



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

# HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY



## ATT&CK for Emotet

01/28/2021



- What Is ATT&CK?
- Why Use ATT&CK?
- How To Start With ATT&CK
- Emotet Malware Profile
- Recent Emotet Updates
- Emotet Threat to HPH
- ATT&CK Techniques for Emotet
- ATT&CK Mitigations for Emotet
- References

## Slides Key:



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



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



- ATT&CK framework developed by the MITRE Corporation in 2013 and released to the public in May 2015
- Stands for “Adversarial Tactics, Techniques, and Common Knowledge”
- Comprehensive matrix of tactics and techniques associated with malware families and threat groups
- Leveraged by cybersecurity professionals to better classify attacks and assess an organization’s risk
- Platforms: Windows, macOS, Linux, Cloud, Network
- Three different matrices:
  - Enterprise ATT&CK
  - Pre-ATT&CK
  - Mobile ATT&CK
- 14 tactics correspond to attack stages
- 177 techniques and 348 sub-techniques
- 42 enterprise mitigations
- 512 software / malware
- 109 groups
- And growing!

# ATT&CK®

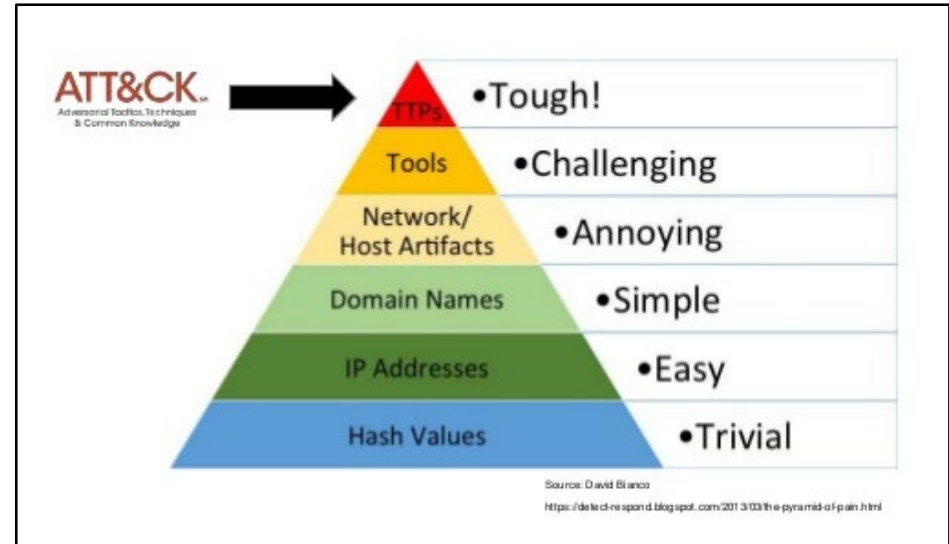
## Enterprise Tactics

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact

# Why Use ATT&CK?



- David Bianco's Pyramid of Pain (2013)
- TTPs are tough for adversaries to change!
- ATT&CK provides a framework for analyzing and defending against attacker TTPs
- Improve threat intelligence and detection capabilities
- ATT&CK helps teams communicate in common language
- ATT&CK can be leveraged by teams of all sizes and maturity levels
- Identify security gaps and rate detection coverage
- Compare TTPs across threat groups to identify overlaps
- Improve post-compromise detection of adversaries



Source: David Bianco





- Start small!
- Choose one threat group or software that targets your industry
- Choose one ATT&CK technique each week to discuss across teams on how your organization can detect, defend, and emulate this attacker behavior
- Collect one log source that will improve ATT&CK visibility
- What are the countermeasures or mitigations for each ATT&CK technique?



