Severity

High

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

- 95dbab0a97c0a5f40d3683350cef8143
- e33ba5da7314b38e6e96adf915247583
- 5fd5e6453bf579a1dd628a75dbef6071

SHA-256

- aec74de68b784abd0b40a123a06480e09c3f00cceb88245e766606ea8650eb4a
- 221d26db1c7c1a27ed2e31cc8efe06ff53b3dafbab4f86a5396c54f31f514aa3
- 3bb2d01333b78a2d4b58a3d27e22c7f84ce2a1fa277f8a4d9034a482389dfc25

SHA-1

- c6fa75767a45a4707ca1bdfb86a4a027398b42da
- 6ea2f11597e7eba75fb9ade48ef0cfe7b49a00ea
- 85503c3679f13c622b983714ef34eca279c96f29

Remediation

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