1st International Conference on the Mutation of Management Science, Economics and Accounting
www.mmea.ir
Adib Mazandaran Institute of Higher Education
ISC
Islamic World Science Citation Center
License code: 00201-91046

The Analysis of Advanced Persistent Threat (APT), Detection and Defence

Seyed Reza Hadianfar[a], Alireza Pourebrahimi[b], Mohammad Malekinia[a,b,*]

PhD student in Information Technology Management, Islamic Azad University, Kish
faculty members of Alborz Islamic Azad University, Karaj
A.pourebrahimi@kiau.ac.ir
faculty members of Islamic Azad University of South Tehran, Tehran
M_malekinia@azad.ac.ir
* Corresponding author: Seyed Reza Hadianfar and E-mail: Sr.hadianfar@iaukishint.ac.ir

Abstract
Advanced Persistent Threat can be defined as a very complex and targeted cyberattack. Hackers are always looking for a way to penetrate users' systems, especially those who have important and valuable information. On the other hand, organizations, companies, and institutions have always sought to detect various types of anti-malware to prevent cyberattacks, so hackers are trying to create an undetectable malware so that it can remain in the user's system for a long time. Therefore, they move towards Advanced Persistent attacks. These attacks have been one of the biggest threats to the information technology in recent years. In this article, we will briefly discuss Advanced Persistent Threat, its identification, and ways to deal with it.

Keywords: Advanced Persistent Threat (APT), Cybersecurity, Backdoor, Cyberattacks, Server Command and Control Introduction

A.Introduction

With the increase of cybercriminals' complex tools, conventional solutions can't cope with the current complexities of this type of threat. APT is a real threat to public and private institutions around the world and will continue to be so in the future [١]. The number of reported cases of sustained advanced attacks has increased significantly in recent years [٢]. The vulnerability of people, organizations, or governments that trade online is exploited by hackers and cybercriminals [٣].

Cybercriminals abuse current issues that are of interest to the public. The situation of Covid١٩ has created a good excuse to start the attacks. In this case, the deception of advisory information about the state of health care in different countries of the world. [٤] In recent years, researches have been done on Advanced Persistent Threat.

The purpose of this article is to review the Advanced Continuous Threat (APT), identify it, and how to deal with it. This article is a compilation and is organized as follows: Section ٢ generally describes the trend of Advanced Persistent Threat. Section ٣ describes the APT life cycle analysis. Sections ٤ and ٥ identify and counteract the attacks, and Section ٦ conclusion.

B. Advanced Persistent Threat (APT)

Advanced Persistent Threat is a complex and long-term set of actions taken against specific individuals, organizations, or companies. They are often provoked by attackers who study a company and its employees for months before the attack begins. They use a device that minimizes the chance of detection. [٥] Since the appearance of Stuxnet, APT attacks have been carried out with greater caution and damage. At the moment, many of these threats are undetectable. Many of these threats reappear after identification with changes to achieve their goal. [٦] The UK National Cybersecurity Center defines APT as "a targeted cyberattack in which a hacker gains access to a system and goes undetected for a long time" [٢٧].

McAfee defines APT as "sophisticated and covert attacks that illegally steal valuable data from target companies." Their relentless interventions typically target main users of organizations for access to trade secrets, intellectual property, government and military secrets, computer code sources, and other valuable information available. While APT uses many of the traditional attack techniques, it differs from common botnets and malware because it targets strategic users to gain unknown access to core assets. APT can inflict heavy damage long before the organization

knows it has been damaged [۳۹]. While victim organizations vary in size, type, and industry, the people targeted by

APT usually have the same characteristics: the people with the highest level of access to the most valuable assets and resources [٤٠].

Advanced Persistent Threat Features

The Advanced Persistent Threat was developed by the United States Air Force (USAF) in ۲۰۰٦. [۷] The components of the term are described below: Advanced means that the enemy can operate in the full range of computer intrusion. They can take the most advantage of the known vulnerabilities. Persistent means that the enemy is formally tasked with carrying out the mission. They receive directives as an information unit and work to satisfy their commander. Persistent does not necessarily mean that they have to constantly use malicious code on the victim's computers, but that they maintain the level of interaction needed to accomplish their goals. The enemy here is Threat because it is organized, budgeted, and motivated. [۸] The Threat is mostly related to the human factor and well-organized groups. APT attackers are usually teams of IT professionals and their clients - usually governments - who use advanced technology and obscure points of attack to obtain vulnerable data. [۲٦]
The differences between APT attacks and traditional web application threats include the following:
-An APT attack requires more resources than a standard Web application attack. The perpetrators are usually teams of experienced cybercriminals with significant financial support. Some APT attacks are government-sponsored and used as weapons of cyber warfare.
-APT attacks are significantly more complex.
-APT attacks stay on a network to gain the most information possible and do not attack immediately.
-APT attacks often target the entire network rather than a specific segment. [۹]

The main actors of APT

The main actors can be divided into two major groups of government actors and organized criminal groups. Governments cyberattacks are becoming more frequent. Suspicion of interfering in elections or power outages in other countries due to the high cyber capabilities of these actors has caused widespread concern among the people. The following is a brief description of these APT actors.
China: Chinese cyberattacks focus on industrial espionage aimed at stealing intellectual property. APT has been the actor's most enduring cyber threat. [۱۰]
United States: The actor has carried out the most sophisticated cyberattacks and used the most advanced technologies. APT attacks have been used mainly to pursue geopolitical interests. An example is the world-famous Stuxnet۱۰ operation, which targeted SCADA systems to cause significant damage to Iran's nuclear program. [۱۱]
Russia: This actor is supported by the government in terms of APT activities. Microsoft has detected and reported spear phishing attacks by this player through APT۲۸. Their targets were German government employees. The group has tried to gain access to employee information and infected sites with malware. [۱۲]
North Korea: Cyber-groups affiliated with the actor have carried out numerous operations, including routine espionage, bank hacking, and malicious attacks. [۱۳]
Israel: The actor is known as one of the possible authors of the Stuxnet۱۰ attack. This is known as the high potential of the country's intelligence services. The Duqu ۲,۰ attack was sponsored by the actor and has infected many systems in several countries in recent years. [۱٤] The malware used zero day vulnerabilities to send data to command-and-control servers.

The most famous APT groups

APT attacks are usually named by the teams that designed them. Some of the most famous and active of these groups are:

• Ghost Net

The group was based in China and their attacks were carried out by phishing emails containing malware. The group risked computers by focusing on access to government networks and embassies in more than ۱۰۰ countries. The attackers turned on their cameras and microphones with machines inside these organizations and turned them into

surveillance devices. [۱۵]

• Stuxnet
The worm used to attack Iran's nuclear program, which was carried through an infected USB device and damaged the centrifuges used to enrich uranium. Stuxnet is malware that targets SCADA systems (industrial control and monitoring) and was able to disrupt the operation of machines in the nuclear program without the knowledge of the operators. [۱۶]
Stuxnet caused installation damage by targeting programmable logic controllers in industrial control systems that manage uranium enrichment centrifuges. [۳۰]

• FIN۴
Cybersecurity company FireEye has revealed that more than ۱۰۰ companies have been hacked by Wall Street hackers through their email accounts since mid-۲۰۱۳ to exploit information about their activities in the stock market.
Citing the victims, FireEye said most of them were pharmaceutical and healthcare companies, bankers and lawyers who "regularly discuss confidential and volatile market information." [۱۷]

• APT۲۹
The US Cyber Security and Infrastructure Agency says the APT Group has used more than one primary access vector to target US government agencies. The attacks initially targeted a software service provider called Solar Winds done. By installing a backdoor on one of the company's popular software called Orion, hackers were able to infiltrate all the organizations that used this software. Orion software is installed on the servers of many private and public companies and therefore, infecting it allowed hackers to infiltrate their computer systems as well. CISA investigations in the United States show that hackers have hacked into the computer networks of dozens of private companies and government agencies in this way. Has been present in the networks of these organizations for a long time. [۱۸]

