China's Role in the Increase of Global Cyber Attacks

Jordan Hillis[1†],

Marymount University, Arlington, VA, USA

Abstract
Cybercrime has quickly become one of the most pressing issues to mitigate as more reliance on technology is created each day. Advanced persistent threat groups have established themselves as critical threats to organizations and governments as the sophistication of their attacks advances as technology does. One of the most significant threats currently is advanced persistent threat groups that originate from the country of China. China has some of the highest numbers of known advanced persistent threat groups, such as Double Dragon (APT41), PLA Unit 61398 (APT1), and now a new and emerging group dubbed HAFNIUM has been discovered.

Keywords:
Cyber Attacks, Advanced Persistent Threat (APT), Persistent Threat (PT), Phishing, Spear Phishing, Remote Access Tool (RAT)

1. Introduction

Cyber-attacks have long plagued the internet with devastating results for organizations and large corporations. The most significant threat among these is derived from an Advanced Persistent Threat (APT). According to Nate Lord [1], "an advanced persistent threat is an attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected. Advanced persistent threats are hazardous for enterprises, as hackers have ongoing access to sensitive company data." Advanced persistent threats meticulously plan their attacks and do not act erratically in their actions. Every aspect of their attack is pre-planned with multiple stages and counter plans in the event issues arise. These groups typically will have the goals of intellectual/classified data theft, sabotage, surveillance, or credential breaching.

Malicious threats such as these can hail from various powerful countries around the world. The United States and others have currently identified China as the most prominent cyber threat actor. This country has the goal of global dominance in terms of economics, cyber defense, and offense, which does not uphold the same morals and ethics other countries do. This, in return, creates an unfair landscape for China to take advantage of countries such as the United States and others, as their cyber operations are much more limited in comparison.

This paper explores some of the most recent cyber attacks associated with China to address the concern for their role in increasing global cyber-attacks on systems and networks.

2. Methodology

This paper aims to look at some of the most recent cyber attacks associated with China to inform security teams, experts, and researchers of the global Chinese cyber threat. This research examines these attacks for motives, outcomes, and potential future threats from these attacks. Finally, security mitigation strategies are provided that could have taken place to prevent many of these attacks from being successful.
The following criteria were used to narrow the results of attacks to be examined.
• Date of attack (Only recent attacks in the last 15 years were used)
• Confirmed Chinese affiliations
• Severe damage caused to systems, networks, or national security of the given victim.

3. Related Work

Over the last decades, China has continued to grow in terms of economic power and offensive operations, both physically and digitally. This growth has led to some of the most notorious attacks witnessed today. In this research, we will explore past attacks and their impact on nations.

A. Operation Aurora

The infamous Operation Aurora was a collection of planned cyber attacks by the Elderwood Group (Chinese Advanced Persistent Threat Group) in Beijing, China. This vulnerability affected versions 6, 7, and 8 of Microsoft Internet Explorer running on Windows 2000, XP, 2003, Vista, 2008, and 7. Many large technology organizations were targeted by this attack, such as Google, Akamai Technologies, Yahoo, Rackspace, and many more.
One of the driving factors of this attack not becoming successful was an abundance of versions at the time that

Manuscript received March 5, 2023
Manuscript revised March 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.3.8

were using Microsoft Internet Explorer 8 or updated versions of Windows, which has Data Execution Prevention (DEP) installed and enabled by default. According to Rohit Varma [2] of the McAffee Labs, "DEP is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system."

The primary objective of this sophisticated attack was to leverage access to key high-tech and defense contract companies' source code repositories so that further malware could be implanted for a more globalized attack in the future.

B. HAFNIUM

Recently a new and emerging threat actor named HAFNIUM has plagued various Microsoft Exchange Exchange Servers in early 2021. Microsoft has published multiple findings which indicate that this threat actor has used various zero-day exploits to attack on-premise versions of Microsoft Exchange Server to access email accounts and deploy malware to establish long-term access to each server exploited. Among these vulnerable versions of Microsoft Exchange Server are versions 2013, 2016, and 2019 which comprise the supported versions available to customers. On March 2nd, 2021, Microsoft issued four security updates to its customers to remediate the vulnerabilities found previously by the HAFNIUM group, allowing for lateral movement within servers and breaches of sensitive information. Although this group primarily targeted United States government entities, healthcare, and higher education, it has also affected Germany and Denmark in recent findings.

The HAFNIUM group has been shown to attack in three different phases. First, the group gains access to the Microsoft Exchange servers by utilizing stolen credentials or using unknown zero-day vulnerabilities to establish their foothold within the servers and act as authorized users. Next, the group creates a web shell to communicate from the breached server back to their command and control server so that remote command execution can take place. Lastly, the group uses their newly established shell access from their command and control server to steal sensitive information from the exploited Microsoft Exchange server. The Microsoft Exchange Server exploitation has been identified as an attack chain consisting of CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. CVE-2021-26855 can be described as a remote code execution vulnerability that allows unauthorized parties to execute remote code to a server or service. In this incident, threat actors can perform server-side request forgery by sending arbitrary HTTP requests to authenticate them to an unauthorized Microsoft Exchange Server. According to CVE statistics, this vulnerability has a network vector, low complexity, no privileged requirements or user interactions, and high confidentiality and integrity.

C. GhostNet

In 2009, a new Chinese espionage operation was formed with the given name, GhostNet. The attack targeted mainly high-value politicians, technology industries, and governments. According to Harvard reports [4], more than 1,300 computer systems were compromised, associated with government offices, foreign ministries, and embassies. This attack was unleashed using socially engineered emails containing malicious malware within the victim's file attachments. Once the victim had executed the file, the malware connected to the attacker command and control server to receive further commands.

According to Canadian-based researchers SecDev Group [5], it was discovered that during this attack, IP addresses belonging to the People's Republic of China were associated with the Tibetan-based victims of GhostNet. Further research shows consistencies with Hainan, China being one of the main operational points of the attacker in GhostNet, which holds the Lingshui signal intelligence facility and Third Technical Department of the People's Liberation Army

4. Limitations

Often large cyber attacks are difficult to prove association based on collected data alone. China, among other countries, continues to deny having a role in offensive cyber operations worldwide. Due to the limitations of direct association with China's involvement in cyberattacks, this research can only detail cyber attacks with strong evidence publicly correlating China to each attack. As time passes, this research should be explored further with new and emerging evidence of Chinese involvement in cyber offensive operations.

5. Results

From the data gathered on various Chinese threats, it is easy to see how significant this threat is for the entire globe. Threat actors hailing from China often use unethical and persistent means of gaining access to systems and networks. Chinese threat actors have historically attacked their victims with a spear-phishing attack which can often be confused with regular phishing, although it differs significantly. Phishing is a more widespread attack that aims to trick the victims into providing sensitive information

regarding accounts or access credentials, disguising themselves as trustworthy individuals or organizations. These attacks are not personalized and do not contain information regarding the victim they are targeted towards. Spear phishing is a more personal phishing attack where the attacker sends out a phishing attack, usually in the form of an email, towards their victim with information about the victim within. This information is typically gathered from online sources such as social media, blogs, and other forms of websites where your information could be publicly displayed to the masses. Social engineering is a reoccurring theme in all of the attacks associated with the country of China. Mitigation in this area is highly recommended as it has the potential to prevent lateral movement and the success of these malicious groups.

Based on historical threat information gathered, the following mitigation strategies are suggested to mitigate the vulnerability exposure from Chinese advanced persistent threat actors.

• Education: employees within the organization or business should all be educated on not only how to identify spear-phishing but also the detrimental damage that can happen from a failure to identify and react appropriately to spear-phishing threats. This training should be conducted frequently and adapt to changes in threat behavior to apply to real-world cases employees may encounter.
• Filters: security can start with a strong rule set in place to identify and filter malicious messages. The organization should determine what type of messages should automatically be flagged for quarantine and investigated further. These messages will typically be from an outside source apart from your organization's email as well as senders that attach files to their emails. Links can also be a vital indicator of the need to investigate, as these are often presented to users as legitimate login sources.
• Software Updates: software continues to transform over time with new features and the latest security patches. These are extremely important to implement as malicious actors prey upon out-of-date software to conduct their attacks and breaches. Creating a schedule update period can greatly alleviate much of the manual labor away from this task.
• Backups: these can serve as a critical factor in a successful incident recovery. Should the actor gain unauthorized access, a backup can be uploaded to overwrite any previous changes that were done and restore services and operations to the organization..

6. Conclusion

In conclusion, this research has shed light on the pivotal role China plays in the escalation of global cyberattacks, with a particular focus on advanced persistent threat (APT) groups such as Double Dragon (APT41), PLA Unit 61398 (APT1), and HAFNIUM. By analyzing China's cyber threat landscape and evaluating the impact of multiple high-profile cyberattacks, this paper underscores the urgency of comprehending and addressing these threats.

The study also presents practical mitigation strategies that organizations and governments can adopt to proactively counter these cyber threats. These strategies encompass employee education, the implementation of filters and rules, maintaining up-to-date software, and conducting regular data backups. In the face of continuously evolving cybercrime, it is of paramount importance for the global community to stay vigilant in identifying, mitigating, and combatting cyber threats originating from China and other potential threat actors. Future research should continue to monitor emerging evidence of Chinese involvement in cyber offensive operations and update the strategies accordingly to protect against the ever-evolving cyber threat landscape.t

References

[1] "What is an Advanced Persistent Threat? APT Definition," Digital Guardian, Jun-2015. [Online]. Available: https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition. [Accessed: 25-April-2021]

[2] R. Varma and M. LabsTM, "McAfee Labs: Combating Aurora," [Online]. Available: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Combating%20Threats%20-%20Operation%20Aurora.pdf

[3] C. Osborne, "Hafnium's China Chopper: a 'slick' and tiny web shell for creating server backdoors," ZDNet, 15-Mar-2021. [Online]. Available: https://www.zdnet.com/article/hafniums-china-chopper-a-slick-and-tiny-web-shell-for-creating-server-backdoors/. [Accessed: 01-May-2021]

[4] ["GhostNet - Cybersecurity Wiki," Harvard.edu, 2012. [Online]. Available: https://cyber.harvard.edu/cybersecurity/GhostNet#:~:text=G

hostNet%20is%20the%20name%20given,media%20locations%20in%20103%20countries.. [Accessed: 03-May-2021]

[5] "Information Warfare Monitor Investigating a Cyber Espionage Network," 2009 [Online]. Available: https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651/download_file?file_format=pdf&safe_filename=Gh0stNet.pdf&type_of_work=Report

Jordan Hillis received the B.S. and M.S. degrees from Champlain College in 2019 and 2020, respectively. He is currently a Doctororal Candidate in Cybersecurity at Marymount University, in Arlington, VA, USA. Jordan has over 14 years of experience in the information technology and cybersecurity fields with prior service as a United States Marine. His research interest includes cyber threat intelligence, cyber warfare, advanced persistent threat groups, secure coding, malware and cybersecurity.