Severity

High

Analysis Summary

The AZORULT malware is an information stealer which was discovered in 2016. This malware steals IDs, browsing history, cookies, passwords, and other information. AZORult serves as a malware downloader and it was advertised on Russian underground forums as a way to extract sensitive data from compromised computers. Browser history, bitcoin, ID, cookies, and passwords can be stolen by this malware. Phishing emails and the Fallout Exploit Kit (EK), in combination with social engineering tactics, are the primary infection vectors for the AZORult virus. The virus can also act as a loader, allowing more malware to be downloaded.

Impact

- Information Theft
- Credential Theft
- Exposure of Sensitive Data

Indicators of Compromise

MD5

- 683600b61a32d3eb2cd44cb34fdf7ab3
- d9f8fa114ba4c96934ef33c8c24f14d5

SHA-256

- 26f35270f714065705474f3a330a9b7676c2d7e30b9cb9de57d726930768fe29
- fd48ebb9c6da16d3f371ee0e1bd94c7027ffacb7b99d27e59c81c8504477fd60

SHA-1

- e8bdd864c2610495850bf525cd1529c66c0b0b53
- cf45ccff33f4d30ef174010cb5d52247f4f0b7e3

Remediation

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