Emotet Malware | CISA

Published: 2020-10-24 · Archived: 2026-04-06 01:08:10 UTC

Summary

This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

This product was written by the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC).

Emotet—a sophisticated Trojan commonly functioning as a downloader or dropper of other malware—resurged in July 2020, after a dormant period that began in February. Since August, CISA and MS-ISAC have seen a significant increase in malicious cyber actors targeting state and local governments with Emotet phishing emails. This increase has rendered Emotet one of the most prevalent ongoing threats.

To secure against Emotet, CISA and MS-ISAC recommend implementing the mitigation measures described in this Alert, which include applying protocols that block suspicious attachments, using antivirus software, and blocking suspicious IPs.

Technical Details

Emotet is an advanced Trojan primarily spread via phishing email attachments and links that, once clicked, launch the payload (*Phishing: Spearphishing Attachment* [T1566.001], *Phishing: Spearphishing Link* [T1566.002]).The malware then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives (*Brute Force: Password Guessing* [T1110.001], *Valid Accounts: Local Accounts* [T1078.003], *Remote Services: SMB/Windows Admin Shares* [T1021.002]).

Emotet is difficult to combat because of its “worm-like” features that enable network-wide infections. Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities.

Since July 2020, CISA has seen increased activity involving Emotet-associated indicators. During that time, CISA’s EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected roughly 16,000 alerts related to Emotet activity. CISA observed Emotet being executed in phases during possible targeted campaigns. Emotet used compromised Word documents (.doc) attached to phishing emails as initial insertion vectors. Possible command and control network traffic involved `HTTP POST` requests to Uniform Resource Identifiers consisting of nonsensical random length alphabetical directories to known Emotet-related domains or IPs with the following user agent string (*Application Layer Protocol: Web Protocols* [T1071.001]).

```
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727;
.NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR
```

Traffic to known Emotet-related domains or IPs occurred most commonly over ports 80, 8080, and 443. In one instance, traffic from an Emotet-related IP attempted to connect to a suspected compromised site over port 445, possibly indicating the use of Server Message Block exploitation frameworks along with Emotet (*Exploitation of Remote Services* [T1210]). Figure 1 lays out Emotet's use of enterprise techniques.

Figure 1: MITRE ATT&CK enterprise techniques used by Emotet

Timeline of Activity

The following timeline identifies key Emotet activity observed in 2020.

- **February**: Cybercriminals targeted non-U.S. countries using COVID-19-themed phishing emails to lure victims to download Emotet.[1]
- **July**: Researchers spotted emails with previously used Emotet URLs, particularly those used in the February campaign, targeting U.S. businesses with COVID-19-themed lures.[2]
- **August**:
  - Security researchers observed a 1,000 percent increase in downloads of the Emotet loader. Following this change, antivirus software firms adjusted their detection heuristics to compensate, leading to decreases in observed loader downloads.[3]
  - Proofpoint researchers noted mostly minimal changes in most tactics and tools previously used with Emotet. Significant changes included:
    - Emotet delivering Qbot affiliate `partner01` as the primary payload and
    - The Emotet mail sending module's ability to deliver benign and malicious attachments.[4]
  - CISA and MS-ISAC observed increased attacks in the United States, particularly cyber actors using Emotet to target state and local governments.
- **September**:
  - Cyber agencies and researchers alerted the public of surges of Emotet, including compromises in Canada, France, Japan, New Zealand, Italy, and the Netherlands. Emotet botnets were observed dropping Trickbot to deliver ransomware payloads against some victims and Qakbot Trojans to steal banking credentials and data from other targets.[5],[6],[7],[8]
  - Security researchers from Microsoft identified a pivot in tactics from the Emotet campaign. The new tactics include attaching password-protected archive files (e.g., Zip files) to emails to bypass email security gateways. These email messages purport to deliver documents created on mobile devices to lure targeted users into enabling macros to "view" the documents—an action which actually enables the delivery of malware.[9]
  - Palo Alto Networks reported cyber actors using thread hijacking to spread Emotet. This attack technique involves stealing an existing email chain from an infected host to reply to the chain—using a spoofed identity—and attaching a malicious document to trick recipients into opening the file.[10]

MITRE ATT&CK Techniques

According to MITRE, Emotet uses the ATT&CK techniques listed in table 1.

