Analysis of Project CameraShy Findings

Introduction

Project CameraShy is a report published in 2019 by ThreatConnect detailing activity of Chinese advanced persistent threat group “Naikon” and their activity over the course of several years against South Asian countries using a sophisticated command and control network. The research was able to link a specific domain tied to the Naikon APT group to a specific person, Ge Xing, associated with Unit 78020.

The Chinese People’s Liberation Army (PLA) has historical and continued interest in the control of the South China Sea and monitoring neighboring South Asian countries and do so through targeted cyber campaigns in these areas. The report details activity of Naikon and domain resolutions tied back to them through analysis of malware attributed to their group and activity in these South Asian nations. One particular domain consistently found within this malware, greensky27.vicp.net, is found to hold key information in linking malicious activity to the PLA and Unit 78020.

Through various research techniques and the use of public information, the researchers are able to definitively target an individual who is the owner of the command and control infrastructure detailed in the report. This analysis will extract the key methods of discovery from the report and the application of those methods to other scenarios.

Naikon APT Method of Attack

Research of Naikon shows a pattern of attack per Baumgartner (2024):

Step 1: Phishing email with malware attachment containing an executable file.

Step 2: An encrypted file is injected into the browser with configuration data to connect with Command and Control (C2) server; handled in memory, not stored.

Step 3: Reverse connection to C2 server; attacker can remotely control the machine.

C2 servers are sometimes directly connected to the victim computer and other times routed through a series of proxy servers in various countries. To prevent being blocked by geofencing (preventing connections from outside the country in question), the group ensure some proxies are located within the target country. The threat actors use a variety of one-time use IP addresses as well as some recurring IP addresses, but the locations of these IP addresses can be generally mapped to specific locations that house these proxy servers as well as the destination to Kunming.

Targets of Naikon include various political and military offices with the intent of continuous monitoring of affected individuals for the purposes of espionage. In the case of Project Camerashy, the phishing email was a replica of a Thai news article where the attachment mirrored the real article while containing the executable file (ThreatConnect, 2019, p. 22).

Methods of Research/Discovery: GreenSky27

Malware analysis is used to discover to which domain/IP addresses the command and control structure is resolving to, which illuminate the greensky27.vicp.net domain. From here, the researchers mapped the locations from the start through proxies back to the domain revealing an intricate web of locations including a proxy located within the United States. The final destination is in Kunming, China, which is where unit 78020 is located.

Next, taking "greensky27" and researching Chinese social media to quickly discover a user with the same name: GreenSky27. This was found on QQ Weibo, a popular Chinese social media site. The same username is located across several social media sites going back to at least 2004. By going through these social media sites, it is determined that the user resides in Kunming through photos of his license plate, postings of items for sale where his address is listed, and more. The name, Ge Xing, is corroborated through a picture that shows his ancestral name, the same for sale listings, and a service that identifies users on QQ Weibo with their names.

To tie this person specifically to Unit 78020, the researchers discovered academic papers authored by Mr. Ge Xing related to Thai politics and PLA interests. Photos posted to the user's accounts are traced to specific location of Unit 78020 by looking at the vantagepoint of the photos, their relation to nearby surroundings to known location of Unit 78020, and the similarity to other geographical features.

The wealth of information found using publicly available sources is staggering and seem to definitely identify this individual and his ties to the PLA and Unit 78020.

Significance and Application

This particular case, while it may not be the norm, it showcases two main points. First, it is possible to locate the individual perpetrating these attacks through detailed research and analysis of patterns in everyday life and the widespread use of social media. This is assuming they are careless and reuse the same name for their command and control server domain or some other piece of infrastructure, but this is human error and certainly does occur. Even if this level of mistake is not common, even one such slip up leads to a wealth of information in the operation of these attacks, which helps offensive and

defensive measures and highlights the importance of tackling such types of threat analysis. The information from ThreatConnect's report demonstrates this well.

Second, this individual's actions illustrate the need for control in the infrastructure that is carrying out any offensive or defensive measures, which could be taken as a lesson for the United States and its allies to make sure that they maintain control over something as simple as domain names, continued use of certain aliases, or identities on social media to prevent the leakage of any one person or group to adversaries.

Finally, the importance of this piece of work is showing all the many methods of research that go into identifying and classifying an APT and their methods. Whether it was down to one individual or not, the ability to first obtain the malware and its origin, reverse engineer the malware to extract key pieces of information, and then locating the command and control infrastructure is critical to understanding how these groups operate.

References

Baumgartner, K. (2024, May 30). *The naikon apt*. Securelist. https://securelist.com/the-naikon-apt/69953/

Naikon. Naikon, Group G0019 | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/groups/G0019/

ThreatConnect. (2019). Project Camerashy: Closing the Aperture on China's Unit 78020. https://threatconnect.com/wp-content/uploads/ThreatConnect-Project-Camera-Shy-Report.pdf