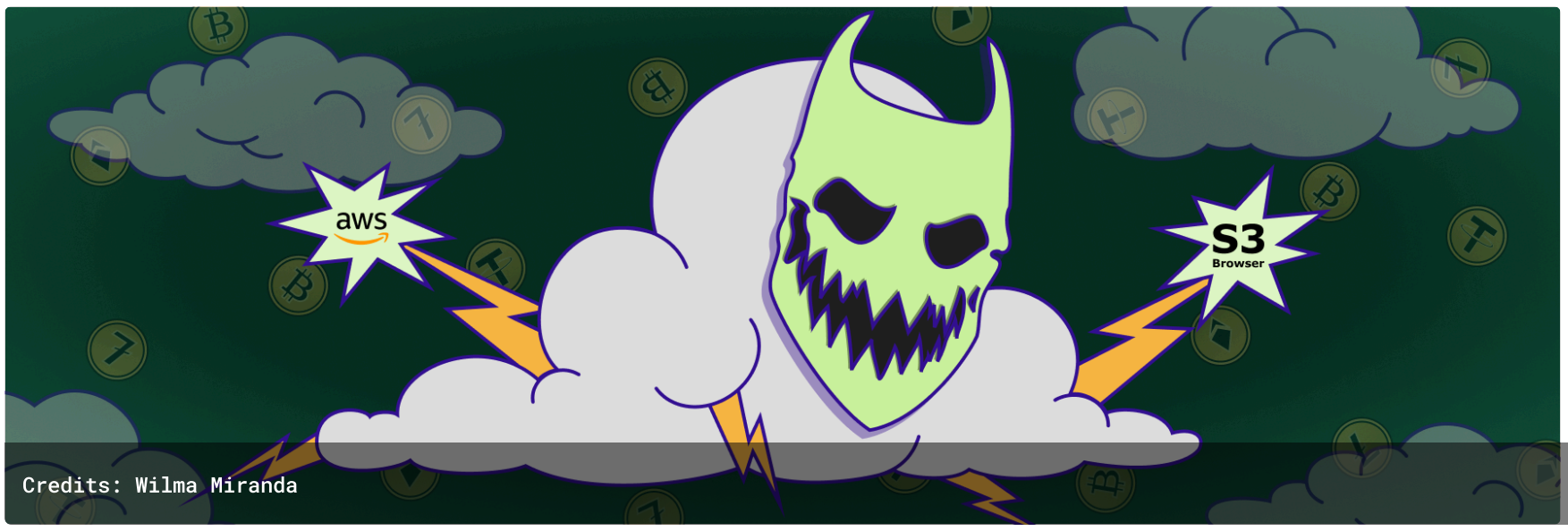
IAN AHL | 22 MAY 2023

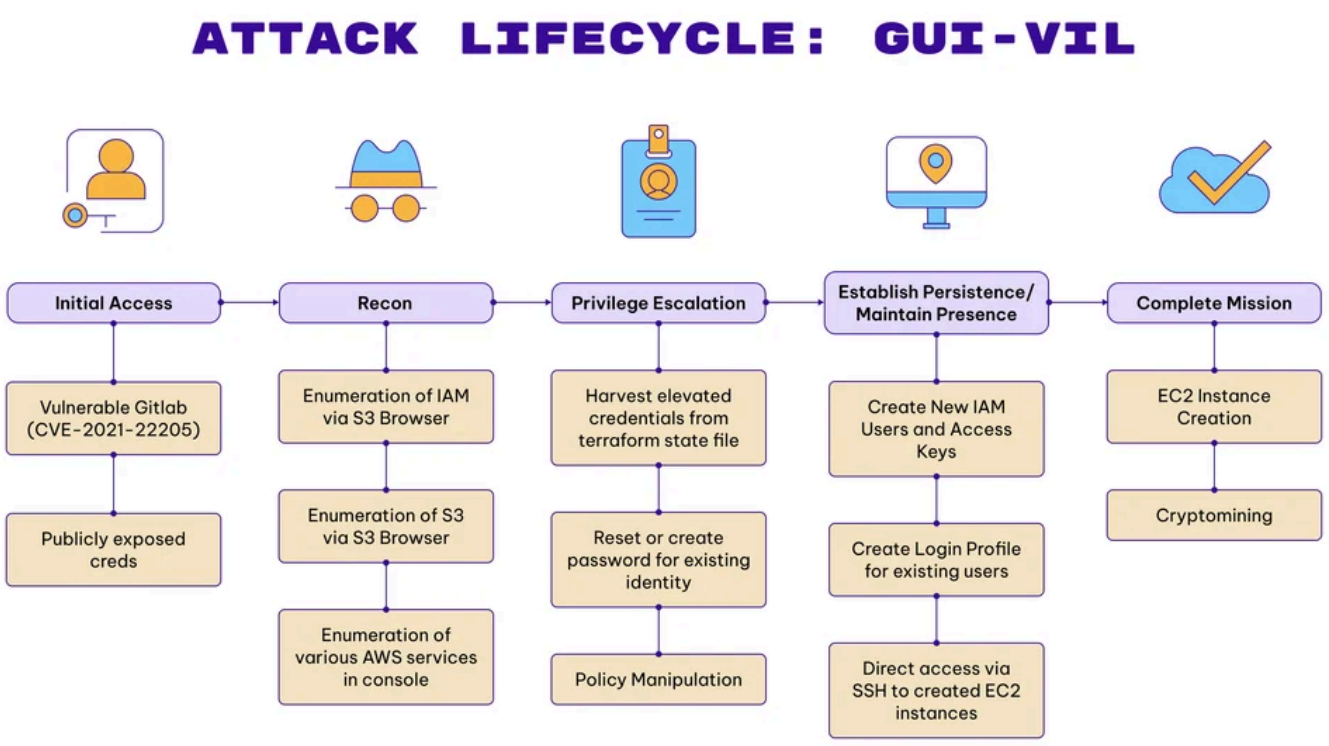
BACK TO BLOGS

UNMASKING GUI-VIL: FINANCIALLY MOTIVATED CLOUD THREAT ACTOR



Credits: Wilma Miranda

SUMMARY (THE TL;DR)



Permiso's p0 Labs has been tracking a threat actor for the last 18 months. In this article we will describe the attack lifecycle and detection opportunities for the cloud-focused, financially motivated threat actor we have dubbed as p0-LUCR-1, aka GUI-vil (Goo-ee-vil).

GUI-vil is a financially motivated threat group sourcing from Indonesia whose primary objective is performing unauthorized cryptocurrency mining activities. Leveraging compromised credentials, the group has been observed exploiting Amazon Web Services (AWS) EC2 instances to facilitate their illicit crypto mining operations. Permiso first observed this threat actor in November of 2021, and most recently observed their activity in April of 2023.

The group displays a preference for Graphical User Interface (GUI) tools, specifically an older version of S3 Browser (version 9.5.5, released January of 2021) for their initial operations. Upon gaining AWS Management Console access, they conduct their operations directly through the web browser.

The source IP addresses associated with the attacker's activities are linked to two (2) specific Indonesian Autonomous System Numbers (ASNs) - PT. Telekomunikasi Selula and PT Telekomunikasi Indonesia.

In their typical attack lifecycle, GUI-vil initially performs reconnaissance by monitoring public sources for exposed AWS keys (GitHub, Pastebin) and scanning for vulnerable GitLab instances. Initial compromises are predominantly achieved via exploiting known vulnerabilities such as CVE-2021-22205, or via using publicly exposed credentials.

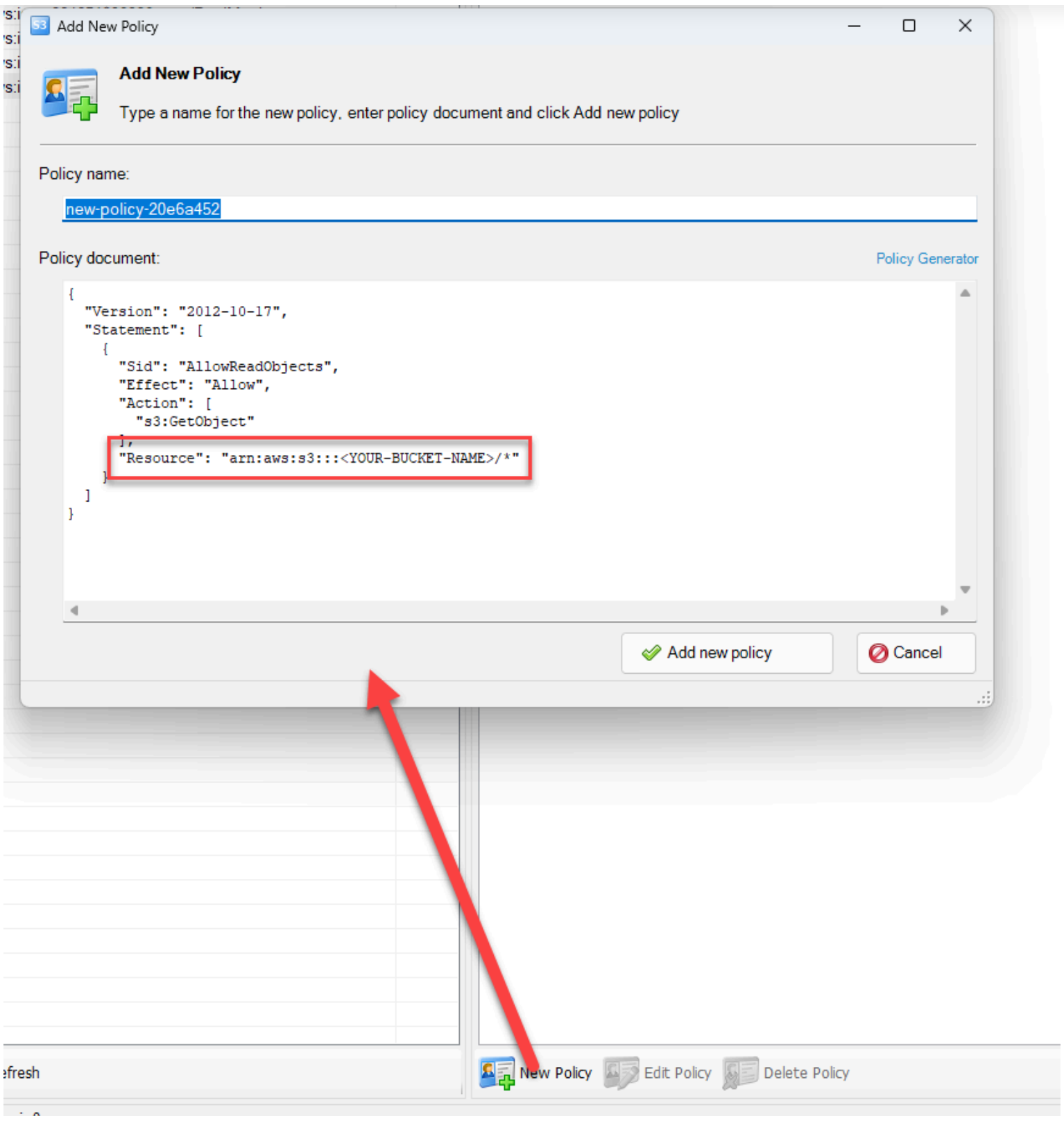
GUI-vil, unlike many groups focused on crypto mining, apply a personal touch when establishing a foothold in an environment. They attempt to masquerade as legitimate users by creating usernames that match the victim's naming standard, or in some cases taking over existing users by creating login profiles for a user where none existed (takeover activity appearing as `iam:GetLoginProfile` failure followed by successful `iam:CreateLoginProfile`).

The group's primary mission, financially driven, is to create EC2 instances to facilitate their crypto mining activities. In many cases the profits they make from crypto mining are just a sliver of the expense the victim organizations have to pay for running the EC2 instances.

ATTACKER ATTRIBUTES

Highlights:

- Unlike many commodity threat actors in the cloud that rely on automation, GUI-vil are engaged attackers at the keyboard, ready to adapt to whatever situation they are in.
- They are allergic to CLI utilities, using S3 Browser and AWS Management Console via web browsers as their tooling.
- They apply a personal touch. They model the name of their IAM Users, and sometimes their policies, keypairs, etc., on what they find present in the environment. Often time this helps them blend in.
- They fight hard to maintain access in an environment when defenders find them. They don't just tuck their tail and leave.
- They often make mistakes by leaving S3 Browser defaults.
  - "`<YOUR-BUCKET-NAME>`" being a favorite, but also default policy and IAM user names




```
{
    "userName": "FileBackupAccount",
    "policyName": "dq",
   "policyDocument": "{\\r\\n \\"Statement\\": [\\r\\n {\\r\\n \\"Effect\\": \\"Allow\\"
}
```

Example request parameters from iam:PutUserPolicy event in CloudTrail logs

Mission

GUI-vil is a financially motivated threat actor, that leverages compromised credentials to spin up EC2 instances for use in crypto mining.

