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

- 0ed0dfc93eea20875ed5729a9ce86c78
- 704a31dfd70783dac991a46617da8df5

SHA-256

- 7e69c34a04cb51232232893684f6560b6ea5e3160bd0d5810f6e5ff03f5e2eb3
- 91614aabdbf98ad426f806edd1c9d8fcb3f36b011280aaebb92c7d9d066d0215

SHA-1

- f3d66aa80320d256cdb9c802599e7f4361a0c5ac
- c4b9a27429c2c0be46a5b213756d6e960e624689

Remediation

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