TLP:WHITE

# LE CODE MALVEILLANT DRIDEX : ORIGINES ET USAGES

25/05/2020


TLP:WHITE

# Sommaire

# 1 Le code malveillant Dridex

## 1.1 Evolution des fonctionnalités depuis 2014

### 1.1.1 Fonctionnalités

Dridex, apparu en juin 2014, est la cinquième variante du code malveillant Bugat actif de 2010 à 2013 [1], agrémenté de particularités propres à GameOverZeuS (GoZ) [2], actif jusqu'en 2014.

Sa fonctionnalité première est celle d'un *stealer*, c'est-à-dire le vol de codes d'accès de banque en ligne[1], afin que les attaquants puissent réaliser des virements frauduleux depuis des comptes en banque compromis. A cette fin, Dridex dispose d'au moins trois méthodes [3] :

- Injection d'un script HTML sur des pages Internet légitimes de banques en ligne préalablement compromises, faisant apparaître des formulaires malveillants requérant au client de fournir ses codes d'accès ;
- Redirection vers une page malveillante usurpant la banque[2] ;
- Interception de la réponse du serveur depuis le site de la banque et relais vers le serveur PHP des attaquants, qui y injecte du code.

### 1.1.2 Modularité

Dridex est modulaire. Il est composé :

- D'un *loader*, chargé :
  - du téléchargement d'une liste de pairs[3] ;
  - de la reconnaissance initiale au sein du système d'information (SI) ;
  - de l'installation de la charge utile ;
  - du téléchargement des modules supplémentaires.
- D'une charge utile, aussi appelée *core module*, qui contient des fonctionnalités intégrées, auxquelles peuvent être ajoutées des modules, permettant l'extension de ses fonctionnalités.

Les principales fonctionnalités intégrées du *core module* de Dridex sont :

- Un *keylogger*, permettant de fournir aux attaquants du contexte sur la victime (captures d'écran, enregistrement de frappes, etc.) ;
- La collecte d'informations et modification de contenus de sites Internet (*Web injection*), via l'interaction avec les navigateurs Internet. D'après Bromium [4], Dridex disposerait d'au moins cinq techniques de *Web injection*[4].

Les principaux modules permettant d'étendre ces fonctionnalités sont :

- VNC : ce module fournit un support *Virtual Network Computing* (VNC)[5] pour un accès à distance de l'attaquant sur le poste de la victime ;
- SOCKS : il fournit à Dridex un support proxy SOCKS[6] ;

[1] Mais aussi de données personnelles et du solde des comptes.
[2] Technique préalablement utilisée par le code malveillant Dyre et qui lui a été probablement empruntée.
[3] Dans le cadre du fonctionnement en pseudo-réseau *peer-to-peer* de Dridex.
[4] *DLL order hijacking, process hollowing, PE injection, thread execution hijacking* et *AtomBombing*.
[5] Système de visualisation et de contrôle de l'environnement de bureau d'un ordinateur distant, utilisant le protocole RFB pour les communications.
[6] Le protocole réseau *Secured over credential based kerberos* (SOCKS) permet à une application d'utiliser les services d'un pare-feu dans le cadre d'un échange avec un serveur externe.

- Pony : basé sur le code malveillant Pony[7], il permet le vol de codes d'accès ;
- Kill OS : déployé sur des systèmes identifiés comme étant ceux de chercheurs ou de systèmes d'analyse automatique de codes malveillants, il efface le *master boot record* (MBR) du disque dur afin de saboter le poste infecté ;
- Spammer : il est utilisé pour envoyer des spams ;
- Email stealer : il est utilisé pour collecter les courriels de la victime.

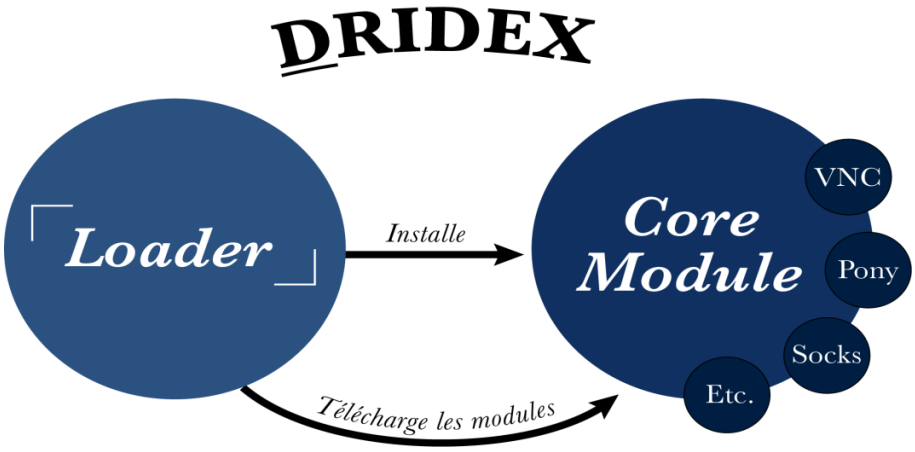


Fig. 1.1 : Composition générale

### 1.1.3 Développement

Dridex est en constant développement. Depuis 2014, ses développeurs y apportent des correctifs et des mises à jour régulières. Par exemple :

- En novembre 2014, Dridex adopte aussi bien l'usurpation de la signature numérique que le protocole P2P [6].
- Dridex est le premier code malveillant connu à mettre en oeuvre en février 2017 une nouvelle technique d'injection de code découverte en octobre 2016, AtomBombing [4].
- Les vecteurs d'attaque changent rapidement. Ainsi, le passage de la version 3 à la version 4 de Dridex début 2017 a été accompagné de l'ajout de la faille 0-day MS Word (CVE-2017-0199)[8] [4, 7].

## 1.2 Fonctionnement du botnet

Dridex utilise plusieurs botnets[9] Peer-to-Peer (P2P)[10] composés de postes qu'il compromet [9]. Leur architecture P2P est composée de trois couches (*layers*) hiérarchiques. Les machines finales de *command and control (C2 backend)* sont donc plus difficiles à identifier, rendant l'infrastructure plus résiliente.

Le *C2 backend*, autrement dit l'infrastructure racine, contient la base de données et la logique de gestion du botnet. Il est constitué d'environ 24 serveurs [10]. Il transmet de nouvelles mises à jour des modules Pony, Kill OS, Spammer

[7] Code malveillant et contrôleur de botnet actif depuis 2011, spécialisé dans le vol de codes d'accès et de crypto-actifs, mais également dans la distribution de codes malveillants, dont la version 1.9 a fuité fin 2012 [5]. Pony a distribué des codes malveillants tels que GoZ, Necurs, Dyre, Vawtrak, Cryptolock et Cribit. En 2013, il existait de nombreux botnets Pony.

[8] Faille permettant de dissimuler des instructions malveillantes dans un document sauvegardé au format .RTF.

[9] Pour une meilleure appréhension de la notion de botnet, un état de la menace relatif aux botnets est disponible sur le site du CERT-FR [8].

[10] Dans les botnets utilisant cette architecture, les machines zombies ne communiquent pas directement avec l'infrastructure C2, mais avec d'autres machines zombies définies dans une liste de pairs évolutive. Ainsi, seul un petit nombre de machines est en contact avec l'infrastructure C2 opérée directement par l'attaquant. Ces machines relaient ensuite les informations transmises par le C2 aux autres machines infectées présentes dans leur liste qui feront de même.

et Email Stealer aux *nodes*. Les *C2 frontends* (*admin node*), qui agissent comme des *reverse proxies*, constitués d'environ 15 serveurs [10], communiquent avec les *nodes*, qui seraient plusieurs centaines. Ces derniers sont constitués de systèmes infectés (bots), et représentent la première couche de communication à laquelle s'adresse le reste des systèmes infectés. Ils communiquent ensemble pour maintenir le réseau, l'agrandir, distribuer les modules VNC et SOCKS et transférer des requêtes aux *C2 frontends*.

