TLP:WHITE

THE MALWARE-AS-A-SERVICE EMOTET

12/02/2021

TLP:WHITE

Table of contents

1 Emotet origins

Emotet (aka Heodo) first appeared in March 2017 and is the fourth iteration of the Geodo malware.

The origin of Geodo can be traced back to the Business Club, a cybercriminal group whose activity began around 2008, in collaboration with M. Bogatchev, creator of ZeuS malware [1]. This group successively operated JabberZeuS and GameOverZeuS (GoZ). [2, 3].

In parallel to the activities of the Business Club, one of its members, M. Yakubets, and an operator of its bulletproof hoster[1], A. Ghinkul, appear to have operated, or even developed, Bugat malware (aka Cridex, Feodo), which appeared in 2010.

One month after the FBI takedown of GoZ's infrastructure in May 2014, Dridex and Geodo banking trojans emerged. They were operated by past members of the Business Club, respectively Evil Corp and TA542 :

- Dridex, operated by Evil Corp, of which M. Yakubets and A. Ghinkul are part of, is the fifth iteration of Bugat malware, with some GoZ peculiarities [4, 5] ;
- Geodo, operated by TA542 (aka Mummy Spider, MealyBug or GoldCrestwood), would not have code similarities with Bugat but its network infrastructure would be inherited from that of Bugat version 4 [6].

  Comment: To simplify matters, Emotet refers to all versions of Geodo from 2014 to 2020.

Although informations about TA542 are very limited compared to those of Evil Corp, TA542 appears to be a Russian-speaking cybercriminal group [7]. According to Trend Micro, this group operates in the UTC+10 time zone, which includes Vladivostok region in Russia [6].

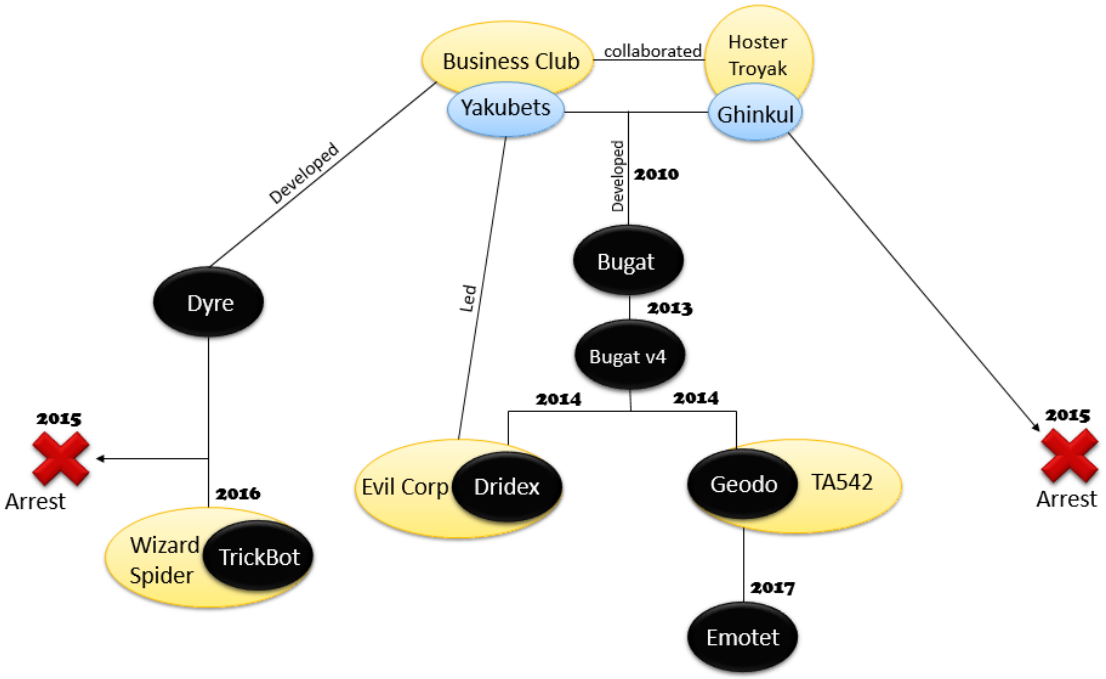

Fig. 1.1: Emotet origins

[1] On the black market, operators offer to rent servers in jurisdictions beyond the reach of judicial cooperation treaties. These servers are called bulletproof. The bulletproof hoster used by the Business Club, called Troyak, was dismantled in 2010 [2].

2 Evolution of Emotet's activity

2.1 From a banking trojan to a loader of malwares on behalf of other attackers

Initially spotted in 2014 as a banking trojan, the first three versions of Emotet targeted clients of banks in Germany, Austria and Switzerland. [8, 9]. The objective of these attacks was to carry out automatic fraudulent transfers from compromised bank accounts of individuals whose online banking access codes had been exfiltrated using Emotet [10].

