Blog, “Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia’s APT28 in Highly-Targeted Attack,” *FireEye*, 18-Apr-2015. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html. [Accessed: 24-Oct-2017].

[83] P. Kafeine, “APT28 racing to exploit CVE-2017-11292 Flash vulnerability before patches are deployed,” 19-Oct-2017. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed. [Accessed: 24-Oct-2017].

[84] Palo Alto Networks, “Technical Walkthrough: Office Test Persistence Method Used In Recent Sofacy Attacks,” *Palo Alto Networks Blog*, 20-Jul-2016. [Online]. Available: https://researchcenter.paloaltonetworks.com/2016/07/unit42-technical-walkthrough-office-test-persistence-method-used-in-recent-sofacy-attacks/. [Accessed: 24-Oct-2017].

[85] A.-S. K. Pathan, *Securing Cyber-Physical Systems*. CRC Press, 2015.

Appendix A The Unified Kill Chain

Table 28 - The Unified Kill Chain

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Delivery	• Techniques resulting in the transmission of a weaponized object to the targeted environment.
Social Engineering	• Techniques aimed at the manipulation of people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Defense Evasion	• Techniques an attacker may specifically use for evading detection or avoiding other defenses.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its network environment.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on a system or network.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Credential Access	• Techniques resulting in the access of, or control over, system, service or domain credentials.
Lateral Movement	• Techniques that enable an adversary to horizontally access and control other remote systems.
Collection	• Techniques used to identify and gather information from a target network prior to exfiltration.
Exfiltration	• Techniques that result or aid in an attacker removing files and information from a target network.
Target Manipulation	• Techniques aimed at manipulation of the target system to achieve the objective of the attack.
Objectives	• Socio-technical objectives of an attack that are intended to achieve a strategic goal.

Appendix B Red Team Attack Specific Kill Chains

Case study 1: Phishing for a foothold to pave a path for admin-level access to supporting asset (C1-1)

Table 29 – Case Study 1– Attack Path 1: the User-Level Access Kill Chain (C1-1)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on a system or network.
Credential Access	• Techniques resulting in the access of, or control over, local administrator credentials.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Execution	• Techniques that result in execution of attacker-controlled code on a local or remote system.
Credential Access	• Techniques resulting in the access of, or control over, user-level credentials to a supporting asset.
Action on Objectives	• Post-comprimise actions on the objectives, such as the controlled release of (mis)information.

Case study 1: Phishing for a foothold to pave a path for admin-level access to supporting asset (C1-2)

Table 30 – Case Study 1 – Attack Path 2: the Admin-Level Access Kill Chain (C1-2)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on a remote system.
Execution	• Techniques that result in execution of attacker-controlled code on a remote system.
Credential Access	• Techniques resulting in the access of, or control over local administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 1: Phishing for a foothold to pave a path for Domain Administrator access (C1-3)

Table 31 – Case Study 1 – Attack Path 3: The Domain Administrator Access Kill Chain (C1-3)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on the local system.
Credential Access	• Techniques resulting in the access of, or control over, local administrator credentials.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Execution	• Techniques that result in execution of attacker-controlled code on a remote system.
Credential Access	• Techniques resulting in the access of, or control over, domain administrator credentials.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 2: Social engineering for a foothold to pave a path for user-level access (C2-1)

Table 32 – Case Study 2 – Attack Path 1: the User-Level Access Kill Chain (C2-1)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Credential Access	• Techniques resulting in the access of, or control over, local administrator credentials.
Pivoting	• Tunnelling traffic through a controlled system to other systems that are not directly accessible.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 2: Social engineering for a foothold to pave a path for Domain Administrator access (C2-2)

Table 33 – Case Study 2 – Attack Path 2: The Domain Administrator Access Kill Chain (C2-2)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Social Engineering	• Techniques aimed at the psychologically manipulating people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Defense Evasion	• Techniques an attacker may use for the purpose of evading detection or avoiding other defenses.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on the local system.
Execution	• Techniques that result in execution of attacker-controlled code on a remote system.
Credential Access	• Techniques resulting in the access of, or control over, local administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Credential Access	• Techniques resulting in the access of, or control over, domain administrator credentials.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 3: Phishing for foothold and a vulnerable server for access to critical infrastructure (C3-1)

Table 34 – Case Study 3 – Attack Path 1: Critical infrastructure access via phishing and vulnerable server kill chain (C3-1)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Execution	• Techniques that result in execution of attacker-controlled code on a remote system.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on the local system.
Credential Access	• Techniques resulting in the access of, or control over, domain administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 3: Phishing for foothold and vulnerable protocols for access to critical infrastructure (C3-2)

Table 35 – Case Study 3 – Attack Path 2: Critical infrastructure access via phishing and vulnerable protocols kill chain (C3-2)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Weaponization	• Preparatory activities aimed at setting up the infrastructure required for the attack.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Delivery	• Techniques resulting in the transmission of the payload to the targeted environment.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions
Persistence	• Any access, action or change to a system that gives an attacker persistent presence on the system.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Spoofing	• Techniques that falsify data to illegitimately masquerade as another system or entity.
Credential Access	• Techniques resulting in the access of, or control over, server administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Credential Access	• Techniques resulting in the access of, or control over, domain administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 3: Physical foothold and a vulnerable server for access to critical infrastructure (C3-3)

Table 36 – Case Study 3 – Attack Path 1: Physical foothold and vulnerable server for critical infra access (C3-3)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Credential Access	• Techniques resulting in the access of, or control over, user and/or administrator credentials.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Execution	• Techniques that result in execution of attacker-controlled code on a remote system.
Privilege Escalation	• The result of techniques that provide an attacker with higher permissions on the local system.
Credential Access	• Techniques resulting in the access of, or control over, domain administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Case study 3: Physical foothold and vulnerable protocols for access to critical infrastructure (C3-4)

Table 37 – Case Study 3 – Attack Path 2: Physical foothold and vulnerable protocols for critical infra access (C3-4)

Reconnaissance	• Researching, identifying and selecting targets using active or passive reconnaissance.
Social Engineering	• Techniques aimed at the psychological manipulation of people to perform unsafe actions.
Exploitation	• Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
Credential Access	• Techniques resulting in the access of, or control over, user and/or administrator credentials.
Command & Control	• Techniques that allow attackers to communicate with controlled systems within a target network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Spoofing	• Techniques that falsify data to illegitimately masquerade as another system or entity.
Credential Access	• Techniques resulting in the access of, or control over, server administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Credential Access	• Techniques resulting in the access of, or control over, domain administrator credentials.
Lateral Movement	• Techniques that enable an adversary to access and control remote systems on a network.
Pivoting	• Tunnelling traffic through a controlled system to other systems in the internal network.
Discovery	• Techniques that allow an attacker to gain knowledge about a system and its internal network.
Action on Objectives	• Acting on the objectives, such as compromising the confidentiality, integrity and availability of data.