Tooling

GUI-vil leverages mostly GUI tools in their attacks. Initial access, reconnaissance, and persistence are all completed using the GUI utility S3 Browser. We have observed the threat actors continued use of the same version of S3 Browser (version 9.5.5, released January of 2021) to carry out their attacks since November 13, 2021. Once GUI-vil is able to create or take ownership of an IAM user with AWS Management Console access, they perform the rest of their activities directly through the web browser and AWS Management Console.

Hours of operations (UTC/GMT)

Infrastructure

All source addresses the attacker has originated from belong to two ASNs in Indonesia

- PT. Telekomunikasi Selula
- PT Telekomunikasi Indonesia

Victimology

GUI-vil is an equal opportunity attacker. Rather than targeting specific organizations, they are opportunistic and will attempt to attack any organization for which they can discover compromised credentials.

ATTACKER LIFECYCLE

In order to support their mechanisms for initial access, GUI-vil performs two (2) main forms of reconnaissance:

- Monitoring common public sources for exposed AWS access keys such as GitHub and Pastebin.
- Scanning for vulnerable versions of software repositories such as GitLab.

Initial Compromise & Establishing Foothold

We have observed this threat actor leverage two (2) methods of initial compromise:

- Leverage CVE-2021-22205 to gain Remote Code Execution (RCE) on vulnerable GitLab instances. Once GitLab is exploited the threat actor reviews repositories for AWS access keys.
- In most instances this threat actor is able to find publicly exposed credentials and directly leverage them.

The discovered access keys become their foothold into the AWS environment. They validate the access key and secret are active credentials by entering them into the Windows GUI utility S3 Browser, which will first execute the `ListBuckets` command against the `S3` service.


```
{

    "eventVersion": "1.08",
     "userIdentity": {
            "type": "IAMUser",
             "principalId": "redacted",
            "arn": "arn:aws:iam::redacted:user/external_audit",
            "accountId": "redacted",
            "accessKeyId": "AKIA******",
            "userName": "external_audit"
    },
     "eventTime": "2023-04-18T14:47:39.0000000Z",
     "eventSource": "s3.amazonaws.com",
     "eventName": "ListBuckets",
     "awsRegion": "us-east-1",
     "sourceIPAddress": "36.85.110.142",
     "userAgent": "[S3 Browser 9.5.5 https://s3browser.com]",
     "requestParameters": {
            "Host": "s3.us-east-1.amazonaws.com"
    },
     "responseElements": null,
     "requestID": "T1ACJXN3EJQ4T58X",
     "eventID": "af6814ab-10e1-4c8a-88b6-384874592519",
     "readOnly": true,
     "eventType": "AwsApiCall",
     "managementEvent": true,
     "recipientAccountId": "redacted",
     "eventCategory": "Management",
     "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.us-east-1.amazonaws.com"
    },
     "additionalEventData": {
            "SignatureVersion": "SigV4",
            "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "x-amz-id-2": "2ZRMAF9dvfjiLRZq1UoaE6tspOgoHk4X/Vtvjb8orWdQPGgJQiOuXhn13eOL3
            "bytesTransferredOut": 389
    }


    }
```


Escalate Privileges

Given that cloud credentials are often grossly over-privileged, this threat actor does not often need to elevate their privileges. In one attack by GUI-vil though, the credentials the threat actor started with had read-only permissions across all services. The attacker used these credentials to review data in all available S3 buckets, and was able to find credentials with full administrator privileges in a Terraform `tfstate` file.

Internal Recon

Services we have observed them exploring (in order of descending prevalence) include:

`ec2.amazonaws.com`
`health.amazonaws.com`
`iam.amazonaws.com`
`organizations.amazonaws.com`
`elasticloadbalancing.amazonaws.com`
`autoscaling.amazonaws.com`
`monitoring.amazonaws.com`
`cloudfront.amazonaws.com`
`billingconsole.amazonaws.com`
`s3.amazonaws.com`
`compute-optimizer.amazonaws.com`
`ce.amazonaws.com`
`dynamodb.amazonaws.com`
`config.amazonaws.com`
`ram.amazonaws.com`
`ssm.amazonaws.com`
`kms.amazonaws.com`
`securityhub.amazonaws.com`
`servicecatalog-appregistry.amazonaws.com`
`sts.amazonaws.com`
`cloudtrail.amazonaws.com`
`trustedadvisor.amazonaws.com`
`logs.amazonaws.com`
`dax.amazonaws.com`
`sso.amazonaws.com`
`support.amazonaws.com`
`account.amazonaws.com`
`elasticfilesystem.amazonaws.com`
`resource-groups.amazonaws.com`
`ds.amazonaws.com`
`tagging.amazonaws.com`
`cloudhsm.amazonaws.com`
`access-analyzer.amazonaws.com`
`resource-explorer-2.amazonaws.com`

Additionally, we observed GUI-vil monitoring CloudTrail logs for changes that the victims' organizations were making when trying to evict GUI-vil from their environments. This allowed GUI-vil to adapt their persistence to bypass restrictions the victim organization was putting in place.


```
{
	"eventVersion": "1.08",
	"userIdentity": {
		"type": "IAMUser",
		"principalId": "redacted",
		"arn": "arn:aws:iam::redacted:user/andy",
		"accountId": "redacted",
		"accessKeyId": "ASIA****",
		"userName": "andy",
		"sessionContext": {
			"sessionIssuer": {},
			"webIdFederationData": {},
			"attributes": {
				"creationDate": "2023-04-19T01:16:27.0000000Z",
				"mfaAuthenticated": "false"
			}
		}
	},
	"eventTime": "2023-04-19T01:21:14.0000000Z",
	"eventSource": "cloudtrail.amazonaws.com",
	"eventName": "LookupEvents",
	"awsRegion": "us-east-1",
	"sourceIPAddress": "36.85.110.142",
	"userAgent": "AWS Internal",
	"requestParameters": {
		"maxResults": 50,
		"lookupAttributes": [
			{
				"attributeKey": "ReadOnly",
				"attributeValue": "false"
			}
```

Maintain Presence (IAM)

In order to maintain a presence in the victim organization, GUI-vil has leveraged several different mechanisms. Based on observed activity, they exclusively utilize S3 Browser to make creations and modifications to the `IAM` service.

- GUI-vil will often create new IAM users to maintain ensure they can persist in an environment in case their original compromised credentials are discovered. When creating IAM users GUI-vil will often attempt to conform to the naming standards of existing IAM users. For example, in one environment they created a user named `sec_audit` which they modelled off of other audit users in the organization. They do often move too fast for their own good, sometimes forgetting to take out the default name that S3 Browser supplies when creating a new user.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
                "type": "IAMUser",
                "principalId": "redacted",
                "arn": "arn:aws:iam::redacted:user/terraform",
                "accountId": "redacted",
                "userName": "terraform",
                "accessKeyId": "AKIA*****"
        },
        "eventTime": "2023-04-18T15:05:27.0000000Z",
        "eventSource": "iam.amazonaws.com",
        "eventName": "CreateUser",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "36.85.110.142",
        "userAgent": "S3 Browser 9.5.5 <https://s3browser.com>",
        "requestParameters": {
                "userName": "sec_audit",
                "path": "/"
        },
        "responseElements": {
                "user": {
                        "arn": "arn:aws:iam::redacted:user/sec_audit",
                        "userName": "sec_audit",
                        "userId": "redacted",
                        "createDate": "Apr 18, 2023 3:05:27 PM",
                        "path": "/"
                }
}
```

- GUI-vil will create login profiles, to enable access to AWS Management Console. We have observed GUI-vil apply this tactic to avoid the noise of creating a new user. They look for identities that do not have login profiles and, once found, create a login profile. This allows the attacker to inherit the permissions of that identity and stay under the radar of security teams that do not monitor new login profiles being created.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
                "type": "IAMUser",
                "principalId": "redacted",
                "arn": "arn:aws:iam::redacted:user/terraform",
                "accountId": "redacted",
                "accessKeyId": "AKIA****",
                "userName": "terraform"
         },
         "eventTime": "2023-04-18T15:27:22.0000000Z",
         "eventSource": "iam.amazonaws.com",
         "eventName": "GetLoginProfile",
         "awsRegion": "us-east-1"
```

```
        "responseElements": null,
        "requestID": "33147b1e-f106-440e-b63a-f4fca8da0170",
        "eventID": "7d7ad4e4-3f50-42d1-af4f-6d7db737ecdb",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "redacted",
        "eventCategory": "Management",
        "tlsDetails": {
              "tlsVersion": "TLSv1.2",
              "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
              "clientProvidedHostHeader": "iam.amazonaws.com"
        },
         "errorCode": "NoSuchEntityException",
         "errorMessage": "Login Profile for User andy cannot be found."
}
{
         "eventVersion": "1.08",
         "userIdentity": {
              "type": "IAMUser",
              "principalId": "redacted",
              "arn": "arn:aws:iam::redacted:user/terraform",
              "accountId": "redacted",
              "accessKeyId": "AKIA****",
              "userName": "terraform"
          },
          "eventTime": "2023-04-18T15:27:29.0000000Z",
          "eventSource": "iam.amazonaws.com",
          "eventName": "CreateLoginProfile",
          "awsRegion": "us-east-1",
          "sourceIPAddress": "36.85.110.142",
          "userAgent": "S3 Browser 9.5.5 <https://s3browser.com>",
          "requestParameters": {
               "userName": "andy",
               "passwordResetRequired": false
          },
          "responseElements": {
               "loginProfile": {
                    "userName": "andy",
                    "createDate": "Apr 18, 2023 3:27:29 PM",
                    "passwordResetRequired": false
               }
        },
        "requestID": "281e395e-3614-44f6-8531-5bcdca3a5507",
        "eventID": "4ced3dd4-1ab7-4e23-b659-7ca7d88c5d6e",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "redacted",
        "eventCategory": "Management",
        "tlsDetails": {
              "tlsVersion": "TLSv1.2",
              "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
              "clientProvidedHostHeader": "iam.amazonaws.com"
        }
```


iam:GetLoginProfile with error showing that a login profile does not currently exist


```
{
        "eventVersion": "1.08",
        "userIdentity": {
                "type": "IAMUser",
                "principalId": "redacted",
                "arn": "arn:aws:iam::redacted:user/terraform",
                "accountId": "redacted",
                "accessKeyId": "AKIA****",
                "userName": "terraform"
        },
        "eventTime": "2023-04-18T15:27:29.0000000Z",
        "eventSource": "iam.amazonaws.com",
        "eventName": "CreateLoginProfile",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "36.85.110.142",
        "userAgent": "S3 Browser 9.5.5 https://s3browser.com",
        "requestParameters": {
```

```
                        "userName": "andy",
                        "createDate": "Apr 18, 2023 3:27:29 PM",
                        "passwordResetRequired": false
                }
        },
        "requestID": "281e395e-3614-44f6-8531-5bcdca3a5507",
        "eventID": "4ced3dd4-1ab7-4e23-b659-7ca7d88c5d6e",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "redacted",
        "eventCategory": "Management",
        "tlsDetails": {
                "tlsVersion": "TLSv1.2",
                "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
                "clientProvidedHostHeader": "iam.amazonaws.com"
        }
}
```


iam:CreateLoginProfile for the user that did not have a login profile already defined

When GUI-vil creates IAM users, they also directly attach an inline policy via `iam:PutUserPolicy` to grant their user full privileges.


```
{
        "userName": "backup",
        "policyName": "backupuser",
        "policyDocument": "{\\r\\n \\"Statement\\": [\\r\\n {\\r\\n \\"Effect\\": \\"Allo
}
```


iam:PutUserPolicy to add inline policy granting full privileges to newly created user

Maintain Presence (EC2)

