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

- 958b2413a34997f88ba23cd7bd3f93d8

SHA-256

- a3987d853eb144e67990c5144b873019249bc17c3a08c05f39adc9138a5d609e

SHA-1

- 67f4457fc7b2cf2603218b28ca039c446863a169

Remediation

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