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In early 2016, LokiBot was originally made available on underground forums for cybercriminals to use against Microsoft Android phones.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

- 7ba0a67eba8abd1e0300e152729c49e6
- 3369ce745b233c6036e13b9b9cea8478
- cc35a94fc2833c0fb64c802aed458bec

SHA-256

- 526b7a200e7b6d1851c412d911a9715213f02d488ea850ab969dbe76e246c532
- 1cbd3ecf572c37b93f699661da9a981d88a35cc4d27e8048dfeac01f2cdd706f
- 135b69d3c201ad8634d1ac39177dea87226dd58621829e42ac3023c29b0b5f7b

SHA-1

- 1be37eced573802e0a152b7391ea8d9e2b32d401
- a414919109c896ce480f0d0cc601be9dd09ba7cb
- ca070b329c9bef01ee5df8800f78f81db67de83f

Remediation

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