• Flame
Another APT first detected in ۲۰۱۲ is Flame, which appears to have been active for years and has compromised thousands of Windows systems in the Middle East, given its small size. Less than ۲۰ MB, this statistic is impressive. [۳۰]

• Red October virus
Red October is another APT identified in ۲۰۱۲ that targeted government and industrial centers, especially in Russian-speaking countries, for political espionage and IP theft. [۳۱] The virus spreads through targeted emails containing malicious Word and Excel files within the system and can steal information from computers and smartphones. Virus scanning activities include logging, tracking emails and recovering detected files. [۳۰]

C. APT Life Cycle Analysis
Life cycle is essential for understanding how APT attacks work and identifying the most common malicious techniques. There are several ways in which an APT attack uses its resources for anonymity. In recent years, researchers have proposed multi-stage, organized life cycles. These steps consist of the techniques, methods, and tools used to perform a targeted infiltration. A life cycle can be organized from three stages to eleven stages. [۱۹]

Three-staged attack

In the paper [۱۹], a general approach to APT attack in three stages is presented. These steps are:

۱- Initial agreement: At this stage, attackers try to access the target system. The most common techniques used at this stage are spear phishing, server-side attacks, and infected storage devices.

Lateral movement: Attackers try to compromise other services in the target system or network. Some of the techniques used are standard operating system tools such as Powershell and RDP that use a vulnerability.

۳- Command-and-control: When the system is compromised, it is necessary to create an external connection to filter the data. Attackers use services such as HTTP, HTTPS or FTP. They can also use tools such as remote connection tools such as VNC or RDP.

Four-staged attack

In the paper [۲۰], a four-stage model of APT attack is presented. The following steps are described:

۱- Influence on the target
In the first stage, it is necessary to penetrate the target. Companies or organizations are usually hacked in one of the following ways: Web assets, network resources, and users. This can be achieved either through malicious downloads (eg RFI injection, SQL) or social engineering attacks (eg phishing and email attachments) which are threats that large organizations regularly face. These intruders may simultaneously launch a DDoS attack against their target.

۲- **Insert malware**
After gaining initial access, attackers quickly install the backdoor. Malware that allows access to the network and allows remote encryption operations, provide more space for their activities and somehow increase the platform for the expansion of activities. On the back it can also be a trojan and appear as a legitimate software.
۳- Expansion
At this point, it is time for attackers to deepen their access to the target system and increase the means of penetration to gain more control over the target. They will also work on creating tunnels to transfer the data they need later.

Depending on the ultimate goal of the attack, the collected data can be sold to a competing company, the data can be modified to sabotage a company's product line, or it can be used to overthrow the entire organization. If the motive is sabotage, this step is used to precisely control multiple vital functions and manipulate them in a specific sequence to see the most damage. For example, attackers could delete the entire company database and then disrupt network communications to prolong the recovery process.

D. Exploration and extraction of data
Once attackers gain deeper access to the system, they can discover the information and data they need and transfer it to another location within the network, compress it and transfer it through the tunnels they have created. In the same way, they continue to expand, discovering and transmitting more data.

At this point, the target is officially compromised. When data is stored in a secure location on the network and is often encrypted by an attacker. White noise methods are commonly used to get the attention of security teams to get information out.

Five-staged attack

In this work [۲۱], a model for analyzing the APT life cycle, which is organized in five stages, is presented. This model is called the "attack chain". The five steps are as follows:

۱- Delivery: Javelin phishing is used to send emails to recipients within the network.
۲- Exploitation: The vulnerability of services, systems or programs is used.
۳- Installation: At this stage, it is possible to install malware such as RAT (Remote Access Tool).
٤- Command-and-control: The remote attacker has access to a damaged host or server.

٥- Measures: Measures taken include accessing other hosts or servers on the same network to extract confidential information.

Six-staged attack
The authors in articles [۲۲] and [۲۳] have proposed a six-step life cycle model to describe the APT attack. This model emphasizes that attackers must deceive the person to run the malware and take advantage of any zero-day vulnerabilities. The attackers then gain access to the network through a compromised computer. The six stages of this life cycle are as follows:

۱- Gathering information: The purpose of this step is to gather information about the structure of the target organization or company through public social network profiles.
۲. Point of entry: Social engineering, spear phishing, and zero-day exploitation are the most commonly used

techniques for the victim that allow the attacker to access the computer.
۳- Command and control server: The attacker accesses the command-and-control server by communicating with the host at risk.
٤- Lateral movement: The attacker can access the vulnerable host by moving in the network.
٥. Important data: Important information about hosts or servers is specified.
٦- External server: Important and vital data is transferred to the command-and-control servers of the attackers.

Seven-staged attack

In the paper [٢٤], a general approach to APT attack in seven stages is presented. These steps are:
١. Investigation: Attackers seek public information about the victim.
٢. Preparation: Attackers prepare the initial attack to exploit vulnerabilities using network scans to create custom exploits.
٣. Infiltration: Attackers make the first attack, which usually involves spear phishing.
٤. Network Conquest: Remote access tools or backdoors are used to control the system when the attacker has at least one host to attack.
٥. Hide presence: The attacker seeks to remain hidden in the network for a long time.
٦. Data collection: The attacker seeks the data he wants and hides it as legal traffic to be extracted slowly.
٧. Maintaining access: The attacker can modify or create abuses, remote access tools and command and control servers for long-term access to the network.

Eight-staged attack

In the paper [٢٥], a general approach to the APT attack in eight steps is presented. These steps are:

١- Initial cognition: In this stage, the initial cognition of the goal is done.
Initial agreement: Describes the methods used to first penetrate the target, for example: spear phishing.
٣- Stabilization: At this stage, it ensures control of the target outside the network.
٤- Access development: The attacker is looking for documents that allow access to more resources in the system.
٥- Internal recognition: At this stage, the attacker gathers all possible information about the victim.
٦- Lateral movement: The attacker can access the resources.
٧- Preserving the presence: The attacker takes actions that stay in the network for a long time without being detected.
٨- Completion of the mission: The information to be sent to the command and control servers is compressed.

Eleven-staged attack
In the paper [١], a general approach to the APT attack in eleven stages is presented. These steps are:

١- Initial access: In this step, the initial contact with the target is made.
٢- Stability: The attacker seeks to achieve the goal for a long time.
٣- Development of access: Development of access to confidential data by installing malware on the network is essential.
٤- Discovery: includes access to target information such as location or username.
٥- Lateral movement: refers to how the attacker moves in the network to search for important vulnerable information or services.
٦- Collection: In this step, relevant information is collected.
٧- Extraction: In this step, the collected data is extracted.
٨- Execution: Malware is executed through remote connection.
٩- Escape from defense: includes not being recognized by defense mechanisms such as firewalls.
١٠- Access to credentials: Gets full access to the credentials of the system at
risk.
١١- Command and control: Creating a command-and-control channel to communicate with attacking servers and compromised systems is the goal.

E. Detecting APT Attacks

Although APT attacks can be difficult to detect, and even more so when they successfully enter a target network, data theft is not completely secret. In most cases, APT starts with a standalone malware such as rootkit, which emails an affiliate member of the target organization. If this member opens their email attachment, they will launch a cyberattack anonymously. This is considered a kind of social engineering, which is one of the common methods through which attackers use an internal member to infiltrate the defense system of the company or organization [۲۸]. APT attacks pose a dangerous threat to networks, and current diagnostic programs and actions fail to detect many APT attacks. Apart from high manpower skills, malware is very important in the success of APT [۲۹].
These attacks can be identified by detecting abnormal behavior in the organization's outbound traffic - which may be the best possible way. Organizations can detect symptoms by continuous monitoring and security controls. Some of these symptoms include:
• Unusual and suspicious activity in user accounts (especially high access accounts)
• Extensive use of malware on the back (to maintain access)
Suspicious and unusual activity in databases.
• Detects anomalies in information when leaving the network
The series of complex and persistent network penetration attacks consist of several intangible and covert stages. One of the reasons for the inefficiency of intrusion detection systems against these attacks is the use of defense mechanisms based on low-level network traffic analysis, which does not pay attention to the hidden relationships between alerts [٤١].

