CHECK POINT
RESEARCH

RAPPORT SÉCURITÉ 2018

WELCOME
TO THE FUTURE
OF CYBER SECURITY

Check Point
SOFTWARE TECHNOLOGIES LTD

TABLE DES MATIÈRES

INTRODUCTION

2017 était une année charnière qui a surpris de nombreuses personnes dans le secteur de la sécurité informatique. Résurgence de logiciels rançonneurs destructifs, botnets sur objets connectés, fuites de données, logiciels malveillants mobiles, technologies sophistiquées multi-vecteurs... il est clair que nous assistons à un point d'inflexion et une transition vers la cinquième génération des cyberattaques.

Avec l'évolution du paysage informatique, le Forum économique mondial a récemment élevé les cyberattaques au rang des trois principaux risques pour 2018. En effet, des pirates transforment efficacement des logiciels rançonneurs en armes pour paralyser de grandes institutions, affectant la santé et la vie des populations de pays entiers, et impactant très négativement les finances de nombreuses entreprises.

Les fuites de données ont pris le devant de la scène au cours de l'année écoulée, avec des révélations choquantes concernant des failles importantes pour les données des clients. De plus, l'ampleur et la fréquence de ces attaques, qu'il s'agisse d'Uber ou d'Equifax, ne montrent aucun signe de ralentissement.

Les failles de sécurité dans les fonctionnalités mobiles telles que Bluetooth, ainsi que dans les boutiques d'applications mobiles, font que de nombreuses variantes de logiciels malveillants continuent de circuler librement. En fait, des millions d'appareils mobiles dans le monde ont été infectés par des applications malveillantes générant des revenus élevés pour ceux qui parviennent à infiltrer les boutiques d'applications.

La popularité croissante et la hausse fulgurante de la valeur des cryptomonnaies ont également pris d'assaut le monde et ont conduit à une augmentation significative de la diffusion d'outils d'extraction de cryptomonnaies, qui sont rapidement devenus un vecteur d'attaque favori à des fins de monétisation.

Et finalement, la fuite des cyberoutils de la CIA par des groupes d'hacktivistes a semblé jeter une ombre sur l'écosystème de la sécurité de l'information dans son ensemble. Du prétendu piratage des élections jusqu'au sabotage d'infrastructures critiques, de nouvelles preuves ont vu le jour concernant les technologies sponsorisées par des états utilisées au cœur de certaines des plus grandes cyberattaques mondiales.

Dans ce rapport, nous apportons un regard rétrospectif sur l'année écoulée et essayons d'y donner un sens. Nous étudions également comment le paysage des menaces, à l'ère de la cinquième génération de la cybersécurité, s'étend désormais à de nombreux pays et secteurs d'activité empruntant de multiples vecteurs de réseaux, de Clouds et d'appareils mobiles, et utilise des technologies sponsorisées par des états. En examinant les attaques récentes, nous comprenons pourquoi 97 % des entreprises ne sont pas préparées à la cinquième génération des cyberattaques. Nous regardons ensuite de plus près ce que 2018 pourrait nous réserver et, surtout, comment nous y préparer au mieux.

CALENDRIER DES PRINCIPALES CYBER-ATTAQUES DE 2017

Jan

Princeton University fait partie des 27 000 victimes dont les données ont été effacées par la vulnérabilité de MongoDB.

Feb

PlayStation

2,5 millions de profils utilisateurs Xbox et PlayStation, y compris les noms, emails et identifiants personnels, sont piratés.

Mar

Verifone

La solution de point de vente du géant des paiements par carte bancaire Verifone a été attaquée.

Apr

NEW YORK POST

L'application mobile du New York Post est piratée et difffuse une vague de fausses actualités.

May

Emmanuel Macron, un candidat à la présidentielle, a été victime d'une fuite de 9 Go de documents confidentiels pour tenter de saboter les élections présidentielles en France.

Jun

MAERSK

Après WannaCry en mai, Petya provoque des perturbations massives dans le monde entier auprès de FedEx, Maersk, WPP et bien d'autres.

CopyCat, un logiciel malveillant mobile, infecte plus de 14 millions d'appareils Android dans le monde et rapporte 1,5 million de dollars de revenus publicitaires frauduleux aux pirates en seulement deux mois.

EQUIFAX

143 millions de dossiers clients comprenant des numéros de sécurité sociale, des détails de cartes bancaires ont été dérobés à Equifax, une importante agence de notation de crédit.

UBER

57 millions de dossiers de clients et de chauffeurs Uber sont dérobés via le piratage de son compte AWS. Uber paie 100 000 dollars pour taire la fuite.

Jul | Aug | Sep | Oct | Nov | Dec

УКРПОШТА
ГОЛОВНА ПОШТА КРАЇНИ

Le service postal de l'Ukraine est la cible d'une attaque DDoS visant à perturber ses activités nationales.

The National Lottery®

Une vaste attaque DDoS paralyse la loterie nationale du Royaume-Uni, empêchant des millions de personnes d'acheter des billets.

bitcoin

La plate-forme d'extraction de cryptomonnaie NiceHash est compromise par des pirates et perd 4 700 bitcoins (70 millions de dollars).

CYBERINCIDENTS MAJEURS DE 2017

FUITES DE DONNÉES CHOQUANTES

FUITE DE DONNÉES EQUIFAX

En septembre, Equifax, l'une des trois principales agences de notation de crédit aux États-Unis, a été victime d'une fuite qui a touché plus de 145 millions de clients. En exploitant une faille de sécurité dans le logiciel Apache Struts, les pirates ont pu dérober des données hautement confidentielles, notamment les noms, adresses, dates de naissance, numéros de cartes bancaires, numéros de sécurité sociale et numéros de permis de conduire.

FUITE DE DONNÉES UBER

Les informations personnelles de 57 millions de clients et de chauffeurs ont été dérobées grâce à l'obtention par des pirates d'identifiants pour accéder aux données stockées sur le compte AWS d'Uber. Plus grave encore, Uber a choisi de taire la fuite en payant les pirates 100 000 dollars pour qu'ils détruisent les documents confidentiels.

FUITE DE DONNÉES UNC

Plus de 1 300 patients en soins périnatals à l'Université de Caroline du Nord ont été victimes d'une grave fuite de données. Les informations dérobées comprenaient les noms complets, adresses, races, ethnies, numéros de sécurité sociale et différentes informations liées à la santé.

La promesse d'une plus grande agilité, d'une facilité d'intégration et d'une réduction des coûts a favorisé le développement du Cloud.

Cependant, les principaux problèmes de sécurité des services dans le Cloud résident dans leur exposition à l'extérieur. Cela signifie qu'ils sont accessibles en tout lieu et depuis tout appareil. Leur sécurité par défaut est par ailleurs inefficace.

Nous faisons tout pour encourager nos clients à ne pas dépendre uniquement de leur prestataire de services, mais plutôt de les associer dans un modèle de responsabilité mutuelle, afin de protéger à la fois leurs données et tous les moyens utilisés pour y accéder.

Yoav Daniely, Responsable de la gestion de produit, sécurité du Cloud

78 %

DES ENTREPRISES CONSIDÈRENT QUE LA SÉCURITÉ DES IAAS ET DES SAAS EST LEUR PRINCIPALE PRÉOCCUPATION [1]

64 %

DES ENTREPRISES ONT FAIT L'OBJET D'UNE ATTAQUE DE PHISHING AU COURS DE L'ANNÉE PASSÉE [2]

LOGICIELS MALVEILLANTS SPONSORISÉS PAR DES ÉTATS

FUITE « VAULT 7 »

En avril, le groupe de hacktivistes de WikiLeaks a publié un ensemble d'outils de piratage censés appartenir à la CIA. La fuite a montré que des technologies sponsorisées par les états sont utilisées dans la cinquième génération des cyberattaques. Cet ensemble extraordinaire d'outils de piratage met à disposition de son possesseur toute la capacité de piratage de la CIA. Son arsenal de logiciels malveillants et des dizaines d'exploitations de vulnérabilités zero-day visaient différents produits d'entreprises américaines et européennes, notamment l'iPhone d'Apple, le système Android de Google, les téléviseurs Samsung et Microsoft Windows.

INFRASTRUCTURE CRITIQUE AMÉRICAINE

Le gouvernement américain a signalé que « Dragonfly », un groupe de pirates apparemment sponsorisé par un état, a utilisé différentes tactiques et techniques pour essayer d'accéder à des systèmes de contrôle industriels (ICS) vitaux d'entreprises d'énergie et des infrastructures critiques américaines, via les réseaux de leurs fournisseurs et de tiers de confiance.

TAUX D'ATTAQUES EN EMEA

Check Point Research a révélé que les attaques de logiciels rançonneurs dans la zone EMEA ont doublé, passant de 28 % en 2016 à 48 % en 2017, déclenchées notamment par des pirates novices utilisant des logiciels malveillants hautement sophistiqués. Près de 20 % des entreprises ont été touchées par le logiciel malveillant Fireball, infectant plus de 250 millions d'ordinateurs dans le monde. Des pirates ont par ailleurs été en mesure de décupler les ravages causés par WannaCry grâce à des outils et des techniques de haut niveau sponsorisés par des états.

Les hacktivistes et les cybercriminels utilisent désormais avec des effets dévastateurs des logiciels malveillants sponsorisés par des états.

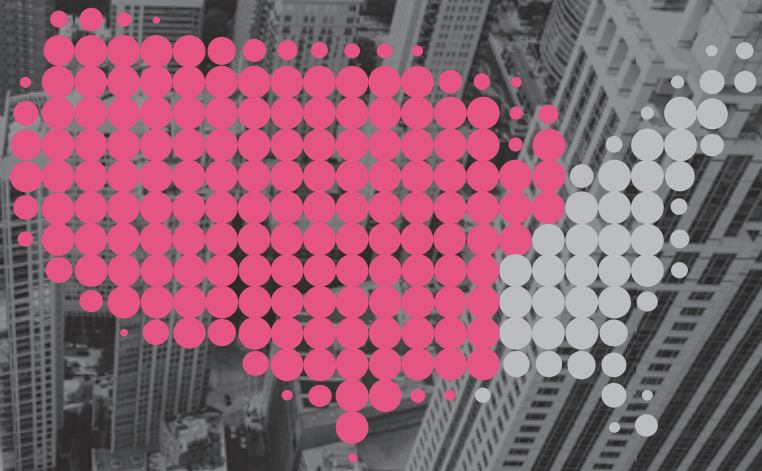
Dans de nombreux cas, l'élément humain au sein d'une entreprise du secteur public est exploité.

Avec autant d'enjeux géopolitiques, sans parler de la vie des gens, c'est un domaine de la cybersécurité qui doit être pris très au sérieux par toutes les agences gouvernementales du monde entier.

Richard Clayton, Responsable de la recherche sur les cybermenaces persistantes

39 ÉTATS SUR 50

AURAIENT ÉTÉ PIRATÉS LORS DE LA DERNIÈRE ÉLECTION PRÉSIDENTIELLE AMÉRICAINE[3]



BRAQUAGES RUSÉS DE CRYPTOMONNAIES

PIRATAGE DE YOUBIT

Avec le vol de bitcoins d'une valeur de 120 millions de dollars de Youbit, une place de change de cryptomonnaie sud-coréenne relativement inconnue, des cybercriminels ont exploité l'engouement pour la cryptomonnaie de manière plutôt radicale. Plutôt que de se consacrer au dur labeur d'extraction de ce précieux actif numérique, les cybercriminels choisissent souvent de le dérober à d'autres qui s'en sont chargés. En raison de la hausse fulgurante des cours des cryptomonnaies l'année dernière, des milliards de dollars ont déjà été dérobés tant à des individus qu'à des places de change.

ESCROQUERIE CONFIDO

Confido, une startup sur la plate-forme ethereum, a escroqué des milliers d'investisseurs puis s'est volatilisée après avoir recueilli 374 000 dollars lors d'une levée de fonds (ICO). Alors que de nombreuses cryptomonnaies tentent encore de trouver une application utile dans le monde réel, ethereum est devenu un chouchou parmi les financiers parce que ses ICO permettent à des startups de lever des sommes conséquentes lors de tours de financement ultra rapides.

BRAQUAGE ETHEREUM

Un pirate a réussi le second cambriolage le plus important de l'histoire des cryptomonnaies en exploitant une faille critique dans le portefeuille multi-signatures de Parity sur le réseau ethereum, drainant en quelques minutes trois portefeuilles massifs équivalent à plus de 31 000 000 de dollars. L'agresseur aurait pu dérober beaucoup plus sans l'intervention rapide de pirates éthiques qui se sont rapidement organisés pour le stopper.

