View this email in your browser

FLINT.

21/01/2021

SEKOIA THREAT INTELLIGENCE **FLASH REPORT**

Malware

EMOTET Update

OBJECTIVES:
FINANCIAL GAIN

STATUS:
ONGOING, PAST

INTRUSION SET:
MUMMY SPIDER, aka TA542

TTPs (MITRE ATT&CK):
Phishing: Spearphishing Link (T1566.002)
Phishing: Spearphishing Attachment (T1566.001)
Account Discovery: Email Account (T1087.003)
Archive Collected Data (T1560)
Email Collection: Local Email Collection (T1114.001)
Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
User Execution: Malicious Link (T1204.001)
User Execution: Malicious File (T1204.002)
Valid Accounts: Local Accounts (T1078.003)
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Brute Force: Password Guessing (T1110.001)
Command and Scripting Interpreter: PowerShell (T1059.001)
Command and Scripting Interpreter: Visual Basic (T1059.005)
Command and Scripting Interpreter: Windows Command Shell (T1059.003)
Create or Modify System Process: Windows Service (T1543.003)
Exfiltration Over C2 Channel (T1041)
Exploitation of Remote Services (T1210)
Obfuscated Files or Information (T1027)
OS Credential Dumping: LSASS Memory (T1003.001)
Process Discovery (T1057)
Process Injection: Dynamic-link Library

Injection (T1055.001)
Scheduled Task/Job: Scheduled Task (T1053.005)
Windows Management Instrumentation (T1047)

AFFECTED SECTORS: **ALL**

IMPACTED GEOGRAPHIES**: WORLDWIDE**

Summary

First detected in 2014, the first strains of Emotet were designed as banking trojans, operating to target banks customers worldwide.

The malware is authored by Mummy Spider aka TA542. A financially-motivated group. This group usually conducts their attacks for a few months before ceasing operations until they come back with a new variant of the malware. Emotet operations paused in October and November and returned in the end of December last year.

Since 2016, Emotet’s new variant has not been acting as a banking trojan anymore, but rather as a self-propagating worm and a loader delivering other malware. In 2020, Emotet was indeed used to deliver secondary payloads such as Trickbot, Dridex, IcedID and Qbot, which took part in the installation of ransomware such as Maze, Ryuk and ProLock.

Analysis

Emotet is a modular malware in which each module serves a specific purpose that enables the malware to:

- collect passwords stored on a system and from browsers
- steal contact list, subject, body and attachments from Outlook
- spread within the systems of the infected network using bruteforce, stolen credentials or by exploiting vulnerabilities

Delivery:

Emotet uses compromised Word documents (.doc) with VBA macros as initial insertion vectors. These are spread via phishing email attachments and links that, once clicked, launch the payload. Moreover, it uses a technique called "thread hijacking" whereby it steals an existing email chain from an infected host to reply to the chain—using a spoofed identity—and attaching a malicious document to trick recipients into opening the file. The latest phishing email tactics include attaching password-protected archive files (e.g., Zip files) to emails to bypass email security gateways and antiviruses.

Current malicious documents use VBA macro to run a Powershell script directly through WMI, or indirectly through WMI invoking cmd.exe prior to executing Powershell. In recent samples, the Powershell code executes msg.exe first to display a fake message “Word experienced an error trying to open the file.” before contacting a compromised website and downloading the Emotet executable.

C2 communications:

Emotet uses hundreds of command and control servers (C2s) in parallel in order to ensure uptime and bypass blocking. The C2 infrastructure is divided into three distinct botnets called Epoch 1, Epoch 2 and Epoch 3 that are identifiable by the RSA key used to encrypt network traffic. This RSA key is changed every month. Each Emotet sample embeds around 40 C&C servers on average in the IP:Port format. Most common ports are 80, 8080 and 443.

The botnet C2 infrastructure is highly hierarchized. For each Epoch, a malware sample communicates directly with a Tier-1 C2 server or with a “Bot C2s”, a compromised host that is used as a proxy. These Bot C2s do not handle actual C2 communications, but instead, act as a proxy by forwarding the communications on to a Tier 1 C2. In contrast to the Bot C2s, Tier 1 C2s are typically compromised webhosts which forward their C2 communications on to a Tier 2 server. There is a good chance that the C2 server will respond with a ‘404: page not found’ status, even though the body contains the encrypted replies.

Persistence:

Currently, Emotet achieves persistence through adding the executable to the registry key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. Other techniques have also been used in the past:

- Task Scheduler
- Service
- Startup folder

Actions on objective:

Emotet will exfiltrate emails and contact information stored in Outlook archives, which are then used to spread further (see Delivery). It will steal credentials stored on the compromised host and web browser and will also try to spread to other computers on the network through network admin shares or via bruteforce attacks.

Emotet may sell access to the infected computer to other threat actors and drop their backdoors. The operators of Trickbot, Qakbot, Dridex and IcedID are regular customers of Mummy Spider. They may eventually try to compromise the Active Directory to launch a severe ransomware attack.

Any Emotet infection should be considered a serious threat.

Course Of Actions

To prevent infection you may disable document macro in MS office. Training users to notice malicious emails should also be performed on a regular basis. You may also restrict Powershell script execution to allow signed scripts only.

To detect infected devices, you can use EmoCheck to see if a host is infected with Emotet, or you can check Indicators of Compromise in SEKOIA.IO or other public repositories such as:

- Feodo Tracker
- URLHaus
- Cryptolaemus

You could also consider monitoring Powershell processes invoked directly through WMI or indirectly through cmd.exe invoked by WMI.
Monitoring suspicious modifications to auto-start registry keys, startup folders, task scheduler and service execution may allow detecting an Emotet installation as well.

If you detect an infection, you should investigate the extent of the compromise, and check whether other malware have been downloaded. If you react soon enough after the occurrence of the event, you should isolate the infected computer from the network to prevent lateral propagation. If however you react a few days after the infection, try to avoid severing the compromised host from the network before a full forensics investigation is done as it may trigger a ransomware encryption if such adversaries have infiltrated the network.

To prevent lateral movement, enforce a strong password policy and consider using dedicated workstations for

network and system administration.

The best remediation posture is to reinstall the Operating System on the compromised computer(s), and reinitialize all access credentials linked to the compromised host(s).

Finally, an Emotet infection should be considered as a confidentiality breach. Search compromised emails for sensitive information such as confidential documents, customer information, network infrastructure information, applications credentials, etc. Report the theft of Personal Identifying Information to the relevant authority.

IOCs & Technical details

IOCs list is available on our GitHub repository.

All indicators are related to the Emotet Epoch2 botnet.

CONFIDENCE

HIGH

REFERENCES

- [ANSSI] Le Malware-as-a-Service EMOTET
- [JP-CERT] Alert Regarding Emotet Malware Infection
- [JP-CERT] EmoCheck
- [CISA] Emotet Malware
- [AnyRun] Emotet
- [Deutsche Telekom] Dissecting Emotet – Part 1
- FLINT 2020-163 - Beware of Emotet resurgence targeting France, Japan and New Zealand

SEKOIA.IO

You can now access all FLINT reports and associated IOCs on our SEKOIA.IO Intelligence Center web portal.

https://app.sekoia.io/

Our mailing address is:
SEKOIA.IO
18-20 place de la Madeleine
Paris 75008
France

Add us to your address book