University of Houston – College Of Technology

CIS 6322 – Secure Enterprise Computing

Advanced Persistent Threat

Paper Submission

Dhanaraj Chalil
dvchalil@uh.edu
Submitted on: 26th April 2019

TABLE OF CONTENT

ADVANCED PERSISTENT THREAT

ABSTRACT

This paper describes the Advanced Persistent Threat (APT), which has become a major concern for organizations. The cyber world has seen several APT attacks on various organizations and their devasting impact. This paper analyses the important aspects about APT for providing a great idea on it. Either its information technology sector or operational technology sector, there have been several APT incidents. Not only the big organizations but even small companies are also the target of APT attacks. APT is quite different from other cyber attacks depending on several factors. The major one is the ability of this threat to persist in an organization network undetected and perform several exploitations. This paper provides a broad view of how this threat act on the organization.

There are several APT groups identified, which possesses several different characteristics based on their attack tactics, threat vectors they choose, motivation for attacking, industry sector they focus on, etc. After analyzing these details on APT groups, this paper describes some common characteristics of APT groups, which could be used as indicators for companies to figure out whether they have become a target for APT attack.

As it is mentioned before, both IT and OT industries have been suffering from APT attacks, and the cybersecurity measures they have adopted does not effectively detect, respond, or even prevent the threat, which makes it hard to resist. There have been several incidents reported worldwide, and this paper makes an analysis of the victims of this threat. A detailed description of APT versus organizations and lessons that the cyber world should interpret are also presented in later sections. Moreover, those ideas with which organizations should frame their protection strategies are explained in this paper. As the threat becomes sophisticated, it is also important that organizations should focus on adopting effective protection strategies as well as enhance their existing cybersecurity measures.

1. Introduction

An Advanced Persistent Threat (APT) is a term that describes a computer network attack campaign in which intruders establishes an illicit, long term undetected presence on the network or system in order to mine highly sensitive data. The target of this attack usually includes large enterprises or governmental networks. Since this is a well-planned and well-sponsored cybercrime executed by highly skilled intruders, the consequences of this attack are severe and vast. An APT will have either have a business or political motive, aiming for critical damage to the target.

The APT activities require a high degree of secrecy over a long period of time. The name itself can be used to provide a better description of the threat. The “advanced” process indicates sophisticated techniques used to exploit vulnerabilities in systems. The “persistent” process denotes that an external system is continuously monitoring and extracting data from the target. This could be the command and control system managed by attackers. The “threat” process indicates human involvement in orchestrating the attack. This attack outcomes devasting consequences which include intellectual property theft that even can include trade secrets or patents of the organization, compromised sensitive information including employee and user private data, sabotaging of critical organizational infrastructures, and even total site takeovers.

The perpetrators of an APT are usually a group of highly skilled cybercriminals with a strong substantial financial backing. This attack was traditionally associated with state sponsorship. But over the last few years, there have been multiple attacks that were conducted by non-state sponsored attack groups over large-scale targeted intrusions for specific goals. The attack vectors include infected media, supply chain compromise, and human intelligence and deception, with which attackers place malicious codes on one or multiple computers some specific tasks and to remain undetected for the longest possible period. This attack is significantly more complex compared to other traditional application threads. There is no hit-and-run strategy, once a network is infiltrated, the attackers remain in order to attain as much information as possible from the target. More common attacks like remote file inclusion, SQL injection, phishing emails, cross-site scripting are frequently used by perpetrators to establish a foothold in the network. Later, Trojans or backdoor shells are often used to expand the foothold and create a persistent infection within the target.

2. Characteristics of an APT

The following points can be stated as characteristics of an APT. Most of the APT groups have these characteristics in common.

- Increase in elevated log-ons – APTs rapidly escalate from compromising a single host in target’s network to taking over multiple hosts or the whole network in short time interval. They perform this mostly by accessing an authentication database, stealing credentials, and reusing them. They identify access privileges and permissions of all stolen credentials, then go through those accounts to compromise assets within the environment. Often, a high volume of elevated log-on occurs at an unusual time because the attackers act when nobody is interfering with systems. If you suddenly notice a high volume of elevated log-ons across multiple servers or high-value individual computers while the legitimate work crew away, it’s time to start thinking about APT.
- Widespread backdoor Trojans – APT hackers often install backdoor trojan programs on compromised systems within the exploited environment, in order to ensure that they can always get back in, even if the

captured log-on credentials are changed. Trojans deployed through social engineering hacks provide the avenue through which most companies are exploited. They are common in every environment, and they proliferate in APT attacks.

