ISSN: 2977-0041

Research Article

Journal of Material Sciences and Engineering Technology

Advanced Persistent Threats Detection Through Machine Learning Techniques

Pedro Ramos Brandão[1*] and José Inácio Gonçalves Rodrigues[2]

[1]*Full Professor, Instituto Superior de Tecnologias Avançadas (ISTEC), Lisbon, Portugal*
[2]*Master's Student in Informatics Instituto Superior de Tecnologias Avançadas (ISTEC), Lisbon, Portugal*

[*]**Corresponding author**
Pedro Ramos Brandão, Full Professor, Instituto Superior de Tecnologias Avançadas (ISTEC), Lisbon, Portugal.

Received: July 26, 2023; **Accepted:** August 02, 2023; **Published:** August 09, 2023

ABSTRACT
An Advanced Persistent Threat (APT) can be defined as a targeted and very sophisticated cyberattack. System administrations of all institutions need tools to help prevent this type of attack from happening. Several approaches have already been presented for providing solutions to this type of problem, based on the life cycle of the attack. In recent times, some Machine Learning practices have been implemented in an attempt to ensure improvements in the ability to find and mitigate these threats.

Keywords: APT, Advanced Persistent Threat, Cyberattacks, Machine Learning, Malware

Introduction

The establishment of security policies is one of the tasks of those responsible for computer and cyber security.

Internally, an organization uses these policies to define the steps to be followed for data management in its technological infrastructure. However, the use of obsolete equipment, security policies not regularly reviewed, software not updated or lack of awareness of employees, lead to security flaws and vulnerabilities that allow intrusion into organizations by attackers / hackers.

Today's existing conventional solutions cannot prevent cyber-attacks by criminals due to their high complexity, which have increasingly sophisticated tools, such as exploiting zero-day vulnerabilities or Denial of Service (DoS) attacks.

Today, Advanced Persistent Threat attacks pose a danger to all types of organizations around the world, whether public or private, and will continue to be so in the future [1].

This type of attack is a constant threat because it is extremely difficult to detect early. Usually attackers use different techniques, both to remain undetectable during long periods, as well as being able to escape efficiently.

There are large differences between an Advanced Persistent Threat (APT) and a "common" cyber-attack. The number of resources required to perform an attack is one of these differences.

Common cyberattacks are commonly targeted at organizations with poor or even non-existent cybersecurity policies. The purpose of these attacks is to steal information regarding a company's customers or financial activities. These attacks can usually be detected and the damage caused is not very significant [2].

On the other hand, APT focuses on larger organizations and industry sectors, causing very serious problems. Failure of essential services, intellectual property theft, and critical infrastructure destruction are some examples of the problems that can be caused by these attacks. It is very complicated to detect these attacks and the damage caused can be very critical.

In recent years, the number of identified cases of APTs has grown exponentially, although one of the main objectives of the attackers is to remain undetectable [3,4]. Several researchers have suggested different approaches in trying to perceive and detect this type of threat. It is perceived that the life cycle of this type of attack is a sign to understand how they work [5-7]. In addition, Machine Learning techniques allowed the collection and study of the tools used by attackers to improve the early detection of these attacks.

An example of the scope that an APT has, is the use that the attacker obtains from current affairs and that give rise to great interest in the population. A COVID-19 situation has given rise to the ideal panorama for launching several attacks. Health recommendations and information on the situation in different countries were used to attract users, using attack techniques such as spear-phishing, exploits with remote access tools and ransomware [8].

Methodology

APT is a type of long-range, long-running attack in which attackers seek to remain hidden without being found, for as long

Citation: Brandão PR, Rodrigues JIG. Advanced Persistent Threats Detection Through Machine Learning Techniques. J Mat Sci Eng Technol. 2023. 1(3): 1-7.
DOI: doi.org/10.61440/JMSET.2023.v1.12

as they can. Usually, this type of attack is carried out to be able to steal data from various types of institutions, public and private, and also from different sectors.

Thus, it is considered that currently, the Advanced Persistent Threats (APT) are virtually undetectable attacks.

Based on this assumption, we try to answer the following question: Is an Advanced Persistent Threat undetectable even using practices and techniques of Machine Learning or will it be possible to create defenses against this type of attack?

Thus, bibliographical research will be carried out, based on the characteristics of APT attacks and also on the attack detection capabilities, by Machine Learning technology, which understands the necessary concepts for the development of work.

Literature Review

Advanced Persistent Threat

An Advanced Persistent Threat (APT) is a type of attack that seeks to access information and communication systems in an unauthorized manner, trying to obtain confidential information or even cause harm to public or private entities [2,9].

After the emergence of Stuxnet, APT attacks became more careful and harmful, giving the notion of the ease that exists to penetrate computer systems, managing to avoid many of the sophisticated defense tools used in the protection of the computing environment [10].

Today, many of these threats remain undetected. When they are detected, they reappear with changes to achieve their goal; some examples are, FIN6, APT10, APT41 which were attacks that resulted in large losses of money, confidential information and intellectual property [11-13].

Features of an APT

Some United States Air Force (USAF) experts coined the term "advanced persistent threat" in 2006 to simplify the debate about intrusive activities with their civilian counterparts. In this way, the military managed to exchange ideas about the characteristics of this type of attack without having to reveal secret identities [9]. The USAF used the following terminology to identify an APT:

- **Advanced:** the enemy is familiar with intrusion tools and techniques, capable of developing custom exploits.
- **Persistent:** the enemy intends to fulfill a purpose, take orders and attack specific objectives.
- **Threat:** the enemy is coordinated, supported and motivated.

Attackers who use APTs have different intentions and goals than other criminals who use computers to commit their crimes, mainly because of the targeted nature of their attacks. Industrial, military, economic espionage, appropriation of technical and intellectual property, financial extortion and political manipulation are several examples of the objectives that attackers who use APTs have.

Briefly, the differences between an APT and a common malware attack are:

- **Definition**
  - o APT is a sophisticated, targeted and highly organized attack (e.g. Stuxnet);
  - o Malware is malicious software used to attack and disable any system (e.g. ransomware);
- **Attacker**
  - o APT - Government actors and organized criminal groups;
  - o Malware - A cracker (a hacker in illegal activities);
- **Target**
  - o APT - Diplomatic organizations, information technology industry and other sectors;
  - o Malware - Any personal or business computer;
- **Purpose**
  - o APT - Filter sensitive data or cause harm to a specific target;
  - o Malware - Personal recognition;
- **Attack Life Cycle**
  - o APT - Maintain persistence as possible using different ways;
  - o Malware - It ends when it is detected by security actions (e.g. antivirus software);

APT Attack Process

APTs can be described from different perspectives. Each APT attack is performed differently and is typically targeted at a specific victim or institution. Generally, the attack starts by trying to get an entry point into the network that it is intended to attack. The next step will be the creation of a communications network through personalized malware, which will allow attackers to maintain access and thus be able to inject malicious software into the attacked network. This malware sneaks around the system, looking for vulnerabilities it can exploit and infecting other hosts on the network. It is capable of multiplying, making copies of itself, in order to maintain persistence within the network it is attacking.

The APT malware manages to create other connections with the outside as it acquires access within the network and in this way is able to obtain as much information as possible. FireEye conducted research on APT1 and described an example of a lifecycle approach. In the analysis carried out on APT1, FireEye presented a report and in it demonstrated an eight-stage model of the life cycle of an APT attack:

1. Initial recognition,
2. Initial commitment,
3. Establish a foothold - after gaining access to the target, attackers use the gained access to further reconnaissance. They use malware to create networks of backdoors and tunnels to go undetected. APTs are able to use sophisticated malware techniques to cover their tracks.
4. Escalate Privileges - after gaining access to their target's network, APT attackers are able to obtain system access passwords to gain administrative rights. In this way, they can have more control of the system and deeper levels of access.
5. Internal Recognition,
6. Move laterally - after obtaining administrator rights, attackers can move within the target's network at will and attempt to access other servers and other secure areas of the network.

7. Maintain Presence - Attackers can remain undetected for long periods and can create a backdoor to gain access to the system at any other time they want.
8. Complete Mission.

It will not be necessary for the stages between point 3 (establish the support point) and point 8 (complete mission) to always occur in that order [14]. This report is known for identifying and understanding these types of threats.

As you discover some APT attacks, you can see that its structure can be different and that it changes according to the specific objective for which it was created. Its different forms of attack make it very difficult to detect them.

Methods and Techniques

APT attacks use different methods and techniques to achieve their goals. They usually start with an analysis and observation of the victim. Spear-phishing or emails, in conjunction with social engineering, are used in various situations to get the user/victim to transfer an infected file to their machine. After that, the attacker manages to penetrate the victim's machine and, through the organization's network, obtains access to the other computers connected to it.

The use of zero-day exploits and unknown infection vectors are the methods that best characterize the most "advanced" APT groups. With these methods, groups are able to attack various government institutions in different countries in order to steal confidential information and remain undetected for long periods of time.

Generally, the techniques used to carry out APT attacks can be combined or adjusted depending on the target to be attacked. Some examples of these techniques are:

- *Social engineering:* Manipulating people with privileged access, so that they compromise information systems, leading them to disclose personal information and thus being able to carry out malicious attacks through control and persuasion, as an alternative to random attacks [15].
- *Spear-phishing:* It is a technique that aims to collect confidential, financial information or even user credentials from a particular institution [16].
- *Watering hole:* It's a technique very similar to spear-phishing in which attacks are tailored to the 'victims' needs. Taking into account 'victims' personal interests, attackers try to get information from them [17].
- *Drive-by-download:* When a web page with malicious code is consulted, an unintentional download is performed and the malicious software contained therein is executed [18]. Malware is transferred "stealthily" without users noticing it, taking advantage of security flaws or integrated plugins such as ActiveX, Java/JavaScript or Adobe Flash player [19].

Assignment Problem

Attributing a cyberattack or a particular campaign to an actor is an increasingly complicated matter. It gets worse when trying to relate an APT to a group or state. IP addresses, emails or the malicious code used are some of the different pieces of evidence that experts analyze to be able to identify the attackers. It is customary for attackers to impersonate third parties in order to hide their illicit operations. This is called the "false flag concept". In recent years, attacks identified as having been carried out by government actors and organized groups have shown a significant increase. The main actors can be identified as government actors and organized criminal groups.

Machine Learning

Machine Learning (ML) is a branch of *Artificial Intelligence (AI)* that provides the computational process of automatically inferring and generalizing a learning model from sample data. ML seeks to find solutions to difficult-to-solve questions, through the use of algorithms and techniques to automate answers to complex problems that are difficult to solve through conventional programming methods. ML uses models with mathematical and statistical functions and techniques to trace data dependencies, causalities, and correlations between input and output data.

ML has several utilities that help solve day-to-day problems but also serve as support for those who have decisions to make. Generally, several researchers from different areas of knowledge are combined for its development. ML is capable of solving problems such as recommender systems, fake news detection, sentiment analysis, fraud detection systems, facial recognition, language translation and chatbots.

Techniques and Algorithms

Analyzing the type of data in cause, there are labeled data and unlabeled data. For a given question, if there is a correct answer then this data is considered labeled data. If the answer is unknown, then is considered unlabeled data. ML algorithms have the ability to learn from available data. The main ML models can be classified as supervised learning and unsupervised learning.

Supervised Learning

Supervised ML learning aims to build a model that generates evidence-based predictions in the presence of uncertainty. Its algorithms analyze a set of known input data and known responses to the input data (output) and train the model and generate analytical predictions in response to the new data. Weather forecasts are examples of the use of these algorithms.

In order to create predictive models, supervised learning uses classification and regression techniques. However, the most popular and used techniques for this type of learning are [20]:

- artificial neural networks;
- support vector machines;
- decision trees;
- bayesian networks;
- k-nearest neighbors;
- hidden markov models.

Unsupervised Learning

Unsupervised learning does not have a test or training dataset, as does supervised learning. It receives unlabeled data that is presented and later the model itself should be able to learn from them and also make predictions of future results [21].

When there is a large amount of unlabeled data required by the problem to be addressed, the best learning model is this one, which aims to find hidden patterns or specific structures in the data.

With unsupervised learning, inferences are obtained from data sets, which consist of input data without labeled responses. Dimensionality reduction (such as principal component analysis or PCA) and clustering techniques (e.g. k-means, fuzzy c-means and hierarchical) are used by this learning model to develop predictive models.

The detection and classification of unwanted emails or spam is one of the examples of application of this unattended ML model.

