Severity

Medium

Analysis Summary

Malspam is being used to target victims in an Agent Tesla campaign. Since its initial appearance in 2014, this has been deployed in many forms, most notably via phishing attempts. AgentTesla is renowned for stealing data from a variety of target workstations' apps, including browsers, FTP clients, and file downloaders. Agent Tesla grabs data from the victim's clipboard, logs keystrokes, captures screenshots, and gains access to the victim's webcam. It has the ability to terminate running analytic programs and anti-virus applications. In an attempt to disguise its capabilities and activities from researchers, the malware also runs simple checks to see if it is operating on a virtual machine or in debug mode.

Impact

- Sensitive Data Theft
- Credentials Theft

Indicators of Compromise

MD5

- ed6c3affc857b3c9af61a94e5313bc63
- 3897c0761d49ee750227926c212e89d0
- 6ed68595e87126c3cef7a9d300cfad35
- e5529c0318d92343626438fe0369e184
- d322c4039bc1f109d0e9f7863dbe1bbf

SHA-256

- c68afaf02a334124389e9c37c9a9e5736273d214221ecd384d5fae394117515b
- ecb5f786cbcfdf84840bec703bfdfe364c3d73c141bc37ebc7b868b4fc8324af
- 837f2f991aa1b7ae610c46d0db95d7434425ba9cb28b40b64d0b805d0949c0a4
- 5b5dcfe775133de6691978d840c3ee4e6691f244068c1ad607bd15e206a8fc20
- b14a0b1b447bd5c5eea69ca9c8ad663958f9c23c6c0f77d8d814a42df7a4ec36

SHA-1

- 6981bd62801d483e3a3f02a1e20646a7b54a504b
- 9cf641468a565639d133b663e7bb3bccc93de516
- 991ac5602f5cd43f9599057effe3614ba81e4247
- 3c553b4055516a44ed798b4f9f49c637f9538c8c
- 7a285070671c10c317a178460ba2ad111e959fd7

Remediation

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