ADVANCED PERSISTENT THREATS (APT): AN AWARENESS REVIEW

Hussin J. Hejase, Senior Researcher, Beirut, Lebanon
Hasan F. Fayyad-Kazan, Al Maaref University, Management Information Technology, Beirut, Lebanon,
Imad Moukadem, Al Maaref University, Compuetr Science, Beirut, Lebanon

ABSTRACT

COVID-19 pandemic has become a major threat to all institutions, irrespective of its economic role, private and public, by threatening all the functions capitalizing on the Information and Communications Technology (ICT) infrastructure, networks, systems and Internet-based solutions including Internet of Things and Cloud computing. The field is open to advanced persistent threats (APTs) whereby the outcomes may become very costly to all institutions and governments across the globe. This paper aims to shed light on the premises of APT in order to provide awareness to what it is, understanding its functions and how to mitigate its impact on institutions of all sizes. The approach is based on descriptive analysis based on secondary data reported in books, journals, websites and blogs. The outcomes are presented as an eye opener to the current status-quo of systems and networks and how to remedy the aforementioned threats.

Keywords: Advanced Persistent Threat, APT, ICT, Life Cycle, Mitigation, Cyberattacks.

INTRODUCTION

An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an unauthorized person (an intruder) gains access to a network and stays there undetected for a long period of time (Rouse, 2020; Gonzalez, 2014). According to Jeun, et al. (2012), APT is an invention by a community involved in cyber-espionage to steal information for monetary gains. It was first coined by the United States Air Force in 2006 to describe sophisticated cyber-attacks against specific targets over long periods (Murray, 2011); (Websense, 2011); (Chen, et al., 2014); (Radzikowski, 2015); (Khan & Khan, 2019).

Accordingly, APTs are a sophisticated (Karthik, 2013); (Drew, 2014); (Radzikowski, 2015); Khan & Khan, 2019) cyberattack that use multi stage techniques (Jeun, et al. 2012); (Gonzalez, 2014); (Khan & Khan, 2019) to target and compromise systems that often go undetected for months (Karthik, 2013; Khan & Khan, 2019). Jeun, et al. (2012), contend that these attacks are sometimes so advanced, that even organizations with cutting edge cyber defenses are vulnerable. Google, Adobe Systems, Juniper Networks, and Symantec were all victims of an APT attack called Operation Aurora (Fortinet, 2014; (Radzikowski, 2015); (Khan & Khan, 2019); (Matthews, 2019).

Khan & Khan (2019) assert that APT attackers aim to gain economic (Karthic, 2013; Rouse, 2020), political, and strategic advantage through stealing information from the critical infrastructure and critical resources. APTs target particular organizations (Karthik, 2013; Virvilis et al., 2013). In fact, Rouse (2020) asserts that APT targets sectors such as national defense, manufacturing and the financial industry, as those companies deal with high-value information, including intellectual property, military plans, and other data from governments and enterprise organizations.

Chen et al. (2014) provide a set of differences between common malware and advanced persistent threat attach as shown in Table 1.

Table 1
DIFFERENCES BETWEEN AN ADVANCED PERSISTENT THREAT (APT) ATTACK AND COMMON MALWARE ATTACKS

Feature	APT Attacks	Common Malware Attacks
Definition	Sophisticated, targeted, highly organized	Malicious software used to attack and disable any system
Attacker	Government actors and organized criminal groups	A cracker (a hacker in illegal activities)
Target	Diplomatic organizations, information technology industry and other sectors	Any personal or business computer
Purpose	Filter confidential data or cause damage to specific target	Personal recognition
Attack Life Cycle	Maintain persistence as possible using different ways	Ends when detected by the security actions (e.g., anti-virus software)

Source: Chen et al. (2014).

In a summary, and according to Quadri & Khan (2019), APT are sophisticated, professional, state-supported and systematic cyber-attack programs that continue for an extended period and in which a group of skilled hackers coordinates to design the attack with a particular motive, targeting specific information in high-profile companies and governments. They seek privilege escalation and perimeter expansion using malware-laden email or malware-infested USB drives and then hide inside the critical systems to collect intellectual property and other asset information for further sabotage or corporate espionage.

APT Life Cycle

Many different researchers, IT groups and IT solution suppliers including government specialized groups have developed an array of anti-APT solution life cycle methodologies in their quest to study, analyze and mitigate the negative impacts of APT, and to develop appropriate security policies across the globe. Nevertheless, it is beneficial here to show as well the array of APT life cycles used to take over the attacked systems. According to Karthik (2013, February 21), finding a proven pattern to find defects early in an organization’s cycle saves not just money but also the time required to patch those defects.

Gonzalez (2014) quoting Cobb, assert that the APT life cycle consists of 6 phases: reconnaissance, spear phishing attacks, establishing presence, exploration and pivoting, data extraction, and maintaining persistence. Also, Bere et al. (2015) assert that APTAs are sophisticated multistep cyberattacks and to successfully infiltrate a network APTs follow a 6-stages attack: Choosing a victim, reconnaissance, delivery, exploitation, operation, data collection and exfiltration (Virvilis et al., 2013).

Indeed, it has been suggested that most sophisticated attackers, regardless of their motives, funding or control, tend to operate in a certain cycle when attacking their targets. Figure 1 shows the evolution of APTs and outlines the APT Life Cycle.

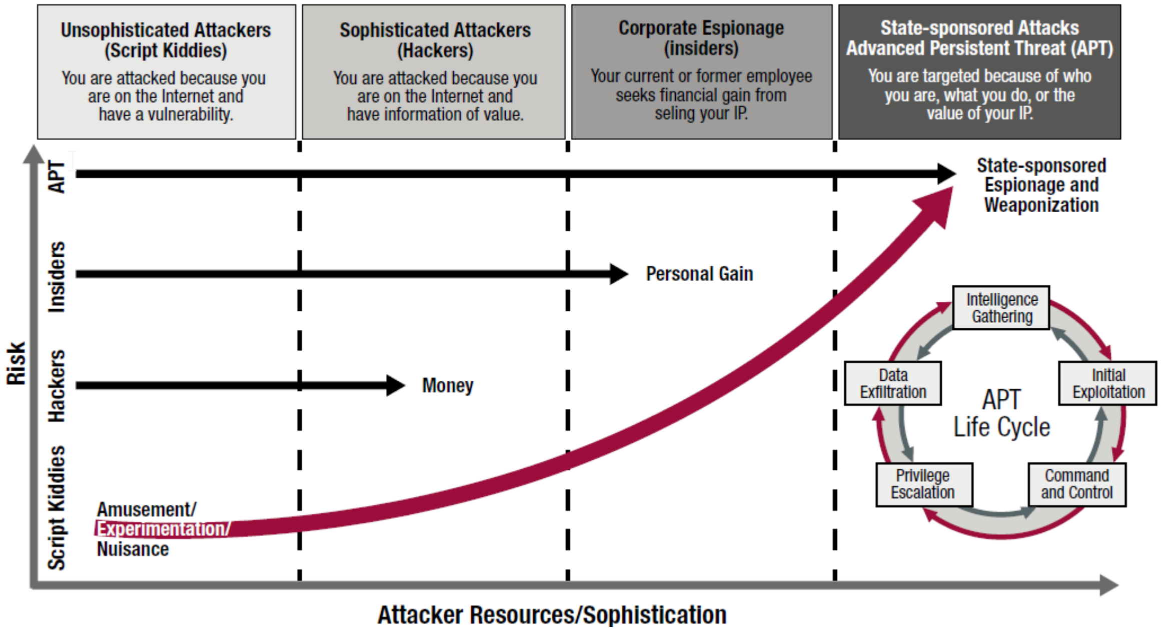

Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.
Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.
Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.
State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.
Risk
APT
Insiders
Hackers
Script Kiddies
State-sponsored Espionage and Weaponization
Personal Gain
Money
Amusement/ Experimentation/ Nuisance
Intelligence Gathering
Initial Exploitation
Command and Control
Privilege Escalation
Data Exfiltration
APT Life Cycle
Attacker Resources/Sophistication

FIGURE 1
EVOLUTION OF APT AND APT LIFE CYCLE

Source: (ISACA, 2013; Radzikowski, 2015).