Role of Machine Learning in Cybersecurity Applications in APT Detection

Currently, targeted and massive attacks that can cause damage to the attacked institutions, such as the loss of confidential information, are commonplace.

Several researchers are looking to study different approaches for preventing or reducing the risk of attacks.

These investigators use some methods and techniques directly related to Machine Learning.

The large amount of data and the rapid progress of today's threats have made preventive measures require greater capacity for analysis and response, in the shortest possible time.

For this reason, automated tools have been created to assist cybersecurity administrators. Machine Learning techniques are useful tools in implementing cybersecurity.

Network traffic behavior models can be created to detect abnormal activities, reduce the number of false positives in alarms and detect threats in real time [22].

However, Machine Learning can be used to create attacks, for example, sending fraudulent emails or password cracking software [23].

Machine Learning applications in cybersecurity can be classified as follows [24]:

- **Detection:** tools that allow detecting abnormal behavior to generate alerts in real time and facilitate decision making.
- **Protection:** detects vulnerabilities to install security patches automatically.
- **Prediction:** Techniques and algorithms to predict attacks and develop anti-malware techniques.
- **Elimination:** automatic elimination of the threat.

Cybersecurity can be improved with the implementation of Machine Learning techniques and thus be a great help for system administrators of different organizations, in the search for unusual behavior in their networks, such as an APT.

There are certain approaches that are very relevant for the detection of APT and that should be taken into account, such as:

- Watch for unusual alert patterns to detect malicious payload-aware malware, known components, and remote-control activities.
- Monitoring suspicious outbound network traffic can display significant parameters such as infected computers, C&C centers and data filtering.
- Monitoring unexpected internal network traffic can reveal escalating privileges, lateral movement and malware propagation.

Some applications that use Machine Learning techniques are:

- **Spam and Phishing Detection:** Unsolicited emails from unknown senders with advertising or commercials are called Spam. Phishing is one of the most used forms of attack to create an entry point for the attacker into the target's network to attack. The victim is tricked into visiting a fraudulent website in order to steal their credentials. Phishing detection is increasingly complicated due to the evolution of evasion strategies used by attackers, such as open redirects to avoid spam filters [25,26]. Some Machine Learning classification techniques help in spam detection. It is necessary to define criteria that help to distinguish an authentic email from a fraudulent one, allowing the algorithm used to learn to recognize the origin of any email. Certain authors have proposed a scoring technique to detect side spear phishing emails using a combination of various resources and have created a practical, deployable, real-time detection system for such attacks [27].
- **Malware Detection:** Malware currently creates executable files that cause problems on a network's systems or steal data without users' knowledge. The malware communicates with a C&C server via randomly created IP addresses or URLs. Thus, creating blacklists is not an efficient method of fighting malware. For this reason, Machine Learning algorithms have been used to detect malicious communication addresses. Some researchers have proposed Machine Learning techniques for malware detection [28]. Some authors presented a new proposal to detect C&C channels used in APT attacks, which consisted of observing certain communication patterns in web browsing and thus identifying and detecting the malware used in these attacks [29]. A different approach aimed to detect malware by analyzing DNS traffic and malicious traffic by monitoring traffic at the network egress point [30].
- **Intrusion Detection:** by monitoring network traffic, it is possible to analyze data flows in search of unusual behavior patterns such as intrusion detection systems and intrusion prevention systems. This method can be divided into misuse and anomaly detection. Anomaly detection uses network modeling techniques and identification of abnormal behavior of the data flow in the network. Misuse detection uses signature-based (hash) techniques on known attacks to detect potential attacks [31]. Certain authors have reviewed the Machine Learning techniques used for these detection methods [32]. Other authors propose the detection of lateral movement based on anomalies in malicious sessions of Remote Desktop Protocol (RDP) in Windows operating systems, taking advantage of the system event logs, several Machine Learning techniques were evaluated in order to classify RDP sessions and detect malicious session entries [5].

Approaches used for APT Detection

In recent years there has been an exponential increase in the volume of data generated by information systems and all devices connected to the Internet, called Internet of Things (IoT). This increase has made it more difficult to detect malware and network attacks.

However, several approaches have been suggested to solve this type of problem. Examples of this are:

- dynamic analysis,
- context based,
- independent access,
- contextual information,
- information flow tracking [33-37].

It is urgent to analyze this data in the shortest possible time, in order to quickly detect an attack. As a result, researchers started using Machine Learning techniques to improve the true positive rate in detecting APT attacks [38].

It was presented in, a system based on Machine Learning called MLAPT [6]. This model uses ML algorithms to perform its analysis and thus managed to detect some APT attacks through early warnings that were created from a correlation structure between several detection modules. MLAPT is based on the analysis of a six-phase life cycle of the APT:

1. Intelligence collection,
2. Entry point,
3. C&C Communication,
4. Lateral Movement,
5. Asset/Data Discovery,
6. Data exfiltration.

The MLAPT framework works in three phases:

- **Threat Detection:** Network traffic is scanned by eight detection modules to find the techniques used by APT. The output of this phase consists of alerts, known as events.
- **Alert Correlation:** Events generated by detection modules are correlated and the output can be two types of alerts.
- **Attack Prediction:** A Machine Learning based prediction module is used to detect APT techniques.

Another framework for APT detection is DFA-AD [39]. It is a new distributed framework architecture, which classifies events in a distributed environment and relates them to detect techniques used by APT. Detects attacks in a distributed environment on the Trusted Platform Module (TPM).

There are three designed phases of the DFA-AD:

- **Network Traffic:** traffic flow is collected, processed and analyzed by a recognition method using Machine Learning algorithms.
- **Correlation Event:** through specific rules provided by an administrator, events generated in the previous phase are collected to be evaluated.
- **Alert Service** previous information is analyzed and alert is generated if an APT attack is detected.

APT Life Cycle Analysis

To understand the functioning of an APT attack, it is essential to understand its life cycle and identify the most used malicious techniques.

APT attacks use different resources to go undetected. Some researchers have proposed in recent years, life cycles organized in stages. These steps are made up of the techniques, methods, and tools used to carry out a targeted attack. The number of stages in a lifecycle varies according to the proposed approach; for example, a life cycle may consist of three stages to eleven stages [1,40].

There are similarities between the various proposed life cycles regarding the techniques and methods employed by attackers at each stage. Lifecycles with more stages are sometimes subdivisions of stages of shorter lifecycles, in order to be able to explain in more detail how the APT attack works. Each of these attacks has distinct attributes and multiple attacks can use identical lifecycles.

A New Proposal

Several lifecycles were recently chosen to write an APT attack. The tactics, techniques and procedures (TTP) used by attackers at each stage of these lifecycles were defined.

The IKC, CKC and chain of attack models were used as a basis for certain models described above.

Used as a basis for the seven-stage lifecycles analyzed, the CKC is a well-known model for this type of attack. For attack models with four to six stage lifecycles, the IKC was the preferred model.

After reviewing the proposed approaches, it was concluded that the initial steps are the study and analysis of the target. The next step is exploiting vulnerabilities to compromise one or more hosts of the target to attack. After that, the attackers perform the data extraction to a C&C server (command-and-control server), in a stealthy way. Mandiant (American cybersecurity company) reveals that when cleaning is performed as a final step, the attacked organization will possibly not realize that it has been attacked.

It should be noted that life cycles are analyzed to better understand how APT attacks work. However, attackers can use tailored TTPs to achieve their intended goals and use the steps in any non-predefined order.

Typically, APT attacks are targeted and carried out stealthily so that they are very difficult to detect early.

APT attacks can be considered passive or active actions, ranging from social engineering attacks to specific attacks such as unauthorized access to servers. Passive actions are all those that do not change data or that do not interfere with the transmission of information. Example of passive actions are port scanning techniques. Active actions are those that modify data or the flow of packets and also those that remove information. An example of these actions is distributed denial of service.

Machine Learning has techniques that provide solutions for analyzing large amounts of data, such as IDS alerts, logs or unauthorized remote connections. IT administrators use the help these scans provide to identify abnormal network behavior that could indicate inappropriate use of computer resources, common malware installed on a network host, or an APT attack.

With this model, it is intended to be able to detect early and efficiently APT attacks. However, some of these attacks are not

detected at one or several stages of their life cycle, so it is proposed that detection solutions are implemented from beginning to end of the active attack, with the help of ML techniques.

Reflection

Currently, one of the great values that organizations have is their data and the information contained in their databases. For this reason, it is not surprising that all institutions begin to invest more and more in the protection of these values.

However, in the same way that security policies have undergone significant evolution, with the development of new defense techniques and technologies, the methods of attack and invasion of business and government systems have also evolved considerably.

In addition to the more traditional methods of cybernetic attack, such as malware, in recent years it has been noticed that Advanced Persistent Threat (APT) are increasingly used in attacks. Despite the efforts made to prevent this type of attack and mitigate the damage that comes from these attacks, it is clear that organizations only realize that they have been attacked long after the attack has taken place.

One of the technologies in which a lot of trust has been placed to be able to detect this type of attack is Machine Learning. It is expected that through its techniques and also with algorithms capable of 'learning' to detect malicious code and abnormal network traffic, it will be able to prevent large-scale attacks with the possibility of causing very significant damage to the attacked institutions.

Conclusion

Advanced Persistent Threat (APT) are personalized, sophisticated, and targeted attacks. It is an attack method that should make all institutions concerned about the security of their data and their entire computer system.

Initially these attacks were aimed at high value targets, such as countries, government institutions or large corporations. However, in recent times, attacks have been carried out on smaller companies, which constitute the network of suppliers of these large corporations in order to gain access to their systems.

One of the major problems with APT attacks is the fact that you can never be absolutely sure that backdoors have not been active, even after the attack has been discovered and the threat is thought to be under control. These active backdoors can allow attackers to re-enter the system at any time.

Attackers can be classified as private actors or government actors. There are several techniques used by these actors to carry out an attack. As the attack progresses successfully, the techniques become more sophisticated.

The Machine Learning techniques and models frequently used in the detection of an APT attack are SVM, k-NN and DT.

We also analyzed the life cycles of an APT attack in which each cycle is formed by different stages. The stages of the different cycles have similarities that allow them to be grouped together, however they represent a non-linear order of attack behavior which means that it does not have to follow a predefined sequence in carrying out the attack. It was recommended to use ML techniques that gave good results.

This model has the advantage of considering the two types of life cycle stages: passive and active. In this way, it simplifies the behavior of an APT attack. It has the disadvantage of not being able to obtain the data sets for training the different Machine Learning algorithms.

Despite the great evolution that has been taking place with Machine Learning techniques, Advanced Persistent Threat continues to be the greatest danger to the computer security of public and private organizations around the world.

The major investment of all institutions will continue to be prevention, investing heavily in training all employees, motivating them to have responsible behavior that does not jeopardize access to their organizations IT systems.

References

1. SLG. Security 2019 Cyber Security Report. www.swisscom.ch Worblaufen - Bern. 2019.
2. Chen P, Desmete LC. Huygens, A Study on Advanced Persistent Threats. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Berlin, Germany: Springer. 2014.
3. Fire Eye I. Fireeye Mandiant Services Special Report; Technical report. FireEye, Inc., Milpitas, CA, USA. 2019.
4. Lemay A, Calvet J, Menete FJ, Fernandez M. Survey of publicly available reports on advanced persistent threat actors. Comput. Secur. 2018.
5. Bai T, Bian H, Daya AA, Salahuddin M, Limame N, et al. A Machine Learning Approach for RDP-based Lateral Movement Detection. IEEE - 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany. 2019.
6. Ghafir I, Hammoudeh M, Prenosil V, Han L, Hegarty R, et al. Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems. 2018.
7. Zhang R, Huo Y, Liue L, Weng F. Constructing APT Attack Scenarios Based on Intrusion Kill. Zhenxing Qian, Haidian District, Beijing, China. 2017.
8. Team TI. APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT. https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/. 2021.
9. Jeun I, Lee Y, Won D. A Practical Study on Advanced Persistent Threats. In: et al. Computer Applications for Security, Control and System Engineering. Communications in Computer and Information Science. Springer, Berlin, Heidelberg. 2012. 339.
10. Falliere N, Murchu LO, Chien E. APT Case Study - W32. Stuxnet Dossier. APT Case Study - W32.Stuxnet Dossier. 2012.
11. Eye IF. Follow the money: Dissecting the Operations of the Cyber Crime Group FIN6 - Technical Report. FireEye, Milpitas, CA, USA. 2016.