Appendix C APT28 Tactics References

Tactic	Occurrence
Reconnaissance	"[APT28] typically begins its attack on an institution by identifying and profiling potential victims [APT28] relies on open-source intelligence (OSINT) [...] to identify targets for spear phishing" [55, p. 4] "exfiltrate and analyze information to gain intelligence value [and] use this information to craft highly targeted spearphishing campaigns" [52, p. 2] "these IPs may be performing vulnerability scans attempting to identify websites that are vulnerable" [52, p. 5] "A particular interest was found for [in February 2015] the APT28 team scanned 8,536,272 IPs for possible vulnerabilities [...] 1.712.363 IPs were marked as vulnerable" [56] "the [probing] script has 11 IP classes hardcoded, which leads us to believe that victim organizations are picked manually." [56, p. 13] "One [server] had its RDP port exposed to internet and was using default username/password." [75]
Weaponization	"Typically, the link will lead to a domain name that is similar to a legitimate domain name used by the service in an effort to fool the user" [55, p. 5] "APT28 also registered a domain name imitating the Organization for Security and Cooperation in Europe (OSCE) [...] Several of the domains APT28 registered imitated NATO domain names" [78, p. 14] "Known C2 Servers: [...] symanttec.org microsofi.org microsof-update.com" [54, p. 19] "APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials" [52, p. 2] "APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns." [52, p. 2] "This group is known for its technique of registering domains that closely resemble domains of legitimate organizations they plan to target." [49] "spearphishing campaign using Bitly accounts to shorten malicious URLs [that] redirected victims to a[n APT28]-controlled URL that spoofed a legitimate Google domain" [79] "The e-mail was sent from a potentially compromised account belonging to the Ministry of Foreign Affairs of another government entity" [80] "The RTF file is a weaponized document that attempts to exploit CVE-2015-1641 to drop two files to the system" [80] "[APT28] often re-uses infrastructure components across multiple attack campaigns" [80] "[APT28] appears to be moving toward deployment of one-off infrastructure that can make analysis of attack campaigns and correlation more challenging" [80] "compromised accounts are used to further penetrate into the network of a victim organization [...] by sending emails using stolen identities" [51, p. 8] "an actor creates and signs up a rogue application with an online service provider" [51, p. 24] "APT28 has a clear preference for some hosting providers, DNS service providers, and domain registrars [...] relatively easy [...] to spot new infrastructure that is being set up [...] sometimes even before the attacks have actually started." [51, p. 36] "the nearby IP address [...] hosted the C2 location [used] in the attack on the Democratic National Committee [...] it does appear that [APT28] continues to use the same hosting services to host their infrastructure" [81] "[APT28] group members have the skills and time to find and weaponize these vulnerabilities, or [have] the budget to purchase the exploits" [47, p. 9] "over the years [APT28] has developed a large software ecosystem to perform its espionage activities" [47, p. 9] "the operators used Bitly to shorten the URLs contained in the [phishing emails,] one of those Bitly accounts was set as "public", which allows everyone to see the list of URLs that were shortened by this account [which] contained the email address and the name of the target." [47, p. 14] "Domain Names: nato-hq.com nato-news.com natoint.com natopress.com [...] osce-info.com osce-press.org" [47, p. 98]
Social Engineering	"[APT28] used spear phishing [...] to target several thousand individuals during the first half of 2015 [...] will repeatedly conduct spear phishing attacks [...] over a long duration, possibly a year or more, until one of the attempts succeeds" [55, p. 4] "the message typically includes a link for [...] which will launch a drive-by download or social engineering attack when clicked" [55, p. 7] "In addition to relying on exploits, [APT28] also uses social engineering to trick victims into installing malware" [55, p. 9] "[APT28] heavily relies on social engineering to entice individual targets into clicking links to malware."[55, p. 19] "malicious document sent in spear phishing emails" [57]

	“ User clicks link to attacker controlled website” [82] “The document “World War 3.docx” contacts DealersChoice.B, APT28’s attack framework” [83] “APT28 sends spear phishing emails to WADA employees” [9, p. 6] “the victim's full email address is passed with this URL, prepopulating a fake Google login page displayed to the victim” [79] “credential phishing attacks against high profile Google, Yahoo and Ukr.net users are relatively voluminous” [51, p. 9] “[Corporate] webmail that can be accessed [...] can be probed [...] by advanced social engineering.” [51, p. 10] “VPN credentials can also be phished” [51, p. 10] “[APT28] has been using a variant of tabnabbing [...] no exploits are being used [...] social engineering trick” [51, p. 14] “[groups like APT28] are taking advantage of OAuth for credential phishing schemes” [51, p. 24] “The client usually gets infected by accessing an URL hosting an exploit kit.” [56, p. 7]
Delivery	“[APT28] primarily uses email to deliver malware to targeted individuals”[55, p. 6] “Other messages include malicious attachments instead of links, typically a document file containing an exploit” [55, p. 7] “[APT28] uses a dropper to deploy a backdoor component, CORESHELL, which eventually downloads other modules” [55, p. 10] “The malicious document contains a macro that base64 decodes a dropper that then deploys APT28’s signature GAMEFISH malware” [57] “originated from a computer on the same subnet, indicating that the attacker machine was physically close to the victim and on the same Wi-Fi network.” [57] “Malware ecosystem [...] surrounding the SOURFACE downloader frequently consists of a dropper, which installs SOURFACE. The SOURFACE downloader then receives another dropper from its C2 server, and this second dropper installs a second stage backdoor, which is usually EVILTOSS” [78, p. 21] “HTML/JS launcher page serves Flash exploit [...] Shellcode downloads and runs executable payload” [82] “delivery documents with filenames that have a Russian military theme” [80] “The CVE-2017-11292 exploit [...] delivered by the server is then decrypted and executed by the Flash object handling the communications” [83] “The exploits used by [APT28] include a wide range of products from multiple vendors, including Adobe Flash Player, the Oracle Java Runtime Environment (JRE), Microsoft Word and Internet Explorer, and some components of the Windows kernel” [55, p. 8] “Sophacy is often delivered by Microsoft Word exploits as RTF, DOC and DOCX files” [54, p. 6] “JHUHUGIT implant was delivered through a Flash zero-day” [48] “target clicks on an exploit URL, he will first get fingerprinted [...] Depending on the fingerprinting results, the exploit server might give back an old exploit, a zero-day, or a social engineering lure” [51, pp. 28–29] “when a target does get infected with malware, he will first get relatively simple first stage malware installed. [...]If the target is interesting enough, the actor will install second stage components like X-Agent and X-Tunnel.” [51, p. 29] “[APT28] has compromised websites that targets are likely to visit” [51, p. 30] “The link in this email points [..] to a fake Gmail login panel” [47, p. 13] “[legitimate] websites [...] were modified to automatically redirect the visitors to the exploit kit—also known as a watering hole attack” [47, p. 20]
Exploitation	“Zero-day exploits [...] form a significant part of [APT28s] arsenal” [55, p. 8] “[APT28] moving swiftly to take advantage of newly disclosed vulnerabilities” [55, p. 8] “recompiled with a privilege escalation exploit (CVE-2015-1701, addressed by Security Bulletin MS15-051)“ [55, p. 19] “execution of the macro within the malicious document results in the installation” [57] “APT campaign exploiting zero-day vulnerabilities in Adobe Flash and a brand-new one in Microsoft Windows” [82] “exploiting CVE-2017-11292, a Flash vulnerability that can lead to arbitrary code execution across Windows, Mac OS, Linux, and Chrome OS systems” [83] “Sophacy is often delivered by Microsoft Word exploits as RTF, DOC and DOCX files” [54, p. 6] “JHUHUGIT implant was delivered through a Flash zero-day and used a Windows EoP exploit to break out of the sandbox” [48] “spear-phishing emails that contained a link to the private exploit kit” [51, p. 26] “remote server may respond with a chain of exploits, zero-days and privilege escalation that will infect the target’s computer” [51, p. 29]