According to Radzikowski (2015), APTs represent a fundamental shift compared to the high-profile hacking events of prior years that commonly targeted networks. Focusing on the weakest links of one’s defense chain, APTs target specific system vulnerabilities and, more importantly, specific people. While the victimized organizations vary in size, type, and industry, the individuals they [APTs] target usually fit the same profile: people with the highest-level access to the most valuable assets and resources (Villeneuve & Bennett, 2012).

Mediating APTs

“*Cybersecurity professionals find themselves struggling to keep up with technical innovation as learning resources for would-be hackers have increased and are often freely available online. The Metasploit framework has revolutionized vulnerability testing, making powerful vulnerability scanners freely available to anyone who calls themselves a penetration tester*” (ISACA, 2013). According to Holik et al. (2014), Metasploit framework performs a penetration test, that is, it simulates an attacker's malicious activity. However, in order to keep a proactive stance against cyberattacks, simulation of malicious activities is performed as a major function in the development of appropriate solutions. This is where threat modeling comes to close the gaps to the detected vulnerabilities of the existing software and IT systems. Threat modeling is a tested and proven method (Shevchenko, 2018) to meet the aforementioned objective.

Threat Modeling

According to EC-Council (2020), "*Threat modeling can be defined as a structured process in which IT professionals and cybersecurity experts can detect likely security vulnerabilities and threats, measure the severity of each potential impact, and prioritize methods to protect IT infrastructure and mitigate attacks*" (Para 2). Furthermore, "*threat modeling methodologies can be applied to develop:*

1. *A collection of probable threats that may arise*
2. *An abstraction of the system*
3. *The profiles of likely malicious attackers, their goals, and techniques*" (ibid).

For example, "*threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It's an engineering technique one can use to help identify threats, attacks, vulnerabilities, and countermeasures that could affect one's application. Threat modeling is used to shape one's application's design, meet the company's security objectives, and reduce risk*" Microsoft (2020). For the aforementioned purpose, there are five major threat modeling steps: Defining security requirements; creating an application diagram; identifying threats; mitigating threats, and validating that threats have been mitigated.

Threat modeling should be part of one's routine development lifecycle, enabling the end user to progressively refine one's threat model and further reduce risk. In Fact according to Microsoft (2020), "*the Threat Modeling Tool*" enables any developer or software architect to:

1. Communicate about the security design of their systems.
2. Analyze those designs for potential security issues using a proven methodology.
3. Suggest and manage mitigations for security issues.

The Kill Chain

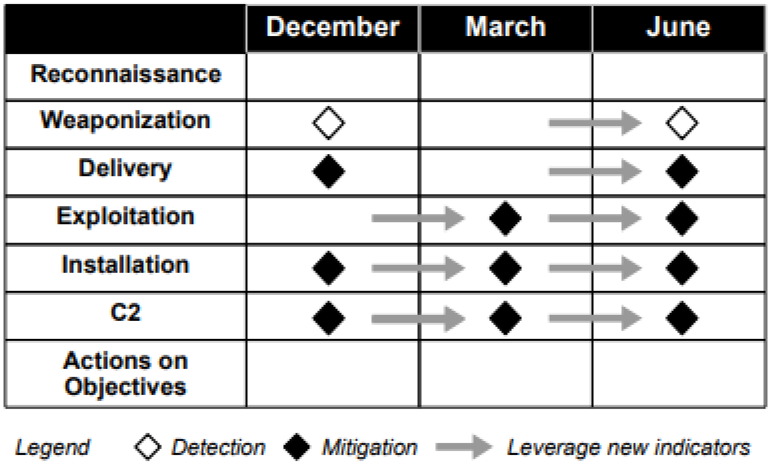
Smart (2011) introduced a United States Department of Defense Joint Staff methodology labeled, "*kill chain*" as a "*guide to cyber targeting in five key areas: (1) positive identification of targets, (2) location of targets, (3) attribution of attack, (4) capability/target pairing, and (5) assessment of potential collateral damage*" (p.70).

According to Smart (2011), an updated 'JP 3-60' approach should "*introduce the concepts of an adversary's cyber center of gravity and a cyberspace joint operations area. An adversary's cyber presence consists of computers, information systems, hardware, online personas, and so forth, which may be geographically separated from his physical center of gravity. Once planners identify the cyber center of gravity (a critical point—a source of power for the adversary's cyber operations), they can target it*" (p. 72).

