DOI: http://dx.doi.org/10.26483/ijarcs.v11i1.6502

Volume 11, No. 1, January-February 2020

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ADVANCED PERSISTENT THREATS AND ITS ROLE IN NETWORK SECURITY VULNERABILITIES

Feras Mohammed Al-Matarneh
Department of Computer Science, University of Tabuk,
University of College Duba,
Kingdom of Saudi Arabia.

Abstract: The paper presents an overview ofAdvanced Persistent Threats (APTs), and its core concepts, lifecycle and characteristic features. In addition, the key factors; actors, targets and motives of an APT were highlighted in detail. The critical challenges currently facing organisations due to APT attacks on its systems, networks and IT infrastructure were critically examined. Lastly, the potential strategies for mitigating APTs were identified and highlighted. The findings demonstrated that an APT is a series of long term, covert and persistent cyber threats that target, penetrate and exploit organisations, businesses or states toacquire valuable proprietary (industrial espionage) data or political reasons (activism)resulting in losses of over USD$500 Billion annually. Consequently, the prevalence and sophistication of APTs have soared astronomically accounting for 39% of all cyber-attacks on computer networks. Furthermore, the potential damage from APTs is responsible for 60-65% downtime, network disruption, and financial losses. Hence, thepotentially damaging effects of APTs,has prompted various organisations to invest in cyber securityprogramsand other mitigation strategies to timely detect, prevent and eradicate future APT attacks. The paper reveals that APTs can be mitigated by deploying computer analytics, network security mechanisms such as the "defense in depth" (D-in-D), network traffic introspection, and endpoint security measures. However, other strategies include the deployment of Advanced Persistent Security measures. In conclusion, the paper reveal that APTs pose significant threats to global computer networks and require considerable resources, and investment to forestall future problems.

Keywords: Advanced Persistent Threat, Network Security, Hacking, Vectors, Vulnerability.

1. INTRODUCTION

The termAdvanced Persistent Threat (APT) typicallydescribes a series of highly organized and persistent attacks on computer networkscoordinated by hackers or cybercriminals to extract valuable information from organizations (Ask *et al.*, 2013; Cobb, 2013; Kumar and Kumar, 2014). The term Advanced Persistent Threat (APT) is often credited to Gregory Rattray, a United States Air Force Colonel, who coined the expression to describe data-exfiltration Trojans used to exploit the vulnerabilities of computer networks(Rattray, 1994; Rattray and Healey, 2010; Arsene, 2017). In principle, an APTis a generic term thatdescribes a series of long term, covert and persistentcyber threats targeted at organisations, states or businesses for the purpose of extracting valuable data for industrial espionage or political activism(Rudner, 2013; Lindsay, 2015).According to Friedberg *et al.* (2015), an APT is deliberate slow-movingcyber-attack designed to secretly compromise the security of interconnected information systems with the objective to gain unauthorised access. At the beginning, an APT seeks to gain access to a system, however, in the long run, the purpose is to spread across the networkto steal legal documents, intellectual or propriety data among other vital information(Friedberg *et al.*, 2015).Tankard (2011) describes APTs as a "new breed of insidious threats" used to perpetuate multiple, stealthy, and undetectable attacks on computer networks or systems for long periods of time. The threats gain access through advanced vectors or techniques and persist for long periods of time(Tankard, 2011).

However, one of the most widely accepted definitions of APTs was proposed by the United States National Institute of Standards and Technology(NIST, 2017). According to the NIST, an APT is, "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)". According to the report, the objectives comprise creating and spreading its bases inside network or information technology infrastructure oftargeted organizations with the aim toextract vital information. In the process, the APT seeks to eitherdamage, obstruct or position itself to further manipulate IT network of the organization. Consequently, an APTperpetuates its objectives by persistentlyadapting andmaintaining the level of interaction required to implement its objectives(NIST, 2017).

However, the general consensus is that APTs are deceptive cyber threats that breach the security of computer networks through "low and slow" attacks that are hard to detect until the breach is completely executed on the host network. This suggests that APTs function beyond the detection limits of conventional IT cybersecurity tools (Lock, 2017). This underlying scenario presents significant challenges for IT and cyber security analysts around the globe. Hence, the spate and growing sophistication of APTs has become a recurring problem.As a result, APTscontinue to significant risksnot only global computer networks and the security of data driven organisations but financial, commercial and industrial concerns worldwide. According to the Radware ERT 2015 report, APTs account for 39% of the most menacingthreats to computer networks and systems in various organisations worldwide(Radware, 2015). Analysts opine that APTs and other cybercrimescost states, businesses and organisations over US$400 billion dollarsannually(McAfee, 2005; Choo, 2007; Lock, 2017).According to Tankard (2011),cybercrimes cost the UK taxpayer and the global economy £27 Billion and $1 Trillion, respectively.In the year 2013, the UK Cyber Security watchdog, OCSIA (Office of Cyber Security and Information Assurance) estimated that over 90% and 85% of large and small business corporations, respectively, experienced various degrees of cyber-attacks. The estimated costs of the reported cyber intrusions were approximately $7 million per organisation amounting an average increase of 30% per annum (Brewer, 2014). As a result, many observers opine that by the year 2020, the global cyber security budget of firms, organisations and states will soar by over 60% significantly bloating the cost of doing business. This will require significant investment to comprehensively understand the *modus operandi*, detect intrusions and prevent damage by APTs toglobal computer systems and IT networks.

Therefore, the main objective of this paper is to present a critical overview of Advanced Persistent Threats (APTs), the current status, life cycle and characteristic features. The paper will outline the operational steps of APTs and the challenges currently faced by organisations. It will present examples of previous attacks on systems, networks and IT infrastructure around the globe. Lastly, the paper willidentify, examine and highlight potential mitigation strategies required to address the growing cyber menace of APTs across the global IT domain. It is envisaged that the findings will provide useful insights into APT required by the cyber community to address the growing importance of APTs against the backdrop of globalization.

2. CORE CONCEPT OF ANAPT

In theory, the term APT is an amalgamation of three rudimentary terms namely; Advanced, Persistent, and Threat as illustrated in Figure 1.Despite the numerous definitions and conceptual analyses, an Advanced Persistent Threats (APT) is typically characterized by unique dynamic features. Based on this premise, the concept of APTs will be analysed to determine the unique contribution of each part to the overall concept.

