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

- b7987801fc8e173a135e151c51f27663
- e0cb220561dc3b1ae0c18378b98e3b4b
- 077ff783b255796619df02d0c819aee9
- 4c9a0ea2f183052549589d03183d062d
- 398a6f26f2df1f3d54120c3dcc6220e1
- 655696d2ba16020542ae6074dbc40049
- 5307e08dcd8ff9cf4c38cb066cc22d23
- de770bfbba58dc7e5f2b5227b15dff4a
- bc88c4f1c6a5983dc7113da5477b4113

SHA-256

- 2b14c9d8a3433638ca27935ee55bb2475960dac0a5156ccc4e772178f8a8b3ea
- dd89073ba4011ceee15a47fc89991921e6f04eed784f43274061eedcaceb4101
- 74534c4cb0f08dd0a44b8ede96a94eb806ed48afbb262da8beb20622cae7b4b5
- dbb17754a83bb695ac98ad63058137acfb75b007c3f4c24d05aebeb1e6ecbe19
- 405c727aa97f9bcbc47fefb85dee0be2a96ce75e955d617408dfb38264f941fa
- 5384462d90fdc43f855c79de04aa68ef48ca5e41aec72464336f732034632c3e
- 4484bf0a4f9a9de34384f209652b833acb6a95c143252dc5552fbe02d3d8b9ee
- 99242cd4755c4c9aaaf4d39d77adec7981e6c4f25dbaefc5ecadddce576a35a8
- 4e4ca22f0ebfd1e09206da639566bcfb0db6cca9e94b402a07821ae5e64f0a2f

SHA-1

- 25a2f704bb208de579ce02c39a4508f3570a35e0
- e371d77ea3f9b304faf86abaa22031484a56fd6e
- c0b156bcfc34bc8009c5df4d714b81efef75a852
- 205baa1ddc2296848098ce02a87e8ef4816d875a
- fa5aa7938f17480212ef7fdf0929f8d2a6197236
- eb3aff5d6966b225eb62f0f7ddddaf4c76a50527
- 93ea94d069aed1d3ae45b138183c0f162671263f
- e101c210c4db7e1ed5a3129f2cd79c57b37b944e
- e7c42b178efe4da8f85cf7c6d83898b41fe9394b

Remediation

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