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In early 2016, LokiBot was originally made available on underground forums for cybercriminals to use against Microsoft Android phones.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

- ae9148f46dd287d9e9722a31813aab72
- b988bdca9e73cce5010b470fe1466d26

SHA-256

- 12fbae486c3533a58dec8921ecdf9343158e04a2cf71c04f2c91c0e181743446
- a11bfd4c7f64298ec17dfea5949e980a53bcc2e810b064eabd6dc995381ae139

SHA-1

- bd6a300b9fe49d81d3e7c6432d8c33b79361f5d0
- 0a9d6fbdba04b82e067a979af90dccbef74d1f9b

Remediation

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