

HiveForce Labs

# THREAT ADVISORY



## ATTACK REPORT

### SafePay Ransomware Surges Past 600 Victims Worldwide

Date of Publication

October 23, 2026

Admiralty Code

A1

TA Number

TA2026312

# Summary

**First Seen:** August 2024

**Targeted Regions:** North America, South America, Europe, Asia, Middle East, Oceania

**Targeted Platform:** Windows

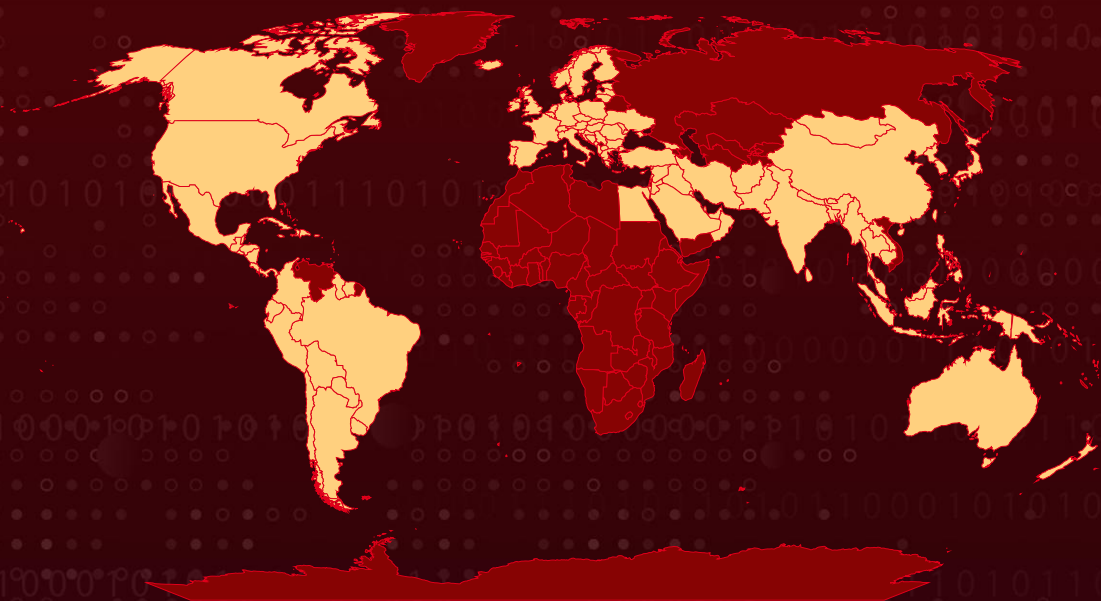
**Targeted Products:** Edge Devices (VPN Gateways and Firewalls), Internet-Exposed Systems

**Targeted Industries:** Aerospace, Defense, Agriculture, Aviation, Business Services and Consulting, Charitable Organizations, Critical Infrastructure, Education, Energy, Financial Services, Food Service, Government, Healthcare, Hospitality, Information Technology, Insurance, Legal, Managed Service Providers, Manufacturing, Media, Pharmaceutical, Real Estate, Religious Organizations, Retail, Small and Medium Businesses, Telecommunications, Transportation

**Malware:** SafePay Ransomware

**Attack:** SafePay is a closed, double extortion ransomware operation active since August 2024 that has impacted at least 600 organizations across North America, South America, Europe, and Australia and leak-site claims extending into Asia, the Middle East, and Oceania. The group gains entry through stolen, guessed, or phished credentials, VPN access, and exploitation of five known flaws in edge devices and internet-exposed systems, then relies on living-off-the-land tooling and legitimate remote access software to escalate privileges, move laterally, and exfiltrate data. It finishes with a LockBit-derived encryptor that wipes out recovery options, including network-attached backups, and pressures victims with revenue-based cryptocurrency demands, leak-site exposure, and direct phone calls.

## Attack Regions



 Targeted

 Non-Targeted

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Powered by Bing



**THREAT ADVISORY** • **ATTACK REPORT** (Red)

2

 **Hive Pro**

| CVE            | NAME                                                                                                | AFFECTED PRODUCT                                               | ZERO-DAY                                                                            | CISA KEV                                                                              | PATCH                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| CVE-2020-3259  | Cisco ASA and FTD Information Disclosure Vulnerability                                              | Cisco ASA and FTD                                              |    |    |    |
| CVE-2023-20269 | Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability    | Cisco Adaptive Security Appliance and Firepower Threat Defense |    |    |    |
| CVE-2023-27532 | Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability | Veeam Backup & Replication, Veeam Cloud Connect                |    |    |    |
| CVE-2024-40711 | Veeam Backup and Replication Deserialization Vulnerability                                          | Veeam Backup and Replication                                   |  |  |  |
| CVE-2024-40766 | SonicWall SonicOS Improper Access Control Vulnerability                                             | SonicWall SonicOS                                              |  |  |  |

# Attack Details

#1

[SafePay](#) ranks among the most active ransomware operations of 2026, with at least 600 victims across businesses and multiple critical infrastructure sectors in North America, South America, Europe, and Australia, and investigated intrusions as recent as August 2026.

