Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

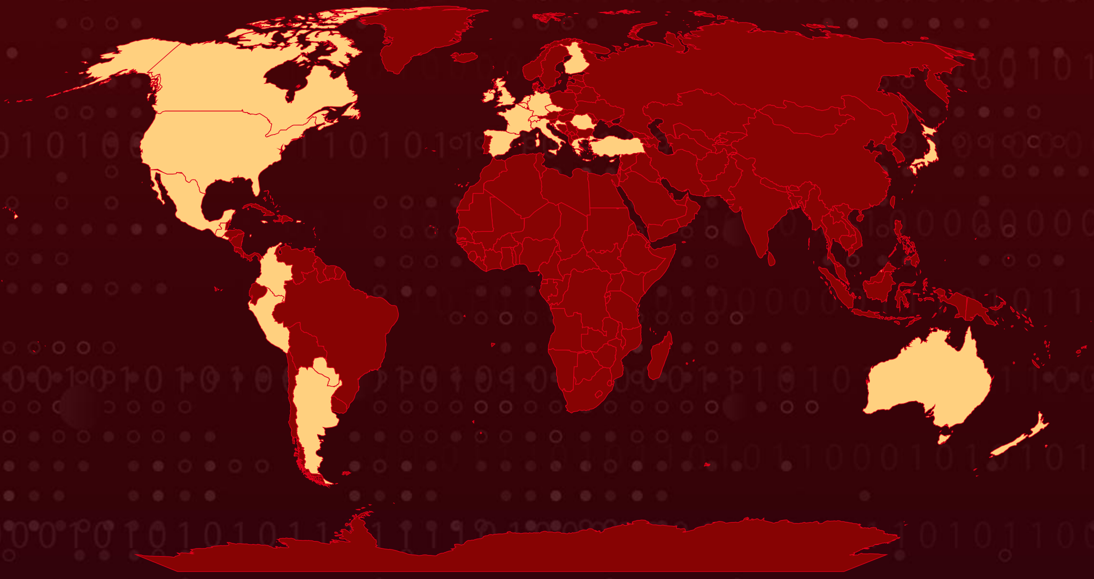
SafePay Ransomware's Rapid Ascent to the Top of the Cybercrime Scene

Date of Publication	Admiralty Code	TA Number
August 7, 2025	A1	TA2025241

Summary

First Seen: September 2024
Malware: SafePay ransomware, Qdoor
Affected Platform: Windows
Targeted Countries: United States, Australia, United Kingdom, Curacao, England, Peru, Paraguay, Japan, Canada, Guatemala, Croatia, Ireland, Italy, Germany, Romania, Greece, Switzerland, Colombia, Spain, Mexico, Czech Republic, Argentina, Singapore, Netherlands, Jamaica, Turkey, Finland, Puerto Rico, Belgium, France, Cyprus, Barbados, New Zealand, Brunei, El Salvador
Targeted Industries: Government, Legal, Technology, Business Services & Consulting, Telecommunications, Energy, Associations, Healthcare, Manufacturing, Charitable Organizations, Education, Retail, Agriculture, Real Estate, Religion, Financial Services, Hospitality, Transportation, Food Service, Aerospace and Defense, Media, Insurance, Pharmaceutical, Aviation
Attack: SafePay, a rapidly rising ransomware group that emerged in September 2024, has quickly become one of the most aggressive and active cybercriminal groups in 2025, responsible for over 200 attacks. Targeting industries such as managed service providers (MSPs) and small-to-medium businesses (SMBs), SafePay's attacks primarily focus on the United States, Germany, and other regions, while avoiding CIS countries. Unlike Ransomware-as-a-Service models, SafePay operates privately, maintaining tight control over its attacks and consistently high-impact operations.

Attack Regions



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

Attack Details

#1 SafePay is a ransomware group that surfaced in September 2024. Initially targeting just over 20 victims, it gained attention by encrypting files and demanding cryptocurrency payments for restoration. By 2025, the group escalated its activity, claiming responsibility for over 270 attacks, primarily against managed service providers (MSPs) and small-to-medium businesses (SMBs) across various industries.

#2 The United States has been the hardest hit, with over 130 confirmed victims, followed by Germany with 50 cases. Additional attacks have been reported in countries such as the United Kingdom, Canada, Australia, and several nations in Latin America and Asia. Notably, SafePay has avoided targeting Commonwealth of Independent States (CIS) countries, likely steering clear of Russian-speaking or allied regions.

#3 SafePay operators conduct detailed pre-attack reconnaissance to identify vulnerable access points, often acquiring user credentials through stealers or dark web marketplaces. They also scan for exposed remote access services, such as VPN gateways and RDP endpoints, alongside known system vulnerabilities.

#4 Upon gaining access, they deploy scripts and payloads to establish control, often using batch files or PowerShell scripts stored in inconspicuous locations and executed manually or via scheduled tasks. In some cases, the group deployed malware like QDoor, a remote access tool for command execution and tunneling. Then, escalate privileges, disable endpoint security, delete shadow copies, and clear event logs to hinder recovery and detection efforts.

#5 SafePay encrypts files with the .safepay extension and drops a ransom note titled "readme_safepay.txt." The group uses a double extortion tactic, threatening to release stolen data if the ransom is not paid. While the ransomware shares similarities with LockBit, particularly a version from late 2022, it also incorporates elements from other groups like ALPHV and INC Ransom.

#6 A prominent 2025 attack on Ingram Micro, a global IT distributor, exemplified SafePay's impact. The group exfiltrated 3.5TB of data from the company and threatened to leak it. Unlike many ransomware gangs, SafePay operates privately and does not use a Ransomware-as-a-Service (RaaS) model. This gives them tighter control over their operations and enables consistent attack strategies.

Recommendations

Network and System Hardening: Restrict SMB (Server Message Block) traffic where possible, especially lateral movement via open shares. Disable unnecessary SMB services on endpoints and servers. Limit administrative privileges to essential personnel and apply the principle of least privilege across all systems. Enforce strong network segmentation to isolate critical systems and limit lateral propagation opportunities.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

Patch Vulnerabilities Promptly: SafePay targets known vulnerabilities in systems, so it's essential to keep all software, including operating systems, applications, and security tools, up to date with the latest patches. Where feasible, automate updates and vulnerability scanning to ensure no critical patches are missed.

Adopt a Zero Trust Security Model: Always verify and authenticate users and devices before granting access to critical resources, even if they are inside the network. Implementing a Zero Trust architecture helps limit the ability of attackers to move laterally within networks.

Improve Credential Security: SafePay's operators often gain access using stolen or weak credentials. Enforce the use of complex passwords across all systems and networks. Encourage employees to use password managers to generate and store secure, unique passwords for different platforms. Regular credential audits of user access and account permissions to ensure that only authorized personnel have access to sensitive systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1078 Valid Accounts	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell
T1202 Indirect Command Execution	T1548.002 Bypass User Account Control	T1070 Indicator Removal	T1070.004 File Deletion
T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1003 OS Credential Dumping	T1135 Network Share Discovery
T1482 Domain Trust Discovery	T1021 Remote Services	T1560.001 Archive via Utility	T1048 Exfiltration Over Alternative Protocol
T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery	T1190 Exploit Public-Facing Application
T1543 Create or Modify System Process	T1543.003 Windows Service	T1133 External Remote Services	T1027 Obfuscated Files or Information
T1027.002 Software Packing	T1082 System Information Discovery	T1614.001 System Language Discovery	T1021.001 Remote Desktop Protocol
T1531 Account Access Removal	T1071.001 Web Protocols	T1574 Hijack Execution Flow	T1057 Process Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	VanessaCooke94[@]protonmail[.]com, ColinSolomon[@]protonmail[.]com, DepaolaKristabelle[@]protonmail[.]com
Filename	locker.dll, ShareFinder.ps1, readme_safepay.txt, readme_safepay_ascii.txt
IPv4	45[.]91[.]201[.]247, 77[.]37[.]49[.]40, 80[.]78[.]28[.]63, 88[.]119[.]167[.]239
SHA1	07353237350c35d6dc2c8f143b649cd07c71f62b
SHA256	a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526, 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae, 6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a, e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346
TOR Address	nj5qix45sxnl4h4og6hcgwengg2oqloj3c2rhc6dpwiofx3jbivcs6qd[.]onion, nz4z6ruzcekriti5cjjiiylzvrmysyqwibxztk6voem4trtx7gstpjid[.]onion, j3dp6okmaklajrsk6zljl5sfa2vpui7j2w6cwmhmmqhab6frdfbphhid[.]onion, cqkrkmmivhakl3fwgxscurduu3znmroablt7jskxszkctixyseij5gad[.]onion, safepaypfxntwixwjrlcscft433ggemlhgkkdupi2ynhtcmvdgubmoyd[.]onion
URLs	hxxps[:]//github[.]com/darkoperator/Veil-PowerView/blob/master/PowerView/functions/Invoke-ShareFinder[.]ps1, hxxps[:]//gist[.]github[.]com/gleeda/988da614e6740fac66dbaa6d92121302

Recent Breaches

https://chamberlainhuckeriede.com
https://ingrammicro.com

https://wta-inc.com
https://tele-optics.com
https://bussepc.com
https://swfldermatology.com
https://appagroup.com
https://havtechpa.com
https://teamsignal.com
https://appsnw.com
https://rhschool.org
https://naxis.net
https://salemma.com.py
https://qtmi.net
https://landwwilson.co.uk
https://norpak.com
https://hlb.ie
https://divgroup.eu
https://ashland.k12.ma.us
https://palmasdelixcan.com
https://nod.ro
https://bartec.com
https://relucent.com
https://fmsarchitects.com
https://cascobay.org
https://caredig.co.uk
https://silverdalebc.com
https://profile-ind.com
https://ppa-eng.com
https://avgouleaschool.gr
https://chirurgiemaxillo.com
https://lowcostspayneuterindiana.org
https://lewis-manning.org.uk

References

https://socradar.io/dark-web-profile-safepay-ransomware/

https://www.acronis.com/en-us/tru/posts/safepay-ransomware-the-fast-rising-threat-targeting-msps/

https://www.huntress.com/blog/its-not-safe-to-pay-safepay

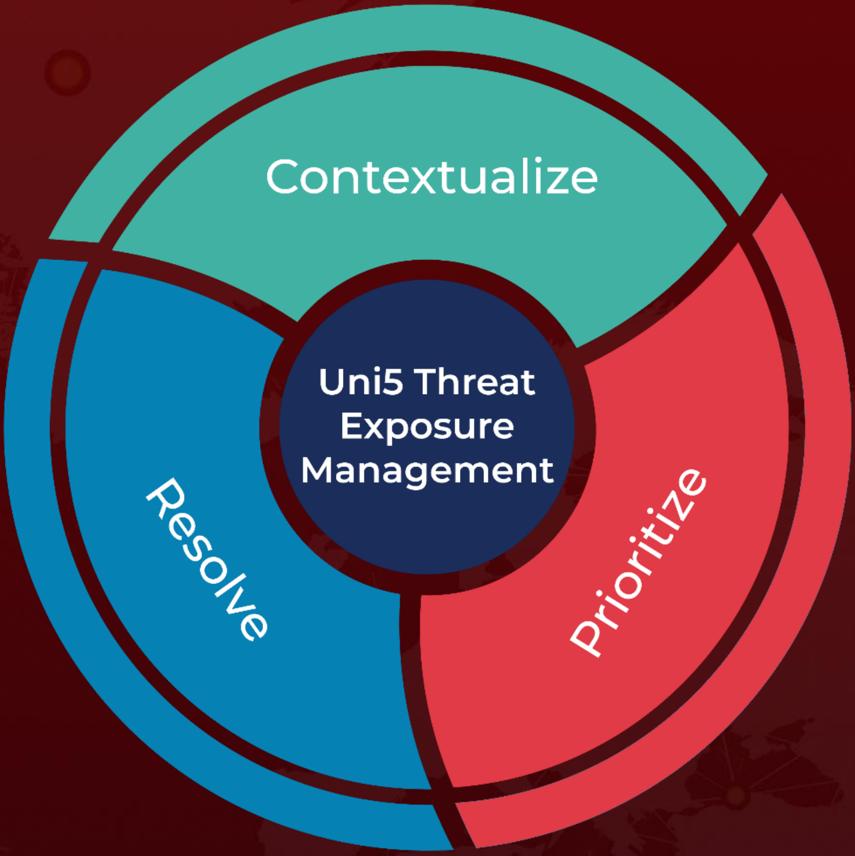
https://www.nccgroup.com/us/research-blog/weak-passwords-led-to-safepay-ransomware-yet-again/

https://hivepro.com/threat-advisory/lockbit-ransomware-evolving-tactics-and-pervasive-impact-in-2023/

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 7, 2025 • 4:30 AM

More at www.hivepro.com