Advanced Persistent Threats: Behind the Scenes

Martin Ussath, David Jaeger, Feng Cheng, Christoph Meinel
Hasso Plattner Institute (HPI)
University of Potsdam, 14482, Potsdam, Germany
Email: {martin.ussath, david.jaeger, feng.cheng, christoph.meinel}@hpi.de

***Abstract*—Advanced persistent threats (APTs) pose a significant risk to nearly every infrastructure. Due to the sophistication of these attacks, they are able to bypass existing security systems and largely infiltrate the target network. The prevention and detection of APT campaigns is also challenging, because of the fact that the attackers constantly change and evolve their advanced techniques and methods to stay undetected. In this paper we analyze 22 different APT reports and give an overview of the used techniques and methods. The analysis is focused on the three main phases of APT campaigns that allow to identify the relevant characteristics of such attacks. For each phase we describe the most commonly used techniques and methods. Through this analysis we could reveal different relevant characteristics of APT campaigns, for example that the usage of 0-day exploit is not common for APT attacks. Furthermore, the analysis shows that the dumping of credentials is a relevant step in the lateral movement phase for most APT campaigns. Based on the identified characteristics, we also propose concrete prevention and detection approaches that make it possible to identify crucial malicious activities that are performed during APT campaigns.**

***Index Terms*—Advanced Persistent Threat, Attack Phases, Attack Analysis, Detection Approaches**

I. Introduction

Recently, the number of detected and revealed advanced persistent threat (APT) campaigns has increased significantly. Most of these campaigns use sophisticated methods, tactics and procedures to compromise their targets. Generally, one main objective of APT campaigns is to exfiltrate sensitive data or intellectual property. Due to the sophistication of these attacks, most of the security systems are not able to detect or prevent such type of attacks [1]. Therefore, APT campaigns are often able to successfully compromise companies, organizations or public authorities. Usually, security companies that investigate and analyze APT campaigns publish the results of their work in reports. This allows other potential targets to use this information to detect or even prevent similar attacks. The usefulness of the investigation reports highly depends on the identified and publicly shared indicators and details of the attack. Nevertheless, it needs to be considered that the attackers are often constantly changing and evolving their methods as well as tactics and therefore APT attacks pose a significant risk to most network infrastructures.

One main characteristic of APT campaigns is that these attacks are able to bypass existing security systems that use signature- or anomaly-based detection and prevention approaches. Next to the evasion of security systems, these attacks often use social engineering techniques to infiltrate systems or gather valuable information. Furthermore, APT attacks try to gain long-term access to the target environment and therefore the attackers often compromise multiple systems and accounts to not get pushed out easily. For such sophisticated attacks it is not uncommon that the attackers also use pre-installed administrative tools and legitimate credentials to move laterally, because this makes the detection of these malicious activities very difficult. The usage of sophisticated approaches and the lateral movement within an infrastructure require specific detection and analysis methods that allow the identification of relevant malicious activities. Due to the fact that the attackers are capable to evade existing security systems, new methods, which allow the identification of relevant malicious steps, need to be applied.

In this paper, we analyze the techniques and methods of 22 different recent APT campaigns. Furthermore, we determine common methods and techniques that are used within the different phases of such an attack. We also propose approaches that can be used to detect different key characteristics of APT attacks. These approaches are of course not able to identify all malicious activities that belong to an APT campaign, but they can be used to detect crucial steps that are common for different phases.

The paper is structured as follows: Section II describes the related work on APT phases and their analyses. In the next section, we give a comprehensive overview of the analyzed APT campaigns and their relevant characteristics. Section IV proposes concrete approaches for the prevention and detection of selected malicious activities that are typical for APT attacks. Finally, we conclude our paper and propose future work in Section V.

II. Related Work

Advanced persistent threat campaigns have different characteristics than traditional attacks. The most relevant characteristics of APTs are: (1) attack specific targets, (2) use sophisticated tactics, techniques and procedures, (3) constantly evolve their attack steps, (4) largely infiltrate a network, (5) perform repeating attack attempts and (6) maintain long-term access to target environment [2], [3]. Due to the mentioned characteristics APTs are capable to evade existing security systems and are difficult to prevent, detect and analyze. Furthermore, the properties of such campaigns require that certain steps of the attack are performed manually to stay stealthy and to bypass detection approaches.

In most cases the objective of an APT campaign is to exfiltrate sensitive information or intellectual property. Nevertheless, there are also campaigns where the attackers had

978-1-4673-9457-4/16/$31.00 ©2016 IEEE

other objectives, for example Stuxnet sabotaged centrifuges of a nuclear facility to disturb the nuclear program of Iran [4].

A. APT Phases

APTs belong to the type of attacks that require various phases to infiltrate a large part of the network and to maintain long-term access to the environment. A kill chain [3] and an attack life-cycle [5] were proposed to describe the different phases that are common for APT attacks.

Hutchins et al. [3] propose a kill chain that consists of the seven phases: (1) reconnaissance, (2) weaponization, (3) delivery, (4) exploitation, (5) installation, (6) command and control (C2) and (7) actions on objectives. One kill chain represents one intrusion or intrusion attempt and therefore an APT campaign usually consist of multiple kill chains. Each kill chain contains indicators of an intrusion and these indicators can be used to detect other intrusions or intrusion attempts of the same campaign. The assumption is that attackers reuse for example exploits or command and control infrastructure components for different intrusions, which allows to detect related kill chains of an APT campaign. The objective is to detect or even prevent an intrusion in an early phase of the kill chain, so that the adversary cannot gain a foothold in the environment and achieve the intended objectives.

In [5] Mandiant proposes an attack life-cycle model, which is based on the experiences the company gained during the analysis of the APT1 campaign. The life-cycle consists of eight phases: (1) initial reconnaissance, (2) initial compromise, (3) establish foothold, (4) escalate privileges, (5) internal reconnaissance, (6) move laterally, (7) maintain presence and (8) complete mission. The phases 4 to 7 are performed repeatedly by the attackers to gain and maintain long-term access to the target environment. The different phases of this model are focused on very specific steps of an attack and they seem to be derived from the different actions that are performed during an investigation of an APT campaign.

Although the described models are similar, the different phases of each model show that the focuses are diverse. The models try to describe an APT campaign in a holistic way, although some of the phases are difficult to identify during an investigation of an APT. For example, in the phase that describes the initial gathering of information, most often called (initial) reconnaissance, the attackers do not have to directly interact with the environment of the target. Therefore, it is very difficult, if not impossible, to detect or reveal how the attacker performed the reconnaissance. It is even more difficult to identify such details of an attack when the reconnaissance was performed a long time ago. For our analysis of the different APT campaigns we will focus on information that describes the main characteristics of an attack. Furthermore, the analysis can only rely on information that is typically revealed during an investigation and considered as relevant enough to be published in the investigation report. Due to this, we believe that three main phases are relevant to characterize an APT. These phases are: (1) the initial compromise, (2) the lateral movement and (3) the command and control activity. In Section III we will have a closer look at these three phases.

B. APT Analyses

It is important to perform a comprehensive analysis of APT campaigns to understand the used tactics, techniques and procedures. Only with detailed information about an APT, it is possible to improve the existing security systems and countermeasures.

Chen et al. [2] analyzed the reports of four APT campaigns and used the retrieved details as well as the proposed APT attack model to compare these campaigns. The provided results of the analyses do not contain very detailed information and therefore the comparison is also relatively abstract. Furthermore, due to the low number of analyzed APT campaigns, it is not possible to determine what kind of activities are common for such sophisticated attacks.

Virvilis et al. [6] also performed an analysis of four well known APT campaigns that had a lot of media attention. The comparison of these four campaigns is focused on the initial infection vector and the capabilities and features of the used malware. The conducted comparison does not contain details about all crucial phases of the APT campaigns, which are relevant to develop suitable countermeasures.

Although, it is in most cases difficult to obtain comprehensive details about the different characteristics of an APT campaign, these details are necessary to propose meaningful countermeasures for at least some phases of such campaigns.