Source: iamWire

For more:

[Getting Started with ATT&CK](#) by The MITRE Corporation

[Using ATT&CK for Cyber Threat Intelligence Training](#) by MITRE

[Getting Started with ATT&CK: Threat Intelligence](#) by Katie Nickels





- **Malware Name:** Emotet (aka Geodo)
- **Malware Description:** Emotet is a modular Trojan initially associated with banking fraud which, since 2017, has been limited to spam and secondary payload distribution. There are hundreds of variants of Emotet and the malware continues to update with new capabilities and evasion techniques.
- **Malware Type:** Trojan
- **Associated Threat Group(s):** TA542, MummySpider, Mealybug; Wizard Spider, UNC1878, Temp.MixMaster, Grim Spider
- **First Discovered:** 2014
- **Last Active:** December 2020
- **Primary Distribution:** phishing e-mails
- **Malware Capabilities:** self-propagation, brute-forcing passwords, credential theft, defense evasion, lateral movement, persistence
- **Secondary Payloads:** Qakbot, Dridex, IcedID, Trickbot, Ryuk, Conti, ProLock, Zloader, and more.
- **Targeted Industries:** Pharmaceutical, Healthcare, Biotechnology, Government, Technology, Transportation, and more.



Source: ZDNet



## Feb 2020:

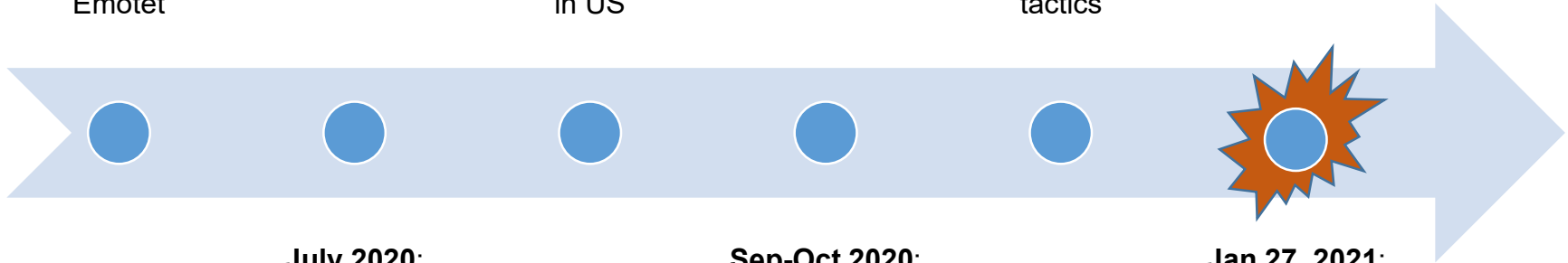
Non-US countries targeted with COVID-19-themed phishing emails to lure victims to download Emotet

## Aug 2020:

1,000 percent increase in downloads of Emotet loader with uptick targeting state and local governments in US

## Dec 2020:

Emotet returns with 100k daily emails and new evasion tactics



## July 2020:

US businesses targeted with COVID-9-themed phishing emails with previously used Emotet URLs

## Sep-Oct 2020:

Emotet surge impacting Canada, France, Japan, New Zealand, Italy, and Netherlands.

## Jan 27, 2021:

Europol announces international law enforcement takedown of the EMOTET botnet





- Authorities from Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol
- Emotet infrastructure involved several hundreds of servers located across the world
- The infected machines of victims have been redirected to law enforcement-controlled infrastructure
- Dutch police have launched a [website](#) that lets users see if their emails were present in Emotet's internal spam database
- Ukrainian police announced the arrest of two suspects who were allegedly tasked with keeping Emotet infrastructure up and running
- Possible that actors who remain at large could rebuild the botnet in the future
- Emotet will be uninstalled globally on March 25

## 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)

### How did Emotet work?

- Luring the victims:** Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.
- Installation:** If victims opened the attachment or the link, the malware got installed.
- Infection:** The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

### Emotet opened doors for:

- Information stealers
- Trojans
- Ransomware

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

### What made Emotet so dangerous?

- Long lasting:** Started as a banking Trojan in 2014, evolving over time.
- Go-to-solution for criminals:** It acted as a door opener for other computers, allowing unauthorised access to other malware families.
- Polymorphic:** It changed its code each time it was called up.
- Resilient:** Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.