F.Ways to deal with APT attacks

APTs have the resources, perseverance, and skills to design sophisticated attacks and to overcome defense systems and prevent recognition. The network of many companies has been attacked and robbed while even the company itself is unaware of this issue. APTs have become a serious threat to cyber security by taking advantage of poor coordination and poor implementation of corporate cybersecurity measures. Poor defense means that APTs can always successfully penetrate the network and steal its information without the victim realizing it. Most companies are attacked when they find out that months have passed since the attack, and it is usually a third-party company that notifies them. Most successful attacks require only basic techniques, and most of them can be stopped only with the consistent and consistent use of relatively basic preventive measures. One of the reasons that cybercrime has become so widespread is that attackers do not have to put much effort into a successful attack.

The most successful form of APT defense is continuous monitoring and response to most APT efforts. Defense strategies based on one or two APT levels are not enough. In most cases, anti-virus software has not been a barrier to APT attacks. Therefore, first-generation security tools are not valuable enough to protect targets, and other prevention systems do not guarantee protection [۳۲]. Experts acknowledge that "any effective approach to defense against APTs should include deep defense, reconnaissance, disaster response plan, recovery plan, awareness and security training" [۳۳].

The main tool for counteracting APT attacks is a set of basic methods that limit the relatively simple elements of the APT process. When APT is broken down into its basic elements, it is usually known and easy to deal with. It is their combination that makes it difficult to defend against the APT. This is why even the best network security tools, including proxy servers, firewalls, VPNs and antivirus software, cannot defend against APT alone. Primary protection methods include implementing a vulnerability management process, system updates, and intrusion testing. These should be complemented by detailed documentation of the impact and risk assessment. Determining vital resources and elements of the need for special protection is very important for commercial purposes [۳۳].
Today, two main types of APT defense can be distinguished: hardware and cloud[۳٤]. In the first case, a dedicated device is placed on the edge of the protected network and monitors and reports suspicious traffic based on indicators (does not block real-time transmission). More advanced models perform behavioral analysis and sandboxing. Hardware-based solutions have certain limitations. Despite the high costs - which limit their number and limit their use to large companies, especially for models that control encrypted traffic - due to the increasing use of mobile devices and Remote workstations, these devices are not able to fully record network traffic. The hardware approach is replaced by a comprehensive analysis (behavioral, vulnerabilities, address filtering, SSL transfer monitoring, active content, etc.).

Monitoring the organization's incoming and outgoing traffic is the best way to prevent the installation of backdoors and prevent the extraction of stolen data. Inspection of traffic within the network environment can also alert security experts to any unusual behavior that may indicate malicious activity.

The Web Application Firewall (WAF), located on the edge of the network, filters traffic to Web application servers, thus protecting one of the application's most vulnerable levels from attack. In WAF, it can help eliminate application layer attacks (such as RFI injection attacks) and SQL, which are commonly used in the APT penetration phase.

Internal traffic monitoring services (such as network firewalls) are the other side of the equation. Finally, incoming traffic control services can be useful for detecting and removing backdoors. These cases can be detected by tracking remote requests from operators [۳۵].

A whitelist is a way to control domains that can be accessed over a network, as well as applications that can be accessed by users. This is another useful way to reduce the success rate of APT attacks by minimizing available attack levels.
However, malicious files are usually entered as legal software. In addition, older versions of software products are vulnerable to compromise and unauthorized exploitation. To have an effective whitelist, strict update policies must be in place to ensure that users always have the latest version of any application running in the list [۳۶].

For criminals, ordinary users are usually the biggest and most vulnerable from a security perspective. Potential targets fall into one of three categories:

• Careless users who ignore network security policies and unknowingly allow access to potential threats.
• Malicious insiders who intentionally abuse their credentials to gain access to the offender.
• Endangered users whose network access is compromised and used by attackers.

Access level control: Classifying data as needed helps block the intruder's ability to convert login credentials from a low-level employee to a high-level user. The main points of access to the network must be secured by two-factor authentication. Therefore, users need to use two-factor authentication (typically the passcode sent to the user's mobile device) when accessing sensitive areas. Thus, unauthorized attackers trying to identify themselves as legitimate users will not be able to access the network [۳۷].

In addition to the following, [۳۸] are the steps that must be taken when securing the network:

• Install security patches for networked software and operating system vulnerabilities as soon as possible
• Encrypt telecommunications to prevent attacker intrusion
• Filter incoming emails to prevent Email spam and Fishing attacks
• Use security operations centers to quickly record security events to help improve whitelists and other security policies
• Regular scans to identify back doors

Given that cyber-attacks, including APT attacks, are spreading day by day, it is necessary to ensure that all anti-virus software and programs used in the organization are up-to-date and in order to prevent any abnormal behaviors such as unexpected traffic, suspicious logins, malicious events, and data theft can be periodically identified by running a Penetration test for vulnerabilities and appropriate security measures taken to address them as soon as possible[٤١].

G.CONCLUSION:

Cyber threats have been a major concern since the advent of the information age, but the biggest concern is the latest category of threats known as Advanced Persistent Threat (APT). This has attracted increasing attention from security researchers around the world. APTs are sophisticated cyberattacks carried out by sophisticated enemies with sufficient capabilities and targeting specific information in companies, organizations and government. APT is a long-term campaign that includes various stages. This form of attack, if successful, will have significant consequences for countries and large organizations, which can range from financial loss to credibility. This article briefly describes APT, its description and features, life cycle analysis of APT attacks, identification and ways to deal with them. This study also highlights and recommends security tips and countermeasures that can help reduce APTs.

