blackpoint

THREAT PROFILE:

SafePay Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2024

Operation style:
Likely private operation

Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:

- Industrials (Manufacturing)

Most frequently targeted victim HQ region:

- North America

Known Associations:

- BlackSuit Ransomware
- Conti Ransomware
- INC Ransom Ransomware
- LockBit Ransomware
- Lynx Ransomware

INITIAL ACCESS	PERSISTENCE	LATERAL MOVEMENT
Valid accounts, vulnerability exploitation; social engineering (MITRE ATT&CK: T1078, T1190, T1566)	External remote services; create or modify system processes (MITRE ATT&CK: T1133, T1543)	Remote Services (MITRE ATT&CK: T1021)

Description

SafePay Ransomware was first identified in October 2024 and operates in the double extortion method - which combines the standard encryption method with data theft and the threat of leaking or selling the data if the ransom demand is not paid.

SafePay Ransomware has been assessed to be built using the LockBit 3.0 leaked builder. However, there are also reports of the group utilizing a backdoor, QDoor, that has previously been linked to the BlackSuit Ransomware operation and using the same living-off-the-land binaries (LOLBins) as the INC Ransom Ransomware operation. These observations highlight the interconnectedness of ransomware operations and reinforce the need for intelligence driven, proactive defense strategies.

SafePay has been reported to gain initial access via valid accounts and exploiting public-facing applications. These tactics have been reported to include targeting misconfigured Fortinet firewalls, exposed remote desktop protocol (RDP) instances, and using valid credentials to access virtual private network (VPN) accounts that do not have multi-factor authentication (MFA) enabled.

SafePay has also been reported to send thousands of spam email messages to victims and follow up by using Microsoft Teams to contact employees. The group reportedly impersonates the victim organization's IT help desk and lures the victim into downloading remote access software, effectively providing the threat actors with access to the network.

Similar to other ransomware operations, SafePay has been reported to create new processes, utilize tools such as ScreenConnect, and backdoor malware to maintain persistence on targeted devices.

SafePay Ransomware is reportedly built using the leaked LockBit 3.0 builder.

SafePay has been reported to utilize RDP and SMB/Windows Admin Shares for lateral movement, which is in line with multiple other ransomware operations, including LockBit, Akira, and more.

SafePay Ransomware has been reported to utilize tools, like FileZilla and Rclone, for exfiltration. The group has been reported to demand between 1-3% of the victim organization's yearly revenue as the ransom demand.

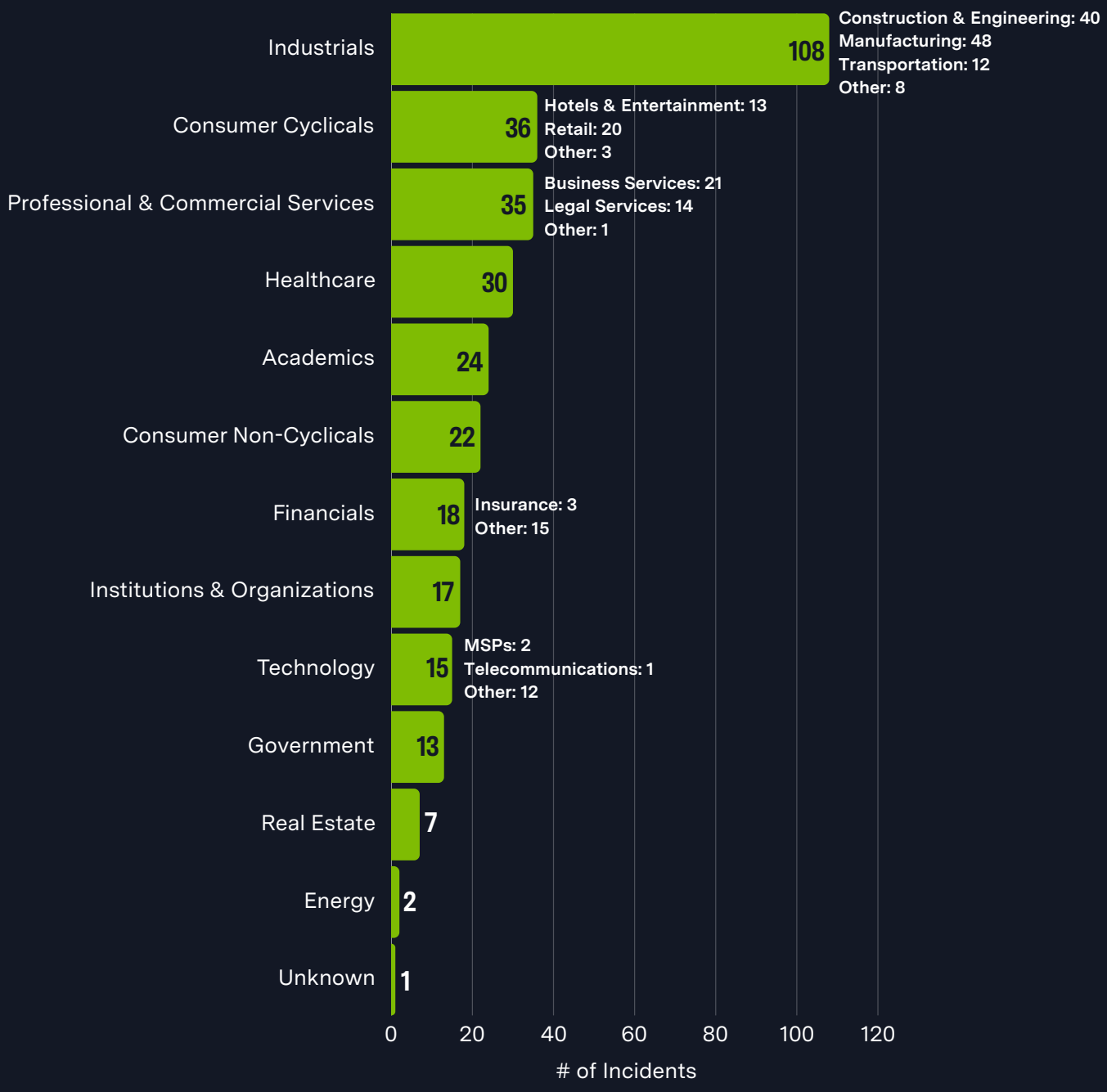
SafePay Ransomware likely operates in a similar manner to the LockBit 3.0 operation due to being built off the leaked builder. At the time of writing, there has been little public reporting related to the SafePay Ransomware operation; it is likely that SafePay will continue to target organizations worldwide over the next 12 months.

As additional information has become available related to the SafePay operation, additional connections between the group and other ransomware operations have been identified. Security researchers have assessed that SafePay's emergence and rapid success likely indicates that the group is comprised of sophisticated threat actors from various established operations - including Akira, Play, Qilin, and more.

This level of overlap makes attribution to specific threat groups and individuals more difficult and highlights the extensive interconnectedness of the ransomware landscape.

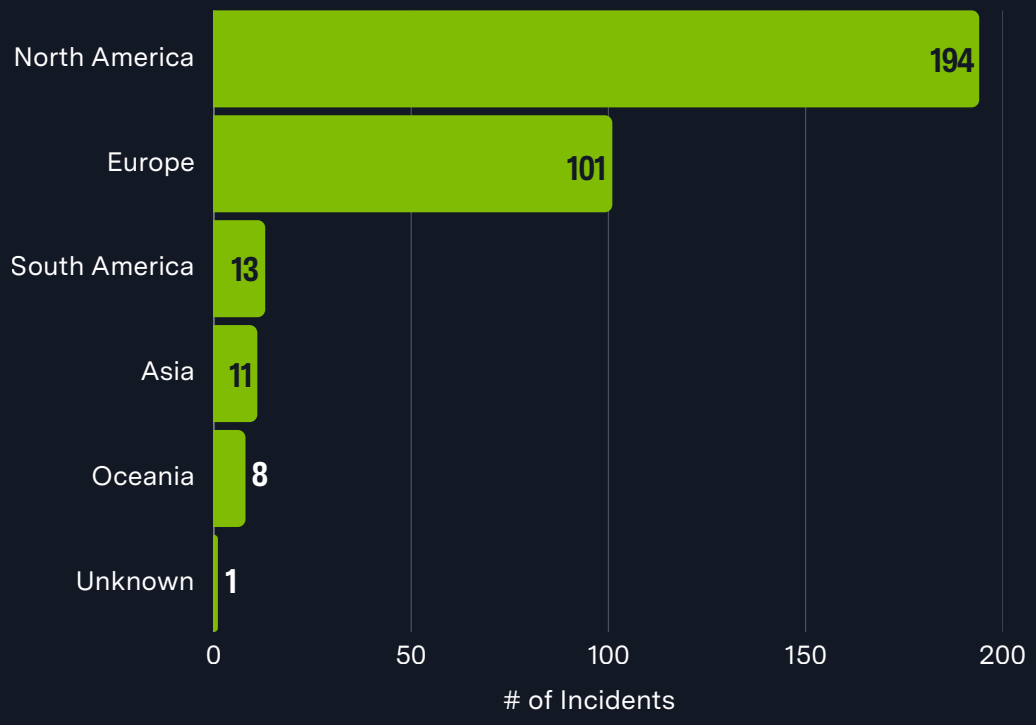
Previous Targets

Previous Industry Targets from 01 Oct 2024 to 30 Sep 2025

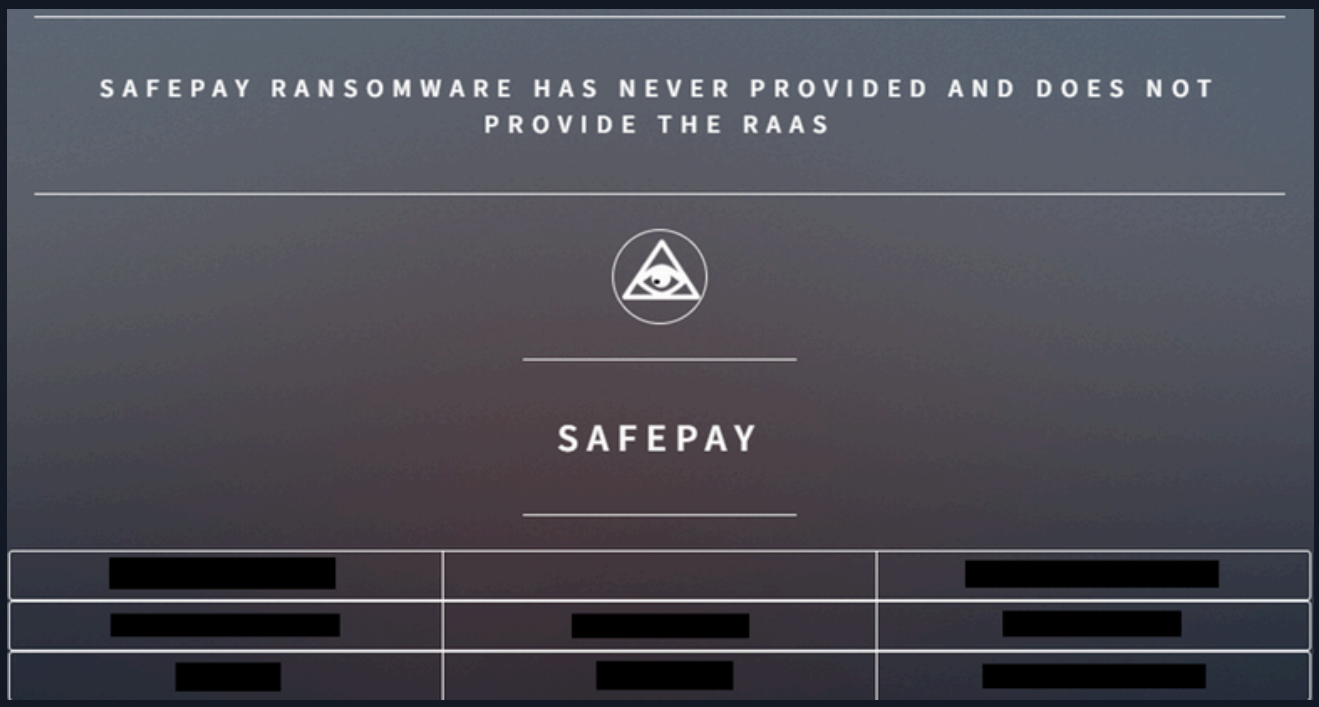


Previous Targets

Previous Victim HQ Regions from 01 Oct 2024 to 30 Sep 2025



Data Leak Site



hxxp://j3dp6okmaklajrsk6zljl5sfa2vpui7j2w6cwmhmmqhab6frdfbphhid[.]onion/

Associations

BlackSuit Ransomware

Security researchers identified that the backdoor, QDoor, observed in a SafePay Ransomware incident was potentially attributed to BlackSuit Ransomware, indicating there is an even chance the two groups have cooperated in some way. However, the level of relationship is not known.

Conti Ransomware

Security researchers have reported that the SafePay Ransomware is likely linked to former Conti members based on their TTPs, overlaps in tooling, and other long-established Conti behaviors.

INC Ransom Ransomware

SafePay Ransomware operators have been reported to use the same LOLBin commands observed during an INC Ransom deployment that has been previously reported, including the use of a PowerShell script, ShareFinder.ps1.

LockBit Ransomware

SafePay Ransomware is purportedly built using the LockBit 3.0 Ransomware builder that has previously been leaked. Therefore, SafePay has been purported to operate in a similar manner to the LockBit 3.0 Ransomware variant.

Lynx Ransomware

Security researchers have reported that INC Ransom, SafePay, and Lynx likely operate in a triad model, sharing group members, TTPs, and even cross-posting victims.

Known Tools

7zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
bcdedit	A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options.
FileZilla	A free open-source file transfer protocol software tool tat allows users to set up FTP servers or connect to other FTP servers to exchange files.
Microsoft Teams	A instant messaging app that has been abused by malicious actors to impersonate victims' IT staff or help desk and deliver social engineering attacks that facilitated malware attacks.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerView	A PowerShell tool used to gain network situational awareness of Windows domains.
ProtonMail	A free and secure email service that allows users to remain anonymous. It has been used by threat actors to create email addresses that can be used in social engineering attacks.
PsExec	A command-line utility that allows users to execute processes on remote systems; it is part of the Sysinternals suite and is frequently used by system admins for remote management tasks. The tool is also repeatedly abused by threat actors for lateral movement and remote execute.
QDoor	A backdoor malware that allows attackers to maintain persistent access to compromised systems and potentially exfiltrate data. It establishes a connection between the attacker's command and control server and a target machine, effectively creating a tunnel for traffic to be proxied.
QuickAssist	A RMM tool that threat actors have been reported to abuse for initial access and persistence.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.

Known Tools

RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection. This is frequently used by threat actors for initial access and lateral movement.
REgsvr32	A command line utility in Microsoft Windows used to register and unregister OLE controls. The is often utilized to execute malicious executables.
Rundll32	A command line utility in Microsoft Windows used to run DLLs on the Windows operating system.
RunPE	A publicly available tool that creates a new process in a suspended state and injects the process with the content of an embedded executable using standard process hollowing techniques.
ScreenConnect	AKA ConnectWise. A self-hosted remote desktop software application that can be used to remotely access victim environments.
ShareFinder	A family of tools used for network share discovery and enumeration in Windows networks, especially within Active Directory.
TON	The Open Network (formerly Telegram Open Network). A decentralized and open internet platform that includes various components such as the TON Blockchain, TON DNS, TON Storage and TON Sites. TON was created by the Telegram team.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes. The is frequently used by ransomware operators to delete shadow copies.
Windows Settings GUI	Windows settings that has been reported to be abused by threat actors to disable some Windows Defender settings.
WinRAR	A trialware file archiver utility for Windows devices that can backup data and reduce the size of email attachments, open and unpack RAR, ZIP and other files downloaded from Internet, and create new archives in RAR and ZIP file format.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Behaviors: Windows

Tactic	Commands Observed
Execution	"C:\Windows\SysWOW64\regsvr32.exe" /n "/i:-pass=[REDACTED] -enc=3 -uac -path=\\[REDACTED]\[SHARE]\ -uac=[REDACTED]" C:\locker.dll C:\ProgramData\<single digit>.bat
Persistence	CreateThread ThreadHideFromDebugger ZwSetInformationThread NtResumeThread
Privilege Escalation	SeDebugPrivilege ZwOpenProcessToken LookupPrivilegeValueA PrivilegeCheck AdjustTokenPrivileges DuplicateToken CreateThread ThreadHideFromDebugger ZwSetInformationThread
Defense Evasion	C:\Windows\system32\cmd.exe /c "C:\Users\[redacted]\AppData\Local\Temp\Uninstall__Rar.Bat“ "C:\Windows\system32\regsvr32.exe" /s /u "C:\Program Files\FileZilla FTP Client\fzshellext_64.dll“ wmic shadowcopy delete vssadmin delete shadows /all / quiet bcdedit / set{default}bootstatuspolicy ZwTerminateaProcess ControlService
Discovery	GetSystemDefaultUILanguage
Lateral Movement	start C:\1.exe -pass=<string of characters> -path=\<location> -enc=1

