Emotet's back and it isn't wasting any time

By Pieter Arntz

Published: 2021-12-02 · Archived: 2026-04-05 20:19:27 UTC

Emotet is one of the best known, and most dangerous, malware threats of the past several years.

On several occasions it appeared to take an early retirement, but it has always came back. In January of this year, a global police operation dismantled Emotet's botnet. Law enforcement then used their control of this infrastructure to send a "self-destruct" update to Emotet executables. Infected organizations were given a few months grace to clean up the the neutered malware before the remaining copies did as they'd been instructed and ate themselves in April.

However, that wasn't the end of the story.

Last month we reported on how another notorious bit of malware, TrickBot, was helping Emotet come back from the dead. And then yesterday, several security researchers saw another huge spike in Emotet's activity.

Blinking light

The presence of Emotet in the threat landscape has had the appearance of a blinking red light for years. Emotet started out in 2014 as an information-stealing banking Trojan that scoured sensitive financial information from infected systems (which is why Malwarebytes detects some components as Spyware.Emotet). Over the years, it evolved into a global-scale distribution infrastructure for other malware.

During this time we have seen Emotet disappear and show up again on several occasions. In September 2019, Emotet emerged from a four month hiatus with a new spam campaign, before going back into hiding early in 2020 and reappearing in July of the same year. Its use then declined, with occasional spikes, before it returned just in time for Christmas and was then dealt a massive blow by collective law enforcement action in January this year.

Recent spikes

On the December 1, 2021, our Threat Intelligence team noted a huge spike in Emotet C2 activity.

Other researchers also noted spikes in the number of URLs being used to distribute the malware, and the number of malware samples.

From all the reports and alerts by researchers and analysts we can see a few interesting trends.

- First of all, our own research shows the global distribution of Emotet has a clear focus on the US.
- Looking at the malware URLs that URLhaus has associated with the latest Emotet campaigns, we see a lot of compromised WordPress sites.

- Only yesterday we talked about how Emotet was being spread via malicious Windows App Installer packages. While this was not an entirely new method, it is not something we see every day.
- The spam campaign used to spread the mails with the links leading to the App Installer packages was done by hijacking existing conversations, using stolen reply-chain emails.
- Researchers are seeing an uptick in the number of Emotet C2 servers.

Speculation

From this point on the content of this post is speculation, so feel free to skip it if you have developed your own theories. Or feel free to compare notes and leave your remarks in the comments.

Emotet is growing a lot faster than any newcomer to the scene could do. This seems to indicate that old relationships have been renewed, which usually means that the persons that tied these knots in the past are still working on the project and bringing "old friends" back in.

Given the global distribution and the different campaigns that are ongoing it's likely there are several different affiliates at work. And looking at their methods we can tell that these are not some "fresh out of their mother's basement script kiddies" either. They are using sophisticated methods and abusing vulnerabilities that haven't been patched yet by quite a lot of organizations. For example, some Microsoft Exchange vulnerabilities will allow them to hijack existing email threads, which gives the spam messages a higher credibility.

I checked the hosting companies for the WordPress sites, expecting to find a lot of GoDaddy domains that might have been compromised while their credentials were for sale. But I found a lot of different hosting companies, which makes WordPress the common denominator. It's likely therefore that the attackers are exploiting vulnerable versions of WordPress plugins like OptinMonster, WP Fastest Cache, and WooCommerce Dynamic Pricing and Discounts, all of which were recently patched. (Although there are probably others that we do not know about yet too.)

Hard fact

Emotet is back! For how long is hard to predict, but they don't behave as if they have any plans to retire again soon.

Stay safe, everyone!

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
