Emotet's Takedown: Have We Seen the Last of the Malware?

By Lindsey O'Donnell

Published: 2021-02-03 · Archived: 2026-04-05 17:59:44 UTC

A week after law enforcement agencies said they took down Emotet, there has been no sign of the prolific malware.

Sherrod DeGrippo, senior director of threat research and detection with Proofpoint, shares insights on the global law enforcement and private-sector takedown of the major cybercrime tools such as Emotet.

Last fall, agencies targeted TrickBot's infrastructure to disrupt the prolific malware, and last week, they took down servers supporting the Emotet malware.

Threatpost discusses with DeGrippo how effective these law enforcement operations are when it comes to fully wiping out malware? TrickBot returned just months after the disruption effort, for instance. DeGrippo said that no activity involving Emotet has been detected since the takedown effort occurred last week.

"I think that it was so splashy and such big news and had video and had all of this collaborative action across working groups, the community law enforcement, it seems to have been much more effective," she told Threatpost.

"And I am hopeful that we will continue to see Emotet off the threat landscape," she said. "I honestly think at this point, it's going to take so much work and will be so much risk to get Emotet back up… I don't know that it even will be worth it to them at this point, because it's so dangerous, and it has so much visibility on it."

In this week's Threatpost podcast, DeGrippo talks about how these law enforcement operations are carried out – and what makes a malware takedown successful versus a flop.

Download the podcast direct here, or listen below.

Below is a lightly edited transcript of this week's Threatpost podcast.

Lindsey Welch: This is Lindsey Welch with Threatpost and I am here today with Sherrod DeGrippo. Sherrod is the senior director of threat research and detection with Proofpoint. Sherrod thanks so much for joining me today.

Sherrod DeGrippo: Thanks for having me, Lindsay. It's great to talk with you again.

LW: You too. We've talked in the past about malware families and kind of what you're looking out for, from your perspective, in terms of threat intel. Today, we're talking about some of the biggest malware takedowns over the past few months. And this is pretty timely, because just last week, the Emotet malware, which we've talked about a ton in the past, and which is one of the most prolific malware strains out there globally, it was dealt a blow, thanks to a takedown by an international law enforcement consortium. So Sherrod, I know from your perspective

that you've been tracking Emotet for a while now. And the malware itself has been around since 2014. So this is this is a pretty big deal, right?

SD: It is a very, very big deal. And it's something that I think that if most threat researchers, especially on my team, if they had a wish list, Emotet getting taken down would probably be number one on a lot of people's wishlists. So the fact that this has actually happened, and here we are, a week later, still having seen zero activity in terms of actually sending that threat, trying to deliver that threat through email vectors, certainly; we don't see it. So you know, congratulations to the groups that worked on getting this done and everyone that contributed because we've gone a week, and there's been nothing. So we're all sort of holding our breath. But this is looking pretty good so far.

LW: Yeah, yeah, I think that is very true that this was kind of on the top wish list of many security researchers but also defense teams, and reading about the the takedown by law enforcement agencies, was there anything that really stuck out to you beyond the fact that we have now not seen Emotet in the past week since it's occurred?

SD: Sure, I think that most people that work on malware, certainly the majority of my team, you know, this is something that they're very interested in. This is something they want to know about, whether it's part of the landscape that we work on at that moment or not. So this was huge news across the industry, certainly in threat research communities. The things that stood out to me about the actual law enforcement actions, to be honest, I mean, there was a lot of spectator excitement watching some of the videos that were, you know, shocking, fascinating – seeing inside of what is purported to be the actual law enforcement action against operators of the botnet, potentially looking at video of the back ends, seeing lots of PCs with no case on them, which brought back a lot of memories. So I think that it's really fascinating. This is something you know, we hear about law enforcement action in the past against TrickBot and others. And this really seems different. First of all, we see these videos, we've gotten quite a bit of information and fascinating looks inside with those videos. And then on top of that, the difference here is that this really seems to have worked. And so it just has a feeling that's a little bit different. I hope that I'm not jinxing anything. I hope this doesn't come back to bite me. But this seems very real and very effective. So it's reverberating throughout the industry. People are kind of shocked.

LW: Yeah, I really, I thought it was really interesting that there was kind of that video footage accompanying this takedown. And it was kind of cool to see officers seize computer equipment and the gold bars and kind of foreign currency.