Table 1: Common exploit tools

Technique	Use
OS Credential Dumping: LSASS Memory [T1003.001]	Emotet has been observed dropping password grabber modules including Mimikatz.
Remote Services: SMB/Windows Admin Shares [T1021.002]	Emotet leverages the Admin$ share for lateral movement once the local admin password has been brute forced.
Obfuscated Files or Information [T1027]	Emotet has obfuscated macros within malicious documents to hide the URLs hosting the malware, `cmd.exe` arguments, and PowerShell scripts.
Obfuscated Files or Information: Software Packing [T1027.002]	Emotet has used custom packers to protect its payloads.
Network Sniffing [T1040]	Emotet has been observed to hook network APIs to monitor network traffic.
Exfiltration Over C2 Channel [T1041]	Emotet has been seen exfiltrating system information stored within cookies sent within a `HTTP GET` request back to its command and control (C2) servers.
Windows Management Instrumentation [T1047]	Emotet has used WMI to execute `powershell.exe`.
Process Injection: Dynamic-link Library Injection [T1055.001]	Emotet has been observed injecting in to `Explorer.exe` and other processes.
Process Discovery [T1057]	Emotet has been observed enumerating local processes.
Command and Scripting Interpreter: PowerShell [T1059.001]	Emotet has used Powershell to retrieve the malicious payload and download additional resources like Mimikatz.

Technique	Use
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	Emotet has used `cmd.exe` to run a PowerShell script.
Command and Scripting Interpreter: Visual Basic [T1059.005]	Emotet has sent Microsoft Word documents with embedded macros that will invoke scripts to download additional payloads.
Valid Accounts: Local Accounts [T1078.003]	Emotet can brute force a local admin password, then use it to facilitate lateral movement.
Account Discovery: Email Account [T1087.003]	Emotet has been observed leveraging a module that can scrape email addresses from Outlook.
Brute Force: Password Guessing [T1110.001]	Emotet has been observed using a hard-coded list of passwords to brute force user accounts.
Email Collection: Local Email Collection [T1114.001]	Emotet has been observed leveraging a module that scrapes email data from Outlook.
User Execution: Malicious Link [T1204.001]	Emotet has relied upon users clicking on a malicious link delivered through spearphishing.
User Execution: Malicious File [T1204.002]	Emotet has relied upon users clicking on a malicious attachment delivered through spearphishing.
Exploitation of Remote Services [T1210]	Emotet has been seen exploiting SMB via a vulnerability exploit like ETERNALBLUE (MS17-010) to achieve lateral movement and propagation.
Create or Modify System Process: Windows Service [T1543.003]	Emotet has been observed creating new services to maintain persistence.

Technique	Use
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	Emotet has been observed adding the downloaded payload to the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` key to maintain persistence.
Scheduled Task/Job: Scheduled Task [T1053.005]	Emotet has maintained persistence through a scheduled task.
Unsecured Credentials: Credentials In Files [T1552.001]	Emotet has been observed leveraging a module that retrieves passwords stored on a system for the current logged-on user.
Credentials from Password Stores: Credentials from Web Browsers [T1555.003]	Emotet has been observed dropping browser password grabber modules.
Archive Collected Data [T1560]	Emotet has been observed encrypting the data it collects before sending it to the C2 server.
Phishing: Spearphishing Attachment [T1566.001]	Emotet has been delivered by phishing emails containing attachments.
Phishing: Spearphishing Link [T1566.002]	Emotet has been delivered by phishing emails containing links.
Non-Standard Port [T1571]	Emotet has used HTTP over ports such as 20, 22, 7080, and 50000, in addition to using ports commonly associated with HTTP/Hypertext Transfer Protocol Secure.
Encrypted Channel: Asymmetric Cryptography [T1573.002]	Emotet is known to use RSA keys for encrypting C2 traffic.