Effective Defense against Intrusion

Hutchins, et al. (2011) contends that defenders against APTs can generate metrics to build systems' resiliency by measuring the performance and effectiveness of defensive actions against the cyberattacks and intruders. They provide an example whereby "*a series of intrusion attempts from a single APT campaign that occurs over a seven month timeframe Figure 2.*

For each phase of the kill chain, a white diamond indicates relevant, but passive, detections were in place at the time of that month's intrusion attempt, a black diamond indicates relevant mitigations were in place, and an empty cell indicates no relevant capabilities were *available. After each intrusion, analysts leverage newly revealed indicators to update their defenses, as shown by the gray arrows*" (p. 6).



	December	March	June
Reconnaissance			
Weaponization	◇		→ ◇
Delivery	◆		→ ◆
Exploitation		→ ◆	→ ◆
Installation	◆	→ ◆	→ ◆
C2	◆	→ ◆	→ ◆
Actions on Objectives			

Legend ◇ *Detection* ◆ *Mitigation* → *Leverage new indicators*

FIGURE 2
ILLUSTRATION OF THE RELATIVE EFFECTIVENESS OF DEFENSES AGAINST SUBSEQUENT INTRUSION ATTEMPTS (HUTCHINS ET AL., 2011)

Therefore, by framing metrics in the context of the kill chain, defenders had the proper perspective of the relative effect of their defenses against the intrusion attempts and where there were gaps to prioritize remediation (Hutchins et al. 2011).

Examples of Advanced Persistent Threats

Usually, APT intruders use advanced attack methods to gain access to the targeted institution including advanced exploits of zero-day vulnerabilities, highly-targeted spear phishing and other social engineering techniques (Rouse, 2020). To maintain continuous access to the targeted network without being discovered, intruders or cyber-attackers "*use advanced methods, including continuously rewriting malicious code to avoid detection and other sophisticated evasion techniques. Some APTs are so complex that they require full-time administrators to maintain the compromised systems and software in the targeted network*" (Rouse, 2020).
APTs are usually assigned names by their discoverers, though many advanced persistent threat attacks have been discovered by more than one researcher, so some are known by more than one name. Table 2 depicts a summary of the examples.

Detecting APTs

Advanced persistent threats have certain warning signs despite typically being very hard to detect. An organization may notice certain symptoms after it has been targeted by an APT, including (Rouse, 2020):

1. Unusual activity on user accounts
2. Extensive use of backdoor Trojan horse malware, a method that enables APTs to maintain access; odd or uncharacteristic database activity, such as a sudden increase in database operations involving massive quantities of data; and
3. Presence of unusual data files, which may indicate data that has been bundled into files to assist in the exfiltration process.

4. Detecting anomalies in outbound data is perhaps the best way for cybersecurity professionals to determine if a network has been the target of an APT attack.

