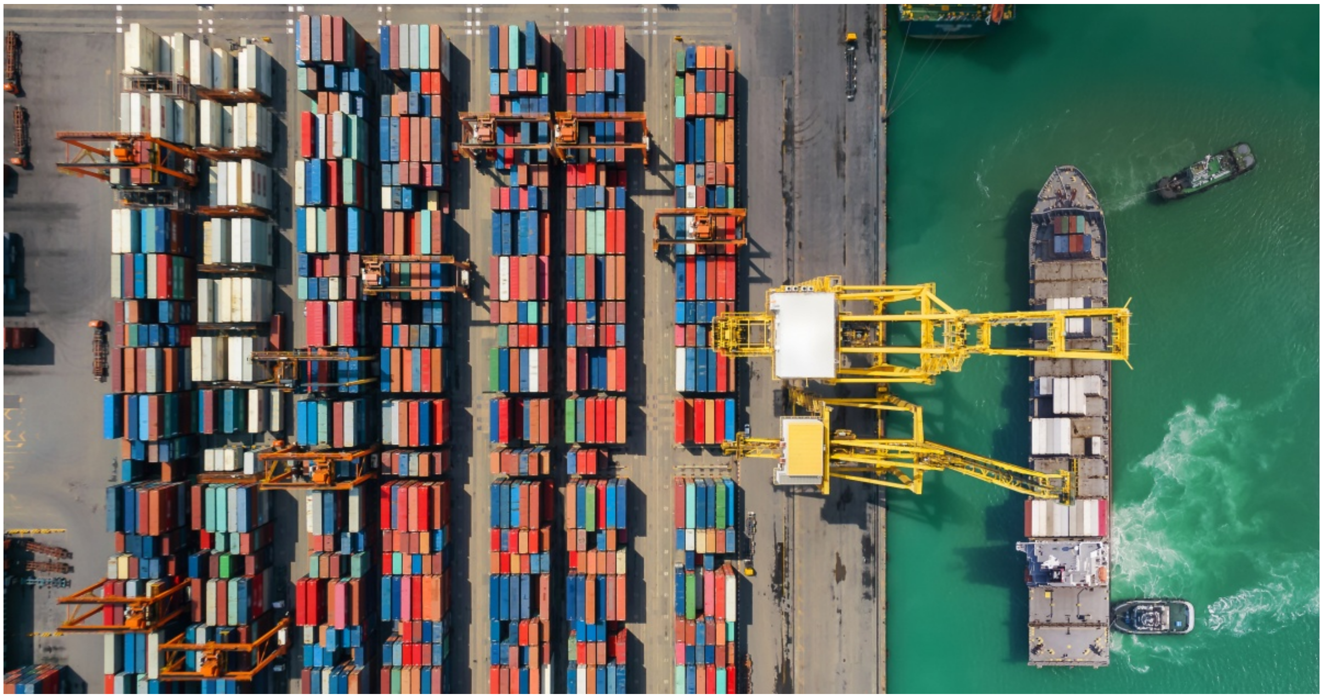
The Evolution of Emotet: From Banking Trojan to Threat Distributor

symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor



Threat Hunter TeamSymantec

Evidence indicates that Mealybug, the threat group behind Emotet, has evolved from maintaining its own custom banking Trojan to operating as a distributor of threats for other groups.

Mealybug is a cyber crime actor that has been active since at least 2014. It is identified by its use of its custom malware, Trojan.Emotet. It appears to have changed its business model in recent times, evolving from targeting banking customers in Europe to using its infrastructure to act as a global packing and delivery service for other threat actors.

Because it can self-propagate, Emotet presents a particular challenge for organizations. Network worms have been experiencing a kind of renaissance, with notable examples like WannaCry (Ransom.Wannacry) and Petya/NotPetya (Ransom.Petya). Network spreading also means that victims can become infected without ever clicking on a malicious link or downloading a malicious attachment. Once on a computer, Emotet downloads and executes a spreader module that contains a password list that it uses to attempt to brute force access to other machines on the same network.

"Group behind #Emotet Trojan start global packing, delivery service for other threat actors https://symc.ly/2KHADCx"
Click to Tweet
Emotet's method of self-propagation—brute forcing passwords—has additional potential to cause major headaches for organizations as it may result in multiple failed login attempts, which can lead to users becoming locked out of their network accounts. This has the knock-on effect of increased calls to IT helpdesks and general loss of productivity. This was a hallmark of the notorious Conficker (W32.Downadup) threat and, 10 years later, threats continue to cause similar problems.

As well as brute forcing passwords, Emotet can also spread to additional computers using a spam module that it installs on infected victim machines. This module generates emails that use standard social engineering techniques and typically contain subject lines including words such as "Invoice". Some subject lines include the name of the person whose email account has been compromised, to make it seem less like a spam email. The emails typically contain a malicious link or attachment which if launched will result in them becoming infected with Trojan.Emotet.

Most recently, Mealybug appears to have expanded its operations to primarily become a distributor of threats for other attack groups.

Emotet becomes a global threat

When Mealybug was first identified in 2014 it was using Emotet to spread banking Trojans, and was focused on targeting banking customers in Germany. At the time, Mealybug was using Trojan.Emotet as the loader portion of W32.Cridex.B, a rewritten version of the Cridex banking Trojan. In 2015, Mealybug started targeting Swiss banking customers as well and evolved Emotet into more modular malware. The new version of Emotet had separate modules for its loader, banking data theft, email login theft, distributed denial of service (DDoS) attacks, and malicious spam.

Mealybug has primarily been engaged in using Emotet for the delivery of banking Trojans, and in 2017 it was the first group to deliver the IcedID (Trojan.IcedID) banking Trojan. However, also in 2017, it was observed delivering the Trojan.Trickybot and Ransom.UmbreCrypt ransomware. Mealybug has developed its capabilities over the years and now appears to offer an "end-to-end" service for delivery of threats. It delivers the threats, obfuscates them to reduce the chances of detection, and provides a spreader module that allows the threats to self-propagate.

Emotet gets an initial foothold on a victim machine or network by sending an email containing either a malicious link that leads to a downloader document or that has a malicious document attached. Anti-analysis tactics have been present in Emotet since at least 2015 and, in 2018, Emotet's payload consists of a packed file containing the main component and an anti-analysis module. The anti-analysis module performs multiple checks to ensure it is not being run on a malware research machine, then loads the main component. Either PowerShell or JavaScript is used to download the Trojan, which delivers a packed payload file to the victim machine. Once on a machine, the latest version of Emotet:

1. Moves itself to its preferred directory
2. Creates a LNK file pointing to itself in the start-up folder
3. Collects victim machine information and sends it to the C&C server

It can then download any new payloads from the C&C server, and execute them. Emotet can download an updated version of itself, or any other threat. Existing versions of Emotet download modules from the C&C server that include:

- **Banking module**: This module intercepts network traffic from the browser to steal banking details entered by the user. This is what gave Trojan.Emotet its reputation as a banking Trojan.
- **Email client infostealer module**:This module steals email credentials from email client software.
- **Browser infostealer module**: This module steals information such as browsing history and saved passwords**.**
- **PST infostealer module**: This module reads through Outlook's message archives and extracts the sender names and email addresses of the messages, presumably to use for spamming.

> According to Symantec telemetry for the first half of 2018, its focus now is mainly on targets in the U.S.

All information stolen by these modules is sent to the C&C server. Emotet also has a DDoS module that can add the infected machine to a botnet to carry out DDoS attacks.

