Advanced Persistent Threat (APT)
Beyond the hype

Project report in IMT4582 Network security at Gjøvik University College during spring 2013

Merete Ask 12HMISA - Management

Petro Bondarenko 12HMISA - Management

John Erik Rekdal 12HMISA - Forensics

André Nordbø 12HMISA - Forensics

Pieter Bloemerus Ruthven 12HMISA - Forensics

Dmytro Piatkivskyi 12HMISA - Technology

ABSTRACT

By Merete Ask (Group Coordinator)

Advanced Persistent Threat, hereinafter APT, is currently reported to be the most important threat on the rise for information security professionals to look out for and adequately protect against. Since the term was coined in 2006, it has flourished as a "security marketing buzzword" throughout the information security industry representing the "nightmare of attacks". An Internet search[1] on the term "Advanced Persistent Threat" produced an approximate result of 2,6 million hits, so is APT a real threat to be concerned about or is it just another "hype"?

This paper is constructed through the assembly of a set of individually contributed papers, written by six Master students in Information Security at Gjøvik University College (GUC) in Norway. The contributing students constituted a group, with members from all electable study tracks of the GUC Information Security Masters program[2] approaching the topic from different perspectives.

By approaching the term broadly, this paper takes a closer look at APT "beyond the hype". This, with the aim to shed light on different aspects of APT and as such provide a paper that can be a source for peers looking for a broad, yet collected, source of information on the topic. The paper is put together on the basis of providing answers to questions such as:

- What is this APT phenomenon and what is it not?
- What is new about APT, what are the characteristics to look out for?
- What makes APT relevant for everyone to consider?
- How does APT affect our society and our ways of protecting it?
- How can the threat of APT be efficiently addressed and handled?

This paper finds APT to be a threat relevant for any organization to consider and take seriously. Avoidance as a security strategy is virtually a waste of time, given the targeted nature of APT attacks. No doubt challenging, this paper concludes it quite possible in many ways to enhance security to better protect against and efficiently handle APT attacks, should they occur. Due to its sophisticated and complex nature however, this report finds that APT does represent one of the main strong driving forces in information security today. Not only as a considerable threat, but in terms of forcing what seems to become a paradigm shift in how information security is approached in general moving forward.

[1] Google 14-05-2013

[2] Management, Forensics and Technology.

1. INTRODUCTION

By Merete Ask (Group Coordinator)

APT attacks are not new as a phenomenon, but fairly new as a term. The fact that APT type of attacks are not new as a phenomenon, is supported by this paper, especially in section 4, which refer examples of some "spectacular cyber attacks" dating all the way back to 1982. The fairly new term APT was first coined by the US Air Force in 2006 [91], to facilitate military teams' ability to discuss APT attack characteristics and intrusion activities, with un-cleared civilian counterparts. All though fairly new, the term's coining and corresponding definition provides the important ability to classify attacks, i.e. APT or not, and start the establishment of some proper statistics, based on experience and investigation results of classified APT attacks. This also enables for building a better understanding of APT as a phenomenon and study it, for the much needed distribution of relevant knowledge. As such, the classification and the corresponding definition enables for necessary information sharing to ensure individual organizations proper understanding of APT, required for their individual ability to prepare for, efficiently detect and handle APT attacks, should they occur.

Since the term coining, APT has flourished as a "security marketing buzzword" throughout the information security industry, representing "the nightmare of attacks". This flourishing, as happens with most "marketing buzzwords", did certainly not decrease with its introduction to the media, in terms of publicly announced examples of detected APT type attacks. A variety of definitions and explanations can be found searching the Internet for information about APT. Some of them unfortunately contain misleading narratives which, if laid down as a basis for evaluations, could lead to adverse consequences. E.g. organizations drawing important conclusions on false understanding/information basis, potentially leading to erroneous conclusions and subsequent erroneous/lack of action. One example of potentially misleading narratives, can be found by review of the Wikipedia description of APT [93]. Here included for explanatory purposes, fetched from Wikipedia as the information source assumed quite commonly used by the general public:

> "Advanced persistent threat (APT) usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target."

A notable characteristic of APT, as also shown in this paper, relate to the amount of resources available to the group of organized attackers. However, single-tracked and directed exemplifications as the one used by Wikipedia (i.e. "such as foreign government"), is misleading. Supported by this paper, in addition to other sources, our society certainly includes other kinds of organized groups fully capable of funding APT attacks, e.g. groups ranging from competitive industry companies engaged in industrial espionage to organized crime groups, potentially even terrorist organizations. On that basis, it is important that organizations evaluate APT as a generic, relevant threat in relation to their organization and business, no matter "who" the relevant attacker may be. This, to avoid potentially erroneous risk dismissal, based on misleading narratives on that aspect. One of the objectives of APT, often recognized in known APT attack investigations, do relate to "Internet-enabled espionage" as outlined in the above Wikipedia description. In fact, most media published cases do include elements of such activity. There are however, other APT objectives such as sabotage, as also outlined in this paper, which the above Wikipedia description do not outline to the same extent as "Internet-enabled espionage", showing yet another potentially misleading and unfortunate narrative in describing APT.

Different organizations, on a daily basis, face the challenge of "keeping up to date with" terms flourishing as "security marketing buzzwords" in their objective to protect the organizations adequately from relevant threats (i.e. APT in addition to numerous others such as ID theft, DDOS, phishing etc.). As such, information security professionals in particular, should be careful in their choice and use of terms, its context of use and corresponding exemplifications. This, to ensure the different organization's proper understanding, and avoid any potential contribution to adverse consequences, based on any unfortunate use of directed or potentially erroneous narratives. It would be unfortunate, if use of such narratives for instance contributed to a situation where organizations in general simply dismiss or narrow down APT to be "a threat not applicable to them", instead of addressing APT as a relevant risk towards their business. Especially, when investigations of known APT attacks, in line with information put forward in this paper, shows APT to be a generic and relevant threat to consider. With this in mind, and review of several APT definitions, this paper's use of the term APT, is based on the following NIST APT definition, provided by NIST in a special publication released in 2011 [60]:

> "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:
>
> 1. pursues its objectives repeatedly over an ex-

tended period of time;

2. adapts to defenders' efforts to resist it; and
3. is determined to maintain the level of interaction needed to execute its objectives."

The NIST definition is quite broad, but at the same time does not assume anything about the APT attacker, beyond its identification of the typical characteristics, i.e. "sophisticated levels of expertise and significant resources". The NIST definition also takes into account various APT objectives, both in relation to aspects of espionage and sabotage. This way, the definition itself covers APT broadly as a term, without directions or narratives that allow for any potential misconceived interpretations of it.

Combined, the recent US Air Force coning of the term in 2006 and the subsequently published NIST definition of the term in 2011, or any other definition one would choose to use, serve as a critical success factor for classification and understanding of APT. Especially relevant now, when various, recently published, threat and vulnerability reports worldwide, jointly alert to APT as one of the main threats on the rise for organizations to be aware of and adequately protect themselves against. APT is now recognized and reported to increase rapidly, being a sophisticated threat, difficult to prevent, protect against, detect, recover and stay adequately secure from. The below cited selection of summary highlights from three recently published reports of different sources, provides some introductory insights to this.

- Translated, the joint public threat and vulnerability report 2013 [63] issued by the Norwegian Intelligence Service (E-tjenesten), the National Security Authority (NSM) and the Police Security Service (PST), including these entities individual public reports which the joint report is based on, amongst others state the following:

  > "(. . .) Norway and Norwegian interests are exposed to advanced, targeted espionage on a daily basis. This is malicious activity with the ability to undermine security and damage national interests. (. . .) Audits and investigations often show that entities fail in basic, traditional security. (. . .) High focus on external perimeter security and less focus on internal threats, increase the general vulnerability should the network be compromised. (. . .) Number of advanced espionage operations towards specific targets of high economical or societal value increase. The operations are characterized by repeated attempts to attack, even if an attempted attack is prevented. The attacker often gains a foothold within the information system so that the attack can continue even if one attempt is detected, i.e. advanced persistent attack."

- The executive summary of the Trustwave published global security report 2013 [88] amongst others state the following:

  > "In 63% of incident response investigations IT support was outsourced to a third party. (. . .) Businesses are slow to "self-detect" breach activity. Average time from initial breach to detection was 210 days, more than 35 days longer than in 2011. Most victim organizations (64%) took more than 90 days to detect the intrusion, while 5% took three or more years to identify the criminal activity. (. . .) Basic security measures are still not in place. (. . .) The use of encryption by attackers during data exfiltration is on the rise; over 25% of all data was encrypted by cybercriminals."

- The Mandiant M-trends report 2013 highlights [53] amongst others state the following:

  > "Nearly two thirds of organizations learn they are breached from an external source. (. . .) organizations are getting better at discovering targeted attacks on their own. Still, a full 63% of victims were made aware they had been breached by an external organization such as law enforcement. (. . .) Typical advanced attacks goes unnoticed for approximately 8 months. Attackers spend an estimated 243 days on a victim's network before they are discovered – 173 days fewer than in 2011. Though organizations have reduced the average time between compromise and detection by 40%, many are still compromised for years before detecting the breach. (. . .) Attackers are increasingly using outsourced service providers (e.g. finance, accounting, HR, procurement etc.) as a means to gain access to their victims.(. . .) Advanced Persistent Threat (APT) attackers continue to target industries that are strategic to their growth and will return until their mission is complete. (...) Of the top three industries repeatedly targeted (by APT), aerospace topped the list, followed by energy, oil and gas, and pharmaceuticals (. . .) Once a target always a target. (. . .) Of the total cases Mandiant investigated in 2012, attackers lodged more than one thousand attempts to regain entry to former victims."

Even if the summarized highlights cited above only represent a limited number of reports, compared to the numerous one can find, they are published by different types of sources and still jointly refer to several communalities worth noticing, e.g.:

- Organizations tend to fail on basic security measures.
- Detection time increases, i.e. time from the initial compromise/infection to its detection.
- Number of attacks classified as APT type attacks increases.

Even if the selection of report summary highlights here are limited, the communalities shown above, should alone provide a justified basis for concern. On this basis, it is only fair to ask the question if organizations today adequately acknowledge relevant threats to the appropriate level or understand them properly enough to do so. Also, if organizations tend to fail on basic security measures, it is fair to question their actual ability to adequately protect against what seems to be a steadily increasing number of sophisticated attacks, such as APT classified attacks.

In addition to the above, it is worth noticing the Mandiant M-trends report 2013 highlights statement that "attackers are increasingly using outsourced service providers (e.g. finance, accounting, HR, procurement etc.) as a means to gain access to their victims". The fact that ICT is not included in the Mandiant exemplification of the outsourced service providers is notable. Traditionally, outsourcing of ICT services or the risk involved in outsourcing them, has been given allot of attention in relation to information security. An attention also picked up in most international standards and business relevant best practice information security guidelines. In relation to the aspect of privacy it is also covered by laws. Since ICT is not amongst the mentioned examples of types of "business services relevant to outsource", the mentioned types may be suffering from not gaining the adequate level of attention in relation to information security previously, even if aspects of them are just as relevant to consider in terms of establishing adequate business information security in general. This could be a notable remainder that information security is not limited to the organizations ICT security, i.e. IT department either in- or outsourced. It requires a holistic, broad perspective, including the complete supply chain with procurement, but also other aspects such as finance and HR, typically also regulated to some extent by law.

The above outlined summary highlights, combined with a quick look at publicly available information, shows by example that even if organizations in general may still have "a way to go" to acknowledge and assess threat on an adequate level, cyber security, with APT as one of the current main driving forces, is acknowledged as a global threat and does make an impact on several levels of society, e.g:

Global/national/governmental levels of threat acknowledgement:

- Norway has recently politically reorganized the responsibility of civil ICT security and placed it under the Department of Justice to clarify the departments overall responsibility for security [61]. In addition, Norway has recently reorganized to gain relevant focus, by assembling its cyber defense and warfare capabilities in a separate military branch [3].
- During a recently published statement from the US military, regarding the development of cyber weapons, it was outlined that for the first time, the risk of cyber attacks outrank the risk of terrorist attacks on the US list of top level risks for the nation [42].
- The published cross-government UK cyber security strategy (2013), states that UK had cyber attacks ranked as one of the top four UK national risk in 2010 [58].
- A flash note published by ENISA early this year "Cyber-attacks – a new edge for old weapons" [25] is calling for Europe's businesses and government organizations to take urgent action to combat emerging attack trends (i.e. APT).

Commercial levels of threat acknowledgement:

- As supported by different types of known APT attacks and published threat and vulnerability reports, support the fact that APT has an effect also on the commercial levels of our society. In fact, just days after this group decided to focus this paper on the topic of APT, Telenor published a press release in Norway informing the public of the fact that they had detected and notified law enforcement of a detected compromise of their systems with the intent to exfiltrate sensitive information. Given the fact that the case is currently under investigation, the in depth details are not known, but the descriptions of the attack provided in the initial press release strongly indicates compromised through an APT type attack [41]. In relation to the commercial aspect, it is also worth mentioning that some commercial industries also launch quite creative campaigns to reveal potential vulnerabilities (in general but also in direct relation to typical APT attack vector characteristics) and raise awareness amongst employees. One fairly new example is the Northrop Grumman Corporation's spear-phishing campaign, designed and launched by their team of security professionals, targeted towards a large number of their employees [29]. A type of campaign which may be regarded as controversial, but has proven to be quite effective when performed professionally for the right purposes.

Experience shows that adequate knowledge of relevant threats and risk is a precondition and a critical key success factor for any establishment of adequate security for any object.

On a high level, as also supported by this paper, APT attack phases in general, does not distinctly separate it from traditional sophisticated attacks, i.e. planning, initial penetration/compromise, obtaining adequately high level access rights, mapping the network for lateral movement and execute actions to complete intent/mission without "getting caught doing it". As such, the high level attack phases of APT may not provide a very good basis for APT security planning, protection and detection, as opposed to for instance a more clearly recognizable threat such as a virus. The fact that it utilize several attack vectors, potentially also over some considerable time, also makes it hard to recognize incidents as "elements of APT". One could be in the risk of handling them as the one of the common "occasional opportunistic incidents", thereby handling an element of the APT attack as a single incident, failing to recognize it as an element of an APT attack.

What specifically does distinguish APT, as opposed to the constant opportunistic or sometimes coincidental incidents IT departments and organizations deal with on a daily basis,

is that is specifically targeted. APT is a carefully planned attack against a specific target with the aim to complete a very specific mission. It involves careful strategic and tactical planning to enable persistent target footholds to complete the mission. APT utilize several attack vectors and methods based on what is found most adequate to complete the mission. The APT attack is well organized and continuously monitored by skilled personnel during its execution, allowing for the attack progress to be dynamically changed by the attackers as found relevant to complete the mission, for instance upon suspicion of detection. APT attacks are specifically designed to circumvent traditional detection mechanisms and utilize advanced and sophisticated methods to "stay under the radar" of them. APT is not a type of attack that will "stick out" as an attack towards you, it is a malicious attack disguised as you where a lot of effort is made to avoid showing up on your normal security attack sensors.

As APT attacks are specifically targeted for completion of a specific mission, this paper does not focus on aspects of security in terms of APT avoidance. It is generically recognized that if an organization is specifically and persistently targeted by APT, complete avoidance is not an option given the sophisticated characteristics of APT attacks. Instead, this paper has a strong focus on providing a basis for thorough understanding of the different aspects of the threat through sections 2 to 4, as a precondition for any establishment of adequate security as covered by sections 5 and 6. The basis for thorough understanding, is introduced by section 2 presenting APT as a generic threat. Section 3 moves further into increase the understanding through a story of a real APT attack. Since the espionage aspect of APT is already dualy covered in most current reports and the media in general, this paper section 3 aims to balance this out by providing the story of Stuxnet. An APT attack at first assumed to be "the normal espionage", discovered by chance and later found to be one of the most sophisticated sabotage attacks seen so far, i.e. according to the NIST definition with the purpose of "undermining or impeeding critical aspects of a mission, program or organization". Without going into deep technical detail the story shows the real challenges of APT in relation to its high level of sophistication and persistence. Section 4 broadens the basis of understanding by reviewing APT from the governmental and commercial aspects of it. Based on the established understanding, this paper section 5 moves further into measures for APT protection, in the meaning of proactive measures that can be taken to protect networks against APT. This includes measures aimed to reduce the likelihood of being compromised by an APT attack and measures aimed at reducing the consequences, should an APT attack occur. Then, section 6 of this paper reviews measures for APT detection, in the meaning of reactive measures that can be taken to increase the likelihood of efficient detection and recovery from an APT attack, should it occur, making the paper cover the topic of APT in the following structured manner:

1. "APT as a generic threat" see section 2, page 6
2. "Case studies" see section 3, page 14
3. "Government and commercial aspects" see section 4, page 19
4. "Protecting against APT attacks" see section 5, page 30
5. "Detection of APT attacks" see section 6, page 37

Then the this paper is rounded up with the presentation of the paper's overall summarized conclusion and corresponding suggested future work regarding APT, to the extent it has unfolded; "Conclusions" see section 7, page 45
, completed with the full list of references presented in section 8.

2. APT AS A GENERIC THREAT

By Petro Bondarenko

2.1 Abstract

The main concern of the contemporary society is security of life, data transition and social structures. One can hardly deny the fact, that our world, and Information Security one, has undergone significant changes, on the one hand, and are not secure any more, on the other one. The development of information and computer technologies involves the corresponding development of cybercriminal activity.

Within the last few years Advanced Persistent Threats (APTs) have become one of the major problems for IT security specialists all over the world. The main goal of this section is to clarify the nature of APT risks and to provide a practical understanding of APTs for security professionals. The subject of the investigation is the following: APT methods, the purpose of their usage, general overview of APT characteristics, specific features and particular qualities of APT life cycle and tools used for the attack.

It goes without saying, that these tools may vary from one attack to another, but the characteristic feature is the systematic approach). Our analysis of APT attacks shows that they may be divided into two stages, that is, an APT attack stages and specific features of APT attacks. The majority of attacks uses and follows the same pattern. The traditional way to start the attack is the use of a spear phishing with the sending out e-mail in order to install the necessary malware on a victim's computer.

It allows being "invisible" for a considerate period of time, and moreover, by the time the antivirus software or IT team discovers the presence of such components and eliminate them, the signatures are useless as the malware is never usually used for the second time. The successful infiltration into the system gives the attackers the possibility to steal the administrative credentials with the further Backdoors placement through the system. The latter allow free access to the system and data gathering. Being treated as the legitimate users, the attackers have the possibility to move through the compromised network as they get the valid user's credentials.

This section analyzes the main three stages of an APT attack in details:

- Stage 1 - Reconnaissance, Launching, and Infection: the attacker provides reconnaissance, searches for identification of vulnerabilities, begins the attack, infecting targeted hosts;
- Stage 2 - Control and management, Detection, Persistence: attacker controls compromised hosts, update the code, its distribution onto other machines, and finds and gathers targeted data.
- Stage 3 - Extract and Take Action: the attacker receives the necessary data from the target network, and takes action. [91]

Using the infected computer, the attacker uses it to get access to the net, admin or service accounts, and choose and evaluate the target computer. We have found that there are the automated and manual methods of the information gathering and infiltration. Using manual processes, potentially valuable databases and documents are located, and searches of the operating system are conducted using specific keywords to further identify data. The automated method is based on the following approach: a target system receiving encrypted data, stores and transmits it while the target system infiltrates and processes the information.

APT life cycle is also analyzed in this section. The result of our investigation is that its life cycle is determined by a simple task: to perform a hostile penetration and to stay in as long as possible. Moreover, some APT may be given another task after the primary target has been reached. Nevertheless, the APT has a weak point: during the process of infiltration, the network traffic will appear or will be modified. The performance cycle functions in a non-stop mode: the malware is updated, it establishes the connection with the command-and- control unit, it scans and analyses the data on a victim's computer, and so on. It may be assumed, that the long-life persistence may be explained by the combination of factors, the most important of which are the following: the use of different approaches, the clear target, constant scanning, and the ability to install/remove the victim's software and so on. Also, the main problem is that the company detects an attack, it tries to clean the threat using the traditional anti-virus software, and when the malware is deleted, the company gets down to business again. The point is that the malware is not the attack itself, it is just one of the tools to perform the attack, and its removal does not prevent the attackers staying in the system. Each time the IT teams try to eliminate the threat; they make it stronger because the APT attackers search the system for new vulnerabilities. Moreover, the attackers may run the complicated attack consisting of one or more operations.

2.2 Introduction

Nowadays the attacks mainly on the cloud services and companies which provide such services have one common feature: their nature gives all the reasons to determine them as APT (Advanced Persistent Threat). According to one of the McAfee's reports [21], such attacks are interrelated and are becoming more and more massive, and, due to their potential danger, specialists define them as the Operation Shady RAT (Remote Access Tool).[21]

The term APT was used for the first time in 2006 by the USAF (United States Air Forces) for the personnel having no access to the classified information to nominate the conventional source and the style of attacks against the USA.[91] The abbreviation contains the nature of these attacks, that is, they are both well prepared, continuous, creative, and advanced persistent threat; which is more, they are really threatening the interests of the country, company or an enterprise. It is worth giving more profound explanation what is meant under APT.

This section focuses on such aspects as the APT attacks main characteristics, methods and techniques used by the attackers, APT's life cycle and the problems with the attacks

termination.

2.3 General Notes

As it has already been mentioned, an advanced persistent threat (hereinafter-APT) is a kind of a network attack due to which an APT attacker gets the access to the network or a system which, in its turn, allows him to stay there for a long period of time without being detected. Some specialists state that it is rather the data stealing and system control than the certain damage of the system which are the APT attacks target. Other specialists say that the APT's aim depends on the attacker's will. As a rule these are the high-value information sectors (national defence, financial institutions, etc.) which are the APT attacks target.[71]

In case of a simple attack, the intruder has to get into a system for a short time, otherwise he may be detected and traced by the network's intrusion detection system (IDS). As for an APT attack, however, one of the most relevant aims is to get the access to the system or database. It may require the continuous rewriting of the code and the sophisticated evasion techniques application from the part of the intruder. At the same time, some APTs are so complicated that they require a full time administration.

Spear fishing is said to be one of the most frequent means of social engineering for gaining access to the network by means of the illegitimate ways. As the result, the attacker may establish/implement the back door. To expand his presence, the attacker gathers valid user credentials, primarily, the administrative ones, and browse the network placing and installing as much backdoors as possible. The latter allows him to establish the "ghost infrastructure" for the malware distribution which remains hidden.[71]

It has been thought that it is just enough to construct the protection for the accidental culprit attacks directing to other host. Nowadays the situation is quite different. It is the APT attack model which has changed everything. Nowadays they are highly diligent, persistent and have vast financial and material resources. As no advanced technological methods are used in APT, the term Determined Adversaries (Persistent Opponents/Attackers) has been introduced. It allows to reflect the processes taking place in Information Security in a much more clear way and to link such accidents as Stuxnet to APT.[102]

The APT is different to other attacks in the organized project approach, planning, financial and methodological execution. The attack, depending on the attacker's tasks, may last for months, even a year. Such an attack is persistent; the attackers do not try to "hide" in case the attack is detected. Moreover, in case of disclosure they become more aggressive and increase their attempts to try to stay in a system longer. The Information Security industry knows the main software and technological tools of such attacks for a long time; the majority of these tools out-of-date. The main danger of APT is not the technology, but purposefulness and the resources involved. The word "Advanced" is related not to the IT/IS technologies used during the attack, but to the method that is used during the attack. It is not just a single method which is used during the attack, but many vectors of them. The APT methodically use different approaches, don't try to gain profit at once, and logically analyze all the vulnerabilities and their combinations.