The first part of an APT is the “Advanced” feature which typically involves the use of sophisticated intrusion techniques by hackers or cyber criminalsto disrupt computer networks, gather intelligence, or steal valuable data(Rudner, 2013). In practice, an APT begins with target acquisition and gaining access to a network through advanced malware, other sophisticated intelligence gathering or interception tools and technologies (Command Five, 2012). The advanced malware subsequently gains remote control of the network access and vulnerabilities through command and control (c-and-c) servers(Virvilis *et al.*, 2013; Choi *et al.*, 2015). Once established, the malware creates additional access points to further compromise the network, extracts the target data on a staged server and harvests the data from the network(Rudner, 2013; Sood and Enbody, 2013).Therefore, the key feature of the “Advanced” factor of an APT is stealth and sophistication which ensureshitch free access on the host network.

The second aspect of an APT is the “Persistent” feature. This typically involves consistent, continuous, target specific attacks on the host network. In principle, the term persistent arises from the “low-and-slow” nature of the process in which the attackers continuously monitor the host network periodically and systematically harvesting information. The key feature of the “Persistent” feature of an APT is the long-term nature of the process. As a result, the hackers ensure continuous, long term harvesting or extraction of data from the host without detection(Rudner, 2013; Virvilis *et al.*, 2013).

The third and last part an APT is the “Threat” feature. This basically involves exploiting the vulnerabilities of computer networks (Jover and Giura, 2013)to gain unauthorised access and remain undetected while disrupting the network to extract valuable data(Virvilis *et al.*, 2013). According to analysts, the potential damage from APTs is responsible for 60-65% downtime, network disruption, financial losses(Tankard, 2011; Arsene, 2017). However, some analysis opine future losses could effectively result in the breakdown of communications(Tankard, 2011), network communications(Arsene, 2017) power or energygrid systems(Lemay, 2013; Industrial Control Systems, 2016)or worse result in man-made disasters (Radware, 2015; NIST, 2017) or terrorist acts(Dean *et al.*, 2012; SecureWorks, 2017). The potentially disastrous effects of these events on global economies accentuates the urgent need to critically understand the lifecycle and characteristic of APTs.

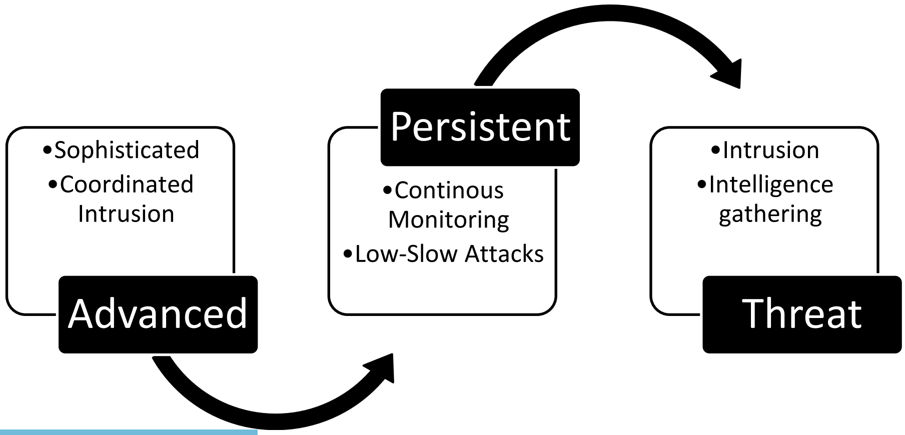


Figure 1: Core Concept of an Advanced Persistent Threat

3. LIFECYCLEAND CHARACTERISTICSOF AN APT

In principle, the aim of an APT is to leverage sophisticated cyber tools and computing techniques to attack networks or computers(Abomhara, 2015). In broad terms, the characteristics of an APT are generally dependent on the target objective, tools, and time-frame.Therefore, an APT is typically characterised by the purpose, resources, and sophistication of the proposed attack(SecureWorks, 2017). In spite of this, an APT isdesignated by uniquefeatures as described by Bodmer *et al.* (2012).Based on the authors, an APT istypically characterized by the following features;

- Objectives,
- Timeliness,
- Resources,
- Risk tolerance,
- Skills and methods,
- Actions,
- Attack origination points,
- Numbers involved in the attack,
- Knowledge source.

The first step is to define the target or objective or end goal of the threat. Subsequently, the system or networkis timely probed by means of sophisticated tools and computing resources at the disposal of the hackers.This is typically executed stealthily to gain accessor establish afootholdor acquire crucial information.At this stage, the precise actions and attack points of the hackerspredefined at the outsetenhancethe target specific extraction of vital information from the system or network(s)(Bodmer *et al.*, 2012). As a result, the APT creates a defined pattern of operation which can be exemplified pictorially using the lifecycle chart in Figure 2 (SecureWorks, 2017).The chart reveals that an APT is described by four factors; Response, Intelligence, Operations and Visibility with the aim to target, penetrate and exploit computer or system networks.

