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

- b812c58db819c2dd9093791d9bca72ee
- b35d42ee49c4b498e280725080d14684
- 645d920866ea103c537d915fcaf29c20
- 39412a282eb93e170a0a4aa68120d4e1
- 2d82b3e22b17fac0f67fbf1b56cd7082
- 2e338d17a10c5c6c6bde9fb903af70e2

SHA-256

- 4c934702874a158c678f5fce2404c52e0ef0382bb82771dc2ab5f4e9e68139a9
- 25264afa4264c96a9c6edca538ad90847080d899da89821ccc5bf651b0ab332d
- d506c3c06f79c0d09973b62938a0927b0ef9591114a13fa80c4c4b072c485b7c
- 5517fb2f61d9a5ebdaa32b241f919bbe53c7f8d25962afa992650f1fe002e18a
- f54abb130531be6b10246e80aab676e13f3d635d701140dda46befe1b39511f2
- 990f36639c443ec3624323f7a23bbe4b03da06aedf9f353e65c2575e3638026a

SHA-1

- c6c49b3dea65910bac895d79df0e3710fb2daec3
- 006c9fc8e999a136a0fd9732294fa27ec5425bd1
- 0795b8e02ec43a9ae4a4a0930f126ee1498f91de
- 745b6ccf66d19c966425a48e5a7b973e0b28e6d4
- c87a546375b5b3ba99c3616f4254600e0527ab12
- cead2a4251ce5648b78eb0d4e0b01afd26f0d264

Remediation

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