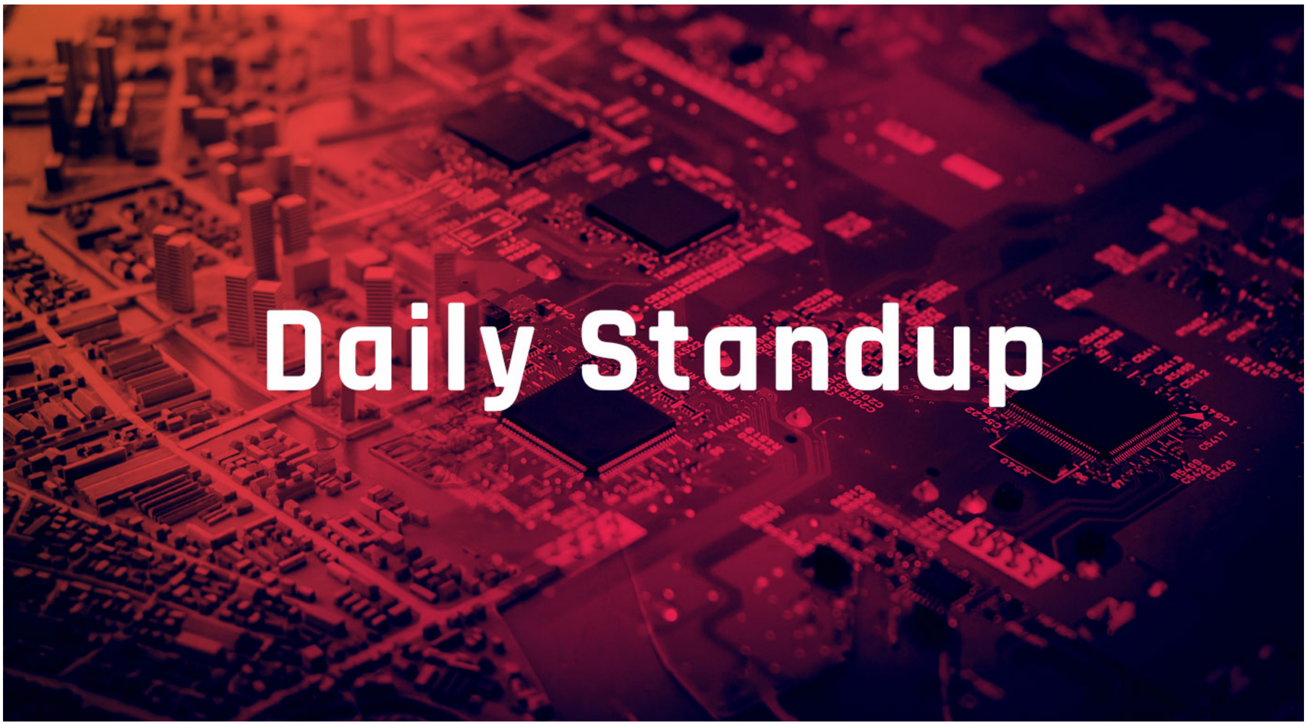
FLASHPOINT

Intelligence Report

Daily Standup

December 11, 2023



North Korean Hacking Ops Continue to Exploit Log4Shell (CyberScoop)

Target audience: Authentication Teams, Board, CISO, CIO, Corporate Communications, Incident Response, Security Ops, Threat Intel/CTI, Windows or Unix Admin Teams

Summary: *Two years after the Log4j vulnerability was revealed, North Korean hackers are continuing to use the flaw in a ubiquitous piece of open source software to carry out attacks as part of a hacking campaign targeting manufacturing, agricultural and physical security entities, according to research released Monday. Carried out over the course of 2023 and described in a report released by Cisco's Talos Intelligence Group on Monday, the campaign employed at least three new malware families and relied, in part, on the Log4Shell exploit, highlighting the long tail of the Log4j vulnerability and how failure to patch the flaw is providing a ready tool to malicious hackers. The campaign was the work of one of a plethora of North Korean hacking units operating under the broad Lazarus umbrella, a term industry and government researchers use to refer to the array of North Korean government hacking operations that engage in everything from cyberespionage to cryptocurrency thefts, ransomware and supply chain attacks. The research is another reminder of the prolific nature of North Korean-linked cyber operations that have targeted South Korea, the U.S. and entities around the world for years. On Dec. 1, the U.S. government announced sanctions on Kimsuky, a premiere*

North Korean cyberespionage unit that also carries out financially motivated cybercrime to both fund itself and generate money for the government.

Analyst comment: "Log4Shell" (CVE-2021-44228) exploits the vulnerability in Log4j, which has been highly targeted because it is relatively easy to exploit and can lead to full control of the targeted server. This new research detailing its continued use by North Korean actors underscores the importance for organizations to monitor for disclosed vulnerabilities and develop a plan to mitigate or patch them to prevent compromise, as threat actors will continue to target organizations that fail to promptly update known vulnerabilities.

See also:

"Operation Blacksmith: Lazarus Targets Organizations Worldwide Using Novel Telegram-Based Malware Written in DLang" (Cisco Talos Blog)

"Over 30% of Log4J Apps Use a Vulnerable Version of the Library" (BleepingComputer)

"Zero-Day Vulnerability in Apache Log4j Disclosed" (Flashpoint)

"Lazarus Group"" (Flashpoint)

Norton Healthcare Discloses Data Breach after May Ransomware Attack (BleepingComputer)

Target audience: Authentication Teams, Board, CISO, CIO, Corporate Communications, Fraud Teams, Incident Response, Security Architects, Security Engineers, Security Ops, Threat Intel/CTI

Summary: *Kentucky health system Norton Healthcare has confirmed that a ransomware attack in May exposed personal information belonging to patients, employees, and dependents. Norton Healthcare serves adult and pediatric patients in more than 40 clinics and hospitals across Greater Louisville, Southern Indiana, and the Commonwealth of Kentucky. Roughly 2.5 million individuals had their data exposed in the attack, according to breach notification letters sent to those affected by the data breach. "On May 9, 2023, Norton Healthcare discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack," it said in a press release published on Friday. "Our investigation determined that an unauthorized individual(s) gained access to certain network storage devices between May 7, 2023, and May 9, 2023, but did not access Norton Healthcare's medical record system or Norton MyChart." The attackers gained access to a wide range of sensitive information, including name, contact information, Social Security Number, date of birth, health information, insurance information, and medical identification numbers. Norton Healthcare says that, for some individuals (likely employees), the exposed data may have also included financial account numbers, driver's licenses or other government ID numbers, and digital signatures. While Norton Healthcare didn't link the attack to a specific ransomware operation, the attack was claimed in late May by the ALPHV (BlackCat) gang.*

Analyst comment: The "BlackCat" (aka "ALPHV") ransomware group first posted on its blog site that it had targeted the Norton Healthcare health system as one of its victims in May 2023. Flashpoint analysts assess that ransomware groups will remain a large threat to several sectors, including critical infrastructure, healthcare, education systems, and financial services. Attacks on organizations in these industries can have outsized impacts on organizations' operations, as well as high visibility, which may provide additional pressure to pay a ransom.

See also:

"Notice of Security Incident" (Norton Healthcare)

ALPHV/BlackCat Ransomware Blog Site (Flashpoint Collections)

Stolen Checks Are for Sale Online. We Called Some of the Victims. (New York Times)

Target audience: Fraud Teams, Threat Intel/CTI

Summary: *Check fraud is growing rapidly, and there's one big reason: Anyone with a smartphone can download an app and within minutes get access to bundles of stolen checks that thieves are selling in open forums. It starts with a pretty low-tech operation, after people pay bills, put checks in envelopes and drop them into a blue mailbox. At that point, criminals find ways to take them out. Or it's an inside job at the post office, or elsewhere. Next, the thieves choose from a number of paths that could involve selling the checks on Telegram, or keeping them. Either way, their next move is often to assume a fake identity in order to open a bank account where the check will end up. They typically will wash the ink off a stolen check, rewrite it to their new identity, deposit it, withdraw the money and then abandon the new account. Rinse and repeat. It's a fast-growing business. During the first year of the pandemic, the Postal Service received 299,020 mail theft complaints, an increase of 161 percent from the previous year, according to the Financial Crimes Enforcement Network. Financial institutions also reported triple-digit increases. Socure, a company that sells digital identity confirmation services to banks, says it believes there may be nearly 2.5 million so-called synthetic identity accounts out there in the world, sitting in wait for nefarious dealings.*

Analyst comment: Threat actors will often employ stolen checks in their fraud methods, and the buying and selling of this data remains very popular across many areas of Flashpoint collections. The data taken from these checks can be used to facilitate account theft or identity theft, or for the creation of synthetic identities. Tools within the Flashpoint Intelligence Platform such as Optical Character Recognition searches can help identify where threat actors may be posting checks, as well as to better understand the tactics of the actors who are acquiring or selling them.

See also:

"Check Fraud in Illicit Online Communities" (Flashpoint)

Check Image Optical Character Recognition Search (Flashpoint Collections)

Additional stories are included below, as they are of interest to threat intelligence teams:

"The EU Just Passed Sweeping New Rules to Regulate AI" (Wired)

“Apple Confirms It Has Blocked iMessage Exploit” (Engadget)

“ALPHV/BlackCat Takedown Appears to Be Law Enforcement Related” (Dark Reading)

“Microsoft: Outlook Email Sending Issues for Users with Lots of Folders” (BleepingComputer)

“SLAM Attack: New Spectre-Based Vulnerability Impacts Intel, AMD, and Arm CPUs” (Hacker News)

“Bitcoin, Ether, and Major Altcoins in Deep Red” (CoinDesk)

Please find past standups at https://fp.tools/home/intelligence/standup.