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

- 8da9b05fd038121414d0ca3d44518133
- 0292d736142e81cbc35310de782b78ba
- d084050073da47d34f39f8f471ead57c
- 6d1dd90ab41d602d97658749563526fc
- 8626cfdf80a099bdc60f54f36552ea26
- b5ff1bcda92e477b09da89dd802508b7
- 0e741508f192e755948e9d522955569b
- 79cf0c907bf11bb416ef0950e81b5042
- ef0bfed39df203f1a6f902c4f091cc76
- 709782a1984c34c24f41f1fb0a96cd5d

SHA-256

- 2f4df54e63d52ee02191565ea5787e1ecbbdf070433a5a986561ebf78abcb91d
- fb1afa6e7bae619514d7d2ff10a9cc96a03b5e10640059f592c7e5f3d6093d31
- c5ed23b273a18cbe37e250a41fbc72faac02ffff6877c37ed33661e445f1001e
- c21a8dd72ddc290ddef34bcf4af46c4fa56a5aba45b612ebcaa4eb4a1b955993
- d71cf7a62479b0575847eeafd4acf947866a82dba4614ea9cd9493a8f59a85b3
- 1b7382ea2de070f5b428fc1cab6608b28f475e928ac8bc26ab30bbfa21703a5c
- d039a7ce3ad7b04f31e216966f1fb8f7bd90f982df74dfa34a7ae228f1b6efab
- 6922c5cc87b43c29aedcc0ffa783587fd9f9ba05dbf5d2cdd07da01a50a8b931
- 5f3ebf73e8084a3f0e9d2249516ed683222d2922301afbb81645df80bfdc1b5a
- 36970d4f72161f9f6cbd444994359e0c416be009593960413870f5c0ebcf345b

SHA-1

- 07c6389c7ff2ec8aabec300cb2e3298838b6c95b
- cd76636de1d8fdda05909ec70a3022c865222df1
- 833d5623b1f349969e452b562fa40e8b2aa72fe0
- a5b4dfe0d8f5e6453c1c14bf57d9eccae8a68abe
- cb167b9de50fd0534a51fd7806f1080c98328e6d
- 4e0a070fa62602096eef4562d7f6bcb29cddf4a9

- e05de634a391db80fb4d89b4cf0474a1db0c43b1
- e73cb409884612b001f93d87ecb87acdf5e883d8
- 4b10f06af79f495aaf828f4632ac3ed72e6a9131
- 9525f3d3a49cc64bf616ff175a541372c5e1a061

Remediation

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