A typical non-APT attacker isn't usually interested in a challenging target, as his interest is in financial institutions attacks, credit cards numbers, breaking into accounts or botnet establishment. Accordingly, the security measures against such attackers are quite typical: firewalls, antivirus software, traffic volume control methods. As for an APT, the situation is quite the opposite one: the target is being constantly attacked, and the attack may last for years. It is the absolute level of security measures which may stop the attacker, but is it a disputable issue.[82] Thus, it is possible to say that the APT nature may be presented as follows:

- Sophisticated attack;
- Targeted attack;
- Attacker adapts to your security measures;
- Using multiple attack vectors;
- The attacker stays in a system not being detected for a considerable period of time;
- Scanning and waiting to find out the system vulnerability.

The nature of APT defines its characteristics.

2.4 APT Characteristics

We can divide main APT characteristics into four groups:

- Targeted: The main aim of an APT attack is the stealing of a targeted information or specific data, as well as to cause the certain damage. Unlike an ordinary attack on a randomly selected computer, the APT one has a systemic and organized character. The recent examples of it, such as a notorious Aurora/Google attack [100] was aimed at the source code, while the Sony attack targeted PII (personal identifiable information). The examples are numerous. On the contrary to non-APT attacks, APT's spent significant financial resources as well as time and efforts. This gives ground for two main conclusions: the subjects for the APT methods are not individuals but any organizations, and the probability of being attacked equals the value of information/data the organization has, as well as the acts of sabotage. Figure 1 shows the main components of an APT attack due to which it will always be in demand [91] (see Figure 1).
- Persistent: In general, the following aspects do characterize any APT attack. The persistent nature of an attack means that at first the attackers know the organization/target only, they know nothing about information security means, the required data allocation, and system vulnerabilities. So, in order to get ready for the attack they have to find any vulnerable aspect, evaluate the efficiency of information security means, and get access to the privileged host inside the targeted network. It is a really time consuming process and it

may take up to several months, even years, to start the attack. It means that in case to see the attack, the IT security teams must not treat any penetration as a single accident, but to try to see the systematic approach [91] (see Figure 1).

- Evasive: The peculiarity of APT technology is that it allows to overcome almost all known means of data protection, even those which have been used for years. To do it, the attackers may try a variety of ways: to carry threats by means of content sent through commonly accepted and allowed protocols. On the other hand, they may install the malware on the VIP hosts computers with no problems as the specific codes for attack are designed exclusively for the targeted system, thus avoiding the threat of being detected. In case of a successful attack the stolen data may be sent circumvention the firewalls by means of custom encryption [91] (see Figure 1).

- Complex nature of an APT attack. The typical APT attack in the majority of cases involves the following:

  1. the use of the telephone base to identify the key persons in a targeted organization;
  2. phishing e-mails with the links to the sites with the remote access tool, for example, JavaScript code malware to be installed;
  3. privilege escallation command-and-control code;
  4. custom encryption technology. It goes without saying that these tools may vary from one attack to another, but the characteristic feature is the systematic approach.

The scheme given in the Figure 1 illustrates the main components of an APT attack. [91]

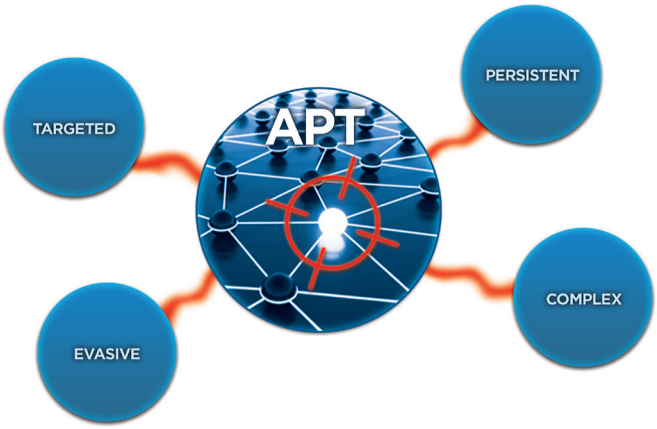

Figure 1: Main APT characteristics [91]

Generally, one may say that there are three main constituent parts in an ATP attack, that is,

1. financial or competition motivation of an attacker;
2. a continuous attack;
3. a specific company, organization as a target of an attack. [91]

As for the financial or competition components, business has both aspects: the attackers are interested in reaching their aim. As for states and official organizations, any state has outer opponents and has the data to hide. The sustained character of an attack stands for the fact that an attacker may continue it for months and may be even years unless he reaches the target. At the same time, depending on the aim of an attack, its duration may also be adjusted: it may take several days or weeks to find out the commercial secrets after the protocol details, applications characteristics and their vulnerabilities are investigated. On the other hand, it may take just several hours or days to steal the passwords or install malware. Such APTs use the advantages of the services delivery. The analysis of APT attack has two aspects, that is, an APT attack stages and specific features of APT attacks. [82]

2.5 APT attack stages

First of all, it should be mentioned that each ATP attack is the unique one due to the combination of methods applied. At the same time, according Mandiant's M-Trends report [55], the majority of attacks use and follow the same pattern. The scheme looks as follows: the attackers conduct a reconnaissance in order to identify the VIP persons in an organization. The social networks and other applications are useful tools for attacker to find a proper target taking the personal information into consideration the links and other data. The use of a spear phishing with the sending out e-mail in order to install the necessary malware on a victim's computer is the traditional way to start the attack.

It allows being "invisible" for a considerate period of time, and moreover, by the time the antivirus software or IT team discovers the presence of such components and eliminate them, the signatures are useless as the malware is never usually used for the second time. According to the report mentioned above, just 24% of APT malware is detected and eliminated by the antivirus software. The successful infiltration into the system gives the attackers the possibility to steal the administrative credentials with the further Backdoors placement through the system. The latter allow free access to the system and data gathering. Being treated as the legitimate users, the attackers have the possibility to move through the compromised network as they get the valid user's credentials. The researches show that APT attackers may get access to up to 40 different systems within the victim's network. Once the intruders penetrate, they install a lot of malware which makes them almost "invulnerable". [68]

The exfiltrated data is usually sent to the attackers' command-and-control unit. From that moment, the aim of APT attackers is to stay in a compromised system for as much time as possible and give the adequate responses to the company's IT teams attempts to get rid of them. [68]In order to understand the threat of an APT attack one should realize its components. A typical APT attack is said to consist of three main stages which occur within a long period of time during the APT process:

1. Stage 1 - Reconnaissance, Launching, and Infection: The attacker provides reconnaissance, searches for identification of vulnerabilities, begins the attack, infecting targeted hosts.
2. Stage 2 - Control and management, Detection, Persistence: Attacker controls compromised hosts, update the code, its distribution onto other machines, and finds and gathers targeted data.
3. Stage 3 - Extract and Take Action: The attacker receives the necessary data from the target network, and takes action. [91]

Attack Stage 1

The attack phases can be divided into three subparagraphs.

Reconnaissance: APT attackers investigate points of entry and vulnerabilities, core persons and core assets. Senior managers, IT administrators, and computers that can provide access to the target resource inside the company are of then among those targets under attack.

Launching: This stage usually includes one or more methods to obtain privileged access to the host. Having a special purpose attacks and spear fishing keep a low profile to avoid recognizing in future. There are overall methods including the following:

- Spear phishing with integrated links to web-resources automatically trying to infect the user with zero-day exploits
- E-mails with different attachments to general Office formats, PDF files, or applications, etc. Such embedding's may include zero-day malware aimed at previously unknown vulnerability
- Compromised websites of core person's habits and interests determined by social media accounts
- Social engineering in order to get access to preferred credentials of user accounts

Infection: The user code can be tending to mounted on the privileged host. This code shall be reported to the command-and-control block in the network, as well as other information that can be important to the attackers for the further attack's development. [91]

Attack Stage 2

As it has already been mentioned, this phase is also divided into three subparagraphs.

Control and management: intruder controls infected host using the command and control services remotely. Though there were instances where this service is installed on a compromised computer within the destination network, it might also be found on the Internet, often on DNS dynamic hosts. C&C may allow an attacker to update and thus to upgrade the malicious software remotely, to add new malicious software (encryption tools etc.) and to launch new commands to the host. Although the original infections frequently include a user (day zero) attack code, we often see public tools used for command and control.

Detection: On this step, infected hosts download supplementary components capable of detecting the objective data on the infected hosts on mapped network drives, and other locations of networks. Core purposes may include Active Directory (AD) and PKI certificate servers to establish an account and get access privileges to sensitive data on the network, or a cloud-based storage. There is another way to detect and break into systems where users have administrator rights, that is the use data monitoring. An intruder can also try to get more control by opening additional nodes within the objective network, and use the network or other system-level vulnerabilities in order to infect them. Very frequently used toolkits to obtain more control for standard web tools are such as gsecdump, Cain and Abel (to crack passwords), SSH and RDP.

Persistence: The main difference between conventional malicious programs and APT is the possibility of persist. Conventional malware often removes itself or is detected and removed by antivirus software being recognized and identified. APT is designed for the invisible staying. Moreover, it is designed to remain persist by calling back to command-and-control centers for updating and upgrading to retrieve new previously undetected code to avoid detection by means of updated antivirus tools. [91]

Attack Stage 3

On this step, the APT attackers having taken control over one or more hosts in the objective network may generate credentials required for access to expand their presence and determine the objective data (assume that the data was the main purpose). The only one thing left is to send data beyond the network or command-and-control server or to the formerly unused one. This server can be arranged at the same place as an attacker or in another country. If the new objective data still becomes available (new client accounts or refreshed business plans) and is of value for the attacker, this final step may last for a long period of time. Eventually the attack stops, either because the attacker has reached his purpose or because the victim notices and stops/blocks the attack. The following methods and results are known:

- Ransom: The attacker threatens to reveal the classified or private information in case the victim refuses to pay. The organization may agree to pay the ransom in order to prevent the commercial or political damage. It is the common way to make money on the stolen data.
- Share or sell attack methods: If the attack hasn't been traced and detected by the victim, successful approach is being shared or sold to other attackers who repeat the attacks on the given victim or choose the other one.

- Sell information: In case it is the PII which has been stolen (names, credit card numbers, e-mail addresses, etc.), the attacker may sell that information to other criminals interested in it to commit a downstream crime against the victims. For instance, a stolen credit card may be used to make a purchase.

- Public disclosure: Eventually, the stolen private or confidential information may be disclosed to the media. It is typical of a victim to disclose the fact of a theft as soon as it is detected or in case such a procedure is required by the local compliance regulations. However, the attackers may be first to disclose such information or the fact of a successful attack. [91]

2.6 The APT-attacks specific features

Having realized the meaning of the term "APT", one may understand the unique character of such attacks. These are not only the vast resources, definite target and the attackers' patience due to which the APT-attack differ from other similar ones, but also the way it is usually performed.

The majority of attackers "scan" networks and computers in search of the vulnerable aspects; in case of a success, they try to make use of them. As a rule, it is the access to such data as credit cards information, users' names and passwords or other personal data which may be sold to the interested parties. Attackers also try to compromise the applications with the help of such methods as SQLi (SLQ built-in commands), for instance, to get access to the web application data bases. The other typical attack is the XSS (cross-site scripting attack), during which the Java Script malware applications are run in a browser and get the access to the cookie-files and other data among which there may be users names and passwords, and the victim may even know nothing about it. Having completed their task, the attackers usually terminate the attack, although they may install the software to allow the access to the data bases in the future. [73]

The peculiarity of an APT attack is that it may use any of the methods mentioned above, but in majority of cases the methods are combined with the other approaches, for instance, to make the user run the malware are disclose the accounting data to get the access to the confidential data.[73] The Figure 2 given below gives the schematic outline of an APT attack.

The typical APT attack starts with the user's critical mistake: he/she opens the infected file. The recent examples show that it may be the malware for the Internet Explorer 6.0 lacuna (Operation Aurora) or the Excel file (RSA Company's case). Moreover, the penetration into the system may not be the primary target but just the means to get the real target.

After that the Backdoor is set which gives the possibility to use the Poison Ivy Tool to get the user machine remotely. RAT (Poison Ivy Remote Administrative Tool) is a type of software which has several variants created and controlled by a kit (Poison Ivy management program). In order to "cheat" the system, the typical size of severs (real backdoors) which usually is less than 10kB, may be adjusted.[69] The

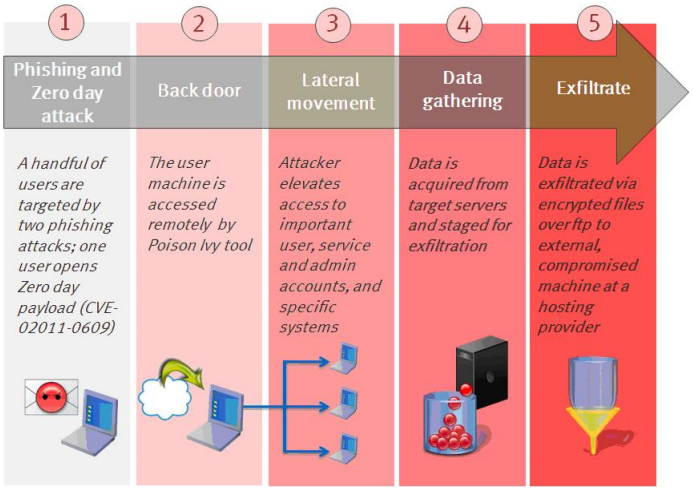

Figure 2: The Anatomy of an Attack [73]

advantage of it is the quick distribution within the system by means of the ability to copy itself to an Alternative Data Stream. [79]

After it a registry entry will added each time the infected computer is booted up, and re-directed to an address pointed out by the server-part. All the communication between the server and the client's computer is duly encrypted and compressed. It all allows bypassing the firewalls. This application gives the attacker the possibility to get practically complete control over the user's computer. In case of a successful injection, he/she get the following options:

1. to rename, delete or execute the files (with the option of the files downloading/uploading).
2. to view and edit the Windows registry; to view, suspend or terminate the currently running processes;
3. to view and shut down the network activity;
4. to stop or start any services on the user's computer;
5. to enable/disable the installed devices;
6. to uninstall software, delete entries and view the applications installed;
7. taking screenshots of the desktops and stealing information;
8. to get the access to the saved passwords;
9. key logger and the third party plugins installation.

Using the infected computer, the attacker uses it to get access to the net, admin or service accounts, and choose and evaluate the target computer. This process is sometimes compared with the home burglary. The intruder penetrates the house, disables the installed alarm systems, and explores the premises, taking all the valuable items. The same happens to the user's computer: the attacker breaches the system establishing the beachhead inside the network. After

establishing the backdoor connection to the command-and-control server to download the necessary toolkits and additional software from an external site. In such a way the initial breach takes place. [107]

According to the Verizon's 2011 Data Breach Investigations Report [106]more than 60% of 2011 breaches happened moths or longer before discovery. As the result of the previous steps, everything is ready for the data gathering. Attackers target information for unauthorized access, manipulation or stealing. They usually establish the collection units and exfiltrate the data gathered through proxy cut-outs of the network or apply the encryption techniques and malware, thus continuing the attack. In fact, the choice of a technique depends on such factors like the probability of quick detection, time resources available, speed of information security teams reaction on the data loss. Once the data has been gathered, it is high time it were exfiltrated. The methods of the data exfiltration are being constantly developed and there are definite sophisticated ways of data gathering.[59]The diagram below shows the results of the investigation conducted by the SpiderLabs team in 24 different countries. 45% of breaches stood for the getting access through the remote access application. At the same time, it was difficult to tell them from the ordinary attacks as there were no zero-date exploits or complex application flaws; they became possible due to the simple procedure (vendor-default, easy passwords, etc). Once the attackers are in, they launch the network enumeration tools to discover additional targets, and the noise usually generated by these tools is often taken for the last preparations for the attack.

There are the automated and manual methods of the information gathering and infiltration. Using manual processes, potentially valuable databases and documents were located, and searches of the operating system were conducted using specific keywords to further identify data. The automated methods is based on the following approach: a target system receiving encrypted data, stores and transmits it to an upstream host which is susceptible to a breach while the target system infiltrates and processes the information. The use of appropriate methods once allowed the attacker to have access to the system during 156 days which was quite enough for them to enter the environment, set up tools to remove data and gather it before they were traced. Sometimes the attackers use the remote access application previously utilized for initial entry to extract data (see Figure 3).

Other existing services, such as native FTP and HTTP client functionality, were also frequently leveraged for data extraction. Specifically, when malware was utilized for data extraction, FTP, SMTP and IRC functionality were regularly observed. With off-the-shelf malware, such as keystroke loggers, attackers most often use built-in FTP and e-mail capabilities to exfiltrate data. When e-mail services were employed for extraction, the attackers often opted to install a malicious SMTP server directly on the compromised system to ensure the data was properly routed.[81]

This figure shows that in the majority of cases it were Microsoft Windows Network Shares (28%) and Native Remote Access Application (27%) which were used for the data exfiltration, while Malware Capability FPT stood for 17% only.

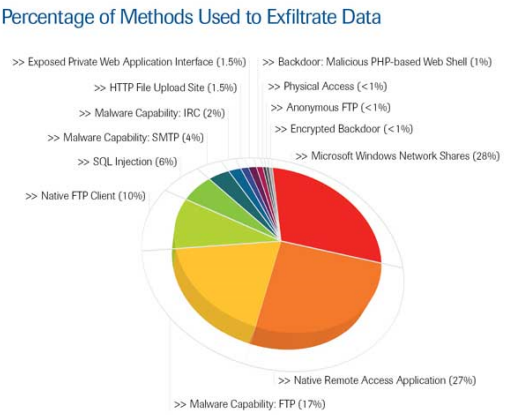

Figure 3: Data exfiltration methods [59]

Native FPT Client stood for 10%, while other Malware Capabilities (SMTP and IRC) stood for 4% and 2% accordingly. Not every organization may become the APT attack target. Nevertheless, the IT specialists are worried that the methods used for the APT attacks may be adopted by criminals. In case it happens, all organizations may become the victims, especially they have something valuable. At the same time, the APT attacks may be used as the means of political protest and hacktivizm.[59]

2.7 APT life cycle and tools used for the attack

The ATPs are both sophisticated and long-life. Their life cycle is determined by a simple task: to perform a hostile penetration and to stay in as long as possible. Moreover, some APT may be given another task after the primary target has been reached. Nevertheless, the APT has a weak point: during the process of infiltration, the network traffic will appear or will be modified. The Figure 4 given below illustrates the APT life cycle. As it can be seen, the performance cycle functions in a non-stop mode: the malware is updated, it establishes the connection with the command-and-control unit, it scans and analyses the data on a victim's computer, and so on. It may be assumed, that the long-lived persistence may be explained by the combination of factors, the most important of which are the following: the use of different approaches, the clear target, constant scanning, and the ability to install/remove the victim's software and so on. That is why it is thought to be difficult to spot the attack once the suspicious activity is detected: the anti-virus signatures will not work, the user's credentials may be changed, and the confidential data may be easily imported long before the victim realizes the importance of the situation. [20]

The main problem is also that the company detects an attack, it tries to clean the threat using the traditional antivirus software, and when the malware is deleted, the company gets down to business again. The point is that the malware is not the attack itself, it is just one of the tools to perform the attack, and its removal does not prevent the attackers staying in the system. Each time the IT teams try to eliminate the thread; they make it stronger because the attackers search the system for new vulnerabilities. Moreover,

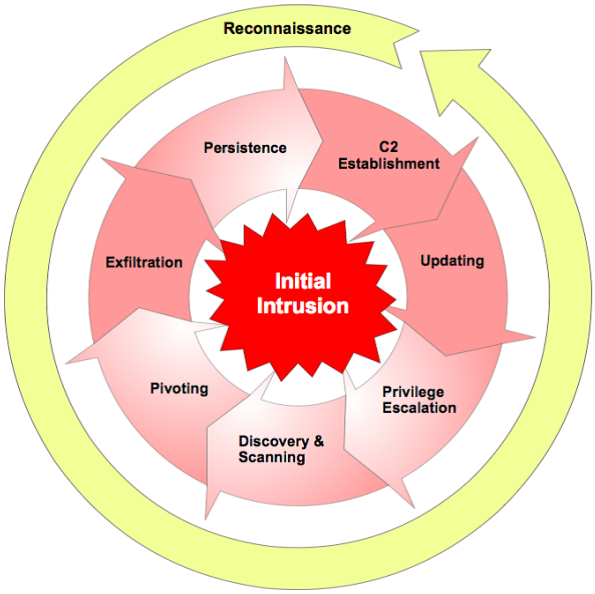

Figure 4: Scheme of APT life cycle [20]

the attackers may run the complicated attack consisting of one or more operations. [79]

According to the attackers will, these operations may be divided into several stages. Much has already been said about stages of the attack that is why we would like to emphasize that the attacker may distribute the tasks among available cells of the network. E-mail turns out to be a useful tool for the exfiltration. The point is that the links direct the user to the sites where the target's web browser and corresponding software is being attacked. The same can be said about malicious Microsoft Office or Adobe PDF documents which exploit the vulnerabilities of the applications. The documents may easily be stolen from the target organization/company network or the victim's computer before the beginning of an attack or as the part of other operation. Being modified in accordance to the attacker's interests, and having the malicious code being installed, the e-mail is sent to the victim (phishing). Some APT groups prefer the public-facing services as the number of potential infected computers increases. When all the vulnerabilities of the target system are known, the 0-day comes. Then the common pattern to get domain administrative privilege level is the following:

- to get the administrative access into the target system;
- to steal the credentials for the domain administrative credentials in the given system;
- to get the access to the other necessary systems by means of the administrative credentials

The passwords are of great use for this task, as the researches state that it takes the attacker up to several hours to crack the password containing 8 or less characters. In case the user has the longer password it makes his system vulnerable as the pattern for it is quite predictable. There is a common belief that the users after being compromised change the passwords in a predictable way, and it gives the attackers the possibility to stay in even after the account has been changed. That is why, in case the attackers had no enough time to complete their task, they are likely to come back with the aim of completing their task. Such tools as key loggers and web form grabbers are very useful to get the modified passwords and other credentials. By the way, it is the common feature for Trojan and Poison Ivy to have key loggers. In case the credentials are not available, the attackers may try to apply different ways: to bribe the official, to infect the USB or CD, and so on. Such a variable approach to get credentials, steal information or destroy the target system leads to a significant life cycle. [79] We think that the use of tools is worth more attention. Much has been said about the tools used for the initial stage of the attack. The Figure 5 given below represents the tools functioning.

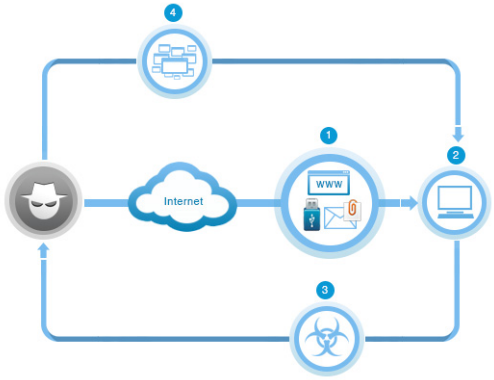

Figure 5: Traditional APT lifecycle [105]

- Step 1: Malware is sent to the victim in any possible way.
- Step 2: Malware is run on the infected computer. The ridicules thing is that it requires manual steps by the victim the majority of cases.
- Step 3: Backdoors (STARSYPOUND or BOUNCER) are installed.
- Step 4: The tools for data exfiltration, lateral movement, and other tasks performance is uploaded.
  The tools given in a table below are daily used by the attackers, and they are typical for the first stage of an attack, such backdoors as Trojans are not included.

