BOOK CHAPTER | Resilient Threats

Understanding Advanced Persistent Threats

Akuffo-Badoo Erastus B.
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: erastusakuffo1@gmail.com
Phone: +233504979293

ABSTRACT

Advanced Persistent Threats (APTs) are a new type of threat that has piqued the interest of experts, particularly in the industrial security industry. APTs are cyber-attacks carried out by skilled and well-resourced adversaries who target specific information in high-profile organizations and governments, usually as part of a multi-step operation. The academic community has largely ignored the specifics of these threats, and as a result, an objective solution to the APT problem is absent. In terms of cybercrime activity, Africa has been one of the fastest rising regions. The continent is also a major source of cyberattacks on the rest of the world. A number of initiatives, however, have been implemented to mitigate cyber-threats and strengthen cybersecurity across the continent. The results of a complete study on APT are presented in this paper, which characterizes its differentiating traits and attack model while also assessing strategies often used in APT attacks. We also list various non-traditional countermeasures that can aid in the mitigation of APTs, highlighting future research prospects.

Keywords : Advanced Persistent Threat, APT(s), Sophisticated Attacks, Cyber Security, Africa

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Akuffo-Badoo Erastus B. (2022). Understanding Advanced Persistent Threats . SMART-IEEE-Creative Research Publications Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 15-22. www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P3

1. INTRODUCTION

An advanced persistent threat is an attack in which an unauthorized person gets access to a computer system or network and persists there without being noticed for a lengthy period of time. In utmost circumstances, advanced persistent attacks do not cause impairment to enterprise networks or stand-alone PCs. The general intent of high-level persistent attacks is data thievery. Hacking the network, evading detection, devising an attack strategy, mapping corporate data to identify where the desired data is most accessible, obtaining sensitive company data, and exfiltrating that data are all common aspects of advanced persistent threats (*"Advanced Persistent Threat, An Overview of APT"*, 2018).

Advanced persistent threats are notorious for their ability to fly under the radar, undetected by typical security measures, and have been responsible for numerous significant, costly data breaches. Furthermore, as cyber thieves seek more complex methods to fulfill their objectives, advanced persistent attacks are becoming more widespread. To get initial access to a network, advanced persistent threats employ a variety of methods (Adelaiye et al., 2018). Attackers may utilize the internet to spread malware and obtain access to more secure networks, as well as physical malware infection and external subjugation (Alshamrani et al., 2019). Viruses and malware are some of the various forms of attack, that have a constant pattern of activity and may be recycled to attack other systems or businesses. Advanced persistent threats do not strike in a wide, generalized way; instead, they're meticulously organized and targeted to target a single corporation or organization. Given this, advanced persistent attacks are extremely differentiated and intelligent, with the aim of bypassing the existing security procedures of an organization.

2. RELATED LITERATURE

Advanced Persistent Threats are one of the primary worries that are delicate in cyber assaults on a global scale (Ghafir et al., 2018). Until the analysis of information that defines the major characteristics of an attack, APT employed a kill chain and an attack life-cycle (Alshamrani et al., 2019) the authors employed seven separate phases of APT in their study (Hutchins et al., 2011), which were reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on goals. The three primary phases eminent in describing the main characteristics of an APT, according to (Ussath et al., 2016), are the initial compromise, lateral movement, and command-and-control activities. Furthermore, the authors developed an attack life cycle model based on the experiences gained during a campaign that included eight phases: initial reconnaissance, first compromise, establishing a foothold, escalation privileges, internal reconnaissance, moving laterally, maintaining a presence, and completing the mission (Staff et al., 2016; Mandient, 2013).

For Advanced Persistent Threats, several approaches are utilized; some organizations use espionage vectors such as social engineering, human intelligence, and penetration to obtain access to a physical site and allow network assaults. This is done so that specialized malicious software may be installed for malicious assaults. Traditional assaults and APT attacks (Khaleefa & Abdulah, 2022), both of which are founded on the concept of a target, the attacker, target zone, aim, and work either run singly and within a short period or repeated efforts that run slowly and low, may be used to determine whether an attack is purposeful APT or not (Khaleefa & Abdulah, 2022). There are many more APTs have been identified and labeled, with new ones being discovered all the time. Due to the difficulty and expense of launching APT assaults, the entities behind them typically target high-value targets such as government agencies or major corporations.