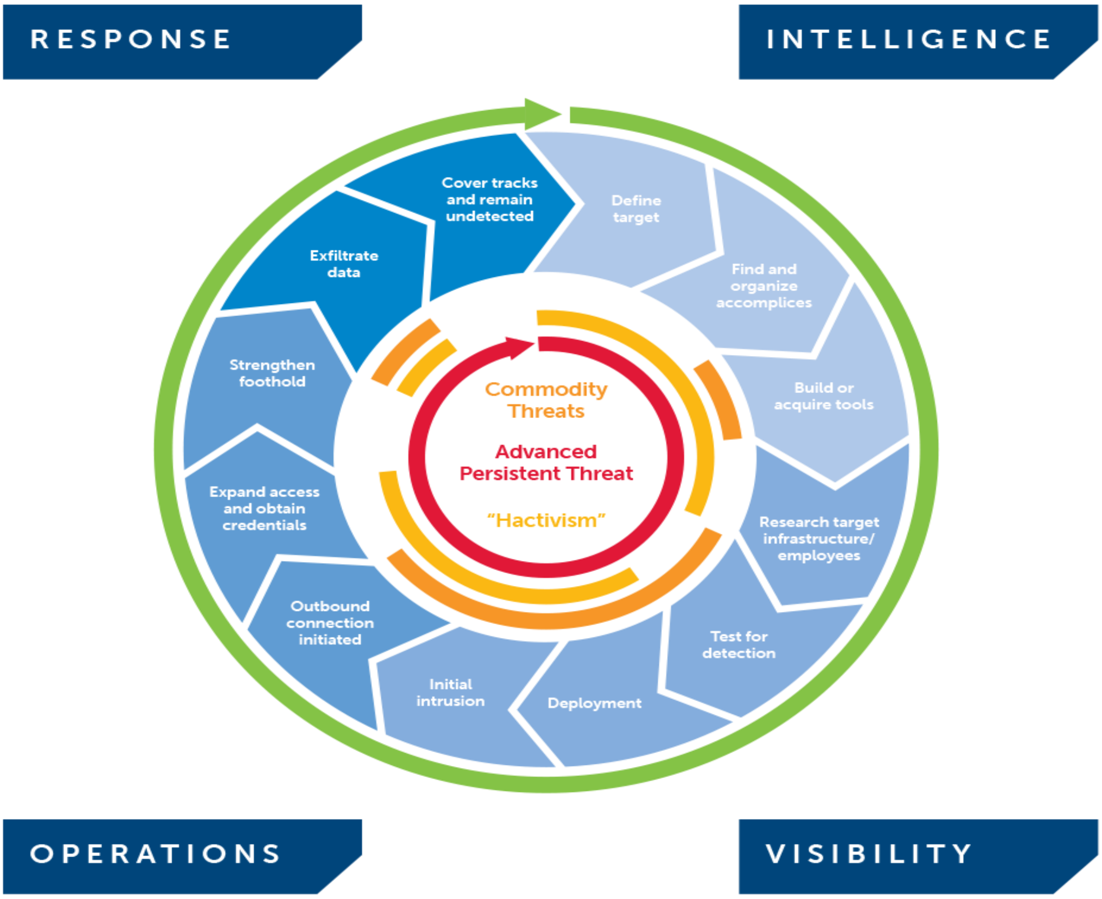

RESPONSE
INTELLIGENCE
OPERATIONS
VISIBILITY
Define target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Figure 2: Lifecycle of APTs (SecureWorks, 2017).

As observed in Figure 2, an APT is aclearly defined process that initially involves targeting and gaining access to vulnerable computer networks using phishing emails, malware or bots. Lastly, the additional tools are installed to complete the target objects, conceal the intrusion and exit undetected(SecureWorks, 2017). This *modus operandi* is corroborated by other researchers in the cybersecurity domain(Tankard, 2011; Bodmer *et al.*, 2012; Virvilis *et al.*, 2013; Sood and Enbody, 2013).Likewise, thereport by the American Cybersecurity firm,Mandiant, demonstrates that the lifecycle of an APT I is characterised by seven (7) basic features namely(Mandiant, 2017);

- Initial compromise,
- Establish Foothold,
- Escalate Privileges,
- Internal Reconnaissance,
- Move Laterally,
- Maintain Presence,
- Complete Mission.

Figure 3 presents another example of an APT lifecycle as proposed by the report. According to the report, the onset of executing an APT requires that the hackers first target and compromise the potential host's network of computers through sophisticated social engineering, phishing malware or viruses (Mandiant, 2017).

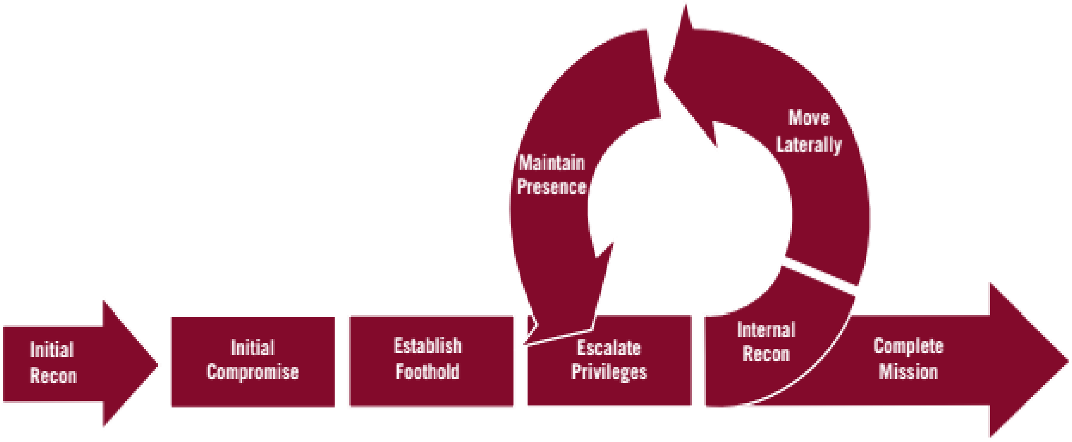


Figure 3: Attack Lifecycle of an APT (Mandiant, 2017)

Next, the hackers exploit network vulnerabilities to gain access and establish a foothold in the host network through backdoor tunnels that grant unhindered access.Figure 4 presents a pictorial depiction of a backdoor installed on a compromised network system during an APT.

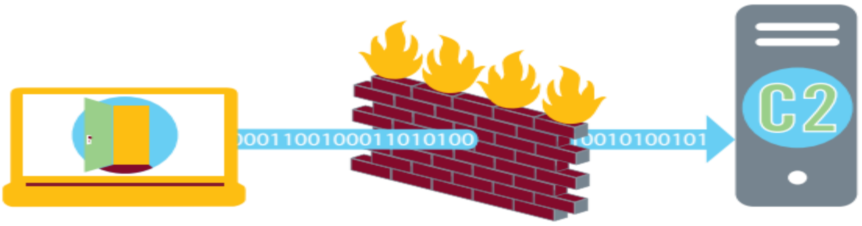


Figure 4: APT Backdoor Access of a Compromised System (Mandiant, 2017).

This invariably enables the hackers to acquire administrator privileges, network passwords and other access codesrequired to conduct information gathering routines, maintain network presence and complete the objective of the APT (Mandiant, 2017).The backdoors provide hackers with information on how to control the host system. In general, APT attacks typically occur over extended periods of time from months to years. During these periods, the APT adapts to counter tools or cyber security measures(Fire Eye, 2017).

4. ACTORS, TARGETS AND MOTIVATION OF AN APT

4.1 Actors in an APT

The execution of an APT requires actors typically an individual, group or organisation that deploys ample time, resources and efforts to target, penetrate and exploit the host.Therefore, the actions of actors in an APT are primarily geared towards timely, persistent and sophisticated exploitation of network system vulnerabilities to achieve its target objectives. In principle, APT actors can range from crime syndicates, terrorists, corporate espionage or nations or states(SecureWorks, 2017). However, actors could also include "lone wolf" opportunistic hackers or hacktivists with a social, religious or cultural agenda.Examples of APT actors in the past include; Unit 61398 of the Chinese People's Liberation Army (PLA) which according to the (Mandiant, 2017)report are responsible for numerous espionage attacks on organisations in the United States (US).The findings indicate that these actors deploy sophisticated tools, tactics and procedures to attack infrastructure, command and control vast computer networks, systems or servers. The scale of damageperpetuated by actors includes the theft of hundreds of terabytes of data from over 140 organisations(Mandiant, 2017). Table 1 presents a list of active APT groups and their mode of operationsover the years(Martin, 2016).

4.2 Motives of an APT

Although APTs are designed to target, penetrate and exploit vulnerable computer systems and networks, several other motives such as financial, political, or sociocultural factors also exist. The motives for APTs can typically include; financial benefit, acquire intelligence or espionage. In addition, an APT can be executed by rival firms or companies to seek competitive advantage in the industry. This is accomplished by gaining proprietary information such as trade secrets, trademarks, and other classified data for financial gain. However, the motive can also be to embarrass, damage, or destroy rival groups or governments(SecureWorks, 2017).

4.3 Targets of an APT

The targets of an APT are varied and numerous. Over the years, cyber reports have estimated that millions of organisations, states or nations have become targets of APTs (Radware, 2015; Mandiant, 2017; NIST, 2017; SecureWorks, 2017). Over the years, APT and like cybersecurity threats have increased geometrically with reported victims in various industries (Thummala, 2016). These include such as Aerospace, Defence, Energy, Healthcare, Pharmaceutical, Technology, Mining, Oil & Gas firms (Rudner, 2013; Sood and Enbody, 2013). Others include Government institutions, Embassies, Education, Research and Development facilities (SecureWorks, 2017). A full list of APT attacks from 2008 till date can be viewed at the dedicatedwebsite,APTnotes(GitHub, 2017). Table 1 presents a concise list of the most active APT hacker groups, their origin, attack methods, victims and motives.

Table 1: Active APT Groups and their Mode of Operations(DiMaggio, 2016; Martin, 2016; Operation Pawn Storm, 2016).

Name of Group	**Year**	**Origin**	**Attack Methods**	**Targets**	**Victims**	**Motives**
Angler-EK	2014	Russia	Drive by downloads.	Random	The Guardian, Lenovo.	Underground Business.
Black Vine	2012	China	Zero-day exploits, Watering-hole attacks, custom-developed malware (Hurix, Sakurel, Mivast)	Aerospace, Energy, Healthcare.	Anthem.	Cyberespionage.
Butterfly	2012	China	Zero-day exploits, custom-developed malware (OSX.Pintsized&Backdoor.Jiripbot)	Pharmaceutical, Technology, law practices, oil, &mining firms.	Twitter, Apple, Facebookand Microsoft.	Cyber espionage, Underground Business.
Dragonfly	2011	European	Spam email, Watering hole attacks, and custom malware (Trojan.Karagany&Backdoor.Oldrea).	Defence, Aviation.	The US & Canada, European Energy firms.	Cyber espionage, Spying, Sabotage.
GovRAT	2015	Government Based.	Targeted distribution (through client-side exploits).	Government officials, Military officials, Large Enterprises.	Government officials, Military officials, Large Enterprises.	Cyber espionage.
Pawn Storm	2004	Economic and Political Cyber espionage.	Spearphishing, Phishing Websites, OWA Phishing, iOS apps, Exploits (including Zero-day).	NATO, Gov't, Military.	Russian Dissidents, Ukraine.	Cyber espionage.

Regin	2008	Government Based.	Long-term intelligence-gathering operations; multi-stage, multicomponent, modular-threat.	Everyone is fair game.	Private firms, Government, Research institutes.	Intelligence gathering, Top-tier Espionage.
Waterbug	2005	State-Sponsor.	Zero-day exploits, targeted emails, stolen certificates, and sophisticated watering-hole distribution network known as Venom.	Government institutions, Embassies, Education, Research facilities.	Government institutions, Embassies, and Education, Research facilities.	Cyberespionage, Spying, Intelligence Gathering.

In general, the actors (hackers) behind APTs seek to target, penetrate and exploit organisations with vast amounts of data based on various motives. As a result, the three variables; actors, targets and motives are invariably interrelated. The relationship between the outline factors can represented diagrammatically as presented in Figure 5.

