Evaluating Advanced Persistent Threats Mitigation Effects: A Review

Oluwasegun Adelaiye*, Aminat Ajibola**, Silas Faki*

*Department of Computer Science, Bingham University, Karu, Nassarawa State, Nigeria.
**Department of Computer Science, University of Huddersfield, United Kingdom.
Corresponding Author; e-mail: oluwasegun.adelaiye@binghamuni.edu.ng

ORCID ID: 0000-0002-4193-5641, 0000-0003-3387-6845, 0000-0002-0818-8314
Review Paper Received: 24.10.2018 Revised: 24.12.2018 Accepted: 24.12.2018

Abstract—Advanced Persistent Threat (APT) is a targeted attack method used by a sophisticated, determined and skilled adversary to maintain undetected access over an extended period for exfiltration of valuable data. APT poses high threat levels to organizations especially government organizations. 60% of the problem is the inability to detect penetration using traditional mitigation methods. Numerous researches indicate that vulnerabilities exists in most organizations and when exploited will have major fininacial implications and also affect the organizations reputation. Traditional methods for mitigating threats to information systems have proved ineffective. This paper aims at evaluating the utilization and effectiveness of Advanced Persistent Threat Mitigation techniques using existing literature and thereby providing a synopsis of APT. A method-based approach is adopted, reviewing the researches and a comparative analysis of the methods used in the mitigation of APT. The study compares 25 researches, which proposed methods in mitigating the threat. The research articles are filtered, separating mitigation methods from review articles, identifying the threats etc. from a wide range of research reports between 2011 and 2017. These 25 researches were analysed to show the effectiveness of 12 mitigation methods utilized by the researchers. In mitigating APT multiple methods are employed by 72% of the researchers. The major methods used in mitigating APT are Traffic/data analysis (30%), Pattern recognition (21%) and anomaly Detection (16%). These three methods work inline with providing effective internal audit, risk management and cooperate governance as highlighted in COBIT5 an IT management and governance framework by ISACA.

Keywords—Anomaly detection, Data exfiltration, Exploit, Pattern recognition, Traffic analysis, Zero-day.

1. Introduction

Information sharing and representation through digital means poses a great threat to data confidentiality for humans and warrants increase in security. Security is attaining a state where information and digital systems are free from undesired events, which may be loss of data, confidentiality, access, modification of data etc. These undesired events may be due to accidents or malign activities.

Over the years these security challenges have grown from attacks to a single node to distributed attacks. The effect of these adverse attacks not only

affects the availability of these machines but also confidential data, finances, aerospace, defence, education technological devices etc. Recently, attacks to information security has posed very serious risk to humans, costing an estimated 7.2million dollars per organization for every successful attack [4], [40].

Some of these attacks have been identified as special types of attacks, with improved difficulty in both preventing and detecting these types of attacks. This sophisticated attack method is referred to as Advanced Persistent Threat [28].

2. Advanced Persistent Threats

Advanced Persistent Threat (APT) is a stealthy, sophisticated attack by a group of skilled adversaries against a company, an organization or government. This type of attack is believed to be impossible to prevent, especially if the attacker is persistent as it takes several months to complete the attack process.

The National Institute for Science and Technology in 2008 defined Advanced Persistent Threat as; A malicious user with unlimited resources and a highly skilled expert giving a leverage in establishing a chance for a successful exploit. The adversary uses several attack methods, with the aim of creating a niche within the target organization. The ultimate aim of the attack is the stealing and exfiltration of sensitive information, creating an opportunity for future attacks and negatively affecting an organization's event or mission. Advanced persistent threats (APTs) makes multiple attempts over a lengthy time interval, mimicking the targets defenses in keeping a low profile so as to successfully complete the mission. [1], [62], [64]

APT thus refers to a developing trend of surreptitious and targeted attacks, utilizing multiple attack vectors and techniques, orchestrated in a stealthy manner so that an adversary can gain unauthorized access and have significant control of the target system undiscovered over a prolonged period [39], [57]. APT being a compound network attack rapidly evolves and spreads while constantly changing its infiltration techniques, posing great threats to organizations. Fuelled with the increased growth of Networked communities, APT like attacks has brought increased concern among IT security experts.

APT became very popular after a number of conspicuous attacks and persistent information security breaches reported by large global organizations in the military, financial, energy, nuclear, education, aerospace, telecommunication, chemical sectors, and government in 2011. A few well-publicized APT attacks are Stuxnet, RAS breach operations, Operation Aurora, Duqu, Ke3chang operation, Flame, Snow Man, Red October and Mini duke, with more recent attacks utilizing Olympic destroyer malware, Ratankba, ActiveX etc. [21], [26]. APTs are often associated with cyber-espionage activities, aiming to steal highly confidential information (e.g. trade secrets, Intellectual Property, national security data etc) for monetary gain or geared towards the sabotage of strategic infrastructure [21].

Unlike other forms of exploits, APTs are premeditated, repeated and stealthy attacks that target specific organizations as opposed to random individuals or regular system users. These sophisticated exploits might not seek instant gain, but rather try to gain surreptitious access over an extended period to extract confidential and important data needed to execute its objectives. These attacks are dynamic in the sense that they are capable of adapting to the defenders efforts, using both hardware devices and software tools to resist them. APT attacks use a systematic approach that often relies on social engineering as the main mechanism to gain unauthorized access to the target organization. Although Zero day approaches are largely utilized with APT

attacks, which refers to software vulnerabilities that are unknown. A recent study by Li, et al. [31] shows that 19% of reported APT cases utilized zero-day vulnerabilities, 70% used existing and known vulnerabilities, while 11% used vulnerabilities that are not yet known.

