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

- ae2901bab810c3d65352ec82b00e8605

SHA-256

- 849b799a93fc53889229c731b298c9eea699f93790e0387589a155852fb53213

SHA-1

- af8ddb111e5936a655c44b45b2ee171be4a56d93

Remediation

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