Their objectives frequently include espionage, data theft, and sabotage. Three major mechanisms can be used to embark upon APT attacks at various stages (Lu-Xing et al., 2021) which are the countermeasures to reconnaissance defense, lateral movement defense, quarantine, and recovery schemes which are dynamic in the minimal impact of APT. (Marchetti et al., 2016) presented a unique framework that integrates various methodologies based on big data analytics and security intelligence to assist human analysts in prioritizing the most vulnerable hosts and that collecting and integrating internal and external indications is a step

forward in the field of early identification and mitigation of APT activities compared to the current state of the art. The proposed approach represents a step forward concerning the state of the art and paves the way for novel methods for early detection and mitigation of APTs.

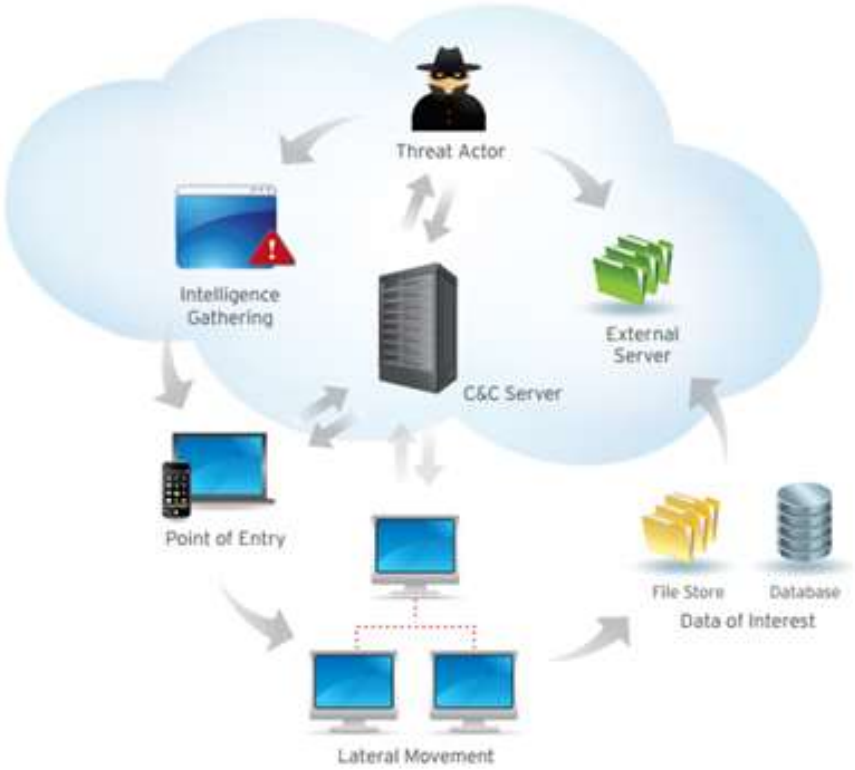

Figure 1: Anatomy of an APT attack (Anatomy of an APT Attack:
(Source: Step by Step Approach, 2021)

3. RESEARCH GAPS/FINDINGS

The majority of the proposed solutions are vague, recommending only generic tactics such as host-based intrusion detection systems (HIDS), network-based intrusion detection systems (NIDS), patch management, and security awareness training even though the suggested framework employs multi-factor techniques in which big data analytics methods are applied to internal and external data to assist human specialists in focusing their security and intelligence assessments on the subset of hosts most likely to be compromised. Of course, these methods are beneficial and should be used to identify and prevent sophisticated attacks, but most of them are already in place, and attackers are able to circumvent them.

The techniques or stages to be used in the APT also vary depending on the goal. However, while individuals profit from the tremendous ease of the Internet, they are constantly in danger of cyber-attacks as the Internet and artificial intelligence (AI) expand in popularity. When it comes to smart grid and industrial Internet technologies, there are no exceptions.

4. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Africa may become a focus for advanced persistent threat (APT) groups in the coming months since it has more than 500 million Internet users, Kaspersky warns and as one of the fastest-growing regions globally, the continent will have 1 billion internet users by the end of 2022 by IT News Africa (The Evolving Cyber Security Threat in Africa, 2021). The security firm has witnessed an increase in hackers-for-hire or cyber mercenaries. This year alone, three cyber mercenary outfits have been discovered around the world.

