LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

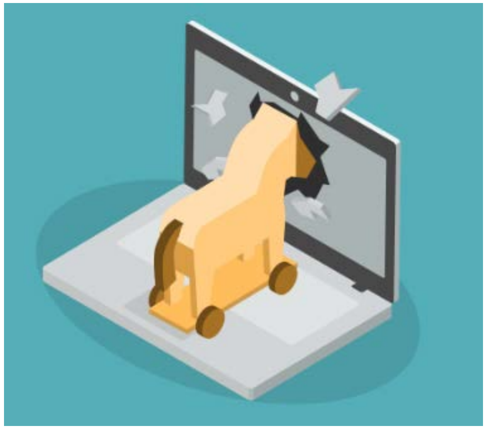
Emotet Update

12/19/2019

Report #: 201912191000

Agenda

- Overview
- Emotet 2019 Highlights
- An Emotet Xmas
- Emotet History/Timeline
- Emotet Capabilities
- Malware Spread by Emotet
- Infection Process
- A Sophisticated Campaign
- Mitigations
- Indicators of Compromise
- References
- Questions



Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

Emotet is an advanced trojan malware

- Designed as an banking trojan; has evolved into a malware delivery primer.
  - Has steadily become more complex over the years
  - Used to deliver other trojans and ransomware
- Has “worm-like”/self-propagating capabilities
- Primarily used for massive malspam campaigns
- Has modular capabilities for different functions

Once deployed, Emotet tries to:

Spread across network

1

Download any malware payload

3

Skim email addresses and name

5

Be a smokescreen for targeted ransomware

6

Send spam to infect other organizations

4

Steal browser histories, usernames, and passwords

“Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.” -US-CERT

Source: Pinnacle, US-CERT

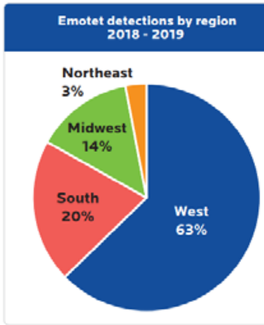
Emotet 2019 Highlights

Multiple research publications have highlighted the resurgence of Emotet campaigns in 2019, **especially within the healthcare industry**

A Malwarebytes “state of healthcare” report, states the healthcare industry has been overwhelmingly targeted by Trojan malware like Emotet, which increased by **82 percent in Q3 2019** over the previous quarter.

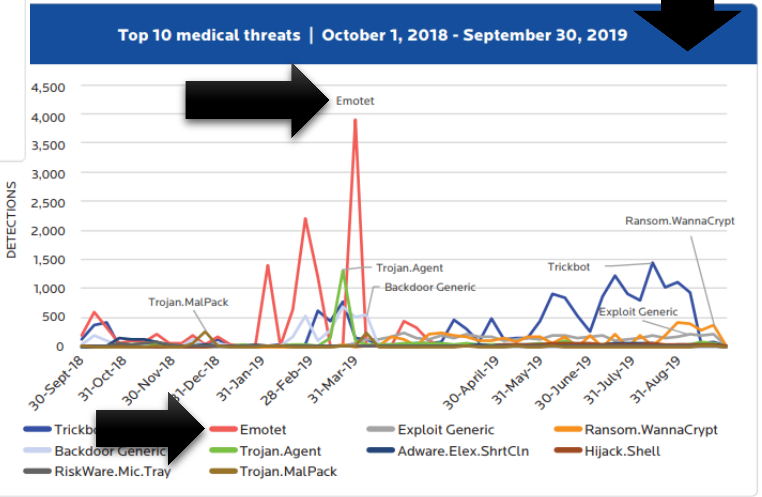
A Proofpoint threat report for 2019 Q1 highlighted that 61% of malicious payloads observed were Emotet

The two most dangerous Trojans of 2018–2019 for all industries—Emotet and TrickBot—were mostly responsible.



