2024-09-05

HUNTER

EMERGING THREATS

INC RANSOMWARE

INC Ransomware is a malware variant that was first observed in July/August of 2023, and has since been a part of major disruptions mostly in North America and Europe. Recently in August 2024, they have been tied to the attack and disruption of the major healthcare network McLaren Health Care - affecting IT infrastructure/devices and phone systems. The threat group, known by the same name as the ransomware (INC Ransom group), has typically been financially motivated and employs a double-extortion system after encrypting targeted systems - double-extortion referring to the exfiltration of proprietary data and threatening to release it to the public if the victim does not adhere to demands. The techniques that are utilized by **INC Ransomware** are similar to other Ransomware variants, with related methods of initial access, reconnaissance, lateral movement and ultimately the encryption of the system - furthermore, newly discovered Lynx ransomware has been observed in July 2024 to potentially be a fork of the malware strain. **INC Ransomware** is considered to be an active threat, and thus poses a significant and present risk that organizations should ascertain and be prepared for.

THREAT SUMMARY

INC Ransomware is a malware variant that was first observed in July/August of 2023, and has since been a part of major disruptions mostly in North America and Europe. Recently in August 2024, they have been tied to the attack and disruption of the major healthcare network McLaren Health Care - affecting IT infrastructure/devices and phone systems. The threat group, known by the same name as the ransomware (INC Ransom group), has typically been financially motivated and employs a double-extortion system after encrypting targeted systems - double-extortion referring to the exfiltration of proprietary data and threatening to release it to the public if the victim does not adhere to demands. The techniques that are utilized by **INC Ransomware** are similar to other Ransomware variants, with related methods of initial access, reconnaissance, lateral movement and ultimately the encryption of the system - furthermore, newly discovered Lynx ransomware has been observed in July 2024 to potentially be a fork of the malware strain. **INC Ransomware** is considered to be an active threat, and thus poses a significant and present risk that organizations should ascertain and be prepared for.

Intel 471 References:

[TITAN Info Report: Actor runs INC Ransom ransomware group]
(https://titan.intel471.com/report/inforep/964ac38d11e8004dff2d4dcb79518e35)

[TITAN Info Report: Inc. aka INC ransomware-as-a-service management panel reviewed]
(https://titan.intel471.com/report/inforep/9a25b6200d9ea91544057ac02a1ad000)

[TITAN Info Report: Actors operate INC aka Inc. ransomware-as-a-service affiliate program]
(https://titan.intel471.com/report/inforep/684ba479902d042c388b72529b3218f3)

[TITAN Info Report: Actor allegedly runs Inc. aka INC ransomware-as-a-service affiliate program]
(https://titan.intel471.com/report/inforep/1c6e9d78aa0d6550c55e1a38afb87b2f)

[TITAN Info Report: Lynx ransomware operators reveal data-leak site, double-extortion tactics]
(https://titan.intel471.com/report/inforep/4c7cfc519fd3b0961d058fc23ae20e80)

SYNOPSIS

INC Ransomware is a ransomware variant that has been around since 2023 and is still active in August of 2024, appearing globally but with a large number of victims being based in the United States and Europe. The **INC Ransomware** group employs a double extortion method, threatening the release of victimâ€™s data to the public if ransom demands are not met - typically to a TOR site where they leak data and information. The malware itself is capable of infecting Windows and Linux based operating systems. The infection involves a sophisticated approach for their victims, utilizing crafted spear-phishing emails or the targeting of services vulnerable to exploitation, such as the Citrix Netscaler vulnerability (CVE-2023-3519) for example. After initial access is achieved, operators utilize LOLBIns and abuse software to conduct reconnaissance and laterally move through the environment. Examples include the use of NETSCAN.exe to scan the victimâ€™s network and ESENTUTL.exe for database management.

With compromised credentials, operators are able to perform enumeration and move laterally throughout the network to search for other potential targets who are vulnerable. Before encryption takes place, attackers abuse the archiving software 7-Zip for data collection/compression and have been observed to use MEGASync tool for data exfiltration. Subsequently, file encryption begins using WMIC and PSExec to execute the **INC Ransomware** payload. This file execution begins the automated encryption process that utilizes scripts to carry out the procedure and ultimately lead to disk encryption. It is worthy to note that files encrypted were appended with the ".inc" extension and ransom notes seen as â€œINC-README.TXTâ€ and â€œINC-README.HTMLâ€ are also dropped into all encrypted folders.

HUNT PACKAGES

7-ZIP ARCHIVE COLLECTION WITH FILE EXCLUSIONS
https://hunter.cyborgsecurity.io/research/hunt-package/f91348d0-2f58-46c4-b1a6-47522dfcf3e4

FIRST TIME SCRIPT OR SYSINTERNALS EXECUTION - REGISTRY KEY MODIFICATION
https://hunter.cyborgsecurity.io/research/hunt-package/d48db011-2f77-4db7-a069-e126340f4273

POTENTIAL EXFILTRATION - COMMON RCLONE ARGUMENTS
https://hunter.cyborgsecurity.io/research/hunt-package/f075c217-783e-459a-aeb4-42ea91e07af7

ADVANCED IP SCANNER TOOL UTILIZATION
https://hunter.cyborgsecurity.io/research/hunt-package/181b11a6-3391-4d98-aaab-a2544f03c2ef

REMOTE WMI COMMAND ATTEMPT
https://hunter.cyborgsecurity.io/research/hunt-package/9f2e163b-4f26-4972-b3d5-31c0b24b98a0

REMOTE PROCESS INSTANTIATION VIA WMI
https://hunter.cyborgsecurity.io/research/hunt-package/dd0ca1e2-046f-4878-b7f8-32b790420ef2

MEGA SYNC INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/1f5bc4e1-439b-478d-915c-d0bb30d65725

RELATED LINKS
Sign up for free HUNTER access
INC Ransomware Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Execution
  - Exfiltration
  - Defense Evasion
- Technique Names:
  - Exfiltration Over Alternative Protocol
  - Windows Management Instrumentation
  - Disable or Modify Tools
- Threat Names:
  - INC Ransomware

REFERENCES

1. https://www.huntress.com/blog/investigating-new-inc-ransom-group-activity
2. https://www.sentinelone.com/anthology/inc-ransom/
3. https://socradar.io/dark-web-profile-inc-ransom/