Severity

Medium

Analysis Summary

Snake is a modular .NET keylogger and credential stealer first spotted in late November 2020. Since then, new campaigns spreading this malware have been seen almost daily. Snake’s name was derived from strings found in its log files and string obfuscation code. Using the malware’s builder, a threat actor can select and configure desired features then generate new payloads. For this reason, the capabilities of samples found in the wild can vary. Analysing Snake reveals that it is a comprehensive keylogger and data stealer.

Impact

- Credential Theft

Indicators of Compromise

MD5

- 697c985cb7f119265f0bb49de543ab34

SHA-256

- eb3210b628ab723969c0e007b910b1b3898c5e901a28fb7ce99321535488bd99

SHA-1

- 1f713b0459f2bcbb141110b055378347413e537f

Remediation

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