Table 2
EXAMPLES OF APTS

Name/Identification	Functionality	Country of Origin
Moonlight Maze 1999	Penetrated systems at the Pentagon, NASA and U.S. Department of Energy, as well as universities and research labs involved in military research	Not definite
Several APTs 2003	Against U.S. government targets in an attempt to steal sensitive state secrets, military data from high-end systems of government agencies, including NASA and the FBI	China: Titan Rain campaign
The Sykipot APT malware family 2006	Collecting and stealing secrets and intellectual property, including design, financial, manufacturing and strategic planning information. The attacks employ spear-phishing emails containing a malicious attachment or a link to an infected website, as well as zero-day exploits. [Attack on UK & USA]	China
GhostNet cyberespionage operation 2009	Used spear phishing emails containing malicious attachments. Gaining access to the network devices of government ministries and embassies.	China
Stuxnet worm 2010	Used to attack Iran's nuclear program. The malware targeted SCADA (supervisory control and data acquisition) systems and was spread with infected USB devices	USA & Israel
Duqu 2011	Captured information such as keystrokes and system information, most likely for the purpose of enabling a future APT attack on industrial control systems.	Server addresses scattered across many countries, including Germany, Belgium, the Philippines, India and China
Flame: Sophisticated cyber espionage 2012	Attacks on governmental ministries, educational institutions and individuals in Middle Eastern countries, infecting around 1,000 machines in Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.	U.S. National Security Agency, CIA and Israel’s military
Eurograbber	Via phishing attemps. Stolen an estimated 36 million euro from more than 30,000 customers in over 30 banks across Europe. The attacks began in Italy and quickly spread to Spain, Germany and Holland.	Customized variants of the Zeus, SpyEye, and CarBerp Trojans
APT-28	Attacks against military and government targets in Eastern Europe, including Ukraine and Georgia, as well as campaigns targeting NATO organizations and U.S. defense contractors	Russian groups: Fancy Bear, Pawn Storm, Sofacy Group and Sednit
APT-29 2015 & 2016	Spear phishing attack on the Pentagon, as well as the 2016 attacks on the Democratic National Committee	Russian Cozy Bear
APT-34 2017	Targeted companies in the Middle East with attacks against financial, government, energy, chemical and telecommunications companies.	Iran Group: FireEye
APT-37 2017	Spear phishing attacks exploiting an Adobe Flash zero-day vulnerability	North Korea: Reaper, StarCruft and Group 123
Ransomware 2007 Ongoing	200 cyber incidents targeting financial institutions since 2007	Multiple countries

Collected from Rouse (2020); IT Business Edge (2020); (Hejase & Hejase, 2011); (Paganini, 2012); (Lyles, 2017); (Carnegie Endowment, 2020).

CONCLUSION

Organizational awareness and having top management with technology and information literacy presiding over an institution are the first building blocks to proactively mitigate threats against the organizational cybersecurity. In fact, "*administrators must learn how to use emerging technology effectively so that it actually provides additional protection*" (Cobb, 2013). Moreover, Quintero-Bonilla & del Rey (2020) warn that "*the increasing development of sophisticated tools used by cybercriminals, such as zero-day vulnerabilities and denial of service (DoS) attacks, conventional solutions cannot cope with the current complexity of these types of threats*" (Quintero & Martin 2020). Furthermore, they assert that "*cybersecurity is responsible for establishing security policies; these policies set out the steps to follow for data to be managed within the technological infrastructure in an organization. However, some security flaws and vulnerabilities (e.g., the use of outdated equipment, use of policies that are not reviewed continuously, failing to install updates at time, awareness deficiency) allow attackers to realize an intrusion in an organization*" (Quintero & Martin 2020).

Radzikowski (2015) recommends that "*advance incident response planning can significantly improve organizational chances of early detection and more effective remediation. The key to effective APT protection, detection, and response is rigorous implementation of security best practices and ongoing education with your most highly targeted users.*

On the other hand, Hejase & Hejase (2015) stress that fact that government, businesses and educational institutions should join efforts to at least start an awareness campaign that may reach all ears in order to get the terms cyberwarfare, cyber-attacks, cybersecurity and cyber-weapons into the dictionary of every day words, simply because "the threat of a cyber-attack is ever present and will not go away" (p. 87).

REFERENCES

Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). How advanced persistent threats exploit humans. *International Journal of Computer Science Issues (IJCSI)*, *12*(6), 170.

Carnegie Endowment. (2020). *Timeline of Cyber Incidents Involving Financial Institutions*. Retrieved December 3, 2020, from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Chen, P., Desmet, L., & Huygens, C. (2014, September). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security* (pp. 63-72). Springer, Berlin, Heidelberg.

Chen, P., Desmet, L., & Huygens, C. (2014, September). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security* (pp. 63-72). Springer, Berlin, Heidelberg.

Cobb, M. (2013). The evolution of threat detection and management. *Search Security*. Retrieved December 5, 2020, from https://searchsecurity.techtarget.com/tip/The-evolution-of-threat-detection-and-management

Fortinet. (2013). Threats on the Horizon: The Rise of the Advanced Persistent Threat. *IT World Canada*. Retrieved December 2, 2020, from https://s3-us-west-2.amazonaws.com/itworldcanada/archive/Documents/whitepaper/ITW274A_Persistent_Threats.pdf

Gonzalez, D. (2014). *Managing online risk: Apps, mobile, and social media security*. Butterworth-Heinemann.

