**-- How much of a threat does Emotet pose to organizations today?**

Any malware, trojan, or worm is going to be a potential threat to organizations. Either through targeted or ‘drive-by’ attacks, these tools (make no mistake these are tools for malicious actors) are built with the purpose to infect and provide value from a company’s infrastructure, and data, or just wreak havoc.

Emotet has seen a resurgence since its takedown, which to me indicates that the actors feel they have invested a great deal of effort and time into something and still see value in it. The reality is that they may not be targeting a specific organization with it but maybe taking a shotgun approach, which is likely to have success. In the end, does it matter if they spend years targeting the largest organization and have a 100% hit rate or if they send malware against 100 organizations and only get 2 successful deploys? No, it does not, they will still be able to gain value out of that successful deployment, and it will often be a lower effort for them.

What makes this approach even more appealing for the group operating the current version of Emotet is that they are malware-as-a-service. They do just need infected systems to allow for the deployment of their customer’s attacks, so the more systems they have, the better off they are. This is why the shotgun approach is going to be the better approach for them. So, to address how big a threat this is for organizations, it is something that every organization should be taking seriously.

With Emotet also being a polymorphic malware (changes it’s code every time it is called), it is less important to key off of hash values and more important to a behavior detection built in. Additionally, organizations should be deploying a defense in depth approach, so having strong spam filtering, email attachment and URL scanning (both reputation and payload detonation), user awareness training, and strong internal network security to assist with minimizing the impact of Emotet in their network. I would say, that SMB organizations are most likely at the highest risk, which can be evidenced by the yearly breach reports that show this market is the most breached.

**-- What does Emotet's recent move to 64-bit code indicate and how might it threaten organizations?**

I will preface this as this is my personal conjecture on why the move to 64-bit. When Emotet first emerged, 32 bit systems were still the predominant processor type, so developing for the lowest-level system was the best approach. Now, nearly, if not all, new systems are 64 bit processors and with this is able to handle larger amounts of RAM. So, my thought is that the group behind it made the shift to take advantage of the better processor to deploy and operate the malware on the end point more efficiently.

Another aspect to keep in mind is that there has been a recent shift of ransomware to not fully encrypt every file it touches but rather to encrypt sections of the file or bytes of the files on the system. This accomplishes the same goal of making the file unreadable or usable but it is much faster and harder to detect than full encryption. So, could this be another reason of Emotet moving to a 64 bit loader? A stronger shift from just malware-as-a-service to ransomware-as-a-service?

**-- What does the pivot away from macro-based attack vectors tell us about Emotet's authors MealyBug/TA542?**

I’ll be honest, I’m do not have the right technical details to answer this question. I’ve not done the research or had discussions with my team on what this impact may be.

**-- In the past year, Emotet has added modules to steal credit cards and spread laterally using SMB. How do these new modules threaten organizations?**

This is a great question. As a CISO for a financial service provider in the B2B space that works with a lot of SMB customers, I can see what this shift is about. SMB companies will have a lower investment in security, this is known. It’s just not feasible for a $50M company to have the same level of tools, teams, and capabilities as a $1B company. Short answer is that this makes them more vulnerable and Emotet more likely to gain access and keep access in those systems. This is not anything earth-shattering new, but shows that the shift is moving to further reestablish the network that was operational before their takedown.

This may also indicate what we have all seen in recent years as for attack strategy for malicious actors. Rather than go up against a well-fortified, well-funded security team at a fortune 100 company, why not target the supply chain? Wouldn’t it be easier to gain access to a much smaller partner that does not have the same level of investment in security, utilize that compromise to then pivot to the fortune 100 that you are targeting? Afterall, that is what we have seen from the Solarwinds and Kaseya breaches.

As for credit cards, these always hold value on the open market. If Emotet is going to continue to offer up malware-as-a-service in the newest iteration, having credit card stealing capabilities seems like a good solution to have in your product (I say product because it is a product on the black market). To further this, there are more and more SMB companies that are utilizing credit cards for payments of services, good, and materials since coming out of COVID. Working capital can be hard for SMB companies to attain to allow them to purchase the goods they need which has driven the market to look towards credit cards to gain the buying power they may need. Afterall, if the SMB is selling to larger companies, they may be offering their services up on terms, as much as 90 day terms, so they will not have that working capital to get the goods or materials needed to provide the services to the larger organization without some sort of float credit.

-- How does Emotet's ability to rapidly change its configuration, attack vectors and C2 infrastructure threaten organizations?

Speaking from the side of someone that is defending against this, it makes it nearly impossible to utilize signature-based detections. I cannot rely on a dirty IP address to tell me that the communication is malicious, I cannot rely on signature-based detections to assist with preventing or stopping the spread. At this point, I have to rely on behavior and strong security controls in my network and on my systems to help prevent or contain the malware after it has landed. These types of detections are much more reactive and oftentimes require a larger investment in people hours to investigate and determine what a file or system is trying to do. This pulls my team away from other tasks like further securing our environment and, in my opinion, leaves us more susceptible in the future.

-- A 2019 Kaspersky blog post said that there's no 100% sure-fire way to protect against Emotet. Is that still true?

Yes, this is true. But this can be true for almost any malware out there these days. It used be signature-based detections that provided protection once the malware was known but with the shift to polymorphic, to combat this detective capability, those have fallen by the wayside. In recent years, threat intelligence has been utilized to help with detection, so keying off of IP addresses, email addresses, etc. but with the new focus on rotating the botnet and email addresses, this has become less effective. Really, where we are at is that we need to use behavior-based techniques, and utilize email systems that detonate the payloads to determine if they are malicious. But even we are seeing malware evolve to defeat these. Recently, my team and I have discussed an uptick in malware that is designed to detect it running in detonation software (O365 analysis, FireEye tools, etc.) and to change it’s behavior to avoid detection in these tools. With this being a cat-and-mouse game, as we evolve our detection and defensive capabilities, attackers will shift or evolve to avoid, neutralize, or to have their own defensive techniques to be successful.

-- What are some other ways in which organizations can defend against Emotet?

I’ve touched on several above, but to summarize, utilize defense in depth. Utilize email-based security tools and detections to attempt to identify the malware coming in via phishing or spam email. Deploy endpoint detection and response tools that are not just signature-based but also behavior base. Utilize segmentation and network security controls to minimize the spread of the malware once it is in the network. But one of the most important things we can do is to do user education.

-- Would research detailing Emotet's recent evolution, including indicators of compromise, additional abilities and new command-and-control infrastructure, be useful to your organization? Would your organization be likely to incorporate such information into its own defenses?

Yes, yes we would incorporate and utilize these to help defend against it.