

Emotet Malware | CISA

Published: 2020-01-23 · Archived: 2026-04-05 15:58:08 UTC

Systems Affected

Network Systems

Overview

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. 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.

This joint Technical Alert (TA) is the result of Multi-State Information Sharing & Analysis Center (MS-ISAC) analytic efforts, in coordination with the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC).

Emotet continues to be among the most costly and destructive malware affecting SLTT governments. Its worm-like features result in rapidly spreading network-wide infection, which are difficult to combat. Emotet infections have cost SLTT governments up to \$1 million per incident to remediate.

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Additionally, Emotet is a polymorphic banking Trojan that can evade typical signature-based detection. It has several methods for maintaining persistence, including auto-start registry keys and services. It uses modular Dynamic Link Libraries (DLLs) to continuously evolve and update its capabilities. Furthermore, Emotet is Virtual Machine-aware and can generate false indicators if run in a virtual environment.

Emotet is disseminated through malspam (emails containing malicious attachments or links) that uses branding familiar to the recipient; it has even been spread using the MS-ISAC name. As of July 2018, the most recent campaigns imitate PayPal receipts, shipping notifications, or “past-due” invoices purportedly from MS-ISAC. Initial infection occurs when a user opens or clicks the malicious download link, PDF, or macro-enabled Microsoft Word document included in the malspam. Once downloaded, Emotet establishes persistence and attempts to propagate the local networks through incorporated spreader modules.

Figure 1: Malicious email distributing Emotet

Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator.

1. NetPass.exe is a legitimate utility developed by NirSoft that recovers all network passwords stored on a system for the current logged-on user. This tool can also recover passwords stored in the credentials file of external drives.

2. Outlook scraper is a tool that scrapes names and email addresses from the victim's Outlook accounts and uses that information to send out additional phishing emails from the compromised accounts.
3. WebBrowserPassView is a password recovery tool that captures passwords stored by Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera and passes them to the credential enumerator module.
4. Mail PassView is a password recovery tool that reveals passwords and account details for various email clients such as Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail, and Gmail and passes them to the credential enumerator module.
5. Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for the enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet's access to SMB can result in the infection of entire domains (servers and clients).

Figure 2: Emotet infection process

To maintain persistence, Emotet injects code into explorer.exe and other running processes. It can also collect sensitive information, including system name, location, and operating system version, and connects to a remote command and control server (C2), usually through a generated 16-letter domain name that ends in ".eu." Once Emotet establishes a connection with the C2, it reports a new infection, receives configuration data, downloads and runs files, receives instructions, and uploads data to the C2 server.

Emotet artifacts are typically found in arbitrary paths located off of the AppData\Local and AppData\Roaming directories. The artifacts usually mimic the names of known executables. Persistence is typically maintained through Scheduled Tasks or via registry keys. Additionally, Emotet creates randomly-named files in the system root directories that are run as Windows services. When executed, these services attempt to propagate the malware to adjacent systems via accessible administrative shares.

Note: it is essential that privileged accounts are not used to log in to compromised systems during remediation as this may accelerate the spread of the malware.

Example Filenames and Paths:

```
C:\Users\\AppData\Local\Microsoft\Windows\shedaudio.exe
```

```
C:\Users\\AppData\Roaming\Macromedia\Flash Player\macromedia\bin\flashplayer.exe
```

Typical Registry Keys:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
```

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

System Root Directories:

C:\Windows\11987416.exe

C:\Windows\System32\46615275.exe

C:\Windows\System32\shedaudio.exe

C:\Windows\SysWOW64\f9jwqSbS.exe

Impact

Negative consequences of Emotet infection include

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Solution

NCCIC and MS-ISAC recommend that organizations adhere to the following general best practices to limit the effect of Emotet and similar malspam:

- Use Group Policy Object to set a Windows Firewall rule to restrict inbound SMB communication between client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At a minimum, create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
- Use antivirus programs, with automatic updates of signatures and software, on clients and servers.
- Apply appropriate patches and updates immediately (after appropriate testing).
- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- If your organization does not have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security or IT department.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Provide employees training on social engineering and phishing. Urge employees not to open suspicious emails, click links contained in such emails, or post sensitive information online, and to never provide usernames, passwords, or personal information in answer to any unsolicited request. Educate users to hover over a link with their mouse to verify the destination prior to clicking on the link.
- Consider blocking file attachments that are commonly associated with malware, such as .dll and .exe, and attachments that cannot be scanned by antivirus software, such as .zip files.
- Adhere to the principle of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Implement Domain-Based Message Authentication, Reporting & Conformance (DMARC), a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.

If a user or organization believes they may be infected, NCCIC and MS-ISAC recommend running an antivirus scan on the system and taking action to isolate the infected workstation based on the results. If multiple workstations are infected, the following actions are recommended:

- Identify, shutdown, and take the infected machines off the network;
- Consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware;
- Do not log in to infected systems using domain or shared local administrator accounts;
- Reimage the infected machine(s);
- After reviewing systems for Emotet indicators, move clean systems to a containment virtual local area network that is segregated from the infected network;
- Issue password resets for both domain and local credentials;
- Because Emotet scrapes additional credentials, consider password resets for other applications that may have had stored credentials on the compromised machine(s);
- Identify the infection source (patient zero); and
- Review the log files and the Outlook mailbox rules associated with the infected user account to ensure further compromises have not occurred. It is possible that the Outlook account may now have rules to auto-forward all emails to an external email address, which could result in a data breach.

Reporting

MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments. More information about this topic, as well as 24/7 cybersecurity assistance for SLTT governments, is available by phone at 866-787-4722, by email at SOC@cisecurity.org, or on MS-ISAC's website at <https://msisac.cisecurity.org/>.

To report an intrusion and request resources for incident response or technical assistance, contact CISA Central by email at SayCISA@cisa.dhs.gov or by phone at 1-844-Say-CISA.

Revisions

July 20, 2018: Initial version|January 23, 2020: Fixed typo

Source: <https://www.us-cert.gov/ncas/alerts/TA18-201A>