Hejase, Ale J., & Hejase, Hussin J. (2011). *Foundations of Management Information Systems* (1st edn.), Beirut, Lebanon: Dar Sader. ISBN: 978-9953-13-719-3

Hejase, A.J., Hejase, H.J., & Hejase, J.A. (2015). Cyber warfare awareness in Lebanon: Exploratory research. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *4*(4), 482-497.

Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014). Effective penetration testing with Metasploit framework and methodologies. In *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)* (pp. 237-242). IEEE.

Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(1), 80.

ISACA. (2013). *Responding to Targeted Cyberattacks*. ERNST & Young and ISACA. Rolling Meadows, IL, USA: ISACA.

IT Business Edge. (2020). *The Most Famous Advanced Persistent Threats in History*. Retrieved December 4, 2020, fromhttps://www.itbusinessedge.com/slideshows/the-most-famous-advanced-persistent-threats-in-istory.html

Jeun, I., Lee, Y., & Won, D. (2012). A practical study on advanced persistent threats. In *Computer applications for security, control and system engineering* (pp. 144-152). Springer, Berlin, Heidelberg.

Karthik (2013). Advanced Persistent Threats – Attack and Defense. *Infosec* [Blog]. Retrieved December 5, 2020, from https://resources.infosecinstitute.com/topic/advanced-persistent-threats-attack-and-defense/#:~:text= Advanced%20 Persistent%20Threats%20(APT)%20was,in%20nature%2C%20and%20evasive%20too

Quadri, A., & Khan, M.K. (2019). The G-War: Race for Technological Supremacy in 5G and 6G The G-War: Race for Technological Supremacy in 5G and 6G. *Policy*.

Lyles, Shawn (2017). What are Advanced Persistent Threats and Why Should your Organization Care? *CGNET* [Blog]. Retrieved December 1, 2020, from https://cgnet.com/blog/advanced-persistent-threats-organization-care/

Matthews, Tim (2019). Operation Aurora – 2010's Major Breach by Chinese Hackers. *Exabeam*. Retrieved December 3, 2020, from https://www.exabeam.com/information-security/operation-aurora/

Microsoft. (2020). *Security Engineering: The STRIDE Model*. Retrieved December 3, 2020, from https://www .microsoft.com/en-us/securityengineering/sdl/threatmodeling#:~:text=The%20Microsoft%20Threat% 20Modeling%20Tool,structure%20of%20their%20software%20design

Murray, Patrick (2011). Advanced Persistent Threats: From FUD to FACTS. Websense Brief. Retrieved November 28, 2020, from https://www.websense.com/assets/html/apt/apt-overview-from-fud-to-facts.pdf

Paganini, Pierluigi (2012). How were stolen 36M euro with Eurograbber malware? *Security Affairs*. Retrieved December 3, 2020, from https://securityaffairs.co/wordpress/10876/cyber-crime/how-were-stolen-36m-euro-with-eurograbber-malware.html

Quintero-Bonilla, S., & Martín del Rey, A. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*, *10*(11), 3874.

Rouse, Margaret (2020). Advanced Persistent Threat (APT). *Tech Target*. Retrieved November 28, 2020, from https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

Radzikowski, Shem (2015). *Cybersecurity: Origins of the Advanced Persistent Threat (APT)*.

Rid, T. (2013). Cyberwar and peace: Hacking can reduce real-world violence. *Foreign Affairs*, *92*(6), 77-87.

Smart, S.J. (2011). *Joint targeting in Cyberspace*. Judge advocate general (air force) washington dc.

Villeneuve, N., & Bennett, J. (2012). Detecting apt activity with network traffic analysis. *Trend Micro Incorporated Research Paper*, 1-13.

Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?. In *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing* (pp. 396-403). IEEE.

Websense. (2011). *Advanced Persistent Threats and Other Advanced Attacks: Threat Analysis and defense Strategies for SMB Midsize and Enterprise Organizations*. Retrieved November 28, 2020, from https://www.academia.edu/8564302/A_Websense_White_Paper_advanced_persistent_threats_and_other_advanced_attacks_threat_analysis_and_defense_strategies_for_smb_mid_size_and_enterprise_organizations_advanced_persistent_threats_and_other_advanced_attacks