Malwarebytes

Emotet Emergency Kit

What is Emotet?

One of the most common and pervasive threats for organizations today is Emotet, a banking Trojan-turned-downloader that has been a top detection at Malwarebytes for nearly a year. Emotet has been leveled at organizations across the globe, fooling users into infecting endpoints through phishing emails, and then spreading laterally through networks using stolen NSA exploits. Its modular, polymorphic form, and ability to drop multiple, changing payloads have made Emotet a thorn in the side of cybersecurity researchers and IT teams alike.

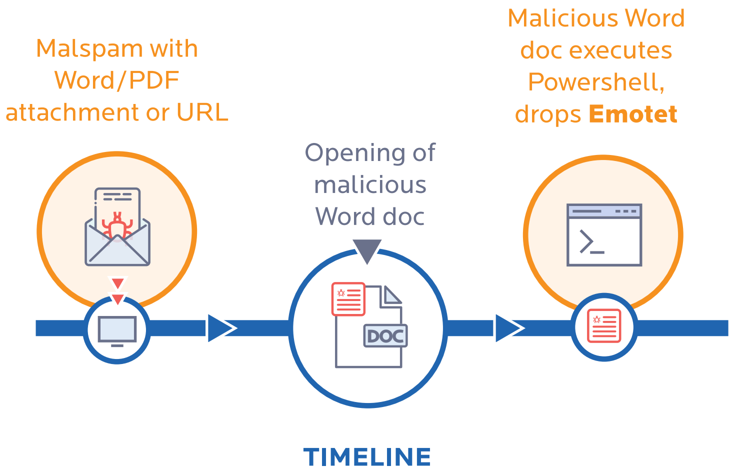
Why is Emotet dangerous to your business?

Emotet first appeared on the scene as a banking Trojan, but its effective combination of persistence and network propagation has turned it into a popular infection mechanism for other forms of malware, such as TrickBot and Ryuk ransomware. It has also earned a reputation as one of the hardest-to-remediate infections once it has infiltrated an organization's network.

A major factor that frustrates remediation is the aforementioned lateral movement via NSA exploits, particularly EternalBlue, which was used to spread the infamous WannaCry ransomware outbreak of 2017. EternalBlue requires admins follow a strict policy of isolating infected endpoints from the network, patching, disabling Administrative Shares, and ultimately removing the Trojan before reconnecting to the network—otherwise, face the certainty that cleaned endpoints will become re-infected over and over by infected peers.

Add to that mix an ongoing development of new capabilities, including the ability to be VM-aware, avoid spam filters, or uninstall security programs, and you'll begin to understand why Emotet is every network administrators' worst nightmare.

Emotet infection vector


Malspam with Word/PDF attachment or URL
Opening of malicious Word doc
Malicious Word doc executes Powershell, drops **Emotet**
DOC
TIMELINE

INFECTED AND NEED HELP?

Contact emeasales@malwarebytes.com and one of our security experts will reach out.

malwarebytes.com/business

emeasales@malwarebytes.com

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.

Malwarebytes

Emotet **Remediation and Protection** Checklist

Remediation tips

Malwarebytes can detect and remove Emotet on endpoints without further user interaction. But to be effective on networked machines, additional steps must be taken.

□ **1.** Identify the infected machine(s). If you have unprotected endpoints/machines, you can run Farbar Recovery Scan Tool (FRST) to look for possible Indicators of Compromise (IOC). Besides verifying an infection, FRST can also be used to verify removal before bringing an endpoint/machine back into the network. Refer to Farbar Recovery Scan Tool instructions for details on how to install and run a FRST scan.

□ **2.** Search the FRST.txt file for the following IOCs:

- HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\1A345B7
- HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\12C4567D
- (Gornyk) C:\Windows\SysWOW64\servicedcom.exe
- C:\WINDOWS\12345678.EXE
- C:\WINDOWS\SYSWOW64\SERVERNV.EXE
- C:\WINDOWS\SYSWOW64\NUMB3R2ANDL3373RS.EXE
- C:\WINDOWS\TEMP\1A2B.TMP

□ **3.** Disconnect the infected machines from the network.

□ **4.** Patch for EternalBlue.

□ **5.** Disable Administrative Shares. Windows server shares install hidden share folders by default specifically for administrative access to other machines. The Admin$ shares are used by Emotet once it has brute forced the local administrator password. A file share sever has an IPC$ share that Emotet queries to get a list of all endpoints that connect to it. These AdminIP shares are normally protected via UAC, however, Windows will allow the local administrator through with no prompt.

The most recent Emotet variants use C$ with the Admin credentials to move around and re-infect all the other endpoints. It is recommended to disable these Admin$ shares via the registry. If you do not see this registry key, it can be added manually and set up to be disabled.

□ **6.** Remove the Emotet Trojan.

□ **7.** Change account credentials, including local and domain administrator passwords. Repeated re-infections are an indication the worm was able to guess or brute force the administrator password successfully.

Protection tips

To keep Emotet off endpoints, follow these security best practices—and teach your employees to do the same.

□ **1.** Scan emails with attachments so that malspam doesn't reach the end user.

□ **2.** Train employees to spot phishing attempts, especially those that are spoofed (which is how Emotet is spread) and report them to the correct authorities at your office.

□ **3.** Train responders' ability to detect an Emotet campaign, identify potentially infected hosts, determine which actions were taken on compromised machines, and confirm whether or not data exfiltration took place.

□ **4.** Apply patches to any software, systems, or browsers that need them.

□ **5.** Limit administrative shares to the absolute minimum for Emotet damage control.

□ **6.** Use strong passwords with multi-factor authentication, or consider rolling out a single password manager for the entire organization.

□ **7.** Invest in anti-exploit technology that can stop lateral infections such as Emotet from spreading throughout the network.

INFECTED AND NEED HELP?

Contact emeasales@malwarebytes.com and one of our security experts will reach out.