Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Lazarus Group Uses ManageEngine Exploit to Unlock Path for QuiteRAT

Date of Publication	Admiralty Code	TA Number
August 25, 2023	A1	TA2023345

Summary

Attack Began: February 2023
Malware: QuiteRAT, CollectionRAT
Threat Actor: Lazarus Group
Attack Region: Europe and the U.S.
Targeted Industry: Healthcare, IT, Critical Infrastructure
Attack: The Lazarus Group, a threat actor associated with North Korea, has been detected utilizing a recently patched critical security vulnerability in Zoho ManageEngine ServiceDesk Plus. This vulnerability was exploited to deploy a remote access trojan known as QuiteRAT.

Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine	✗	✓	✓

Attack Details

#1 The Lazarus Group, a malevolent entity linked to North Korea, has been identified exploiting a recently rectified critical security vulnerability within Zoho ManageEngine ServiceDesk Plus. This security loophole was leveraged to deploy a remote access trojan (RAT) known as QuiteRAT. In addition to deploying the QuiteRAT malware, the Lazarus Group has introduced a new malware named CollectionRAT.

#2 Exhibiting conventional RAT capabilities, CollectionRAT enables the execution of arbitrary commands on compromised systems. This newly emerged threat, CollectionRAT, appears to share connections with Jupiter/EarlyRAT, another strain of malware attributed to **Andariel**, a subgroup nestled within the expansive Lazarus Group threat actor-network.

#3 During the early months of 2023, the Lazarus Group accomplished a successful breach of an internet backbone infrastructure provider in Europe. They subsequently utilized this compromised position to effectively distribute QuiteRAT. This exploit entailed leveraging a vulnerable ManageEngine ServiceDesk instance (CVE-2022-47966) as the initial point of entry. The success of this exploitation triggered the immediate retrieval and execution of a malicious QuiteRAT binary through the Java runtime process.

#4 Upon activation, the implant promptly transmitted preliminary system data to its designated command and control (C2) servers. It then remained dormant, anticipating instructions from the C2, which could encompass command codes for execution or specific Windows commands designed for endpoint reconnaissance.

#5 QuiteRAT functions as a relatively simple remote access trojan, composed of compact statically linked Qt libraries and proprietary code. The Qt framework forms the basis for creating cross-platform applications. Striking similarities between the deployed implants indicate that QuiteRAT stems from the evolution of **MagicRAT**.

#6 Alongside their shared reliance on the Qt framework, both implants offer similar functionalities, including the execution of arbitrary commands on compromised infrastructure. Notable advancements in Lazarus Group's tactics have emerged, involving the integration of open-source tools. Notably, Mimikatz is used for credential theft, PuTTY Link (Plink) aids in remote tunneling, and DeimosC2 facilitates communication for command-and-control operations.

Recommendations

Prioritize Patching CVE-2022-47966: Immediately apply the patch for Zoho ManageEngine (CVE-2022-47966) to mitigate the risk of Lazarus Group exploiting the vulnerability. Timely patching is essential to prevent unauthorized access and potential deployment of malicious software.

Application Whitelisting: Employ application whitelisting to restrict the execution of unauthorized software on systems. This can prevent the execution of malicious code, even if an initial breach occurs.

Zero Trust Architecture: Implement a zero-trust architecture, where trust is not assumed even within the network. Authenticate and authorize every user and device attempting to access resources, reducing the potential for lateral movement by threat actors.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1059 Command and Scripting Interpreter	**T1574.002** DLL Side-Loading	**T1497** Virtualization/Sandbox Evasion	**T1056** Input Capture
T1018 Remote System Discovery	**T1082** System Information Discovery	**T1518.001** Security Software Discovery	**T1087.002** Domain Account
T1071 Application Layer Protocol	**T1095** Non-Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1574** Hijack Execution Flow

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	146[.]4[.]21[.]94, 109[.]248[.]150[.]13, 108[.]61[.]186[.]55:443

TYPE	VALUE
SHA256	db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984, 773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df, 05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d, ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6, e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe
URLs	hxxp[://]146[.]4[.]21[.]94/tmp/tmp/comp[.]dat, hxxp[://]146[.]4[.]21[.]94/tmp/tmp/log[.]php, hxxp[://]146[.]4[.]21[.]94/tmp/tmp/logs[.]php, hxxp[://]ec2-15-207-207-64[.]ap-south-1[.]compute[.]amazonaws[.]com/resource/main/rawmail[.]php, hxxp[://]109[.]248[.]150[.]13/EsaFin[.]exe, hxxp[://]146[.]4[.]21[.]94/boards/boardindex[.]php, hxxp[://]146[.]4[.]21[.]94/editor/common/cmod

Patch Link

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

References

https://blog.talosintelligence.com/lazarus-quiterat/

https://blog.talosintelligence.com/lazarus-collectionrat/

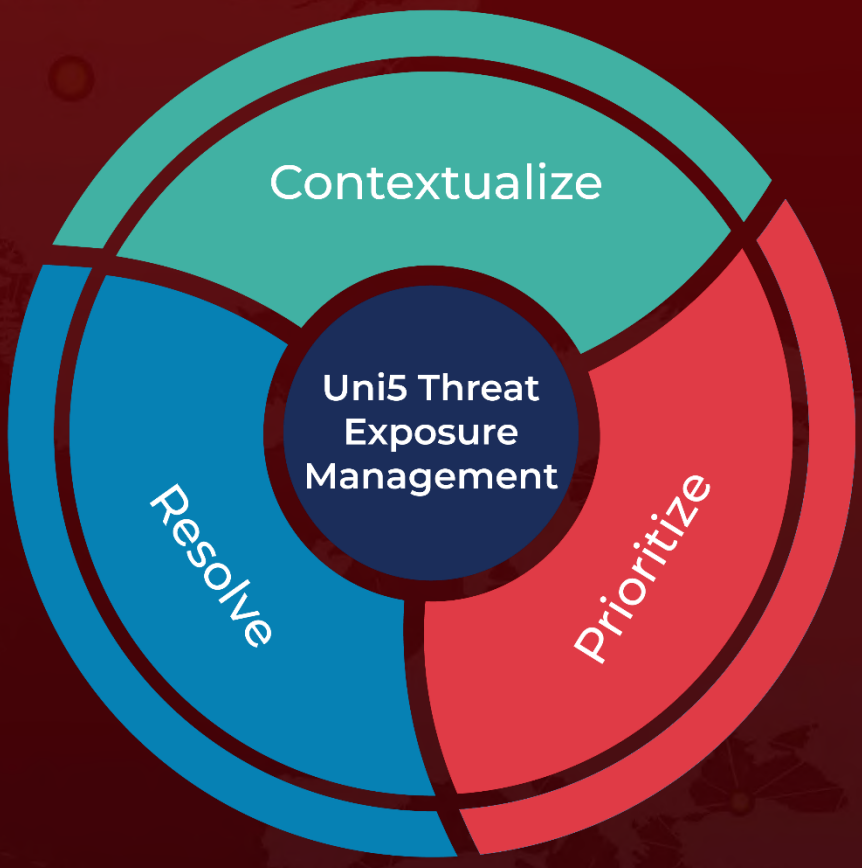
https://www.hivepro.com/lazarus-deploys-new-attack-tool-magicrat-to-target-organizations-worldwide/

https://www.hivepro.com/andariel-group-unleashes-new-earlyrat-malware/

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

August 25, 2023 • 5:30 AM

More at www.hivepro.com