TLP:WHITE

# LE MALWARE-AS-A-SERVICE EMOTET

29/10/2020


TLP:WHITE

# Sommaire

# 1 Origines d'Emotet

Emotet (alias Heodo), apparu en mars 2017, est la quatrième itération du code malveillant Geodo.

L'origine de Geodo remonte au Business Club, un groupe cybercriminel dont l'activité a commencé aux alentours de 2008, en collaboration avec M. Bogatchev, le créateur du code malveillant ZeuS [1]. Ce groupe a opéré successivement les codes malveillants JabberZeuS et GameOverZeuS (GoZ) [2, 3].

En parallèle des activités du Business Club, l'un de ses membres, M. Yakubets, ainsi que l'un des opérateurs de son prestataire d'hébergement *bulletproof*[1], A. Ghinkul, auraient opéré, voire développé, le code malveillant Bugat (alias Cridex, Feodo), apparu en 2010.

Un mois après le démantèlement de l'infrastructure de GoZ par le FBI en mai 2014, émergent les chevaux de Troie bancaires Dridex et Geodo, opérés par des reliquats du Business Club, respectivement Evil Corp et TA542 :

- Dridex, opéré par Evil Corp, dont M. Yakubets et A. Ghinkul font partie, est la cinquième itération du code malveillant Bugat, agrémentée de particularités propres à GoZ [4, 5];
- Geodo, opéré par le groupe TA542 (alias Mummy Spider, MealyBug ou encore GoldCrestwood), n'aurait pas de similarités de codes avec Bugat mais son infrastructure réseau serait héritée de celle de la version 4 de Bugat [6].

  *Commentaire : Par souci de simplicité, Emotet désignera par la suite toutes les versions de Geodo, de 2014 à 2020.*

Bien que les connaissances à son sujet soient très limitées par rapport à celles relatives à Evil Corp, TA542 semblerait être un groupe cybercriminel d'origine russophone [7]. D'après Trend Micro, il opérerait depuis le fuseau horaire UTC+10, qui inclut notamment la région de Vladivostok en Russie [6].

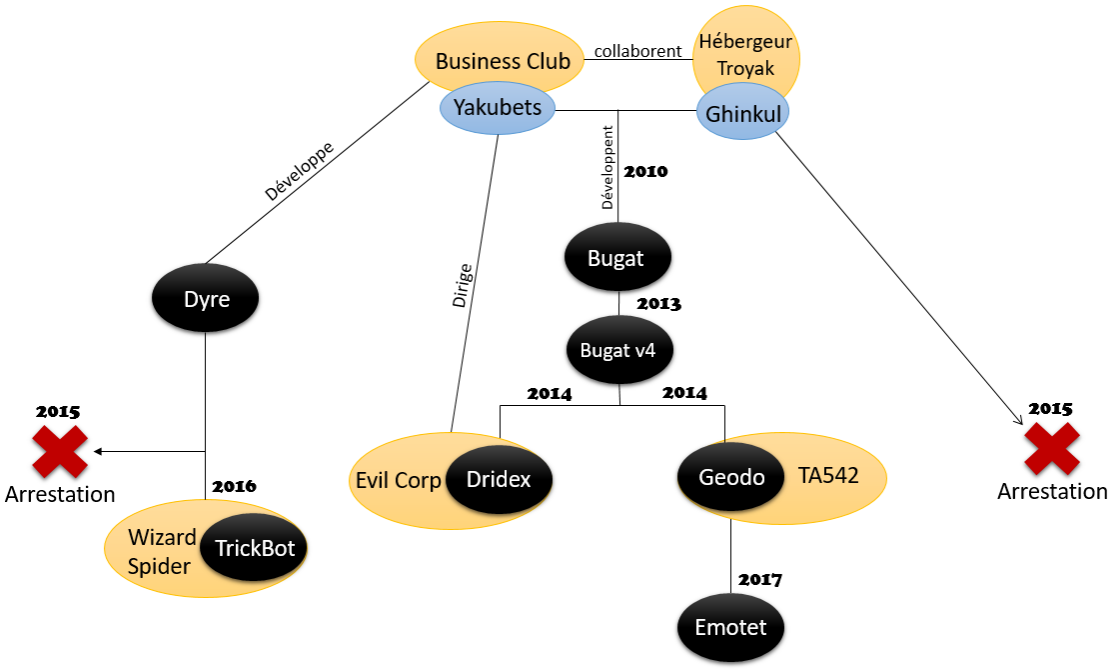


Fig. 1.1 : Origines d'Emotet

[1] Sur le marché noir, des opérateurs peu scrupuleux proposent de louer des serveurs dans des juridictions hors d'atteinte des traités de coopération judiciaire. Ces serveurs s'appellent des *bulletproof*. Le prestataire d'hébergement *bulletproof* utilisé par le Business Club, dénommé Troyak, a été démantelé en 2010 [2].

# 2 Évolution de l'activité d'Emotet

## 2.1 De cheval de Troie bancaire à loader de codes malveillants pour le compte d'autres attaquants

Observé pour la première fois en 2014 en tant que cheval de Troie bancaire, les trois premières versions d'Emotet se sont limitées à cibler les clients de banques notamment allemandes, autrichiennes et suisses [8, 9]. Ces attaques avaient pour objectif d'effectuer des virements frauduleux automatiques depuis les comptes en banque compromis de particuliers dont les codes d'accès de banque en ligne avaient été exfiltrés au moyen d'Emotet [10].

*Commentaire : Il est possible que ces transferts d'argent n'aient pas été réalisés que pour le compte de TA542, mais également pour le compte de clients. En effet, TA542 aurait fait la promotion d'Emotet sur des forums souterrains jusqu'en 2015, date à laquelle les services d'Emotet devinrent privés, au profit exclusif de TA542 et possiblement d'un cercle restreint de clients [11].*

A partir de 2015, Emotet a évolué pour devenir un cheval de Troie modulaire. Ses différents modules actuels lui permettent :

- de récupérer les mots de passe stockés sur un système ainsi que sur plusieurs navigateurs (Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera) et boîtes courriel (Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail et Gmail) ;
- de dérober la liste de contacts, le contenu et les pièces jointes attachées à des courriels ;
- de se propager au sein du réseau infecté en tirant parti de vulnérabilités SMB ainsi que des mots de passe récupérés.

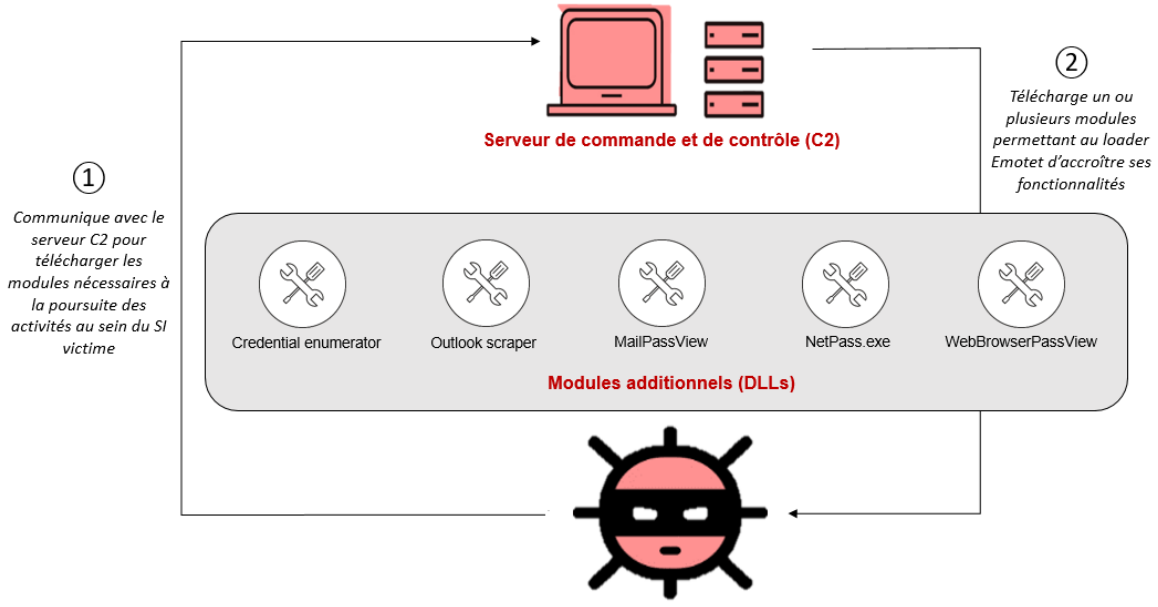


Fig. 2.1 : Modularité d'Emotet

Parmi ces modules, MailPassView et WebBrowserPassView sont des outils légitimes détournés par TA542 [6, 12, 13].

Depuis 2017, Emotet n'est plus utilisé en tant que cheval de Troie bancaire (dont le module correspondant a été retiré [13]) mais distribue des codes malveillants opérés par des groupes d'attaquants clients de TA542 au sein des systèmes d'information (SI) qu'il infecte [12].

## 2.2 Chaîne d'infection associée à Emotet

### 2.2.1 Vecteurs possibles d'infection

**T1566 - Courriels d'hameçonnage**

Emotet est généralement distribué par courriel d'hameçonnage, *via* les botnets opérés par TA542 [14]. Il existe trois botnets Emotet indépendants, dénommés Epoch 1, Epoch 2 et Epoch 3. Chacun d'eux dispose de sa propre infrastructure [15]. Ces botnets sont inactifs de manière simultanée plusieurs fois par an [16]. Par exemple, Emotet a été inactif de février à juillet 2020.

En 2018, environ 98% des courriels de campagnes Emotet contenait une URL conduisant au téléchargement d'un document Office piégé. De plus, environ 66% usurpait l'image d'une entité existante, du type DHL, PayPal ou encore UPS [17].

Depuis 2019, les courriels d'hameçonnage contiennent plus majoritairement une pièce jointe malveillante du type Word, PDF ou encore ZIP, bien que des courriels contenant des URL existent toujours.

Par ailleurs, depuis 2018 le groupe tend à sophistiquer davantage ses attaques. En effet, TA542 a la capacité de détourner des fils de discussion de courriels (*email thread hijacking technique*). Une fois la boîte courriel d'un employé de l'entité victime (ou la boîte courriel générique de l'entité elle-même) compromise, Emotet exfiltre le contenu de certains de ses courriels. Sur la base de ces derniers, les attaquants construisent des courriels d'hameçonnage prenant la forme d'une réponse à une chaîne de courriels échangés entre l'employé et des partenaires de l'entité pour laquelle il travaille. L'objet légitime du courriel d'hameçonnage est alors précédé d'un ou plusieurs "Re :", et le courriel lui-même contient l'historique d'une discussion, voire même des pièces jointes légitimes. Ces courriels sont envoyés à des contacts de la victime, et plus particulièrement aux tierces parties de l'entité (clients et prestataires notamment) ayant participé au fil de discussion originel, afin d'accroître leur crédibilité auprès des destinataires.

*Commentaire : A partir d'août 2020, la France (secteurs privé et public) a été la cible de campagnes d'hameçonnage Emotet exploitant la technique de détournement des fils de discussion des courriels.*

Outre cette technique, en 2020, TA542 :

- construit également des courriels d'hameçonnage sur la base d'informations récupérées lors de la compromission de boîtes courriel, qu'il envoie aux listes de contact exfiltrées ;
- usurpe l'image d'entités, victimes préalables d'Emotet ou non (sociétés de transport, de télécommunication, institutions financières, etc.). Ces courriels peuvent contenir de fausses factures, de fausses informations de livraison ou encore de fausses opportunités d'emploi. Une telle campagne datant de juillet 2020 a distribué la chaîne d'infection Emotet-TrickBot-Ryuk/Conti [18] ;
- exploite le thème du Coronavirus en guise de leurre [19, 20]. Par exemple, en mars 2020, une campagne Emotet de ce type a touché le Japon à des fins de distribution de TrickBot en tant que seconde charge utile ;
- cible des adresses courriel professionnelles avec des spams de "sextorsion" visant à soutirer de l'argent aux employés destinataires mais également à distribuer Emotet au sein du SI de leur entreprise [21].

Ces courriels sont le plus souvent envoyés depuis l'infrastructure des attaquants sur la base d'adresses courriel expéditrices souvent typosquattées, même si des éditeurs indiquent qu'il est possible qu'ils soient envoyés depuis des boîtes courriel compromises [6].

**T1189 - Point d'eau**
**T1566.002 - Hameçonnage contenant des liens piégés**

Plus rarement, Emotet peut également être distribué par le kit d'exploitation RIG, *via* des sites Internet compromis [13], mais également par SMS. En effet, en février 2020, des SMS ont été envoyés depuis des numéros de téléphone américains, usurpant l'identité de banques et alertant les destinataires de la clôture de leur compte bancaire. En cliquant sur le lien contenu dans le SMS, les destinataires étaient redirigés vers une page Internet imitant celle de

la banque en question, et distribuant Emotet [19, 22].

*Commentaire : Les campagnes de "sextorsion" ainsi que celles par SMS suggèrent que TA542 diversifie ses sources de revenus et méthodes de compromission, à moins que le groupe ne se soit ouvert, de manière ponctuelle, à une clientèle moins sophistiquée qu'à l'accoutumée.*

### 2.2.2 Déroulement d'une attaque post réception d'un courriel d'hameçonnage

Une fois les macro activées par la victime, un script est exécuté, contactant une URL pour télécharger une charge Emotet[2], avant de l'exécuter [6]. Les URLs de téléchargement d'Emotet correspondent à des sites Internet (généralement Wordpress) compromis. Certains sites pourraient également avoir été créés par les attaquants eux-mêmes, comme cela était le cas en 2017 [23]. Elles changent très rapidement, plusieurs dizaines de nouvelles URL apparaissant chaque jour.

En juillet 2020, il a été constaté que sur les sites Wordpress compromis, TA542 utilisait un webshell[3] disponible sur Github associé au même mot de passe. Un *white hat* a découvert le mot de passe commun et a ainsi réussi à remplacer les charges utiles Emotet de certains des sites Wordpress compromis par TA542 par des GIFs. Ainsi, pendant plusieurs jours, un quart des URLs utilisées par TA542 distribuaient des GIFs inoffensifs [24].

Une fois installé, Emotet communique avec un serveur C2, en contactant directement l'adresse IP, et non un nom de domaine. Un échantillon Emotet contient souvent plusieurs adresses IP de C2 dans sa configuration [6] : si le premier C2 de la liste ne répond pas, le code malveillant tentera d'établir une communication avec l'adresse IP suivante, et ainsi de suite. Un ou deux C2 disparaît chaque jour, laissant place à un ou deux nouveaux. Environ 100 C2 sont actifs par version d'Emotet et trois versions sont actuellement en circulation, soit 300 C2 environ au total[4].

En 2018, la majorité des C2 en question était localisés aux Etats-Unis, au Mexique et au Canada. 3% d'entre eux étaient quant à eux localisés en France [6].

Le protocole utilisé par TA542 pour les communications entre Emotet et le C2 est Protobuf, un code *open source* développé par Google [13, 6].

Ces C2 permettent notamment à TA542 de télécharger des charges additionnelles pour le compte de groupes d'attaquants clients.

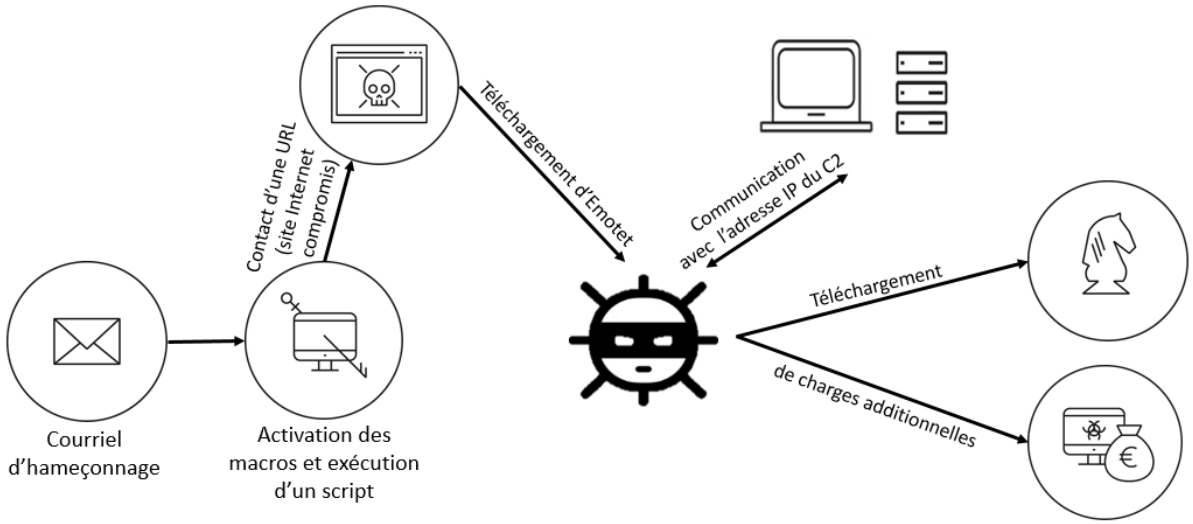


Fig. 2.2 : Chaîne d'infection

[2]Trois différentes versions d'Emotet sont en circulation.
[3]Interface malveillante permettant un accès à distance à un serveur Web.
[4]Deux versions différentes d'Emotet n'utiliseront pas les mêmes URL, ni les mêmes C2.

# 3 Liens avec d'autres groupes d'attaquants

L'éditeur Checkpoint estime que le prix de base du service de distribution Emotet avoisine les 2000 dollars [13]. D'après Symantec, TA542 pourrait s'attribuer une part des profits réalisés par ses clients au cours de leurs attaques [8].

## 3.1 Clientèle

### Clientèle passée

Sur la période 2017-2018, Emotet aurait principalement distribué les codes malveillants IcedID, Nymaim et Gootkit, ainsi que les rançongiciels UmbreCrypt et MegaCortex (voir chapitre 6).

### Récupération des clients du botnet Necurs

De 2016 à 2019, le botnet Necurs aurait été la méthode la plus répandue pour délivrer des spams et des codes malveillants pour le compte de cybercriminels. Le botnet aurait été à l'origine de 90% des codes malveillants distribués par courriel à travers le monde. Il serait passé de 1 million de systèmes infectés en 2016 à 9 millions en date du 10 mars 2020 [25]. L'évolution vers des attaques plus ciblées aurait conduit des groupes d'attaquants clients de Necurs à se tourner vers l'un des services de distribution concurrents, Emotet. C'est par exemple le cas des opérateurs de Dridex, TrickBot et d'IcedID [26]. Necurs n'a alors plus distribué que des campagnes de spams peu sophistiquées jusqu'à son démantèlement début 2020.

### Clientèle actuelle

Dridex et DoppelDridex

Le groupe cybercriminel Evil Corp aurait utilisé les services d'Emotet entre avril 2017 et mars 2020 pour distribuer Dridex, lui-même chargé de distribuer Bitpaymer [27, 28]. Depuis mars 2020, Evil Corp n'utilise plus Bitpaymer, ni Dridex pour son compte et a introduit le rançongiciel WastedLocker [29, 30, 31] distribué au travers du framework FakeUpdates (alias SocGholish)[5] un autre service cybercriminel.

*Commentaire : La collaboration de TA542 et d'Evil Corp pourrait légitimement se perpétuer dans le futur. Il est donc envisageable que le rançongiciel WastedLocker puisse être distribué par Emotet.*

De plus, depuis avril 2019,le groupe d'attaquants Doppel Spider opère une version modifiée de Dridex, DoppelDridex, ainsi qu'une variante du rançongiciel BitPaymer, DoppelPaymer. Le groupe utiliserait lui aussi les services d'Emotet [33].

TrickBot

TrickBot (alias TheTrick) est un cheval de Troie apparu en 2016, prenant la suite du code malveillant Dyre. Il serait opéré par le groupe cybercriminel Wizard Spider et utilisé par un nombre restreint d'autres groupes d'attaquants. Bien que les affiliés de TrickBot ne soient pas clairement identifiables, les campagnes impliquant TrickBot se différencient par leur vecteur d'infection et un paramètre codé en dur : le *Group Tag* (alias Gtag) [34].

Le Gtag dont la racine est "mor" et le suffixe est un nombre (mor 84 [15] ou mor114 [35] par exemple) serait, d'après Intel471, exclusivement distribué par Emotet en 2020[6] [36]. Apparu en septembre 2019, c'est cette même famille de Gtag qui déploie en 2020 le rançongiciel Ryuk après primo-infection par Emotet.

[5] Ce framework fonctionne par point d'eau : une fois une site Internet légitime compromis visité, une fausse mise à jour de navigateur apparait et conduit à l'installation du fichier Javascript malveillant FakeUpdates. FakeUpdates distribue ensuite au cas par cas les codes malveillants opérés par ses clients, dont Dridex, DoppelDridex, Chtonic, AZORult et NetSupport RAT [32].

[6] Cependant, il est possible que d'autres Gtags soient également distribués par Emotet étant donné qu'en 2018, Trend Micro a identifié les Gtags del72, del77, arz1, jim316 et lib316 être distribués par Emotet [6].

*Commentaire : Néanmoins, Ryuk étant actif depuis au moins août 2018, et déjà distribué en tant que charge finale de la chaîne d'infection Emotet-TrickBot, d'autres gtags que les morXXX ont participé à des attaques par le rançongiciel Ryuk sans qu'il ne puisse être identifié si ces attaques, perpétuées depuis maintenant plus de deux ans, sont le fait d'un unique groupe d'attaquants qui aurait vu son gtag évoluer, ou de plusieurs.*

Le rançongiciel Conti, apparu en juin 2020 [37], est également distribué par la chaîne Emotet-TrickBot depuis juillet 2020 [19].

QakBot

Apparu en 2009, QakBot (alias Qbot, Pinkslipbot) est un cheval de Troie modulaire. Il permet également de distribuer d'autres charges utiles. Le rançongiciel ProLock (alias PwndLocker) est la charge principale qu'il distribue en 2020 [38, 39].

QakBot est lui-même distribué par Emotet depuis 2017. Il apparaît d'ailleurs être la charge utile la plus distribuée par Emotet depuis août 2020 [40, 41].

Bien qu'aucun incident de ce type n'ait été signalé à l'ANSSI, l'un de ses partenaires a confirmé l'existence de la chaîne d'infection Emotet - QakBot - ProLock. Le risque que cette chaine d'infection aboutisse en France est d'autant plus prégnant que QakBot cible actuellement le pays au travers de deux campagnes parallèles :

- une campagne d'hameçonnage distribuant les codes malveillants Emotet puis QakBot (bien que non exclusivement) en tant que seconde charge utile ;
- une campagne d'hameçonnage distribuant directement QakBot, sans que l'existence d'une seconde charge utile n'ait encore pu être identifiée.

SilentNight

SilentNight est un cheval de Troie vendu sur des forums russophones souterrains depuis fin 2019. Il est une variante du code malveillante Zloader (issu du code source de ZeuS) dont la dernière activité remonte à 2018 [42].

SilentNight, non-exclusif à un groupe d'attaquants, est distribué en tant que seconde charge utile par Emotet depuis 2020 [43, 44, 45].

Parmi les utilisateurs de SilentNight, se trouve notamment TA511 (alias Hancitor gang, Chanitor, MAN1, Moskalvzappe) [46]. Le groupe d'attaquants a distribué Zloader jusqu'en novembre 2017, puis Panda Banker[7] jusqu'à son arrêt en octobre 2018 [6, 12], et enfin SilentNight en 2020.

*Commentaire : Etant donné que Panda Banker [47] et SilentNight ont tous deux été distribués par Emotet, il est légitime de se demander, au vu du cercle relativement restreint de clients de TA542 et de la longévité de leur relation avec ce groupe, si le groupe d'attaquants utilisant actuellement le service de distribution d'Emotet pour déployer SilentNight n'est pas le même qui l'utilisait en 2018 pour déployer Panda Banker. Si c'est le cas, ce groupe pourrait alors éventuellement être TA511.*

AZORult

Découvert en 2016, AZORult est un *information stealer* et un *loader* vendu sur les forums souterrains russophones [48], distribué par Emotet depuis au moins 2018.

[7] Panda Banker (alias ZeuS Panda) est un cheval de Troie bancaire opéré actif de 2016 à fin 2018 et fonctionnant selon un système d'affilié. Il aurait été développé et opéré par le groupe cybercriminel dénommé Bamboo Spider par Crowdstrike.

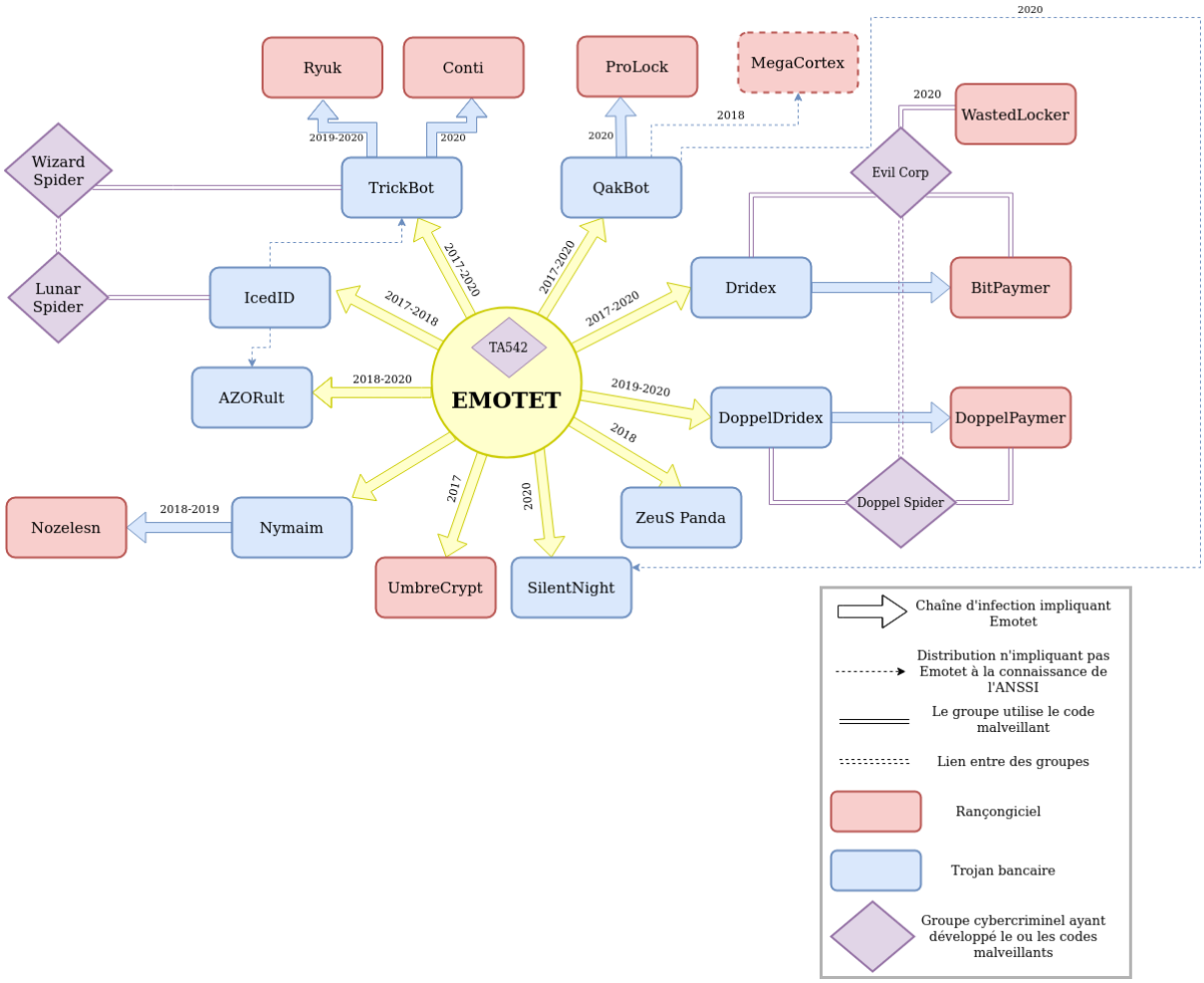


Fig. 3.1 : Clientèle principale de TA542

## 3.2 Liens entre Emotet et les opérateurs de Dridex, Gozi ISFB et QakBot

D'après Trend Micro, les opérateurs d'Emotet, de Gozi ISFB (alias Ursnif) et de Dridex partageraient le même fournisseur de PE[8] *loader*[9], voire échangeraient des ressources [49].

En outre, la méthode de dissimulation de macro utilisée par TA542 dans ses pièces jointes malveillantes a également été observée au cours de campagnes visant à distribuer Gozi ISFB. Trend Micro n'aurait constaté l'utilisation de cette méthode que par les attaquants distribuant Emotet et Gozi ISFB [6].

Enfin, QakBot et Emotet présentent au moins trois similitudes :

- les deux codes utiliseraient le même *packer*[10] [8] ;
- les opérateurs de QakBot ont, tout comme ceux d'Emotet, déjà utilisé la technique de détournement de fils de discussion, notamment en 2020 [50].
- les deux codes sont distribués par des sites Wordpress compromis [51].

*Commentaire : Au vu de ces différents éléments, il est envisageable que la collaboration entre les opérateurs d'Emotet et ceux de Gozi ISFB et de QakBot dépasse la seule intéraction client/prestataire.*

[8] Format des fichiers exécutables et des bibliothèques sur les systèmes d'exploitation Windows, incluant .exe (pour les programmes) et .dll (pour les bibliothèques).
[9] Le PE *loader* permet à Windows d'exécuter les instructions d'un fichier PE.
[10] Outil utilisé pour masquer un fichier en le chiffrant, le compressant ou en changeant le format.

# 4 Conclusion

Emotet est un code malveillant à l'origine de nombreuses campagnes depuis ses débuts en 2014. Les campagnes d'attaques actuelles ne semblent pas sectoriellement ciblées, bien qu'un ciblage géographique puisse parfois être identifié. Ainsi, Emotet a tendance à compromettre des entités aux Etats-Unis (58% des infections), au Royaume-Uni (12%) et au Canada (8%), ainsi que dans une moindre mesure au Mexique et en Allemagne [14], bien que des pays comme la France, l'Italie, le Japon, la Nouvelle-Zélande et les Pays-Bas puissent également être plus ponctuellement touchés comme en attestent les différentes alertes publiées par les CERT de ces pays en septembre 2020 [52], et les signalements traités par l'ANSSI.

Ces campagnes visent le plus souvent à distribuer une seconde charge utile à la suite d'Emotet. Une même campagne peut distribuer des charges utiles différentes en fonction de la victime, du type rançongiciel, cheval de Troie bancaire ou *information stealer*.

# 5 Moyens de détection et de suivi

Plusieurs flux existent contenant des indicateurs de compromission actualisés relatifs à Emotet, ce code faisant l'objet de nombreuses investigations dans les secteurs publics et privés. Parmi ces flux, https://paste.cryptolaemus.com/ et https://feodotracker.abuse.ch/browse/ représentent des sources fiables qu'il est recommandé d'intégrer dans ses moyens de détection et de blocage.

L'outil HaveIBeenEmotet offre quant à lui une vision partielle de l'action d'Emotet, indiquant avant tout les entités visées par l'attaquant et non celles effectivement compromises et ne permettant donc pas d'obtenir une confirmation fiable de l'absence de compromission.

# 6 Annexe : clientèle de TA542 sur la période 2017-2018

Sur la période 2017-2018, TA542 a distribué les codes malveillants suivants :

- IcedID : opéré par le groupe cybercriminel Lunar Spider, IcedID (alias BokBot) fonctionne sur un modèle d'affiliés, dont l'un des clients serait le groupe opérant ou un groupe affilié de TrickBot. En matière sectorielle, les campagnes IcedID cibleraient principalement les clients de banques américaines ainsi que les secteurs du eCommerce, des médias et des télécommunications, en particulier aux Etats-Unis. En juin 2017, TA542 a été le premier groupe cybercriminel à distribuer IcedID [6].
- Gootkit : découvert en 2014, l'*information stealer* Gootkit est à l'origine d'opérations de petite envergure ciblant des clients de banques [53].
- Nymaim : apparu en 2013, Nymaim est un code malveillant distribué par Emotet en 2018. Une chaîne d'infection Emotet-Nymaim pouvait parfois aboutir à la distribution d'une charge finale de type rançongiciel comme en atteste l'utilisation du rançongiciel Nozelesn à l'encontre du secteur hôtellier en février 2019 [54] ainsi qu'au cours d'une campagne ciblant la Pologne en juillet 2018 [55].
- UmbreCrypt et MegaCortex : ces rançongiciels ont été distribués à quelques reprises par Emotet respectivement en 2017 et 2019 [56, 8].

# 7 Bibliographie

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

[2] Dell Secureworks. *Evolution of the GOLD EVERGREEN Threat Group*. 15 mai 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*. 23 jan. 2020. URL : https://www.institut-pandore.com/hacking/analyse-malware-zeus/.

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

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

[6] Trend Micro. *Exploring Emotet's Activities*. 1er jan. 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*. Avr. 2020.

[8] Symantec. *The Evolution of Emotet : From Banking Trojan to Threat Distributor*. 18 juil. 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*. 28 avr. 2017. URL : https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/.

[10] Kaspersky. *The Banking Trojan Emotet : Detailed Analysis*. 9 avr. 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'*. 24 juil. 2018. URL : https://research.checkpoint.com/2018/emotet-tricky-trojan-git-clones/.

[14] Trend Micro. *EMOTET Returns, Starts Spreading via Spam Botnet*. 10 sept. 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*. 28 jan. 2020. URL : https://isc.sans.edu/forums/diary/25752/.

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

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

[18] Bleeping Computer. *Emotet-TrickBot Malware Duo Is Back Infecting Windows Machines*. 20 juil. 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*. 27 juil. 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*. 5 fév. 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*. 13 fév. 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*. 19 fév. 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*. 22 déc. 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*. 8 sept. 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 ?* 15 mar. 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*. 29 jan. 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*. 15 mai 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*. 10 août 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*. 10 juil. 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*. 6 juil. 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*. 23 juin 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*. 28 mai 2020.

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

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

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

[36] Intel 471. *Understanding the Relationship between Emotet, Ryuk and TrickBot*. 14 avr. 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*. 9 juil. 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*. 19 mai 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*. 16 juin 2020. URL : https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/.

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

[41] Dark Reading. *TA542 Returns With Emotet : What's Different Now*. 28 août 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*. 19 août 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*. 7 oct. 2020. URL : https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/.

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

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

[46] Proofpoint. *ZLoader Loads Again : New ZLoader Variant Returns*. 20 mai 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*. 9 oct. 2018. URL : https://www.zdnet.com/article/panda-trojan-becomes-part-of-emotet-threat-distribution-platform/.

[48] Trend Micro. *Azorult Malware*. 20 déc. 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*. 18 déc. 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*. 4 juin 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*. 13 juil. 2020. URL : https://zvelo.com/wordpress-sites-targeted-to-serve-qakbot-malware/.

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

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

[54] Trend Micro. *Nozelesn and Emotet-Distributed Ransomware Loader*. 29 mar. 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*. 12 mar. 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*. 6 août 2019. URL : https://socprime.com/en/news/megacortex-ransomware-makes-the-next-step-to-mass-attacks/.

- 29/10/2020


**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