Emotet Disruption: what it means for the cyber threat landscape

digitalshadows.com/blog-and-research/emotet-disruption/

February 3, 2021

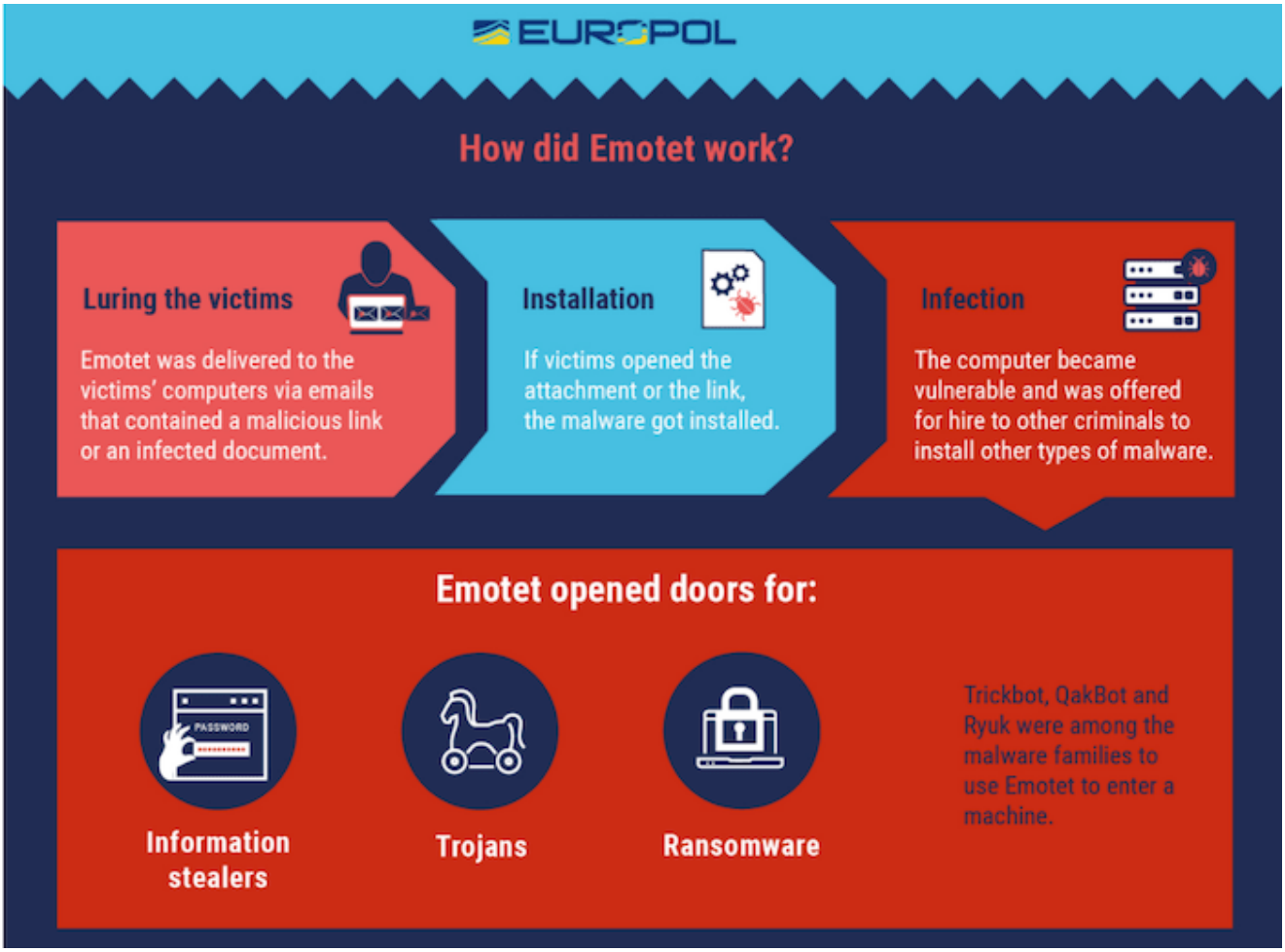
Last week, the European Union Agency for Law Enforcement Cooperation (EUROPOL) published a press release detailing the operation that led to the disruption of Emotet, one of the most prominent trojans that populated the cyber threat landscape. This operation, dubbed “Operation Ladybird”, was a joint effort led by the authorities of several European countries and the US and resulted in the takedown of Emotet’s infrastructure and the arrest of two Ukrainian members of this cybercriminal organization.

