WEBROOT
an opentext company

CARBONITE
an opentext company

WEBROOT

THREAT REPORT

SOMMAIRE

AVANT-PROPOS

Hal Lonas, Vice-président général et directeur technologique, PME et consommateur, OpenText

Alors que nous entamons une nouvelle décennie, il est frappant de penser à toutes les évolutions majeures qui se sont produites récemment. Réfléchissez à cela : nous vivons dans l'ère des smartphones depuis plus de dix ans. Si nous repensons à un passé plus lointain, le « cloud » est passé d'un simple concept dans les années 1960 à un mot à la mode au début des années 2000, pour devenir l'état universel de l'informatique stratégique actuelle, dans laquelle les clouds publics, privés et hybrides sont omniprésents. Les attentes des utilisateurs, en particulier, remettent en question le fonctionnement des entreprises dans le monde. Pour ceux d'entre nous qui se souviennent de l'époque des accès commutés : essayez de vous rappeler combien de temps il fallait pour se connecter, sans parler pour télécharger une image ! Aujourd'hui, chacun de nous s'attend à recevoir des expériences personnalisées, pertinentes et immédiates, rapidement et sans décalage, via le cloud, l'intelligence mobile, sociale et artificielle, tout en exigeant que nos données personnelles restent sécurisées et privées.

Toutefois, la persévérance des pirates informatiques, qui déploient des efforts pour usurper les données, compromettre les systèmes et générer des profits, reste une constante. Beaucoup de tactiques restent les mêmes ; le hameçonnage existe depuis bien longtemps et reste un outil de choix pour insérer des logiciels malveillants et bénéficier d'un accès non autorisé aux informations sensibles. Ce faisant, d'autres tactiques ont considérablement évolué ; il y a dix ans en arrière, nous n'avions pas encore entendu parler de rançongiciels, l'effet du cloud computing sur la sécurité était un gros point d'interrogation, et seulement 28 % des attaques utilisaient des tactiques d'ingénierie sociale.[1] Ces deux dernières années, en particulier, ont eu un impact remarquable sur le paysage des menaces. Par exemple, des adresses IP malveillantes, des URL qui redirigent des utilisateurs non avertis vers des sites dangereux, le cryptojacking qui exploite des cryptomonnaies à l'insu de l'utilisateur ou sans son consentement, des variations des rançongiciels et des logiciels malveillants de plus en plus vicieux et furtifs : tous ces dangers constituent des menaces récentes, tant pour les entreprises que pour les particuliers.

Dans le Rapport sur les menaces® Webroot de cette année, nous approfondissons ce que nous avons vu dans ces catégories et dans d'autres, et incluons davantage de contexte supplémentaire sur les industries ciblées et les emplacements des logiciels malveillants courants. Grâce à une vue approfondie de quantités massives de trafic Web, comprenant à la fois des données licites et d'autres malveillantes, nous nous appuyons sur notre solide compréhension de ce qui s'est passé au cours de la dernière décennie pour anticiper ce que présage 2020 et pour vous aider à comprendre ces tendances dans un monde en évolution rapide.

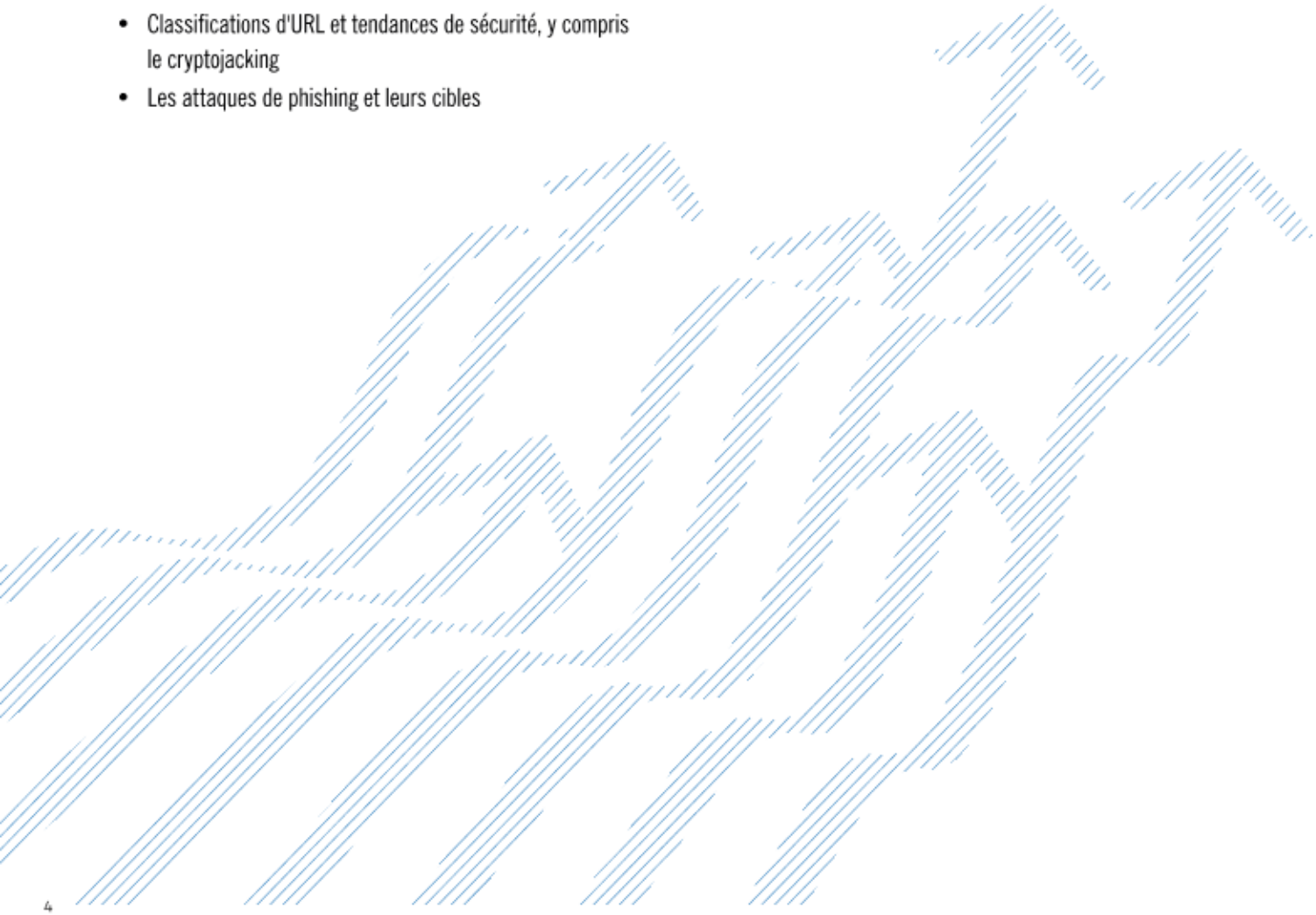
> Aujourd'hui, chacun de nous s'attend à recevoir des expériences personnalisées, pertinentes et immédiates, rapidement et sans décalage, via le cloud, l'intelligence mobile, sociale et artificielle, tout en exigeant que nos données personnelles restent sécurisées et privées.

LA PERSPECTIVE WEBROOT

Les statistiques, les tendances et les informations contenues dans ce Rapport sur les menaces Webroot 2020 sont basées sur de gigantesques quantités de données capturées en continu et automatiquement par notre architecture avancée basée sur l'apprentissage automatique, à savoir la plateforme Webroot®. Ces données, qui proviennent de millions de points de terminaison et de capteurs du monde réel, de bases de données tierces spécialisées et d'utilisateurs finaux protégés par nos partenaires technologiques, sont ensuite analysées et interprétées en continu par nos moteurs avancés de machine learning et notre équipe de recherche sur les menaces. Les rétrospectives, les tendances et les prévisions de ce rapport couvrent un vaste éventail d'activités de menace, notamment :

- Tendances des logiciels malveillants, les acteurs affectés, où ces menaces se dissimulent, et une analyse géographique et sectorielle
- Classifications d'URL et tendances de sécurité, y compris le cryptojacking
- Les attaques de phishing et leurs cibles
- Adresses IP malveillantes et leur impact sur la sécurité
- Le fléau persistant des rançongiciels
- Les menaces des applications mobiles et leur évolution

Chacune des menaces susmentionnées a des impacts de grande envergure dans plusieurs secteurs, régions géographiques et groupes d'utilisateurs. Nous décomposerons tout cela par des chiffres, et démontrerons également comment la sensibilisation des utilisateurs et la formation permettent d'atténuer les risques de compromis. Enfin, dans la section Prévisions, nous verrons comment notre vision globale nous permet de déterminer les tendances que nous prévoyons pour l'année à venir.



RENSEIGNEMENTS SUR LES MENACES WEBROOT BRIGHTCLOUD®

Plus de 95 millions de capteurs du monde réel

Plus de 78 millions d'utilisateurs finaux protégés par des partenaires technologiques

Plus de 842 millions de domaines

Plus de 37 milliards d'URL

Plus de 4 milliards d'adresses IP

Plus de 36 milliards d'enregistrements de comportement de fichier

Plus de 31 millions d'applications mobiles actives

LOGICIELS MALVEILLANTS

Au cours des dix dernières années, nous avons constaté que les créateurs des logiciels malveillants et les pirates informatiques disposent de grandes capacités d'adaptation et sont extrêmement déterminés. Il suffit d'observer l'augmentation rapide des fichiers malveillants trouvés sur un seul appareil pour constater comment les auteurs ont appris à échapper aux cyberdéfenses traditionnelles via le polymorphisme.

*En 2019, **93,6 % des logiciels malveillants** n'ont été détectés que **sur un seul PC.** Il s'agit là du taux annuel le plus élevé que nous ayons jamais vu, bien que ce chiffre dépasse les 90 % depuis 2014.*

Les logiciels malveillants sont devenus un outil de prédilection des États-nations, qui emploient (et, parfois, perdent le contrôle) des exploits « zero-day » très avancés pour faire des ravages sur les entreprises, les gouvernements et les organisations en général, comme l'a prouvé l'exploit EternalBlue.[2] Ajoutez à cela l'impact du cloud et l'omniprésence des téléphones mobiles, et il est facile de voir combien de logiciels malveillants ont évolué au cours de la dernière décennie.

Une chose est sûre : les logiciels malveillants® n'ont pas disparu. Les points de terminaison Windows protégés par Webroot détectent plus de 1,6 million de nouveaux programmes malveillants et applications Windows chaque jour. Ce nombre continue de croître, partant d'environ 1,369 million par jour l'année précédente. Cela représente jusqu'à 500 millions en 2018 et près de 600 millions en 2019. En d'autres termes, nous observons un flux massif, croissant et perpétuel de données de fichiers.

APPAREILS GRAND PUBLIC ET PROFESSIONNELS

Parmi les points finaux signalant une infection, 62 % étaient des appareils grand public (utilisateurs à domicile), tandis que 38 % étaient des systèmes d'entreprise. Cet écart est probablement dû au fait que les entreprises disposent de davantage de niveaux de sécurité en place, et que davantage d'entre elles offrent une formation de sensibilisation à la sécurité à leurs employés. Dans l'ensemble, le nombre de fichiers malveillants par appareil diminue d'année en année pour les ordinateurs grand public, mais il reste à peu près le même que l'année précédente pour les ordinateurs professionnels.

Les appareils grand public continuent d'être infectés beaucoup plus souvent que les appareils professionnels. C'est pour cette raison qu'il est important de souligner les risques encourus par les entreprises lorsque celles-ci autorisent leurs employés à connecter des appareils personnels au réseau de l'entreprise. De par une prévalence plus élevée de logiciels malveillants et généralement moins de défenses de sécurité en place, il est plus facile pour les logiciels malveillants de pénétrer le réseau de l'entreprise via l'appareil personnel d'un employé.

Les appareils grand public restent environ 2 fois plus susceptibles d'être infectés que les systèmes d'entreprise.