	“[APT28] injected the so-called Browser Exploitation Framework (BeEF) exploit on legitimate websites” [51, p. 30] “In 2015, the group exploited no fewer than six 0-day vulnerabilities” [47, p. 9]
Persistence	“[APT28] ensures that its backdoor will run every time the computer starts by creating autostart extensibility point (ASEP) registry entries and shortcuts” [55, p. 11] “execution of the macro within the malicious document results in the installation of APT28’s signature GAMEFISH malware” [57] “Sofacy persists on infected machines as an encrypted and compressed payload” [54, p. 9] “X-Agent will persist via a Registry Run key [or] may persist as a Windows service, or as a Shell Icon Overlay Handler, like Sofacy” [54, p. 26] “characteristics of the Sofacy group [include] the use of multi-backdoor packages for extreme resilience” [82] “[APT28] using a new persistence mechanism that we call “Office Test” to load their Trojan each time the user opened Microsoft Office applications” [84] “uses Komplex to download and install the XAgentOSX tool to use its expanded command set on the compromised system” [81] “component [was] run at startup [by] by creating [a run key in the registry]” [56, p. 22] “Seduploader’s dropper has employed a variety of persistence methods for its payload” [47, p. 31] “Persistence is ensured by a kernel mode rootkit installed as a Windows service” [47, p. 82] “Persistence is ensured by a bootkit infecting the MBR of the hard drive” [47, p. 82] “[APT28] only has to phish for the second authentication token one or two times to get semi-permanent access to a mailbox. They can set up a forwarding address or a token that allows third party applications full access to the system.” [51, p. 10] “once OAuth access has been authorized, the target account can be accessed until the user or the provider revokes the token. If the target changes his password, the actor can still use the OAuth token to access the mailbox.” [51, p. 25] “[APT28] can establish a session with Google and access the victim's account [...] keep this session alive and maintain persistent access” [79]
Defense Evasion	“[CHOPSTICK] also tests for the installation of specific security products [...] and applications” [78, p. 35] “Once the contents [of the collected data] are uploaded, CHOPSTICK deletes the file.” [78, p. 37] “The loader contains three distinct blobs of encrypted data: [...] A list of antivirus and personal security products to detect” [54, p. 11] “To avoid detection, Sofacy systematically disables crash reporting, logging and post-mortem debugging each time it starts” [54, p. 16] “Deletes a specified file using the NSFileManager:removeFileAtPath method” [81] “anti-forensic analysis measures, such as periodic event log clearing [...] and resetting timestamps of files” [49] “deployed binaries used a User Account Control (UAC) bypass technique” [47, p. 84] “This shows that the Pawn Storm is somewhat brazen: the actors don’t really care if they get caught at some point [...] hiding activities is not always a high priority for the Pawn Storm actors” [51, p. 36]
Command & Control	“The [APT28] backdoor can [use] different network protocols, including HTTP, SMTP, and POP3 [to establish] communication with its C&C servers.” [55, p. 13] “correlation of technical indicators and command and control infrastructure, FireEye assess that APT28 is probably responsible” [82] “APT28’s attack framework that allows loading exploit code on-demand from a command and control (C&C) server” [83] “Sofacy will pick a C2 that matches the cloned process: HTTP, SMTP or POP3” [54, p. 17] “The dropped [...] file is an external C&C communications library” [48] analysis of those payloads revealed one primary C2 domain [and] three secondary C2 domains” [80] “[dropper] contacts the C&C server and downloads the second stage component.” [56, p. 7] “first operation of the Seduploader payload is to find a reliable way to reach its C&C server on the Internet [using a] Direct Connection [or] Via Proxy [or by injecting] Into a Running Browser” [47, p. 32] “One [server] had its RDP port exposed to internet and was using default username/password.” [75] “The attacker came back later on, this time, with a compromised third-party account to connect through the TV5Monde VPN” [75]
Pivoting	“[APT28] uses a component that is designed to infect connected USB storage devices, so that information can be captured from air-gapped computers that are not on the network when a user transfers the USB device to the air-gapped computer and then back to the network again” [55, p. 11] “[APT28] using a tunnel component designed to provide a remote encrypted interactive shell to a pre-configured IP address using proxy software on the victim’s computer” [55, p. 13] “[APT28] has displayed an advanced understanding of military and classified government networks, and uses a component that is designed to extract information from air-gapped computers” [55, p. 14]

