Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

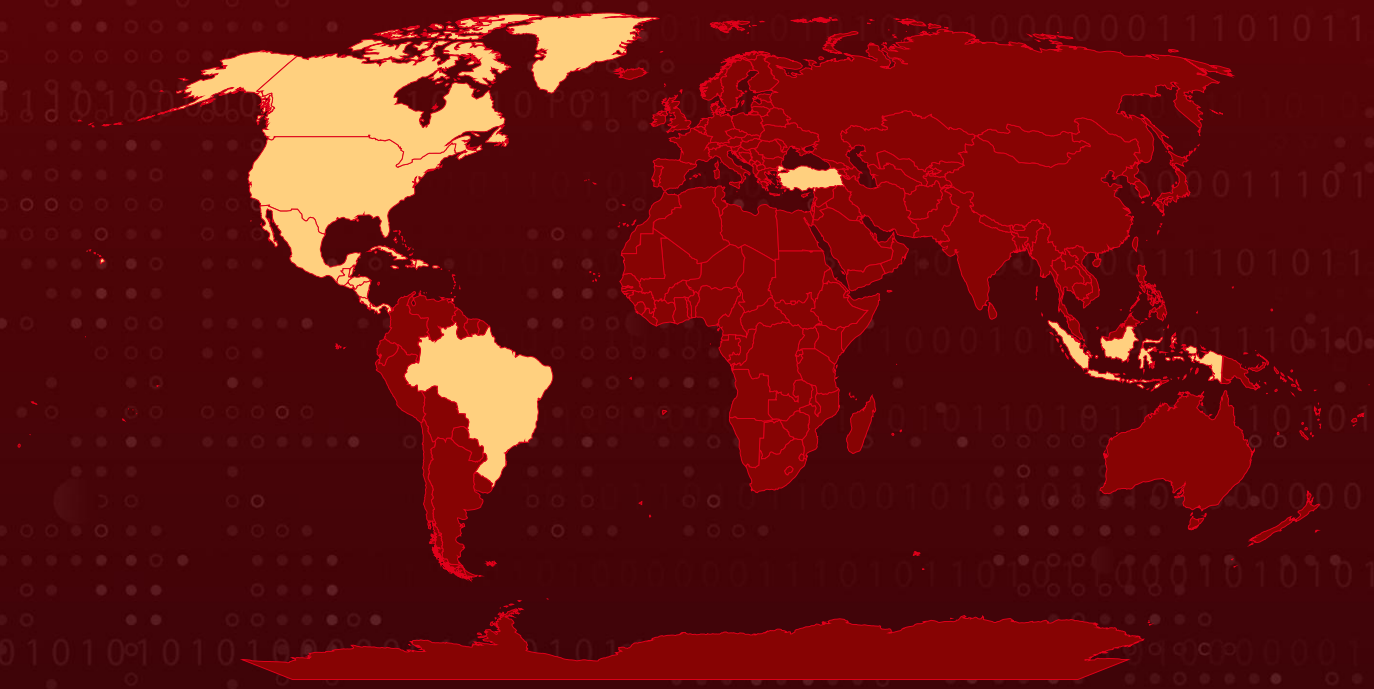
Prometei Botnet's Persistent Playbook

Date of Publication	Last Update Date	Admiralty Code	TA Number
March 15, 2023	June 24, 2025	A1	TA2023137

Summary

Active Since: 2016
Malware: Prometei botnet
Attack Regions: North America, Brazil, Indonesia, and Turkey
Targeted Sector: Cryptocurrency
Affected Platforms: Windows and Linux
Attack: By early 2023, the Prometei v3 botnet, an upgraded version of the Prometei botnet malware, had compromised over 10,000 systems mining the Monero cryptocurrency. In its latest iteration, identified in March 2025, Prometei stepped up with new Linux-specific variants.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-27065	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-26858	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2017-0144	EternalBlue (Microsoft SMBv1 Remote Code Execution Vulnerability)	Microsoft SMBv1	✓	✓	✓
CVE-2019-0708	BlueKeep (Microsoft Remote Desktop Services Remote Code Execution Vulnerability)	Windows: 10 - 11 23H2, Windows Server: 2019 – 2022 23H2	✗	✓	✓

Attack Details

#1

Since November 2022, more than 10,000 systems have been infected by the Prometei v3 botnet, an improved version of botnet malware. The Prometei botnet, a highly modular botnet with worm-like capabilities that predominantly installs the Monero cryptocurrency miner, has been regularly upgraded and updated since its discovery in 2016, providing a chronic threat to corporates.

#2

After successfully establishing a foothold using techniques such as brute-forcing credentials and leveraging vulnerabilities, a PowerShell operation is launched to download the Prometei botnet malware from a remote server. The core module of the Prometei botnet is then utilized to extract the real crypto-mining payload and other system auxiliary components. To develop its command-and-control (C2) infrastructure, Prometei v3 employs a domain generation algorithm (DGA). It also has a self-update mechanism and a broader set of commands for harvesting sensitive data and controlling the host.

#3

The latest variants of the Prometei Linux botnet activities were accounted in March 2025, and are being distributed via HTTP GET requests from Indonesian-hosted servers. These Linux samples, deceptively named “k.php,” are UPX-packed ELF executables. The malware collects system details, including CPU, motherboard, OS version, uptime, and kernel information, and transmits them to designated command-and-control (C2) servers.

Recommendations

Network Defense and Threat Hunting: Set up IDS/IPS rules to detect connections to known or suspicious C2 infrastructure, prioritizing newly registered or Indonesian-hosted domains. Actively hunt for outbound traffic patterns consistent with Prometei C2 protocols.

Patch and Secure Server Infrastructure: Regularly update and patch systems, including third-party packages, to eliminate known vulnerabilities exploitable by botnets. Additionally, harden web applications and servers to prevent their misuse as infection vectors or payload delivery points, ensuring secure configurations, timely vulnerability remediation, and minimal exposed attack surfaces.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0011 Command and Control	**TA0040** Impact	**T1584** Compromise Infrastructure	**T1584.005** Botnet
T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1569** System Services	**T1569.002** Service Execution
T1505 Server Software Component	**T1505.003** Web Shell	**T1027** Obfuscated Files or Information	**T1106** Native API
T1070 Indicator Removal	**T1070.004** File Deletion	**T1140** Deobfuscate/Decode Files or Information	**T1036** Masquerading
T1210 Exploitation of Remote Services	**T1090** Proxy	**T1090.003** Multi-hop Proxy	**T1059.001** PowerShell

T1543 Create or Modify System Process	**T1562** Impair Defenses	**T1078** Valid Accounts	**T1203** Exploitation for Client Execution
T1059.004 Unix Shell	**T1071.001** Web Protocols	**T1036.008** Masquerade File Type	**T1082** System Information Discovery
T1588.006 Vulnerabilities	**T1588** Obtain Capabilities	**T1496** Resource Hijacking	**T1057** Process Discovery
T1110 Brute Force	**T1071** Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	23[.]148[.]145[.]237, 69[.]84[.]240[.]57, 103[.]40[.]123[.]34, 103[.]184[.]128[.]180, 103[.]184[.]128[.]244, 194[.]195[.]213[.]62, 211[.]232[.]48[.]65, 103[.]65[.]236[.]53, 177[.]73[.]237[.]55, 221[.]120[.]144[.]101, 196[.]7[.]210[.]6, 196[.]7[.]209[.]178, 196[.]7[.]210[.]160, 88[.]198[.]246[.]242, 187[.]79[.]243[.]171, 103[.]41[.]204[.]104, 155[.]207[.]200[.]242, 45[.]194[.]35[.]180
IPv4:Port	134[.]88[.]5[.]200[:]22, 142[.]4[.]205[.]155[:]80, 89[.]163[.]213[.]192[:]3333, 145[.]239[.]200[.]92[:]3333, 88[.]198[.]246[.]242[:]80
Domains	xinchaodbcdbh[.]org, xinchaodbcdbh[.]com,

TYPE	VALUE
Domains	xinchaoabcdcf[.]org, xinchaocecclk[.]org, xinchaocecclk[.]net, p1.feefreepool[.]net, p2.feefreepool[.]net, p3.feefreepool[.]net, gb7ni5rgeexdcncj[.]onion, p2[.]feefreepool[.]net
URLs	hxxp[:]//23[.]148[.]145[.]237:180/update[.]7z, hxxp[:]//69[.]84[.]240[.]57:180/AppServ180[.]zip, hxxp[:]//103[.]40[.]123[.]34/k[.]php, hxxp[:]//103[.]40[.]123[.]34/7z32[.]dll, hxxp[:]//103[.]40[.]123[.]34/7z32[.]exe, hxxp[:]//103[.]40[.]123[.]34/std2[.]7z, hxxp[:]//103[.]40[.]123[.]34/dwn[.]php?d=rdpclip[.]exe, hxxp[:]//103[.]40[.]123[.]34/dwn[.]php?d=7z32[.]exe, hxxp[:]//103[.]40[.]123[.]34/dwn[.]php?d=7z32[.]dll, hxxp[:]//103[.]126[.]6[.]233:180/AppServ180[.]zip, hxxp[:]//103[.]40[.]123[.]34/srch[.]7z, hxxp[:]//103[.]40[.]123[.]34/desktop[.]txt, hxxp[:]//103[.]40[.]123[.]34/bklocal2[.]php, hxxp[:]//103[.]40[.]123[.]34/bklocal4[.]php, hxxp[:]//103[.]40[.]123[.]34/update[.]7z, hxxp[:]//194[.]195[.]213[.]62:180/srch[.]7z, hxxp[:]//103[.]184[.]128[.]244/update[.]7z, hxxp[:]//211[.]232[.]48[.]65:180/update[.]7z, hxxp[:]//p2[.]feefreepool[.]net/cgi-bin/prometei[.]cgi, hxxp[:]//mkhkjxgchtfgu7uhofxzgoawntfzrkdccymveektqgpxrpjb72oq[.]zero/cgi-bin/prometei[.]cgi, hxxps[:]//gb7ni5rgeexdcncj[.]onion/cgi-bin/prometei[.]cgi, hxxp[:]//mkhkjxgchtfgu7uhofxzgoawntfzrkdccymveektqgpxrpjb72oq[.]b32[.]i2p/cgi-bin/prometei[.]cgi, hxxp[:]//103[.]40[.]123[.]34/k[.]php?B=_AMD64,PSDN0020,504K45A188441R4UE, hxxp[:]//103[.]41[.]204[.]104/7z32[.]dll, hxxp[:]//103[.]41[.]204[.]104/srch[.]7z, hxxps[:]//gb7ni5rgeexdcncj[.]onion/cgi-bin/prometei[.]cgi?r=9&i=N8Q4Y90O9T4MXH, hxxp[:]//103[.]41[.]204[.]104/k[.]php, hxxp[:]//152[.]36[.]128[.]18/cgi-bin/p[.]cgi
File Path	C:\Windows\dell\rdpclip.exe, C:\Windows\dell\msdtc.exe, C:\Windows\sqhost.exe, C:\Windows\dell\smcard.exe, C:\Windows\dell\windrlver.exe, C:\Windows\dell\miWalk.exe,

TYPE	VALUE
File Path	C:\Windows\dell\windrlver.exe, C:\Windows\dell\nethelper4.exe
SHA256	a1b3e8de2855b274edd9e6f7d7798e3cefe1aae8697568d333e00979054ecf58, 2e4e64035382eae04c035e2edb6f7080c221064859d95cdc4f458258af0289ae, bfe10104a2709d8dfeea3ddc373e3367a2ba2782ee8a0ee4d0f819869ccb0d4f, c1f8625ad3b13de77372cb4608210792d3f4b1b0909ae3593558d9d8f4306c99, 34efa1b8c185d5ba7290909c4446b1414684b09a9871d5c462c4fc609fbd87d2, 25dc9c2a2d31c42c63de0ed247784e33ea31f140d8035ac2141cb46f25eaefd4, ea8cde21792543d7e55dd9a2a894c3cd4fc4fabaeab20ba689b84416c20a6e37, 85a2d8f020b14cd11e95fd52328048ebe3e86f3f6a7cb76028143b7009a9b294, 44458197aafcb273b91f90a8cc55078b318e4f8a0384303acd1a5b3c13ff1ee0, f4ac4f735b9ff260a275734d86610dccb8558d1a54c6d6a78a94c33b6aaf6e39, 01bee3bb01f34f8da926c6b83980958166f1b10d00a923deb87361e9f34bcd83, 82c19c95f70c2a67be8a4914ed6c6b79b84aef3c1d65fefe85f90d89538bbe23, 6477b1ea0cc53d0c508295dcc53a0d465acc3fa712a56d846ca3bf0e296c83a5, 9788c1614110fa6e1ab957e4563331a8f8bddd926a0c3f8c7b891afa2203cf68, f11adbdad7200b90237dd9bbd5dbbf0b5ad30dd5a931fbef22cb0790e1851d82, 2d3b705d61448b84b89f7cead3c9b7cb9707a8ffcefa38fa81fdda16058a6dd6, dbd60814376047e2be10682110c1a1b3236f937ba522de66566197d939d2e48e, 0ca3a4c2800f9454cdcbb8398a7ec97b00f90f4234c7c5e48e206a8352d86750, ab9314c85b81caa832a49db8d0a86b6b871f749d7d6afcf4042d311cb63bd898, 608b2c8220a595a9766e2fdc5c91899dda635f97bc505e1a41e523aaddb11652, 6f39d02f27e3241224bb16e4753091b9d4ae2b4d0108a3fde2e3ebad0e1627bf, 4482fe91047b1e5c9c6f113893cfaae1b5815d743234807e68809b1235bef00b,

TYPE	VALUE
SHA256	c63074ace67db45003b4bbf7e99a57540956a98cd182c860cf80f3b7fa083565, 60585ca50fd149468d48f219988a3fd895add7a9c618e60e466b49f8695f48d5, a34a47ca8095389e29716418a0e7e98fda0ab9b8547ff7a8604a0e54df07b1fe, 35f9417c7be811df5b366963dc3986e6fb2e486afa0a0f64a092492b617c09e9, 61effa41e84446f6d712abb4707df964b9c82320602772962693caedc45f23b7, beca799029efa98646c861accc607cba8ef8ab52749a906524e8dd7981b38df2, 24654558cc1672532958387c6c0a91064ec58a381bfbbc10ef29447650dfe34f, 5319ee3372c439fb9d85a8174eea814a6c581d81a4af0fe7a9f686d403753c4d, 334e828a09bd64abb9a4f70256f4d2f8ffdf3249153f1e2356e861d188d8ba89, c512cad695fc027f3d3df46159a1f1b43d7641c37d6ade44870c052e36496bae, 3e8c0271c55975663ee03e25a047b1a27ef1905327dea3d1f897c5a27b31d8e6, cf5f1f2d7672d441f592d177e3f4a1a1f87e2abcef21e626d69f552cd0a2864d, 39b1042a5b02f3925141733c0f78b64f9fae71a37041c6acc9a9a4e70723a0f1, 314d2f1cb70c025ab0ba9de8c13914bda674b8f0a23e54454374d14d57fd2786, a546c3defb20bb18205b19c5218795fa9c6388d2e2ec3e65707b4e7afaeac0e1, af000bc9f397975604ec0ffd36ff414005ea49ca97ec176eadd14072ceccac00, 54bf36b5bdb844f46fd9849ac311e2efb62e16030c62597630cf38b4e3f8e8fa, d8f0712345356b5e68467eec43738fb44cca9df03c4a9b76873f48b5eab01b8c, d3c1dc40e7fdd55a037b73f708cdc6761762ebf5161e1fe86cdfc48ac51389dc, d1dfa4ab27798cfc9203c644358fe83e20ebf194a28502e1c8f43ad7a181e023, 655c294a4f4d3d01a9ba3a9563e136109dae7af0772cb3620e42357b59af476d, a6fb2a8604ab7c6c9d349d04741800926dc81dbd6f56c43382b54bc7f8cc7ca4, ca4577de74c66b89aa47bc91dadc8ece1564816b0b4528cbce7f3ab152396e3c,

TYPE	VALUE
SHA256	46cf75d7440c30cbfd101dd396bb18dc3ea0b9fe475eb80c4545868aab5c578c, cc7ab872ed9c25d4346b4c58c5ef8ea48c2d7b256f20fe2f0912572208df5c1a, 205c2a562bb393a13265c8300f5f7e46d3a1aabe057cb0b53d8df92958500867, 656fa59c4acf841dcc3db2e91c1088daa72f99b468d035ff79d31a8f47d320ef, 67279be56080b958b04a0f220c6244ea4725f34aa58cf46e5161cfa0af0a3fb0, 7a027fae1d7460fc5fccaf8bed95e9b28167023efcbb410f638c5416c6af53ff, 87f5e41cbc5a7b3f2862fed3f9458cd083979dfce45877643ef68f4c2c48777e, b1d893c8a65094349f9033773a845137e9a1b4fa9b1f57bdb57755a2a2dcb708, d21c878dcc169961bebda6e7712b46adf5ec3818cc9469debf1534ffa8d74fb7, D4566c778c2c35e6162a8e65bb297c3522dd481946b81baffc15bb7d7a4fe531

Patch Links

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-27065

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26858

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708

References

https://blog.talosintelligence.com/prometei-botnet-improves/

https://raw.githubusercontent.com/Cisco-Talos/IOCs/main/2023/03/prometei-botnet-improves.txt?ref=cisco-talos-blog

https://www.trendmicro.com/en_in/research/24/j/unmasking-prometei-a-deep-dive-into-our-mxdr-findings.html

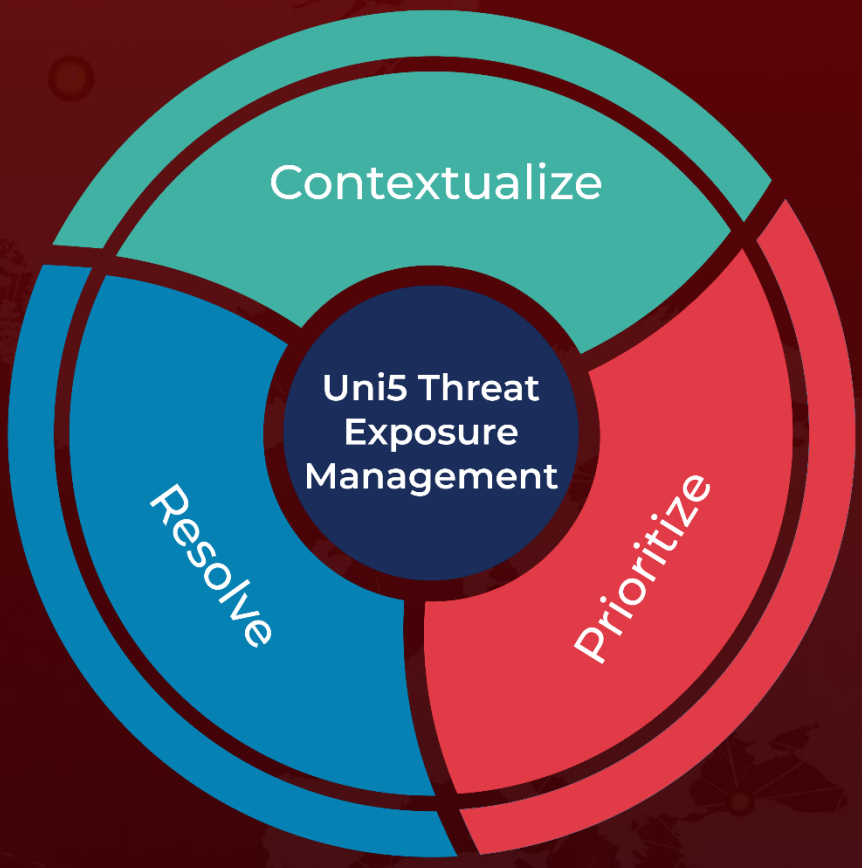
https://www.cybereason.com/blog/research/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities

https://unit42.paloaltonetworks.com/prometei-botnet-2025-activity/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 15, 2023 • 6:19 AM

More at www.hivepro.com