État des malwares 2019

Préparé par

Malwarebytes LABS

Table des matières

Résumé

L'année 2018 a démarré sur les chapeaux de roue et a continué sur cette lancée, malgré quelques variations sur la période. On peut affirmer sans se tromper qu'en dépit d'un deuxième trimestre plus calme, l'année a été explosive du début à la fin. Le boom des programmes de minage de cryptomonnaies au dernier trimestre 2017 était encore dans tous les esprits lorsque, début 2018, les tactiques de minage se sont diversifiées en s'étendant à Android, Mac et aux malwares de minage, et ont innové dans des attaques basées sur navigateur.

Le minage de cryptomonnaies s'est essoufflé au deuxième trimestre, mais de nouvelles menaces se tenaient prêtes à les remplacer : les voleurs d'informations. Ces anciens chevaux de Troie, en particulier Emotet et TrickBot, ont évolué en injecteurs pourvus de modules multiples pour la production de spams, la propagation latérale via des réseaux, le skimming de données et même le vol de portefeuilles de cryptomonnaies. Ces variantes de malwares se sont attaquées aux entreprises, en cherchant à tirer profit de données ultrasensibles pouvant être revendues au marché noir et réutilisées à des fins de ciblage dans de futures campagnes.

Toujours dans le monde de l'entreprise, d'autres familles de malwares n'ont pas tardé à emboîter le pas à Emotet et TrickBot, en se focalisant sur les réseaux d'organisations peu sûrs et n'ayant pas reçu assez de correctifs. On peut dire qu'elles ont eu l'embarras du choix. Entre intrusions informatiques d'envergure et attaques de ransomwares mettant KO des infrastructures critiques, les entreprises ont vécu ce que les particuliers connaissent depuis des années maintenant, mais à une échelle beaucoup plus importante et dangereuse.

Par conséquent, 2018 se termine sur des problématiques différentes selon les types d'utilisateurs, annonçant déjà une année 2019 tout aussi tumultueuse.

Méthodologie

Contrairement à nos rapports « Tactiques et techniques du cybercrime » trimestriels, qui font le point sur les chiffres recueillis sur une période de trois mois, notre rapport annuel sur l'état des malwares compare la période qui va de janvier à novembre 2018 à la même période sur l'année 2017. Nous regroupons les renseignements recueillis par nos chercheurs et ceux collectés par les pots de miel, les sandbox virtuels et les données télémétriques issues de nos produits consommateur et entreprise, afin d'identifier les grandes menaces et les tendances de l'année, tant en volume qu'en distribution.

En outre, notre rapport annuel examine les menaces par région (Amérique du Nord, Asie-Pacifique, Amérique latine et Europe, Moyen Orient et Afrique [EMEA]), ainsi que les industries les plus touchées par les principales formes de malware.

Sans plus attendre, découvrez vite ce que nous avons appris sur l'état des malwares en 2018.

Les 10 enseignements clés

Place au minage de cryptomonnaies

Les ransomwares ont été détrônés durant la première moitié de 2018 par l'arrivée massive des programmes de minage de cryptomonnaies, suite à la hausse fulgurante de la valeur du bitcoin à la toute fin de l'année 2017. Les cybercriminels ont de toute évidence abandonné toute autre forme d'attaque pour expérimenter cette nouvelle technique, qui s'est étendue aux ordinateurs de bureau, aux appareils mobiles, aux systèmes d'exploitation Mac, Windows et Android, et aux attaques basées sur logiciel et sur navigateur. La détection des programmes de minage de cryptomonnaies a augmenté de 7 % par rapport à l'année précédente, un pourcentage au final faible, étant donné que la seconde moitié de l'année a été calme à ce niveau.

L'année des intrusions de masse

Contrairement à l'épidémie de ransomwares qui avait caractérisé 2017, aucune attaque internationale de grande envergure n'a été à déplorer en 2018. L'année a été plutôt marquée par des intrusions de masse. De grandes entreprises, telles que Facebook, Marriott, Exactis, MyHeritage et Quora ont été infiltrées et des centaines de millions de clients affectés. Le nombre d'événements de compromission a augmenté de 133 % en 2018 par rapport à l'année précédente.

Les ransomwares sont plus sophistiqués

En 2018, un glissement s'est opéré du côté des techniques d'attaque par ransomware. Au lieu de l'acte en deux coups caractéristique des exploits de malvertising distribuant leurs charges utiles de ransomware, les menaces ont pris la forme d'attaques manuelles et ciblées. L'approche tous azimuts a été remplacée par des attaques par force brute, comme on a pu le constater lors des campagnes SamSam les plus abouties de l'année.

Les entreprises accusent le coup

Lors de la seconde moitié de 2018, les auteurs de malware se sont détournés des consommateurs pour se focaliser sur les organisations, misant sur le fait que les entreprises représentaient des victimes pourvoyeuses de profits bien plus élevés que les individus. La détection globale des malwares dans les entreprises a augmenté de façon importante au cours de l'année écoulée (79 % exactement), principalement en raison de la prolifération des backdoors, programmes de minage, spywares et voleurs d'informations.

La détection côté consommateurs baisse de façon minime

Malgré le ciblage accru des entreprises, la détection de malwares chez les consommateurs a diminué de 3 % seulement par rapport à l'année précédente, à cause de la présence de backdoors, chevaux de Troie et spywares tout au long de 2018. 775 327 346 menaces ont été détectées chez les consommateurs en 2017, et environ 25 millions de moins en 2018, une baisse encourageante en termes d'instances d'infection, si on laisse de côté les pourcentages.

Les vulnérabilités SMB ont permis la diffusion virulente des chevaux de Troie

Les répercussions de la fuite d'exploits de la NSA orchestrée par les Shadow Brokers en 2017 continuent à se faire sentir, puisque les cybercriminels se sont servis des failles SMB EternalBlue et EternalRomance pour lancer des chevaux de Troie dangereux et sophistiqués, tels qu'Emotet et TrickBot. En réalité, les voleurs d'informations ont représenté la plus grande menace tant côté entreprise que consommateur en 2018, ainsi que la menace régionale numéro un pour l'Amérique du Nord, l'Amérique latine et la zone EMEA (Europe, Moyen-Orient et Afrique).

Les malspams remplacent les exploits en tant que vecteur d'attaque privilégié

Les exploits se sont faits plus rares en fin d'année 2017, du fait de l'arrestation de nombreux créateurs de kits. Par conséquent, les pirates se sont tournés vers un vieil outil bien connu, le malspam, qui a remplacé les exploits à la première place des mécanismes de distribution des menaces en 2018.

Les fausses extensions et applications malveillantes font leur apparition dans les boutiques en ligne légitimes

La sécurité des navigateurs est devenue d'une importance cruciale depuis que de fausses applications et extensions trompent les utilisateurs, mais aussi les plateformes de téléchargement d'applications, en passant insidieusement outre les contrôles de sécurité de Google Play et d'iTunes, ainsi que des boutiques Web officielles de Chrome, Firefox, Safari et d'autres encore, à l'aide de tactiques d'ingénierie sociale sournoises.

Des attaques de sites Web pour dérober des données d'utilisateur

Le groupe criminel Magecart est à l'origine d'une série d'attaques médiatisées contre des sites Web de commerce en ligne visant à extorquer des informations de carte bancaire et d'autres informations d'identification personnelle sur les plateformes de paiement, en texte clair et en temps réel.

Arnaques par sextorsion

Enfin, les grandes arnaques de l'année ont exploité de vieilles informations d'identification personnelle recueillies lors d'intrusions passées. Des e-mails d'hameçonnage ont été envoyés à des millions d'utilisateurs dans le cadre de tentatives d'extorsion (voir, dans certains cas, de sextorsion). Les mots de passe anciens mais potentiellement toujours utilisés des victimes ont été subtilisés, et celles-ci ont alors reçu des demandes de rançons les menaçant de dévoiler leurs secrets en cas de non-paiement.

Classement des détections en 2018

Détections chez les consommateurs

Dans notre rapport « Tactiques et techniques du cybercrime » du troisième trimestre 2018, nous avions noté une baisse du nombre de menaces contre les consommateurs. Si l'on prend en considération l'année entière, on observe que la quantité totale de détections de malwares n'a que très peu évolué entre 2017 et 2018. De façon surprenante, la baisse globale n'est que de 3 % par rapport à l'année précédente, du fait d'une forte hausse des détections de chevaux de Troie, de backdoors et de spywares.

Menaces détectées chez les consommateurs, évolution 2017/2018		
Pos.	**Menace**	**Évolution A/A en %**
1	Adwares	**-39 %**
2	Cheval de Troie	**19 %**
3	Logiciel à risque	**7 %**
4	Backdoor	**34 %**
5	Outils de piratage	**-36 %**
6	Hijacker	**-84 %**
7	Vers	**-28 %**
8	Spywares	**27 %**
9	Ransomwares	**-29 %**
10	Rogues	**-39 %**
Total des détections		
2017	**775 327 346**	**-3 %**
2018	**750 296 307**	

Figure 1. Classement des 10 menaces consommateur principales détectées par Malwarebytes en 2018

Ceci étant, nous avons observé un déclin de nombreux types de malware qui ne ciblaient auparavant que les consommateurs. Sur l'année, nous avons relevé davantage d'attaques contre les entreprises, détecté plus de malwares sur leurs terminaux, et constaté une plus grande attention des cybercriminels sur ce qu'ils considèrent être une plus grande source de profit.

Les adwares ont chuté de manière spectaculaire, tout comme les outils de piratage, les hijackers, les vers, les ransomwares et les rogues. Ce déclin est probablement dû au fait que ces types de malware sont souvent détectés ensemble, étant donné qu'ils entraînent des modifications système similaires sur les machines affectées. Par exemple, de nombreuses modifications de système causées par les adwares sont identifiées et corrigées par notre outil de détection des hijackers, et les détections d'hijackers ont baissé de 84 %.

Nous avons également observé une hausse des détections de chevaux de Troie, de RiskwareTools (le nom que nous employons pour parler du minage de cryptomonnaies), de backdoors et de spywares en 2018, hausse importante dans plus d'un cas. L'exemple de Backdoor.Vools, le backdoor que nous détectons le plus actuellement, a été repéré partout dans le monde cette année, alors qu'il n'existait même pas l'année d'avant. La hausse des détections de backdoors, de spywares et de chevaux de Troie est liée au phénomène actuel d'exploitation de failles, telles qu'EternalBlue, dans le but de s'infiltrer dans un réseau en y injectant des malwares.

D'un autre côté, la légère augmentation globale des détections de RiskwareTool est due à l'afflux massif de malwares de minage en début d'année, qui a fini par se tarir en milieu d'année.

Détection de BitCoinMiner pour les consommateurs en 2018

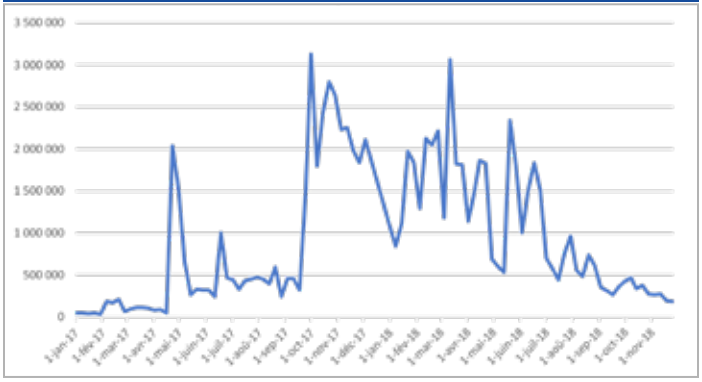

Figure 2. Détection de la menace RiskWare.BitCoinMiner chez les consommateurs en 2018

RiskWare.BitCoinMiner, le programme de minage que nous détectons le plus, a progressivement décliné courant 2018. En juillet, sa fréquence de détection était redevenue comparable à ce que nous observions début 2017. Nous avons toutefois enregistré un léger pic de détection qui a débuté mi-septembre.

Le minage de cryptomonnaies en 2017

Figure 3. Pic de détection des programmes de minage à l'automne 2017

Ce pic a précédé d'environ un mois la hausse de la valeur du bitcoin qui s'est produite en octobre 2017. Il est possible que les criminels à l'origine de ces activités de minage aient su quelque chose que le reste du monde ignorait.

Cours du Bitcoin Core (BTC), juin à déc. 2018

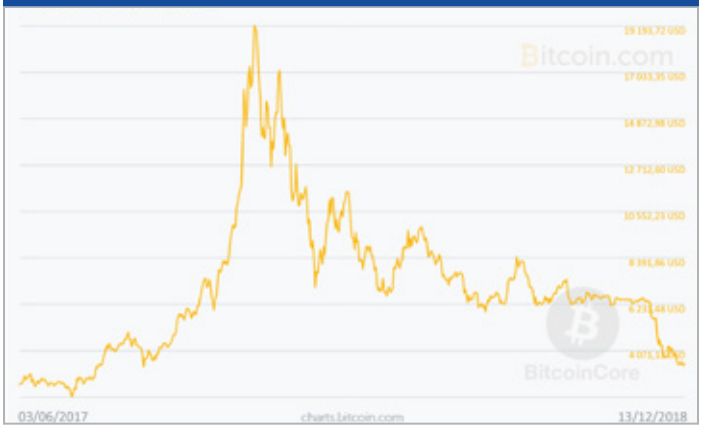

Figure 4. La hausse de la valeur du bitcoin en octobre 2017. Crédit photo : Bitcoin 2018

Une quantité impressionnante de programmes de minage de cryptomonnaies a été déployée entre octobre 2017 et mars 2018. Au même moment, les malwares dirigés contre les consommateurs enregistraient également une légère hausse. Il est à noter toutefois que la fièvre de la cryptomonnaie est retombée quelques mois après, entraînant une baisse de l'intérêt des cybercriminels envers les consommateurs.

La majorité des menaces que nous voyons en circulation aujourd'hui a recours à des tactiques et techniques que nous avons pu observer par le passé dans des malwares commandités par des États.

Cela signifie que des cibles plus importantes, comme des réseaux de plusieurs terminaux, seront visées plus fréquemment. À moins que nous soyons témoins d'une nouvelle évolution d'attaques de malware contre les consommateurs exploitant spécifiquement les faiblesses au niveau individuel, alors l'intérêt grandissant pour les entreprises pourrait se poursuivre au-delà de la tendance actuelle.

Détection dans les entreprises

Étant donné la baisse de 3 % du nombre global de détections sur les terminaux des consommateurs par rapport à l'année précédente, on pourrait s'attendre à ce que la production de malwares en général soit en baisse. Au contraire, cette tendance montre la perte d'intérêt des cybercriminels pour l'individu lambda, qui se concentrent désormais sur des cibles plus prometteuses telles que les entreprises. Dans les faits, quatre de nos sept détections principales en entreprise ont augmenté de plus de 100 % entre 2017 et 2018.