Comment : It is possible that these money transfers were not only made on behalf of TA542 but also on behalf of other clients. Indeed, TA542 have sold Emotet on underground forums until 2015, when Emotet's services became "private" to the exclusive benefit of TA542 and possibly a limited circle of clients [11].

From 2015, Emotet evolved and became a modular trojan. Its various modules allow it to :

- retrieve passwords stored on a system as well as on several browsers (Internet Explorer, Mozilla Firefox, Google Chrime, Safari, Opera) and mailboxes (Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo!Mail and Gmail);
- steal contact list, content and attachments from emails ;
- spread within the infected network by taking advantage of SMB vulnerabilities and recovered passwords.

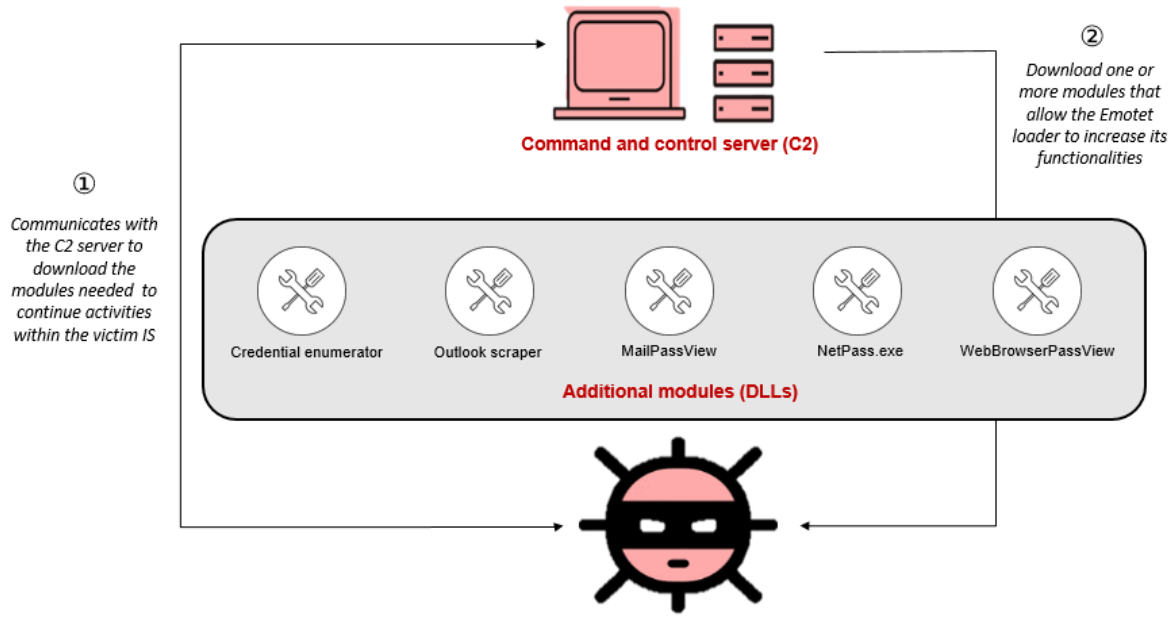

Fig. 2.1: Emotet modularity

Among these modules, MailPassView and WebBrowserPassView are legitimate tools hijacked by TA542 [6, 12, 13].

Since 2017, Emotet is no longer used as a banking trojan horse (the corresponding module has been removed [13]) but distributes malwares operated by attackers, customers of TA542, within the information systems (IS) it infects [12].

2.2 Emotet associated chain of infection

2.2.1 Possible vectors of infection

T1566 – Phishing emails

Emotet is usually distributed through phishing email sent by botnets operated by TA542 [14]. There are three independent Emotet botnets, named Epoch 1, Epoch 2 and Epoch 3, each of which has its own infrastructure [15]. These botnets are inactive simultaneously several times a year [16]. For example, Emotet was inactive from February to July 2020.

In 2018, approximately 98% of emails from Emotet campaigns contained a URL leading to the download of a trapped Office document. In addition, about 66% of the emails impersonated an existing entity, such as DHL, PayPal or UPS [17].

Since 2019, phishing emails have more often contained a malicious attachment such as Word, PDF or ZIP file, although emails containing URLs still exist.

Moreover, since 2018 the group has tended to become more sophisticated in its attacks. Indeed, TA542 has the ability to hijack email threads (email thread hijacking technique). Once the mailbox of an employee of the victim entity (or the generic mailbox of the entity itself) has been compromised, Emotet exfiltrates the content of some emails. Attackers then build phishing emails taking the form of a response to a chain of emails exchanged between the employee and partners of the entity he works for. The legitimate subject line of the phishing email is then preceded by one or more « Re : », and the email itself contains a history of a discussion or even legitimate attachments. These emails are sent to contacts of the victim, and more specifically to third parties within the entity (clients and providers in particular) who participated in the original thread, in order to increase their credibility with the recipients.