The fact is that a lot of these tools are installed or copied by the attacker are never removed. [105]

2.8 Conclusion

In conclusion, APTs really turn out to be a serious threat to IT teams and the great challenge to anti-virus working groups' teams. It has been found that:

- A typical APT is divided into 3 stages, each of which has its own specific features;

- it is almost impossible to secure/guard one's computer or the organization's network as this kind of an attack is a really special one, that is, a clear target, several combinations of methods used, sufficient funding;
- the attack technology is characterized by the complicated architecture: the malware is detected after a long period of staying in a system, the components of malware are updated, and even the removal of its components does not stand for the termination of an attack;
- because of an APT life cycle's peculiarities, why it is thought to be difficult to spot the attack once the suspicious activity is detected: the anti-virus signatures will not work, the user's credentials may be changed, and the confidential data may be easily imported from the compromised computer long before the victim realizes the importance of the situation.

There is a common belief that that joint efforts will benefit this problem solving as the leading anti-virus developers have accumulated significant experience. Because of the factors mentioned above, the APT protection seems to be a great and complex challenge. However, the question of the governmental structures' participation in the APTs threat elimination also arises.

3. CASE STUDY

By John Erik Rekdal

3.1 Abstract

This is not a technical in depth review of the malware known as Stuxnet, it is a small insight in the story and investigation behind, leading up to the discovery and the reverse engineering of the functionality of the malware. Stuxnet was a malware discovered in January 2010, when it had already been active since June 2009. At first it was thought this was a simple espionage case.

Experts determined that the malware was designed to attack the software used in industry to control/program controllers that drive motors, valves and switches. At first it was thought that Stuxnet was merely stealing configuration and design data files from the systems, since attacking the controllers have no financial gain. So it was thought that Stuxnet was just another case of industrial espionage but it turned out to be one of the most sophisticated cyber weapons created.

The malware infected machines through USB sticks, so the attackers planted infected USB sticks in four different companies in Iran which have dealings with the target. By doing this, they were hoping that some of the infected sticks would find its way into the systems of the uranium enrichment center which was not connected to the Internet. It installed itself as a rootkit between the machine and the PLC (programmable logic controller), and hijacked the traffic coming to and from the PLC. These values where then changed, so the PLC would send a signal to the frequency converters connected to the PLC to run at frequencies not supported for a short period of time, and then return to normal operations. The malware also changed the data that came back from the equipment so everything seemed normal, to the statt uisng and monitoring the system. By doing this, the connected equipment would burn out much faster than usual.

This malware utilized four zero day exploits and also had valid certificates signing its code, to make it both difficult to detect and resilient to get rid off. The fact that it had four zero day vulnerabilities states how eager the adversaries was to infect the target system. If you also take the certificates into account, this is a really sophisticated piece of malware with a lot of time and money spent on development. It was speculated during the investigation that this was a government sanctioned attack, but this would not be confirmed until much later in the book "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power".

In the time after the discovery of Stuxnet two more malware surfaced, Flame and Duqu, both designed to do espionage, and both seems to be in family with Stuxnet. They share many common traits such as certificates, the same zero-day exploits and also some of the same source code and they all target Iran. However these two have not been taken credit for.

The fact that these types of attacks can go unnoticed for such a long time, makes them a valuable intelligence or sabotage tool. If you also are able do deny any involvement in this, you have the perfect spy basically. It seems attacks like Stuxnet will become more and more common, as seen through Duqu and Flame.

3.2 Introduction

Everything is this section is based on information from the article "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History" [109] unless noted otherwise.

In January 2010 investigators from the IAEA (International Atomic Energy Agency) had just completed an inspection at the uranium enrichment plant in Natanz, Iran, when they realised something was off in the cascade rooms housing thousands of centrifuges enriching uranium.

The purpose of uranium enrichment is to increase the percentage of the U-235 isotope in uranium. It's the U-235 isotope that is used in reactors and weapons. In its raw form, uranium is about about 99% U-238. One of the methods used to enrich the uranium is to use hydrofluoric acid which reacts with the uranium and creates the gas uranium hexafluoride. When the uranium is in a gaseous form it is passed into these centrifuges, which spins up with a force thousand times the force of gravity to be able to separate the U-238 atoms from the U-235 ones. [8]

Normally, around 10% of the centrifuges where replaced each year. With about 870 centrifuges, this equaled between 800 to a 1000 centrifuges a year. However when the IAEA later reviewed surveillance footage, they saw that the workers had replaced between 1000 and 2000 centrifuges each month.

The inspectors, officially had no right to dig into this and Iran wasn't required to disclose any information on reasons for replacing the centrifuges. The inspectors sole job was to monitor what happened to nuclear material.

The answer to this however, was hidden all around them, buried in the disk space and memory of the computers in the facility. Months earlier in June 2009, someone had unleashed a sophisticated and destructive worm on computers in Iran, with a single goal, to sabotage the uranium enrichment program.

This whole ordeal would not be discovered for nearly a whole other year, when some computer security researchers got a hold of the malware and could do some extensive reverse engineering and analysis. What they found was maybe the world's first real cyberweapon.

3.3 Discovery

On the 17th of June in 2010, Sergey Ulasen in a company called VirusBlokAda located in Minsk, was browsing through his email when he saw a report on a customers machine in Iran stuck in a reboot loop.

Ulasens research team in the antivirus division of the company got a hold of the virus infecting the computer, and realised shortly that the virus was using a zero-day exploit.

According to Wikipedia[104] a zero-day vulnerability is:

> "A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on 'day zero' of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability."

In addition to the zero-day vulnerabilities, the authors of the malware had managed to some how get signed certificates from RealTek Semiconductor, in order to fool systems into thinking the malware was a trusted program from Realtek. This certificate was quickly revoked, but Stuxnet was also using a second certificated issued to JMicron Technology. They had gone to great lengths to make sure the malware would execute and run unnoticed.

Stuxnet spread from computer to computer through infected USB sticks. The initial vulnerability exploited was in the LNK file in Windows Explorer. When an infected USB stick was inserted, the USB stick was scanned, and the exploit code awakened and transfered an encrypted file on to the host machine.

This vulnerability was reported to Microsoft, and VirusBlokAda went public with the information on the 12th of July. A few days later the larger antivirus companies scrambled to get samples of the malware, dubbed Stuxnet by Microsoft, based on file names found in the code.

The community was surprised to find out that the code had been launched as early as a year before, in June 2009, and the creator(s) had updated and refined it over time, releasing three different versions.

3.4 Further study

When Symantec got their hands on the malware their interest was piqued, this malware looked to be unique from all others, since usually many viruses and worms are variations of others already known. But, malware with zero-day exploits are examined by hand.

This malware was larger than the usual, this one was 500k as opposed to 10k-15k. Malware this large usually have an image file hogging space, such as a fake bank login. But, there was no image in Stuxnet, just plain code. When an experienced analyst looked at the code he saw that Stuxnet was carefully crafted and organized. It contained multiple components, all compartmentalized into different locations to make it easy to swap out functions and modify the malware as needed. What was most peculiar was the way the malware hid those functions. Normally, Windows functions are loaded as needed from a DLL file stored on the hard drive. Doing this with malicious files would be a giveaway to the antivirus however. Instead, Stuxnet stored its decrypted malicious DLL file in memory only, as a kind of virtual file with a specially crafted name. It then reprogrammed the Windows API, so every time a program tried to call a function from a library with that name it was loaded from the memory instead of the hard drive.

Figure 6: The stuxnet command and control servers. Picture from Wired

Every time Stuxnet infected a system, it communicated with with one of two domains www.mypremierfutbol.com and www.todaysfutbol.com in Malaysia and Denmark to report information about the infected host. Information like internal and external IP-address, host name, operating system and version and if Siemens Simatic WinCC Step 7 was installed. These command and control servers made the attackers able to update Stuxnet with new functionality or install more malicious files on the compromised system. As can be seen in figure 6[3] the command and control server seems like a legit website to keep people from getting suspicious.

The DNS providers for the two domains had already deadlettered the incoming traffic to prevent it from reaching the attackers. Symantec on the other hand had another idea, they wanted to reroute the traffic to a server they controlled. After this was done the reports from infected machines piled up, within a week 38000 infected machines had reported in and after a while the number surpassed 100000. Stuxnet was spreading rapidly, despite the signatures deployed by the antivirus companies. When Symantec looked at the geographical location of these infections a pattern emerged. Of the initial 38000 infections, 22000 were in Iran, the US had less than 400. only a small number of the machines had the Step7 software installed, 217 in Iran and 16 in the US.

This pattern was abnormal compared to other worldwide infections, usually the US and South Korea topped the charts because of the sheer amount of Internet users. It started to look like Iran was targeted. With the level of sophistication, plus the stolen certificates. Stuxnet looked more and more like the work of professionals.

[3] `http://www.wired.com/images_blogs/threatlevel/2013/02/Stuxnet-CC-Home-Page-660x577.png`

After more tedious study, Symantec discovered three more zero-day exploits in the malware

> "In addition to the LNK vulnerability, Stuxnet exploited a print spooler vulnerability in Windows computers to spread across machines that used a shared printer. The third and fourth exploits attacked vulnerabilities in a Windows keyboard file and Task Scheduler file to escalate the attackers' privileges on a machine and give them full control of it. Additionally, Stuxnet exploited a static password that Siemens had hard-coded into its Step7 software. Stuxnet used the password to gain access to and infect a server hosting a database used with Step7 and from there infect other machines connected to the server." [109]

The attackers really wanted to succeed in spreading the malware, but as opposed to other popular methods like e-mail of websites, stuxnets exploits helped it propagate through local area networks. The primary way to spread was still through infected USB sticks though. Because of this it seemed the attackers were targeting systems not connected to the Internet, and given the amount of work put into the malware the targets had to be of high value.

So to be able to infect the enclosed systems they would have to infect other system first that probably would have some sort of relationship/connection with the wanted target.

The attacks where focused on five organizations in Iran that the attackers believed could be used as gateways[110]

3.5 Payload

After more extensive study Symantec figured out that Stuxnet had three main parts and 15 components, all wrapped to together in layers of encryption. Stuxnet decrypted and extracted each component only when needed, depending on the condition it found an infected machine. In addition to this Stuxnet also had an extensive configuration file, where you could tweak more than 400 parameters. Some of these parameters were how long it should spread and how long each exploit should work. In these parameters the analyst found an end-date - June 24 2012, on infection Stuxnet would check the date on the system, if it was later then the date, it would shut down.

If Stuxnet found that the host machine had Siemens Step7 software installed, the malware decrypted and loaded a DLL file onto the machine. This DLL file impersonated a legitimate DLL file called s7otbxdx.dll - that serves as a common repository used by functions in the Step7 software.

The Step7 software has a Windows-based interface for programming and monitoring Programmable Logic Controller (PLC). These controllers can control all different sorts of things, motors and valves etc.

When workers tried to communicate with the PLC through an infected computer, the DLL would intercept these commands going from Step7 to the PLC and replace them with

Figure 7: How these devices interacted. Picture from Wired.

its own malicious commands. To keep these actions hidden, another part of Stuxnet disabled any automated alarms that might trigger, it also masked what was happening on the PLC by intercepting the status reports sent by the PLC and stripping out any signs of malicious code. Workers monitoring these PLC through Step7 would only see legitimate commands on the device. Figure 7 [4] shows how the Step7 software communicate with the PLC, Stuxnet would hijack these Read/Write requests.

To help hide itself and execute its commands, Stuxnet also installed itself on the actual PLCs through a root kit.

> "Previously, we reported that Stuxnet can steal code and design projects and also hide itself using a classic Windows rootkit, but unfortunately it can also do much more. Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems. In addition, Stuxnet then hides these code blocks, so when a programmer using an infected machine tries to view all of the code blocks on a PLC, they will not see the code injected by Stuxnet. Thus, Stuxnet is not just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC." [28]

In particular, Stuxnet hooks the programming software, which means that when someone uses the software to view code blocks on the PLC, the injected blocks are nowhere to be found. This is done by hooking enumeration, read, and write functions so that you can not accidentally overwrite the hidden blocks as well.

Stuxnet contains 70 encrypted code blocks that appear to replace some "foundation routines" that take care of simple yet very common tasks, such as comparing file times and others that are custom code and data blocks. Before some of these blocks are uploaded to the PLC, they are customized depending on the PLC.

> "By writing code to the PLC, Stuxnet can potentially control or alter how the system operates."[28]

[4] `http://www.wired.com/images_blogs/threatlevel/2099/07/Step7-and-PLC-660x248.jpg`

The evidence that Stuxnet was sabotaging a PLC was a huge breakthrough, this was not a "simple" case of espionage anymore. However, Symantec had one problem, they did not know enough about PLC to be able to figure out what Stuxnet was doing on the PLCs. So they posted a note on their blog asking if anyone had experience with PLCs and STL (the programming language used on PCLs) and asked them to make contact. But they received no response.

Two weeks after this, traffic from the infected machines in Iran stopped reporting in. Iran had started blocking outgoing traffic, to prevent any information about what kind of machines were infected and to shut down the open channel to them through Stuxnet.

However the blogpost was picked up by a German company that were well traversed in the Siemens PLCs and they sat down and gave it a go. After three weeks of looking at this code they saw that Stuxnet wasn't just targeting a specific type of PLCs, it was targeting a specific setup of machines 8[5], which you could find in the uranium enrichment center.

In the code they found information about technical configuration of the facility it sought. Systems that did not match these settings would be unharmed. Stuxnet shut itself down and moved on to the next system until it found a match.

When they saw this, they realized that this was most certainly a targeted attack by a government with inside information of the target. If it was the US, Israel or even Germany they had no idea.

Back at Symantec they were still heavy at work, and had bought some books on PLC programming, by end of September they had slowly built a profile on the target. They had reversed engineered it enough to understand that it was changing some values on something connected to the PLC, but they still had no idea what was on the receiving end, or what the changes values did.

They had discovered that the system that Stuxnet targeted used the Profibus standard. Process Field Bus is a standard for field bus communication in automation technology[101]. The malware also searched for a specific value "2C CB 00 01" before deciding to attack the PLC. They thought this might be an ID designated by Step7 to the connected equipment, so they made a small lab with the equipment, and the ID popped up when they connected a Profibus network card.

In addition however there were two more numbers Stuxnet searched for; 9500h and 7050h. Neither of these showed up during the testing. They got a breakthrough in November 2010 after putting this info on the blog again. They received information that every Profibus component had an unique ID, it occurred to them that the numbers were manufacturer IDs.

They found a PDF online with the numbers, and it turned out to be product IDs for two types of frequency converters made in Finland and Iran. (These converters are used to modulate the speed of motors and rotors.) In the documentation found online, they saw a list of commands to control frequencies, which matched exactly the commands in Stuxnet.

[5] `http://www.wired.com/images_blogs/threatlevel/2099/07/Frequency-Converters_Symantec-660x495.jpg`

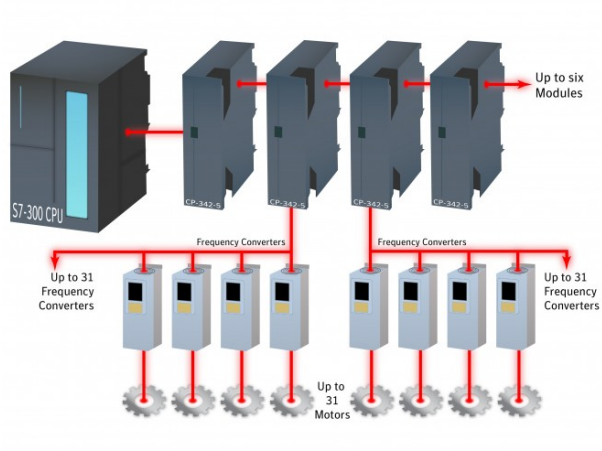

Figure 8: Stuxnet searches for a facility that has a minimum of 33 frequency converters installed. (Graphic: Symantec) [109]

> "Based on information in the code, Stuxnet was targeting a facility that had 33 or more of the frequency converter drives installed, all operating at between 807Hz and 1,210Hz."

The malware would sit quietly on the system doing reconnaissance for about two weeks, then launch its attack swiftly and quietly, increasing the frequency of the converters to 1,410Hz for 15 minutes, before restoring them to a normal frequency of 1,064Hz. The frequency would remain at this level for 27 days, before Stuxnet would kick in again and drop the frequency down to 2Hz for 50 minutes.

The drives would remain untouched for another 27 days, before Stuxnet would attack again with the same sequence. The extreme range of frequencies suggested Stuxnet was trying to destroy whatever was on the other end of the converters."[109]

They did a search online and found that converters used above 600Hz could be used for uranium enrichment.

3.6 Aftermath

The evidence Symantec uncovered about Stuxnet provided a case that the malware had been aimed at Iran's nuclear program. But other than the excessive number of centrifuges being replaced, there was little proof the Natanz facility was the target or that the malware was the cause.

The only statement from Iran on the malware, indicated that Stuxnet had infected some computers belonging to workers at Bushehr, but that computer in other facilities such as nuclear ones were unaffected.

On the 23rd of November Ali Akbar Salehi, head of Iran's Atomic Energy Organization, said the following:

> "One year and several months ago, Westerners sent a virus to [our] country's nuclear sites," [109]

He downplayed the success of the virus's success, saying that workers managed to discover and prevent it from harming any equipment.

If Stuxnet was a success or not is debatable. It managed to destroy some centrifuges and slowing Iran's nuclear program, so in means of slowing it down, yes it had worked, but stopping it, no.

The suspicion people had about Stuxnet being a government funded cyberweapon was confirmed when The New York Times wrote the following:

> "From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program."[74]

After Stuxnet was discovered two more malware popped up on the radar Duqu (2011) and Flame (2012). Duqu is believed to be written by the same people that wrote Stuxnet, or at least, they had access to the source code of Stuxnet. Stuxnet and Duqu are quite alike, but made for different purposes. Stuxnet was made for sabotage, Duqu was made for surveillance and information gathering, maybe for future attacks.[96]. For further reading check out Symantecs report on Duqu [84]] and Laboratory of Cryptography and System Security [17]

Flame did also gather information, according to Wikipedia [97] Flame spread to other system through a local network or through USB sticks. It recorded audio, screenshots, keyboard activity, network traffic and could also record skype calls. In addition to this it could turn infected computers into Bluetooth beacons and attempt to download information from other nearby Bluetooth enabled devices. This malware also had features in common with Stuxnet, for instance it also utilized some of the same zero days attack and also came with a certificate. In June 2012 Washington Post published an article saying that the flame was develop by NSA, CIA and Israel's military [24] However no official statement has been given regarding this. For further reading check the report written by Laboratory of Cryptography and System Security [18]

Both of these were mainly targeting computers in Iran, which backs up the theory of both of these being state sponsored malware. However, as mentioned earlier none of this has been confirmed.

3.7 Conclusion

Stuxnet is classified as an APT and it follows the different stages of attacks put forward in section 3.5. With the zero day attack, backdoor or in this case the command and control servers, elevation of privileges, data gathering and finally in this case the actual sabotage and exfiltration.

Measures that could have been put in place to prevent this from working could be a much stricter policy on bringing devices to work and connecting them to the work machines. However, for this to be more secure, you would basically have to do a frisk search on every employee to make sure they do not bring any such devices to/from work. Also, the USB ports could have been plugged so these are not available for use . This would help to protect you from an attack since you disable one attack vector for a zero-day vulnerability to get a foot hold.

It seems like attack likes this becomes more and more common, and also since some of them are not credited to anyone they can not be seen as an act of war according to US Law [16], however it might not be that the target agree with this assumption. I can see why these types of attacks are worth doing, they are initially covert and difficult to detect, so when you first detect these attacks they might have been in your system for many years already, gathering intelligence or doing sabotage.

4. GOVERNMENTAL AND COMMERCIAL

By André Nordbø

4.1 Abstract

In this section main focus is on governmental, commercial and individual aspects of Advanced Persistent Threat. The reason for doing so is to highlight different perspectives and get a broader understanding of the term.

From a governmental perspective, the main concern is protecting national security. The specific threat is nation states stealing or causing damage to other nation states for strategic gain by targeting computer network technology. Governments report on targeted, long lasting, technically advanced attack patterns as an escalating threat with consequences not yet thoroughly understood. Some countries even consider this type of attack pattern a top priority threat.

Major players known for utilizing APT techniques are United States, China and Russia, but we also know Iran, Japan, North Korea, France and several other countries are preparing for both offensive and defensive capacities. In a governmental context, resources in terms of money, man power, time and leadership are available for crafting custom attack code and use it so that traditional security measures[6] have difficulty detecting it. The spectra of infection and ex-filtration methods extend what is typical for individual attackers and organized crime. E-mail traps crafted using sophisticated intelligence. USB sticks as bate planted at strategic locations. Usage of insiders. Attacking the software and hardware supply chain implementing back doors in commercially available common off-the-shelf [7] equipment are all examples of how far the reach can be.

The damage potential ranges from denying communication using distributed denial of service attacks, stealing intellectual property and intelligence of political decision makers and of military capacities. Even destruction of equipment such as industrial monitor and control systems (SCADA) is possible by digital attacks using logic bombs. The Stuxnet attack is an example of this as described in section 3. This effort can be thought of as targeting the opponent's benefit gained from using technology as a force multiplier because of the realized weakness that our societies no longer have manual fall-back solutions capable of keeping up the efficiency.

In trying to deal with this threat, national CERTs are being established responsible for collecting situational awareness and coordination of response. Military organizations expand cyber as a 5th element of warfare in addition to land, sea, air and space, focusing on both defending (CND) and attacking (CNA). Traditional response is blocking and restore, but from a tactical perspective we see a shift to silently monitor the attackers in order to learn their methods and capabilities, and extending it by running counter-intelligence operations "playing" the enemy with false information. Sometimes we might even have to continue using a compromised system because the net benefit is considered higher than any potential loss because of unavailability. Air gapping disconnecting system from other networks like the Internet is a understood need, but is difficult in practice. In monitoring the threat, we see APT databases are being built in order to establish ground for attribution, combining data from real systems and honeypots. Talking about such matters has traditionally been classified, but we see a tendency of opening up for intelligence sharing as seen with the recent Mandiant report and regulation like CISPA being proposed, although not passed because of privacy concerns.

The APT phenomena can be though of as existing sophisticated threat agents realize attacking networked digital equipment in cyberspace has benefit, and it is made easy because of wide usage of cheap standardized common off the selves equipment, and because convenience often triumph security. APT is a key ingredient in cyberwar, and there are ongoing discussions on what rules (like rules of engagement) shall apply in cyberspace. Questions like is it allowed to hack back and what is the borderline of conventional war is being discussed. The recent Tallin manual use existing international law to answer these questions.

APT in a commercial organizational perspective is tightly related to the governmental view, because any attacker wants to attack the weakest link. Why confront military forces if the same goal can be achieved going after a smaller less aware contractor in a long supply chain, or trying to destroy the economy supporting the opponents center of power. While governments main concern is national security, commercial organizations main focus typically is profit. Currently there is little incentive spending money on massive protection and monitoring unless the loss of breaches can be determined (return of investment). From a commercial perspective there is also a constant high threat of attacks with the intent of economic gain like bank trojan attacks and blackmailing, credit card theft and access to user databases in which APT type of attacks drown. Forensics readiness is a way of thinking trying to maximize the available evidence for investigating such breaches and also deter insiders.

At the individual level, the APT threat is not relevant targeting an individual for the person itself, but for the role the person represent. Trends using private equipment is a considerable risk as these devices tend to be less secured. APT typically go for key personnel and people in their circles in order to have targeted attacks look genuine. Other concerns related to APT methodology is it being used as an excuse to implement even more regulation skewing privacy concerns even more aside and to spy on citizens using "lawful interception trojans".

[6]Traditional meaning anti virus solutions, network intrusion detection systems and the like depending on known attack signatures

[7]Commercial off-the-shelf "ready made for purchase; not custom-made" [source: thefreedictionary.com]

4.2 Introduction

In the previous sections you have read about what Advanced Persistent Threat is, the anatomy of it and read a case study. In this section the focus will be on APT from a national viewpoint followed by a part on commercial aspects and lastly some thoughts at an individual level[8]. The main goal is to put APT in a context by discussing topics such as national security, cyber warfare, threat agents being called Advanced Persistent Threats and typical targets. Later sections will explore how to detect and protect against it.

4.3 Governmental

There are no national borders in cyberspace, making the separation between military external threat focus from police internal focus a bit artificial. Governmental perspectives regarding national security is the focus now, and although especially focus will be on military aspects, there are also other services such as police secret services and governmental ministries/departments equally relevant for the topic. Our societies are increasingly depending on standardized digital interconnectivity, opening up a variety of new possibilities for efficiency and convenience but often at the cost of new vulnerabilities. One example is how military operations require huge amounts of information to be shared in as close to real time as possible in order to take advantage of increasingly more advanced equipment

> ”cyber enables us to “see, hear, and talk” faster and over longer distances, which enables us to perform our military objectives faster and with a greater accuracy”[39, page 5]

Critical infrastructure is being interconnected in order to utilize new sources of information for automation and also allowing for remote monitoring and control vastly outperforming manual human work. The Advanced Persistent Threat term, as noted earlier in this report, was originally coined by the U.S. Air Force around 2006 [91]

> ”Originally, the term was used to describe nation states stealing data or causing damage to other nation-states for strategic gain”[91, page 2]

The APT acronym is used when referring to a group of people being considered such a threat. In the Mandiant report of 2013 one such group believed to be supported by the Chinese military is nicknamed ”APT1”[54]. Still, another way to look at APT is as a methodology or strategy.

The quoted explanation has a very important distinction: Where the goal is to steal and where the goal is causing damage. The first is related to surveillance and intelligence operations, espionage in other words and require a back channel for ex-filtrating the gained knowledge. The other is focused on disabling, limiting or causing damage to equipment and it does not necessarily require any means of a back channel. It can be blind or triggered by an insider.

[8]One group member decided to quit our project group, and thus his topic ”commercial aspects” was merged into this one

A term was needed to describe a new kind of threat different from already known attack patterns performed by script kiddies writing worms for fun and fame, and criminals seeking short term economic gain. These attacks typically target the widest audience possible, the lowest hanging fruit, and triggering whistles as bank accounts are emptied and websites brought drown in distributed denial of service attacks. The new patterns[5] were advanced methods, persistence and being targeted.

Advanced methods include a variety of methodology ranging from very technical crafting of novel exploits[9], to social attacks like leaving USB drives as bait and fooling users with targeted well written e-mails as mentioned in the NIST definition[60]. It has to be noted that much harm can come from little effort, like this claim of the attack on Swedish ”NemID” only costed 10 dollars in renting a botnet[9] and as Gavin Reid[10] said:

> ”most APT attackers tend to be only as sophisticated as they need to be, which often isn’t too sophisticated ... People will say, ‘Well, this attack wasn’t very advanced, so it can’t be APT’, but I will tell you the folks who are behind some of this stuff are not going to use cool zero-day stuff if they can go in the underground economy and say, ’Hey, I need an infected machine in this organization’, and pay $50 in Paypal in order to get that”[48]

> ”In military, it is about effect, not about means. The cheapest most powerful and best effect combination of means will be applied. It is always about combination.”[37]

Persistence implies stealthy execution as a strategy in order be to efficient, and stealth usually require a combination of patience in combination with uncommon methods. The most important aspect is the nature of the threat. The victim is targeted, and resources are spent dedicating the attack for this purpose alone. In other words, it’s useless to hide in the crowd.

In order to illustrate the targeted nature, a recent malware Gauss has an interesting method for making sure it does not cause collateral damage: It’s considered a ”cousin” of Stuxnet [31] and:

> ”has the ability to steal funds and monitor data from clients of several Lebanese banks, making it the first publicly known nation-state sponsored banking trojan”[31]

Perhaps it is implemented to misdirect attention? Gauss also has code for distribution via USB drives, suggesting

[9]Zero-day vulnerabilities: Attack vectors unknown to the industry when discovered, meaning no anti-virus or intrusion detection system signatures are available

[10]senior manager of Cisco’s computer security incident response team

that 'airgapped'[11] systems might be a target.

> "The coding techniques [of Stuxnet] were largely limited to conditional 'if/then' range checks that identified computers running German conglomerate Siemens's Simatic Step7 software inside Natanz. If an infected computer met the criteria, the sabotage payload was activated. If not, the exploit sat dormant."[31]

What's new in Gauss is that a part of the payload is encrypted with an encryption key derived from a combination of the state of the targeted machine(s), the path variable and folder structure. The key generation algorithm is hardened in order for brute force to be very slow. As explained in the article, this has two very neat properties: Firstly we don't know what the target is, because we don't know what triggers the decryption, and secondly we don't know what will happen because no example of a host performing encryption has been found. Another interesting fact is that a strange font is found on a tiny fraction of the Gauss infected machines[49], called 'Palida Narrow' and the author in the cited article suggest it's being used as a marker

> "It is the scout malware, marking the target and awaiting for extraction"[49]

One might imagine a scenario where a new release of malware looks for this font being installed, then creating a folder and editing the path in order for the original payload to be activated, this allowing for control of activation. Also as noted in the comments of the article[77]:

> "if you have a mole inside the organization you want to attack, you can easily tell him (or her) to add a specific string to PATH (which may not even be a directory at all). This way, you conceal the payload, and you control the timing of your attack with a simple command"[77]

4.3.1 What does governments say about this threat?

According to this article[80] Lieutenant General John Hyten explains on behalf of the U.S. Air force they are developing cyber capabilities as a response to

> "escalating cyber attacks by China, Russia, Iran and others"[80]

The workforce dedicated to cyber operations is planned to be expanded from the current 6000 to about 7200 and six 'cyber tools as weapons' is being mentioned in the battle for resources from Pentagon.

> "Hyten's remarks came a month after U.S. intelligence officials warned that cyber attacks have supplanted terrorism as the top threat to the country."[80]

[11] Systems not directly connected to the rest of the network, like the Internet

Although this quote does not address APT specifically, it is still very relevant. The U.S. also realize that military cannot fight this 'war' alone and needs corporation with commercial entities by making sure information is shared:

> "Two members of the House of Representatives introduced the controversial information-sharing bill, the Cyber Intelligence Sharing and Protection Act (CISPA)"[32]

> "The bill purports to allow companies and the federal government to share information to prevent or defend against network and other Internet attacks[56]"

> "Rogers and Ruppersberger believe that if United States intelligence agencies could share classified information with the private sector, then the security industry and private corporations will be better armed to defend themselves. Similarly, the intelligence community could also benefit from private companies sharing what they know about attacks with the government.[7]"

Both the Mandiant report and this talk[19] shows the same trend in governments starting to realize keeping these aspects secret might not be the best strategy and start sharing in order to fight the problem together. At the same time, discovery and creation of cyber weapons, including zero-day vulnerabilities can be considered a tactical advantage. There is a "battle" even inside countries between groups discovering and crafting attacks and security companies trying to protect against them. These security firms can have customers on both sides of an APT operation. Operations like Stuxnet and Red October, claimed to be state sponsored, both got taken apart and disclosed by private anti virus companies, probably upsetting officials behind these operations relying on keeping unknown vulnerabilities and techniques hidden. Security and software firms rely on their reputation, and any proven claim of them helping either side would seriously hurt their marked position. With Microsoft's position in the operating system marked, controlling the source code (blueprint) and able to patch machines at will, one can only guess at what the U.S. Government potentially could make Microsoft do.

In Norway, public reports for 2013 from the Norwegian Intelligence Service (E-tjenesten), National Security Authority (NSM) and Police Security Service (PST)[63][67] describe trends relevant for APT. Translated they mention that

> "Particularly worrying is the increasing number of targeted espionage operations against Norwegian industry and Norwegian interests"

> "Several states are developing advanced malware that is designed to destroy infrastructure, disrupt important social activities or influence decision-making and information processes."

> "Many businesses focus on attacks from outside, but is poorly equipped to resist compromise of systems from the inside"
>
> "Increasingly communities build up expertise in intrusion on SCADA systems in critical infrastructure. Because of the anticipated large vulnerability of these systems, there is an urgent need for better assessment of threats and vulnerabilities"
>
> "There is too little focus on security in the supply chain for IT equipment and components. Security in the supply chain between the manufacturer and the system owner should be strengthened."
>
> "Most attempts to obtain technology from Norwegian companies, which are relevant for the development of weapons of mass destruction, can be linked to Iranian actors"
>
> "Such industrial espionage might be carried out by foreign intelligence services exploiting or placing students and researchers inside the relevant research environments and companies"

An article from the Norwegian military "Forum"[23] covers how NorCERT deals with long lasting threats.

> "We're not very concerned with who is behind the attacks, but rather the techniques being used and what they are attacking ... Some attacks last several months and consists of a series of battles"[23]

NorCERT is a national center for dealing with serious cyber attacks targeted against critical infrastructure, focusing on sharing of information, coordinate and helping both government and civil organization respond to these threats[62].

To summarize, we see both military escalation and openness as possible solutions, with the internal conflict is raises. Supply chain and SCADA systems are mentioned as weak spots, and the low focus on threats internally is quite interesting. According to the 2013 Verizon data breach report[76]

> "Contrary to popular memes, only 14% of attacks involve "insiders" – whereas external attacks remain responsible for 92% of data breaches. Interestingly, "only" 1% of data breaches were traceable to business partners."

[76] Still, since one of the goals of APT type of attacks is to be stealthy, as discussed in a previous section, compromising an internal users account and acting on behalf of it's access makes defining "insider" difficult and it leads to the need of limiting what even legitimate insiders have access to inside a network.

4.3.2 How serious is the threat?

In order to understand the seriousness of APT, lets look at some examples. They are selected, shortened and translated from an article by the Norwegian "Teknisk Ukeblad" in their article "16 spectacular cyber-attacks"[34]: The question marks are added because attribution can be very uncertain unless the attack has been acknowledged by the attacker. The target is usually more clear.

- 1982: U.S. attacks Russian: In-planted code cause overload and explosion of trans-Siberian gas pipeline cables
- 1998: U.S. attacking Serbia: Compromising air navigation systems in order to ease bombing from allied forces (Radar-hack 1)
- 1998: Russia? attacking U.S: Pentagon, NASA with others compromised for 2 years stealing maps of military installations, movements and equipment design (Moonlight Maze)
- 2003: China? attacking U.S.: Trying to steal defense secrets from major defense contractors like Lockheed Martin, SNL and Redstone Arsenal (Titan Rain)
- 2007: Israel? attacking Syria: Syrian air control compromised in order to ease Israelian fighters bomb a target (Radar hack 2)
- 2008: Russia? attacking U.S.: Planted USB flash drive in a military base in the Middle East infecting central command network (Centcom)
- 2008: Russia? attacking Georgia: Three days before Georgia launched its invasion of South Ossetia, national media and governmental sites were being flooded to make them unavailable
- 2009: China? attacking 103 countries: Software written to infiltrate and spy on governmental computer systems, mostly Southeast Asian countries tracking Dalai Lama and Tibetan exiles[19] (GhostNet)
- 2010: U.S./Israel attacking Iran: Software written to infiltrating Iran's uranium enrichment facility in order to sabotage their nuclear program (Stuxnet)
- 2012: Iran? attacking Saudi Arabian: Computer virus wiping information off 75% of Saudi Aramco computers, replacing all of it with an image of a burning American flag.[66]
- 2012: Russia? targeting diplomatic, governmental and scientific research mainly in Eastern Europe, former USSR members and countries in Central Asia. Active since 2007 using sophisticated technologies like file recover for deleted files, and a resilient command and control architecture. The campaign targeted mobile devices in addition to workstations[45]. (Red October)

Other campaigns like Duqu, Red October, Flame, Shady rat, Gauss and the recent attacks on South Korean banks and broadcast station all draw a picture of a very real threat,

and it also tells us many details might still be classified, unknown to the public. In terms of attribution we don't know for sure who is behind, but we see major players being U.S. China, Russia and it's a game in both directions. Other active offensive states are Israel, UK, Germany, North Korea and Brasil[13]. These operations or campaigns range from denying information flow, gathering intelligence, to actually causing physical damage to infrastructure. The method of attacks is not limited to remote attacks over IP as both planting of memory sticks and introducing "modified" hardware and software in the supply chain as seen in the examples. In order to summarize so far, we see that cyber attacks are considered a major threat, targeting critical infrastructure including military systems, decision makers and industry. Attribution is difficult.

4.3.3 What is the weakness?

What makes cyber attacks and APT in particular such a threat? We know governments control and regulate many critical tasks, and are responsible for national security defined as:

> "maintain(ing) the survival of the state through the use of economic power, diplomacy, power projection and political power"[99]

Typical tasks lie within the term "critical infrastructure" which can be defined as

> "a term used by governments to describe assets that are essential for the functioning of a society and economy"[70]

Examples given are:

- Electricity production using gas, oil and nuclear resources.
- Telecommunication like phone, mobile and data.
- Water supply and cleaning.
- Agriculture and food supply
- Medical care like hospitals and ambulances.
- Transportation like railways, airports, train and harbors.
- Financial banking services and
- Security services like police and military.

Many of these functions are being controlled by a kind of industrial control systems, typically known as SCADA[6]. A simplistic view on SCADA is remote monitoring and control of industrial processes. Most of these systems have been developed with the assumption of a secure environment, and this assumption is now broken with the move to Internet technology. What could possible go wrong if unauthorized persons got access to atomic reactor controls, were able to change how water is cleaned, could kill power in a hospital, or disable communication before a military attack?

Figure 9: This figure illustrates the force multiplication factor of using technology in military operations. It also illustrates what the weakest link might be. (KAL's cartoon @ economist.com) [22]

In order to exemplify SCADA and a new term force multiplication, let's look at this video of Walt Boyes[6]. He mentions how 6 pump technicians continuously drove around visiting all well stations belonging to the company looking for errors and fixing them as discovered. With the earliest SCADA systems they were able to cut down on resources as alarms could be put in place, allowing for sending technicians on demand rather than have them move around all the time. Technology allows for "force multiplication"[98] as fewer people can be equally effective assuming the technology is available. Another answer to why APT is effective probably lies in knowledge of what makes the opponent more effective, and being able to disable those factors of the opponent at the right time. A funny illustration is given in figure 9 showing this concept. In other words, using APT strategies in order to shift the balance of power.

As mentioned in the introduction, another important reason for the major vulnerability in these interconnected systems is that they all utilize standardized equipment. Running Microsoft Windows, using Cisco network equipment, "off the shelves[12]" equipment in general. Since everybody has the same components, everybody also have the same vulnerabilities. Still, it's cheaper and leads to interoperability[13]. A commonly used strategy for protecting critical systems is to "airgap" them, not connecting them to the Internet. Administrative and convenience considerations might still lead to closing the gap using USB sticks and introducing code and hardware via insiders like suppliers and partners.

One way to solve the monitoring problem could be using a "dualdiode" configuration using fiber optics, physically limiting communication one way.

> "The company I work for has solutions in place

[12]Common off the shelves equipment is often shorted COTS equipment

[13]Interoperability means able to work together, ready to be connected without much hassle

> at more than half of the nuclear facilities in the United States. These solutions consist of a pair of machines. One is connected to a secure internal network or device, while the other is on a separate, less secure network, perhaps with Internet connectivity"[30]

The Military is known for being very careful with confidentiality, dividing information in several sensitivity domains, regulated by law, but even the military make use of "off the shelves" equipment, and military command and control systems fall withing the definition of SCADA systems.

We have already seen examples of governments restricting commercial suppliers of critical infrastructure from foreign countries as seen mentioned in the governmental reports earlier:

> "In fact, there is a growing recognition of vulnerabilities resulting from foreign-sourced telecommunications supply chains used for U.S. national security applications. The FBI, for example, has assessed with high confidence that threats to the supply chain from both nation-states and criminal elements constitute a high cyber threat" ..."U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects"[64]

Concluding so far, we have looked at force multiplication being using technology to increase effectiveness at the cost of reliance on technology, critical infrastructure is vulnerable because of this, air gapping is a known solution, but being consistently gapped is hard, and it is also important to protect the supply chain bringing new equipment in.

4.3.4 Cyber war and APT as a weapon?

What is cyber war and how does it relate to APT? Richard A. Clarke has written a book on "Cyber War", "the next threat to national security and what to do about it", and in this interview[13] he classifies the threats in cyberspace like this:

- Crime: basically theft of money, going on all the time
- Hacktivism: Steal information for political reasons (or selling to the highest bidder)
- Espionage: Theft of information, particular from private companies and universities
- War: Disruption, destruction or damage

He mentions two major concerns: first industrial espionage, accusing primarily China of stealing intellectual property and research results U.S. and Europa has spent billions of dollars researching, and secondly cyber attacks targeting critical infrastructure[12] disabling banking, power, airliners and other systems highly dependent on digital processing and networking. He also talks of how we might have to consider attacks as war, even though nobody directly gets killed.

Richard also mention how the U.S. Military, and many other countries[44] as well, have established cyber as a 5th domain and having dedicated cyber branches performing offensive and defensive operations.

> "The military has recognized cyberspace as an operational domain similar to land, sea, air and space, that is, as a space to be used for military purposes and for waging war."[39]

, and he points out that the military way of "dominating each domain" is not helpful as the cyber threat require collaboration from people around the world and militarizing the issue is not the solution.

In order to clarify, espionage is not considered an act of war unless it's as a preparation for war, because it's not use of force. It arguably has [33, at 11:20] stabilizing effects. Crossing the line of war, as he argues, has to do with disruption and destruction at a larger scale often involving deaths and using cyberattacks in combination with kinetic traditional vectors as bombs and arms, but at the same time stressing deaths should not be the defining criteria as cyber attacks can make a society halt without actually causing harm to humans.

Other important aspects he mention is that cyberspace has an offensive preference, meaning it's much easier to attack than defend it, using a number 1000 times more expensive in favor of protection. This is an interesting observation, opposite of conventional warfare where it's the other way around. Another interesting property of offensive cyber operations as he mention is that once a "cyber weapon" is released, it can relatively easy be taken apart and be "thrown back" at the attackers.

A weapon can be defined as:

> "any device used in order to inflict damage or harm to living beings, structures, or systems"[103]

and one might ask, can APT be considered a weapon? The methods used and intentions of APT's most certainly can hurt systems, and indirectly hurt humans, but it's important to separate between the methods used and the threat itself. A well written way of summarizing APT is:

> "One cannot stress enough the point about APTs being, first and foremost, a new attack doctrine built to circumvent the existing perimeter and endpoint defenses. It's a little similar to stealth air fighters: for decades you've based your air defense on radar technology, but now you have those sneaky stealth fighters built with odd angles and strange composite materials. You can try building bigger and better radars, or, as someone I talked to said, you can try staring more closely at your existing radars in hope of catching some faint signs of something flying by, but this

isn't going to turn the tide on stealthy attackers. Instead you have to think of a new defense doctrine.[73]

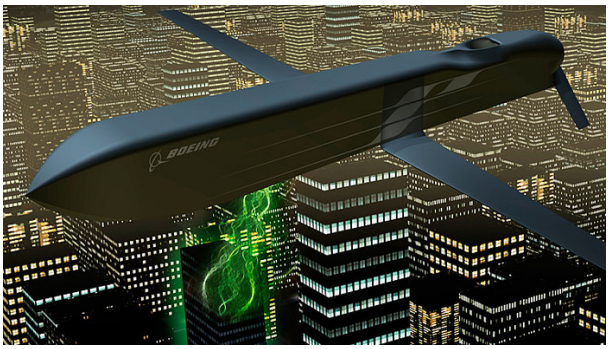

Figure 10: Illustration used in an article[10] describing using high power microwaves to damage computer equipment. Can we consider an attack on cyberspace using conventional kinetic attacks as part of a cyber attack?

It's also important not to confuse conventional attacks destroying opponents communication equipment via means like jamming, bombing, microwave attack[10] and even releasing an EMP[14]. They are attacks on cyberspace, and might be an important aspect of cyberwar, but not typically something associated with any APT campaign. Figure 10 shows an illustration of usage of microwave for attacking computer systems limiting damage to humans and buildings using airborne delivery. Knocking a society "back to the stone age" was the main plot in the James Bond movie GoldenEye using EMP, and exemplifies the damage potential cyberwar has.

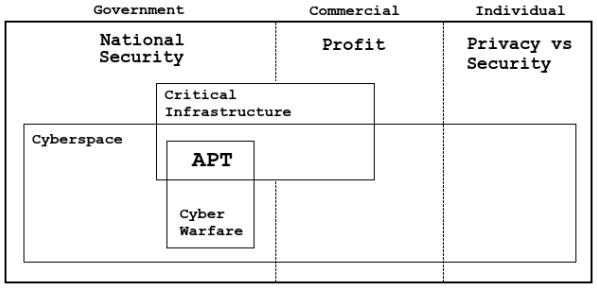

Figure 11: Parts of the critical infrastructure are being connected to cyberspace, and one way of looking at the APT phenomena is the intersection of cyber warfare with infrastructure critical for national security.

Concluding this we see APT methodology can be a part of cyberwar, although cyberwar covers a larger collection of means to reach the goal. We might also consider viewing systematic pressure from APT as equally serious as war in the long term. By combining the terms critical infrastructure, cyber space and cyber warfare in figure 11, one way to think of APT from this perspective is as the intersection. At least if cyber warfare is extended to include strategic industrial espionage.

[14]Electro Magnetic Pulse, an effect discovered from nuclear reactions causing electric equipment nearby to blow up. The effect can be induced using other means too

4.3.5 What laws apply?

The Tallin manual[26] recently published discuss questions related to what rules of engagement apply in cyberspace. It was initiated by NATO, and describes 95 rules, the result of 3 years of work of a group of 20 international experts. The goal was to look at current international law and how it could be applied. It's not a formal NATO policy document, but intended for discussion. The manual states that civil cyber attackers could be legitimate military targets and use of traditional force can be a valid response to cyber attack, giving rise to several news articles[83][35], but it also states any retaliation has to be proportional to the original attack, and that cyber attacks are legitimate means in conflicts as long as they are not directed at civil targets using hospitals as an example[83].

> "Cyber conflict has been divided by two schools of thought, the first of which feels that cyber is so new, so different that no existing laws, customs or norms can apply. ... These nations assert, for example, that a new treaty is needed to regulate how states use cyberspace for military purposes ... The United States, the United Kingdom and other like-minded nations have accordingly taken the opposite approach, asserting for years that the world should first embrace existing laws and only create new ones to address the gaps"[35]

4.3.6 Deception, the Fabian strategy and attribution

The military has traditionally had the main responsibility of protecting national security against external threats. Besides usage of technology, the Wikipedia article on force multiplier[98] also mentions deception and the Fabian strategy as important factors. They are very relevant for APT and for network centric warfare[15].

The authors of the paper Spy vs. Spy[2] argues that if an intruder is able to access a system where classified or highly sensitive data is accessible then it might not be sufficient simply to clean the system, but rather

> "a counter-intelligence operation may be initiated to track the infiltration back to its source. It is important that the counter-intelligence operations are not visible to the infiltrator."

The authors then cite relevant objectives like who the attacker is, the objective, capability and depth of penetration and how to detect without alerting the adversary using root-kit technology. If an APT type of attack is detected, resources can be routed towards misguiding the intruders by spreading false information.

[15]Network Centric Warfare can be thought of as a similar idea to the general trend of networking everything in the name of more efficiency, but also includes organizational changes in order to fully utilize the technology

An offensive view APT methods can be attacking the enemy without direct confrontation as described by the Fabian strategy:

> "...one side avoids large, pitched battles in favor of smaller, harassing actions in order to break the enemy's will to keep fighting and wear them down through attrition"[36]

Attacking the supply chain or the economy is an effective way of wearing down the opponent.

Another important thing to remember is that even if your network is under attack, operational considerations might still be too important for it to be disabled. Roger Johnsen, current head of Norwegian Defence Cyber Academy describes this in an interview:

> "In many situations it is favorable to continue using the [infiltrated] systems. It's about determining the risk of having the opponent in your system - versus the military advantage of using the system. In the Norwegian military, performing these considerations and choices is cyber defense in practice."[translated][43]

Attribution is linking a person or a group to an event. How can the question of attribution be dealt with?

> "Typically when hacking or malware traffic is reported on the Internet, the location of the source IP is not a reliable indicator of the true origin of the activity, due to the wide variety of programs designed to tunnel IP traffic through other computers. However, occasionally we get a chance to peek behind the curtain, either by advanced analysis of the traffic and/or its contents, or due to simple programmer/user error."[40]

The author of this blog[52] divides people discussing attribution in two camps: engineers knowing everything of how easy it is to hide technically, and the analytics looking for human patterns behind attacks utilizing also non technical means. He also discuss whether it is possible to respond to a cyber attack by counter attack[47], or if releasing a planned attack might be the only way. This is interesting because most major strategies seen in APT rely on operations planned way ahead of execution.

This article [57] claims Japanese government is building APT database to aggregate threat intelligence in order to study targeted attacks. It's claimed to be an 800 million yen project in cooperation with foreign and domestic companies and governments. Methods mentioned is using "fake servers", also known as honey pots. The goal is to build better cyber defence strategies.

The Mandiant report[16][54] 2013 shows us companies in U.S. are doing the same thing and gives some examples of how the attribution question can be answered. It focuses on a (claimed) Chinese threat group called "APT1", one of several discovered. Attribution is possible not because of packet tracing, but because of small artifacts like comments and metadata in backdoors, as the tools used are custom made. By building and finding the same tools and methodology in different cases for different companies, a bigger picture emerges. Mandiant released a huge set of indicators including fingerprints of tools found, URL's and IP's. Mandiant reports increasingly APT style attacks are being discovered, but also notes it could be because of getting better at spotting the activity, and

They report on typical goals for APT1 including

> "intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership."[54]

> "Jaime Blasco, labs director at security tools firm AlienVault, described APT1, aka Comment Crew, as one of the more successful hacking group based on the number of targets attacked - but not necessarily on the skill level of its members."[51]

Concluding the governmental perspective, we have now seen an increase in military budgets for a 5th domain of warfare with both offensive and defensive goals. One reason is an offensive preference in cyber attacks. Governments also think in direction of more openness with sharing and collaboration internal and externally. It is a need for better assessment of SCADA system vulnerabilities, better control in IT supply chains, and a need to shift focus to protecting compromise of systems from the inside. Critical infrastructure being connected gives force multiplication effects, but is also a major cause of vulnerability. Air-gapping is an understood means of dealing with the problem, but it is difficult in practice. APT is threatening in terms of industrial espionage and damage to critical infrastructure. APT is a part of cyberwar, but cyberwar also includes attacks on cyber-domain using physical means such as jamming and EMP. The Tallin manual apply current international law on cyber domain. We have also looked at APT as the Fabian strategy, discussed the importance of discovering such attacks without it being given away, allowing for deception operations. Attribution is possible by looking for human patterns in methods and tools, and also technical mistakes. Lastly, even if your network is compromized, you still need to consider the operational consequences regarding the potential loss by keeping it running versus the potential loss of not having it available.

4.4 Commercial (Organizational)

We now change focus from governmental "national security" to a smaller scale consisting of commercial and internal affairs. Typical threats at this level is concerned with protecting results of own research and development, information critical to contract negotiations and public reputation. Claims of Chinese government stealing product ideas and

[16] American cybersecurity firm

giving it to their own industries is one example as already mentioned[13], and represent a borderline case because it's systematic and external to a whole society. Anther example can be how Comodo was set out of business as their trust as a Trusted Third Party was totally broken after their compromise and handling of the situation.[33]. From the commercial perspective, whether it was another government, a competitor or criminals isn't really that important. What's important is that it hurts the company financially.

Other examples

- 2005: The Athens Affair[89]: over 100 high ranked officials customers of the Greek Vodafone-Panafon phone company, including the prime minister, were being bugged. software at the "heart of the phone system" was changed, probably aided by an insider.
- 2009: Operation Aurora[15], several companies including Google, Yahoo, Symantec, Adobe and Rackspace were targeted by a group "Elderwood Crew" tied to the Chinese army. The attack vector included a zero-day in Internet Explorer, and the goal seemed to be to access and modify source code repositories and retrieve access to Gmail accounts of Chinese dissidents.
- 2011: RSA, a U.S. security firm was attacked using phishing e-mails with Adobe PDF zero-day, targeting their two-factor authentication token system[73]
- 2012: New York Times[65] compromised, presumably by Chinese actors.

  > "The malware was identified by computer security experts as a specific strain associated with computer attacks originating in China ... Experts found no evidence that the intruders used the passwords to seek information that was not related to the reporting on the Wen family."

These examples are highlighted because they target commercial organizations, although the motive could be political as seen in the New York Times and Athens Affair examples. M. Daly's in his talk[19] asks the question:

> "I'm not in the military. Why do I care? [of APT]"

He also answers it by talking of how supply chains are not limited to governments, and because it's easier to go after smaller companies. Even if you think your organization is of no interest to any APT, it could still be used to reach other targets, and he mention examples as being a drop site[17], a command and control server (making it look like you are the bad guy) or infecting your web portal targeting users of your popular services.

A difference between the governmental view and the commercial view has to do with the amount of resources available. Huge multinational corporations might have resources at the level of some (small) states, but when it comes to small and medium sized, money for protection, detection and investigation is limited. If we look aside from the typical cyber warfare related scenarios, most of the APT pressure today reside on commercial organizations. This is because of the low protection and because they can be leveraged as back doors into more valuable networks like military networks and critical infrastructure as previously mentioned, and not to forget their role in the economy and innovation.

There is a cost of paying for security and unless the benefit pays of, a return of investment, security is not currently going to be prioritized, and the hard part is proving any benefit of spending huge amounts of resources on security. When an intrusion is detected, many organizations will be in a dilemma: investigate or simply restore the infected machines. Investigating might lead to learning more of the intentions behind the attackers, learn how they got in and what was taken, perhaps even take legal action. It comes at a cost, critical systems might have to be shut down in order to protect evidence and unless prepared for this could be down prioritized by the leadership. Forensics readiness[72] is a term used to describe measures organizations can implement in order to be able to efficiently secure evidence necessary for investigation and at the same time reduce the business impact of not being prepared. Several aspects like deterring insiders, minimizing disruption when an attack is discovered and having evidence with higher confidence are arguments for having it.

A SANS newsletter[1] has an interesting take on the issue claiming:

> "The number of bad actors, spread among nations, terrorists, anarchists and criminals, is so great that their identity is not as important as what we do to defend our systems - because they usually exploit the same weaknesses"

and it cites a CSIS report[50] "Raising the Bar for Cybersecurity" focusing on finding preventive measures targeting most attacks, as it claims

> "More than 90% of successful breaches required only the most basic techniques."

Websense summarize the easiness of using hacking tools and methods in their quote:

> "The important thing for security professionals to understand is that the same APT techniques used by nation-states for strategic gain are now used by cybercriminals to steal data from businesses for financial gain"[91]

In a discussion on APT [5] the author claims going after money is not considered APT. With the perspective of governments that's probably true as there is nothing new to theft. Still, if we look at banking trojan attacks from the perspective of banks, they are certainly advanced, they are

[17] An intermediate stage to transfer stole data

persistent and somewhat targeted. As methodology typical for APT is being adopted by organized crime, we are probably going to need better labels separating between the techniques and the intentions of these attacks, be it economic gain or information dominance[37].

The European Union released a cybersecurity strategy[27] early 2013. They say:

> "Our freedom and prosperity increasingly depend on a robust and innovative Internet ... the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognize its leading role." [27]

One of the main motives for focusing on securing Internet is economic growth and it's hindered by confidence in the technology:

> "Europe could boost its GDP by almost €500 billion a year ...2012 Eurobarometer survey showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases ... Across the EU, more than one in ten Internet users has already become victim of online fraud ... The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies."[27]

Suggested action focuses mainly on information sharing, cross border cooperation, building Computer Emergency Response Teams (as exemplified with NorCERT in the governmental view), and strengthening the European Network and Information Security Agency ENISA. They also talk of making security more attractive by introducing security labels:

> "labels indicating adequate cybersecurity performance will enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge"[27][18]

Concluding the commercial view, we see commercial organizations being targeted because they are less protected, they can be targeted as an intermediate steps and also directly targeted because of their position as a supplier or partner with trust withing a more valuable network for the APT. Because of the protection resource gap between small / medium sized commercial organizations compared to governments, European Union suggested building a hierarchy of national and sector based Computer Emergency Response Teams (CERT) and also a transnational Information Security Agency in their cyber security report. Forensic readiness is another method developed for easing collaboration between organizations and Police during investigations. We see actors not associated with APT adopting APT techniques and methodology for opportunistic (economic) gain, and it calls for a need to separate between APT methodology versus the goals and intentions of threat agents.

[18] A problem with the implementation of this solution was way too many certificates to choose from, according to Professor Bernhard M. Hämmerli

4.5 Individual

A final perspective on APT is at an individual level. APT attack humans exemplified earlier with targeted e-mails (spear phishing) and plating of USB sticks as bait. Succeeding often requires in depth survey of key individuals within the organization. The term "Bring your own device"[92] (BYOD) is a trend in employees using their own phones, laptops and similar technologies for work related tasks. Issues as mentioned in the article are security breaches because infections from private usage is brought inside the company, and at the same time company information is brought out and potentially lost. Having the same smart device in meetings perhaps later privately in pubs and in public is a huge risk considering the recording properties of the devices. Not to mention cloud storage and backups.

Another question is whether a government act as a persistent threat against it's own population? Turning advances technology against its citizens, possible threatening democracy. With the constant battle between fighting crime versus privacy concerns:

> "In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online."[27]

Even inside EU we got an example of poorly handled networked wiretapping package "QuellenTKÜ". It was described by the "Chaos Computer Club"[14] of what they call "lawful interception malware" used by German police for remote control of suspects computers enabling extraction of users data, activating microphone and web-cameras. It had flaws that enabled anyone on the Internet to take advantage of it, and it also had features for updating the "malware" which could potentially be used for planting evidence.

> "The screenshots and audio files it sends out are encrypted in an incompetent way, the commands from the control software to the trojan are even completely unencrypted. Neither the commands to the trojan nor its replies are authenticated or have their integrity protected ... CCC was told that all versions of the 'QuellenTKÜ' software would manually be handcrafted for the specifics of each case. The CCC now has access to several software versions of the trojan, and they all use the same hardcoded cryptographic key and do not look handcrafted at all ... Unfortunately, for too long the legislator has been guided by demands for technical surveillance, not by values like freedom or the question of how to protect our values in a digital world. It is now obvious that he is no longer able to oversee the technology, let alone control i."[14]

Potential APT groups have so far been assumed to be organized, well founded, typically viewed as either supported or directly driven by governments. We also noted organized crime starts to implement methodology seen in APT attacks for economic gain. There is no reason why individual attackers can't use the same techniques at smaller scales, as exemplified in Stieg Larsson trilogy "Millennium"'s character Lisbeth Salander able of targeting individuals, hide inside their computers and exfiltrate their deepest secrets.

4.6 Conclusion

In the governmental perspective, the main concern is protecting national security, involving protecting critical infrastructure, avoiding foreign intelligence operations and protecting economic interests. Networked computer systems enable for great efficiency boost, gives force multiplication effects, but at the cost of dependency on the technology. We realize manual backups are no longer a viable option if current efficiency is to be expected. We also see governments being less secretive and starting to share information with commercial organizations in order to fight the threat together, both internally and externally. It is a need for better assessment of SCADA system vulnerabilities, better control in IT supply chains, and a need to shift focus to protecting compromise of systems from the inside. Security in depth in other words. Air-gapping is an understood means of dealing with the problem, but it is difficult in practice.

Many countries increase military budgets for a 5th domain of warfare with both offensive and defensive goals, and having huge resources available for developing and administering advanced persistent attacks potentially at a much larger scale than organized crime. We start to see Computer Emergency Response Centers (CERT's) taking responsibility for organizing situational awareness on the matter, and databases are being built in order to track the threat groups.

Rules in cyberspace are somewhat unclear, as to whether digital counterattacks are allowed and how escalation from cyberwar to traditional kinetic warfare is deal with. The Tallin manual answer these questions by applying existing international laws. APT is a part of cyberwar, but cyberwar also includes attacks on cyberdomain using physical means such as jamming and EMP, and great damage can be caused to a society over time even without explicit deaths and material damage.

We have also looked at APT as the Fabian strategy attacking without direct confrontation, discussed the importance of discovering such attacks without it being given away, this allowing for deception operations. This in contrast to traditional blocking and restore thinking "pulling the plug". Attribution is possible by looking for human patterns like flaws and inconsistencies, and in methods and correlation of tools across incidents. Lastly, even if your network is compromised, you still need to consider the operational consequences regarding the potential loss by keeping it running versus the potential loss of not having it available.

At a commercial / organizational level, main focus is on profitability, and protective measures must pay off. We see commercial organizations being targeted because they are less protected, they can be targeted as an intermediate steps and also directly targeted because of their position as a supplier or partner with trust inside a more valuable network for the APT. A high pressure of attacks from organized crime and hacktivism hides APT types of attacks in the noise, and because of the protection resource gap between small / medium sized commercial organizations compared to governments, European Union suggested building a hierarchy of national and sector based Computer Emergency Response Teams (CERT) and also a transnational Information Security Agency in their cyber security report. Forensic readiness is another method developed for easing collaboration between organizations and Police during investigations. We see actors not associated with APT adopting APT techniques and methodology for opportunistic (economic) gain, and it calls for a need to separate between APT methodology versus the goals and intentions of threat agents.

At an individual level it's important to remember an APT is a relative term. Even a single person can be both advanced, persistent and targeted against less sophisticated targets. The social aspects of APT methodology targets individuals, often based on their role in an organization, and represent a weak link in protecting against APT. It's also seen that methods used in APT is now being used by law enforcement for wiretapping purposes without necessary controls in place to avoid misuse.

5. PROTECTING AGAINST APT ATTACKS

By Pieter Bloemerus Ruthven

5.1 Abstract

As mentioned during the introduction of this paper, the elements that make up APT attacks are not new. What does set it apart is its highly targeted nature and defined objectives. If an organization has been targeted, the attack is not likely to stop before the attacker has met a clear objective.

This targeted characteristic of APT attacks is a key concept to keep in mind when securing a network. Organizations have to take into account that they could be a target. Due to their economic footprint, type of business or profile, an organization might think that they would not be an attractive target. However, they might be targeted as part of a bigger attack, with the end objective being located at another organization. [19] The point is that it is no longer sufficient to protect only against opportunistic attacks, an organization must also protect against highly targeted attacks.

The traditional view on securing a network focuses on enforcing strong perimeter security. The internal network is considered to be trusted. However, this is no longer the case, even organization's own employees are doing more and more nefarious things on the network (the insider threat). Also, attackers assume the identities of users on your own network to avoid detection. The rise of the insider threat is proving the traditional view to be insufficient, and APT is another good reason for shifting more focus to security on the inside.

All of this necessitates a new way of thinking about securing a network. What is important to realize is that protecting against APT does not involve a single solution. In reality, it might not even be anything but enforcing good security practices. The key difference is the mindset taken when considering security controls. Protecting against APT calls for more emphasis on securing different elements of a network than would have been previously considered. It is important for an organization to assess what assets on its network could be targeted, and aligning security efforts around this - securing from the outside as well as from the inside.

Unfortunately, in a lot of cases, organizations' basic level of security is not mature enough. Thus, starting with establishing a basic level of security has to be the first step. However, by considering APT as a real risk, organizations can save money by budgeting for spend in areas where it would have the most impact. The core elements of the generic APT attack pattern, discussed in Chapter 2.5, such as spear phishing, privilege escalation and data exfiltration should be high on the list of priorities.

Security mechanisms can either be technological or organizational (human aspects). APT attacks necessitates an increase of focus in both areas. Individual security components can be viewed differently in light of being a potential target of an APT attack. More effort should be invested in certain areas.

On the technological front this could include protecting important data assets by understanding what data is sensitive, and how it is leaving the organization. Limiting administrator and normal user privileges, and monitoring their behavior to minimize the risk of a compromised account. Allowing only a set of trusted applications (white-listing), instead of relying on known "bad" signatures to keep malicious software at bay. This relates, respectively, to data exfiltration, privilege escalation, and zero-day elements of APT attacks.

On the organizational front this could include user awareness training as a very important aspect, considering how prevalent spear phising is as part of an APT attack. Upper management should also be made fully aware of the reality of APT attacks in order to ensure security management is enabled to address the problem.

It is clear that a combination of different security components are required to provide better protection against APT attacks.

In additional to each individual organization's efforts, the need for better collaboration between organizations and governments on an international level could be argued. A central database containing knowledge of past APT attacks, such as attack patterns and attack group methods could be used to derive better solutions to the APT problem.

5.2 Introduction

This chapter will look at what protection mechanisms can be used to defend against APT. The difference between traditional attack mitigation strategies and APT will be discussed as well as a paradigm shift from traditional security methods that are required.

As mentioned, most attack elements of APT are not new, and thus most individual elements can be protected against by traditional security controls. However, the combination of tailored attack elements with highly focused targets combined with the determination of the APT attacker requires a new way of thinking.

5.3 Does APT concern me - am I a target?

APT attacks have very specific targets, in line with the end objective of the attackers.

Any organization could be a potential target for an APT attack, it is not limited to large organizations and governmental agencies. An attack on a small organization could be part of a bigger planned operation. An example could be affecting the output of a number of smaller suppliers with the motive of disrupting a critical service such as power production. The power plant is in this case the primary target, and other smaller organizations simply acting as a means to an end.

Other examples show how organizations could be used as stepping stones leading to the actual target, such as a third party connection enabling the attacker to gain access to his target. [19]

What makes it worse is that an organization could be in the position where an attacker has a bigger budget for performing an attack than the business has for its security defenses.

This allows for sophisticated, tailored attacks, impervious to traditional protection mechanisms. What this shows is that no matter how big or small they are, any organization could fall victim to an APT attack, which necessitates reconsidering what an organization deem to be a likely attack against them and adjusting their security posture accordingly.

5.4 Mitigations - how to protect against APT?

Protecting against APT starts with normal good security practices. There are countless security control frameworks and suggested security mitigation strategies out there, all saying more or less the same things when it comes to security. By following such leading practice security procedures an organization can already be well down the road towards preparing itself for APT attacks.

The first thing for any organization should be to ensure that it is adequately covering the basics in terms of security. However, a change in the way security is thought about is required. No longer can one only protect against the "generic" external attacker, organizations should also think about attacks specifically targeting them. The risk of the insider threat is also on the rise, which along with APT further necessitating strengthening controls in this area.

Traditional views. Focus has traditional been on perimeter security, with protection on the host level mostly limited to anti-virus solutions. This view dictated that the "bad guys" are on the outside, trying to get in through your external perimeter and that systems inside this perimeter is considered trusted. Firewalls and proxies protected the organizations from the outside world, and if something did penetrate your defenses it was likely a virus brought on by users of the systems.

Protection on desktop machines was usually taken care of with signature based anti-virus and anti-malware solutions. The use of signatures to identify an attack, is also becoming less effective. A signature is a pattern of code that has been identified as malware. Computers can be programmed to look for that malicious pattern and block it. If the pattern is not known, the attack is not blocked.

This point is supported in [50, page 6].

> "The New York Times found that only one of the 45 kinds of malware used in a recent attack on its networks was detected by its antivirus program. Attackers have also become more sophisticated in evading signature-based controls, often testing their malware on antivirus programs before deployment to see if they can be detected. Advanced attacks can bypass signature-based defenses."

In addition to protecting against potential breaches from the outside, security departments traditionally direct large efforts to maintain uptime for business operations. Perhaps even sometimes compromising on other aspects of security due to budget constraints.

Pressure from the business to keep operations running usually out-weighs expensive implementations of security mechanisms which are seen by executives to rarely deliver value to their organizations.

> "In the past, many organizations needed to simply have better security than other Internet-connected organizations and businesses, as many attackers would choose easier targets. However, with APTs, organizations need to be able to defend against a motivated enemy who will take the time to look for weaknesses rather than moving on to another target. [11, page 5]"

A new paradigm. [4, page 1], describes the limitations of the traditional view well.

> "The rise of APTs has demonstrated the limitations of network centric perimeter security as we've practiced it for more than 20 years. With APTs, all networks are untrusted and the security perimeter has become user-centric. The user is the attackers' new focus; spear-phishing emails and malicious software on USB devices have become attackers' favorite weapons. The software powering IT infrastructures and running business processes is now the line separating a compromised user from the information the attackers seek. If exploited, it helps the attack propagate itself within the organization. In a user-centric perimeter, the software has become the new firewall and therefore must become an active element to defend organizations against APTs."

Further support for a new view on security is mentioned in [11, page 5].

> "The most critical difference between APTs and normal threats is that an organization is specifically targeted. While defending "the perimeter" and using standard security controls may protect an organization from more traditional attack attempts, these techniques may not be sufficient when facing APTs. Patient attackers can wait for new vulnerabilities to open up a weakness or can combine seemingly small vulnerabilities into a large-scale and damaging attack."

This targeted nature of APT attacks require that more focus be placed on implementing security measures uniquely tailored to the organization. Security implementations should move from general, catch all blanketed security, to targeted protection on multiple levels of the IT system.

With the inconspicuous nature of APT it is clear that the biggest threat is currently coming from within the organization's own network and security mechanisms must be adapted to take this into account.

5.5 Technological

Technological means of protecting against APT do not differ vastly from protecting against any potential breach by an attacker. It has more to do with designing security architecture in a slightly different way and aligning security measures to APT attack patterns. It could also include adding more protection to areas previously overlooked or not considered.

[50] shows a good example of how the experience of weak cybersecurity has had one advantage -

> "in simple terms, there have been so many attacks that defenders have (if they choose to use it) a very full data set on what kind of attacks have worked. Data, measurement, and analysis of actual events and successful cyber attacks can now guide proactive security strategies."

[50] alludes to the case that most organizations are not addressing basic security concerns.

> "Independently, Australia's Defence Signals Directorate (DSD), an intelligence agency responsible for cybersecurity, and the U.S. National Security Agency (NSA), began to count which attacks were most effective and most frequent. They then analysed why the most frequent attacks succeeded. Like the other surveys, they found that most successful attacks exploited fundamental vulnerabilities."

Four strategies are described, which according to analysis performed by DSD, prevents the majority of cyber intrusions.

- Application whitelisting
- Patch common applications
- Patching operating system vulnerabilities
- Minimizing the number of users with administrative privileges

> "Implementing the top four strategies can be achieved gradually, starting with the employees most likely to be targeted by intrusions and eventually extending them to all users. The DSD strategy lays the foundation for security upon which companies can build additional defensive structures tailored to other business needs and the risks to information that they face. Both DSD and NSA found that mitigating these vulnerabilities led to dramatic reductions in attacker success." [50]

These items, and a few more, will be looked at in the following section. To provide some structure to the this section, protection mechanisms will arranged according to the following categories:

- Data
- Network systems (Servers, supporting devices such as network infrastructure)
- Software
- Endpoints

5.5.1 Data

Data is arguably the most important asset of any organization. It can also prove to be the most challenging to secure. Data is scattered across all areas of information systems in a company. Data can be structured or unstructured.

Structured data is located in databases that can more easily be managed and controlled. Whereas unstructured data are those small fragments spread out across the entire organization, such as spreadsheets. This is where the biggest challenge lies. Unstructured data can be highly sensitive, and without knowing exactly where it is located, it is difficult to protect.

As previously mentioned, one of APT attacks' primary objective is the exfiltration of sensitive information over an extended period of time. This makes it even more critical to identify and protect all important data assets. Technologies such as Data Leakage Prevention (DLP) can assist with such endeavors.

> "Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance." [75, Control 17]

[91, Page 6] mentions that

> "although target organizations may not know exactly what an individual APT looks like, most organizations can manage to identify their own sensitive data. Therefore, DLP solutions can be applied as a layer of defense to identify sensitive data and prevent outbound transfers of that data. It can also assist with identifying the use of proprietary encryption on outbound web traffic which is also important to an APT defense."

In order to best protect against APT attacks, all important data should be identified and ranked in order of sensitivity. A structured way should be chosen to classify and store data.

It is however not just business data in the traditional sense that an organization should protect. In addition, meta-data

that could give the attacker information about the layout of infrastructure, internal business activities and movement of people, amongst others, should be guarded. Analysis of such information by the attacker could be leveraged to perform more targeted attacks, leading to greater success of compromise. Such aspects are more closely related with how systems are configured, and what information can be enumerated from them. The following sections will look at this.

5.5.2 Network systems

Administrative privileges. The number of users with administrative privileges should be limited. In additional, the level of administrator access should be restricted based on the administrator's role in the organization. Administrator accounts should not have full access to all systems, access should be segregated across different systems to limit the risk in case of compromise. As found in the surveys DSD and NSA performed [50]

> "easy access to administrative privileges lets criminals who obtain them (and this is a frequent initial goal for most hackers) to install malicious software and change settings to make it easier to exfiltrate data and to hide their criminal activities."

This will be elaborated upon further in this section.

Outbound traffic. One important change in network security is the view on analyzing outbound data vs. mostly being concerned with inbound traffic.

> "Networks with firewalls, IDS/IPS, and antivirus defenses focus on inbound threat protection using signatures and individual defense analytics, and mostly ignore outbound communications. Behavioral context analysis and threat scoring from multiple defense analytics is missing, as is outbound traffic analysis for data theft as noted above. Traditional defenses such as firewall and antivirus are necessary because they block known threat vectors; however, they are not sufficient and their limitations against APT techniques, such as the use of zero day exploits, and targeted attacks must be recognized and fixed." [91, Page 6]

System hardening. As part of common best practice principles, systems should be hardened to protect against possible attacks. This includes keeping systems up to date, configuring systems with as few services as required and not having any unnecessary software installed that could introduce vulnerabilities into the system. Access restrictions are also put in place to protect against unauthorized access and modification.

As mentioned earlier in this section, APT attacks frequently make use of zero-day exploits to gain access to systems that would be considered to be secure.

Privilege escalation. As previously described in this section, APT typically involves an attacker gaining privilege escalation on a system within the organization's network. With the proper level of escalated privileges it could be quite trivial for an attacker to gain access to other systems on a network. Administrator accounts are the usual target, as this would allow the attacker to easily move laterally through the network. Thus it makes sense to protect such privileged accounts against misuse.

There are various technologies out there that make the task of management of privileged accounts easier. Typical features include monitoring usage of accounts and additional security mechanisms as part of the authentication process. For example, enforcing strict password control mechanisms by having administrators check out a single use password that is changed with each session. This is especially useful in organizations with legacy systems where there are only a single administrator account shared amongst a team of users. This also helps with accountability and tracking down the source of a possible attack. Recording of administrator sessions is also used to monitor for strange behavior and can be used as part of a forensic investigation.

By keeping a close guard on these accounts, it can be more difficult for the attacker to realize his objective, or at the very least have him trip over an alarm.

Role management. As part of privileged account management, it is also important to follow the rule of least privilege when assigning user access to information resources. User accounts should be restricted, so that if compromised the impact is reduced.

Administration tools. In most cases attackers under APT utilize and misuse common system administration tools to avoid detection and attribution. Developing unique exploits could potentially be easier to trace back to the perpetrator, and in many cases are not even needed due to easily exploitable systems. Renaming of common administration tools can be a technique used to discover potential attackers posing as legitimate users on a system. The use of standard named commands could trigger an alert, indicating unexpected behavior. [19]

External monitoring. Monitoring of systems with third party solutions could help circumvent attempts at hiding evidence on compromised machines. Once a machine has been compromised it can be a trivial task for an attacker to modify access logs in order to remove traces of his activity. If an attacker has compromised a system, that system is no longer trusted, the built in monitoring systems' integrity has been lost. An example could be using a dedicated external log server that is configured to only accept log entries. No other services should be running on this server, and it should discard all other requests.

This does of course not mean that the external monitoring systems can not be compromised themselves. However, due to their limited function they can be restricted to a higher

level which reduces the risk.

Honeypots. The use of externally facing honeypots for studying and analysing malware and attacks are widely used. Honeypots can also be used internally on a network, in the form of a honeynet, configured to act as decoys. The honeypots can be made attractive to would-be attackers, exposing vulnerable services or storing seemingly sensitive information. Their compromise could lead to early detection of an attack.

Malware. Malware under APT also creates more challenges. Attackers use malware to keep a foothold in an organization by staying dormant, and only taking action in a covert manner when called upon. The attacker has a key objective of going unnoticed for the maximum period of time, thus he is less likely to have risky behavior and set off alarm bells. Though this is not new in itself, with backdoor exploits reaching far back, it is a much more common and widely used attack vector. Notice should be taken of those seemingly benign signs of anomalies on the system.

> "Since most APTs use custom-developed code and/or target zeroday vulnerabilities, no single IPS or antivirus signature is likely to positively identify the threat. Without definitive attack signatures, reliance must be placed on less definitive indicators. Although a single suspicious indicator is not enough to identify an attack, if we evaluate each suspicious indicator in the context of other indicators, we can amass enough evidence to reliably identify malicious activity." [91, Page 6]

Obscurity. It has to be considered that since APT will be a highly focused attack, recon missions might have already revealed a lot about your network. Any protection mechanism relying on secrecy of design and implementation could be disadvantaged by such knowledge. Systems should thus be secured in a way that takes this into account - the attacker quite likely knows your network layout, maybe even has inside information via a successful social networking attack.

5.5.3 Software

Application whitelisting. This can be used to only allow known trusted applications to be executed within the environment. Instead of trying to block malicious software that might not be known yet, only approved applications are allowed to run. This can be applied on the server level as well as on the endpoint level. [50]

Patch common applications. Applications such as PDF readers, Microsoft Office, Java, Flash player and web browsers. Many organizations do not apply application patches, perhaps the administration overhead is considered too high, the in-house developed legacy applications are not compatible. Most only apply to server software, and even this is seldom done in a timely manner due to the risk of impacting a core business function. Application patching should be applied as soon as possible to lower the risk of attackers exploiting vulnerabilities. [50]

Patching operating system vulnerabilities. For the same reasons as listed above, operating system vulnerabilities should be applied as soon as they have been release and have been tested in the organization's environment. Operating system and operating system patching can together be handled as part of patch management strategy. [50]

Attack aware. In [4] the need for "attack aware software" is motivated. Applications should not rely solely on protection further down the IT stack, for example at firewall or IDS/IPS level. The likelihood of the lower level system completely understanding the context of an action taken within an application is less likely. Also, this gives the opportunity to identify warning signs much earlier while the threat is still lower, than waiting for the problem to escalate high enough for something lower down in the stack to identify it.

> "In a world with APTs, early detection is critical in stopping attacks. Defensive software development techniques alone won't be sufficient. We need to innovate and develop new techniques to build "attackaware products" that facilitate early detection of advanced threats.
>
> If secure software can detect and stop malicious strings, it can and should also log and report incidents that are being prevented. This will provide the intelligence that security products need to better monitor activity and ensure quick attention, which can lead to prevention of data breaches.
>
> Software security must become ubiquitous, designed into modern software components, and accessible to any software developer."

[4]

Full Disclosure. System patching has been mentioned, and another important aspect of this availability of patches from vendors. As soon as vulnerabilities are found, vendors should release a patch or mitigation for the problem. Organizations can choose to put pressure on vendors to provide full disclosure of new vulnerabilities and provide fixes quickly. However, this could be seen as a double edged sword, if vulnerabilities are made public organizations without a proper patch management strategy in place might have additional risk exposure. This is another good reason to always keep software up to date.

5.5.4 Endpoints

Virtualisation. or sandboxing techniques can be used to try and contain untrusted programs. Highly sensitive areas of the network could utilise virtual machines in order to execute untrusted executables. As well as opening file formats known for vulnerabilities, such as Adobe PDF. Limit the use of software that is known for common vulnerabilities, such as Adobe PDF, or open such file formats in a sandboxed environment.

Mobile users. Users traveling should be dissuaded of taking a large amount of data with them. One idea is to issue clean laptops to traveling users and only have them take the required data with them. This will lower the risk of compromise should a laptop fall into the wrong hands while traveling or operating the laptop on potentially unsafe networks outside of the organization's control. [19]

Closely related to the previous point, VPN access should be limited to isolated portions of the network based on the users' role and requirements.

5.6 Correlation

To tie all the different aspect mentioned thus far together, a system that correlates all the information generated from security systems is required. Gathering of relevant information enables better protection as new attack metrics can be learned.

[50] also describes the use of continuous monitoring systems to assist with the collection of data. Continuous monitoring allows companies to observe the behavior of their networks and take rapid action to stop problems and is a critical complement to mitigation. The approach combines constant automated diagnostic monitoring of networks for anomalous behavior with mitigation strategies that address the most frequently exploited vulnerabilities. In addition to reducing costs associated with manual verification, continuous monitoring will highlight security deficiencies before they can be exploited and more rapidly identify ongoing threats to the environment so they can be stopped before achieving their goals. [50]

These systems are very closely related with detection methods which will be described in the following section on detection techniques. Detection leads to better protection in the future.

5.7 Organizational

It has already been noted that APT attacks frequently use non-technical means such social engineering and phising to target high profile end users directly. In order to protect against this, organizational aspects should also be considered. Also, certain actions can not be restricted, but has to be performed within proper constraints. Security management should provide proper procedures and policies in order to minimize the risk.

This section will look at some organizational management aspects to consider when thinking about protecting against APT.

Structure. As is stated in most IT governance frameworks, security should have adequate role within an organization and have proper authority to take the necessary actions to protect against compromise. This is especially true in the case of APT. Firstly, security should get adequate consideration from top management. Security managers should have power to, within defined procedure, take the necessary action to protect against all possible threats the organization might face.

Risk assessment. The first step for designing most security architectures should involve a risk assessment step. During this step APT specific assessments can be held in order to identify would-be attacker profiles, and attack scenarios. This could be used in order to develop a mitigations.

DLP. DLP solutions was mentioned in the technological section. However, there are also very important organizational aspects to this solution that has to be implemented. The most important is going through a process to create a classification system for data. All existing and new data should then be classified accordingly. Security policies should clearly state how data should be labeled and where it should be stored, and any additional security controls that has to be taken.

Policies. Information security policies should be kept up to date and aligned to current trends in technology. One such trend is Bring Your Own Device, where users connect their personally owned mobile devices to a organization network. This introduces a lot of new risks, and is an attractive attack vector for a APT attacker. Since attacks target individuals, and personal device security is not always at the same level of the organization, malware can be transfered from the private domain to the organization. This is especially a concern in high secure areas where the risk of breaching an air gapped network exists.

Security Awareness. Training should be provided to all users to educate them against potential spear phishing attempts. Users should also be made aware of common attack vectors, and periodically tested as part of an ongoing learning effort. Users should be given insight into how attackers think about fooling them and this could be demonstrated by historic examples.

The system design is only as strong as its weakest link. Due to the dynamic interaction between end users and information systems it is very important to ensure that users are made aware of potential pitfalls. Technological means should be used to support users and help them maintain a good level of security. It might not be realistic to think that training users will turn every single user into a security expert. However, continuous training should re-enforce what users learn and at least have them think twice if they do come across something strange and report it to the IT department for further investigation.

Sharing. In the event of an APT incident occurring, relevant information about the attack should be shared with other organizations that might also be at risk. This could be through membership to an incident response cooperation network. This could provide organizations with an early warning system.

Return on investment. Information security is usually seen as a grudge purchase, much like insurance. However, the potential loss of not spending money on adequate protection is something to consider. In the case of APT attacks and the loss of sensitive information it could include reputation damage that is hard to quantify.

The cybersecurity problem is often presented as the result of a lack of resources. Yet every year, increasing amounts of money are devoted to cybersecurity. The research in [50, page 6] suggests that the real problem is that cybersecurity resources, adequate or not, are often spent on ineffective activities. Another major problem in cybersecurity is the tendency of corporate leadership to treat it as an "IT problem" best left to chief information officers and technicians. This may have been the right course of action a decade ago, but it is now badly outdated. A better way for top management to think about cybersecurity is that it is the source of a damaging "material effect," hurting a company's profits, value, and financial future, that will be increasingly difficult to ignore. [50, page 6]

The example in [50, page 6] showed surprising results for the cost of cybersecurity.

> "Implementation of whitelisting, and the other four techniques mentioned as part of the DSD analysis, significantly reduced incident response costs. Rough estimates suggest that the savings from reduced incident response tasks and reduced "repair" costs for system and data replacement outweighed the cost of implementing and managing the security controls." [50, page 6]

Organizations that implement better overall security stand to gain more trust from consumers and partners which could result in a competitive advantage.

5.8 Conclusion

It is clear is that there is no single solution that can protect against APT. What is important is that an organization first try to achieve a basic level of security by following good practice guidelines. There are still elementary security principles, such as system patching, that are not being followed in a lot of organizations. In addition, more emphasis should be placed on areas that relate closely to APT attack patterns.

Current APT threat models necessitates protection against breaches through spear phishing and social engineering, compromise for persistence such as privilege escalation and the exfiltration of data. One of the most important aspects to take note of is that of the internal threat. APT attackers hide behind the identities of known users on the organization's own network. This means that users on a system can not be explicitly trusted according to who owns the account. User rights have to be sufficiently locked down to minimize the impact in case of compromise.

Threat models are constantly evolving. This necessitates maintaining a database of new attack vectors through a continuous process. Such a database allows for the identification of new metrics and could assist with strengthening protection mechanisms. Due to highly motivated attackers with big budgets, it may be difficult for all organizations to protect themselves adequately. Collaboration with other organizations can help to address this problem. However, this also raises the question whether governments have to take a more active role in defending against APT.

There are different levels of security that can be utilized. It is important to remember that each organization is unique, and not all solutions might be considered feasible. Organizations with high security requirements will naturally choose more secure solutions, regardless of APT risks. This might include using completely isolated systems or operating in an offline mode when working with highly sensitive or critical resources. This is especially true when considering governmental aspects such as military and critical infrastructure, as detailed in Chapter 4.

However, for a more generally feasible approach the real answer has to be that a more focused combination of existing security components are required to provide better protection against APT attacks. In addition, the view organizations take on security has to change. All organizations have to consider the risk of an APT attack as a reality. This requires a re-evaluation of what security means to an organization and whether their stance adequately takes into account that they could fall victim to a highly targeted attack such as APT.

6. DETECTION OF APT ATTACKS

By Dmytro Piatkivskyi

6.1 Abstract

The importance of attack detection has been growing for the last years. Many specialist has acknowledged the fact that the role of detection was underestimated at the beginning of the IT-security era. When it comes to APT the significance of detection rises a lot. Many breaches of authoritative companies were reported by by some other company. It proves that many successful attack campaigns go undetected for a long time. Assuming that the most important thing is to detect the breach as early as possible and recover the compromised system. This section is about APT detection techniques and the remediation methods.

There are three approaches to APT detection distinguished: network traffic analysis, change controlling and sandboxing. They are used as a basis for building a complex analytic engine which implements big data analysis. It is important to correlate information provided from different sources, since APT is usually not aimed at one machine, but at whole organization. While it is necessary to prevent a system from being compromised by known attacks and malware, the real challenge is to detect unknown malware which exploit zero-day vulnerabilities. Change controlling detects better unseen before malware, while network traffic analysis is more robust against known types of malware and its small variations.

APT detection differs from conventional detection techniques in the way a system is viewed. APT detection has a global view on processes and considers every event as a part of a complex attack. But, in fact, none of the mentioned APT detection techniques are new. Thus, APT detection uses conventional detection techniques.

For the last few years many APT detection solutions were designed. Since there is no data available to compare them, only the description of them is given in this section. White papers is the only source available. Since they are all commercially oriented, no demerits are stated and the solutions are claimed to be very efficient. Three solutions were discussed in details: Triumfant, Deep Discovery and Seculert. Triumfant implements change controlling approach, while Deep Discovery is based on network traffic analysis. Thus, Triumfant will more likely detect new types of unknown before attack, while Deep Discovery will surely detect know malware. Seculert‘s solution does big data analysis performed on logs gathered from customers. This is cloud-based solution and it unites all organizations under one goal - fighting against maliciousness.

The important piece of knowledge introduced in the paper ”Assessing Outbound Traffic to Uncover Advanced Persistent Threat” [38]. It is described there how to detect APT using open source tools such as OSSEC, Snort, Splunk, Sguil, and Squert. The authors claim that the proper combination and wise management make it possible to detect an APT behavior at its early stages.

Detection is naturally followed by reacting. Two questions that have no certain answers about remediation are when and how to recover the compromised system. In order to gather more information about malware and attacker the remediation might be postponed. This is the ”when” question. The ”how” question is whether re-imaging is is a proper way of reacting. Meanwhile it guarantees full recovery but it requires a lot of resources.

A search of scientific works on APT detection was made and no relevant papers were found. Only few works says ”APT detection” in the header but the presented formulation substantially differs from ours. Thus, these works are not considered in details.

A detection itself is an investigation and it requires forensic readiness. As an inherent part of forensic preparedness of any system, detailed logging must be enable. In addition to logging of events in a system, logging of network traffic can be used. The methods of assuring forensic preparedness differ one from another and mostly depend on the approach used for detecting advanced malware.

APT detection is a complex and difficult task. It requires a lot of resources. It is important to unite efforts and share you own findings. From my perspective, the possible solution is either maintaining one malware signature database or correlation of events on the global basis.

6.2 Introduction

Answers to security questions are always uncertain. ”Is your system secure?” you might ask a security officer. ”Well, we did everything what was possible” or ”We did what we had money for” might be the answers. There is no way to say that a system is fully protected. Assuming that a system is compromised it is desirable to detect the breach as well as elements of the attack in your system. When it comes to sophisticated and long term attacks the APT detection is of focus.

As it is said in earlier chapters APT is a buzzword, and it is nothing new, but complex and targeted attacks. Of course, adversaries can use zero-day vulnerabilities, but they were using it in the past as well, before APT was coined as a term. Most researches say that majority of organizations have already been compromised and this fact either not acknowledged or not discovered. Thus, it is reasonable to assume that your organization is compromised. But this is not reason for panic. The best thing to do is to discover it and recover your IT-system. Ideally, discovering and remediation is continuous process acknowledging the fact that APT are long term attacks.

APT is a huge problem nowadays and, of course, first thing people intend to do is to have benefits of it. First of all, hackers are getting paid on a permanent basis now for doing nasty things. But also, APT is a good word to scare people and say ”you will not be protected until you buy our product solution against APT”. Many APT detecting solutions were developed during the last years and describing these solutions is the goal of this part of the paper.

Why it is so important to have detection system if we are fully protected and there is nothing to detect? Well, nobody

can say that the IT-system is fully protected. Moreover, according to Seculert white paper:

> " Art Coviello, executive chairman of RSA, says: "Roughly 70% to 80% of the budget is spent on prevention; only 15% to 20% on the detection; and, inexplicably, only 5% to 10% on response." According to Coviello, organizations often make the error of directing too large a percentage of their budget towards prevention rather than detection. Instead of investing in suboptimal prevention tactics, the smarter investment is to invest in a bullet-proof detection strategy."" [78]

For clarity sake it has to be mentioned that protection prevents an attack being successful. Meanwhile detection assumes that protection has failed and the system is compromised. There is no doubts, protection system is of highest importance, but might let you down. And when protection system fails detection system is aimed to react and discover the attack as soon as possible. When the attack is detected the targeted system must be recovered. Very often this is challenging because it is almost impossible to detected every single detail of an attack. Having some elements of an attack left in the system after cleanup, it is much more easy to start new attack campaign.

The main sources for this section are white papers of information security companies on their products which are designed to detect APT. It is worth noting that there is very few scientific works around APT, probably because APT as a term is an advertisement trick not followed by scientific society.

The rest of the section is organized as follows. First, possible detection techniques are described in the subsection 6.3, after that how it differs from conventional detection techniques is shown in the subsection 6.4. The biggest part of the section is description of commercial solutions in the subsection 6.5. Also detecting with open source tools is described in the subsection 6.6. Subsection 6.7 introduces remediation techniques and discusses its pros and cons. In the subsection 6.8 scientific works are discussed. After all, conclusions are given.

6.3 Detection techniques

It is not that difficult to detect known attacks, but it is much more difficult to detect zero-day attacks. Some heuristic approaches must be designed to detect 0-day attacks and advanced malware. This section described such approaches and states its merit and demerits.

The main global approaches are traffic analysis, change controlling and sandboxing. Usually commercial solutions implement few of these approaches.

Traffic analysis is the oldest approach. The most popular methods is rule-based or signature-based approach. Having discovered an attack, the analysts are trying to define distinguishing characteristics of it. Having defined such characteristic either firewall to protect or IDS to detect this attack can be configured. In the works [38] and [90] the rules for some specific malwares are described. Rules are applicable at different levels of networking. One can analyze HTTP requests or TCP flags or layer 2 information of IP/TCP stack. A very good method used for detecting APT is analyzing outbound traffic looking for indicators of data exfiltration. In this case, it does not matter how the machine was infected (even if using 0-day vulnerabilities) the attack can be detected. While rule-based approach cannot detect attacks which exploit zero-day vulnerabilities, it deals well with known attacks and, which is more important, can be a good base for statistical and correlation engines. This is another method within traffic analysis approach and it is quite promising. Correlation is very appropriate since APT usually attacks multiple machines and correlation of the events from multiple machine gives a global view. The traffic analysis approach itself has a significant drawback due to incapability to analyze encrypted traffic and the cloud.

> " The use of SSL encryption evades detection based on patterns in URL parameters and HTTP headers. The use of legitimate services in the cloud, meanwhile, evades attempts to simply block access to known “bad” locations. Together, these two factors make detecting APT activity challenging.” [90]

The second global approach to be discussed here is change controlling. The main idea is simple and straightforward - check every changes to sensitive objects on your machine. If the change is legitimate do nothing, otherwise either alert an administrator or launch an automatic recovery mechanism. The main advantage of the approach is that it can possibly detect new types of unknown before attacks. No prior knowledge is required. It can be fully automatic and transparent for the end-user. The problem is that such integrity checking (change control) can not be continuous and malware can do its work between two consequent checks and change the state of machine before checking to legitimate. Although it seems difficult. Another demerit is that it does not control memory, thus additional forensics tools for memory analysis must be deployed. Apart from all, the number of attributes to check is usually quite big (hundreds of thousands) which results in huge performance slowdown.

Sandoxing is basically the way of fighting with malicious executable files. It is implemented mostly in cloud-oriented solutions. Before actual executing the file is executed or opened (if it is non-PE file such as jpg, doc, pdf, etc) in isolated environment - a sandbox. The effect of its execution is examined and decision of whether it is the legitimate effect or not is made. It provides robust malware profiling, but such a process is hard to make automatic, meanwhile the manual work is expensive.

6.4 Difference from conventional detection techniques

A reasonable question to ask would be "How described methods differs from already existing ones"? Indeed, all three methods are not new. The key insight is how you treat things. While implementing APT detection solutions every alert, every change is considered to be a part of one complex

attack, not isolated event. That means that APT detection tools include conventional detection tools and in addition they analyze all events in order to get a global picture of what is happening.

