

Identify and Analyze Cyber Threats

Malware Analysis

[Sample Link](#)

[Analysis Link](#)

22
/ 63
Community Score

22/63 security vendors flagged this file as malicious

76aad0a8f0aa57f8ced5ad25e0a3133000f93aa5fff45153e4730d048efe8

Size
898.99 KB

Last Analysis Date
10 hours ago

AG
ELF

Popular threat label trojan.prometei

Threat categories trojan

Family labels prometei

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Linux.Prometei.SE260	ALYac	Trojan.Linux.GenericKDZ.481
Antiy-AVL	Trojan[Backdoor]/Linux.Prometei.a	Arcabit	Trojan.Linux.Generic.481
Avast	ELF:Prometei-C [Trj]	Avast-Mobile	ELF:Prometei-B [Trj]
AVG	ELF:Prometei-C [Trj]	BitDefender	Trojan.Linux.GenericKDZ.481
CTX	Elf.trojan.generickdz	DrWeb	Linux.Siggen.8485
Emsisoft	Trojan.Linux.GenericKDZ.481 (B)	eScan	Trojan.Linux.GenericKDZ.481
ESET-NOD32	A Variant Of Linux/Prometei.B	Fortinet	Linux/Prometei.Bltr
GData	Trojan.Linux.GenericKDZ.481	Huorong	Trojan/Prometei.g
Jiangmin	Backdoor.Linux.jbew	Kaspersky	HEUR:Backdoor.Linux.Prometei.a
Microsoft	Trojan:Linux/Coinminer.B	Rising	Backdoor.Prometei/Linux!1.DBE7 (CLAS...
Trellix (HX)	Trojan.Linux.GenericKDZ.481	VIPRE	Trojan.Linux.GenericKDZ.481
Acronis (Static ML)	Undetected	AliCloud	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected
Cynet	Undetected	Elastic	Undetected
Google	Undetected	Gridinsoft (no cloud)	Undetected
Ikarus	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kingsoft	Undetected

Basic properties

MD5

99ba8fd508563a946e811d80be35002e

SHA-1

e3938ac112daa883ba5dc72a2fa114b1acb777fd2

SHA-256

76aad0a8f0affe57f8ced5ad25e0a3133000f93aa5fff45153e4730d048efe8

Vhash

b3a5fcdabefb53a724715687a591dob

SSDEEP

12288:qb14350q+8eXS1/f2Wc3sIC3yjTjMv+9XSJhBXEsV3b9gh4J8zMSv7MzOup8Mplb:qmShf4OTJmGXSJhBXEsVrmz9MOup1Khk

TLSH

T1441558653700EF5EF39DE27108F287E046D125F31AD24296A278C71C6EE161D28AFDE9

File type

ELF

executablelinuxelf

Magic

ELF 32-bit MSB executable, MIPS, MIPS32 rel2 version 1 (SYSV), statically linked, for GNU/Linux 3.2.0, BuildID[sha1]=bc565f9f2dafc5618defa8eccf705f85712c87da, stripped

TriD

ELF Executable and Linkable format (generic) (100%)

DetectItEasy

ELF32 | Operation system: Unix [EXEC MIPS-32] | Compiler: gcc ((Ubuntu 7.5.0-3ubuntu1-18.04) 7.5.0) [EXEC MIPS-32]

Magika

ELF

File size

898.99 KB (920568 bytes)

History

First Seen In The Wild

2025-01-20 15:01:32 UTC

First Submission

2025-01-20 14:44:45 UTC

Last Submission

2025-01-20 14:44:45 UTC

Last Analysis

2025-01-20 14:44:45 UTC

Contacted Domains (1)

Domain	Detections	Created	Registrar
p3.feefreepool.net	11 / 94	2017-05-10	Internet Domain Service BS Corp

Contacted IP addresses (2)

IP	Detections	Autonomous System	Country
8.8.8.8	0 / 94	15169	US
88.198.246.242	8 / 94	24940	DE

Graph Summary

Activity Summary

Download Artifacts

Full Reports

Help

Detections

NOT FOUND

Mitre Signatures

NOT FOUND

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

NOT FOUND

Network comms

1 DNS1 IP

Behavior Tags

detect-debug-environment

executes-dropped-file

persistence

Network Communication

DNS Resolutions

+ p3.feefreepool.net

IP Traffic

8.8.8.8:53

Behavior Similarity Hashes

ELF DIGEST

d49b1645e3e9c1d86e735afb9cb66948

Behavior Similarity Hashes ⊙	
ELF DIGEST	d49b1645e3e9c1d86e735afb9cb66948
File system actions ⊙	
Files Opened	
⊙	/etc/Commld
⊙	/etc/host.conf
⊙	/etc/ld.so.cache
⊙	/etc/nsswitch.conf
⊙	/etc/passwd
⊙	/etc/pcc0
⊙	/etc/pcc1
⊙	/etc/resolv.conf
⊙	/etc/uplugplay
⊙	/lib/libc.so.6
⋮	
Files Written	
⊙	/etc/Commld
⊙	/etc/hosts
⊙	/lib/systemd/system/uplugplay.service
⊙	/usr/sbin/uplugplay
⊙	task.cron
Files Deleted	
⊙	task.cron
Process and service actions ⊙	
Shell Commands	
⊙	/bin/pidof, [pidof, analyzed_bin]
⊙	/bin/pidof, [pidof, uplugplay]
⊙	/bin/pidof, [pidof, upnpsetup]
⊙	/usr/bin/crontab, [crontab, -l]
⊙	/usr/bin/crontab, [crontab, task.cron]
⊙	/usr/bin/nslookup, [nslookup, p3.feefreepool.net, 8.8.8.8]
⊙	/usr/sbin/uplugplay, [/usr/sbin/uplugplay, -Dcomsvc]
⊙	0x4b6954, [0x4b6950, 0x4b694c, 0x4b708c]
⊙	0x4b6954, [0x4b6950, 0x4b694c, crontab task.cron]
⊙	0x4b6954, [0x4b6950, 0x4b694c, nslookup p3.feefreepool.net 8.8.8.8]

Detection Rate: 34% (22 out of 63 vendors have identified this)

Malware Family: Trojan

File Information: ELF, exe

Network Indicators: p3.feefreepool.net

IP Traffic: 8.8.8.8:53

Behavior Indicators/ Indicators of Compromise: Detects debug environments; executes dropped files; persistence

System Impact/ Potential Damage Assessment: Opens, writes, and delete files;

Unleashes a series of commands;

Phishing Template Creation

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

`set> 1`

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules

99) Return back to the main menu.

`set> 2`

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

`set:webattack>3`

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

`set:webattack>1`

1. Java Required
2. Google
3. Twitter

`set:webattack> Select a template: 2`

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: clear
```

```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...
```

```
10.0.2.15 - - [20/Jan/2025 20:29:09] "GET / HTTP/1.1" 200 -
```

```
[*] WE GOT A HIT! Printing the output:
```

PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hI
cDhtUFdlldzBENhIfVwsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAAA
AAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX

```
PARAM: service=ls
```

PARAM: dsh=-7381887106725792428

```
PARAM: _utf8=â
```

```
PARAM: _utis-a
PARAM: bgresponse=js_disabled
```

```
PARAM: pgResponse=js_disabled
PARAM: pstMsg=1
```

```
PARAM: p5Conn=1
PARAM: dnConn=
```

```
PARAM: unConn=
PARAM: checkConnection=
```

```
PARAM: checkedDomains=youtube
```

```
PARAM: PersistentCookie=yes
```

Potential Impact:

- Credential leaks
- Changed passwords/credentials
- Loss of access
- Fraud/ Unauthorized use

Prevention Methods:

- 2FA/ MFA
- Log-in attempts emailed
- Changing passwords frequently
- Use password manager

APT Campaign Analysis

APT28

Campaign Overview

Name: APT28 (Fancy Bear)

Target: Europe, United States, Nato allies

Industry Focus: Government, military, media
Active Date: Minimum since 2007
Primary Goals: Espionage, influence operations, data exfiltration
Tools: X-Agent, Sofacy, Zebrocy, Mimikatz

MITRE ATT&CK Mapping

Initial Access

T1190 - Exploit Public-Facing Application

Exploited vulnerabilities in web applications to gain initial access, such as using vulnerabilities in Microsoft Exchange or web servers

T1566.001 - Spear Phishing Attachment

Delivered malicious email attachments to target individuals as part of phishing campaigns.

Execution Method

T1203 - Exploitation for Client Execution

Leveraged vulnerabilities in Microsoft Office documents with macros or embedded scripts to execute payloads

T1059.003 - Command and Scripting Interpreter: Windows Command Shell

Utilized Windows commands for initial payload execution and post-compromise activity

Persistence Mechanisms

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder

Modifies registry keys to maintain persistence on compromised systems

T1053.005 - Scheduled Task/Job

Used scheduled tasks to execute malware at regular intervals

Command and Control

T1068 - Exploitation for Privilege Escalation

Exploited known vulnerabilities to escalate privileges on target systems, such as CVE-2017-0263

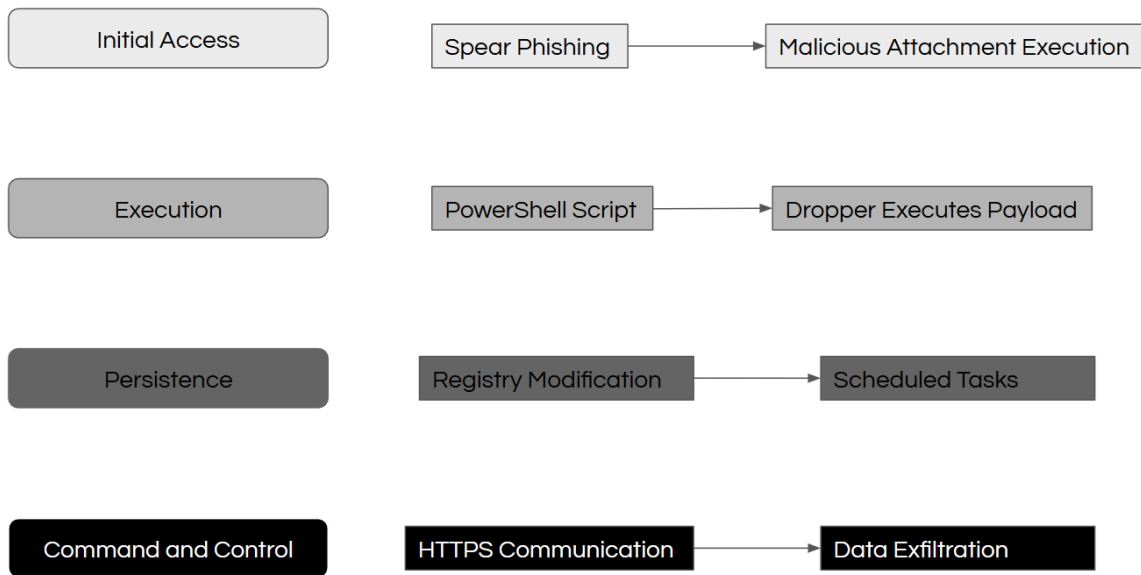
T1027 - Obfuscated Files or Information

Used obfuscation techniques in scripts and malware to evade detection

T1070.004 - Indicator Removal on Host: File Deletion

Deleted artifacts from infected systems to avoid forensic analysis

Attack Flow Diagram



Impact Analysis

Operational Impact

- Disruption of government communications.
- Theft of classified data.

Reputational Impact

- Compromised trust in targeted organizations.

Economic Impact

- Cost of incident response and remediation.

Geopolitical Impact

- Influence on elections and political decisions.

Apply Vulnerability Assessment Techniques

Part 1: Asset Discovery Scan

Initial Network Mapping

ifconfig

sudo nmap -sn [target ip]

```
(test@test)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.8.105 netmask 255.255.255.0 broadcast 192.168.8.255
    inet6 fe80::a00:27ff:fe5d:d4d7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:5d:d4:d7 txqueuelen 1000 (Ethernet)
    RX packets 954 bytes 59579 (58.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1515 bytes 93602 (91.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(test@test)-[~]
$ sudo nmap -sn 192.168.8.105/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 18:45 EST
```

```
Nmap scan report for Pixel-6.lan (192.168.8.133)
Host is up (0.18s latency).
```

```
Nmap scan report for console.gl-inet.com (192.168.8.1)
Host is up (0.0019s latency).
```

```
Nmap scan report for test.lan (192.168.8.105)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.71 seconds
```

Number of Responsive Hosts: 3

Found IP Addresses:

- 192.168.8.133
- 192.168.8.1
- 192.168.8.105 (VM)

Host Names:

- console.gl-inet.com
- Pixel-6.
- test (VM)

Service Enumeration

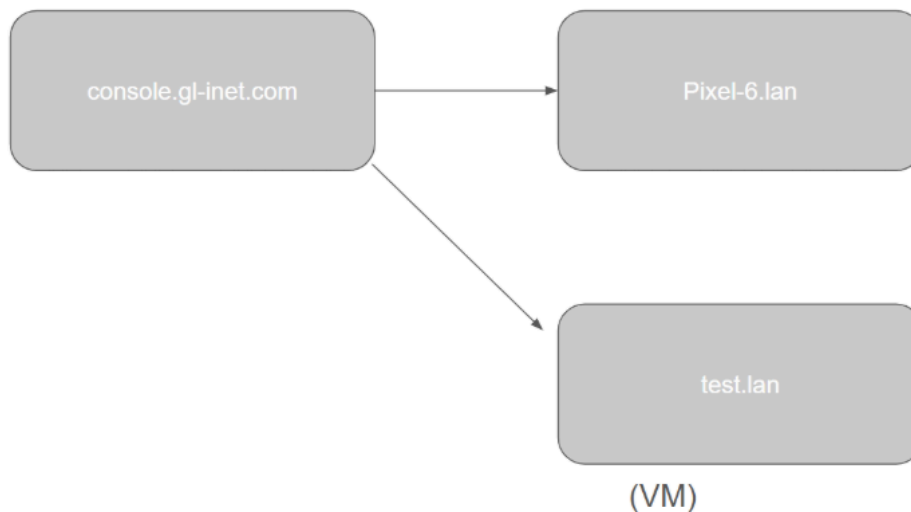
(Only will scan the host "Pixel-6" for this portion; "console.gl-inet.com" is a network router; "test" is the VM itself)
sudo nmap -sV -p- [discovered_host_ip]

Pixel 6

```
(test@test)-[~]  
$ nmap -sV -p- 192.168.8.133  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 19:00 EST  
Nmap scan report for Pixel-6.lan (192.168.8.133)  
Host is up (0.013s latency).  
All 65535 scanned ports on Pixel-6.lan (192.168.8.133) are in ignored states.  
Not shown: 65535 closed tcp ports (reset)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 23.54 seconds
```

Open Ports: No open ports exist
Running Services: Cannot be found
Service Version: Cannot be found

Network Map



Critical Assets: Pixel 6, VM, Router
Initial Risk Assessment:
Low, all IPs listed start with 192.168 which is only for internal use within networks.
Therefore, attackers can not easily intrude into systems.

Part 2: Vulnerability Scan

Perform Vulnerability Scan:

sudo nmap -sV --script vuln [target_ip]

```
[test@test]~$ sudo nmap -sV --script vuln 192.168.8.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 20:53 EST
Stats: 0:01:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.68% done; ETC: 20:55 (0:00:01 remaining)
Debugging Increased to 1.
NSE: Finished http-slowloris-check against 192.168.8.1:443. Reason: EOF
NSE: Finished http-slowloris-check against 192.168.8.1:80. Reason: EOF
NSE: Finished http-slowloris-check against 192.168.8.1:443. Reason: EOF
NSE: [http-slowloris-check 192.168.8.1:443] Time difference is: -2
NSE: Finished http-slowloris-check against 192.168.8.1:443.
NSE: Finished http-slowloris-check against 192.168.8.1:80. Reason: EOF
NSE: [http-slowloris-check 192.168.8.1:80] Time difference is: 2
NSE: Finished http-slowloris-check against 192.168.8.1:80.
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 1 (0 waiting)
NSE Timing: About 99.81% done; ETC: 20:55 (0:00:00 remaining)
NSE: Script http-enum: 1 threads running, 0 threads waiting
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE: Active NSE Script Threads: 1 (0 waiting)
NSE Timing: About 99.81% done; ETC: 20:55 (0:00:00 remaining)
NSE: Script http-enum: 1 threads running, 0 threads waiting
NSE: [http-enum 192.168.8.1:80] HTTP pipeline: Number of received responses: 2203
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (//)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/mj_wwwusr)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/vcs)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/ffileman.cgi?)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/ck/mimencode)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/masterG1?)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/awstats.pl)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (//)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (//)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (/sdk/../../../../../../../../etc/vmware/hostd/vmInventory.xml)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (/sdk/%2EX2E/%2EX2E/%2EX2E/%2EX2E/%2EX2E/etc/vmware/hostd/vmInventory.xml)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (/../../../../../../../../etc/passwd)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (/../../../../../../../../boot.ini)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (..%2f..%2f..%2f..%2f..%2f/var/mobile/Library/AddressBook/AddressBook.sqitedb)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/export_debug_msg.exp)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/config.exp)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (//)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (?feed-rss)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (?feed-rss2)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (?feed-atom)
```

