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

- 075977856d1c634ea311bdd1eba673b7
- e35acf9ae12109e5775a2af1f07e1bdc
- 3d4ec24237a79489058f48a5a8b33601
- 36d2cf00c94d60e1a6de0366cfa2dccc
- 02f133c03974c05bd22276da9acfcbc5
- 28b979714d777ecea89a0c0e7182ef78
- 19fd13d1e4efdd1788144184578ca2a7
- 5c88a7b42e9a27c99bd68d8379be1e28
- 8d8cec84fb1bdc0bcc1d8f80df6e4e6b
- 888cf173c9532faec808cf0aa62f6686

SHA-256

- b3bf452d980ca75487ef92e5728d5845184545d8c1c9c9b1d841f64bb38df8e6
- cc84f3e926202f3e913c474a280a193b2f7a754922ecdbde907571c7e98779d9
- f53a5b3e6d00972ac8130fbcf5ddae0bbc3cdd5e1cf0b132144853351f2178a8
- ebc915e13b69f6a63c78f82eba06a5852b18239dbe07a265a2b07ec5abad9aa8
- 1aed7661a990d34584f7687545b78a8debc0a905e91bdccb9f2160606c1965c4
- 89ce93397cc9b5fae1209e68500959ba10d348614540c108f128ab08c54d7904
- 35e7644f3ed1443d506d573df87e03d965d234f4ee4a94c3bcdbc5c4580e58b6
- 98386b2cb6643d632a2076067cee9d06e7feaef7719984697428f4fe1bbc8be5
- 8bf77994fb5759f8be8d739cd651531fda75de8888c7f579ccafbbadb3b3decb
- cbd8728918d019597b3355577293cb9bc108543fda09c002ae7a283b3a963431

SHA-1

- 8d94ff84e182a3a26393c2e2a5cabb38c1f292eb
- 55ad64524a7259be3df7e9af68cf12db2718a4ad
- b99b496e80e518552243ed09514c999ca9e08909
- 8307934cb68a868ff582a8ddc1c74431d466f0a6
- 34805b82703e6b279d1240c3c164a7c3c22088c7
- aa00dae1b2aea928997d2740c07374682996b06e

- 1307365f20aaaad1b0a34b4d3c650e13a0cc849c
- dbf4c18c4c5a771247a0dc101f567bd958eba867
- 6a759c813b6ab846bc324d5296c2619ca4de9b1a
- a237d892bf244351a060ba11494c5f3de39d7ca9

Remediation

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