Emotet Detections in the U.S. Healthcare organizations

Top 10 malware medical threats, worldwide: 2019

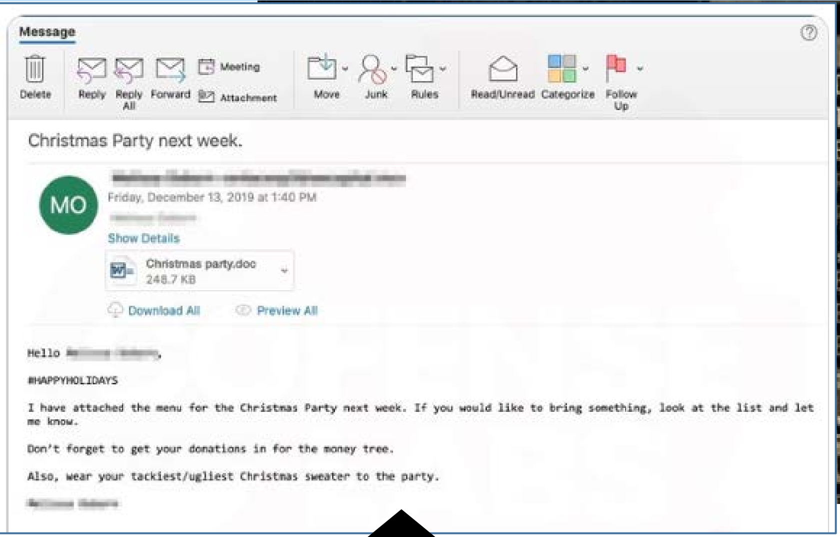


Phishing (Emotet’s primary medium) is the top attack vector for healthcare.

- A 2019 study found that hospital employees will click on 14% of phishing emails they receive.

Source: Malwarebytes, Proof Point, Bleeping Computer

An Emotet Xmas



Christmas Party next week.

MO [redacted]
Friday, December 13, 2019 at 1:40 PM
[redacted]
Show Details

Christmas party.doc
248.7 KB

Download All Preview All

Hello [redacted],

#HAPPYHOLIDAYS

I have attached the menu for the Christmas Party next week. If you would like to bring something, look at the list and let me know.

Don't forget to get your donations in for the money tree.

Also, wear your tackiest/ugliest Christmas sweater to the party.

[redacted]

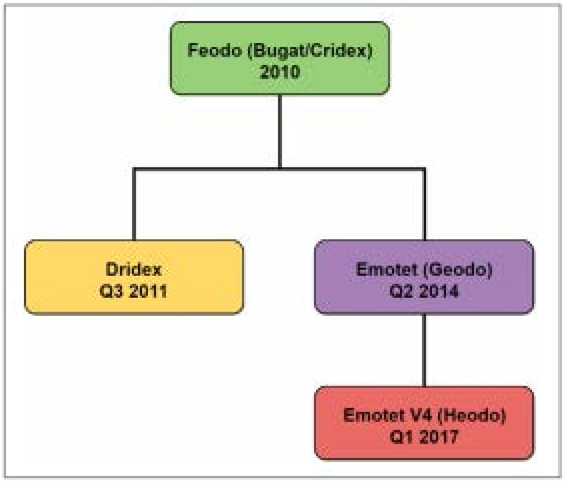
Phishing Email Example

- Security Researchers have observed Emotet botnets distributing Christmas-themed phishing lures.
- Malicious actors often exploit special events, holidays or even disasters to trick users.
- In 2018, a similar campaign strategy targeted UK users with Emotet.

Source: Infosecurity-magazine

Emotet History/Timeline

Emotet evolution from discovery to Present:



First reported in Germany, Austria and Switzerland in 2014.

