Emotet Resurgence Continues With New Tactics, Techniques and Procedures

By Lindsey O'Donnell

Published: 2019-11-06 · Archived: 2026-04-05 13:05:42 UTC

Since Emotet came out of hibernation last month, researchers are seeing the banking trojan's authors take on a consistent trend of new evasion tactics and social engineering techniques.

The notorious banking trojan Emotet, that mysteriously disappeared over the summer, returned last month dropping a new collection of malware including information stealers, email harvesters, self-propagation mechanisms and ransomware.

But since the malware returned from its hiatus, there was no clear novel post-infection technique or tactic that researchers observed. Detection-evasion and obfuscation techniques, for the most part, remained the same, researchers believed. That is until security researcher Suweera De Souza, after weeks of analysis, started seeing new developments.

De Souza reports that the malware has taken on new obfuscation and anti-virus detection techniques, as well as novel features such as a new export function delivered via Emotet binaries and a new list of words for the command-and-control (C2) servers to generate process names and keep track of installed modules.

In addition, De Souza warned that Emotet's authors have been changing their social engineering tactics with current events, sending out malicious emails purporting to be Edward Snowden's new memoir when it came out in September, as well as more recent Halloween-themed lures. De Souza discusses the new techniques with Threatpost on this week's Threatpost Podcast.

Listen to the podcast below or download direct here.

Below is a lightly-edited transcript of the podcast.

Lindsey O'Donnell: Hi, everyone, welcome back to the Threatpost podcast. You've got Lindsey O'Donnell here today with Threatpost and we're going to be discussing Emotet. Emotet has been in the news recently because after a short lived hibernation over the summer, it had recently reappeared and I've actually got Suweera De Souza, principal security research analyst with Netscout, who today came out with some new research around some of the new tactics and techniques that she has observed Emotet using since its reemergence just last month, so Suweera thank you so much for joining us today.

Suweera De Souza: Thank you, Lindsey. Thank you for having me.

LO: Just to start, let's take a step back here for a second and talk about Emotet's history. The banking Trojan is is best known for the Mauer has been around since 2014. So, you know, why is this banking Trojans still staying strong as a viable threat in the security landscape today?

SD: Yeah, so, that's true, Emotet has been seen since 2014. In fact, it started out as a banking trojan but right now over the years, its course of action has changed. In fact, it has become more modular. And what that means is as a platform, it has different modules that it can run. So essentially, its most popularly known module is its downloader module, and its spam module. So it's mainly seen downloading and distributing other malware as well as spreading itself for spam. So to answer the question as to why this is such a viable threat in today's landscape, it's because these authors that create Emotet, they don't remain quiet. They are constantly evolving, constantly changing the techniques that they use to propagate their payload, as well as they use to obfuscate their payload. So mainly, they're looking at bypassing current AV [anti-virus] protections and trying to infect as many machines as possible.

LO: So speaking of the actors, do we know anything about the developers behind Emotet and kind of who their targets are? Is that something – in terms of targeting – that has changed as well over the years?

SD: It's still not so clear about who the actors are. I mean, they do share a lot of similarity with some of the past banking Trojan families and that could mainly be that a lot of these malware families tend to copy each other. And they copy each other's code. As to their targets, it can be anyone, because when Emotet spreads, they infect a machine, and then they steal all the email credentials that are present on that machine and essentially goes on to spam those set of email lists. So the targets can be anyone. And if on a particular machine they have email credentials of targets based in a foreign country, you will see the malspam reaching out to those places as well.

LO: If I remember correctly, it was June 2019, when Emotet started to kind of disappear, and activity declined. So when did you guys first see it pick up and did you have any kind of indication around why that activity decline occurred in the first place?

SD: So regarding Emotet's hiatus, there's no clear indication as to why they went quiet for that four-month period since June. But then again, this is not new with malware campaigns and malware campaigns have been seen doing something similar in the past. And it's normally around holidays or sometimes they remain quiet in order to update their infrastructure. But since Emotet has, you know, you started seeing the activity in September, at least on Twitter, you would see a lot of posts being made about the C2 coming live. So everyone was being on top of the C2 servers. And then towards the end of September, that's when we started observing payloads being delivered. But right off when it started, when it got back from its hiatus, there was no clear novel technique and eventually throughout the weeks, we started seeing more and more development.

LO: Yeah. So talk a bit about that. You outlined this really clearly in your report that came out today about some of the new TTPs and what you're seeing in terms of these new tactics. So what were kind of the biggest takeaways from your reports?

SD: Sure. So this report came about as I was researching, Emotet and I was also researching TrickBot at the same time. So TrickBot for those that may not know it's a malware campaign that's mainly a banking trojan. And it's also very modular nature. What I've noticed was Emotet and TrickBot were being packed by the same packer. And so this led me to investigate further as to whether they were the same thing. So the payload was still very different;

Emotet had their own payload and TrickBot had its own payload. But the way that both files were being packed was the same. And this could be clear because Emotet is a known distributor of other malware and one of its biggest malware is that it distributes is TrickBot. So it gives us an indication that, to keep up to date with the way they pack their files to avoid AV detection, so they want to make sure that the malware they distribute are also packed with the same version of packing so as to bypass AV detections.