This proportion of users to the population is around 38%, implying that the number will continue to rise in the next years as digitization accelerates. Kenya, with 83 per cent of its people online, Nigeria, with 60 per cent, and South Africa, with 56 per cent, are the top three countries. In these three countries, mobile banking, in particular, is widely used, adding to Africa's active engagement in digital financial services. As of January 2022, the internet penetration rate in Ghana reached 53 per cent, up from 50 per cent in the same month in the preceding year according to Doris Dokua Sasu who is a research expert covering primarily society and agricultural topics for Africa, particularly Ghana and Nigeria for statista.com.

With the rise of rogue software on mobile devices exploiting expanding vulnerabilities, it poses a serious future threat. Despite the rising demand for online mobile banking, the digital divide remains a challenge, especially as the number of people who have access to the internet grows, African member countries work to integrate digital infrastructure into their society's foundations, such as government, banking, business, and essential infrastructure. This shift emphasizes the critical importance of ensuring that cybersecurity criteria and standards fit the demands and future needs of this population, particularly financial inclusion.

In Africa, however, the lack of these criteria is widespread. 90% of African companies do not have the appropriate cybersecurity protocols in place. Weak and outdated security systems are estimated to cost the continent a staggering USD4 billion a year, so the time to take planned and concerted action to improve Cyber Security according to a cyber security report in August 2021 (The Evolving Cyber Security Threat in Africa, 2021). Without these standards, threat actors can exploit emerging vulnerabilities as they develop new cyber attack methods. This results in substantial financial loss.

5. IMPLICATIONS FOR PRACTICE, RESEARCH AND POLICIES

Implications for Practice

As the world continues to recover from the disruptions of the COVID-19 pandemic, coping mechanisms such as increased use of virtual workspaces, online marketplaces and e-governance have become the norm. While this presents opportunities to revamp economies and streamline public service delivery, it may also heighten exposure to cybercrime. The GCI report evaluated 194 nations' commitment to strengthening cybersecurity by the end of 2020, based on five pillars: legal, technical, organizational, capacity development, and cooperation. African governments can take a number of initiatives to increase their capacity to avoid and respond to cybersecurity risks in order to strengthen cybersecurity. To begin, officials must create a medium- and long-term cybersecurity policy and plan that integrates cybersecurity into government efforts and specifies the resources required to achieve these goals.

This necessitates the establishment of national authorities or agencies with adequate financial resources to carry out the strategy and improve the country's cyber-resilience. To boost individuals' and businesses' trust in the cyber economy, digital services, and the larger internet, governments must also foster a responsible societal cybersecurity culture. States must develop cybersecurity education and training programs for the general public, business, academia, and civil society. Governments must also build the necessary legal structures to govern cyberspace use and punish cybercrime. Cybersecurity capacity building (CCB) is the foundation on which countries may develop their digital economies while also increasing their resilience to cyber threats. Many global CCB programs are already active in African institutions and governments.

The Global Cyber Security Capacity Centre (GCSCC) and the Commonwealth Cyber Program's Cybersecurity Capacity Maturity Model (CMM), the Global Forum on Cyber Expertise (GFCE), and the International Telecommunication Union's GCI (Global Cybersecurity Index), to mention a few. These efforts encourage international cooperation, which is critical for both global and national cybersecurity. They also serve as a guide for governments as they develop national cybersecurity policies and plans. The Cybersecurity Capacity Maturity Model (CMM) from the GCSCC is the most complete of the frameworks available for capacity building projects (Signé & Signé, 2021). According to this approach, the five dimensions of policy and strategy, culture and society, education and training, legal and collaboration, standards and technology are critical to a country's cybersecurity capacity Capacity building is a long-term aim that must be well-planned, suitably resourced, and assessed on a regular basis to be effective. Better policy and cybersecurity implementation are made possible by increased state capacity.

