Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

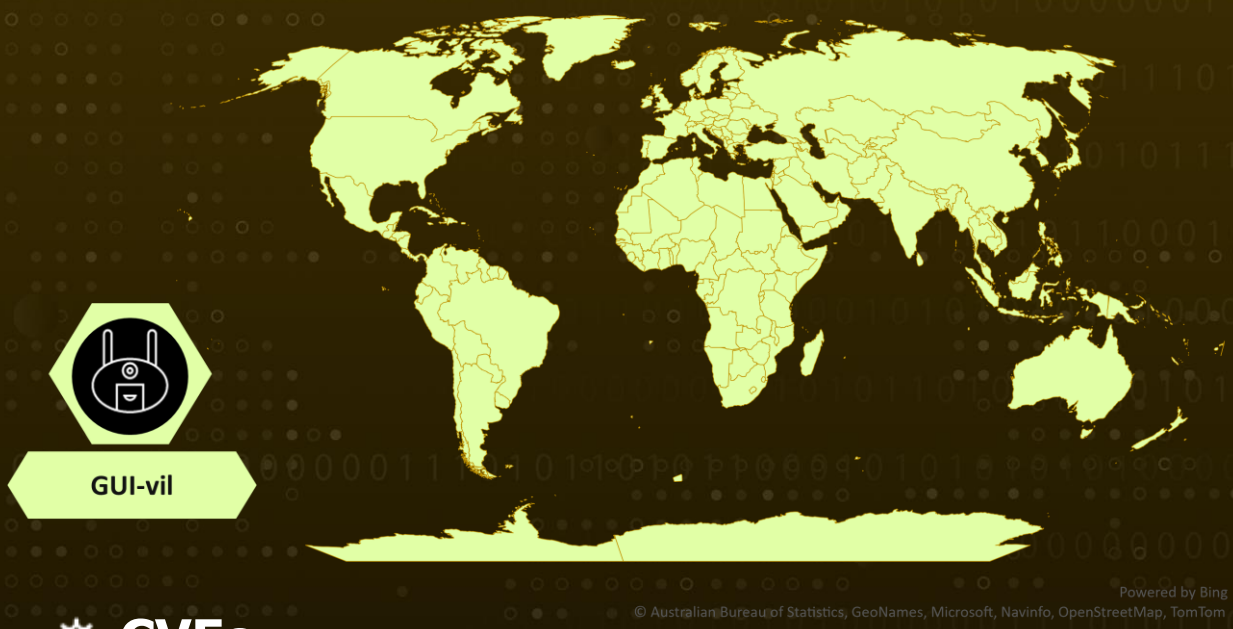
GUI-Vil Threat Group Exploits AWS for Crypto Mining

Date of Publication	Admiralty Code	TA Number
May 24, 2023	A1	TA2023244

Summary

First seen: November 2021
Actor: GUI-vil (aka p0-LUCR-1)
Attack Region: Worldwide
Affected Platform: AWS
Attack: GUI-Vil (p0-LUCR-1), an Indonesian threat group, conducts unauthorized cryptocurrency mining using personalized infiltration tactics. They exploit AWS, leveraging compromised credentials and vulnerabilities like CVE-2021-22205. GUI-Vil favors GUI tools and was last observed in April 2023.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-22205	GitLab Remote Code Execution Vulnerability	Community and Enterprise Editions From 11.9	✗	✓	✓

Attack Details

#1 GUI-vil, also known as p0-LUCR-1, is a threat group based in Indonesia driven by financial motives. Their main objective is to engage in unauthorized cryptocurrency mining activities. By using compromised credentials, this group has been observed exploiting Amazon Web Services (AWS) EC2 instances to carry out their Contraband crypto-mining operations.

#2 The first sighting of GUI-vil occurred in November 2021, and their most recent activity was observed in April 2023. Notably, this group prefers to utilize Graphical User Interface (GUI) tools, particularly an older version of S3 Browser (version 9.5.5) released in January 2021, for their initial operations. Once they gain access to the AWS Management Console, they conduct their operations directly through the web browser.

#3 GUI-vil initiates its operations with a reconnaissance phase, which involves monitoring public sources like GitHub and Pastebin for exposed AWS keys, as well as scanning vulnerable GitLab instances. The initial compromises primarily stem from exploiting known vulnerabilities such as CVE-2021-22205 or leveraging publicly exposed credentials.

