Severity

Medium

Analysis Summary

AveMaria RAT is a remote access trojan that targets Windows systems that provides the capability to gain unauthorized access to a victim’s PC or allow covert surveillance of it. It acts as a keylogger, can steal passwords, escalate privileges, and much more. AveMaria, like most malware, first arrives at systems as a result of phishing mails (as invoices and shipping orders), but is also available on the dark web for subscriptions.

Impact

- Unauthorized Access

Indicators of Compromise

MD5

- 66916d5cc3685f50e1f00a8bd860e6ca
- e263c5f68ae4b63424834da4f60c5aa2

SHA-256

- dc6af37f5633e93bc1073303956eee320568c2a66bc705e9f14573eb3fe9eae0
- 984107429953e79b5635db4f49e63c0d0b3a9a03be60e5f48d5da2e1ee3fae64

SHA-1

- ee187a36fe58d91c0b095945c21562ed6e5e6912
- c2b21d65dcf7b3d1a169350ace6e6caac5b27456

Remediation

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