```
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (?feed=rss2)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (400 Bad Request) (?feed=atom)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (/)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (/)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (/)
NSE: [http-enum 192.168.8.1:80] HTTP: Page was '200 OK', it exists! (/)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/cgi-bin/)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/i18n/)
NSE: [http-enum 192.168.8.1:80] HTTP: Page didn't match the 404 response (403 Forbidden) (/js/)
NSE: Finished http-enum against 192.168.8.1:80.
NSE: Starting runlevel 2 (of 2) scan.
NSE: [ssl-cert-intaddr 192.168.8.1:22] 192.168.8.1 is a private address - skipping.
NSE: Starting http-cookie-flags against 192.168.8.1:80.
NSE: [http-cookie-flags 192.168.8.1:80] start check of /
NSE: [http-cookie-flags 192.168.8.1:80] end check of / : 0 issues found
NSE: Finished http-cookie-flags against 192.168.8.1:80.
NSE: Starting ssl-known-key against 192.168.8.1:443.
NSE: Finished ssl-known-key against 192.168.8.1:443.
NSE: Starting ssl-ccs-injection against 192.168.8.1:443.
NSE: Starting http-cookie-flags against 192.168.8.1:443.
NSE: [http-cookie-flags 192.168.8.1:443] start check of /
NSE: [http-cookie-flags 192.168.8.1:443] end check of / : 0 issues found
NSE: Finished http-cookie-flags against 192.168.8.1:443.
NSE: Starting http-server-header against 192.168.8.1:443.
NSE: Starting tls-ticketbleed against 192.168.8.1:443.
NSE: Starting ssl-dh-params against 192.168.8.1:443.
NSE: Starting ssl-poodle against 192.168.8.1:443.
NSE: Starting http-server-header against 192.168.8.1:80.
NSE: [ssl-cert-intaddr 192.168.8.1:80] 192.168.8.1 is a private address - skipping.
NSE: [ssl-cert-intaddr 192.168.8.1:53] 192.168.8.1 is a private address - skipping.
NSE: Starting ssl-heartbleed against 192.168.8.1:443.
NSE: [ssl-cert-intaddr 192.168.8.1:443] 192.168.8.1 is a private address - skipping.
NSE: [ssl-ccs-injection 192.168.8.1:443] Handshake completed (TLSv1.2)
NSE: Finished ssl-ccs-injection against 192.168.8.1:443.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured certificate record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_key_exchange record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello_done record.
NSE: [tls-ticketbleed 192.168.8.1:443] Unknown message type: change_cipher_spec
NSE: [tls-ticketbleed 192.168.8.1:443] Server did not send a NewSessionTicket record.
NSE: Finished http-server-header against 192.168.8.1:443.
NSE: [ssl-heartbleed 192.168.8.1:443] we're done!
NSE: [ssl-heartbleed 192.168.8.1:443] Server does not support TLS Heartbeat Requests.
NSE: Finished http-server-header against 192.168.8.1:80.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured certificate record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_key_exchange record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello_done record.
NSE: [tls-ticketbleed 192.168.8.1:443] Unknown message type: change_cipher_spec
NSE: [tls-ticketbleed 192.168.8.1:443] Server did not send a NewSessionTicket record.
NSE: [ssl-heartbleed 192.168.8.1:443] we're done!
NSE: [ssl-heartbleed 192.168.8.1:443] Server does not support TLS Heartbeat Requests.
NSE: [ssl-heartbleed 192.168.8.1:443] we're done!
NSE: [ssl-heartbleed 192.168.8.1:443] Server does not support TLS Heartbeat Requests.
NSE: Finished ssl-heartbleed against 192.168.8.1:443.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured certificate record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_key_exchange record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello_done record.
NSE: [tls-ticketbleed 192.168.8.1:443] Unknown message type: change_cipher_spec
```