Although APT has drawn increased attention among security practitioners, there is a prevailing lack of understanding of the APT research problem. For instance, APT has put to test current anti-virus softwares and network/host intrusion detection systems because they majorly depend on known attack identities and patterns, APTs on the other hand are succesful because they utilize unknown vulnerabilities to bypass defensive efforts of the organization [32]. As a result, traditional defensive tools, methods and security controls often become ineffective when dealing with targeted APT-styled attacks [34]. Work done by reaserchers on APT [7], [9], [31], [52], [55] were majorly on; (a) Gaining knowledge and understanding the attributes of the attacks. (b) Building a model to illustrate the attack type in stages and (c) Identifying mitigation methods and proving its effectiveness.

3. Research Problem

The ineffectiveness of traditional mitigation techniques in preventing against APT has cost large organizations and government agencies the loss of valuable data. Most of the methods that have been created have not been effective in detecting and/or preventing APT activities in the user, application, network or physical plane. Most researchers have attributed the successes in these attacks to human vulnerability. The ability of these malwares to bypass security mechanisms show that vulnerabilities still exists even in the midst of existing technical mitigation techniques and thereby results in threats.

Recent studies have shown the difficulty in detecting Advanced Persistent Threats and the seriousness of APT is visible from the high profile attacks and exfiltration of data from sensitive organizations like RSA security, NASA, FBI, Sony, Citigroup, Fox broadcasting etc. [46]. These organizations had tradition security methods implemented but yet could not prevent the attack. Researchers have identified and looked into this problem, these largely relate to the inefficiency of traditional prevention and detection techniques in mitigating targeted attacks as highlighted in Figure 1 by [5], [12], [15], [19], [43], [51], [55], [62], [63], [65]. Increasing number of researchers have identified the low success rate in mitigating APT through traditional methods as highlighted in Figure 1. This is a problem and a hot issue in the research on information security in general and APT in particular.

This Study reviews published articles with the aim of identifying the strength and limitations of various methods for mitigating the vulnerabilities that exist in Advanced Persistent Threat attacks

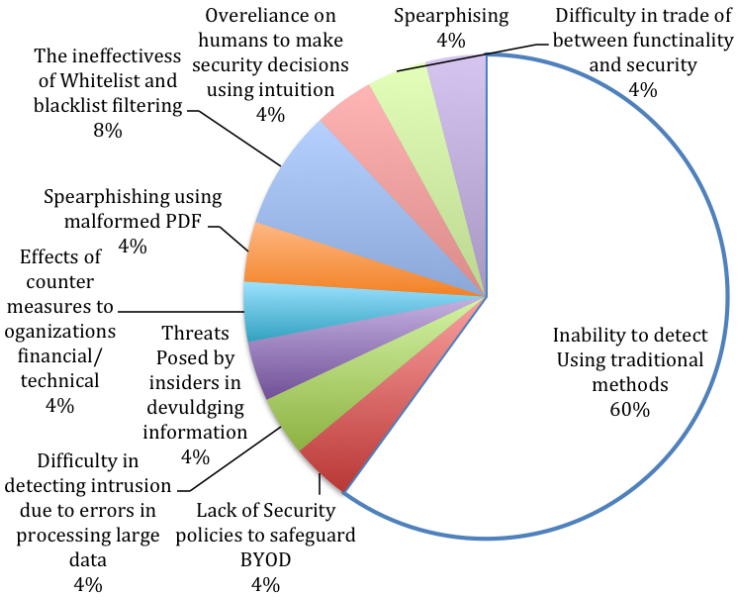

Fig. 1. A Pie Chart of Common Vulnerabilities Associated with APT Attacks

4. APT Attack Process

In 2006 the US Air Force described targeted, skilled, experienced, determined and stealthy attacks to organizations and termed it Advanced Persistent Threats [1], [3], [57]. Although this type of attacks have been occuring since 2003 [54], the attacks are seen as impossible to completely prevent hence, making organisations vulnerable.

The attack process has been categorized into an average of 7 stages by different authors and is illustrated in Figure 2.

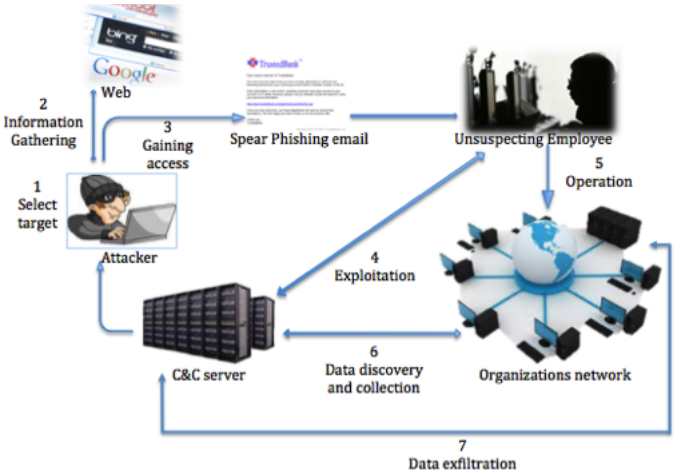

Fig. 2. APT attack process

4.1. Selecting A Target Organization

The APT attack method is more sophisticated than regular information attack methods that exist. APTs are well-planed and organized attacks targeted at selected organizations. The aim of this form of attack is to gain access to sensitive information and data [26]. Targets are selected based on data required or data of choice. The sensitivity of the data and its economical worth is taking into account. A large number of organizations posses data that would be of very high financial and economic value [4], [42].

