blackpoint

THREAT PROFILE:

INC Ransom Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2023

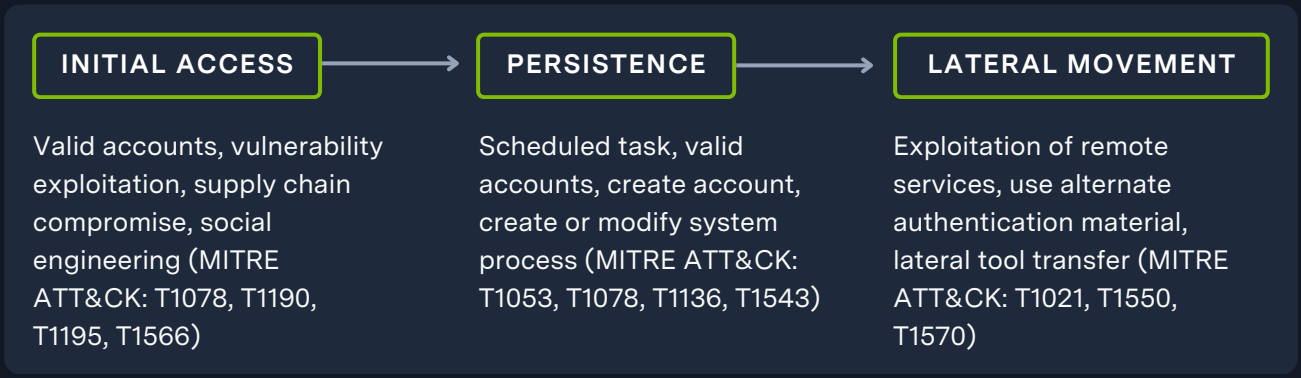
Operation style:
Ransomware-as-a-Service (RaaS)

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:
- GOLD IONIC
- Lynx Ransomware
- Tarnished Scorpius
- Water Anito



Diamond Model

Description

INC Ransom ransomware was first observed in July 2023 and operates in the double extortion method, where victim data is stolen and leaked via a data leak site if the ransom demand is not paid. The operators maintain a data leak site and a separate site for victims to negotiate the ransom payments.

INC Ransom operators have been observed gaining initial access via social engineering attacks and using valid credentials to target external remote services, such as RDP.

The initial behavior of the ransomware depends on the command line argument the operators enter. INC Ransom has been assessed to conduct a significant amount of reconnaissance on a victim organization, which likely allows the affiliate to choose the type of encryption they want to use.

Similar to other ransomware variants, INC Ransom deletes shadow copies and avoids certain files and directories when encrypting, which include .msi, .exe, .dll, .inc, Windows, Program Files, $RECYCLE.BIN, and appdata. INC Ransom uses multi-threading to speed up the encryption process, the number of threads will be the number of processors multiplied by 4. In order to speed up the encryption process, INC Ransom utilizes partial encryption.

- If the file is smaller than 1MB then the entire file will be encrypted.
- If the file is larger than 1MB but smaller than 3MB then 1MB will be encrypted and the rest will not be encrypted.
- If the file is larger than 3MB then encryption intervals of encrypting 1MB and not encrypting 2MB.

INC Ransom uses multi-threading to speed up the encryption process, the number of threads will be the number of processors multiplied by 4.

After setting the parameters, the ransomware decrypts its ransom notes. In each encrypted directory, the ransomware will drop two ransom notes, one as a .txt file and the other in .html format. Additionally, INC ransom actively seeks out available printers in the network and sends the command to print the ransom note. INC Ransom also has the ability to change the host background wallpaper image. INC Ransom changes the desktop wallpaper to display the ransom note.

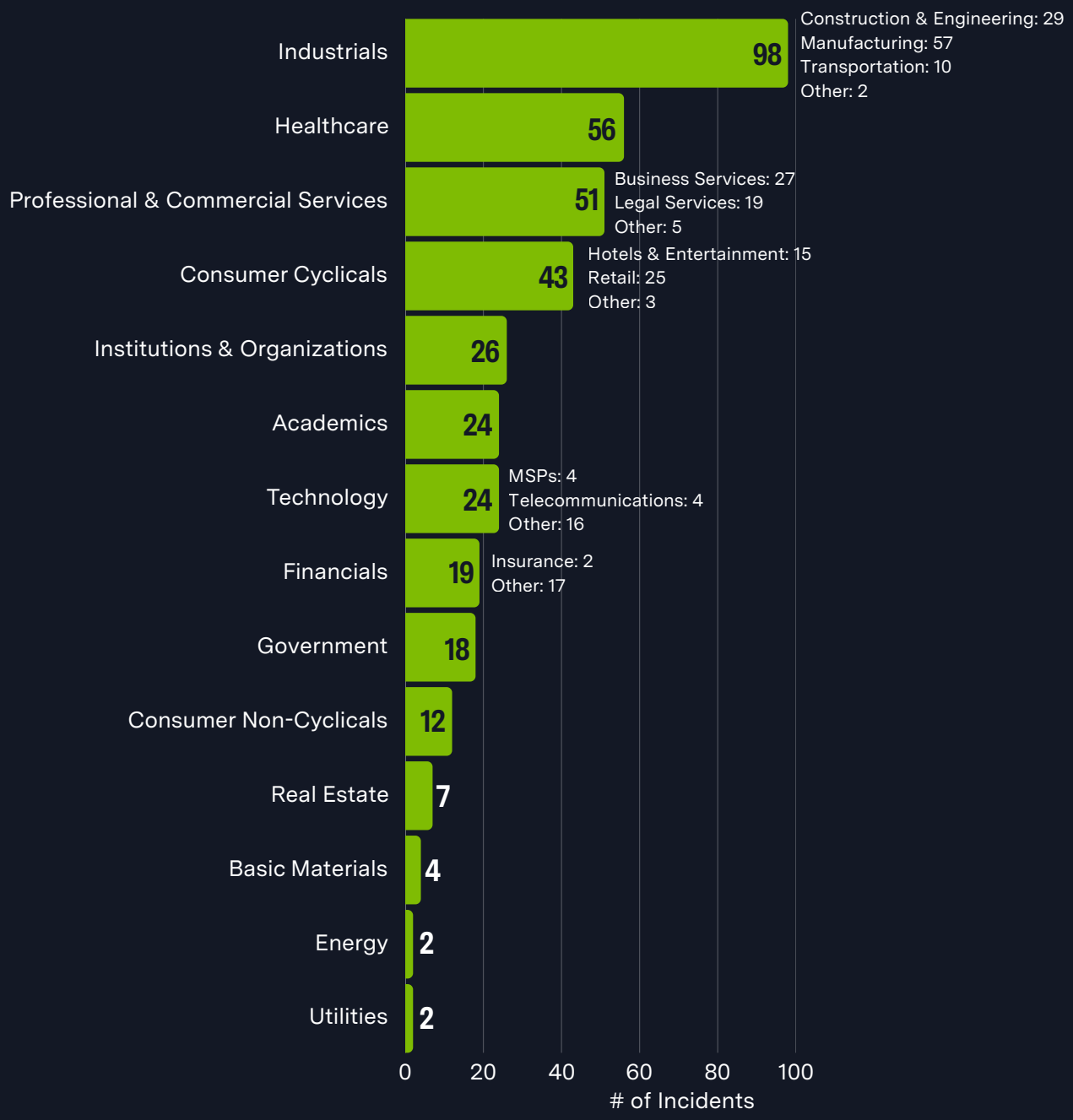
Security researchers have reported that INC Ransom and Lynx Ransomware variants have a significant overlap in code. Various security researchers have reported that the Windows variants have a 40% code similarity and a 70.8% similarity in specific functions, while the Linux variants have a 91% code similarity and a 87% overall overlap.

In 2024, INC Ransom operators listed their source code for sale on a dark web forums for $300,000. There is an even chance that Lynx operators purchased the source code and created their own variant.

INC Ransom has significantly increased their activity in 2025. INC Ransom listed 162 victims in 2024; and listed more than 300 so far in 2025. The increase in activity and their ability to remain a credible threat in the ransomware landscape has been attributed to their ability to adapt.

