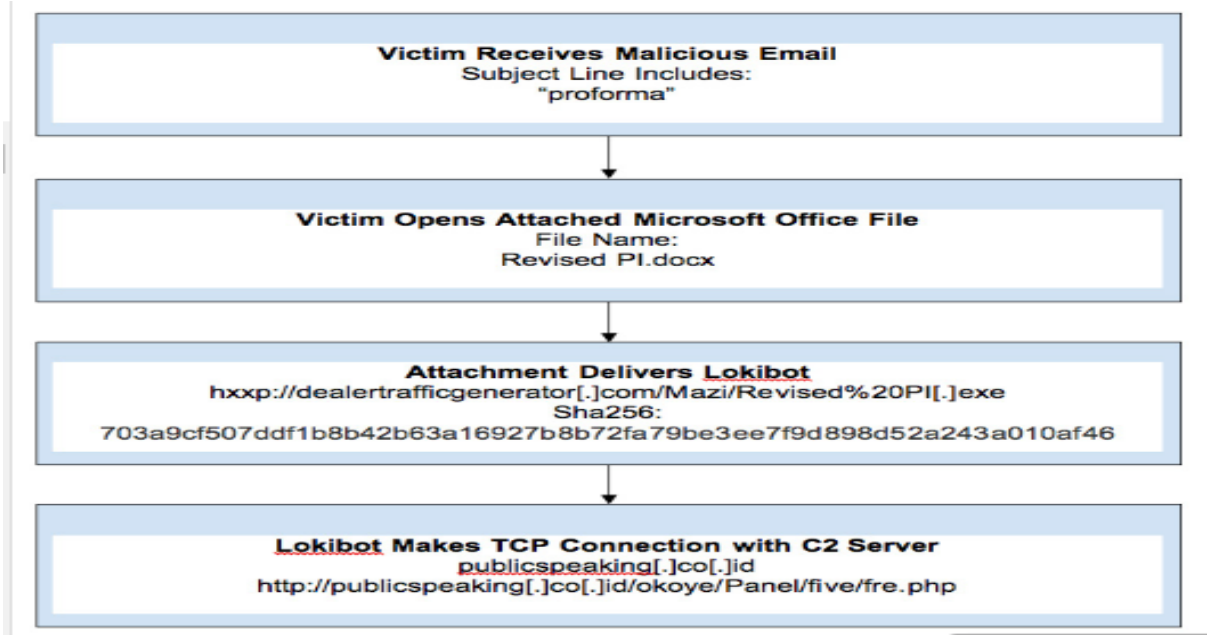
LokiBot Malware
(CSB20-17)

SUMMARY

- **LokiBot Malware** infects computers and use its built-in capacities to search for locally installed apps and extract credentials from their internal databases.
- It evolved and now comes with a real-time key-logging component to capture keystrokes and steal passwords for accounts that aren't always stored in a browser's internal database and a desktop screenshot utility to capture documents after they've been opened on the victim's computer.
- Functions as a backdoor, allowing hackers to run other pieces of malwares on infected host and potentially escalates attacks.
- LokiBot payload is delivered via MS Office files - by exploiting a vulnerability in Windows known as CVE-2017-11882.
- The method used to deliver LokiBot, which involves an MSI installer, has been used in the past to deliver low-grade threats and Potentially Unwanted Program (PUPs), such as adware and similar threats.

HOW IT WORKS



SECURITY RISK

LokiBot Malware is capable of collecting login credentials, data from the infected computes, cryptocurrency wallet login credentials, and track keystrokes and other actions executed on the infected computers.

RECOMMENDATION

- Download software from official sources;
- Scan all software downloaded from the internet prior to executing;
- Maintain up-to-date antivirus signatures and engines;
- Enforce a strong or multifactor authentication and password; and
- Keep operating system patches updated.

MITIGATIONS

- Be cautious when browsing the internet and downloading or installing software;
- Limit access to sites with unsuitable content;
- Restrict user's permissions to install and run unwanted software application;
- Enable a personal firewall on workstations;
- Scan and remove suspicious email attachments;
- Exercise a caution before opening email attachments; and
- Be vigilant in using removable media like external drives and USB thumb drives.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa20-259a
- https://www.enigmasoftware.com/