The APT attacks that have happened are sometimes linked to government organizations trying to steal government secrets of other nations. This is the first phase of the seven phases of the APT attack process. [29]

4.2. Information Gathering

The attacker after narrowing down the target organization collects information about the target of choice. The information extracted at this point is very vital for the success of the attack. At this point the weakest link is taking into account, which has been proven to be the human factor [24], [45]. Many organizations adopt high security standards however, with a human present in the functioning of the system poses vulnerability in that organization [4].

The process used in gathering the information is referred to as reconnaissance. This can be subdivided into three parts [12]:

1 External reconnaissance
2 Internal reconnaissance
3 Gain access to the information.

4.3. Gaining Access

The information-gathering phase points the attacker to possible areas for intrusion. This phase is where the attacker gains access to the organization. At this point a malware usually a zero-day is used to penetrate the organizations network [3], [18].

This phase deals with using the information gathered from the reconnaissance phase to penetrate through the target organization's defences mostly through utilizing malware deliveries [9].Besides gaining access through the deployment of a zero day, there also exist alternative ways of gaining unauthorized access. The method used in gaining

access depends greatly on the outcome of the reconnaissance phase. Other popular methods by which an attacker can gain unauthorized access are: Spear-phishing, watering hole attack, USB etc. [9], [18]

4.4. Exploitation

Exploitation is the stage after a malicious application has been used to gain access usually through a zero day malware. This stage deals with establishing a connection with a Command and Control (C&C) server, which bypasses security by utilizing secure ports such as port 443 [18]. This stage uses legitimate tools and services to reduce suspicion and possible detection. This stage provides full exploitation of the organizations network as commands can be issued from a remote location to the target organization's information systems [37].

The C&C server is responsible for upgrading and updating the malware for better performance as well as issuing commands to compromised systems. Fast-flux DNS is a technique also adopted by a C&C server to aid in avoiding detection. This method prevents existing defence systems from detecting any unusual traffic to or from a single destination [1].

4.5. Operation

When a connection is established and secured with the C&C server, the earlier deployed malware tries to spread to other machines within the network firstly by scanning for vulnerable systems [18]. The attacker through the C&C server uses this method to gain access to a system with highly valuable information.

This phase involves some internal reconnaissance to aid in locating confidential data being sort after. At this point the detection of an intrusion in the system becomes very difficult. The malware at this point continuously mutates and changes its location, which aids the malware in easily evading detection.

The attacker also evades detection by using off-the-shelf products, exploiting existing features in operating systems and ultimately stealing access credentials and escalating privileges of highly confidential systems [9].

4.6. Data Discovery And Collection

Lateral movement of the malicious content around the organization creates a channel to transmit data out of the organization. At this point data of high value is located and collected to a single or fewer locations for easy exfiltration of the data out of the orgnization and to a remote location [18], [61].

4.7. Data Exfiltration

The ultimate purpose of APT is to gain access to valuable highly confidential information. This stage marks the end of the attack process and is the point where the attacker gets the desired information. The data is usually transferred using secured channels majorly SSL/TLS to evade detection and to hide the transmission process [9].

The losses at this point include data loss leading to loss of finances, customer data, access rights, intellectual property, trade secrets, intelligence information and other sensitive and vital information. [23], [66].

5. Methodology

The research is carried out using a method-based approach in line with a systematic literature review. This review methodology is exclusive to a particular question comprehensively sort for, using properly outlined procedures at each step, that would arrive

at the same results, if repeated [47]. Among the numerous researches into Advanced Persistent Threat, a filtering process is used to separate the articles on prevention and detection methods that defines the samples, from other articles on Advanced Persistent Threats. These articles are selected from publications between 2011 and 2017. The data collected from these articles are the authors name and year of publication, research title, method, findings and recommendations. The data collected is grouped into clusters to reflect the frequency of utilization for each method (Hult 2015). The results of the study are represented using tables and discussed in detail.

6. APT Mitigation Techniques

By mitigation we refer to reducing the adverse effect of unwanted events. There are many proposed methods for mitigating APT, a few common methods are:

1 Anomaly Detection
2 Whitelists
3 Blacklists
4 Intrusion Detection System (IDS)
5 Awareness
6 Deception
7 Cryptography
8 Traffic/ Data analysis
9 SIEM
10 Pattern Recognition
11 Risk assessment
12 Multi-layer security

Anomaly Detection: There is an expected behavioral pattern in network traffic, which is presumed to be normal. This method detects deviation from normal by detecting abnormal behavior. An anomaly detection system provides a baseline for normal network and system behavior. [36], [48]

Whitelists: This is when only a few well-known and trusted domains, applications, network traffic and processes are granted access while others are not considered. This only allows known processes which limits the system and does not consider unknown applications, processes, domains etc. whether it is genuine or non-genuine. [25], [68]

Blacklists: This is the mechanism used by traditional preventive methods. This is a list of know malicious applications and processes which identifies and blocks their operations. This method is the opposite of whitelist and can only prevent preknown attack types [14].

