Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

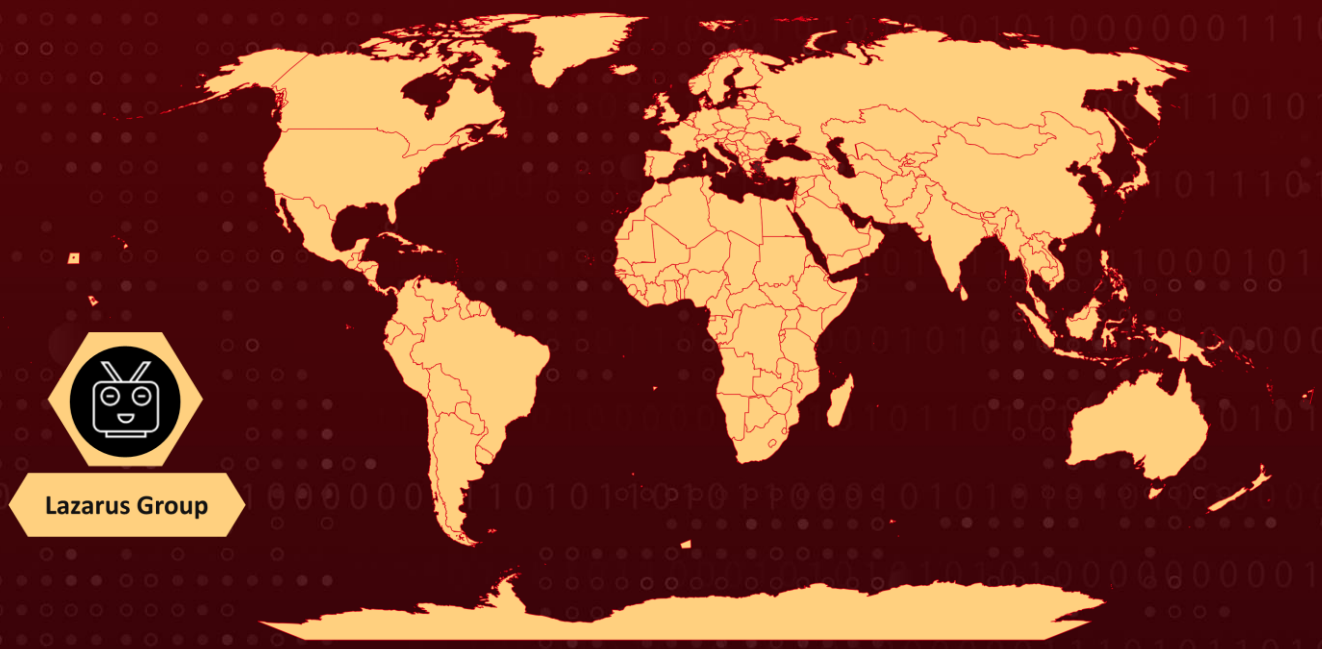
Lazarus's Operation Blacksmith Deploys Novel Dlang RATs

Date of Publication	Admiralty Code	TA Number
December 12, 2023	A1	TA2023498

Summary

First Discovered: March 2023
Attack Region: Worldwide
Targeted Industries: Manufacturing, Agricultural and Physical security companies
Actor: Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)
Malware: NineRAT, DLRAT, BottomLoader, HazyLoad
Attack: The Lazarus Group, a North Korea-linked threat actor, has been identified in a new global campaign called "Operation Blacksmith." In this campaign, the group opportunistically exploits the security vulnerability CVE-2021-44228 in Log4j to deploy previously undocumented RATs on compromised hosts, namely NineRAT, DLRAT, and BottomLoader.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-44228	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✓	✓	✓

Attack Details

#1 The famous North Korean hacking group, Lazarus, is persistently exploiting the Log4j vulnerability (CVE-2021-44228), also known as "Log4Shell." In this instance, Lazarus is deploying three previously undiscovered malware families, all written in DLang. These include two remote access trojans (RATs) named NineRAT and DLRAT, as well as a malware downloader called BottomLoader.

#2 Lazarus Group's new RAT, NineRAT, uses the Telegram API for C2 communication, allowing attackers to send commands, exfiltrate files, and establish persistence on compromised systems. Developed in May 2022, NineRAT was used in attacks against a South American agricultural organization in March 2023 and a European manufacturing entity in September 2023. It offers capabilities like command sending, system information gathering, file uploading, downloading, self-uninstallation, and upgrades.

#3 Lazarus utilizes DLRAT, a trojan and downloader, to deploy additional payloads on compromised systems. DLRAT executes pre-defined commands to collect system information, such as the operating system and network MAC address, and transmits this data to the C2 server. The C2 server responds with the victim's IP address and instructions for local execution. The malware is designed to recognize specific command codes or names, triggering corresponding actions on the infected system.

#4 BottomLoader, a malware downloader employed by Lazarus, is responsible for fetching and executing payloads from a hardcoded URL using PowerShell. It establishes persistence by modifying the Startup directory. Additionally, BottomLoader equips Lazarus with the capability to exfiltrate files from the infected system to the C2 server, enhancing operational versatility.

