

# 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

- 46fab278cc194b3a8980451a2835f9ba

## SHA-256

- 25271a9f2ae211c6553372578b1eafd5aebd9c5a03440d7f5e1094ba4189f751

## SHA-1

- 9469ea03b7893de13291485074cf3daf3326bf0d

# Remediation

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