- Unexpected information flows – Look for large, unexpected flows of data from internal origination points to other internal computers or to external computers. In some scenarios, these data flows might also be limited, while the attackers steal only relevant data.

- Unexpected data bundles – APTs often aggregate stolen data to internal collection points before moving it outside. Look for large, usually, gigabytes sized chunks of data appearing in places where that data should not be, especially if compressed in archive formats not normally used by the company.

- Focused spear phishing or other social engineering campaigns – One another best indicator of APT attack will be a focused spear phishing email campaigns against the target company's employees, containing attachments like document files which have an executable code or malicious URLs. Even though attackers use other social engineering tactics, spear phishing emails are the usual method. Smart conspirator’s phish email is not sent to everyone in the company, but instead to a more selective target of high-value individuals within the company, using information that was collected from previously compromised systems.

APT hacks are difficult to detect because the hackers use custom coding in addition to exploiting known network and software vulnerabilities. But still, we can identify an APT attack using the above mentioned five characteristics as indicators for companies when they’ve been the target of an APT.

3. Victims of APT

Often, APT cybercriminals target large organizations such as government agencies, financial institutions and IT sector with valuable data. They also target critical infrastructures and large manufacturing units as targets to this attack. However, smaller companies also have the potential to be victims. With a detailed analysis of the history of APT incidents, we could say that both IT, as well as OT sectors, are targets of APT actors.

APT on information technology sector are initiated through two main tactics. Attacks through public servers and public websites on the Internet is the first tactic. There are several public websites on the internet, that contains malicious codes. Whenever a user from an organization access it or perform some actions in these webpages, these malicious codes flow to the organization’s network along with data traffic. Once these malicious programs reach to any system, it tries to compromise the system by running in it. If they go successful in compromising the system, they try to spread throughout the network and steal relevant information from all compromised systems and servers. The other tactic of attack is social engineering focused on organization employees. The usual way followed by attackers is sending out spear-phishing emails employees in the organization. Users who unknowingly act on this will get their systems compromised by attackers to make a foothold for further interventions. Attackers also use other social engineering tactics like a watering hole, whaling attacks, etc. Most of the IT sector APT attacks are intended for financial gains, political and social espionage, information theft, public humiliation of organization, etc.

APT on Industrial Control Systems (ICS) is also the main concern. Attackers have targeted critical infrastructures, manufacturing units, large scale public and private industries, etc. for APT as attacks on these units will make a devasting disaster to community. Most of the international cyber-attacks, cyberterrorism, and high criminal incentive attacks are being focused on ICS due to the high threat and impact it makes. Rather than heavy financial loss, it could also result in information theft, infrastructure breaks down, or even disasters which include the explosion in manufacturing or industrial plants, impact to the environment, and loss of life.

No organization should assume its data and resources are of little or no value. Attackers aren't just looking for classified information, but sensitive business details, intellectual property, scientific data and government policies, critical infrastructures, industries are all being targeted.

4. APT versus Enterprise

It's no secret that security threats keep evolving over the year. Even though security technologies and processes keep evolving, breaches still happen at a higher rate. Today's advanced persistent threats are increasingly sophisticated, diverse, targeted, aggressive, and successful. The lack of in-house enterprise expertise remarks the organizational gap that exists between the day-to-day operations team and the advanced security teams that contain and resolve incidents. This gap is worsened by the tendency of traditional advanced threat solutions to operate in a silo – and not share new threat intelligence across the security environment. Enterprises mostly lack the skills and technology to address the latest cybersecurity threats. According to the Verizon Data Breach Report, 84 percent of advanced persistent threats took seconds, minutes or hours to compromise targets. 78 percent of threats took weeks, months or years to discover. Today's enterprises are experiencing material security breaches because of an organizational gap between day-to-day security operations and advanced security operations teams. A recent survey found that most respondents did not have the tools, personnel or funding to determine root causes of a data breach. The top two reasons for failing to prevent a malicious breach are lack of in-house expertise and lack of adequate forensics capabilities.