## #2

SafePay gains entry by stealing or guessing passwords, running brute force attacks, abusing exposed credentials, and exploiting VPN access, often connecting from Mullvad VPN infrastructure and using phished account profiles to exploit CVE-2020-3259 and CVE-2023-20269 in edge device products. In parallel, automated scripts sweep internet-exposed systems for CVE-2023-27532, CVE-2024-40711, and CVE-2024-40766, showing that long-disclosed flaws remain a dependable way in.

## #3

Once inside, operators grant administrative privileges to existing accounts or create new ones with built-in tools and deploy ScreenConnect for persistent access. They disable security software before moving laterally, change user passwords to lock out legitimate staff, and conceal code through software packing and virtual machine protection, with an injected PE and a RunPE-bundled DLL recovered alongside a soc.dll component that talks to dedicated command and control infrastructure. Privileges are escalated through a COM-based User Account Control bypass and token impersonation.

## #4

Lateral movement relies on PsExec, WinRM, remote monitoring and management tools, and RDP, with new accounts created whenever administrative access is lacking. Mimikatz and DCSync tooling harvest credentials, ShareFinder.ps1, SharpShares.exe, netscan, NetExec, and nltest enumerate shares, hosts, and domain trusts, and SOCKS proxy binaries, one likely masquerading as a Windows process, tunnel traffic.

## #5

Data is staged and compressed with WinRAR and 7-Zip, then exfiltrated through FileZilla, WinSCP, and RClone to actor-controlled accounts, to OneDrive, and to Backblaze B2 storage via b2.exe, supported by separate infrastructure for exfiltration, stolen data hosting, and client login panels. AnyDesk and TeamViewer are installed to move the ransomware and supporting tools onto victim systems.

## #6

Before encryption, SafePay halts the Volume Shadow Copy Service, resets network-attached storage holding backups to factory settings, and in some cases deletes all network-attached backups. Files are then encrypted with a hybrid ChaCha20 and RSA scheme that applies full or partial encryption based on file type and size, appending .SafePay and leaving data unrecoverable without the key, after which the ransomware may delete itself.

## #7

A ransom note left on the desktop or root directory directs victims to a Tor chat portal accessed with a victim ID, where the group demands a share of company revenue in cryptocurrency. Representatives phone victims to raise pressure, and those who refuse to pay see their stolen data published on the SafePay leak site. With backup destruction, phone-based coercion, and continued exploitation of known edge device flaws, SafePay remains a priority threat for any organization with exposed remote access or reachable backups.

# Recommendations



**Remediate SafePay-Exploited Vulnerabilities:** Patch CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711, and CVE-2024-40766 immediately, starting with firewalls, VPN gateways, and every other internet-facing system, and review affected devices for signs of prior compromise, since SafePay sweeps for these flaws with automated scripts.



**Enforce Phishing-Resistant MFA on Remote Access:** Require MFA for VPN, webmail, remote desktop gateways, and every account that reaches critical systems, because SafePay's entry repeatedly relies on stolen, phished, or guessed credentials.



**Scrutinize VPN Logins From Anonymizing Services:** Alert on or block VPN authentication from commercial anonymizing VPN providers such as Mullvad, which SafePay has used for initial access, and investigate sessions from unfamiliar hosts carrying default Windows names such as WIN-3IUUOFVTQAR.



**Harden Passwords and Lockout Policies:** Enforce passwords of at least 15 characters, ban credential reuse, and lock accounts after repeated failed logins to blunt brute force attacks against VPN and RDP.



**Conduct Regular Data Backups and Test Restoration:** Regularly back up critical data and systems and store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a SafePay ransomware attack, up-to-date backups enable recovery without paying the ransom.



**Allowlist Remote Access Software:** Block unapproved remote access tools such as AnyDesk, TeamViewer, and ScreenConnect through application control and alert on their installation, since SafePay uses them for persistence and to deliver ransomware.



**Monitor Account Creation and Privilege Changes:** Alert on new accounts, additions to privileged groups, and unexpected password resets, and regularly review domain controllers, servers, and Active Directory for unrecognized or dormant accounts.



