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

- 395ce2aca9a3d8ad874c2c061fa6a610

SHA-256

- e43428c32fa34a6f075f99254fc03552481579b656444f4f9c27e4a8e61b936e

SHA-1

- 6ab3b1fc71c665321269694cc2c274adbf7282f4

Remediation

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