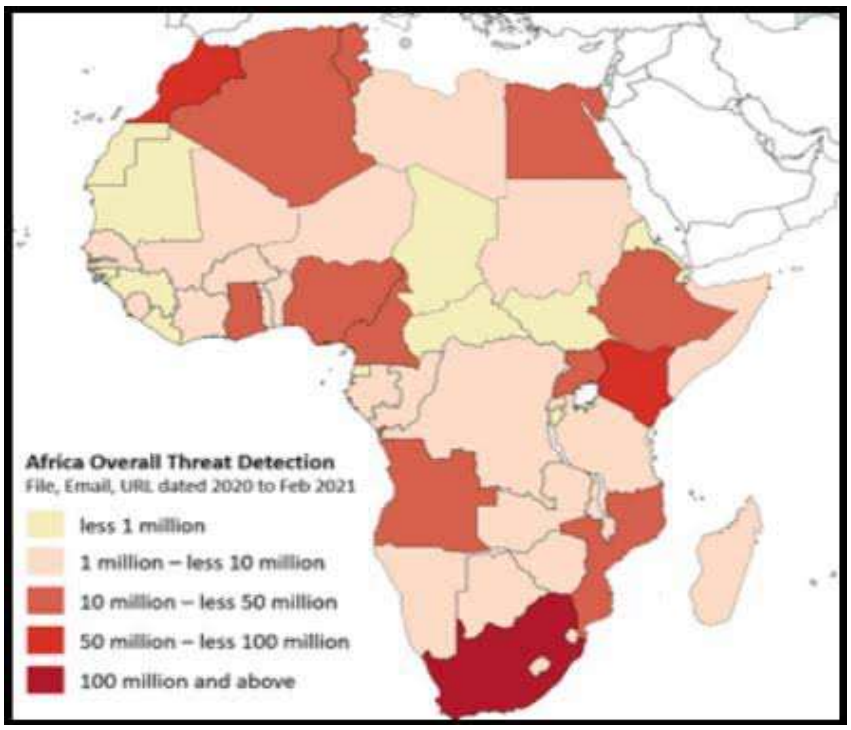

Figure 2: Overall detection of cyber threats in Africa using Trend Micro sensors
(Source: INTERPOL,2021)

Implications for Research and Policies

Cyber threats are becoming more prevalent among African businesses and consumers. This pattern underscores the importance of strengthening cybersecurity defences. This means that businesses must raise their investment in cybersecurity technologies, offer personnel cybersecurity training, and hire specialists such as CISOs. It's also critical to raise customer awareness about cybersecurity. Policymakers on the continent should focus on increasing public awareness of cybersecurity practices as well as boosting regulatory and enforcement capabilities. Regulations mandating firms to take effective cybersecurity precautions should be introduced and amended. Initiatives should also focus on improving law enforcement capabilities to increase the certainty of punishment for cybercriminals.

Several projects to improve the continent's cybersecurity landscape have been launched and implemented at various levels. Improving regulatory quality is the most essential of these. According to a November 2016 report by the African Union Commission (AUC) and cybersecurity firm Symantec, Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda, and Zambia had specific laws and provisions in place to deal with cybercrime and electronic evidence. A further 12 countries had taken some, albeit modest, legislative actions. Many other nations had drafted draft cybercrime legislation, and bills had previously been introduced in national legislatures in some of them. There are also sector-specific regulations and since the banking and financial institutions are the most affected sector the Bank of Ghana issued a Cyber Security Directive for Financial Institutions in October 2018. The Directive requires the active involvement of senior executives and the board to strengthen cybersecurity.

All banks in the country are required to appoint a Cyber and Information Security Officer (CISO) who would advise senior management and the board on cybersecurity issues, and also formulate adequate measures to manage cyber and information security risks. In 2016, Ghana’s financial institutions were reported to experience more than 400,000 incidents related to malware, 44 million related to spam emails and 280,000 related to botnets (Kshetri, 2019). The Central Bank of Nigeria (CBN) announced that it was developing a risk-based cybersecurity framework for banks and financial institutions. The idea of this framework is to identify the existing gaps and address them. In August 2018, the Central Bank of Kenya asked the country’s payments service providers to submit their cybersecurity policies to the government (Kshetri, 2019).

Many African economies have likewise tightened enforcement. Private-sector cybersecurity initiatives have also become prominent such as Serianu establishing what it calls a Cyber Immersion Centre in Nairobi in 2017. Multinational corporations have also partnered with local organizations to educate consumers about cybercrime and set ethical standards. Microsoft, for example, partnered with Paradigm Initiative Nigeria (PIN) to educate Nigerians about cybercrime and offer economic opportunities. In October 2009, the country's EFCC stated that it had shut down around 800 websites linked to cybercrime and arrested 18 cybercrime gangs. Numerous actors are involved in the fight against cybercrime in Africa. In order to combat cybercrime, organizations and individuals are upgrading technological and behavioural defence systems. In this regard, a final area of future research would be to compare the relative effectiveness of these actors as well as the potential challenges they face in controlling cybercrimes.

