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

- bc4460ed81c5f44b20b8905f40129896

SHA-256

- a2a9244ab528189b5fdcdf248b0571b0e83896ff8a5400450cdb60fcd66cd020

SHA-1

- 48d50843836d802e2fc97d43ad7fa59bd993ce80

Remediation

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