REFERENCES

[۱] Swisscom. Targeted Attacks Cyber Security Report ۲۰۱۹; Technical report; Swisscom (Switzerland) Ltd. Group Security: Bern, Switzerland, ۲۰۱۹.
[۲] Lemay, A.; Calvet, J.; Menet, F.; Fernandez, J.M. Survey of publicly available reports on advanced persistent threat actors. Comput. Secur. ۲۰۱۸, ۷۲, ۲۶–۵۹.
[۳] Cox, C. (۲۰۱۵). Cyber capabilities and intent of terrorist forces. Information Security Journal: A Global Perspective, ۲٤(۱-۳), ۳۱-۳۸.
[٤] Threat Intelligence Team, M.L. APT۳٦ Jumps on the Coronavirus Bandwagon, Delivers Crimson RAT. Available online: https://blog.malwarebytes.com/threat-analysis/۲۰۲۰/۰۳/apt۳٦-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/ (accessed on ۱٦ March ۲۰۲۰).
[٥] Gajewski, M., „Cyberataki typu APT nowym frontem wojny", Chip.pl, ۲۰۱۳, http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa /۲۰۱۳/۰۳/cyberataki-typu-apt-nowym-frontem-wojny.
[٦] Falliere, N.; Murchu, L.O.; Chien, E. W۳۲. stuxnet dossier. White Pap. Symantec Corp., Secur. Response ۲۰۱۱, ٥, ۲۹.
[۷] Jeun, I.; Lee, Y.; Won, D. A Practical Study on Advanced Persistent Threats. Commun. Multimed. Secur. ۲۰۱۲, ۸۷۳٥, ۱٤٤–۱٥۲.
[۸] Chen, P.; Desmet, L.; Huygens, C. A Study on Advanced Persistent Threats. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin, Germany, ۲۰۱٤; Volume ۸۷۳٥ LNCS, pp. ٦۳–۷۲.
[۹] Threat Intelligence Team, M.L. APT۳٦ Jumps on the Coronavirus Bandwagon, Delivers Crimson RAT. Available online: https://blog.malwarebytes.com/threat-analysis/۲۰۲۰/۰۳/apt۳٦-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/ (accessed on ۱٦ March ۲۰۲۰).
[۱۰]Mandiant. APT۱ Exposing One of China's Cyber Espionage Units; Technical report; Mandiant: Alexandria, VA, USA, ۲۰۱۳.
[۱۱]Kim Zetter. Researchers connect flame to us-israel stuxnet attack. http://www. wired.com/۲۰۱۲/۰٦/flame-tied-to-stuxnet/. Accessed: ۲۰۱٥-۰۱-۲۹.
[۱۲]ThaiCERT. Threat Group Cards: A Threat Actor Encyclopedia. Available online: https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf (accessed on ۲٤ June ۲۰۱۹).
[۱۳]Fireeye. M-Trends ۲۰۱۹: Fireeye Mandiant Services Special Report; Technical report; Fireeye: Milpitas, CA, USA, ۲۰۱۹.
[۱٤]Kasperky Lab. The Duqu ۲,۰-Technical Details (V۲,۱); Technical Report; Kasperky Lab: Moscow, Russia, ۲۰۱٥.
[۱٥]Bhadane, A.; Mane, S.B. Detecting lateral spear phishing attacks in organisations. IET Inf. Secur. ۲۰۱۹, ۱۳, ۱۳۳–۱٤۰.
[۱٦]Lamprakis, P.; Dargenio, R.; Gugelmann, D.; Lenders, V.; Happe, M.; Vanbever, L. Unsupervised Detection of APT C&C Channels using Web Request Graphs. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin, Germany, ۲۰۱۷; Volume ۱۰۳۲۷ LNCS, pp. ۳٦٦–۳۸۷.
[۱۷]Geluvaraj, B.; Satwik, P.M.; Ashok Kumar, T.A. The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. In Lecture Notes on Data Engineering and Communications Technologies; Springer Singapore: Singapore, ۲۰۱۹; Volume ۱٥, pp. ۷۳۹–۷٤۷._٦۷.
[۱۸]Kaspersky Lab. Targeted Cyberattacks LOGBOOK; Kasperky Lab: Moscow, Russia, ۲۰۱۹.
[۱۹]Ussath, M.; Jaeger, D.; Cheng, F.; Meinel, C. Advanced persistent threats: Behind the scenes. In Proceedings of the ۲۰۱٦ Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, ۱٦–۱۸ March ۲۰۱٦; pp. ۱۸۱–۱۸٦.
[۲۰]Zhang, R.; Huo, Y.; Liu, J.; Weng, F. Constructing APT Attack Scenarios Based on Intrusion Kill Chain and Fuzzy Clustering. Secur. Commun. Netw. ۲۰۱۷, ۲۰۱۷, ۱–۹.
[۲۱]Sexton, J.; Storlie, C.; Neil, J. Attack chain detection. Stat. Anal. Data Min. ASA Data Sci. J. ۲۰۱٥, ۸, ۳٥۳–۳٦۳.
[۲۲]Ghafir, I.; Prenosil, V. Proposed Approach for Targeted Attacks Detection. Lect. Notes Electr. Eng. ۲۰۱٦, ۳٦۲, ۷۳–۸۰._۷.
[۲۳]Trend Micro. The Custom Defense Against Targeted Attacks; Technical report; Trend Micro: Tokyo, Japan, ۲۰۱۳.
[۲٤]Vukalovic, J.; Delija, D. Advanced Persistent Threats-detection and defense. In Proceedings of the ۲۰۱٥