6. CONCLUSION

Remarkably, the investigation indicated that vulnerabilities for such complex assaults are not as widespread as one might think. Instead, the attackers targeted vulnerabilities that previously had been patched. The aforementioned characteristics might be viewed as a chance to uncover APT campaigns. We've offered four alternative APT prevention and detection strategies. It is feasible to detect critical harmful actions throughout important attack phases using these methods and while cyberattacks targeting and emanating from African economies are on the rise there are other signals that are optimistic. The continent's cybersecurity regulations and enforcement mechanisms are gradually improving. A number of private-sector efforts have emerged to help the continent's cybersecurity landscape be strengthened.

7. RECOMMENDATION FOR POLICY AND PRACTICE

A specific APT phase can be used or implemented in the course of cyber threat countermeasures based on the type of threat mitigation performance. This suggests that dependent on countermeasure tackling, one APT phase would perform better than the other.

Future Works

The detected APT operation indicators might be examined and connected, also the various phases' efficiency and performance would be compared in the future works to come work which performs than the other, that is a comparative study of the various APT phases. It could be particularly interesting to investigate the threat actors' preferred service providers and domain registrars. Implementation and assessment of the proposed preventive and detection measures might be another undertaking.

REFERENCES

1. Adelaiye, O., Ajibola, A., & Faki, S. (2018). Evaluating Advanced Persistent Threats Mitigation Effects: A Review. *Internation Journal of Information Security Science*, *7*(4), 159–171.
2. *Advanced Persistent Threat, An overview of APT.* (2018, September 11). Digital Guardian. Retrieved May 5, 2022, from https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition
3. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851–1877. https://doi.org/10.1109/comst.2019.2891891
4. Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems*, *89*, 349–359. https://doi.org/10.1016/j.future.2018.06.055
5. Khaleefa, E., Abdulah, D. (2022). Concept and difficulties of advanced persistent threats (APT): Survey. *International Journal of Nonlinear Analysis and Applications*, 13(1), 4037-4052. DOI: 10.22075/ijnaa.2022.6230
6. Lu-Xing, Y., Pengdeng, L., Xiaofan, Y., Yong, X., Jiang, F., & Wanlei Z, Z. (2021). "Effective quarantine and recover scheme against the advanced persistent threat." *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(10), 5977–5991.

7. Staff, H. (2016, May 18). *APT1: Exposing One of China's Cyber Espionage Units*. Homeland Security Digital Library. https://www.hsdl.org/c/apt1-exposing-one-of-chinas-cyber-espionage-units/
8. Ussath, M., Jaeger, D., Feng Cheng, & Meinel, C. (2016). Advanced persistent threats: Behind the scenes. *2016 Annual Conference on Information Science and Systems (CISS)*. https://doi.org/10.1109/ciss.2016.7460498
9. Mandiant, APT1: Exposing One of China's Cyber Espionage Units, 2013. https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf
10. Marchetti, M., Pierazzi, F., Guido, A., & Colajanni, M. (2016). Countering Advanced Persistent Threats through Security Intelligence and Big Data Analytics. The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved May 12, 2022, from https://www.ccdcoe.org/uploads/2018/10/Art-15-Countering-Advanced-Persistent-Threats-through-Security-Intelligence-and-Big-Data-Analytics.pdf
11. Anatomy of an APT attack: Step by step approach. (2021, July 24). Infosec Resources. https://resources.infosecinstitute.com/topic/anatomy-of-an-apt-attack-step-by-step-approach/ (Figure 1)
12. Kshetri, N. (2019, April 9). Cybercrime and Cybersecurity in Africa. Taylor & Francis. https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527
13. The evolving Cyber Security threat in Africa. (2021, August). Liquid Intelligent Technologies. https://liquid.tech/wps/wcm/connect/corp/00d614b5-e6cf-4552-9085-c12e47b6246c/Liquid+Intelligent+Technologies+Cyber+security+Report+2021.pdf?MOD=AJPERES&CVID=nKxjVS0
14. Signé, L., & Signé, K. (2021, April 6). How African states can improve their cybersecurity. Brookings. https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/
15. INTERPOL. (2021, October). AFRICAN CYBERTHREAT ASSESSMENT REPORT. https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf