Let’s talk Emotet malware

You may have heard about Emotet in the news.

What is it: Ancient Egyptian king, your teenage sister’s favorite emo band?

We’re afraid not.

The Emotet banking Trojan was first identified by security researchers in 2014.

Emotet was originally designed as a banking malware that attempted to sneak onto your computer and steal sensitive and private information.

Later versions of the software saw the addition of spamming and malware delivery services—including other banking Trojans.

Emotet uses functionality that helps the software evade detection by some anti-malware products.

Emotet uses worm-like capabilities to help spread to other connected computers.

This helps in distribution of the malware.

This functionality has led the Department of Homeland Security to conclude that Emotet is one of the most costly and destructive malware, affecting government and private sectors, individuals and organizations, and costing upwards of $1M per incident to clean up.

What is Emotet?

Emotet is a Trojan that is primarily spread through spam emails (malspam).

The infection may arrive either via malicious script, macro-enabled document files, or malicious link.

Emotet emails may contain familiar branding designed to look like a legitimate email.

Emotet may try to persuade users to click the malicious files by using tempting language about “Your Invoice,” “Payment Details,” or possibly an upcoming shipment from well-known parcel companies.

Emotet has gone through a few iterations.

Early versions arrived as a malicious JavaScript file.

Later versions evolved to use macro-enabled documents to retrieve the virus payload from command and control (C&C;) servers run by the attackers.

Emotet uses a number of tricks to try and prevent detection and analysis.

Notably, Emotet knows if it’s running inside a virtual machine (VM) and will

lay dormant if it detects a sandbox environment, which is a tool cybersecurity researchers use to observe malware within a safe, controlled space.

Emotet also uses C&C; servers to receive updates.

This works in the same way as the operating system updates on your PC and can happen seamlessly and without any outward signs.

This allows the attackers to install updated versions of the software, install additional malware such as other banking Trojans, or to act as a dumping ground for stolen information such as financial credentials, usernames and passwords, and email addresses.

Latest Emotet news

Emotet is back: botnet springs back to life with new spam campaign

Emotet on the rise with heavy spam campaign

Malware analysis: decoding Emotet, part 2

Malware analysis: decoding Emotet, part 1

How does Emotet spread?

The primary distribution method for Emotet is through malspam.

Emotet ransacks your contacts list and sends itself to your friends, family, coworkers and clients.

Since these emails are coming from your hijacked email account, the emails look less like spam and the recipients, feeling safe, are more inclined to click bad URLs and download infected files.

If a connected network is present, Emotet spreads using a list of common passwords, guessing its way onto other connected systems in a brute-force attack.

If the password to the all-important human resources server is simply “password” then it’s likely Emotet will find its way there.

Researchers initially thought Emotet also spread using the EternalBlue/DoublePulsar vulnerabilities, which were responsible for the WannaCry and NotPetya attacks.

We know now that this isn't the case.

What led researchers to this conclusion was the fact that TrickBot, a Trojan often spread by Emotet, makes use of the EternalBlue exploit to spread itself across a given network.

It was TrickBot, not Emotet, taking advantage of the EternalBlue/DoublePulsar vulnerabilities.

What is the history of Emotet?

First identified in 2014, Emotet continues to infect systems and hurt users to this day, which is why we're still talking about it, unlike other trends from 2014 (Ice Bucket Challenge anyone?

).

Version one of Emotet was designed to steal bank account details by intercepting internet traffic.

A short time after, a new version of the software was detected.

This version, dubbed Emotet version two, came packaged with several modules, including a money transfer system, malspam module, and a banking module that targeted German and Austrian banks.

"Current versions of the Emotet Trojan include the ability to install other malware to infected machines.

This malware may include other banking Trojans or malspam delivery services."

By January of 2015, a new version of Emotet appeared on the scene.

Version three contained stealth modifications designed to keep the malware flying under the radar and added new Swiss banking targets.

Fast forward to 2018—new versions of the Emotet Trojan include the ability to install other malware to infected machines.

This malware may include other Trojans and ransomware.