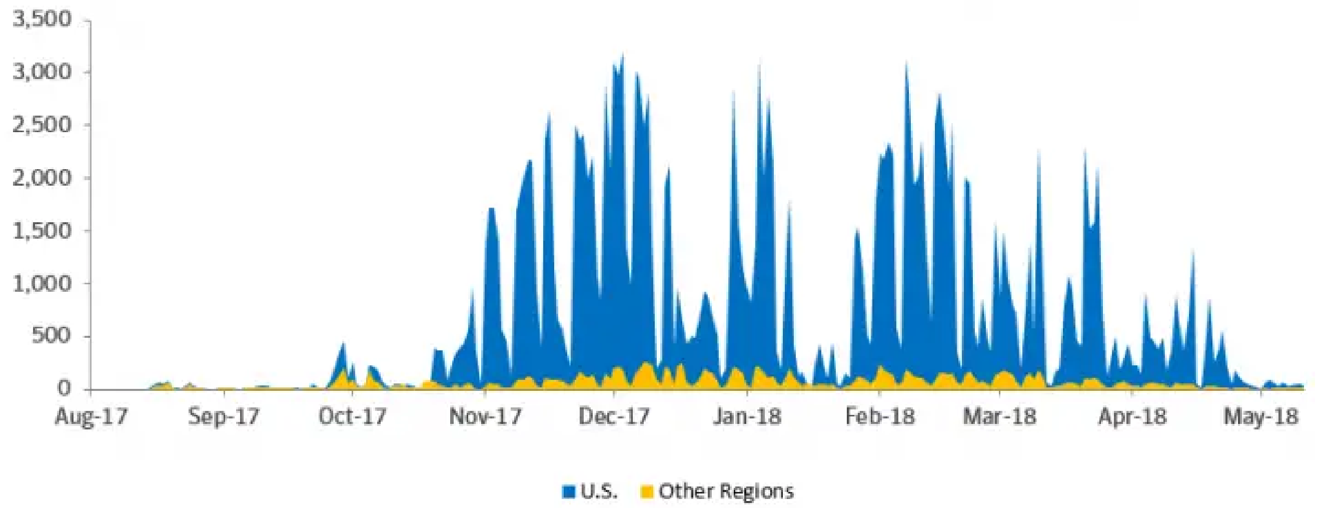


Figure 1. Trojan.Emotet primarily focusing on targets in the U.S.

Emotet's geographic targets have also increased significantly over the years. After a relatively quiet period since 2015, detections of Emotet surged in the second half of 2017, and in that year Mealybug's targets included victims in Canada, China, the UK, and Mexico. However, according to Symantec telemetry for the first half of 2018, its focus now is mainly on targets in the U.S.

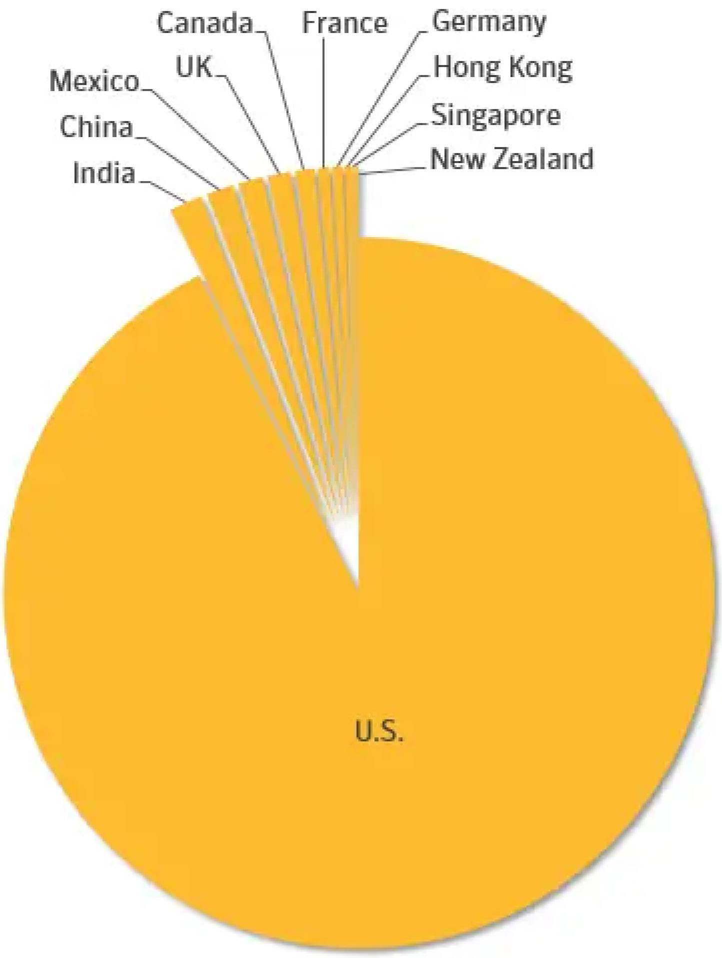


Figure 2. Trojan.Emotet detections by geographical region

Qakbot

Since February 2018, Emotet has been used to spread W32.Qakbot, a family of banking Trojans known for behaving like network worms.