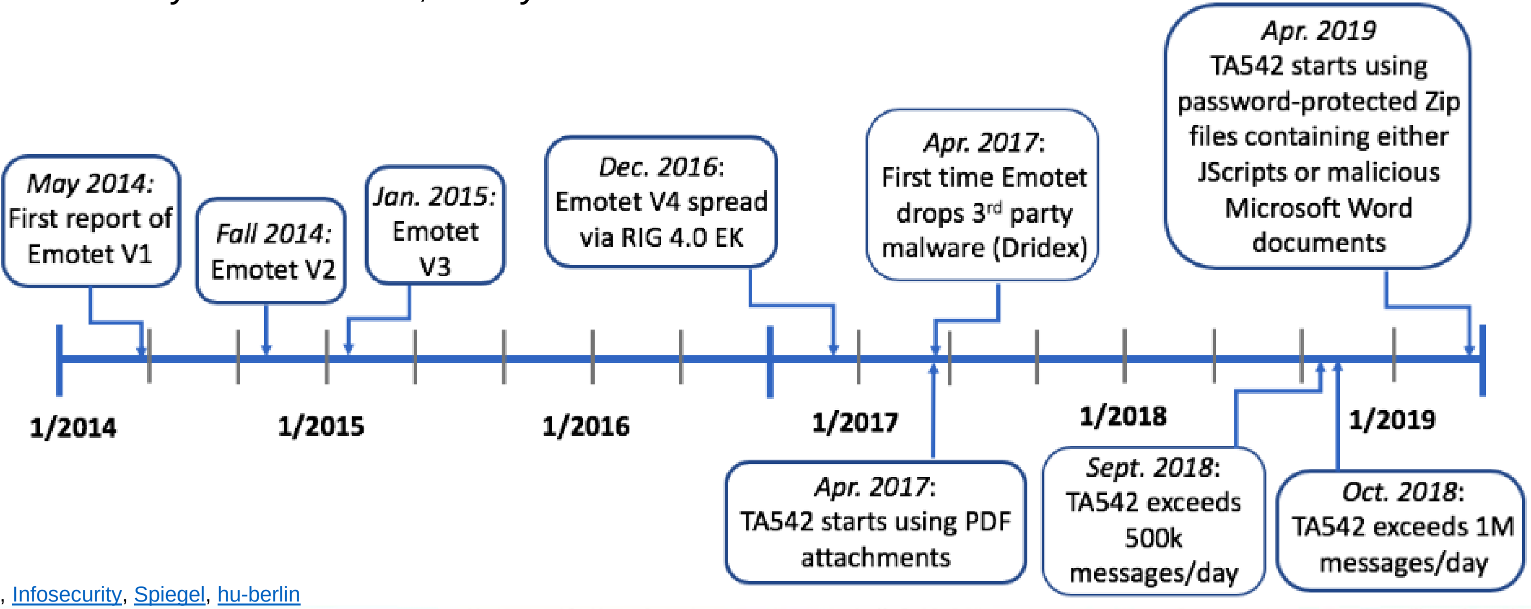
Noteworthy Infections:

City of Allentown, PA – $800k to $900k of damage

Heise Online – German IT/Security Website

Berlin Court of Appeals – Predicted to be offline until 2020

Humboldt University of Berlin – 43,000 systems affected



May 2014: First report of Emotet V1
Fall 2014: Emotet V2
Jan. 2015: Emotet V3
Dec. 2016: Emotet V4 spread via RIG 4.0 EK
Apr. 2017: First time Emotet drops 3rd party malware (Dridex)
Apr. 2019 TA542 starts using password-protected Zip files containing either JScripts or malicious Microsoft Word documents
1/2014
1/2015
1/2016
1/2017
1/2018
1/2019
Apr. 2017: TA542 starts using PDF attachments
Sept. 2018: TA542 exceeds 500k messages/day
Oct. 2018: TA542 exceeds 1M messages/day

Source: Proofpoint, Infosecurity, Spiegel, hu-berlin

Emotet Capabilities

Emotet Capabilities as of June 2019:

- Download and run other families of malware, typically banking Trojans

- Brute force attacks on weak passwords using a built-in dictionary

- Steal credentials from web browsers and email clients using legitimate third-party software, specifically NirSoft Mail PassView and WebBrowserPassView

- Steal network passwords stored on a system for the current logged-on user using legitimate third-party software, namely NirSoft Network Password Recovery

- Steal email address books, message header and body content

- Send phishing campaigns from hosts that are already infected, i.e. the Emotet botnet

- Spread laterally across a network by copying and executing itself via network shares over Server Message Block (SMB) protocol

Emotet has several anti-analysis features, designed to frustrate detection of the malware:

- A polymorphic packer, resulting in packed samples that vary in size and structure

- Encrypted imports and function names that are deobfuscated and resolved dynamically at runtime

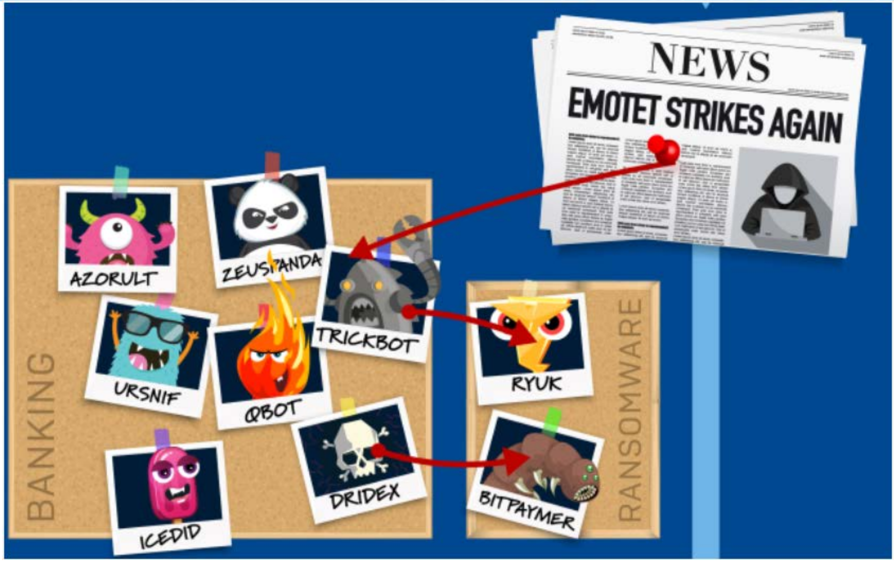
- A multi-stage initialization procedure, where the Emotet binary is injected into itself

- An encrypted command and control (C2) channel over HTTP. Version 4 of Emotet uses an AES symmetric key that is encrypted using a hard-coded RSA public key. Older versions of Emotet encrypted the C2 channel using the simpler RC4 symmetric-key algorithm

Source: Bromium, Proof Point

Malware Spread by Emotet

- Although it can be used as a stand-alone banking trojan, Emotet has evolved to serve as a distribution network for a variety of malware families.
  - Serves as a dropper for a other trojans
  - Used to download and spread ransomware
  - The combo of Trickbot trojan, and Ryuk payload have been widely seen in Emotet campaigns



Malware known to be distributed via Emotet:

Azorult – Credential and payment card information stealer

ZeusPanda – Trojan designed to steal banking information and other sensitive credentials

Ursnif – Banking Trojan spyware

Qbot – Wormlike information-stealing Trojan

Trickbot – Trojan spyware that steals banking information

Icedid – Banking Trojan which performs web injections on browsers and acts as proxy to inspect and manipulate traffic

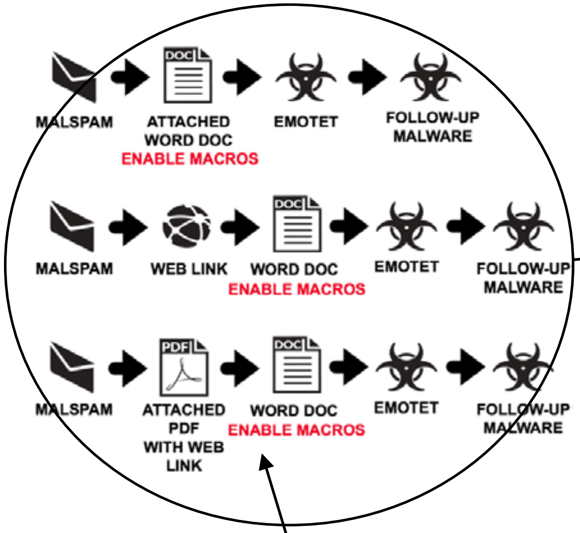
Dridex – Banking Trojan that targets banking and financial Institutions

