BOOK CHAPTER | *“Actions, Inactions & Omissions”*

A Review of Attacker Attribution

Ferdinand Kpieleh
Digital Forensics & Cyber Security Graduate Programme
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: ferdinand_kpieleh@yahoo.com
Phone: +233541088417

ABSTRACT

Rather than focusing on technical solutions, a more appropriate argument would be that, measures to stopping the most serious attacks, multistage multijurisdictional attacks, will necessitate not only technical but also legal/policy answers. There is currently a dearth of understanding of the social, cultural, economic, and political characteristics of the nation-states where cyber threat actors operate. The present focus of national security attribution efforts is on law enforcement concepts aimed at gathering evidence to punish an individual perpetrator. This is frequently determined via technological attribution methods. It is difficult to determine who engages in hostile cyber activity. This paper provides insights and directions on the foregoing

Keywords: Attribution; Cyber Attribution; Attack Attribution, Cyber Threat Attribution.

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

Citation: Ferdinand Kpieleh (2022): A Review of Attacker Attribution
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 197-202
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P32

1. INTRODUCTION

Cyberattacks can have major ramifications for a company's public image, compliance reputation, and profitability. Following an attack, an organisation may conduct investigations to attribute the occurrence to specific threat actors in order to acquire a full picture of the attack and ensure that the perpetrators are brought to justice. These cyber attribution operations are frequently carried out in tandem with formal law enforcement investigations. Cyber attribution can be very difficult because, the underlying architecture of the internet offers numerous ways for attackers to hide their tracks. Cyber attribution is the process of hunting down, identifying, and blaming the perpetrator of a cyberattack or other hacking exploit is known as cyber attribution. (Rosencrance, 2017)

1.1 Background To The Study

Attack attribution should be a major concern if you want to thrive in today's threat climate. Knowing who attacked you gives you insight into why you were chosen and what the attackers were after, and you can use that information to strengthen your defenses and prevent future attacks. The below will enlighten you on the challenges and techniques in the area of attacker attribution.

1.2 Challenges of cyber attribution

Organisations that need to undertake cyber attribution frequently hire outside information security professionals because they lack the resources or experience needed to track down cybercriminals. Even with cybersecurity experts, though, cyber attribution can be difficult. Experts typically perform lengthy forensic investigations to uncover the person or players responsible for a cyberattack, which include assessing digital forensic evidence and historical data, establishing intent or reasons, and taking into account the overall situation. Attackers can fake their own IP addresses or use other techniques, such as proxy servers, to bounce their IP addresses around the world to confuse attempts at cyber attribution, making it more difficult to identify them.

1.3 Cyber attribution techniques

Although cybercrime detectives have access to a variety of specialized tools for undertaking cyber attribution, definite and accurate cyber attribution is not always attainable. To unearth essential information regarding assaults, investigators employ analysis tools, scripts, and programs. Investigators of cybercrime are frequently able to unearth information regarding the programming language and related information, such as the compiler used, compile time, libraries utilized, and the order in which events linked to a cyberattack were carried out. Investigators working on cyber attribution look at any metadata associated with the assault. Because cyberattack systems frequently interface with nodes outside the network being attacked, metadata such as source IP addresses, email data, hosting platforms, Domain names, domain name registration information, and data from third-party sources can help make the case for attribution. These data points, however, are easily manipulated.

Understanding the motivations of the attacker can also help with cyber attribution. Because it's not always about money, security specialists try to figure out what the attackers' goals are. Investigators are attempting to determine whether the cybercriminals are simply lurking or have been spying for some time. They also want to know if the hackers are seeking for specific data during their attacks and how they plan to use it.

2. RELATED LITERATURE

One can protect against a cyber-attack, but attackers lack a disincentive without attribution. Secure systems, at best, extend the amount of time it takes an attacker to discover a vulnerability beyond what the attacker is prepared to invest. It is unrealistic to expect the current scenario to change without sufficient incentives to curb harmful attacker conduct, whether state or non-state. The table below shows the research works by different researchers in the area of attack attribution.

Table 1: Review of Related Literature.

Paper Title	Journal Name	Author	Purpose of the Study	Research Gaps/ Findings	Direction for Future Works
Attribution of Cyber Attacks on Industrial Control Systems	EAI Endorsed Transactions on Industrial Networks and Intelligent Systems	Allan Cook, Andrew Nicholson, Helge Janicke, Leandros Maglaras, Richard Smith	Identify the current state of the art of attribution in industrial control systems.	What are the most effective techniques for tracing attacks	1. Collection of evidence in the absence of persistent memory. 2. Hardware-based capture devices for control systems network audit trails. 3. Honeypots for control systems as part of the investigatory process. 4. Radio frequency forensics. 5. Intrusion detection systems for control systems.
A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise	Future Generation Computer Systems	Umara Noor, Zahid Anwar, Tehmina Amjad and Kim-Kwang Raymond Choo	A framework to automate cyber threat attribution	Aside from technology harriers, what other harriers exist for tracing attacks both inside and outside our borders?	Build a context-specific cyber threat source reputation model.
Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures	ICST Transactions on Security and Safety	Maglaras, Leandros Ferrag, Mohamed Derhab, Abdelouahid Mukherjee, Mithun Janicke, Helge Rallis, Stylianos	provide an overview of current methods and practices regarding cyber attribution and cyber peace keeping	What is an effective deterrent to prevent assaults if we can detect them?	A discussion on how the right expertise can be secured in the necessary numbers, and at a price that is within an operation's budget