Another feature that makes the difference is that APT detection is complex. It uses few or all of above described approaches. It also slightly modifies the detection in order to adjust to APT detection.

The solutions are not panacea, they are just additional protection methods which have a broader global view on the system.

6.5 Solutions

Recently plenty of APT detection solutions were introduced in security market. They use different approaches and it is almost impossible to compare them in the light of effectiveness. Thus, in this section these solutions are just described and my personal comments are given.

It is worth saying that white papers on commercial products state no demerits of their products and say that described solutions are the answers to all problems and you will be safe having bought it. Obviously, there is no such 100% effective solution and either false positives or false negatives are present in the system. It is stated in majority of papers that solutions do not have false positives. That makes me wonder about false negatives rate and where the threshold must be placed. The reason why developers might have eliminated false positives is that APT detection systems usually include automatic remediation subsystem. Of course, false remediation might be worse than undetected attacks, but the another question is if the including automatic remediation is worth it. In my opinion, the function of detection system is to detect and this systems must perform well doing it.

6.5.1 *Triumfant*

> " At the heart of the Triumfant approach is the concept of change detection and analysis; continuously monitoring host machines for change and then analyzing those changes for malicious activity. The basic premise behind the use of change detection to identify malicious attacks is simple and fundamentally sound: malware will change a machine as a function of the attack and Triumfant will detect and characterize those changes and therefore detect the attack. A solution that detects changes and then accurately analyzes those changes is able to identify malicious activity without the need for prior knowledge. Using change detection enables Triumfant to see the constantly evolving attacks that evade traditional protections, effectively closing the gaps left by firewalls, IPS, and antivirus solutions. This includes zero day attacks, rootkits, and the Advanced Persistent Threat (APT), as well as the work of malicious insiders."[87]

Even though it is claimed in the whitepaper [87] that the solution is complex network-based, but it seems that the server usually works in isolation with a single host using only very few network-oriented facilities (such as software comparison across multiple machines). The following is how the detection works.

> " The best method for detailing how Triumfant detects and remediates malicious activity is to break down the process into the Collect, Analyze and Act cycle."[87]

The Collect phase just assembles all changes for further analysis in the Analyze phase. The Act phase is basically remediation and is discussed in Section 6.7. The are two types of checking - real-time and daily scan. The "real-time" detection is not truly real-time. The checking script is launched every n seconds which is configurable parameter. Setting n value is a trade-off between performance slowdown and time of reaction. Also the pseudo real-time scanning differs from daily scanning in the amount of attributes to check. Having detected any changes the Triumfant does a small analysis to define whether this is anomalous change. This is not the Analyze phase, it is just part of its functions build in the Collect phase. If the change was identified as anomalous the complete scan is triggered which makes a delta snapshot of a whole host system and initiates the Analyze phase.

The purpose of daily scan is to conduct more comprehensive checking and to detect "low and slow" attacks:

> " The full scan will collect the changes associated with those attacks that do not trigger the real-time scan. It is the intent of the real-time scan is to detect the majority of malicious attacks as they occur and initiate real-time analysis. However, there are legitimate scenarios where an attack would fail to trigger the real- time scan. One such scenario is the "low and slow" attack introduced earlier in the architecture discussion of the agent. In this scenario, the attack downloads malicious content but the malicious executable remains dormant for some period before running on the machine."[87]

There is also an option to initiate a scan when it is needed, using so called on-demand scans. The on-demand scan is exactly the same as in real-time detection when the change is identified as anomalous.

The Analyze phase takes a delta snapshot as an input and reconstructs the state of the machine combining the delta snapshot with a base snapshot stored in the database.

> " Part of this analysis is the identification of anomalies and the associated anomalous attributes. For example, in the case of the addition of a new application to a machine, the analytics will check the context to determine if this application exists elsewhere in the population. If not found, the analytics classify the application as anomalous, and will then analyze the associated changes to

> look for other signs of malicious activity. If the application does exist, the analytics will compare the new install with existing installs, checking attributes such as the hash values of the executables and associated configuration settings. If the new install is consistent with the other occurrences of the application, the analytics classify it as normal; if not, they classify it as anomalous. The context of the model also helps identify configuration and policy changes made with the intent of diminishing the machine's ability to detect further malicious activity." [87]

What attributes does Triumfant check? As it is stated in the 2-pages brochure of the solution description, these are:

- Registry keys
- MD5 hash of every file
- Processes
- Services
- Event Logs
- Security settings
- Hardware attributes
- Open ports
- Performance metrics
- System calls

In total it is about 200,000 attributes. Except the comparison part, Truimfant has implemented

> " the analytic engine which does the correlation of the all changes associated with that incident. The goal is to create a complete picture of the attack and the associated collateral damage for the purposes of constructing the final analysis and a remediation." [87]

It seems that the solution itself introduces additional potential attack vectors since it operates on high-privileged level.

Once again, in commercial paper only merits are stated and they have no scientific value. Their intent is to make people believe they need it.

6.5.2 Deep Discovery

The most referenced paper on APT detection is Trend Micro incorporated Research Paper 2012 "Detecting APT activity with Network Traffic Analysis" [90]. In this paper prior to introducing the Deep Discovery solution examples of how known APT attacks can be detected based on rules. Namely GnostNet, Nitro, PoisonIvy, Tiadoor, IXESHE, Lurid and Sykipot. The main focus was on network traffic activity, specifically on C&C[19] commands:

> " While new executable files that cannot be detected without new file signatures can be routinely created with automated builders and embedded in documents designed to exploit vulnerabilities in popular office software, the traffic malware generated when communicating with a C&C server tends to remain consistent.1 This is likely due in part to the considerable amount of effort required to change a C&C protocol, including code changes in both the malware and C&C server. By increasing awareness, visibility, and information sharing, however, details of these campaigns are beginning to emerge. A significant portion of these ongoing campaigns can be consistently detected with the aid of network indicators. While detecting this kind of traffic requires prior knowledge or threat intelligence, network detection can effectively defend against known threats. Network traffic can also be correlated with other indicators in order to provide proactive detection.2 In addition, proactive detection of unknown threats can be further extended by extrapolating methods and characteristics from known threat communication behaviors to derive more generic and aggressive indicators." [90]

The argument to use rule or signature-based approach is that

> " most of the campaigns documented in highly publicized reports, including GhostNet and Nitro, and the RSA breach, employed malware with consistent indicators that can be routinely detected by analyzing the network traffic produced as they communicate with C&C servers. Moreover, activity related to other less-known but longrunning campaigns such as Taidoor, IXESHE, Enfal (aka "Lurid"), and Sykipot can also be consistently detected at the network level." [90]

Those named advanced malware keep widely affecting hosts and it is important to eliminate these major threats. The striking word here is "major", because these malware still make a big portion of APTs. As authors claimed these malware remain consistent over years even in spite of the fact they are modifiable.

One might ask "What are indicators that can help to detect an attack?". Examples are:

- "Protocol-aware detection: Many of the RATs used in targeted attacks use HTTP/HTTPS ports to communicate, often because only these ports are open at the firewall level. This means that detecting any non-HTTP traffic on port 80 or any non-HTTPS traffic on port 443 flags potentially malicious traffic for further investigation. While not conclusive, such alerts can provide direction as to where to focus investigative resources.

[19] Command and control channel, the way a malware gets commands

- HTTP headers: Many targeted campaigns use HTTP for C&C communication but send requests using application programming interface (APT) calls that can often be distinguished from typical browsing activity. Analyzing HTTP headers can be a useful generic way to detect malware communications.
- Compressed archives: Attackers have been known to use password-protected, compressed archives such as .RAR files to exfiltrate data from compromised networks. While it may generate a high level of false positives, detecting such files that leave the network is trivial.
- Timing and size: Since malware typically "beacon" to C&C servers at given intervals, monitoring consistent intervals for Domain Name System (DNS) requests or requests to the same URL will help. As more APT campaigns move from HTTP to HTTPS communications, as Sykipot did, communications may still be detected by analyzing traffic based on the "volume of transferred data, timing, or packet size." Such requests can then be further investigated." [90]

Stated in the whitepaper merits and demerits seems to be true. Thus, it is said that the Deep Discovery has false positives and false negatives which means it can fail to detect some attacks. Moreover, knowing that the organization uses this detection method gives an adversary a possibility to launch a lot of fake attacks with indicators of real attacks. This will cause a lot of false positives which in turn will make an analysis much more difficult. It is also stated that the approach used in the solution is not new. It seems that the biggest contribution is analysis of existing attacks and generating rules. This is not that impressive but it reflects real state of things in the world.

Although the main approach of Deep Discovery is quite weak, the solution itself comprises more sophisticated techniques which makes it a pretty good detection mechanism.

> " Deep Discovery uses a three-level detection scheme to perform initial detection, simulation and correlation, and, ultimately, a final cross-correlation to discover "low-and-slow" and other evasive activities discernible only over an extended period of time. Specialized detection and correlation engines provide the most accurate and up-to-date protection aided by global threat intelligence from the Trend Micro™ Smart Protection Network™ infrastructure and our dedicated threat researchers. The result is a high detection rate, low false positives, and in-depth incident reporting information designed to speed up the containment of an attack." [90]

Some insight of how and what Deep Discovery detects is given of the Fig. 12 . What is worth the particular attention here is that Deep Discovery uses sandboxing for detecting malicious content in addition to convenient signature scanning (I suppose like anti-viruses do). Also it uses blacklisting and whitelisting in addition to rule-based detection. Generally, it is nothing more than collection of the best known techniques.

On the 20th of March [85] and then again on 21th [86] of March Trend Micro posted two articles about incident in South Korea. As they reported that

> " several attacks hit various South Korean government agencies and corporations." [85]

and what is the most important

> " Trend Micro was able to protect our enterprise users in Korea against this threat." [85]

In the articles [85] and [85] they explained what has happened and how the Deep Discovery solution helped.

6.5.3 Seculert

Seculert's whitepaper states that

> " If the real question is post-infection detection, the answer is big data analytics." [78]

That is not new, since correlation described above can be considered as big data analysis. In fact, correlation is said to be one of the seculert's methods. The main innovation is the way the developers implemented big data analysis. Namely, the cloud. It gives high convenience using the service such as scalability and independence. But the main advantage is uniting all organization under one goal - detecting maliciousness. You are not fighting alone, you are fighting together.

> " In the cyber-security arena, harnessing big data analytics makes it possible to create a powerful threat detection engine that will achieve better results than any known malware prevention methods. Seculert's big data engine collects and analyzes terabytes of data collected from sources both internal and external to the organization.
>
> 1. By actually joining live botnets, Seculert allows for effective interception of live botnet traffic. The botnet traffic is compiled into a large dataset which can then enable infection detection on both internal and remote devices.
> 2. Customers can upload suspicious executables to a cloud-based elastic sandbox and allow the malware to evolve over time. The sandbox enables robust malware profiling by simulating different environments and geographical regions.

	Attack Detection	Detection Methods
Malicious content	• Document exploits • Drive-by downloads • Zero-day and known malware	• Embedded file decoding and decompression • Suspicious file sandbox simulation • Browser exploit kit detection • Malware (e.g., signature and heuristic) scanning
Suspect communications	• C&C communication for all types of malware—bots, downloaders, data stealers, worms, backdoors, RATs, and blended threats	• Destination (e.g., URL, IP address, domain, email, Internet Relay Chat [IRC], and channel) analysis via dynamic blacklisting and whitelisting • Smart Protection Network URL reputation checking • Communication fingerprinting rule use • Comparison with suspicious and known malicious SSL certificates
Attack behaviors	• Malware activity (e.g., propagation, downloading, and spamming) • Attacker activity (e.g., scanning, brute-forcing, and service exploitation) • Data exfiltration	• Rule-based heuristic analysis • Identification and analysis of the use of hundreds of protocols and applications, including HTTP-based applications • Behavior fingerprinting rule use

Figure 12: What and how Deep Discovery detects [90]

3. Seculert facilitates crowdsourcing[20] in the truest sense of the word. The system is vendor agnostic, allowing customers to upload HTTP traffic log files and share data no matter which security solutions they are using. This is a win-win: the more data available, the more malware that can be discovered.
4. As a pure cloud service, Seculert is able to digest huge amounts of data over time. Over 40,000 unique samples of unknown malware are collected and profiled by Seculert on a daily basis. Seven million new infected IP addresses are identified every day. Tens of thousands of compromised enterprises are detected worldwide. Petabytes of botnet traffic and customer logs are analyzed monthly. Over time, Seculert continues to digest huge amounts of data in order to identify persistent attacks that have gone undetected by other on-premises security solutions for days, weeks, months or even years." [78]

Seculert accumulates big amount of logs from different sources and continuously analyzes it, comparing it to the database of known malware samples. It is said that Seculert has different types of analysis, but details are not provided. The idea given in the whitepaper seems to be extremely good, but no details on how it works and numerical data for comparison is provided.

Moreover, it is stated that Seculert solution is able to partially solve the bring your own device problem. [21] It can determine the compromised devices externally.

To conclude on Seculert solution it is to be said that

> " This approach of correlating enterprise-supplied (internal) data with live botnet (external) intelligence allows Seculert to provide industry-leading forensics investigation and real-time detection of APTs, alerting users to compromised endpoints, while drastically improving threat detection rates and reducing false positives." [78]

6.6 Detection with open source tools

While I was reading all whitepapers described above I was wondering whether it is possible to fight against APT using the best open source tools as building blocks. The answer was found in the work of SANS Technology institute "Assessing Outbound Traffic to Uncover Advanced Persistent Threat" [38]. In this paper APT detecting technique using open source tools are described. As it is stated

> " Tools such as OSSEC, Snort, Splunk, Sguil, and Squert may allow early detection of APT behavior." [38]

However, it is obvious that just deployment of these tools is not enough to efficiently detect APT. Some sophisticated

[20] The practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people, and especially from an online community, rather than from traditional employees or suppliers.[95]

[21] Means the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged company information and applications. [94]

analytical engines must be developed to correlate event and alerts. The most challenging part of using open source products is maintaining your own database of patterns of advance attacks. Indeed, it is very difficult to determine a pattern for an attack which can be modified. Fighting alone you will face much more difficulties. In the paper it is recommended to analyze outbound traffic, since less variations are presented in it. Indeed, there are plenty of ways to break the system, but not so many ways to control remotely compromised machine. Also, it is much more easy to detect the undesirable leaking of information analyzing outbound traffic. The goal of the paper is to propose methodology for the detection of APT.

Authors defined four approaches or methodologies for detection of APT using network traffic analysis. These are namely:

- Rule sets
- Statistical and Correlation Methods
- Manual Approaches
- Automatic Blocking of Data Exfiltration

As building blocks the following tools were suggested which fit into the general category of network security monitoring (NSM):

- "Snort is open source network-based intrusion prevention and detection system (IDS/IPS) originally developed by Martin Roesch. Snort employs signature and protocol, as well as anomaly-based inspection.
- Scapy is a packet manipulation program. Scapy can create packets for a wide range of protocols. It can send and receive packets and match requests and replies. It is extensible via Python scripts and can be used for a variety of detective measures.
- OSSEC is a host-based open source IDS, as opposed to Snort. Its correlation and analysis engine provides log analysis, file integrity checking, Windows registry monitoring, rootkit detection, and time-based alerting as well as active response and can support most operating systems.
- Splunk is a search, monitoring and reporting tool integrating logs and other data from applications, servers and network devices. The data repository is indexed and can be queried to create graphs, reports and alerts.
- Sguil includes an intuitive GUI that provides access to realtime events, session data, and raw packet captures. Sguil facilitates the practice of network security monitoring and event driven analysis.
- Squert is a web application used to query and view event data stored in a Sguil database. Through the use of metadata, time series representations, weighted and logically grouped result sets it provides additional context to events.
- ModSecurity is a firewall for web applications." [38]

Later on in the paper methods of detection are discussed and pointed out the tools which are relevant for solving particular problem. For example, the methods related specifically to the RSA attack that fall within Rule Sets category are:

- identification of phishing campaigns (rule maintained by The Sourcefire Vulnerability Research Team)
- recognize and block malicious traffic such as that associated with PIRAT (Snort)
- monitor the Windows registry for known bad entries (OSSEC)

As was mentioned a few times in the paper,

> " the signature lacks the ability to identify completely new attacks or even significant variants of the same attack. This fact points out the importance of multiple detection methods leading to varied but related alerts that can be correlated (see Statistical and Correlation Methods)." [38]

Authors also showed another reason why it is important to have correlation methods in place by mention fast-flux. Fast-flux is basically changing an IP-address assigned to a particular domain name very often smashing normal detection of the malicious behavior. The way of generation of such traffic is given in the paper. The way to deal with it is also described.

Manual approach is proposed as a way of detecting of APT, although it seems unreasonable to me. Of course, it could be useful for forensic investigation when the alert was raised. Examples are:

- odd egress traffic initiated from the target enterprise rather than the attacker source
- DNS logs (i. e., Fast Flux)
- anomalous traffic as compared to known good netflow baselines. [38]

It is stated also that some security information and event managers (SIEM) could be useful for either manual or automatic watching hosts.

Automatic blocking of data exfiltration is nothing else but IDS configured in the way to block or alerting of the characteristics of outgoing traffic. Of course, it uses rules or signatures and could be viewed as a part of Rule Sets category. The following is recommended to be blocked:

- detect and block RAR files
- OSSEC Active Response
- limit outbound access
- monitor for precursor attacks [38]

To conclude here it is important to say that the paper provided overview of tools that could be used within a framework to detect APT. No standalone tool can efficiently detect APT, but in combination with others where particular function is assigned to each tool, it became a powerful mechanism.

6.7 Recovery and remediation

The question of recovery is very controversial. Dealing with APT is not like with script-kiddies - you implement the detection and if something goes wrong you immediately recover the system. There is no right answer on how you should react on APT attack detection. APT is not one time occurrence, it is a war. The security officer must be clever enough to keep the network safe. Like in case of Coventry city in the WWII one might want not to show to the enemy that something is known to the protection side. Why it can be useful? Well, first of all, you can keep watching the attack in order to detect as much of its elements as possible. Of course, the most critical assets must be protected anyway, but some assets might be exposed as honeypots to an attacker. Thus, automatic remediation is not always good. Moreover, after the remediation the attacker can still use the same attack to break in the system. An alert raised must initiate the change of the protection of the system in order to be robust against the given attack.

Apart from above reasoning, another question is whether re-imaging is a proper tool for remediation. Very often full re-imaging causes great amount of inconvenience in addition to consumption significant IT staff resources and network bandwidth. On the other hand, full re-imaging guarantee total remediation if the image was made before an infection. Much more heuristic method is the one used in Triumfant. Having conducted the analysis Triumfant defines attributes that have been changed. Recovery of these attributes is enough to re-mediate the system. It is quick, automatic and does not require significant resources. But the drawback is that there is no guarantee that all the malware was fully removed, since Triumfant does not control everything in the system (for example, memory).

6.8 Scientific works on APT detection

What I found among scientific papers on APT is mostly new Chinese and Korean works which seems for me not very relevant. Examples are "CAS: A framework of online detecting advance malware families for cloud-based security" [108] and "A study on cyber threat prediction based on intrusion detection event for APT attack detection" [46]

The first paper introduces a new "on-the-fly" approach to APT detection in the cloud. It is based on signature correlation. I would say it is more antivirus then APT detection since it does not correlate multiple sources. It was tested only on known families of malware, thus real performance estimation is difficult to predict. The main goal pursued in the paper is maintaining a lightweight signature database for "on-the-fly" scanning.

In the second paper, the prediction model is introduced based on intrusion detection events. It shows a possibility of threat prediction by analyzing correlation of intrusion detection events. While this work might have a scientific significance it does not seem to be useful in practice. Moreover, it makes a prediction which might be helpful in detection of APT but it is not a detecting tool itself.

6.9 Forensic preparedness in APT detecting tools

Since detection assumes that an attack has already happened, it is very important to assure forensic preparedness. In fact, all described tools do that. Logging of events in the system is an inherent part of any detection system. Sometimes, just logging is considered to be sufficient. For example, Seculert (section 6.5.3) has nothing else in his detection logic except logs. And this is reasonable since the logging level is detailed enough to investigate any occurrence. Other systems, like Truimfant (section 6.5.1), rely more on delta snapshots which give basis for analysis and remediation. A delta snapshot is made of a whole system which allows to define what was change, but not how. Thus, some level of logging is still required.

In the network-based solutions the logging of network traffic is possible. In that case, even attempts on the network level may be investigated. The methods of assuring forensic preparedness differ one from another and mostly depend on the approach used for detecting APT.

6.10 Conclusion

In this section APT detection techniques were discussed and commercial solutions implementing these techniques were described. The APT detection differs in the way the incidents are viewed. It is global holistic view. The techniques are not new, but the way they implemented gives a chance to detect undesirable events and elements in a system. Fighting APT is a complex and difficult task and requires a lot of resources. The described solutions seems to be controversial in the sense of effectiveness. One might say they are silver bullets, another might say that it is just waste of money. Security officers have to make a difficult choice.

It is important to collaborate while fighting APT which is difficult to achieve since nobody wants to disclose or acknowledge the fact of compromising. One of the solutions, Seculert, offers a unified cloud approach for all their clients. That seems to be promising. All companies offer either solutions based on their own malware signature databases or solutions that require no prior knowledge.

There is no right or wrong choice, but the choice is to be made.

7. CONCLUSIONS

By Merete Ask (Group Coordinator)

This paper concludes that the USAF coining of APT as a term in 2006 and its subsequent definition by NIST in 2011, all though fairly new, allowed for the ability to classify APT attacks, establish proper statistics and study the phenomenon of APT in a structured manner. Thus, representing a critical success factor to collect and share basic knowledge of APT, required for different organizations understanding, to establish efficient protection against APT and handle APT attacks, should they occur. In relation to APT as a term, it may also be relevant to note, as previously outlined in this paper, that the current NIST definition is fairly broad. With the number of APT attacks are increasing, being utilized by different types of organized groups, towards quite different targets, with different missions, it is assumed that the NIST definition may be required to be supported by/expanded with subdefinitions of APT in the future, subdefinitions to differentiate different types of APT as a basis for better statistics and more in detail studies of different types of APT attacks.

The threat of becoming a victim of APT is increasing and relevant to consider for any organization. APT is targeted to complete a specific mission and can as such hardly be totally disregarded by anyone. Combined with the generic business network dependency for business operation and continuity, a security strategy focused on APT avoidance is virtually wasted in terms of time and resources. All though an organization may not consider itself a relevant target of APT attacks, the organization may just as well become a victim on other terms, e.g. practically serving as the APT attack enabler or contributor to a successful attack:

- The organization may store information, which to the organization in question may not seem particularly business critical in terms of information security protection measures, but to an APT attacker provides "the missing piece of the puzzle" allowing for the launch of a successful full scale APT attack towards its main target.
- The organization forms part of a relevant supply chain, has relevant contact, interaction or access with the APT main target, which, if compromised, provides the APT attacker with "the doorway" to successful compromise of the main APT attack target "from the inside", i.e. through a targeted trusted third party organization.
- The organization has no main target relation relevant for the APT attacker, but the network generally vulnerable and as such provides the APT attacker with a fortunate and target unrelated shielding. E.g. as a stepping stone towards the main target of the APT attack, or in the process of APT attack withdrawal. Possibly functioning as the APT attackers "conveniently available" remote control site for the attack or a "mid way storage"/dropping site utilized by the APT attackers in the process of data exfiltration from the APT attack main target.