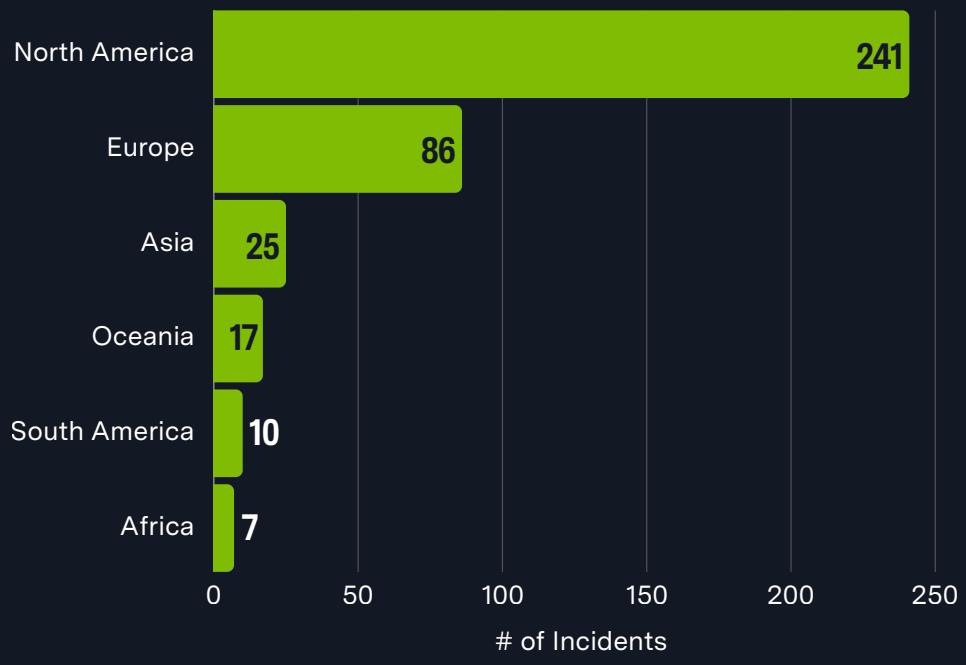
Previous Targets

Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

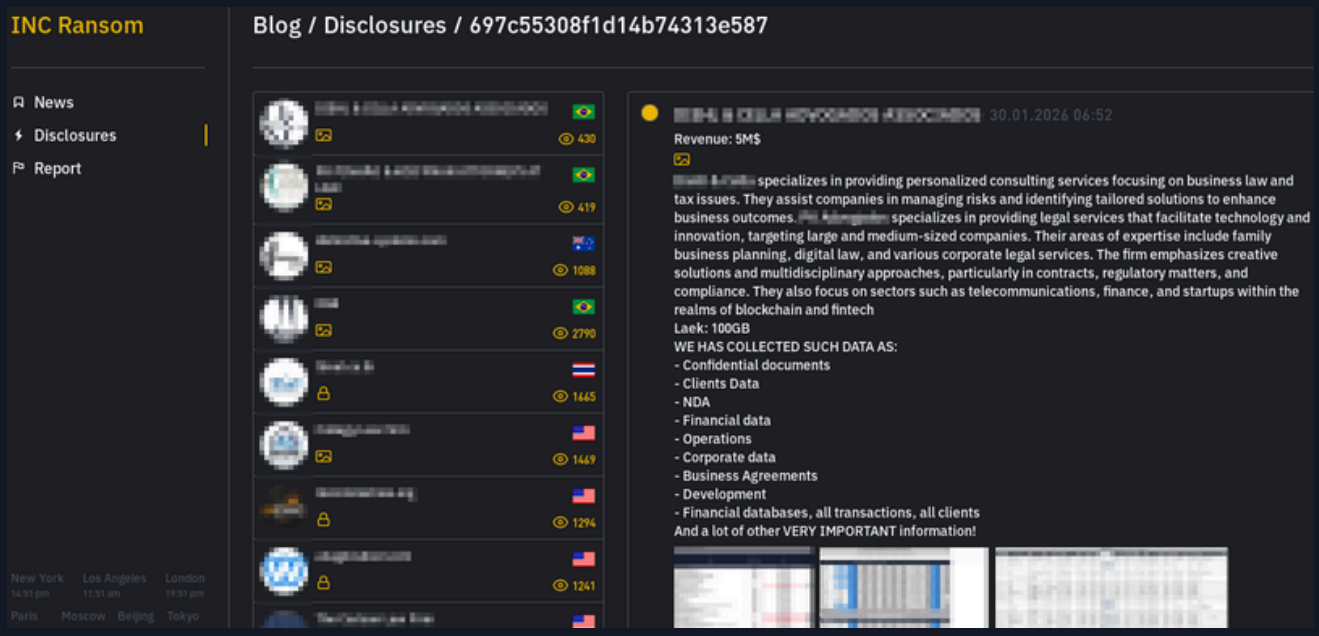


Previous Targets

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



Data Leak Site



hxxp://incapt[.]blog
hxxp://incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid[.]onion/blog/leaks

