Task-5: Case Study

Three Large-Scale Malware Attacks of Recent Time

1.*Emotet* (Prominent in 2022–2024)

Goals of the Attack:

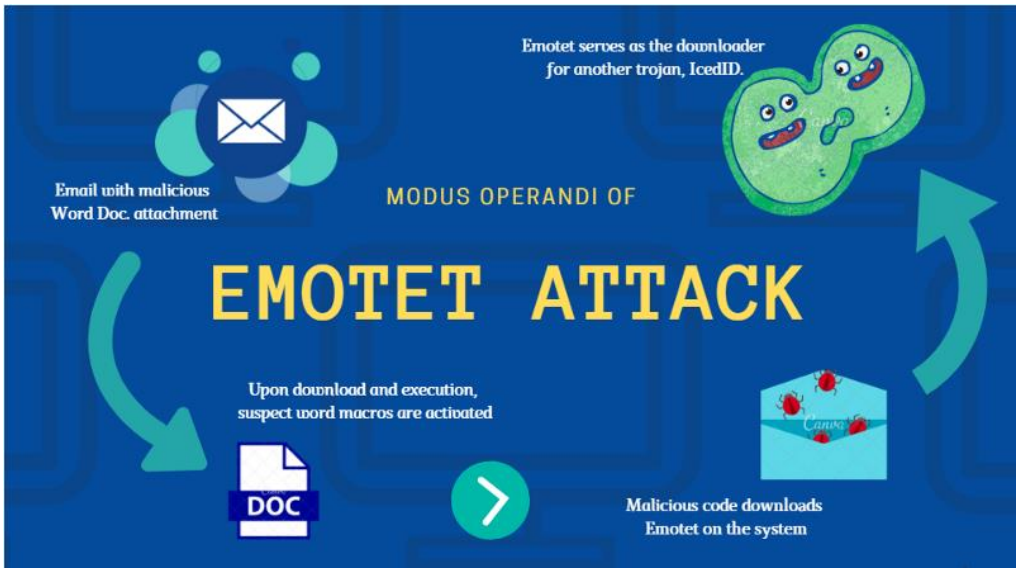
Emotet is a malware that started as a banking trojan and later mutated into a modular platform for delivering other malware. The direct objective is to gain entry into the computer systems through phishing emails, then steal sensitive data and other instances for attacks such as ransomware.

Impacts of the Attack:

- Disrupt individuals and organizations by stealing banking credentials, email contacts, and installation of other malware.
- Leads to email account hijacking.
- Leads to business outages and high costs of recovery and hardening.

Preventive Measures against Emotet:

- Train users to recognize suspicious emails and phishing links(provide awareness).
- Keep antivirus/anti-malware tools updated.
- Keep software and systems updated with security patches.
- Backup critical files and rescue them with strong passwords.
- Block malicious emails with an advanced filter.



2. Agent Tesla (Active 2019–2025, with a surge in early 2025)

Goals of the Attack:

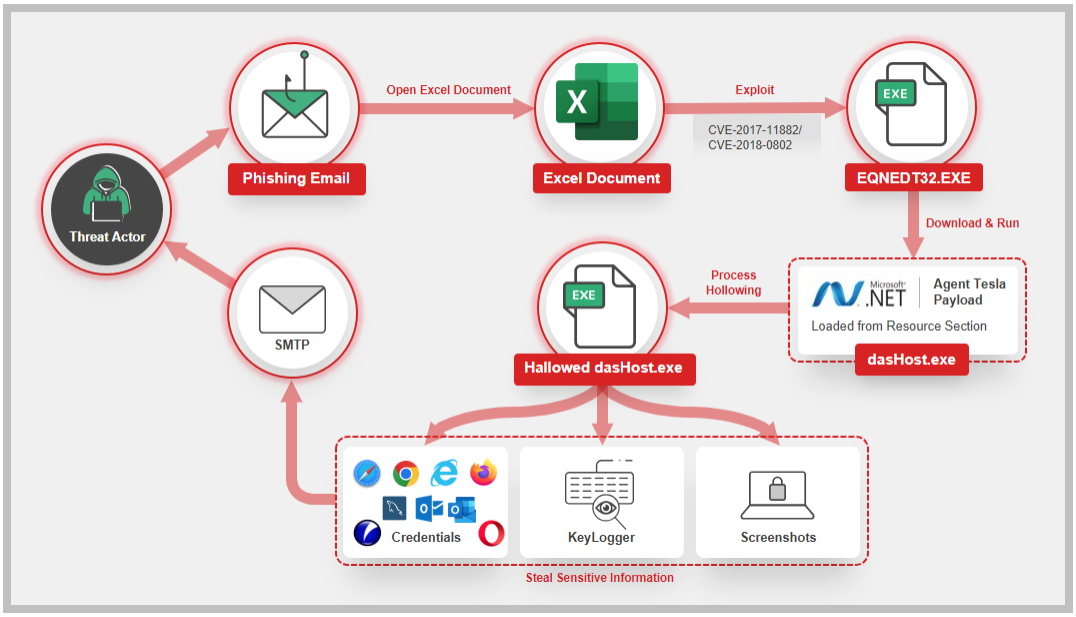
It is a kind of simple-to-use keylogger and credential stealer, mainly distributed by means of phishing emails. It logs keystrokes and captures screenshots and passwords for emails, web services, etc.

Impacts of the Attack:

- Credentials were stolen both for personal and business uses, thus causing financial damage and entering without permission.
- Attackers are thereby able to impersonate a user, send further phishing/fraud emails, and escalate data theft inside organizations.

Preventive Measures against Agent Tesla:

- Use anti-phishing email gateways and content-filtering options.
- Train employees to spot suspicious e-mails and attachments.
- Use multi-factor authentication (MFA).
- Track and limit account logins.
- Patch and protect all systems.



3. *Olympic Vision Keylogger* (Broad Scale 2023-2025)

Goals of the Attack:

Olympic Vision is a very basic keylogger that serves to record a user's keystrokes without their knowledge as the victim unknowingly types in their passwords, banking details or personal conversations. Olympic Vision was usually encountered as email attachments or downloads.

Impacts of the Attack:

- Loss of credentials & financial details that could be utilized for identity theft or fraudulent purposes.

- Gain of access to the victim's computer usage to track a person's habits, potential to install other malware through the keylogger.

- Most often caused breaches resulting in loss of personal data (i.e. data loss, privacy).

Severity:High

This attack could pose a serious security threat. You should take immediate action to stop any damage or prevent further damage from happening.

Description

This signature detects Spyware.SuperKeylogger communicating and requesting information from its controlling server.

Additional Information

When Spyware.SuperKeylogger is executed, it performs the following actions:

1. *Creates the following files*:
* %UserProfile%\Desktop\SuperKeylogger.lnk
* %SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Sklgr30\SuperKeylogger.lnk
* %ProgramFiles%\Sklgr30\1\aslee.log
* %ProgramFiles%\Sklgr30\appLog1.log
* %ProgramFiles%\Sklgr30\appLog2.log
* %ProgramFiles%\Sklgr30\Aslee.dll
* %ProgramFiles%\Sklgr30\config.dll
* %ProgramFiles%\Sklgr30\Mainapppath.sys
* %ProgramFiles%\Sklgr30\ms.dll
* %ProgramFiles%\Sklgr30\Naslee.dll

* %ProgramFiles%\Sklgr30\PCService.exe
* %ProgramFiles%\Sklgr30\SChal.exe
* %ProgramFiles%\Sklgr30\ServiceName.ini
* %ProgramFiles%\Sklgr30\Settings.dll
* %ProgramFiles%\Sklgr30\Sk.exe
* %ProgramFiles%\Sklgr30\sklgr.exe
* %ProgramFiles%\Sklgr30\UnInstaller.exe

2. *Adds the value*:
"sysApp" = "C:\Program Files\Sklgr30\sklgr.exe"
to the registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

3. *Monitors and records keystrokes, instant message conversations, and Web sites visited.*

4. *Periodically captures screenshots.*

Response

The following instructions pertain to all Symantec antivirus products that support security risk detection.

1. Update the definitions.
2. Run a full system scan.

Preventive Measures against Olympic Vision Keylogger:

- Do not open attachments or downloads received from anything untrusted peoples or suspicious emails.

- Ensure antivirus installations on all devices , and perform scans for malware on a regular basis.

- Ensure you are applying recommended updates by the software developers to mitigate any vulnerabilities.

Prepared for: *MuLearn Bootcamp*

Prepared By: *Atul H*

Date: *17/08/2025*