ATT&CK for Emotet

01/28/2021
Agenda

- 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)
What Is ATT&CK?

- 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!

**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
How To Start With ATT&CK

• 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?

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 Profile: Emotet

- **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.
### Recent Emotet Updates

#### 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

#### Sep-Oct 2020:
Emotet surge impacting Canada, France, Japan, New Zealand, Italy, and Netherlands.

#### 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

#### 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 Threat to HPH

• April 2019: “Emotet Trojan Is the Most Prevalent Threat in Healthcare Systems” according to Malwarebytes
  o 80% of malware affecting computer systems in the healthcare industry are Trojans, with the most common one being Emotet
  o 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.
  o 45% increase in attacks on the healthcare sector, versus less than half this figure (22%) for all other industry verticals.
  o 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
<table>
<thead>
<tr>
<th>ATT&amp;CK ID</th>
<th>Tactic</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1566.002</td>
<td>Initial Access</td>
<td>Phishing: Spearphishing Link</td>
</tr>
<tr>
<td>T1566.001</td>
<td>Initial Access</td>
<td>Phishing: Spearphishing Attachment</td>
</tr>
<tr>
<td>T1078.003</td>
<td>Initial Access</td>
<td>Valid Accounts: Local Accounts</td>
</tr>
<tr>
<td>T1059.001</td>
<td>Execution</td>
<td>Command and Scripting Interpreter: PowerShell</td>
</tr>
<tr>
<td>T1059.005</td>
<td>Execution</td>
<td>Command and Scripting Interpreter: Visual Basic</td>
</tr>
<tr>
<td>T1059.003</td>
<td>Execution</td>
<td>Command and Scripting Interpreter: Windows Command Shell</td>
</tr>
<tr>
<td>T1053.005</td>
<td>Execution</td>
<td>Scheduled Task/Job: Scheduled Task</td>
</tr>
<tr>
<td>T1204.001</td>
<td>Execution</td>
<td>User Execution: Malicious Link</td>
</tr>
<tr>
<td>T1204.002</td>
<td>Execution</td>
<td>User Execution: Malicious File</td>
</tr>
<tr>
<td>T1047</td>
<td>Execution</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>T1547.001</td>
<td>Persistence</td>
<td>Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder</td>
</tr>
<tr>
<td>T1543.003</td>
<td>Persistence</td>
<td>Create or Modify System Process: Windows Service</td>
</tr>
<tr>
<td>T1055.001</td>
<td>Privilege Escalation</td>
<td>Process Injection: Dynamic-link Library Injection</td>
</tr>
</tbody>
</table>

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

Source: Mitre
ATT&CK Mitigations for Emotet (Graphic)

Initial Access
- User Training: Phishing
- Antivirus/Antimalware
- Network Intrusion Prevention
- Restrict Web-Based Content
- Password Policies
- Privileged Account Management

Execution
- Disable or Remove Feature or Program
- User Training: Phishing
- Privileged Account Management
- User Account Management
- Code Signing
- Antivirus/Antimalware
- Execution Prevention
- Audit
- Operating System Configuration
- Restrict Web-Based Content

Persistence
- Monitor Registry
- Monitor Windows Services
- Audit
- User Account Management

Privilege Escalation
- Behavior Prevention on Endpoint

Defense Evasion
- Antivirus/Antimalware

Credential Access
- Multi-Factor Authentication
- Encrypt Sensitive Information
- User Training
- Audit
- Account Use Policies
- Password Policies
- Credential Access Protection
- Privileged Account Management
- Privileged Process Integrity
- Restrict File and Directory Permissions
- Operating System Configuration

Discovery

Lateral Movement
- Application Isolation and Sandboxing
- Disable or Remove Feature or Program
- Exploit Protection
- Network Segmentation
- Privileged Account Management
- Threat Intelligence Program
- Update Software
- Vulnerability Scanning
- Filter Network Traffic
- Limit Access to Resource Over Network
- Password Policies

Collection
- Audit
- Encrypt Sensitive Information

Command and Control
- Network Intrusion Prevention
- SSL/TLS Inspection
- Network Segmentation

Exfiltration
- Network Intrusion Prevention

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

Source: Mitre
# ATT&CK Mitigations for Emotet (cont.)

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

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

Source: BleepingComputer
References


References


Upcoming Briefs

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

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.

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.

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

About Us

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, or call us Monday-Friday between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3