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CitrixBleed (CVE-2023-4966)	Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	7.5
CVE-2023-27997	Heap-Based Overflow Vulnerability	Fortinet FortiOS	9.8
CVE-2023-3519	RCE Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	9.8
CVE-2023-48788	SQL Injection Vulnerability	Fortinet FortiClient EMS	9.8
CVE-2024-57726	Privilege Escalation Vulnerability	SimpleHelp	9.9
CVE-2024-57727	Path Traversal Vulnerability	SimpleHelp	7.5
CVE-2024-57728	Arbitrary File Upload Vulnerability	SimpleHelp	7.2
CVE-2025-24472	Authentication Bypass Vulnerability	Fortinet FortiOS	8.1
Follina (CVE-2022-30190)	RCE Vulnerability	Microsoft Windows Support Diagnostic Tool (MSDT)	7.8

Associations

GOLD IONIC

INC Ransom operator group, tracked by Secureworks.

Lynx Ransomware

Security researchers have linked Lynx Ransomware to INC Ransom Ransomware based on behaviors and source code overlap. INC Ransom Ransomware listed their source code for sale on cybercriminal markets; there is an even chance that Lynx operators purchased the INC Ransom source code and created a new operation.

Tarnished Scorpius

INC Ransom operator group, tracked by Palo Alto.

Water Anito

INC Ransom operator group, tracked by Trend Micro.

Known Tools

Function	Tool	Description
Initial Access	Microsoft Support Diagnostic Tool (MSDT)	Legitimate Windows troubleshooting utility historically abused to execute malicious code or deliver payloads.
Execution	cmd	Utility used to execute commands on Windows systems.
	Meterpreter	Payload framework used for command execution, persistence, and post-exploitation activities.
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
	WMIC	Windows command-line tool used to execute commands and interact with systems remotely.
Persistence	AnyDesk	Remote access tool abused for persistent access.
	SystemSettingsAdminFlows.exe	Windows component abused to trigger elevated execution and maintain persistence mechanisms.
	TightVNC	Remote desktop tool that can be installed to maintain attacker-controlled access.
Privilege Escalation	Process Hacker	Administrative tool capable of manipulating processes, tokens, and services for privilege escalation.
	Service Control Manager	Windows service management utility used to create or modify services with elevated privileges.
Defense Evasion	Process Terminator	Utility used to kill processes, including security or monitoring software.
	wevutil	Windows event log utility used to clear or manipulate logs to hide attacker activity.
	Windows Restart Manager	Legitimate API abused to terminate processes and bypass defenses protecting files or services.
Credential Access	LSASSY.py	Python-based tool used to dump credentials from LSASS remotely.
	Mimikatz	Credential harvesting tool used to extract passwords, hashes, and Kerberos tickets from memory.

Known Tools

Function	Tool	Description
Credential Access	VeeamCreds	Utility used to extract stored credentials from Veeam backup software environments.
Discovery	Adfind	Active Directory reconnaissance tool used to enumerate users, groups, and domain structure.
	AdRecon	PowerShell-based tool for collecting detailed Active Directory environment information.
	Advanced IP Scanner	Network scanning utility used to identify hosts and shared resources.
	Internet Explorer	A legacy browser that has been abused to view folders on other systems.
	net	Windows networking command used to enumerate users, shares, and domain resources.
	nltest	Windows command-line utility used to enumerate domain controllers and trust relationships.
	SoftPerfect NetScan	Network scanning tool used to discover hosts, ports, and services in the environment.
Lateral Movement	MSTSC	Microsoft Terminal Service Client. Remote Desktop client used for interactive lateral movement between hosts.
	PsExec	Sysinternals tool used to execute commands remotely on other systems.
	PuTTY	SSH/Telnet client used to access remote systems or pivot through compromised infrastructure.
	RDP	Protocol used by attackers to access systems remotely and move laterally.
Collection	MSPaint	Utility occasionally used to open image files during manual data review.
	NotePad	Simple text editor used to view and collect text artifacts such as logs and configuration files.

