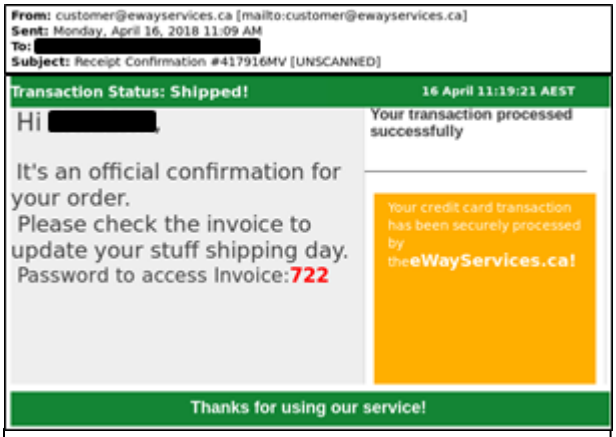
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Security Primer
December 2018 • SP2018-0949

Emotet

Emotet continues to be among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) governments. Its highly infectious nature makes it difficult to combat and has cost SLTT governments up to $1 million per incident to remediate due to its worm-like features resulting in rapid, network-wide infections. Emotet is an advanced, modular banking trojan that primarily functions as a downloader or dropper of other banking trojans. Additionally, Emotet is polymorphic allowing it to evade typical signature-based detection. It has several methods for maintaining persistence, including auto-start registry keys and services. The trojan uses modular Dynamic Link Libraries (DLL) to continuously evolve and update its capabilities. Furthermore, Emotet is Virtual Machine (VM) 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, including the MS-ISAC name. As of July 2018, the most recent campaigns imitate PayPal receipts, shipping notifications, or "past-due" invoices purportedly from the MS-ISAC. Initial infection occurs when a user opens or clicks the malicious download link, XML, 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.