Case in point, a July 2019 Emotet strike on Lake City, Florida cost the town $460,000 in ransomware payouts, according to Gizmodo.

An analysis of the strike found Emotet served only as the initial infection vector.

Once infected, Emotet downloaded another banking Trojan known as TrickBot and the Ryuk ransomware.

After going relatively quiet for most of 2019, Emotet came back strong.

In September of 2019, Malwarebytes Labs reported on a botnet-driven spam campaign targeting German, Polish, Italian, and English victims with craftily worded subject lines like "Payment Remittance Advice" and "Overdue invoice." Opening the infected Microsoft Word document initiates a macro, which in turn downloads Emotet from compromised WordPress sites.

Who does Emotet target?

Everyone is a target for Emotet.

To date, Emotet has hit individuals, companies, and government entities across

the United States and Europe, stealing banking logins, financial data, and even Bitcoin wallets.

One noteworthy Emotet attack on the City of Allentown, PA, required direct help from Microsoft's incident response team to clean up and reportedly cost the city upwards of $1M to fix.

Now that Emotet is being used to download and deliver other banking Trojans, the list of targets is potentially even broader.

Early versions of Emotet were used to attack banking customers in Germany.

Later versions of Emotet targeted organizations in Canada, the United Kingdom, and the United States.

"One noteworthy Emotet attack on the City of Allentown, PA required direct help from Microsoft's incident response team to clean up and reportedly cost the city upwards of $1M to fix."

How can I protect myself from Emotet?

You're already taking the first step towards protecting yourself and your users from Emotet by learning how Emotet works.

Here's a few additional steps you can take:

Keep your computer/endpoints up-to-date with the latest patches for Microsoft Windows.

TrickBot is often delivered as a secondary Emotet payload, and we know TrickBot relies on the Windows EternalBlue vulnerability to do its dirty work, so patch that vulnerability before the cybercriminals can take advantage of it.

Don't download suspicious attachments or click a shady-looking link.

Emotet can't get that initial foothold on your system or network if you avoid those suspect emails.

Take the time to educate your users on how to spot malspam.

Educate yourself and your users on creating a strong password.

While you're at it, start using two-factor authentication.

You can protect yourself and your users from Emotet with a robust cybersecurity program that includes multi-layered protection.

Malwarebytes business and premium consumer products detect and block Emotet in real-time.

How can I remove Emotet?

If you suspect you've already been infected by Emotet, don't freak out.

If your computer is connected to a network—isolate it immediately.

Once isolated, proceed to patch and clean the infected system.

But you're not done yet.

Because of the way Emotet spreads across your network, a clean computer can be re-infected when plugged back into an infected network.

Clean each computer on your network one-by-one.

It's a tedious process, but Malwarebytes business solutions can make it easier, isolating and remediating infected endpoints and offering proactive protection against future Emotet infections.

If knowing is half the battle, head on over to the Malwarebytes Labs and you can learn more on how Emotet evades detection and how Emotet's code works.

ID	Name	Identified Sentence
T1063	Security Software Discovery	Later versions of the software saw the addition of spamming and malware delivery services—including other banking Trojans. Emotet uses functionality that helps the software evade detection by some anti-malware products.
T1064	Scripting	The infection may arrive either via malicious script, macro-enabled document files, or malicious link.
T1204	User Execution	The infection may arrive either via malicious script, macro-enabled document files, or malicious link.
T1003	Credential Dumping	This allows the attackers to install updated versions of the software, install additional malware such as other banking Trojans, or to act as a dumping ground for stolen information such as financial credentials, usernames and passwords, and email addresses. Latest Emotet news Emotet is back: botnet springs back to life with new spam campaign Emotet on the rise with heavy spam campaign Malware analysis: decoding Emotet, part 2

		Malware analysis: decoding Emotet, part 1 How does Emotet spread? The primary distribution method for Emotet is through malspam.
T1192	Spearphishing Link	Since these emails are coming from your hijacked email account, the emails look less like spam and the recipients, feeling safe, are more inclined to click bad URLs and download infected files. If a connected network is present, Emotet spreads using a list of common passwords, guessing its way onto other connected systems in a brute-force attack.