```

NSE: [tls-ticketbleed 192.168.8.1:443] Server did not send a NewSessionTicket record.
NSE: [ssl-heartbleed 192.168.8.1:443] we're done!
NSE: [ssl-heartbleed 192.168.8.1:443] Server does not support TLS Heartbeat Requests.
NSE: [ssl-heartbleed 192.168.8.1:443] we're done!
NSE: [ssl-heartbleed 192.168.8.1:443] Server does not support TLS Heartbeat Requests.
NSE: Finished ssl-heartbleed against 192.168.8.1:443.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured certificate record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_key_exchange record.
NSE: [tls-ticketbleed 192.168.8.1:443] Captured server_hello_done record.
NSE: [tls-ticketbleed 192.168.8.1:443] Unknown message type: change_cipher_spec
NSE: [tls-ticketbleed 192.168.8.1:443] Server did not send a NewSessionTicket record.
NSE: Finished tls-ticketbleed against 192.168.8.1:443.
NSE: Finished ssl-poodle against 192.168.8.1:443.
NSE: Finished ssl-dh-params against 192.168.8.1:443.
Nmap scan report for console.gl-inet.com (192.168.8.1)
Host is up (0.0037s latency).
Scanned at 2025-01-21 20:53:26 EST for 154s
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Dropbear sshd (protocol 2.0)
53/tcp    open  domain       Cloudflare public DNS
80/tcp    open  http         nginx 1.17.7
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_vulners:
|_  nginx 1.17.7:
|_    DF1BBD4-8715-5ABE-985E-91DD3BB87773  7.8  https://vulners.com/githubexploit/DF1BBD4-8715-5ABE-985E-91DD3BB87773  *EXPLOIT*
|_    676D4F16-4FB3-11ED-A374-8C164567CA3C  7.8  https://vulners.com/freebsd/676D4F16-4FB3-11ED-A374-8C164567CA3C
|_    ADDC71B8-6024-11EF-86A1-8C164567CA3C  5.7  https://vulners.com/freebsd/ADDC71B8-6024-11EF-86A1-8C164567CA3C
443/tcp    open  ssl/http     nginx 1.17.7
|_http-server-header: nginx/1.17.7
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2011-3192:
|_  VULNERABLE:
|_    Apache byterange filter DoS
|_    State: VULNERABLE
|_    IDs: CVE:CVE-2011-3192 BID:49303
|_    The Apache web server is vulnerable to a denial of service attack when numerous
|_    overlapping byte ranges are requested.
|_    Disclosure date: 2011-08-19
|_    References:
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_      https://seclists.org/fulldisclosure/2011/Aug/175
|_      https://www.securityfocus.com/bid/49303
|_      https://www.tenable.com/plugins/nessus/55976
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_vulners:
|_  nginx 1.17.7:
|_    DF1BBD4-8715-5ABE-985E-91DD3BB87773  7.8  https://vulners.com/githubexploit/DF1BBD4-8715-5ABE-985E-91DD3BB87773  *EXPLOIT*
|_    676D4F16-4FB3-11ED-A374-8C164567CA3C  7.8  https://vulners.com/freebsd/676D4F16-4FB3-11ED-A374-8C164567CA3C
|_    ADDC71B8-6024-11EF-86A1-8C164567CA3C  5.7  https://vulners.com/freebsd/ADDC71B8-6024-11EF-86A1-8C164567CA3C

```

sudo nmap -p80,443 --script "http-* and not http-brute*" [target_ip]

```
(test@test)-[~]
$ sudo nmap -p80,443 --script "http-brute" 192.168.8.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 21:21 EST
Nmap scan report for console.gl-inet.com (192.168.8.1)
Host is up (0.0026s latency).
```

```
PORT      STATE SERVICE
80/tcp    open  http
| http-brute:
|_ Path "/" does not require authentication
443/tcp    open  https
| http-brute:
|_ Path "/" does not require authentication
```

