ITMS
INFORMATION SYSTEMS SECURITY DIVISION
PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
INFORMATION SYSTEMS SECURITY DIVISION

TrickBot Malware (CSB20-19)

TrickBot is a banking trojan that was designed to steal user's banking credentials and digital wallets via dynamic and static injection attacks.

TrickBot malware is usually spread through MalSpam (Malware Spam) or email campaign that used current events of financial lures to entice users to download and open infected documents or click links to websites hosting malicious files. Once the user downloaded and opened the document, the malware will infect the computer and begin spreading across the network. In some cases, TrickBot is used to infiltrate a network where it can be used to deploy other malware, including ransomware and post-exploitation toolkits.

Once infected, TrickBot can download new capabilities onto the user's device without consent or interaction from the victim. TrickBot can also perform the following attacks:

- Gather detailed information about infected devices and networks
- Steal saved online account passwords, cookies and web history
- Steal log in credentials from infected devices
- Download further malicious files such as Remote Access Tools and ransomware

HOW IT WORKS

1 Threat actor sends TrickBot malware via email that contains malicious links or infected documents to unsuspected users

2 Once the recipient clicked on the link or downloaded the attached document, the TrickBot malware infects the computer, enabling threat actor to steal personal information and spreads across the network

IMPACT

- Steal financial data and other personally identifiable information (PII), infects computer with ransomware that may encrypt victim's files.

MITIGATIONS

- Do not open emails or download files from unknown sources;
- Use latest version of operating systems and software;
- Apply and keep security patches up to date;
- Regularly conduct anti-virus scanning on your computer and network;
- Use multi-factor authentication (MFA), also known as Two-Factor Authentication (2FA);
- Store a backup copy of files offline to reduce impact of ransomware;
- Keep antivirus software up to date; and
- Regularly change passwords to network systems and accounts. Avoid reusing passwords for different accounts.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- https://www.cisecurity.org/white-papers/security-primer-trickbot/