Detection

Signatures

MS-ISAC developed the following Snort signature for use in detecting network activity associated with Emotet activity.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"[CIS] Emotet C2 Traffic Using Form Data to Send Passwords"; content:"POST"; http_method; content:"Content-Type|3a 20|multipart/form-data|3b 20|boundary="; http_header; fast_pattern; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|"; http_client_body; content:!"------WebKitFormBoundary"; http_client_body; content:!"Cookie|3a|"; pcre:"/:?(chrome|firefox|safari|opera|ie|edge) passwords/i"; reference:url,cofense.com/flash-bulletin-emotet-epoch-1-changes-c2-communication/; sid:1; rev:2;)
```

CISA developed the following Snort signatures for use in detecting network activity associated with Emotet activity. **Note:** Uniform Resource Identifiers should contain a random length alphabetical multiple directory string, and activity will likely be over ports 80, 8080, or 443.

```
alert tcp any any -> any $HTTP_PORTS (msg:"EMOTET:HTTP URI GET contains '/wp-content/###/'"; sid:00000000; rev:1; flow:established,to_server; content:"/wp-content/"; http_uri; content:"/"; http_uri; distance:0; within:4; content:"GET"; nocase; http_method; urilen:<17; classtype:http-uri; content:"Connection|3a 20|Keep-Alive|0d 0a|"; http_header; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"EMOTET:HTTP URI GET contains '/wp-admin/###/'"; sid:00000000; rev:1; flow:established,to_server; content:"/wp-admin/"; http_uri; content:"/"; http_uri; distance:0; within:4; content:"GET"; nocase; http_method; urilen:<15; content:"Connection|3a 20|Keep-Alive|0d 0a|"; http_header; classtype:http-uri; metadata:service http;)
```

Mitigations

CISA and MS-ISAC recommend that network defenders—in federal, state, local, tribal, territorial governments, and the private sector—consider applying the following best practices to strengthen the security posture of their organization's systems. System owners and administrators should review any configuration changes prior to implementation to avoid unwanted impacts.

- Block email attachments commonly associated with malware (e.g.,.dll and .exe).
- Block email attachments that cannot be scanned by antivirus software (e.g., .zip files).
- Implement Group Policy Object and firewall rules.
- Implement an antivirus program and a formalized patch management process.
- Implement filters at the email gateway, and block suspicious IP addresses at the firewall.
- Adhere to the principle of least privilege.
- Implement a Domain-Based Message Authentication, Reporting & Conformance validation system.
- Segment and segregate networks and functions.
- Limit unnecessary lateral communications.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Enforce multi-factor authentication.
- Exercise caution when opening email attachments, even if the attachment is expected and the sender appears to be known. See Using Caution with Email Attachments.

- Enable a firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to suspicious or risky sites.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Visit the MITRE ATT&CK Techniques pages (linked in table 1 above) for additional mitigation and detection strategies.
- See CISA's Alert on Technical Approaches to Uncovering and Remediating Malicious Activity for more information on addressing potential incidents and applying best practice incident response procedures.
- See the joint CISA and MS-ISAC Ransomware Guide on how to be proactive and prevent ransomware attacks from happening and for a detailed approach on how to respond to an attack and best resolve the cyber incident.

For additional information on malware incident prevention and handling, see the National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

Resources

- MS-ISAC Security Event Primer – Emotet
- CISA Alert TA18-201A – Emotet Malware
- MITRE ATT&CK – Emotet
- MITRE ATT&CK for Enterprise

References

[1] Bleeping Computer: Emotet Malware Strikes U.S. Businesses with COVID-19 Spam

[2] IBID

[3] Security Lab: Emotet Update Increases Downloads

[4] Proofpoint: A Comprehensive Look at Emotet's Summer 2020 Return

[5] ZDNet: France, Japan, New Zealand Warn of Sudden Strike in Emotet Attacks

[6] Bleeping Computer: France Warns of Emotet Attacking Companies, Administration

[7] ESET: Emotet Strikes Quebec's Department of Justice: An ESET Analysis

[8] ZDNet: Microsoft, Italy, and the Netherlands Warn of Increased Emotet Activity

[9] Bleeping Computer: Emotet Double Blunder: Fake 'Windows 10 Mobile' and Outdated Messages

[10] Palo Alto Networks: Case Study: Emotet Thread Hijacking, an Email Attack Technique

Revisions

October 6, 2020: Initial Version