C. APT Countermeasures

Various works [7], [2], [3], [8], [6] propose different countermeasure to prevent or detect APT campaigns. Most of the suggested measures are relatively abstract and only propose general approaches like host-based intrusion detection systems (HIDS), network-based intrusion detection systems (NIDS), patch management or security awareness trainings. These approaches are of course valuable and should be used to detect and prevent sophisticated attacks, but most of them are already in place and attackers are able to evade these mechanisms. Furthermore, it is necessary to have suitable and meaningful signatures as well as thresholds in place, otherwise the deployed security systems are not able to detect customized and sophisticated APT attacks. Therefore, we want to propose different concrete approaches that allow to detect certain steps of an APT campaign. Nevertheless, there are also common phases of sophisticated attacks that change very rapidly or that are highly customized. For those phases it is often not possible to propose a reliable and generic detection approach.

III. Overview of APT campaigns

To create a general survey of various APT campaigns and their used tactics, techniques and procedures, we analyzed 22 recently published APT reports. We selected the campaigns and the corresponding reports based on the revealed and released details of the attack. Furthermore, we focused only on APT campaigns and excluded other types of sophisticated attacks like targeted attacks.

Although different models [2], [3], [5] already describe the phases of an APT campaign, we will focus only on the three main phases for our analysis. These main phases allow to characterize the relevant attributes of an APT campaign and make it possible to propose prevention and detection approaches. The three phases are: (1) initial compromise, (2) lateral movement and (3) command and control. The mentioned models use more fine granular phases to describe a campaign, but in most cases it is very difficult to reveal such details during an investigation and therefore most often the reports do not provide such information.

In the following we will give an overview of the mainly used techniques and methods of the analyzed APT campaigns. Table I shows all campaigns and reports we considered during our analysis. Furthermore, also the used techniques and methods are displayed in this table for each phase and campaign. The analysis does not include details about the used malware, because attackers can easily change or replace the utilized malware and so it cannot be used to characterize an campaign. Additionally, the adversaries primarily attack and interact with Windows-based systems during their campaigns and therefore the analysis is also focused on Windows.

A. Initial Compromise

The first step of an APT campaign is the initial compromise, where the attackers try to get access to the target environment. The usual techniques are spear phishing, watering-hole-attacks, attacks on Internet-facing servers and infected storage media. Although the attackers often perform different steps in advance, like preparation of malware or information gathering, these preparation steps are difficult to discover. Furthermore, it is not possible to propose meaningful countermeasures for these early malicious activities, because only very few details are available. Therefore, our analysis is focused on the techniques and exploits that were used in this phase.

Most APT campaigns used spear phishing for the initial compromise. 15 campaigns used attachments and eight campaigns used embedded links to web servers or websites to compromise the target system. Only four campaigns utilized a watering-hole-attack for the initial phase of their attack. The remaining two techniques, direct attacks on web servers and infected storage media, are only rarely used. Various campaigns even use multiple initial compromise methods to gain access to the target environment.

1) Spear Phishing: When spear phishing is used for the initial compromise, the attackers try to trick the corresponding victim to open a provided link or an attached file. The victim might be interesting for the attackers due to the privileges of his/her account or because of the information that is available about this person. The attackers often use different social engineering methods to convince the target that the email was sent from a trustworthy person or colleague. Furthermore, also the content of an email or its attachment is often related to the interests of the target to increase the likelihood that the victim performs the intended activity. Some attackers increase the trustworthiness of the spear phishing emails by spoofing or mimicking the sender of the email.

Spear phishing attempts use either an email attachment or an embedded link to a website or web server to compromise the target system. Depending on the file type of the attachment or the hosted file, the attackers can exploit a vulnerability in the application that is used to display the file or use a method to directly execute the malicious code. The most common file types are PDF files, Flash files, Microsoft Office files with and without macros as well as portable executable (PE) files. These file types, except the PE files, are interesting for the attackers, because some widely used applications, which are utilized to open and view such files, regularly suffer from vulnerabilities. Overall, 11 different vulnerabilities were utilized from all APT campaigns for the initial compromise phase. Only two campaigns exploited unknown vulnerabilities with their spear phishing attempts to initially compromise the target system. If a link is embedded into the mail, the attackers can also exploit the default web browser or a browser plugin-in of the target system to gain access.

Additionally, single APT campaigns use further methods to hinder detection or to make the spear phishing attempt less obvious. One method is to compress the malicious attachments to make it more difficult for the anti-virus scanner to detect the malicious file. Another method tries to convince the user that the attached file is less suspicious by using the right-to-left-override (RTLO) method to manipulate the displayed file extension.