SD: Looking inside, it was really interesting. One of the things that caught my attention that I've mentioned to some people is, if you go back and watch the videos, there's a lot of prescription medicine boxes; silver bars or gold bars; lots and lots of currency, U.S. currency, euros. The thing that we're thinking too, essentially part of what enabled this is that they were located in Ukraine, which, when when an actor is located physically in Russia or the infrastructure is heavily located in Russia, typically we kind of say, "Look, they're never getting caught there, there will be no law enforcement action, and Russia just doesn't allow it." You just kind of have to say, "look, if you're in Russia, you're protected." The joke is, you know, among my team is sort of the biggest mistake they made was being located in Ukraine. So the fact that we went that far is really impressive.

LW: Right. Yeah, that's, that's a good point. And I mean, to your point, too, about takedown efforts in general and why they're so interesting, at least for me as a reporter to cover and for you as a security researcher to kind of look

into how they play out. I feel like there's a lot of you know, news and research out there about the campaigns themselves and the malware and the hacks and exploits. But there's not a lot of follow up like this about actual action being taken. And I'm very curious if you think that will be different, or, if this will change at all.

SD: I hope so. I hope that we continue to get a better and better look into these. I've mentioned before on Twitter that I am fascinated by indictment documents, when those come out, they are absolutely brimming with really helpful information, specifically victim information. Fin7, a really well known financial threat actor, very sophisticated threat actor has multiple indictments and multiple court filings that allow you to see who those victims were that allow you to see IP addresses, infrastructure, that allow you to understand the actual daily work processes, the tools that are being used. And those can be really, really helpful in understanding the landscape, the culture, the entire crimeware system. And so I'm hoping that as this Emotet investigation is processed, that we will start seeing more of that information released, and that we'll start to see the court filings – whatever court those end up happening in if it's multiple, if it's one – so that we can see inside even more, and then also possibly use that for further detection.

LW: Right, right. Yeah, I imagine those resources would be kind of invaluable to the security research community and defense teams – not just for particular cybercrime groups, but also, you know, for the TTPs that could be adopted or are being used by other similar cybercrime groups as well.

SD: Absolutely, you can definitely pick up a lot of that. And in my role at Proofpoint, I'm responsible for detection. Emotet, over the years, as long as I've been in this role, because Emotet has been around, even longer than I've been at my current job. It has been something that literally has kept me up at night. Literally, I see the campaigns coming in. I see my team working on that detection. They're amazing. We have an amazing team focused, previously focused on Emotet. And I would go to bed at night sometimes thinking when I wake up in the morning, are we going to have new Emotet, are they going to change their techniques? Are they going to try to evade us? What are they going to do? And I quite literally am able to sleep a little better.

LW: Yeah, it's definitely like, I'm sure it's some peace of mind for you and for others as well. I guess one question I have, and this also points to law enforcement takedown efforts, overall. But you mentioned the TrickBot takedown operation last fall and TrickBot returned after I think it was one or two months after that. Do you see this being the end of Emotet as we know it? Or what's kind of the course of action here? For attackers in terms of getting their infrastructure set up? Or, you know, kind of making some sort of comeback?

SD: Sure. I think that TrickBot – I hope I don't regret saying this in the future – But I feel like the TrickBot and Emotet takedowns, while they were just a few months apart are very, very different. TrickBot came back very quickly. We were seeing it as soon as three weeks after that action, continuing to ramp up the efforts from being out of commission for a couple of weeks. So we track them as TA547, one of the main TrickBot actors and TrickBot is one of those pieces of malware that is distributed amongst multiple actors. The takedown action was against the botnet. It was not against the authors, the back end, it was a really different focus. And I think that that is what allowed it to come back up so quickly is that it was really dispersed. It was really distributed, and multiple actors had been using it and still continue to use it to this day. We see a TrickBot campaign once or twice a week now. So we saw eight in January, I would imagine that we'll continue to see one or two a week for the next several months.

Emotet, we haven't seen any sending since this action happened approximately a week ago. I think that it was so splashy and such big news and had video and had all of this collaborative action across working groups, the community law enforcement, it seems to have been much more effective. And I am hopeful that we will continue to see Emotet off the threat landscape. And I honestly think at this point, it's going to take so much work and will be so much risk to get Emotet back up, if they didn't get all of those human actors. I don't know that it even will be worth it to them at this point, because it's so dangerous, and it has so much visibility on it.