Commentaire : From August 2020, France (private and public sectors) has been the target of Emotet phishing campaigns exploiting email thread hijacking technique.

In 2020, in addition to this technique, TA542 :

- also builds phishing emails based on informaiton retrieved from compromised mailboxes, which it send to exfiltrate contact lists ;
- spoofs the image of entities, whether or not they were previous victims of Emotet (transportation companies, financial institutions, etc.). These emails may contain false invoices, delivery information or false job opportunities. Such a campaign dated July 2020 distributed the Emotet-TrickBot-Ryuk/Conti infection chain [18] ;
- exploits the Coronavirus theme as a decoy [19, 20]. For example, in March 2020, an Emotet campaign of this type reached Japan to distribute TrickBot as a second payload ;
- targets business email addresses with « sextortion » spam aimed at extorting money from the recipient employees and distributing Emotet within their company's IS [21].

These emails are most often sent from the attackers' infrastructure based on typosquatted sender email addresses, although some vendors indicate that they may be sent from compromised mailboxes [6].

T1189 - Watering hole
T1566.002 – Phishing containing trapped links

More rarely, Emotet is also distributed by RIG exploit kit, *via* compromised websites [13] and by SMS. Indeed, in February 2020, SMS messages were sent from US phone numbers, usurping the identity of banks and alerting recipients of the closure of their bank accounts. By clicking on the link in the SMS, the recipients were redirected to a web page mimicking that of the bank in question, and distributing Emotet [19, 22].

Comment : « Sextortion » campaigns as well as SMS campaigns suggest that TA542 may have diversify its sources of revenue and methods of compromise, unless the group has opened up, on an ad hoc basis, to a less sophisticated customer base than usual.

2.2.2 Proceeding an attack after receiving a phishing email

Once the macros are activated by the victim, a script is executed, contacting a URL to download an Emotet payload [2], before executing it [6]. These URLs correspond to compromised websites (usually Wordpress). Some websites may also have been created by the attackers themselves, as it was the case in 2017 [23]. They change very quickly, with dozens of new URLs appearing every day [23].

In July 2020, it was pointed out that TA542 was using webshells [3] available on Github to control compromised websites and employs the same password for all of its webshells. A white hat discovered the common password and was able to replace the Emotet payloads with GIFs on some of the Wordpress sites compromised by TA542. Thus, for several days, a quarter of the URLs used by TA542 distributed harmless GIFs [24].

Once installed, Emotet communicates with a C2 server, contacting the IP address directly, not a domain name. An Emotet sample often contains several IP addresses of C2 in its configuration [6] : if the first C2 in the list does not respond, the malware will try to establish communication with the next IP address, and so on. One or two C2s disappear every day, leaving room for one or two new ones. Approximately 100 C2s are active per version of Emotet and three versions are currently in circulation, for a total of approximately 300 C2s [4].

In 2018, the majority of the C2s in question were located in the United States, Mexico and Canada. 3% of them were located in France [6].

The protocol used by TA542 for communications between Emotet and the C2 is built on Protobuf, an open source code developed by Google [13, 6].

In particular, these C2s allow TA542 to download additional payloads on behalf of customers.

