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 the 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

- 5d56cd68112d48c35090e75b3edaa12e
- e8570f34b94b6baae24ee25c4fa37b6e
- f660105b981e29b734fa4e9d5baf9c19
- 0c2bcc0df599b5a9406b9a9419d59d11
- 985b93a87d4baab2ffb35755c335e263

SHA-256

- 25d7fa2bfc89484d806bae297d6b5b81ff2de51f93d414c5ba9b86c0dff1a513
- e8ee83f88ca4002f3705768b89c154e280e7b30ec022ae9ee54988c9499a9560
- ef83f00952dab1229b5943f9afde55837ef0d46d3dfe6b11063d85bbd4a1a8fe
- c2f156ddeef8be85d38f8483656d9d657bf8f147657dfbb18b84a235c2bcada2
- 46864364581f4a18b628a1b68bfe231d72f4f871eaa712c1c3150cb01c65e6bc

SHA-1

- 9acc881fc4eef8deaedd8ab98aecb86434ce52a9
- 802787ea5e9b6ab2527c00bbe47e65a2fac20faf
- 2262d8aa62f88fc7874f7ae91d4dbe414d345dd6
- 0a16121f6c9cf340574c7a31e811628449897186
- 18c305201980cb2ee6aebfbaae4b3f9ce7402b55

Remediation

- Block all threat indicators at your respective controls.

- Search for IOCs in your environment.