Intrusion Detection System (IDS): This is a method in detecting intrusions based on analysis of service ports, protocols, IP addresses, system events, system calls etc. This is aimed at alerting the user/ administrator of a suspected breach in the system. These systems are either host based or network based [16].

Awareness: Most cases of security breaches exploits the human factor in the security chain. This chain consists of various components and also humans, who interact directly with the system. The human brain can be skilfully manipulated, this is a threat to information systems. Since these interactions cannot be avoided, it is important to sensitize the users, of the risks and importance of confidentiality [50]. This is also an assessment of the users level of knowledge and understanding of information security and its implications [6].

Deception: This is the art of truth bias to prevent suspicion, which is mostly done through devices that hide their true identity. An attacker is made to believe his efforts are paying off by granting him access to a dummy system or honey device and keep him busy until he is tracked [44], [56].

Cryptography: This is the art of secret writing, changing information to a format that cannot be

understood. This method is used when the adversary is able to gain unauthorized access to information; in this case the attacker would not be able to understand it. [7], [49].

Traffic/ Data analysis: This is the use of statistical methods to analyse traffic and data based mostly on Network protocol, category of user, operations carried out etc. [10]

SIEM: Security Information and Event Management tool is a system that collects data for analysis in trying to detect and prevent unauthorized access. This system uses multiple statistics and data to make a decision [11].

Pattern recognition: When the identity of a malicious application is not known, the manner of operation can be used in detecting the application. This method is based on the ideology that malicious applications are similar in the way in which they operate and can be traced using these operational similarities [67].

Risk Assessment: Assessing the risks and the possibility of an attack that an application poses, by monitoring its activities in a confined environment. The impact value of the risks and risk level is aggregated. This method aids in highlighting suspected attacks [35].

Multi-layer Security: Communication in computer system involves various layers, which have various uses. This method uses multiple defence mechanisms in trying to trap the activities of malicious applications. This method combines methods like: Access Control Lists (ACLs), encryption, redundancy check, logs, etc. These methods are implemented in the network plane, application plane, user plane, physical plane etc. [17], [43], [69].

Researchers have proposed the implementation of the methods highlighted above in various ways with the aim of mitigating APT. The results of their studies showed different levels of accuracy and effectiveness. The statistics classifying the methods employed by 25 researchers are highlighted in Figure 3.

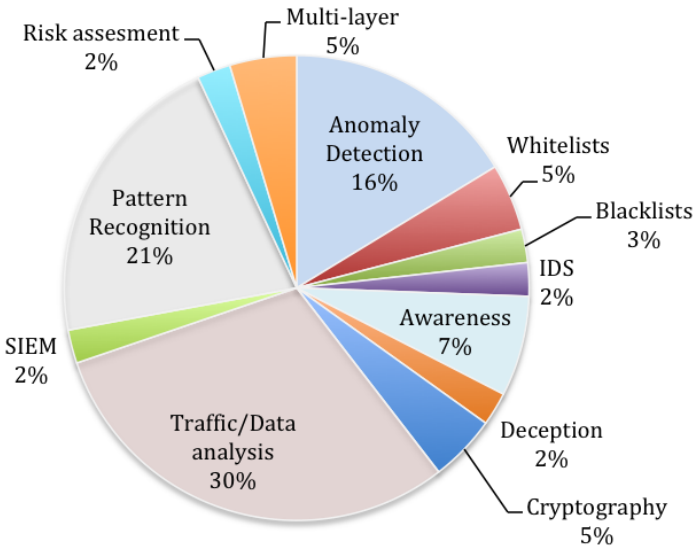

Fig. 3. Pie chart showing Mitigation Techniques Used against APT by 25 researchers

Figure 3 shows the utilization of 12 mitigation techniques by 25 researchers although, Tables 1-4 shows the utilization of more than one technique by most of the researchers, this brings the frequency of all methods used to 46. From Figure 3, the most popular technique used is traffic/data analysis, which shows a frequency utilization of 12 out of 25. Based on the work done by these researchers the assumption is that one method is inadequate in effectively mitigating APT attacks as seen in Table 1, where 11 out of 15 used more than one method. The other 4 researchers, proposed the implementation of only traffic/data analysis with no other method for mitigating the threat. The implementation of these methods were done differently and at different layers and phases. These studies differ in the data presented for analysis, which ranges from logs to web graphs and data from packets.

Lin et al. [33], Ghafir et al. [20], Virvilis and

TABLE 1
Implementation of Traffic/Data analysis

Author	Anomaly Detection	Whitelist	Blacklist	IDS	Awareness	Cryptography	Traffic/Data Analysis	SIEM	Pattern Recognition	Multilayer Security	No. of Methods
Ghafir and Prenosil [19]			✓	✓		✓	✓				4
Lamprakis, et al. [30]	✓	✓					✓				3
Friedberg et al. [15]	✓	✓					✓				3
Lin [33]							✓				1
Ghafir et al. [20]							✓				1
Su et al. [55]							✓				1
Skopik et al. [53]	✓						✓				2
Virvilis and Gritzalis [62]							✓				1
Mirza et al. [41]							✓	✓	✓		3
Vance [58]	✓						✓				2
De Vries et al. [12]	✓						✓				2
Bhatt et al. [2]							✓		✓	✓	3
Sigholm and Bang [51]					✓		✓				2
Giura and Wang [21]							✓			✓	2