Like Emotet, Qakbot can self-propagate. Qakbot attempts brute force access to spread across networks and also uses “living-off-the-land” tools to propagate. It uses PowerShell to download and run Mimikatz (Hacktool.Mimikatz), an open-source credential stealing tool that allows attackers to move rapidly across a network once they have established an initial foothold.

The fact that both Emotet and Qakbot have self-spreading capabilities mean that once these threats get onto your network they can spread aggressively. The fact that both attempt brute force access to spread across networks also increases the risk of users being locked out of their devices. A spike in Qakbot detections in February 2018 indicates that “double-spreading” of the threat was taking place, meaning that Mealybug was using Emotet to spread Qakbot across networks, while Qakbot was simultaneously using its own self-spreading capabilities. The account lockout scenario is a very real danger, and a potential major headache for organizations.

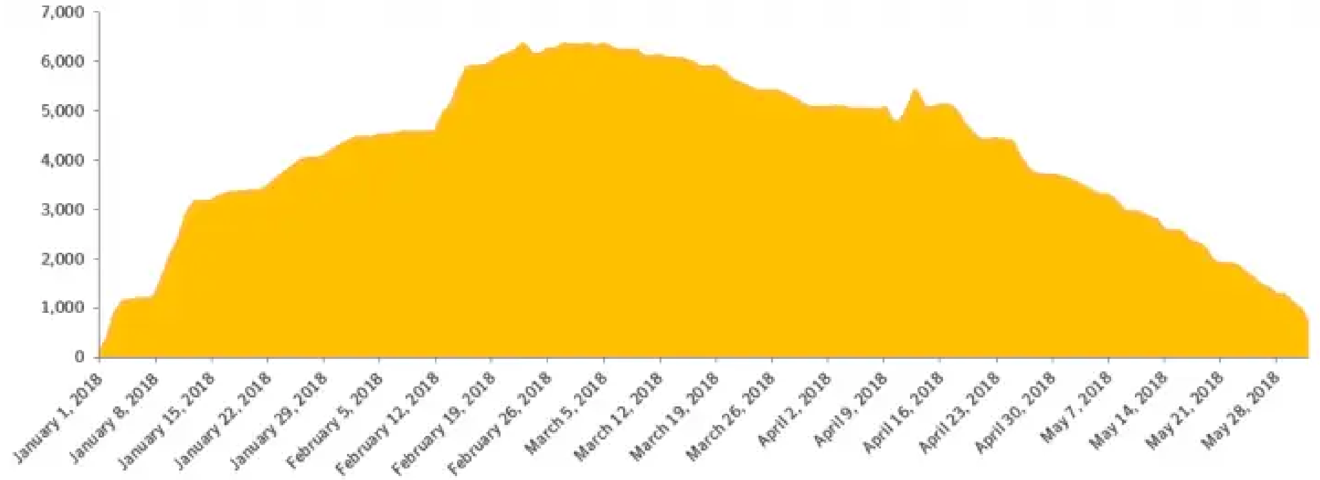


Figure 3. W32.Qakbot detections January 1 to May 28, 2018

Symantec analysis shows that Emotet and Qakbot are packed with the same packer, but there are multiple factors that suggest Mealybug is only providing Emotet as a delivery service for the actors behind Qakbot, and is not controlling the Trojan.

There does not appear to be any overlap between the C&C infrastructure of the two Trojans, and analysis also revealed differences in the code of their main components and in their anti-debugging techniques.

Mealybug using two different spreading mechanisms is also surprising because, as mentioned above, both Trojans attempting to brute force passwords could trigger account lockouts and stop the Trojans from spreading. It is unlikely Mealybug would use the two different spreading techniques if it was controlling both Trojans. For these reasons we believe Emotet and Qakbot are controlled by two separate groups, and that Mealybug is offering Emotet as a delivery mechanism for other threats.

