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

- 1ae9379c64c9c4720aacf3c51e1448b2
- 6bc2ebd00a0a941c8569d28c4027e3fc
- d3d04b9a91899184dd243d0c9339928a
- c07630d7e5834a347172ff3b71e5d2bd
- 853192e452519de7da3e388d14dbb619
- dc99561dae63ff736f4b9b46b04f28df

SHA-256

- e5c00fe79b015685e64d6424bae88386a3af52d1c97bcce639576386a10bb67a
- 4936b932ed21901cf8267a2fb5a8a4324b749c298b0e688a01c1286134a44549
- b0773d0dcca492d5ac179ef976c7e8dbd2f8c251edd30ab02d89c7850b85d858
- 78e187e1318e74767b22c668d8ff398af5dad9a9668d4ef183db3d4bb818e865
- 5a9f7b86d93a84e03f6cf6dd71f1f5dac02fa4c6b778e74421a29fa0e45ba5ea
- 1634ba6c1fa74312f9bbb7b90c420a48908fed1def489d92fdcd1f3cde1cabf8

SHA-1

- 1b1676a89476c6f1798508018166fae3975ad328
- 85b4d783fbddf0d009124f9860495b47f4c9eb30
- eb800e251c67c1539ea1ff527c4f2aaccb7f9bde
- d1dcabfb3c624238094c18bb8b60bd133ae13db9
- 763bb28812935034cc2d58a7b8d0da43e573cb74
- 5febf32392943b015a903fb172efe8f2a12bb2b0

Remediation

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