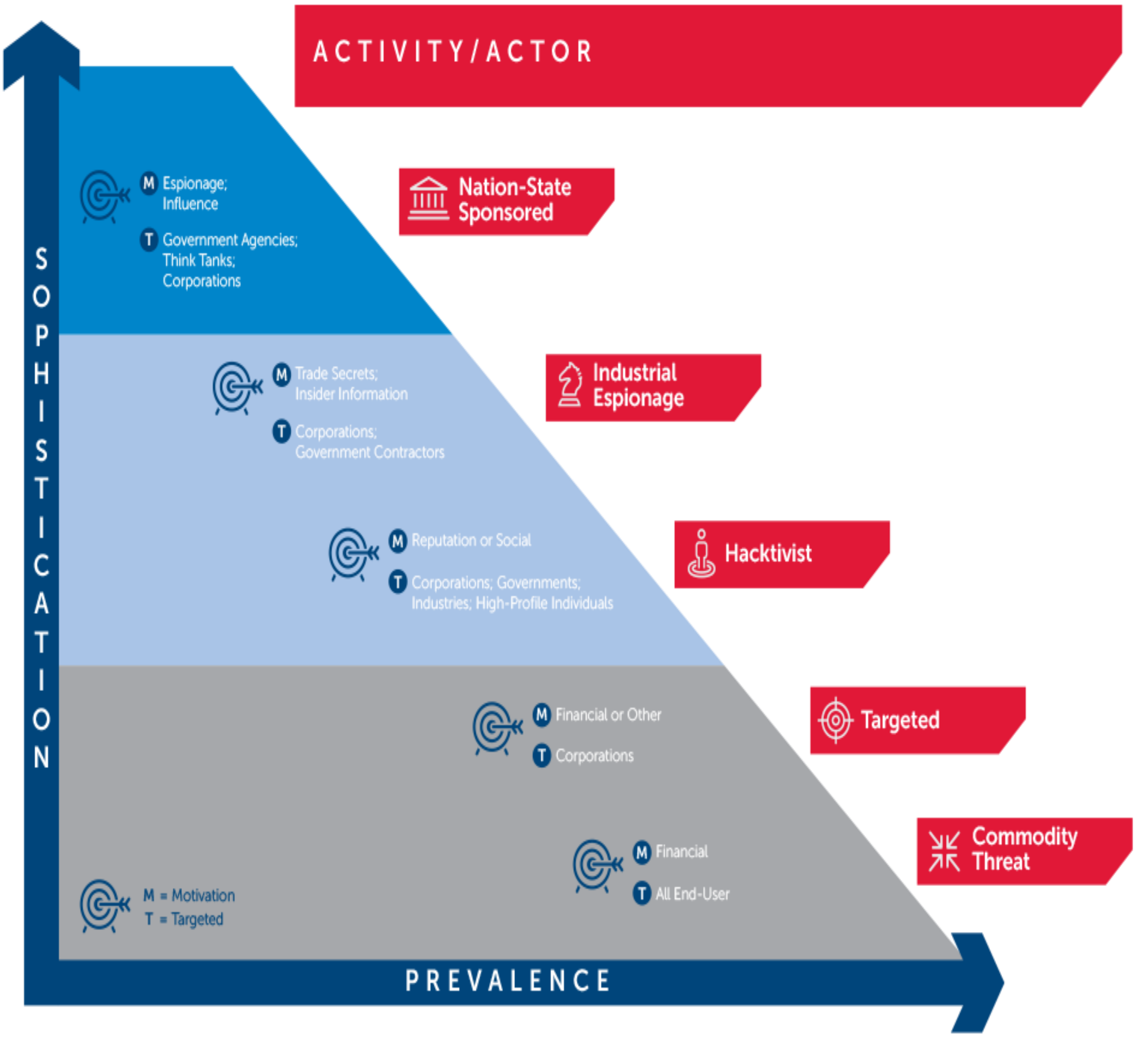
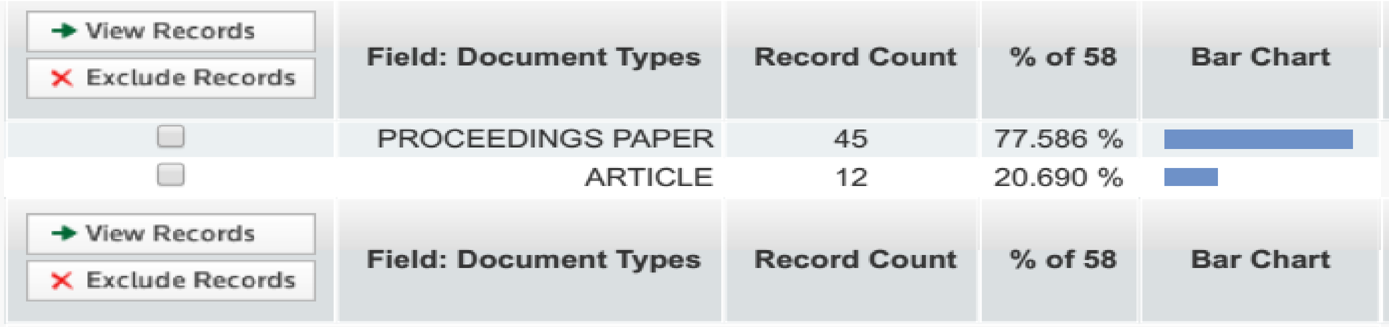


Figure 5: Actors, Motivations and Targets of APTs

As observed in Figure 5, there exists a linear relationship betweenthelevel of sophistication and prevalence of an APT. Furthermore, the motivation (M) and targets (T) of an APT are significantly influenced by the levels of sophistication and prevalence.

5. CURRENT STATUS OF APT

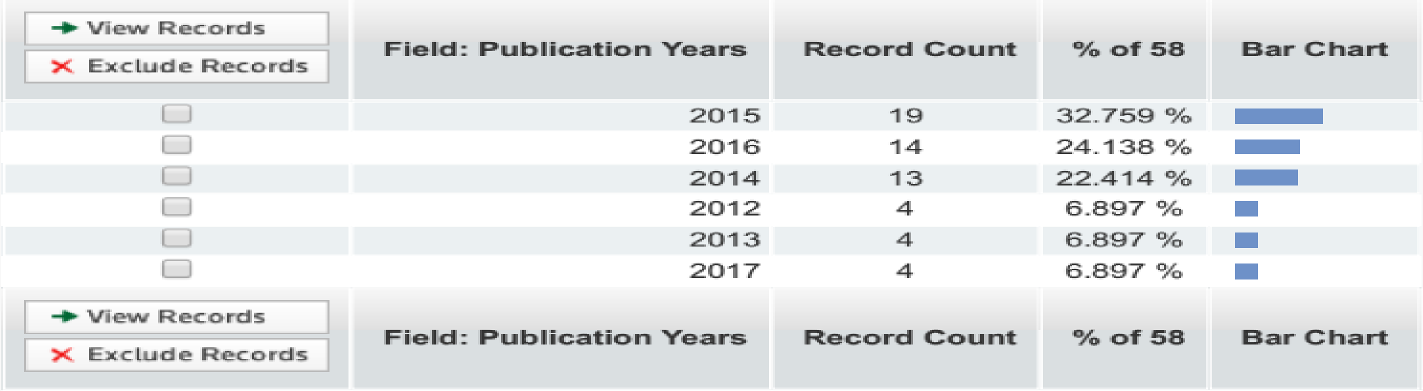
The spate, span and sophistication of Advanced Persistent Threats (APTs) have increased over the years. This form of cyber-attacks poses significant threats to global computers and network systems. As a result, the growing trend has been widely researched, discussed and reported in literature and conferences on APT. Therefore, analysis of recent publications presents a suitableindication of the current status of APTs in literature. Consequently, the author performed a Web of Science (WoS)search of APTpublications from the years 2012to2017. The search analyses examined the number of publications, research areas, document types, and source titles. The WoS search results returned a total of 58 high-qualitypeer-reviewed publications on APTs of which 77.6% were proceedings as presented Figure 6(a).