Ryuk – Ransomware used to target enterprises and organizations

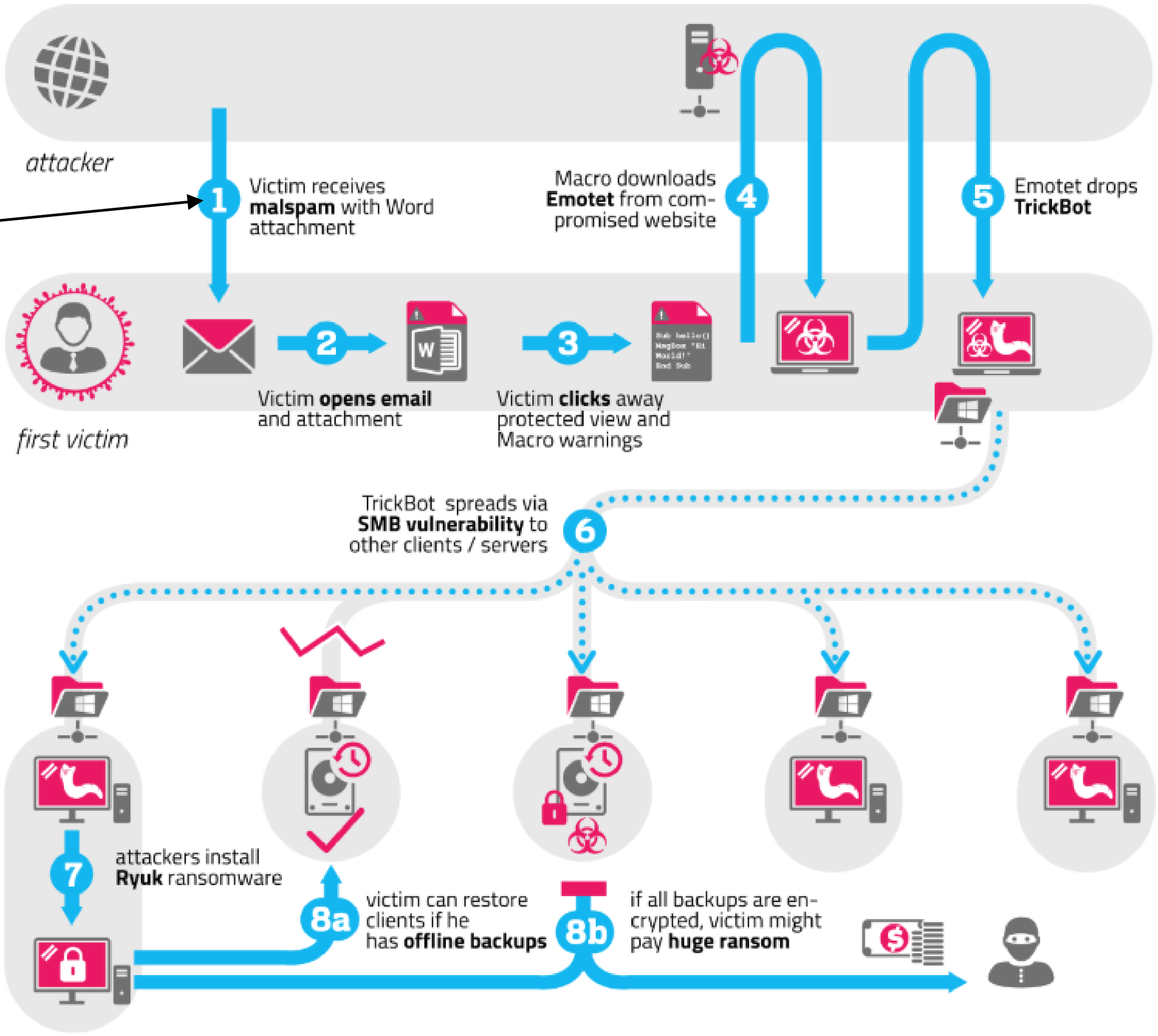
BitPaymer- Ransomware usually distributed via RDP compromise