LW: Right. And, you know, speaking of these, these takedown operations, and different types of operations, would love to know kind of your insight into what goes into the takedown of different malware, infrastructure and servers or botnets or attackers themselves? What really needs to happen from law enforcement agencies, what do they need to know? And what are the specific methods that they need to take to really kind of put the nail in the coffin here?

SD: Sure. So it's been quite a while since I've been in a federal position. I've been in the private sector for quite a long time. But essentially, the things that law enforcement needs to do are really varied. And I think that with cyber operations, it really comes down to a lot of jurisdictional responsibility, these agents will do their work in one location and then need to get deputized to be able to travel to another location or involve an internationally deputized law enforcement agency. So the coordination across those agencies, from my point of view, that actually is the more difficult piece of this, as opposed to a lot of the technical capabilities. It's a bit controversial but insofar as my one and only hot take that I'll try to give you today, I really think that law enforcement, when it comes to Emotet, when it comes to TrickBot, those are definitely worth it. They're huge. They have millions, if not billions, of dollars of victims, in terms of money that that has been siphoned out. But unless it's these really big, heavily impactful takedowns, I don't always see this as the best use of law enforcement. It's so difficult to make this happen. It takes so much energy and effort, Emotet was worth it. But every little crime gang operating out of Eastern Europe is not going to be worth it for law enforcement to go after, which is why as security professionals, we have to make sure that we're doing our due diligence.

We can't just say, "Oh, you know, well, they're gonna get arrested." And that's our solution, like, law enforcement is not security. So it's one of those things where we still have to do the same kind of work differently than law enforcement is focusing on.

LW: Right. That's a really good point. I mean, where does the onus lie in terms of preventing these types of hacks? And you're absolutely right, in my opinion, that part of it does still rest on kind of the security community and defense teams to make sure that these these don't, because there will always be cyber criminals, right. I mean, you're right, you can't really weed out every single one.

SD: Yeah. And I think that's really important. I think it's really important to recognize the role of the community and the various organized groups that worked on this, Emotet was the friends we made along the way, it really is one of those things where it's one of the nicest communities you could ever find those those people participating in that were fans, they are fantastic people, and I'm sure that they'll stay together in their friendships.

But I also think it's really important to say the real blame here lies with the organized criminals in Ukraine. So I really want to make sure that we're not saying things like, well, you shouldn't have clicked on that, or you shouldn't have downloaded that. You shouldn't. But maybe they shouldn't do crime either.

LW: Yeah, exactly, that's a good point. Well, beyond Emotet. What are some other malware families that we should really kind of be keeping our eyes on? I know Agent Tesla has been one that's really been kind of hammering companies hard over the past year and has come out with various new tactics and whatnot. What are you seeing from your standpoint?

SD: Oh, that's funny that you when you started talking, the first thing I was gonna say was Agent Tesla. It's a keylogger that has evolved and evolved to have lots of really cool features and capabilities. We're seeing an Agent Tesla every day, for the most part in terms of campaign volumes.

Also, when we're talking things that are big and bad, like Emotet and TrickBot, you know, Dridex and Ursnif. I mean, they're number two and three on my wish list, probably Ursnif is number two and Dridex is number three. I think that if we see more law enforcement action, those are the best targets for them to go after those are large banking Trojans, they are distributed very well. So Agent Tesla is definitely a threat. Ursnif and Dridox have been around a lot longer and are up in that sort of legendary air with Emotet. So I would love to see if they're next on the list.

LW: Yeah, and I know with Dridex, at least in the US, law enforcement also seems to be keeping their their eyes on that one. I mean, was it 2019 or something where US authorities were were offering like $5 million for information on the alleged leader of a company associated with Dridex.

SD: I'll be interested to see if we end up with law enforcement action against Dridex or Ursnif. If I was running some cyber intelligence law enforcement agency worldwide and just had all that access, I think I'd probably go after Ursnif next.

LW: Absolutely. Yeah. Well, Sherrod, thank you so much for coming on today to the Threatpost podcast to talk a little bit about Emotet and what other malware families we should be on the lookout for.

SD: Thanks for having me, Lindsey. It's always great to talk to you.

LW: You too. And to all of our listeners, once again, this is Lindsey Welch talking with Sherrod DeGrippo with Proofpoint. Thank you for tuning in. And be sure to catch us next week on the Threatpost podcast.

Want more in-depth security interviews and infosec insights? Check out our podcast microsite, where we go beyond the headlines on the latest news.