→ View Records ✕ Exclude Records	Field: Document Types	Record Count	% of 58	Bar Chart
☐	PROCEEDINGS PAPER	45	77.586 %	
☐	ARTICLE	12	20.690 %	
→ View Records ✕ Exclude Records	Field: Document Types	Record Count	% of 58	Bar Chart

Figure 6(a): WoS Documents Types on APTs (Web of Science, 2017)

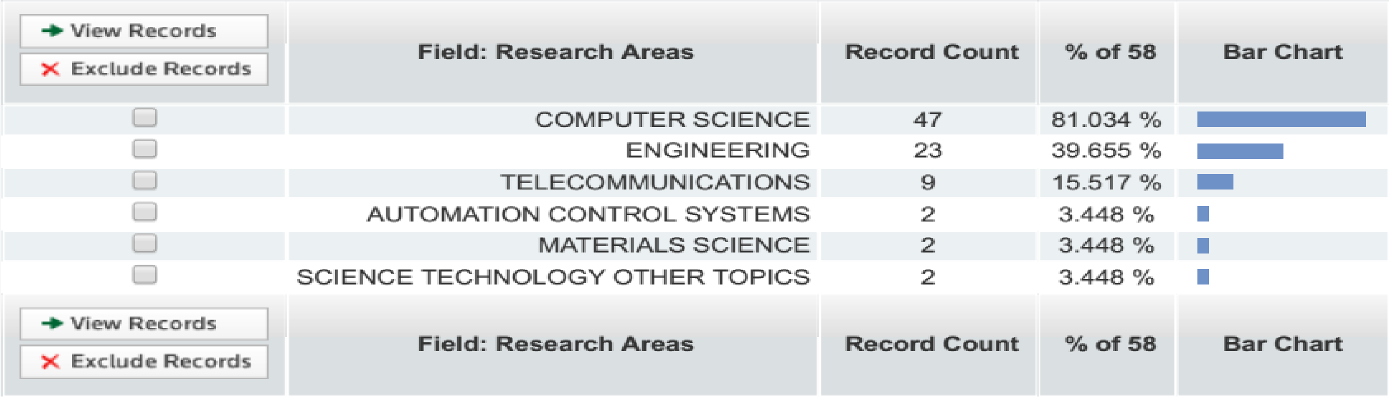
Figure 6(b) presents the results of the share of publications over the period examined.



→ View Records ✕ Exclude Records	Field: Publication Years	Record Count	% of 58	Bar Chart
☐	2015	19	32.759 %	
☐	2016	14	24.138 %	
☐	2014	13	22.414 %	
☐	2012	4	6.897 %	
☐	2013	4	6.897 %	
☐	2017	4	6.897 %	
→ View Records ✕ Exclude Records	Field: Publication Years	Record Count	% of 58	Bar Chart

Figure 6(b): WoS Publication Years on APTs (Web of Science, 2017)

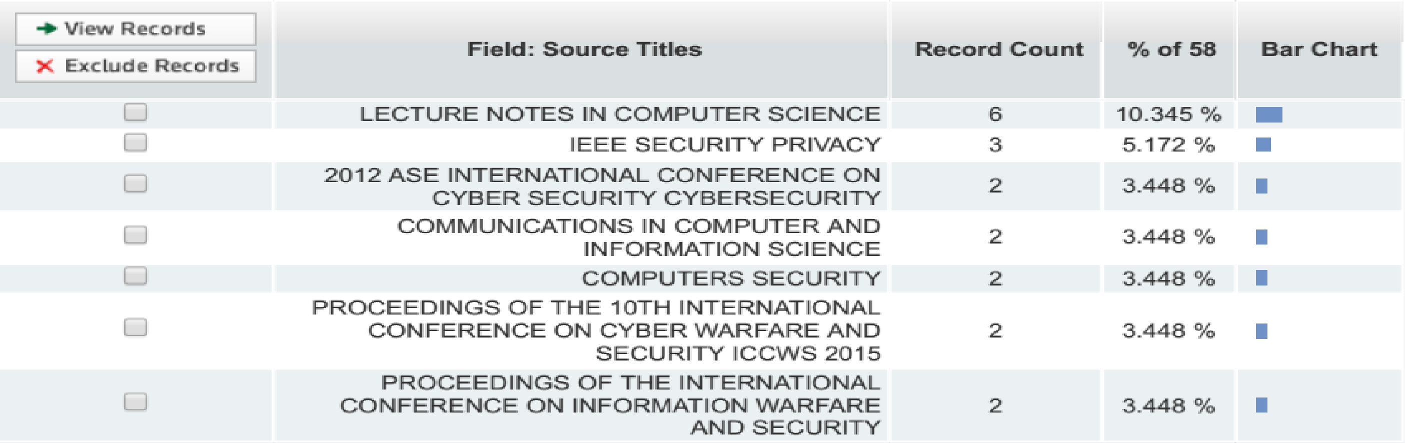
As observed the number of publications on APTs increased significantly from 2013 to 2014. This indicates that research interest in APT increased geometrically from6.9% in 2013to 32.8% in 2015. This is due to an increase in the spateand sophistication of APTs over the period of time examined. In addition, the analytics from GitHub indicate that APT and like cyber-attacks have soared geometrically over the years(GitHub, 2017).In addition, the results demonstrated that computer science, engineering and telecommunications accounted for the largest publications on the fieldinWoSas presented in Figure 6 (c).



→ View Records ✕ Exclude Records	Field: Research Areas	Record Count	% of 58	Bar Chart
☐	COMPUTER SCIENCE	47	81.034 %	
☐	ENGINEERING	23	39.655 %	
☐	TELECOMMUNICATIONS	9	15.517 %	
☐	AUTOMATION CONTROL SYSTEMS	2	3.448 %	
☐	MATERIALS SCIENCE	2	3.448 %	
☐	SCIENCE TECHNOLOGY OTHER TOPICS	2	3.448 %	
→ View Records ✕ Exclude Records	Field: Research Areas	Record Count	% of 58	Bar Chart

Figure 6(c): WoS Research Areas on APTs (Web of Science, 2017)

Furthermore, the source titles were examined to determine the publications that publish the most materials on APT in the WoS database. Figure 6(d) presents the source or publication titles that published the most materials on APTs in the period under examination.