2) Watering-Hole-Attacks: For watering-hole-attacks the attackers compromise a website that is regularly visited from the target and include malicious code on the site to compromise the target system. Four different APT campaigns used this approach for their initial compromise. Attackers usually exploit browser or browser plug-in related vulnerabilities within watering-hole-attacks. In two of these campaigns the attackers used 0-day exploits to gain access to the target system.

3) Attacks on Internet-Facing Servers: Another method, which is used by attackers during the initial compromise phase of an APT campaign, is to infiltrate Internet-facing servers and use these systems to get access to the internal infrastructure of the target. The attackers can exploit existing vulnerabilities on the servers or try to guess or brute-force credentials to gain access. Only one campaign used this technique for the initial compromise. In this case a known vulnerability of an Adobe ColdFusion system was exploited to infiltrate the Internet-facing server and access the internal environment.

4) Infected Storage Media: Furthermore, also storage media are utilized during the initial compromise phase of APT campaigns. Usually, USB drives or CDs/ DVDs are provided to the target, so that the media will be inserted into a system of the target infrastructure. The execution of the malware on the storage media can per performed automatically or with the help of the target. The analysis shows that two campaigns used storage media for the initial compromise phase.

B. Lateral Movement

In the lateral movement phase of APT campaigns the attackers try to compromise additional systems within the internal environment of the target. Furthermore, most often also legitimate credentials are collected during this phase. The reason for this is that the attackers want to persist in

APT Campaign/ Group	Initial Compromise				Lateral Movement			C2			Report
	Spear-Phising	Watering-Hole-Attacks	Server Attacks	Storage Media	Standard OS Tools	Hash and Password Dumping	Exploit Vulnerabilities	HTTP/ HTTPS	Others	Custom Protocols	
Cozy Duke	✓							✓			[9]
Hellsing	✓										[10]
MsnMM (Naikon Group)	✓				✓			✓			[11]
Carbanak	✓	✓			✓	✓		✓	✓		[12]
Duqu 2.0	✓				✓	✓	✓	✓	✓	✓	[13]
HeartBeat	✓									✓	[14]
Darkhotel	✓	✓						✓			[15]
Thamar Reservoir	✓										[16]
Naikon APT	✓				✓			✓			[17]
APT30	✓							✓	✓		[18]
Woolen-Goldfish	✓							✓	✓		[19]
EquationDrug (Equation Group)	✓			✓			✓				[20]
Animal Farm		✓									[21]
Waterbug Group	✓	✓		✓				✓			[22]
Desert Falcons	✓							✓			[23]
Operation Cleaver	✓				✓	✓	✓	✓	✓		[24]
Shell Crew			✓		✓	✓				✓	[25]
Icefog	✓					✓		✓		✓	[26]
Regin					✓			✓	✓		[27]
APT28	✓							✓	✓		[28]
Anunak	✓				✓	✓	✓	✓	✓	✓	[29]
Deep Panda	✓				✓	✓			✓		[30]

TABLE I
TECHNIQUES AND METHODS OF THE APT CAMPAIGNS

the environment of the target and also reach their actual objective of the campaign. Through the infiltration of various systems and the collection of credentials it is very difficult to completely push out such attackers of the environment.

Similar to the initial compromise phase, the lateral movement phase also includes steps like the preparation of the lateral movement and the scanning as well as internal reconnaissance. Other APT models propose additional phases that support the lateral movement. Nevertheless, in most cases it is quite difficult to provide detailed information about these single steps of the lateral movement, because often these activities are not very noisy. Therefore, the majority of the APT reports do not provide any detailed information about these supporting steps.

For an APT campaign it is crucial to have long-term access to the target environment. Therefore, it is relevant for the attackers to perform lateral movement to gain a stronger foothold in the target environment and to not get pushed out easily. Due to the fact that the lateral movement activities should stay undetected, the attackers try to hide between legitimate traffic and activities. This is also the reason why APT campaigns often use standard operating system methods and tools for the lateral movement. Through the usage of such methods it is difficult to detect the lateral movement, because benign and malicious utilization of these methods looks similar and therefore distinction is complex. For the usage of operating system methods and tools the attackers often need to have access to valid accounts with the correct privileges to successfully execute the corresponding lateral movement activities.