Paper Title	Journal Name	Author	Purpose of the Study	Research Gaps/ Findings	Direction for Future Works
Cyber Attribution: Can a New Institution Achieve Transnational Credibility?	Army Cyber Institute	Milton Mueller, Karl Grindal, Brenden Kuerbis, Farzaneh Badiei	This paper argues that authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions.	There exists no automatic dynamic system to handle attacks due to the dynamic nature of Cyberattacks	Artificial Intelligence, monitoring campaigns from start to end and improved monitoring of infrastructure.
Air University Air Force research institute Perspectives on Cyber Power strategies for resolving the Cyber Attribution Challenge	Library of Congress Cataloging-in-Publication Data	Yannakogeorgos, Panayotis A	The purpose of this study was to determine what, if any, benefit could be accrued from the US engagement with the UN/ITU in cybersecurity.	There exist no legal/policy and organisational capabilities in attack attribution	Enable the timely development of response framework for Africa with sound global norms to guide global cybersecurity.
A Survey of Challenges in Attribution	Interagir: pensando a extensão	Aceh, kue tradisional khas, Rios, Elizabeth Dos Santos, Donato, Ana Maria, Sprott, David	The problem of attributing cyber intrusions, both technical (can you determine which machine or machines are generating or controlling the intrusion?) and nontechnical (can you determine the party that should be held responsible for the intrusion?).	A semantic gap exists between attacks and detection techniques	Covert communication requirements of attack tools

From table 1 above, it is clear to the best of my knowledge that few studies have been done on the area of attack attribution. Hence the current study seeks to address these gaps by providing an overview of the literature.

3. IMPLICATIONS FOR ONLINE SAFETY IN AFRICA

The sophistication of some cybercriminal attacks and strategies reveals how vulnerable individuals are online, and it has eroded public trust in online security and trade. Data breaches, government monitoring, and good old-fashioned con artists have all combined to further infringe on human privacy, whether it's through personal images, login credentials, or medical records. Africa's cybercrime has progressed far beyond the renowned 419 Nigerian email scams, which were named after a piece of legislation designed to combat them. The sophistication of some cybercriminal attacks and strategies reveals how vulnerable individuals are online, and it has eroded public trust in online security and trade.

Traditional scams and malware attacks to collect personal information were common in 2015, according to Symantec. One hoax, for example, promised big numbers of free Instagram followers in exchange for users providing their passwords. Some attacks pretended to be tax officials in order to get individuals to open dangerous email attachments. Many scams still rely on the general public's poor security practices to succeed in their most basic form. However, we've seen how insecure websites can reveal client information. It makes no difference how strong a password is if the website is subject to a data leak in the latter case.

Data breaches, government monitoring, and good old-fashioned con artists have all combined to further infringe on human privacy, whether it's through personal images, login credentials, or medical records. Attacks in 2015 that used sophisticated social engineering to get around two-factor authentication methods designed to protect users are even more worrying. One scam took advantage of the public's faith in a renowned brand by going through a valid password-reset process and posing as Google through SMS to obtain access to email accounts without raising the victims' suspicions. Scammers continue to target social media, attempting to take advantage of people's confidence in their own social networks to disseminate frauds, bogus links, and phishing.(Symantec, 2016).

4. CONCLUSION

Since anonymity allows state and non-state actors to engage in hostile cyber activities, attribution is a critical component of an effective cyber deterrence strategy. The intelligence community has made enormous investments in all source collection, analysis, and dissemination capabilities, all of which lessen the anonymity of state and non-state actor behavior in cyberspace. Intelligence and attribution capabilities aid in the identification of an attacker's cyber persona, as well as the determination of tactics, strategies, and processes.

REFERENCES

1. Rosencrance, L. (2017, October). What is cyber attribution? - Definition from WhatIs.com. https://www.techtarget.com/searchsecurity/definition/cyber-attribution.
2. Hanso, B. (2016). Cyber Attribution: Can a New Institution Achieve Transnational Credibility? Army Cyber Institute, 4(1), 1-23. https://www.jstor.org/stable/10.2307/26623070
3. Aceh, K.T.K., Rios, E.D.S., Donato, A.M., Sprott, D. A. (2010). A Survey of Challenges in Attribution. National Academic Press, (15), 1-9. http://www.nap.edu/catalog/12997.html.
4. Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H., Rallis, S. (2018). Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. ICST Transactions on Security and Safety, 5(16), 155856. http://eudl.eu/doi/10.4108/eai.15-10-2018.155856.
5. Yannakogeorgos, P.A. (2016). Air University Air Force research institute Perspectives on Cyber Power strategies for resolving the Cyber Attribution Challenge. Air University Press. https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF.
6. Noor, U., Anwar, Z., Amjad, T., Choo, K.K.R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems 96, 227-242. https://doi.org/10.1016/j.future.2019.02.013.
7. Cook, A., Nicholson, A., Janicke, H., Maglaras, L., Smith, R. (2016) Attribution of Cyber Attacks on Industrial Control Systems. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems. 3(7), 151158. http://eudl.eu/doi/10.4108/eai.21-4-2016.151158.
8. Symantec. (2016). Cyber Crime & Cyber Security Trends in Africa. Cyber-security-trends-report-Africa-en.pdf (securitydelta.nl)