Talking ‘bout an evolution

Mealybug seems to have found its niche as a provider of delivery services for other threats. The main component of Trojan.Emotet functions as a loader, and can theoretically support any payload. While it is still primarily known for distributing banking Trojans, it can in theory spread any threat, and there have been reports of it distributing the Ransom.UmbreCrypt ransomware. Mealybug presumably makes its money by taking a cut of the profits made by the threat actors who use its services. From what we can see, Mealybug appears to be operating for more than one attack group at a time, so we have no evidence that it offers itself as an “exclusive” distributor. In November 2017, Mealybug was observed delivering the Trojan.Trickybot and W32.Qakbot threats simultaneously onto the same machine in a few instances, and in one case within a few minutes.

Mealybug’s shift from distributing its own banking Trojan to a relatively small number of targets, to acting primarily as a global distributor of other groups’ threats is interesting, and backs up an observation we made in the ISTR that threat actors are evolving and refining their techniques and business model to maximize profits. In the ISTR we outlined how some threat actors appeared to be turning to coin mining as it became hugely profitable due to the rise in the value of cryptocurrencies. It appears Mealybug has decided that it can best maximize its returns through taking a role as distributor.

It may be that Mealybug was finding it harder to make money exclusively from banking Trojans so it had to change its approach. The growth in popularity and use by banks of two-factor authentication (2FA) has made it more difficult to compromise accounts by stealing credentials, and awareness and protection has improved as online banking has matured.

Challenges for organizations

Mealybug activity presents a number of challenges for organizations, including:

- Its worm-like capabilities mean it can spread rapidly across organizations.
- Emotet’s network-spreading capabilities mean that computers can become infected without any user interaction.
- Brute forcing passwords increases the chances of users being locked out of their machines in victim organizations, causing headaches for IT teams and affecting productivity.

Best practices

- Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single point failures in any specific technology or protection method. This includes deployment of endpoint, email, and web gateway protection technologies as well as firewalls and vulnerability assessment solutions. Always keep these security solutions up-to-date with the latest protection capabilities.
- Employ two-factor authentication (such as Symantec VIP) to provide an additional layer of security and prevent any stolen or cracked credentials from being used by attackers.
- Educate employees and urge them to exercise caution around emails from unfamiliar sources and around opening attachments that haven't been solicited.
- Require everyone in your organization to have long, complex passwords that are changed frequently. Encourage users to avoid reusing the same passwords on multiple websites, and sharing passwords with others should be forbidden.

Protection

Symantec has had protection for Mealybug attacks since the initial identification of the group's activities in 2014 and blocks such activities at every level of Mealybug's attack chain.

Detections by stage

Email:

Symantec Email Security products block malicious emails associated with Emotet.

Embedded link stage:

Web Attack: Emotet Download 2

Macro downloader stage:

W97M.Downloader!g20

Main module file stage:

- W32.Emotet.B
- Trojan.Emotet
- Trojan.Emotet!g1
- Trojan.Emotet!g2
- Trojan.Emotet!g3
- Trojan.Emotet!gen4
- Trojan.Emotet!g5

Main module loaded stage:

Trojan.Emotet!gm

C&C communication stage:

- System Infected: Trojan.Emotet Activity 3
- System Infected: Emotet Activity 2
- System Infected: Trojan.Emotet Activity 4

Spam and stealer and spreader module stage:

Ransom.Crypto!im

Emotet spreader infection stage:

- SONAR.SuspPE!gen39
- SONAR.Heur.RGC!g571

Targeted Attack Analytics

Symantec's new Targeted Attack Analytics (TAA), available in our ATP Product can detect attacks where an executable spreads to multiple machines across a network via credential theft, brute forcing, or an exploit. TAA detects Emotet's malicious activity due to patterns in its spreading behavior. In particular, TAA will detect when files are dropped by Emotet's spreader module on multiple machines in an organization.

Threat intelligence

Customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received multiple reports on Emotet. These reports detail methods of detecting and thwarting activities of the group that leverages this Trojan.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?