This operation has the potential to significantly shape the threat landscape. Emotet has been used in numerous cybercriminal operations, including ransomware operations, to gain initial access. Given its widespread distribution, the Emotet trojan has likely infected millions of devices worldwide. In this blog, we’ll analyze how Emotet came to be, the significance of Operation Ladybird, and reactions from the cybercriminal underground.

The Evolution of Emotet: From Banking Trojan to Ransomware Facilitator

The importance of Emotet in the threat landscape cannot be overstated. First discovered in 2014, Emotet initially functioned as a common banking trojan highly committed to remaining unnoticed. It was not long, however, before Emotet’s operators noticed that their malware variant could also serve other purposes, further increasing their payouts.

Emotet’s modular structure allowed the malware to be versatile. Its developers can reconfigure the trojan and reshape it as a loader in order to deploy second-stage payloads after getting access to a victim network. These changes turned Emotet into a multi-functional tool. Its ability to distribute other malware variants meant that it is also able to facilitate larger-scale ransomware campaigns.

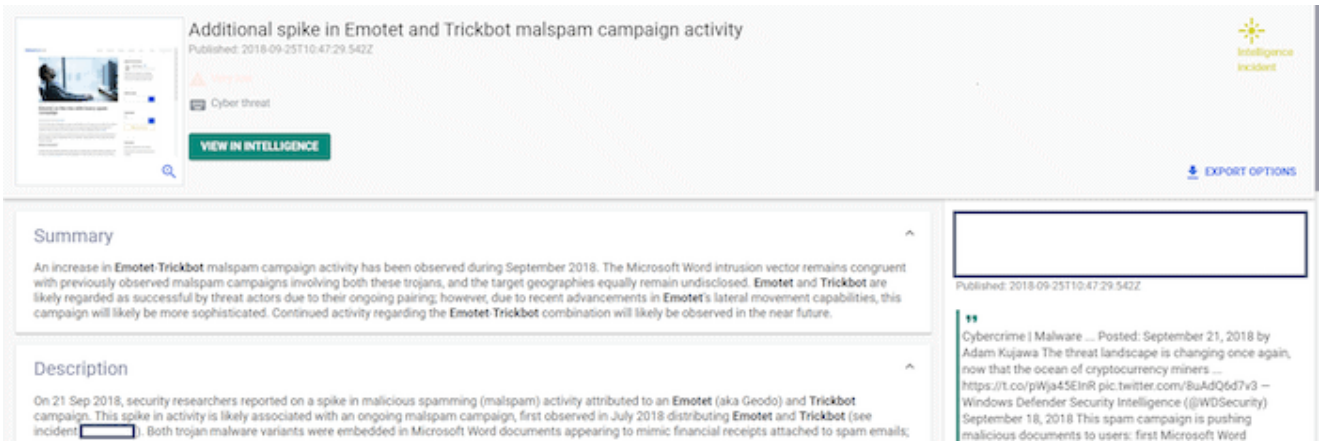


Emotet FAQ Infographic (Europol)

This shift has been crucial for Emotet's success within the cybercriminal community— used in tandem with other information-stealing trojan and ransomware variants, Emotet has been able to significantly expand and scale its operations at an astounding pace. At the same time, Emotet continued to use enticing lures in its social engineering efforts and developed highly successful spear-phishing techniques to ensure victims interact with its malicious emails.

Emotet's operators primarily use malicious email attachments and links to deliver its payload. Its operators have employed numerous techniques to remain undetected by antivirus software and download these malicious files onto the victims' devices. Once Emotet gains access to the targeted machine, it proliferates within a network. This can be achieved very quickly, thanks to its "worm-like" features and aggressive behavior.