	“[APT28] uses a VPN connection to join one of its own Kali Linux computers to the victim’s network, possibly using the tunnel component that was previously deployed” [55, p. 16] “One variant of CHOPSTICK focuses on apparent air gap / closed network capabilities by routing messages between local directories, the registry and USB drives.“ [78, p. 24] “[X-Agent] can operate in an air-gapped environment via an ad-hoc pseudo-network of USB flash drives” [54, p. 17] “[after deploying X-Agent and X-Tunnel APT28] might try to penetrate deeper into the network infrastructure, so that it can control more nodes in the victim’s network.” [51, p. 29] “In the case we analyzed [APT28 downloaded] a tool that acts as a proxy and allows the attacker to contact the system even if it is behind a router” [56, p. 8] “X-Tunnel network tunneling tool, which facilitates connections to NAT-ed environments” [49] “The network tool Xtunnel comes later, in order to reach other accessible computers” [47, p. 40] “An Xtunnel infected machine serves as a network pivot to contact machines that are normally unreachable from the Internet.” [47, p. 67] “Xtunnel found on the servers of the Democratic National Committee (DNC)” [47, p. 68] “The network link between the Xtunnel-infected machine and the C&C server is encrypted to complicate network detection at the external boundary of the network. However, the links with the target computers remain unencrypted to allow any kind of traffic to be sent to the target [...] those target computers are not necessarily under the control of [APT28]” [47, p. 69] “Xtunnel is the developers name for this software [...] determined by the function export table left unremoved” [47, p. 69] “We believe Xtunnel to be of high importance to [APT28] [...] it is the only [APT28] component we know with heavy code obfuscation [and] numerous features [were] added over the last three years indicate an ongoing development effort” [47, p. 76]
Discovery	“[APT28] can deploy a large set of tools to perform tasks including [...] information gathering about the local computer” [55, p. 11] “CHOPSTICK collects detailed information from the host” [78, p. 35] “This [Uploader] malware has basic capabilities used for reconnaissance on the target systems.” [83] “Sofacy tries to read a value PhysicalLocation_Name [...] as part of its machine survey” [54, p. 17] “data sent in the network beacons contains information regarding the compromised system [that contains] a list of running processes and the name of the storage device” [80] “[user] visits a website that has been compromised to link to a BeEF exploit URL, the attacker has ample time to do reconnaissance” [51, p. 30] “Seduploader serves as reconnaissance malware [...]. If the victim is considered interesting, Seduploader is instructed to download a spying backdoor” [47, p. 27] “Seduploader builds a report on the compromised machine” [47, p. 34] “discovered two machines (ROB1 & ROB2), after scanning its internal network” [75]
Execution	“This was combined with the heavy use of py2exe to compile Python scripts” [57] “deploying X-Agent malware with capabilities to do remote command execution” [49] “tools were deployed via RemCOM, an open-source replacement for PsExec” [49] “Executes a specified file on the system using the NSTask:launch method” [81] “Its main purpose is to drop a file and execute it using rundll32.exe” [56, p. 7] “The DLL backdoor is installed via execution of rundll32” [55, p. 10] “downloading and execution of those plugins can be requested by the C&C server” [47, p. 65] “execute the shellcode, the rootkit then queues a kernel asynchronous procedure call (APC) a little-known code injection technique” [47, p. 95]
Privilege Escalation	“Privilege escalation: executed as DLL, but in-memory (diskless)“ [55, p. 9] “[APT28] using [...] a privilege escalation exploit (CVE-2015-1701, addressed by Security Bulletin MS15-051)” [55, p. 14] “To spread through the hospitality company’s network, APT28 used a version of the EternalBlue SMB exploit [for privilege escalation to SYSTEM]” [57] “The payload exploits a local privilege escalation vulnerability in the Windows kernel if it detects that it is running with limited privileges” [82] “JHUHUGIT implant [...] used a Windows EoP exploit to break out of the sandbox” [48] “remote server may respond with a chain of exploits, zero-days and privilege escalation that will infect the target’s computer” [51, p. 29] “In the case we analzyed [APT28 downloaded] a tool that exploits a privilege escalation vulnerability [...] to gain system privileges” [56, p. 8] “Before making the payload persistent on the system, Seduploader may execute local privilege escalation exploits” [47, p. 31] “hijacking of the Windows executable sysprep.exe, which possesses the property to auto-elevate its privileges” [47, p. 83]

Credential Access	"[APT28] uses the captured credentials to access the victim's email account to identify additional targets" [55, p. 5] "[APT28] uses publicly available tools such as [...] Mimikatz (a Windows credential gathering tool)" [55, p. 14] "[APT28] using a customized version of Mimikatz that was recompiled with a privilege escalation exploit [...] and stored captured credential information" [55, p. 14] "[APT28] extensively uses credential-stealing spear phishing attacks" [55, p. 19] "APT28 gained initial access to a victim's network via credentials likely stolen from a hotel Wi-Fi network" [57] "Sofacy recovers cached email credentials from several sources" [54, p. 17] "APT28 deployed Responder [that] masquerades as the sought-out resource and causes the victim computer to send the username and hashed password to the attacker-controlled machine [...] to steal usernames and hashed passwords" "OLDBAIT is a credential harvester [...] Credentials for the following applications are collected" [78, p. 42] "APT28 uses a legitimate user account belonging to a Russian athlete to log into WADA's Anti-Doping Administration and Management System (ADAMS) database" [9, p. 6] "establish phishing sites [that] spoof [...] web-based email services in order to steal their credentials" [49] "If a victim enters their credentials, [APT28 can] access the victim's account" [79] "XAgent also has a keylogger functionality that allows the threat actors to steal credentials as the user types them" [81] "In the case we analzyed [APT28 downloaded] a tool to dump passwords from logged-in users [...] based on the source of a public tool (mimikatz)" [56, p. 8] "who fall prey [to the phishing email] will be redirected to the legitimate Google Drive webpage, while their credentials will be collected by APT28" [47, p. 13] "[APT28] regularly deploys [...] Password retrieval tools for browsers and email clients [...] Windows password retrieval tools, with custom builds of the infamous mimikatz" [47, p. 77]
Lateral Movement	"After gaining a foothold on one computer, [APT28] attempts to move laterally through the organization by compromising additional computers to gain access to more data and high-value targets" [55, p. 14] "[APT28] uses publicly available tools such as WinExe (a remote command-line execution tool) [...] to move between computers via methods such as Pass the Hash (PtH)." [55, p. 14] "[APT28] relies on pass-the-hash techniques and elevation of privileges to successfully move laterally across networks" [55, p. 19] "the attacker deployed tools on the machine, spread laterally through the victim's network" [57] "X-Agent has the ability to spread via autorun invocation on USB flash drives" [54, p. 33]
Action on Objectives	-
Target Manipulation	"[Russian civilian and military intelligence Services] actors conducted damaging and/or disruptive cyber attacks, including attacks on critical infrastructure networks" [52, p. 1] "At 20:58, the online presence is affected through social media accounts (YouTube, Facebook, Twitter) and the website of TV5Monde which is modified." "At 21:48, the attacker runs a series of destructive commands ([...] to erase the firmwares from the switches and routers that results into the black screens [of broadcasted TV5monde channels]"
Collection	"[APT28] can deploy a large set of tools to perform tasks including key logging, email address and file harvesting" [55, p. 11] "the backdoor may simply harvest the entire contents of the USB device and save it on the local computer for later extraction" [55, p. 15] "Cyber espionage activity against the hospitality industry is typically focused on collecting information on or from hotel guests of interest" [57] "[CHOPSTICK] records user activity on the host, capturing desktop screenshots in JPEG format, tracks current window focus, collects keystrokes, and scrapes window contents (text, context menus, etc.)" [78, p. 36] "Sofacy temporarily queues data it gathers on disk. This data is LZSS-compressed and encrypted" [54, p. 17] "Outbound messages are buffered in two local queue files on disk, one each for high and normal priority messages" [54, p. 26] "APT28 gains access to an International Olympic Committee account created specifically for the 2016 Olympic Games, and views and downloads athlete data" [9, p. 6] "data theft module [...] is designed to watch removable drives and collect files from them, depending on a set of rules defined by the attackers" "spearphishing campaigns [...] leading to the theft of information" [52, p. 1]

