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

- 3f9d960e80adb5d41a5d02df66a51d94
- 46bece0e0ae9b696619564b3407f2477
- 8825c8df732e6e0b5de89fd0e7feb735

SHA-256

- ef9d8dc478aae66e769f4e7e5ad3fc266775596581376d6a757a8415212b8800
- 6bb096fc82c51dc8f76ceaa0566b4410ad88acea20bcb2141cbac63dedae89bb
- 102b42df7c9783ac7aab05a97af9169479806a47ebedec7ee1a7dd16cd6d0c07

SHA-1

- 1dde53b9d06fb38b5cedd74bed3d312cc748af53
- 5c926c5f7546afab1776fd16aa33e971c7ea97ad
- 83b88d3ef1b6049f73e141a5aefdfb811e58ee73

Remediation

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