In the past years Emotet partnered with other cybercriminals to scale its operations and increase its reach. Some of its more prominent partnerships include its association with the "Ryuk" ransomware and "TrickBot" trojan. Operators of these two malware variants were reported to have leveraged machines compromised by Emotet to install their own malware and solicit additional malware attacks.



Digital Shadows' SearchLight view of an Emotet and Trickbot incident briefing

Based on estimates (conservative ones), Emotet has insofar managed to make away with millions of US dollars throughout its campaigns—the Ukrainian police estimates a whopping $2.5 billion. One of Emotet's latest malicious operations was conducted in partnership with TrickBot and used different COVID-19-related phishing lures to increase the likelihood of a successful infection. Hopefully, the law enforcement intervention will cause this operation to be their last one for quite some time.

Operation Ladybird: How Law Enforcement Disrupted Emotet

On 27 January 2021, Europol declared that it had successfully infiltrated and disrupted Emotet's infrastructure in a coordinated international action. The "Operation Ladybird" was reported to have severely dismantled the "most dangerous malware in the world" and taken over its command-and-control (C2) infrastructure.

According to the information disclosed by Europol, a team of law enforcement officers, judicial authorities, and security researchers simultaneously hijacked numerous C2 servers used by Emotet and redirected their traffic towards law enforcement-controlled infrastructure. This practice known as "DNS sinkholing" is crucial to disrupting the infected machines' communication and can cause considerable damage to the botnet's operation.

DNS sinkholing à la Jonah Hill

Following Europol's press release, a Ukrainian law enforcement agency published a video of their raid against alleged Emotet operators. In the video, officers were seen seizing computer equipment, gold bars, and a large quantity of foreign currencies. Given Emotet's operation size, one would have expected the operation being conducted from a fancy mansion in a Caribbean island—but maybe cybercrime isn't always as glamorous as it looks on TV shows.

A screenshot of the Ukrainian law enforcement raid video

With this takedown, German law enforcement officers are using their access to affected servers to deploy an Emotet update that will remove the malware from all compromised devices on 25 April 2021. This update will prevent Emotet's C2 servers from communicating with compromised devices, thus inhibiting any further malware download. The delay has been set to give law enforcement agencies the opportunity to investigate compromised machines prior to the malware's removal.

Reactions from the cybercriminal underground to Emotet's disruption

Such a move will likely raise some eyebrows. From a researcher standpoint, looking at the behavior and reaction of cybercriminals is crucial to understanding the impact of these operations on the threat landscape. It can give us important insights into potential further activity. So, as soon as Operation Ladybird's news broke, we turned to cybercriminal forums to see how the cybercriminal community has responded to the operation.

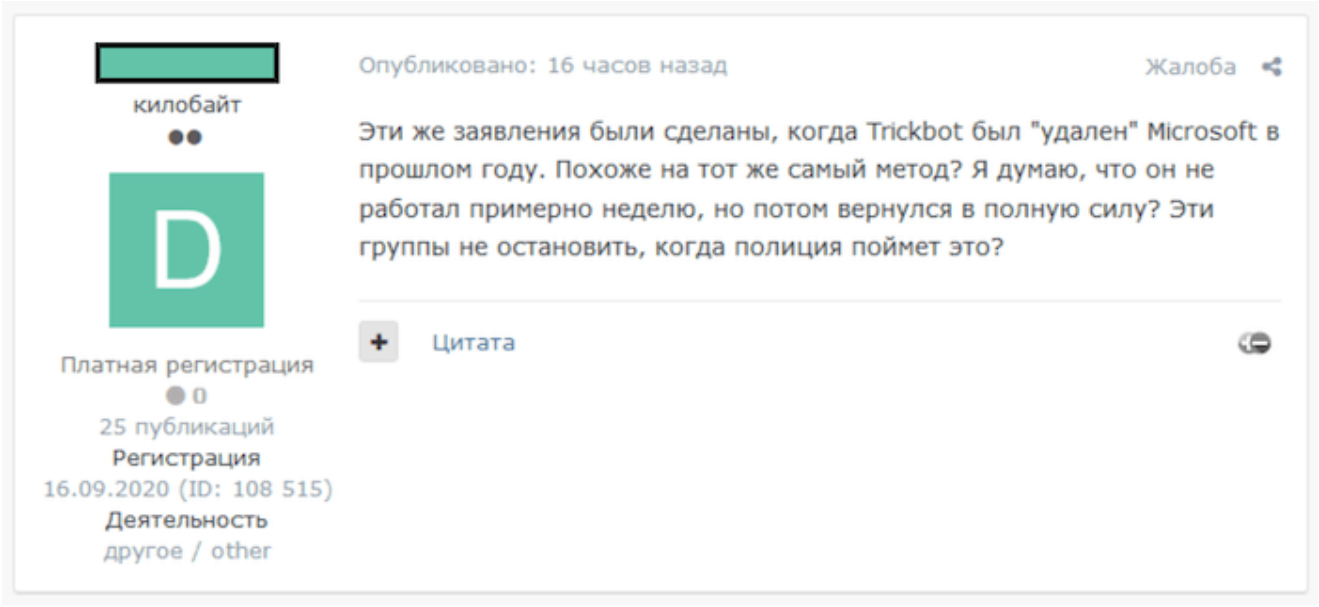
Actionable intelligence remains one of the most vital aspects of Cyber Threat Intelligence (CTI) and it appears that cybercriminals too, are interested in having some actionable information of their own. Besides nationalistic derogatory comments about Ukrainian law enforcement's involvement in the operation, we observed users on Russian-language cybercriminal forums complaining about the lack of technical details in Europol's press release on the operation.

Cybercriminal forum user complaining about how takedown stories are reported by the media

Others offered some common cybercriminal wisdom. One user mused that "the longer you work, the more footprints there are", implying that threat actors behind a successful cybercriminal operation leave traces that could lead to their identification and downfall. Cybercriminals usually pay careful attention to their operational security (OPSEC), but every now and then someone will inevitably get comfortable and let their guard down, leading law enforcement to their doors.

Cybercriminal forum user warning about threat actors making mistakes and getting caught

On another cybercriminal forum, a different user provided their take and raised an interesting point regarding the lasting impact of these operations. CTI enthusiasts will remember that back in October 2020, the US Cyber Command attempted to neutralize the TrickBot botnet in the run-up to the US Presidential elections. Although effective in the short-term, the reality is that TrickBot's operations continue to run today and the trojan is nowhere near being completely crippled. Drawing comparisons to that attempt, this user suggested that it remains to be seen whether Operation Ladybird will actually knock Emotet down.



Cybercriminal forum user comparing Operation Ladybird to last year's TrickBot takedown

Future Implications and Mitigation tools

Previous attempts to combat these malicious activities have so far yielded mixed results. On the one hand, the malicious activities associated with these malware variants are halted. On the other, these takedown operations don't often have permanent effects. The TrickBot example is a poignant one and is testament to the adaptability of these cybercriminals. These botnets' operators are extremely versatile and can recover from these attacks after a short time. If Operation Ladybird were to follow a similar fate, then it is likely that Emotet is not completely immobilized.

However, the "new and unique approach" of this law enforcement action has likely caused severe disruption to Emotet's networks and command-and-control infrastructure. While conducting this operation, law enforcement officers may have gained a unique understanding of Emotet's inner workings and modus operandi. Hopefully, this knowledge will translate to more long-lasting effects, and we can live a world of peace without Emotet haunting the scene.

Only time will tell how severe the damages caused by Europol to Emotet are. Besides, users should be warned that previously-infected machines may still run other malware variants such as TrickBot and QakBot. Since the uninstall update for Emotet will only happen on 21 April 2021, malicious files associated with Emotet will likely remain in compromised machines until then. And who knows what these malicious files can do.

In the meantime, it is highly recommended to use this tool provided by the Dutch police to verify whether Emotet had previously compromised your email address and password. On top of this, Digital Shadows' SearchLight service maintains a constantly-updated threat

intelligence library that monitors trends and key-players in the cyber threat landscape. If you'd like to access the library for yourself, you can sign up for a free seven-day test drive of SearchLight here.

Tags: Cyber Threats / Cybercriminality / emotet