→ View Records ✕ Exclude Records	Field: Source Titles	Record Count	% of 58	Bar Chart
□	LECTURE NOTES IN COMPUTER SCIENCE	6	10.345 %	■
□	IEEE SECURITY PRIVACY	3	5.172 %	■
□	2012 ASE INTERNATIONAL CONFERENCE ON CYBER SECURITY CYBERSECURITY	2	3.448 %	■
□	COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE	2	3.448 %	■
□	COMPUTERS SECURITY	2	3.448 %	■
□	PROCEEDINGS OF THE 10TH INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY ICCWS 2015	2	3.448 %	■
□	PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY	2	3.448 %	■

Figure 6(c): WoS Source Titles on APTs (Web of Science, 2017)

In summary, the WoS results indicated that there has been significant research and discussion on the APTs in industry and academia over the years. This is indicated the number of publications, research areas, document types, and source titles on APT over the years. Furthermore, this emphasizes the importance of APTs and the crucial need to address the menace of such cyber security threats. This can be achieved by establishing comprehensive cyber security orstrategic mitigation programmes to detect and protect global computers and IT networks from future APT attacks.

6. MITIGATIONSTRATEGIES

The growing menace of APTs has become a source of concern for cyber security industry over the years. This isdue to its attendant risk to the integrity of computers, systems and networks around the globe(Arsene, 2017). This is because the growing sophistication, spate and prevalence of APTs present significant risks to businesses, national and global security.This is corroborated by Thummala (2016)whopositsno industry is immune to the sophisticated nature of advanced malware and zero-day exploits used for APT attacks. However, the threats from APTs can be mitigated by adopting theappropriatecomputeranalytics (Brewer, 2014) and secure network solutions(Kumar and Kumar, 2014). In addition, the deployment of multiple security mechanisms ranging from network trafficintrospection, events log management and endpoint security measures can lower the risk of APT attacks(Arsene, 2017).Nonetheless, the challenges of addressing APTs particularly using conventional firewalls, anti-viral software, and intrusion recognition measures,are growing by the day.

Hence, Thummala (2016) proposes the adoption of "defense in depth" (D-in-D) approach to tackle the menace of APTs.Based on this approach, APTs can be addressed by adopting and deploying advanced tools, tactics and security frameworks. The approach seeks to reduce the impact of APTs before damage is done to the host network. In addition, the D-in-D approach has been described by Tankard (2011) as a potentially practical approach for mitigating the impact of APTs.In addition, other proponents of the approach(Lippmann *et al.*, 2006; Byres, 2008; Crossler *et al.*, 2017; Jayanthi, 2017), foresee it as an effective strategy to continuously monitor and control computer networks against future threats from APTs.

However, other studies have proposed the deployment of Advanced Persistent Security (APS) measures to curtail the effects of APTs. According to this strategy, networks or computer systems require round the clock monitoring to guard against potential attacks. This will involve persistentlymodifying cyber defences to imitate the dynamic environments of an APT(Zorz, 2017), thereby increasing the resources, cost and time required by hackers to compromise network systems (Arsene, 2017). Therefore, it is evident that the development and deployment of network security measures can provide some measure of protection from APTs (Kumar and Kumar, 2014). Nonetheless, more effort is required to stem the tide of growing cyber-attacks and prevent data breaches. The report by (Thummala, 2016) proposes other key measures to combat APTs using a six pronged approach. This involves creating Social Engineering Awareness, Shared Threat Intelligence, Skilled Resources, Malware Analysis, Behavioural Analytics, and lastly Next Generation Detection and Prevention Tools.However, the author is quick to note addressing the scourge of APTs will require tailor made "adaptable" solutions as well as incorporating all the aspects of the six pronged approach. This can be executed alongside a comprehensive information security strategy to adequately prepare, detect, contain, eradicate and handle future advanced threats.

In summary, the development and deployment of appropriate tools, techniques and strategies can potentially lower APT attacks and lower the damage from such cyber-attacks. However, this requires concerted efforts in detection, monitoring and control of network security systems and frameworks.

7. CONCLUSIONS

The paper presented an overview of current state ofAPTs, its core concept and characteristics. In addition, the critical challenges currently faced by organisations due to APT attacks on systems, networks and IT infrastructure was highlighted. Lastly, the potential strategies for mitigating this growing cyber menace of APTs were examined. The findings demonstrated that an APT is deliberate slow-moving cyber-attack designed to secretly compromise the security of interconnected computer systems. In addition, the term APT is an amalgamation of three rudimentary terms namely; Advanced, Persistent, and Threat. In principle, the aim of an APT is to target, penetrate and exploit host systems in order to gain vital information. The papers also highlighted the strategic importance of actors, targets and motives as critical factors in the concept of APT. Furthermore, the study examined the current status of APTs from the year 2012 to 2017 using the Web of Science (WoS) search data base. Hence, the number of publications, research areas, document types, and source titles within the period was examined. The query returned a total of 58 high-quality peer-reviewed publications on APTs indicating substantial research and discussion on the APTs in industry and academia.

In spite of this, the growing menace of APTs continues to pose problems for various organizations, states and businesses globally. The study revealed that APTs account for nearly 40% of all threats to computer networks globally costing entities between US$400 Billion to US1 Trillion annually. However, the threats from APTs can be mitigated by adopting the appropriate computer analytics and secure network solutions.The most widely proposed mitigation strategy is the defense in depth" (D-in-D) approach. Numerous authors have championed the (D-in-D) approach–as a holistic strategy to address APTs by deploying advanced tools, tactics and frameworks for implementing network security. In addition, the use of security mechanisms ranging from introspection of network traffic, events log management and endpoint security measures canalsolower the risk of APT attacks.

8. REFERENCES

[1] Abomhara, M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 4(1)**,** 65-88.

[2] Arsene, L. (2017). The Anatomy of Advanced Persistent Threats [Online]. USA: Dark Reading, UBM LLC Available: http://ubm.io/1xfLYhT [Accessed 5th August 2017].

[3] Ask, M., Bondarenko, P., Rekdal, J. E., Nordbo, A. and Ruthven, P. (2013). Advanced Persistent Threat (Apt) Beyond the Hype. Project Report in IMT4582 Network Security at GjoviN University College.

[4] Bodmer, S., Kilger, M., Carpenter, G. and Jones, J. (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw Hill Professional.

[5] Brewer, R. (2014). Advanced Persistent Threats: Minimising the Damage. Network Security, 2014(4)**,** 5-9.

[6] Byres, E. (2008). Defense in Depth. Control Engineering Asia June 2008.

[7] Choi, J., Choi, C., Lynn, H. M. and Kim, P. (2015) Published. Ontology Based Apt Attack Behavior Analysis in Cloud Computing. Broadband and Wireless Computing, Communication and Applications (BWCCA), 2015 10th International Conference on, 2015. IEEE, 375-379.