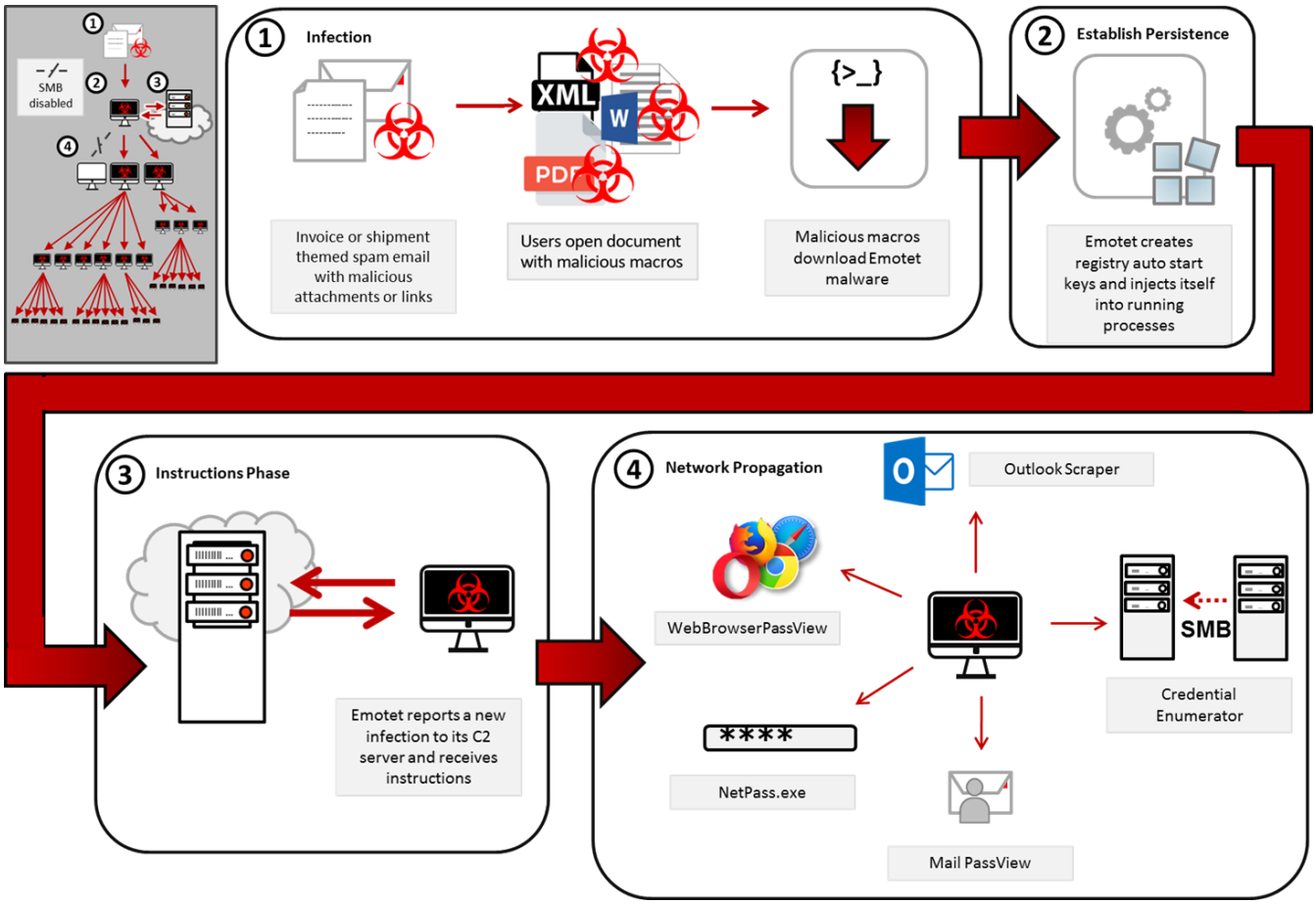
Malicious email distributing Emotet

Currently, there are five known spreader modules:

- **NetPass.exe**: 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.
- **Outlook Scraper**: a tool that scrapes dates, names, email addresses, and email bodies from the victim's Outlook accounts and uses that information to send out additional phishing emails from the compromised accounts.
- **WebBrowserPassView**: 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.
- **Mail PassView**: 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.
- **Credential Enumerator**: a self-extracting RAR file containing two components, a bypass and a service component. The bypass component is used for 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 then writes the service component on the system, which writes Emotet onto the disk. Access to SMB can result in entire domains (servers and clients) becoming infected.

To maintain persistence, Emotet injects code into explorer.exe and other running processes. The trojan can also collect sensitive information including system name, location, and operating system version, sending it to a remote command and control server (C2). The C2 is a compromised web server, commonly hosting Nginx, and the connection is over a common web port to a URL containing the IP address. Once Emotet establishes the connection with the C2, it reports a new infection, receives configuration data, downloads and runs files, receives instructions, and uploads base64 encoded data to the C2 server.

Emotet artifacts are typically found in arbitrary paths located off of the AppData\Local and AppData\Roaming directories and mimicking 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. It is essential that privileged accounts are not used to login to compromised systems during remediation as this may accelerate the spread of the malware.



Example filename and path:
C:\Users\<username>\AppData \Local\Microsoft\Windows\shedaudio.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

RECOMMENDATIONS:

The MS-ISAC recommends organizations adhere to the following general best practices, to limit the effect of Emotet and similar malspam in your organization.

- Use Group Policy 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 minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
- Use antivirus programs on clients and servers, with automatic updates of signatures and software.
- Disable all macros except those which are digitally signed.
- 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 you do not have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security and/or IT departments.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- Provide social engineering and phishing training to employees. Urge them to not open suspicious emails, click links contained in such emails, post sensitive information online, and to never provide usernames, passwords and/or personal information to any unsolicited request. Teach users to hover over a link with their mouse to verify the destination prior to clicking on the link.
- Adhere to the principal 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.
- Adhere to best practices, such as those described in the CIS Controls, which are part of the CIS SecureSuite.

If a user opened a malicious email or an infection is believed to exist, we recommend running an antivirus scan on the system and take action based on the results to isolate the infected computer. If multiple machines are infected:

- Consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware. Emotet could be dropping malware with Remote Access Trojan (RAT) capabilities damaging the integrity of the overall network.
- Identify, shutdown, and take the infected machines off the network.
- Do not login to infected systems using domain or shared local admin accounts.
- After reviewing systems for Emotet indicators, reimage and move clean systems to a containment VLAN, segregated from the infected network.
- Issue password resets for both domain and local credentials.
- As Emotet scrapes additional credentials, consider password resets for other applications that may have had stored credentials on the compromised machine(s).
- Review log files and the Outlook mailbox rules associated with the 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.
- Search base64 encoded network stream data referencing the organization's email domain. If references are found, perform additional analysis to see if a data breach has occurred.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.