### Protect yourself from malware

Always check your emails carefully and watch out for:

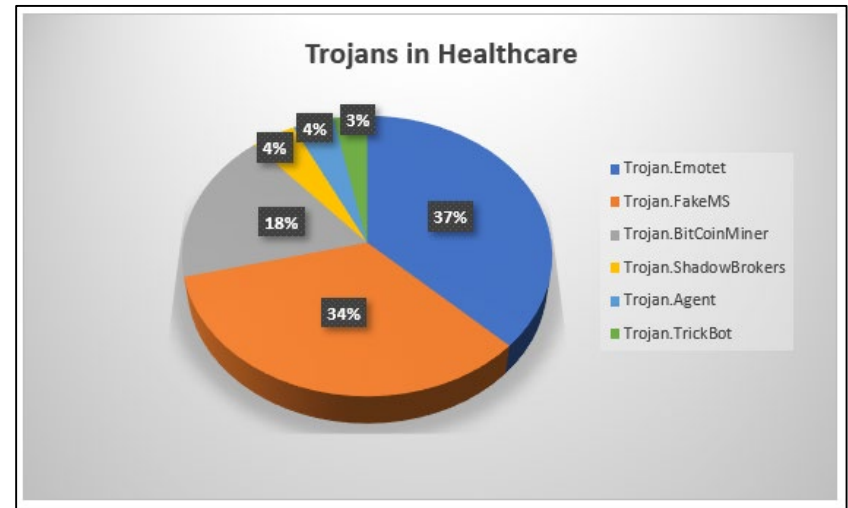
- attachments or embedded links from unknown senders.
- messages with a sense of urgency asking you to download something.
- offers with a promise of reward that sounds too good to be true.

Source: EUROPOL





- **April 2019: “Emotet Trojan Is the Most Prevalent Threat in Healthcare Systems” according to Malwarebytes**
  - 80% of malware affecting computer systems in the healthcare industry are Trojans, with the most common one being Emotet
  - 37% of Trojans affecting healthcare were a result of Emotet infections in 2019
- **January 2021: “Cyber-attacks on global healthcare organizations (HCOs) increased at more than double the rate of those targeting other sectors over the past two months,” according to Check Point.**
  - 45% increase in attacks on the healthcare sector, versus less than half this figure (22%) for all other industry verticals.
  - Ryuk and Sodinokibi (REvil) were highlighted as the main culprits and it is widely known that Emotet is often leveraged in Ryuk ransomware attacks



Source: BleepingComputer



- **Emotet hit a European country's national public health center in December 2020. The following details were pulled from media reports:**
  1. Phishing emails socially engineered targets to open Zipped archive with password included in message
  2. Malware was encrypted and password-protected
  3. Evaded anti-malware solutions by using password-protected archives as attachments
  4. Emotet loader contained benign code from a Microsoft DLL to evade antivirus solutions
  5. Thread hijacking to distribute malicious code using password-protected archives as attachments
  6. Compromised systems at the health center were leveraged to send malicious emails to other government entities in the same country as well as researchers
  7. E-mail systems shut down temporarily to stop further spread of Trojan
  8. Impacted internal networks
  9. Likely attempted to distribute Trickbot

### ATT&CK Interpretation

1. T1566.001 - Spearphishing Attachment
2. T1204.002 - User Execution: Malicious File
3. T1027 - Obfuscated Files or Information
4. T1036 - Masquerading
5. T1586.002 - Compromise Accounts: Email Accounts
6. T1586.002 - Compromise Accounts: Email Accounts
7. T1499 - Endpoint Denial of Service
8. T1498 - Network Denial of Service

# ATT&CK Techniques for Emotet (Graphic)



Source: Mitre





ATT&CK ID	Tactic	Technique
T1566.002	Initial Access	Phishing: Spearphishing Link
T1566.001	Initial Access	Phishing: Spearphishing Attachment
T1078.003	Initial Access	Valid Accounts: Local Accounts
T1059.001	Execution	Command and Scripting Interpreter: PowerShell
T1059.005	Execution	Command and Scripting Interpreter: Visual Basic
T1059.003	Execution	Command and Scripting Interpreter: Windows Command Shell
T1053.005	Execution	Scheduled Task/Job: Scheduled Task
T1204.001	Execution	User Execution: Malicious Link
T1204.002	Execution	User Execution: Malicious File
T1047	Execution	Windows Management Instrumentation
T1547.001	Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1543.003	Persistence	Create or Modify System Process: Windows Service
T1055.001	Privilege Escalation	Process Injection: Dynamic-link Library Injection

Source: Mitre

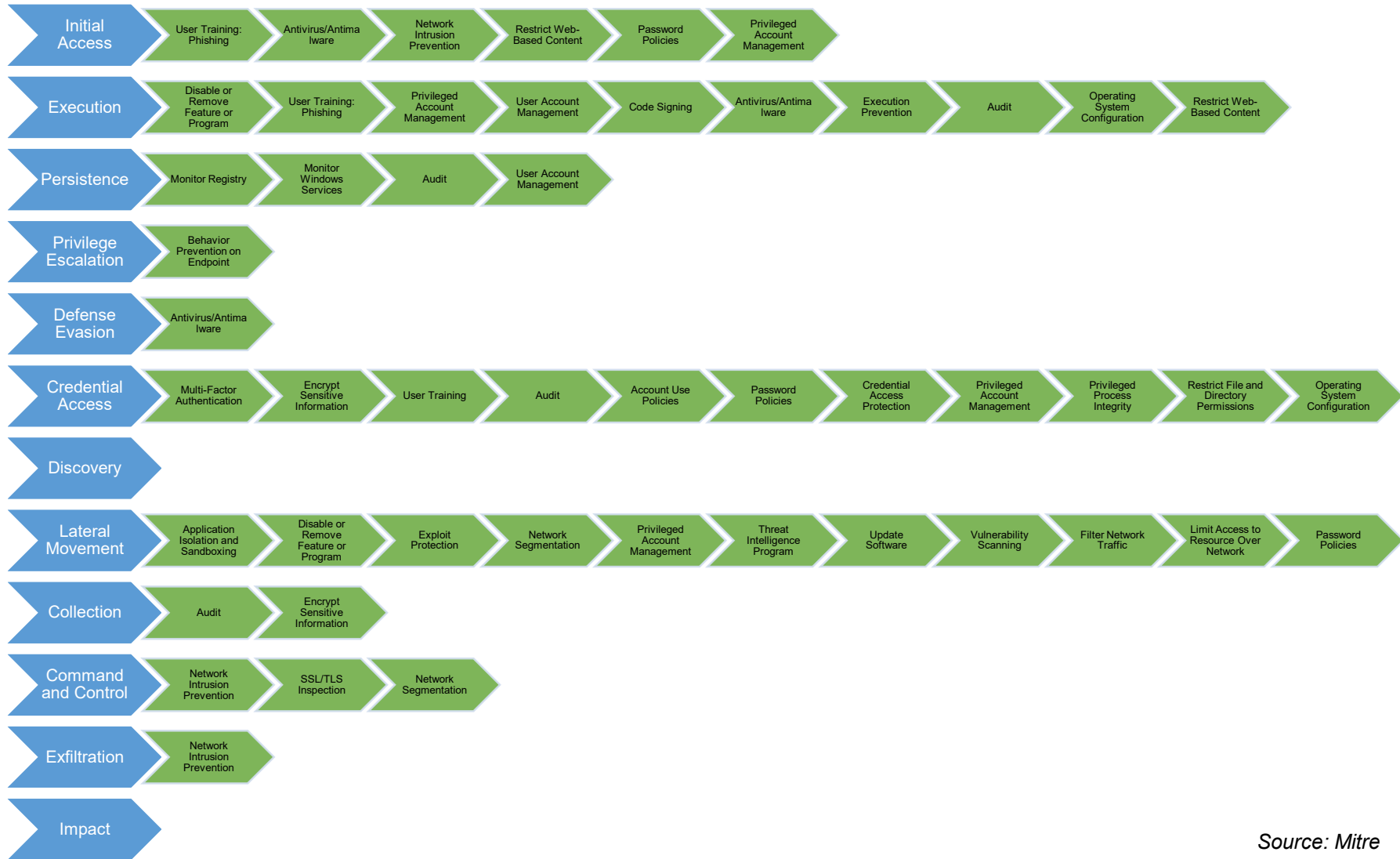


ATT&CK ID	Tactic	Technique
T1027	Defense Evasion	Obfuscated Files or Information
T1027.002	Defense Evasion	Software Packing
T1110.001	Credential Access	Brute Force: Password Guessing
T1555.003	Credential Access	Credentials from Password Stores: Credentials from Web Browsers
T1040	Credential Access	Network Sniffing
T1003.001	Credential Access	OS Credential Dumping: LSASS Memory
T1552.001	Credential Access	Unsecured Credentials: Credentials In Files
T1087.003	Discovery	Account Discovery: Email Account
T1057	Discovery	Process Discovery
T1210	Lateral Movement	Exploitation of Remote Services
T1021.002	Lateral Movement	Remote Services: SMB/Windows Admin Shares
T1560	Collection	Archive Collected Data
T1114.001	Collection	Email Collection: Local Email Collection
T1573.002	Command and Control	Encrypted Channel: Asymmetric Cryptography
T1571	Command and Control	Non-Standard Port
T1041	Exfiltration	Exfiltration Over C2 Channel