#5 In Operation Blacksmith, the Log4Shell vulnerability enabled remote code execution on VMWare Horizon servers. The attackers set up a proxy tool called HazyLoad, executed reconnaissance commands, created new admin accounts, and deployed credential-stealing tools. Lazarus introduced NineRAT, which conducts re-fingerprinting suggesting that data collected by Lazarus via NineRAT may be shared among other APT groups and stored in a different repository than during their initial access and implant deployment phase.

#6 This campaign marks a significant change in the tactics and tools employed by Lazarus, showcasing the threat group's ability to adapt and evolve its strategies.

Recommendations

Apply Patch: Install the security patch provided by Apache to address the CVE-2021-44228 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations can contain the spread of malware and prevent it from accessing critical systems and sensitive data.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
T1574 Hijack Execution Flow	T1134 Access Token Manipulation	T1547 Boot or Logon Autostart Execution	T1102 Web Service
T1082 System Information Discovery	T1003 OS Credential Dumping	T1003.005 Cached Domain Credentials	T1112 Modify Registry
T1518 Software Discovery	T1136 Create Account	T1098 Account Manipulation	T1033 System Owner/User Discovery
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee, 534f5612954db99c86baa67ef51a3ad88bc21735bce7bb591afa8a4317c35433, ba8cd92cc059232203bcadee260ddbae273fc4c89b18424974955607476982c4, 47e017b40d418374c0889e4d22aa48633b1d41b16b61b1f2897a39112a435d30, f91188d23b14526676706a5c9ead05c1a91ea0b9d6ac902623bc565e1c200a59, 5b02fc3cfb5d74c09cab724b5b54c53a7c07e5766bffe5b1adf782c9e86a8541, 82d4a0fef550af4f01a07041c16d851f262d859a3352475c62630e2c16a21def, 0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f, e615ea30dd37644526060689544c1a1d263b6bb77fe3084aa7883669c1fde12f, 9a48357c06758217b3a99cdf4ab83263c04bdea98c347dd14b254cab6c81b13a
Domain	tech[.]micrsofts[.]com, tech[.]micrsofts[.]tech
IP	27[.]102[.]113[.]93, 185[.]29[.]8[.]53, 155[.]94[.]208[.]209, 162[.]19[.]71[.]175, 201[.]77[.]179[.]66
URL	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

Patch Details

Upgrade Log4j to the latest version or, at a minimum, to the fixed versions: Log4j 2.3.1 (for Java 6), 2.12.3 (for Java 7), or 2.17.0 (for Java 8 and later)

Link:
https://logging.apache.org/log4j/2.x/security.html

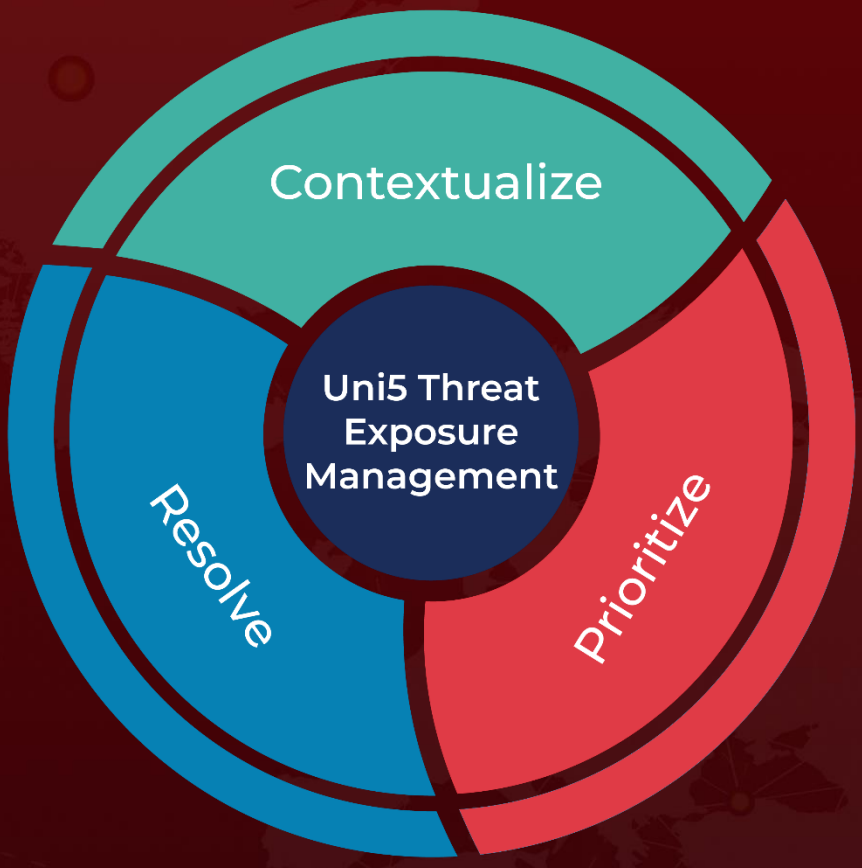
References

https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 12, 2023 . 4:45 AM

More at www.hivepro.com