Observed Behaviors: Windows

Tactic	Commands Observed
Collection	WinRAR.exe a -v5g -ed -r -tn1000d -m0 -mt5 -x*.rar -x*.JPEG -x*.RAW -x*.PSD -x*.TIFF -x*.BMP -x*.GIF -x*.JPG -x*.MOV -x*.pst -x*.FIT -x*.FIL -x*.mp4 -x*.avi -x*.mov -x*.mdb -x*.iso -x*.exe -x*.dll -x*.bak -x*.msg -x*.png -x*.zip -x*.ai -x*.7z -x*.DPM -x*.log -x*.dxf -x*.insp -x*.upd -x*.db -x*.dwg -x*.nc1 -x*.metadata -x*.dg -x*.inp -x*.dat -x*.TIFF -x*.tiger -x*.pcp -x*.rvt -x*.rws -x*.nwc -x*.tif -x*.frx -x*.dyf -x*.rcs -x*.diff C:\[redacted].rar \\[redacted]\C$\Users\
Impact	bcdedit /set {default} recoveryenabled no CryptGenRandom

MITRE ATT&CK® Mappings

Reconnaissance	
T1596: Search Open Technical Database	
T1589: Gather Victim Identity Information	
T1592: Gather Victim Host Information	
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment
Execution	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1204: User Execution	.002: Malicious File
Persistence	
T1133: External Remote Services	
T1543: Create or Modify System Process	.003: Windows Service
Privilege Escalation	
T1134: Access Token Manipulation	.001: Token Impersonation/Theft
T1543: Create or Modify System Process	.003: Windows Service

MITRE ATT&CK® Mappings

Privilege Escalation	
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
Defense Evasion	
T1027: Obfuscated Files or Information	.002: Software Packing
T1055: Process Injection	.012: Process Hollowing
T1070: Indicator Removal	.004: File Deletion
T1202: Indirect Command Execution	
T1562: Impair Defenses	.002: Disable Windows Event Logging
Credential Access	
T1003: OS Credential Dumping	
T1110: Brute Force	
Discovery	
T1012: Query Registry	
T1082: System Information Discovery	
T1135: Network Share Discovery	
T1614: System Location Discovery	.001: System Language Discovery

MITRE ATT&CK® Mappings

Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
Collection	
T1005: Data from Local System	
T1560: Archive Collected Data	.001: Archive via Utility
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1219: Remote Access Software	
Exfiltration	
T1048: Exfiltration Over Alternative Protocol	
Impact	
T1486: Data Encrypted for Impact	
T1490: Inhibit System Recovery	
T1531: Account Access Removal	
T1657: Financial Theft	

References

- Barry, Christine (2025, July 25) Barracuda: “SafePay: Email bombs, phone scams, and really big ransoms.” https://blog.barracuda.com/2025/07/25/safepay--email-bombs--phone-scams--and-really-big-ransoms
- Brown, Jade (2025, September 04) Bitdefender: “SafePay Ransomware: How a Non-RaaS Group Executes Rapid Fire Attacks.” https://www.bitdefender.com/en-us/blog/businessinsights/safepay-ransomware-attacks-ttps
- NCC Group (2025, April 02) “Weak Passwords Led to (SafePay) Ransomware…Yet Again.” https://www.nccgroup.com/us/research-blog/weak-passwords-led-to-safepay-ransomware-yet-again/
- Poireault, Kevin (2025, July 10) Infosecurity Magazine: “Unmasking the SafePay Ransomware Group.” https://www.infosecurity-magazine.com/news-features/unmasking-safepay-ransomware-group/
- Red Piranha (n.d.) “What is SafePay Ransomware? - Everything You Need to Know.” https://redpiranha.net/news/what-is-safepay-ransomware-everything-you-need-know
- Surefire Cyber (2024, November 15) “Emerging Threat Analysis: Profiling a New Ransomware Group, SafePay.” https://www.surefirecyber.com/emerging-threat-analysis-profiling-a-new-ransomware-group-safepay/
- WatchGuard (n.d.) “SafePay (Active).” https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/safepay

Adversary Pursuit Group

blackpoint