Source: Mitre



# ATT&CK Mitigations for Emotet (Graphic)

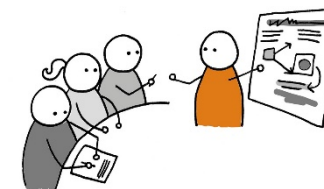


Source: Mitre





Mitigation ID	Mitigation Name
M1049	Antivirus/Antimalware
M1031	Network Intrusion Prevention
M1021	Restrict Web-Based Content
M1017	User Training
M1027	Password Policies
M1026	Privileged Account Management
M1045	Code Signing
M1042	Disable or Remove Feature or Program
M1038	Execution Prevention
M1047	Audit
M1028	Operating System Configuration
M1018	User Account Management
M1040	Behavior Prevention on Endpoint
M1036	Account Use Policies



Source: Mitre





Mitigation ID	Mitigation Name
M1032	Multi-factor Authentication
M1041	Encrypt Sensitive Information
M1043	Credential Access Protection
M1025	Privileged Process Integrity
M1022	Restrict File and Directory Permissions
M1048	Application Isolation and Sandboxing
M1050	Exploit Protection
M1030	Network Segmentation
M1019	Threat Intelligence Program
M1051	Update Software
M1016	Vulnerability Scanning
M1037	Filter Network Traffic
M1035	Limit Access to Resource Over Network
M1020	SSL/TLS Inspection



Source: Mitre







# Takeaways

- ATT&CK knowledge base and training is FREE!
- TTPs are TOUGH for adversaries to change which makes ATT&CK valuable from a security standpoint
- It is EASY to get started implementing ATT&CK!
- While Emotet was taken down this week, it remains to be seen if this will have a long standing impact

```

7701CFA0 C5CD  FFD ECK  LDS ECX,EBP  Illegal use of register C5CD
7701CFA2 FE  OS DWORD PTR DS:[EDI]  Unknown command 7701CFA2 FE
7701CFA3 FFE9  BYTE PTR DS:[EDX],ALCK  Illegal use of register FFE9
7701CFA5 AB  ADD BYTE PTR DS:[EDI],AL  7701CFA5 AB
7701CFA6 8402  SHORT ntdll  TEST BYTE PTR DS:[EDX],AL  7701CFA6 8402
7701CFA8 00BF 230000C0  ADD BYTE PTR DS:[EDI],BH  7701CFA8 00BF 2
7701CFAE ^EB E9  AX,38003000  JMP SHORT ntdll  DS:ECX,EBP  7701CFAE ^EB E9
7701CFB0 7B 00  BYTE PTR DS:[EDI],AL  JPO SHORT ntdll  7701CFB0 7B 00
7701CFB2 25 00300038  AND EAX,00003000  JMP EAX,EBX  7701CFB2 25 003
7701CFB7 006C00 78  STOS DWORD PTR ES:[EDI]  7701CFB7 006C00
7701CFB8 002D 00250030  ADD BYTE PTR DS:[EDI],AL  TEST BYTE PTR DS:[EDX],A  7701CFB8 002D 0
7701CFC1 003400  X,30002500  ADD BYTE PTR DS:[EDI+C00]  ADD BYTE PTR DS:[EAX+EAX]  7701CFC1 003400
7701CFC4 78 00  JS SHORT ntdll  EB,70000000  JMP SHORT ntdll  7701CFC4 78 00
7701CFC6 2D 00250030  SUB EAX,30002500  JPO SHORT ntdll  7701CFC6 2D 002
  AND EAX,38003000
Address Hex dump
00408000 40 10 40 00 49 10 40 00  UNIC
00408008 52 10 40 00 5B 10 40 00  002D 00250030
  ADD BYTE PTR DS:[30002500] 00408000 40 10 4
  ADD BYTE PTR DS:[EAX+EAX] 00408008 52 10 4

