Severity

Medium

Analysis Summary

In early 2016, LokiBot was originally made available on underground forums for cybercriminals to use against Microsoft Android phones. This malware steals sensitive information including, usernames, cryptocurrency wallets, and other credentials via Trojan software. Malware grabs credentials by monitoring browser and desktop activities from the password storage using a keylogger. LokiBot can also install a backdoor into affected systems, allowing an attacker to install other payloads. Spam emails, communication channels such as SMS, Skype, and malicious websites are all used to spread LokiBot. To keep track of what users are doing (for instance, recording keystrokes), this malware can be utilized.

Impact

- Information Theft
- Exposure of Sensitive Data
- Credential Theft

Indicators of Compromise

MD5

- 2aa6d5fafd87e8987d39ccfe3471b468

SHA-256

- e0fb87e9ad0d063d8627006f57bf3a75fdd2ee4f4dcd4ff7933b8a6a3a41eab4

SHA-1

- 0b6ed48cc277482913d65d2edd5a2b2298b37e47

Remediation

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