Severity

Medium

Analysis Summary

W32/Shodi-F — a virus targeting Windows platform — seeks to infect all files with the EXE extension, except for specific Windows system files. W32/Shodi-F specifically targets Scandskw.exe, Winmine.exe, Sol.exe, Pbrush.exe, and Notepad.exe files in the Windows folder. After targeting, it creates a thread to look for additional exe files on the system, including any open network shares to the infected host. W32/Shodi-F drops Troj/Remadm-C, a remote administration Trojan, and also drops JPG file to the Windows system folder with the USR_Shohdi_Photo_USR.jpg filename.

Impact

- Information Theft
- Credential Theft

Indicators of Compromise

MD5

- 7225f35065084d717b92f6287141adbb

SHA-256

- c91a787fa8a0ea2eeea74d2694902bb1b552b22450d0a312e2ad2954d088e999

SHA-1

- e25645ee1048bc5a781e7b1dbfe2e4ce9a03391b

Remediation

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