blackpoint

THREAT PROFILE:

SafePay Ransomware

TABLE OF CONTENTS

Executive Summary	2
Diamond Model	3
Description	4
Previous Targets: Industries & Regions	5
Data Leak Site	7
Associations	8
Known Tools	9
Observed Behaviors: Windows	11
Kill Chain	14
MITRE ATT&CK® Mappings	15
References	19

Executive Summary

First Identified:
2024

Operation style:
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, external remote services, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

External remote services, create or modify system processes, event triggered execution, boot or logon autostart execution (MITRE ATT&CK: T1133, T1543, T1546, T1547)

Remote service, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

Diamond Model

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.

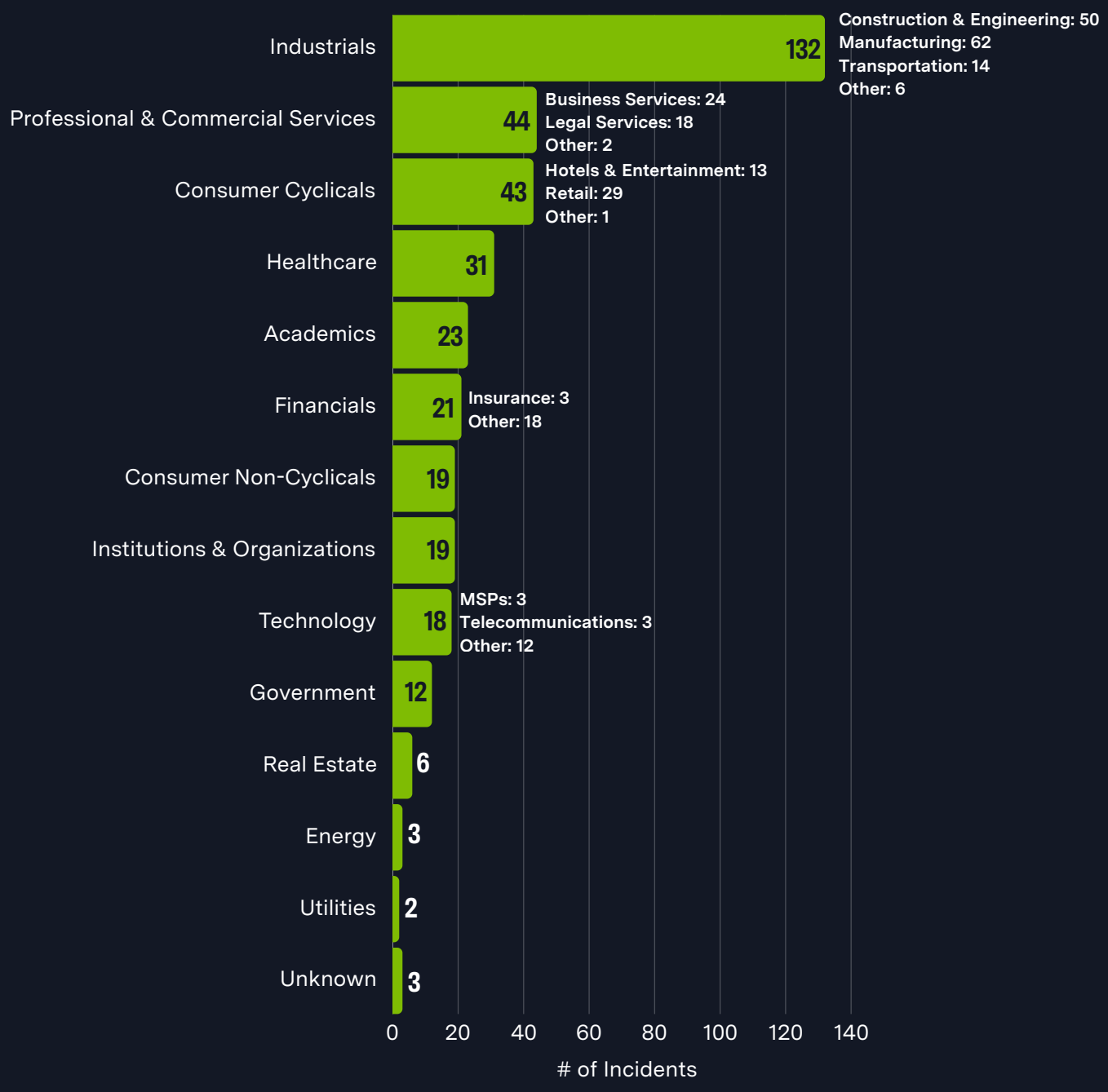
SafePay Ransomware likely operates in a similar manner to the LockBit 3.0 operation due to being built off the leaked builder. At the time of writing, there has been little public reporting related to the SafePay Ransomware operation; it is likely that SafePay will continue to target organizations worldwide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

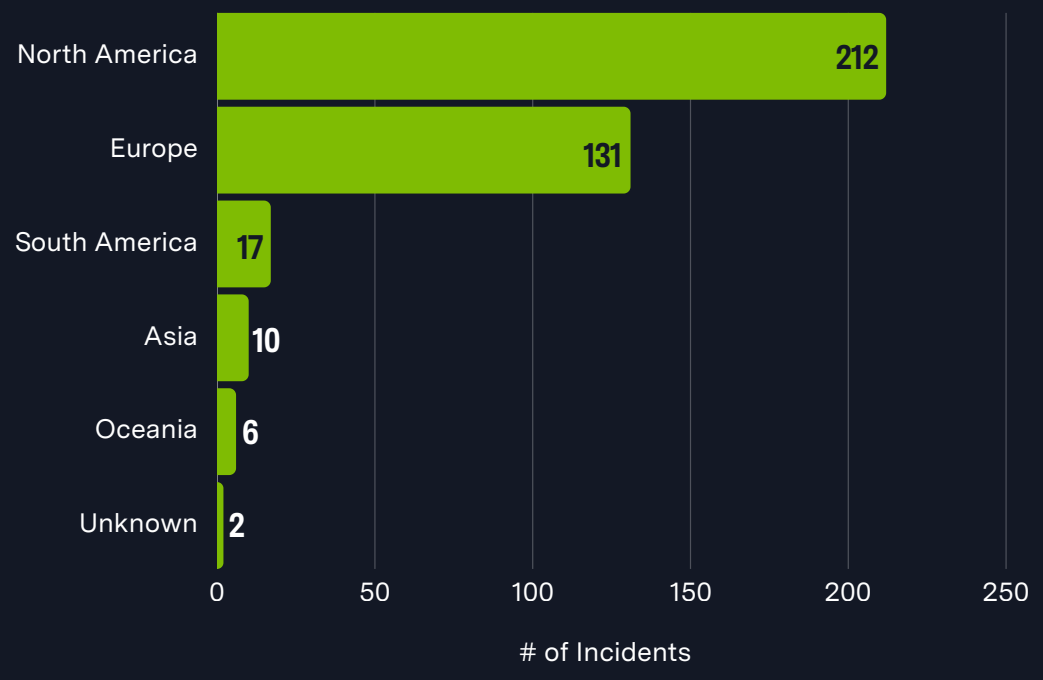
Previous Targets

Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

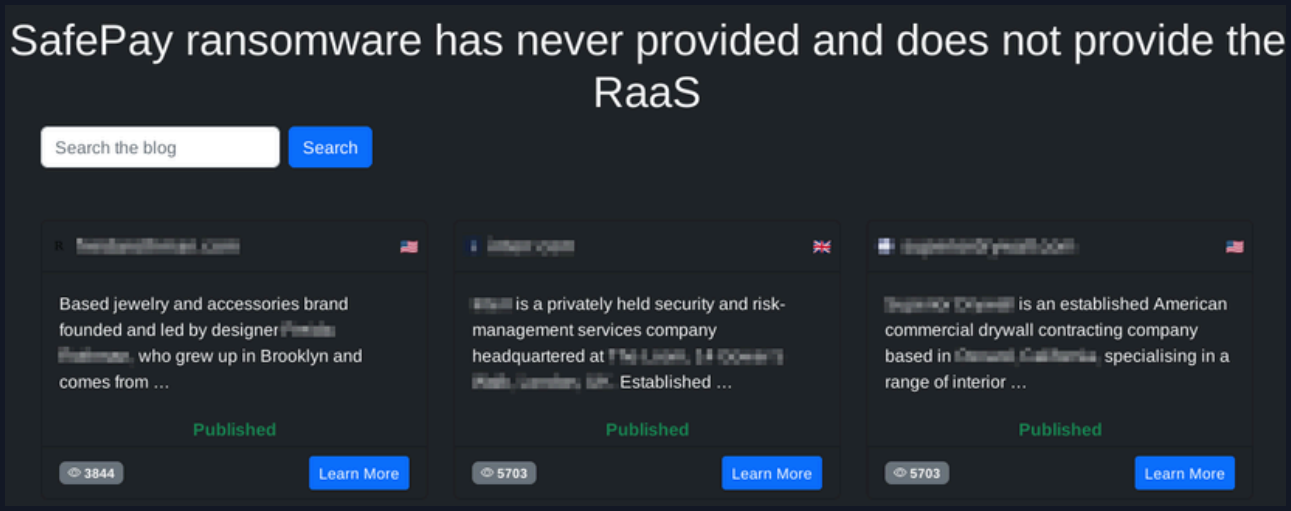


Previous Targets

Previous Victim HQ Regions from 01 Jan 2025 to 31 Dec 2025



Data Leak Site



hxxp[:]//j3dp6okmaklajrsk6zljl5sfa2vpui7j2w6cwmhmmqhab6frdfbphhid[.]onion/
hxxp[:]//nz4z6ruzcekriti5cjjiiylzvrmysyqwibxztk6voem4trtx7gstpjid[.]onion/
hxxp[:]//safepaypfxntwixwjrlcscft433ggemlhgkkdupi2ynhtcmvdgubmoyd[.]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

Function	Tool	Description
Initial Access	Microsoft Teams	Instant messaging app that is frequently abused for initial access via social engineering attacks.
Execution	CMSTP	Command line utility used to install or remote Connection Manager service profiles; frequently abused to execute malicious code.
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
	Regsvr32	Command line utility used to register and unregister OLE control; used to execute malicious code.
	WMI	Microsoft's framework for managing data and operations used to execute commands and queries remotely.
Persistence	QDoor	Backdoor malware that allows attackers to maintain persistent access to compromised systems.
	QuickAssist	RMM tool that has frequently been abused for intiail access and persistence.
	schtasks	Command line tool used to create, delete, run, manipulate, and query scheduled tasks.
	ScreenConnect	AKA ConnectWise. RMM tool that can be used to gain persistent remote access to victim environments.
Defense Evasion	bcdedit	Command line tool used to modify boot configuration data for system level changes.
	Rundll32	Windows utility used to load DLLs that lack an executable; used to bypass security controls.
	RunPE	Utility used for process hollowing to inject and execute portable executables (PE) files directly into memory.
	UPX	Open-source executable packer used to compress programs and DLLs.
	Windows Settings GUI	Central hub for customizing, configuring, and managing system preferences; used to evade detection.
Credential Access	Mimikatz	Hacktool used to extract Windows passwords in plain-text from memory.

Known Tools

Function	Tool	Description
Discovery	PowerView	Enumerates Active Directory relationships; used to map network shares, enumerate users/groups, and more.
	ShareFinder	Part of the PowerSploit framework; used to enumerate accessible network shares.
Lateral Movement	PsExec	Command line tool abused to execute a program on another computer.
	RDP	Microsoft protocol used to remotely connect to a Windows computer.
	WinRM	Windows utility that executes commands remotely via Windows Remote Management.
Command and Control	TON	The Open Network. A decentralized messaging/network platform used for anonymity and secure communications.
Exfiltration	FileZilla	File transfer protocol software tool that allows users to set up FTP servers or connect to other FTP servers to exchange files.
	Rclone	Command line program used to manage, sync, and transfer files.
	WinRAR	File archiver utility that can backup data, open and unpack RAR, ZIP, and other files from the internet; often used for exfiltrating sensitive data.
Impact	7-zip	Open-source file archiver used to compress, decompress, and encrypt files.
	VssAdmin	Command line tool abused to delete Volume Shadow Copy Service (VSS).
Infrastructure	ProtonMail	Free email service used to communicate with victims while remaining anonymous; can also be abused for initial access.
	TOR	Open-source software enabling anonymous malicious activities, such as command and control, operating data leak sites, and more.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	regsvr32.exe /n /i:"-pass=<redacted> -enc=3 -uac -path=\\<share>\ -uac= <redacted>" C:\locker.dll
	Output/Artifact	C:\ProgramData\<digit>.bat
Privilege Escalation	Command Execution	Token privilege manipulation via SeDebugPrivilege
		Process token access via ZwOpenProcessToken()
		Privilege lookup and validation via LookupPrivilegeValueA() / PrivilegeCheck()
		Token adjustment and duplication via AdjustTokenPrivileges() / DuplicateToken()
Defense Evasion	Command Execution	Execution of cleanup/uninstall script (Uninstall__Rar.bat)
		Unregister shell extension via regsvr32.exe /u fzshellext_64.dll
		Shadow copy deletion via wmic shadowcopy delete
		Shadow copy deletion via vssadmin delete shadows /all /quiet
		Process termination via ZwTerminateProcess()
		Service manipulation via ControlService()
		Anti-debugging / thread manipulation via CreateThread, ThreadHideFromDebugger, ZwSetInformationThread, NtResumeThread
	Configuration Change	Boot policy modification via bcdedit /set {default} bootstatuspolicy
Discovery	Command Execution	System locale discovery via GetSystemDefaultUILanguage()
Lateral Movement	Command Execution	SMB-based propagation using start C:\1.exe -pass=<string> -path=\\ <location> -enc=1
Collection	Command Execution	Selective data aggregation using WinRAR.exe with extensive file-type exclusions
		Collection from administrative share \\<redacted>\C$\Users\

