The infamous Log4j vulnerability is proving to be a major long term problem as experts expected. Back in November of 2021 it was announced that Log4j, universally adopted open source software, had major security vulnerabilities. This meant that countless applications, ranging from services provided by Google and Amazon, and personal devices such as computers and phones have been at risk for a long time (TheConversation, 2021). Jen Easterly, director of the U.S. Cybersecurity & Infrastructure Security Agency, has called it "the most serious vulnerability she's seen in her career.…" (TheConversation, 2021) , and likewise many cyberattacks are emerging from various angles.

On September 8th 2022 Cisco Talos, a threat intelligence company, announced that North Korean hackers were exploiting Log4j to steal information from energy companies located in the US, Canada and Japan. These exploits were being looked into starting April of 2022, but the exact group was only recently pinpointed to be APT Lazurus, a malicious hacking group, which according to security researchers, have been at large since 2009. That being said, this attack was first attributed to a different North Korean group named "Stonefly" by the Symantec Corporation back in April of 2022. The main contributions of Talos were discussing and analyzing the perpetrator's methods of attack and discovery of a new pattern of software trojan that the researchers are dubbing as "MagicRat". In simple terms, a trojan is a piece of malicious software that is implanted into a user's device or server discreetly, usually with some intent to manipulate information or take control of a device. In the case of these attacks, MagicRat is a remote access trojan that allows for deleting, renaming and moving files as well as extracting information about how to access the device.

As Lazurus is sponsored by the North Korean government, researchers Jung soo An, Asheer Malhotra and Vitor Ventura have noted that, "The main goal of these attacks was likely to establish long-term access into victim networks to conduct espionage operations in support of

North Korean government objectives” (). According to cybersecurity journalist Carly Page, North Korea has also “turned its attention to blockchain and cryptocurrency organizations”, likely in order to support their nuclear weapons programs through funds and international intelligence operations.

Works Cited

Page, C. “North Korea's Lazarus Hackers Are Exploiting Log4j Flaw to Hack US Energy Companies.” TechCrunch, 8 Sept. Retrieved September 12, 2022, https://techcrunch.com/2022/09/08/north-korea-lazarus-united-states-energy/

https://www.econotimes.com/Log4j-And-The-Societal-Threat-Posed-By-Open-Source-Vulnerabilities-1640945

Malhotra, A. “Lazarus and the Tale of Three Rats.” Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Lazarus and the Tale of Three RATs, 1 Jan. Retrieved September 15, 2022, https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html