Known Tools

Function	Tool	Description
Collection	WordPad	Document viewer sometimes used to open or review collected documents.
Exfiltration	MEGASync	Client used to synchronize stolen data with MEGA cloud storage accounts.
	Rclone	Command-line tool commonly used by ransomware operators to transfer large volumes of data to cloud storage.
	Restic	Backup tool abused to stage and transfer collected data to attacker-controlled repositories.
Impact	7-zip	File archiving tool used to compress data prior to exfiltration or staging.
	esentutil	Windows database utility abused to copy locked files such as Active Directory databases.
	VssAdmin	Windows utility used to delete shadow copies and backups before ransomware deployment.
	WinRAR	Compression utility used to package stolen files for exfiltration.
Infrastructure	TOR	Anonymous network used for ransomware negotiation portals, leak sites, and attacker communication infrastructure.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	Remote command execution using wmic /node:"<node>" process call create to copy and run ransomware payloads on remote systems.
		Lateral execution using psexec.exe \\<node> -u <user> -p <password> -s to deploy the ransomware payload.
		Encoded payload decoding and execution via CryptStringToBinaryA.
Persistence	Configuration Change	Creation of Windows service dmksvc used to maintain persistence on compromised systems.
		Creation of new local or domain user accounts to maintain administrative access.
Defense Evasion	Command Execution	Kernel interaction via DeviceIoControl using control code 0x53C028.
		Security or monitoring processes terminated using TerminateProcess.
Discovery	Command Execution	Drive enumeration via GetDriveTypeW to identify available storage volumes.
		Domain administrator enumeration using net group "domain admins" /domain.
		Domain controller and trust enumeration using nltest.exe.
Collection	Command Execution	Data archived for staging using 7.exe a -mx3 with exclusions for media and executable file types.
	Output/Artifact	Creation of compressed archive files containing staged victim data prior to encryption or exfiltration.
Impact	Command Execution	Removal of volume shadow copies using utilities such as vssadmin delete shadows to prevent recovery.
		Encryption of local and network files using configurable ransomware parameters.
	Configuration Change	Forced Safe Mode execution to terminate processes and services prior to encryption operations.

Arguments: Windows

Category	Argument	Description
Impact	--file	Encrypts a specific file.
	--dir	Encrypts a specified directory.
	--ens	Enables encryption of network shares.
	--lhd	Encrypts hidden and recovery volumes.
Configuration	--mode	Selects encryption mode or speed (fast / medium / slow).
Process	--sup	Stops targeted processes before encryption.
	--safe-mode	Terminates processes/services matching defined masks.
	--kill	Forces the system to reboot into Safe Mode before encryption.
Defense Evasion	--hide	Hides the ransomware console window during execution.
Operational	--debug	Displays debug logs during execution.
	--help	Displays available execution arguments.

Arguments: Linux

Category	Argument	Description
Persistence	--daemon	Executes the ransomware as a background daemon process.
Defense Evasion	--skip	Anti-analysis behavior enabled to avoid virtualized environments.
Impact	--motd	Modifies the system message of the day (MOTD) to display the ransom mesage.

Kill Chain

Initial Access

- Phishing attachments
- Exploited public services
- Stolen credentials

Persistence

- Remote access tools
- New admin accounts
- Malicious services

Defense Evasion

- Security tool termination
- Hidden execution
- Log clearing

Lateral Movement

- PsExec deployment
- RDP sessions
- WMI execution

Exfiltration

- Data staging archives
- Cloud sync tools
- Large file transfers

Impact

- File encryption
- Network share encryption
- Shadow copy deletion

MITRE ATT&CK® Mappings

Reconnaissance	
T1598: Phishing for Information	
Resource Development	
T1586: Compromise Accounts	
T1588: Obtain Capabilities	.002: Tool .007: Artificial Intelligence
T1650: Acquire Infrastructure	
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts
T1190: Exploit Public-Facing Application	
T1195: Supply Chain Compromise	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	