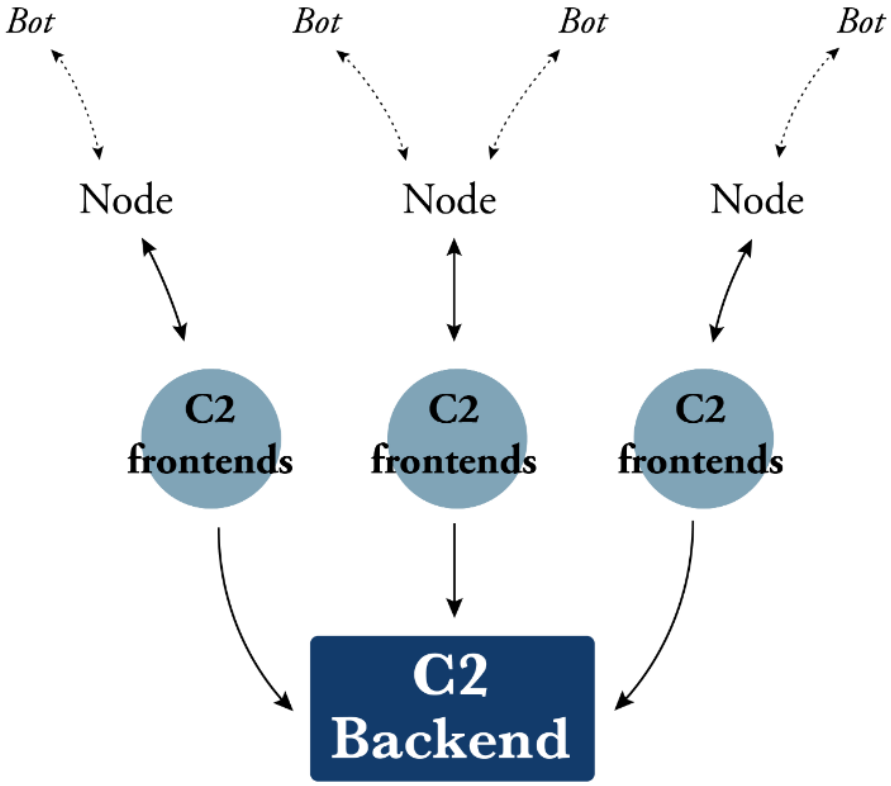


Fig. 1.2 : Fonctionnement du botnet Dridex

Chaque bot (*peer*) peut être identifié au sein du réseau P2P via deux IDs qu'il génère : le bot ID identifie l'utilisateur infecté sur un ordinateur et le computer ID identifie l'ordinateur. Les infections multiples sur un même ordinateur sont ainsi repérables. De plus, chaque bot maintient une liste des autres *peers*, c'est-à-dire d'adresses IP et de numéros de ports. Afin d'assurer que cette liste soit actualisée, les *peers* demandent régulièrement des mises à jour aux *nodes*.

Le taux d'infection maximal de Dridex est réputé avoir eu lieu sur la période 2015-2016. En 2015, les principaux pays victimes de Dridex étaient le Royaume-Uni, l'Italie et la France, qui comptait 1804 bots. Les Etats-Unis sont ensuite particulièrement ciblés [11].

## 1.3 Modèle d'affiliation

Alors que certains chevaux de Troie bancaires sont vendus seuls et propagés par les soins du client, Dridex fonctionne selon un modèle d'affiliés. Chaque affilié a accès à un sous-ensemble de bots [12], tandis que le groupe Evil Corp contrôle les *C2 backends* des différents botnets Dridex.

Selon l'acte d'accusation du Tribunal du district ouest de Pennsylvanie dressé à l'encontre de membres d'Evil Corp, les affiliés achèteraient l'usage de Dridex au groupe (par exemple pour 100000 dollars dans le cas d'une mule[11] britannique s'étant convertie en affilié), puis lui fourniraient la moitié des profits ainsi que 50000 dollars par semaine

[11] Individu qui transfère des fonds d'origine frauduleuse via différents comptes bancaires dans différents pays.

afin de continuer à jouir du droit de l'utiliser. En contrepartie, Evil Corp fournirait un support technique [10].

Les affiliés se distinguent par :

- leur botnet ID, autrement dit le numéro attribué à la version de Dridex associée au sous-ensemble de bots qu'ils gèrent. Ces botnet IDs permettent de différencier l'activité de chacun des affiliés, et d'associer différents botnets IDs à un même opérateur [13]. Par exemple, en 2015, Dridex disposait de neuf botnets appuyant sa propagation, dont les trois botnets les plus actifs 120[12], 200[13] et 220[14] ;
- leurs cibles, sectorielles et géographiques : par exemple, en 2015, le botnet ID 120 avait pour cible première les banques, les botnets 220, 120, 302, 125, 322, 225 et 228 en 2016 et le botnet 1011 en 2019 ciblaient notamment la France [9, 15] ;
- le vecteur d'infection choisi.

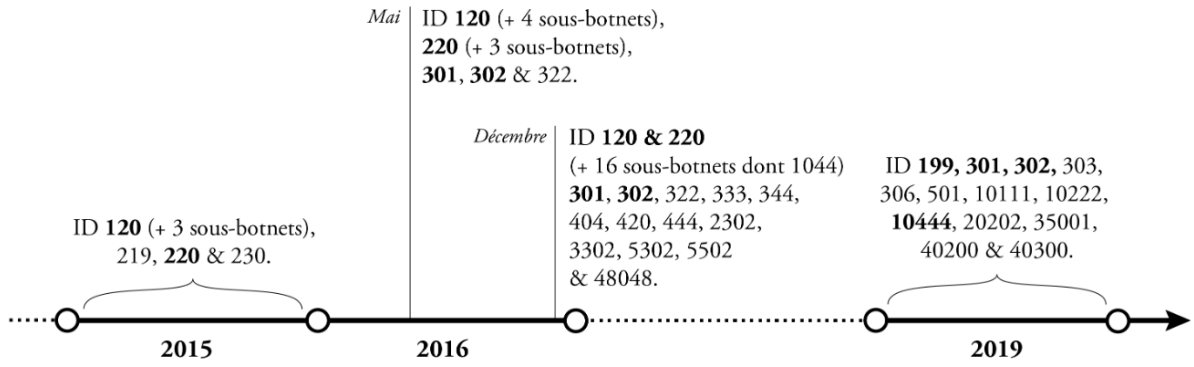


Fig. 1.3 : Principaux Botnets ID Dridex de 2015 à nos jours

[12]Il aurait contenu 100000 bots en mai 2015 [10].
[13]Il aurait contenu 750 bots en avril 2015 [14].
[14]Il aurait contenu 9650 bots en avril 2015 [14, 9].

# 2 Les développeurs de Dridex : Evil Corp

*Les noms cités dans ce chapitre sont issus de sources ouvertes et d'actes de justice systématiquement référencés.*

## 2.1 Origine du groupe : ZeuS, JabberZeuS et GameOverZeuS

Aux alentours des années 2005-2006, M. Bogatchev (alias Slavik, lucky12345) a créé le code malveillant ZeuS (alias Zbot) (voir annexe 6.1). ZeuS est loué en tant que *malware-as-a-service* à d'autres groupes cybercriminels [16].

Début 2009, M. Bogatchev commence à travailler avec le groupe cybercriminel dénommé "Business Club", dont le leader serait M. Yakubets (alias Aqua) [17]. Le groupe aurait fait appel à M. Bogatchev pour développer en collaboration avec ce dernier une version améliorée de ZeuS capable de transmettre des informations aux attaquants sur les comptes bancaires compromis, et en particulier les notifier lorsqu'une victime se connecte sur son compte bancaire en ligne [18]. Cette version, agrémentée de l'utilisation du protocole XMPP (*Extensible messaging and presence protocol*), communément appelé Jabber [19], sera baptisée JabberZeuS (voir annexe 6.2).

En fin d'année 2010, M. Bogatchev prétend prendre sa retraite, après avoir généré des gains avoisinant les 100 millions de dollars durant ses cinq ans d'activité [20]. Le FBI publie toutefois une mise en accusation à l'encontre de M. Bogatchev en juin 2014, laissant à penser qu'il continuait ses activités malveillantes.

En mai 2011, le code source de ZeuS devient public. A ce jour, on recense 447 variantes de ZeuS associées à 27 familles [21].

En septembre 2011, une variante de ZeuS, Murofet (alias Licat), émerge : elle serait utilisée par des membres du Business Club [17], et deviendrait leur outil phare, bientôt appelé GameOverZeuS (GoZ) (voir annexe 6.3). En 2012, le botnet GoZ propage également le rançongiciel Cryptolocker.

En mai 2014, l'opération Tovar du FBI, épaulé par la police russe [20], démantèle l'infrastructure de GoZ et de Cryptolocker, ainsi que le réseau P2P du botnet GoZ. Celui-ci incluait alors environ 1 million de bots, et était responsable de transactions frauduleuses à hauteur de plusieurs dizaines de millions de dollars [18].

## 2.2 Evil Corp

### 2.2.1 2014 : de JabberZeuS à Evil Corp

En juin 2014, le cheval de Troie bancaire Dridex apparaît pour la première fois[15]. Dridex est la version 5 du code malveillant Bugat, apparu en 2010, et manifestement opéré (voire développé) par au moins un membre du Business Club, M. Yakubets, et A. Ghinkul, l'un des opérateurs de Troyak, le prestataire d'hébergement *bulletproof*[16] (démantelé en 2010) du Business Club [18].

A. Ghinkul (alias Smilex) [10], d'origine moldave, est arrêté en août 2015 à Chypre et extradé aux Etats-Unis [22], après que les experts de Dell SecureWorks avaient redirigé les points de contrôle du botnet Dridex vers un serveur *sinkhole*[17], permettant au FBI d'en démanteler l'infrastructure et de l'identifier parmi 14 distributeurs de Dridex. A. Ghinkul aurait en effet fait partie de l'équipe administrant le botnet ID 120.

