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

- 729abfeeb8eed93812d752bd9a6a0799

SHA-256

- 61d5fbc6b18acbb1728b17ad4123f269292992dc826282e1db0a46da953ec665

SHA-1

- 148755e5a180ab2eb4f0f38afbbc99c523cbfd18

Remediation

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