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

- ee489c5548dc8f8190a76cfacfe4ff8b

SHA-256

- 314337dc40ae820032963be57003f835d3e9ba783eb1fdbba7dc2f3e925144c6

SHA-1

- 62a47c1899d7f7c65f6fdbfee2c5ade60fecd5a7

Remediation

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