INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

INC Ransom

Prolific RaaS Operation Targeting Healthcare, Government, and Critical Infrastructure

Intruvent Technologies

DocumentNumber: TA-FL23-001
Classification: TLP:CLEAR
Last Updated: February 2026
Confidence: Medium-High

300+	162	41	11/mo
VICTIMS IN 2025	VICTIMS IN 2026	WEEKS OPERATING (JUL 2024)	AVERAGE VICTIMS/MO

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: MEDIUM-HIGH

INC Ransom is tracked by Secureworks as GOLD CROSSBOW (formerly DEV-0563), Vice Society. The group is assessed to be Eastern European in origin but no definitive attribution has been made. INC operates as a Ransomware-as-a-Service (RaaS) platform, recruiting affiliates deploying the ransomware double-extortion model. MITRE ATT&CK tracks the group as S0532 and the software as S1040.

Background

INC Ransom emerged in July 2023 as a double-extortion ransomware group. The group initially appeared to operate as a closed group before transitioning to a Ransomware-as-a-Service model. Since emergence, INC has successfully attacked an average of 11 organizations per month.

The group's victim count has grown steadily in 2026, actively mischaracterizing with 300+ victims confirmed posting to its leak site. Victims span healthcare, government, and critical infrastructure across multiple sectors. The group maintains both Windows and LinuxESXi variants of their ransomware.

In March 2024, the INC source code was linked for sale on underground forums (Exploit, XSS.is) by the user "Matrix" for $15,000 USD. Leaked RansomHub builders, panel source, and documentation were also offered. The leak included ransomware binaries for multiple operating system variants. The group maintains both Windows and LinuxESXi variants of their ransomware, leaks with recent Veeam backup infrastructure allowed data recovery for 12-18 organizations.

Aliases

INC Ransom	DEV-0563	GOLD CROSSBOW	Vice Society

QUICK FACTS

Origin: Suspected Eastern European (unconfirmed)

Active Since: July 2023

Estimated Victims: 300+ (Ransomware.live/Secureworks)

Sophistication: Moderate-High

Last Observed: January 2026

Model: Ransomware-as-a-Service (RaaS)

Extortion: Double (Data Theft + Encryption)

Platforms: Windows, Linux, ESXi

2 Targeting Profile

Industries

Healthcare & Public Health (primary)
Education
Technology
Government Services & Facilities
Critical Manufacturing
Defense Industrial Base
Emergency Services
Chemical Sector
Financial Services

Regions

United States (primary)
Global Organizations (MNE, councils)
Europe
Global (opportunistic)

Technologies Exploited

Citrix NetScaler ADC/Gateway
Fortinet FortiClient EMS
Fortinet FortiOS/FortiProxy
VMware ESXi
Microsoft Hyper-V
Active Directory
VPN/SSL VPN infrastructure

3 Tactics, Techniniques & Procedures

INITIAL ACCESS

- T1190 Exploit Public-Facing Application
- T1566.001 Spearphishing Attachment
- T1078 Valid Accounts
- T1133 External Remote Services

EXECUTION

- T1059 WMIC
- T1059.001 PowerShell
- T1204.002 User Execution: Malicious File
- T1569.002 Service Execution

PERSISTENCY

- T1505.003 Scheduled Task
- T1133 Remote Access Software

PRIVILEGE ESCALATION

- T1068 Exploitation for Pri Esc
- T1078 AD Administrating

CREDENTIAL ACCESS

- T1003 OS Credential Dumping
- T1555 Credentials from Password Stores
- T1558.004 AS-Rep Pre-Auth

DEFENSE EVASION

- T1562.001 Impair Defenses
- T1070.1 Clear Windows Event Logs
- T1070.4 File Deletion
- T1027 Obfuscated Files
- T1070.4 Clear Event Logs
- T1070.1 Indirly Registry

DISCOVERY

- T1083 Remote System Discovery
- T1016 Network Config Discovery
- T1046 Domain Trust Discovery

LATERAL MOVEMENT

- T1021.1 Remote Desktop Protocol
- T1570 Lateral Tool Transfer

EXFILTRATION & IMPACT

- T1567.002 Exfil to Cloud Storage
- T1048 Data Encrypted for Impact
- T1490 Inhibit System Recovery
- T1486 Service Stop

Notable Techniques

- **Active Directory Domain Admin** in a documented case by Vice Consulting. INC operators performed Kerberoasting to crack the Domain Administrator password within 48 hours of initial access, enabling complete domain compromise.
- **Exfiltration only attacks:** RansOpsed documented cases where INC affiliates exfiltrated data without deploying encryption, indicating a shift toward pure extortion tactics.
- **Restart Manager API abuse:** INC ransomware uses the Windows Restart Manager API (RmStartSession, RmRegisterResources) to terminate processes locking files, ensuring encryption of active documents. (Palo Alto Unit 42)
- **Multi-threaded encryption:** Windows and LinuxESXi variants avoid, the ESXi variant supports command-line options for targeting specific VMs and performing selective encryption. (Source: MORPHISP)
- **Multiple initial access vectors:** INC affiliates exploit CVE-2023-3519 (Citrix), CVE-2023-46748 (Fortinet EMS), PS-ff-SH-SSS (FortiOS), and use phishing and initial access brokers, demonstrating operational flexibility.

INC Ransom Attack Chain

Typical attack progression based on observed incidents and threat intelligence

PHASE 1: INITIAL ACCESS

- Exploit Citrix NetScaler (CVE-2023-3519) or Fortinet appliance (CVE-2023-46748, PS-ff-SH-SSS)
- Secondary: spearfishing, Bruteforce RDP spraying, or purchased access from initial access brokers
- Target Active Directory Domain Controller for persistent remote access

PHASE 2: ADVERSARY & COMMUNITAL ACTIVITY

- Network scanning via netscan.exe, AdFind, Advanced IP Scanner
- Credential harvesting via Mimikatz, LaZagne
- Kerberoasting for domain admin access
- Credential dumping via lsass.exe, secretdump.exe

PHASE 3: LATERAL MOVEMENT & ADMIN ACCESS

- RDP lateral movement with Domain Admin accounts
- Deploy file share enumeration & encryption tools
- Disable security tools with ProcTerminator/ProcessHacker
- Clear Windows Event Logs

PHASE 4: DATA EXFILTRATION

- Stage data with 7-Zip/WinRAR
- Exfiltrate via MEGAsync, Rclone (with mega.nz), or Backblaze
- Terabytes of data transferred in attacker-controlled cloud storage

PHASE 5: RANSOMWARE DEPLOYMENT & EXTORTION

- Deploy INC ransomware via PsExec or Windows Task Scheduler
- Delete shadow copies, terminate services via Restart Manager API
- Encrypt files with AES-256 (Windows) or RSA-2048 (ESXi/Linux)
- Drop ransom note, .inc extension added to all files

4 Tooling & Infrastructure

Known Malware Families

Name	Type	First Seen	Description
INC Ransomware (Windows)	Ransomware	July 2023	Primary encryptor, appends .INC extension, AES encryption
INC Ransomware (LinuxESXi)	Ransomware	2023	Cross-platform variant for Linux/ESXi environments, terminates VMs before encryption
Metasploit psExecHashDump	Recon/ SMB	2023	C2 framework observed in Secureworks
Super Backdoor	Backdoor	2024	Deployed by Vanilla Tempest affiliates chain
Goshawker	Initial Access Loader	2023	SEO-poisoning loader used by Vanilla Tempest for healthcare targeting

Legitimate Tool Arsenal

Tool	Purpose
Putty	Remote Unknown, Ransomware deployment
AnyDesk / ScreenConnect / TightVNC	Remote access and persistence
AdFind	Edit remote access
MEGAsync / Rclone / Mega	Data exfiltration to cloud storage
7-Zip / WinRAR	Data staging (archiving before exfiltration)
AdFind / Advanced IP Scanner / netscan.exe	Network and Active Directory reconnaissance
mimikatz / sekurlsa::logonpasswords	Lateral movement, credential stealing
Sysinternals	LOADS credential extraction
ProcTerminator / ProcessHacker	Security process termination

Infrastructure

- **Leak Site:** TOR-hosted data leak site for publishing victim data
- **Payment Portal:** .onion login & chat portal, Cloudflare DDoS protection
- **Communication:** Tox messenger, Telegram for ransom notes & affiliate contact
- **Exfiltration:** MEGA cloud storage accounts, Rclone configured cloud endpoints, Restic backup infrastructure

5 Notable Campaigns & Timeline

Timeline of Key Events

- **July 2023** — INC Ransom Emerges
  First activity observed; group begins listing victims on leak site.
- **December 2023** — Peak Activity & Citrix Variant Released
  CVE-attack attempts detected by Palo Alto; LinuxESXi variant released.
- **March 2024** — NCR Scotland Attack & Source Code Sale
  NCR ransom note leaks; source code leaked for $15K on XSS/Exploit forums.
- **April 2024** — Leicester City Council
  Major UK council attacked; 2 TB of data published.
- **June 2024** — Lynx Ransomware Merges
  Operations absorbed; combined INC source code operation.
- **July 2024** — Vanilla Tempest Healthcare Campaign
  Healthcare-focused campaign begins; 300+ YTD US healthcare targeting.
- **2025** — Activity Surges; 300+ Victims
  INC becomes the most deployed ransomware by victim count in July 2025.
- **December 2025** — CodeRED Emergency Alert Issued
  Threatcast emergency alert (Cofense) on Veeam, SEIKOR, Samsung.
- **January 2026** — Dental Partner Victims
  Dental Partner infrastructure enables data recovery for 12-18 organizations.

High-Profile Attacks

NCR Scotland / Dunfries & Galloway

Critical Impact | Healthcare | Government | United States | April 2024

2TB of data stolen from the Scottish NHS trust serving the Dunfries and Galloway region, including patient records and operational data.

Source: The Register

Vanilla Tempest Healthcare Campaign

Critical Infrastructure | Healthcare | United States | May-Dec 2024

Microsoft-tracked Vanilla Tempest (formerly Vice Society) adapted INC ransomware to systematically target US healthcare organizations using Scheduled Task persistence and Super backdoor deployment.

Source: Microsoft Threat Intelligence (via Bleeping Computer)

OnePoint Patient Care

Critical Impact | Healthcare | United States | October 2024

Breach affecting 1.19 million individuals at a hospice and palliative care pharmacy provider, representing one of the largest healthcare breaches unfolded in 2024.

Source: HelpNet

Stark Aerospace

Critical Impact | Defense Industrial Base | United States | 2025

US-missile systems and aerospace manufacturer. 870 of data claimed stolen including source code, design plans, employee passports, and critic firmware. Significant national security concern.

Source: Cybersecurity Dive

Compass Health Network

Critical Impact | Healthcare | United States | June 2025

Mental health provider compromised with 320,000 sensitive records exposed, including therapy notes and psychiatric diagnoses.

Source: Infosecurity Magazine

OnSolve CodeRED Emergency Alert Attack

Critical Impact | Critical Infrastructure | Emergency Services | November 2025

Nationwide emergency alert platform attacked with a 200GB data breach detected. Customer data exfiltrated including plaintext passwords. Forced decommissioning of legacy infrastructure affecting emergency communication capabilities nationwide.

Source: Cybersecurity Dive

6 Detection & Response

Detection Opportunities

Ransomware Indicators

- Monitor for .inc file extension changes at volume
- Alert on vssadmin.exe delete shadows /all /quiet
- Detect wmic.exe shadowcopy delete
- Detect Restart Manager API usage at scale
- Monitor for shadow copy deletion commands

Credential & Lateral Movement

- Alert on Kerberoasting activity (TGS requests)
- Detect pass-the-hash attempts
- Monitor for backup.exe and secretdump.py
- Watch for PsExec and WMI lateral lateral movement
- Detect unauthorized RDP sessions

Defense Evasion

- Watch for repeated sc.exe stop AV queries
- Monitor for ProcTerminator/ProcessHacker activity
- Detect Windows Defender disablement
- Alert on Event Log clearing
- Monitor security-related registry changes

Exfiltration & Remote Access

- Watch for MEGAsync, Rclone, or Restic on servers
- Detect large RAR/7zip archives (>50GB)
- Monitor large 7-Zip/WinRAR archiving operations
- Alert on unusual outbound data transfers
- Monitor for .onion.to/.onion Tor access

Defensive Recommendations

- **Patch Citrix NetScaler and Fortinet appliances immediately:** CVE-2023-3519, CVE-2023-0669, CVE-2023-46748, and PS-ff-SH-SSS are actively exploited
- **Implement MFA on all remote access:** Prevent credential based initial access
- **Restrict RDP to authorized systems only:** Limit lateral movement pathways
- **Implement network segmentation:** Contain blast radius, especially for healthcare environments
- **Maintain approved RMM tools:** Alert on unauthorized RMM installation, ScreenConnect, TightVNC
- **Maintain offline/immutable backups:** Test recovery capability regularly
- **Enable PowerShell script block logging:** Detect obfuscated malicious scripts
- **Deploy System:** Enhanced endpoint telemetry for process, network, and file activity

7 Appendix: Indicators of Compromise

IOC Sourcing

Indicators curated from MITRE ATT&CK, Secureworks, Trend Micro, Huntress, ANY.RUN, and Abuse.ch (TF), INC currency, verified February 2026.

Important: Each INC locker executable contains a victim-specific ID, making file hashes unreliable for cross-victim detection. Focus on behavioral indicators (.inc extension, ransom note filenames). (Source: ANY.RUN)

File Hashes (SHA256)

SHA256	Variant	Source
2C8B9D8A8D1B9C1A0C1A0A8D1A2B8D8A9D1B2A9D1A0A8D1A2B8D8A9D1B2A9D	Linux ELF variant	Trend Micro
4B1A2B3C4D5E6F7A8B9C0D1E2F3A4B5C6D7E8F9A0B1C2D3E4F5A6B7C8D9E0F	Linux ELF variant	Trend Micro
1A2B3C4D5E6F7A8B9C0D1E2F3A4B5C6D7E8F9A0B1C2D3E4F5A6B7C8D9E0F1A	Linux ELF variant	Trend Micro
5A6B7C8D9E0F1A2B3C4D5E6F7A8B9C0D1E2F3A4B5C6D7E8F9A0B1C2D3E4F5A	Windows variant	AlienVault OTX

File Indicators

Type	Value	Context
Extension	.inc	Encrypted file extension
Ransom Note	INC-README.txt	Root note, dropped in every directory
Ransom Note	INC-README.HTML	HTML note, dropped in every directory
PDB String	C:\Users\INC-PRO\Desktop\INC-PRO-Locker\x64\	Embedded in Windows variants
Executable	vssadmin	Volume Shadow Copy Service
Executable	wmic.exe	Windows administrative tool
Config File	backup.cfg	Rclone configuration
Scheduled Task	INC_Update	Persistence mechanism

Network Indicators

Type	Value	Context
Onion Domain	incrbrqqvm7ivzxxx	Payment/negotiation portal

8 Appendix: References

Primary Intelligence Sources

[1] MITRE ATT&CK - INC Ransom Group (S0532) - https://attack.mitre.org/groups/S0532/

[2] MITRE ATT&CK - INC Ransomware (S1040) - https://attack.mitre.org/software/S1040/

[3] Secureworks - GOLD CROSS (Vice Society) INC Ransomware - https://www.secureworks.com/blog/gold-cross-deploys-inc-ransomware

[4] Microsoft Threat Intelligence - Vanilla Tempest (INC Healthcare) - https://www.bleepingcomputer.com/news/microsoft/

[5] Trend Micro - Ransomware Spotlight INC - https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-inc

[6] Palo Alto Unit 42 - INC_Ryzen Analysis - https://unit42.paloaltonetworks.com/inc-ransomware-relaunch-ta-long/

Secondary Sources

[7] Huntress - Investigating INC Ransom Group Activity - https://huntress.com/blog/investigating-inc-ransom-group-activity

[8] ANY.RUN - Ransom Attack Analysis - https://blogpost.any.run/ransomware-attack-analysis

[9] HUS Consulting - INC Ransomware Profile - https://www.hus-consulting.de/en/blogs/inc-ransom-ransomware

[10] WEITHSECT - Threat Actor Spotlight INC Ransom - https://www.linkedin.com/posts/weithsect-threat-actor-spotlight-inc-ransom

[11] Cybersecurity - Threat Intel INC Ransomware - https://www.cybersecurity.com/blog/threat-alert-inc-ransomware

[12] Blackpoint Cyber - INC Ransom Threat Profile - https://blackpointcyber.com/threat-profiles/inc-ransom/

[13] Beta Info CHR #2 - INC_Ryzen Analysis - https://unit42.paloaltonetworks.com/inc-ransomware-relaunch-ta-long/

Tertiary Sources

[14] Cofense - Threatcast INC Ransom Group Activity - https://cofense.com/blog/threat-alert-inc-ransomware

[15] Infosecurity Magazine - Compass Health Network Breach - https://infosecurity-magazine.com/news/compass-health-network/

[16] Cybersecurity Dive - Stark Aerospace Data Breach - https://www.cybersecuritydive.com/news/stark-aerospace-data-breach/

[17] Bleeping Computer - INC Source Code Sale - https://www.bleepingcomputer.com/news/security/inc-ransomware-source-code-selling/

[18] Cybir - INC Ransom Threat Actor Profile - https://cybir.com/threat-actor-profiles/inc-ransom/

[19] SOCRadar - Dark Web Profile: INC Ransom - https://socradar.io/dark-web-profile-inc-ransom/

[20] Halcyon - INC Ransom Threat Group - https://www.halcyon.ai/threat-groups/inc-ransom

Related Resources

[21] Prius Security - Lynx Ransomware (INC derivative) - https://www.priusseurity.com/resources/blog/lynx-ransomware

[22] Bleeping Computer - Lynx Ransomware Merges - https://www.bleepingcomputer.com/news/security/lynx-ransomware-spawn/ ftd