Menaces détectées dans les entreprises, évolution 2017/2018

Pos.	Menace	Évolution A/A en %
1	Cheval de Troie	132 %
2	Hijacker	43 %
3	Logiciel à risque	126 %
4	Backdoor	173 %
5	Adwares	1 %
6	Spywares	142 %
7	Ransomwares	9 %
8	Vers	-9 %
9	Rogues	-52 %
10	Outils de piratage	-45 %
Total des détections		
2017	39 970 812	79 %
2018	71 823 114	

Figure 5. Classement des 10 menaces entreprise principales détectées par Malwarebytes en 2018

La détection globale des malwares dans les entreprises a augmenté de façon importante au cours de l'année écoulée (79 % exactement), principalement en raison de la prolifération des backdoors, programmes de minage, spywares et voleurs d'informations. La folie des cryptomonnaies n'a pas frappé uniquement les consommateurs ; de nombreux programmes de minage malveillants sont entrés de force dans les réseaux d'entreprise.

Les chevaux de Troie que nous avons détectés ont été dominés par la famille Emotet, capable de se déplacer latéralement dans les réseaux d'entreprise à l'aide d'exploits et d'attaques d'identifiants par force brute. Cette fonctionnalité se retrouve dans d'autres malwares de vol d'informations, tels que TrickBot, mais aussi dans des malwares de backdoor, comme Vools, l'infection de backdoor que nous avons le plus détectée en 2018. Vools utilise ces mêmes exploits pour infecter les terminaux et s'y propager.

Les détections de ransomwares dans le monde de l'entreprise n'ont que peu augmenté cette année, de 9 % exactement, et la plupart d'entre elles provient d'infections de WannaCry en cours, mais dormantes, signalées dans nos systèmes. Bien que nous ayons vu des avancées dans des familles de ransomware telles que GandCrab et SamSam, nous n'avons pas connu d'attaques problématiques telles que celles qui s'étaient produites en 2017.

Enfin, la détection de spywares a connu une hausse significative due à l'identification comme spywares en circulation de variantes et de familles semblables à Emotet et TrickBot. Cette tendance illustre bien l'attention que portent les acteurs de menace au vol d'informations et au contrôle des réseaux d'entreprise.

Menaces régionales

Les attaques de malware ne se focalisent pas toutes sur une région du monde en particulier. En réalité, de nombreuses familles finissent par être présentes dans un grand nombre de pays, car les attaques fonctionnent par opportunités, et Internet n'a pas de frontières (sauf en Chine et en Corée du Nord). Cependant, certaines campagnes sont lancées dans des pays ou régions en misant sur l'idée que leur culture, économie ou climat politique rende les habitants plus vulnérables face à un type de malware.

Bien que le cybercrime soit un problème international et que nous préférions analyser les tendances et événements d'un point de vue global, il nous faut observer de plus près ce qui se passe dans des régions données afin de comprendre les modèles d'attaque, ainsi que les difficultés rencontrées par les clients basés dans ces régions. Nous avons regroupé dans cette section le fruit de nos recherches pour l'Amérique du Nord, l'Asie Pacifique (APAC), l'Europe, le Moyen-Orient et l'Afrique (EMEA) et l'Amérique latine (LATAM).

Amérique du Nord

Détections principales pour l'Amérique du Nord, évolution 2017/2018				
Entreprises		Pos.	Particuliers	
A/A	Menace		Menace	A/A
99 %	Cheval de Troie	1	Adwares	-19 %
33 %	Hijacker	2	Cheval de Troie	7 %
121 %	Logiciels à risque	3	Logiciels à risque	38 %
29 %	Adwares	4	Backdoor	10 %
82 %	Spywares	5	Hijacker	-41 %
11 %	Backdoor	6	Spywares	18 %
-27 %	Vers	7	Outils de piratage	-40 %
-15 %	Ransomwares	8	Rogues	-35 %
-55 %	Rogues	9	Rootkits	-50 %
-64 %	Rootkits	10	Virus	-57 %

Figure 6. Principales menaces consommateur et entreprise en Amérique du Nord

L'Amérique du Nord est principalement touchée par un afflux de malwares de vol d'informations d'entreprise et de programmes de minage de cryptomonnaies dirigés contre les entreprises, à un degré jamais vu auparavant. Côté consommateurs, nous observons une baisse dans la plupart des grandes catégories de détection, à l'exception du minage de cryptomonnaies.

Asie pacifique (APAC)

Classement des détections pour l'APAC en 2018, par rapport à 2017				
Entreprises		Pos.	Particuliers	
A/A	Menace		Menace	A/A
5 137 %	Backdoor	1	Cheval de Troie	88 %
261 %	Cheval de Troie	2	Backdoor	591 %
-48 %	Adwares	3	Adwares	-36 %
170 %	Logiciels à risque	4	Logiciels à risque	-18 %
148 %	Ransomwares	5	Ransomwares	79 %
305 %	Vers	6	Vers	-26 %
50 %	Hijacker	7	Outils de piratage	-25 %
3 690 %	Exploit	8	Exploit	740 %
-7 %	Outils de piratage	9	Spywares	16 %
9 %	Spywares	10	Hijacker	-48 %

Figure 7. Classement des détections en APAC, consommateur et entreprise

La région Asie-Pacifique a connu une forte montée en puissance des backdoors et des exploits contre les terminaux. Étant donné que la première menace de backdoor en 2018 était Vools, une famille de malware qui utilise des exploits pour se propager, il est logique que nous constations une hausse de ces deux types de menace. Cependant, la raison pour laquelle l'APAC a été bien plus ciblée que les autres régions n'apparaît pas encore clairement.

Côté consommateur, nous avons observé les mêmes pics de détection de backdoors et d'exploits, en même temps qu'une baisse de la plupart des autres types de malware.

Europe, Moyen-Orient et Afrique (EMEA)

Classement des détections pour l'EMEA en 2018, par rapport à 2017				
Entreprises		Pos.	Particuliers	
A/A	Menace		Menace	A/A
150 %	Cheval de Troie	1	Adwares	-40 %
122 %	Hijacker	2	Cheval de Troie	-15 %
-59 %	Adwares	3	Logiciels à risque	-23 %
20 %	Logiciels à risque	4	Outils de piratage	-41 %
-6 %	Backdoor	5	Backdoor	-15 %
-41 %	Outils de piratage	6	Vers	-5 %
-1 %	Spywares	7	Spywares	25 %
-14 %	Ransomwares	8	Hijacker	-57 %
-37 %	Vers	9	Ransomwares	-53 %
-56 %	Rogues	10	Rogues	-62 %

Figure 8. Classement des détections en EMEA, consommateur et entreprise

La région Europe, Moyen-Orient et Afrique (EMEA) s'est retrouvée en proie aux mêmes problématiques que l'Amérique du Nord. Nous savons que derrière l'augmentation de 150 % de l'activité des chevaux de Troie pour les entreprises de l'EMEA se cache Emotet, comme en Amérique du Nord. Étant donné l'attention soutenue que portent maintenant les cybercriminels à certaines familles de malware, nous observons une chute de presque tous les autres types de menaces.

Malgré des pics intéressants de détection de chevaux de Troie et d'hijackers chez les consommateurs, nous avons globalement observé une baisse significative de presque tous les types de malware, exception faite des spywares. Il s'agit là d'un autre signe qui montre que l'attention des cybercriminels se détourne des consommateurs pour se focaliser sur les entreprises.

Amérique latine (LATAM)

Classement des détections en LATAM en 2018, par rapport à 2017				
Entreprises		Pos.	Particuliers	
A/A	Menace		Menace	A/A
176 %	Cheval de Troie	1	Adwares	-55 %
137 %	Logiciels à risque	2	Cheval de Troie	-1 %
-56 %	Adwares	3	Logiciels à risque	-25 %
137 %	Ransomwares	4	Outils de piratage	-32 %
23 %	Backdoor	5	Backdoor	-33 %
343 %	Spywares	6	Vers	-16 %
101 %	Vers	7	Outils de craquage	-35 %
-47 %	Outils de piratage	8	Spywares	43 %
-60 %	Hijacker	9	Ransomwares	59 %
473 %	Rootkits	10	Outils de fraude	-97 %

Figure 9. Classement des détections en LATAM

L'Amérique latine a vécu une année remarquable sur le plan du développement des malwares. Les cybercriminels qui ciblent cette région ont lancé en grande quantité toutes sortes de malwares contre les entreprises, depuis les chevaux de Troie aux programmes de minage, en passant par les spywares et même les rootkits, se détournant de tout le reste. Les organisations qui travaillent avec la région LATAM ont tout intérêt à renforcer rapidement leur sécurité, car l'année à venir pourrait être celle d'une avancée encore plus spectaculaire de ces menaces.

Tandis que la distribution de malwares a été soutenue du côté des entreprises, on ne peut pas en dire autant pour les consommateurs. En effet, la seule augmentation que nous avons observée concerne les spywares et les ransomwares. Il faut cependant garder à l'esprit que de nombreux ransomwares détectés cette année sont liés à la mise en circulation de WannaCry, qui identifie les systèmes vulnérables et les infecte, sans toutefois chiffrer leurs fichiers. L'infection passe simplement d'un système à un autre, sans répercussions apparentes. Ainsi, nous détectons de nombreuses instances de WannaCry dans des zones où les correctifs contre cette menace n'ont pas été largement appliqués.

Menaces par pays

Classement des 10 pays enregistrant le plus de détections chez les consommateurs		
	Pays	**Menace principale**
1	États-Unis	Vol d'informations
2	Brésil	Fraude au clic
3	Royaume-Uni	Adwares
4	Vietnam	Backdoors
5	Inde	Backdoors
6	Indonésie	Backdoors
7	France	Adwares
8	Italie	Minage de cryptomonnaie
9	Thaïlande	Backdoors
10	Russie	Backdoors

Figure 10. Classement des 10 pays enregistrant le plus de détections chez les consommateurs, et leur principale menace

Les États-Unis prennent la tête de ce classement des détections de malwares chez les consommateurs, cette année ayant été marquée par la menace Emotet. Ce résultat n'est pas vraiment surprenant, puisque les malwares ont tendance à cibler les pays occidentaux, souvent des économies puissantes, et plus particulièrement les États-Unis.

Le Brésil n'est pas en reste en 2018, en proie à des malwares de fraude au clic, tout comme l'année passée. Le Royaume-Uni et la France ont été ciblés par des adwares, plus que par d'autres catégories de malwares. Notez que les capacités des adwares ne sont plus à démontrer. Ceux-ci peuvent en effet modifier les paramètres d'un système et désactiver les logiciels de sécurité pour installer des malwares.

La plus grande menace qui pèse sur les consommateurs dans bon nombre de ces pays entre dans la catégorie des backdoors, un type de malware qui se fraye un chemin dans le système, puis laisse une porte ouverte pour que d'autres menaces puissent y entrer. Le Vietnam, l'Inde, l'Indonésie, la Thaïlande et la Russie (pays de l'APAC pour la plupart) connaissent un réel problème avec les backdoors, dû probablement à un manque de correctifs et de sécurisation des terminaux.

Classement des 10 pays enregistrant le plus de détections dans les entreprises		
	Pays	**Menace principale**
1	États-Unis	Vol d'informations
2	Indonésie	Backdoors
3	Royaume-Uni	Vol d'informations
4	France	Vol d'informations
5	Malaisie	Backdoors
6	Thaïlande	Backdoors
7	Australie	Minage de cryptomonnaie
8	Allemagne	Vol d'informations
9	Brésil	Adwares
10	Philippines	Vol d'informations

Figure 11. Classement des 10 pays enregistrant le plus de détections dans les entreprises, et leur principale menace

Notre classement des 10 pays comptabilisant le plus de détections en entreprise montre que les malwares de vol d'informations représentent un problème de taille en de nombreux points du globe. Cette catégorie de malware infecte un terminal, y dépose d'autres malwares et se déplace latéralement dans le réseau en infectant tous les ordinateurs connectés possibles. À partir de là, le malware peut voler des identifiants, installer d'autres menaces et continuer à se propager par e-mail.

Les pays occidentaux, tels que les États-Unis, le Royaume-Uni, la France et l'Allemagne, semblent avoir particulièrement fait les frais de ces attaques de vol d'informations, même si d'autres pays ont été également touchés. En Asie, des pays tels que l'Indonésie, la Malaisie et la Thaïlande ont dû repousser un afflux de malwares de type backdoor dans leurs réseaux d'entreprise.

D'autres pays, comme l'Australie et le Brésil, attaqués principalement en 2018 par des adwares et du minage du cryptomonnaies, ont de bonnes raisons de s'inquiéter, car de nombreux programmes de minage et familles d'adwares déposent sur leur passage des malwares supplémentaires, modifient les paramètres système, ralentissent les ordinateurs ou exploitent leur puissance de calcul, ou perturbent d'une façon ou d'une autre les opérations.

Menaces par secteur

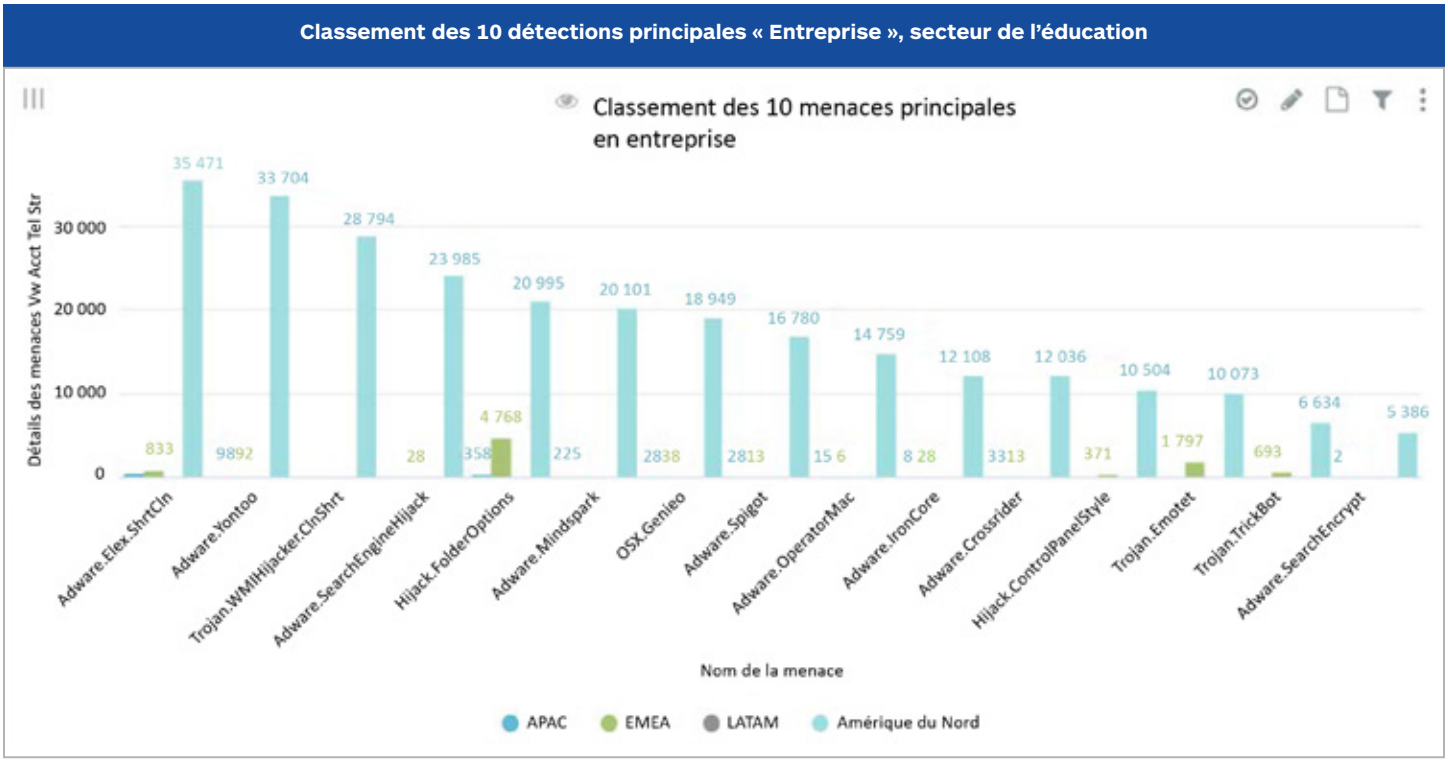

Figure 12. Les 10 principales détections dans le secteur de l'éducation, 2018

L'éducation, la production industrielle et la distribution sont les secteurs les plus touchés par le malware le plus répandu de l'année, les chevaux de Troie. Cependant, si l'on observe de plus près la catégorie des chevaux de Troie et sa famille dominante, Emotet, on aperçoit des différences entre les secteurs. Le conseil figure en première place du classement et l'hôtellerie apparaît à la quatrième place.