A long-term persisting attack will cost the business a huge amount of money, time, productivity and reputation. The enterprise still upholds traditional security defenses that are designed to detect, and block known threats. Enterprises are remaining blind to today's zero-day threats and novel malware that are hard to trace and defend. Moreover, attackers have started being smart and systematic in performing an attack. They do set different vectors of exploiting vulnerabilities which help them hold to attack plan even though the primary vector gets blocked. APT actors have effective skills and tactics that help them set their tasks in victim's infrastructure hidden against regular vulnerability assessments, anti-malware programs, and other defenses adopted by victim body. Most of the organizations find it feasible to build a security operation center within their operational infrastructure with available professionals and resources. Holding an effective security center with extreme skilled professionals and resources or outsourcing security to third-party who research on new threats, tactics, vulnerabilities stays as a heavy financial burden.

The organized nature of APT attacks is what makes them advanced and hard. The APT actors appear to organize on several levels which make them the growing risk to organizations' financial assets, intellectual property, and reputation. They follow a continuous process or kill chain. This includes to target a specific organization for a singular objective, perform attempts to gain a foothold in the environment, use the compromised systems as access into the target network, deploy additional tools that help in fulfilling the attack objective, and cover tracks to maintain access for future initiatives. In detail, these major actions can be divided into several phases to identify how APT progress against the enterprise.

The reconnaissance phase of an APT includes defining the target, finding and organizing accomplices, building or acquiring tools, researching target infrastructure/employees, and testing for detection milestones. In this phase, actors start focusing on their target. They enumerate the components necessary to execute their plan and begin their efforts to collect these components which include infrastructure, tools, data, information on the targets' environment and other required assets. Actors also collect intelligence on security controls and procedures they are likely to encounter to create evasion and response plans. For example, actors may register new domains or configure domains at dynamic DNS providers, set up malware command and control (C2) servers at hosting sites or on previously compromised systems, allocate web and FTP (File Transfer Protocol) servers to host phishing or exploit sites and data drops, acquire email servers for relaying spam or for data exfiltration, and so on. For attack operations, actors may need to construct or rent botnets. The infrastructure needed to carry out operation will vary based on the target and the objective, but necessary resources will be identified and prepared ahead of the direct action against the target. These research activities on target infrastructure go systematic and an excellent view made thereby help them to plan a persistent nontraceable attack. Monitoring of preparation activities can sometimes provide insight into upcoming targets and objectives.

The compromise phase includes the deployment of attack, initial intrusion, and outbound connection initiation phases in the lifecycle. After the attacker completes preparations, the next step is attempting to gain a foothold in the target's environment. An extremely common entry tactic is the use of spear phishing emails containing a web link or attachment which lead to sites where the target's web browser and related software are subjected to various exploit techniques. Other tactics are also used by intruders to gain access to the organization network. These include stolen credentials, malware execution via infected patch, infecting any active server, spoofing network traffic to gain connection as a legitimate host, etc. The attackers will try to exploit all possible vulnerabilities during this phase to gain a foothold to the target's environment. A successful exploit installs an initial malware payload on the victim's computer. Gaining a foothold is the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions to spread all over. They try to catch hold of core from where they can access sensitive data. The malware placed could be a simple downloader, basic Remote Access Trojan or a simple shell. After the requisite steps of preparation and gaining control of a system becomes successful, the APT actor can use the infected system as a conduit into the target network and as a deployment mechanism for additional tools that will facilitate the fulfillment of their primary objectives.

The lateral movement phase of the APT comprises of expanding access to systems and obtaining credentials. Thereafter attackers try to strengthen foothold to sustain in the target environment. The main objective is to gain privileges to additional systems and authentication material that will help in expanding their attack. A common pattern to gain domain level administrative privilege is to obtain administrative access to the initial target, capture cached credentials for a domain administrator account that has logged into the initial target, and utilize techniques to gain access to other systems. Once the APT actors possess the target's account credentials, it becomes tough to track attackers' activities. The attackers' movement through the network can become more difficult to identify, as they have the correct username and password. It could be stated that they are no longer hacking, but a person with those credentials is logging in. When done from the right systems and in the right patterns, it can be very difficult to differentiate between authorized and unauthorized access. Changing the credentials is a good practice, but it doesn't completely mitigate the data loss. Passwords with similar patterns are even easy for attackers to crack and take over the account. If the actors behind the intrusions have not completed their tasks, then they will be back in the future to complete their objectives. Tools like keyloggers and web form grabbers are useful to steal credentials. Even APT actors may employ vulnerability exploitation, social engineering, distribution of infected physical media such as USB sticks or CDs, human bribes, screen capture utilities and other techniques to gain access to target's system. They will use any means within their power to complete their tasks. APT actors perform expansion efforts to support other phases of the operation which include gaining access to systems that host or can retrieve targeted data during the search and exfiltration phase, systems that make good locations for the installation of persistence mechanisms, and systems with good network locations that can be leveraged to exfiltrate data or serve as proxies in and out of the network.