```

Source: BleepingComputer





# Reference Materials



- Bianco, David J. 2014. The Pyramid of Pain. January 17. <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.
- CISA. 2020. Alert (AA20-280A) - Emotet Malware. October 24. <https://us-cert.cisa.gov/ncas/alerts/aa20-280a>.
- Davis, Jessica. 2020. Emotet Malware Returns with 100K Daily Emails, New Evasion Tactics. December 31. <https://healthitsecurity.com/news/emotet-malware-returns-with-100k-daily-emails-new-evasion-tactics>.
- —. 2020. Emotet Malware Threat Actors Return with Massive Email Campaign. July 22. <https://healthitsecurity.com/news/emotet-malware-actors-return-with-malicious-email-campaign>.
- F, Axel. 2019. Threat Actor Profile: TA542, From Banker to Malware Distribution Service. May 15. <https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service>.
- Gatlan, Sergiu. 2020. Emotet malware hits Lithuania's National Public Health Center. December 30. <https://www.bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/>.
- Gutman, Yotam. 2020. Revisiting the Pyramid of Pain | Leveraging EDR Data to Improve Cyber Threat Intelligence. September 21. <https://www.sentinelone.com/blog/revisiting-the-pyramid-of-pain-leveraging-edr-data-to-improve-cyber-threat-intelligence/>.
- Lemos, Robert. 2020. Emotet Campaign Restarts After Seven-Week Hiatus. December 22. <https://www.darkreading.com/threat-intelligence/emotet-campaign-restarts-after-seven-week-hiatus/d/d-id/1339792>.
- Malwarebytes. n.d. Emotet. <https://www.malwarebytes.com/emotet/>.



- Nair, Prajeet. 2020. Emotet Botnet Returns After 2-Month Hiatus. December 23. <https://www.bankinfosecurity.com/emotet-botnet-returns-after-2-month-hiatus-a-15656>.
- Nickels, Katie. 2019. Getting Started with ATT&CK: Threat Intelligence. June 10. <https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f>.
- Oren, Shimon, and Dave Bitner. 2021. Emotet reemerges and becomes one of most prolific threat groups out there. Ep 165 | 1.9.21. January 9. <https://thecyberwire.com/podcasts/research-saturday/165/notes>.
- The MITRE Corporation. 2019. Mitre ATT&CK, Software, Emotet. March 25. <https://attack.mitre.org/software/S0367/>.
- Toulas, Bill. 2020. Emotet Returns for Christmas With a New Bag of Tricks. December 2020. <https://www.technadu.com/emotet-returns-christmas-new-bag-tricks/234489/>.
- Trend Micro. 2020. Emotet Uses Coronavirus Scare in Latest Campaign, Targets Japan. January 31. <https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/emotet-uses-coronavirus-scare-in-latest-campaign-targets-japan>.
- Wunder, John. 2019. Getting Started with ATT&CK: Detection and Analytics. June 18. <https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0>.
- Yizhak, Ron Ben. 2020. Emotet Analysis: Why Emotet's Latest Wave is Harder to Catch than Ever Before. August 12. <https://www.deepinstinct.com/2020/08/12/why-emotets-latest-wave-is-harder-to-catch-than-ever-before/>.
- —. 2020. Why Emotet's Latest Wave is Harder to Catch Than Ever Before – Part 2. October 12. <https://www.deepinstinct.com/2020/10/12/why-emotets-latest-wave-is-harder-to-catch-than-ever-before-part-2/>.



**Questions**



## Upcoming Briefs

- Threats in Healthcare Cloud Computing (2/4)
- Malicious SendGrid Campaigns (2/11)

## Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.



**HC3 Customer  
Feedback**

## Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV), or call us Monday-Friday between 9am-5pm (EST), at **(202) 691-2110**.

## 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. HHS does not endorse any specific person, entity, product, service, or enterprise.



*HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector*

## Products



### Sector & 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.



### White Papers

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



### Threat Briefings & Webinar

Briefing 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.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to [HC3@HHS.GOV](mailto:HC3@HHS.GOV), or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.

Visit us at: [www.HHS.Gov/HC3](http://www.HHS.Gov/HC3)



# Contact



[www.HHS.GOV/HC3](http://www.HHS.GOV/HC3)



(202) 691-2110



[HC3@HHS.GOV](mailto:HC3@HHS.GOV)