While they can maintain presence on the infrastructure level via the users and access keys they have created or taken over, the attacker can also maintain persistence to the environment via EC2. Simply by being able to connect to the EC2 instance they can assume the credentials of the EC2 instance. Often times the attacker will execute `ec2:CreateKeyPair`, enabling them to connect to the EC2 instance directly via SSH which they ensure is open to the internet on any EC2 instances they create.


```
"data": {
        "eventVersion": "1.08",
        "userIdentity": {
                "type": "AssumedRole",
                "principalId": "AROA****:andy",
                "arn": "arn:aws:sts::redacted:assumed-role/AdminUser/andy",
                "accountId": "redacted",
                "accessKeyId": "ASIA*****",
                "sessionContext": {
                        "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA****",
                                "arn": "arn:aws:iam::redacted:role/AdminUser",
                                "accountId": "redacted",
                                "userName": "AdminUser"
                        },
                        "webIdFederationData": {},
                        "attributes": {
                                "creationDate": "2023-04-18T15:30:24.0000000Z",
                                "mfaAuthenticated": "false"
                        }
                }
        },
        "eventTime": "2023-04-18T15:33:12.0000000Z",
        "eventSource": "ec2.amazonaws.com",
        "eventName": "CreateKeyPair",
        "awsRegion": "us-east-1",
```

```
                "keyFormat": "ppk"
        },
        "responseElements": {
                "requestId": "21e1134f-109e-4b4a-bea8-cc651b9e0db8",
                "keyName": "su32",
                "keyFingerprint": "e9:86:03:1e:81:4e:65:fb:78:41:f0:32:e0:29:ff:6e:9b:0e:
                "keyPairId": "key-0123456789abcdef0",
                "keyMaterial": "<sensitiveDataRemoved>"
        },
        "requestID": "21e1134f-109e-4b4a-bea8-cc651b9e0db8",
        "eventID": "9338ea0b-b929-4a76-b024-2b3ea36cd484",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "redacted",
        "eventCategory": "Management",
        "sessionCredentialFromConsole": "true"
}
```


ec2:CreateKeyPair to create public and private key pair for remote access


```
{
        "groupId": "sg-0123456789abcdef0",
        "ipPermissions": {
                "items": [
                        {
                                "ipRanges": {
                                        "items": [
                                                {
                                                        "cidrIp": "0.0.0.0/0"
                                                }
                                        ]
                                },
                                "prefixListIds": {},
                                "fromPort": 22,
                                "toPort": 22,
                                "groups": {},
                                "ipProtocol": "tcp",
                                "ipv6Ranges": {}
                        }
                ]
        }
```


ec2:AuthorizeSecurityGroupIngress to add inbound (ingress) rule for port 22 to specified security group

Complete Mission

GUI-vil is financially motivated. They create EC2 instances in victim AWS organizations that they then use for crypto mining. Often times as they encounter resource limitations set by the victim organizations they will switch to other regions and attempt again.

All EC2 instances they created have had these attributes:

- Size xlarge and bigger (c4.4xlarge, p3.16xlarge, p3.2xlarge, p3.8xlarge)
- TCP/22 open to 0.0.0.0
- IPv4 Enabled, IPv6 Disabled
- Detailed CloudWatch monitoring disabled
- Xen hypervisor

Once an EC2 instance is created they connect to it via SSH, install required packages, then install and launch XMRIG:

- `apt-get update`
- `apt-get install git build-essential cmake libuv1-dev libssl-dev libhwloc-dev -y`
- `/home/ubuntu/xmrig`

Indicator	Type	Notes
182.1.229.252	IPv4	PT. Telekomunikasi Selular
114.125.247.101	IPv4	PT. Telekomunikasi Selula
114.125.245.53	IPv4	PT. Telekomunikasi Selula
114.125.247.101	IPv4	PT. Telekomunikasi Selula
114.125.232.189	IPv4	PT. Telekomunikasi Selula
114.125.228.81	IPv4	PT. Telekomunikasi Selula
114.125.229.197	IPv4	PT. Telekomunikasi Selula
114.125.246.235	IPv4	PT. Telekomunikasi Selula
114.125.246.43	IPv4	PT. Telekomunikasi Selula
36.85.110.142	IPv4	PT Telekomunikasi Indonesia
S3 Browser 9.5.5 https://s3browser.com/	UA	
[S3 Browser 9.5.5 https://s3browser.com/]	UA	
su32	SSH Key Name	
new-user-<8 alphanumeric characters>	IAM User	default naming standard for creating a user with S3 Browser
sec_audit	IAM User	
sdgs	IAM Policy	
ter	IAM Policy	
backup	IAM User	
dq	IAM Policy	

Detections

Permiso CDR Rules

Permiso clients are protected from these attackers by the following detections:

