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In early 2016, LokiBot was originally made available on underground forums for cybercriminals to use against Microsoft Android phones.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

- 113e2d59524e5ad25183f99a3860a713
- a44e337c68747accaac5122754261182
- 0a8e67551962b74ff294c2b33524bd0b
- dd65c776ddb51f61c843cea948cba2cd

SHA-256

- ce2927d527d4f74dbea54d4a3b048ac19b8fdaedb4fef9dc709b75de4ce0b447
- 00120d86ee7297543c0c9537ac1f22569d5eca13ba55e49ba9c06fb06d05180f
- 001e74b98d8f65bc9170ef6921743b7f269f26f837ac59d358a2d224b41782fb
- 002539c07b8f32f3f900d652276dacc893e328f41f4baeedda70df85b5785916

SHA-1

- 36918d346e9ed885a5cd988a08035a5070fde255
- 8b2786cfd5e9685215afd36612f35c342ce0ea2e
- 593502b394dce2fbbe88fb30559693cf207067c4
- a3484c3750f49b16539b6193ee8224332aed91a5

Remediation

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