From Beachhead to Breach: A Multi-Stage Intrusion Leading to INC Ransomware Deployment

By Ali Hussein, Joao Marques

By Ali Hussein, Joao Marques

The INC Ransomware Group (INC) is a threat actor known for executing sophisticated cyberattacks characterised by stealthy reconnaissance and deliberate planning. The group continues to demonstrate a structured and methodical approach throughout its attack lifecycle. The Intrinsic Security team observed a consistent operational pattern marked by disciplined reconnaissance, credential exploitation, and controlled lateral movement.

Rather than relying on exploits, the INC threat group uses legitimate administrative tools and unauthorised remote-access software to establish a foothold and compromise victim environments.

The following sections detail the technical analysis and techniques employed by the INC Ransomware Group, based on forensic findings identified during a recent investigation by Intrinsic Security.

Incident Summary

Intrinsic Security was recently engaged to investigate a ransomware incident after a client discovered extensive signs of network compromise and large-scale encryption activity linked to the INC Ransomware Group.

Investigation by the Intrinsic Security Threat Intelligence team revealed a coordinated, multi-stage intrusion, following tactics consistent with INC's broader campaigns observed throughout 2024.

The attackers gained initial access through compromised credentials and went on to leverage legitimate remote-administration tools to maintain persistence and control. By using trusted software already present in the environment, they blended seamlessly into normal administrative activity, a tactic that allowed them to remain undetected while preparing systems for encryption.

Importantly, no exploit-based entry was identified. Instead, the threat actors relied on trust abuse and the deployment of dual-use tools such as AnyDesk, TightVNC, and common network-scanning utilities to move laterally across systems. Before executing the ransomware, they disabled backup processes and deleted shadow copies to hinder recovery.

The ransom note pointed victims to an onion-based negotiation portal, a hallmark of INC's known infrastructure. Overall, the behaviour, tooling, and operational discipline observed in this incident align with INC's ongoing pattern of human-operated, credential-driven ransomware attacks.

By Ali Hussein, Joao Marques

Detailed Attack Analysis

Initial Attack Vector

During our investigation, we identified a series of successful logins into the victim's network via a VPN device. These logins began approximately a few weeks before the INC group released its ransom notes. The initial access appeared to have been achieved using weak or compromised credentials.

computer_name	[redacted]
data_type	windows:evtx:record
datetime	2025-04-16T18:32:50.721103+00:00
display_name	[redacted]
event_identifier	4624
event_level	0
event_version	2
message	[4624] Source Name: Microsoft-Windows-Security-Auditing Strings: ['S-1-0-0', '-', '-', '0x0000000000000000', 'S-1-5-21-1047617109-355623775-1864969818-104631', [redacted] '0x00000002bd0e5442', '3', 'NtLmSsp ', 'NTLM', 'WIN-AG3PGET9035', '{00000000-0000-0000-0000-000000000000}', '-', 'NTLM V2', '128', '0x0000000000000000', '-', '172.24.252.93', '53585', '%%1833', '-', '-', '-', '%%1843', '0x0000000000000000', '%%1842']
message_identifier	4624
offset	0
path_spec	{"__type__": "PathSpec", "location": "/mnt/d/Cases/SecX-Nexio/DCACC03/C/Windows/System32/winevt/Logs/Security.evtx", "type_indicator": "OS"}
provider_identifier	{54849625-5478-4994-a5ba-3e3b0328c30d}
record_number	2354591316
recovered	false
sha256_hash	32c484f0899cea4ac9ae4da9d1ccb99e8f9e351674e3aa83918638e36e948d01
source_long	WinEVTX
source_name	Microsoft-Windows-Security-Auditing
source_short	EVTX
strings	["S-1-0-0", "-", "-", "0x0000000000000000", "S-1-5-21-1047617109-355623775-1864969818-104631", [redacted] "0x00000002bd0e5442", "3", "NtLmSsp ", "NTLM", "WIN-AG3PGET9035", "{00000000-0000-0000-0000-000000000000}", "-", "NTLM V2", "128", "0x0000000000000000", "-", "172.24.252.93", "53585", "%%1833", "-", "-", "-", "%%1843", "0x0000000000000000", "%%1842"]

The early activity timeline revealed patterns consistent with stolen or reused credentials being used against remote-access services such as VPN, RDP, or other remote-management gateways. These sessions bore the classic signs of account takeover, interactive logons from legitimate remote-access vectors, followed by administrative actions that mimicked typical IT behaviour but originated from unexpected locations or at unusual times.

Although definitive attribution of the initial entry point was limited by gaps in pre-intrusion telemetry, multiple supporting indicators suggest that credential abuse was the primary vector for compromise.

By Ali Hussein, Joao Marques

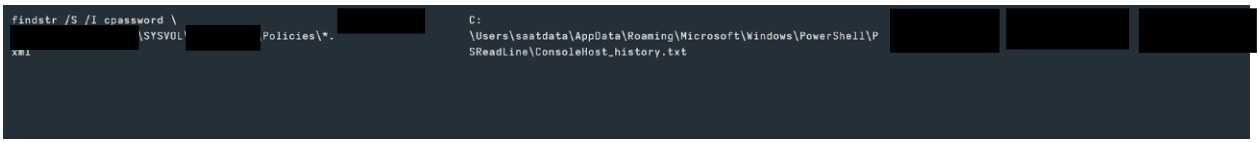
Reconnaissance

Once initial access was obtained, the threat actor began conducting reconnaissance activities to map the victim's network. The executable netscan.exe was observed running on multiple compromised hosts a few weeks before the day of encryption. This executable is part of SoftPerfect Network Scanner, a legitimate network administration tool commonly used to scan and manage network environments.

The INC Ransomware Group is known to abuse netscan.exe for internal network mapping, identifying reachable systems and locating high-value targets for lateral movement and eventual data encryption.

ModificationTime	Path	ExecutionFlag	Fqdn
2024-05-04T22:09:42Z	C:\Users\ \Desktop\netscan.exe	1	com
2024-05-04T22:09:42Z	C:\Users\Default\Desktop\netscan.exe	34484	com
2024-05-04T22:09:42Z	C:\Users\ \Downloads\netscan.exe	34484	com
2024-05-04T22:09:42Z	C:\Users\ Desktop\netscan.exe	1	com
2024-05-04T22:09:42Z	C:\Users\Default\Desktop\netscan.exe	34484	com
2024-05-04T22:09:42Z	C:\Users\ Downloads\netscan.exe	34484	com

During the reconnaissance phase, the threat actor also leveraged PowerShell to execute the findstr command, searching the domain SYSVOL share for stored credentials. This is a well-documented technique used to extract administrative credentials from Group Policy Preferences, providing elevated access for further compromise.



```
findstr /S /I cpassword \                                    C:
\SYSVOL\ Policies\*.                                         \Users\saatdata\AppData\Roaming\Microsoft\Windows\PowerShell\P
xml                                                          SReadLine\ConsoleHost_history.txt
```

Persistence

For persistence, our team identified traces of multiple remote monitoring and management (RMM) tools used by the threat actors to maintain access to the victim's network. The remote-access utilities discovered included AnyDesk, TightVNC, Atelier Web Remote Management Agent, and other RMM frameworks.

AnyDesk and TightVNC are legitimate administration tools but are also commonly abused by the INC Ransomware Group as part of their persistence and post-exploitation tactics. Their use allows attackers to maintain continuous access to compromised systems under the guise of authorised remote administration.

By Ali Hussein, Joao Marques

Anydesk

AnyDesk is a powerful remote-access tool that enables users to control and manage systems remotely. While it is commonly used by IT teams for legitimate support and administration, it is also frequently abused by threat actors to maintain persistence, facilitate lateral movement, and exfiltrate data within compromised networks.

In this case, AnyDesk was installed using a compromised service account on several servers in mid-April. Outbound TCP connections from anydesk.exe on the compromised hosts were observed resolving to AnyDesk's relay infrastructure. Because the tool routes traffic through its own network, the true external endpoint of these sessions could not be determined — effectively allowing the attacker to obscure their destination and blend into normal outbound activity.

We utilised the ad_svc.trace artefact to detect and verify external connections associated with AnyDesk activity on the affected systems.

TightVNC

The INC Ransomware Group is known to abuse the TightVNC remote-access tool. TightVNC is a desktop application that allows users to control another computer over a network. It supports file transfers, provides stealthy remote access, and can run invisibly in the background, making it particularly attractive to threat actors seeking to maintain persistent, covert access within a compromised environment.

Remote Monitoring and Management RMM

During the investigation, a remote-access utility identified as a Remote Monitoring and Management (RMM) tool was discovered within the victim's environment. This software provides administrators with the ability to remotely manage systems — including performing network maintenance, controlling firewalls, and monitoring security events.

However, according to the Cybersecurity and Infrastructure Security Agency (CISA), RMM tools are frequently abused by threat actors. They are often distributed through phishing campaigns, tricking victims into installing them and thereby granting attackers persistent remote access to corporate networks.

By Ali Hussein, Joao Marques

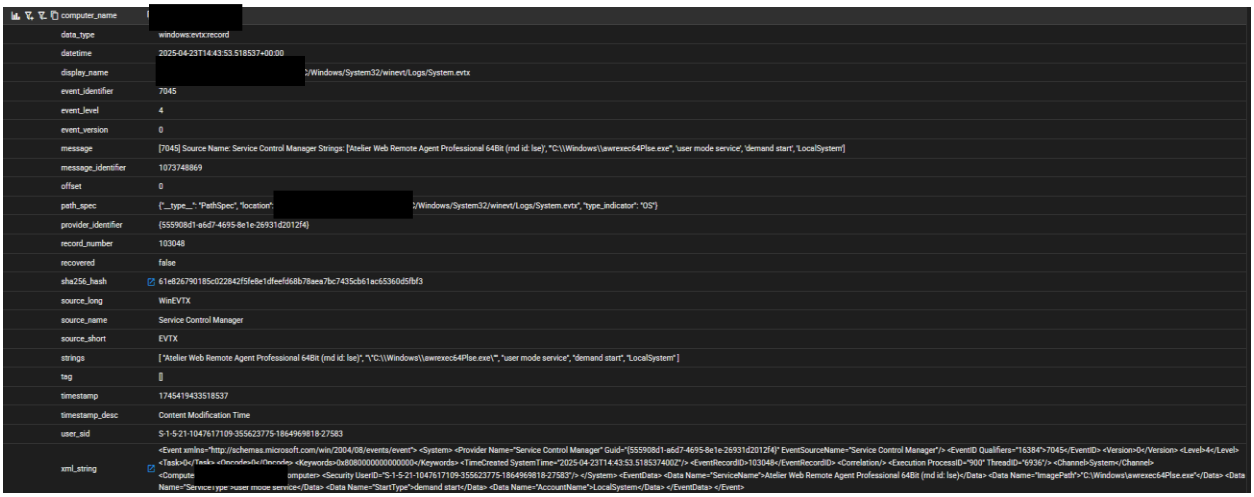
As part of this case, our team observed the creation of a service named rmmExecSvc on one of the compromised systems. This service appeared to be linked to the RMM tool, which — although legitimate — was likely repurposed by the attackers to maintain long-term access and continue remote operations under the guise of legitimate administrative activity.

The executable associated with the rmmExecSvc service is ‘DPLService.exe’.

Atelier Web Remote Agent Professional

During the investigation, we identified that the threat actor had installed an additional Remote Monitoring and Management (RMM) tool, Atelier Web Remote Agent. This remote-access utility enables control of machines without requiring software installation on the remote endpoint, making it a convenient — yet potentially risky — tool when misused.

On one of the infected hosts, analysis of the Windows System Event Logs revealed the creation of a service associated with Atelier Web Remote Agent, confirming its installation and use within the compromised environment, as illustrated below.



The threat actor proceeded to delete and remove traces of the tools 2 hours later.

By Ali Hussein, Joao Marques

Lateral Movement

Once the threat actor had established persistence, they began conducting lateral movement activities within the network.

A deprecated service account was used by the attacker to establish SSL VPN sessions during May, originating from a known malicious external VPN IP address (154.47.30[.]104).

This account was subsequently used to access internal hosts via the SMB protocol (port 445), enabling further movement across the environment.

SSH Tunnelling and RDP Activity

Suspicious RDP connections involving the IPv6 loopback address ::%16777216 were identified on two hosts, activity indicative of RDP tunnelling. Prior to this, a suspicious SSH command resembling a reverse SSH tunnel was executed by a compromised user account on an internal server. This technique is commonly used to bypass firewalls and maintain covert, bidirectional communication through RDP channels.

Although RDP appeared to be the primary lateral movement method, we also identified the use of PsExec, a legitimate Sysinternals command-line utility that allows users to execute commands and processes on remote machines.

In addition, executions of putty.exe were observed on several hosts. PuTTY is a legitimate terminal emulator that enables remote connections typically via SSH, but in this context was likely leveraged by the threat actor to expand access within the compromised network.

Exfiltration

Through the analysis of AnyDesk logs we identified a consistent data transfer rate of approximately 1.5 GB per hour on the file server starting around April 20th, 2025. This is a strong indicator of data exfiltration, as the client did not recognize this activity.

By Ali Hussein, Joao Marques

Conclusion

The INC Ransomware Group is an example that cyberattacks do not always rely on sophisticated exploits or zero-day vulnerabilities. In this case, our investigation showed that the attackers did not need to break down the door. They simply walked through it, using stolen credentials, trusted remote-access tools, and normal IT processes to blend in and take control.

This incident highlights a crucial truth: The misuse of legitimate tools already inside of the network can compromise networks and interrupt business operations.

This means that we need shifting focus from chasing every new exploit to detecting abnormal behaviour, tightening credential policies, and closely monitoring remote-administration software. Prevention now depends on understanding what "normal" looks like in your environment and spotting when something quietly deviates from it.

At Intrinsic Security, we help organisations do exactly that. Our forensic and threat intelligence teams not only uncovered how INC operated but also provided our client with the insights needed to rebuild stronger. Every investigation we lead ends with one goal: **turning a breach into an opportunity to build long-term resilience.**

Because the best outcome after a cyberattack isn't just recovery — it's emerging more secure than before.

By Ali Hussein, Joao Marques