Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

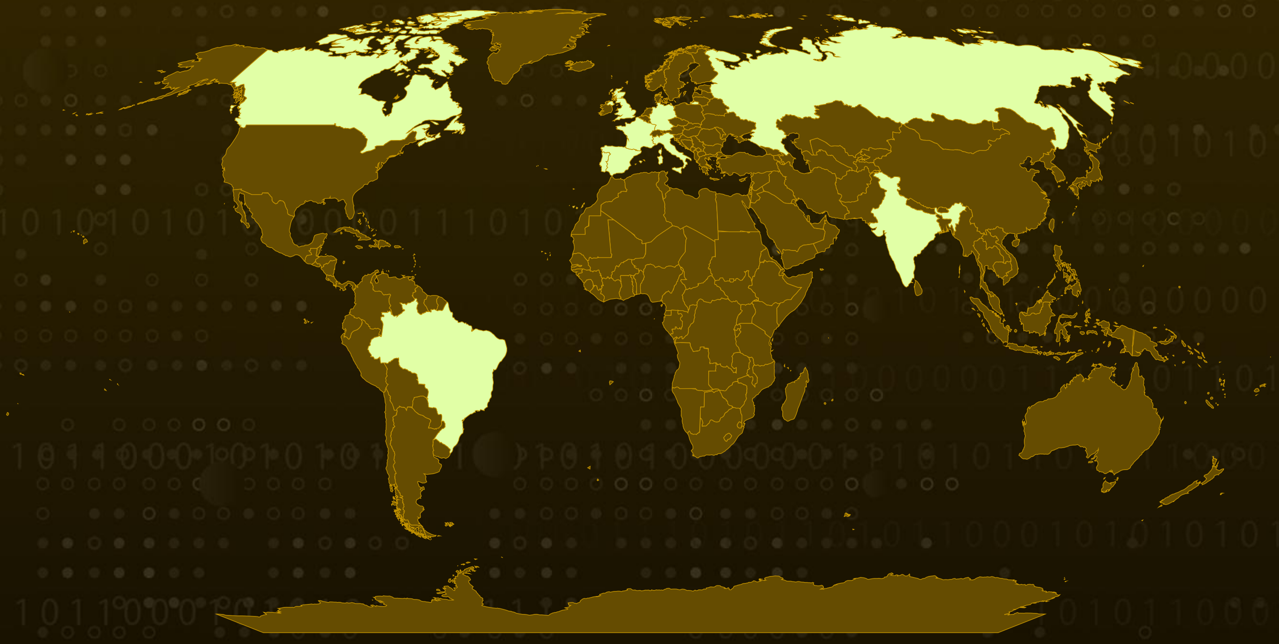
Efimer Trojan: From Fake Lawsuits to Crypto Heists

Date of Publication	Admiralty Code	TA Number
August 13, 2025	A1	TA2025248

Summary

Attack Discovered: October 2024
Targeted Countries: Brazil, India, Spain, Russia, Italy, Germany, UK, Canada, France, Portugal
Targeted Industry: Cryptocurrency
Malware: Efimer
Attack: A large-scale cybercrime operation is leveraging phishing emails, compromised WordPress sites, and fake torrent downloads to distribute the Efimer Trojan, a stealthy cryptocurrency-stealing malware. Disguised as legal notices from major law firms, the emails pressure recipients over alleged domain trademark infringements to lure them into opening malicious attachments. Once active, Efimer hijacks clipboard data, swaps wallet addresses, and steals recovery phrases, using the Tor network for covert communication. Beyond phishing, the attackers brute-force WordPress admin credentials to host malicious payloads and harvest email addresses for future spam, targeting cryptocurrency users, website owners, and unwary downloaders alike.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 A sweeping phishing operation has been making the rounds, masquerading as urgent legal notices from well-known law firms. The emails falsely accused website owners of trademark infringement, alleging that certain words or phrases in their domain names violated registered trademarks. Behind this convincing legal façade lurked Efimer, a cryptocurrency-stealing Trojan. First detected in late 2024 spreading through compromised WordPress sites, the malware's operators expanded their tactics in June with large-scale phishing campaigns to reach a wider pool of victims.

#2 The phishing emails arrived with a ZIP archive containing a password-protected file and a decoy text document labelled "password." To bypass automated scanning tools, the attackers embedded a special Unicode character in the filename, making it harder for security systems to read the password directly. Once opened, the archive revealed a Windows Script File that quietly deployed the Efimer Trojan. When run with elevated privileges, Efimer excluded its installation folder from Windows Defender scans, created persistence in the Windows registry, and threw up a fake error message to mislead the victim into thinking nothing had happened.

#3 Efimer functions as a ClipBanker Trojan, designed to monitor the clipboard for cryptocurrency wallet addresses or mnemonic recovery phrases. If detected, it swiftly swaps them with attacker-controlled addresses, redirecting funds without the victim's knowledge. To avoid detection during communication with its C2 server, the malware installs a Tor proxy client, downloaded from several hardcoded sources to ensure availability. Efimer also hunts for "SEED" files containing wallet recovery phrases, exfiltrates them to its operators, and captures screenshots for additional intelligence gathering.

#4 The malware also spreads through WordPress websites and fake torrent downloads disguised as pirated films. Victims are enticed to download an XMPEG video file bundled with a fake media player, which is in fact another Efimer installer, this time preloaded with spoofed cryptocurrency wallet addresses for multiple digital currencies. The operation uses additional scripts from the C2 to brute-force WordPress admin credentials, generating password guesses from Wikipedia-sourced words and exploiting compromised sites to host malicious payloads.

#5 These auxiliary modules reveal the scale of the attackers' infrastructure. Some scripts harvest email addresses from targeted sites, while others automate brute-force attacks and credential stuffing. They operate on constant loops, checking in with the C2 server for new instructions, from executing remote JavaScript code to wiping all traces of malware via a "KILL" command. In certain cases, stolen data is encrypted before being sent to the attackers, giving the operation an added layer of stealth.

Recommendations

Be cautious with unexpected emails: If you get an email claiming you've broken the law or infringed trademarks especially if it comes with an attachment treat it as suspicious. Legitimate legal notices will not arrive via a random ZIP file.

Avoid shady downloads: Stay away from pirated movies, torrents, or "free" downloads from unknown sources. These are common tricks cybercriminals use to deliver malware like Efimer.

Secure your website: If you run a WordPress site, update your themes, plugins, and core software regularly. Use strong, unique passwords and enable two-factor authentication to keep attackers out.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1566 Phishing	T1566.001 Spearphishing Attachment
T1189 Drive-by Compromise	T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1059.007 JavaScript	T1059.001 PowerShell	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1562** Impair Defenses	**T1027** Obfuscated Files or Information
T1110 Brute Force	**T1082** System Information Discovery	**T1115** Clipboard Data	**T1113** Screen Capture
T1056 Input Capture	**T1005** Data from Local System	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1090 Proxy	**T1090.003** Multi-hop Proxy	**T1036** Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	39fa36b9bfcf6fd4388eb586e2798d1a, 5ba59f9e6431017277db39ed5994d363, 442ab067bf78067f5db5d515897db15c, 16057e720be5f29e5b02061520068101, 627dc31da795b9ab4b8de8ee58fbf952, 0f5404aa252f28c61b08390d52b7a054, Eb54c2ff2f62da5d2295ab96eb8d8843, 100620a913f0e0a538b115dbace78589, B405a61195aa82a37dc1cca0b0e7d6c1, 5d132fb6ec6fac12f01687f2c0375353
SHA256	006C397EC5B65E0C646598EE6014813FF601802D927FB90571E5AD1204D7F70F, 787797BFBF690D05DB8A796E3CA948578FB9BA7189D9F9BC53D99FB5EA626BB7, DC4FD2E5604D12AE4F8444E6429DC3EB6CB592214A8E998D9C76B810B102C3F8, 6199960F2EC96D4851E4F36D5A5095922E422E3B4265BDB537CCDBB8D44AC8DC, C77FCF134A8D81B3FC329EB767D62C997708D6FEDB2D33898F79184F22D542A5, 75102507763CE008917613F11EC3301F59F0F0115799DC9AD1BE147D9E69584E, 1569FA17748B501121EADCDF64723A448B21839B8922FD6E2C176F1ED8D6B0AA, 32709EFBF41289FF2BE8D34A1067AD70B6AC1D9BC05384285C41545C22ED7DF7

TYPE	VALUE
URLs	hxxps[:]//lovetahq[.]com/sinners-2025-torent-file/, hxxps[:]//lovetahq[.]com/wp-content/uploads/2025/04/movie_39055_xmpg[.]zip, hxxp[:]//cgky6bn6ux5wvlybtmm3z255igt52ljml2ngnc5qp3cnw5jlglamisad[.]onion hxxp[:]//he5vnov645txpcv57el2theky2elesn24ebvgwfoewlpftksxp4fnxad[.]onion

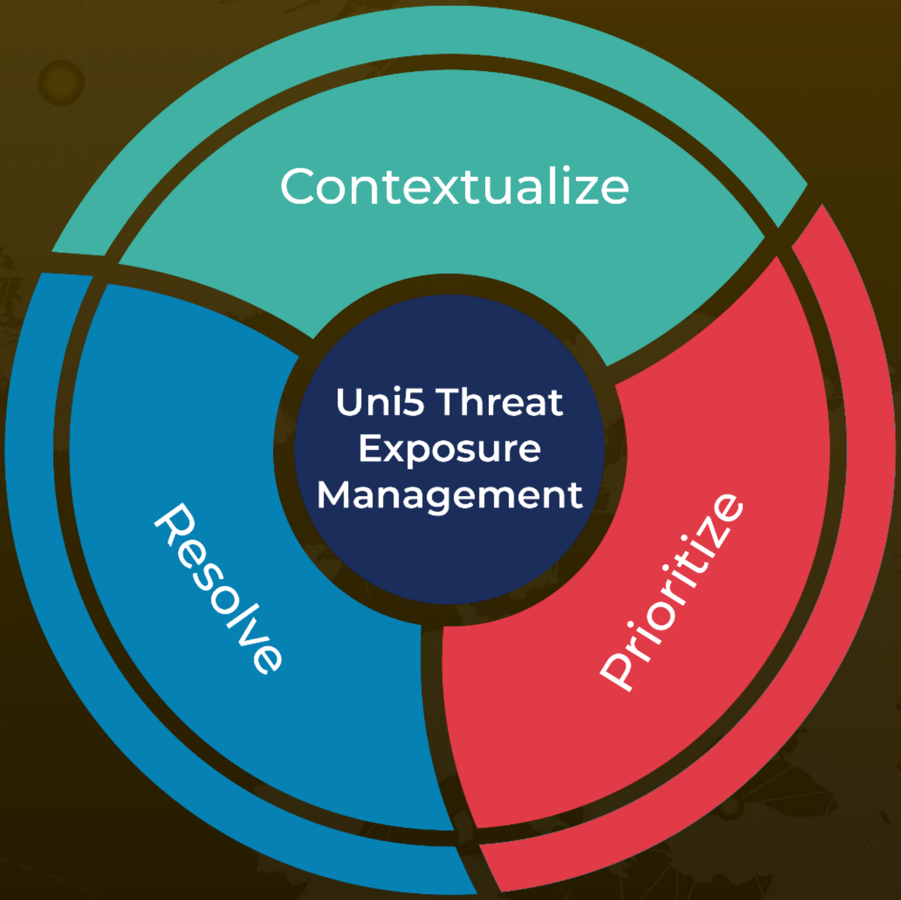
References

https://securelist.com/efimer-trojan/117148/

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

August 13, 2025 • 5:30 AM

More at www.hivepro.com