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

- e003da977b301d2cbfe38e2198db861b
- 994d16ca9cb22b04a86920acf52977d6
- 164076414dd3be991ebc9d4d17101296

SHA-256

- 0558b42ee8b76a1b9c7da99b76e90083dd5f6b7b9dcd7218d2bcb069b4a48003
- 1555f5962f947a48940133ac60dd5b4c9c4afa10b159247d85682b0fe2f87b92
- 219156c02502e38cfd6273b4293f737b8404c043de6df402b322e813f3a223f0

SHA-1

- d9eed4b23772b1509e1427041a58d5fd2be766ef
- 92e28299742f638a6825f7902a82657258936a6c
- 0fa986a6834c79eb1b756b1a05954d96a770e4d7

Remediation

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