Severity

Medium

Analysis Summary

The NanoCore remote access Trojan (RAT) was first discovered in 2013 when it was being sold in underground forums. The malware has a variety of functions such as a keylogger, a password stealer which can remotely pass along data to the malware operator. It also has the ability to tamper and view footage from webcams, screen locking, downloading and theft of files, and more.The current NanoCore RAT is now being spread through malspam campaign which utilizes social engineering in which the email contains a fake bank payment receipt and request for quotation. The emails also contain malicious attachments with .img or .iso extension. The .img and .iso files are used by disk image files to store raw dumps of either magnetic disk or optical disc. Another version of NanoCore is also distributed in phishing campaigns leveraging specially-crafted ZIP files which is designed to bypass secure email gateways. The malicious ZIP file can be extracted by certain versions of PowerArchiver, WinRar, and older 7-Zip. The stolen information is sent to the command and control (C&C) servers of the malware attacker.

Impact

- Credential Theft
- Unauthorized Access
- Theft of Sensitive Information
- File manipulation
- Remote command execution
- Keylogger

Indicators of Compromise

MD5

- a93162e62b49a591e0d481e030ffc9ea
- f32d1f6e94da654932e73e42f0f4773a
- c1b99cb9c9cf56fe0355737e4e5df1fa
- 08c261ade5c2d31437da373d90a2f6d0
- a6fe8903e741154bc80352d0ee73efff
- 55d261de4ebfec14610e3019bdb47e1d
- 717fc8318eb370b1e8ae630af9fe431d

SHA-256

- 692bb93169319eba2f556174d781a8636d610a67e6838e19300a8a2454cd8b2b
- 43f670b439ef8ea9765ef3a61e84f1997e3dfd30067dc11c3203caf258553398
- 425e84ac9fe60970bd317ede9d84555b1f994e9c2c102e44d6ed71e7f47797c6
- 17952248625aaa9c25208dc4ab2d7849aa39d2c189aac5b26fe2f3d130301e1a
- 63ad21733d5e1db06faa9c863422889ae1f185116e02b45a50259e286ee42e50
- 28a8b5760f88ff56fccac79f506aa87de847161f5b3af7158792d098a60785dd
- 6035a6b2488b6c073d4b1cda9c9879e207b73e94c3551624667e59cc8719dd01

SHA-1

- b0c48a0fc418977051bea837c16aa7928f654da7
- 04e51bb4dedfc85cb6d4dfceb3bf48bf69c2a58a
- c02627c990717d30ff577c6fbd6381393ade7bb1
- 2a18a2cefe110cfee786afabaed53db3af3b0e4b
- 772e00c83eeae03ea4c7433f737b8d6a1d8b967e

- a89750499dca367037b9388a820e8fb56cd2f3bb
- 842ee97ed218857603188de6831afcc9919addd6

Remediation

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