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In early 2016, LokiBot was originally made available on underground forums for cybercriminals to use against Microsoft Android phones.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. This malware is utilized to keep track of what users are doing (for instance, recording keystrokes).

Impact

- Information Theft
- Exposure of Sensitive Data
- Credential Theft

Indicators of Compromise

MD5

- a13e3b18282318c65f096bad322b3c50

SHA-256

- ba981a94852325debf0e4b478266f6efd8e4e9c5b149fd9ad277be0be5045768

SHA-1

- 2c76179e95e583b588bcd516e94e7a2da52d5299

Remediation

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