12. Coopers P. Operation Cloud Hopper; Technical report. PwC UK Cyber Security and Data privacy, London, UK. 2017.
13. Fire Eye I. Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation; Technical report. FireEye, Milpitas, CA, USA. 2019.
14. Mandiant. APT1 Exposing One of China's Cyber Espionage Units. Mandiant, VA, USA. 2013.
15. Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks," Journal of Information Security and Applications. 2015.
16. Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: A survey. Computers & Security. 2017.
17. Symantec. Internet Security Threat Report; Technical Report 2. Symantec, AZ, USA. 2016.
18. Tanaka Y, Akiyama M, Goto A. Analysis of malware download sites by focusing on time series variation of malware. Journal of Computational Science. 2017. 22: 301-313.
19. Paganini P. Turla APT group's espionage campaigns now employs Adobe Flash Installer and ingenious social engineering. https://www.cyberdefensemagazine.com/turla-apt-groups-espionage-campaigns-now-employs-adobe-flash-installer-and-ingenious-social-engineering/. 2018.
20. Dua S, Du X. Data Mining and Machine Learning in Cybersecurity, London, UK: Auerbach Publications. 2011.
21. Portugal I, Alencar P, Cowan D. The use of machine learning algorithms in recommender systems: A systematic review. Expert Systems with Applications. 2017.
22. Guan Z, Bian L, Shang T, Liu J. When Machine Learning meets Security Issues: A survey. EEE International Conference on Intelligence and Safety for Robotics (ISR). 2018.
23. Geluvaraj B, Satwik PM, Kumar TAA. The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace," Springer, Singapore. 2018.
24. Mohanty S, Vyas S. Cybersecurity and AI. In How to Compete Age Artificial Intelligence," Berkeley, CA, USA, Apress 143-153. 2018.
25. OWASP. Unvalidated Redirects and Forwards Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html. 2019.
26. Paganini P. Phishers continue to abuse Adobe and Google Open Redirects. https://securityaffairs.co/wordpress/91877/cyber-crime/adobe-google-open-redirects.html. 2019.
27. Bhadane A, Mane SB. Detecting lateral spear phishing attacks in organisations. 2019. 133-140.
28. Torres JM, Comesaña CI, García-Nieto PJ. Review: machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics 10: 2823-2836.
29. Lamprakis P, Dargenio R, Gugelmann D, Lenders V, Happe M, et al. Unsupervised Detection of APT C&C Channels using Web Request Graphs," em Lecture Notes in Computer Science book series (LNSC,volume 10327), Springer, Cham. 2017. 4: 6.
30. Zhao G, Xu K, Xu L, Wu B. Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis. IEEE Access. 2015. 3: 7.
31. Buczak AL, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials. 2015. 18: 1153-1176.
32. Liang F, Hatcher WG, Liao W, Gao W, Yu W. Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. IEEE Access. 2019. 7: 158126-158147.
33. Su Y, Li M, Tang C, Shen R. A Framework of APT Detection Based on Dynamic Analysis," em Proceedings of the 2015 4th National Conference on Electrical, Electronics and Computer Engineering, Xi'an, China. 2015. 1047-1053.
34. Giura P, Wang W. A Context-Based Detection Framework for Advanced Persistent Threats. Proceedings of the 2012 International Conference on Cyber Security, Washington, DC, USA, 2012 International Conference on Cyber Security. 2012. 69-74.
35. Xu W, Zheng K, Niu X, Wu B, Wu C. Detection of command and control in advanced persistent threat," em Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia. 2016. 1-6.
36. Aparicio-Navarro FJ, Kyriakopoulos KG, Ghafir I, Lambothar S. Multi-Stage Attack Detection Using Contextual Information," Loughborough, UK, MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM). 2018. 920-925.
37. Brogi G, Tong VVT. TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking. Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, IEEE. 2016.
38. Quintero-Bonilla S, Rey AM. Proposed models for advanced persistent threat detection: A review. Springer, Cham. 2020.
39. Sharma PK, Moon SY, Moon D, Park JH. DFA-AD: a distributed framework architecture for the detection of advanced persistent threats. Cluster Comput. 2017. 20: 597-609.
40. Ussath M, Jaeger D, Cheng F, Meinel C. Advanced persistent threats: Behind the scenes. Proceedings of the 2016 Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, IEEE. 2016. 181-186.