Meet the white-hat group fighting Emotet, the world's most dangerous malware

By Catalin Cimpanu

Published: 2020-02-29 · Archived: 2026-04-06 01:24:55 UTC

Background image via Guido Bohne (CC-BY-SA-2.0)

For more than a year, a group of security researchers and system administrators have banded together to fight back against Emotet, today's most active and dangerous malware operation.

By working together, the Cryptolaemus group has seriously hindered Emotet operations. Daily, the group publishes updates on its website and Twitter account. They share so-called indicators of compromise (IOCs). These include IP addresses for Emotet command servers, subject lines used in Emotet spam campaigns, and file hashes for Emotet-infected files.

Also: 30 years of ransomware: How one bizarre attack laid the foundations for the malware taking over the world

The Cryptolaemus members share these details so that system and network administrators around the world can import the IOCs into their cyber-security products and protect against possible Emotet infections, or help with early detections before the malware can do extensive damage.

"Personally, I just want to help people and stop this threat," said Joseph Roosen, one of the Cryptolaemus members.

"When Emotet infected my network at my day job in November of 2017, it was only stopped by us having a rather robust VLAN scheme, and therefore lateral movement was isolated and easier to clean up," Roosen said.

"However, the experience changed my life, though, and pissed me off at the same time."

Emotet -- from banking trojan to cybercrime empire

The reason for Roosen's anger was Emotet, a name that describes both a malware strain and the criminal operation behind it.

Emotet appeared online in 2014. It began its operations as a banking trojan. Banking trojans were all in the rage in the mid-2010s.

Emotet would infect a victim, lurk around on a system until the user would access its bank account, steal the user's credentials, and then allow the Emotet gang to access the bank account and steal funds.

SEE: Cybersecurity: Let's get tactical (ZDNet/TechRepublic special feature) | Download the free PDF version (TechRepublic)

But by 2014, banks had already faced banking trojans in the likes of Emotet for more than a decade, and they were starting to deploy anti-fraud measures. Multi-factor authentication systems, IP geo-fencing, and transaction alerts made stealing funds from someone's bank account without their knowledge much harder.

The Emotet gang saw the writing on the wall, and in the spring and summer of 2016, they became one of the first major banking trojan operations to morph into something else.

During 2016 and the next year, in 2017, Emotet slowly replaced most of its codebase and transformed itself from a banking trojan into a malware loader.

A "loader" is an incredibly simplistic malware strain. It infects a victim and then downloads (or loads) other malware. Emotet would download its own modules, or it would download someone else's malware.

Basically, Emotet shifted its entire mode of operation in only two years, from a closed group that stole money from people's bank accounts, into an open group that allowed other malware gangs to rent access to infected computers all over the world.

Nowadays, Emotet is one of the biggest "loader" operations on the market. It's effectively a cybercrime empire. They're so big that other "loaders" -- like TrickBot -- rent access to its huge network of infected computers.

Ransomware, crypto-miners, info-stealers, and banking trojans have been seen being planted on Emotet-infected hosts.


emotet-infographic.png

Image: Sophos

Nowadays, an Emotet infection means much more than many other malware infections. An Emotet infection usually means that Emotet has also expanded its reach from the initial point of entry to your entire network.

Emotet now comes with a plethora of modules that allow it to spread inside a network once it gets a foothold inside it. Its lateral movement tools are so advanced it's now pioneering a novel method of spreading via Wi-Fi connections, something not seen in any other malware operation.

Emotet is a litmus test for the infosec (information security) community. If a security researcher is playing down an Emotet infection, then they've most likely lost touch with what's what in the malware world. All good security researchers will tell you that Emotet is one of the most dangerous infections you can get, right next to TrickBot, another similar banking-trojan-turned-downloader operation.

> Anybody else depressed by the fact everyone in #threatintel can see that #emotet is coming back online and yet none of use can do anything to stop it? When it does go active it will start compromising systems and inflicting millions of dollars in damages. Maybe its just me 🤷‍♂️
>
> — Nick Biasini (@infosec_nick) August 23, 2019

Authorities in Germany and the Netherlands currently treat Emotet the same way as they do ransomware attacks. When a company gets infected with Emotet, cyber-security authorities in those two countries tell the victim company to shut down its entire network and immediately take it off the internet. Emotet infections left to run wild eventually turn into data breaches and ransomware infections.

Getting together to fight Emotet

It was in June 2018 when the idea of an anti-Emotet group came to be. In a Twitter group chat, a US-based system administrator named JayTHL asked "Any interest in a dedicated Emotet working group?"

Almost all in the chat said yes.

"Before you know it, we are chatting daily about Emotet TTPs (Tactics, Techniques, and Procedures) and sharing intel," Roosen told *ZDNet* in an interview.

"Eventually, after things got going, we started to add more members and made a joint effort to publish our IoCs instead of doing it as individual piecemeal stuff," Roosen added.

That's how a formal group came to be.

When it came to naming it, they had the perfect title.

"This name -- Cryptolaemus -- is based on the genus of beetles that are known to be 'Mealybug destroyers'," Roosen said.

"Back in the summer of 2018, Symantec had published a threat intel blog claiming that the name for the Emotet actors was 'Mealybug'," Roosen said.

"None of us had heard of this before and scratched our heads as to where this came from. It quickly became somewhat of a joke to us that we were the destroyers of Mealybug(s), and thus, the Cryptolaemus name was born."

The Cryptolaemus name idea came from a security researcher going on Twitter by @ps66uk, a trained biologist, showing how diverse the group was becoming.

Now, the Cryptolaemus team lists over 20 members on its website, but their ranks are far larger. Many can't disclose their affiliation with the group due to non-disclosure agreements they've signed. Some work as IT administrators for big corporations while others work at cyber-security firms. Most work on contracts that don't allow them to share threat intel freely on the internet.

However, many are doing it anyway.

Taking down Emotet one water drop at a time

They're doing it because they want to see Emotet shut down and its mastermind -- an individual known only as Ivan -- arrested and behind bars.

But bringing down Emotet is not an easy feat. Emotet is one of the most sophisticated malware operations known to date. It operates from three distinct botnets, not just one, created for this very same reason -- to make takedowns harder.

Furthermore, Ivan is believed to reside in Russia, a country that hasn't been too forthcoming in helping take down local cybercrime operations.

"I'd love it if they were arrested, but if they just give up, I'll be happy too," said James Quinn, a malware analyst at Binary Defense and a Cryptolaemus member.

Making Emotet and Ivan give up, or tap out, is what Cryptolaemus members have in mind. Most know that an arrest or a takedown is far away.

Instead, they hope that by sharing daily Emotet IOCs they can cut into Emotet's infection rate and into Ivan's profits.

Right now, Cryptolaemus members have regular meetings in Slack and Telegram channels, where they discuss new ways to hinder Emotet. Some spend their time reverse-engineering Emotet malware payloads, others track the botnet's command and control servers, while others crack encryption and other Emotet-related protocols.

Their efforts have not gone unnoticed. Today, the group's work is often closely followed by law enforcement and cyber-security firms alike. But Cryptolaemus' biggest fan is the Emotet gang itself.

"I am quite sure they are aware and reading our daily reports," Roosen said.

"We have seen them change tactics minutes after our posts, often enough that it is more than simple coincidence. I am quite sure they are part of the many reading our posts as soon as they go live," the researcher added.

"We have even joked that they are now calling the three botnets as Epoch 1, Epoch 2, and Epoch 3 internally [based on the names we assigned them]."

A stalemate

Right now, the fight between Cryptolaemus and Emotet appears to be a stalemate; however, the group's efforts are widely appreciated and respected in the infosec community, where, slowly but surely, the group's members have

become de-facto Emotet experts, whose opinions are always highly valued.

But while the Cryptolaemus group may never get their wish to see Ivan in handcuffs, the group is still pretty happy at how things turned out.

"Honestly, seeing the amount of cooperation in the group is really cool, because some of us literally work for direct competitors of each other, but we're still able to work together and push out IOCs, which is rare to see in the industry," Quinn said.

"I learn something new every day it seems, and I am helping the world," Roosen said. "To me, this is a win-win! I am truly touched by people reaching out to us explaining how we have helped them in their battles with Emotet.

"I think we have had some minor victories in this fight with the Emotet actors, but our greatest single accomplishment is the open collaboration and sharing amongst different entities in the industry," Roosen added.

"Because we are viewed as a neutral party, people will work together with us more freely, and through that collaboration, we have accomplished great things together."
