Severity

High

Analysis Summary

Snake emerged for the first time in late November 2020. Since November 2020, malicious actors have started releasing Snake through phishing attacks. Snake Ransomware is built-in Golang, an open-source programming language that supports several operating systems. It deletes the computer's Shadow Volume Copies and terminates processes linked to SCADA systems, virtual machines, industrial control systems, remote management tools, network management applications, and other programs. This ransomware has been attacking industrial control systems' operations and files. Snake bypasses all Windows and other system directories on the machine during encryption. In comparison to other ransomware attacks, its encryption procedure is slower.

Impact

- File Encryption

Indicators of Compromise

Filename

- fresh[.]exe
- fresh_Djctepjr[.]png

IP

- 45[.]137[.]22[.]163

MD5

- 14e258bcf447d5ded0129738d1b092a4
- dd4c7dca2b8b5c3d93e7faa9dba00193

SHA-256

- 0ca1b6214ae961565b610b7bc05de81fe9450334cd5300f0200e6212a2732079
- f4fff95fd7d2ffd0b8030a4c43b463b2aaa4ac850b751305249a9f9ba58d2bc8

SHA-1

- 11d5f7a1c7e1c307a209e333139537fc475b7c4e
- 46010c9828a4e7ce33158fd49d6421f502230471

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment