1.1.1 *GUI-vil*

Threat Actor Group	
Name	GUI-vil, p0-LUCR-1
Class	Cybercrime
Active since	2021
Source geography	Indonesia
Primary language	English
Associated actors	No known associated threat actors.
Summary	GUI-vil, also known as p0-LUCR-1, is an Indonesian threat actor group that conducts unauthorized cryptocurrency mining for financial motives. The group is known to achieve this through the exploitation of Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances. The group is assessed to not have a specific target region, but rather attacks any organization they can compromise credentials from. They were first observed to be active on November 13, 2021.[1] The group is observed to obtain initial access by monitoring public sources for exposed AWS keys (GitHub, Pastebin) and scanning for vulnerable GitLab instances. The group most often utilizes Graphical User Interface (GUI) tools, especially an older version of S3 Browser (version 9.5.5) released in January 2021, and AWS Management Console. Once they gain access to the AWS Management Console, they conduct their operations directly through the web browser. The group is an engaged attacker that does not rely on automation. They often mimic the victims' usernames and create login profiles from existing users that don't have login profiles to maintain undetected and access the environment for as long as possible. The threat actor group has also been observed to create Identity and Access Management (IAM) users with access keys to ensure that they can persist in the environment with these new users after the original compromised credentials are discovered. The group creates EC2 instances with new SSH key pairs to achieve their goal of cryptomining. They make sure that the SSH port (22) is openly accessible to the internet for any EC2 instances they create to maintain access to the AWS environment. The group was most recently observed to be active on April 18, 2023.

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

Goal orientation	
Motivation	Given its modus operandi and target on cryptocurrency mining, we assess GUI-vil to be financially motivated.
Intended effect	The primary intended effect of this threat actor is to conduct unauthorized crytocurrency mining for financial gain.

Intent	
Target geography	There is insufficient information available on GUI-vil's victim list, however given their targeting of the AWS environment, a globally used tool, we posit they are opportunistic in nature and conducted worldwide targeting.
Target sector	Due to insufficient information available on victims, we cannot confirm if the group targeted specific sectors. However, as with above, we posit they are opportunistic in nature and target victims based on their AWS environments, rather than geolocation or industry.
Target areas	The threat actor is known to target Amazon Web Services (AWS).
Intent score	Given GUI-vil's targeting is driven by targeting organisations with vulnerable AWS environments, including the services in use by CLIENTHK, we assess the threat actor to have a **MEDIUM** intent to target CLIENTHK.

Capability	
Resources	From the timeframe of 2021-2023, we observe the threat actor prefers deploying Graphical User Interface (GUI) tools, specifically version 9.5.5 of S3 Browser for their initial operations, and the AWS Management Console web browser after gaining access. GUI-vil's initial compromises are most often achieved through the known vulnerabilty CVE-2021-22205 and publicly exposed credentials, suggesting a low to moderate level of technological resources. GUI-vil has no associated actors and there is no indication on the size of manpower or finances. Due to resource limitations set by victim organizations, GUI-vil most often would only be able to create a few EC2 instances from each account, limiting their profit from each attack.[2] In fact, the profit they make from cryto mining is most likely much smaller than the cost of running the EC2 instances. Based on this, we suspect the threat actor has **VERY LOW** level of resources.
Skills	The threat actor displays a **LOW** technical skillset in their ability to target AWS environments using vulerabilities to GitLab and exposed access keys on public sources. The group showcases a **LOW** technical understanding of AWS environments.
Resolve	The threat actor is willing to continue fight for access after defenders detect them, particularly by monitoring the CloudTrail logs to bypass the restrictions the organization is imposing on them. The threat actor also has been observed to create IAM users to persist in the environment after the original compromised credentials are discovered. As such, they are assessed to have a **MEDIUM** degree of resolve against disruption/detection efforts.
Access to target	The threat actor has demonstrated a **LOW to MEDIUM** level of competency in gaining entry to a victim's network, utilising vulnerable instances of GitLab or public sources to obtain AWS access keys.
Risk sensitivity	There is insufficient information available on the threat actor's risk sensitivity. However, given that the group is financially motivated by small sums from crytomining and that they have very low level of resources, we posit the group has a **LOW** risk appetite.
Capability score	Given the above observations and our understanding of the capability of other threat actors in this category, we assess that this threat actor has **LOW** capability.