[15] Deux semaines après le démantèlement de GoZ, le code malveillant Dyre serait également apparu. En plus de disposer du même développeur que Gozi Neverquest, certaines attaques impliquant Dyre pourraient être connectées au Business Club. Il est alors possible que le groupe ait diversifié son activité, en utilisant Dyre pour dérober de l'argent depuis des comptes en banques de grandes entreprises, et Dridex pour voler de l'argent depuis des comptes en banque du secteur de la vente. En novembre 2015, l'arrestation d'opérateurs de Dyre conduit à son arrêt total [18].

[16] Sur le marché noir, des criminels proposent de louer des serveurs loin de toute juridiction. Ces serveurs s'appellent des *bulletproof*. Une fois le serveur bulletproof loué, on peut y installer un centre de commande.

[17] Le *sinkholing* consiste à rediriger les communications des machines zombies vers un serveur hors du contrôle des opérateurs malveillants.

*Commentaire : il est intéressant de remarquer qu'à la suite de l'arrestation d'A. Ghinkul, le botnet ID 120 n'est pas le seul à s'être temporairement arrêté, le botnet 220 associé à TA505 n'ayant repris son activité que trois mois après.*

Malgré cette arrestation, le Business Club, dorénavant appelé Evil Corporation (alias EvilCorp, Indrik Spider), à la tête duquel se trouve M. Yakubets, renouvelle ses infrastructures et poursuit ses activités.

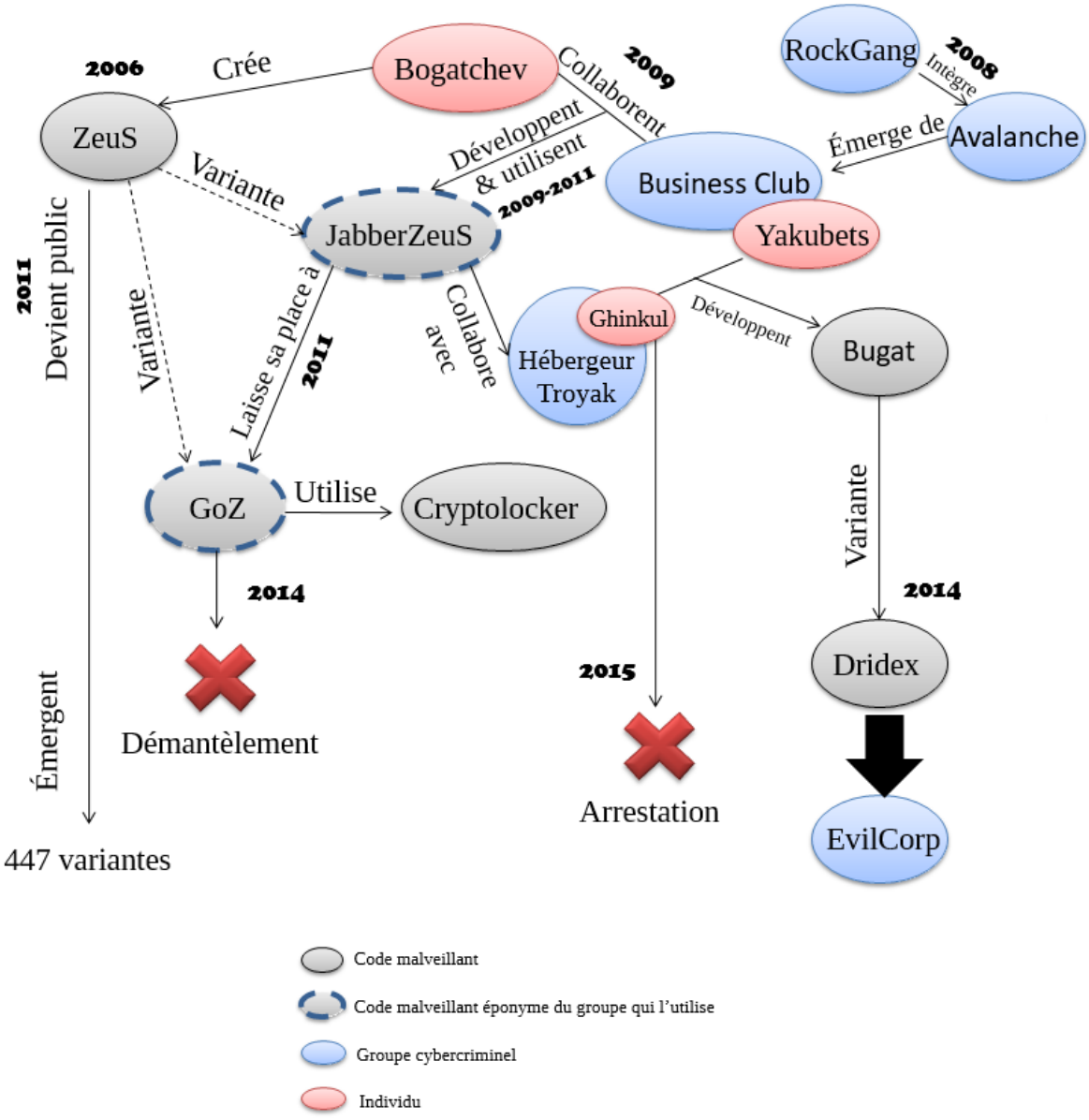


Fig. 2.1 : Cartographie des liens entre des groupes cybercriminels russophones, de ZeuS à Evil Corp

Dans un acte d'accusation conjoint daté du 5 décembre 2019, le Département américain de la Justice et l'agence britannique de lutte contre la criminalité identifient neuf des membres du groupe Evil Corp. Outre M. Yakubets :

- I. Tourachev aurait servi d'administrateur du code malveillant Dridex et fourni une assistance technique à ses opérateurs ;
- D. Goussev est quant à lui accusé d'avoir soutenu matériellement et financièrement Evil Corp, six entreprises implantées en Russie dont il était le directeur général se voyant imposer des sanctions par le Trésor américain [23] ;

- Les six membres principaux restants d'Evil Corp[18] ont notamment été identifiés grâce à des publications sur les réseaux sociaux [24], la plupart s'y affichant avec d'importantes sommes d'argent en liquide et des voitures de luxe immatriculées « BOP » (« voleur » en russe).

Outre Dridex, Evil Corp aurait, d'après Blueliv, propagé d'autres codes malveillants tels que des codes malveillants spécifiques aux terminaux de points de vente (*POS malware*) [25], mais aussi Carbanak[19] [26]. En effet, Evil Corp serait composé de deux équipes opérationnelles, chacune disposant de *spammers*, c'est-à-dire d'individus spécialisés dans la distribution de campagnes d'hameçonnage pour le compte aussi bien d'Evil Corp que d'autres groupes d'attaquants [27].

### 2.2.2 Evolution d'Evil Corp depuis 2017

#### Le rançongiciel BitPaymer

Découverte en juillet 2017 [28], la première occurrence notoire du rançongiciel Bitpaymer (alias FriedEx) remonte à l'attaque contre le *National Health Service* (NHS) en Écosse en août 2017.

Bitpaymer est un binaire, qui n'a ni la capacité de s'autopropager ni la possibilité de se connecter à un serveur C2. Il est donc diffusé manuellement par ses opérateurs. Il présente de nombreuses similarités de code avec Dridex [28]. De plus, de nombreuses attaques conduisant à un chiffrement par le rançongiciel Bitpaymer impliquait une compromission préalable par le code Dridex. Ces liens laissent penser que Bitpaymer est développé et opéré par Evil Corp.

Bitpaymer représente une évolution des tactiques d'Evil Corp, privilégiant un nombre réduit d'attaques ciblées à plus forte rentabilité (*Big Game Hunting*) plutôt que ses campagnes massives Dridex lancées depuis 2014. En 2019, il apparaît que Dridex est utilisé par Evil Corp non plus dans le cadre de fraudes bancaires mais afin d'effectuer de la reconnaissance sur les SI qu'il compromet et de juger de l'intérêt d'y propager ou non BitPaymer [25]. La chaîne d'infection usuelle de Bitpaymer impliquant Dridex est la suivante :

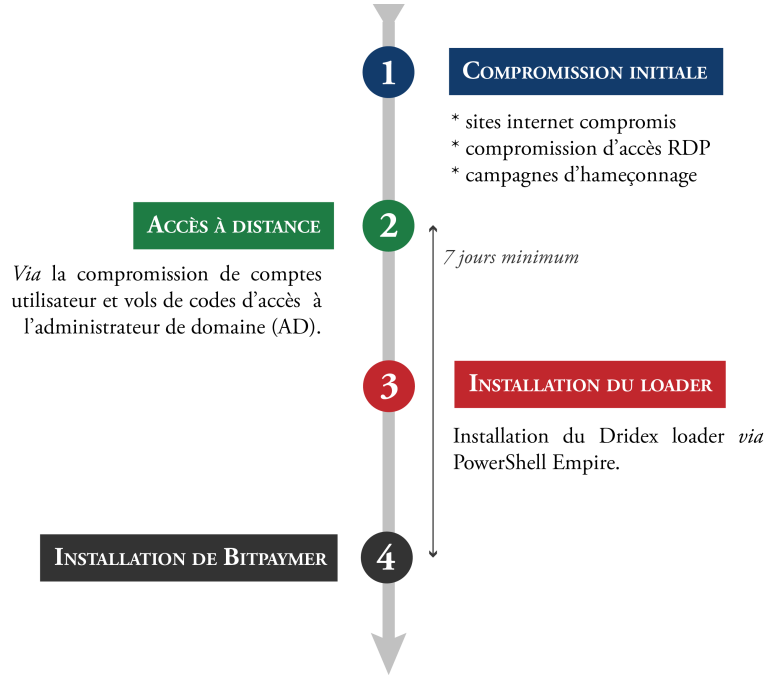


Fig. 2.2 : Chaîne d'infection de Bitpaymer impliquant Dridex

Pour autant, il apparaît que Bitpaymer peut également être propagé par Emotet plutôt que par Dridex (lui-même parfois propagé par Emotet) [29, 30].

[18] Nommément Dmitry Smirnov, Artyom Yakubets, Ivan Toutchkov, Andreï Plotnitsky, Dmitry Slobodskoï et Kirill Slobodskoï.
[19] En 2016, Carbanak aurait même été parfois téléchargé par *Dridex loader* au sein de SI infectés.

Malgré la mise en accusation de M. Yakubets et d'autres membres d'Evil Corp publiée début décembre 2019, l'activité du groupe cybercriminel ne semble pas troublée, au vu de la continuité des campagnes BitPaymer.

### Scission au sein d'Evil Corp

En avril 2019, Evil Corp se serait séparé en deux groupes : Indrik Spider et Doppel Spider[20] [31]. Tandis qu'Indrik Spider opérerait comme à l'accoutumée depuis 2018 les codes malveillants Dridex et Bitpaymer, Doppel Spider opérerait lui une version modifiée de Dridex, DoppelDridex, ainsi qu'une variante du rançongiciel BitPaymer, DoppelPaymer. Il mènerait ainsi aussi bien des campagnes de fraudes bancaires via DoppelDridex uniquement, que des campagnes de rançonnage via DoppelPaymer.

Compte tenu du fait que :

- le code malveillant FakeUpdates a distribué Dridex en octobre 2019, et que Dridex a distribué soit du BitPaymer soit du DoppelPaymer au sein du SI des victimes [32],
- lors d'un incident DoppelPaymer, FireEye a constaté le téléchargement de Dridex v4 botnet ID 501 (associé à Evil Corp), puis de Dridex v2 botnet ID 12333 dans le but de distribuer DoppelPaymer (associé à Doppel Spider) [32];
- Doppel Spider utilise les services d'Emotet [31], tout comme le fait Evil Corp,

Il apparaît que les deux groupes continuent de collaborer, voire que Doppel Spider est un sous-groupe d'Evil Corp.

Pour autant, depuis le premier trimestre 2020, les opérateurs de DoppelPaymer se différencient de ceux de Bitpaymer par le fait qu'ils se sont mis à publier des données exfiltrées depuis le SI de leurs victimes (sur le site www.doppleshare[.]top/), à l'instar des opérateurs d'autres rançongiciels (Maze, Sodinokibi, Clop et Nemty notamment) [33].

[20] Indrik Spider et Doppel Spider sont deux alias établis par Crowdstrike.

# 3 Distribution de Dridex par les principaux affiliés

Le vecteur d'infection semble être la caractéristique la plus discriminante des différents botnets ID, et donc des différents affiliés. Cependant, la difficulté réside dans le risque de confondre l'affilié et le distributeur pour lequel il a opté. Par exemple, l'opérateur d'un botnet propageant le Dridex d'un botnet ID spécifique ne doit pas être spontanément confondu avec l'affilié du botnet ID en question.

## 3.1 Courriels d'hameçonnage

### 3.1.1 Le botnet CraP2P (alias Necurs)

Actif de 2012 à 2020, le botnet CraP2P est un botnet spécialisé dans la distribution de campagnes d'hameçonnage et de codes malveillants, pour le compte de différents groupes d'attaquants. Au cours de son activité, le nombre des bots qui le composait a atteint les 9 millions. Or un seul de ces bots était capable d'envoyer plusieurs millions de spams en seulement quelques dizaines de jours [34]. CraP2P a entre autres été utilisé par ses opérateurs pour distribuer GoZ en 2013, Cryptolocker en 2014 et Dridex à partir d'au moins 2015 [35].

CraP2P a été à l'origine de la distribution, sur la période 2015-2016, de campagnes d'hameçonnage délivrant notamment Dridex botnet IDs 120, 122, 123, 220, 223 et 301. Tandis que le botnet ID 120 est associé à A. Ghinkhul jusqu'à la mi-2015, les botnets ID 220 et 223 sont associés à TA505 [36].

Proofpoint [37] précise que le groupe cybercriminel TA505 aurait utilisé Dridex à partir de juillet 2014, soit un mois après sa création (juin 2014). TA505 a utilisé Dridex de manière éparse jusqu'en juin 2016 puis a stoppé définitivement son utilisation en juin de l'année 2017. Les botnets ID utilisés par TA505 entre 2014 et 2015 pour propager Dridex auraient été les botnets 125, 220 (ciblant le Royaume-Uni, la France et l'Australie), 223 (ciblant l'Allemagne et l'Autriche). Il aurait ensuite utilisé les botnets ID 7200 et 7500 (sans doute en 2017).

*Commentaire : Du fait que TA505 ait utilisé l'un des trois botnets ID les plus actifs du réseau Dridex (ID 220), il a pu être confondu avec Evil Corp, alors que ce n'était finalement qu'un affilié particulièrement impliqué du réseau P2P, et donc effectivement en étroite collaboration avec Evil Corp.*

Il apparaît donc que les opérateurs de CraP2P étaient en étroite collaboration avec Evil Corp et certains de ses affiliés pour le volet distribution, celle-ci découlant de la collaboration passée avec GoZ.

*Commentaire : Certaines sources indiquent qu'Evil Corp pourrait être l'opérateur du botnet CraP2P, tandis que d'autres avancent que ce pourrait être TA505. Sans plus d'éléments, il est uniquement possible de confirmer une relation privilégiée entre ces différents groupes.*

### 3.1.2 Le botnet Cutwail

TA544 (alias Narwhal Spider) est un prestataire de services cybercriminel, qui proposerait à la location l'utilisation du botnet Cutwail sur des forums souterrains russophones[21] [38].

Au cours de sa période d'activité, GoZ a loué l'accès à une partie de l'infrastructure du botnet Cutwail pour la diffusion de courriels d'hameçonnage [39]. Ses successeurs présumés, Evil Corp, auraient également fait appel aux services de TA544 [40].

En 2019, le botnet Cutwail distribue Dridex ID 1044 via des campagnes d'hameçonnage [41], principalement à l'encontre des Etats-Unis, du Canada et de l'Australie. Au moins une fois en novembre 2019, la chaîne d'infection ne se serait pas terminée avec Dridex, ce dernier ayant propagé le rançongiciel Hermès [22] [15].

[21] Botnet fondé en 2007, dont GameOver ZeuS aurait été client en 2012.

[22] Utilisé par Lazarus lors de l'attaque contre la Far Eastern International Bank, Hermès est un rançongiciel disponible à la vente sur le Dark Web.

*Commentaire : Il n'est pas évident d'identifier si TA544 est un affilié de Dridex, ou si une partie du botnet qu'il opère est utilisée par Evil Corp ou l'un de ses affiliés pour distribuer Dridex, faisant de TA544 uniquement un distributeur.*

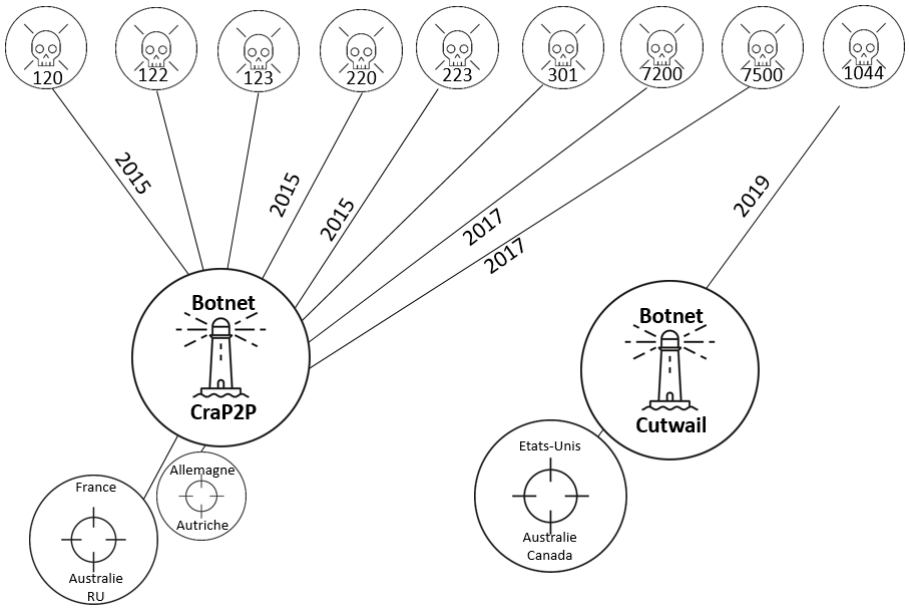


Fig. 3.1 : Distribution de Dridex via les botnets CraP2P et Cutwail

### 3.1.3 Le botnet Andromeda

Avant son démantèlement en 2017, le botnet Andromeda (alias Gamarue) a été chargé de la distribution de Dridex, notamment à l'encontre du Royaume-Uni en 2016 [13].

## 3.2 En tant que seconde charge utile

D'après Trend Micro, les opérateurs d'Emotet, Gozi ISFB (alias Ursnif)[23] et Dridex partageraient le même fournisseur de PE[24] *loader*[25], voire échangeraient des ressources [29].

Emotet[26] a la capacité de propager Dridex, depuis au moins 2017 [43]. Il arrive également à Emotet de propager Bitpaymer, rançongiciel exclusivement utilisé par Evil Corp. Les premiers liens entre Emotet et les opérateurs de Dridex, Evil Corp, sont établis en avril 2017 [44].

*Commentaire : Il apparaît qu'Evil Corp fait appel aux opérateurs d'Emotet (Mummy Spider, Mealybug, TA542) pour propager Dridex en tant que seconde charge utile au sein de SI préalablement compromis par leurs soins. Les opérateurs de TrickBot (Wizard Spider) procèdent de la même manière.*

Concernant Gozi ISFB, TA551 (alias Shathak) a utilisé son loader RM3[45] pour distribuer Dridex botnets ID 301, 302, 303, 3101 et 35001 en 2018 et 2019 [15, 46] aux Etats-Unis, au Canada et en Italie. Lors de ces mêmes chaînes d'infection, Gozi v2 RM3 a parfois été accompagné du code malveillant Predator the Thief [27] ou du rançongiciel

[23] Le cheval de Troie bancaire d'origine de Gozi a été développé en 2006 en tant que concurrent du cheval de Troie ZeuS. Le code source de Gozi a fuité en 2010 et a été réutilisé par d'autres groupes cybercriminels pour créer d'autres codes malveillants, parmi lesquels Gozi ISFB, Vawtrak (Neverquest), et GozNim, combinaison de Gozi IFSB et Nymain [16]. La version 2.13.24.1 de Gozi ISFB a fuité en février 2015.

[24] Format des fichiers exécutables et des bibliothèques sur les systèmes d'exploitation Windows, incluant .exe (pour les programmes) et .dll (pour les bibliothèques).

[25] Le PE loader permet à Windows d'exécuter les instructions d'un fichier PE.

[26] Cheval de Troie bancaire apparu en 2014, devenu *loader* de codes malveillants, tels que TrickBot, Gootkit, IcedID, à partir de 2017. Les opérateurs d'Emotet louent l'accès à des postes qu'ils ont infectés à d'autres groupes cybercriminels [42, 29].

[27] Code malveillant vendu sur le Dark Web en juin 2018.

GandCrab (occurrences en décembre 2018)[28].

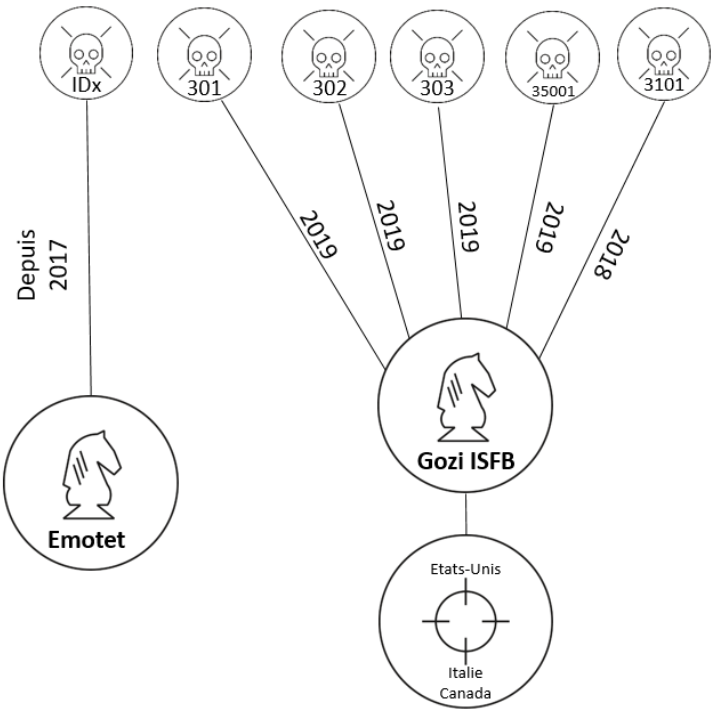


Fig. 3.2 : Distribution de Dridex en tant que seconde charge utile d'Emotet et Gozi ISFB

## 3.3 Point d'eau

Dridex v4 botnets ID 199 et 501 seraient distribués, depuis 2019, via FakeUpdates (alias SocGholish)[29]. L'infection, par point d'eau ou par courriel d'hameçonnage pointant vers une URL malveillante, consiste en l'apparition d'une fausse mise à jour de navigateur, qui conduirait à l'installation du code malveillant FakeUpdates, puis de la propagation de Dridex, et de celle de BitPaymer ou de DoppelPaymer [32]. Le prestataire en services informatiques espagnol Everis System en aurait par exemple été victime en novembre 2019 [25]. Dans le cas de DoppelPaymer, Dridex ID 12333 serait téléchargé sur le SI après qu'il a été infecté par Dridex v4 botnets ID 199 ou 501.

*Commentaire : Dridex ID 12333 serait donc logiquement associé à Doppel Spider. Ce serait également le cas pour Dridex ID 40300.*

[28] GandCrab aura également été propagé fin 2018 au cours de chaînes d'infection impliquant Dridex botnet ID 10202 et TA547, identifié par Proofpoint comme l'opérateur du cheval de Troie bancaire Danabot [47].
[29] Dridex botnet ID 11122 aurait été propagé de la même manière courant 2018.

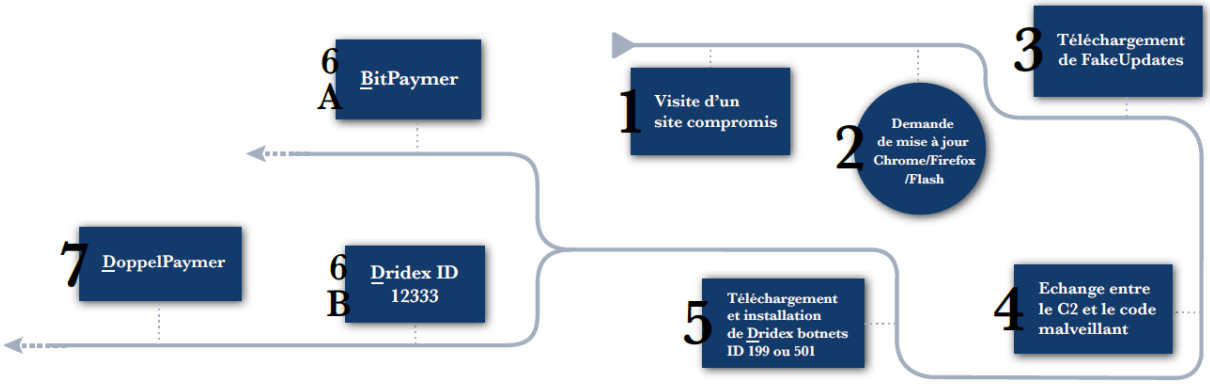


Fig. 3.3 : Chaîne d'infection Dridex via FakeUpdates

Ces mêmes campagnes propagent alternativement Dridex v4 botnets ID 199 ou 501, AZORult, Chthonic[30] et NetSupport RAT[31], illustrant le fait qu'Evil Corp fait appel à l'opérateur de FakeUpdates, à la manière d'autres groupes cybercriminels, afin de distribuer Dridex puis BitPaymer.

## 3.4 Kits d'exploitation

En juin 2019, le kit d'exploitation Spelevo[32] a propagé Dridex, de même qu'entre septembre et novembre, concomitamment au kit d'exploitation Fallout [15], via des sites Internet compromis [52].

L'affilié correspondant au botnet ID 10111 est réputé privilégier le kit d'exploitation Fallout comme vecteur d'infection, tandis que le botnet ID 30102 privilégie le kit d'exploitation Spelevo.

[30] Cheval de Troie bancaire découlant du code malveillant ZeusVM, lui-même variante de ZeuS, dont le binaire du *builder* a fuité en juin 2015 [48, 49], et lui-même basé sur le code malveillant Zeus, dont le code source a fuité en 2011. Chthonic est conçu à la manière de Dridex avec une architecture modulaire et partage trois de ses modules (Pony, SOCKS et VNC) [50].
[31] Logiciel légitime d'accès à distance [51].
[32] Ce kit d'exploitation est aussi connu pour avoir propagé le rançongiciel Maze.

# 4 Conclusion

Le code malveillant Dridex illustre à quel point la profusion de groupes interconnectés qui compose l'écosystème cybercriminel russophone (prestataires, clients, opérateurs de botnet etc.) complexifie l'attribution des attaques. Dridex a un héritage multiple (Bugat, GoZ), des opérateurs provenant de groupes variés (Rock Gang, Avalanche, JabberZeuS), tout comme le sont ses affiliés, et est propagé via de multiples vecteurs d'infection, à l'encontre de cibles diverses à travers le monde.

Cependant, les actes d'accusation échelonnés sur près de 10 ans à l'encontre de membres d'Evil Corp ont permis de mieux cerner les activités du groupe, en liant des individus à des attaques informatiques et des codes malveillants.

En tout état de cause, Dridex demeure une menace dans les mains d'Evil Corp, de Doppel Spider et de leurs affiliés actuels notamment, dans le cadre de campagnes plus ciblées visant à propager des rançongiciels.

# 5 Moyens de détection

Les indicateurs de compromission précisés ci-dessous peuvent être bloqués et recherchés sur un système d'information pour prévenir ou détecter des attaques impliquant le code malveillant Dridex.

| Marqueur | Type | Commentaire |
|---|---|---|
| admin@belpay.by | Adresse courriel | Campagne Dridex |
| faber@imaba.nl | Adresse courriel | Campagne Dridex |
| s.palani@itifsl.co.in | Adresse courriel | Campagne Dridex |
| yportocarrero@elevenca.com | Adresse courriel | Campagne Dridex |
| tom@blackburnpowerltd.co.uk | Adresse courriel | Campagne Dridex |
| pranab@pdrassocs.com | Adresse courriel | Campagne Dridex |
| admin@sevpazarlama.com | Adresse courriel | Campagne Dridex |
| farid@abc-telecom.az | Adresse courriel | Campagne Dridex |
| bounce@bestvaluestore.org | Adresse courriel | Campagne Dridex |
| web1587p16@mail.flw-buero.at | Adresse courriel | Campagne Dridex |
| fabianurquiza@correo.dalvear.com.ar | Adresse courriel | Campagne Dridex |
| info@melvale.co.uk | Adresse courriel | Campagne Dridex |
| faturamento@sidestecaminhoes.com.br | Adresse courriel | Campagne Dridex |
| cariola72@teletu.it | Adresse courriel | Campagne Dridex |
| info@golfprogroup.com | Adresse courriel | Campagne Dridex |
| info@antonioscognamiglio.it | Adresse courriel | Campagne Dridex |
| http://owenti.com/fprl.exe | Domaine | Dridex |
| http://tamboe.net/frap.exe | Domaine | Dridex |
| http://owenti.com/fprl.bin | Domaine | Dridex |
| http://saitepy.com/glps.exe | Domaine | Dridex |
| http://klerber.com/glps.exe | Domaine | Dridex |
| http://fdistus.com/glps.exe | Domaine | Dridex |
| http://uprevoy.com/opxe.exe | Domaine | Dridex |
| http://typrer.com/qrpt.exe | Domaine | Dridex |
| http://urefere.org/opxe.exe | Domaine | Dridex |
| http://inesmoreira.pt/img/galeria/beloura/123.bin | Domaine | Dridex |
| https://masteronare.com/function.php?3b3988df-c05b-4fca-93cc-8f82af0e3d2b | Domaine | Dridex |
| urefere.org/opxe.exe | Domaine | Dridex |
| hxxp://bienvenidosnewyork.com/app.php | Domaine | Dridex |
| hxxp://photoflip.co.in/lndex.php | Domaine | Dridex |
| hxxp://everestedu.org/lndex.php | Domaine | Dridex |
| https://thinkunicorn.com/wp-admin/css/colors/fish/HraXJHWvJbyTvdLwdaAu/0ev7Bg.bin | Domaine | DoppelDridex (botnet ID 40300) |
| https://unfocusedprints.co.kr/HraXJHWvJbyTvdLwdaAu/0ev7Bg.bin | Domaine | DoppelDridex (botnet ID 40300) |
| 62.149.158.252 | Adresse IP | Dridex |
| 177.34.32.109 | Adresse IP | Dridex |
| 2.138.111.86 | Adresse IP | Dridex |
| 122.172.96.18 | Adresse IP | Dridex |
| 69.93.243.5 | Adresse IP | Dridex |
| 200.43.183.102 | Adresse IP | Dridex |
| 79.124.76.30 | Adresse IP | Dridex |
| 188.125.166.114 | Adresse IP | Dridex |
| 37.59.52.64 | Adresse IP | Dridex |
| 50.28.35.36 | Adresse IP | Dridex |
| 154.70.39.158 | Adresse IP | Dridex |
| 108.29.37.11 | Adresse IP | Dridex |
| 65.112.218.2 | Adresse IP | Dridex |
| 47.254.236.15 | Adresse IP | Dridex |
| 194.99.22.193 | Adresse IP | Dridex |
| 194.99.22.193 | Adresse IP | Dridex |
| 178.63.67.20 | Adresse IP | Dridex |
| 5.127.14.171 | Adresse IP | Dridex |
| 34.213.221.29 | Adresse IP | Dridex |

| | | |
|---|---|---|
| 209.40.205.12 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 79.143.178.194 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 188.165.247.187 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 185.234.52.170 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 107.152.33. 15 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 199.101.86.6 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 188.165.247.187 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 176.10.250.88 | Adresse IP | DoppelDridex (botnet ID 40300) |
| 7239da273d3a3bfd8d169119670bb745 | MD5 | Dridex (botnet ID 199 ou 501) |
| 72fe19810a9089cd1ec3ac5ddda22d3f | MD5 | Dridex (botnet ID 199 ou 501) |
| 07b0ce2dd0370392eedb0fc161c99dc7 | MD5 | Dridex (botnet ID 199 ou 501) |
| c8bb08283e55aed151417a9ad1bc7ad9 | MD5 | Dridex (botnet ID 199 ou 501) |
| 6e05e84c7a993880409d7a0324c10e74 | MD5 | Dridex (botnet ID 199 ou 501) |
| 63d4834f453ffd63336f0851a9d4c632 | MD5 | Dridex (botnet ID 199 ou 501) |
| 0ef5c94779cd7861b5e872cd5e922311 | MD5 | Dridex (botnet ID 199 ou 501) |
| 9aa3089af134627ef48b178db606268a | MD5 | DoppelDridex (botnet ID 40300) |
| e614a69d706913376ab2bb20a703dcf5 | MD5 | Dridex |
| 1d778359ab155cb190b9f2a7086c3bcb4082aa195ff8f754dae2d665fd20aa05 | SHA256 | Dridex (botnet ID 199) |
| abf99a028dae6812f6f0ca633d7424ce9272dfcfbebf6b518c1e6c97f872f3e7 | SHA256 | Dridex |
| 6712500bb0de148a99ec940160d3d61850e2ce3803adca8f39e9fa8621b8ea6f | SHA256 | Dridex |
| 86bcfce2dd342e9a1c04cfc65731d40ed1c397a4ec47bd9f5b41771297d81100 | SHA256 | Dridex |
| 005e77a55b8f1bf4049d6231c2349a01d019b46f47b6930103458a2aadd1bfa6 | SHA256 | Dridex |
| a1388cb3e6ae68a6130ae12f9db4881238c97718875a3362b6bc5788e61c6663 | SHA256 | Dridex |
| ca087f46f97cd465f46e4ccb04181e6eae7b2c751ae7fd9e262191b979728ccc | SHA256 | Dridex |
| 4ad0998882a3fbd3412f0c740faebb8ef78bec4c3e566650424c40a878e6a23a | SHA256 | Dridex |

Dridex étant susceptible de télécharger les rançongiciels BitPaymer et DoppelPaymer en tant que seconde charge utile, il peut être pertinent de porter ses efforts de détection sur ces codes au cas où Dridex ait été identifié sur le SI.

Dridex étant susceptible d'être propagé en tant que seconde charge utile par les codes malveillants FakeUpdates, Emotet, Gozi ISFB , il peut être également pertinent de porter ses efforts de détection sur ces codes afin de stopper l'attaque à ses débuts.

# 6 Annexes

## 6.1 Annexe 1 : Caractéristiques du code malveillant ZeuS

ZeuS a deux utilités premières :

- il fait de ses victimes les machines zombies du botnet portant le même nom ;
- il reconnaît lorsque sa victime se trouve sur le site Internet d'une banque et enregistre les codes d'accès à ses comptes. Ainsi, ses opérateurs peuvent transférer de l'argent depuis les comptes des victimes vers des comptes contrôlés par des mules.

Ses fonctionnalités principales sont les suivantes [53] :

- le vol ciblé d'informations : par exemple, en 2007, ZeuS dérobe des informations au Département du Transport américain, les Etats-Unis étant sa cible première [54] ;
- l'accès à distance via le protocole VNC ;
- le téléchargement et l'exécution de programmes[33] ;
- la suppression de composants essentiels au fonctionnement du système d'exploitation afin de détruire la machine infectée.

*Commentaire : Le code malveillant Zeus aurait ainsi eu la possibilité de saboter des SI, tout comme Dridex au travers de son module KillOS.*

## 6.2 Annexe 2 : JabberZeuS

Le Business Club a pour origine le groupe cybercriminel Rock Gang, qui a opéré de 2004 à 2008, et qui était composé d'individus de nationalités ukrainienne, russe, roumaine et moldave [18]. En 2008, beaucoup de membres du Rock Gang se seraient mis à utiliser Avalanche, un large réseau d'hébergement d'infrastructure mondial utilisé par différents groupes de cybercriminels [55]. Parmi eux, certains, regroupés au sein du Business Club, auraient fait appel à M. Bogatchev pour développer en collaboration avec lui une version améliorée de ZeuS : JabberZeuS.

Le nouveau groupe formé autour de JabberZeuS comprend une cinquantaine d'individus, dotés de privilèges acquis avec l'ancienneté et répartis en plusieurs activités :

- la fraude : pour participer aux activités de fraude, il était nécessaire de payer une cotisation et de signer un accord de partage de profit ;
- le recrutement de mules : certaines mules étaient localisées dans deux villes chinoises, adjacentes à la frontière russe, au nord de Vladivostok [17]. En septembre 2010, le réseau de mules britanniques de JabberZeuS est arrêté lors de l'opération Trident breACH[34] [18] ;
- le support technique ;
- la prestation de services : le groupe proposait l'accès à ZeuS (pour 3000 ou 4000 dollars [20], modules non inclus) ainsi qu'à d'autres codes malveillants. Ainsi, en octobre 2010, le FBI, avec l'aide de ses équivalents britanniques et ukrainiens, démantèle un réseau de cybercriminels, composé d'une douzaine d'individus, ayant utilisé le code malveillant ZeuS afin de cibler des comptes bancaires américains et de leur dérober environ 70 millions de dollars [56, 57].

[33] Fonctionnalité généralement utilisée par les affiliés du botnet ZeuS, à qui il arrivait de propager d'autres programmes malveillants en tant que seconde charge utile afin d'accroître leurs revenus.
[34] ACH désigne des transferts de fonds non autorisés réalisés sur des comptes bancaires.

Parmi les membres du groupe, sont identifiés M. Bogatchev, M. Yakubets (chargé notamment du recrutement des mules), Y. Pentchukov (alias tank), I. Klepikov (alias petr0vich), A. Bron (alias thehead), Y. Kulibaba (alias jonni), Y. Konovalenko (alias jtk0) et A. Tikonov (alias kusanagi) [58]. Ce dernier aurait développé Leprechaun, un système permettant d'automatiser les transactions frauduleuses sur les plateformes de banques en ligne, utilisé par JabberZeuS. Il permettait notamment de modifier en temps réel la transaction bancaire d'une victime [18]. Des mésententes au sein du groupe entre M. Yakubets et M. Bogatchev sont identifiées par Brian Krebs[35] [59].

## 6.3 Annexe 3 : GameOverZeuS

S'inspirant du modèle de botnet de ZeuS, le groupe construit via GameOverZeuS une structure de botnets fonctionnant en P2P. Cette structure comprenait 27 botnets, dont les *C2 backends* étaient chacun contrôlés par une personne ou un groupe différent, opérant à côté d'autres codes malveillants. La majorité de ces botnets existait déjà et a simplement migré vers la version P2P de GoZ à sa création. GoZ a ainsi pénétré les ordinateurs déjà infectés par JabberZeuS [18].

GoZ incluait un système de transfert automatique de fonds, à la manière de Leprechaun, dénommé *The World Bank Center* [18].

De plus, le groupe d'attaquants était client du même *bullet proof hoster* (Troyak) pour l'utilisation de serveurs que le Rock Gang et les opérateurs d'Avalanche et de Gozi, et louait l'accès à une partie de l'infrastructure du botnet Cutwail pour la diffusion de courriels d'hameçonnage. Ils utilisaient également le kit d'exploitation BlackHole[36] qui distribuait Pony Loader afin d'installer la charge utile GameOver ZeuS, mais aussi le kit Dirt Jumper afin d'opérer des attaques DDoS sur les sites Internet de banques et de camoufler ainsi leurs opérations de virements frauduleux [39].

## 6.4 Annexe 4 : Sur les liens entre Dridex et Cridex

La proximité patronymique et leur comportement ont longtemps laissé penser que les logiciels Dridex et Cridex pouvaient avoir été créés par les mêmes développeurs. Ce ne semble pas être le cas en réalité.

Le 10 décembre 2015, le compte DridexBOT apparaît sur le réseau Twitter [60], vraisemblablement enregistré à l'aide de l'adresse mail dridex[@]mail.ru créée spécifiquement pour l'occasion.

Si ce compte se présente comme un bot, ses tweets sont en réalité écrits par une ou plusieurs personnes physiques comme en témoignent ses nombreuses interactions avec des comptes d'utilisateurs proches du milieu de la cybersécurité, notamment le blog MalwareTech qui va authentifier le compte le 4 avril 2016 [61]. Entre décembre 2015, et le 14 avril 2017, date de son dernier tweet, DridexBOT postera 153 messages cherchant régulièrement à démontrer l'inexistence de liens entre son code source et ceux de la famille Cridex (Feodo, Geodo, etc.) [62, 63, 64].

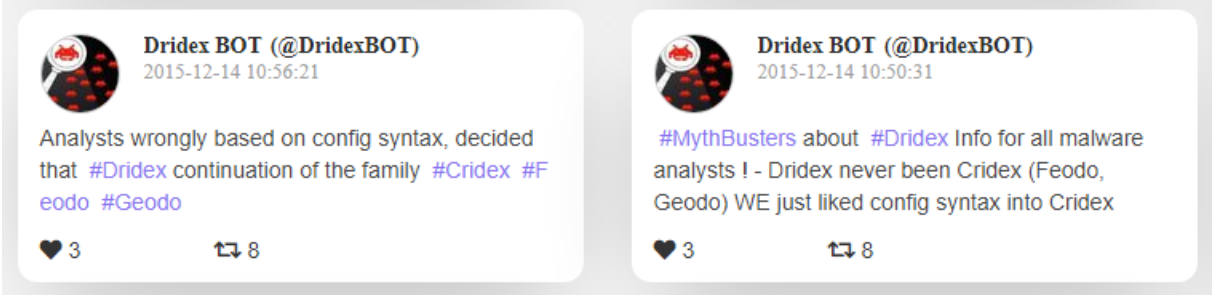


Fig. 6.1 : Tweets de DridexBOT

[35] Au cours d'un tchat, M. Yakubets acquiesce à ces propos de l'un des membres de JabberZeuS concernant M. Bogatchev : « he, fucker, annoyed the hell out of everyone, doesn't want to write bypass of interactives and trojan penetration 35-40%, bitch ».

[36] Également utilisé pour propager les variantes de ZeuS Bugat, Feodo et Cridex, mais aussi les chevaux de Troie bancaires Mebroot et Torpig.

Enfin, il n'hésitera pas à affirmer l'intérêt de Dridex pour d'autres domaines que le bancaire, et notamment l'espionnage industriel [65].


Fig. 6.2 : Tweet de DridexBOT

# 7 Bibliographie

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

[2] 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/.

[3] DEVCENTRAL. *Dridex BOTnet 220 Campaign DevCentral*. 25 fév. 2016. URL : https://devcentral.f5.com/s/articles/dridex-botnet-220-campaign-17873.

[4] BROMIUM. *Dridex Threat Analysis : Masquerading and Code Injection Techniques*. 29 juil. 2019. URL : https://www.bromium.com/dridex-threat-analysis-july-2019-variant/.

[5] ACUNETIX. *Pony : A Breakdown of the Most Popular Malware in Credential Theft*. 25 sept. 2018. URL : https://www.acunetix.com/blog/articles/pony-malware-credential-theft/.

[6] KASPERSKY. *Dridex : A History of Evolution*. 27 jan. 2020. URL : https://securelist.com/dridex-a-history-of-evolution/78531/.

[7] PROOFPOINT. *Dridex Campaigns Hitting Millions of Recipients Using Unpatched Microsoft Zero-Day*. 10 avr. 2017. URL : https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day.

[8] ANSSI. *Etat de La Menace Liée Aux Botnets*. 4 nov. 2019.

[9] BIT SIGHT. *Dridex Botnets*. 24 jan. 2017. URL : https://www.bitsight.com/blog/dridex-botnets.

[10] UNITED STATES DISTRICT FOR THE WESTERN DISTRICT OF PENNSYLVANIA. *Declaration of Special Agent Brian Stevens in Support of Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction*. 8 oct. 2015.

[11] FIREEYE. *Evolution of Dridex*. 18 juin 2015. URL : https://www.fireeye.com/blog/threat-research/2015/06/evolution_of_dridex.html.

[12] TREND MICRO. *Dealing with the Mess of DRIDEX*. 6 déc. 2014. URL : https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3147/dealing-with-the-mess-of-dridex.

[13] BOTCONF 2020. *Dridex Gone Phishing*. 25 sept. 2016. URL : https://www.botconf.eu/2016/dridex-gone-phishing/.

[14] Anubis NETWORKS. "Dridex : Chasing a Botnet from the Inside". 2015. In : (2015).

[15] TWITTER. *@Kafeine*. 5 déc. 2019. URL : https://twitter.com/kafeine/status/1202684242905448448.

[16] ZDNET. *10 ans de malwares : les pires botnets des années 2010*. 11 déc. 2019. URL : https://www.zdnet.fr/actualites/10-ans-de-malwares-les-pires-botnets-des-annees-2010-39895641.htm.

[17] FOX-IT. "Backgrounds on the Badguys and the Backends". 2015. In : (2015).

[18] SECURE WORKS. *Evolution of the GOLD EVERGREEN Threat Group*. 15 mai 2017. URL : https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

[19] XAKER.RU. *Le solitaire contre la "société du mal". Comment Brian Krebs s'est battu contre les pirates russes d'Evil Corp*. 31 jan. 2020. URL : https://xakep.ru/2020/01/31/evil-corp-vs-brian-krebs/.

[20] 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/.

[21] *Zeus Museum*. 9 avr. 2020. URL : https://zeusmuseum.com/.

[22] CNEWS. *Un Ressortissant de La Communauté Des Etats Indépendants Sera Incarcéré 15 Ans Pour Le Piratage Informatique d'écoles et d'une Entreprise Pétrolière*. 15 fév. 2017. URL : https://safe.cnews.ru/news/top/2017-02-15_vyhodets_iz_sng_syadet_v_tyurmu_na_15_let_za_vzlom.

[23] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware*. 5 déc. 2019. URL : https://home.treasury.gov/news/press-releases/sm845.

[24] NATIONAL CRIME AGENCY. *International Law Enforcement Operation Exposes the World's Most Harmful Cyber Crime Group*. 5 déc. 2019. URL : https://www.nationalcrimeagency.gov.uk/news/international-law-enforcement-operation-exposes-the-world-s-most-harmful-cyber-crime-group.

[25] BLUELIV. *Spanish Consultancy Everis Suffers BitPaymer Ransomware Attack : A Brief Analysis*. 6 nov. 2019. URL : https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/everis-bitpaymer-ransomware-attack-analysis-dridex/.

[26] MALWAREBYTES. *The Forgotten Domain : Exploring a Link between Magecart Group 5 and the Carbanak APT*. 22 oct. 2019. URL : https://blog.malwarebytes.com/threat-analysis/2019/10/the-forgotten-domain-exploring-a-link-between-magecart-group-5-and-the-carbanak-apt/.

[27] Dell Secure WORKS. "Banking Botnets Persists despite Takedowns". Avr. 2015. In : (avr. 2015).

[28] ESET. *FriedEx : BitPaymer, nouveau rançongiciel des auteurs de Dridex*. 31 jan. 2018. URL : https://www.welivesecurity.com/fr/2018/01/31/friedex-bitpaymer-dridex/.

[29] 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/.

[30] MICROSOFT. *Human-Operated Ransomware Attacks : A Preventable Disaster*. 5 mar. 2020. URL : https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

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

[32] FIREEYE. *Head Fake : Tackling Disruptive Ransomware Attacks*. 1er oct. 2019. URL : https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html.

[33] BLEEPING COMPUTER. *Three More Ransomware Families Create Sites to Leak Stolen Data*. 24 mar. 2020. URL : https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/.

[34] United States District Court Eastern District of NEW-YORK. *Complaint*. 5 mar. 2020.

[35] CYWARE. *The Many Faces and Activities of Ever-Evolving Necurs Botnet*. 29 déc. 2019. URL : https://cyware.com/news/the-many-faces-and-activities-of-ever-evolving-necurs-botnet-1e8d2734.

[36] PROOF POINT. *Locky Ransomware : Dridex Actors Get In The Game*. 6 avr. 2016. URL : https://www.proofpoint.com/us/threat-insight/post/dridex-actors-get-in-ransomware-with-locky.

[37] PROOF POINT. *Threat Actor Profile : TA505, From Dridex to GlobeImposter*. 27 sept. 2017. URL : https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter.

[38] SECURE WORKS. *Cutwail Spam Swapping Blackhole for Magnitude Exploit Kit*. 18 oct. 2013. URL : https://www.secureworks.com/blog/cutwail-spam-swapping-blackhole-for-magnitude-exploit-kit.

[39] SECURE WORKS. *The Lifecycle of Peer to Peer (Gameover) ZeuS*. 23 juil. 2012. URL : https://www.secureworks.com/research/the-lifecycle-of-peer-to-peer-gameover-zeus.

[40] MALPEDIA. *NARWHAL SPIDER*. Mar. 2020. URL : https://malpedia.caad.fkie.fraunhofer.de/actor/narwhal_spider.

[41] TWITTER. *@FaLconIntelligence*. 8 avr. 2020.

[42] ZDNET. *Meet the White-Hat Group Fighting Emotet, the World's Most Dangerous Malware*. 29 fév. 2020. URL : https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/.

[43] SOPHOS. "Emotet's Goal : Drop Dridex Malware on as Many Endpoints as Possible". 10 août 2017. In : (10 août 2017).

[44] 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.

[45] TWITTER. *@Vitali Kremez*. 11 déc. 2019.

[46] TWITTER. *@Vitali Kremez*. 17 nov. 2018.

[47] PROOFPOINT. "DanaBot - A New Banking Trojan Surfaces Down Under". 31 mai 2018. In : (31 mai 2018).

[48] COMPUTER WORLD. *Leak of ZeusVM Malware Building Tool Might Cause Botnet Surge*. 6 juil. 2015. URL : https://www.computerworld.com/article/2944041/leak-of-zeusvm-malware-building-tool-might-cause-botnet-surge.amp.html.

[49] MalwareMustDie. *MMD-0036-2015 - KINS (or ZeusVM) v2.0.0.0 Tookit (Builder & Panel Source Code) Leaked.* 5 juil. 2015. URL : https://blog.malwaremustdie.org/2015/07/mmd-0036-2015-kins-or-zeusvm-v2000.html.

[50] Kaspersky. *Trojan-Banker.Win32.Chthonic*. Mar. 2016. URL : https://threats.kaspersky.com/fr/threat/Trojan-Banker.Win32.Chthonic/.

[51] FireEye. *Fake Software Update Abuses NetSupport Remote Access Tool*. 5 avr. 2018. URL : https://www.fireeye.com/blog/threat-research/2018/04/fake-software-update-abuses-netsupport-remote-access-tool.html.

[52] SocPrime. *Spelevo Exploit Kit Spreads IcedID and Dridex Trojans*. 1er juil. 2019. URL : https://socprime.com/en/news/spelevo-exploit-kit-spreads-icedid-and-dridex-trojans/.

[53] Le pouvoir clapratique. "Inside a ZeuS botnet". 2015. In : *Le pouvoir clapratique* (2015).

[54] Comodo. *What Is Zeus Malware ?* 31 juil. 2018. URL : https://enterprise.comodo.com/blog/what-is-zeus-malware/.

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

[56] LeMondeInformatique. *Forte montée des attaques ciblées via le malware Zeus*. 27 mai 2013. URL : https://www.lemondeinformatique.fr/actualites/lire-forte-montee-des-attaques-ciblees-via-le-malware-zeus-53727.html.

[57] Reuters. "Analysis : Top Hacker "Retires"; Experts Brace for His Return". 29 oct. 2010. In : *Reuters* (29 oct. 2010).

[58] United States District Court for the District of Nebraska. *Criminal Complaint*. 13 juil. 2012.

[59] Krebs on Security. *Inside 'Evil Corp,' a $100M Cybercrime Menace*. 16 déc. 2019. URL : https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/.

[60] Twitter. *@Dridex BOT*. 10 déc. 2015. URL : http://archive.vn/SoHYv.

[61] Twitter. *@MalwareTech*. 4 avr. 2016. URL : http://archive.vn/Zw5MD.

[62] Twitter. *@Dridex BOT*. 14 déc. 2015. URL : https://twitter.com/dridexbot/status/676353569180774400.

[63] Twitter. *@Dridex BOT*. 17 déc. 2015. URL : https://twitter.com/dridexbot/status/677561943171952641.

[64] Twitter. *@Dridex BOT*. 14 déc. 2015. URL : https://twitter.com/dridexbot/status/676355038441299968.

[65] Twitter. *@Dridex BOT*. 16 déc. 2015. URL : https://twitter.com/dridexbot/status/677205919630024704.

- 25/05/2020


**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