Les ransomwares ont quant à eux ciblé d'autres industries. Le conseil apparaît encore une fois comme la cible de prédilection des auteurs de malwares, et l'éducation le talonne à la deuxième place. La production industrielle, la distribution et l'administration complètent ce top cinq.

Si l'on adopte une autre approche et que l'on trie nos données télémétriques sur les produits d'entreprise plutôt en fonction du secteur, quelles tendances se dégagent ? Par exemple, on constate que l'éducation, citée dans presque toutes nos catégories de menaces, a été frappée le plus durement en 2018 par les adwares.

Notons aussi que deux familles de malwares dirigées contre Mac (OSX.Genieo et Adware.OperatorMac) font partie de ce classement, ce qui prouve la popularité des Mac dans le secteur de l'éducation et en tant que cibles spécifiques.

Dans le même temps, le conseil, qui occupe la première place du classement tant pour les ransomwares que pour la famille de chevaux de Troie Emotet, a aussi été victime d'autres attaques de chevaux de Troie, de type bancaires, downloader et packer. Les backdoors, les hijackers et les vers ont eux aussi jeté leur dévolu sur le secteur du conseil en 2018.

Classement des 10 détections principales « Entreprise », secteur de la santé

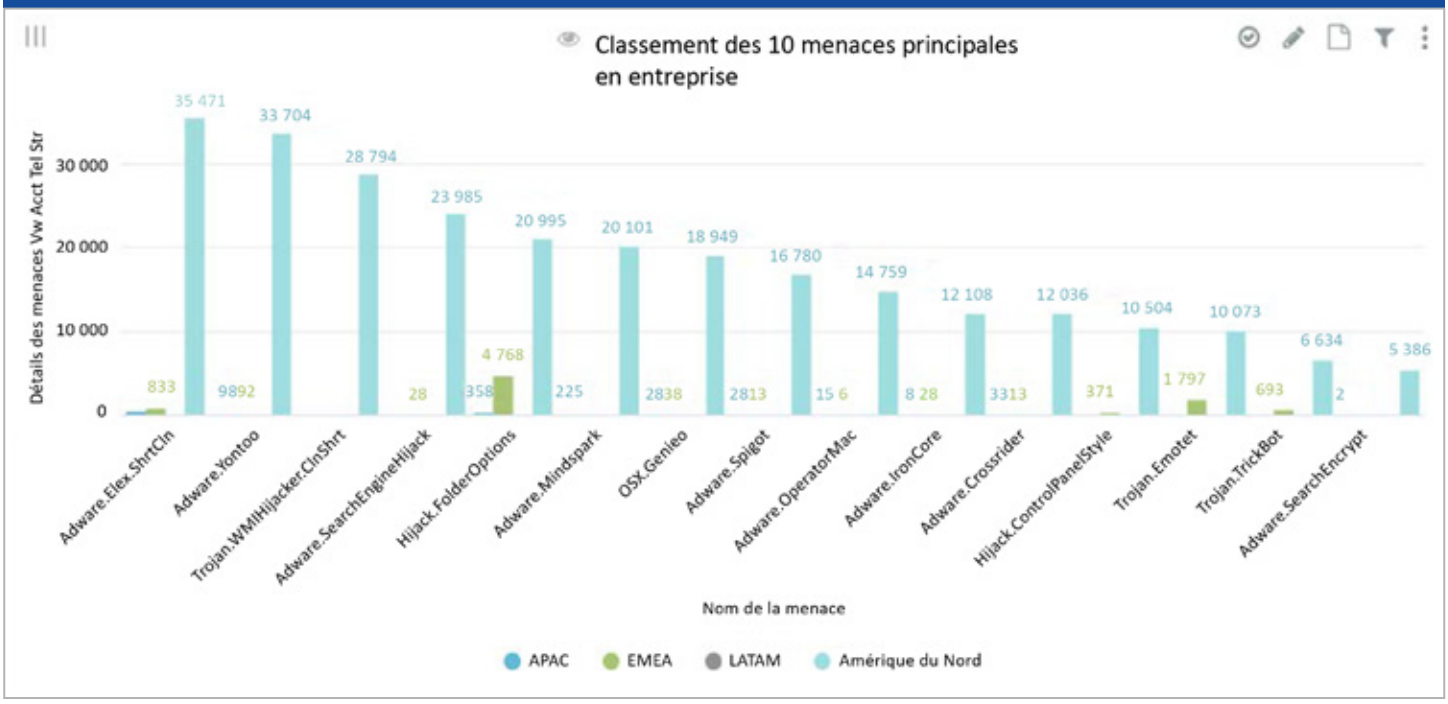

Figure 13. Les 10 plus grandes menaces qui frappent le secteur de la santé

Le nombre d'attaques contre le secteur de la santé et les gouvernements en 2018 reste presque anecdotique, malgré les faits divers marquants qui ont égrené l'année. Ces secteurs n'entrent parfois même pas dans nos classements des 10 industries les plus touchées par les menaces les plus remarquées de l'année. Cependant, en ce qui concerne le secteur de la santé, on peut identifier clairement les formes de malware qui s'y sont attaquées : Emotet et TrickBot, nos nouveaux « Bonnie et Clyde ». Les hijackers, rootkits et autres logiciels à risque complètent ce classement des principales menaces dans le secteur de la santé.

Les menaces dirigées contre les gouvernements sont sensiblement similaires à celles affectant la santé, bien que les hijackers dépassent Emotet, qui n'arrive qu'en deuxième place. En outre, d'autres variantes d'adware entrent dans ce classement, tandis que TrickBot est resté en dehors des attaques contre les gouvernements.

Malwares notables

Bien que la présence de catégories telles que les adwares et les backdoors se fasse fortement sentir, ce sont bien les chevaux de Troie (voleurs d'informations) et les programmes de minage de cryptomonnaies qui sont les grandes vedettes de l'année. Les ransomwares, quant à eux, ont opéré des changements discrets, mais conséquents, en toile de fond. Observons de plus près ces menaces et leurs conséquences sur les consommateurs et les entreprises en 2018.

Programmes de minage

Dans nos prédictions de sécurité pour 2018, nous commencions par annoncer que la « ruée vers l'or » du minage de cryptomonnaies serait la priorité des cybercriminels. Et nous avons pu constater qu'un certain nombre de menaces, surfant sur la vague de la valorisation des cryptomonnaies, distribuait des programmes de minage sous forme binaire classique, ou bien via du minage intempestif.

Minage sur les appareils infectés

Les criminels du Web ont lancé toute une variété de programmes de minage, parfois plusieurs sur une même victime, via des kits d'exploit, parmi lesquels RIG. Contrairement à d'autres menaces, les ransomwares par exemple, ce type de malware cherche à passer inaperçu. Les besoins en termes de cycles de processeur sont souvent le premier signe que quelque chose ne va pas ; le fonctionnement des machines ralentit, mais leurs ventilateurs continuent à tourner à plein régime.

Minage intempestif : même sans infection

Côté navigateurs, le minage intempestif est rapidement devenu notre menace Web la plus couramment détectée, éclipsant complètement les kits d'exploit. Grâce à des failles présentes dans les systèmes de gestion de contenu (CMS), et en particulier via les tristement célèbres campagnes Drupalgeddon, les cybercriminels ont injecté des scripts de cryptojacking dans des sites Web au cours des premier et deuxième trimestres.

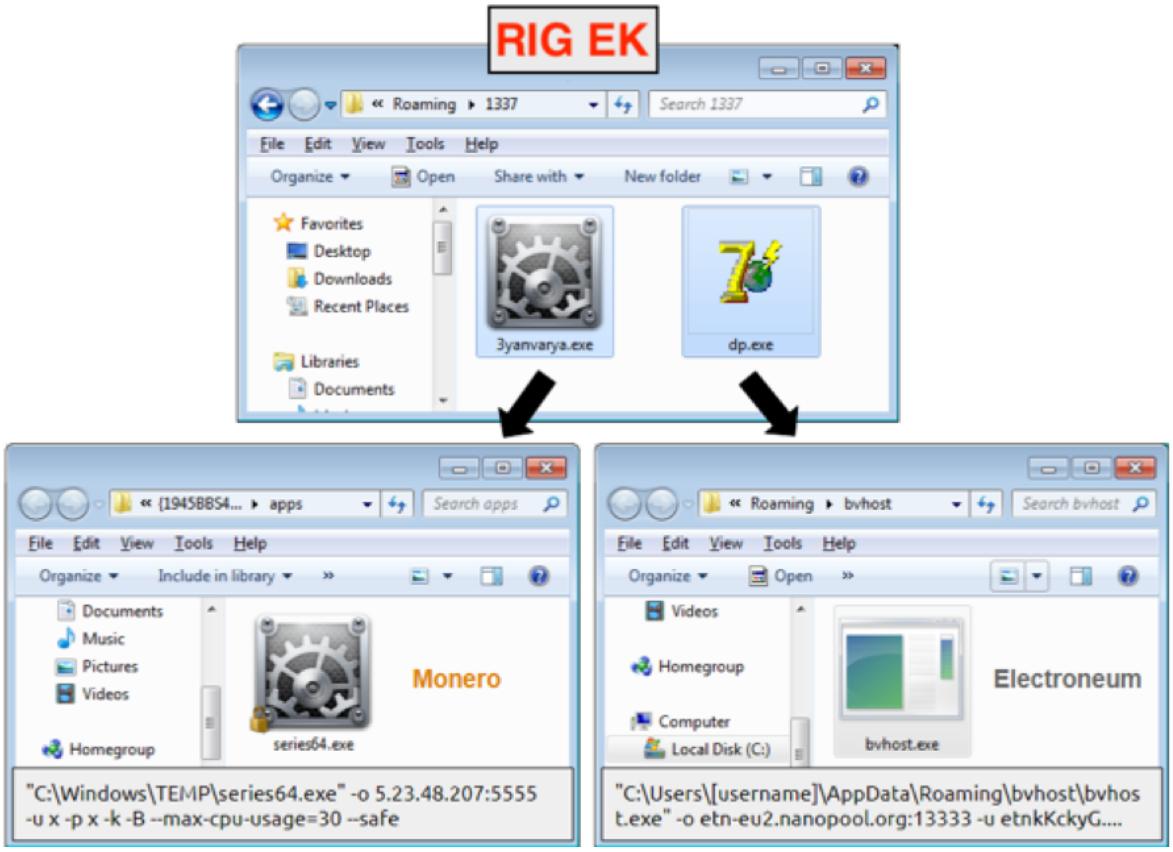

Figure 14. RIG EK dépose des programmes de minage Monero et Electroneum

#	Server IP	Protocol	Host	URL	Body	Comments
882	223.165.64.100	HTTP	www.nzsap.org	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
883	13.228.219.59	HTTPS	www.odysseypremier.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
884	118.143.50.216	HTTPS	www.orbusneich.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
885	136.243.4.40	HTTP	www.pixshock.net	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
886	52.64.6.39	HTTP	www.progility.com.au	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
887	143.106.32.80	HTTPS	www.prp.unicamp.br	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
888	35.200.201.129	HTTPS	www.questin.co	/sites/default/files/advag...	365,227	Drupal Drive-by Mining HTML/JS
889	80.241.209.95	HTTPS	www.radiodogo.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
890	139.162.23.226	HTTP	www.sankalpindia.net	/sites/default/files/js/js_0...	23,757	Drupal Drive-by Mining HTML/JS
891	217.218.243.197	HTTP	www.semnaniau.ac.ir	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
892	81.246.25.226	HTTPS	www.sesvanderhave.com	/RU/misc/jquery.once.js?...	3,670	Drupal Drive-by Mining HTML/JS
893	173.44.46.188	HTTPS	www.sicrediuniaomsto.coop.br	/sites/default/files/js/js_-...	96,973	Drupal Drive-by Mining HTML/JS
894	202.146.214.234	HTTPS	www.silver-sewing-sisters.com.au	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
895	162.144.65.226	HTTP	www.snellrealestate.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
896	91.194.60.51	HTTP	www.spil.org	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
897	104.200.18.26	HTTP	www.thebigwiki.com	/sites/default/files/js/js_...	98,825	Drupal Drive-by Mining HTML/JS
898	205.186.132.167	HTTPS	www.thenationalpastimemuseum.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
899	104.199.98.224	HTTPS	www.thense.co.uk	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
900	151.80.115.77	HTTPS	www.tmtg.org.uk	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
901	184.168.231.182	HTTPS	www.umbiesoft.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
902	83.169.6.193	HTTP	www.welayetnews.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
903	76.72.163.154	HTTPS	www.wood-mode.com	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
904	23.196.199.47	HTTPS	www.wowengage.com.au	/misc/jquery.once.js?v=1.2	3,670	Drupal Drive-by Mining HTML/JS
905	34.232.250.21	HTTPS	www.xplor.ai	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
906	46.243.119.189	HTTP	www10.pmu.ro	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
907	216.187.97.215	HTTP	www3.zipangcasino.com	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS
908	41.87.228.50	HTTP	zainbspectramedwhl01.spectramed.co.za	/misc/jquery.once.js?v=1.2	3,641	Drupal Drive-by Mining HTML/JS

Figure 15. Des scripts de minage de cryptomonnaie injectés dans des milliers de sites Web Drupal

Le minage à travers les plateformes

D'autres plateformes comme Android ou macOS ont elles aussi été frappées par le minage de cryptomonnaies. En février, nous avions évoqué sur notre blog un programme de minage pour Mac, dont l'analyse a montré qu'il possédait déjà pas moins de 23 variantes. Quelques mois plus tard, nous signalions l'existence d'un autre programme de minage qui se servait de l'implémentation malveillante du programme XMRig.

Notre dernière découverte a été celle d'OSX.DarthMiner, installé en même temps que le backdoor EmPyre et issu d'une application piégée, comme souvent avec les malwares Mac.

Le déclin des programmes de minage : déjà la fin ?

D'après nos données télémétriques, les troisième et quatrième trimestres commencent à confirmer que la tendance des programmes de minage est à la baisse. L'engouement généré par la valeur élevée du bitcoin semble s'être quelque peu dissipé, et plusieurs études s'accordent à dire que les profits issus du minage, en particulier des programmes basés sur le Web, sont plus bas qu'attendus.

Figure 16. Un script qui télécharge une application MacOS malveillante

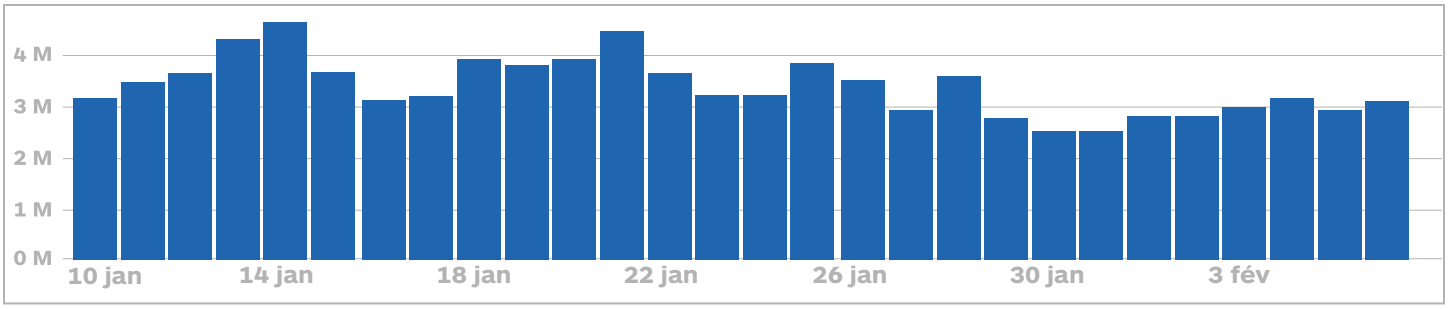

Figure 17. Les détections de Coinhive entre janvier et février 2018 font état de 3 millions de cibles quotidiennes en moyenne

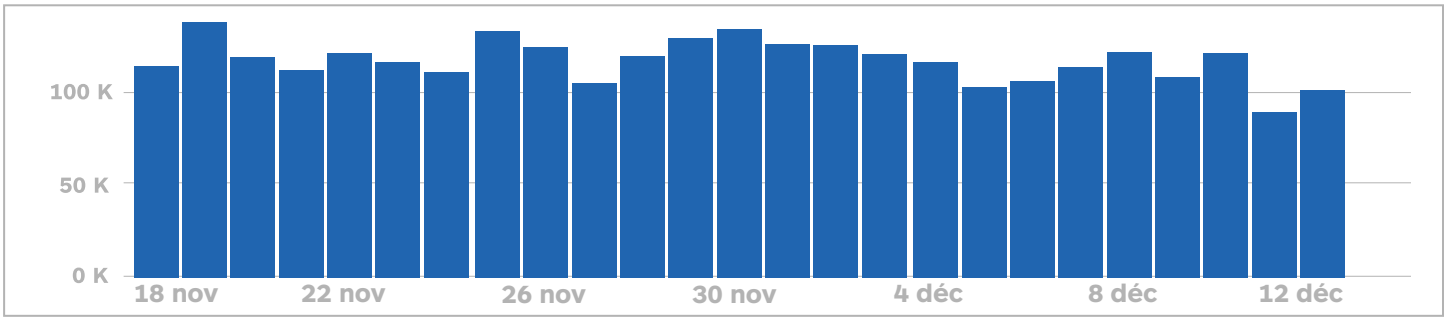

Figure 18. Les détections de Coinhive entre novembre et décembre 2018 font état de 100 000 cibles quotidiennes en moyenne

Malgré la baisse d'activité du côté de Coinhive, d'autres services axés eux aussi sur Monero montrent des signes que le minage basé sur le Web n'est pas complètement relégué aux oubliettes. Le programme CoinIMP en particulier a gagné en popularité ces derniers mois.

De manière générale, il semblerait que les cybercriminels soient parvenus à la conclusion que parfois, le vol vaut mieux que le minage. Un certain nombre de familles de malwares, telles que TrickBot, sont maintenant capables de voler directement des portefeuilles de cryptomonnaies. Dans le même genre, les pirates informatiques montrent un grand intérêt pour l'exploitation des failles dans l'implémentation du protocole JSON-RPC de nombreuses cryptomonnaies.

Dans ce cas, il suffit qu'un utilisateur navigue sur un site Web malveillant pour qu'il se fasse voler son portefeuille.

Malgré la baisse de leur valeur, les cryptomonnaies restent attractives pour les criminels en ligne. Ainsi, en 2018, de grandes campagnes de programmes de minage distribuées via diverses plateformes ont très bien fonctionné. Cependant, il est possible que l'âge d'or du cryptojacking ait déjà eu lieu fin 2017 et dans les tout premiers mois de 2018, notamment dans sa version sur navigateur. En fait, d'autres types de charges utiles s'avèrent bien plus lucratifs, comme nous avons pu le constater lors de la récente vague d'attaques de skimming sur le Web.

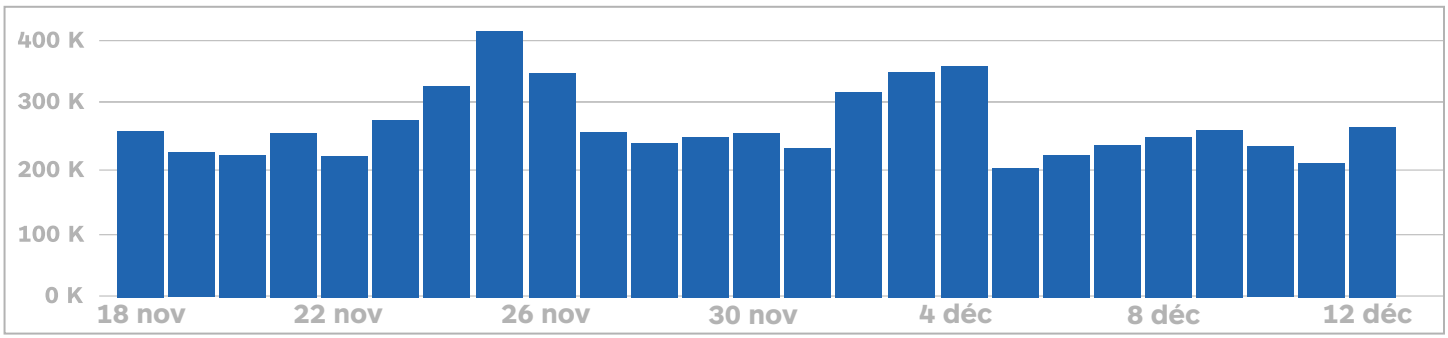

Figure 19. Détection de CoinIMP en novembre et décembre 2018

Chevaux de Troie

Le terme « cheval de Troie » recouvre une grande variété de malwares aux cibles, objectifs et comportements variés. Le terme de chevaux de Troie tel qu'on l'emploie en cybersécurité fait référence à la légende du cheval de Troie, mais il s'agit plus spécifiquement de la capacité d'un malware à s'introduire subrepticement sous couvert d'une attitude amicale. Par exemple, on a affaire à un cheval de Troie lorsqu'une portion de code se cache dans une autre pour échapper à la vigilance des mesures de sécurité.

Lorsque le terme « cheval de Troie » a commencé à être employé pour décrire un certain type de malware, peu de menaces avaient recours à cette tactique pour se propager. Aujourd'hui, la situation a changé et presque tous les malwares, d'une manière ou d'une autre, sont dotés d'une fonctionnalité « cheval de Troie ». En effet, échapper aux logiciels de sécurité est devenu l'un des piliers de la cyberguerre. En outre, « cheval de Troie » est un terme pratique pour désigner les familles de malware qui ne rentrent pas directement dans les catégories spyware, adware ou backdoor, mais qui revêtent plusieurs casquettes.

La famille Emotet, par exemple, était à ses débuts un cheval de Troie bancaire quelconque. Après l'infection, ce dernier observait les utilisateurs lorsqu'ils se connectaient à leur compte bancaire ou entraient des données financières sur un site Web, volait leurs données, puis les renvoyait au serveur contrôle et commande (C&C).

Au fil du temps, Emotet a évolué de manière intéressante : il peut maintenant utiliser des exploits pour infecter des systèmes, propager de nouveaux malwares et même envoyer des e-mails à des contacts. Ces fonctionnalités, prises seules, placeraient Emotet dans différentes catégories de malware : vers, spywares, backdoors et downloaders. Ensemble, elles forment un cheval de Troie.

Dans cette section, nous allons examiner dans quelle mesure les chevaux de Troie ont posé problème sur la scène internationale cette année par rapport à l'année précédente, et les tendances des grandes familles de chevaux de Troie que nous surveillons.

Les chevaux de Troie qui menacent les entreprises

Les chevaux de Troie étaient moins nombreux sur les terminaux d'entreprise en 2017, faisant de l'afflux des chevaux de Troie voleurs d'informations un problème presque entièrement propre à 2018. La figure 20 illustre la faible activité de détection de chevaux de Troie entre le premier et le troisième trimestre 2017, avant le pic de septembre qui a marqué le début d'une nouvelle ère en termes de fréquence de détection de cette menace chez nos clients professionnels.

Détection de chevaux de Troie pour les entreprises dans le monde, 2017 – 2018

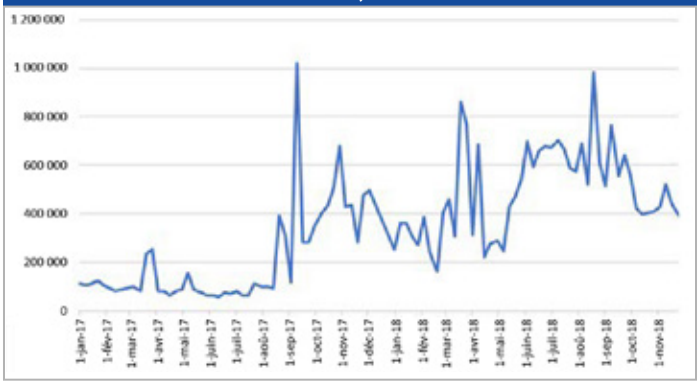

Figure 20. Détection des chevaux de Troie en entreprise dans le monde

Les malwares de vol d'informations sont les chevaux de Troie les plus détectés en 2018. Diverses raisons peuvent expliquer ce phénomène : répercussions du RGPD (Règlement général sur la protection des données), recours aux exploits, comme EternalBlue, et aux backdoors, comme DoublePulsar.

L'exploitation de chevaux de Troie voleurs d'informations dans le cadre d'intrusions dans des entreprises ne semble pas s'essouffler. Cependant, le déploiement de correctifs et la segmentation des réseaux et des données, ainsi que la configuration de la gestion des droits d'utilisateur, pourraient empêcher l'invasion des chevaux de Troie de se propager trop facilement.

Les chevaux de Troie qui menacent les consommateurs

Les chevaux de Troie ont mené la vie dure aux entreprises, mais sont restés assez discrets côté consommateurs, n'enregistrant qu'une faible variation entre 2017 et 2018.

Détection de chevaux de Troie pour les consommateurs dans le monde, 2017 – 2018

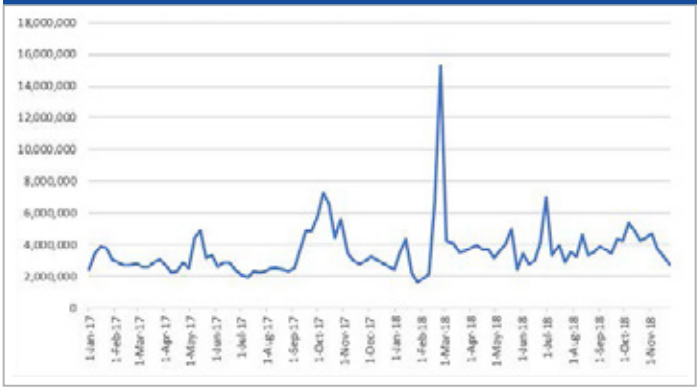

Figure 21. Détection des chevaux de Troie pour les consommateurs dans le monde

L'écart total des détections entre 2017 et 2018 s'est élevé à 30 millions ; 190 millions de chevaux de Troie ont été détectés en 2018, contre 160 millions en 2017. La majorité des menaces que nous avons observées était constituée de voleurs d'informations, de programmes de minage malveillants ou de détections génériques.

Nous ne nous attendons pas à de grands changements à l'échelle de l'année 2019, mais les évaluations trimestrielles permettront de révéler des différences intéressantes entre les familles de chevaux de Troie.

Voleurs d'informations

Parmi les plus grandes menaces de type cheval de Troie rencontrées cette année, on peut citer Emotet et TrickBot, des malwares de vol d'informations qui infectent les systèmes et se propagent pour infecter à nouveau. Nous avons longuement analysé ces deux familles sur notre blog et dans d'autres rapports publiés cette année. À présent, observons de plus près les tendances de détection globales de l'année écoulée.

Emotet

Ce spammer de vol d'informations a représenté une menace majeure en 2018, notamment parce qu'il s'agit d'une des familles capables d'infecter des systèmes à grande échelle, à la fois dans les entreprises et chez les consommateurs.

Détection d'Emotet pour les entreprises dans le monde, 2017 – 2018

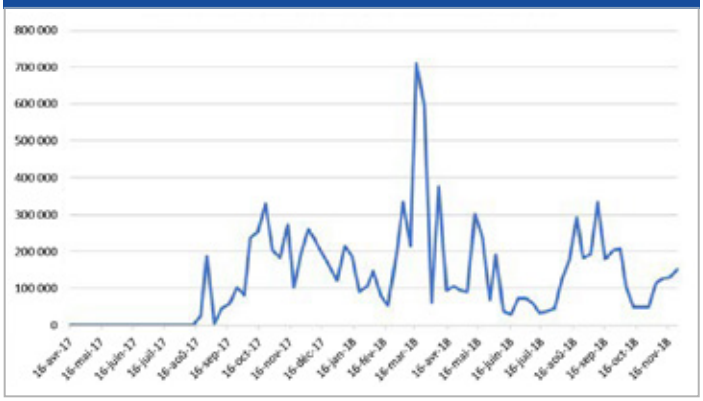

Figure 22. Détection d'Emotet en entreprise, avril 2017–novembre 2018

Les détections d'Emotet dans les entreprises et chez les consommateurs sont similaires, bien que leur nombre soit moins élevé dans les entreprises. Sur la figure 23, observez la concordance entre les pics de détection des infections Emotet chez les consommateurs et dans les entreprises.

À présent, repérez la forme et l'ampleur de la courbe des détections pour les consommateurs et les entreprises au troisième trimestre 2018 (elle ressemble un peu à une tête de chien). La différence entre les deux courbes représente environ 78 000 détections, tandis que la courbe des consommateurs affiche 475 000 détections de plus que celle des entreprises lors du premier pic.

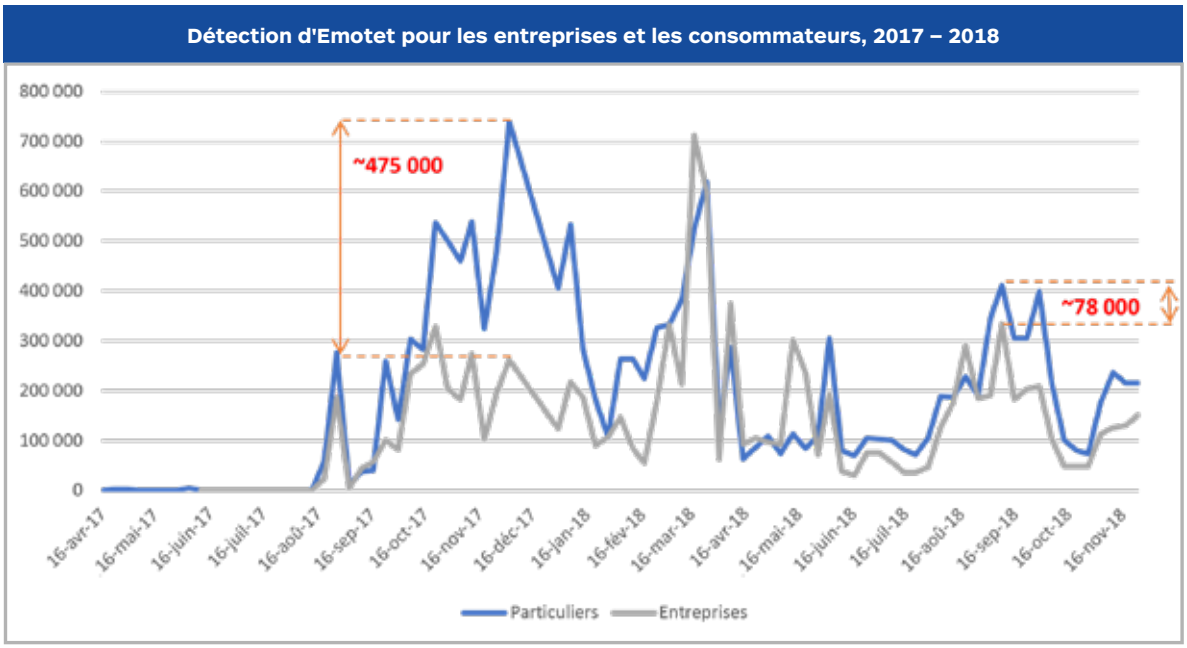

Figure 23. Détection d'Emotet pour les entreprises et les consommateurs

Pourquoi faut-il le souligner ? La similitude des courbes de détection pour les consommateurs et les entreprises sur la même période nous montre que les campagnes Emotet visent large, et les entreprises comme les consommateurs. Par le passé, les victimes étaient bien plus nombreuses côté consommateurs, mais le fossé entre les deux groupes tend à se résorber.

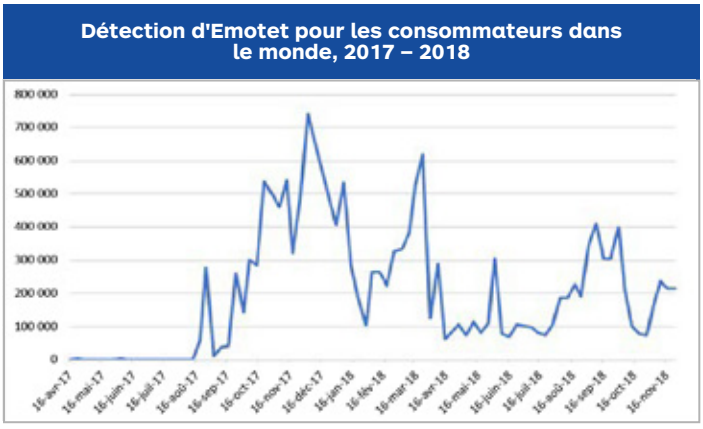

Figure 24. Détection d'Emotet chez les consommateurs, avril 2017–novembre 2018

Les cybercriminels derrière Emotet cherchent sciemment à lancer leurs malwares contre des entreprises. Associez à cela les nouvelles fonctionnalités de cette famille, telles que la capacité à se déplacer latéralement et à propager des spams malveillants à partir des terminaux infectés, et les objectifs de ceux qui pilotent Emotet apparaissent clairement.

TrickBot

Si la hausse des attaques Emotet contre les entreprises ne vous avait pas convaincu que les voleurs d'informations avaient trouvé là une cible plus intéressante, en voilà une preuve supplémentaire : un malware capable non seulement de faire ses propres victimes dans le monde de l'entreprise, mais aussi de se diffuser comme charge utile secondaire par le biais d'Emotet, encore lui.

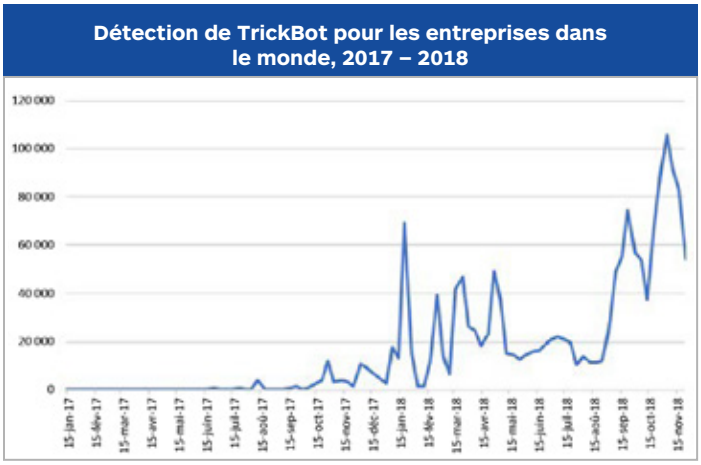

Figure 25. Détection de TrickBot en entreprise dans le monde

TrickBot est un malware de vol d'informations capable de télécharger des composantes pour des opérations malveillantes spécifiques, telles que de l'enregistrement de frappe et des déplacements latéraux au sein d'un réseau. Comme le montre la figure 25, cette famille a commencé à faire parler d'elle seulement fin 2017. Elle représentait l'une des charges utiles les plus communes lancées par Emotet.

Détection de TrickBot pour les consommateurs dans le monde, 2017 – 2018

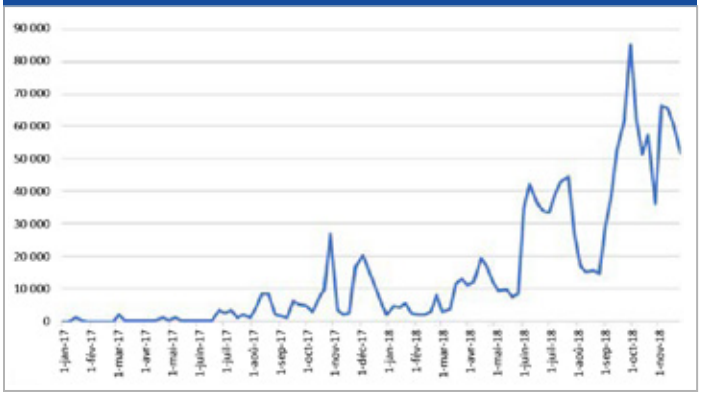

Figure 26. Détection de TrickBot chez les consommateurs dans le monde

Les chiffres de la détection de TrickBot sur les terminaux des entreprises et des consommateurs affichent une différence de 200 000 entre ces deux catégories. Les terminaux d'entreprise ont détecté TrickBot 1,5 million de fois, contre presque 1,3 million de fois pour les consommateurs.

La plupart des malwares que nous traitons sont plus fréquemment détectés chez les consommateurs que sur les terminaux d'entreprise. En analysant ces nouveaux résultats de détection côté entreprises, on peut entrevoir l'intention des cybercriminels : cibler les entreprises et exploiter leurs vulnérabilités.

Chevaux de Troie par secteur

Comme nous l'avons mentionné dans notre introduction sur les chevaux de Troie, ces derniers peuvent faire référence à de nombreux types de malwares qui dissimulent leurs intentions ou qui ne rentrent pas clairement dans une catégorie. Les industries ciblées par les chevaux de Troie sont les mêmes que celles qui ressortent de nos résultats de détection généraux. L'éducation, la production industrielle et la distribution sont en tête du classement, suivies par le conseil, les administrations et la santé. La restauration occupe la dernière place, et l'hôtellerie, qui a fait la une des médias récemment avec l'intrusion dans les systèmes de Marriott, n'apparaît même pas dans la liste.

Les 10 industries les plus touchées par les chevaux de Troie	
1	Éducation
2	Industrie
3	Commerces
4	Conseil
5	Gouvernement
6	Télécommunications
7	Santé
8	Technologie
9	Services professionnels
10	Restauration

Figure 27. Les 10 industries les plus affectées par les chevaux de Troie

Cependant, si l'on observe de plus près la catégorie des chevaux de Troie et en particulier la famille qui la domine, Emotet, on aperçoit des différences entre les secteurs. Le conseil figure en première place du classement et l'hôtellerie apparaît à la quatrième place. En outre, le transport, la logistique et l'industrie chimique rejoignent le top 10 et éjectent les télécommunications, les services aux entreprises et la restauration.

Les 10 industries les plus touchées par le cheval de Troie Emotet	
1	Conseil
2	Éducation
3	Industrie
4	Hôtellerie/Loisirs
5	Gouvernement
6	Commerces
7	Transport et logistique
8	Industrie chimique
9	Santé
10	Technologie

Figure 28. Les 10 industries les plus affectées par Emotet

Les chevaux de Troie du futur

Les tendances que nous observons actuellement en termes de chevaux de Troie devraient se poursuivre, si les cybercriminels continuent à pouvoir exploiter des configurations peu sécurisées et des ressources dépassées. Cependant, nous sommes surtout préoccupés par les imitations et les nouvelles générations de familles qui risquent de dominer la scène en 2019.

À l'heure actuelle, nous ne connaissons pas de concurrent sérieux à Emotet (en dehors de TrickBot), capable comme lui de cibler les organisations de son propre chef ou d'agir comme vecteur d'infection pour une autre famille. Cependant, si l'historique des ransomwares entre 2012 et 2019 peut servir d'indicateur dans le cas présent, alors nous verrons apparaître rapidement des concurrents à Emotet dans les 12 prochains mois.

Ransomwares

Les ransomwares ne sont plus aussi répandus qu'en 2017, mais ils restent une menace avec laquelle il faut composer. Les tendances générales montrent une baisse en volume sur l'année, mais une hausse des attaques sophistiquées et ciblées sur les entreprises. En réalité, la seule vraie hausse notable en nombre a concerné le monde des entreprises, le manque d'intérêt et d'innovation pour les attaques dirigées contre les consommateurs étant flagrant.

On a bien aperçu quelques fichiers anciens étonnamment retravaillés réaliser de nouvelles attaques, et quelques vagues impressionnantes de la part de variantes connues comme WannaCry, mais de manière générale, le calme a régné sur les ransomwares en 2018.

Détections de ransomwares dans le monde, 2017 – 2018

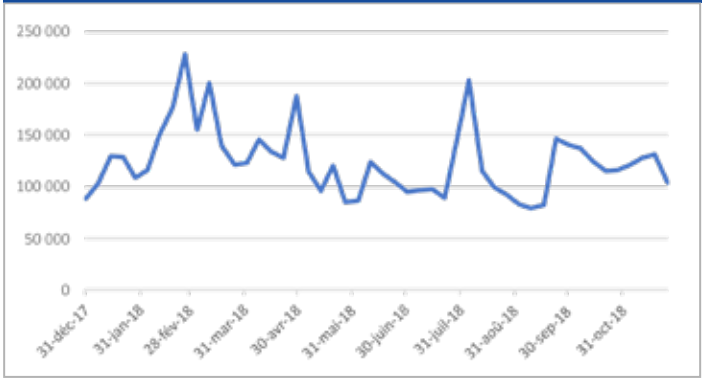

Figure 29. Détections de ransomwares dans le monde en 2018

Consommateurs et entreprises

La baisse globale du nombre d'attaques est bien visible : En 2017, 8 016 936 attaques s'étaient produites dans le monde, entreprises et consommateurs confondus. L'année 2018 a comptabilisé 5 948 417 détections, soit un déclin de 26 %.

La différence d'intérêt entre les cibles professionnelles et les consommateurs est remarquable, tant l'un augmente de manière régulière alors que l'autre décline.

Détection de ransomwares pour les entreprises dans le monde, 2017 – 2018

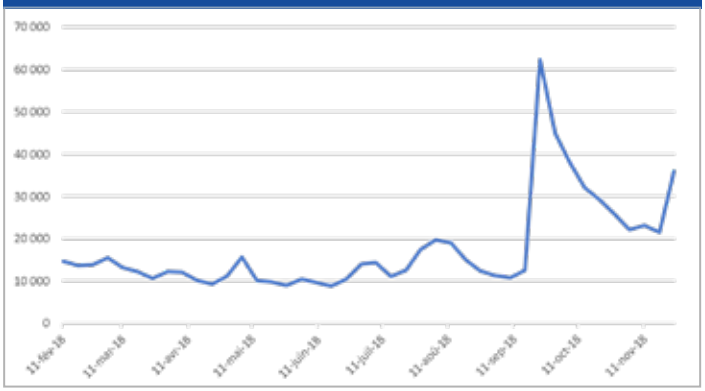

Figure 30. Détection des ransomwares en entreprise dans le monde

Détection de ransomwares pour les consommateurs dans le monde, 2017 – 2018

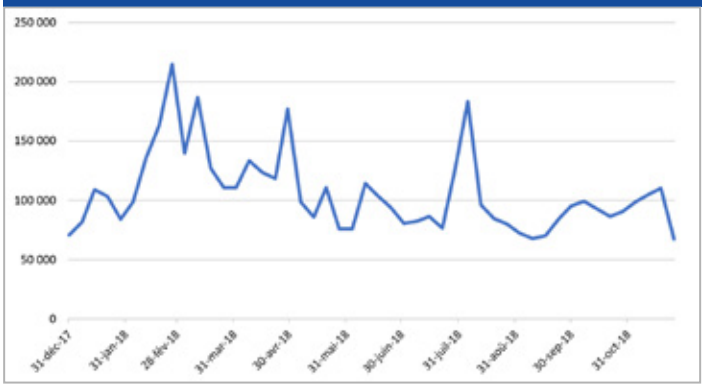

Figure 31. Détection des ransomwares chez les consommateurs dans le monde

Les entreprises abritent tant de données de valeur et de systèmes critiques qu'elles s'avèrent être des cibles bien plus rentables pour les cybercriminels. Elles disposent non seulement des fonds nécessaires au paiement des rançons, mais elles sont également plus susceptibles de vouloir retrouver un fonctionnement normal au plus vite. Les retards provoqués par les ransomwares peuvent s'avérer extrêmement coûteux, en particulier lorsqu'une organisation touchée n'a pas prévu de plan de sauvegarde et que de nombreux terminaux doivent être remis sur pied. La réponse aux incidents et les investigations numériques ont un coût, souvent bien supérieur au simple paiement d'une rançon (une technique que nous ne recommandons pas).

Statistiques par secteur

Vous vous posez peut-être des questions sur la popularité des ransomwares dans tel ou tel secteur, ou souhaiteriez connaître les secteurs les plus touchés par cette menace. Nos données montrent que le conseil remporte le palmarès, l'éducation décrochant la deuxième place.

Les 10 secteurs les plus touchés par les ransomwares	
1	Conseil
2	Éducation
3	Industrie
4	Commerces
5	Gouvernement
6	Transport
7	Télécommunications
8	Électronique
9	Santé
10	Technologie

Figure 32. Secteurs les plus touchés par les ransomwares

Malgré les nombreux faits divers relatant des attaques contre des administrations et des établissements de santé en 2018, ce sont en réalité d'autres secteurs qui ont le plus fait les frais de la menace ransomware : les administrations arrivent en milieu de classement, tandis que la santé occupe la neuvième place.

SamSam

SamSam a provoqué le chaos dans les milieux médicaux aux États-Unis. S'introduisant dans les systèmes à l'aide d'exploits et d'attaques par force brute, il est parvenu à les tenir en otage et à obtenir le paiement de rançons s'élevant à plus d'un million de dollars. L'une de ses nombreuses variantes a été retravaillée pour attirer davantage de cybercriminels, qui demandent aux victimes une somme d'argent inférieure au coût des autres méthodes de récupération, et engrangent ainsi des sommes bien plus importantes qu'avant.

Entre janvier et mars, SamSam a attaqué tous azimuts : hôpitaux, administrations municipales, et notamment le service de transport et les applications de la ville d'Atlanta. D'autres attaques notables se sont produites en septembre, dont les ports de Barcelone et de San Diego ont fait les frais.

Détections de SamSam dans le monde, 2017 – 2018

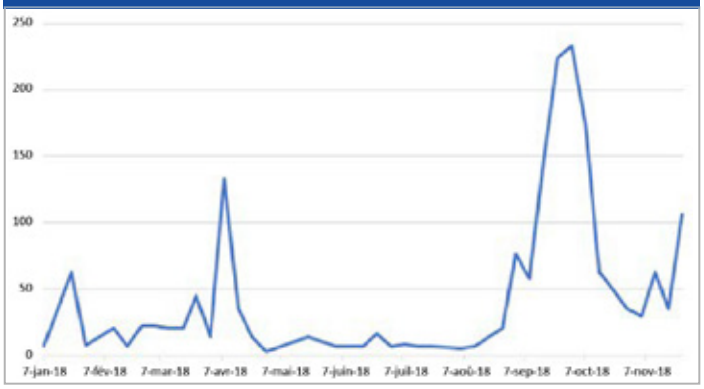

Figure 33. Détections de SamSam dans le monde en 2018

Bien que les autorités pensent savoir qui se cache derrière l'infection, le duo présumé sévit toujours et nous continuons à observer des pics d'attaque. SamSam restera une source d'infection par malware tenace en 2019.

GandCrab

GandCrab a lui aussi joué un rôle important en 2018 en utilisant différents kits d'exploit peu de temps après sa première apparition en janvier. Les chiffres se sont stabilisés et sont restés constants tout au long de l'année, à l'exception du mois de février qui a connu un fort rebond, provoqué par le lancement de plusieurs campagnes de spam au premier trimestre.

En se tournant vers le kit d'exploit Magnitude pour assurer sa distribution, GandCrab a continué à causer du tort aux administrateurs de réseau et aux particuliers. Les méthodes de chargement des malwares peu conventionnelles de Magnitude ne sont pas étrangères à ce succès. Pour remporter le titre de plus grande menace du moment, GandCrab n'a pas lésiné sur les moyens, entre techniques sans fichier et bourrage binaire (lorsque des données supplémentaires sont ajoutées aux fichiers pour contourner les analyses).

Détections de GandCrab dans le monde, 2017 – 2018

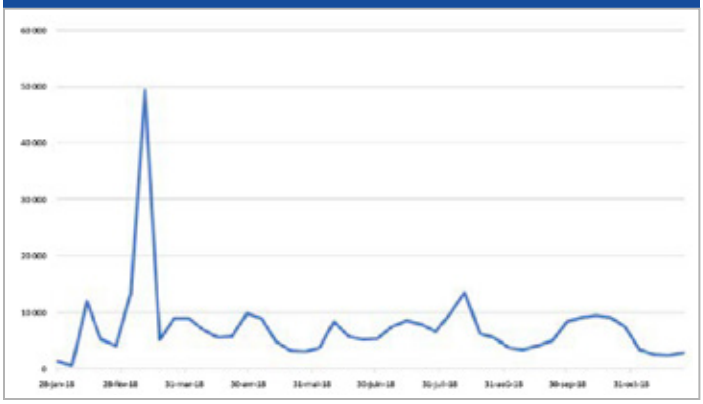

Figure 34. Détections de GandCrab dans le monde en 2018

GandCrab, la variante de ransomware la plus active du deuxième trimestre 2018, est remarquable à plus d'un titre, car il s'agit aussi du premier ransomware qui demande à ses victimes des paiements en cryptomonnaies autres que le bitcoin. À une période où les détections des ransomwares en entreprise ont augmenté de 28 %, mais où leur volume global est resté bas, GandCrab est devenu l'une des sources majeures de campagnes de ransomwares malveillantes, au grand détriment de ses victimes.

En fin d'année

Bien que les ransomwares aient perdu du terrain face à d'autres acteurs, tels que les programmes de minage et les chevaux de Troie, il faut encore compter avec eux. Somme toute, l'année 2018 a été celle des expérimentations discrètes et des reconsidérations. Le grand public est bien plus conscient du danger qu'il ne l'a été, et les tactiques vues et revues des cybercriminels ne fonctionneront pas éternellement. Nous nous attendons à voir apparaître des versions retravaillées innovantes d'anciens fichiers et des liens renforcés vers des kits d'exploit de pointe, chargés de propager encore plus loin les ransomwares.

Vecteurs d'attaque notables

L'année 2018 a représenté un savant mélange de déjà-vu et de nouveauté. Les auteurs de malware se sont intéressés aux techniques de distribution traditionnelles, comme le malspam et l'ingénierie sociale, tout en explorant de nouveaux territoires avec le minage de cryptomonnaies basé sur navigateur. En outre, les menaces rivalisent de créativité pour échapper à la détection. Elles injectent du code malveillant dans les plateformes de paiement en ligne, glissent de fausses applications sur des boutiques en ligne légitimes et volent des informations sous les yeux des utilisateurs à l'aide de plug-ins plus nuisibles qu'utiles. Jetons un œil aux vecteurs d'attaque les plus remarquables de l'année.

Malspams

Emotet et TrickBot, deux des pires menaces qu'a connues l'année 2018, ont travaillé en équipe pour mener à bien des attaques efficaces distribuées via des malspams dissimulés sous la forme d'e-mails authentiques. Une campagne d'hameçonnage/harponnage classique, direz-vous. Non, ce qui a rendu ces attaques si percutantes, ce n'est pas simplement la méthode de distribution des malwares, mais leur propagation.

Emotet se diffuse généralement par des malspams du type pièces jointes infectées ou encore URL imbriquées. Le facteur de l'ingénierie sociale est aussi à prendre en compte. Depuis qu'Emotet est capable de prendre le contrôle des comptes de messagerie de ses victimes, les utilisateurs ont l'impression que les e-mails malveillants proviennent de sources fiables. Les pièces jointes infectées prennent souvent la forme d'un document Microsoft Word dans lequel les macros sont activées.

Une fois qu'Emotet s'est infiltré sur un réseau, il a recours à EternalBlue, l'une des failles SMB exploitée par le groupe des ShadowBrokers l'an dernier, pour exploiter les systèmes non corrigés. Les machines infectées tentent de diffuser Emotet latéralement via une attaque par force brute des identifiants du domaine, ainsi qu'en externe, via son module de spam intégré. Par conséquent, le botnet Emotet est assez actif et reste à l'origine d'une grande partie des malspams que nous rencontrons.

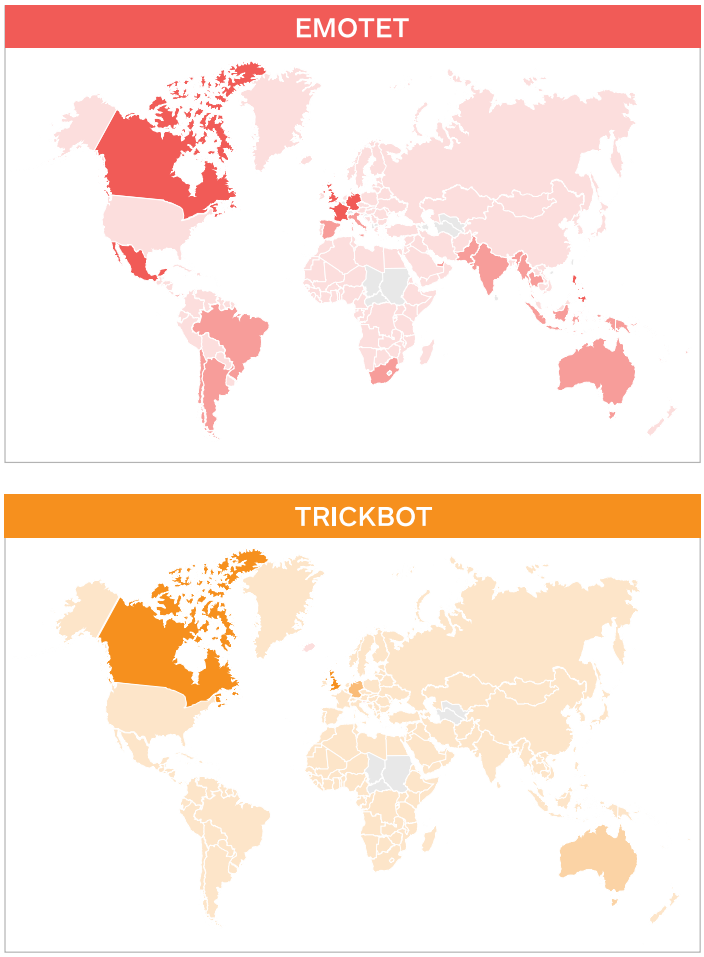

Figure 35. Détections d'Emotet et de TrickBot dans le monde

TrickBot est un cheval de Troie actif qui se sert de malspams pour infecter les systèmes. Il sévit essentiellement par le biais de documents Word infectés, mais utilise aussi des URL imbriquées redirigeant vers des fichiers PDF infectés. À l'image d'Emotet, TrickBot tire profit des vulnérabilités SMB, dans ce cas d'EternalRomance, pour se déplacer latéralement au sein d'un réseau.

Plutôt nouveaux côté malwares, voici les documents Office qui parviennent à échapper au sandbox macOS pour les macros Office. Le malware de macro Word, détecté actuellement sous le nom OSX.BadWord, installe sur le système de la victime un backdoor à l'aide de Python.

Attaques de sites Web

En 2018, nous avons été témoins d'une hausse constante d'attaques très en vue contre des sites d'e-commerce légitimes et de confiance, via la compromission de tierces parties, dans le but de voler des données de carte de crédit et d'autres informations d'identification personnelle. Une de ces attaques, qui visait British Airways, a affecté près de 400 000 de ses clients, dont les noms, adresses et données financières ont été dérobées.

En rôdant sur des sites Web de confiance, le groupe de menaces connu sous le nom de Magecart volait les informations de contact et de paiement que les visiteurs saisissent lorsqu'ils passent commande. Les attaques Magecart exploitaient des faiblesses dans le code des pages de traitement des paiements et utilisaient des scripts multiplateforme (XXS). Plusieurs groupes ayant recours aux tactiques de Magecart se font parfois concurrence en trafiquant le code des uns et des autres.

La portion de code malveillant ci-dessous, qui est l'œuvre de Magecart, a été aperçue sous une forme obscurcie dans un script légitime et réputé fiable.

Après avoir décodé le script, on peut repérer le code à l'origine de la collecte des données qui se produit lorsque les clients d'un site cliquent sur le bouton qui leur permet de passer commande. Au niveau du réseau, on a affaire à ce qui ressemble à une requête POST, où chaque champ (nom, adresse, numéro de carte de crédit, date d'expiration, code de vérification, etc.) est envoyé au format Base64 vers un serveur indésirable (dans ce cas, info-stat[.]ws), contrôlé par les cybercriminels.

Cette forme d'attaque se produit en toute transparence du côté du site marchand et des clients. Contrairement aux intrusions liées à des fuites de bases de données, cas dans lesquels les informations peuvent être chiffrées, les procédés de skimming sur le Web peuvent collecter les données en texte clair et en temps réel.

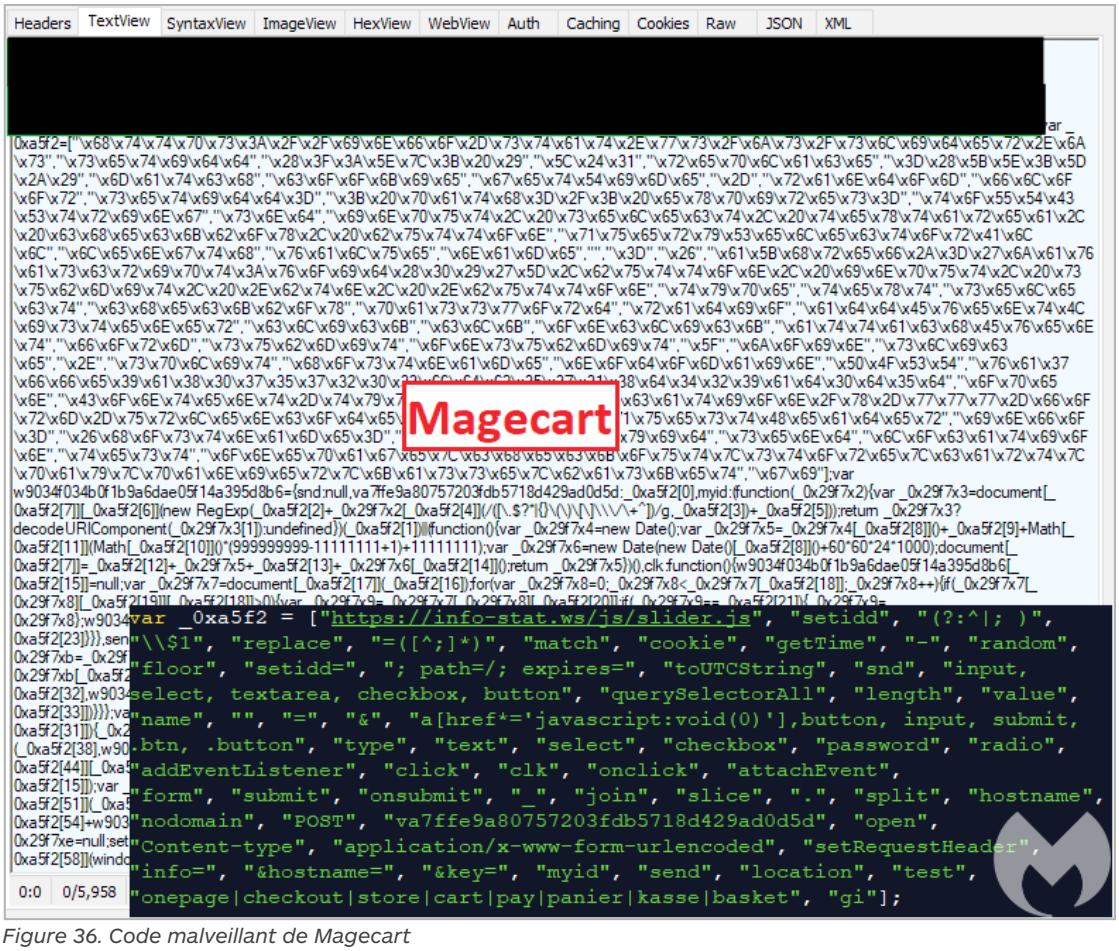

Figure 36. Code malveillant de Magecart

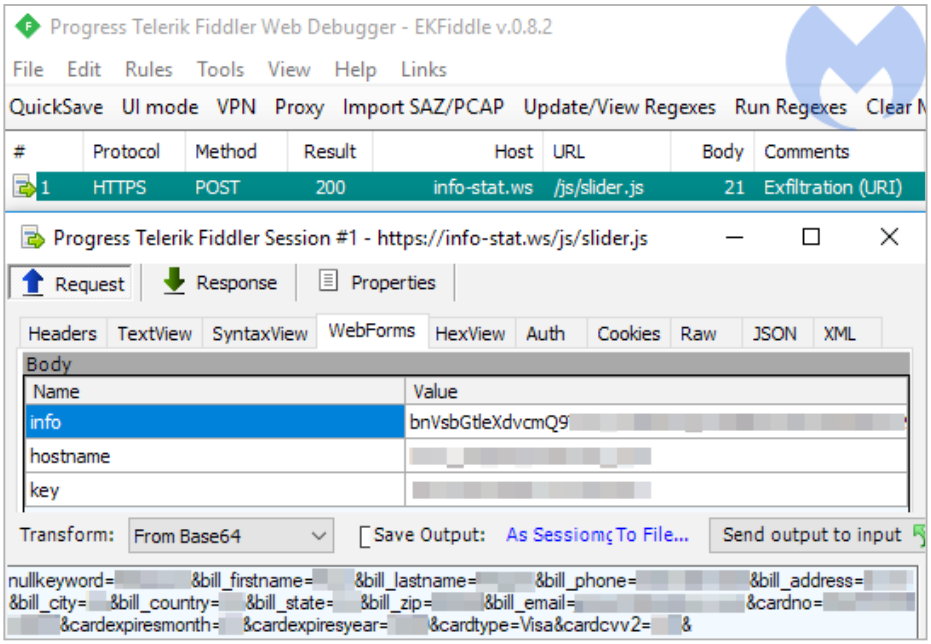

Figure 37. Le code de Magecart envoie des informations à un serveur indésirable

Extensions de navigateurs malveillantes

En 2018, les extensions de navigateur (plug-ins) malveillantes ont fait parler d'elles. Les exemples ne manquent pas, entre les extensions légitimes compromises et utilisées dans des attaques de chaînes d'approvisionnement, ou encore les extensions indésirables garantissant une confidentialité exemplaire aux utilisateurs tout en épiant leurs moindres faits et gestes en ligne. Voici quelques cas qui se sont distingués :

- Des extensions légitimes compromises dans une attaque de chaîne d'approvisionnement, notamment l'extension Chrome MEGA.nz de partage de fichiers, volaient des noms d'utilisateur et des mots de passe. Les utilisateurs pouvaient faire la différence entre cette extension et l'originale uniquement en faisant attention aux autorisations supplémentaires que la version piratée demandait.
- Une flopée d'extensions Firefox (et quelques extensions Chrome) ont été prises la main dans le sac à espionner l'historique de navigation des utilisateurs.
- Des extensions imitaient des plug-ins populaires pour amener les utilisateurs à les installer, notamment une extension qui affirmait ne pas pister les utilisateurs ni conserver leurs données, mais promettait au contraire de les protéger contre l'indiscrétion des navigateurs. Bien entendu, ce que les utilisateurs voyaient, c'était une extension redirigeant leur page d'accueil vers Yahoo!

Pour voir le bon côté des choses, disons que la plupart des navigateurs ont été poussés à prendre des mesures contre ces extensions malveillantes. Voici les changements apportés à ce stade :

- Arrêt des installations en ligne. Toutes les extensions doivent désormais être installées via les webstores officiels.
- Blocage du code obscurci dans les extensions.
- Fin de la prise en charge des protocoles anciens comme TLS 1.0 et 1.1. Cette mesure prendra effet en 2020.

Alors que les navigateurs principaux ont pris des mesures pour empêcher les extensions malveillantes de s'introduire sur leurs plateformes, on constate que les adwares et les programmes potentiellement indésirables sont encore nombreux à passer entre les mailles du filet. La plupart de ces programmes sont des hijackers, capables de modifier le moteur de recherche par défaut des navigateurs, ou bien ses pages Démarrer ou Nouvel onglet. Ils prétendent même parfois renforcer la confidentialité des recherches effectuées par les utilisateurs.

Nous nous évertuons à conseiller aux utilisateurs de télécharger leurs applications sur les plateformes officielles, mais la version Android du très populaire jeu Fortnite a été délibérément mise à disposition en dehors de Google Play. Pour obtenir le jeu, les utilisateurs doivent activer l'option « autoriser l'installation à partir de sources inconnues », qui peut entraîner d'autres installations non voulues. Pire encore, le programme d'installation du jeu laissait le champ libre aux attaques Man-in-the-Disk, un moyen pour les applications indésirables de pirater le programme d'installation et d'installer leurs propres junkwares à la place de l'application légitime.

Exploits

Nous nous attendions à voir se produire des attaques via du spam et des documents Microsoft Office malveillants en 2018, dans la droite ligne de ce que nous avions pu observer l'année d'avant.

Nous avons en revanche été témoins d'une évolution intéressante concernant l'exploitation des vulnérabilités. Les navigateurs étant de plus en plus sûrs et soumis à des mises à jour automatiques, les téléchargements intempestifs reculent largement. Par conséquent, le vecteur des e-mails est l'une des méthodes sur lesquelles les menaces s'appuient le plus pour compromettre les systèmes.

Exploits contre les plug-ins et les navigateurs

En début d'année, une vulnérabilité zero-day du Flash Player (CVE-2018-4878) a permis de lancer des attaques ciblées contre la Corée du Sud, attribuées par beaucoup au groupe Lazarus.

L'exploit était imbriqué dans une feuille de calcul Excel servant d'appât et chargé sous la forme d'un objet ActiveX. Peu de temps après, un certain nombre d'auteurs de kits d'exploit avaient intégré cette vulnérabilité dans leurs kits d'outils de distribution sur le Web.

Une autre menace zero-day dans le moteur VBScript (CVE-2018-8174) a été découverte fin avril et mérite qu'on en parle, car cela faisait deux ans qu'un nouvel exploit n'avait pas affecté le navigateur populaire Internet Explorer. Notons qu'une fois de plus, cette menace zero-day était intégrée à un document, et pas liée à une attaque intempestive. Suivant le cycle classique zero-day ➔ correctif ➔ démonstration de faisabilité, ce nouvel exploit s'est largement répandu parmi les kits d'exploit de navigateur, détrônant son prédécesseur, CVE-2016-0189.

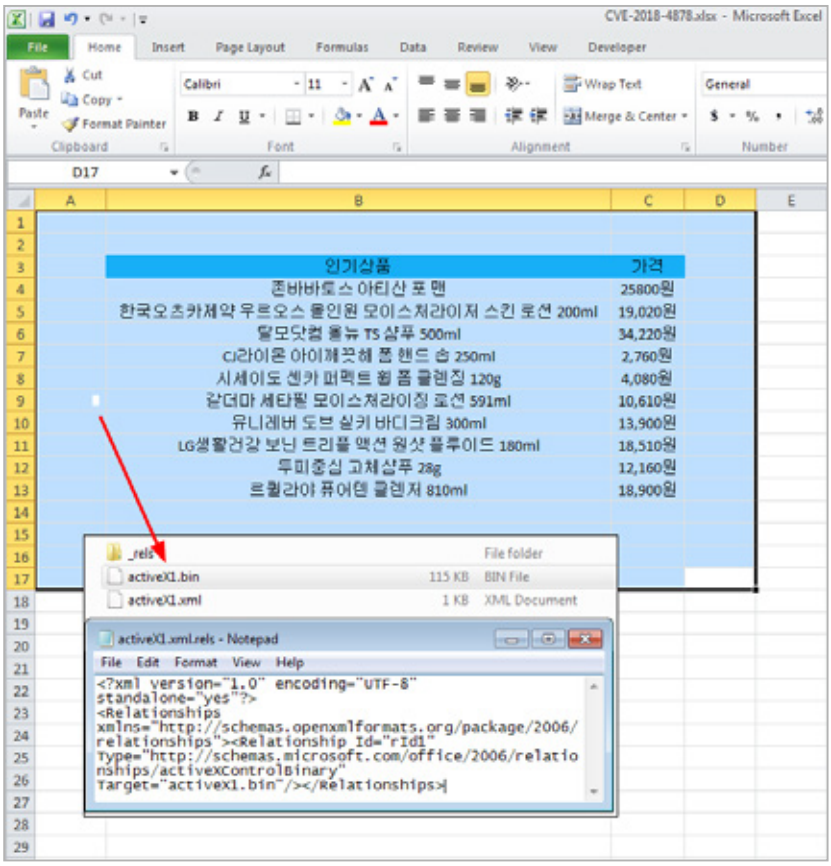

Figure 8. Flash ActiveX masqué et imbriqué dans un document d'appât

Compromissions de masse via des routeurs

Le mois d'avril a été particulièrement agité, un défaut critique touchant les routeurs MikroTik (CVE-2018-14847) ayant été détecté à l'intérieur de RouterOS, le système d'exploitation alimentant ces appareils.

Pour prévenir les intrusions, il était fortement recommandé de restreindre l'accès à Winbox, le tableau de bord de gestion de MicroTik, via le pare-feu. Les pirates étaient parvenus à automatiser les tentatives de connexion et utilisaient même des malwares pour exploiter la faille dite de « traversée de répertoires » (« path traversal » ou « directory traversal » en anglais).

Pour corriger ce problème, il a fallu non seulement appliquer des correctifs de sécurité, mais aussi nettoyer certains fichiers de configuration. Ces fichiers étaient souvent utilisés pour injecter des scripts de cryptojacking Coinhive, ce qui amenait toute personne connectée à un routeur infecté, quel que soit l'appareil utilisé ou le site Web visité, à miner des cryptomonnaies.

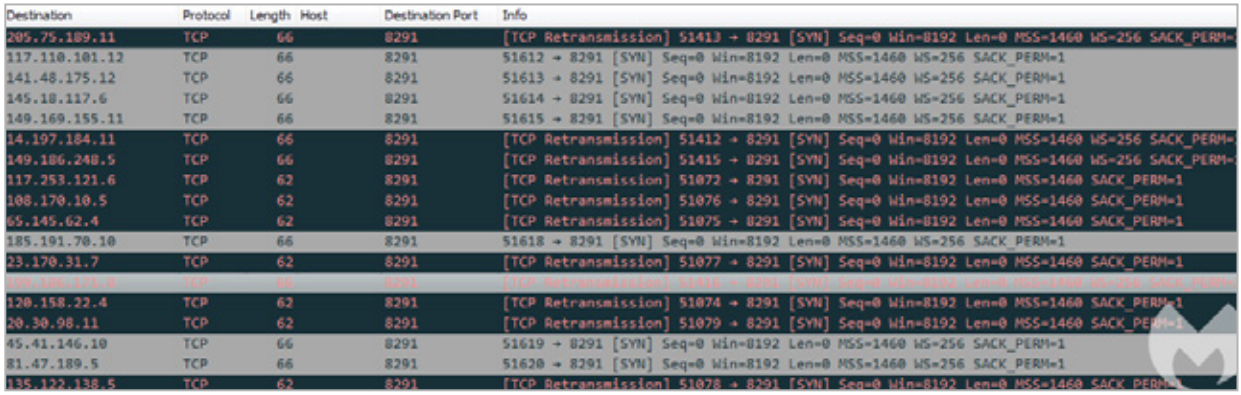

Figure 39. Analyse antimalware à la recherche d'autres appareils vulnérables sur le port Winbox par défaut (8291)

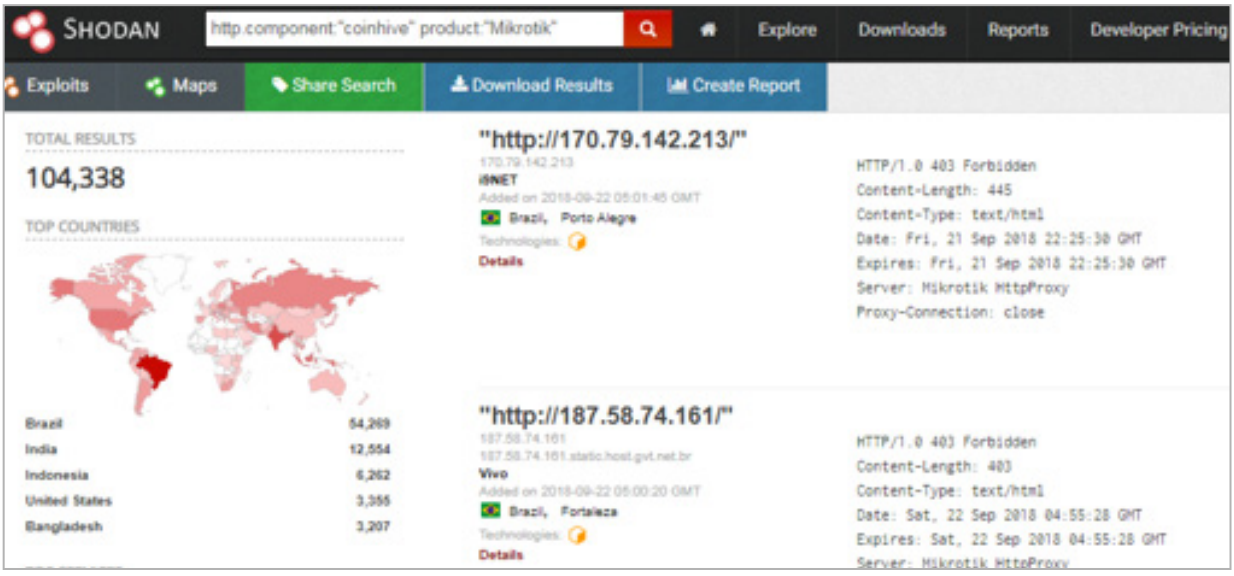

Figure 40. Analyse Shodan montrant plus de 100 000 appareils MikroTik compromis

Attaques de CMS

Il serait difficile de faire l'impasse sur les CMS (Content Management Systems), vu la mesure dans laquelle ils ont été touchés par les exploits en 2018. Les pirates ont découvert ou exploité à de nombreuses reprises des failles permettant l'exécution de code à distance dans des logiciels populaires tels que WordPress, Jooma et Drupal.

Drupal était l'un des CMS les plus surveillés au cours du premier semestre 2018, en raison principalement de défauts « back-to-back » (CVE-2018-7600 et CVE-2018-7602) ayant entraîné des compromissions massives.

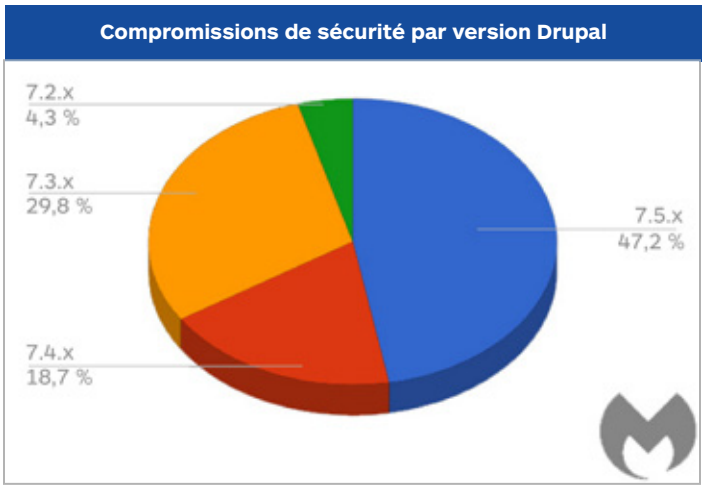

Figure 41. Sites les plus compromis par la version Drupal (branche 7.x)

La majorité des propriétaires de sites Web ne maintiennent pas leurs CMS (ou leurs plug-ins) à jour et rencontrent sans surprise des problèmes de compromission. La peur d'endommager son site en le mettant à niveau est souvent citée parmi les raisons qui poussent à garder une version dépassée. Ceci étant, à moins que les sites en question ne soient protégés derrière un quelconque pare-feu d'application, ils sont à la merci du piratage.

Les menaces zero-day dans les navigateurs et les plug-ins ont été bien réelles en 2018, mais pas forcément employées d'une manière attendue. Les pirates les ont combinées à des attaques d'harponnage ou d'ingénierie sociale imbriquées dans des fichiers Office.

Ils ont également visé les appareils physiques, en particulier les routeurs, pour réaliser des compromissions à grande échelle. Comme nous le savons, ces appareils sont souvent dépassés, et il est probable qu'ils ne reçoivent jamais de correctifs avant de cesser complètement de fonctionner. Cette situation est idéale pour les pirates, et difficile à combattre pour les fournisseurs de solutions de sécurité sans le concours des utilisateurs inconscients du danger.

Arnaques notables

Nous avons pu observer en 2018 la prolifération d'arnaques diverses, qui reflétaient souvent les développements en matière de création et de distribution de malwares. Au premier trimestre, le minage de cryptomonnaies a dominé toute la scène du cybercrime, y compris les arnaques. Les attaques les plus efficaces ont combiné consolidation des ressources et tactiques plus innovantes, en dépassant les simples arnaques au faux support technique pour vider les portefeuilles de leurs cryptodevises. Au deuxième trimestre, nous avons constaté que les arnaques tournées vers les cryptomonnaies avaient été remplacées par le ciblage d'informations d'identification personnelle, une tactique toujours employée à l'heure actuelle.

Les arnaques au faux support technique pour Coinbase ont notamment permis des vols spectaculaires, notamment parce que le Bitcoin et Coinbase n'offrent aucune protection contre la fraude. Les signalements de victimes sur Twitter faisant état de portefeuilles drainés et de pertes atteignant des dizaines de milliers de dollars semblent indiquer que ces criminels préfèrent se contenter de vider les portefeuilles de leurs cryptodevises plutôt que de fournir un faux service de support technique.

Début 2018, les auteurs d'arnaques semblaient avoir actualisé leurs tactiques de prospection à l'aide d'API détournées pour bloquer les navigateurs de leurs victimes. Cette technique cible en premier lieu Chrome, mais aussi Firefox et Brave.

Pratiques commerciales exploitables

Les arnaques au faux support technique reposent plus sur des processus commerciaux exploitables que sur des outils spécifiques. Dans le cas des arnaques sur Coinbase, les auteurs exploitent l'absence de protection anti-fraude inhérente aux transactions en Bitcoin afin d'engranger des revenus largement supérieurs à la moyenne. Dans le cas du détournement d'API présenté, le véritable exploit se situe dans les délais importants entre le signalement aux sociétés concernées et la mise à disposition d'un correctif.

Sachant qu'une fonction de navigateur donnée a généralement une utilisation légitime pour de nombreux utilisateurs, les délais de publication d'un correctif par le support technique ont tendance à être longs. Les auteurs d'arnaques exploitent ces délais pour engranger d'importants revenus.

Nous nous attendons à ce que les arnaques au Bitcoin et les détournements de navigateur restent des techniques populaires d'arnaque pendant un bon moment.

Ciblage d'informations d'identification personnelle

Au deuxième trimestre, les arnaques se sont principalement mises à cibler les informations d'identification personnelle. Nous avons d'abord vu les escrocs voler de manière éhontée des informations d'identification personnelle à leurs victimes par le biais d'arnaques au bitcoin. La réglementation laxiste, la protection contre la fraude limitée et le peu d'assistance autour des échanges ont contribué à rendre les attaques basées sur l'ingénierie sociale contre les portefeuilles de bitcoins très lucratives. Cependant, les victimes d'arnaques au faux support technique traditionnelles se sont raréfiées à mesure que les utilisateurs ont pris conscience du phénomène et que la législation s'est durcie, et les escrocs se sont jetés avec d'autant plus de ferveur sur le vol de mots de passe, d'informations bancaires et de comptes de messagerie électronique. La nouvelle règlementation introduite par le RGPD a sûrement entraîné la hausse des vols d'informations d'identification personnelle, car ce type d'informations vaut plus que jamais son pesant d'or sur le marché noir.

Sextorsion

Début juillet, une campagne d'arnaque par extorsion a attiré notre attention en raison de sa taille et de son originalité. Contrairement aux arnaques classiques par extorsion basées sur le sexe, cette campagne d'e-mail mentionnait un mot de passe utilisateur démontrant que l'expéditeur avait « piraté » la victime. Probablement rassemblés à partir de plusieurs grandes collectes de fuites au cours des quatre années passées, ces identifiants provenaient de différentes intrusions majeures commises antérieurement. Les identifiants étaient corrects même si la plupart des victimes ont expliqué que les malfaiteurs utilisaient des mots de passe anciens et souvent expirés.

L'utilisation d'identifiants volés comme outil d'ingénierie sociale est une approche relativement nouvelle pour ce genre d'attaque et offre un réseau de monétisation supplémentaire pour les identifiants eux-mêmes, tout en enduisant d'un

vernis de plausibilité l'attaque par extorsion susceptible de s'ensuivre. Les intrusions tierces ne montrant aucun signe de faiblesse, nous pensons que cette technique continuera à être utilisée en complément de l'hameçonnage, de l'extorsion et des autres arnaques.

Affaiblir l'ennemi

Au cours du dernier trimestre, nous avons pu constater que les cybercriminels se détournaient massivement du traitement des cartes de crédit par des arnaques ciblant les clients Malwarebytes. Les systèmes de traitement de cartes de crédit ont pris des mesures drastiques contre les arnaques sévissant sur leurs plateformes, poussant celles-ci à se tourner vers des plateformes moins bien surveillées comme PayPal, ainsi que des formats disposant d'une protection intégrée contre la fraude moins performante comme Bitcoin et les chèques de comptes personnels. Bien que ces types de plateforme et de format offrent une source de revenus plus stable aux cybercriminels, ils limitent aussi l'étendue de leurs activités, ce qui s'est traduit par une baisse de signalements de victimes au cours du dernier trimestre.

Le durcissement des règles de sécurité s'est aussi traduit par le recul progressif du démarchage téléphonique en aveugle et la hausse du nombre de messages vocaux demandant un rappel. Les rappels représentent une technique éprouvée pour entrer en contact uniquement avec les victimes potentielles les plus vulnérables, excluant les personnes enclines à poser des questions « test » lors du premier appel.

Pour voir plus loin

À l'avenir, nous pensons voir davantage d'attaques d'ingénierie sociale basées sur des vols d'informations d'identification personnelle, à la manière de la vague d'e-mails de sextorsion qui a déferlé par le passé. Avec l'accélération de la cadence des grandes intrusions, combinée à la réutilisation généralisée des identifiants sur plusieurs plateformes, l'utilisation des informations d'identification personnelle pour améliorer l'efficacité de l'ingénierie sociale offre aux cybercriminels des possibilités démultipliées tout en limitant les inconvénients et les frais. Et cerise sur le gâteau pour le cybercriminel, comme on a pu le voir lors de la campagne de sextorsion, il n'est même pas nécessaire que les informations d'identification personnelle utilisées dans le cadre de l'ingénierie sociale soient exactes ou à jour pour être d'une redoutable efficacité. Par conséquent, on peut s'attendre à ce qu'un plus grand nombre de campagnes de cet acabit se produisent à l'avenir.

Prévisions pour 2019

Lorsque vient le moment de se tourner vers la nouvelle année, on nous demande souvent de prédire les tendances qui seront amenées à s'essouffler et celles qui feront leur apparition. Bien sûr, nous pouvons exploiter nos données pour parvenir à des conclusions éclairées sur les hauts et les bas du cybercrime, mais l'expérience ne suffit pas à nous préparer à des innovations inédites comme celle que nous avons vécu avec le phénomène des cryptomonnaies. En matière de cybercrime, nous ne savons jamais ce que nous ne savons pas encore.

Cela ne veut pas dire que nous ne devons pas prendre le temps de réfléchir à ce que le futur nous réserve, et nous préparer aux dangers tout proches qui nous guettent peut-être. Voici donc ce qui pourrait d'après nous se produire en 2019. Vous êtes prêts ?

De nouvelles intrusions au succès retentissant pousseront l'industrie de la sécurité informatique à résoudre enfin la problématique de la configuration nom d'utilisateur/mot de passe.

Le casse-tête nom d'utilisateur/mot de passe tourmente les consommateurs comme les entreprises depuis de nombreuses années. De nombreuses solutions existent, comme le chiffrement asymétrique, la biométrie, les chaînes de blocs, les solutions matérielles, etc., mais jusqu'ici, l'industrie de la cybersécurité n'est pas parvenue à s'accorder sur une norme capable de régler le problème. En 2019, des efforts concertés pour remplacer complètement les mots de passe devraient être mis en œuvre.

Les botnets de l'internet des objets frapperont les appareils qui nous entourent.

Au deuxième semestre 2018, nous avons pu constater que des milliers de routeurs MikroTik avaient été piratés à des fins de minage de cryptomonnaies. Ce n'est qu'un aperçu de ce qui nous attend en cette nouvelle année. En effet, de plus en plus d'appareils seront sans doute compromis pour servir les intérêts de menaces diverses et variées, des programmes de minage aux chevaux de Troie. La compromission à grande échelle de la sécurité des routeurs et des appareils de l'IoT deviendra une réalité, avec toutes les difficultés, bien plus importantes que pour les ordinateurs, que leur réparation entraîne. L'application de correctifs ne peut pas à elle seule résoudre le problème d'infection d'un appareil.

Le skimming numérique augmentera et se complexifiera.

Les cybercriminels afficheront leur intérêt pour les sites Web qui traitent les paiements et compromettront directement la page de paiement. Si le logiciel d'un panier d'achats est défaillant, les informations que l'utilisateur saisira sur la page de paiement de ses nouveaux patins à roulettes ou de billets de concert seront envoyées en texte clair, ce qui permettra aux cybercriminels de s'en emparer en temps réel. Les sociétés de sécurité ont pu le constater lors des attaques contre British Airways et Ticketmaster.

EternalBlue ou une imitation deviendra la méthode de facto de diffusion des malwares en 2019.

EternalBlue, grâce à sa capacité à s'autopropager, et d'autres menaces jouant sur la faille SMB, dont EternalRomance et EternalChampion, posent un problème bien spécifique aux organisations, et les cybercriminels les exploiteront encore pour distribuer de nouveaux malwares.

Le minage des cryptomonnaies sur les ordinateurs de bureau, du moins côté grand public, est sur le point de disparaître.

À nouveau, comme nous l'avons vu en octobre 2018 avec le piratage des routeurs MikroTik au profit de programmes de minage, les profits engrangés par les attaques de minage de cryptomonnaies contre des consommateurs individuels ne sont pas suffisants aux yeux des cybercriminels. Les attaques de programmes de minage viseront donc les systèmes en mesure de générer davantage de revenus (serveurs, IoT) et disparaîtront des autres (minage basé sur navigateur).

Les attaques conçues pour échapper à la détection, telles que les enregistreurs de son ou « soundloggers », entreront en circulation.

Les enregistreurs de frappe capables d'enregistrer les sons sont parfois surnommés « soundloggers ». Ils peuvent déterminer la cadence et le volume de frappe afin d'identifier les touches utilisées sur un clavier. Déjà au point, ce type d'attaque a été développé par des États pour nuire à leurs adversaires. Les attaques ayant recours à cette méthode et à d'autres techniques innovantes, conçues pour échapper à la détection, risquent de se retourner contre les entreprises et le grand public une fois en circulation.

L'intelligence artificielle servira à créer des exécutables malveillants.

Bien que l'idée d'exécuter une IA malveillante sur le système d'une victime relève de la pure science-fiction, au moins pour les 10 années à venir, des malwares créés et modifiés par une IA, et communiquant avec celle-ci représentent une réalité très dangereuse. Une IA qui communique avec des ordinateurs compromis et qui sait quels malwares sont détectés et comment peut rapidement déployer des contremesures. Les individus contrôlant l'IA mettront au point des malwares capables de modifier leur propre code pour éviter d'être détectés sur le système et ce, quel que soit l'outil de sécurité en place. Imaginez une infection par malware qui se comporterait un peu à la manière des Borgs dans Star Trek, adaptant ses méthodes d'attaque et de défense au fur et à mesure, en fonction des menaces qui l'entourent.

Le principe du « Bring your own security » se généralise tandis que la confiance s'amenuise.

De plus en plus de consommateurs apportent leurs propres dispositifs de sécurité au travail, qui constituent alors la première ou la deuxième couche de défense de leurs informations personnelles. À mesure que les entreprises prennent conscience des dangers qui entourent la politique du « Bring your own security », elles adoptent des procédures visant à se protéger contre la fuite de données sensibles. Malwarebytes a récemment mené une étude internationale et a constaté que près de 200 000 entreprises possédaient une version de Malwarebytes destinée aux particuliers.

L'éducation ressortait comme le domaine le plus prompt à adopter la politique du « Bring your own security », suivi par les technologies/logiciels, et par les services aux entreprises.

Conclusion

2018 a encore été une année exceptionnelle pour les malwares. Entre les attaques par minage de cryptomonnaies frénétiques qui semblaient sévir au quotidien et les campagnes de ransomwares froidement pensées en amont, les cartes ont été rebattues plusieurs fois pour suivre les tendances du marché, s'adapter aux répercussions des nouveaux règlements, et garder en éveil les entreprises, les consommateurs, et oui, nous, les chercheurs en sécurité.

Si l'on jette un œil à ce que nous réserve 2019, on peut d'ores et déjà se dire que le jeu du chat et de la souris continuera encore un moment ; de vieilles tactiques seront appliquées à de nouvelles menaces, et à l'inverse, de nouvelles méthodes seront employées sur des menaces maintes fois éprouvées. Comme à chaque fois, nous conseillons à nos lecteurs de se tenir informés, de rester vigilants, et de ne jamais tenir pour acquis la sécurité de leurs données ou de leurs appareils.

Nous prenons conscience des dangers, c'est vrai, mais les menaces s'adaptent à cette évolution. Si nous mettons tout en œuvre pour rendre leurs cibles plus difficiles à atteindre, notre sécurité et celle de nos organisations et des communautés en ligne en seront d'autant plus renforcées en 2019.

Contributeurs

Adam Kujawa : Directeur de Malwarebytes Labs

Wendy Zamora : Responsable de contenu, rédactrice en chef

Jovi Umawing : Rédacteur technique principal

Jerome Segura : Responsable de la cyberveille

William Tsing : Responsable des opérations

Pieter Arntz : Analyste principal de malwares

Chris Boyd : Analyste principal de malwares