#4 GUI-vil distinguishes itself from other groups by focusing on crypto mining is their personalized approach to establishing a foothold in the targeted environment. They create usernames that match the victim's naming standards, striving to appear as legitimate users.

#5 In some instances, GUI-vil even seizes control of existing user accounts by generating login profiles where none existed previously. By utilizing compromised credentials, GUI-vil deploys EC2 instances explicitly for carrying out crypto mining activities.

Recommendations

Strengthen Vulnerability Management: Organizations should prioritize regular vulnerability assessments and patch management to mitigate the risk of known vulnerabilities like CVE-2021-22205. By promptly applying security patches and updates, the chances of exploitation by threat actors like GUI-Vil can be significantly reduced.

Enhance threat detection: Alongside traditional security measures, organizations should deploy advanced solutions like AWS GuardDuty. Leveraging machine learning and threat intelligence, these services detect sophisticated threats, including those employed by threat actors like GUI-Vil. By monitoring for malicious activities, anomalies, and unauthorized access attempts, they offer early warnings and actionable insights to swiftly respond to potential threats.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0040 Impact	**T1596** Search Open Technical Databases	**T1098** Account Manipulation	**T1078** Valid Accounts
T1068 Exploitation for Privilege Escalation	**T1496** Resource Hijacking	**T1021** Remote Services	**T1021.004** SSH
T1211 Exploitation for Defense Evasion	**T1538** Cloud Service Dashboard		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	182.1.229[.]252 114.125.247[.]101 114.125.245[.]53 114.125.247[.]101 114.125.232[.]189 114.125.228[.]81 114.125.229[.]197 114.125.246[.]235 114.125.246[.]43 36.85.110[.]142

Patch Links

https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

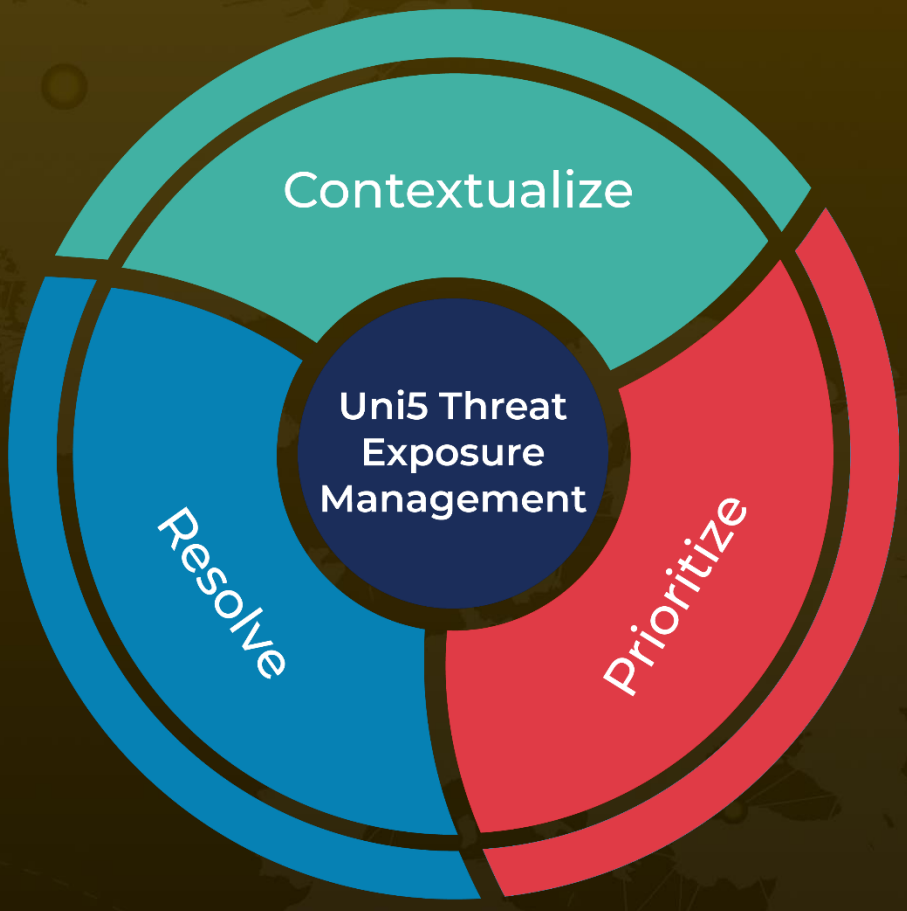
References

https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor/

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

May 24, 2023 • 5:46 AM

More at www.hivepro.com