TABLE 2
Implementation of Pattern Recognition

Author	Anomaly Detection	Whitelist	Traffic/Data Analysis	Pattern Recognition	No. of Methods
Lamprakis, et al. [30]	✓	✓	✓		3
Friedberg et al. [15]	✓	✓	✓		3
Skopik et al. [53]	✓		✓		2
Vance [58]	✓		✓		2
De Vries et al. [12]	✓		✓		2
Wang et al. [65]	✓			✓	2

Gritzalis [62] and, Su et al. [55] proposed the implementation of traffic/data analysis using different techniques. Ghafir and Prenosil [19] with the aim of solving the challenges with the prevention of APT attacks, proposed the addition of features to an open source Intrusion Detection System. These features are to include analysing the data traffic in the networks, in detecting malicious activities based on the requests sent and the protocols being used, filtering using blacklists and the use of hash algorithm in protecting the confidentiality and integrity of the organization's data.

Table 2. shows the work done by 6 researchers who proposed the use of anomaly detection in mitigating the threat, out of which 5 researchers as illustrated also in table 1, proposed the implementation of anomaly detection with traffic/data analysis. The data and the results of the data and traffic analysis, are used in determining normal behavior and abnormal behaviour. Lamprakis et al. [30] and Friedberg et al. [15] also proposed the use of whitelist, which combines three methods to militate the threat. The use of blacklist has been said to be ineffective in mitigating targeted and sophisticated attacks which is why Lamprakis P. et al. [30] and Friedberg I. et al. [15] have adopted the use of whitelist in preventing malicious activities.

A gene based approach in detecting Advanced persistent threats was employed by Wang et al. [65] which identified some similarities with APT attacks using the pattern of pre-existing attacks which have occurred with anomaly detection as seen in Table 2 and Table 3. This work focused on network protocol behavioural pattern to form a gene based detection system.

Baht et al. [2], and Guira and Wang [21] as seen in Table 1 and Table 4 proposed the use of multilayer security in addition to data and traffic analysis. Baht et al. [2] proposed a multi stage approach to militating APT where mitigation methods are implemented at every stage of the attack. Guira and Wang [21] proposed analysis and correlation of security scenarios across the user, network, physical and application plane. Baht et al. [2] also used pattern recognition in aiding a trigger sensor to determine the presence of malicious activities.

Binde et al. [3] amongst all the researches done using pattern recognition from Table 3 only used one method. Vert et al. [60] and Moon et al. [43] as

TABLE 3
Implementation of Pattern Recognition

Author	Anomaly Detection	Awareness	Cryptography	Traffic/Data Analysis	SIEM	Pattern Recognition	Multilayer Security	No. of Methods
Vert et al. [60]						✓	✓	2
Chandra, et al. [8]			✓			✓		2
Brogi and Tong [5]		✓				✓		2
Wang et al. [65]	✓					✓		2
Mirza et al. [41]				✓	✓	✓		3
Binde et al. [3]						✓		1
Moon et al. [43]						✓	✓	2
Bhatt et al. [2]				✓		✓	✓	3
Julisch [27]		✓				✓		2

TABLE 4
Implementation of Multilayer Security

Author	Traffic/Data Analysis	Pattern Recognition	Multilayer Security	No. of Methods
Vert et al. [60]		✓	✓	2
Moon et al. [43]		✓	✓	2
Bhatt et al. [2]	✓	✓	✓	3
Giura and Wang [21]	✓		✓	2

seen in Table 3 and 4, used multilayer security with pattern recognition, which will aid in preventing and detecting threats at different layers.

Awareness as proposed by Shigolm and Bang [51], Brogi and Tong [5] and Julisch [27] as seen in Table 1 and Table 3 with other methods. Awareness is none technical and is implemented separately from the proposed technical method. Shigolm and Bangs [51] also proposed traffic and data analysis. Brogi and Tong [5] and Julisch [27] also propose the use of pattern recognition, which was to provide more information for awareness. Other methods implemented with pattern recognition from Table 3, includes Mirza et al. [41] and Chandra et al. [8], which utilized cryptography and Traffic/data analysis.

Other researchers who didnt fall within the major range are Virvilis et al. [63] and Granadillo et al. [22]. Virvilis et al. [62] proposed the art of deception to detect and prevent APT. They utilized honey devices to deceive the attacker and trace the source of the attack. Granadillo et al. [22] proposed assessing the risks to determine the potential risk of an attack. These methods have metrics attached to them, which is based on the number of methods proposed.

7. Discussion

Advanced Persistent Threats is a growing threat to information systems, organizations and government. This study has highlighted the anatomy of APT and the common vulnerabilities associated with the threat. As shown in Figure 1, 60% of the challenge borders around the inability to mitigate APT using traditional methods. From the studies carried out by researchers and as shown in Figure 3, some of the results showed better signs of mitigating APT than others, and showed signs of popularity, which is used as a measure of effectiveness [38]. The popularity is attained based on the percentage of proposed implementations for each method, in militating APT attacks. The results show a move towards the combination of multiple methods in mitigating APT, 72% of the researchers combined multiple methods in mitigating the threat. None of the researchers proposed the conventional antivirus but rather identified its limitations, which is majorly due to its ineffectiveness in militating the threat. Sight-

ing the attack phases involved with APT and the methods used in gaining access, which is majorly through zero day malwares, it is understandable why traditional methods prove ineffective. Conventional methods work based on pre-known malware identity in detecting malicious activities and the presence of malwares, this makes it totally inefficient in detecting and preventing APT. On the other hand, using popularity in measuring effectiveness, the high percentage in utilization of traffic/data analysis, pattern recognition and Anomaly detection shows that these methods exhibit signs of effectiveness depending on how it is implemented.

