Jackson Warren

Jeremy Bergen

CSCI 370

9/3/21

Week 1 Assignment: Threat Agent Profiling

**Title: Fancy Bear (APT28)**

***Overview***

The global threat known as Fancy Bear, APT28, or Sofacy, has been in operations since 2008. Based in Russia, it is believed the group is tied to the Russian Military Intelligence (GRU or SVR) and has been implementing remote access malware called X-Agent working against Android and IOS devices by collecting data on users such as texts, audio, photographs, and more. Aggressive and brute force oriented, they have been seen attacking a variety of areas around the world such as the United states, Ukraine, Russian dissidents, and more, in attacks like the 2016 presidential election and Pawn Storm. Targets within countries are spread out, threatening aerospace, governments, energy industries, media, and defense to name a few.

***Goals***

One of the main goals of Fancy Bear is to gather information on its targets using phishing tactics to install malware such as X-Agent. This process is able to gather access using its malware to things like microphones, texts, photos, contacts, locations, and more. The primary parties targeted by Fancy Bear have been/is the US and related groups, NATO, dissident Russian groups, and Ukrainian groups. The groups targeted within these organizations have been vast, including their governments, military, and media. In “Operation Pawn Strom”, they used X-Agent to collect data on economic and political targets with the goal of cyber-espionage. Fancy Bear have also been involved in things like the US 2016 Presidential Election.

***Mode of Operation***

Finding exactly the hierarchy and people involved with Fancy Bear proves to remain in the shadows. The US strongly believes that Russia’s Intelligence groups GRU and/or SVR are responsible for Fancy Bear and its attacks. Although there is not much information on the group available to the public, it recently became somewhat obvious that they have a large number of hackers with varying skill levels. In a Pawn Storm hack, they used a very simple remote access trojan (RAT), which was a very easily stopped and dealt with, but was highlighted because it showed the inexperience of some these Fancy Bear hackers as mentioned in later reports.

Still, exactly how they operate, communicate, and how many people are in their ranks is still unknown, and the group is still at large as a result. Whether Russia’s government is directly in charge of this is also still unknown; however, theories tend to believe that the government is indeed aiding these threat agents.

***Level of Motivation: High Motivation***

Fancy Bear has proven to use brute force to gather information. Their involvement with the 2016 US election proved to create serious doubts among its community, therefore disrupting millions of Americans.

Although their attacks thus far have not been physically threatening, they no doubt pose a large threat by creating such disruptions. They seem to have little concern with the repercussions of their actions, and no doubt intend to use their information to change circumstances of situations they deem worthy.

***Capabilities and Constraints***

Successful attacks by Fancy Bear range from very well thought out and complex hacking tactics, to very basic hacking tactics that are so simple they might just be hoping that will be so simple it may go unnoticed.

However, should the US be correct in assuming that Fancy Bear is government operated, they could very well have unlimited resources and man power, leaving their capabilities nearly limitless depending on how much the Russian government wants them to get involved.

At the moment, their only constraint appears to be secrecy and deniability. Russia may very well not want Fancy Bear to become high enough on the radar that another country views it as a direct attack or threat. At the moment, they deny any relations to the group, and may be limited in their attacking abilities to remain that way.

**References**

Council on Foreign Relations. (n.d.). *Russia, Trump, and the 2016 U.S. ELECTION*. Council on Foreign Relations. https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

cyber.nj.gov. (n.d.). https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/x-agent.

*Fancy bear hackers (apt28): Targets & methods: Crowdstrike*. crowdstrike.com. (2019, February 12). https://www.crowdstrike.com/blog/who-is-fancy-bear/.

Lyngaas, S. (2020, December 18). *When fancy Bear isn't So fancy: APT Group's 'crude' methods continue to work*. CyberScoop. https://www.cyberscoop.com/fancy-bear-trend-micro-russia-espionage/.

*Operation pawn storm: Fast facts and the latest developments*. Security News. (n.d.). https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts.

Rfe/rl. (2020, December 8). *Russian Hacker GROUP 'FANCY Bear' accused of cyberattack On Norwegian Parliament*. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/russian-hacker-group-fancy-bear-accused-of-cyberattack-on-norwegian-parliament/30990725.html.