BLACKSWAN CYBERSECURITY

THREAT ADVISORY

December 14, 2023

North Korea's Lazarus Group's DLang-Based RAT Targeting VMWare Horizon Servers via Log4j

SUMMARY

The Lazarus group (North Korea) continues to leverage the Log4Shell vulnerability (CVE-2021-44228) as an opportunity to deploy 3 Dlang-based malware families.

TECHNICAL DETAILS

Cisco Talos identified several attacks that exploited the Log4Shell vulnerability, specifically targeting VMWare Horizon servers publicly exposed and utilizing a Log4j version susceptible to remote code execution (RCE). Talos named this attack campaign "Operation Blacksmith", which uncovered 2 new remote access trojans (RATs), NineRAT and DLRAT, along with a malware downloader named BottomLoader. A noteworthy shift in Lazarus' tactics is observed, marked by the uncommon use of the D programming language to develop the malware strains, possibly to evade detection:

- NineRAT leverages the Telegram API for command-and-control communication, executing commands and exfiltrating files from compromised systems.
- DLRAT, a trojan and downloader that initiates its activity by collecting system information and sending it to a command-and-control server.
- BottomLoader fetches and executes payloads using PowerShell, establishing persistence, and allowing file exfiltration.

Talos also indicated that Lazarus may share the collected victim data with other APT groups or clusters within its umbrella, based on observed system "re-fingerprinting".

INDICATORS OF COMPROMISE

SHA256:

HazyLoad

- 000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee

NineRAT

- 534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433
- ba8cd92cc059232203bcadee260ddbae273fc4c89b18424974955607476982c4
- 47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30
- f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59
- 5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541
- 82d4a0fef550af4f01a07041c16d851f262d859a3352475c62630e2c16a21def

BottomLoader

- 0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f

DLRAT

- e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f
- 9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a

Domains and IPv4:

- tech[.]micrsofts[.]com
- tech[.]micrsofts[.]tech
- 27[.]102[.]113[.]93
- 185[.]29[.]8[.]53
- 155[.]94[.]208[.]209
- 162[.]19[.]71[.]175
- 201[.]77[.]179[.]66
- hxxp://27[.]102[.]113[.]93/inet[.]txt
- hxxp[://]162[.]19[.]71[.]175:7443/sonic/bottom[.]gif
- hxxp[://]201[.]77[.]179[.]66:8082/img/Index[.]php
- hxxp[://]201[.]77[.]179[.]66:8082/img/images/header/B691646991EBAEEC[.]gif
- hxxp[://]201[.]77[.]179[.]66:8082/img/images/header/7AEBC320998FD5E5[.]gif

RECOMMENDATIONS

- Urgently update and patch the Log4j library on all publicly facing VMWare Horizon servers to address the vulnerability and prevent remote code execution.
- Implement network segmentation to restrict access to critical systems and reduce the attack surface, isolating the VMWare Horizon servers from unnecessary exposure.
- Review and reinforce access controls, ensuring that only authorized personnel have access to critical systems. Employ the principle of least privilege to minimize potential attack vectors.
- Endpoint protection is crucial to thwart the execution of the malware outlined in this advisory.
- Implement web scanning tools to proactively block access to malicious websites and identify malware commonly used in such attacks.
- For email security, deploy solutions to block malicious emails that threat actors may use as part of their campaigns.
- Utilize advanced firewall appliances capable of detecting and mitigating malicious activities associated with emerging threats.
- Leverage malware analytics tools to identify and proactively protect against malicious binaries, integrating robust security across your infrastructure.
- Secure your internet gateway to block connections to malicious domains, IPs, and URLs, regardless of user location.
- Automate web security measures to automatically block potentially harmful sites and assess suspicious sites before user access.
- Enhance protection by leveraging additional security measures tailored to your specific environment and threat data.
- Implement multi-factor authentication solutions to ensure only authorized users access your network securely.

REFERENCES

- https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/
- https://thehackernews.com/2023/12/lazarus-group-using-log4j-exploits-to.html
- https://www.bleepingcomputer.com/news/security/lazarus-hackers-drop-new-rat-malware-using-2-year-old-log4j-bug