LO: Is that relationship with between Emotet and TrickBot something that you guys had seen in the past? Or is this more of focusing on those obfuscation techniques around TrickBot and Emotet?

SD: So this was not something that was seen in the past. In the past, we did see Emotet distributing TrickBot, but you know, TrickBot had its own sort of code obfuscation, and right now it looks like they share the same packer, but up to a certain point. And of course, within the payload, they have similar styles of execution as in when they resolve for DLL names or Windows API call names, it uses the same technique of looking at different hash values. And this is the same with other banking malware families as well. But you can definitely say that they're still both very different. And also TrickBot is known to spread itself by the malspam, so Emotet it sells itself as a malware as a service. And TrickBot uses Emotet's service to help spread itself. And in the time that Emotet was on hiatus TrickBot was using Ursnif to help distribute its payload.

LO: You also mentioned too in the report that, you know, Emotet's authors are using a new list of words to generate process names and to keep track of installed modules. And this definitely would make sense for them, especially as they become more modular. So can you kind of break down and go into more detail about this new list?

SD: Sure. So yes, Emotet has a list of words – that are actually quite consistent – of the binaries that are compiled within a certain time range. And the set of words remains consistent for up to a certain time point, after which you'll start to see Emotet distributing newer binaries with a different set of words. And this set of words is used to create a predictable process name. So it's actually a very clever technique that the bot uses to create an identity of itself on an infected machine. So now say it's infected a machine and uses a set of words to make a predictable name. And that that name gets relayed back to its C2 server. So now the C2 server has an identity of the bot, where it's communicating from, and also has an idea about what version the bot is being run. So then accordingly it's able to send an update binary back to the bot. And this update binary has a different set of words. So the list of words is nothing other than for the bot to be able to track which version of itself it's being run and for the C2 to also track which updated bot is communicating with it, so it can send the you know, correct version. And each version has its own list of C2 servers.

LO: So it's almost for like organizational purposes between the bots and the C2, that should be interesting to see how that plays out for sure. Is that something that you guys have seen with other malware, or is that a new trick that you guys are seeing emerging?

SD: This is not that typical with other malware is especially using a predictable file name. Emotet has been using this for a while, but it hasn't been talked about as often. And it's one thing that I thought about mentioning in this paper, because it brought to my attention that there is a reason why it's being made predictable. And, and it's also a great way to be able to detect if such a file is present on your machine, especially if you have this list of words in your analysis. But yes, it's not something that's seen done by other malware.

LO: Right. Yeah. And then you guys had also outlined how there was a new export function on Emotet binaries – what's that all about?

SD: This was a style in which the packer was created. So the export function was nothing other than we saw these executable is having an export function call. And typically an executable file having export functions is not as common, though it is normal for them to have it, and is usually seen in DLLs. So that was one abnormality. And also what was unique with this packer was the similar packer was seen with Emotet as well as with TrickBot. Yeah, and I think the reason they changed the style in which they packed their files is mostly to evade antivirus detection or any other security detections. Oftentimes you have a lot of signatures that will try to emulate a file from the entry point of the malware binary rather than from its export function, for example. Or you have signatures that detect on the static properties at the entry point or file. So it's pretty easy to evade detection.

LO: In terms of delivery mechanisms or targeting are you guys seeing any changes there since Emotet came back out of sleep, anything new there?

SD: So in its delivery mechanisms it hasn't changed drastically, it still uses updated spam templates. And these are templates that it obtains based on its being able to steal messages from an infected machine. So after using the stolen messages it's able to create different spam templates. And what was commonly heard about before was, where these templates had an ongoing conversation. So it looked like a response to an existing email thread, but what we noticed was that the Emotet authors, they adapt to the current times, let's say. And so they try to make sure that, to increase the chance for a user to click on the attachments, it adapts to the current times. So recently what we saw was the Halloween theme. So you saw attachments having documents with the Halloween theme, there was a "trick or treat" message in it. And earlier in September when it first came out from its hiatus, a week after it came out with a document lure claiming to be Edward Snowden's new book, so they're definitely not being quiet. They're using different social engineering definitely. So anything that could get a user to download it.

LO: Right definitely sounds like they're keeping up with the times of any holidays around or new books in the case of Snowden. So how can potential victims protect themselves from the Emotet threat moving forward?

SD: Yes. I mean, that's something we have to always keep in mind. And so Emotet, you know, these authors, they're always looking at the news. So they know the vulnerabilities out there, what's the newest vulnerability and how they can try and take advantage of it. And this is clear in some of the modules that they propagate. And so when we analyze these modules we see like, especially in their worm module, where its able to propagate itself through the network and try to infect as many hosts. So as a user, I think having an updated system is really important. So as for these vulnerabilities to not take effect. And then for the social engineering part, you know, it's really hard. They're getting more and more clever in their tactics and how they lure people to click on attachments. I think what would help is just staying on top of trends and following advisories. And just I think being more vigilant about emails in general, since it is still such a primary mode of communication.

LO: Right, for sure. Well, we will be tracking the Emotet threat as it continues over the next few months. Suweera thank you so much for coming on to the Threatpost podcast.

SD: Thank you. Thank you for having me.

LO: And once again, this is Lindsey O'Donnell here with Suweera De Souza, principal security research analyst, catch us next week on the Threatpost podcast.