Source: Sophos, Healthcareitnews, Malpedia, Trend Micro, Threatposts, Symantec

Infection Process



- Emotet infections are initiated by different malspam campaigns.
- A malicious email attachment clicked by the user will initiate the Emotet infection
- Once Emotet is downloaded it will, undetected, install Trickbot onto the host system
- As trickbot establishes command and control over the system, the attacker can then deploy Ryuk Ransomware onto potentially lucrative targets.
- Ryuk will begin encrypting target information on the system and send a ransom note to the victim.

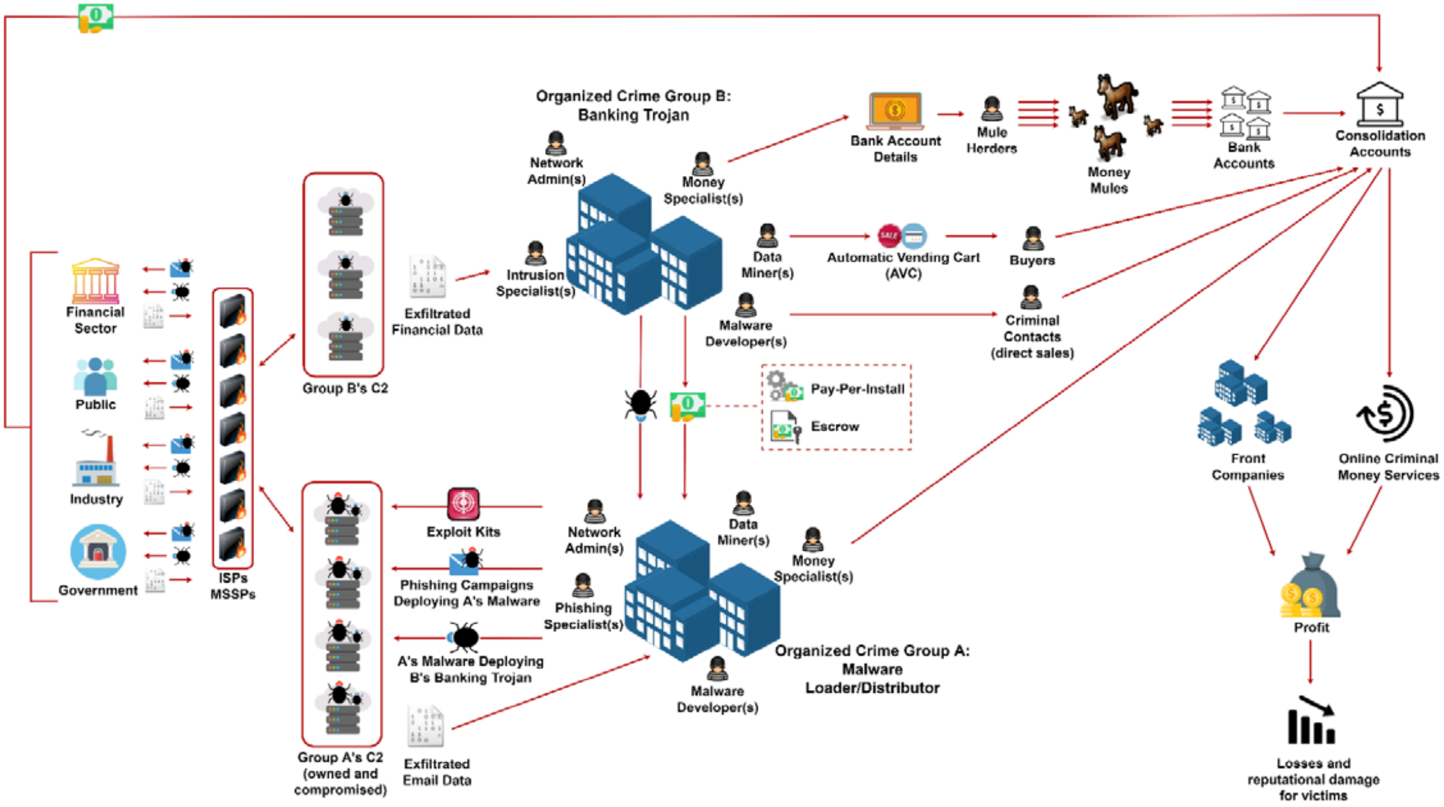


attacker
1 Victim receives **malspam** with Word attachment
4 Macro downloads **Emotet** from compromised website
5 Emotet drops **TrickBot**
first victim
2 Victim **opens email** and attachment
3 Victim **clicks** away protected view and Macro warnings
6 TrickBot spreads via **SMB vulnerability** to other clients / servers
7 attackers install **Ryuk** ransomware
8a victim can restore clients if he has **offline backups**
8b if all backups are encrypted, victim might pay **huge ransom**

A Sophisticated Campaign

- The rise in the underground economy has led to increased collaboration and dependencies between criminal actors.
- The Malware-as-a-Service model has been developed to enable low skilled criminals to utilize malware for malicious campaigns
- Research suggests Emotet's business model has evolved in concert with it's TTPs.

Emotet MaaS business model



Source: Bromium

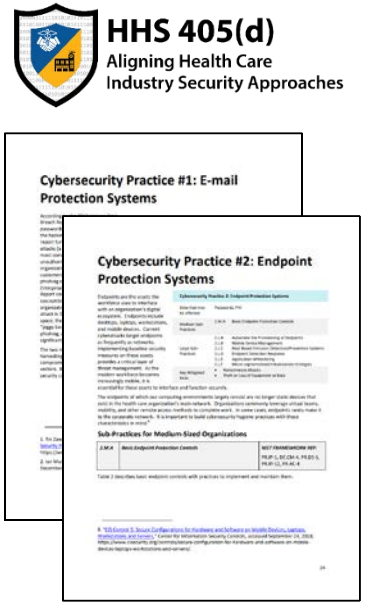
Mitigations

Remember!

- Enterprise spam filters are effective at blocking malspam that pushes Emotet.