[2] https://cybr.com/cloud-security/how-crypto-miners-hijack-aws-accounts-cryptojacking-gui-vil-case-study/

Modus Operandi	
Reconnaissance	GUI-vil will monitor common public sources such as GitHub and scan for vulnerable versions of software repositories such as GitLab for exposed AWS access keys. The group will then review the accessibility of each access key on S3 Browser and execute the list bucket command for those that are active. The threat actor also has been observed to explore the accessible services utilized by the victim organization via the AWS Management Console.
Preparation	The threat actor group is not known to use malware. ***Vulnerability exploits:*** The vulnerability known to have been used by this threat actor is: • CVE-2021-22205[3] – GitLab vulnerability that enables threat actors to upload malicious image files to a file parser, resulting in Remote Code Execution (or RCE). GUI-vil is known to exploit this vulnerability to obtain the victim organization's AWS access keys.
Infiltration	Upon accessing the cloud credentials, the threat actor most often does not require to perform privilege escalation as the threat actor has obtained an administrative account. However, in one case, the threat actor only had access to read-only permissions. They then reviewed all the S3 buckets and was able to find credentials with full administrator privileges in a terraform state file.
Entrenchment	The threat actor is observed to establish persistence in the following ways: • GUI-vil has been observed to create Identity and Access Management (IAM) users with access keys to ensure that they can persist in the environment after the original compromised credentials are discovered. They would masquerade as real users, such as naming the new IAM user as *sec_audit* to resemble the other audit users in the organization. However, the threat actor has also been observed to make mistakes by leaving the S3 Browser's default name. • GUI-vil has been observed to create login profiles to existing identities in the organization without login profiles. The group would have access to the identities without alarming security teams that do not monitor the creation of login profiles. • GUI-vil maintains persistence in the AWS environment by being connected to the EC2 instances via new SSH key pairs. The attacker makes sure that the SSH port (22) is openly accessible to the internet for any EC2 instances they create. • GUI-vil disabled detailed CloudWatch monitoring on all their EC2 instances. • After being detected by the organization, the threat actor is known to monitor CloudTrail logs to bypass the restrictions the defenders are imposing on them.
Compromise	---
Exploitation	Unlike other threat actors explored, GUI-vil does not, that we know of, deploy ransomware, or encrypt data. Instead, the group is focused on leveraging compromised systems to hijack resources to facilitate cryptocurrency mining, with the motive of earning virtual currency.

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22205

MITRE ATT&CK Techniques deployed	• Search Open Websites/Domains: Code Repositories – T1593.003 • Account Manipulation: Additional Cloud Credentials – T1098.001 • Account Manipulation: Additional Cloud Roles – T1098.003 • Account Manipulation: Additional Cloud Credentials – T1098.004 • Valid Accounts: Cloud Accounts – T1078.004 • Exploitation for Privilege Escalation – T1068 • Resource Hijacking – T1496 • Remote Services: Cloud Services – T1021.007 • Remote Services: Direct Cloud VM Connections – T1021.008 • Remote Services: SSH – T1021.004 • Exploitation for Defense Evasion – T1211 • Cloud Service Dashboard – T1538 • Masquerading: Match Legitimate Name or Location – T1036.005 • Exploit Public-Facing Application – T1190 • Create Account: Cloud Account – T1136.003 • Account Discovery: Cloud Account – T1087 • Active Scanning: Vulnerability Scanning – T1595.002 • Compromise Accounts: Cloud Accounts –T1586.003 • Exploitation for Credential Access – T1212 • Financial Theft – T1657 • Disable or Modify Cloud Logs – T1562.008 • Cloud Infrastructure Discovery – T1580 • Cloud Service Discovery – T1526 • Cloud Storage Object Discovery – T1619 • Data from Cloud Storage – T1530

Activity	
Activity score	We have observed GUI-vil to be **Not Known or Reported to be Active** with actively most recently observed on April 18, 2023.