Une chose particulièrement intéressante à noter est la fréquence à laquelle les PC ont été réinfectés.

En 2019, 12,6 % des PC grand public ont été infectés.
Parmi ceux-ci :

- 46,3 % n'ont subi qu'une seule infection
- 35,8 % en ont subi entre 2 et 5
- 8,6 % en ont subi entre 6 et 10
- 9,2 % ont subi plus de 10 infections

En revanche, seulement 7,8 % des PC professionnels ont subi une infection.

PC grand public infectés

PC professionnels infectés

Parmi ceux-ci :

- 50,4 % ont subi une seule infection
- 33,2 % en ont subi 2 à 5
- 7,9 % en ont subi 6 à 10
- 8,5 % en ont subi plus de 10

Il existe plusieurs raisons possibles pour expliquer pourquoi les systèmes subissent plusieurs infections ; cela peut être le résultat de plusieurs fichiers polymorphes attaquant un seul PC, ou un seul logiciel malveillant supprimant plusieurs fichiers. En outre, la protection Webroot peut, lors de sa première installation sur un appareil, détecter plusieurs infections actuelles. Quoi qu'il en soit, le message à retenir est que les administrateurs et les particuliers doivent rester vigilants.

POURQUOI LE SYSTÈME D'EXPLOITATION EST IMPORTANT

Comme nous l'avons vu au cours des deux dernières années, le passage à Windows® 10 (un système d'exploitation généralement plus sûr) permet d'expliquer le déclin de certains logiciels malveillants dans les statistiques. Dans l'ensemble, les systèmes exécutant Windows® 7 sont près de trois fois plus susceptibles d'être infectés que les appareils Windows 10 ; chaque système d'exploitation enregistre une moyenne de 0,11 et 0,04 infection par point final, respectivement.

En général, nous pouvons dire que Windows 10 enregistre moins d'infections, avec 0,06 par appareil pour les PC grand public et 0,02 par appareil pour les PC d'entreprise. L'ampleur du problème de Windows 7 dépend du nombre d'ordinateurs personnels et professionnels exécutant ce système d'exploitation. En 2019,

Ciblage de logiciel malveillant Windows 7 a augmenté de 125 %.

nous avons vu que 82 % des PC grand public fonctionnaient sous Windows 10, contre seulement 10 % sous Windows 7, tandis que 63 % des PC professionnels fonctionnaient sous Windows 10 et plus de 25 % d'entre eux exécutaient Windows 7. Nous prévoyons une diminution de ce pourcentage, car Microsoft ne prend plus en charge Windows 7.

Lorsque l'on examine les taux d'infection par point final, les différences entre les consommateurs et les entreprises sont claires. Les infections par système consommateur diminuent globalement de manière constante (de 0,11 en 2017 à 0,10 en 2018 et tombent à 0,08 en 2019), mais les chiffres agrégés masquent un fait important : les taux de Windows 7 sont passés de 0,17 à 0,20 infection par appareil. Bien que nous nous attendions à ce que le nombre de points de terminaison Windows 7 diminue, la quantité de logiciels malveillants ciblant spécifiquement Windows 7 est susceptible d'augmenter pour la même raison ; si Microsoft ne prend plus en charge Windows 7, les vulnérabilités de ce système d'exploitation ne seront plus corrigées.

La légère baisse du total annuel des fichiers malveillants est probablement due à plusieurs facteurs.

- **Formation de sensibilisation à la sécurité (SAT)**
  Les utilisateurs étant la première ligne de défense, les formations de sensibilisation à la sécurité sont de plus en plus importantes. Gartner affirme que la sensibilisation et la formation axées sur l'utilisateur final en matière de sécurité est un marché en croissance rapide et estime que « d'ici 2022, 60 % des grandes entreprises et organisations disposeront de programmes de formation complets de sensibilisation à la sécurité. »[3]

- **Efficacité technologique**
  Les données que nous présentons sont collectées à partir de points de terminaison protégés par Webroot. Notre approche multi-vecteur en couches détecte et bloque l'activité plus tôt dans la chaîne de destruction. Par exemple, en empêchant les exécutables d'atteindre les points de terminaison via des URL malveillantes ou en empêchant les .exes de télécharger des fichiers malveillants supplémentaires, nous pouvons réduire l'incidence des programmes malveillants s'exécutant sur les points de terminaison protégés.

- **Évolution de l'activité cybercriminelle**
  Certains cybercriminels se sont recentrés sur des méthodes d'attaque qui génèrent plus aisément des profits avec des systèmes distants qu'avec des logiciels malveillants, comme le phishing ou le cryptojacking. De plus, les criminels sont passés à un modèle économique de logiciel malveillant plus ciblé, dans lequel ils lancent moins d'attaques et déploient moins de logiciels malveillants, mais le font avec un taux de réussite plus élevé.

- **Un système d'exploitation plus sécurisé**
  L'adoption massive de Windows 10 (avec antivirus toujours activé) et les efforts de la communauté de sécurité et de l'industrie de la sécurité en général constituent également un facteur.

INFECTIONS PAR RÉGION ET INDUSTRIE

Si nous suivons les taux d'infection survenus sur les appareils Windows par région géographique, nous constaterons des différences frappantes. À première vue, il est plus facile de voir le taux d'appareils grand public infectés par rapport aux PC professionnels.

De plus, les taux d'infection varient considérablement selon la zone géographique. Près d'un quart (23 %) des appareils au Moyen-Orient ont subi une infection en 2019 ; l'Asie emboîte le pas, suivie de l'Afrique et de l'Amérique du Sud. En revanche, l'Europe, l'Amérique du Nord et le Japon ont enregistré des taux beaucoup plus bas.

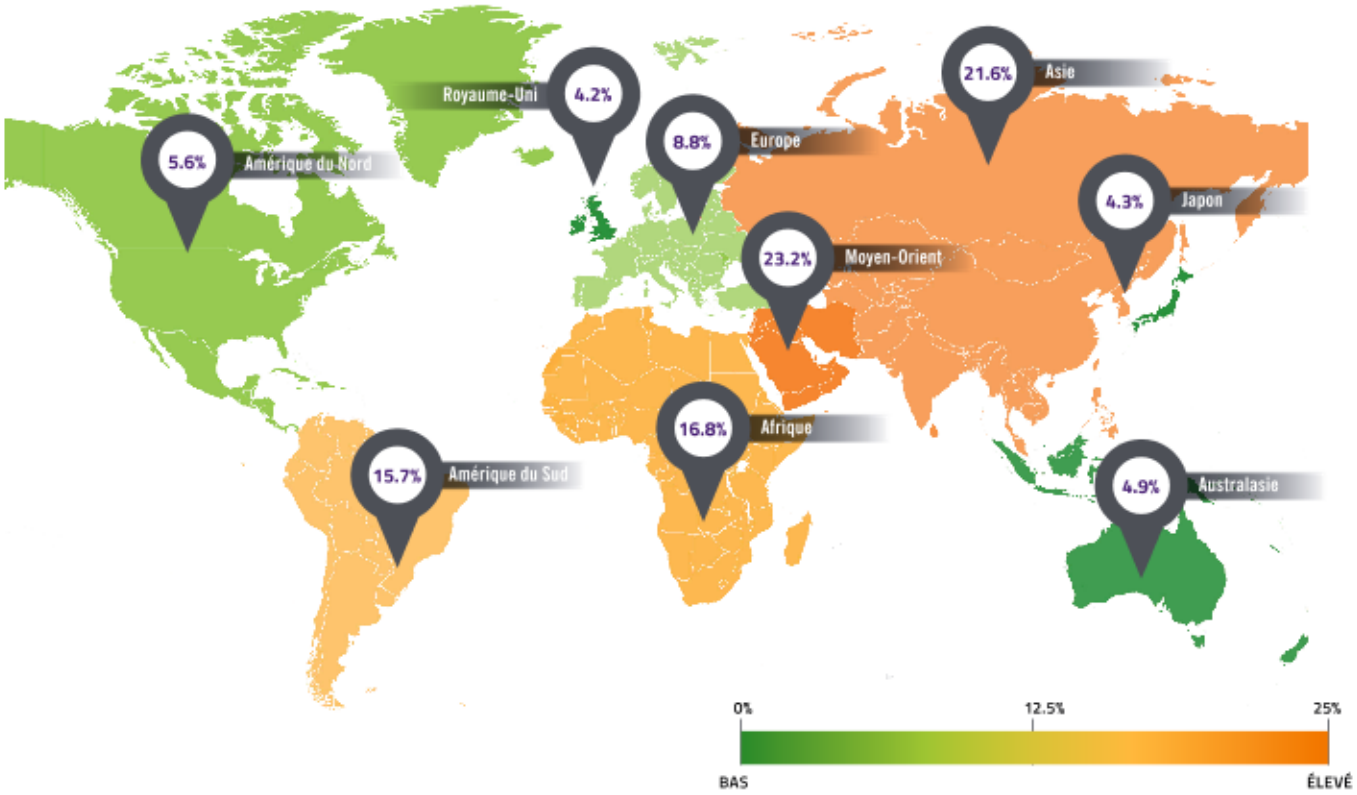


Figure 1a : Appareils infectés par région

	Appareils grand public infectés	Appareils professionnels infectés
Afrique	20.3%	15.7%
Asie	27.9%	16.6%
Australasie	11.6%	4.6%
Europe	21.5%	7.3%
Japon	4.6%	4.1%
Moyen-Orient	26.9%	16.6%
Amérique du Nord	6.9%	3.9%
Amérique du Sud	17.9%	10.5%
Royaume-Uni	9.6%	3.7%

0% 14% 28%

Figure 1b : Appareils grand public et professionnels infectés par région

	Appareils exécutant Windows 7	Appareils exécutant Windows 10
Afrique	31.5%	53.9%
Asie	33.4%	54.6%
Australasie	24.8%	62.0%
Europe	26.9%	59.2%
Japon	39.6%	51.3%
Moyen-Orient	35.3%	50.1%
Amérique du Nord	19.6%	69.8%
Amérique du Sud	22.5%	63.1%
Royaume-Uni	26.0%	62.2%

0% 35% 70%

Figure 1c : Appareils Windows 7 et Windows 10 infectés par région

Pour mieux comprendre les taux d'infection, nous devons examiner les données régionales par système d'exploitation. En général, Windows 7 représente 21 % de la base, tandis la part de Windows 10 est de 68 %. Mais si nous observons les régions enregistrant des taux d'infection très élevés, nous pouvons corréler cela à la prévalence de Windows 7. Par exemple, en Amérique du Sud, plus de 22 % des PC exécutent Windows 7 ; en Afrique, ce chiffre est de 31,5 % ; en Asie, 33,4 % ; et au Moyen-Orient, 35,2 %. Toutes ces régions affichent des taux d'infection élevés par appareil, et les régions comptant un grand nombre de PC Windows 7 sont soumises à un nombre croissant de menaces. Encore une fois, le taux de menace augmente pour Windows 7 alors qu'il reste stable ou diminue pour Windows 10. En revanche, en Amérique du Nord, près de 70 % des PC utilisent Windows 10 et les taux d'infection sont faibles.

Divers facteurs peuvent contribuer à ces taux d'infection. Par exemple, les régions qui disposent de ressources économiques plus importantes, d'un meilleur accès à des technologies à jour et qui sont plus sensibilisées aux préoccupations et aux risques de cybersécurité (comme les États-Unis et l'Europe) ont tendance à enregistrer moins d'infections par appareil, en particulier concernant les ordinateurs professionnels. Les régions comptant moins d'appareils à jour, c'est-à-dire un grand nombre de PC Windows 7, présentent un plus grand nombre de menaces.

Une autre façon d'examiner les taux d'infection consiste à comparer les taux de diverses industries avec la moyenne globale. Parmi les clients Webroot qui nous ont signalé leurs secteurs d'activité, tous ont observé un pourcentage de logiciels malveillants par appareil inférieur en 2019 par rapport à 2018. Cependant, nous observons une évolution au niveau des cibles rencontrant plus de logiciels malveillants que d'autres. Par exemple, l'industrie, l'administration publique, l'extraction de ressources et le transport et l'entreposage enregistrent des taux de logiciels malveillants par appareil supérieurs à la moyenne. Ce faisant, des cibles d'attaque plus traditionnelles, telles que le secteur financier, des assurances, les soins de santé et l'assistance sociale, les organisations à but non lucratif et les services d'éducation, enregistrent des taux de logiciels malveillants inférieurs à la moyenne. (Étant donné que ces dernières industries sont dans la ligne de mire des cybercriminels depuis plusieurs années, et que beaucoup d'entre elles ont, par conséquent, réalisé des investissements massifs pour améliorer la sécurité, il n'est pas surprenant que leurs pourcentages se soient améliorés.)

OÙ SE CACHENT LES LOGICIELS MALVEILLANTS

Les logiciels malveillants sont partout, mais les emplacements système dans lesquels ils se cachent diffèrent, selon qu'il s'agit de PC consommateur ou professionnels. Prenez % appdata % par exemple. Pour les PC grand public, 26,5 % de l'ensemble des infections se trouvent dans ce dossier.

En revanche, 16,7 % des menaces détectées dans % appdata % pour les PC professionnels sont des logiciels malveillants. La popularité d'appdata dans les systèmes grand public provient notamment du fait que l'utilisateur n'a pas besoin des services d'un administrateur local pour installer un programme avec Windows 8 ou une version ultérieure. La majorité des appareils grand public comptent un seul utilisateur, qui est l'administrateur de l'appareil. Ceci est différent dans les environnements d'entreprise, où l'utilisateur a souvent des restrictions quant aux emplacements où de nouvelles applications peuvent être installées.

85 % des menaces se dissimulent dans l'un de ces quatre emplacements : % temp %, % appdata %, % cache % et % windir %.

Les autres exemples incluent %temp% qui représente 54,4 % des fichiers malveillants pour les PC professionnels et 28,7 % pour les PC grand public. Temp est deux fois plus susceptible d'être une cachette pour les infections de PC professionnels que pour les PC grand public. (Il y a cependant une bonne nouvelle : il est facile de configurer une stratégie Windows pour empêcher les programmes de s'exécuter à partir du répertoire %temp%, qu'ils soient malveillants ou licites. Il s'agit d'une bonne hygiène cybernétique qui, associée à une formation de sensibilisation à la sécurité des utilisateurs, peut grandement améliorer la protection.

Nous continuons de constater l'impact positif d'un système d'exploitation plus propre, Windows 10 en particulier. Il est important de garder à l'esprit que lorsque les consommateurs achètent un nouveau PC, Windows 10 est le système d'exploitation généralement fourni par défaut, d'autant que Microsoft a l'intention de retirer complètement Windows 7. Cependant, pour les entreprises, il est plus difficile d'effectuer une mise à niveau massive ; des applications existantes peuvent nécessiter Windows 7, et il existe des coûts associés à la mise à niveau.

RANÇONGICIELS

Les rançongiciels n'ont fait leur apparition qu'en 2015. Avant cela, nous avons observé une grande quantité de faux logiciels antivirus, dans lesquels une fenêtre contextuelle informait l'utilisateur de manière alarmante que son système avait été compromis, et qu'il devait cliquer sur un lien pour « nettoyer » son système. Cette action entraînait généralement un coût quel qu'il soit et compromettait davantage le système. Vers le milieu des années 2010, les pirates ont commencé à utiliser la crypto-monnaie afin que les autorités judiciaires aient plus de mal à suivre leurs activités. Outre cet avantage, cette monnaie présentait une valeur élevée, ce qui en a fait une activité en plein essor. Suite à une attaque par rançongiciel, l'utilisateur se voyait proposé diverses offres de déchiffrement gratuit de fichiers uniques, de support multilingue et de service client, tous proposés par des acteurs malveillants qui avaient commis l'attaque en premier lieu.

En 2017, les attaques de rançongiciel ont semé la panique dans le monde. Les organisations se sont efforcées de protéger leurs données stratégiques et ont souvent payé les rançons, mais elles n'ont pas toujours reçu les clés capables de déchiffrer leurs fichiers perdus. Nous avons constaté un déclin du nombre d'attaques par rançongiciels menées à bien en 2018, ce qui s'explique en partie par de meilleures sauvegardes, une plus grande sensibilisation et des défenses évolutives, qui compliquent le lancement de telles campagnes malveillantes.

Bien que Webroot ait observé un nouveau recul des attaques par rançongiciel au cours de l'année dernière, ces dernières sont loin d'avoir disparu. Au lieu de cela, les rançongiciels sont désormais plus ciblés, mieux implémentés et beaucoup plus impitoyables, les criminels ciblant spécifiquement des valeurs plus élevées et des cibles plus vulnérables. En outre, cette menace a continué de cibler les RDP afin d'enfreindre les systèmes, en particulier afin de compromettre les outils de protocole de bureau à distance (RDP), lesquels sont fréquemment utilisés par les fournisseurs de services gérés (MSP). L'infraction d'un seul MSP peut permettre aux pirates informatiques d'accéder à toute la clientèle d'une entreprise, ce qui fait de ces fournisseurs une cible particulièrement lucrative.

EternalBlue, qui avait été à l'origine développé par la US National Security Agency (agence de sécurité nationale américaine), puis infiltrée par la suite par des pirates informatiques, constitue un exemple d'exploit utilisant le hameçonnage et dont l'impact a été particulièrement conséquent. L'attaque mondiale par

LES DERNIÈRES TENDANCES EN TERMES DE RANÇONGICIELS

DAVANTAGE D'ATTAQUES PAR RECONNAISSANCE

Les pirates informatiques étudient scrupuleusement une entreprise et son infrastructure, y compris les serveurs critiques et les emplacements de sauvegarde. Ainsi, ils savent quels logiciels malveillants et quels exploits utiliser pour augmenter leurs chances de réussite. Ces types d'attaques par reconnaissance sont particulièrement efficaces pour cibler les petites et moyennes entreprises (PME), souvent moins préparées à de telles situations (c'est-à-dire sans plans d'urgence, structures d'évaluation des risques, cyberassurance, etc.)

AUGMENTATION DU MONTANT DES RANÇONS

Le montant moyen des rançons augmente. Au troisième trimestre 2019, il a atteint 41 198 USD, contre 36 295 USD au premier trimestre.[4] Ces chiffres sont rapportés par Coveware, une société spécialement créée pour aider les victimes de rançongiciels à payer leur rançon. L'existence même d'une telle entreprise témoigne du succès continu des attaques par rançongiciels.

rançongiciel WannaCry, qui a débuté comme une attaque de la chaîne d'approvisionnement contre des cibles ukrainiennes via un logiciel fiscal, a utilisé cette vulnérabilité pour attaquer des systèmes où aucun correctif n'était implémenté. Malgré un arrêt d'urgence, cette attaque a engendré des dommages et des temps d'arrêt qui se sont traduits par des pertes de l'ordre de plusieurs milliards de dollars. Le même exploit a été utilisé plus tard pour mener à bien l'attaque NotPetya sur des systèmes encore moins à jour en termes de correctifs.

DOUBLE TROUBLE

L'attaque par enchaînement Trickbot-Emotet, survenue en 2018 a été prédominante en 2019. Emotet est un réseau de diffusion de botnets qui permet de déployer d'autres attaques ; ce malware installe souvent sur le système un Trickbot (un cheval de Troie bancaire qui vole des données, mais recueille également des informations au sujet de l'organisation). Ces attaques ont récemment ciblé de plus grandes entreprises, tentant de trouver des victimes lucratives susceptibles de payer de grosses rançons. En 2019, Trickbot a lancé une attaque à deux volets, usurpant des informations tout en installant sur les systèmes Ryuk, un autre type de rançongiciel. En plus de voler des données personnelles et des informations d'identification, Trickbot était capable de retrouver les victimes et de les attaquer à nouveau plus tard via un rançongiciel.

Ces attaques utilisent essentiellement des e-mails de hameçonnage pour s'emparer d'un réseau. Elles exploitent des sujets d'actualité, comme les souscriptions à des couvertures de soins de santé ou le changement climatique, afin que les individus soient plus enclins à cliquer sur un lien et télécharger un cheval de Troie, un rançongiciel ou un autre logiciel malveillant.

« Evil Corp » est une autre organisation de rançongiciels extrêmement performante qui est actuellement pourchassée par le ministère américain de la Justice, lequel offre une prime de 5 millions de dollars pour toute information permettant d'aboutir à la condamnation de Maksim Yakubets, le pirate informatique présumé coupable de ces crimes. Cette organisation russe a dérobé environ 100 millions de dollars à des entreprises et consommateurs. Le groupe utilise des logiciels malveillants Dridex pour usurper les informations d'identification bancaire des employés des petites et moyennes entreprises, puis recrute des « mules financières », à savoir des collaborateurs involontaires ou complices, qui aident l'organisation à blanchir l'argent ainsi extorqué. Le groupe est également à l'origine de l'attaque BitPaymer, un rançongiciel qui a frappé plusieurs entreprises en Espagne fin 2019.[5]

DES ENJEUX PLUS IMPORTANTS

Une récente tendance constatée dans les attaques par rançongiciel consiste non seulement à voler ou à verrouiller les données d'une organisation, mais également à menacer la victime de fuite ou d'utilisation abusive de ces données. Les victimes sont ainsi plus susceptibles de payer la rançon, même si elles disposent de sauvegardes adéquates.

UNE ÉVOLUTION AU NIVEAU DES CIBLES

2019 a été le théâtre d'une véritable épidémie d'attaques par rançongiciels contre des villes américaines, ainsi que d'attaques systématiques contre des cibles privilégiées, telles que les secteurs des transports, des soins de santé, de l'éducation et les PME. Nombre de ces attaques utilisent des logiciels malveillants Rançongiciels en tant que service, lesquels sont disponibles gratuitement via le dark web et sont très simples à utiliser, même pour des cybercriminels inexpérimentés.

URL À HAUT RISQUE

Webroot a examiné des milliards d'URL au fil des années, étudiant en permanence leur comportement, leur historique, leur ancienneté, leur popularité, leur emplacement, leurs réseaux, leurs liens et leurs performances en temps réel. Cette année, nous avons constaté une légère augmentation du volume d'URL à haut risque. Cependant, le nombre d'URL malveillantes trouvées sur des sites non malveillants a diminué ; il est désormais de 24 % (contre 40 % en 2018). Ce chiffre n'est toutefois pas négligeable.

1 URL malveillante sur 4 est hébergée sur un site non malveillant.

Pour renforcer la sécurité d'un site Web, il convient de s'adonner à des pratiques de diligence raisonnable, d'appliquer des correctifs à jour, de mettre en place un processus d'examen du contenu existant et de contrôler l'accès, pour savoir qui peut publier du contenu. Bien qu'il soit clair que de nombreuses organisations ont d'ores et déjà pris toutes ces précautions, 24 % reste un chiffre élevé, qui traduit le fait que les cybercriminels savent qu'il est difficile de bloquer le contenu malveillant sur des domaines qui sont par ailleurs fiables. Gardez à l'esprit que le trafic HTTPS étant crypté, la visibilité est moindre sur les pages hébergées dans des sites HTTPS. De plus, l'adoption de la norme HTTPS a augmenté, limitant la visibilité au niveau du domaine sur les appareils qui ne déchiffrent pas le trafic. Ces appareils sont généralement destinés à un usage personnel ou à une petite entreprise, mais peuvent également s'étendre à la sphère d'une entreprise, ce qui signifie que l'impact de ces attaques peut avoir une vaste ampleur. Enfin, les solutions qui se limitent à l'inspection des domaines afin d'évaluer les risques ne sont pas aussi efficaces que celles qui évaluent également les pages des sites.

CLASSIFICATION DES URL

Nous classons les URL à haut risque dans plusieurs catégories : hameçonnage, réseaux zombies, enregistreurs de frappe et surveillance, évitement de proxy et anonymiseurs, sites malveillants, sites de spam et logiciels espions et publicitaires. Le hameçonnage représente 45 % des URL à haut risque détectées cette année ; nous avons observé des pics conséquents en juillet et août (26 % du total annuel des sites de hameçonnage détectés) ainsi qu'une intensification vers la fin de l'année. En effet, 62 % des URL de hameçonnage ont été observées au cours du second semestre. Un tel fait peut s'expliquer par la hausse de l'activité en ligne pendant les périodes de rentrée scolaire et les vacances.

La multiplication des URL à haut risque est une tendance qui se poursuit par rapport aux années précédentes, et la croissance constatée en 2019 est largement due aux sites de hameçonnage. Le hameçonnage est une pratique qui n'a de cesse d'augmenter, avec un pic d'activité juste avant la période des fêtes : les sites de hameçonnage ont enregistré un taux de visite de 21 % durant le Black Friday et de 58 % durant le Cyber Monday, tandis que les visites de sites de spam, douteux, espions, de logiciels publicitaires et de proxy ont augmenté durant le Cyber Monday.

Les URL de hameçonnage ont augmenté de 640 % durant l'année.

En revanche, nous avons constaté une baisse progressive du pourcentage d'URL qui semblent être liées à l'hébergement de logiciels malveillants. Alors que les taux variaient entre 1 et 1,5 %, nous avons observé une baisse significative, passant de 1,45 % en début d'année à 1,06 % en fin d'année.

Nous avons également constaté une baisse constante de l'incidence des URL liées aux spams, à l'évitement de proxy et anonymiseurs et aux logiciels publicitaires et espions.

SUR LA SELLETTE : DISTRIBUTION DE CONTENU MALVEILLANT

Plus d'un quart (28 %) des URL classées dans la catégorie Sécurité en 2019 étaient des sites de distribution de contenu malveillant. Lorsque nous examinons les catégories de distribution de contenu malveillant, nous constatons que les raccourcisseurs d'URL et le stockage dans le cloud sont, comme l'année dernière, les deux principales méthodes utilisées pour masquer l'origine du contenu. Si nous observons les dix mille domaines les plus populaires publiés par Alexa Internet, plus de 20 catégories de contenu différentes hébergent des URL malveillantes, et 96 % d'entre elles le font via des modificateurs / raccourcisseurs de liens URL. Bien que les raccourcisseurs d'URL soient populaires et faciles à utiliser, car ils permettent aux utilisateurs de communiquer avec un nombre limité de caractères (par exemple pour Twitter), ils masquent où l'utilisateur est réellement redirigé.

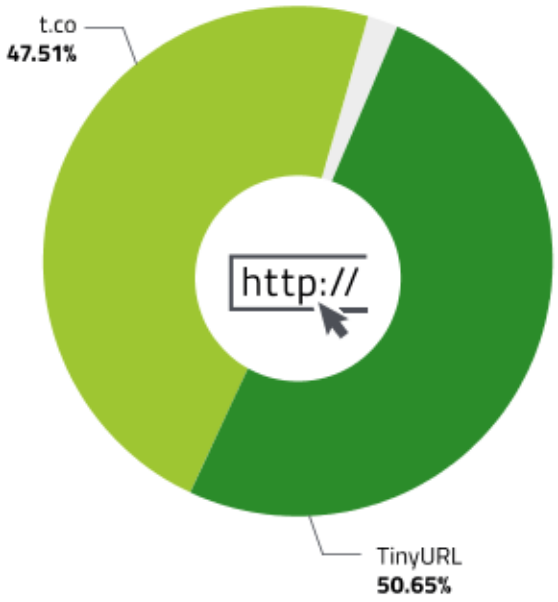


Figure 2 : Les deux principaux coupables en ce qui concerne les URL malveillantes dans la catégorie Modificateur de lien URL

Le stockage dans le cloud peut également présenter un risque pour les utilisateurs. Bien que le domaine lui-même ne soit pas classé comme malveillant, le chemin de l'URL peut l'être. Par exemple, l'utilisateur peut recevoir un lien vers le service Cloud, mais le fichier vers lequel pointe l'URL peut être malveillant. L'année dernière, 3 % des chemins d'URL de stockage dans le Cloud étaient malveillants, une augmentation significative par rapport au chiffre observé en 2018, soit 1,28 %.

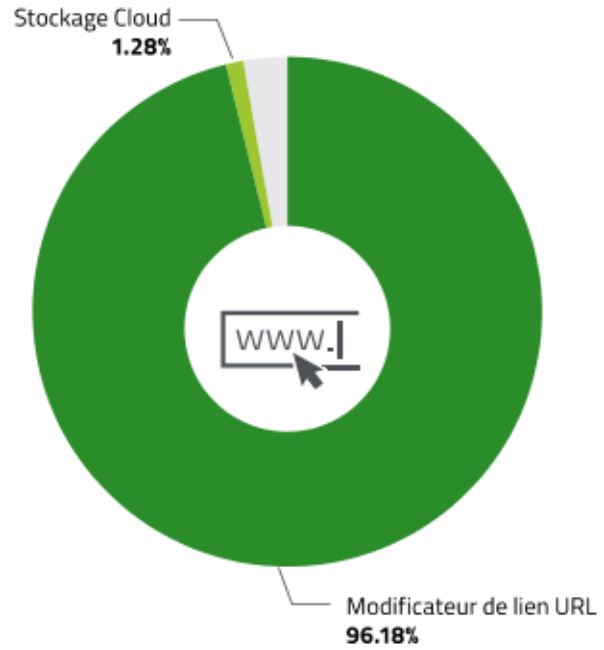


Figure 3 : Distribution de contenu malveillant sur des domaines fiables parmi les 10 000 domaines les plus populaires d'Alexa

La distribution de contenu malveillant se produit dans de nombreux types de domaines bénins, comme en témoigne le million de domaines les plus populaires d'Alexa.

Catégorie des URL	Pourcentage hébergeant une mauvaise URL
Production	19.87 %
Logiciels contributifs / Torrents	11.84 %
Sites pour adultes	9.43 %
Réseaux sociaux	8.71 %
Loisirs	8.63 %
Médicaments	7.66 %
Modificateur de lien URL	5.81 %
Autre	28.06 %

Figure 4 : Principales catégories de sites hébergeant des URL malveillantes en 2019

Bien qu'il soit facile de comprendre comment les partagiciels / torrents, les sites pour adultes et les réseaux sociaux peuvent être des véhicules évidents pour la distribution de contenu malveillant, il n'est pas si évident de comprendre pourquoi d'autres sites apparaissent dans la liste. La production, par exemple, arrive en tête de liste en tant que catégorie la plus ciblée. Cela peut être dû au fait que les sites de production sont moins susceptibles d'être corrigés et parfaitement à jour, ce qui les rend plus vulnérables. Les organisations de production entretiennent également des relations complexes au niveau des chaînes d'approvisionnement qui sont souvent pilotées par des API susceptibles de faire l'objet d'attaques. Comme nous l'avons indiqué dans la section Logiciels malveillants, les appareils de production ont connu un taux d'infection légèrement plus élevé que la moyenne globale des clients Webroot ayant indiqué leur secteur d'activité, ce qui confirme l'hypothèse que les cybercriminels pourraient cibler cette industrie. Les sites d'immobilier, d'alimentation et boissons et les blogs font également partie des 10 catégories les plus ciblées.

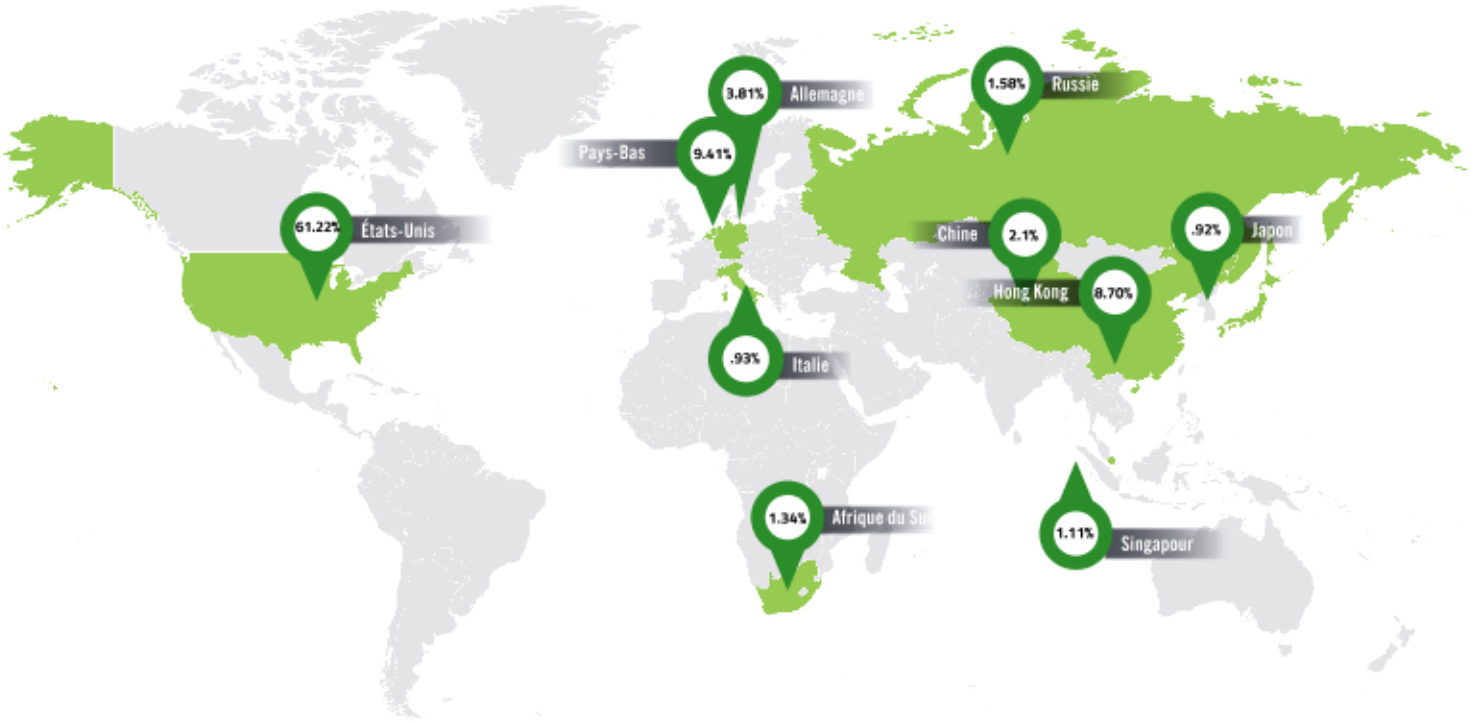


Figure 5 : Les 10 premiers pays hébergeant la majorité des URL à haut risque en 2019

DISTRIBUTION GÉOGRAPHIQUE

En 2019, la liste des dix pays qui hébergeaient la majorité des URL à haut risque était assez semblable à celle de 2018, mais le Royaume-Uni, le Canada et la France n'y figurent plus. Ils ont été remplacés par l'Afrique du Sud, Singapour et l'Italie (tous représentant moins de 5 % du total).

Comme nous l'avons vu l'année dernière, la majorité des sites hébergeant des logiciels malveillants proviennent des États-Unis. Ce pourcentage est resté relativement stable, en légère hausse par rapport aux 63 % l'an dernier.*

CRYPTOJACKING ET CRYPTOMINAGE

En 2018, le cryptojacking (une pratique consistant à utiliser des programmes basés sur un navigateur pour extraire de la crypto-monnaie à l'insu ou sans le consentement de l'utilisateur) et le cryptominage (un logiciel malveillant qui usurpe le processeur d'un utilisateur pour extraire de la crypto-monnaie) sont devenus des menaces majeures. Les cybercriminels pouvaient utiliser ces méthodes pour monétiser aisément leurs attaques, et la valeur extrêmement élevée de la crypto-monnaie a rendu cette pratique assez lucrative. Des vols, piratages et opérations de minage massives ont fait la une des journaux.