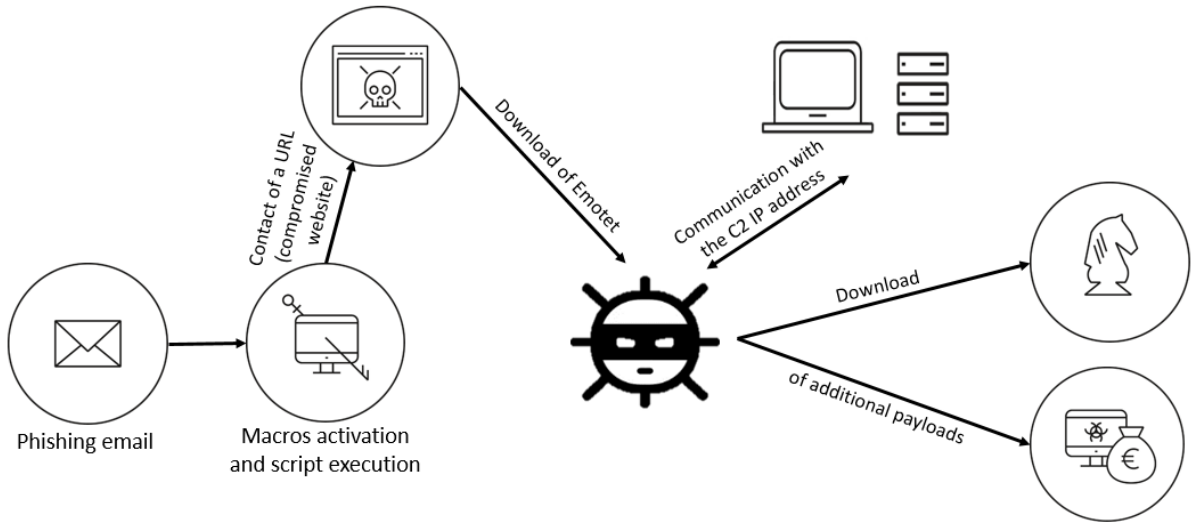

Fig. 2.2: Infection chain

[2] Three different versions of Emotet are in circulation.
[3] Malicious interface allowing remote access to a Web server.
[4] Two different versions of Emotet will not use the same URLs or C2s.

3 Links with other groups of attackers

Checkpoint believes that the price of the Emotet distribution service is around $2,000 [13]. According to Symantec, TA542 may be able to claim a share of the profits made by its customers during their attacks [8].

3.1 Customers

Past customer base

Over the 2017-2018 period, Emotet have mainly distributed IcedID, Nymaim and Gootkit, as well as UmbreCrypt et MegaCortex ransomwares (see chapter 6).

Gaining clients of Necurs botnet

From 2016 to 2019, Necurs botnet appeared to have been the most widespread method for delivering spam and malwares on behalf of cybercriminals. The botnet have been responsible for 90% of malwares distributed by email around the world. It have evolved from 1 million infected devices in 2016 to 9 million as of March 10, 2020 [25]. The move towards more targeted attacks may have led attackers groups who were Necurs customers to turn to another competing distribution service, Emotet. This is for example the case of Dridex, TrickBot and IcedID operators [26]. Necurs then only distributed unsophisticated spam campaigns until it was dismantled.

Current customer base

Dridex and DoppelDridex

The cybercriminal group Evil Corp have apparently used the services of Emotet between April 2017 and March 2020 to distribute Dridex, wich in turn delivered BitPaymer [27, 28]. Since March 2020, Evil Corp no longer uses BitPaymer or Dridex and introduced the WastedLocker ransomware [29, 30, 31] delivered through the FakeUpdates framework (aka SocGholish)[5] another cybercriminal service.

Commentaire : The collaboration between TA542 and Evil Corp could legitimately continue into the future. It is therefore plausible that WastedLocker ransomware is distributed by Emotet.

In addition, since April 2019, the Doppel Spider group operates a modified version of Dridex, DoppelDridex, as well as a variant of BitPaymer ransomware, DoppelPaymer. The group is believed to use Emotet services too [33].

TrickBot

TrickBot (aka TheTrick) is a banking trojan that appeared in 2016, taking over from the Dyre malware. It is said to be operated by the cybercriminal group Wizard Spider and used by a limited number of other attackers groups. Although TrickBot affiliates are not clearly identifiable, campaigns involving TrickBot are differentiated by their infection vector and a hard-coded parameter: the Group Tag (aka Gtag) [34].

Gtags starting with « more » and ending with a number (mor 84 [15] or mor114 [35] for example) is, according to Intel471, exclusively distributed by Emotet in 2020[6] [36]. Appeared in September 2019, it is this same family of Gtag that in 2020 deployed the Ryuk ransomware after an initial infection by Emotet.

Commentaire : Nevertheless, Ryuk being active since at least August 2018, and already distributed as the final payload of the Emotet-TrickBot infection chain, other Gtags than morXXX may be associated with attacks by Ryuk. However these

[5] This framework works in conjunction with watering hole : a victim visits a legitimate compromised website, a fake browser update leads to the installation of the malicious Javascript file FakeUpdates. FakeUpdates then delivers a malware operated by its customers on a case-by-case basis, including Dridex, DoppelDridex, Chtonic, AZORult and NetSupport RAT [32].

[6] However, it is possible that other Gtags correspond to Emotet since in 2018, Trend Micro has identified the Gtags del72, del77, arz1, jim316 and lib316 to be distributed by Emotet [6].

attacks perpetuated more than two years ago, may have been conducted by a single group of attackers who would have seen their gtag evolve, or several different groups.

The Conti ransomware, which appeared in June 2020 [37], is also distributed by the Emotet-TrickBot chain since July 2020 [19].

QakBot

Appeared in 2009, QakBot (aka Qbot, Pinkslipbot) is a modular trojan. It can also be used to distribute secondary payloads. The ProLock ransomware (aka PwndLocker) is the main payload it distributes in 2020 [38, 39].

QakBot is itself distributed by Emotet since 2017. It also appears to be the most distributed payload by Emotet since August 2020 [40, 41].

Although no such incidents have been reported to ANSSI, one of its partners has confirmed the existence of the Emotet – QakBot – ProLock infection chain. The risk associated with this infection chain is significant as QakBot is currently targeting the country through two parallel campaigns :

- a phishing campaign delivering Emotet and QakBot (although not exclusively) as a second payload ;
- a phishing campaign delivering QakBot directly, without the existence of a second payload having yet been identified.

SilentNight

SilentNight is a trojan sold on Russian speaking underground forums since the end of 2019. It is a variant of the malware Zloader (which ca from the source code of ZeuS) whose last activity dates back to 2018 [42].

SilentNight, non-exclusive to a group of attackers, has been distributed as a second payload by Emotet since 2020 [43, 44, 45].

SilentNight users include TA511 (aka Hancitor gang, Chanitor, MAN1, Moskalvzappe) [46]. The group of attackers distributed Zloader until November 2017, then Panda Banker[7] until its shutdown in October 2018 [6, 12], and finally SilentNight in 2020.

Comment : Given that Panda Banker [47] and SilentNight were both delivered by Emotet, it is legitimate to wonder, given the relatively small circle of TA542 customers and the longevity of their relationship with this group, whether the group of attackers currently using Emotet's distribution service to deploy SilentNight is not the same one that was using it in 2018 to deploy Panda Banker. If this is the case, then this group could possibly be TA511.

AZORult

Discovered in 2016, AZORult is an information stealer and a loader sold on Russian-speaking underground forums [48], distributed by Emotet since at least 2018.

[7] Panda Banker (aka ZeuS Panda) is a banking trojan active from 2016 to the end of 2018 and operating under an affiliated system. It was allegedly developed and operated by the cybercriminal group called Bamboo Spider by Crowdstrike.

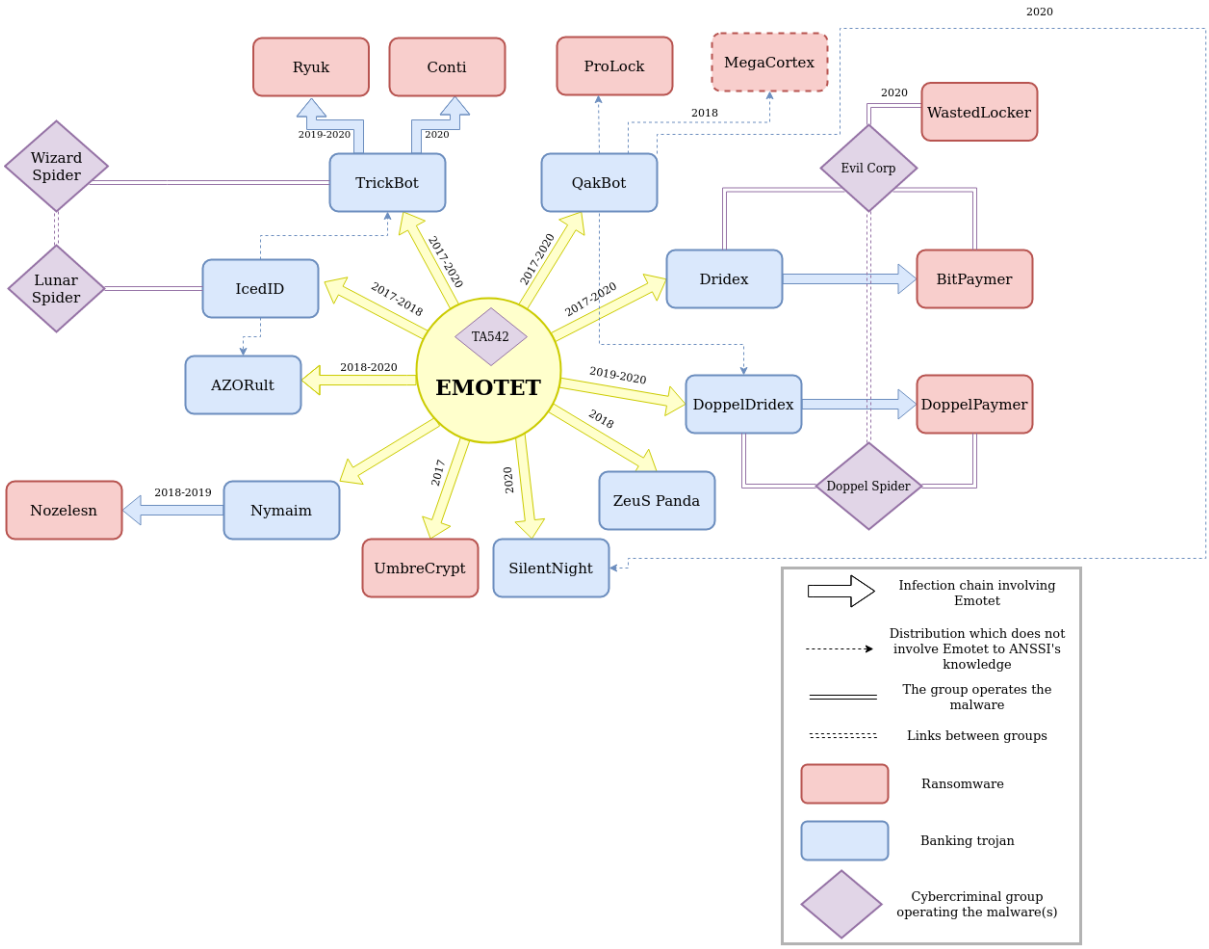

Fig. 3.1: Main TA542's customer base

3.2 Links between Emotet and Dridex, Gozi ISFB and QakBot operators

According to Trend Micro, the operators of Emotet, Gozi ISFB (aka Ursnif) and Dridex would share the same PE provider[8] loader[9], or even exchange resources [49].

In addition, the macro obfuscation method used by TA542 in its malicious attachments has also been observed during campaigns to distrbute Gozi ISFB. Trend Micro reportedly found this method used only by attackers distributing Emotet and Gozi ISFB [6].

Finally, QakBot and Emotet have at least three similarities :

- both codes would use the same packer[10] [8] ;
- the operators of QakBot have, just like those of Emotet, already used the thread hijacking technique, notable in 2020 [50].
- both codes are distributed by compromised Wordpress sites [51].

Commentaire : In view of these different elements, it is conceivable that the collaboration between the operators of Emotet and those of Gozi ISFB and QakBot goes beyond the only customer/provider interaction.

[8] Format of executables files and libraries on Windows operating systems, including .exe (for programs) and .dll (for libraries).
[9] The PE loader allows Windows to execute instructions from a PE file.
[10] A tool used to hide a file by encrypting, compressing or changing the format.

4 Conclusion

Emotet is a malware at the origin of many campaigns since its beginning in 2014. Current attack campaigns do not appear to be sectorally targeted, although geographic targeting can sometimes be identified. Thus, Emotet tends to compromise entities in the United States (58% of infections), the United Kingdom (12%) and Canada (8%), and to a lesser extent in Mexico and Germany [14], although countries such as France, Italy, Japan, New Zealand and the Netherlands may also be more punctually affected as evidenced by the various alerts published by the CERTs of these countries in September 2020 [52], and the alerts processed by ANSSI.

These campaigns most often aim to distribute a second payload following Emotet. The same campaign can distribute different payloads depending on the victim, such as ransomware, banking trojan or information stealer.

5 Means of detection and monitoring

Several feeds exist containing updated indicators of compromise related to Emotet, this code being the subject of numerous investigations in the public and private sectors. Among these feeds, https://paster.cryptolaemus.com/ and https://feodotracker.abuse.ch/browse represent reliable sources that it is recommended to integrate into its detection and blocking means.

The HaveIBeenEmotet tool offers a partial view of Emotet's action, indicating above all the entities targeted by the attacker and not those actually compromised, and therefore does not provide a reliable confirmation of the absence of compromise.

6 Appendix : TA542's customer base over the period 2017-2018

Over the period 2017-2018, TA542 distributed the following malwares :

- IcedID : operated by the cybercriminal group Lunar Spider, IcedID (aka BokBot) operates on an affiliate model, one of whose customers would be the operating group or an affiliate group of TrickBot. In termes of industry sectors, IcedID campaigns would primarily target U.S. bank customers as well as the eCommerce, media and telecommunication sectors, particularly in the United States. In June 2017, TA542 was the first cybercrime group to distribute IcedID [6].
- Gootkit : discovered in 2014, the informations stealer Gootkit is behing small-scale operations targeting bank customers [53].
- Nymaim : appeared in 2013, Nymaim is a malware distributed by Emotet in 2018. An Emotet-Nymaim infection chain could sometimes lead to the distribution of a final ransomware-like payload as evidenced by the use of the Nozelesn ransomware against the hospitality sector in February 2019 [54] and during a campaign targeting Poland in July 2018 [55].
- UmbreCrypt and MegaCortex : these ransomware were distributed a few times by Emotet respectively in 2017 and 2019 [56, 8].

7 Bibliography

[1] DHS CERT-US. *Avalanche (Crimeware-as-a-Service Infrastructure)*. Dec. 1, 2016. URL: https://www.us-cert.gov/ncas/alerts/TA16-336A.

[2] Dell Secureworks. *Evolution of the GOLD EVERGREEN Threat Group*. May 15, 2017. URL: https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

[3] Institut Pandore. *On décortique Zeus, le malware le plus hardcore jamais découvert*. Jan. 23, 2020. URL: https://www.institut-pandore.com/hacking/analyse-malware-zeus/.

[4] Assiste. *Botnet Dridex*. Apr. 9, 2020. URL: https://assiste.com/Botnet_Dridex.html.

