blackpoint

THREAT PROFILE:

INC Ransom Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2023

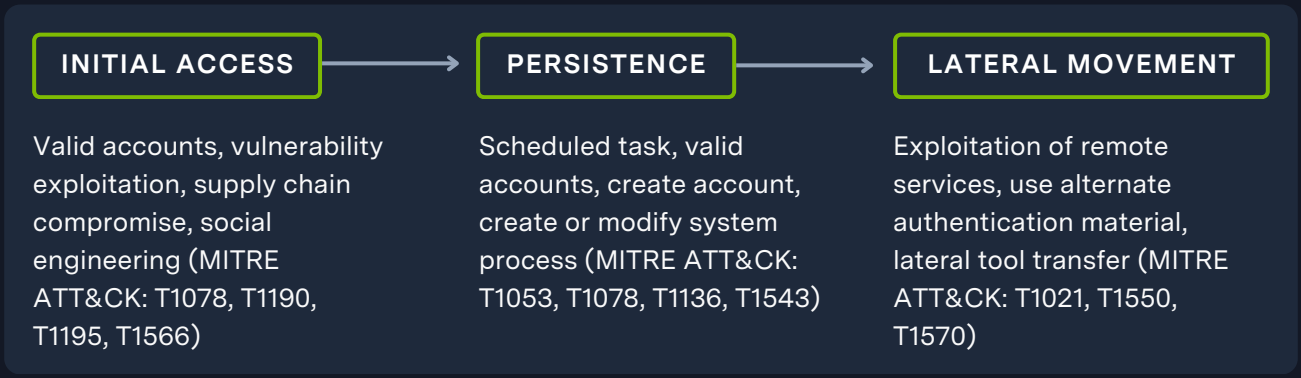
Operation style:
Ransomware-as-a-Service (RaaS)

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:
- Healthcare

Most frequently targeted victim HQ region:
- North America

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



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.

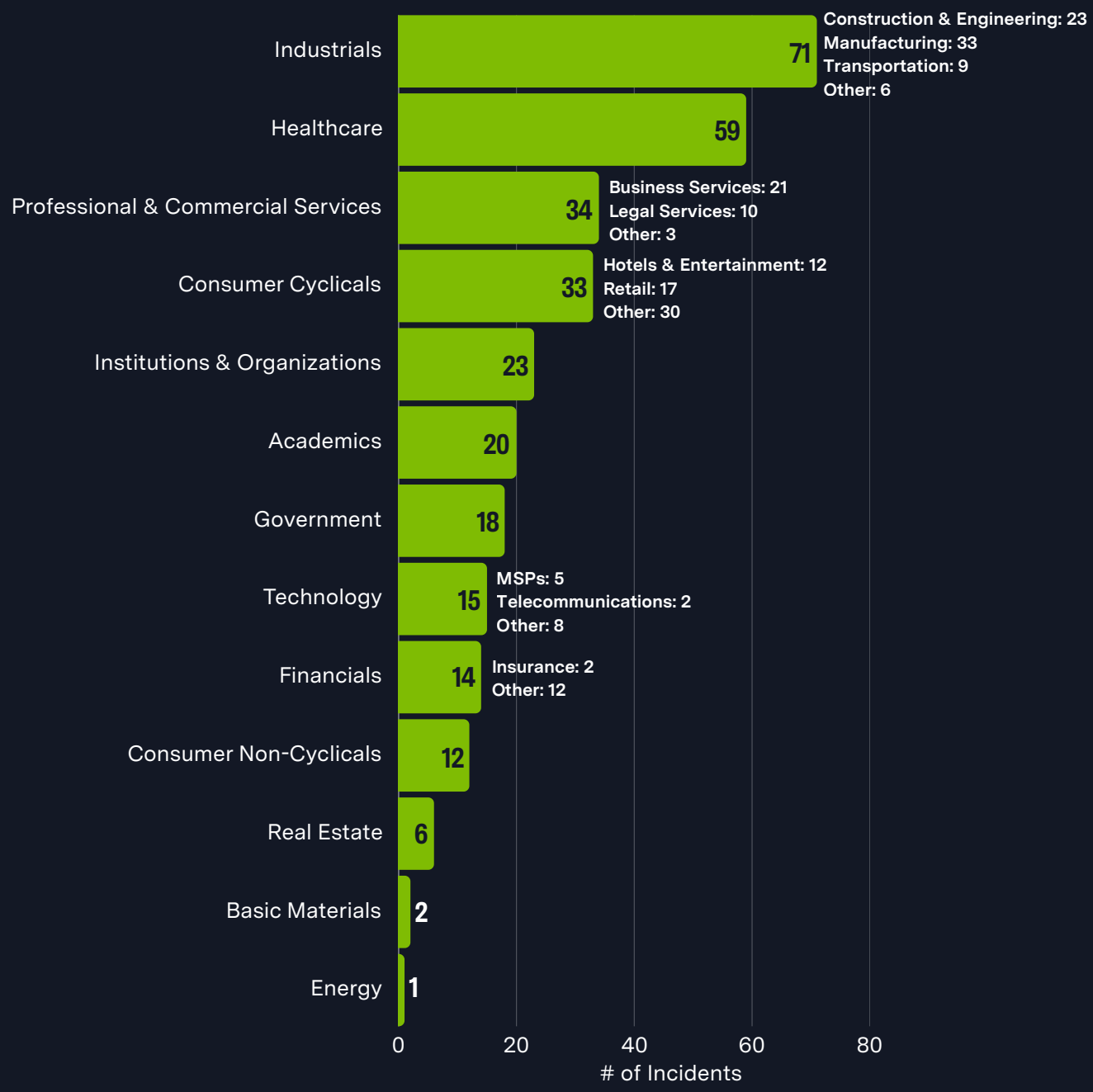
Security researchers have reported that INC Ransom and Lynx Ransomware variants have a significant overlap in code. Various security researchers have reported that the Windows variants have a 40% code similarity and a 70.8% similarity in specific functions, while the Linux variants have a 91% code similarity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

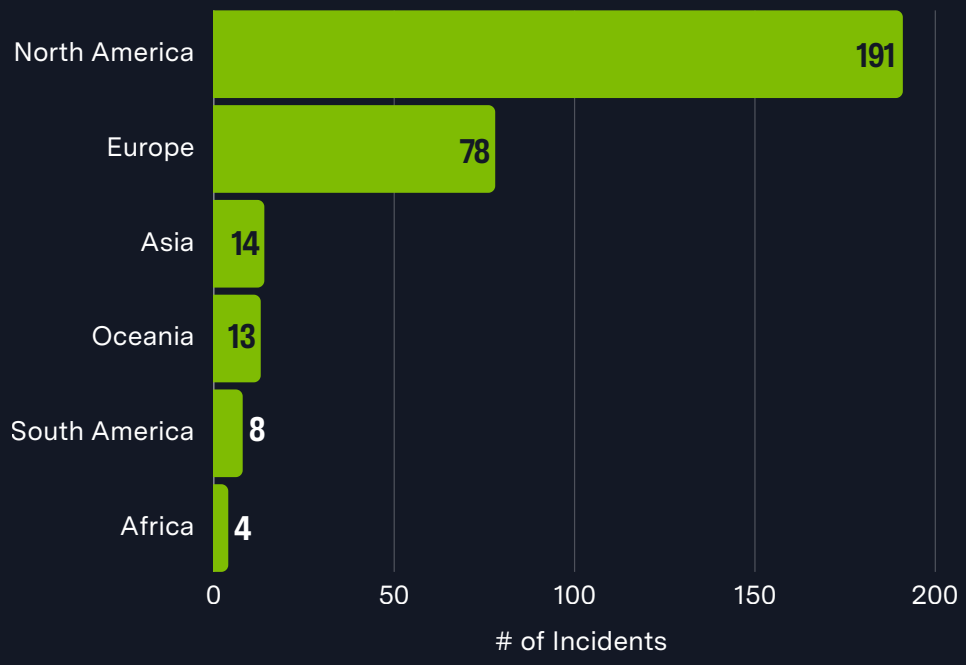
Previous Targets

Previous Industry Targets from 01 Oct 2024 to 30 Sep 2025

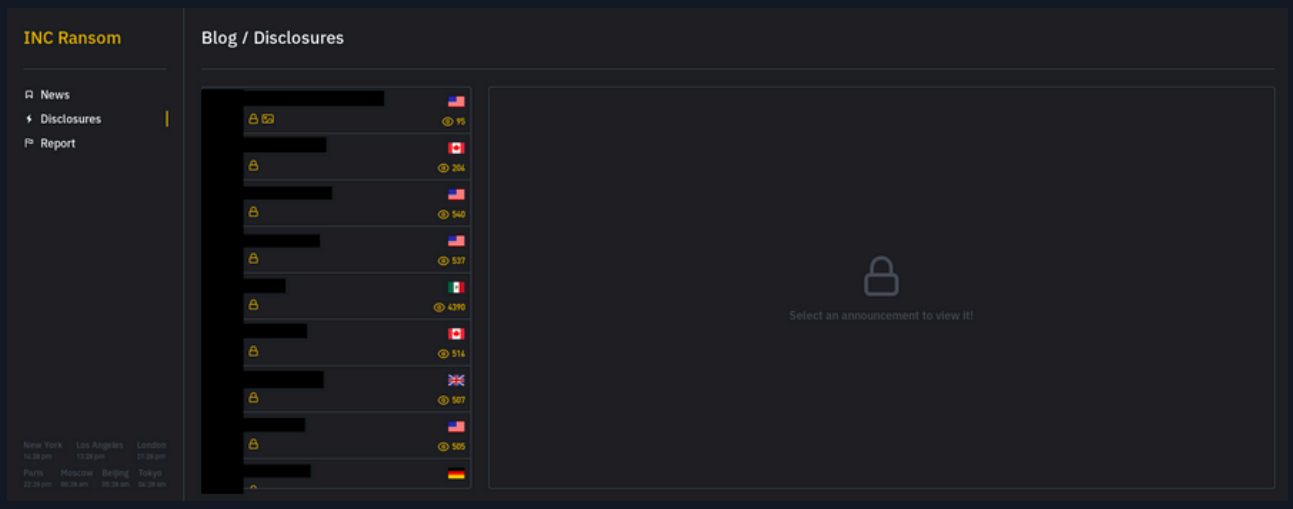


Previous Targets

Previous Victim HQ Regions from 01 Oct 2024 to 30 Sep 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

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

7-zip	A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration.
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
cmd	A program used to execute commands on a Windows computer.
esentutl	A command-line tool that provides database utilities for the Windows Extensible Storage Engine. It can be used to collect sensitive information.
Internet Explorer	A retired series of graphical web browsers developed by Microsoft that were used in the Windows line of operating systems.
LSASSY.py	A Python tool to remotely extract credentials on a set of hosts.
MEGASync	A cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.
Meterpreter	Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
MSDT	Microsoft Support Diagnostic Tool (MSDT) is a legacy service in Microsoft Windows that allows users to analyze diagnostic data remotely.
MSPaint	A simple raster graphics editor that has been included with all versions of Microsoft Windows. The program opens, modifies and saves image files in Windows bitmap, JPEG, GIF, PNG, and single-page TIFF formats.

Known Tools

MSTSC	Microsoft Terminal Service Client. A Windows utility that creates connections to Remote Desktop Session Host servers or other remote computers and edits an existing Remote Desktop Connection configuration file.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
NetScan	A utility that scans within a subnet or IP range to check for devices.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.
Notepad	A simple text editor for Windows; it creates and edits plain text documents.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
Process Hacker	An open-source tool that allows users to see what processes are running on a device and identify network connections that are associated with a process.
Process Terminator	A tool designed to terminate running processes. The tool has been reported to be used by ransomware operators to terminate processes during an incident - both to evade detection and maximize impact.
PsExec	A utility tool that allows users to control a computer from a remote location.
PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
Rclone	A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.

Known Tools

Restic	A backup program that can be used for exfiltration of sensitive data.
Service Control Manager	A system process under the Windows NT family of operating systems that can start, stop, and interact with Windows service processes.
SystemSettingsAdminFlows.exe	A legitimate Windows operating system file that manages administrative tasks and permissions within the Windows Settings app; it has been abused by threat actors to disable Windows Defender.
TightVNC	A remote desktop software that allows users to access and control a computer over the network.
TOR	An open-source software for enabling anonymous communication, making it more difficult to trace a user's internet activity.
VeeamCreds	A script designed to harvest credentials from Veeam Backups.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes..
wevutil	A command utility used primarily to register a provider on the computer and can be used to retrieve information about event logs and publishers.
Windows Restart Manager	A library for reducing required reboots during software updates. The tool is often used by threat actors to support the encryption process and retrieve processes running on the system.
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.
WordPad	A word processor software included with Windows 95 and later, until Windows 11.

Observed Behaviors: Windows

Tactic	Commands Observed
Execution	wmic/node:"<node>" /user:"<user>" /password:"!Secure4u123!" process call create "cmd.exe /c copy \\<node>\c$\windows\temp\<redacted>.exe c:\windows\temp\" psexec.exe \\<node> -u <user> -p "!Secure4u123!" -d -h -r winupd -s -accepteula -nobanner c:\windows\temp\<redacted>.exe CryptStringToBinaryA
Persistence	Adds a service named dmksvc
Defense Evasion	DeviceIoControl with the dwIoControlCode parameter set to 0x53C028 TerminateProcess
Discovery	GetDriveTypeW net group domain admins /domain, nltest.exe
Collection	7.exe a -mx3 -xr!*.exe -xr!*.mp4 -xr!*.wmv -xr!*.mov -xr!*.avi -xr!*.MXF -xr!*.MTS -xr!*.vhd <archive name> <source folder>

Arguments: Windows

Argument	Description
--debug	Displays debug logs in the terminal
--file	Encrypts a specific file
--dir	Encrypts a directory
--sup	Stops the use of processes
--ens	Encrypts network shares
--lhd	Encrypts hidden and recovery volumes
--mode	Choice of encryption mode (fast/medium/slow)
--hide	Hides the console window
--safe-mode	Terminates processes/services by mask
--help	Displays available arguments
--kill	Starts the victim machine in safe mode

Arguments: Linux

Argument	Description
--daemon	Turns the sample into a daemon process
--motd	Modifies message of the day
--skip	Prevents VM termination

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

MITRE ATT&CK® Mappings

Execution	
T1106: Native API	
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

MITRE ATT&CK® Mappings

Defense Evasion	
T1112: Modify Registry	
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
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	
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/
- Team Huntress (2023, August 11) “Investigating New INC Ransom Group Activity.” https://www.huntress.com/blog/investigating-new-inc-ransom-group-activity
- 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