۳۸th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, ۲۵–۲۹ May ۲۰۱۵; pp. ۱۳۲٤–۱۳۳۰.
[۲۵]Lockheed Martin. Cyber Kill Chain; Lockheed Martin: Bethesda, MD, USA, ۲۰۰۹.
[۲٦]Wang, D.; Xu, J. Principal Component Analysis in the local differential privacy model. Theor. Comput. Sci. ۲۰۲۰, ۸۰۹, ۲۹٦–۳۱۲.
[۲۷]Centre, N. C. S. (۲۰۱۹) APT. National Cyber Security Centre.
[۲۸]J. De Vries, H. Hoogstraaten, J. van den Berg, and S. Daskapan. "Systems for Detecting Advanced Persistent Threats: A Development Roadmap Using Intelligent Data Analysis". In ۲۰۱۲ International Conference on Cyber Security (CyberSecurity), pages ٥٤-٦۱.
[۲۹]P. Bhatt, E. Toshiro Yano, and P. Gustavsson. "Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks". In ۲۰۱٤ IEEE ۸th International Symposium on Service Oriented System Engineering (SOSE), pages ۳۹۰-۳۹٥.
[۳۰]N. Virvilis, D. Gritzalis, and T. Apostolopoulos. "Trusted Computing vs. Advanced Persistent Threats: Can a Defender Win This Game?". In Ubiquitous Intelligence and Computing, ۲۰۱۳ IEEE ۱۰th International Conference on and ۱۰th International Conference on Autonomic and Trusted Computing (UIC/ATC), pages ۳۹٦-٤۰۳.
[۳۱]Verizon. "۲۰۱٤ Data Breach Investigations Report".Retrieved from http://www.verizonenterprise.com/DBIR/۲۰
[۳۲]۱٤/reports/rp Verizon-DBIR-۲۰۱٤ en xg.pdf, ۲۰۱٤.
[۳۳]I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, ۲۰۱۷.
[۳٤]Ashford W., "How to combat advanced persistent threats: APT strategies to protect your organization", ۲۰۱٦, http://www. computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation.
[۳٥]Rot A., "Zarządzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki", Projektowanie i realizacja systemow informatycznych zarzadzania. Wybrane aspekty, Komorowski T.M., Swacha J. (eds.), Polish Information Processing Society PTI, Warsaw ۲۰۱٦.
[۳٦]Quintero-Bonilla, S.; del Rey, A.M. Proposed models for advanced persistent threat detection: A review. Adv. Intell. Syst. Comput. ۲۰۲۰, ۱۰۰٤, ۱٤۱–۱٤۸.
[۳۷]Aparicio-navarro, F.J.; Kyriakopoulos, K.G.; Ghafir, I.; Lambotharan, S.; Chambers, J.A.; Technology, F. Multi-Stage Attack Detection Using Contextual Information; Loughborough University: Loughborough, UK, ۲۰۱۸; pp. ۹۲۰–۹۲٥.
[۳۸]Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. DFA-AD: A distributed framework architecture for the detection of advanced persistent threats. Clust. Comput. ۲۰۱۷, ۲۰, ٥۹۷–٦۰۹.
[۳۹]Singh, S., Sharma, P. K., Moon, S. Y., Moon, D. and Park, J. H. (۲۰۱۹) A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing ۷٥ (۸), ٤٥٤۳-٤٥۷٤.
[٤۰]U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, "An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, ۲۰۱۷.
[٤۱]Shenwen, L.; Yingbo, L.; Xiongjie, D. Study and research of APT detection technology based on big data processing architecture. In Proceedings of the ۲۰۱٥ IEEE ٥th International Conference on Electronics Information and Emergency Communication, Beijing, China, ۱٤–۱٦ May ۲۰۱٥; pp. ۳۱۳–۳۱٦.
[٤۲]Chen, J., Su, C., Yeh, K.-H. and Yung, M. (۲۰۱۸) Special Issue on Advanced Persistent Threat. Future Generation Computer Systems ۷۹, ۲٤۳-۲٤٦.