[5] Security Intelligence. *New Variant of Bugat Malware Uses Lucrative Gameover Zeus Techniques*. Aug. 14, 2014. URL: https://securityintelligence.com/new-variant-of-bugat-malware-borrows-lucrative-gameover-zeus-techniques/.

[6] Trend Micro. *Exploring Emotet's Activities*. Jan. 1, 2018. URL: https://documents.trendmicro.com/assets/white_papers/ExploringEmotetsActivities_Final.pdf.

[7] Malwarebytes. *APTs and COVID-19: How Advanced Persistent Threats Use the Coronavirus as a Lure*. Apr. 2020.

[8] Symantec. *The Evolution of Emotet: From Banking Trojan to Threat Distributor*. July 18, 2018. URL: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor.

[9] CIS. *Emotet Changes TTPs and Arrives in United States*. Apr. 28, 2017. URL: https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/.

[10] Kaspersky. *The Banking Trojan Emotet: Detailed Analysis*. Apr. 9, 2015. URL: https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/.

[11] Malpedia. *Mummy Spider*. URL: https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider.

[12] Bromium. *EMOTET: A TECHNICAL ANALYSIS OF THE DESTRUCTIVE, POLYMORPHIC MALWARE*.

[13] Checkpoint. *Emotet: The Tricky Trojan That 'Git Clones'*. July 24, 2018. URL: https://research.checkpoint.com/2018/emotet-tricky-trojan-git-clones/.

[14] Trend Micro. *EMOTET Returns, Starts Spreading via Spam Botnet*. Sept. 10, 2020. URL: https://www.trendmicro.com/en_us/research/17/i/emotet-returns-starts-spreading-via-spam-botnet.html.

[15] SANS Internet Storm Center. *Emotet Epoch 1 Infection with Trickbot Gtag Mor84*. Jan. 28, 2020. URL: https://isc.sans.edu/forums/diary/25752/.

[16] Dell Secureworks. *GOLD CRESTWOOD*. Sept. 9, 2020. URL: https://www.secureworks.com/research/threat-profiles/gold-crestwood.

[17] Cofense. *Into a Dark Realm: The Shifting Ways of Geodo Malware*. Aug. 27, 2018. URL: https://cofense.com/dark-realm-shifting-ways-geodo-malware/.

[18] Bleeping Computer. *Emotet-TrickBot Malware Duo Is Back Infecting Windows Machines*. July 20, 2020. URL: https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/.

[19] Cyware. *Emotet-TrickBot Duo Is Back With More Tricks*. July 27, 2020. URL: https://cyware.com/news/emotet-trickbot-duo-is-back-with-more-tricks-e81a4386.

[20] Security Intelligence. *Emotet Activity Rises as It Uses Coronavirus Scare to Infect Targets in Japan*. Feb. 5, 2020. URL: https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/.

[21] Security Intelligence. *Sextortion Scams Delivered by Emotet Net 10 Times More Than Necurs Sextortion — Here's Why*. Feb. 13, 2020. URL: https://securityintelligence.com/posts/sextortion-scams-delivered-by-emotet-net-10-times-more-than-necurs-sextortion-heres-why/.

[22] Security Intelligence. *Emotet SMiShing Uses Fake Bank Domains in Targeted Attacks, Payloads Hint at TrickBot Connection*. Feb. 19, 2020. URL: https://securityintelligence.com/posts/emotet-smishing-uses-fake-bank-domains-in-targeted-attacks-payloads-hint-at-trickbot-connection/.

[23] F-Secure Blog. *Hunting for Emotet*. Dec. 22, 2017. URL: https://blog.f-secure.com/hunting-for-emotet/.

[24] ZDNet. *A Vigilante Is Sabotaging the Emotet Botnet by Replacing Malware Payloads with GIFs*. Sept. 8, 2020. URL: https://www.zdnet.com/article/a-vigilante-is-sabotaging-the-emotet-botnet-by-replacing-malware-payloads-with-gifs/.

[25] The Shadowserver foundation. *Has The Sun Set On The Necurs Botnet?* Mar. 15, 2020. URL: https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/.

[26] ThreatPost. *As Necurs Botnet Falls from Grace, Emotet Rises*. Jan. 29, 2020. URL: https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/.

[27] Proofpoint. *Threat Actor Profile: TA542, From Banker to Malware Distribution Service*. May 15, 2019. URL: https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service.

[28] Naked Security. *Emotet's Goal: Drop Dridex Malware on as Many Endpoints as Possible*. Aug. 10, 2017. URL: https://nakedsecurity.sophos.com/2017/08/10/watch-out-for-emotet-the-trojan-thats-nearly-a-worm/.

[29] Malwarebytes Labs. *WastedLocker, Customized Ransomware*. July 10, 2020. URL: https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/.