- Properly-administered and up-to-date Windows hosts are not likely to get infected.
- Windows warns potential victims if such Word documents are downloaded from the Internet
- Recent versions of Microsoft Office have a Protected View feature that should prevent people from accidentally enabling Emotet macros.

Enterprise Best Practices to Safeguard Systems from Emotet

- ✓ Conduct user awareness training around spam emails and suspicious documents
- ✓ Implement the principle of least privilege to limit the chance of an attacker gaining administrative access (the malware requires local administrative access on the remote system to copy and execute from the $admin SMB share)
- ✓ Ensure the use of strong and unique passwords across the corporate environment
- ✓ Disable macros from running within Microsoft Office documents
- ✓ Software Restriction Policies (SRP) should be deployed to allow only known applications to run and prevent the execution of files from temporary directories
- ✓ Ensure that Anti-Virus software conducts scans in regular and frequent intervals
- ✓ Segregate networks and business functions
- ✓ Perform out-of-band network management on critical devices
- ✓ Block or restrict access to SMB file shares
- ✓ Implement account lockout policies for mitigating attempts to brute force access to other accounts and machines on the network in the case of an infection



HHS 405(d)
Aligning Health Care
Industry Security Approaches

Cybersecurity Practice #1: E-mail Protection Systems

Cybersecurity Practice #2: Endpoint Protection Systems

https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Source: ICS.SANS, USCERT