The analysis of the different APT campaigns shows that almost all campaigns, where details of the lateral movement were identified, used standard operating system tools and methods to perform lateral movement. These nine campaigns used techniques and tools like PsExec, Windows Management Instrumentation (WMI), Remote Desktop Protocol (RDP) and Powershell to access remote systems during the lateral movement. All of these techniques and tools are often used for the remote administration of systems and some of them are also de facto standards for this benign activity. As already mentioned, for the execution of these techniques and tools the attackers usually need valid accounts, often with higher privileges, to access the remote systems. One option to gain access to valid accounts is to brute-force the credentials, but nowadays corresponding countermeasures are already deployed and such brute-force attacks are very noisy and easy to detect. Therefore, seven APT campaigns used hash or password dumping tools to gather the needed account credentials or the corresponding hashes. If the attackers only have access to the password hash and not the clear text password itself, they can use the pass-the-hash method. Common tools for gathering credentials are mimikatz and Windows Credential Editor (WCE). The advantage of mimikatz is that this tool is able to dump passwords in clear text and not only the corresponding hashes. Furthermore, the source code of this tool is publicly available and therefore attackers can modify and obfuscate it on their own to make the detection of mimikatz difficult.

Another way to move laterally in an environment is to exploit vulnerabilities. The analysis of the APT reports shows that four campaigns exploited vulnerabilities during the lateral movement. Three of the four campaigns used exploits to elevate the privileges. The reason for this might be that hash and password dumping requires administrative privileges, which a normal user account should not have. Only two campaigns used a vulnerability to compromise further systems, because this lateral movement approach is probably not very reliable and stealthy in comparison to other methods. The analysis revealed that not a single campaign used a 0-day exploit for the lateral movement.

C. Command and Control

Another crucial phase within APT campaigns is the command and control (C2) phase. The attackers use this phase to control or provide commands to compromised systems within the target environment. Depending on the used C2 protocol, at least one system of the target environment needs to communicate with an external server in the Internet. Furthermore, also the exfiltration of sensitive data from the target environment, which is most often the main objective of APT campaigns, is part of the C2 phase.

The APT reports show that 15 campaigns used HTTP or HTTPS to communicate with command and control servers. The reason for this might be that companies often only allow access to the Internet over the standard web ports and other connections will be blocked. Nevertheless, the majority of the campaigns utilized additionally command and control methods and protocols. For example, three campaigns used FTP to exfiltrate data. Additionally, for manually performed activities, which require a graphical user interface, the attackers used tools like RDP, VNC, Ammyy Admin or Team Viewer. The analysis of five campaigns showed that they used custom protocols. Overall, most of the protocols used encryption or obfuscation techniques to hide from detection.

IV. Prevention and Detection Approaches

The analysis of the different APT campaigns shows that attackers try to hide their malicious activities between legitimate actions, which makes the detection difficult. Especially, the usage of valid credentials and standard operating system tools and techniques are difficult to identify, because they are also used for benign administrative activities. Furthermore, the attackers also perform different steps of an APT campaign manually, which allows them to move very stealthy through an environment and make it possible to evade security systems. Although these attacks are very sophisticated, the analysis revealed that most of the campaigns utilized exploits for already patched vulnerabilities and only a few campaigns made use of 0-day exploits.

As already described in Section II-C, different countermeasures were already proposed to prevent and detect APT campaigns. Most of these countermeasures are very abstract and do not provide any details or technical explanations how they should be implemented or work. Security systems like NIDS, HIDS, firewalls and other signature- as well as anomaly-based systems need to be configured correctly and meaningful signatures as well as analysis algorithms are required for detecting attacks. Although these systems can be used for detecting APT campaigns, it requires a concrete approach or idea to utilize such security systems to prevent or detect sophisticated attacks.

In the following, we propose prevention and detection approaches that focus on special characteristics of APT campaigns. Nevertheless, it needs to be considered that there are manifold possibilities to conduct APT campaigns and therefore the proposed approaches cannot detect or prevent all APT campaigns.

A. Exploitation of Vulnerabilities

The analysis shows that 11 campaigns used exploits in the initial compromise or lateral movement phase and only four campaigns utilized 0-day exploits. Therefore, a well known and effective approach to prevent certain attack activities is to apply security patches shortly after their release.

An additional approach is to use tools that can detect certain exploitation techniques, which are used in most cases. Companies like Microsoft or Malwarebytes offer solutions that try to detect and block memory corruption exploits. The Enhanced Mitigation Experience Toolkit (EMET) from Microsoft is probably the most well-known exploit mitigation tool that can be used to protect applications. Different mitigation techniques are implemented in EMET to detect exploits that use for example return-oriented programming (ROP) or heap spraying. Furthermore, EMET tries to harden the protected application with mechanisms like mandatory address space layout randomization (ASLR) or structured exception handler overwrite protection (SEHOP). If EMET detects a suspicious memory activity, it terminates the corresponding application to prevent the attacker from successfully exploiting the vulnerability and executing the payload. By using these mitigation techniques, it is more difficult to develop an exploit that works reliably. Nevertheless, even if such a tool is in place, not all exploitation attempts can be detected and prevented.

The analyzed APT campaigns exploited nine vulnerabilities where EMET could be used to detect and prevent the used exploit. This shows that EMET probably would have blocked 50 % of the exploits. Even in cases where the attackers use 0-day exploits EMET could be helpful, due to its generic mitigation techniques.

B. Hash and Password Dumping

Due to the usage of valid credentials, APT campaigns can move stealthy within an environment and hide from detection. The main method for gathering hashes and passwords is to utilize appropriate applications that are able to dump this information from a system. The currently most widely used hash and password dumping tool is mimikatz, because it is able to dump clear text passwords and it also offers further interesting features. WCE is another tool that is used within APT campaigns to gather credentials.

Although, there are different techniques for dumping Windows credentials, the most common method is to extract and analyze parts of the Windows Local Security Authority Subsystem Service (LSASS) process. Therefore, we propose to implement a detection approach that monitors if a process requests a handle to the LSASS process and performs suspicious function calls with the help of this handle. The direct access to the memory of other processes should be very limited, especially for sensitive processes like LSASS. Such a detection approach should be useful for different credential dumping techniques and it would of course also be possible to block such attempts to prevent the attackers from successfully gathering the credentials.

C. Usage of Standard Tools and Techniques

The analysis of the APT campaigns shows that the utilization of standard operating system tools and techniques is common for the lateral movement phase. Due to the fact, that these built-in tools and techniques are also used for benign activities, it is complex to distinguish between benign and malicious usage. One approach is to analyze log information and try to detect potential lateral movement activities. The crucial point is to have the correct logging policy in place, so that it can be ensured that the correct events are logged. Furthermore, also a decent knowledge base is required to identify legitimate activities.

Windows uses audit policies to configure what kind of events should be logged. For example, events with ID 4697 are relevant to detect lateral movement activities that use the PsExec utility. Events with this ID are recorded when a new service was installed in the system. PsExec creates a service on the target system to execute the intended program. Especially on sensitive systems, such kind of events should be very rare.

This example shows that with a carefully configured audit policy it is possible to detect lateral movement that is performed with standard operating system tools and techniques.

V. Conclusion and Future Work

By analyzing 22 recently published APT reports we found out that a majority of the campaigns used spear phishing for the initial compromise, standard operating system tools and techniques for lateral movement and HTTP(S) for command and control. Another common activity to support the lateral movement is to dump credentials. With these methods the attackers can hide between legitimate traffic and activities, which make the detection difficult and allow them to bypass existing security systems.

Interestingly, our analysis revealed that 0-day exploits are not as common as expected for such advanced attacks. Instead, the attackers exploited vulnerabilities where corresponding patches were already available.

The mentioned characteristics can be seen as a chance to uncover APT campaigns. We have proposed three different prevention and detection approaches that target common APT characteristics. With these approaches it is possible to identify crucial malicious activities within relevant attack phases.

In future, the identified indicators of the APT campaigns could be analyzed and correlated. In particular, it might be interesting to have a look at the used service providers and domain registrars of the threat actors. Another task could be the implementation and evaluation of the proposed prevention and detection approaches.