[30] Cisco Talos. *WastedLocker Goes "Big-Game Hunting" in 2020*. July 6, 2020. URL: http://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html.

[31] NCC Group. *WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group*. June 23, 2020. URL: https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/.

[32] ANSSI. *Le Code Malveillant Dridex : Origines et Usages*. May 28, 2020.

[33] Crowdstrike. *CrowdStrike Discovers New DoppelPaymer Ransomware & Dridex Variant*. July 12, 2019. URL: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/.

[34] SANS Internet Storm Center. *InfoSec Handlers Diary Blog - Trickbot*. Dec. 11, 2019. URL: https://isc.sans.edu/diary.html?storyid=25594.

[35] Twitter. *@cryptolaemus1*. Aug. 26, 2020. URL: https://twitter.com/GossiTheDog/status/1298486442159677440.

[36] Intel 471. *Understanding the Relationship between Emotet, Ryuk and TrickBot*. Apr. 14, 2020. URL: https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/.

[37] Bleeping Computer. *Conti Ransomware Shows Signs of Being Ryuk's Successor*. July 9, 2020. URL: https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/.

[38] HOTforSecurity. *FBI Warns That ProLock Ransomware Decryptor Corrupts Encrypted Files*. May 19, 2020. URL: https://hotforsecurity.bitdefender.com/blog/fbi-warns-that-prolock-ransomware-decryptor-corrupts-encrypted-files-23295.html.

[39] Hornetsecurity. *QakBot Malspam Leading to ProLock: Nothing Personal Just Business*. June 16, 2020. URL: https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/.

[40] Cyware. *TA542 Fortifies Emotet's Attack Tactics*. Sept. 2, 2020. URL: https://cyware.com/news/ta542-fortifies-emotets-attack-tactics-5a8c2c2c.

[41] Dark Reading. *TA542 Returns With Emotet: What's Different Now*. Aug. 28, 2020. URL: https://www.darkreading.com/threat-intelligence/ta542-returns-with-emotet-whats-different-now/d/d-id/1338785.

[42] Infosec Institute. *ZLoader: What It Is, How It Works and How to Prevent It*. Aug. 19, 2020. URL: https://resources.infosecinstitute.com/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/.

[43] Crowdstrike. *Duck Hunting w/Falcon Complete Pt. 2: QakBot ZIP-Based Campaign*. Oct. 7, 2020. URL: https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/.

[44] Twitter. *@Cryptolaemus1*. Sept. 18, 2020. URL: https://twitter.com/Cryptolaemus1/status/1306850671531044865.

[45] Twitter. *@peterkruse*. Sept. 21, 2020. URL: https://twitter.com/peterkruse/status/1307914831522131969.

[46] Proofpoint. *ZLoader Loads Again: New ZLoader Variant Returns*. May 20, 2020. URL: https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns.

[47] Charlie Osborne. *Panda Banker Trojan Becomes Part of Emotet Threat Distribution Platform*. Oct. 9, 2018. URL: https://www.zdnet.com/article/panda-trojan-becomes-part-of-emotet-threat-distribution-platform/.

[48] Trend Micro. *Azorult Malware*. Dec. 20, 2019. URL: https://success.trendmicro.com/solution/000146108-azorult-malware-information-kAJ4P000000kEK2WAM.

[49] Trend Micro. *URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader*. Dec. 18, 2018. URL: https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/.

[50] Kroll. *QakBot Malware Exfiltrating Emails for Thread Hijacking Attacks*. June 4, 2020. URL: https://www.kroll.com/en-ca/insights/publications/cyber/qakbot-malware-exfiltrating-emails-thread-hijacking-attacks.

[51] Zvelo. *Wordpress Sites Targeted to Serve Malware*. July 13, 2020. URL: https://zvelo.com/wordpress-sites-targeted-to-serve-qakbot-malware/.

[52] ZDNet. *Microsoft, Italy, and the Netherlands Warn of Increased Emotet Activity*. Sept. 23, 2020.

[53] Malware Traffic Analysis. *Malware-Traffic-Analysis.Net - 2019-01-14 - Emotet Infection with Qakbot*. Jan. 14, 2019. URL: https://www.malware-traffic-analysis.net/2019/01/14/index.html.

[54] Trend Micro. *Nozelesn and Emotet-Distributed Ransomware Loader*. Mar. 29, 2019. URL: https://www.trendmicro.com/en_us/research/19/c/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response.html.

[55] Proofpoint. *Nymaim Config Decoded*. Mar. 12, 2019. URL: https://www.proofpoint.com/us/threat-insight/post/nymaim-config-decoded.

[56] SOC Prime. *MegaCortex Ransomware Makes the Next Step to Mass Attacks*. Aug. 6, 2019. URL: https://socprime.com/en/news/megacortex-ransomware-makes-the-next-step-to-mass-attacks/.

- 12/02/2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN