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

Filename

- HashtableDebugV[.]exe

MD5

- 809e2358238ce40472671e9b9d983a09
- d8ee01a14dae8e3706a4c71db3491c9e

SHA-256

- 6f77b02eff6c8b9189c9a395390c4e77ac6f5d8285db813e78734854c6e65538
- 1f7e0fe7c2541395a0c7ed0dcd7d6caabd70c4008da3fa27025780b2e3e2fcfe

SHA-1

- d9f60342a9498b44659189efe3a5b4c098ce4bdb
- c5f438c2151e1c22fdc0c284fc827f7ec915bc79

Remediation

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