# Potential MITRE ATT&CK TTPs

| Tactic               | Technique                                         | Sub-technique                                  |
|----------------------|---------------------------------------------------|------------------------------------------------|
| Initial Access       | <u>T1078</u> : Valid Accounts                     |                                                |
|                      | <u>T1133</u> : External Remote Services           |                                                |
|                      | <u>T1190</u> : Exploit Public-Facing Application  |                                                |
|                      | <u>T1566</u> : Phishing                           | <u>T1566.004</u> : Spearphishing Voice         |
| Execution            | <u>T1059</u> : Command and Scripting Interpreter  | <u>T1059.001</u> : PowerShell                  |
|                      |                                                   | <u>T1059.003</u> : Windows Command Shell       |
|                      | <u>T1569</u> : System Services                    | <u>T1569.002</u> : Service Execution           |
|                      | <u>T1047</u> : Windows Management Instrumentation |                                                |
| Persistence          | <u>T1098</u> : Account Manipulation               |                                                |
|                      | <u>T1136</u> : Create Account                     |                                                |
|                      | <u>T1547</u> : Boot or Logon Autostart Execution  |                                                |
| Privilege Escalation | <u>T1548</u> : Abuse Elevation Control Mechanism  | <u>T1548.002</u> : Bypass User Account Control |
|                      | <u>T1134</u> : Access Token Manipulation          | <u>T1134.001</u> : Token Impersonation/Theft   |
|                      | <u>T1055</u> : Process Injection                  |                                                |



| Tactic             | Technique                                      | Sub-technique                                                 |
|--------------------|------------------------------------------------|---------------------------------------------------------------|
| Stealth            | <u>T1027</u> : Obfuscated Files or Information | <u>T1027.002</u> : Software Packing                           |
|                    | <u>T1218</u> : System Binary Proxy Execution   | <u>T1218.010</u> : Regsvr32                                   |
|                    | <u>T1070</u> : Indicator Removal               | <u>T1070.004</u> : File Deletion                              |
|                    |                                                | <u>T1070.001</u> : Clear Windows Event Logs                   |
|                    | <u>T1036</u> : Masquerading                    | <u>T1036.005</u> : Match Legitimate Resource Name or Location |
|                    | <u>T1622</u> : Debugger Evasion                |                                                               |
| Defense Impairment | <u>T1685</u> : Disable or Modify Tools         |                                                               |
| Credential Access  | <u>T1110</u> : Brute Force                     |                                                               |
|                    | <u>T1003</u> : OS Credential Dumping           | <u>T1003.006</u> : DCSync                                     |
| Discovery          | <u>T1135</u> : Network Share Discovery         |                                                               |
|                    | <u>T1046</u> : Network Service Discovery       |                                                               |
|                    | <u>T1482</u> : Domain Trust Discovery          |                                                               |
|                    | <u>T1614</u> : System Location Discovery       | <u>T1614.001</u> : System Language Discovery                  |
| Lateral Movement   | <u>T1021</u> : Remote Services                 | <u>T1021.001</u> : Remote Desktop Protocol                    |
|                    |                                                | <u>T1021.002</u> : SMB/Windows Admin Shares                   |
|                    |                                                | <u>T1021.006</u> : Windows Remote Management                  |

| Tactic              | Technique                                                      | Sub-technique                                             |
|---------------------|----------------------------------------------------------------|-----------------------------------------------------------|
| Collection          | <a href="#">T1560</a> : Archive Collected Data                 | <a href="#">T1560.001</a> : Archive via Utility           |
|                     | <a href="#">T1039</a> : Data from Network Shared Drive         |                                                           |
| Command and Control | <a href="#">T1219</a> : Remote Access Tools                    | <a href="#">T1219.002</a> : Remote Desktop Software       |
|                     | <a href="#">T1105</a> : Ingress Tool Transfer                  |                                                           |
|                     | <a href="#">T1090</a> : Proxy                                  |                                                           |
| Exfiltration        | <a href="#">T1048</a> : Exfiltration Over Alternative Protocol |                                                           |
|                     | <a href="#">T1567</a> : Exfiltration Over Web Service          | <a href="#">T1567.002</a> : Exfiltration to Cloud Storage |
| Impact              | <a href="#">T1486</a> : Data Encrypted for Impact              |                                                           |
|                     | <a href="#">T1490</a> : Inhibit System Recovery                |                                                           |
|                     | <a href="#">T1489</a> : Service Stop                           |                                                           |
|                     | <a href="#">T1531</a> : Account Access Removal                 |                                                           |
|                     | <a href="#">T1667</a> : Email Bombing                          |                                                           |

## ✂ Indicators of Compromise (IOCs)

| TYPE     | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SHA256   | 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae,<br>6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a,<br>e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346,<br>327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917,<br>a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526,<br>BBDD3620A67AEDEC4B9A68B2C9CC880B6631215E129816AEA19902A6F4BC6F41 |
| SHA1     | 07353237350c35d6dc2c8f143b649cd07c71f62b,<br>b498a2683640c983bb069fa2ea9e67cef4a3797d,<br>BBFED53E3BB1F306F4DA97D995CF4AE5B73AD081,<br>d711a5af5aed48a3b36b98f4fcf52809aebef7a2                                                                                                                                                                                                                                           |
| IPv4     | 104[.]26[.]2[.]223,<br>140[.]82[.]114[.]4,<br>185[.]199[.]108[.]133,<br>77[.]37[.]49[.]40,<br>173[.]194[.]194[.]94,<br>167[.]235[.]225[.]149,<br>5[.]255[.]11[.]134,<br>88[.]119[.]167[.]239,<br>37[.]10[.]71[.]188                                                                                                                                                                                                       |
| Hostname | WIN-SBOE3CPNALE,<br>WIN-SBOE3CPNAL,<br>WIN-3IUUOFVTQAR,<br>WIN-DK18BI83M0S,<br>WIN-I1HRRJHCEIV                                                                                                                                                                                                                                                                                                                            |

| TYPE     | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filename | 1 – Copy.bat,<br>CCleaner.exe,<br>CCleaner64.exe,<br>CCleaner*.exe,<br>CCleaner*.dll,<br>dcsync.exe,<br>domains.txt,<br>DYRasWtb.exe,<br>libsmb2.dll,<br>Libwa*.dll,<br>License.txt,<br>locker.dll,<br>netscan.exe,<br>netscan.lic,<br>netscan.xml,<br>netscanNEW.zip,<br>nltest.exe,<br>oui.txt,<br>ping.txt,<br>portable.dat,<br>scan.xml,<br>sharefinder.ps1,<br>Socks.exe,<br>Socks_werfault.exe,<br>subs.txt,<br>svchost.exe,<br>wa_3rd_party_host_*.exe,<br>winrar.exe,<br>AnyDesk.exe,<br>SharpShares.exe,<br>AcronisDiskDirector-12.5,<br>acro.exe,<br>DiskDirector.exe,<br>Acronis.exe,<br>b2.exe,<br>nxc.exe,<br>1.exe,<br>soc.dll,<br>readme_safepay.txt |



## Recent Breaches

<https://hiqbio.com>  
<https://www.dwi-bau.de>  
<https://hoteldelfinolugano.ch>  
<https://stuecheli.ch>  
<https://halservice.it>  
<https://sterrer.net>  
<https://dd-automation.ch>  
<https://ikhasas.com>  
<https://www.t-systems.com>  
<https://bwi-bau.de>  
<https://grundens.com>  
<https://anwo.cl>  
<https://duhaas.sk>  
<https://econ-tec.com>  
<https://wolfusofsky.de>  
<https://assist2enjoy.be>  
<https://eagroep.com>  
<https://bio-strath.com>  
<https://cromados.com>  
<https://auromex.com>  
<https://manno.ch>  
<https://sumperk.cz>  
<https://lfgholding.com>  
<https://holidayinnvilnius.com>  
<https://fedelmundo.com.ph>  
<https://marlinhvac.com>  
<https://meterex.com>  
<https://stoecklin-kuechen.ch>  
<https://triniticaring.org>  
<https://www.gob.pe>  
<https://ara-lyss.ch>  
<https://neumerkel-gmbh.de>  
<https://laconcepcion.com.mx>  
<https://ryomo.co.jp>  
<https://compunnel.com>  
<https://gsngestion.es>  
<https://hbpro.pt>  
<https://recoverycafe.org>  
<https://mcnishsteel.com>  
<https://gayafores.es>  
<https://reichenau.at>  
<https://assiprime.it>



## Patch Links

### **CVE-2020-3259:**

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB>

### **CVE-2023-20269:**

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC>

**CVE-2023-27532:** <https://www.veeam.com/kb4424>

**CVE-2024-40711:** <https://www.veeam.com/kb4649>

**CVE-2024-40766:** <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015>

## References

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a>

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

<https://www.hivepro.com/threat-advisory/safepay-ransomware-rapid-ascent-to-the-top-of-the-cybercrime-scene>

<https://therecord.media/fbi-says-safepay-ransomware-gang-among-most-active-600-victims>

<https://blog.barracuda.com/2025/07/25/safepay--email-bombs--phone-scams--and-really-big-ransoms>

# 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 Demo of HivePro.

REPORT GENERATED ON

**October 23, 2026 • 05:35 AM**

© 2026 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)