Severity

Medium

Analysis Summary

A new AgentTesla campaign is seen targeting victims with malspam. AgentTesla is known for stealing data from different applications on victim machines, such as browsers, FTP clients, and file downloaders. Agent Tesla collects personal information from the victim's machine, steals data from the victim's clipboard, can log keystrokes, capture screenshots and access the victim's webcam. It can kill running analysis processes and AVsoftware. The spyware also performs basic actions to check whether it is running on a virtual machine or in debug mode, in an attempt to hide its capabilities and actions from researchers. All the data it obtains is sent in encrypted form via SMTP protocol.

Impact

- Credential Theft
- Data Exfiltration
- Information Disclosure

Indicators of Compromise

MD5

- 2683e0dfc5036f639093e560edd8582b
- fe54e102040b7108826fda1eba1a50b1
- ca7003dd812c6fa672b599b9c0b8b3e0
- 232d2c029921948aa15cb237e83e79ad

SHA-256

- 2508c1dcc08421741f5c2ad81aea72148d5a7b23bdf5fc84292b914a56448ad6
- e79c501ec0282d7dd54b3c9da23489858726eee953b391d2e3f9f40044ce4e2e
- a9a3cf652bccfa1482aa9856a8c3ffe6ecd932d877f807cbe657130bd93f4de9
- 271fc69b06a989c8a860578cce97e42a0db94d58fec14544acfaabf2af7a8d9f

SHA-1

- 349ec0e5a86969ef2cb141e3023e0aba43d0c667
- 949c34a65a802cb2b7f1bbb66ba8841582d6d255
- eddc78b0d682cbef73b9982dcd197e82e2e4213c
- e2486a5ad2c182dd5d09cb36d1bc86ee6a2088ac

Remediation

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