Permiso Detections
P0_AWS_S3_BROWSER_USERAGENT_1
P0_MULTI_NEFARIOUS_USERAGENT_1
P0_AWS_SUSPICIOUS_ACCOUNT_NAME_CREATED_1
P0_GENERAL_SUSPICIOUS_ACCOUNT_NAME_CREATED_1
P0_COMMON_USER_ACTIVITY_NO_MFA_1
P0_AWS_IAM_INLINE_POLICY_ALLOW_ALL_1
P0_AWS_IAM_INLINE_POLICY_SHORT_NAME_1
P0_AWS_IAM_INLINE_POLICY_PASSROLE_1
P0_AWS_IAM_INLINE_POLICY_TEMPLATE_LANGUAGE_1
P0_AWS_EC2_MULTI_REGION_INSTANCE_CREATIONS_1

For folks not on the Permiso platform, here are some basic sigma rules that can be used to identify GUI-vil:

S3 Browser - IAM Policy w/Templated Language

```
 title: AWS IAM S3Browser Templated S3 Bucket Policy Creation id: db014773-7375-4f4e-b83b
description: Detects S3 Browser utility creating Inline IAM Policy containing default S3
references:
 - <https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor> author: daniel.boh
date: 2023/05/17 modified: 2023/05/17 tags:
    - attack.execution
 - attack.t1059.009     - attack.persistence
 - attack.t1078.004 logsource:
    product: aws
    service: cloudtrail
detection:
    selection_source:
        eventSource: iam.amazonaws.com
        eventName: PutUserPolicy
    filter_tooling:
        userAgent|contains: 'S3 Browser'
    filter_policy_resource:
 requestParameters|contains: '"arn:aws:s3:::<YOUR-BUCKET-NAME>/*"'     filter_policy_acti
 requestParameters|contains: '"s3:GetObject"'     filter_policy_effect:
 requestParameters|contains: '"Allow"'     condition: selection_source and filter_tooling
falsepositives:
    - Valid usage of S3 Browser with accidental creation of default Inline IAM Policy wit
level: high
```

S3 Browser - IAM LoginProfile

```
 title: AWS IAM S3Browser LoginProfile Creation id: db014773-b1d3-46bd-ba26-133337c0ffee
description: Detects S3 Browser utility performing reconnaissance looking for existing IA
references:
 - <https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor> author: daniel.boh
date: 2023/05/17 modified: 2023/05/17 tags:
    - attack.execution
 - attack.t1059.009     - attack.persistence
 - attack.t1078.004 logsource:
    product: aws
    service: cloudtrail
detection:
    selection_source:
        eventSource: iam.amazonaws.com
        eventName:
            - GetLoginProfile
            - CreateLoginProfile
    filter_tooling:
        userAgent|contains: 'S3 Browser'
    condition: selection_source and filter_tooling
falsepositives:
    - Valid usage of S3 Browser for IAM LoginProfile listing and/or creation
level: high
```

S3 Browser - IAM User and AccessKey

```
 title: AWS IAM S3Browser User or AccessKey Creation id: db014773-d9d9-4792-91e5-133337c0
description: Detects S3 Browser utility creating IAM User or AccessKey.
references:
 - <https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor> author: daniel.boh
date: 2023/05/17 modified: 2023/05/17 tags:
    - attack.execution
 - attack.t1059.009     - attack.persistence
 - attack.t1078.004 logsource:
    product: aws
    service: cloudtrail
detection:
    selection_source:
        eventSource: iam.amazonaws.com
```

```
        condition: selection_source and filter_tooling
    falsepositives:
        - Valid usage of S3 Browser for IAM User and/or AccessKey creation
    level: high
```

Observed Events (write level):

`ec2:AuthorizeSecurityGroupIngress`
`ec2:CreateKeyPair`
`ec2:CreateSecurityGroup`
`ec2:CreateTags`
`ec2:RunInstances`
`ec2:TerminateInstances`
`iam:CreateAccessKey`
`iam:CreateLoginProfile`
`iam:CreateUser`
`iam:DeleteAccessKey`
`iam:DeleteLoginProfile`
`iam:DeleteUser`
`iam:DeleteUserPolicy`
`iam:PutUserPolicy`
`signin:ExitRole`
`signin:SwitchRole`

VIEW MORE POSTS →

PERMISO