Table 1-4 shows metrics based on the frequency of utilization of methods in each study. From the methods adopted, traffic/data analysis has the highest count which is 30, anomaly detection 14, Pattern recognition 19 and multilayer security 9. The pattern of these studies shows that in detecting APT using technical methods at least two methods should be used. All proposed implementation of anomaly detection were combined with a second method of which 5 out of 6 were combined with traffic/data analysis and 1 with pattern recognition.

The use of whitelists and blacklist has limitations and by using whitelist only known applications will be allowed to run while, blacklist can prevent only known malicious applications and data traffic. Other methods, which include deception and awareness, rely on human intelligence and human behavioural pattern in preventing and detecting APT attacks. The low level of effectiveness is obvious by their low utilization as a preventive method as indicated in Figure 3.

The level of effectiveness in mitigating APT is not obtainable from the studies done because of the mutating nature of the threat although this study provides a guide and has filtered more effective techniques in mitigating APT.

This study provides a synopsis of several studies, which proposed different methods and techniques to securing organizations and their infrastructure.

8. Conclusion

Advanced Persistent Threat attack increases every year with increasing levels of sophistication. With the inability to detect and prevent these attacks in many organizations as seen in Figure 1, the government are at a high risk of losing valuable information. Having investigated into the challenges in securing information systems againts APT, 12 mitigation techniques are highlighted by 25 researchers, from the work done, it is evident that there is a need to combine some of the methods highlighted based on their effectiveness. This study is a synopsis on the effectiveness of existing mitigation techniques against APT. Traffic/data analysis, pattern recognition and anomaly detection are the most promising mitigation methods as is evident from being the top three most utilized methods amongst all the methods outlined in this study. As highlighted by the researchers the point of implementation may differ and also have an effect on the results. Future work in developing a behavioural pattern, implementation of mitigation techniques and the plane where the methods are implemented will reduce the occurrence of false positives, and will improve the effectiveness in mitigating APT. From the results of this paper, we reccomend the use of multiple methods in securing against APT like attacks, with increased focus in the areas of anomaly detection, traffic/data analysis and pattern recognition.

References

[1] Merete Ask, Petro Bondarenko, John Erik Rekdal, André Nordbø, Pieter Bloemerus, and Dmytro Piatkivskyi. Advanced persistent threat (apt) beyond the hype. *Project Report in IMT4582 Network Security at Gjøvik University College, Springer*, 2013.

[2] Parth Bhatt, Edgar Toshiro Yano, and Per Gustavsson. Towards a framework to detect multi-stage advanced persistent threats attacks. In *2014 IEEE 8th International Symposium on Service Oriented System Engineering*. IEEE, apr 2014.

[3] Beth Binde, Russ McRee, and Terrence J OConnor. Assessing outbound traffic to uncover advanced persistent threat. *SANS Institute. Whitepaper*, page 16, 2011.

[4] Ross Brewer. Advanced persistent threats: minimising the damage. *Network Security*, 2014(4):5–9, apr 2014.

[5] Guillaume Brogi and Valerie Viet Triem Tong. TerminAPTor: Highlighting advanced persistent threats through information flow tracking. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, nov 2016.

[6] Bulgurcu, Cavusoglu, and Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3):523, 2010.

[7] Christian Cachin, Marko Vukolic Sorniotti, and Thomas Weigold. Blockchain, cryptography, and consensus, 2016.

[8] J Vijaya Chandra, Narasimham Challa, and Mohammed Ali Hussain. Data and information storage security from advanced persistent attack in cloud computing. *International Journal of Applied Engineering Research*, 9(20):7755–7768, 2014.

[9] Ping Chen, Lieven Desmet, and Christophe Huygens. A study on advanced persistent threats. In *Communications and Multimedia Security*, pages 63–72. Springer Berlin Heidelberg, 2014.

[10] Mauro Conti, Luigi V. Mancini, Riccardo Spolaor, and Nino Vincenzo Verde. Can't you hear me knocking: Identification of user actions on android apps via traffic analysis. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pages 297–304. ACM, 2015.

[11] Luigi Coppolino, Michael Jger, Nicolai Kuntze, and Roland Rieke. A trusted information agent for security information and event management. *SECURITY ANALYSIS OF SYSTEM BEHAVIOUR*, page 265, 2014.

[12] Johannes de Vries, Hans Hoogstraaten, Jan van den Berg, and Semir Daskapan. Systems for detecting advanced persistent threats: A development roadmap using intelligent data analysis. In *2012 International Conference on Cyber Security*. IEEE, dec 2012.

[13] Alex Drozhzhin. The greatest heist of the century: hackers stole $1 bln, 2015. Assesed 04 May 2015.

