PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
INFORMATION SYSTEMS SECURITY DIVISION

Emotet Malware
(CSB20-18)

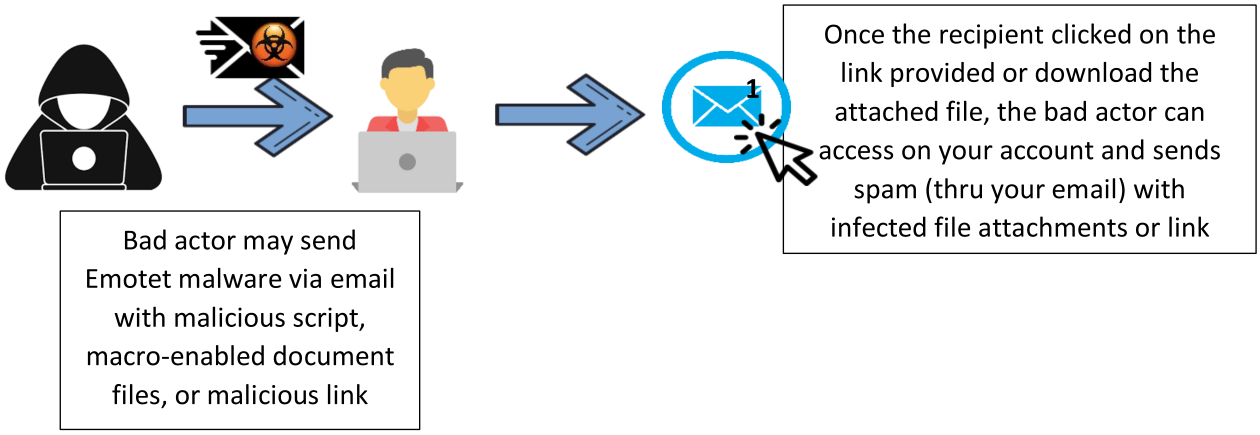
Emotet is a kind of malware originally designed as a banking Trojan aimed at stealing financial data, but it's evolved to become a major threat to users everywhere.

It is primarily spread through spam emails. It ransacks your contact list and sends itself to your friends, family, coworkers and clients. Since these emails are coming from your hijacked email account, the emails look less like spam and the recipients, feeling safe, are more inclined to click bad URLs and download infected files.

If a connected network is present, Emotet spreads using a list of common passwords, guessing its way onto other connected systems in a brute-force attack. If the password to the all-important human resources server is simply "password" then it's likely Emotet will find its way there

The infection may arrive either via malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email. It may try to persuade users to click the malicious files by using tempting language from well-known companies.

HOW IT WORKS



Bad actor may send Emotet malware via email with malicious script, macro-enabled document files, or malicious link

Once the recipient clicked on the link provided or download the attached file, the bad actor can access on your account and sends spam (thru your email) with infected file attachments or link

If a connected network is present:

Emotet spreads using a list of common passwords, guessing its way onto other connected systems in a ***brute-force attack***

IMPACT

Steal financial data that can use by bad actors to ruin good reputation of a personnel

MITIGATIONS

- Block email attachments commonly associated with malware (e.g dll and exe)
- Block email attachments that cannot be scanned by antivirus software (e.g zip files)
- Keep your computer/endpoints up-to-date with the latest patches for Microsoft Windows
- Do not download suspicious attachments or click a shady-looking link
- Educate yourself and your users on creating a strong password. Use two-factor authentication
- Implement appropriate access control lists.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa20-239a
- https://www.malwarebytes.com/emotet/