SafePay ransomware explained: IOCs, TTPs, and defense strategies

By Rayton Li and John Moutos, ThreatLocker Threat Intelligence

Published: 2025-07-31 · Archived: 2026-05-09 02:01:25 UTC

Observing SafePay ransomware, ThreatLocker® Intelligence has seen Mutexes being created to prevent additional copies of the ransomware running on already affected/encrypted devices. Typically, a different Mutex would be used for each victim. The switch to a more aggressive approach to choosing targets may be partially due to all the coverage of the Ingram Micro breach and the likely growing intensity of law enforcement pressure.

SafePay ransomware overview

SafePay is a ransomware group that was discovered by security vendors sometime in November 2024 and has since made international headlines as the group has threatened to release over 3.5 TB of internal data from Ingram Micro, a US based information technology product and service distributor. The group has quickly become among the most prolific, with over two hundred organizations claimed on its Tor data leak website.

The group primarily targets organizations in the United States, Germany, the United Kingdom, Australia, Canada, and a few other countries. SafePay does not intentionally target organizations that are either current or former members of the Commonwealth of Independant States (CIS), which may indicate the group originates or resides in Eastern Europe or Asia.

Tactics, techniques, and procedures (TTP)

Initial access

The primary initial access vector for SafePay operators is through vulnerabilities in edge devices, such as VPN gateways, firewalls, and Remote Desktop Gateway servers. Another common tactic for accessing an organization involves obtaining leaked credentials through phishing, initial access brokers, or public credential dumps.

Discovery

Once the SafePay operators have obtained initial access to an environment, they immediately enumerate the network, SMB shares, and any other assets that can be accessed. Based on observed activity, SafePay consistently leverages ShareFinder.ps1 from the PowerTools collection.

Lateral movement

Living-off-the-land utilities such as PSExec, WinRM, RDP, and RMM software are the primary means of navigating an organization’s network.

Defense evasion

Commonly observed by ransomware groups, SafePay will attempt to disrupt security services, eliminate backup software, and halt the Volume Shadow Copy service. SafePay will also perform privilege escalation through token impersonation if needed.

Exfiltration

SafePay is known to use the following applications for exfiltrating data: WinRAR, 7-Zip, Rclone, FileZilla, and the RDP clipboard.

Impact

Once the Shadow Copy service is stopped, shadow copies and any third-party backups are silently deleted. This severely limits recovery options for affected organizations, forcing them to resort to offline backups which may be outdated or untested.

This group is known to utilize the double-extortion scheme, where organizations must pay for the decryption tool and then must pay to have their data removed from SafePay servers. Because of this, it is highly advised that organizations do not make any ransom payments.

Known ransomware samples

One of the easiest samples associated with SafePay had a language check kill-switch for any Cyrillic languages. This could indicate that an Eastern European state sponsor may have backed SafePay. The language check was removed in later samples of SafePay. Early samples exhibit numerous similarities to the leaked LockBit Black, and Hive ransomware. Despite inspiration from other groups, the encryptor SafePay leverages is likely developed independently.

SHA-256 Hashes

- A0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526
- fd509df74a8d6a9e96762337efd46280ebf8d154c6c5dfbac7b3e8f7bb61f191
- 625abbf876f256662f33a88c122bf787edf74b882c35adbd61562b5bd1b2ac27
- 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae
- 22df7d07369d206f8d5d02cf6d365e39dd9f3b5c454a8833d0017f4cf9c35177
- 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917
- 12139246b8c5232d6d074df37acddc20f0bc233e42ed8eb00dfe2af5d3de3275
- 241c3b02a8e7d5a2b9c99574c28200df2a0f8c8bd7ba4d262e6aa8ed1211ba1f
- 654c11935448b3229434ec7d9d165a5f135ae4735d35700cffcb3b84f6a0fbc3

- 961346470d15d7795c5e35bc90c17d293fba7a8b811f8f5c26a3dc7c971cdc4e

Mutexes

- Global\DB1D-19B4-5094-D570-9841-E4BC-8ABD-29AA-03BB-84AD-C61B-1355-4FF2-194B-96BD-7E49
- Global\347F-7B6B-6AFB-3C55-2602-369D-65B9-58A0-16F1-0F42-35DA-0B37-52C3-293C-8975-CAB4
- Global\622D-BA6A-4BE9-5D15-5C84-898C-1760-4BAF-2BB1-D7D1-389D-6C01-AAFC-1645-BB6E-DC88
- Global\A8D1-50A2-679B-3D55-D639-9810-8679-7409-02EC-EF50-EA87-5641-0086-74B7-A14E-EE4C

How ThreatLocker can help

Application Allowlisting

ThreatLocker Application Allowlisting can block applications that are not explicitly permitted by ThreatLocker or learned during the learning process, such as unauthorized Remote Management and Management applications.

Additional explicit deny policies can be created to prevent the usage of high-risk applications, such as MSBuild, or PSExec.

For applications that are high-risk, but are required by business processes, permit policies with Ringfencing™ can be utilized to restrict what resources applications can interact with, such as certain files, internet access, the registry, or executing other applications.

Network Control

ThreatLocker can limit ransomware operators from accessing your organization network by utilizing Network Control to block non-ThreatLocker monitored devices from accessing resources such as Remote Desktop, Windows Remote Management shell, and PSexec from the edge VPN or firewall.

Detect and MDR

ThreatLocker Detect can detect and alert your organization or the ThreatLocker MDR team to possible ransomware operators' tactics and procedures, including installing ransomware tools, attempting to disable security services, deleting shadow copies, and performing data exfiltration.

Want to learn how ThreatLocker protects environments?

Schedule a demo to see how a prevention-first approach can lock down your most valuable assets

---