TLP:WHITE

ÉVOLUTION DE L'ACTIVITÉ DU GROUPE CYBERCRIMINEL TA505

22/06/2020

TLP:WHITE

Sommaire

1 TA505 de 2014 à 2017

L'activité du mode opératoire TA505 remonterait à au moins 2014 mais c'est seulement en juillet 2017 que la première mention publique de TA505 fait son apparition sur Twitter. Jusqu'en 2017, son activité semble se concentrer sur la distribution de chevaux de Troie bancaires et de rançongiciels [1].

1.1 Codes malveillants distribués

1.1.1 Chevaux de Troie bancaires

En matière de charge finale, TA505 fait usage depuis ses débuts de chevaux de Troie bancaires répandus qui ne lui sont pas propres, tels que Dridex et Trickbot :

Dridex

TA505 aurait propagé le code malveillant **Dridex** [2] à partir de juillet 2014, soit un mois après sa création (juin 2014) [1]. Son utilisation de botnets ID[1] spécifiques au sein du réseau de botnets Dridex, contrôlé par le groupe cybercriminel Evil Corp, laisse à penser que TA505 a été un affilié de Dridex de 2014 à 2017. Les botnets ID utilisés par TA505 entre 2014 et 2015 auraient été les botnets ID 125, 220 et 223. Le botnet 220 aurait contenu 9650 bots en avril 2015 [3], et aurait principalement ciblé des banques [4], notamment en France. En 2016, TA505 se serait très majoritairement concentré sur l'utilisation du rançongiciel Locky, au détriment du code malveillant Dridex, puis aurait repris la propagation de Dridex en 2017 au travers des botnets ID 7200 et 7500. TA505 a finalement cessé définitivement l'utilisation de Dridex courant 2018 [5].

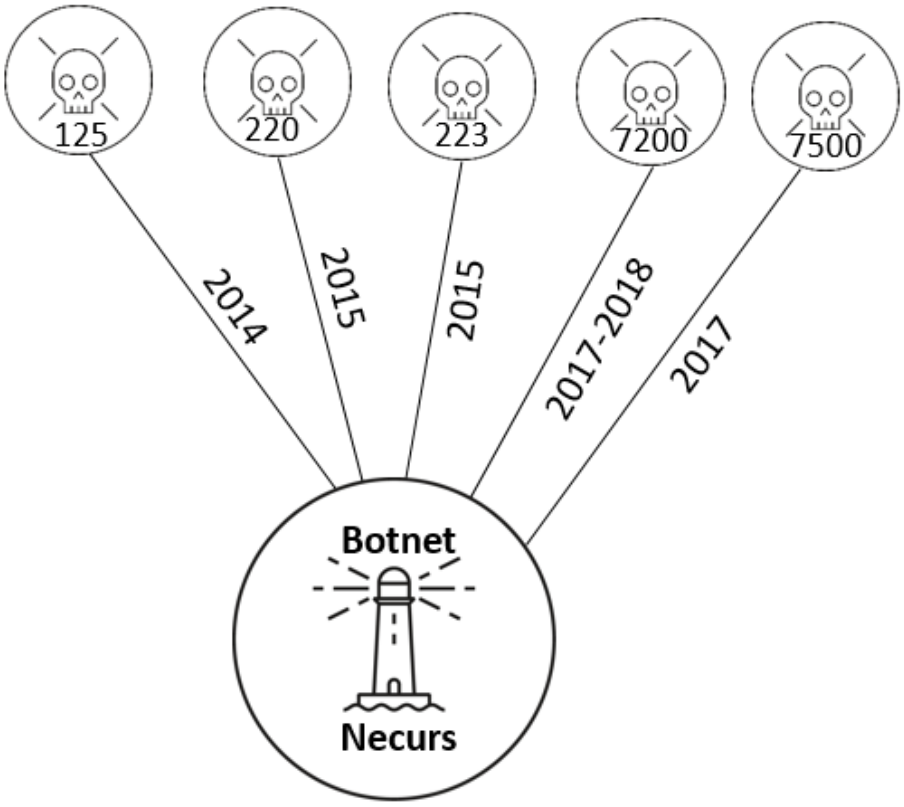

Fig. 1.1 : Botnets ID Dridex correspondant à TA505

[1] 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.

TrickBot

TA505 aurait également été un affilié de TrickBot[2], connu sous le pseudonyme *mac1* [5]. L'utilisation de **TrickBot** par TA505 n'aurait duré que quelques mois en 2017. Par exemple, une campagne datant de juin 2017 a ciblé la France et le Royaume-Uni [5].

1.1.2 Rançongiciels

En 2016, le rançongiciel **Locky** fait son apparition. Très utilisé, il fait de nombreuses victimes. De la même manière que **Dridex**, **Locky** fonctionne sur le principe d'un modèle d'affiliés [1].

D'après Proofpoint, l'affilié numéro 3 de **Locky** et l'affilié du botnet **Dridex** ID 220, alors TA505, auraient des points communs, tels que des leurres similaires au niveau de leurs courriels d'hameçonnage ainsi que de fortes similitudes au niveau des codes Javascript, VBScript et macros Microsoft Word utilisés [7]. Il est également à noter une absence de campagnes **Dridex** 220 concomitantes à l'émergence de Locky [8]. Proofpoint [7] dresse également des liens entre **Locky** et l'affilié du botnet **Dridex** ID 7200, alors TA505, comparant des campagnes **Dridex** de 2017 à des campagnes **Locky** passées [1]. Ainsi, TA505 serait l'affilié numéro 3 (« Affid=3 ») de ce rançongiciel.

Bien que le principal rançongiciel utilisé par le groupe demeure **Locky**, TA505 aurait pratiqué un usage ponctuel d'autres rançongiciels (**Bart**[3], **Jaff**[4], **Scarab** [5], **Philadelphia**[6], **GlobeImposter**[7] et **GandCrab**[8]).

L'activité de Locky cesse en 2017.

1.2 Méthodes de distribution et compromission

TA505 semble avoir procédé à la distribution de ses charges malveillantes uniquement par campagnes de courriels d'hameçonnage. Ce mode opératoire se distingue à cette époque par son recours massif au botnet Necurs (voir annexe en chapitre 5) pour la distribution de ses courriels [9].

Commentaire : les rapports en sources ouvertes associent tous les rançongiciels distribués par le botnet Necurs à TA505. Pourtant, certains de ces rançongiciels ont été utilisés sur les mêmes périodes. Il semble peu vraisemblable que TA505 ait opéré simultanément d'aussi nombreux codes de chiffrement. Il est plus probable que Necurs ait eu plusieurs clients simultanément.

Ce mode opératoire s'appuie exclusivement durant cette période sur de l'ingénierie sociale pour faire exécuter ses charges contenues dans des pièces jointes malveillantes liées aux courriels envoyés [9]. Ces pièces jointes pouvaient notamment être des archives zip ou 7zip contenant des scripts VBS ou Javascript à faire exécuter par ses victimes, des pages HTML contenant du Javascript malveillant, ou des documents Office piégés via macros malveillantes.

Bien que TA505 ne semble avoir eu recours à aucune vulnérabilité logicielle pour compromettre ses cibles, il est intéressant de constater qu'il s'est tenu au courant des dernières techniques d'ingénierie sociale découvertes. Ainsi, il a distribué des documents Office piégés via le mécanisme DDE moins d'un mois après que le potentiel d'abus de cette fonctionnalité ait été largement médiatisé [10].

[2] **Trickbot**, apparu en octobre 2016, serait un dérivé de **Dyre**, possiblement opéré par des membres du Business Club jusqu'en novembre 2015. Pour rappel, le Business Club a été à l'origine des codes malveillants JabberZeuS et GameOverZeuS (GoZ). Lors du démantèlement du botnet GoZ, le Business Club aurait scindé ses activités entre les codes malveillants Dridex et Dyre. **Trickbot** pourrait donc être opéré par d'anciens membres du Business Club, ou par un *copycat* ayant acquis le code source de **Dyre** [6].
[3] Rançongiciel dont l'usage a été très limité courant 2016.
[4] Rançongiciel actif de mai à juin 2017.
[5] Variante du premier rançongiciel open-source **Hidden Tear** (publié en 2015), utilisé pour la première fois par TA505 en juin 2017.
[6] *Ransomware-as-a-Service* disponible pour 400 dollars sur le Dark Web.
[7] Rançongiciel utilisé de juillet à décembre 2017. 24 campagnes distribuant **GlobeImposter** ont été comptabilisées par Proofpoint en décembre 2017 [9, 5]
[8] *Ransomware-as-a-Service* utilisé de janvier à mars 2018 [5]

2 Evolution de TA505 depuis 2018

L'année 2018 marque un tournant dans les méthodes d'attaque du mode opératoire. TA505 diminue alors graduellement sa distribution de codes malveillants bancaires et rançongiciels pour passer à la distribution de portes dérobées.

Cependant, le mode opératoire ne semble pas non plus se contenter d'exécuter une charge sur le poste de sa victime. En effet, s'il le juge d'intérêt, TA505 tente alors de compromettre l'intégralité du système d'information (SI) dans lequel il a pénétré.

Il semble également, dans certains cas, revendre les accès aux portes dérobées qu'il a installées, ce qui rend complexe la distinction entre les activités spécifiques à TA505 et celles de ses potentiels clients.

La chaîne d'attaque décrite dans ce chapitre correspond aux activités que l'ANSSI pense liées au mode opératoire.

2.1 Vecteur d'infection

L'unique vecteur d'infection pour l'instant connu du mode opératoire TA505 demeure le courriel d'hameçonnage incluant une pièce jointe ou un lien malveillant. Jusqu'en 2018, le mode opératoire s'appuyait quasi-exclusivement sur le botnet Necurs pour distribuer ses charges. Cependant, suite à l'indisponibilité du botnet en janvier et février 2018, TA505 semble avoir moins souvent recours à ses services [9].

Ce dernier point est cependant incertain car peu d'informations existent sur les méthodes de distribution de courriel alternatives du mode opératoire. Étant donné que TA505 a, à plusieurs reprises, déployé un implant de vols d'identifiants de messagerie chez ses victimes [11][12], il est possible que ce dernier accumule des adresses courriel compromises pour distribuer ses nouvelles campagnes d'hameçonnage.

Il a également été mentionné que certains de ses courriels d'hameçonnage avaient été distribués via des machines infectées par le code malveillant **Amadey** [11]. Etant donné que TA505 utilise également le code malveillant **Amadey**, comme indiqué en section 2.3.1, il est possible que ce dernier se constitue son propre botnet Amadey pour distribuer ses courriels malveillants, ou qu'il loue les services d'un botnet Amadey déjà existant.

Ce mode opératoire usurpe également les adresses d'envoi de ses courriels, ce qui rend difficile l'analyse de son infrastructure de distribution de courriels [13].

2.2 Ingénierie sociale

Le mode opératoire continue de s'appuyer sur de l'ingénierie sociale pour exécuter ses charges malveillantes sur les machines des destinataires de ses courriels, utilisant de nombreux formats de fichiers de pièces jointes pour contourner les systèmes de sécurité de ses cibles : .url [14], .iqy [9], SettingContent-ms [15], MS publisher files [16], .wiz et .pub [17], .iso [18]. Le but de ces documents était souvent d'exécuter via des macros des commandes msiexec[9] sur la machine de la victime pour télécharger et exécuter un code malveillant.

Cependant, au cours du deuxième semestre 2019 et premier semestre 2020, TA505 semble avoir modifié et stabilisé sa méthode d'ingénierie sociale. Ce mode opératoire envoie maintenant comme pièce jointe une page HTML contenant du code Javascript malveillant. Ce dernier redirige la victime vers une URL d'un site légitime mais compromis.

Cette même URL correspond à une page HTML contenant un code Javascript minimal redirigeant la victime vers une page hébergée par une machine contrôlée par le mode opératoire. Cette page imite celle d'un site légitime

[9] Outil permettant d'interagir en ligne de commande avec le moteur d'installation, de mise à jour et de désinstallation de logiciels propres aux systèmes d'exploitation de Microsoft

de partage de fichiers adapté à la cible tel que Onedrive, Dropbox [19] ou Naver[10] (lors d'une de ses campagnes en Corée du Sud) [20]. La victime est alors incitée à télécharger, ouvrir et activer les macros VBA d'un document Office, généralement Excel, contenant une charge malveillante.

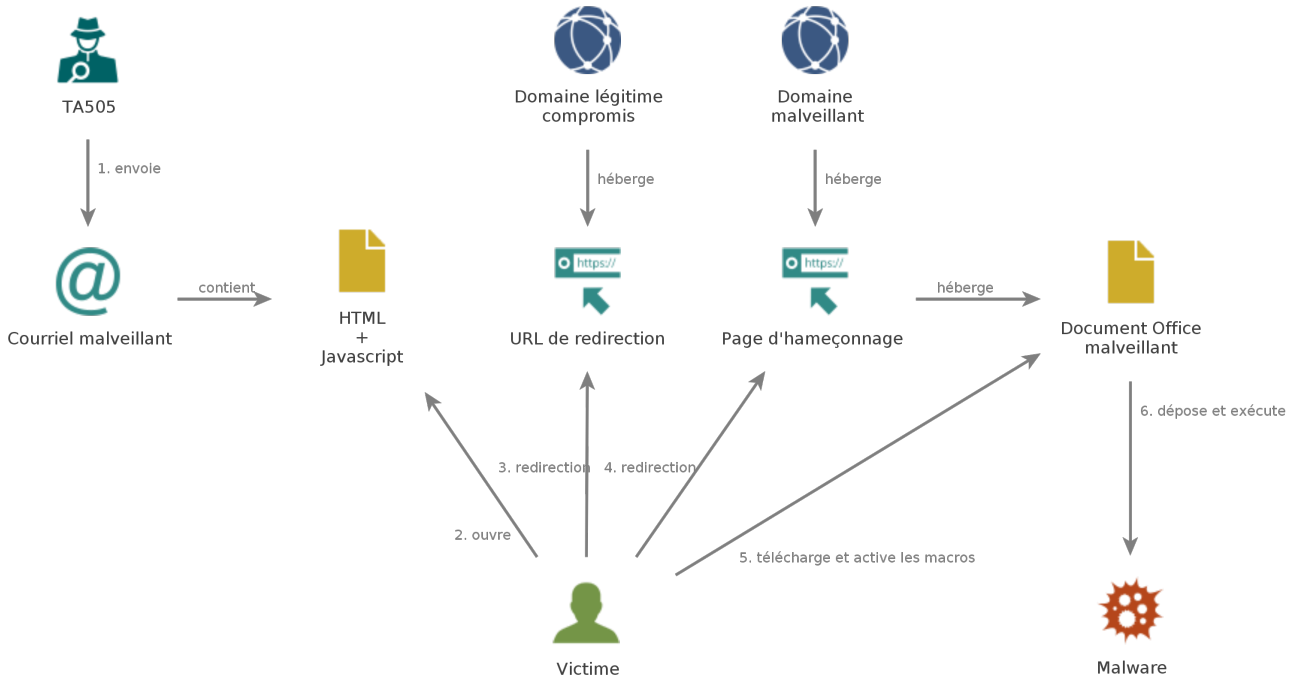

Fig. 2.1 : Méthode de compromission initiale de TA505

Le mode opératoire augmente graduellement la complexité de sa méthode d'ingénierie sociale. En octobre 2019, ce dernier envoyait directement des liens vers ses pages d'hameçonnage dans ses courriels malveillants. Il a ensuite eu recours à des raccourcisseurs d'URL pour masquer ces liens malveillants.

En fin de février 2020, il a abandonné la stratégie des raccourcisseurs d'URL et a commencé à utiliser des pièces jointes HTML avec Javascript avec une redirection depuis un site compromis, ce qui complique encore la détection de ses courriels. De plus, certaines de ses pages de redirection intègrent un lien vers iplogger.org, un service permettant au mode opératoire d'inspecter les adresses IP venant visiter ces pages [21].

Enfin, il a déjà été observé que les pages d'hameçonnage du mode opératoire distribuaient des documents Office vides lorsqu'une personne autre que la victime les visitait. Ce comportement peut s'expliquer par le fait que le mode opératoire filtre les adresses IP auxquelles il choisit de distribuer ses documents piégés ou qu'il ne distribue ses documents malveillants que dans des plages de temps restreintes.

2.3 Compromission initiale

TA505 dispose d'un arsenal d'attaque varié à déployer chez les victimes ayant exécuté ses pièces jointes malveillantes. Il est composé de codes aussi bien disponibles publiquement que commercialement sur le marché noir, ou qui semblent lui être exclusifs. Il dispose donc de capacités de développement ou des ressources financières pour s'en procurer. Le mode opératoire déploie son arsenal en plusieurs étapes et dispose de codes différents pour chacune d'entre elles.

[10] Service de portail Internet coréen.

2.3.1 Codes de premier niveau

Le mode opératoire TA505 semble avoir expérimenté plusieurs codes de premier niveau[11]. Il a ainsi brièvement utilisé les codes suivants :

- **Quant Loader** est un simple code de téléchargement disponible à bas prix sur le marché noir. Le mode opératoire y a eu recours de janvier à avril 2018 [9].
- **Marap** est un code de téléchargement qui semble spécifique au mode opératoire. Bien que construit de façon modulaire et disposant d'un module de reconnaissance connu, peu d'attaques faisant appel à ce code ont été documentées et le mode opératoire semble avoir cessé de l'utiliser depuis août 2018 [22].
- **Amadey** est un code de téléchargement disponible sur le marché noir. Ce code aurait été utilisé de avril à juin 2019 par le mode opératoire [23].
- **Andromut**, aussi connu sous le nom de **Gelup**, est un code de téléchargement qui semble spécifique au mode opératoire. Ce code se distingue des précédents par la mise en place de mécanismes d'anti-analyse. Toutefois, aucune occurrence de ce code ne paraît avoir été détectée en dehors de l'été 2019 [24].

Le mode opératoire TA505 ne semble donc pas hésiter à mettre de côté certains de ses codes d'attaque pour en tester d'autres. Malgré cela, une tendance se dégage : il semble utiliser de façon plus régulière le code malveillant de premier niveau **Get2**, dont la composante porte dérobée est également appelée **Friendspeak** [13]. Depuis la première publication sur ce code malveillant en septembre 2019 [19], le mode opératoire y a régulièrement eu recours.

Get2 effectue une reconnaissance basique de la machine qu'il infecte en envoyant à son serveur C2 des informations telles que le nom de la machine infectée, le nom de l'utilisateur, la version du système d'exploitation Windows et une liste des processus actifs sur la machine. Il reçoit en retour, si la machine est jugée d'intérêt, l'URL à laquelle il peut télécharger le code malveillant de niveau supérieur.

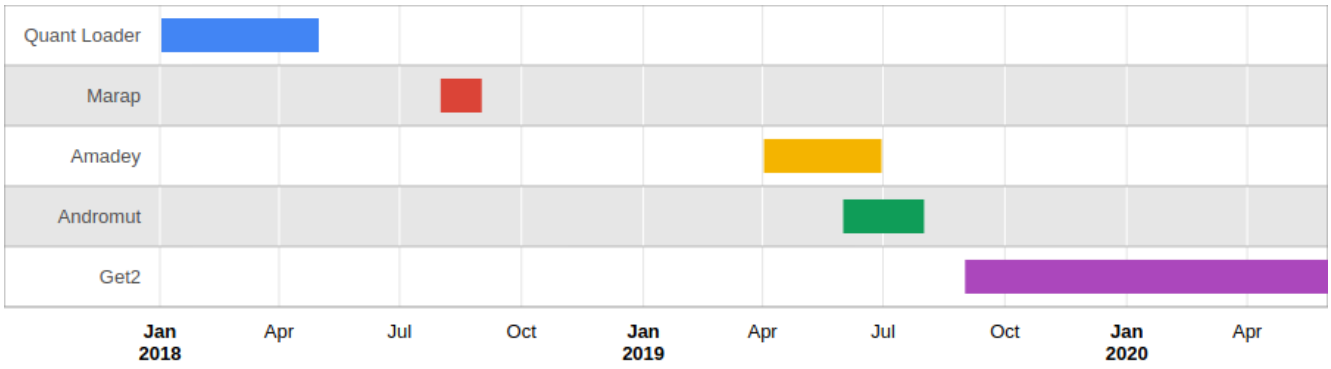

Fig. 2.2 : Frise chronologique d'utilisation de codes de niveau 1 par TA505

2.3.2 Codes de deuxième niveau

Une fois son code de premier niveau déployé, le mode opératoire peut déployer plusieurs codes malveillants.

- Le code malveillant **FlawedAmmyy** existe depuis 2016 et est construit à partir du code source publiquement divulgué de l'outil légitime d'administration à distance Ammyy Admin. Bien que disposant de fonctionnalités de RAT[12], **FlawedAmmyy** a également été utilisé par le mode opératoire comme code de premier niveau. Le mode opératoire y aurait eu recours entre mars 2018 et septembre 2019 [18]. **FlawedAmmyy** semble être exclusivement utilisé par TA505 depuis 2018. Cependant, cette porte dérobée a aussi été utilisée avant cette période, alors que TA505 n'utilisait pas encore ce type de code. Il n'est donc pas entièrement établi que **FlawedAmmyy** soit exclusif à TA505.

[11] Un code de premier niveau, aussi connu sous la dénomination *Stage-1*, est défini ici comme un implant aux fonctionnalités restreintes dont le but est de déployer un code plus sophistiqué et éventuellement de faire une reconnaissance rapide du système infecté pour aider le mode opératoire à déterminer si la victime et son SI sont intéressants.

[12] *Remote Administration Tool* ou outil d'administration à distance.

- Le code malveillant **tRat** a été utilisé par TA505 en octobre 2018 [16]. Peu d'informations sont disponibles sur cette porte. En effet, ce dernier nécessite de télécharger des modules pour acquérir des fonctionnalités, or aucun de ses modules n'a été documenté.
- Remote Manipulator System, également appelé RMS ou RmanSyS, est un outil légitime développé par l'entreprise russe TEKTONIT, détourné pour être utilisé à des fins malveillantes. Cet outil est disponible gratuitement à des fins non commerciales et des versions corrompues sont également disponibles sur le marché noir. TA505 aurait commencé à déployer cet outil à partir de novembre 2018, et ce jusqu'à juin 2019 [25].
- La porte dérobée **ServHelper** existe en deux versions [17] : une version sert de code de premier niveau, l'autre dispose de fonctionnalités de RAT. Le mode opératoire aurait utilisé cette porte dérobée sur une période couvrant au moins novembre 2018 à août 2019 [18]. **ServHelper** ne semble pas spécifique au mode opératoire : plusieurs chercheurs en sécurité informatique ont ainsi observé des attaques l'incluant mais employant également des méthodes et outils différents de ceux de TA505 [26][18][27].
- **FlawedGrace**, également connue sous le nom de **Gracewire**, est une porte dérobée disposant de fonctionnalités standards de RAT. Elle a été mentionnée comme utilisée pour la première fois par TA505 en décembre 2018 [17] et serait toujours utilisée par ce dernier en 2020 [28]. A l'instar de **FlawedAmmyy**, TA505 semble pour l'instant être le seul à utiliser cette porte dérobée. Cependant, son existence antérieure à 2018 rend son usage exclusif par TA505 incertain.
- La porte dérobée **FlowerPippi** a été détectée une fois en juin 2019 [11]. Ce code malveillant dispose de fonctionnalités basiques de RAT et est également prévue pour être utilisé comme un code de premier niveau en faisant une reconnaissance initiale du système infecté.
- **SDBbot** est un code malveillant apparemment spécifique au mode opératoire. Sa première utilisation a été relevée en septembre 2019 [20] et le mode opératoire n'a pas cessé de l'utiliser depuis.

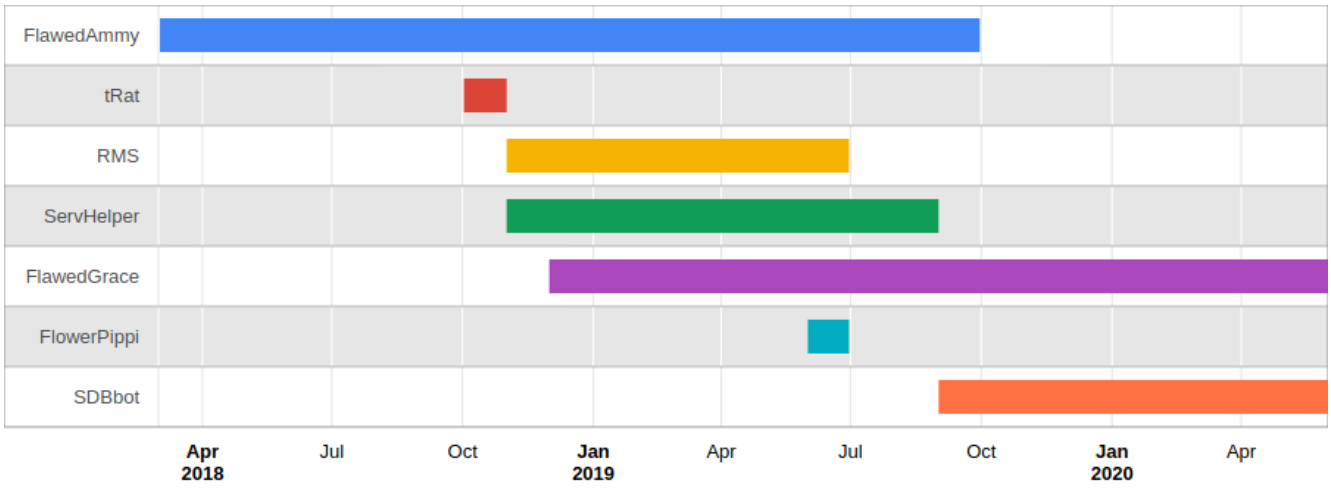

Fig. 2.3 : Frise chronologique d'utilisation de codes de niveau 2 par TA505

2.4 Compromission du système d'information

Une fois ses codes installés, le mode opératoire peut chercher à se latéraliser au sein du réseau compromis. Son objectif est alors de devenir administrateur de domaine. Pour arriver à ses fins, il emploie plusieurs méthodes.

2.4.1 Exploration du SI

Le mode opératoire scanne le réseau pour collecter plus d'informations sur le SI et découvrir des services vulnérables [29]. Un des outils utilisés par TA505 est la suite d'outils PowerSploit, un ensemble de scripts PowerShell

disponibles en source ouverte utilisés pour tester la sécurité d'un réseau informatique. Il s'intéresse particulièrement à l'*Active Directory* du SI et a déjà déployé par le passé un autre outil de test de pénétration, PingCastle, pour établir un diagnostic des failles de configuration affectant ce service.

Bien que cruciales pour sa prise de contrôle du réseau, le mode opératoire ne semble pas nécessairement mener en premier ces opérations. Dans plusieurs cas de figure observés, le mode opératoire semble d'abord chercher à compromettre plusieurs autres machines avant de scanner le SI et l'*Active Directory*.

Le mode opératoire semble continuer son travail de cartographie du réseau après avoir compromis les informations d'authentification d'un administrateur de domaine. En effet, il a déjà été observé que TA505 utilisait le logiciel de requête d'*Active Directory* nommé AdFind sur un contrôleur de domaine pour cartographier intégralement un SI dont il était passé administrateur de domaine.

2.4.2 Élévation de privilèges

La méthode privilégiée par TA505 pour augmenter ses privilèges et se latéraliser dans un réseau semble être la collecte d'informations d'authentification sur les machines compromises. L'outil de collecte Mimikatz, disponible gratuitement en source ouverte, est régulièrement utilisé par le mode opératoire et il n'est pas à exclure qu'il ait utilisé d'autres outils de ce type. Des hypothèses, non confirmées à ce stade, ont également été formulées sur l'utilisation de la vulnérabilité MS17-010[13] par le mode opératoire [29].

2.4.3 Latéralisation

Pour faciliter ses opérations de latéralisation et pour augmenter sa persistance au sein du réseau compromis, le mode opératoire a très fréquemment recours au logiciel de test de pénétration Cobalt Strike et à l'outil TinyMet[14]. Cependant, TA505 utilise également souvent des outils natifs de Windows tels que WMIC et RDP pour exécuter ses codes malveillants sur de nouvelles machines en utilisant des identifiants volés.

2.5 Actions sur objectif

2.5.1 Chiffrement du SI

Le but principal du mode opératoire est de déployer un rançongiciel. L'utilisation de rançongiciels par ce mode opératoire remonte à au moins 2016 avec son emploi du code malveillant **Locky**.

Les évolutions majeures depuis 2018 résident dans le fait que TA505 cherche désormais à compromettre par rançongiciel des entités à même de payer une rançon de montant élevé (*big game hunting*) et à chiffrer toutes les machines du SI compromis.

Lors des attaques associées à TA505, le rançongiciel **Clop**, également appelé **Ciop**, a été déployé. Ce code malveillant a été observé pour la première fois en février 2019 [20]. Il est dépourvu de fonctionnalités de propagation automatique. Par conséquent, le mode opératoire utilise certains outils spécifiques pour le déployer à l'échelle d'un parc informatique entier. Il exécute via un script un code malveillant, peu documenté en source ouverte mais jusqu'ici nommé systématiquement « `sage.exe` » par le mode opératoire, sur plusieurs machines [29]. Ces machines se connectent alors à l'ensemble des machines du SI victime pour exécuter sur chacune d'entre elles successivement deux charges avec un compte d'administrateur de domaine :

- un code malveillant nommé **DeactivateDefender** dont le but est précisément de désactiver Windows Defender [20][29] ;
- le rançongiciel lui-même.

[13] Vulnérabilité critique dans le service SMB (*Server Message Block*) des machines Windows. Cette vulnérabilité a été exploitée lors de la campagne mondiale WannaCry en 2017.

[14] Cet outil, librement disponible en source ouverte, est un code de chargement de taille particulièrement réduite permettant de télécharger et d'exécuter l'outil de test de pénétration Meterpreter.

Il est probable que TA505 s'appuie sur les cartographies effectuées au cours de la compromission graduelle du SI pour choisir les machines sur lesquelles « `sage.exe` » sera exécuté et maximiser l'impact de son rançongiciel.

Une occurrence d'utilisation du rançongiciel **Rapid** par TA505 a été également été constatée par l'Institut de sécurité financière sud-coréen (FSI) [20] en décembre 2019.

2.5.2 Chantage

Un site Internet a été créé en mars 2020 afin de publier les données exfiltrées de victimes du rançongiciel **Clop** qui n'auraient pas payé leur rançon, probablement afin d'ajouter une pression supplémentaire sur les futures victimes. Un communiqué y a également été publié par les attaquants stipulant qu'au cas où un hôpital soit malencontreusement victime de leur rançongiciel, le déchiffreur des données lui serait immédiatement fourni. Si, comme supposé en section 2.5.3, **Clop** est spécifique à TA505, cela illustre la capacité de ce mode opératoire à suivre une tendance initiée par d'autres opérateurs de rançongiciels [30].

Cette tendance est également intéressante car elle indique que le mode opératoire est obligé d'exfiltrer des données du SI de sa victime. Si ces données dépassent un certain volume, il est alors probable que le mode opératoire soit obligé de déployer des outils et de l'infrastructure spécifiques à cette mission. De tels signes n'ont pour l'instant pas été observés à propos de ce mode opératoire.

2.5.3 Spécificité de Clop à TA505

L'ANSSI avait évoqué un lien technique entre le rançongiciel **Clop** et TA505. En effet, **Clop** et **FlawedAmmyy** avaient été signés par le même certificat de sécurité valide mais malveillant [31].

On peut également ajouter à cette observation le fait que ces deux codes malveillants ont été compilés dans des environnements similaires et modifiés simultanément pour changer dans leurs chaînes de caractères la lettre « `l` » en « `i` » majuscule [20]. De plus, ils ont porté le même nom caractéristique « `swaqp.exe` » lors d'attaques distinctes.

Il parait donc probable qu'un unique mode opératoire manipule ces deux codes. Etant donné que TA505 est le seul qui a été observé y avoir eu recours depuis 2018, il semble que ces deux codes lui soient spécifiques.

2.6 Méthodes d'évasion

Le mode opératoire multiplie les stratégies pour minimiser la détection de ses codes malveillants. Au delà de l'utilisation de formats de pièces jointes inhabituels mentionnés en section 2.2, TA505 utilisait également des macros de type Excel 4.0. Ces macros particulièrement anciennes étaient généralement peu détectées par les solutions de sécurité au moment de leur adoption par le mode opératoire. De la même façon, TA505 s'appuie beaucoup sur des outils natifs de Windows, qui demandent une surveillance plus poussée du SI pour que leur utilisation malveillante soit détectée.

2.6.1 Utilisation de codes de compression

TA505 utilise un code de compression[15] pour rendre ces codes malveillants plus difficiles à analyser. Ce code, appelé **Minedoor** [13], a été utilisé pour compresser aussi bien les codes de compromission initiale du mode opératoire tels que **FlawedGrace**, que les codes finaux déployés par TA505 tels que **Clop** ou **DeactivateDefender** [32].

Bien que ce code de compression constitue un moyen de suivi intéressant de l'arsenal de TA505, il convient d'être prudent. Des attaques utilisant des codes protégés par **Minedoor** aux chaînes de compromission très différentes de celle de TA505 ont déjà été observées [13]. Il semble donc que ce code ne soit pas propre à TA505.

[15] Appelé *packer*.

2.6.2 Utilisation de binaires signés

Le mode opératoire signe ses codes malveillants en utilisant des certificats de sécurité légitimes mais malveillants. Ces derniers usurpent souvent des noms d'entreprises existantes. Les codes de TA505 deviennent donc plus difficiles à détecter [20].

A l'instar du code malveillant **Minedoor**, il n'est pas certain que l'ensemble des codes malveillants signés par les certificats utilisés par TA505 soient liés à ce mode opératoire. En effet, il est possible que TA505 ait eu recours à un intermédiaire pour lui signer ses codes et que cet intermédiaire réutilise ces certificats pour signer les codes malveillants d'autres modes opératoires.

2.7 Infrastructure d'attaque

Comme mentionné en section 2.1, l'infrastructure utilisée par le mode opératoire pour distribuer ses courriels est peu documentée.

TA505 semble particulièrement recourir à de l'infrastructure louée pour mener à bien ses opérations, notamment pour héberger ses documents Office piégés et pour ses serveurs C2[16] **Get2**. La durée de vie de cette infrastructure est généralement de moins d'un mois et le mode opératoire génère en permanence de nouveaux noms de domaine. Ces noms de domaine sont souvent composés de plusieurs mots séparés d'un « - » et cherchent généralement à typosquatter[17] des services de partage de fichier tels que Onedrive ou Onehub par exemple.

TA505 emploierait une stratégie différente pour les serveurs C2 de ses outils de pénétration comme TinyMet ou Cobalt Strike. Il utilise ainsi directement des adresses IP comme serveur C2 et non plus des noms de domaine, mais s'appuie toujours sur de l'infrastructure louée.

Peu d'informations sont disponibles sur l'infrastructure compromise par le mode opératoire. Une analyse a été faite de serveurs web compromis par le mode opératoire en février 2019 [20], indiquant que plusieurs exemplaires de la console web malveillante **Filesman** avaient été retrouvés ainsi qu'une porte dérobée Linux non documentée.

2.8 Ciblage

Bien qu'elles ne représentent qu'une fraction de l'activité véritable du mode opératoire, le tableau ci-dessous présente un ensemble de campagnes menées par TA505, documentées en source ouverte depuis 2018.

Période	Zone géographique ciblée	Secteur ciblé	Source
Janvier 2018	N/A	Industrie automobile	[14]
Aout 2018	N/A	Financier	[22]
Septembre-Octobre 2018	N/A	Financier	[33]
Novembre 2018	N/A	Financier Vente	[17]
Décembre 2018	N/A	Financier Vente	[17]
Novembre-Décembre 2018	États-Unis	Industrie alimentaire Distribution Vente Restauration	[34] [35]
Décembre 2018 – Mars 2019	Chili, Inde, Italie, Malawi, Pakistan, Afrique du Sud, Corée du Sud, Chine, Royaume-Uni, France, États-Unis	Financier Hotellerie	[25]
Février 2019	Corée du Sud	N/A	[20]

[16] Serveurs de commande et contrôle : ces machines sont utilisées pour envoyer des instructions à des codes malveillants et recevoir leurs résultats.
[17] Présenter de fortes similarités à un autre nom de domaine à des fins trompeuses.

Période	Zone géographique ciblée	Secteur ciblé	Source
Avril 2019	N/A	Financier	[36]
Avril 2019	Chili, Mexique, Italie, Chine, Corée du Sud, Taïwan	N/A	[23]
Juin 2019	Émirats Arabes Unis, Corée du Sud, Singapour, États-Unis, Arabie Saoudite, Maroc	N/A	[11]
Juin-Juillet 2019	États-Unis, Bulgarie, Turquie, Serbie, Inde, Philippines, Indonésie	Banques	[19] [18] [11]
Juin 2019	Japon, Philippines, Argentine	N/A	[11]
Juillet-Aout 2019	Arabie Saoudite, Oman	Agences gouvernementales	[18]
Juillet-Aout 2019	Turquie	Agences gouvernementales Education	[18]
Septembre 2019	Canada, États-Unis	N/A	[19]
Septembre 2019	Grèce, Singapour, Émirats Arabes Unis, Géorgie, Suède, Lituanie	Financier	[19] [18] [37] [11]
Octobre 2019	Royaume-Uni, France, États-Unis	Financier, Santé, Vente, Education Recherche	[19]
Décembre 2019	Corée du Sud	N/A	[20]
Décembre 2019	Allemagne, Pays-Bas	Education	[38]
Janvier-Mars 2020	États-Unis	Pharmaceutique Santé Vente	[28] [19]

Le secteur financier était la cible exclusive du mode opératoire avant 2018 et en est restée une cible régulière depuis.

TA505 a cependant depuis progressivement élargi sa victimologie vers de nombreux autres secteurs.

D'un point de vue géographique, tous les continents sont ciblés par ce mode opératoire. Un point d'intérêt est l'attention particulière que TA505 semble porter à la Corée du Sud. Cet intérêt pourait être lié au fait que ce mode opératoire aurait pu travailler en lien avec le mode opératoire Lazarus comme indiqué dans le chapitre 3.

3 Liens avec d'autres groupes d'attaquants

3.1 Clientèle

Au vu de son arsenal varié, du champ étendu de ses cibles, de ses campagnes parfois massives, parfois ciblées, il est possible que TA505 soit un *hacker-for-hire* c'est-à-dire un prestataire de service en compromission et qualification d'accès au sein de SI. Ses clients lui fourniraient une liste de cibles potentielles, que TA505 essaierait de compromettre, pour ensuite vendre ces accès compromis ou qualifiés réalisés aux clients.

Au moins deux clients potentiels ont pu être identifiés par des éditeurs : le mode opératoire d'attaque (MOA) Lazarus réputé lié à des intérêts nord-coréens en sources ouvertes, et le groupe Silence [39].

3.1.1 Lazarus

La présence simultanée de Lazarus et de TA505 aurait déjà été constatée par différentes sources. Début janvier 2018, le CERT vietnamien a publié une alerte relative à des attaques ciblant le secteur financier, mêlant des indicateurs de compromission attribués à des MOA réputés liés à des intérêts nord-coréens en sources ouvertes à d'autres attribués à TA505 [40]. D'après Lexfo, des IOCs trouvés simultanément sur des réseaux de banques, ainsi que des scripts Powershell, attribués à TA505 et à Lazarus semblent similaires [41].

En outre, le ciblage privilégié de la Corée du Sud par TA505 pourrait illustrer la commande d'un client final tel qu'un MOA réputé lié en sources ouvertes à des intérêts nord-coréens.

3.1.2 Silence

Il existe des liens de codes et d'infrastructure entre **FlawedAmmyy** et **Truebot** (aka **Silence.Downloader**), outil d'administration à distance propre à Silence[18]. Selon l'éditeur Group-IB, **FlawedAmmyy.downloader** et **Truebot** auraient été développés par le même individu [42]. De plus, Silence aurait attaqué au moins une banque en Europe en passant par TA505 pour compromettre son SI [43].

Commentaire : Si Silence fait bien appel à TA505 pour la compromission initiale, il s'agirait d'un changement de TTPs, Silence étant, depuis ses débuts en 2016, autonome en matière d'envois de courriels d'hameçonnage et de compromission initiale.

3.2 FIN7

D'après l'Institut de sécurité financière sud-coréen (FSI) [20], il existe des similitudes entre TA505 et le groupe cybercriminel FIN7, héritier de Carbanak et dorénavant spécialisé dans le vol de données de cartes bancaires. Les deux groupes :

- partageraient des adresses IP de serveurs C2 communes ;
- utiliseraient **FlawedAmmyy**, Cobalt Strike et TinyMet (BabyMetal pour FIN7) ;
- utiliseraient des *batch script* pour faire de la reconnaissance interne ;
- se latéraliseraient par le biais du protocole RDP et de PSExec ;
- utiliseraient Shim Database (SDB) de la même manière. Cette particularité est également soulignée par Proofpoint [19].

Commentaire : à défaut de similitudes, FIN7 et TA505 pourraient en fait collaborer. En effet, il semble que le FSI ait observé qu'une chaîne d'infection en adéquation avec celles de TA505 déployait des codes malveillants ciblant des terminaux de point de vente (PoS systems), appartenant à FIN7.

[18] Groupe cybercriminel russophone spécialisé dans la compromission de distributeurs automatiques de billets à des fins de retraits frauduleux [39].

4 Conclusion

Malgré l'ampleur de son activité en tant qu'affilié de **Dridex** et **Locky**, TA505 n'a été identifié en tant que tel qu'en 2017, concomitamment à ses premières utilisations de portes dérobées.

Souvent confondu avec le groupe cybercriminel Evil Corp (opérant le botnet Dridex et le rançongiciel BitPaymer), et parfois considéré comme l'opérateur du botnet Necurs, TA505 utilise un arsenal d'attaque évolutif qu'il met en œuvre lors de campagnes variées et parfois simultanées, pouvant porter à confusion sur ses motivations. A ce titre, les liens qu'il présente avec Lazarus et Silence suggèrent que TA505 mènerait en parallèle des campagnes pour son compte et des campagnes pour le compte de sa clientèle.

L'ampleur de ses campagnes depuis 2019, et son ciblage de nombreux secteurs en France, fait de ce mode opératoire une menace particulièrement préoccupante en 2020.

5 Annexe : le botnet Necurs

5.1 Retour sur le botnet Necurs

En 2011, apparaît le botnet Necurs (alias CraP2P) [44].

Deux des modules connus du botnet sont les suivants :

- spam, utilisé par exemple :
  - lors de campagnes de type *pump and dump* (notamment relatives à des cryptoactifs) comme en mars 2017 ;
  - en 2018, lorsque Necurs acquiert un nouveau module *.NET spamming* [45]) ;
  - entre 2016 et 2017, lorsque Necurs a notamment propagé le cheval de Troie bancaire **Kegotip** via aussi bien **The Uprate loader** que **The Rockloader**[19], afin de récupérer les adresses courriels disponibles dans les disques durs et de les utiliser lors de campagnes de spams à venir [47] ;
  - après le démantèlement du botnet Kelihos en 2017, lorsque Necurs aurait récupéré une partie de son activité, consistant notamment en des *dating spam*.
- proxy/DDoS (ajout du module DoS en février 2017) [3].

Le botnet Necurs communique avec ses opérateurs par différents moyens [48] :

- Son mécanisme de communication principal consiste en une liste d'adresses IP et de domaines statiques codés en dur dans l'échantillon du code malveillant Necurs ;
- Si cette méthode n'est pas capable d'obtenir un C2 actif, Necurs utilise son algorithme de génération de domaines (DGA) : la DGA principale produit 2048 domaines C2 possibles tous les 4 jours. Lorsque les opérateurs de Necurs enregistrent un domaine DGA pour informer les bots de l'existence d'un nouveau C2, le domaine ne pointe pas vers la réelle adresse IP du C2. Cette adresse IP est obfusquée avec un algorithme de chiffrement. Tous les domaines sont essayés jusqu'à ce que l'un d'eux soit résolu et réponde en utilisant le protocole correct ;
- Si cette méthode échoue également, le domaine C2 est récupéré sur le réseau P2P.

De plus, l'infrastructure du C2 est divisée en trois niveaux, le dernier étant le *C2 backend*. Ainsi, un système infecté communique avec au moins deux couches de proxy C2 lorsqu'il cherche à communiquer avec le *C2 backend*. La première couche de C2 est constituée de serveurs virtuels privés bon marché de pays comme la Russie ou l'Ukraine tandis que la seconde couche est généralement hébergée en Europe, et parfois en Russie. Il y aurait 11 botnets Necurs, soit 11 *C2 backends*, étroitement contrôlés par un seul groupe [4]. Quatre de ces botnets représenteraient 95% de toutes les infections [48, 49].

5.2 Distribution massive par Necurs

De 2016 à 2019, Necurs aurait été la méthode la plus répandue pour délivrer des spams et des codes malveillants pour le compte de cybercriminels, et aurait été responsable 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 [49].

Entre 2016 et 2017, Necurs distribue principalement les rançongiciels **Locky**, **Jaff** (copy cat de **Locky**, **GlobeImposter**, **Philadelphia**, **Lukitus** et **Ykcol** (variantes de **Locky**) et **Scarab**, ainsi que les chevaux de Troie bancaires **Dridex** et **TrickBot**.

A partir d'août 2018, Necurs commence à réaliser des campagnes d'hameçonnage ciblées à l'encontre d'entités financières, tout en continuant sa propagation massive de codes malveillants (**FlawedAmmyy**, **Quant Loader**, **AZOrult**,

[19] Loader utilisé lors de compromissions afin de notamment propager le rançongiciel **Locky**, **Dridex** 220, **Pony** et **Kegotip** [46].

ServHelper), dont une majorité appartenant à l'arsenal de TA505.

En 2020, Necurs perd des clients au profit d'**Emotet**, qui le remplace dans la distribution de **Dridex** et de **TrickBot** [50], et distribue des campagnes de spams massives du type *get-rich-quick*. Ses infections quotidiennes ont principalement cours en Inde, en Indonésie, en Iran, au Mexique, en Turquie, au Vietnam et en Thaïlande. En France, 4892 infections ont été comptabilisées. [48, 49].

TA505 aurait massivement distribué des codes malveillants via le botnet Necurs au point qu'il peut être envisagé que le groupe opère ce botnet, ou tout du moins qu'il soit en étroite collaboration avec son véritable opérateur.

Commentaire : bien qu'il soit possible que TA505 et l'opérateur du botnet Necurs aient été confondus, il semble que la source ouverte a tendance à attribuer à TA505 l'intégralité des campagnes propagées par Necurs jusqu'à au moins fin 2017 (campagnes de spams de type pump-and-dump et autres escroqueries étant exclues), alors que c'est un gigantesque botnet probablement utilisé par d'autres groupes cybercriminels que TA505. En effet, les propriétaires de botnets, contrôlés à distance, sont souvent en mesure de louer l'accès à des segments de leur botnet sur le marché noir, pour l'envoi de DDoS, de campagnes de spam etc.

6 Bibliographie

[1] Proofpoint. *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 (visité le 03/05/2019).

[2] CERT-FR, "Le Code Malveillant Dridex : Origines et Usages". In : (25 mai 2020).

[3] Bitsight, *Dridex : Chasing a Botnet from the Inside*. 1er jan. 2015.

[4] Bit Sight. *Dridex Botnets*. 24 jan. 2017. URL : https://www.bitsight.com/blog/dridex-botnets (visité le 09/04/2020).

[5] Twitter, "@Kafeine". In : (1er jan. 2019).

[6] Secureworks. *Evolution of the GOLD EVERGREEN Threat Group*. 15 mai 2017. URL : https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group (visité le 24/04/2020).

[7] Proofpoint, "High-Volume Dridex Banking Trojan Campaigns Return". In : (4 avr. 2017).

[8] Palo Alto. *Locky : New Ransomware Mimics Dridex-Style Distribution*. 16 fév. 2016. URL : https://unit42.paloaltonetworks.com/locky-new-ransomware-mimics-dridex-style-distribution/ (visité le 24/04/2020).

[9] Proofpoint. *TA505 Shifts with the Times*. 8 juin 2018. URL : https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times (visité le 20/11/2019).

[10] SensePost, "Macro-Less Code Exec in MSWord". In : (9 oct. 2017).

[11] Trend Micro. *Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi - Trend-Labs Security Intelligence Blog*. 4 juil. 2019. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new-malware-tools-gelup-and-flowerpippi/ (visité le 27/11/2019).

[12] Korea Internet & Security Agency, *KISA Cyber Security Issue Report : Q2 2019*. 13 août 2019.

[13] FireEye. *STOMP 2 DIS : Brilliance in the (Visual) Basics*. 5 fév. 2020. URL : https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html (visité le 09/04/2020).

[14] Proofpoint. *Leaked Ammyy Admin Source Code Turned into Malware*. 7 mar. 2018. URL : https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware.

[15] Proofpoint, "TA505 Abusing SettingContent-Ms within PDF Files to Distribute FlawedAmmyy RAT". In : (19 juil. 2018).

[16] Proofpoint, "tRat : New Modular RAT Appears in Multiple Email Campaigns". In : (15 nov. 2018).

[17] Proofpoint, "ServHelper and FlawedGrace - New Malware Introduced by TA505". In : (9 jan. 2019).

[18] Trend Micro. *TA505 At It Again : Variety Is the Spice of ServHelper and FlawedAmmyy*. 27 août 2019. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/ (visité le 24/04/2020).

[19] Proofpoint. *TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader*. 15 oct. 2019. URL : https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader (visité le 19/11/2019).

[20] Korean Financial Security Institute, "Profiling of TA505 Threat Group". In : (28 fév. 2020).

[21] Microsoft Security Intelligence, "Mise à Jour Dudear". In : (30 jan. 2020).

[22] Proofpoint, "New Modular Downloaders Fingerprint Systems, Prepare for More - Part 1 : Marap". In : (16 oct. 2018).

[23] Trend Micro. *Shifting Tactics : Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns*. 12 juin 2019. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns/ (visité le 09/04/2020).

[24] Proof Point. *TA505 Begins Summer Campaigns with a New Pet Malware Downloader, AndroMut, in the UAE, South Korea, Singapore, and the United States*. 2 juil. 2019. URL : https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south (visité le 09/04/2020).

[25] Cyberint. *Legit Remote Admin Tools Turn into Threat Actors' Tools*. 1er jan. 2019. URL : https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%27%20Tools_Report.pdf (visité le 24/04/2020).

[26] Twitter. *@Kafeine*. 24 déc. 2019. URL : http://www.twianon.com/tweet/kafeine/1209495921995735040 (visité le 24/04/2020).

[27] Blueliv. *TA505 Evolves ServHelper, Uses Predator The Thief and Team Viewer Hijacking*. 17 déc. 2019. URL : https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/ (visité le 09/04/2020).

[28] US-Cert. *COVID-19 Exploited by Malicious Cyber Actors*. 8 avr. 2020. URL : https://www.us-cert.gov/ncas/alerts/aa20-099a (visité le 24/04/2020).

[29] Fox IT *Reactie Universiteit Maastricht Op Rapport FOX-IT*. 5 fév. 2020.

[30] 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/ (visité le 09/04/2020).

[31] CERT-FR, "Informations Concernant Le Rançongiciel Clop". In : (22 nov. 2019).

[32] Deutsch Telekom. *TA505's Box of Chocolate - On Hidden Gems Packed with the TA505 Packer*. 26 mar. 2020. URL : https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672 (visité le 09/04/2020).

[33] 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 (visité le 16/04/2020).

[34] Morphisec, "Morphisec Uncovers Global "Pied Piper" Campaign". In : (29 nov. 2018).

[35] Proofpoint, "TA505 Targets the US Retail Industry with Personalized Attachments". In : (12 juin 2018).

[36] Cybereason. *Threat Actor TA505 Targets Financial Enterprises Using LOLBins and a New Backdoor Malware*. 25 avr. 2019. URL : https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware (visité le 09/04/2020).

[37] Yoroi. *TA505 Is Expanding Its Operations*. 29 mai 2019. URL : https://yoroi.company/research/ta505-is-expanding-its-operations/ (visité le 09/04/2020).

[38] Bleeping Computer, "Ransomware Hits Maastricht University, All Systems Taken Down". In : (27 déc. 2019).

[39] CERT-FR, "Le Groupe Cybercriminel Silence". In : (7 mai 2020).

[40] Norfolk Infosec. *OSINT Reporting Regarding DPRK and TA505 Overlap*. 10 avr. 2019. URL : https://norfolkinfosec.com/osint-reporting-on-dprk-and-ta505-overlap/ (visité le 09/04/2020).

[41] Lexfo, *The Lazarus Constellation*. 19 fév. 2020.

[42] Group-IB, "SILENCE 2.0". In : (1er août 2019).

[43] Group-IB. *New Financially Motivated Attacks in Western Europe Traced to Russian-Speaking Threat Actors*. 27 mar. 2020. URL : https://www.group-ib.com/media/silence_ta505_attacks_in_europe/ (visité le 24/04/2020).

[44] Twitter. *@Kafeine*. 24 avr. 2020. URL : https://pbs.twimg.com/media/ERxmxQnWAAM8Fmj.jpg (visité le 24/04/2020).

[45] Threatpost. *Necurs Botnet Evolves to Hide in the Shadows, with New Payloads*. 27 jan. 2020. URL : https://threatpost.com/necurs-botnet-hide-payloads/142334/ (visité le 27/01/2020).

[46] Proofpoint. *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 (visité le 24/04/2020).

[47] SECURITY INTELLIGENCE. *The Necurs Botnet : A Pandora's Box of Malicious Spam*. 24 avr. 2017. URL : https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/ (visité le 24/04/2020).

[48] BITSIGHT. *Joint Effort with Microsoft to Disrupt Massive Criminal Botnet Necurs*. 10 mar. 2020. URL : https://www.bitsight.com/blog/joint-effort-with-microsoft-to-takedown-massive-criminal-botnet-necurs (visité le 24/04/2020).

[49] 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/ (visité le 24/04/2020).

[50] 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/ (visité le 29/01/2020).

- 22/06/2020

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