En raison de l'anonymat des cryptomonnaies, les cybercriminels ont été parmi les premiers à les adopter. Mais avec la capitalisation boursière de bitcoin passant de 1 à 500 milliards de dollars en un an (à la date de publication), il est difficile de ne pas avoir remarqué le boom des cryptomonnaies.

Les criminels n'ont plus besoin d'essayer de cambrioler les grandes banques. Au lieu de cela, ils concentrent leurs efforts sur la conception de nouveaux moyens créatifs de dérober des portefeuilles numériques uniques. Non seulement, cela leur profite mais retire également des ressources à ceux qui extraient légitimement ces actifs numériques de plus en plus précieux.

Steve Johnson, Responsable de la prévention avancée des menaces

59 %

DES ENTREPRISES CONSIDÈRENT QUE LES LOGICIELS RANÇONNEURS SONT LA PLUS GRANDE MENACE [4]

ATTAQUES EFFRAYANTES DE LOGICIELS RANÇONNEURS

WANNACRY

Des milliers de chirurgies et de rendez-vous patients ont été annulés au NHS (système de santé publique du Royaume-Uni), et des milliers d'entreprises et d'organismes de services publics dans le monde entier, y compris Telefónica et les chemins de fer allemands, ont été victimes de perturbations massives à la suite de l'attaque du logiciel rançonneur WannaCry. L'attaque a obligé les entreprises à recourir à des méthodes traditionnelles employant des stylos et du papier pendant que les logiciels rançonneurs verrouillaient leurs systèmes informatiques et exigeaient un paiement en bitcoins pour déchiffrer leurs fichiers et y restituer l'accès.

NOTPETYA

En perturbant la chaîne de production et d'expédition de Reckitt Benckiser, le fabricant de Nurofen et de Durex, le logiciel rançonneur NotPetya lui a causé plus de 100 millions de dollars de pertes et a provoqué des ravages à grande échelle dans le monde entier. Quand bien même il visait principalement l'Ukraine, NotPetya a touché des entreprises dans le monde entier, notamment la société de logistique danoise Maersk, le service de livraisons américain FedEx et la société de publicité britannique WPP. Après s'être rendu maître d'un ordinateur infecté, le logiciel malveillant exige le paiement de 300 dollars en équivalent bitcoins à ses auteurs.

BAD RABBIT

En octobre, une nouvelle attaque à grande échelle de logiciel rançonneur a été lancée contre des sociétés d'infrastructures critiques ainsi que des entreprises des secteurs de la santé, de la finance, de la distribution et des logiciels. L'attaque s'est principalement concentrée sur l'Ukraine, impactant le métro de Kiev, l'aéroport international d'Odessa, le ministère des finances et d'autres infrastructures critiques. Cette fois, les auteurs ont verrouillé les ordinateurs de leurs victimes et ont exigé 280 dollars en équivalent bitcoins pour les déchiffrer.

19 494

CONSULTATIONS HOSPITALIÈRES ONT ÉTÉ ANNULÉES EN RAISON DE L'ATTAQUE DU LOGICIEL RANÇONNEUR WANNACRY[5]

Les logiciels rançonneurs jouent un rôle dans la cybersécurité depuis la fin des années 1980. Trente ans plus tard, ils ont pris le devant de la scène.

Dans les années 1980, les entreprises de soins et de santé étaient la cible principale. Les logiciels rançonneurs s'attaquent désormais à chaque entreprise et chaque individu.

Tant que cela continuera d'être une méthode extrêmement efficace et lucrative, et que les entreprises ne seront pas suffisamment informées quant à la nécessité d'adopter de bonnes mesures de cybersécurité, nous ne devrions pas être surpris de voir ces attaques se poursuivre dans les années à venir.

Tal Eisner, Responsable du marketing produit, Prévention des menaces

ATTAQUES DDOS RAVAGEUSES

EXTORSION DANS UNE BANQUE CORÉENNE

Contre la promesse de ne pas déclencher une attaque DDoS (déni de service distribué) qui perturberait les services en ligne de sept banques sud-coréennes, un groupe appelé « Armada Collective » a exigé environ 315 000 dollars en équivalent bitcoins. Les institutions financières sud-coréennes sont habituées à être la cible de cyberattaques, faisant face à des menaces similaires depuis 2011.

LOTERIE NATIONALE BRITANNIQUE

Des millions de clients ont été déçus de ne pas pouvoir acheter leurs billets de loterie hebdomadaires, car l'accès au site web de la loterie nationale britannique a été rendu impossible par une attaque DDoS à grande échelle. Pire encore, l'organisme avait été averti quelque temps auparavant d'une telle attaque si une rançon en bitcoins n'était pas payée.

DREAMHOST ATTAQUÉ

En août, l'hébergeur web DreamHost a subi une attaque DDoS paralysante qui a empêché l'accès à la plupart de ses services, perturbant notamment gravement ses services d'hébergement, son webmail et ses serveurs privés virtuels, ainsi que la performance de sa messagerie. L'attaque, qui a rapidement submergé les systèmes de l'entreprise, a probablement été déclenchée par des hacktivistes pour des raisons idéologiques.

24 %

DES ENTREPRISES ONT SUBI UNE ATTAQUE DDOS AU COURS DE L'ANNÉE ÉCOULÉE[6]

Au cours de l'année passée, les attaques DDoS ont atteint des cibles allant des sites web de grands médias à des infrastructures critiques. Comme les auteurs de ces attaques sont souvent des personnages de l'ombre, leurs raisons exactes de les déclencher sont difficiles à déterminer. Il s'agit cependant généralement d'hacktivisme politique ou de manœuvres contre des concurrents.

Nos études montrent que ces dernières années, les tentatives de recrutement d'objets connectés, à partir desquels de nombreuses attaques DDoS sont désormais lancées, se sont généralisées. Ceci est principalement dû au fait que ces appareils en ligne ne disposent que de mécanismes d'authentification faibles et que les pirates peuvent donc y pénétrer et les manipuler avec facilité.

Yariv Fishman, Responsable de la gestion des produits, Solutions verticales de sécurité

LOGICIELS MALVEILLANTS MOBILES INVASIFS

COPYCAT ET EXPENSIVEWALL

CopyCat, le logiciel malveillant mobile qui a infecté plus de 14 millions d'appareils à travers le monde, a généré des millions de dollars de profit en exploitant des appareils obsolètes à l'aide de fausses applications. Il a permis aux pirates de générer environ 1,5 million de dollars de revenus publicitaires frauduleux en seulement deux mois. Une nouvelle variante du logiciel malveillant Android, baptisée ExpensiveWall, qui enregistre les utilisateurs d'appareils mobiles auprès de services payants sans leur autorisation, a été découverte dans la boutique Google Play Store. Ce logiciel malveillant s'est infiltré dans la boutique Google Play Store et a infecté au moins 50 applications. Les applications infectées ont été téléchargées entre 1 et 4,2 millions de fois avant que Google ne les supprime.

LE GROUPE LAZARUS S'INTÉRESSE AUX MOBILES

Un nouvel ensemble de logiciels malveillants ciblant les appareils Samsung et des internautes coréens a été découvert, notamment dans certaines applications de bible coréennes. On soupçonne le groupe Lazarus, apparemment soutenu par la Corée du Nord, d'être l'instigateur de l'attaque qui cible spécifiquement la population de la Corée du Sud.

LOGICIEL MALVEILLANT MOBILE PRÉINSTALLÉ

Notre équipe de recherche sur les menaces mobiles a découvert que chaque entreprise avait subi une attaque de logiciel malveillant au cours de l'année écoulée ; 89 % d'entre elles ayant subi au moins une attaque de type homme du milieu sur un réseau wifi. Par ailleurs, 36 appareils Android dans seulement deux entreprises de notre échantillon d'enquête contenaient des logiciels malveillants qui ont été préinstallés quelque part dans la chaîne de distribution. Certains logiciels malveillants avaient même accès aux privilèges système, ce qui signifie qu'ils ne pouvaient être supprimés par l'utilisateur et que l'appareil devait être réinitialisé.

Comme indiqué dans notre Rapport Impact Mobile, toutes les grandes entreprises ont subi une attaque de logiciel malveillant l'année passée.

Les résultats montrent également que même les boutiques d'applications les plus fiables présentent des faiblesses qui sont exploitées régulièrement, et proposent constamment des applications malveillantes.

La cinquième génération du cyberpaysage fournit aux criminels une surface d'attaque plus étendue et donc plus d'opportunités pour en profiter. De nouvelles vulnérabilités, que ce soit par Bluetooth ou wifi, signifient également que les entreprises et les consommateurs doivent être conscients des risques posés par les appareils mobiles.

Jeremy Kaye, Responsable de la sécurité mobile

PLUS DE **300**

APPLICATIONS DE LA BOUTIQUE GOOGLE PLAY STORE CONTENAIENT DES LOGICIELS MALVEILLANTS QUI ONT ÉTÉ TÉLÉCHARGÉS PAR PLUS DE 106 MILLIONS D'UTILISATEURS[7]

100 %

DES ENTREPRISES ONT ÉTÉ VICTIMES D'UNE ATTAQUE DE LOGICIEL MALVEILLANT MOBILE[8]

RECRUTEMENT POUR L'ARMÉE DE BOTS

BOTNET HAJIME

Comme le fameux botnet Mirai, Hajime se propage via des appareils non sécurisés qui ont des ports Telnet ouverts et qui utilisent des mots de passe par défaut. Hajime s'est répandu sur plus de 300 000 appareils, mais son objectif reste inconnu. Quand bien même certains estiment qu'il s'agit d'une opération visant à purger l'Internet des objets du botnet Mirai, il pourrait facilement être utilisé à des fins malveillantes.

BLUEBORNE

Un nouveau vecteur d'attaque, surnommé « BlueBorne », a été découvert, ciblant une combinaison de huit vulnérabilités différentes affectant Android, iOS, des objets connectés, Windows et Linux. Les vulnérabilités BlueBorne sont capables de se propager d'un appareil à un autre sans intervention de l'agresseur, créant ainsi de grands botnets. Ce vecteur d'attaque ne nécessite aucune action de la part des utilisateurs, et aucune précondition ou configuration n'est requise, hormis l'activation de Bluetooth.

