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

- a19f421ae981a064de2bb5266d8ded4c
- 375a259143403a173b32f29ae97f12e1
- 377eee86fc7eb8f94e79983f87e4bbd1
- 0460f138b09fedfe25112e6bebe76407
- 943e6aa650e7aed223b5ba62ec74c01c
- 2c31a00a50a72c3366ee31a684c3868b
- faf514c2e80b339e00c0576855c113b2
- 0908d567e0bcbd6c1c774fe5cf6408a2
- dafb5f90a7e12d6c989b1b3be1ff45f4
- f699aabbc3cb7e60c9d4438c23ee1fad
- ce1fbbc13247772eb945dedbf98d63d1
- 3dc482fc808624a30b33c22f01bf3383
- 9f8508a8d462fce66853aaf6d92aff85
- 55d8a0869cafd95a1c004e78e1de3c7d
- a334f4371987c64cc5110ec5468a5a05
- 981db7c13aa8543dca5f534b45ffa2bc

SHA-256

- 1eb519d5fc2a3c747e4be5fd4308efe26606024b53059e40839874240514769f
- 2d7973f6cfe587d100f824851c0f2fb5f897387fe372a7d24019ccf362252aa1
- 3cc46b047dce85c4ddf9f39894a6c67e42fe985e9835303e35f204a12b09c512
- 4dec45a4095ce92e7bc46962358c73f3e52b57a13128947fcebeeed3d866ff5e
- 29950f41687b112e2a061fcb1f73449e804afc9531d879eaab0ab3c03134a570
- 4a439eeff9ac89541417b65a07f9d3a9359dd72d23502f49a8d4e8945cfb7e78
- 4fec5400f6123353f23459460c3329573f7b4f0a473082ed1e0dbb3ca3c36e80
- eac3905ad73fd40904c78250a66f960fd1814e3d0abc10301f13f6e17bb079ea
- 0a840e0d003dbbe94510ba7ce6db2c41e5bcdbe4d8dfcb8f1a8b0f15d710419d
- 5d49dfb5e3ee04074a1e7972bb57e1edc37b4783c5b6c356036a36442dac2a48
- 0ba9062b8eb11757bc473d870b85bb111f251d7e3b6e615133c01c99c6076a15
- 7686ac2172f774100227dc9bd20239a503225adf567c183e1354e5858bbefbce
- 4ac70e6596359a19fddd3380edc192f01f7e789c9cf8dd3afa68fd5f9ef8bdb5

- ea036e229b606c5ba247854bd37c2dba7ea2c244ea587053d534b352c5058336
- d9c638afabe803afbe1949b402858ce3875395791a524cb56ae0e8369645424c
- e28373004354934e8cdfd0b7edfbaeab53f2d9d6c97992db5e572b9489ef61dc

SHA-1

- fa9ebd9b24a95adfc134d2d7dbbae54c6f9e8ea6
- 70716f1bf103d965f1dfd86360f62b2dfb1794f9
- 20585418c8a1041cdf503d39e607e53a3ad60698
- 94d3d40b693eb81647931c0a00cefaf6bb588357
- 46b174894031dde159a6f12fbad63a2088cb40bc
- 4210dfead0f423bfe50df3bf64d901e25f41accf
- 2f705daa3f3716b4d8bcb95f277e1d14fa84bd9c
- 742ae3df153ce4ce4e10cc7a1f2ac072d8bacc43
- f52402ea9c8a6fefb872ce51a2fdfbbc212225b5
- d92016e303ec615360082e1b7e8c300608abf774
- 508dd9fd1e404d7ed5054bbfe096b36b10794c06
- c40f3768aa609d709564b2998d7530c06aba35ba
- 66c0be89117db63d88665de9f7cf3d4ab24d0768
- f6e0328447a0bb5fcaf6c0c6b23d630372579b22
- 47cad43d59e483bfdb70f11d24594603a2054836
- 72aed08de927b2bcce1d546bca0d320e6d54cb5c

Remediation

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