Le cryptojacking est resté une pratique répandu en 2019. Des millions de dollars en crypto-monnaie ont été dérobés via des transactions de crypto-monnaies au cours de l'année.[6] Un type d'attaque sur routeur extrêmement dangereux, qui peut créer un script sur chaque page Web, s'est répandu. Le problème a pris suffisamment d'ampleur pour attirer l'attention des forces de l'ordre ; une opération de cinq mois coordonnée par INTERPOL a entraîné une baisse de 78 % du nombre de routeurs infectés par des mineurs de cryptomonnaies situés en Asie du Sud-Est.[7]

En 2019, Webroot a identifié plus de 146 000 domaines hébergeant des scripts de cryptojacking, ce qui représente 8,9 millions d'URL hébergeant un script de cryptojacking.

Bien que l'année 2019 se soit terminée avec un recul significatif du nombre d'URL de cryptojacking en décembre par rapport au moins de janvier, des pics notables ont été observés tout au long de l'année, et les sites continuent d'exploiter cette technique. Les statistiques ont été particulièrement affectées par la fermeture de Coinhive, l'acteur majeur dans ce domaine. Début 2019, Coinhive représentait 84,5 % de l'activité de cryptominage. À la fin de l'année, malgré sa fermeture, l'organisation, représentait toujours 60,67 % de l'activité. En mars, près de 700 000 URL exécutaient le script. À la fin de l'année, Coinhive fonctionnait toujours, mais ne s'adonnait plus à des activités de minage. Le fait que les scripts Coinhive demeurent actifs dans de nombreux domaines suggère qu'ils ont probablement été placés par des acteurs malveillants, à l'insu des propriétaires de site Web.

8,9 millions d'URL hébergent un script de cryptojacking.

* Remarque : ce chiffre inclut les sites de phishing, ce qui peut expliquer le pourcentage élevé provenant des États-Unis. Les URL malveillantes se trouvent souvent dans la même région géographique que leurs cibles, et la plus forte densité de clients Webroot se trouve aux États-Unis.

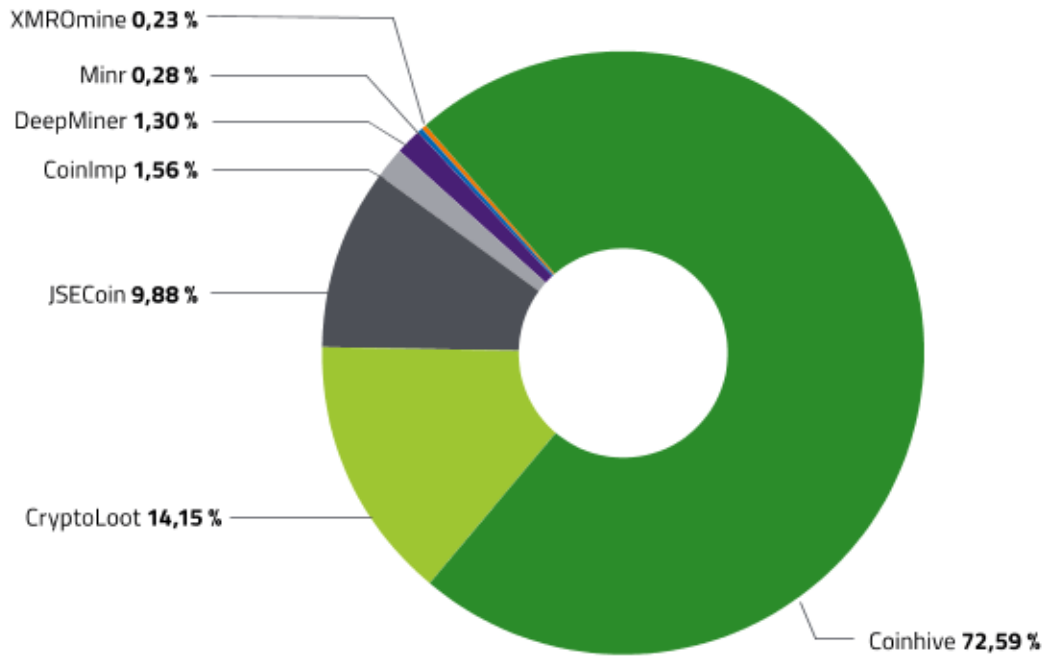


Figure 6 : URL hébergeant un script de cryptojacking, suivies à travers les sept services de cryptojacking les plus répandus (Remarque : Coinhive ne s'adonne plus à des activités de minage.)

Le vide engendré par la dissolution de Coinhive a été en partie comblé par CryptoLoot (14,15 % du trafic vers les sites de crypto), JSEcoin (9,88 %) et CoinImp (1,56 %). Dans l'ensemble, presque tous les services de cryptojacking ont enregistré une baisse tout au long de l'année, à l'exception de CoinImp, qui a affiché une légère augmentation. Les 20 principaux domaines représentent 25 % de l'ensemble du trafic client vers les domaines de cryptojacking.

Tout comme l'année dernière, nous avons observé une diminution progressive des détections sur les points de terminaison tout au long de l'année ; 22 % des incidents de cryptojacking de l'année ont été détectés en début d'année, tandis que ce chiffre a baissé entre 7 et 8 % à la fin de l'année. Cela est probablement dû au renforcement de la sécurité basée sur le navigateur pour mieux lutter contre les cryptomineurs du Web.

ass1st.com	5.64 %
tpbproxyone.org	2.48 %
rotate4refs.com	1.93 %
propertiesyoulike.com	1.66 %
smokingarchive.com	1.63 %
anddev.org	1.32 %
cheatcodesgalore.com	1.10 %
vidics.to	1.05 %
koinohajimari.com	0.98 %
erogifs.com	0.94 %
airproxyunblocked.org	0.89 %
warly.ir	0.77 %
svobdoska.ru	0.73 %
oklahomaball.com	0.71 %
themelike.net	0.62 %
nepallist.com	0.60 %
coinhive.com	0.60 %
boya.com.sg	0.59 %
pepitos.tv	0.59 %
thepiratebay.bet	0.57 %

Figure 7 : Les 20 principaux domaines de cryptojacking

ATTAQUES DE PHISHING

Bien que le hameçonnage existe depuis bien plus de dix ans, il a considérablement évolué. Les premières tentatives « ratissaient large » et étaient envoyées à un grand nombre de destinataires, sans distinction. Cependant, les pirates ont appris par la suite que s'ils pouvaient cibler leurs victimes de manière sélective via le hameçonnage, ils pourraient augmenter leurs chances de réussite. La richesse des informations personnelles librement partagées sur les réseaux sociaux leur a permis de se familiariser beaucoup plus facilement avec les habitudes en ligne d'une victime donnée, ce qui facilite la création d'e-mails de phishing ciblés et spécifiquement destinés à cette personne.

Le piratage des chaînes de réponse par e-mail constitue un exemple récent de l'évolution continue du phishing. Un pirate informatique accède au compte e-mail d'une personne et prend le relais d'une conversation légitime, puis la transmet à l'un de ses amis ou collègues avec une charge utile malveillante. L'e-mail est susceptible de passer par n'importe quel filtrage d'e-mail et le destinataire est susceptible de l'ouvrir, car les détails de la conversation sont convaincants, car réels. Cependant, l'ouverture du fichier pourrait entraîner une infection par Emotet ou un autre cheval de Troie bancaire, tel que Ursnif / Gozi.

D'année en année, nous continuons de constater une croissance des attaques par hameçonnage, qui restent un vecteur efficace pour capturer les informations d'identification et autres données sensibles. La menace est omniprésente ; 1,6 % des clients Webroot rencontrent une page de hameçonnage chaque mois, ce qui représente environ 20 % des clients de la solution de protection des points de terminaison Webroot chaque année. Dans l'ensemble, le nombre de sites de hameçonnage connus a été multiplié par six entre janvier et décembre 2019 : de 0,15 % à 0,96 % de tous les sites. L'augmentation du nombre de sites de hameçonnage HTTPS a constitué l'évolution du phishing la plus marquée que nous avons constatée en 2019. En 2018, 15 % des sites de hameçonnage ont utilisé le protocole HTTPS pour inciter l'utilisateur à penser que le site était sûr ; en 2019, ce pourcentage est passé à 27 %.

LES ENTREPRISES LES PLUS SOUVENT VICTIMES D'USURPATION D'IDENTITÉ

En général, parmi les entreprises les plus victimes d'usurpation d'identité dans le cadre d'attaques de hameçonnage en 2019, huit d'entre elles faisaient déjà partie des dix entreprises les plus usurpées en 2018. Chase (à 3,1 %) a remplacé Bank of America, qui est sorti de ce « top 10 », mais continue de figurer dans le top 20, à 2,4 %.*

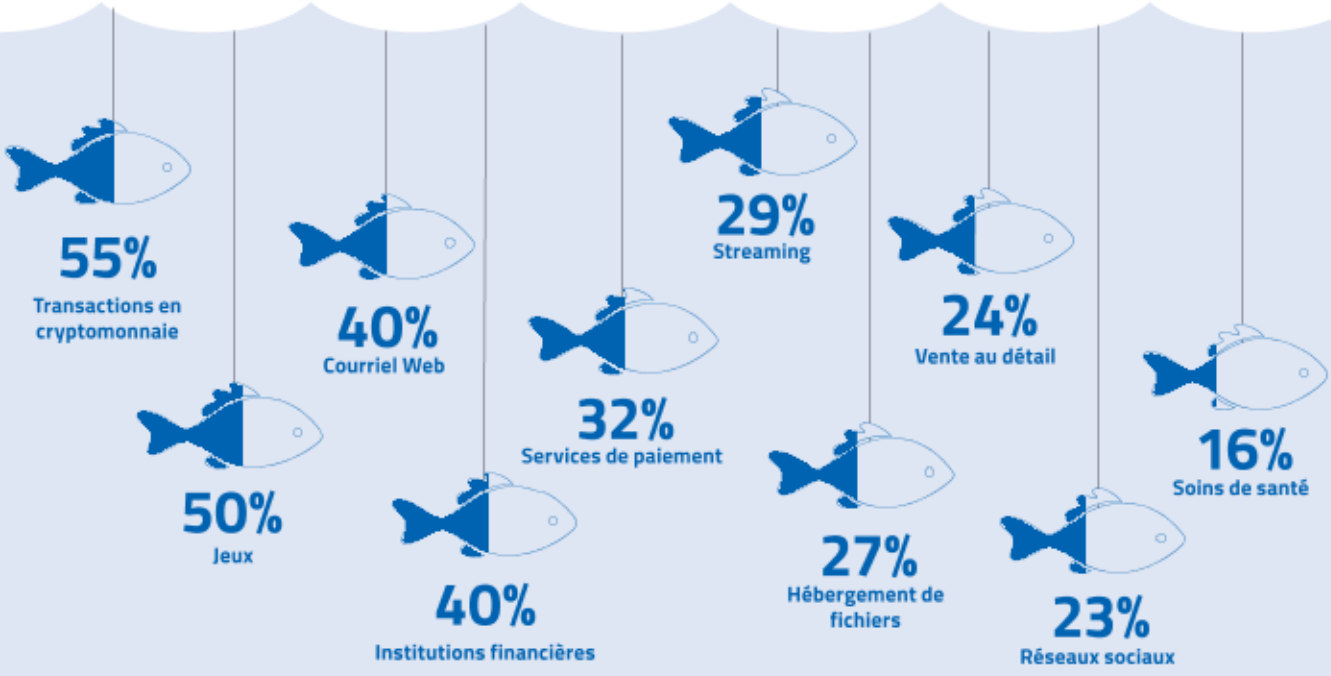


Figure 8 : Les 10 industries les plus ciblées par l'hébergement HTTPS

* Les données Webroot proviennent de notre clientèle utilisant une protection des points de terminaison, laquelle est principalement située aux États-Unis, par conséquent les données suivantes traduisent essentiellement les habitudes en ligne américaines.

L'année dernière, Google était en tête de liste avec 15,6 %, suivi de Microsoft, Dropbox et PayPal. Lorsque nous étendons la liste au top 20, nous trouvons de nombreux autres noms familiers, tels qu'Amazon et Netflix, ainsi que DocuSign, Instagram et Steam. DocuSign est un participant particulièrement intéressant en raison de son utilisation fréquente comme moyen de signature électronique de documents importants ; usurper l'identité de DocuSign pourrait conduire une victime sans méfiance à renseigner un formulaire avec des informations personnelles, pensant que les données seront transmises à un utilisateur légitime. De même, le service de distribution numérique de jeux vidéo Steam, qui permet des mises à jour automatiques des jeux, pourrait servir à télécharger des logiciels malveillants sur un appareil.

Sur une base mensuelle, les attaques contre les dix marques les plus victimes d'usurpation d'identité nous révèlent des faits intéressants. Microsoft a débuté l'année en enregistrant un taux d'attaques de hameçonnage destinées à usurper son identité plus de deux fois supérieur à celui de Facebook. Le nombre a atteint un pic de mars à mai, puis a diminué de façon spectaculaire avant de bondir à nouveau en octobre. Les attaques se faisant passer pour Apple ont quadruplé en mars, puis ont chuté et ont de nouveau augmenté en octobre. (Ceci est probablement lié aux dates de sortie de produits Apple®.) Les attaques contre Google ont démarré lentement dans l'année, mais ont connu une augmentation constante jusqu'à ce que le nombre d'attaques soit à égalité avec celui de Microsoft et d'Apple. De plus, Office 365 et Google Cloud ont tous deux été ciblés par des cybermenaces. Par exemple, une menace de hameçonnage a récemment fait son apparition, laquelle utilise des mots de passe usurpés à des fins de tactiques effrayantes dans le cadre de campagnes de spam. La réutilisation effrénée des mots de passe et l'activité intense sur les réseaux sociaux permettent aux pirates de cibler leurs victimes et de les effrayer en révélant leurs informations d'identification. De plus, l'IA est de plus en plus utilisée pour créer des campagnes pluridimensionnelles, par conséquent les utilisateurs ont de plus en plus de mal à distinguer les e-mails de hameçonnage des campagnes de communication légitimes.

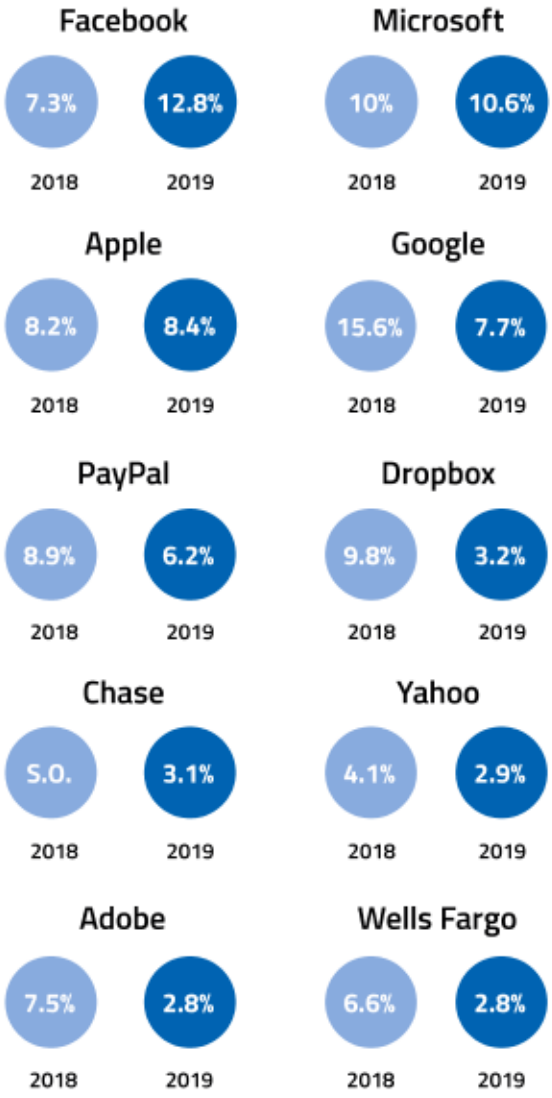


Figure 9 : Les 10 entreprises les plus ciblées par les usurpations d'identité dans les attaques de hameçonnage

LES ATTAQUES ENTRAÎNANT LA COMPROMISSION DES E-MAILS PROFESSIONNELS NE FAIBLISSENT PAS

Comme par le passé, les attaques entraînant la compromission de la messagerie en entreprise (BEC, Business Email Compromise) restent largement répandues. Ce type de fraude par e-mail cible les organisations commerciales, gouvernementales et à but non lucratif en se faisant passer frauduleusement pour un collègue membre de la direction générale ou pour un client de confiance. Ce type d'e-mail contient généralement des instructions indiquant d'envoyer une certaine somme d'argent (généralement par virement bancaire) ou pour divulguer des données client. Les BEC exploitent essentiellement la confiance inhérente des employés envers leurs cadres supérieurs et leurs précieux clients. Le géant de l'édition Nikkei a perdu environ 29 millions de dollars US après qu'un employé de la filiale Nikkei America a été dupé par des escrocs et a transféré des fonds sur un compte bancaire contrôlé par ces derniers (novembre 2019). Un individu lituanien a plaidé coupable d'une escroquerie au BEC ayant dupé des employés de Google et de Facebook, lesquels lui ont transféré 112 millions de dollars US (mars 2019).[8] Selon le FBI, le BEC est une arnaque rapportant globalement 26 milliards de dollars US aux malfaiteurs, qui a enregistré une augmentation de 100 % au niveau des pertes exposées mondiales identifiées entre mai 2018 et juillet 2019.[9] AIG Insurance affirme que les BEC sont devenues la première raison de dépôt de réclamation de cyberassurance par les entreprises dans la région EMEA l'année dernière, surpassant ainsi les rançongiciels et les violations de données.[10]

ADRESSES IP MALVEILLANTES

Au cours des dix dernières années, nous avons constaté l'impact de Tor sur la cybersécurité. Nous avons constaté que des réseaux proxy en couches étaient utilisés pour protéger les acteurs malveillants contre toute exposition, et nous avons observé l'essor de l'hébergement de logiciels malveillants en tant que service. En 2019, nous avons identifié de très nombreuses réutilisations d'IP malveillantes dans l'espace IPv4, ce dernier étant entièrement alloué et attribué. Cependant, IPv6 changera complètement la donne. Jusqu'à présent, l'espace IPv6 permet aux attaquants d'utiliser plus facilement de nouvelles adresses lors du lancement de leurs attaques.

Plus de 26 millions d'incidents de sécurité liés aux IP sont identifiés chaque jour.

Webroot suit les adresses IP via les activités malveillantes qu'elles réalisent (par exemple, scanners ou proxy, spam, exploits Windows, attaques Web, botnets, phishing et menaces mobiles), afin de les bloquer de manière proactive. Dans l'ensemble, 88 % du total des adresses IP malveillantes en 2019 étaient malveillantes en raison de déclencheurs de spam répétitifs. Le nombre total est astronomique ; en une journée, nous avons identifié jusqu'à 4,6 millions d'adresses IP spams. Aux fins de ce rapport, cependant, nous ne présentons pas les millions d'IP que nous suivons, mais nous présentons nos observations concernant les 50 000 IP malveillantes les plus récurrentes, c'est-à-dire celles enregistrant le plus grand nombre de transactions malveillantes observées.

RÉPARTITION GÉOGRAPHIQUE

Les IP malveillantes sont un phénomène mondial. Les 50 000 IP malveillantes les plus répandues couvrent 184 pays. En effet, si nous nous fions aux condamnations de ces IP, 80,6 % d'entre elles proviennent de 23 pays et plus de la moitié ne proviennent que de six pays.

Les six premiers pays à l'origine de 50 % des IP malveillantes :

- États-Unis
- Chine
- Vietnam
- Russie
- Inde
- Indonésie

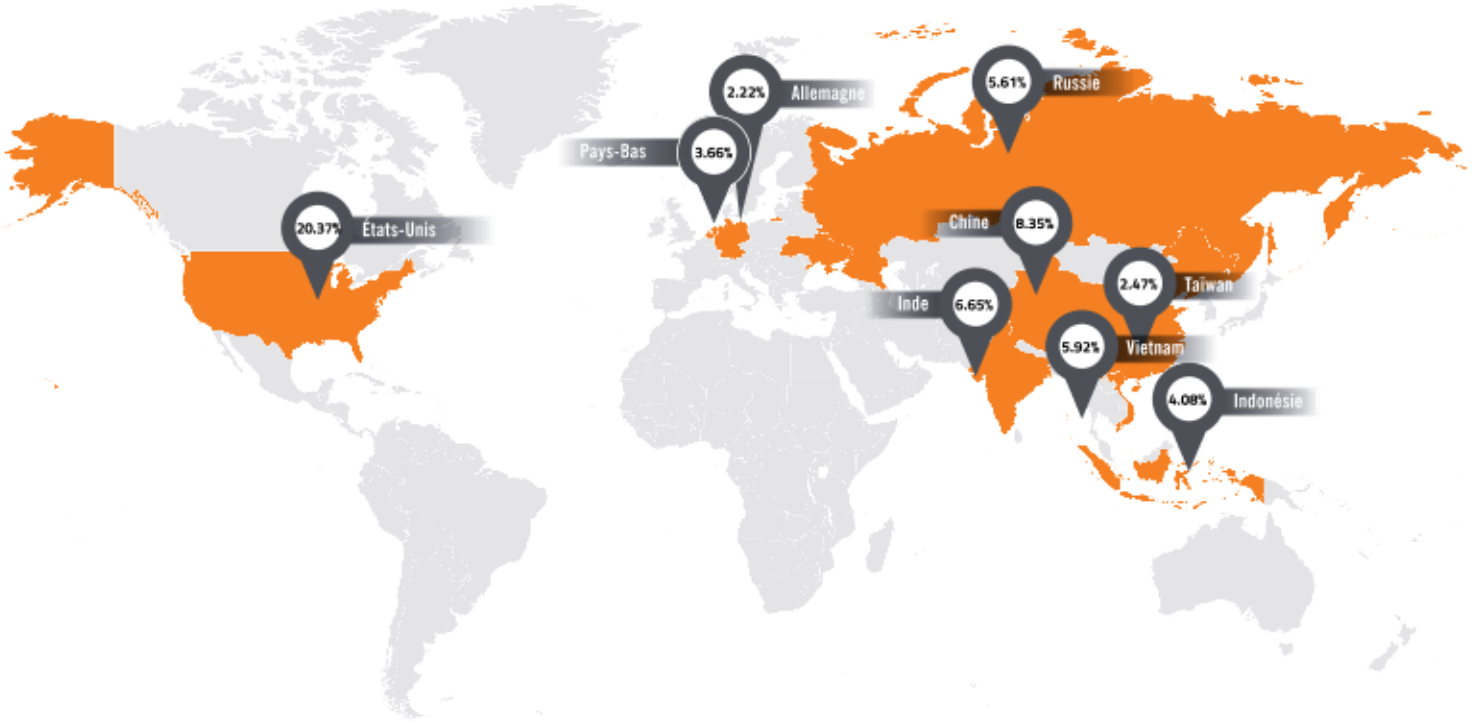


Figure 10 : IP malveillantes par région géographique

Pour compléter le top 10 :

- Pays-Bas
- Ukraine
- Taïwan
- Allemagne

Webroot suit les IP malveillantes de plusieurs manières : via les IP elles-mêmes, via le nombre total d'IP dans chaque catégorie, et via les condamnations. Le terme « condamnation » fait référence au nombre de fois où un comportement malveillant a conduit à classer l'IP comme malveillante ou risquée, et non pas fiable. (Une IP peut présenter plusieurs types de comportements, tels que le spam, le botnet et l'exploit Windows.) Lorsque l'on examine le nombre d'IP, 60 % des IP malveillantes sont réparties dans 10 pays. Toutefois, parmi les 10 premiers pays à l'origine des IP malveillantes, tous comptent des IP présentant des comportements malveillants cinq fois ou plus et 25 pays comptent des IP condamnées dans six catégories ou plus.

UN REGARD APPROFONDI SUR LES IP

Le spam reste le principal comportement des IP malveillantes cette année. Cependant, les réseaux zombies ont augmenté, passant de seulement 3 % l'an dernier à 8 % cette année, et les scanners représentent toujours un pourcentage important du total des 50 000 principales IP malveillantes (16 %), malgré une légère baisse par rapport aux 19 % de l'an dernier.

L'incidence des IP malveillantes utilisées pour le scanning a quelque peu diminué, mais les scanners représentent toujours une menace importante. Les pirates informatiques analysent les environnements pour en savoir plus sur les configurations réseau, les applications utilisées et le comportement des utilisateurs ; armés de ces informations, ils peuvent sélectionner des cibles plus lucratives et adapter les attaques à cet environnement spécifique.

Les exploits Windows représentent une tendance alarmante, malgré le fait qu'il s'agisse d'une catégorie relativement faible. Par exemple, les pirates peuvent rechercher des systèmes qui contiennent des vulnérabilités Windows qui n'ont pas été mises à jour (comme EternalBlue, mentionné plus haut) et les exploiter en déployant des logiciels malveillants ciblés. Le nombre d'IP associées aux exploits Windows a connu la plus forte croissance parmi toutes les catégories en 2019, passant d'environ 26 000 en janvier à plus de 120 000 en décembre. Il s'agit d'une augmentation de 360 %.

DES COMPORTEMENTS MULTIPLES

Les IP malveillantes sont à l'origine de plusieurs types de comportements malveillants. En effet, les 50 000 principales adresses IP malveillantes ont été condamnées dans quatre catégories ou plus. De plus, elles apparaissent plusieurs fois ; 96 % des adresses IP malveillantes ont réalisé des activités malveillantes plusieurs fois.

Faits essentiels sur les adresses IP malveillantes

- 92,9 % ont été condamnées dans au moins 4 catégories
- Seulement 3,4 % des IP malveillantes ont été condamnées une seule fois au cours de l'année
- Plus de 7 millions d'IP ont été condamnées plus de 37 fois au cours de l'année
- Les IP se classant dans l'un pour cent des IP les plus malveillantes ont été condamnées plus de 337 fois en 2019 seulement

Les adresses IP associées aux exploits Windows ont augmenté de 360 %.

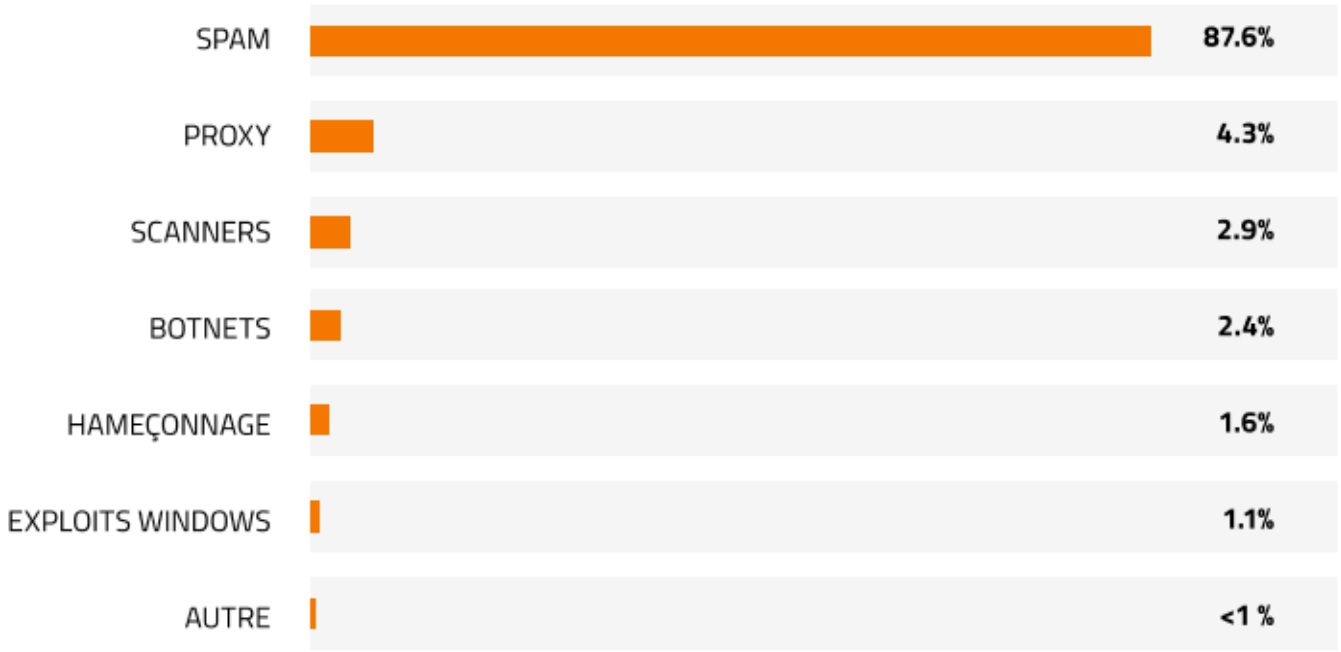


Figure 11 : Activité des IP malveillantes par catégorie

APPLICATIONS MOBILES NOCIVES

Depuis leur lancement, les appareils Android™ ont connu une période particulièrement difficile en matière de sécurité ; plusieurs vulnérabilités critiques ont été décelées au cours de la dernière décennie, et une autre vulnérabilité majeure a été découverte en novembre 2019. Google continue de lutter contre les applications mobiles malveillantes, mais la nature de son système d'exploitation ouvert entrave ses efforts.

Bien que les logiciels malveillants Android ne soient pas aussi répandus que les logiciels malveillants Windows, ils restent une menace réelle et croissante pour environ 120,5 millions d'utilisateurs Android aux États-Unis.[11] À ce jour, des centaines d'applications malveillantes ont été retirées du Google Play Store grâce à un processus d'examen qui implique à la fois des algorithmes informatiques et des équipes humaines chargées de leur examen. Après avoir mis en place un nouveau contrôle plus strict des développeurs souhaitant publier leurs premières applications sur Google Play, Google estime que la probabilité de télécharger une application potentiellement dangereuse (PHA) était de 0,64 % en 2018, et ce risque est beaucoup plus faible si les applications sont téléchargées depuis Google Play.[12]

Néanmoins, il existe encore de nombreuses applications présentant des problèmes de sécurité. Google a détecté un logiciel malveillant dénommé Joker (alias Bread) dans 17 000 applications Android, qu'il a ensuite supprimées du Play Store. Une analyse du code a révélé que les opérateurs de Joker ont utilisé pratiquement toutes les techniques d'obscurcissement disponibles pour échapper à la détection. Étant donné que l'appareil Android moyen comprend entre 100 et 400 applications préinstallées, le risque de failles de sécurité reste élevé.

Pour les utilisateurs mobiles protégés par Webroot, le taux d'infection était de 4,6 % en 2019. Les infections se répartissaient dans plusieurs catégories, les chevaux de Troie et les logiciels malveillants représentant la grande majorité d'entre elles.

40 % des appareils Android utilisent un système d'exploitation antérieur à la version v9, ce qui constitue un problème récurrent. Comme pour les appareils Windows, les appareils non corrigés et plus anciens sont plus vulnérables aux applications malveillantes. Par exemple, l'exploit Bad Binder permet à une application malveillante de rooter et de prendre le contrôle total d'un appareil. Android 9 et les versions précédentes sont affectées par cet exploit, et les anciennes versions du système d'exploitation peuvent être victimes d'exploits encore plus anciens. Les applications conçues pour exploiter des exploits plus anciens ont toujours des chances de parvenir à leurs fins sur les appareils plus anciens qui ne peuvent être mis à jour vers une version plus sécurisée.

Quelle que soit la méthode d'attaque ou l'intention, un code mobile malveillant peut causer des problèmes aux utilisateurs car le pirate peut accéder aux données vocales, aux messages SMS et aux e-mails, surveiller toutes les frappes, accéder à la caméra, suivre l'emplacement de l'appareil via le GPS et bien plus encore. Il est aisé de comprendre pourquoi les téléphones mobiles sont très recherchés en vue d'une compromission.

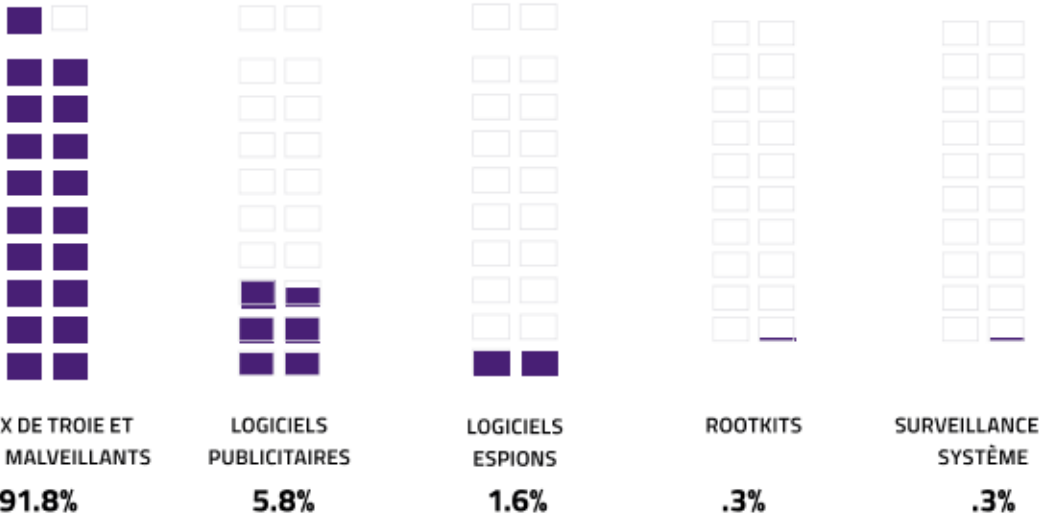


Figure 12 : Panne causée par une application malveillante (Remarque : 12,5 % d'entre elles ont été classées comme étant des applications potentiellement indésirables ou PUA.)

FORMATION DE SENSIBILISATION À LA SÉCURITÉ

Les nouvelles innovations introduisent toujours de nouveaux dangers, mais les formations contribuent grandement à réduire ces risques. L'éducation préventive à la cybersécurité (formation de sensibilisation à la sécurité) est un domaine qui ne cesse de croître et qui s'avère très efficace pour réduire les incidents de sécurité liés à l'ingénierie sociale, tels que le hameçonnage, lesquels sont souvent à l'origine d'infractions de vaste ampleur. Des individus formés constituent la première ligne de défense et contribuent à protéger les données sensibles, la propriété intellectuelle et la viabilité de l'organisation elle-même.

En 2019, nous avons constaté que les organisations qui menaient à bien 1 à 5 campagnes de sensibilisation à la sécurité sur une période d'un à deux mois affichaient un taux de clic moyen de 37 % sur les simulations de phishing. Cependant, l'exécution de 6 à 10 campagnes et la dispense de formations sur une période de trois à quatre mois réduisaient le taux de clics à 28 %. Ces chiffres se sont encore améliorés lorsque l'organisation a dispensé 11 cours ou plus sur une période de 4 à 6 mois : le taux est tombé à 13 %. Ce type de formation est particulièrement pertinent dans la lutte contre le BEC (voir la section Hameçonnage) où d'importantes sommes d'argent pourraient être en jeu.

Le succès accru des formations régulières est dû au fait que les utilisateurs doivent être armés contre des attaques de hameçonnage ciblées, très variables et de plus en plus sophistiquées, d'autant que ces attaques exploitent souvent des tendances et événements d'actualité. Nous avons récemment observé, par exemple, des notifications de livraison de colis, des alertes selon lesquelles les mots de passe de certains sites de réseaux sociaux devaient être modifiés ou indiquant l'expiration d'une carte bancaire, à mettre à jour pour continuer de bénéficier d'un service particulier. Tout thème ou tendance actuelle est bon à prendre pour les pirates informatiques, qui peuvent s'adapter rapidement pour modifier leurs méthodes de spam. Les utilisateurs ont besoin d'une formation continue et pertinente pour ne pas tomber dans ces pièges.

Le fait de dispenser 11 formations ou plus sur 4 à 6 mois réduit le nombre de clics sur des contenus de hameçonnage de

PRÉVISIONS

Les experts en sécurité de Webroot tirent parti des leçons du passé pour prévoir ce que nous observerons en 2020 et dans les années à venir. Voici quelques-unes de leurs prévisions :

QUELLES MENACES VONT ÉMERGER ?

« Attendez-vous à voir davantage d'attaques contre les pays moins développés, non pas pour récolter de l'argent, mais plutôt pour déstabiliser et détruire », déclare Grayson Milbourne, directeur des renseignements de sécurité. Il prévoit que le hameçonnage deviendra encore plus ciblé, car les données collectées suite à des infractions sont ensuite intégrées aux e-mails de phishing.

« Emotet conservera sa position de leader, tant au niveau de la taille de son réseau zombie que de l'ampleur de ses spams malveillants distribués. Les rançongiciels resteront une menace. Des acteurs moins sophistiqués imiteront les tactiques utilisées par des opérations plus efficaces et de plus vaste ampleur. »

Jason Davison | Analyste de recherche avancée sur les menaces

Eric Klonowski, Directeur de la recherche sur les menaces avancées, prévoit que les attaquants avides de rançons étudieront attentivement les solutions de sauvegarde automatique et tenteront de supprimer et / ou de modifier les données sauvegardées ou la tâche elle-même. Tyler Moffitt, analyste de sécurité, ajoute que, compte tenu des réglementations en vigueur en termes de confidentialité telles que le RGPD et le CCPA, il se pourrait que des rançongiciels menacent de divulguer des données clients importantes pour augmenter les chances de paiement des rançons par les entreprises, même si celles-ci disposent des sauvegardes adéquates en place et n'ont pas besoin de récupérer ces fichiers.

QUI SERA CIBLÉ ?

Tyler Moffitt pense que les PME continueront d'être ciblées : elles disposent de budgets plus modestes et comptent peu de personnel de sécurité, ce qui en fait des cibles de choix. Kelvin Murray, analyste principal de la recherche sur les menaces, indique que la formation des utilisateurs constitue la principale protection contre les attaques BEC. Aucune solution de filtrage des e-mails ne sera assez puissante pour bloquer tous les faux e-mails.

« Tout le secteur de l'énergie continuera d'être gravement menacé. En outre, les fournisseurs de services constituent des cibles très lucratives pour les attaquants, car ils constituent un point d'entrée unique dans de nombreuses entreprises. Les cadres continueront d'être la cible d'attaques BEC, lesquelles seront de plus en plus sophistiquées. »

Matthew Aldridge | Architecte de solutions principal

QUEL RÔLE JOUERA L'IA / L'APPRENTISSAGE AUTOMATIQUE ?

Hal Lonas, Vice-président général et directeur technique, nous avertit que les cybercriminels vont de plus en plus exploiter l'intelligence artificielle, ce qui entraînera une augmentation de l'ampleur et de la gravité des attaques en 2020. Dans le même ordre d'idées, Joe Jaroch, directeur principal de la stratégie de cybersécurité, estime que les attaques contre des produits de sécurité basés sur l'IA gagneront à la fois en complexité et en ampleur.

L'un des scénarios les plus effrayants implique l'utilisation de l'IA dans la production de deepfakes (ou hypertrucage). En 2019, nous avons vu les premiers exemples de technologie de synthèse d'images basée sur l'IA de style deepfake déployés avec succès afin de rendre les attaques d'ingénierie sociale encore plus convaincantes.

« Les deepfakes vont devenir une menace majeure. À mesure que la technologie se développe, n'importe qui pourrait faire une fausse vidéo de quelqu'un d'autre disant quelque chose qu'il n'a pas fait, et pourrait effectivement l'exploiter à des fins malveillantes (ou politiques). »

Grayson Milbourne | Directeur du renseignement de sécurité

LE CRYPTOJACKING EST-IL MORT ?

Bien que nous constations un déclin du cryptojacking au cours de l'année écoulée, cette baisse ne fait que refléter, selon Tyler Moffitt, le cours mondial du marché des crypto-monnaies. Si le cours des crypto-monnaies grimpe à nouveau pour atteindre un niveau record durant l'année à venir, nous verrons probablement une résurgence de ce type d'attaque. Matthew Aldridge prévoit que le cryptojacking perdurera en 2020, comme moyen discret pour les criminels de gagner de l'argent en exploitant les ressources des autres. Il prévoit que les malfaiteurs trouveront de nouveaux types d'appareils et réseaux informatiques à cibler, qui leur permettront de mieux rentabiliser le temps investi pour élaborer une attaque, en utilisant des moyens de plus en plus intelligents pour éviter la détection.

CONCLUSION

Si l'on se réfère à 2019 et aux années précédentes, les changements sont clairs. Nous avons observé un mouvement massif vers le cloud, une évolution des demandes des utilisateurs (parfois contradictoires) en matière de confidentialité, de sécurité et de commodité, des innovations constantes de la part des cybercriminels et une surface d'attaque en constante expansion.

En termes d'efforts de protection, le volume et la variation des attaques nécessitent une approche globale et multicouche. Cela doit commencer par les individus eux-mêmes. Il faut les sensibiliser et les former pour qu'ils apprennent à éviter les risques et qu'ils signalent tout incident suspect rapidement et correctement. Il convient ensuite d'introduire des couches de défense supplémentaires afin de s'assurer que si des utilisateurs cliquent par inadvertance sur un lien malveillant, l'opération sera bloquée de manière préventive. (Après tout, même les utilisateurs les plus avertis peuvent faire des erreurs.) S'ils essaient de visiter une adresse IP malveillante, une couche de sécurité doit être en place pour les en empêcher. S'ils tentent de visiter un site de hameçonnage, une autre couche doit être en place pour les protéger. S'ils exécutent un script malveillant, celui-ci doit être bloqué. S'ils tentent d'exécuter un programme malveillant, ou si une application apparemment fiable s'avère malveillante, cela doit être bloqué également.

Et si toutes ces méthodes échouent, toutes les données critiques doivent être sauvegardées en toute sécurité dans le cadre d'une stratégie complète de protection et de reprise après sinistre.

En fin de compte, il n'y a pas de solution miracle, il n'y en a jamais eu et il n'y en aura jamais. Toutefois, en mettant en place des couches de sécurité qui protègent les utilisateurs et les données à chaque étape d'une attaque, il est possible d'atteindre un état de « cyber-résilience », dans lequel les entreprises et les utilisateurs finaux peuvent rebondir, même en cas de violations de sécurité massives, de cyberattaques et de perte de données.

Hal Lonas | Vice-président général et directeur technique, PME et consommateur

[1] Verizon. « 2010 Verizon Data Breach Investigations Report » (Rapport Verizon sur les enquêtes de violations des données en 2010). (Juillet 2010) https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf

[2] « The Untold Story of NotPetya, the Most Devastating Cyberattack in History » (L'histoire inédite de NotPetya, la cyberattaque la plus dévastatrice de l'histoire). Extrait de www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

[3] « Magic Quadrant for Security Awareness Computer-Based Training » (Magic Quadrant pour la formation informatique à la sensibilisation à la sécurité). Extrait de www.gartner.com/doc/reprints?id=1-1QAYVTNP&ct=190723&st=sb

[4] « Ransomware Payments Rise as Public Sector is Targeted, New Variants Enter the Market » (Les paiements de rançongiciels augmentent à mesure que le secteur public est ciblé, de nouvelles variantes arrivent sur le marché). Extrait de www.coveware.com/blog/q3-ransomware-marketplace-report

[5] « Spanish companies' networks shut down as result of ransomware » (Les réseaux d'entreprises espagnoles hors service suite à des rançongiciels). Extrait de arstechnica.com/information-technology/2019/11/spanish-companies-networks-shut-down-as-result-of-ransomware/

[6] « Bitcoin remains strong as 160 million stolen from crypto exchanges in 2019 » (Le Bitcoin reste solide, avec 160 millions dérobés lors de transactions en cryptomonnaies en 2019). Extrait de cryptoslate.com/bitcoin-remains-strong-as-160-million-stolen-from-crypto-exchanges-in-2019

[7] « Cryptojacking Drops by 78% in Southeast Asia After INTERPOL Action » (Le cryptojacking chute de 78 % en Asie du Sud-Est après l'intervention d'INTERPOL). Extrait de www.bleepingcomputer.com/news/security/cryptojacking-drops-by-78-percent-in-southeast-asia-after-interpol-action

[8] « Tech Duo Stung for $122m by BEC Attacker » (Tech Duo Stung subit des pertes s'élevant à 122 millions de dollars suite à une attaque BEC). Extrait de www.infosecurity-magazine.com/news/tech-duo-stung-for-122m-by-bec-1?

[9] « Business Email Compromise Is a $26 Billion Scam Says the FBI » (Les attaques entraînant la compromission de la messagerie en entreprise (BEC) rapportent 26 milliards de dollars US selon le FBI). Extrait de bleepingcomputer.com/news/security/business-email-compromise-is-a-26-billion-scam-says-the-fbi/

[10] « BEC overtakes ransomware and data breaches in cyber-insurance claims » (Les attaques par BEC deviennent le premier facteur de réclamations reçues par les cyberassurances, surpassant ainsi les rançongiciels et les violations de données). Extrait de www.zdnet.com/article/bec-overtakes-ransomware-and-data-breaches-in-cyber-insurance-claims

[11] « Number of Android smartphone users in the United States from 2014 to 2021 » (Nombre d'utilisateurs de smartphones Android aux États-Unis de 2014 à 2021). Extrait de www.statista.com/statistics/232786/forecast-of-android-users-in-the-us

[12] « To Stop Shady Apps, Google To Scrutinize First-Time Developers. » (Pour contrer les applications malveillantes, Google met en place un examen rigoureux des nouveaux développeurs). Extrait de uk.pcmag.com/news-analysis/120501/to-stop-shady-apps-google-to-scrutinize-first-time-developers

À propos de Webroot et de Carbonite

Webroot et Carbonite, des sociétés OpenText, exploitent le potentiel du cloud et de l'intelligence artificielle pour protéger les entreprises et les particuliers contre les cybermenaces et les menaces naturelles qui pèsent sur les données. Les fournisseurs de services gérés et les petites entreprises nous font confiance pour la protection des points d'accès et des réseaux, de même que pour les formations de sensibilisation à la sécurité et pour des solutions de sauvegarde des données et de reprises après sinistre. Webroot BrightCloud® Threat Intelligence Services est utilisé par des entreprises de premier plan telles que Cisco, F5 Networks, Citrix, Aruba A10 Networks, et bien d'autres encore. Webroot et Carbonite exploitent la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Webroot et Carbonite sont implantés en Amérique du Nord, en Europe, en Australie et en Asie. Découvrez les solutions de sécurité des points de terminaison et de reprise après sinistre sur carbonite.com et webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com