References

[1] Mandiant, "M-trends - A View From the Front Lines," Mandiant, Tech. Rep., 2015.

[2] P. Chen, L. Desmet, and C. Huygens, "A Study on Advanced Persistent Threats," in *Communications and Multimedia Security*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, vol. 8735, pp. 63–72.

[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," *Leading Issues in Information Warfare & Security Research*, vol. 1, 2011.

[4] E. Chien, L. OMurchu, and N. Falliere, "W32.Duqu: The Precursor to the Next Stuxnet," in *5th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. Berkeley, CA: USENIX, 2012. [Online]. Available: https://www.usenix.org/w32duqu-precursor-next-stuxnet

[5] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, 2013, [Available online].

[6] N. Virvilis and D. Gritzalis, "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?" in *Eighth International Conference on Availability, Reliability and Security (ARES)*, Sept 2013, pp. 248–254.

[7] P. Bhatt, E. Toshiro Yano, and P. Gustavsson, "Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks," in *8th International Symposium on Service Oriented System Engineering (SOSE)*, April 2014, pp. 390–395.

[8] A. Sood and R. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *Security Privacy, IEEE*, vol. 11, no. 1, pp. 54–61, Jan 2013.

[9] K. Baumgartner and C. Raiu, *The CozyDuke APT*, Kaspersky Lab, Apr. 2015, [Available online].

[10] C. Raiu and M. Golovkin, "The Chronicles of the Hellsing APT: the Empire Strikes Back," https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/, Apr. 2015.

[11] K. Baumgartner and M. Golovkin, *The MsnMM Campaigns - The Earliest Naikon APT Campaigns*, Kaspersky Lab, May 2015, [Available online].

[12] Kaspersky Labs - Global Research & Analysis Team, *Carbanak APT - The Great Bank Robbery*, Feb. 2015, [Available online].

[13] ——, *The Duqu 2.0*, Jun. 2015, [Available online].

[14] R. Dela Paz, *The HeartBeat APT Campaign*, Trend Micro, 2012, [Available online].

[15] Kaspersky Labs - Global Research & Analysis Team, *The Darkhotel APT - A Story of Unusual Hospitality*, Nov. 2014, [Available online].

[16] Clearsky - Cyber Security, *Thamar Reservoir - An Iranian cyber-attack camapaign against targest in the Middel East*, Jun. 2015, [Available online].

[17] K. Baumgartner and M. Golovkin, "The Naikon APT," https://securelist.com/analysis/publications/69953/the-naikon-apt/, May 2015.

[18] FireEye Labs, *APT30 and the Mechanics of a Long-Running Cyber Espionage Operation*, Apr. 2015, [Available online].

[19] C. Pernet and K. Lu, *Operation Woolen-Goldfish - When Kittens Go Phising*, Trend Micro, Mar. 2015, [Available online].

[20] Kaspersky Labs - Global Research & Analysis Team, *Equation Group: Questions and Answers*, Feb. 2015, [Available online].

[21] ——, "Animals in the APT Farm," https://securelist.com/blog/research/69114/animals-in-the-apt-farm/, Mar. 2015.

[22] Symantec, *The Waterbug attack group*, Jan. 2015, [Available online].

[23] Kaspersky Labs - Global Research & Analysis Team, *The Desert Falcosn Targeted Attacks*, Feb. 2015, [Available online].

[24] Cylance, *Operation Cleaver*, Dec. 2014, [Available online].

[25] RSA Incident Response, *Shell_Crew*, Jan. 2014, [Available online].

[26] Kaspersky Labs - Global Research & Analysis Team, *The 'Icefog' APT: A Tale of Cloak and Three Daggers*, Sep. 2013, [Available online].

[27] ——, *The Regin Platform - Nation-State Ownage of GSM Networks*, Nov. 2014, [Available online].

[28] FireEye Labs, *APT28: A Window Into Russia's Cyber Espionage Operations?*, Oct. 2014, [Available online].

[29] GROUP-IB and FOX-IT, *Anunak: APT Against Financial Institutions*, Dec. 2014, [Available online].

[30] D. Aplerovitch, "Deep in Thought: Chinese Targeting of National Security Think Tanks," http://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/, Jul. 2014.