	“silent data gathering over an extended period of time” [51, p. 8] “Checks to see if an IOS device was backed up to the system“ [81] “the attacker searched [...] & collected data on the various internal platform such as the IT Internal Wiki and retrieved as much login and password information as possible and also spend the time to verify those information to make sure they were not expired or outdated” [75]
Exfiltration	“the backdoor may simply harvest the entire contents of the USB device and save it on the local computer for later extraction” [55, p. 15] “After approximately 60 seconds of execution time, CHOPSTICK [...] uploads the file contents [...] to the C2 server using HTTP POST requests” [78, p. 37] “APT28 will steal internal data that is then leaked to further political narratives aligned with Russian interests” [9, p. 2] “APT28 gains access to an International Olympic Committee account created specifically for the 2016 Olympic Games, and views and downloads athlete data” [9, p. 6] “The stolen data is copied into a hidden directory [...] from where it can be exfiltrated by the attackers” [48] “Once APT28 [and APT29] have access to victims, both groups exfiltrate and analyze information to gain intelligence value” [52, p. 2] “Some of the C&C servers may just relay traffic to intermediate proxies and thus relay stolen data back to the actual backend servers over more than one hop” [51, p. 36] “central server [was] investigated [which] contained traces of stolen information in the form of e-mails” [56, p. 9] “data to exfiltrate (logged keystrokes, results of executed commands, etc) are queued in an outbound file and periodically transmitted in bulk to the server” [47, p. 63] “additional component is also downloaded [...] that is a modular component used to upload stolen data to the C&C.” [56, p. 8]

Appendix D Semi-Structured Interviews

Red Team Case Study Validation

A semi-structured interview was performed with Francisco Dominguez Santos, Fox-IT's Red Team Lead on the 17th of October 2017 at Fox-IT in Delft. The following questions served as the basis for the interview, which was performed to validate the data, analysis and results of the Red Team case studies in chapter 3:

1. Which kill chain model(s) are you familiar with?
2. What is the objective of a kill chain model and what should be modeled therein?
3. To what extent is Lockheed Martin's Kill Chain limited in its applicability?
4. To what extent are the Red Team attack visualizations and attack analysis accurate?
5. To what extent is the generalized Red Team MO an accurate reflection of these assessments?
6. To what extent does the RT KC accurately model the Red Team MO?
7. To what extent do you regard a Red Team attack as a suitable proxy for an APT attack?
8. To what extent does the UKC provide additional relevant explanatory power (versus CKC and RT KC)?
9. Which RT KC or UKC phases do you expect to recognize in an APT28 KC?