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Impact	Command Execution	Cryptographic operations supporting encryption via CryptGenRandom()
	Configuration Change	Disable recovery via bcdedit /set {default} recoveryenabled no
	Output/Artifact	readme_SafePay.txt

Execution Parameters

Argument	Description
-pass	Password (32 bytes) to decode additional information in code.
-enc	Encryption percentage (1-9). Value is multiplied by 10 (e.g., 5 = 50%).
-network	Initiates network propagation to encrypt shared folders.
-selfdelete	Deletes the malware executable after encryption completes.

Kill Chain

Initial Access

- Compromised RDP/VPN
- Exploited Vulnerabilities
- Social Engineering Campaigns

Persistence

- Remote Access Software
- Valid Accounts
- Registry Keys and Scheduled Tasks

Defense Evasion

- Process Hollowing
- File Deletion
- Disable/Modify Tools
- UPX for Obfuscation

Lateral Movement

- SMB Share Mounts
- PsExec for Lateral Access
- RDP

Exfiltration

- Rclone/FileZilla data theft
- Archive staging of data to 7-zip
- WinRAR for encrypting and exfiltrating stolen data

Impact

- ChaCha8-based file encryption
- TOR-based leak site

MITRE ATT&CK® Mappings

Reconnaissance	
T1596: Search Open Technical Database	
T1589: Gather Victim Identity Information	
T1592: Gather Victim Host Information	
Privilege Escalation	
T1650: Acquire Access	
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment
Execution	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1072: Software Deployment Tools	
T1204: User Execution	.002: Malicious File
Persistence	
T1133: External Remote Services	
T1543: Create or Modify System Process	.003: Windows Service

MITRE ATT&CK® Mappings

Persistence	
T1546: Event Triggered Execution	.010: AppInit DLLs
T1547: Boot or Logon Autostart Execution	.010: Port Monitors
Privilege Escalation	
T1134: Access Token Manipulation	.001: Token Impersonation/Theft
T1543: Create or Modify System Process	.003: Windows Service
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	
T1218: System Binary Proxy Execution	.010: Regsvr32 .011: Rundll32
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
T1562: Impair Defenses	.001: Disable or Modify Tools .002: Disable Windows Event Logging
Credential Access	
T1003: OS Credential Dumping	

MITRE ATT&CK® Mappings

Credential Access	
T1110: Brute Force	
Discovery	
T1012: Query Registry	
T1018: Remote System Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1135: Network Share Discovery	
T1614: System Location Discovery	.001: System Language Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1560: Archive Collected Data	.001: Archive via Utility

MITRE ATT&CK® Mappings

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1105: Ingress Tool Transfer	
T1219: Remote Access Software	
T1573: Encrypted Channel	.001: Symmetric Cryptography
Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
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
- CloudSEK Editorial (2026, January 27) “SafePay Ransomware: Everything You Need to Know.” https://www.cloudsek.com/knowledge-base/safepay-ransomware
- Halcyon (n.d.) “SafePay.” https://www.halcyon.ai/threat-group/safepay
- Li, Rayton; Moutos, John (2025, July 31) ThreatLocker: “SafePay ransomware explained: IOCs, TTPs, and defense strategies.” https://www.threatlocker.com/blog/safepay-ransomware-explained-iocs-ttps-and-defense-strategies
- Morag, Assaf (2026, January 05) flare: “SafePay Ransomware: Mapping the Real Victims Behind the Leak Sites.” https://flare.io/learn/resources/safepay-ransomware-victims-analysis
- 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/
- Picus Labs (2026, January 07) “Inside SafePay: Analyzing the new Centralized Ransomware Group.” https://www.picussecurity.com/resource/blog/inside-safepay-analyzing-the-new-centralized-ransomware-group
- 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