[14] Benjamin Edwards, Tyler Moore, George Stelle, Steven Hofmeyr, and Stephanie Forrest. Beyond the blacklist: modeling malware spread and the effect of interventions. In *Proceedings of the 2012 workshop on New security paradigms*, pages 53–66. ACM Press, 2012.

[15] Ivo Friedberg, Florian Skopik, Giuseppe Settanni, and Roman Fiedler. Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, 48:35–57, feb 2015.

[16] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2):18–28, feb 2009.

[17] Giovanni Geraci, Harpreet S. Dhillon, Jeffrey G. Andrews, Jinhong Yuan, and Iain B. Collings. Physical layer security in downlink multi-antenna cellular networks. *IEEE Transactions on Communications*, 62(6):2006–2021, jun 2014.

[18] Ibrahim Ghafir and Vaclav Prenosil. Advanced persistent threat attack detection: an overview. *International Journal of Advances in Computer Networks and Its Security (IJCNS)*, 4(4):5054, 2014.

[19] Ibrahim Ghafir and Vaclav Prenosil. Proposed approach for targeted attacks detection. In *Lecture Notes in Electrical Engineering*, pages 73–80. Springer International Publishing, dec 2015.

[20] Ibrahim Ghafir, Vaclav Prenosil, Mohammad Hammoudeh, Francisco J. Aparicio-Navarro, Khaled Rabie, and Ahmad Jabban. Disguised executable files in spear-phishing emails. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems -ICFNDS*. ACM Press, 2018.

[21] Paul Giura and Wei Wang. Using large scale distributed computing to unveil advanced persistent threats. *Science J*, 1(3):93–105, 2012.

[22] Gustavo Gonzalez Granadillo, Joaquin Garcia-Alfaro, Herve Debar, Christophe Ponchel, and Laura Rodriguez Martin. Considering technical and financial impact in the selection of security countermeasures against advanced persistent threats (APTs). In *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, jul 2015.

[23] Pengfei Hu, Hongxing Li, Hao Fu, Derya Cansever, and Prasant Mohapatra. Dynamic defense strategy against advanced persistent threat with insiders. In *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, apr 2015.

[24] Barbara Hudson. Advanced persistent threats: Detection, protection and prevention. *Sophos Ltd., US February*, 2014.

[25] Jun Ho Huh, John Lyle, Cornelius Namiluko, and Andrew Martin. Managing application whitelists in trusted distributed systems. *Future Generation Computer Systems*, 27(2):211–226, feb 2011.

[26] Inkyung Jeun, Youngsook Lee, and Dongho Won. A practical study on advanced persistent threats. In *Communications in Computer and Information Science*, pages 144–152. Springer Berlin Heidelberg, 2012.

[27] Klaus Julisch. Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57(10):2206–2211, jul 2013.

[28] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. Advanced social engineering attacks. *Journal of Information Security and Applications*, 22:113–122, jun 2015.

[29] David Lacey. *Advanced Persistent Threats: How to Manage the Risk to Your Business*. ISACA, 2013.

[30] Pavlos Lamprakis, Ruggiero Dargenio, David Gugelmann, Vincent Lenders, Markus Happe, and Laurent Vanbever. Unsuper-

vised detection of APT c&c channels using web request graphs. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 366–387. Springer International Publishing, 2017.

[31] Meicong Li, Wei Huang, Yongbin Wang, Wenqing Fan, and Jianfang Li. The study of APT attack stage model. In *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*. IEEE, jun 2016.

[32] Young Hwan Lim, Hong Ryeol Ryu, Kyung Sung Choi, Chan Wook Park, Won Hyung Park, and Kwang Ho Kook. A study on malware detection system model based on correlation analysis using live response techniques. In *2012 International Conference on Information Science and Applications*. IEEE, may 2012.

[33] Ken Chang Dr Ying-Dar Lin. Advanced persistent threat: Malicious code hidden in pdf documents. 2014.

[34] Xiaomei Liu, Zijuan Luo, Shuanghua Zhu, Chen yan Kong, Wei Chen, Yuta Nakatani, Shin ya Nishizaki, Xiao dan Li, Yong feng Yin, and Ping Shao. Research on prevention solution of advanced persistent threat. In *2014 2nd International Conference on Software Engineering, Knowledge Engineering and Information Engineering (SEKEIE 2014)). Atlantis Press*, 2014.

[35] Chi-Chun Lo and Wan-Jia Chen. A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, 39(1):247–257, jan 2012.

[36] Vijay Mahadevan, Weixin Li, Viral Bhalodia, and Nuno Vasconcelos. Anomaly detection in crowded scenes. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. IEEE, jun 2010.

[37] Mirco Marchetti, Fabio Pierazzi, Michele Colajanni, and Alessandro Guido. Analysis of high volumes of network traffic for advanced persistent threat detection. *Computer Networks*, 109:127–141, nov 2016.

[38] Philip J McParlane, Yashar Moshfeghi, and Joemon M Jose. Nobody comes here anymore, it's too crowded; predicting image popularity on flickr. In *Proceedings of International Conference on Multimedia Retrieval*, page 385. ACM, 2014.

[39] Ruchika Mehresh and Shambhu J. Upadhyaya. Deception-based survivability. In *Secure System Design and Trustable Computing*, pages 521–537. Springer International Publishing, 2016.

[40] Diego Mendez Mena, Ioannis Papapanagiotou, and Baijian Yang. Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, 27(3):162–182, apr 2018.

[41] Natasha Arjumand Shoaib Mirza, Haider Abbas, Farrukh Aslam Khan, and Jalal Al Muhtadi. Anticipating advanced persistent threat (APT) countermeasures using collaborative security mechanisms. In *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*. IEEE, aug 2014.

[42] Nurul Nuha Abdul Molok, Atif Ahmad, and Shanton Chang. A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management*, 43:351–356, dec 2018.

[43] Daesung Moon, Hyungjin Im, Jae Lee, and Jong Park. MLDS: Multi-layer defense system for preventing advanced persistent threats. *Symmetry*, 6(4):997–1010, dec 2014.

[44] Kara Nance and Matt Bishop. Introduction to deception, digital forensics, and malware minitrack. In *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. Hawaii International Conference on System Sciences, 2017.

[45] Terry Nelms, Roberto Perdisci, Manos Antonakakis, and Mustaque Ahamad. Towards measuring and mitigating social engineering software download attacks. In *USENIX Security Symposium*, pages 773–789, 2016.

[46] Mathew Nicho and Shafaq Khan. Identifying vulnerabilities of advanced persistent threats. *International Journal of Information Security and Privacy*, 8(1):1–18, jan 2014.

[47] Robert W. Palmatier, Mark B. Houston, and John Hulland. Review articles: purpose, process, and structure. *Journal of the Academy of Marketing Science*, 46(1):1–5, oct 2017.

[48] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12):3448–3470, aug 2007.

[49] Chris Peikert. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016.

[50] Shari Lawrence Pfleeger, M. Angela Sasse, and Adrian Furnham. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, 11(4), jan 2014.

[51] Johan Sigholm and Martin Bang. Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. In *2013 European Intelligence and Security Informatics Conference*. IEEE, aug 2013.

[52] Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75:200–222, nov 2016.

[53] Florian Skopik, Ivo Friedberg, and Roman Fiedler. Dealing with advanced persistent threats in smart grid ICT networks. In *ISGT 2014*. IEEE, feb 2014.

[54] Rob Sloan. Advanced persistent threat. *Engineering & Technology Reference*, jan 2014.

[55] Yunfei Su, Mengjun Li, ChaoJing Tang, and Rongjun Shen. A framework of APT detection based on dynamic analysis. In *Proceedings of the 2015 4th National Conference on Electrical, Electronics and Computer Engineering*. Atlantis Press, 2016.

[56] Lyn M. Van Swol, Michael T. Braun, and Miranda R. Kolb. Deception, detection, demeanor, and truth bias in face-to-face and computer-mediated communication. *Communication Research*, 42(8):1116–1142, apr 2013.

[57] Colin Tankard. Advanced persistent threats and how to monitor and deter them. *Network Security*, 2011(8):16–19, aug 2011.

[58] Andrew Vance. Flow based analysis of advanced persistent threats detecting targeted attacks in cloud computing. In *2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*. IEEE, oct 2014.

[59] Andrew Vance. Flow based analysis of advanced persistent threats detecting targeted attacks in cloud computing. In *Problems of Infocommunications Science and Technology, 2014 First International Scientific-Practical Conference*, pages 173–176. IEEE, 2014.

[60] Gregory Vert, Bilal Gonen, and Jayson Brown. A theoretical model for detection of advanced persistent threat in networks and systems using a finite angular state velocity machine (FAST-VM). *International Journal of Computer Science and Application*, 3(2):63, 2014.

[61] Nart Villeneuve and James Bennett. Detecting apt activity with network traffic analysis. *Trend Micro Incorporated Research Paper*, 2012.

[62] Nikos Virvilis and Dimitris Gritzalis. The big four - what we did wrong in advanced persistent threat detection? In *2013 International Conference on Availability, Reliability and Security*. IEEE, sep 2013.

[63] Nikos Virvilis, Bart Vanautgaerden, and Oscar Serrano Serrano. Changing the game: The art of deceiving sophisticated attackers. In *2014 6th International Conference On Cyber Conflict (CyCon 2014)*. IEEE, jun 2014.

[64] Xu Wang, Kangfeng Zheng, Xinxin Niu, Bin Wu, and Chunhua Wu. Detection of command and control in advanced persistent threat based on independent access. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, may 2016.

[65] Yuan Wang, Yongjun Wang, Jing Liu, and Zhijian Huang. A network gene-based framework for detecting advanced persistent threats. In *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. IEEE, nov 2014.

[66] Mark Warren. Modern IP theft and the insider threat. *Computer Fraud & Security*, 2015(6):5–10, jun 2015.

[67] John Wright, Yi Ma, Julien Mairal, Guillermo Sapiro, Thomas S. Huang, and Shuicheng Yan. Sparse representation for computer vision and pattern recognition. *Proceedings of the IEEE*, 98(6):1031–1044, jun 2010.

[68] Jian Wu, Pradeep Teregowda, Juan Pablo Fernández Ramírez, Prasenjit Mitra, Shuyi Zheng, and C. Lee Giles. The evolution of a crawling strategy for an academic document search engine. In *Proceedings of the 3rd Annual ACM Web Science Conference*. ACM Press, 2012.

[69] Xue Yang, Zhihua Li, Zhenmin Geng, and Haitao Zhang. A multi-layer security model for internet of things. In *Internet of Things*, pages 388–393. Springer Berlin Heidelberg, 2012.