In information security, as in general, it is recommended to "learn how to walk before one learns how to run". APT attacks, as complex and challenging as they may well be, does not distinguish itself from the traditional sophisticated attack in terms of attack phases and methods when viewed from a high level perspective. Therefore, the reported, continuous tendency of organizations to fail in basic, traditional security best practices, contributes to the increased number of successful classified APT attacks. APT does not dismiss the importance of establishing adequate security, utilizing basic, traditional security best practices (e.g. ISO27001[22]). In fact, well implemented and efficient security best practices, reduce the likelihood of a successful APT attack and its ability to stay persistently undetected over time, by reducing the number of attack vectors an APT attacker can utilize successfully. When adequate security is deemed established based on best practices, it is however recommended to review this established level of security with specific focus on the threat related to APT. The result of such a review, could lead to implementation of supplementary measures, or tweaking of implemented measures, for the specific purpose of enhanced APT protection and more efficient APT detection, should it occur. This "traditional first, APT second approach" is recommended, because the characteristics of APT and corresponding protection and detection measures, requires a slightly different approach than the basic, traditional security best practices, to become efficient.

APT is targeted and persistent, most often utilizing several different attack vectors in all stages of an operational attack. This quite opposed to the more traditional and opportunistic "hit and run" type of attacks. APT aims to gain different footholds within a targeted compromised network to stay persistent over time completing the mission. As such, elements of an APT attack in operation may be detected as incidents, but erroneously classified as the "traditional occasional or opportunistic incident" and efficiently recovered from accordingly. Thus, allowing the overall APT attack in operation to continue and remain undetected. The alternative would be to review the incident from a more global, holistic view and as such, enable for it to be identified and correctly classified as a suspected element of an APT attack in operation. Upon such a correct classification of the incident, as a suspected element of an operational APT attack, one would potentially handle it differently. Instead of immediate execution of recovery procedures and subsequent implementation to protect for re-occurrence, one could decide to closely monitor the activity for some time, with the aim to detect additional elements of the suspected APT in operation. Monitoring could be interesting with the aim to detect all gained footholds, reducing the likelihood of the APT attack's continued operation as recovery is initiated. Monitoring could also be interesting with the aim to figure out what the mission of the APT attack in operation might be, allowing for additional targeted protective actions ac-

[22]ISO27001 is here referred to as one example, often utilized by organizations as a traditional security best practice, to base their information security establishment upon. The standard includes recommendations that should ensure a balanced focus both on external network perimeters and internal threats/lateral movements of attacks if followed. Something that could reduce the tendency shown in current reports that organizations tend to have too little focus on the internal threat aspect.

cordingly. Such an approach would require the ability to constantly monitor and assess the benefit of obtaining business continuity, compared to loss of/limited business continuity introduced by execution of recovery procedures, and the likelihood that the obtained knowledge during time of monitoring is enough to execute successful APT recovery in an efficient manner.

The current rise of APT as a threat, also assumed relevant for serious consideration for years to come, will require corresponding development in relation to efficient information security countermeasures. As outlined in this paper, currently available tools do contain features that can be enabled or adjusted to provide a higher level of protection against and efficient detection of APT attacks. It does however require a review of already implemented tools for the specific purpose of APT security countermeasures, by taking a global, holistic approach to assure changes can be deemed to strengthen the established security level in a balanced way. I.e. enhancement is made for APT without having unacceptable adverse effects on the established level of security in general. As outlined in this paper, some currently available tools already claim to provide efficient APT protection and they may do, but with APT as with information security challenges in general, there is no "one solution tool" for handling APT and this paper neither assume this to be the case now or expect it to be in the future. It is however assumed that APT will be a driving force to further develop already available tools, add features and parameter settings specifically included to provide better protection and more efficient detection of APT, as one of many information security threats relevant to consider in tools development. This could for instance be features relevant to proper classification, i.e. to avoid detected elements of APT attacks in operation being erroneously classified and recovered from as "the traditional, occasional incident" and as such also provide better solutions for observing incidents from a global, more holistic view.

APT is, and expected to continue to be, one of the main driving forces, not just as a threat, but also in terms of how we approach the challenge of information security in general. As outlined in this paper, tendencies may already indicate it forcing a paradigm shift in this area, by forcing changes to the security culture in general. Traditionally, information security has been "something addressed privately" within organizations and handled without much focus on sharing. The global challenge of information security and the general network dependency for business continuity, combined with the global sophisticated and well organized threats, such as APT, force a whole other level of sharing. This level of sharing requires a change in how we approach information security in general and a change/adjustment of the security culture. This cultural change has been in motion for a while already in generic terms, but is forced utterly forward by APT. Started in 2006 with the USAF purpose of coining APT as a term, evolving through the publicly visible trends of rapid establishment of services such as CERTs and coordinating CERTs on several levels[23], supported by tools such as different types of externally administrated knowledge databases, where organizations may report and share information about issues deemed globally interesting. Initiatives to ensure that even if for instance a classified APT attack is detected in one organization, information can rapidly be processed and shared to avoid or reduce the likelihood that the same or similar APT attacks are successful somewhere else later on. The story of Stuxnet presented in section 3 of this report, outlines how the global, joint investigation and shared information, was a precondition for revealing the details of the sophisticated sabotage abilities possessed by Stuxnet. APT is a dynamic threat which requires dynamic countermeasures, depending on efficient sharing of relevant information as soon as it can be obtained. APT is a global dynamic threat which requires the corresponding global dynamic security countermeasures.

[23]CERTs and coordinating CERTs are rapidly established on several levels, i.e. continents, nations, commercial areas of operation e.g. finance and energy, in addition to governmental areas of operation e.g. health and education, to provide professional, efficient and joint security countermeasures.

8. REFERENCES

[1] Alan. Sans newsbites - volume: Xv, issue: 14 (feb 19th 2013). http://www.sans.org/newsletters/newsbites/newsbites.php?vol=15&issue=14. Visited April 21st 2013.

[2] J. S. Alexander, T. Dean, and S. Knight. Spy vs. spy: counter-intelligence methods for backtracking malicious intrusions. In *Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research*, CASCON '11, pages 1–14, Riverton, NJ, USA, 2011. IBM Corp.

[3] T. A. Andreassen. Aftenposten: Norges nye forsvarsgren (17th jul 2011). http://www.aftenposten.no/nyheter/iriks/Norges-nye-forsvarsgren-5014194.html#.UXY6b884Xiw. Visited April 2013.

[4] E. Baize. Developing secure products in the age of advanced persistent threats. *Security Privacy, IEEE*, 10(3):88–92, 2012.

[5] R. Bejtlich. What is apt and what does it want? (pub 16 jan 2010). http://taosecurity.blogspot.no/2010/01/what-is-apt-and-what-does-it-want.html. Visited 11. April 2013.

[6] W. Boyes. Video: Back to basics: Scada (pub 18 aug 2009). http://www.youtube.com/watch?NR=1&v=bfxr5DikdP0. Visited 11. April 2013.

[7] T. Bradley. Opinion: Cispa isn't the evil, privacy-infringing legislation you think it is. http://www.pcworld.com/article/2030090/opinion-cispa-isn-t-the-evil-privacy-infringing-legislation-you-think-it-is.html. Visited 17. April 2013.

[8] M. Brain. What's a uranium centrifuge? http://www.howstuffworks.com/uranium-centrifuge.htm. Visited 22. April 2013.

[9] H. Brombach. Angrepet kostet 10 dollar (apr 16th 2013). http://www.digi.no/915064/angrepet-kostet-10-dollar. Visited 17. April 2013.

[10] H. Brombach. Slo ut datasenter med kraftige mikrobølger (oct 25th, 2012). http://www.digi.no/904887/slo-ut-datasenter-med-kraftige-mikrobolger. Visited April 18th 2013.

[11] CA. advanced persistent threats: defending from the inside out. http://www.ca.com/~/media/Files/whitepapers/advanced-persistent-threats-wp.pdf. Visited April 2013.

[12] R. A. Clarke. Book tv: Richard clarke "cyber war" (may 25th 2010). http://www.youtube.com/watch?v=6_ek8mugOUc. Visited April 18th 2013.

[13] R. A. Clarke. Cyberwar in 2013 (dec 12th 2012). http://www.youtube.com/watch?v=B6iwkoLALQU. Visited April 18th 2013.

[14] C. C. Club. Chaos computer club analyzes government malware. http://ccc.de/en/updates/2011/staatstrojaner. Visited April 2013.

[15] Cnet. Operation aurora (google vs. china) explained. http://www.youtube.com/watch?v=8Y5Vbp6qQRI. Visited April 21st 2013.

[16] Cornell. 18 usc § 2331 - definitions (pub 15.01.13). http://www.law.cornell.edu/uscode/text/18/2331. Visited 22. April 2013.

[17] CrySyS. Duqu: A stuxnet-like malware found in the wild (v0.93) (pub 14th oct 2011). http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf. Visited 21. April 2013.

[18] CrySyS. skywiper (a.k.a. flame a.k.a. flamer): A complex malware for targeted attacks (v1.05) (pub 31th may 2012). http://www.crysys.hu/skywiper/skywiper.pdf. Visited 21. April 2013.

[19] M. K. Daly. The advanced persistent threat. http://static.usenix.org/events/lisa09/stream1/daly.html. Visited April 2013.

[20] J. Deerman. Advanced malware detection through attack life cycle analysis. http://www.isc8.com/assets/files/CyberadAPT.WhitePaper.7000_HN.pdf, September 2012. Visited April 2013.

[21] T. R. M. Dmitri Alperovitch, Vice President. Revealed: Operation shady rat. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf, 2011. Visited April 2013.

[22] economist.com. Kal's cartoon: May 7th 2009 from the print edition. http://www.economist.com/node/13612429. Visited April 2013.

[23] O. K. Eide. Cybervakten. April 2013. http://www.fofo.no/forsvaretsforum.no/Cybervakten.b7C_w7HW51.ips.

[24] G. M. Ellen Nakashina and J. Tate. Washington post: U.s., israel developed flame computer virus to slow iranian nuclear efforts, officials say (pub 19th jun 2012). http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html. Visited 21. April 2013.

[25] Enisa. Cyber-attacks – a new edge for old weapons. http://www.enisa.europa.eu/media/press-releases/enisa-flash-note-cyber-attacks. Visited April 2013.

[26] M. S. et al. The tallinn manual. http://issuu.com/nato_ccd_coe/docs/tallinnmanual. Visited 15. April 2013.

[27] EU. Cybersecurity strategy of the european union. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[28] N. Falliere. Stuxnet introduces the first known rootkit for industrial control systems (pub 6th aug 2010). http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices. Visited

April 2013.
[29] B. Fung. Nextgov.com: This defense contractor is repeatedly spear-phishing 68,000 innocent people (pub 3rd april 2013). http://www.nextgov.com/defense/2013/04/defense-contractor-repeatedly-spear-phishing-68000-innocent-people/62278/?oref=ng-HPriver&&&&utm_term=2013-04-05-10-22-44. Visited April 2013.
[30] S. Gibson. Listener feedback 155 (nov 21st 2012). http://www.grc.com/sn/sn-379.htm. Visited 16th April 2013.
[31] D. Goodin. Puzzle box: The quest to crack the world's most mysterious malware warhead (pub 14 march 2013). http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/. Visited 14. April 2013.
[32] G. Gross. Intelligence officials see cyberattacks as a top us threat. http://news.idg.no/cw/art.cfm?id=BEA9EB2B-BCB3-FB16-94E7F7B7492A51F5. Visited 14. April 2013.
[33] P. Hallam-Baker. Owasp appsecusa 2012: Iran's real life cyberwar (des 9th 2012). http://www.youtube.com/watch?v=geAc5Rj0Hrg. Visited April 18th 2013.
[34] L. Hamnes. 16 spektakulære cyberangrep. http://www.tu.no/it/2012/06/03/16-spektakulare-cyberangrep. Visited 14. April 2013.
[35] J. Healey. Reason finally gets a voice: The tallinn manual on cyber war and international law (march 27th 2013). http://www.acus.org/new_atlanticist/reason-finally-gets-voice-tallinn-manual-cyber-war-and-international-law. Visited 15. April 2013.
[36] K. Hickman. Fabian strategy: Wearing down the enemy. http://militaryhistory.about.com/od/militarystrategies/p/fabian.htm. Visited April 22nd 2013.
[37] B. M. Hämmerli. Second feedback on first draft (may 7th 2013).
[38] S. T. Institute. Assessing outbound traffic to uncover advanced persistent threat. http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf. Visited April 2013.
[39] M. S. Jari Rantapelkonen. The fog of cyber defence. http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf. Visited April 2013.
[40] D. S. C. T. U. R. T. Joe Stewart, Director of Malware Research. Htran and the advanced persistent threat (pub 03 aug 2011). http://www.secureworks.com/cyber-threat-intelligence/threats/htran/. Visited 10. April 2013.
[41] P. A. Johansen. Aftenposten.no: Spionerte på telenor-sjefer, tømte all e-post og datafiler. http://www.aftenposten.no/nyheter/Spionerte-pa-Telenor-sjefer_-tomte-all-e-post-og-datafiler-7149813.html#.UU74ps_Kziw. Visited April 2013.
[42] M. Jørgenrud. Digi.no: Us airforce utvikler seks kybervåpen (pub 9th apr 2013). http://www.digi.no/914726/us-airforce-utvikler-seks-kybervaapen. Visited April 2013.
[43] M. Jørgenrud. Forsvaret ble hacket i afghanistan (nov 11th, 2011). http://www.digi.no/882447/forsvaret-ble-hacket-i-afghanistan. Visited April 18th 2013.
[44] M. Jørgenrud. Norge kan gå til kyberkrig (feb 5th 2013). http://www.digi.no/910825/norge-kan-gaa-til-kyberkrig. Visited April 18th 2013.
[45] Kaspersky. The "red october" campaign - an advanced cyber espionage network targeting diplomatic and government agencies. http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies. Visited April 22nd 2013.
[46] Y.-H. Kim and W. Park. A study on cyber threat prediction based on intrusion detection event for apt attack detection. *Multimedia Tools and Applications*, pages 1–14, 2012.
[47] J. Kopstein. Hacking back: cops and corporations want cybersecurity to go on the offensive (may 9, 2013). http://www.theverge.com/2013/5/9/4315228/hacking-back-cops-and-corporations-want-offensive-cybersecurity. Visited May 9th 2013.
[48] B. Krebs. Chasing apt: Persistence pays off (april 13th 2013). http://krebsonsecurity.com/2011/10/chasing-apt-persistence-pays-off/. Visited 16. April 2013.
[49] A. Kujawa. Gauss malware: My take on its mystery components (september 7th 2012). http://www.zdnet.com/gauss-malware-my-take-on-its-mystery-components-7000003894/. Visited 15. April 2013.
[50] J. A. Lewis. Raising the bar for cybersecurity (feb 14th 2013). http://csis.org/publication/raising-bar-cybersecurity. Visited April 21st 2013.
[51] J. Leyden. Apt1, that scary cyber-cold war gang: Not even china's best (pub 27 feb 2013). http://www.theregister.co.uk/2013/02/27/apt1_china_dark_visitor_b_team/. Visited 10. April 2013.
[52] B. Malmedal. Er attribution og hack-back umulig? (april 14th 2013). http://norcydef.blogspot.no/2013/04/er-attribution-og-hack-back-umulig.html.
[53] Mandiant. 2013 threat report. https://www.mandiant.com/resources/m-trends/. Visited March 2013.
[54] Mandiant. Apt1 - exposing one of china's cyber espionage units. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. Visited April 2013.
[55] Mandiant. M-treands: An evolving threat. http://www.utdallas.edu/~mxk055100/courses/dbsec12f_files/trend-report.pdf, 2011. Visited May 2013.

[56] K. O. Mark M. Jaycox. Cispa is back: Faq on what it is and why it's still dangerous (feb 25th 2013). https://www.eff.org/cybersecurity-bill-faq. Visited 15. April 2013.
[57] P. Muncaster. Japanese gov builds apt database to study targeted attack info (pub 26. feb 2013). http://www.theregister.co.uk/2013/02/26/japan_apt_database_us/. Visited April 2013.
[58] NationalAuditOffice. The uk cyber security strategy: Landscape review (pub 12th feb 2013). http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf. Visited April 2013.
[59] S. Nicholas J. Percoco. Data exfiltration: How data gets out. http://www.csoonline.com/article/570813/data-exfiltration-how-data-gets-out, March 12 2010. Visited April 2013.
[60] NIST. Nist special publication 800-39: Managing information security risk. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, 2011.
[61] Norsk-Telegrambyrå. Digi.no: Ikt-sikkerhet til nytt departement (22nd mar 2013). http://www.digi.no/914031/ikt-sikkerhet-til-nytt-departement. Visited April 2013.
[62] NSM. Hva er norcert? https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Om-NorCERT/. Visited April 18th 2013.
[63] E.-t. NSM, PST. Trusler og sårbarheter 2013. http://www.pst.no/media/59018/Trusler_og_sarbarheter_2013.pdf. Visited April 2013.
[64] U. H. of Representatives. Investigative report on the u.s. national security issues posed by chinese telecommunications companies huawei and zte (september 7th 2012). http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf. Visited 15. April 2013.
[65] N. Perlroth. Hackers in china attacked the times for last 4 months (jan 30th 2013). http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=1&_r=3&&%2359;pagewanted=all&%2359;hp. Visited April 21st 2013.
[66] N. Perlroth. In cyberattack on saudi firm, u.s. sees iran firing back? (oct 23rd, 2012). http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0. Visited April 18th 2013.
[67] PST. Åpen trusselvurdering 2013. http://www.pst.no/media/58980/PSTs_tv2013_web.pdf. Visited April 2013.
[68] E. A. S. M. publication. Malware: Stopping cyberattacks. http://media.scmagazineus.com/documents/30/apt_attack_0510_7315.pdf, 2010. Visited April 2013.
[69] N. G. Raimund. Permanently remove backdoor:win32/poisonivy.h virus. http://blog.teesupport.com/permanetly-remove-backdoorwin32poisonivy-h-virus-get-backdoorwin32poisonivy-h-off-my-computer-manually/, April 13 2011. Visited April 2013.
[70] reference.com. on critical infrastructure. http://www.reference.com/browse/critical+infrastructure. Visited 13. April 2013.
[71] M. Rouse. Advanced persistent threat (apt). http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT, November 2010. Visited April 2013.
[72] R. Rowlingson. Abstract a ten step process for forensic readiness. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.65.6706.
[73] RSA. Fraudaction research labs: Anatomy of an attack. http://blogs.rsa.com/anatomy-of-an-attack/, April 1 2011. Visited April 2013.
[74] D. E. Sanger. Obama order sped up wave of cyberattacks against iran (pub 1st june 2012). http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Visited April 2013.
[75] SANS. Csis: 20 critical security controls version 4.1. http://www.sans.org/critical-security-controls/. Visited April 2013.
[76] R. Santalesa. 2013 verizon data breach report is out – risks increase (april 24, 2013). http://www.infolawgroup.com/2013/04/articles/information-security/2013-dbir/. Visited May 9th 2013.
[77] B. Schneier. Blog on state-sponsored gauss malware. http://www.schneier.com/blog/archives/2013/03/gauss.html. Visited April 2013.
[78] Seculert. Combating apt through detection. Visited April 2013.
[79] D. SecureWorks. Lifecycle of the advanced persistent threat. http://docs.media.bitpipe.com/io_10x/io_105022/item_550605/Lifecycle_of_the_Advanced_Persistent_Threat%5B1%5D.pdf, 2012. Visited May 2013.
[80] A. Shalal-Esa. Six u.s. air force cyber capabilities designated "weapons". http://www.reuters.com/article/2013/04/09/net-us-cyber-airforce-weapons-idUSBRE93801B20130409. Visited 14. April 2013.
[81] H. E. N. S. S. . Solutions. Cybercrime and advanced persistent threats. http://www.mhprofessional.com/downloads/products/0071780289/0071780289_chap06.pdf, 2012. Visited April 2013.
[82] D. Sullivan. Beyond the hype: Advanced persistent threats.

http://www.trendmicro.com/cloud-content/us/pdfs/business/ebooks/eb_real-time-publishers-esapt.pdf, 2011. Visited May 2013.

[83] S. Sveinbjørnsson. Kan være greit å drepe hackere. http://www.digi.no/913960/kan-vaere-greit-aa-drepe-hackere. Visited April 2013.

[84] Symantec. W32:duqu - the precursor to the next stuxnet (version 1.4) (pub 23rd nov 2011). http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf. Visited April 2013.

[85] TrendMicro. Deep discovery protects users from cyber attacks in south korea. http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiping-trojan-other-attacks-hit-south-korea/. Visited April 2013.

[86] TrendMicro. How deep discovery protected against the korean cyber attack. http://blog.trendmicro.com/trendlabs-security-intelligence/how-deep-discovery-protected-against-the-korean-mbr-wiper/. Visited April 2013.

[87] Truimfant. Detecting and remediating malicious attacks. Visited April 2013.

[88] TrustwaveGlobalSecurityReport. 2013 trustwave global security report. https://www2.trustwave.com/2013GSR.html. Visited April 2013.

[89] D. S. Vassilis Prevelakis. The athens affair. http://spectrum.ieee.org/telecom/security/the-athens-affair/0. Visited April 21st 2013.

[90] N. Villeneuve and J. Bennet. Detecting apt activity with network traffic analysis. Visited April 2013.

[91] Websense. Advanced persistent threats and other advanced attacks. http://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf. Visited April 2013.

[92] Wikipedia. Bring your own device. http://en.wikipedia.org/wiki/Bring_your_own_device. Visited April 10th 2013.

[93] Wikipedia. on advanced persistent threat. http://en.wikipedia.org/wiki/Advanced_persistent_threat. Visited 4. March 2013.

[94] Wikipedia. on bring your own device. http://en.wikipedia.org/wiki/Bring_your_own_device. Visited April 2013.

[95] Wikipedia. on crowdsourcing. http://en.wikipedia.org/wiki/Crowdsourcing. Visited April 2013.

[96] Wikipedia. on duqu. http://en.wikipedia.org/wiki/Duqu. Visited April 2013.

[97] Wikipedia. on flame (malware). http://en.wikipedia.org/wiki/Flame_(malware). Visited 21. April 2013.

[98] Wikipedia. on force multiplication. http://en.wikipedia.org/wiki/Force_multiplication. Visited 15. April 2013.

[99] Wikipedia. on national security. http://en.wikipedia.org/wiki/National_security. Visited 13. April 2013.

[100] Wikipedia. on operation aurora. http://en.wikipedia.org/wiki/Operation_Aurora. Visited 12. May 2013.

[101] Wikipedia. on profibus. http://en.wikipedia.org/wiki/Profibus. Visited April 2013.

[102] Wikipedia. on stuxnet. http://en.wikipedia.org/wiki/Stuxnet. Visited 12. May 2013.

[103] Wikipedia. on weapon. http://en.wikipedia.org/wiki/Weapon. Visited 13. April 2013.

[104] Wikipedia. on zero-day attack. http://en.wikipedia.org/wiki/Zero-day_attack. Visited April 2013.

[105] K. Wilhoit. In-depth look: Apt attack tools of the trade. http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/, March 4 2013. Visited April 2013.

[106] J. Worrall. In-progress cyber attack intelligence blog. http://www.countertack.com/blog/bid/90051/Timing-is-Everything1/12/14/timing-is-everything/, December 14 2011. Visited April 2013.

[107] J. Worrall. Lateral movement – a critical opportunity to detect an in-progress cyber attack. http://www.countertack.com/blog/bid/124216/Lateral-Movement-A-Critical-Opportunity-to-Detect-an-In-progress-Cyber-Attack, April 3 2012. Visited April 2013.

[108] W. Yan. Cas: A framework of online detecting advance malware families for cloud-based security. In *Communications in China (ICCC), 2012 1st IEEE International Conference on*, pages 220–225, 2012.

[109] K. Zetter. How digital detectives deciphered stuxnet, the most menacing malware in history (pub 11th nov 2011). http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1. Visited April 2013.

[110] K. Zetter. Report: Stuxnet hit 5 gateway targets on its way to iranian plant (pub 2nd nov 2011). http://www.wired.com/threatlevel/2011/02/stuxnet-five-main-target/. Visited April 2013.