Written by Alice Marshall
10 January 2020

Administrators need to look out for a new ransomware targeting enterprise networks across the world-- SNAKE, a nasty piece of software designed to encrypt all devices connected to the network.

SNAKE joins a growing number of enterprise ransomware, including Ryuk, Maze, Sodinokibi, LockerGoga, BitPaymer, DoppelPaymer, MegaCortex and LockerGoga. All are find use by threat actors to infiltrate business networks and gather administrator credentials before using post-exploit tools to encrypt all files on the computers on the network.

As BleepingComputer reports, SNAKE was first found by MalwareHunterTeam, who in turn shared with SentinelLabs head Vitali Kremez in order to learn more about the infection. According to Kremez, the ransomware is written in Golang, only with a higher level of obfuscation than typically seen in such infections. Coupled with a targeted approach, this makes it particularly nasty.

SNAKE first removes the Shadow Volume Copies from a computer before killing processes related to SCADA systems, virtual machines, industrial control systems, remote management tools, network management software, among others. It then encrypts all files other than those located in Windows system folders and various system files. Once done with the encryption, SNAKE drops a ransom note on the desktop detailing how the victim can pay to unlock their files. Tellingly, the ransom covers all files on the network, as opposed to an individual machine.

Researchers are still analysing the ransomware for weaknesses, and as such it is not known whether it can be decrypted for free. So far, alas, it appears to be secure.

Go SNAKE Ransomware Is the Next Threat Targeting Business Networks (BleepingComputer)