INC ransomware source code selling on hacking forums

Date: 14th May 2024 | Severity: High

Summary

A cybercriminal using the name “salfetka” claims to be selling the source code of INC Ransom. INC has previously targeted the U.S. division of Xerox Business Solutions (XBS), Yamaha Motor Philippines, and, more recently, Scotland’s National Health Service (NHS).

INC Ransom operation is undergoing changes that might suggest a rift between its core team members or plans to move to a new chapter that will involve using a new encryptor. Inc. ransomware TOR-based blog; two of which are in the healthcare industry. Targets in the technology industry are listed as well.

Attack Vectors

- The threat actor announced the sale of both the Windows and Linux/ESXi versions of INC on the Exploit and XSS hacking forums. KELA also told BleepingComputer that “salfetka” has been active on the hacking forums.
- Legitimacy to the sale is “salfetka” including both the old and new INC Ransom page URLs on their signature, indicating they are affiliated with the ransomware operation.
- Tools associated with Inc. ransomware operations include:NETSCAN.EXE – Multi-protocol network scanner and profiler, MEGAsyncSetup64.EXE – Desktop application for MEGA file sharing/synchronization/cloud services, ESENTUTL.EXE – Microsoft utility for database management and recoveryAnyDesk.exe – Remote management/Remote Desktop.
- Allows security analysts to crack the encryption of a ransomware strain, private source code sales of strains for which there’s no available decryptor have the potential to create more trouble for organizations worldwide.
- The ransomware appears to attempt to delete Volume Shadow Copies (VSS) although we were not able to reproduce this behavior in our testing.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced

Recommendation

- Use anti-malware software or other security tools capable of detecting and blocking known ransomware variants. these tools may use signatures, heuristics, or machine learning algorithms, to identify and block suspicious files or activities.
- Monitor network traffic and look for indicators of compromise, such as unusual network traffic patterns or communication with known command-and-control servers.
- Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.
- Implement a robust backup and recovery plan to ensure that the organization has a copy of its data and can restore it in case of an attack.

Reference Links

- https[:]//www.cybereason.com/blog/threat-alert-inc-ransomware
- https[:]//www.bleepingcomputer.com/news/security/inc-ransomware-source-code-selling-on-hacking-forums-for-300-000/