APT 1

Jared Broyhill

University of Advancing Technology

Author Note

This paper was prepared for NTS405, taught by Professor Aaron Jones.

Abstract

The purpose of this paper is to explore the methodology of APT 1 and discover any and all indicators that an attack is associated with APT 1, along with explaining said indicators.

APT 1

APT1 is generally believed to be the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department, which is itself believed to engage in "Computer Network Operations" (Fireeye Mandiant, 2013). When APT1 makes an attack, they typically tend to follow a general process that has been observed and recorded by security practitioners. Indicators that an attack follow this process will be explained and noted.

Indicators

APT1 almost always utilizes a spear phishing technique. As a result, while one can conclude that spear phishing (through an email that is alleged to be from a known coworker of the target) is technically an indicator, is it also so common that to conclude one is being or has been attacked by APT1 as a result of suffering a spear phishing attempt is not very productive due to how common the method is.

From there, APT1 does not differ in the steps they take after gaining access by installing a backdoor as a result of their phishing attempt. They establish communication from within the network to the outside, mimic legitimate internet traffic that is not just HTTP protocol and escalate their privileges to gain legitimate user credentials. Afterwards, they conduct reconnaissance within the environment utilizing the commands of the operating system either through a command shell or a batch script. These methods are, again, somewhat common and while they are all indicators of an APT1 attack, they are not remotely unique to the organization

Once APT1 has been present for more than a few weeks, they work to keep their presence in the network that they have infiltrated. They install new backdoors on a multitude of new systems (any that they can access), gain legitimate VPN credentials through stolen usernames and passwords that lack MFA (multi-factor authentication), and access web portals

that the network offers (such as Outlook Web Access). As such, the indicators that the infiltrator has not only installed one backdoor but multiple, along with gaining even more credentials and attempting to access whatever they can is distinct of APT1 (a typical cybercriminal wouldn't have as much time or resources to do all these things so quickly) and should be noted.

APT1 will next work to steal files by archiving them via RAR archiving utility. Sometimes they do this manually, other times they utilize batch scripts. They have also been noted to use scripts to only steal information created between certain dates, such as emails exchanged in the previous week from an infiltrator's access. This continued surveillance and theft betrays the organization's intentions, as a typical cyber criminal may act to employ ransomware or some other infrastructure-crippling attack more quickly, and thus should be considered strong indicators of APT1's presence in a network.

Finally, APT1 has tried to utilize English in their tools in a failed attempt at obfuscation. As English is not their first language, a slew of grammatical errors tend to make it into their tools as a result, revealing their lack of proficiency with the language. This, paired with the previous set of indicators of the organization intending to hide its presence to steal information, is another strong indicator of APT1's presence. While this doesn't technically prove that they are the only ones who could be at fault if this is discovered, they are a prime suspect.

All the indicators previously stated belong to APT1 and should be carefully considered, but it is more important to note that the later indicators are the most strong clues to APT1's presence, as their early methods of gaining and maintaining access are more generalized and tend to be utilized by a multitude of cybercriminal organizations. The indicators that betray intentions rather than simply display methods are the greatest indicators to be aware of.

References

Fireeye Mandiant. (2013). *APT1: Exposing One of China's Cyber Espionage Units*. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf