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

- 154d7bfa125d42c8e23edc866de60c1b

SHA-256

- ac668db916d579bf394d4212adb085af89464caa5d0045d5cd959b8ed9b3b4db

SHA-1

- 3a84f6e5a591ff6029c5997178ed72fa9b714bb7

Remediation

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