Joshua T. Miller

SCS 180 Cybercrime

Professor Moore

10/29/19

Leviathan: A Threat Actor Summary

In cyber security a threat actor group is a group of individuals that perform malicious activities against individuals or organizations. The Leviathan group was discovered in 2013 as a cyber-espionage group; this group has been reported on as other names including: TEMP.jumper, APT 40, and TEMP.Periscope (Marchuk). They have also been reported to be a state-sponsored cyber-espionage group with geopolitical, and economic motivations. This group has typically been targeted organizations that have ties to China's One Road, One Belt (OROB) Initiative. Those who have been attacked are typically tied to naval technology, or geographic links to the OROB. They include: defense and government organizations, engineering firms, shipping and transportation companies, manufacturing facilities, government offices, and research universities to name a few (Marchuk).

The Leviathan group is thought to be sponsored by China due to the parallels in the groups interests and the interests of China's government. This relationship between China and Leviathan can be seen in 2016 when China's People Liberation Army Navy seized a U.S. Navy unmanned underwater vehicle (UUV), while that same year the Leviathan group was discovered committing cyber-attacks on U.S. universities researching naval technologies disguised as a UUV manufacturer (Plan). The group geopolitical motivation has been to attack organizations that oppose the development of China's One Road, One Belt initiative. FireEye has presented more information to back Leviathan's state-sponsorship; they found that the group had tools configured in Chinese, IP addresses that resembled Chinese infrastructure, and evidence of Chinese time zones (Dex).

The Chinese One Road, One Belt Initiative was announced in 2013, the same year that the Leviathan group was discovered (reported in various names). The purpose of the OROB was to recreate the ancient Chinese silk road that connected Asian countries to the western world. This new modern silk road (OROB) would consist of two parts, a land connection and a maritime connection. The OROB would give China a more powerful blue water navy capable of traversing open ocean on a regular basis, as well as create more economic links to westward countries; this would significantly improve China's power status and stimulate their economy (Chatzky).

The Leviathan group was generally attacking to steal data that pertained to the OROB; this data could give secret information from an opposing country, to discover those who were opposing China's international policies, or to gather resources to develop a stronger naval force (Dex). Each attack that Leviathan performed worked through a life cycle that had six steps: establish a foothold, escalate privileges, gather information from within, move laterally through the network, maintain its presence, and deliver the stolen data. At nearly every step of the process Leviathan had a piece of malware that helped them progress the attack and gather data. FireEye reports on over thirty pieces of malware used by Leviathan, some of which are publicly available malwares, and others are custom developed (Plan).

Establishing a foothold, escalating privileges set the stage for Leviathan to gain access into the victim's system. They establish multiple points of access for them to work in the victim's environment. To establish their foothold in an environment they have been known to use spear phishing emails with links or attachments to download malware (Dex). The most prevalent malwares used to set up their connection were the backdoors PHOTO, BADFLICK, and CHINA CHOPPER. Once Leviathan made it into the network they would escalate their privileges by harvesting credentials using malware, such as their custom malware HOMEFRY. This malware would work with backdoors to crack and dump user credentials. Using these credentials Leviathan scanned the systems they have infected looking for information they want to export out. Windows commands and web shells were used frequently in searching through a victim's data. The targeted data would be consolidated, compressed, and encrypted before transferring it out of the victim's network (Plan).

Leviathan moves laterally across infected networks to extend their reach into new systems. They used custom scripts, web shells, tunnellers, and Remote Desktop Protocol alongside malwares such as DISHCLOTH or MURKEYTOP to infect these new systems with malware. Leviathan also wanted to stay on their infected systems so they could return to them and search them again, or use them to launch new attacks. To maintain their presence Leviathan installed backdoors and web shells that would allow them to control key systems (Plan).

It is expected that as China continues to work on the OROB, the Leviathan group will also continue to conduct cyber espionage. It can be expected that their targets remain in line with the Chinese interest of developing a more powerful blue water navy, targeting defenses organizations, research facilities, and governments to gather data (Dex). Attacks may also target countries along the One Road, One Belt Initiative to gain economic advantage, development data, or an edge in commercial negotiations.

Works Cited

Chatzky, Andrew, and James McBride. “China's Massive Belt and Road Initiative.” *Council on Foreign Relations*, Council on Foreign Relations, 21 May 2019, www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

Dex. “Leviathan: Geostrategy and TTP (Tactics, Techniques and Procedures).” *lab52*, 30 May 2019, lab52.io/blog/leviathan-geostrategy-and-ttp-technical-tactics-and-procedures/.

Marchuk, Valerii. “Leviathan.” *Leviathan, TEMP.Jumper, APT40, TEMP.Periscope | MITRE ATT&CK*™, 2019, attack.mitre.org/groups/G0065/.

Plan, Fred. “APT40: Examining a China-Nexus Espionage Actor.” *FireEye*, FireEye, 4 Mar. 2019, www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html.