MITRE ATT&CK® Mappings

Execution	
T1203: Exploitation for Client Execution	
T1204: User Execution	.001: Malicious Link
T1569: System Services	.002: Service Execution
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts
T1543: Create or Modify System Process	
Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts
Defense Evasion	
T1027: Obfuscated Files or Information	.010: Command Obfuscation .014: Polymorphic Code
T1036: Masquerading	.005: Match Legitimate Name or Location
T1070: Indicator Removal	.004: File Deletion
T1112: Modify Registry	

MITRE ATT&CK® Mappings

Defense Evasion	
T1140: Deobfuscate/Decode Files or Information	
T1550: Use Alternate Authentication Material	.002: Pass the Hash
T1562: Impair Defenses	.001: Disable or Modify Tools .009: Safe Boot Mode
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .002: Security Account Manager
T1110: Brute Force	.004: Credential Stuffing
T1212: Exploitation for Credential Access	
T1558: Steal or Forge Kerberos Tickets	.003: Kerberoasting
Discovery	
T1007: System Service Discovery	
T1016: System Network Configuration Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1049: System Network Connections Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups

MITRE ATT&CK® Mappings

Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account
T1120: Peripheral Device Discovery	
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1652: Device Driver Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares
T1550: Use Alternate Authentication Material	.002: Pass the Hash
T1570: Lateral Tool Transfer	
Collection	
T1005: Data From Local System	
T1074: Data Staged	
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	.002: Remote Desktop Software
T1573: Encrypted Channel	
Exfiltration	
T1041: Exfiltration Over C2 Channel	
T1537: Transfer Data to Cloud Account	
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage
Impact	
T1485: Data Destruction	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1491: Defacement	.001: Internal Defacement
T1498: Network Denial of Service	
T1657: Financial Theft	

References

- Chassignol, Florent (2025, August 2025) SOS Ransomware: “INC Ransom: anatomy and solutions for a major threat in 2025.” https://sosransomware.com/en/ransomware-groups/inc-ransom-anatomy-and-solutions-for-a-major-threat-in-2025/
- Counter Threat Unit Research Team (2024, April 15) Secureworks: “GOLD IONIC Deploys INC Ransomware.” https://www.secureworks.com/blog/gold-ionic-deploys-inc-ransomware
- HC3 (2024, April 05) “HC3’s Top 10 Most Active Ransomware Groups.” https://www.hhs.gov/sites/default/files/hc3-top-10-most-active-ransomware-groups-analyst-note-tlpclear-r.pdf
- MITRE (2024, October 28) “INC Ransomware.” https://attack.mitre.org/software/S1139/
- MITRE (2024, October 28) “INC Ransom.” https://attack.mitre.org/groups/G1032/
- Montini, Heloise (2024, February 09) SalvageData: “INC. Ransom: Complete Guide on the new Cyber Threat.” https://www.salvagedata.com/inc-ransom-malware-threat/
- MOXFIVE (2025, September 04) “MOXFIVE Threat Actor Spotlight - INC Ransom.” https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-inc-ransom
- Palacios, Jayden (2025, October 21) Morado: “Preventable Paths: How INC Ransomware Continues to Thrive.” https://www.morado.io/blog-posts/preventable-paths-how-inc-ransomware-continues-to-thrive
- Popelov, Marina; Salem, Eli; Alon, Laufer; Mark Tsipershtein (n.d.) Cybereason: “THREAT ALERT: INC Ransomware.” https://www.cybereason.com/hubfs/dam/collateral/reports/threat-alert-inc-ransomware.pdf
- Sectrio (n.d.) “Anatomy of a Ransomware Attack: INC Ransom Breaches Yamaha.” https://sectrio.com/blog/inc-ransom-breaches-yamaha/
- SentinelOne (n.d.) “Inc. Ransom.” https://www.sentinelone.com/anthology/inc-ransom/
- SOCRadar (2024, January 24) “Dark Web Profile: INC Ransom.” https://socradar.io/dark-web-profile-inc-ransom/
- Trend Research (2024, October 29) “Ransomware Spotlight: INC.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-inc

Adversary Pursuit Group

blackpoint