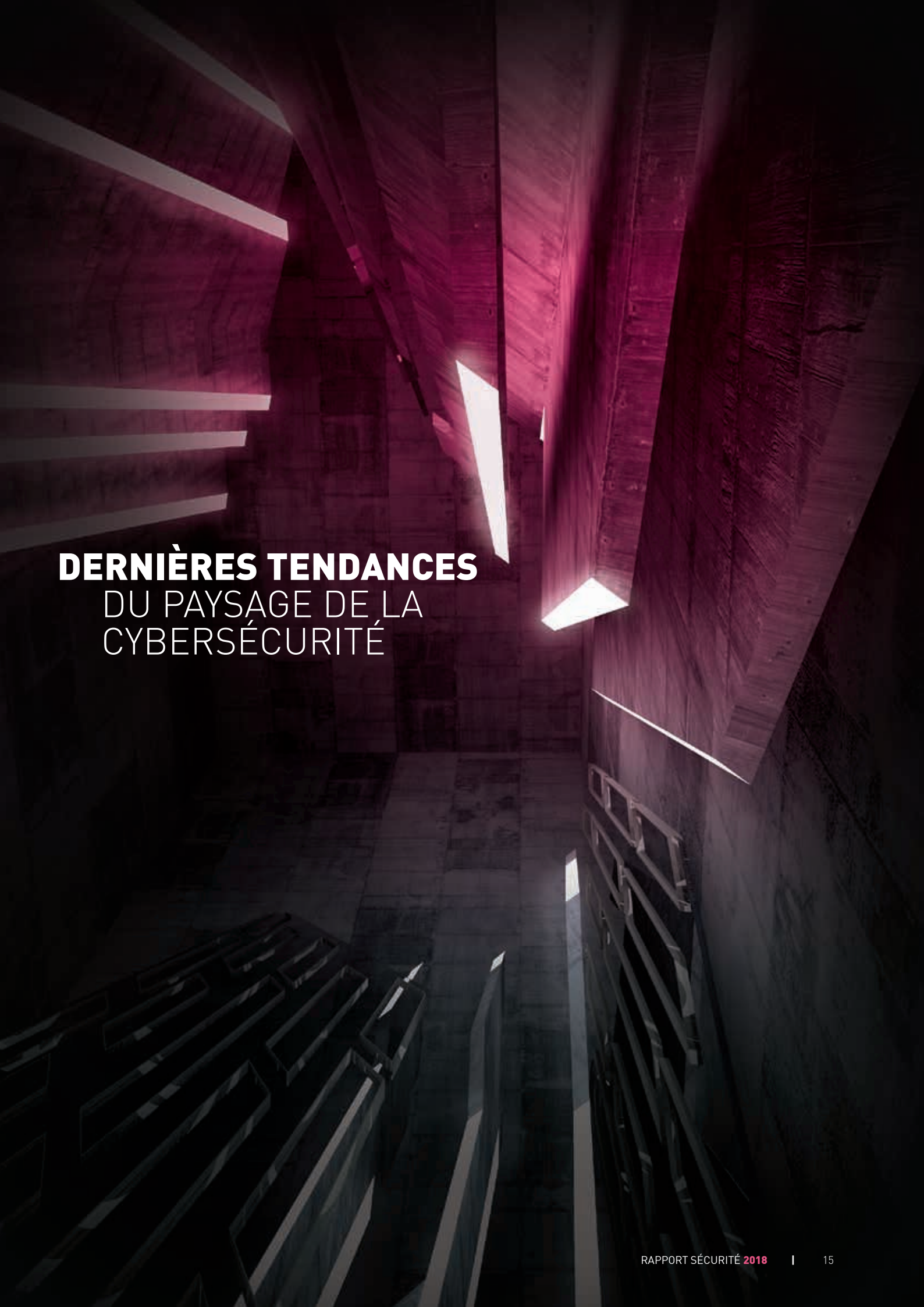
BOTNET IOTROOP

Un tout nouveau Botnet surnommé « IoTroop » a évolué et recrute des objets connectés à un rythme accéléré. Son potentiel de dommages est plus élevé que le botnet Mirai de 2016. IoTroop s'est propagé via des failles de sécurité dans les logiciels et les matériels des objets connectés, et plus d'un million d'entreprises semble avoir été touchées. Le botnet n'a pas encore déclenché son attaque, mais quand ce sera le cas, les conséquences pourraient être potentiellement dévastatrices.

IL A FALLU À

1 ENTREPRISE SUR **5**

ENTRE DEUX SEMAINES ET UNE ANNÉE POUR SE REMETTRE COMPLÈTEMENT D'UNE ATTAQUE[9]



DERNIÈRES TENDANCES DU PAYSAGE DE LA CYBERSÉCURITÉ

LES LOGICIELS MALVEILLANTS RENCONTRENT LES CRYPTOMONNAIES

Les développeurs de logiciels malveillants s'adaptent rapidement et suivent généralement les tendances qui leur permettent de maximiser l'efficacité et la portée de leurs activités. En raison de la hausse spectaculaire de leur valeur en 2017, la tendance actuelle suivie de près par les pirates est celle des cryptomonnaies.

Les cybercriminels ont plusieurs objectifs en ce qui concerne les cryptomonnaies. Certains cherchent à extraire des cryptomonnaies en détournant la puissance de calcul des utilisateurs via des logiciels malveillants appelés « extracteurs de cryptomonnaie ». Ceux-ci peuvent être diffusés via des navigateurs web qui utilisent des bloqueurs de publicités, ainsi que des sites de téléchargement de Torrent.

Une autre méthode utilisée par les cybercriminels consiste à revendiquer une partie des cryptomonnaies extraites par les utilisateurs. En fait, leur intention réelle est d'afficher des publicités frauduleuses ou de mener des activités malveillantes différentes.

Plutôt que de consacrer du temps et des efforts à extraire des cryptomonnaies, les attaques les plus sophistiquées font appel à des méthodes de cambriolage de banques plus « traditionnelles » et se dirigent vers l'argent, s'attaquant directement aux places de change elles-mêmes. Bien sûr, quand les places de change de cryptomonnaie sont trop difficiles à percer, il reste toujours la possibilité d'obtenir de façon illégitime les identifiants du portefeuille de cryptomonnaie d'un utilisateur.

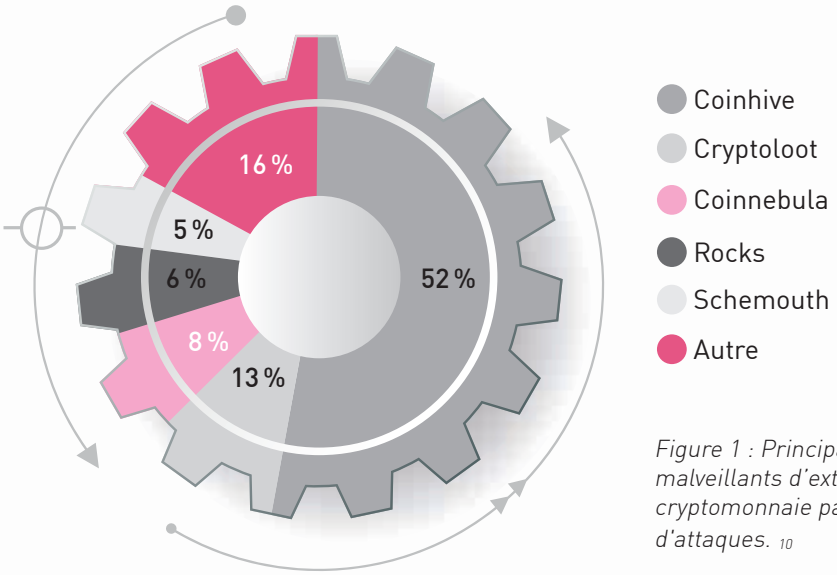


Figure 1 : Principaux logiciels malveillants d'extraction de cryptomonnaie par proportion d'attaques. [10]

LOGICIELS MALVEILLANTS CIBLANT MAC OS

Au cours de l'année écoulée, nous avons été témoins d'un nombre croissant d'attaques ciblant Apple MacOS. Ce qui était autrefois une occurrence rare est désormais devenu une menace réelle. Malheureusement, les développeurs de logiciels malveillants ont réussi à trouver de nouvelles façons créatives de contourner les barrières de protection d'Apple et de cibler les utilisateurs de Mac et d'iOS avec des logiciels malveillants avancés.

Cependant, les logiciels malveillants développés en plus grand nombre pour cibler ces systèmes d'exploitation de bonne réputation ont des objectifs différents. Le plus notable est le logiciel malveillant OSX/Dok, qui cherche à intercepter les mots de passe des utilisateurs et toute autre information confidentielle en contrôlant leurs communications réseau.

Ironiquement, la confiance que les utilisateurs de MacOS témoignent à la sécurité de leur système d'exploitation est souvent ce qui fait leur perte lorsqu'ils sont attaqués. Contrairement à d'autres systèmes d'exploitation, il n'existe que peu de solutions de sécurité pour MacOS, et peu d'utilisateurs les implémentent. En conséquence, une fois qu'un agresseur a réussi à contourner les protections intégrées, aucun obstacle supplémentaire ne subsiste.

Étant donné que le nombre d'utilisateurs de Mac est une bonne motivation pour les pirates informatiques qui cherchent à élargir leur surface d'attaque, nous devrions continuer à observer sur MacOS dans les années à venir la même tendance que celle observée sur Windows. Elle exigera des utilisateurs de Mac qu'ils renforcent leur sécurité et utilisent des technologies dédiées capables de stopper les attaques zero-day.

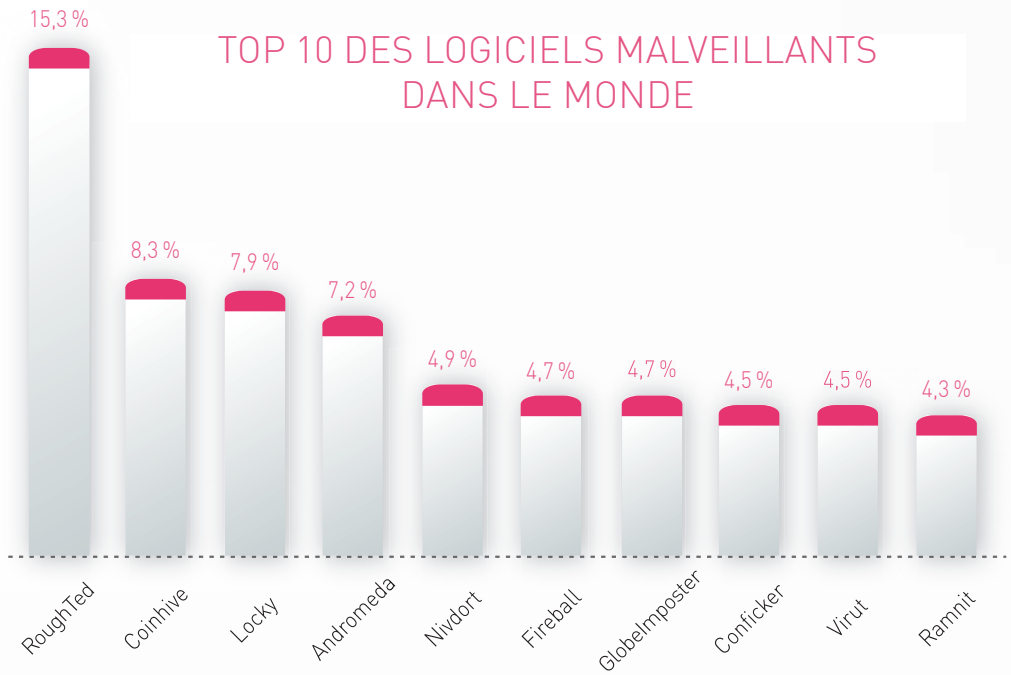


Figure 2 : Logiciels malveillants les plus répandus dans le monde : Pourcentage de réseaux d'entreprise subissant chaque type de logiciels malveillant. [11]

LOGICIELS MALVEILLANTS DE MASSE : L'INDUSTRIALISATION DES BOTNETS

Mirai, le botnet qui a causé des ravages dans le monde entier en 2016, signifie « futur » en japonais. En 2017, alors que les botnets augmentaient en nombre, et étendaient leur portée et leurs objectifs malveillants, ce « futur » était clairement arrivé.

Dans le monde des PC et des mobiles, les botnets sont devenus plus féroces, déclenchant des campagnes encore plus vastes que jamais auparavant.

Plus particulièrement l'année dernière, la découverte du logiciel malveillant « Judy », un logiciel publicitaire auto-cliquant qui, avec près de 18,5 millions de téléchargements, pourrait bien être la plus grande infection de logiciels malveillants mobiles sur Google Play.

Le principal trait commun des botnets est qu'ils essaient d'atteindre une masse critique pour réaliser leurs objectifs. Qu'il s'agisse d'attaques DDoS, d'extraction de cryptomonnaie ou de publicités de masse, l'essentiel est d'infecter autant d'appareils que possible, ce qui rend presque impossible l'éradication de l'attaque par des moyens traditionnels. Des mesures plus préventives grâce à un niveau plus élevé de détection et de prévention des logiciels malveillants sont donc nécessaires.

LES DÉVELOPPEURS DE LOGICIELS MALVEILLANTS S'INSPIRENT DES MEILLEURS

La cybersécurité étant souvent un jeu « du chat et de la souris », la future génération de créateurs de logiciels malveillants commence à utiliser les tactiques les plus avancées actuelles pour contourner les mesures de sécurité et rester en tête de la course. Ils le font de plus en plus en s'inspirant du « chat » (les agences de sécurité) elles-mêmes.

L'attaque des logiciels rançonneurs WannaCry de mai 2017, qui a utilisé la vulnérabilité « EternalBlue », en est un bon exemple. Dans ce cas cependant, comme dans beaucoup d'autres, la réussite de l'opération a été rendue possible grâce à l'application tardive de correctifs de sécurité ou simplement l'absence de tels correctifs. Découverte à l'origine par la NSA, l'attaque exploitait la vulnérabilité pour pénétrer dans des réseaux et s'y propager. Les entreprises qui n'ont pas mis à jour leur sécurité ont fini par payer un lourd tribut.

Une découverte similaire a été faite via la fuite « Vault 7 », qui a révélé qu'une partie du code utilisé par la CIA pour pirater des appareils mobiles était issue d'un logiciel malveillant ordinaire. Le principal avantage pour les entreprises et les utilisateurs est que toutes les cybermenaces sont liées les unes aux autres, quelle que soit leur origine, et devraient être prises en compte lors de la protection des réseaux informatiques.

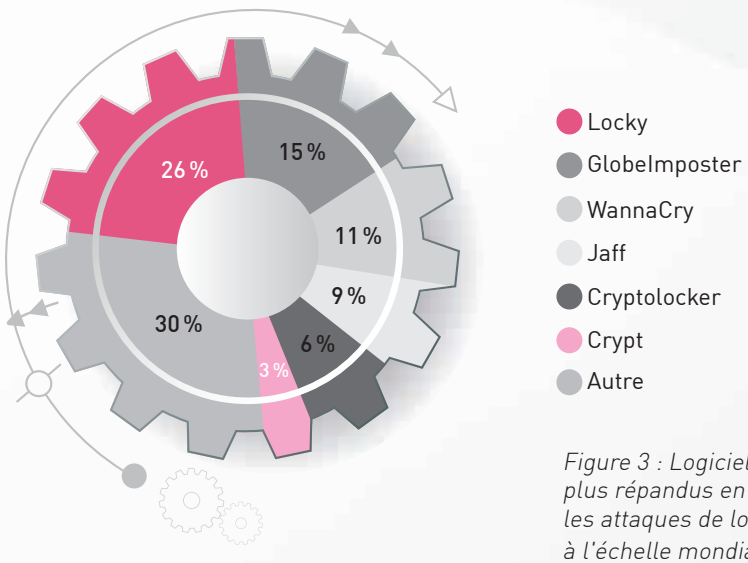


Figure 3 : Logiciels rançonneurs les plus répandus en proportion de toutes les attaques de logiciels rançonneurs à l'échelle mondiale. [12]

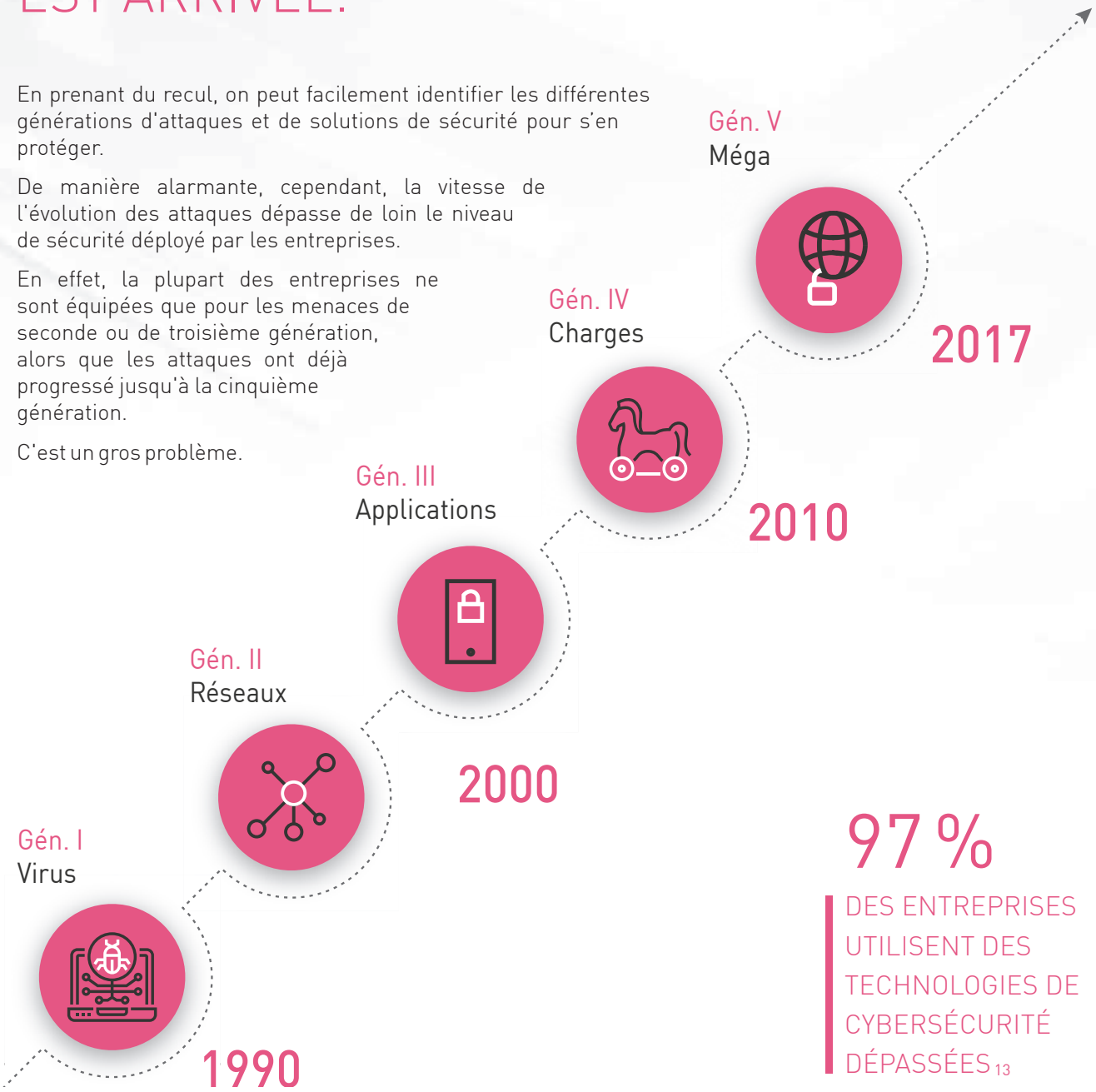
LA CINQUIÈME GÉNÉRATION DES MÉGA-CYBERATTAQUES EST ARRIVÉE.

En prenant du recul, on peut facilement identifier les différentes générations d'attaques et de solutions de sécurité pour s'en protéger.

De manière alarmante, cependant, la vitesse de l'évolution des attaques dépasse de loin le niveau de sécurité déployé par les entreprises.

En effet, la plupart des entreprises ne sont équipées que pour les menaces de seconde ou de troisième génération, alors que les attaques ont déjà progressé jusqu'à la cinquième génération.

C'est un gros problème.



97 %

DES ENTREPRISES UTILISENT DES TECHNOLOGIES DE CYBERSÉCURITÉ DÉPASSÉES [13]

RAPPORT **PAR SECTEUR**

FINANCE : FAIRE TOURNER LE MONDE

INTRODUCTION

L'époque des courtiers en bourse criant des ordres d'achat ou de vente sur fonds de bruits de téléphones et de machines à écrire est depuis longtemps révolue. Aujourd'hui, l'épine dorsale du monde financier est l'informatique, et avec des centaines de milliards de dollars en jeu chaque jour, les attaques sont inévitables.

Le principal motif des cyberattaques dans le secteur financier est évidemment l'argent. Cependant, l'argent n'est pas tout ce qui est en jeu.

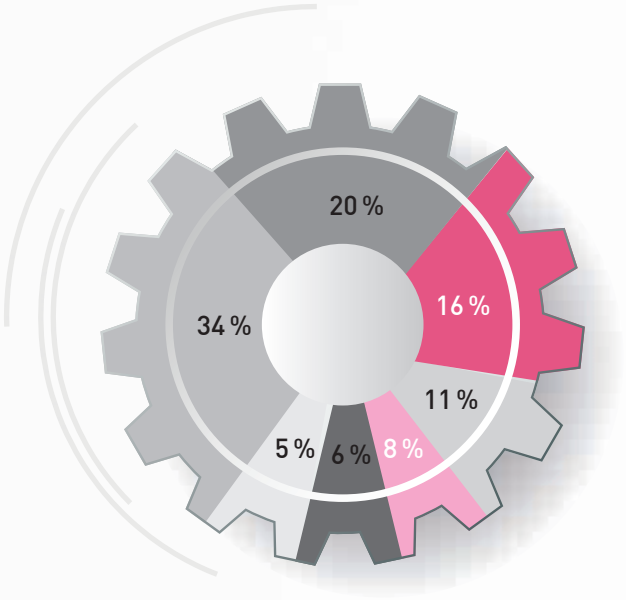


Figure 4 : Logiciels malveillants bancaires les plus répandus en proportion du nombre total de cyberattaques sur les banques. [14]

LE PROBLÈME

Le secteur financier est confronté à des cybermenaces provenant de trois domaines principaux : le réseau SWIFT, les logiciels bancaires pour consommateurs et le vol d'informations.

Comme l'a prouvé le vol de 60 millions de dollars de la Far East International Bank à Taïwan il n'y a pas si longtemps, même les systèmes bancaires propriétaires sont vulnérables à des attaques. Dans ce cas, le logiciel malveillant personnalisé a été inséré non seulement dans des PC et des serveurs web, mais également dans un terminal SWIFT utilisé par la banque. Une fois dans les systèmes, les pirates ont pu obtenir les identifiants nécessaires pour les transferts de fonds des paiements, puis ont falsifié les transferts effectués sur le réseau SWIFT.

En raison des nombreuses mesures que les banques ont désormais mises en place pour détecter et empêcher les attaques sur les comptes de leurs clients, le nombre de logiciels malveillants bancaires a diminué.

Cela a toutefois conduit les développeurs de logiciels malveillants à se tourner vers des cibles plus faciles pour éviter les défenses strictes des banques. Comme les voleurs n'ont plus besoin d'entrer eux-mêmes dans un compte bancaire pour acquérir l'argent de la victime, cela a entraîné une augmentation directe des attaques de logiciels rançonneurs. De cette façon, il suffit de prendre le contrôle de l'ordinateur d'une victime pour obtenir une rançon et lui extorquer de l'argent.

Alors que dans le monde des PC, les logiciels malveillants sont passés des services bancaires aux logiciels rançonneurs, les cybercriminels des services bancaires mobiles continuent de prospérer. En effet, l'essor de la banque mobile a introduit de nouveaux risques pour les utilisateurs à la recherche de commodité, qui ne sont peut-être pas conscients des menaces qui pèsent sur leurs appareils mobiles.

Un autre domaine est celui des informations détenues par les banques et les agences de notation de crédit. Cette année, la fuite d'Equifax, qui a compromis les informations confidentielles de près de la moitié des citoyens des États-Unis, en est un douloureux témoignage.

Enfin, avec la blockchain qui commence à ressembler à l'avenir de la finance, les pirates ont également ciblé la dernière tendance dans le secteur financier : les cryptomonnaies. En décembre dernier, Bitfinex, la plus grande place de change de cryptomonnaie au monde, a été fermée à la suite d'une attaque massive par déni de service. Ce n'était que la dernière d'une longue liste d'attaques qui ont frappé cette place de marché, entraînant des dommages évalués à plusieurs millions de dollars.

CONSEILS ET RECOMMANDATIONS

Pour se protéger de l'exploitation des réseaux SWIFT, les institutions financières doivent mettre en place non seulement des mesures de sécurité standard, mais également des protections de pointe qui dissuaderont même les pirates les plus sophistiqués.

Le braquage de la banque taïwanaise aurait pu être évité à l'aide de fonctionnalités avancées de surveillance pour assurer une visibilité complète, en surveillant et en enregistrant tous les événements, y compris les fichiers concernés, les processus lancés, les modifications apportées au registre système et l'activité réseau. Une solution doit être mise en place pour suivre et signaler les actions des logiciels malveillants, et bloquer les tentatives des pirates de dissimuler leurs traces.

Pour empêcher la diffusion de logiciels rançonneurs via des fichiers malveillants, les institutions financières doivent mettre en place des mesures sophistiquées qui bloquent les menaces connues et inconnues. Un système d'extraction et d'émulation des menaces qui consolide également la surveillance, la consignation, la génération de rapports et l'analyse des événements, pour corréler les données et fournir des informations exploitables sur les attaques, permet également à l'équipe de sécurité informatique de gagner un temps précieux.

Les institutions financières doivent comprendre que la protection des données de leurs clients dans le Cloud est une responsabilité partagée entre elles et leur prestataire de services de Cloud. Dans le cadre de cette responsabilité, les institutions financières devraient veiller à corriger immédiatement toutes les vulnérabilités connues, et à mettre en œuvre des solutions complètes de prévention des menaces dans le Cloud, offrant une protection zero-day et une gestion des livraisons agile et automatisée, adaptée à leurs besoins.

Même si les utilisateurs devraient être équipés de leur propre solution contre les logiciels malveillants dans leurs appareils mobiles, les institutions financières feraient bien d'intégrer des solutions avancées de cybersécurité mobile directement dans les applications bancaires utilisées par leurs clients. De cette façon, elles peuvent protéger non seulement contre les menaces des logiciels malveillants, les tentatives de phishing par SMS (SMiShing) et les problèmes d'authentification, mais également contre toute vulnérabilité dans le système d'exploitation mobile lui-même.

La bonne nouvelle est que les contrôles de sécurité se resserrent. Les pirates sont de plus en plus découragés, comme on le voit avec la disparition des logiciels malveillants bancaires sur PC.

À mesure que de nouvelles technologies telles que la Blockchain se développent, les banques doivent examiner de près leur infrastructure de sécurité et passer à la prochaine génération de technologies de cybersécurité. De cette façon, elles peuvent s'efforcer de ne laisser aucune porte ouverte et bloquer toutes les tentatives des cybercriminels de se servir eux-mêmes.

LE **SHOPPING**

INTRODUCTION

Avec des milliers voire des millions d'informations de cartes bancaires et d'identités de consommateurs logées au plus profond de leurs réseaux, les criminels ont de bonnes raisons d'étendre leurs efforts au ciblage du vecteur de la vente au détail.

Au fil des années, les cybercriminels ont imaginé des moyens sophistiqués d'abuser des terminaux de points de vente (TPV) et de pirater les réseaux des détaillants pour dérober les informations d'identité des clients et de leurs cartes bancaires. L'ampleur et la gravité de ces attaques ne font en effet qu'augmenter.

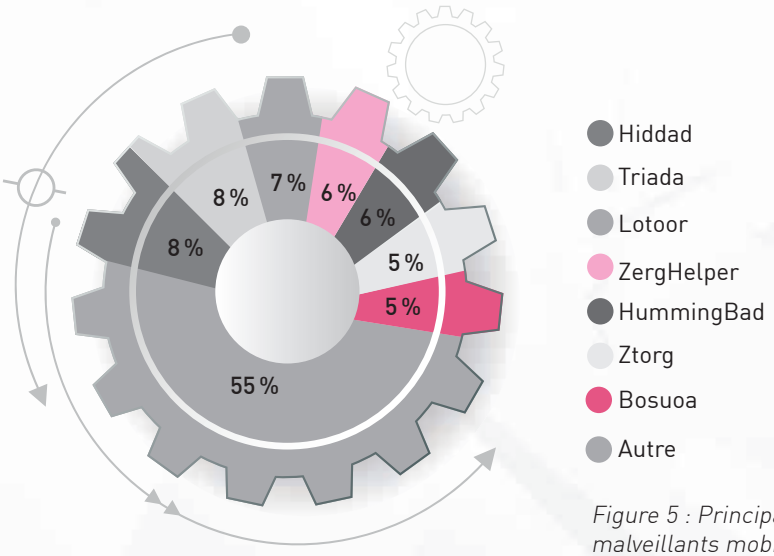


Figure 5 : Principaux logiciels malveillants mobiles. À mesure que de plus en plus de consommateurs effectuent des achats à partir de leurs appareils mobiles, les développeurs de logiciels malveillants mobiles sont de plus en plus incités à étendre leur diffusion. [15]

LE PROBLÈME

Les cybercriminels visant à dérober des données personnelles et financières des clients, fournies via les achats en ligne, le marketing numérique et les programmes de fidélité, il est facile de comprendre pourquoi plus d'un tiers des détaillants ont déjà été victimes d'une cyberattaque.

Les données volées et vendues sur le marché noir peuvent désormais atteindre 20 dollars par dossier. Il n'est donc pas surprenant que les informations de cartes bancaires, les coordonnées personnelles, les dates de naissance et les habitudes d'achat soient les données les plus fréquemment volées.

La fuite de données de GameStop au début de l'année passée en est un bon exemple. Après avoir dérobé des milliers de noms de clients, d'adresses et détails de cartes bancaires, y compris de numéros CVV2, les pirates ont commencé à les vendre sur le dark web.

Forever 21 a rejoint d'autres enseignes telles que Chipotle, Kmart, Brooks Brothers, Target et TJMaxx, ayant subi une attaque contre leurs TPV. Dans ce cas, les pirates ont eu accès aux informations de paiement des clients en désactivant les mesures de chiffrement et de tokenisation que le détaillant avait installées deux ans auparavant.

Comme l'illustrent nos études sur le site d'achat AliExpress, une autre méthode utilisée pour accéder aux informations des détaillants sur leurs clients consiste à mener des attaques de phishing. Dans ce cas, il s'agissait d'une attaque de phishing combinée à une attaque XSS, afin que la victime se sente encore plus convaincue que rien de suspect ne se produisait. Tout au long de l'année passée, de grands détaillants tels que Amazon, Best Buy, Walmart et Nike ont été utilisés pour leurrer des clients dans des escroqueries de shopping en ligne.

Le tort causé à la réputation d'une entreprise, ainsi que les coûts financiers, peuvent être énormes. Selon certaines estimations, le coût moyen pour une entreprise est de 172 dollars par enregistrement client dérobé. Cela comprend les coûts d'assainissement, le coût du manque à gagner en raison des temps d'arrêt, les amendes réglementaires et les frais juridiques. Nos enquêtes ont également révélé que jusqu'à 20 % des acheteurs ne feraient plus d'achats auprès d'une enseigne victime d'une cyberattaque. C'est un prix élevé à payer pour ce qui est essentiellement évitable.

20 %

DES ACHETEURS DISENT QU'ILS NE REVIENDRAIENT PLUS DANS UNE ENSEIGNE QUI A ÉTÉ VICTIME D'UNE CYBERATTAQUE [16]

1 DÉTAILLANT **sur 3**

A DÉJÀ ÉTÉ TOUCHÉ PAR UNE CYBERATTAQUE [17]

CONSEILS ET RECOMMANDATIONS

Mai 2018 voit la mise en application du Règlement Général de l'UE sur la Protection des Données (RGPD), qui aura d'importantes ramifications sur les détaillants, entre autres, dans le monde entier. Pour éviter les conséquences d'une infraction, les entreprises doivent adopter un état d'esprit de sécurité, et implémenter des architectures dynamiques qui se mettent à jour avec des protections en temps réel.

Premièrement, la norme PCI DSS devrait être mise en œuvre pour les activités courantes dans le cadre d'une stratégie de sécurité globale. Cela peut inclure la surveillance active des contrôles de sécurité afin d'assurer un fonctionnement efficace et approprié. Des stratégies d'audit doivent également s'appliquer en temps réel pour garantir la configuration et le fonctionnement corrects des contrôles de sécurité tels que le pare-feu, l'antivirus, la prévention des intrusions et la prévention des fuites de données.

Les détaillants qui utilisent des terminaux de point de vente doivent également chiffrer toutes les transactions par carte bancaire de bout en bout afin de protéger les données des clients. Il est également essentiel de considérer la défense du réseau comme étant un ensemble de points d'accès multiples plutôt qu'un seul périmètre.

Une approche à plusieurs niveaux comprenant une couche de mise en application, une couche de contrôle et une couche d'administration, est également vitale. Nous vous recommandons de créer un plan de protection de type passerelle/postes qui identifie et bloque les programmes malveillants conçus pour infecter des machines, collecter et extraire des informations sur les clients. Les politiques de sécurité définies par l'administrateur et les protections automatisées doivent également comprendre des règles qui définissent spécifiquement les contrôles d'accès et les politiques de sécurité des données avec des points de mise en application.

Enfin, en cas d'attaque, les entreprises ont besoin d'un plan de mesures correctives en place pour assurer le rétablissement de l'intégrité de l'entreprise, de sa réputation et de ses activités. Ce plan doit être bien préparé avec tous les intervenants impliqués, leur rôle et les interactions au sein de l'équipe d'intervention.

LA CURE DE SÉCURITÉ **BONNE POUR LA SANTÉ**

INTRODUCTION

Du point de vue de la cybersécurité, le secteur de la santé est peut-être celui le plus sensible, car il soigne non seulement des personnes vulnérables, mais il est lui-même extrêmement fragile.

Dans un secteur sur lequel le public compte littéralement pour sauver sa vie, les prestataires de soins de santé sont des cibles faciles à des fins d'extorsion. La fuite d'informations sensibles ou l'arrêt des activités n'est pas une option.

LE PROBLÈME

Le matériel du secteur de la santé est souvent privé de mises à jour en raison de la réglementation, et de toute manière doit maximiser la disponibilité de ses dispositifs médicaux.

Malheureusement, cela signifie qu'il a été l'un des secteurs les plus durement touchés par l'attaque de WannaCry qui a empêcher le fonctionnement d'une grande partie du NHS (système de santé publique du Royaume-Uni) en mai dernier. Les ordinateurs essentiels à diverses fonctions, y compris les scanners IRM, les laboratoires d'analyses et les pharmacies, n'ont pu fonctionner, ce qui a entraîné l'annulation de milliers de rendez-vous et d'opérations.

Le secteur de la santé est également visé par des pirates informatiques qui cherchent à dérober de grandes quantités d'informations confidentielles, que ce soit à des fins de vol d'identité, de fraude ou de vente sur Internet. Tel était le cas du système de santé Henry Ford de Detroit l'année dernière, qui a été victime du vol de plus de 18 000 dossiers médicaux de patients uniques.

Et enfin, un autre vecteur de menace qui est devenu de plus en plus important au cours de l'année écoulée est la vulnérabilité des dispositifs médicaux eux-mêmes.

En effet, alors que l'attaque des logiciels rançonneurs WannaCry a affecté plus de 200 000 systèmes Windows au Royaume-Uni, elle a également infecté l'équipement de radiologie Bayer Medrad à la fois localement et aux États-Unis. Les dommages causés à ces dispositifs peuvent souvent passer inaperçus, mais néanmoins les pannes de dispositifs médicaux de ce type augmentent les besoins en ressources, retardent les soins et déclenchent plus d'erreurs cliniques.

C'est aussi effrayant que cela puisse paraître. Permettre à des pirates de potentiellement mettre en danger la santé des patients à distance en exploitant des vulnérabilités existantes est certainement une menace qui doit être adressée et corrigée avant que ces attaques ne se concrétisent.

CONSEILS ET RECOMMANDATIONS

Pour s'assurer que les patients bénéficient des services d'urgence dont ils ont besoin, les organismes de santé ont besoin d'une solution qui non seulement détecte les menaces avancées ciblant leur réseau, mais les empêche finalement d'y accéder. Cela signifie disposer d'une solution qui inclut des fonctionnalités de pare-feu, de prévention des intrusions, de contrôle des applications, antibots et antispam, ainsi que des technologies d'extraction et d'émulation des menaces.

Les prestataires de soins de santé devraient certainement s'assurer qu'ils disposent également des capacités de détection d'exploitations de vulnérabilités au niveau du processeur. Cela leur permet de livrer des documents sains pendant que le fichier est vérifié en arrière-plan, sans impact sur leurs activités. De cette façon, ils peuvent bloquer les logiciels malveillants conçus pour contourner les technologies de sandboxing classiques, et renforcer leur sécurité contre des menaces avancées telles que WannaCry.

Les prestataires de soins de santé devraient également essayer de minimiser la complexité de leurs réseaux, minimiser la disparité des versions logicielles utilisées, et administrer leur sécurité à partir d'une seule interface utilisateur. Cela faciliterait la mise à jour de leurs systèmes et la surveillance des menaces, ainsi que la mise en œuvre de correctifs de sécurité en temps opportun.

Enfin, pour protéger les dispositifs connectés, il est nécessaire de déterminer et maîtriser ce qui est connecté dans l'environnement de soins de santé. C'est seulement à ce moment-là qu'une segmentation appropriée de ces dispositifs et des politiques d'accès appropriées pourront être appliquées. Cela permettra d'empêcher les attaques potentielles grâce à l'inspection approfondie des paquets et le filtrage des URL, par exemple, pour maintenir l'intégrité des données contenues dans ces appareils et les opérations qu'ils effectuent.

ÉVOLUTION DE LA **FABRICATION**

INTRODUCTION

Depuis la révolution industrielle qui a commencé au 18e siècle à Manchester, l'industrie manufacturière a subi une révolution tous les cent ans. À une époque où les progrès technologiques ne cessent de se poursuivre, les temps changent à un rythme plus rapide. L'ère de l'automatisation reposant sur des contrôleurs est désormais progressivement remplacée par « l'industrie intelligente», autrement appelée « industrie 4.0 ».

Bien qu'elle vise à rationaliser la production manufacturière et améliorer les capacités numériques tout au long des processus de la chaîne d'approvisionnement, l'Industrie 4.0 comporte également de nouveaux risques et cybermenaces.

LE PROBLÈME

Pensant que leurs usines ne sont pas une cible pour les cybercriminels, de nombreuses entreprises manufacturières se sont brutalement réveillées en mai 2017. Ce mois-ci, l'attaque du logiciel rançonneur WannaCry a provoqué la fermeture des usines automobiles Renault-Nissan en Europe et de l'usine automobile Honda au Japon, et a provoqué des perturbations massives des cycles de production d'entreprises dans le monde. Au cours de l'été de la même année, environ la moitié des victimes de l'attaque du logiciel rançonneur Petya étaient des fabricants.

Cependant, ce n'est pas seulement les usines de fabrication qui sont ciblées par les cyberattaques. Chaque fabricant possède des informations vitales qui seraient préjudiciables si elles étaient perdues ou volées, notamment des données de recherche et de développement ou des plans, sans oublié les informations des clients. Les risques pour le secteur manufacturier sont vastes et se développent de façon exponentielle.

À mesure que l'industrie mondiale entre dans la prochaine révolution industrielle, l'élaboration d'une approche stratégique intégrant entièrement ces risques sera fondamentale pour les chaînes de valeur manufacturières, car elles combinent la technologie opérationnelle et la technologie de l'information.

Avec plus de points d'accès disponibles pour pénétrer dans le vaste réseau qui couvre non seulement la chaîne d'approvisionnement industrielle mais également les objets connectés utilisés dans l'administration de l'entreprise et de l'usine elle-même, les entreprises doivent se doter de moyens pour éviter tout accès non autorisé.

82 %

DES FABRICANTS ONT SUBI UNE ATTAQUE DE PHISHING AU COURS DE L'ANNÉE PASSÉE [18]

CONSEILS ET RECOMMANDATIONS

Comme pour tout autre secteur, les fabricants devraient mettre en œuvre des programmes de formation à la cybersécurité pour leurs collaborateurs, afin que la main-d'œuvre soit sensibilisée aux pratiques les plus élémentaires en matière de sécurité des technologies de l'information.

De plus, des évaluations des risques devraient être effectuées dans l'ensemble de l'environnement de production pour identifier les biens les plus précieux, leur localisation, qui y a accès et comment ils peuvent être protégés. Cela devrait inclure un examen approfondi de l'entreprise, du DSN, des systèmes de contrôle industriel et de tous les appareils connectés. On ne saurait également trop insister sur de bonnes techniques d'hygiène telles que la segmentation entre les technologies opérationnelles et informatiques.

Il est également nécessaire de déployer des technologies ICS/SCADA spécialisées. L'inspection approfondie des paquets des protocoles SCADA tels que la communication MQTT/BACnet/Modbus entre les machines et les systèmes de gestion qui les contrôlent, est nécessaire afin d'empêcher la manipulation de l'environnement de fabrication. Les solutions doivent également inclure des paramètres de haute visibilité, notamment un contrôle granulaire du trafic ICS/SCADA, des correctifs virtuels grâce à l'utilisation de signatures ICS et des appliances durcies pour les environnements difficiles.

Grâce à l'utilisation d'appliances de sécurité et de services d'émulation des menaces dans le Cloud pour se prémunir contre les logiciels malveillants inconnus et zero-day, les fabricants peuvent également sécuriser leurs réseaux contre les logiciels rançonneurs.

Les fabricants peuvent également empêcher l'accès non autorisé aux informations de l'entreprise à l'aide de technologies de contrôle des applications, d'antiphishing, d'antispywares, de sécurité des données et d'accès à distance, offrant une protection complète grâce à une architecture de sécurité unifiée.

La protection de l'industrie 4.0 est une tâche complexe et de grande envergure, bien qu'il existe de nombreux moyens élémentaires et standard permettant aux entreprises de prendre des mesures pour se protéger.

En combinant cette approche avec des contrôles d'accès robustes, la technologie opérationnelle critique peut être sécurisée au niveau des points de mise en application et des postes pour protéger à la fois les données et les processus.

UNE QUESTION DE **SÉCURITÉ NATIONALE**

INTRODUCTION

En raison de sa nature même, le secteur gouvernemental détient des informations précieuses tant au niveau national que privé. Avec des données confidentielles concernant chaque citoyen, ainsi que des informations sur la politique gouvernementale, notamment en matière d'énergie ou de diplomatie, cela en fait une cible très prisée des pirates informatiques.

Grâce à la mise en œuvre de nouvelles technologies et l'accès à de plus de services en ligne, les agences gouvernementales présentent également une surface d'attaque de plus en plus importante. Ces étapes sont incontestablement nécessaires, mais comportent certains risques qui doivent être évalués pour s'en protéger.

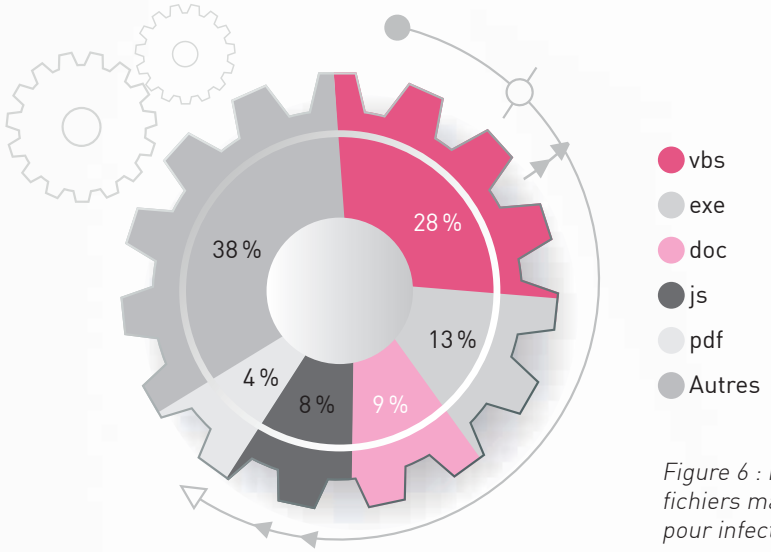


Figure 6 : Principaux types de fichiers malveillants utilisés pour infecter les ordinateurs des utilisateurs. [19]

LE PROBLÈME

Les technologies sponsorisées par des états étant souvent utilisées dans des attaques contre des agences et institutions nationales. Le secteur gouvernemental est souvent pris pour cible par les auteurs les plus avancés, les plus sophistiqués et les plus résolus, généralement appelés groupes de menaces persistantes avancées (APT).

Plutôt que de rechercher la cible la plus facile, les groupes APT choisissent généralement des cibles avec soin et s'y attellent aussi longtemps que nécessaire pour y accéder. Le cas échéant, ils développeront des armes sur mesure pour s'engouffrer dans une faille spécifique de la sécurité réseau, contre laquelle il est extrêmement difficile de se protéger.

L'une des méthodes d'attaque les plus couramment utilisées contre les institutions gouvernementales est le « phishing ». En juin 2017, des voleurs ont piraté le système de gestion de la paie du district d'éducation publique de Denver pour dérober 40 000 dollars aux employés via une escroquerie par phishing. Ce type d'attaque a profité du facteur le plus vulnérable de la sécurité de tout réseau : l'élément humain. Dans de tels cas, les emails de phishing semblent être envoyés depuis une adresse avec laquelle la victime a l'habitude de travailler et lui fait confiance.

Les détournements de compte d'applications dans le Cloud sont également très courants. L'intrusion dans les comptes de messagerie de nombreux politiciens britanniques au début de l'année passée, et même dans le compte de messagerie du Premier ministre via une attaque de brute force, en témoigne.

En outre, comme l'a montré l'indisponibilité de la banque nationale, du réseau électrique et de l'aéroport ukrainiens en juin 2017, les infrastructures gouvernementales faisaient partie des cibles mondiales touchées par l'attaque du logiciel rançonneur Petya. Cette attaque a saboté non seulement l'infrastructure nationale, mais a également causé des dommages économiques aux États-nations en raison de l'arrêt forcé des usines de fabrication.

Ces menaces ne devraient pas être prises à la légère. Les conséquences peuvent aller de l'affaiblissement des positions de négociation et des dommages économiques jusqu'à la dépréciation de la souveraineté nationale d'un État. En termes simples, ces menaces transforment la nouvelle ère de la technologie en un cauchemar pour les fonctionnaires des gouvernements.

CONSEILS ET RECOMMANDATIONS

Pour se protéger contre la myriade d'attaques de phishing de nouvelle génération, une nouvelle approche multidimensionnelle est requise. Ces défenses doivent protéger l'infrastructure de messagerie, fournir une protection antispam hautement fiable, et défendre les gouvernements contre une grande variété de menaces et de virus propagés par email.

Afin d'empêcher les détournements de comptes, tels que ceux subis par le Parlement britannique, les agences gouvernementales doivent mettre en œuvre des solutions de sécurité combinant à la fois des renseignements provenant du réseau et des appareils. Cette technologie doit être en mesure d'inspecter en profondeur la posture de sécurité du réseau et des postes.

Les technologies actuelles sont souvent inefficaces, car elles ne sont généralement pas suffisamment sécurisées et sont lourdes à mettre en œuvre.

Une nouvelle technologie à la fois transparente pour l'utilisateur et simple à utiliser sans que l'utilisateur final n'y prête attention, est nécessaire. De plus, elle doit rapidement prendre des décisions déterministes pour empêcher l'accès d'un imposteur.

Dans le passé, l'exploitation d'une vulnérabilité zero-day signifiait que tout était perdu d'avance, mais plus maintenant. Au cours des dernières années, nous avons développé des technologies capables de détecter et de bloquer les exploitations de vulnérabilités zero-day dont nous ignorions même l'existence. Celles-ci sont utilisées pour contrer les efforts des groupes APT capables de créer ces exploitations de vulnérabilités pour cibler une seule agence gouvernementale avec des logiciels rançonneurs.

Le nombre d'attaques contre les infrastructures critiques d'un gouvernement, souvent développées sans aucune attention portée à la cybersécurité et donc truffées de vulnérabilités, est en augmentation.

Il existe cependant aujourd'hui des solutions dédiées à ces systèmes, conçues pour permettre un fonctionnement sans faille de l'infrastructure tout en la protégeant contre de telles menaces.

32 %

D'AGENCES GOUVERNEMENTALES ONT ÉTÉ VICTIMES D'UNE FUITE DE DONNÉES AU COURS DE L'ANNÉE PASSÉE[20]

CE QUE NOUS **RÉSERVE L'AVENIR**

INTRODUCTION

Comme Abraham Lincoln l'a dit un jour, « Vous ne pouvez pas échapper à la responsabilité de demain en l'évitant aujourd'hui. » On ne saurait trop en souligner l'importance dans le monde de la cybersécurité.

Dans cette section, nous dévoilons quelles pourraient être les menaces qui pèseront sur nos réseaux et nos données à l'avenir, et dans la section suivante, nous verrons comment les entreprises peuvent remplir leur devoir de les éviter.

L'AVENIR : CLOUD ET MOBILITÉ

Les appareils mobiles font partie des écosystèmes informatiques et métiers dans le monde entier. Cependant, dans la plupart des entreprises, ces appareils ne sont pas sécurisés à un niveau proche de ce qu'ils devraient être compte-tenu de la valeur des actifs qu'ils stockent. Des failles dans la technologie et les systèmes d'exploitation mobiles continueront d'être découvertes, soulignant le besoin pour les entreprises de déployer une protection avancée contre les logiciels malveillants mobiles et l'interception des communications.

Les logiciels malveillants mobiles continueront également de proliférer, en particulier les logiciels malveillants bancaires mobiles, et la tendance des logiciels malveillants sous forme de service (MaaS), qui réduit la nécessité pour les pirates de disposer de compétences techniques et facilite ainsi les attaques, continuera de se renforcer.

Nous pouvons nous attendre à ce que des logiciels mobiles d'extraction de cryptomonnaie soient utilisés au service des criminels dans un proche avenir. Jusqu'à présent, les logiciels d'extraction de cryptomonnaie affectaient les serveurs web et les PC, mais comme la sécurité mobile est moins développée, il est probable que ce soit le prochain canal d'attaque.

77 %

DES PROFESSIONNELS DE L'INFORMATIQUE ESTIMENT QUE LEURS ÉQUIPES DE SÉCURITÉ NE SONT PAS PRÉPARÉES AUX DÉFIS ACTUELS DE LA CYBERSÉCURITÉ [21]

MIGRATION VERS LE CLOUD

Les entreprises continueront de migrer leurs données vers le Cloud à un rythme accéléré, à mesure qu'elles cherchent à rendre leurs activités toujours plus rentables dans un monde économiquement difficile.

Bien que l'utilisation du Cloud soit désormais répandue parmi les entreprises en raison de l'agilité et des réductions de coûts qu'il offre, la technologie est encore relativement nouvelle et continue d'évoluer. Cela fournit aux pirates plus de moyens d'accéder plus profondément aux systèmes d'entreprise.

En conséquence, les idées reçues sur les niveaux de sécurité nécessaires, ainsi qu'un manque de compréhension concernant la responsabilité de cette sécurité, sont courants. Cela laisse la porte ouverte aux failles.

En 2017, plus de 50 % des incidents de sécurité traités par l'équipe d'intervention de Check Point étaient liés au Cloud, et plus de 50 % d'entre eux étaient liés à des prises de contrôle d'applications en SaaS ou de serveurs hébergés. Les fuites de données continueront d'être une préoccupation majeure pour les entreprises qui se tournent vers le Cloud, en particulier en raison de l'utilisation accrue des services de partage de fichiers dans le Cloud.

L'adoption croissante de la messagerie en SaaS telle qu'Office 365 et G Suite de Google, ainsi que l'IaaS, en font une cible attrayante pour les cybercriminels. Nous pensons qu'elle sera de plus en plus ciblée en 2018.

Ces menaces potentielles seront également aggravées par les lourdes pénalités que les réglementations régionales telles que le RGPD pourraient infliger aux entreprises qui ne respectent pas ces nouvelles obligations.

50 %

DES INCIDENTS DE SÉCURITÉ TRAITÉS PAR L'ÉQUIPE D'INTERVENTION DE CHECK POINT ÉTAIENT LIÉS AU CLOUD [22]

SÉCURISATION DE VOTRE RÉSEAU

Les logiciels rançonneurs sont un moyen très efficace pour les criminels de gagner de l'argent, et sont de bons déguisements pour masquer des objectifs plus destructeurs. En raison de leur efficacité auprès de tous les types d'utilisateurs, des consommateurs aux entreprises, les logiciels rançonneurs continueront de se développer, et nous pouvons nous attendre à voir de plus grandes épidémies orchestrées dans le monde sur le modèle de WannaCry, Petya et Bad Rabbit.

Nous pouvons également nous attendre à d'autres tactiques d'extorsion créatives de la part des criminels, comme des concepts de « cooptation » pour encourager les victimes à propager les logiciels malveillants en échange d'une réduction de la rançon pour débloquer leurs ordinateurs.

À mesure que les systèmes d'exploitation deviennent plus sécurisés, nous pouvons nous attendre à ce que l'utilisation des exploitations ciblant les vulnérabilités de ces systèmes diminuent. Cela entraînera une augmentation de l'utilisation de techniques de piratage de base qui reposent sur l'erreur humaine et l'ingénierie sociale pour faciliter la propagation des logiciels rançonneurs.

La capacité des logiciels rançonneurs à collecter des fonds pour les cybercriminels est à l'origine de la tendance des logiciels rançonneurs sous forme de service et autres activités artisanales au sein du dark web. Nous pouvons nous attendre à ce que ces services se développent, ciblant non seulement les réseaux informatiques traditionnels, mais également les appareils mobiles et les objets connectés.

75 %

DES ENTREPRISES ÉVOQUENT DES PROBLÈMES DE RESSOURCES ET DE PERSONNEL DE SÉCURITÉ [23]

MISE EN APPLICATION DU RGPD

Le nouveau Règlement Général sur la Protection des Données de l'Union Européenne (RGPD) aura des conséquences importantes sur de nombreuses entreprises dans le monde entier. Les éléments essentiels du RGPD détaillent un certain nombre de « droits des citoyens de l'UE » en ce qui concerne la manière dont leurs données personnelles sont utilisées. La liste est vaste et nécessitera des changements importants dans les applications, les politiques et les procédures, afin d'assurer la conformité. En conséquence, avec le calendrier et les pénalités qu'il implique, le RGPD exercera une pression considérable sur toute entreprise qui gère les données des citoyens de l'UE.

Comme le règlement est tout nouveau, il n'existe aucun précédent d'audit antérieur sur lequel une entreprise peut s'appuyer. De nombreux aspects du RGPD sont également toujours « en cours ». Par exemple, le RGPD établit qu'un Contrôleur européen de la protection des données (CEPD) devra « jouer un rôle actif dans l'application de la législation européenne en matière de protection des données ». Cependant, à la date d'impression de ce rapport, la formalisation du CEPD est encore en cours et les spécificités doivent encore être déterminées.

Néanmoins, le délai d'exécution limité avant l'entrée en vigueur du règlement signifie que les entreprises devraient déjà se concentrer sur l'allocation de ressources pour la mise en œuvre de leur stratégie en matière de personnel, d'audits et de classification des données, d'analyse des risques, de journalisation des activités, d'identification des failles et de contrôles fondamentaux.

LES OBJETS CONNECTÉS DEVIENNENT PLUS INTELLIGENTS

La prolifération des objets connectés va se poursuivre et augmentera la surface d'attaque potentielle. Nous verrons plus de variantes des attaques Mirai et BlueBorne sur l'Internet des objets et les appareils connectés en 2018 et au-delà.

À mesure que de plus en plus d'appareils intelligents sont intégrés aux réseaux des entreprises, ces dernières devront commencer à mettre en œuvre de meilleures pratiques de sécurité pour les appareils et les réseaux auxquels ils se connectent. Ce sera essentiel pour empêcher les attaques à grande échelle. On peut envisager qu'une réglementation internationale oblige leur mise en œuvre.

Au-delà des attaques DDoS à grande échelle que nous avons vues en 2017, les cybercriminels exploiteront les objets connectés personnels pour accéder non seulement au réseau personnel d'une victime, mais également pour espionner son domicile physique. Notre rapport sur les appareils intelligents LG l'année dernière l'a souligné. Comme les utilisateurs n'ont généralement pas conscience de la sécurité de leurs appareils connectés personnels, ils ont tendance à laisser les paramètres par défaut dans leur état d'origine. Cela permet aux agresseurs d'avoir constamment accès au réseau personnel d'un utilisateur.

Les projets d'objets connectés au service de la ville intelligente continueront de se développer, aidant les villes à offrir de meilleurs services à leurs usagers tout en réduisant considérablement les coûts. Des solutions de cybersécurité de cinquième génération devront alors être mises en œuvre à chaque étape afin d'empêcher les attaques potentielles.

En raison de la gravité des attaques de WannaCry contre les organismes de santé, le secteur de la santé devra également commencer à protéger ses dispositifs médicaux connectés à Internet dans les hôpitaux afin d'empêcher les attaques potentiellement mortelles.

CRYPTOMONNAIES

Les cryptomonnaies étant de plus en plus la méthode de paiement privilégiée par les criminels à l'origine des épidémies de logiciels rançonneurs et de financement d'autres activités illégales, des réglementations plus strictes commenceront-elles à leur être appliquées ?

Les ressources importantes nécessaires à la création de cryptomonnaies ont également favorisé l'émergence des logiciels d'extraction. Ce sont de nouveaux outils quasi-malveillants utilisés pour générer des revenus en détournant la puissance du processeur des utilisateurs pour générer de la cryptomonnaie, souvent à l'insu ou sans le consentement des utilisateurs. Nous en avons déjà vu plusieurs exemples et, étant donné la valeur élevée des cryptomonnaies, nous pouvons nous attendre à ce que les cybercriminels trouvent de nouveaux moyens d'exploiter la puissance de calcul de leurs victimes pour extraire ces cryptomonnaies pour leur propre profit.

En raison de la valeur élevée du bitcoin et d'autres cryptomonnaies, les systèmes qui les entourent, tels que les places de change, sont également susceptibles d'être prises pour cible par des criminels cherchant à exploiter leurs vulnérabilités.

Une combinaison de ces facteurs pourrait bien amener les gouvernements et les autorités internationales à prendre des mesures contre l'utilisation abusive des cryptomonnaies, ce qui nuira à leur valeur.

DÉFENDRE LA NATION

En 2018 et au-delà, la cyberdéfense gagnera en importance parmi les organismes gouvernementaux à mesure qu'ils deviendront plus sensibles et plus à l'écoute du monde connecté dans lequel évolue leurs citoyens.

Les organismes parrainés par les états continueront de développer des technologies de cyberattaques pour la défense et l'offensive, et les groupes criminels motivés par des considérations financières continueront de chercher des moyens de monétiser les cyberattaques. Les hacktivistes continueront d'utiliser les cyberattaques pour transmettre leurs messages et des groupes terroristes pourraient également se tourner vers le cyberespace, à mesure que les armes qui étaient auparavant réservées aux services de défense des gouvernements sont rendues publiques.

Par conséquent, nous pourrions commencer à voir les gouvernements déployer davantage de protections sur leurs propres infrastructures critiques telles que les services d'approvisionnement d'eau et d'électricité, les services de santé, les administrations locales et l'infrastructure informatique qui les prend en charge.

RECOMMANDATIONS
POUR LA PLATE-FORME

ADOPTION DE L'ARCHITECTURE DE 5E GÉNÉRATION

Applications et données convergentes sur réseaux IP, déploiement d'applications « natives dans le Cloud », stratégies BYOD, utilisation d'objets connectés... la transformation numérique rapide des entreprises impose des exigences de sécurité toujours croissantes.

Les architectures de sécurité actuelles qui gèrent tout cela sont obsolètes, sont la cause la plus fréquente de problèmes d'indisponibilité et de sécurité, et conduisent à des défaillances catastrophiques.

En mettant en œuvre une architecture de « Gén. V » (cinquième génération), les entreprises peuvent éliminer les points de défaillance en leur apportant la robustesse et la résilience nécessaires à la poursuite des activités et au maintien de la sécurité en toute circonstance.

LES ENTREPRISES QUI UTILISENT DES TECHNOLOGIES DE PRÉVENTION ACCÉLÈRENT DE **30 %** L'IDENTIFICATION ET LE BLOCAGE DES MENACES [24]

L'architecture « Gén. V » crée une architecture de sécurité consolidée et unifiée qui gère et intègre les appareils mobiles, le Cloud et les réseaux pour stopper les cyberattaques de cinquième génération. La prévention intégrée des menaces doit également travailler avec une politique de sécurité dynamique sur toutes les plates-formes qui expriment les besoins de l'entreprise, doit prendre en charge les besoin du Cloud avec évolutivité automatique, et doit être capable de s'intégrer de manière flexible aux API tierces.

Un environnement de prévention des menaces multicouches, avancé et unifié doit inclure des solutions de prévention par technologies de sandboxing au niveau du processeur, d'extraction des menaces, d'antiphishing et d'antiransomwares pour se prémunir des attaques « zero-day » connues et inconnues.

De cette manière, disposer de la bonne architecture sur laquelle repose toute l'infrastructure de sécurité est le seul moyen de garantir un mur de protection unique et cohérent pour stopper les cyberattaques de cinquième génération.

ADMINISTRATION CONSOLIDÉE

UTILISATION DES MEILLEURES TECHNOLOGIES DE SÉCURITÉ

DÉVELOPPEMENT DE VOTRE INFRASTRUCTURE DANS LE CLOUD

Au fur et à mesure que les entreprises évoluent, les données métier sont de plus en plus consultées via des plates-formes dans le Cloud, à tout moment et en tout lieu. Cela signifie que le trafic réseau transite en dehors des protections de sécurité informatique traditionnelles et que les risques associés représentent un énorme défi. De plus, les logiciels malveillants introduits dans le Cloud peuvent se propager facilement parmi les applications dans le Cloud, attaquer des segments virtuels ou même revenir sans encombre dans les réseaux d'entreprise.

Pour surmonter ces défis, les entreprises doivent créer une synergie entre les meilleures pratiques de sécurité et les technologies de sécurité pour le Cloud. Celles-ci devraient principalement inclure des techniques avancées de prévention et de blocage. Elles devraient également inclure des outils et des techniques d'administration robustes et familiers, comprenant visibilité, supervision et rapports complets. Cela permettra aux entreprises d'identifier rapidement une activité réseau malveillante ou des indicateurs de compromissions connues, et d'intervenir en conséquence.

Afin de sécuriser les Datacenters dans le Cloud, il est essentiel de maintenir l'agilité et la vitesse du Cloud pour une automatisation et une orchestration transparente avec un large éventail d'infrastructures de Cloud telles qu'AWS, Cisco ACI, Microsoft Azure, OpenStack, VMWare et autres. La solution doit également inclure des contrôles de sécurité avancés avec prise en charge de la micro-segmentation adaptée à une infrastructure dans le Cloud. Cela peut contribuer à réduire la surface d'attaque et constituer une première étape importante pour empêcher les cyberattaques d'atteindre le réseau virtuel.

La protection des applications SaaS, en empêchant la prise de contrôle des comptes, les tentatives de phishing et la propagation des logiciels malveillants sur les réseaux d'entreprise, nécessite des solutions avancées. Ces solutions devraient permettre d'identifier les accès légitimes des utilisateurs en analysant les données en temps réel, à la fois sur les ordinateurs et les appareils mobiles.

Enfin, pour adopter pleinement le Cloud, les entreprises doivent disposer des technologies et des politiques de sécurité adéquates pour assurer leur protection. Cela signifie adopter le modèle équilibré de « responsabilité partagée » entre elles et leur prestataire de Cloud afin de protéger à la fois l'infrastructure dans le Cloud et les données qui y résident.

AU-DELÀ DE L'ENTREPRISE

Au fur et à mesure que les entreprises se rapprochent du modèle « BeyondCorp », sur les plates-formes mobiles et SaaS, les contrôles d'accès sont déplacés du périmètre vers les appareils et les utilisateurs individuels. Ceci fournit un niveau d'accès sans précédent aux informations métiers critiques. Fournir à vos collaborateurs un accès aux données sur les appareils mobiles de leur choix comporte de nombreux avantages, mais augmente également le risque d'exposition de votre entreprise.

Des logiciels malveillants « zero-day », des attaques de type homme du milieu sur le réseau wifi, des tentatives de SMiShing et les failles des systèmes d'exploitation, peuvent être utilisés pour dérober des informations confidentielles telles que des emails, des messages textes, des photos, des rendez-vous et des pièces jointes.

94 %

DES ENTREPRISES S'ATTENDENT À CE QUE LE NOMBRE D'ATTAQUES SUR LES APPAREILS MOBILES AUGMENTE [25]

Les entreprises doivent s'assurer que leurs appareils mobiles disposent de technologies avancées de détection et de prévention des menaces de nouvelle génération. Pour se protéger contre les failles des système d'exploitation, elles doivent utiliser des techniques statiques et dynamiques de supervision des changements de configuration, et utiliser un moteur d'analyse capable de détecter les comportements inattendus du système.

La prévention des logiciels malveillants inclus dans de fausses applications nécessite le déploiement d'une solution capturant les applications téléchargées, et analysant leur comportement dans un environnement de sandboxing virtuel. La solution devrait être en mesure d'agréger et corréler les informations sur la source et la réputation des serveurs de l'application, et désassembler son code source pour analyser les flux d'instructions.

Seules les solutions comprenant un moteur d'analyse comportementale capable de détecter les points d'accès indésirables et les comportements réseau malveillants pourront désactiver automatiquement les réseaux suspects. Les technologies correctives sur les appareils seront également en mesure de déclencher dynamiquement un VPN sécurisé pour protéger l'intégrité et la confidentialité de vos communications.

Une sécurité mobile et SaaS complète devrait être constituée de composants qui travaillent ensemble de manière cohérente. Seules les solutions capables d'analyser les comportements sur l'ensemble des vecteurs, à la recherche d'indicateurs d'attaque, peuvent efficacement assurer la sécurité des appareils mobiles.

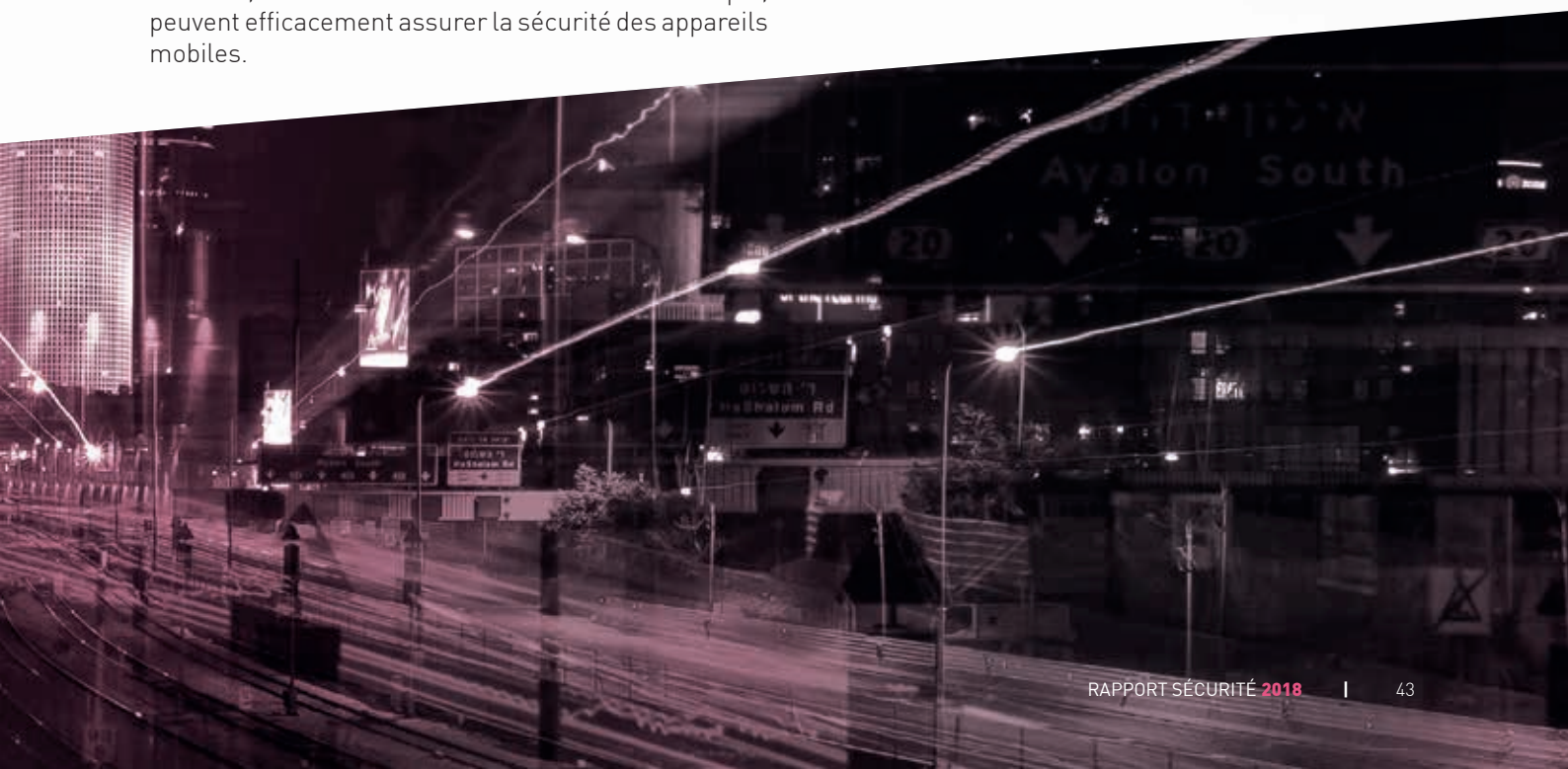
PAS DE MAILLON FAIBLE

L'augmentation rapide du nombre de logiciels malveillants, la sophistication croissante des agresseurs et la progression des nouvelles menaces zero-day inconnues, nécessitent une approche différente des pare-feux traditionnels pour continuer de protéger les réseaux et les données d'entreprise.

La sécurité réseau de 5e génération doit inclure une approche unifiée comprenant des fonctions de sécurité telles que le pare-feu, la prévention des intrusions, l'antibots, l'antivirus, le contrôle des applications et le filtrage des URL, pour lutter contre les cyberattaques connues et inconnues.

Conjuguées aux techniques avancées d'émulation et d'extraction des menaces au niveau des couches OSI supérieures, les technologies de « Gén. V » vont plus loin et approfondissent l'inspection des logiciels malveillants au niveau du processeur, ainsi qu'au niveau du système d'exploitation, pour identifier les exploitations de vulnérabilités. Les techniques de sandboxing innovantes doivent inclure des technologies de détection et de blocage rapides et précises, une résistance aux tentatives d'évasion et des inspections approfondies du plus grand ensemble de fichiers, y compris les fichiers non-exécutables.

En combinant étroitement plusieurs technologies d'extraction des menaces au sein d'une même appliance, la solution de sandbox réseau doit également pouvoir exécuter les technologies de préventions à différents moments, se basant sur des signatures et des analyses dynamiques tout en travaillant rapidement pour contrôler l'accès au réseau.



CONCLUSION

Au cours des 25 dernières années, les attaques ainsi que les protections de sécurité ont rapidement progressé. Les cyberattaques ont progressivement évolué à l'aide des toutes dernières innovations, à des fins de cybercriminalité. Cependant, la plupart des entreprises n'ont pas évolué et utilisent toujours des technologies de cybersécurité de seconde ou de troisième génération. Cela crée un énorme désavantage puisque nous sommes entrés dans la cinquième génération des cyberattaques.

Les cyberattaques de cinquième génération, telles que les méga-attaques de 2017, sont définies comme étant des attaques rapides à grande échelle. Ces attaques sophistiquées contournent facilement les défenses classiques reposant sur la détection statique utilisées par la plupart des entreprises aujourd'hui.

97 %

DES ENTREPRISES UTILISENT DES TECHNOLOGIES DE CYBERSÉCURITÉ DÉPASSÉES [26]

Pour lutter contre ces attaques modernes, les entreprises doivent déployer une cybersécurité de cinquième génération qui utilise une prévention avancée des menaces en temps réel pour protéger les réseaux, les activités virtuelles, le Cloud, les bureaux distants et les appareils mobiles d'une entreprise.

Malheureusement, les attaques d'aujourd'hui sont les plus avancées et les plus percutantes que nous ayons jamais vues, et pourtant la sécurité déployée par la plupart des entreprises est dépassée et incapable d'offrir une protection contre ces attaques. Nos études montrent que la plupart des entreprises n'utilise aujourd'hui que des protections de seconde ou de troisième génération, et que seulement 3 % utilisent des outils et des techniques de cinquième génération.

Afin d'assurer une meilleure protection contre les attaques avancées décrites dans ce rapport, les entreprises doivent passer aux solutions de sécurité de « Gén. V » pour se protéger contre la cinquième génération des cyberattaques.

RÉFÉRENCES

1. Source : Check Point C-Level Perspective Survey, avril 2017, échantillon : 59 directeurs.
2. Source : Check Point C-Level Perspective Survey, avril 2017, échantillon : 59 directeurs.
3. Source : Bloomberg, juin 2017, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections
4. Source : Check Point C-Level Perspective Survey, avril 2017, échantillon : 59 directeurs.
5. Source : UK National Audit Office, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
6. Source : Check Point C-Level Perspective Survey, avril 2017, échantillon : 59 directeurs.
7. Source : Check Point Mobile Threat Research Publications, https://research.checkpoint.com/check-point-mobile-research-team-looks-back-2017/
8. Source : Check Point Mobile Threat Research Report, novembre 2017, échantillon : 850 entreprises.
9. Source : The State of Security Efficiency Survey, février 2018, échantillon : 452 participants.
10. Source : Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
11. Source : Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
12. Source : Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
13. Source : Check Point Research Survey of IT Security Professionals, mars 2018, échantillon : 443 participants.
14. Source : Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
15. Source : Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
16. Source : KPMG Consumer Loss Barometer Survey, août 2017, https://home.kpmg.com/cn/en/home/insights/2016/08/consumer-loss-barometer.html
17. Source : KPMG Consumer Loss Barometer Survey, août 2017, https://home.kpmg.com/cn/en/home/insights/2016/08/consumer-loss-barometer.html
18. Source : Check Point Meta-Analysis by Industry Survey, février 2018, échantillon : 450 participants.
19. Source : Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
20. Source : Check Point Meta-Analysis by Industry Survey, février 2018, échantillon : 450 participants.
21. Source : Check Point Survey of IT Security Professionals, décembre 2017, échantillon : 452 participants.
22. Source : Check Point Incident Response Team.
23. Source : Check Point Survey of IT Security Professionals, décembre 2017, échantillon : 452 participants.
24. Source : Check Point Survey of IT Security Professionals, décembre 2017, échantillon : 452 participants.
25. Source : Check Point Dimensional Research Survey into Mobile Device Security, échantillon : 410 participants.
26. Source : Check Point Research Survey of IT Security Professionals, mars 2018, échantillon : 443 participants.

CONTACTEZ-NOUS

SIÈGE MONDIAL

5 Ha'Solelim Street, Tel Aviv 67897, Israël |
Tél. : +972 3 753 4555 | Fax : +972 3 624 1100
Email : info@checkpoint.com

SIÈGE FRANÇAIS

120 avenue Charles de Gaulle, 92200 Neuilly sur Seine, France
Tél. : +33 (0)1 55 49 12 00 | Email : info_fr@checkpoint.com

VOUS ÊTES ATTAQUÉ ?

Contactez notre équipe d'intervention rapide :
emergency-response@checkpoint.com

WWW.CHECKPOINT.COM