During the maintaining access phase, attackers concentrate on persisting inside the target's environment. APT actors employ various strategies to maintain access. Overcoming a target's perimeter defenses and establishing a foothold inside the network can require substantial effort. APT actors know that most organizations run anti-malware applications. With this, they take steps to ensure their tools will not be detected. They produce or customize malware and rewrite commonly-used tools like psexec and password dumpers. These custom tools are then tested against recent anti-malware and other security tools to evaluate their detection. Modifications continue until the tools evade all scans. This process is effective and makes it less likely to be detected when they are initially deployed to the target's environment.

During the data exfiltration phase of the APT attack, APT actors start exfiltrating necessary data from the target's environment. The aim of network exploitation is generally those resources that can be used for future exploits and those have perceived worth to the intruder. A popular approach to search and exfiltration is to take everything from the network that might be of interest, including every document, email and other types of data discoverable on the network. Picking all available data will be risky for intruders as it will create large network flows and other indicators which in turn may lead to the detection of actor's activities. To avoid this, some actors take a more focused approach, by searching those documents for keywords and metadata that indicate the document may be of interest to the actors. Malware is programmed with this capability too. Some malware can even search for keyword and extension types with no external actor interaction which allows them to find and exfiltrate data automatically. If the actors can elevate privileges either by passing the hash techniques or by gaining credentials for the administrative level account, they are often able to access all files on centrally-managed file servers and many workstations under the stolen administrative account's control. All this data is collected and sent to a location where the actors can retrieve it or to the actor's drop site. It is common to collect the data at a central host, bundled together and exfiltrated to the actor's drop site to avoid detections that might be triggered by many hosts contacting a remote drop site. It also allows the actors to exfiltrate data in chunks, assuring that at least some large set of data can be extracted before security personnel can respond.

A later activity on clean-up includes covering tracks of exploitation and remain undetected. APT actors put efforts for removing evidence of the intrusion, resources accessed and eliminating evidence of who was behind the event. It also involves planting or manipulating data in the environment for a misleading security team of the target enterprise. The better the APT actors are at covering their tracks, the harder it will be for victims to track conspirators and assess the impact of the intrusion.

5. Lessons from past APT attacks

From the past events of APT on several targets in information technology and operational technology sectors, we have learned the following lessons on an APT attack. These could be used as main considerations while implementing or enhancing security measures that safeguard organizations from further possibilities of attack.

1. Focus on the Crown Jewels – This advanced approach is to focus your protection efforts on your most important assets. It would be ideal to protect everything perfectly and continuously. Unfortunately, modern systems, whether they are IT systems or control systems, have become too complex to achieve perfect and uniform security. So, the smart IT teams are focusing on securing those assets that really matter to the survival of the company. They do not rely solely on a perimeter firewall to keep all the bad stuff out of the company. Instead, they install additional layered defenses directly protecting key assets such as servers containing sensitive financial or intellectual property information. There are good reasons for using this approach. The obvious one is that it allows a defense in depth strategy. It also allows the company to focus additional money, effort, and diligence on a few core assets. Another reason is that these assets are the same ones that the intruders will focus on. Hackers and worms will go after any undefended systems, but in most cases, these victims are just a stepping stone to the real target. Focusing your defensive efforts on the same things that your adversary is focusing on makes good security sense. This strategy of focusing your defenses also works for ICS and SCADA security. Every control system has a few assets that would seriously impact production, safety or the environment if successfully attacked. Every control engineer knows what really matters to his or her particular operation. Aggressively protect this asset will massively minimize the chance of a truly serious cyber incident.

2. Focus on Detection too, not only Protection: This thought centers on ‘Control Focus’. Detective Controls are more effective against modern cyber threats when compared to Preventative Controls like firewalls, data diodes, and anti-virus software. Even on reviewing countless control systems and attacks against control systems, the industrial automation world is terrible at detecting anything unusual on their control network. Organizations really seem unaware of the APT attack until attackers succeed in a total takeover of the systems and everything goes out of control. This is because of the lack of adopting good and active detection approaches as a part of security measures. Even making users aware of these detection activities could help organizations to figure out the initial compromise of systems and foothold tactics of attackers.

3. Move Your Perspective from Perimeter-based to Data-centric: This lesson to consider for successful APT containment, is to change your security focus from controlling the perimeter to controlling specific collections of data, regardless of where they are in space and time. If a financial company can ensure that customer credit card records are always encrypted and the keys to decrypt the records are not leaked, then the loss of a laptop with these records is of limited importance. A defense that only focuses on defending the perimeter is a weak defense. At first, glance, applying this lesson to ICS and SCADA systems appears to be difficult as data confidentiality is of far less importance to the control system. But considering 'process' or 'asset' instead of 'data' make a sense to this. A process-centric or asset-centric approach in managing security focus on making sure that specific high-value processes continue to function reliably regardless of attacks happening around them.

4. Compliance versus Threat Detection: This lesson looks at the reason why we log security events. Many of the sites, especially sites trying to pass NERC-CIP audits, log only for compliance reasons. They generate massive log collections, but if anyone ever bothers to analyze the logs, it is only after something bad has happened. By then it will be too late. An effective threat detection means optimizing what information you collect, so that dangerous anomalies standout, rather than get it buried in the noise.

All four lessons are highly related to the concept of focused effort. For example, effective threat detection is only possible if we focus your controls on the detection and focus your coverage on what matters. Unfocused approaches to security that try to protect everything inside a perimeter are too complex and too expensive. So, organizations should think about what information, processes, and assets really matter for active protection and start focusing on those. They should think about major vulnerabilities and focus on detecting that. They should advance security approaches from scattered to focused mode. Most importantly, these approaches could save organizations from the next APT.

6. Defending against APT

Defending APT is a great concern for enterprises as they are still unaware of those lessons mentioned in the above section. A major vulnerability to these enterprises will lead to exploitation by attackers. Operational technology and information technology have its own concerns and focus points to be considered for defending against advanced persistent threats. There are several recommends from many sources for organizations to implement for defending APT attacks. Those organizations believing that they could be at higher risk of being targets of this attack should consider more granular controls strategies. Organizations those previously became victims of this attack should also consider enhancing detective and preventive controls.

A high priority in defending APT goes for consideration of the lessons we learned from previous attack incidents. Implementing a strategy for each lesson learned will help the organization to move ahead in protection. Deeply analyzing the attackers, their attack kill chain, tactics they used, and impact on organizations will help to understand the APT attack. Relate the identified attack mode with the existing database of APT groups. This will help us in planning an enhanced mitigation strategy against APT. Other mitigation plans include risk assessment, vulnerability analysis, and routine patch process and management. Basic defenses should also focus on ensuring that the anti-virus technology is up-to-date, properly tuned and deployed and is working properly. While anti-virus is not a silver bullet, many organizations have a lax configuration policy or do not have the agent deployed to all their assets. Managing permissions is critical as well. Users should only have the rights they need to do their job and nothing more. As users change job roles or otherwise move throughout the organization, provisioning, de-provisioning and access auditing should occur to ensure no 'aggregation of privilege' scenarios exist. The defense should not only focus on mitigation strategies but also on detection strategies too. Since APT follows a silent mode of attack, detection and responding to the situation is the best way to handle the attack. These activities should be periodic. Each time a vulnerability is identified, make necessary actions to cover it and provide necessary enhancements to security measures.

The defense should also focus on employee training. APT attacks can start in a variety of ways, mostly with social engineering. Employees are an enormous attack vector that organizations need to address before moving on to more technical aspects of defense. First and foremost, employees must be taught that giving information over the phone or email or during the conversation to anyone without definitively confirming their identity leaves the company open to a breach. Additionally, it's important for organizations to discuss email phishing. Proper training and periodic assessment on basic security details should be done for employees to keep them act smart to attack situations.

It is also important to focus on ensuring endpoint security for the organization. An endpoint is just an entry point onto a network created by each device of the organization. Managing every single endpoint on an entire network can be an exhaustive process for an administrator. They need a means of consolidating endpoint security into a central console that allows them to protect assets across a wide variety of devices. It is important to change default passwords on purchased equipment. One of the first actions a hacker will take when attempting to break a system is to brute force a list of known default credentials. This simple mistake is one of the easiest ways for a cybercriminal to gain access to your organization's data. Also, consider using powerful endpoint maintenance, management and security tools to bolster an organization's defenses against targeted attacks, while improving business continuity. A multi-layered security approach combined with maintenance automation can help to defend against APTs while also detecting and solving them before it's too late.

Building a robust system architecture will help in defending APT systematically. This includes identifying risk and developing a plan for managing that risk, implementing effective controls to manage the risk, and creating a defense-in-depth model that allows effective and efficient security controls. Risk assessment is a function to identify vulnerabilities and threats, understand their impact, and determine which controls will best mitigate those threats. Risk assessment includes steps to identify assets and their value, identify vulnerabilities and threats, calculate threat probability and business impact, and balance threat impact with security control cost. Managing the risk emphasis on implementing effective controls. This include patching, updating, and maintaining necessary hardware and software assets of the organization based on proper standards. Managing risk should also consider building a contingency plan for handling the organization systems. Implementing defense in depth strategy based on widely accepted standards and recommendations is the final step in building a robust system architecture. Multiple levels of security measures will make it hard for attackers to penetrate to organization's network and perform illegitimate actions. Network segmentation also plays an important role in defending APT, which can be implemented in both IT and OT sectors.

7. Conclusion

The APT actors are focused on persisting in the target network and acquiring sensitive data. They are well adapted to failures and continue to hunt for security vulnerabilities and blind spots in monitoring. If they can break or bypass defenses already implemented in an organization, they can make rapid lateral movements for persistence and exfiltration. Once they locate data, they can move it out of the network for offline review. That data is used for future intrusions, to eliminate technical advantages over the actors' customer or country, to provide advantages in business dealings or for other real-world purposes that can have significant economic and strategic impacts on targeted entities. Considering security and the mindset of the actors behind the threats when planning mitigation and detection strategies can yield better protection against APT threats in the future. Log retention and monitoring strategy are also important. Planning these considerations ahead of time will make it much harder for APT actors to cover their tracks and will make incident response efforts more effective and efficient.

A well-developed communications plan regarding cybersecurity for the organization will help employees to understand the threats and methods to identify them. This will help to mitigate social engineering attempts by APT actors. Maintaining the IT environment through vulnerability assessment and efficient patch management is an important step to eliminate opportunities for initial intrusions. Removing local administrative privileges from users' workstation accounts and limiting access to only what is necessary helps prevent privilege escalation and access expansion efforts. Modeling the threat through penetration testing and training exercises that emulate APT are also a valuable self-assessment and training tools for management and defense staff. Good situational awareness is critical to forming effective defense strategies. Without a thorough understanding of the threat, defensive strategies and spending will be inefficient at best and ineffective at worst. In the case of APT, security controls must be developed that account for the actors, their ability to adapt and the resolve they have towards obtaining your assets. Use mechanisms for blocking adversary scanning and reconnaissance without also blocking legitimate users in IT as well as ICS industries. Adopt network segmentation and access restrictions strategies to defend APT to a greater extent. We have already discussed strategies for defending APT in the above section. Adhere to all these recommendations and validate the effectiveness of established preventive measures to make sure that the organization won't become a victim of APT in the future.

8. References

1. *The Advanced Persistent Threat: Michael K. Daly November 4, 2009 – http://static.usenix.org/event/lisa09/tech/slides/daly.pdf*
2. *A study on the advanced persistent threat: Communications and multimedia security – https://link.springer.com/book/10.1007/978-3-662-44885-4*
3. *Advanced persistent threat – https://en.wikipedia.org/wiki/Advanced_persistent_threat*
4. *Advanced persistent threat: Defense against advanced threats requires integrated threat intelligence – https://www.secureworks.com/resources/sb-advanced-threat-protection*
5. *Aacademia : Advanced Persistent Threat (APT) – https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT*
6. *Search Security: advanced persistent threat – https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT*
7. *Anatomy of advanced persistent threat – https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html*
8. *Proofpoint: Advanced Persistent Threat Defense And Protection – https://www.proofpoint.com/au/threat-reference/advanced-persistent-threat*
9. *Five notable examples of advanced persistent threat (APT) attacks – https://www.getsafeonline.org/business-blog/five-notable-examples-of-advanced-persistent-threat-apt-attacks/*
10. *Imperva: Advanced persistent threat (APT) – https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/?utm_campaign=Incapsula-moved*
11. *Advanced Persistent Threat: Evolution of the attacker – https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493741434.pdf*
12. *Anatomy of an Advanced Persistent Threat (APT) Group – https://www.youtube.com/watch?v=SZCE677ijMU*
13. *Advanced Persistent Threat (APT) - Infosec - InfoSec Institute – https://www.infosecinstitute.com/content-library/advanced-persistent-threat-apt/*
14. *Targeted cyber attacks logbook – https://apt.securelist.com/#!/threats/*