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

- b6716fe669d58434804cdae50e98684c

SHA-256

- dc2b92a9a90417765a70ceccdc8c5dd7d813f543bc6f21145da4388257188124

SHA-1

- 47266d6a266d26cd7771f3ce6a4d32f672320236

Remediation

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