# Investigating New INC Ransom Group Activity | Huntress

Archived: 2026-04-05 19:23:05 UTC

The Huntress team is always keeping our eye on the evolving threat landscape. Now, it seems that a new contender, referred to as “INC” has entered the ransomware fight. 🥊

This new ransomware group began gaining notoriety very recently, with several impacted organizations publicly identified through their leak site, as illustrated in the tweets below.

The Huntress team recently investigated a ransomware attack indicative of the ‘INC’ threat actor. While the file encryption process brought the attack to the attention of the impacted organization immediately, an investigation into what led to the attack indicated that the initial phases of the attack began a week prior to the file encryption event, if not sooner.

Three server systems were the primary focus of the Huntress investigation. Huntress did not have complete visibility across the entire impacted infrastructure, and a number of systems were taken offline before log data could be collected from the endpoint. However, the Huntress team was able to assemble a day-by-day accounting of the threat actor’s observable activity across the systems to which we had access.

## Ransomware Attack Breakdown

### *Day 1 - Initially Observed Access, Enumeration*

Based on the investigation, the first indication of activity likely associated with the ransomware threat actor began with very short (2-3 seconds) connections to Server 1, in quick succession, albeit with three different source system names (**ylqlCXO9VdRiZ5JK**, **aJLXC9TzxgInkqf4**, and **UxUZNZXxMeBN2jox**). All three connections originated from the same IP address and accessed the target system using the same account name.

Approximately four and a half hours later, valid account (compromised) credentials were used to access the same system via Remote Desktop Protocol (RDP). During this brief (~30 min) connection, there was some light enumeration activity (**net group domain admins /domain**, **nltest.exe**).

### *Day 2*

On the next day, the Huntress team observed a brief RDP login to Server 2, via previously observed credentials.

### *Day 3 - Collection, Data Staging, Data Exfiltration*


On day three, the Huntress team observed an RDP login to Server 2, via previously observed credentials, during which there are numerous 7-Zip archival commands to collect and stage data for exfiltration.

The 7-Zip commands all followed the same format:

**7.exe  a -mx3 -xr!*.exe -xr!*.mp4 -xr!*.wmv -xr!*.mov -xr!*.avi -xr!*.MXF -xr!*.MTS -xr!*.vhd <archive name> <source folder>**

During this time, the Huntress team also observed the threat actor's use of native tools such as **Wordpad.exe**, **Notepad.exe**, and **MSPaint** to view the contents of documents and image/JPEG files.

Finally, the threat actor installed MEGASync on Server 2, presumably to facilitate data exfiltration.

### *Day 4 - Collection, Data Staging, Data Exfiltration*

The threat actor again accessed Server 2 via RDP and continued issuing collection and data staging commands, identical to those observed the previous day.

### *Day 5*

The Huntress team observed the threat actor accessing Server 3 via RDP, using previously observed credentials. This logon session was brief, approximately six minutes, with little activity observed via EDR telemetry.

### *Day 6*

No activity was observed.

### *Day 7 - File Encryption*

The seventh day began with the threat actor accessing Server 3 via RDP, installing the Advanced IP Scanner, and shortly thereafter, moving laterally to Server 2 via RDP.

During the logon session to Server 3, the threat actor was observed using Internet Explorer (**iexplore.exe**) to view folders on other systems, as well as using **mstsc.exe** to (attempt to) move laterally to other systems. The threat actor also installed PuTTY.

Approximately three hours after the initial logon to Server 3, the threat actor was observed running credential access commands on all three servers, all of which were indicative of the use of lsassy.py.

Approximately four hours after the initial logon to Server 3, the Huntress team observed the threat actor issuing a number of **copy** commands in rapid succession, indicative of a batch file or script, to push what was determined to be the file encryption executable to multiple endpoints within the infrastructure. These **copy** commands were followed in rapid succession by a similar series of **wmic.exe** commands to launch the file encryption executable on each of those endpoints. All of these commands were of the same format, illustrated by the following:

**wmic /node:"<node>" /user:"<user>" /password:"!Secure4u123!" process call create "cmd.exe /c copy \\<node>\c$\windows\temp\<redacted>.exe c:\windows\temp\"**

The Huntress team also observed the use of PSExec to launch the file encryption executable, illustrated as follows:

**psexec.exe \\<node> -u <user> -p "!Secure4u123!" -d -h -r winupd -s -accepteula -nobanner c:\windows\temp\<redacted>.exe**

Note that in the above command, the PSExec executable was renamed to **winupd** when launched on the remote node. This resulted in a System Event Log record on each endpoint where the command successfully launched the Windows service that appeared as follows:

**Service Control Manager/7045;winupd,%SystemRoot%\winupd.exe,user mode service,demand start,LocalSystem**

Finally, there were indications on Server 3 that the threat actor had difficulty running the file encryption executable, as there was no indication of encrypted files, nor ransom notes, on that server. The Huntress team observed multiple instances of the threat actor running **<redacted>.exe –debug** commands, indicating the threat actor attempting to troubleshoot the file encryption executable.

## Conclusion

When a successful ransomware attack occurs, it is immediately impactful and disruptive to the impacted organization. However, there is often considerable activity that leads to deployment of the file encryption executable, such as initial access, credential access and privilege escalation, and enumeration and mapping of the infrastructure. Where data theft (staging and exfiltration) occurs, this can very often be seen well prior to the deployment of the file encryption executable.

While the Huntress team was unable to discern the threat actor's means of initial access, the investigation clearly demonstrated considerable activity, across several key systems, over the course of a week.

### Indicators

- Ransomware Executable File Name: named for the impacted organization

- Ransomware Executable SHA256 hash: accd8bc0d0c2675c15c169688b882ded17e78aed0d914793098337afc57c289c
- Ransomware Executable PDB string: C:\source\INC Encryptor\Release\INC Encryptor.pdb
- Ransom Note file name: *.inc-readme.txt, *.inc-readme.html
- Encrypted File Extension: *.inc
- Use of compromised valid accounts
- Use of native tools (net.exe, nltest.exe, Wordpad/Notepad/MSPaint, Internet Explorer, Windows Explorer, mstsc.exe, msdt.exe)
- Use of additional tools (7-Zip, MEGASync, Advanced IP Scanner, Putty, lsassy.py, PSExec)

## MITRE ATT&CK

- Initial Access - Valid Accounts/T1078.002
- Execution - Command and Scripting Interpreter/T1059.001, T1059.003; Windows Management Instrumentation/T1047
- Persistence - Valid Accounts/T1078.002
- Privilege Escalation - Valid Accounts/T1078.002
- Defense Evasion - Not Observed
- Credential Access - OS Credential Dumping/T1003.001
- Discovery - Domain Trust Discovery/T1482
- Lateral Movement - Remote Services/T1021.001, T1021.002
- Collection - Archive Collected Data/T1560.001
- Command and Control - Not Observed
- Exfiltration - Exfiltration Over Web Service/T1567.002
- Impact - Data Encrypted For Impact/T186

*Special thanks to Josh Allman (@xorJosh), Matt Anderson (@nosecurething), Harlan Carvey (@keydet89), and Anthony Smith (@KingCrtz) for their contributions to this blog post and investigation.*

**Want to dive into more threat actor tradecraft? Register for Tradecraft Tuesday!**

---