Indicators of Compromise

http://queenlady[.]co.za/cgi-bin/3tpzw_y2mypcfh_h58yuw5e_t80i2e9ryr/open_forum/7764901_LZjCWCK5PZ6/	2019-12-13 18:30:58
http://shabakesaba[.]com/wp-includes/available-section/8NTi1F-hlJ2tgSBvQPRe-profile/537755151597-BlXSy/	2019-12-13 18:30:54
http://showlifeyatcilik[.]com/m3on/private-ft7sd98z-miv9tnj/0u81d38t9-xbc0pzblq-iTsxeNl-dLG7QQBSLvQg/191b5F-gwGciLLiHmM/	2019-12-13 18:30:51
http://social.scottsimard[.]com/wp-admin/private_zone/test_tEXc_gEZtTDQrWcR/mst4g3uacorm_3t8u12w9sy/	2019-12-13 18:30:49
http://test.absurdu[.]net/wp-admin/common-zone/133924-2LYLygGJ0AAs-forum/5327552367-iZ15rKPi/	2019-12-13 18:30:47
http://www.setonmach[.]cn/wp-includes/multifunctional-zone/additional-warehouse/qiQi6OYR8-Kl0v8kr6/	2019-12-13 18:30:43
https://extremedeserttrip[.]com/wp-admin/yhqkw-il5aktcj-zone/corporate-space/GdWgnbcEjKma-676asp4h5/	2019-12-13 18:30:40
https://glacial[.]com.br/wp-admin/multifunctional-module/verifiable-space/75648040832-0WdlxGdg5l5/	2019-12-13 18:30:38
https://hdu23[.]design/wp-includes/multifunctional_module/special_profile/5688904869_TO3ETi/	2019-12-13 18:30:36
https://mydigitalcard[.]co.il/cgi-bin/73102-MGuHWU-module/corporate-mzNy-d7Ph5dvHi2A3h/ly8m2x5u74c4g-622z4238u3vuy1/	2019-12-13 18:30:34

Reference Materials

References

- Cybercrime Tactics and Techniques: the 2019 state of healthcare https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf
- Proofpoint Quarterly Threat Report – Q1 2019 https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research
- Emotet Botnet Behind Most Email-Based Threats in Q1 2019 https://www.bleepingcomputer.com/news/security/Emotet-botnet-behind-most-email-based-threats-in-q1-2019/
- Stop Emotet, the world's most advanced network worm https://www.pinnacle-online.com/blog/2019/march/Emotet-malware-it-security
- Alert (TA18-201A) Emotet Malware https://www.us-cert.gov/ncas/alerts/TA18-201A
- One Emotet infection leads to three follow-up malware infections https://isc.sans.edu/forums/diary/One+Emotet+infection+leads+to+three+followup+malware+infections/24140/
- Trickbot – An analysis of data collected from the botnet https://www.govcert.ch/blog/
- Threat Actor Profile: TA542, From Banker to Malware Distribution service https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service

References

- Allentown Struggles with $1 Million Cyber –Attack
  https://www.infosecurity-magazine.com/news/allentown-struggles-with-1-million/

- Emotet: Trojan attack on Berlin Chamber Court
  https://www.spiegel.de/netzwelt/web/Emotet-berliner-kammergericht-wird-opfer-einer-trojaner-attacke-a-1289919.html

- Data Protection Notice Regarding Emotet
  https://www.hu-berlin.de/en/press-portal/topics/attention-data-protection-notice-regarding-Emotet

- 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’s Central Position in the Malware Ecosystem
  https://news.sophos.com/en-us/2019/12/02/Emotets-central-position-in-the-malware-ecosystem/

Questions

Questions

Upcoming Briefs

- TrickBot

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

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

About Us

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

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently 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 document and presentation that provides 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 or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity
Coordination Center (HC3)

☎ (202) 691-2110

@ HC3@HHS.GOV