APT28 Case Study Validation

A semi-structured interview was performed with an intelligence analyst of Fox-IT on the 14th of November 2017 at Fox-IT in Delft. The interviewee has requested to remain anonymous. The following questions served as the basis for the semi-structured interview that took place to validate the data, analysis and results of the APT28 case study in chapter 4:

1. Which kill chain model(s) are you familiar with?
2. What is the objective of a kill chain model and what should be modeled therein?
3. To what extent is Lockheed Martin's Kill Chain limited in its applicability?
4. To what extent does Table 10 accurately reflect the tactical MO of APT28?
5. To what extent do you agree with the reductions of the attack paths in 4.4?
6. To what extent do the APT28 kill chains accurately reflect their attack paths?
7. Which APT28 kill chains do you regard as the most likely and which are the most impactful?
8. To what extent does the APT28 KC accurately reflect the ordered arrangement of APT28 tactics?
9. To what extent do you regard a Red Team attack as a suitable proxy for an APT attack?
10. To what extent does the UKC provide additional relevant explanatory power in comparison with the CKC for APT28 attacks?

Appendix E Glossary

- **APT**: Advanced Persistent Threat (¶1.1.4)
- **APT28**: threat actor, attributed to Russian military intelligence services (¶4.1)
- **APT29**: threat actor, attributed to Russian civilian intelligence services (¶6.5)
- **ATT&CK**: MITRE’s Adversarial Tactics, Techniques & Common Knowledge framework (¶2.3)
- **Attack vector**: a path or means to gain access to a computer or network [85, p. 17]
- **CKC**: Lockheed Martin’s Cyber Kill Chain® attack model (¶2.1)
- **CORAS**: a risk analysis framework consisting of a methodology, language and a tool (¶2.4)
- **Cyber**: socio-technical interactions between people and systems (¶1.1.1)
- **Cyberspace**: a realm that consists of three interdependent layers (¶1.1.1)
- **End-to-end**: the entire chain of events that is required to perform a successful attack (¶2.1.1)
- **Foothold**: a position that can be used as a base for further advance (¶1.1.4)
- **Grizzly Steppe**: Russian civilian and military intelligence services, APT28 and APT29 (¶4.1)
- **KC**: a kill chain, or a chain of events described on the tactical level of abstraction (¶2.1)
- **Kill Chain**: a chain of events described on the tactical level of abstraction (¶2.1)
- **MO**: modus operandi, or a distinct pattern of operation that is common to an actor (¶1)
- **Phase**: phase of an attack, or an attack tactic in its ordered arrangement (¶1.3.2)
- **Procedure**: standard and detailed steps to perform a specific operational activity (¶1.3.2)
- **RAT**: a Remote Access Trojan, or malware that provides remote access to a system (¶2.1.2)
- **RT**: a Red Team, or a group of ethical hackers that performs threat emulations (¶1.1.6)
- **Red Team**: a group of ethical hackers that performs threat emulations (¶1.1.6)
- **RIS**: Russian civilian and military Intelligence Services, APT28 and APT29 (¶4.1)
- **Risk**: the potential that a negative impact occurs (¶1.1.2)
- **RT KC**: Red Team Kill Chain, an actor specific kill chain (¶3.5)
- **Socio-technical**: layer in the cyberspace model comprising cyber interactions (¶1.1.1)
- **Stage**: a step in the delivery process of attacker controlled code (¶3.2.3)
- **Tactic**: tactical activities that are directed to achieve the objectives on an attack (¶1.3.2)
- **Technique**: a non-prescriptive operational method to perform an activity (¶1.3.2)
- **Threat**: potential cause of an unwanted incident that can affect an asset (¶1.1.2)
- **Threat Actor**: an agent with (malicious) intent towards an asset that causes a threat (¶1.1.2)
- **TTPs**: Tactics, Techniques and Procedures (¶1.3.2)
- **UKC**: Unified Kill Chain, as developed in this thesis (¶1.4.2 and Appendix A)
- **Unified Kill Chain**: an end-to-end attack model for APT attacks (¶1.4.2 and Appendix A)
- **Vulnerability**: a weakness in an asset that can be exploited by a threat (¶1.1.2)