MALWARE

Resurgence of the Prometei Botnet

6 min read

RELATED PRODUCTS

- Advanced DNS Security
- Advanced Threat Prevention
- Advanced URL Filtering
- Advanced WildFire
- Cloud-Delivered Security Services
- Cortex
- Cortex XDR
- Cortex XSIAM
- Unit 42 Incident Response

By: Lee Wei Yeong , Pranay Kumar Chhaparwal

Published: June 20, 2025

Categories: Cybercrime , Malware , Threat Research

Tags: Botnet , Cryptominers , Linux , Monero

Share

Table of Contents

the following activities:

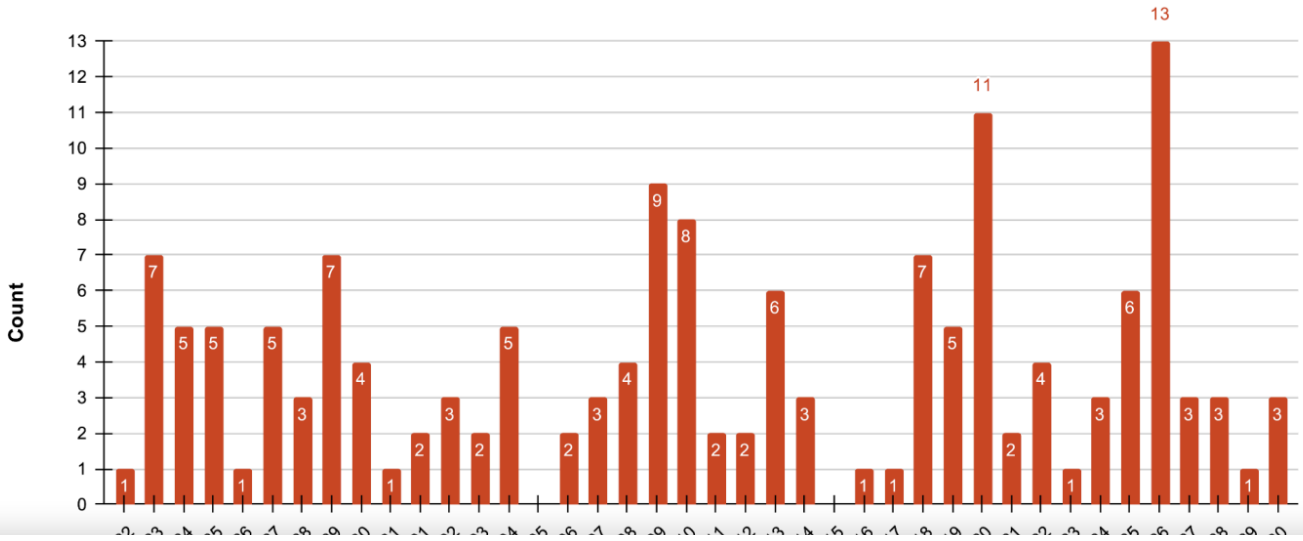
- Brute-forcing administrator credentials
- Exploiting vulnerabilities
- Mining cryptocurrency
- Stealing data
- Communicating with C2 servers

This modular design makes Prometei highly adaptable, as individual components can be updated or replaced without affecting the overall botnet functionality. It operates in multiple stages in the order listed below, which typically include the following:

- Initial Exploitation
- Payload Delivery
- Lateral Movement
- Cryptocurrency Mining
- Data Stealing
- C2 Communication

New Activity Timeline

We have been tracking this new wave of Prometei activity since March 2025. Figure 1 presents a timeline depicting the sample count of the Prometei botnet from late March-late April 2025.



Technical Analysis

The Prometei botnet malware is distributed via an HTTP GET request to `hxxp[://]103.41.204[.]104/k.php?a=x86_64`.

A slight variation, `hxxp[://]103.41.204[.]104/k.php?a=x86_64,<PARENT_ID>` returns the malware sample with an extra `ParentID` field value populated with the `<PARENT_ID>` value. This allows the attacker to dynamically assign a `ParentID` value to the malware sample. Here, `<PARENT_ID>` is used as a placeholder.

This URL is not restricted by geographic location; it serves the same malware sample file, with a randomized configuration each time. The HTTP response headers indicate that this server is an Apache PHP server running on a Windows platform. The server IPv4 address belongs to the network operated by Infinys Network (Autonomous System Number (ASN): 58397), based in Jakarta, Indonesia.

Later versions of this malware released in March 2025 are packed using Ultimate Packer for eXecutables (UPX). Version two, which was released in 2021, did not use this technique.

UPX is used to compress the executable, making it smaller and potentially more difficult to analyze. The malware itself is a 64-bit executable and linkable format (ELF) file, indicating it's designed to run on Linux-based systems.

Despite the file being named `k.php`, it is not a PHP script, likely a tactic to further disguise its true nature. In version two, malware authors named the corresponding file `uplugplay`.

The UPX-packed executable infects compromised systems by decompressing itself in memory during runtime. After decompression, the actual malicious payload is executed, allowing the botnet to begin its operations.

Unpacking Prometei for Static Analysis

Static malware analysis is a process of examining a malware sample without running or executing the file. In this case, because of the way this file is structured, we need to perform some extra operations to unpack this file for analysis. Attempting to use the standard UPX tool's decompression command-line option (i.e., `upx -d`) to restore the original file for further analysis will not successfully unpack it.

The UPX tool will fail because it relies on specific metadata, including a valid `PackHeader` and `overlay_offset` trailer, to identify and decompress UPX-packed files as shown in Figure 2. The presence of a custom configuration JSON trailer appended to the malware disrupts this process, causing the UPX tool to incorrectly determine that the file is not a valid UPX archive.

55 50 58 21: magic constant

0E: version

16: format

08: method

07: level

B8 8F 14 BF: uncompressed Adler-32 checksum

4B 74 01 2A: compressed Adler-32 checksum

F0 08 13 00: uncompressed length

C4 A6 06 00: compressed length

F0 08 13 00: original file size

49: `filter id`

22: `filter_cto`

00: `filter_misc/n_mru`

4B: **`header checksum`**

F4 00 00 00: **`overlay_offset`**

The configuration JSON trailer must be stripped before using the UPX tool to unpack the sample file for analysis. After unpacking, the configuration JSON must be re-attached to the sample file for the malware to use those values during execution.

The sample contains a subroutine to search for and parse the configuration JSON trailer. Table 1 below compares the supported fields in versions two, three and four.

	Version 2	Versions 3 and 4

Fields	`config`
	`id`
	`enckey`
		`config`
		`id`
		`enckey`
		`ParentId`
		`ParentHostname`

Table 3. Comparison of supported fields in the configuration JSON trailer between version two, and versions three and four.

The sample also contains another subroutine responsible for collecting compromised system information. This information includes:

- Processor information (obtained from `/proc/cpuinfo`)
- Motherboard information (obtained using the `dmidecode --type baseboard` command)
- Operating system information (obtained from `/etc/os-release` or `/etc/redhat-release`)
- Information about how long the system has been running (obtained using the `uptime` command)
- Kernel information (obtained using the `uname -a` command)

The collected system information is submitted via HTTP GET to the C2 server at `hxxp://152.36.128[.]18/cgi-bin/p.cgi`.

For a more comprehensive understanding of the Prometei botnet and its evolution you can read the 2021 article IoT Malware Journals: Prometei (Linux). This more recent article, Communication with a Prometei C2, provides a detailed analysis of its newer capabilities.

Conclusion

This research has detailed the resurgence of the Prometei botnet, highlighting its continued evolution and the techniques it employs to evade detection. The new version of the Prometei botnet malware family can be detected with a YARA rule that identifies UPX and the configuration JSON trailer, a detection method that is likely to remain effective. However, as Prometei continues to evolve, security teams must remain vigilant and proactively adapt their defenses.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the IoCs shared in this research.
- Advanced Threat Prevention has an inbuilt machine learning-based detection that can detect exploits in real time.
- Cortex XDR and XSIAM are designed to prevent the execution of known malicious malware, and also prevent the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.
- Advanced URL Filtering and Advanced DNS Security identify known domains and URLs associated with this activity as malicious.

Europe and Middle East: +31.20.299.3130

Asia: +65.6983.8730

Japan: +81.50.1790.0200

Australia: +61.2.4062.7950

India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Malware samples

Version	SHA-256 Hash
v2.87X	46cf75d7440c30cbfd101dd396bb18dc3ea0b9fe475eb80c4545868aab5c578c
v3.05L	cc7ab872ed9c25d4346b4c58c5ef8ea48c2d7b256f20fe2f0912572208df5c1a
v4.02V	205c2a562bb393a13265c8300f5f7e46d3a1aabe057cb0b53d8df92958500867
v4.02V	656fa59c4acf841dcc3db2e91c1088daa72f99b468d035ff79d31a8f47d320ef
v4.02V	67279be56080b958b04a0f220c6244ea4725f34aa58cf46e5161cfa0af0a3fb0
v4.02V	7a027fae1d7460fc5fccaf8bed95e9b28167023efcbb410f638c5416c6af53ff
v4.02V	87f5e41cbc5a7b3f2862fed3f9458cd083979dfce45877643ef68f4c2c48777e
v4.02V	b1d893c8a65094349f9033773a845137e9a1b4fa9b1f57bdb57755a2a2dcb708
v4.02V	d21c878dcc169961bebda6e7712b46adf5ec3818cc9469debf1534ffa8d74fb7
v4.08V	d4566c778c2c35e6162a8e65bb297c3522dd481946b81baffc15bb7d7a4fe531

URLs

Purpose	URL

Additional Resources

Reversing a Prometei botnet binary with r2 and AI - Axelle Apvrille, Fortinet

IoT Malware Journals: Prometei (Linux) - CUJO AI

Prometei botnet and its quest for Monero - Cisco Talos

Back to top

TAGS

Botnet | Cryptominers | Linux | Monero

Threat Research Center

Next: Exploring a New KimJongRAT Stealer Variant and Its PowerShell Implementation

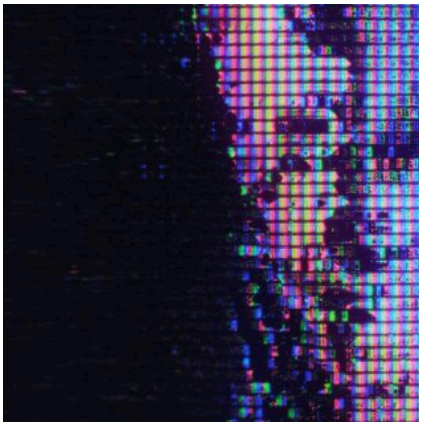
Related Resources

THREAT RESEARCH

June 17, 2025

Exploring a New KimJongRAT Stealer Variant and Its PowerShell Implementation

PowerShell | Infostealer | Backdoor



THREAT RESEARCH

June 12, 2025

JSFireTruck: Exploring Mal Obfuscation Technique

Malvertising | JavaScript

Newsletter

Get updates from Unit 42

Peace of mind comes from staying ahead of threats. Subscribe today.

Your Email

Subscribe for email updates to all Unit 42 threat research.
By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.

Subscribe 

Products and Services

Company

Popular Links

Privacy

Trust Center

Terms of Use

Documents

EN