[8] Choo, K.-K. R. (2007). Zombies and Botnets. Trends & Issues in Crime & Criminal Justice, (333).

[9] Cobb, M. (2013). Advanced Persistent Threats: The New Reality [Online]. USA: Venafi Next. Available: http://bit.ly/2vrUuxZ [Accessed 6th August, 2017].

[10] Command Five. (2012). Command and Control in the Fifth Domain [Online]. Germany: Command Five Pty Ltd. [Accessed 7th August, 2017].

[11] Crossler, R. E., Bélanger, F. and Ormond, D. (2017). The Quest for Complete Security: An Empirical Analysis of Users' Multi-Layered Protection from Security Threats. Information Systems Frontiers**,** 1-15.

[12] Dean, G., Bell, P. and Newman, J. (2012). The Dark Side of Social Media: Review of Online Terrorism. Pakistan Journal of Criminology, 3(3)**,** 103-122.

[13] Dimaggio, J. (2016). The Black Vine Cyber-Espionage Group [Online]. USA: Symantec Security. Available: http://symc.ly/1D9K59m [Accessed 11 August, 2017].

[14] Fire Eye. (2017). Advanced Persistent Threat Groups [Online]. USA: FireEye CyberSecurity. Available: http://bit.ly/2wNPn8t [Accessed 11th August, 2017].

[15] Friedberg, I., Skopik, F., Settanni, G. and Fiedler, R. (2015). Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection. Computers & Security, 48**,** 35-57.

[16] GitHub. (2017). Aptnotes [Online]. USA: GiTHub Inc. Available: http://bit.ly/1zL88YN [Accessed 11th August, 2017].

[17] Industrial Control Systems. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid [Online]. Washington DC, USA: Electricity Information Sharing and Analysis Centre (E-ISAC). Available: http://bit.ly/2ohNwJ1 [Accessed 6th August, 2017].

[18] Jayanthi, M. (Year) Published. Strategic Planning for Information Security-Did Mechanism to Befriend the Cyber Criminals to Assure Cyber Freedom. Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on, 2017. IEEE, 142-147.

[19] Jover, R. P. and Giura, P. (2013). How Vulnerabilities in Wireless Networks Can Enable Advanced Persistent Threats. International Journal on Information Technology (IREIT), 1(2)**,** 145-151.

[20] Kumar, G. and Kumar, K. (2014). Network Security–an Updated Perspective. Systems Science & Control Engineering: An Open Access Journal, 2(1)**,** 325-334.

[21] Lemay, A. (2013). Defending the Scada Network Controlling the Electrical Grid from Advanced Persistent Threats. PhD, École Polytechnique de Montréal.

[22] Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. International Security, 39(3)**,** 7-47.

[23] Lippmann, R., Ingols, K., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M. and Cunningham, R. (Year) Published. Validating and Restoring Defense in Depth Using Attack Graphs. Military Communications Conference, 2006. MILCOM 2006. IEEE, 2006. IEEE, 1-10.

[24] Lock, A. (2017). Cyber Security: The Changing Threat Landscape in Oil and Gas [Online]. United Kingdom (UK): Palladian Publications Ltd. Available: http://bit.ly/2wuFfRB [Accessed 6th August, 2017].

[25] Mandiant. (2017). Apt1: Exposing One of China's Cyber Espionage Units [Online]. USA: Fire Eye Securities. Available: http://bit.ly/2ookhjX [Accessed 11th August, 2017].

[26] Martin, S. (2016). 8 Active Apt Groups to Watch [Online]. USA: Dark Reading UBM LLC. Available: http://ubm.io/2wNAzGI [Accessed 11th August, 2017].

[27] McAfee. (2005). Mcafee Virtual Criminology Report. Santa Clara CA, United States. McAfee Securities.

[28] NIST. (2017). Managing Information Security Risk Organization, Mission, and Information System View [Online]. USA: US Department of Commerce. Available: http://bit.ly/2iPT4qI [Accessed 5th August, 2017].

[29] Operation Pawn Storm. (2016). Operation Pawn Storm: Fast Facts and the Latest Developments [Online]. USA: TREND Micro. Available: http://bit.ly/2fwXLFW [Accessed 11th August, 2017].

[30] Radware. (2015). Global Application & Network Security Report 2015-2016, [Online]. San Francisco, USA: Radware Cyber Security Limited. Available: http://bit.ly/2vC8Ufw [Accessed 5th August, 2017].

[31] Rattray, G. and Healey, J. (Year) Published. Categorizing and Understanding Offensive Cyber Capabilities and Their Use.

Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy, 2010.

[32] Rattray, G. J. (1994). Explaining Weapons Proliferation: Going Beyond the Security Dilemma. DIANE Publishing.

[33] Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. International Journal of Intelligence & CounterIntelligence, 26(3)**,** 453-481.

[34] Secureworks. (2017). Advanced Persistent Threats: Learn the ABCs of Apts - Part A [Online]. USA: SecureWorks Inc. Available: http://bit.ly/2v8k9e1 [Accessed 6th August, 2017].

[35] Sood, A. K. and Enbody, R. J. (2013). Targeted Cyberattacks: A Superset of Advanced Persistent Threats. IEEE Security &Privacy, 11(1)**,** 54-61.

[36] Tankard, C. (2011). Advanced Persistent Threats and How to Monitor and Deter Them. Network Security, 2011(8)**,** 16-19.

[37] Thummala, J. B. (2016). Defending Advanced Persistent Threats - Be Better Prepared to Face the Worst [Online]. USA: Happiest Minds Technologies. Available: http://bit.ly/2vBIvgM [Accessed 6th August, 2017].

[38] Virvilis, N., Gritzalis, D. and Apostolopoulos, T. (2013) Published. Trusted Computing Vs. Advanced Persistent Threats: Can a Defender Win This Game? In: Martino, B. D., ed. 2013 IEEE 10th international conference on and 10th international conference on autonomic and trusted computing (uic/atc), 2013 Napoli, Italy. Italy: IEEE, 396-403.

[39] Web of Science. (2017). Results Analysis "Advanced Persistent Threats" [Online]. USA: CLARIVATE ANALYTICS Available: http://bit.ly/2vVYTJc [Accessed 11th August, 2017].

[40] Zorz, Z. (2017). Advanced Persistent Security [Online]. USA: Helpnet Security. Available: http://bit.ly/2hR2ZNj [Accessed 12th August, 2017].