```
(test@test)-[~]
$ sudo nmap -p445 --script "smb-vuln*" 192.168.8.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 21:23 EST
Nmap scan report for console.gl-inet.com (192.168.8.1)
Host is up (0.0029s latency).
```

```
PORT      STATE SERVICE
445/tcp    closed microsoft-ds
```

```
(test@test)-[~]
$ nmap -p80,443 --script "http-* and not http-brute*" 192.168.8.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 06:07 EST
Pre-scan script results:
|_ http-robtext-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtext.com/api/
Nmap scan report for Pixel-6.lan (192.168.8.133)
Host is up (0.20s latency).
```

```
PORT      STATE SERVICE
80/tcp    filtered http
443/tcp    filtered https
MAC Address: C2:E6:ED:AD:48:3B (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

sudo nmap -p445 --script "smb-vuln*" [target_ip]

```
(test@test)-[~]
$ sudo nmap -p445 --script "smb-vuln*" 192.168.8.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 06:08 EST
Nmap scan report for test.lan (192.168.8.105)
Host is up (0.000026s latency).
```

```
PORT      STATE SERVICE
445/tcp    closed microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

```
(test@test)-[~]
$ sudo nmap -p445 --script "smb-vuln*" 192.168.8.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 06:09 EST
Nmap scan report for Pixel-6.lan (192.168.8.133)
Host is up (0.076s latency).
```

```
PORT      STATE SERVICE
445/tcp    closed microsoft-ds
```

6 Vulnerabilities found on this network...

```

vulners:
  nginx 1.17.7:
    DF18BDC4-B715-5ABE-985E-91DD3BB87773 7.8 https://vulners.com/githubexploit/DF18BDC4-B715-5ABE-985E-91DD3BB87773 *EXPLOIT*
    676D4F16-4FB3-11ED-A374-8C164567CA3C 7.8 https://vulners.com/freebsd/676D4F16-4FB3-11ED-A374-8C164567CA3C
    ADDC71B8-6024-11EF-86A1-8C164567CA3C 5.7 https://vulners.com/freebsd/ADDC71B8-6024-11EF-86A1-8C164567CA3C

http-csrf: Couldn't find any CSRF vulnerabilities.
vulners:
  nginx 1.17.7:
    DF18BDC4-B715-5ABE-985E-91DD3BB87773 7.8 https://vulners.com/githubexploit/DF18BDC4-B715-5ABE-985E-91DD3BB87773 *EXPLOIT*
    676D4F16-4FB3-11ED-A374-8C164567CA3C 7.8 https://vulners.com/freebsd/676D4F16-4FB3-11ED-A374-8C164567CA3C
    ADDC71B8-6024-11EF-86A1-8C164567CA3C 5.7 https://vulners.com/freebsd/ADDC71B8-6024-11EF-86A1-8C164567CA3C

```

Overall Risk Assessment: Very high, 6 different vulnerabilities found with 2 of them ready to be executed

Methodology:

Tools used: Kali Linux, Nmap

Scan Configurations: Ping Scan (-sn), Version Detection Scan (-sV -p-), Vulnerability Script (-sV --script vuln), HTTP Script (-p80,443 --script "http-* and not http-brute*"), SMB Vulnerability Scan (-p445 --script "smb-vuln*")

Assessment Approach: Brute Force

Findings

Assets Discovered: Pixel Phone, Router, VM

Vulnerabilities: None seen

Risk Assessment:

Extremely high, has several controller issues.

Remedy: Exploit for Out-of-bounds Write in F5 Nginx

Patch and Update

- Check if your version of the F5 Nginx Ingress Controller is affected. Refer to the vendor's advisory or changelog.
- Update to the latest, patched version as recommended by F5 Networks. Always ensure your software is up to date.

2. Configuration Hardening

- Review and validate your ingress configurations to prevent potential exploitation.
- Limit resource allocations and permissions for Nginx processes to mitigate the impact of a potential compromise.

3. Network Segmentation

- Isolate the Ingress Controller from untrusted networks using network policies or firewalls.
- Only expose required services and endpoints to external users.

4. Apply WAF Rules

- Use a Web Application Firewall (WAF) to detect and block malicious payloads targeting this vulnerability.
- Configure custom rules to monitor for exploitation attempts specific to CVE-2022-41741.