Check Point
SOFTWARE TECHNOLOGIES LTD

RAPPORT SUR LA CYBERSÉCURITÉ

2021

cp<r>
CHECK POINT RESEARCH

TABLE DES MATIÈRES

« LA PRÉVISION EST UN ART TRÈS DIFFICILE, SURTOUT LORSQU'ELLE CONCERNE L'AVENIR. »

- Niels Bohr, lauréat du prix Nobel de physique

Nous nous souviendrons tous très longtemps de l'année 2020. Il y a douze mois, très peu d'entre nous auraient pu prévoir le bouleversement mondial que causerait la COVID-19, la pire pandémie depuis plus d'un siècle. Les changements considérables qui ont affecté nos vies presque du jour au lendemain continuent de se faire sentir et perdureront en 2021 et après.

La distanciation sociale étant essentielle pour ralentir la propagation du coronavirus, nous avons dû transformer tous les aspects de notre mode de vie, du travail aux achats en passant par les relations avec nos familles et nos proches. Internet nous a permis de continuer à faire avancer le monde. La majorité des entreprises ont été surprises de la rapidité et du succès de leurs initiatives numériques : nous avons estimé qu'en 2020, la transformation numérique s'est accélérée et a pris une avance de sept ans. Ce qui semblait autrefois presque impossible a été réalisé en seulement quelques mois.

Évidemment, cette avancée majeure en matière de connectivité et notre dépendance croissante à la technologie dans notre vie quotidienne ont engendré de nouveaux défis et problèmes. De même que les organisations du monde entier ont transformé leurs méthodes de travail, les acteurs de la menace et les cybercriminels ont également changé leurs tactiques afin de pouvoir tirer parti de la perturbation liée à la pandémie.

Nous avons constaté d'importantes augmentations des attaques contre les nouvelles capacités de travail à distance des organisations. Nous avons assisté à des hausses d'attaques de phishing ciblant les télétravailleurs et les consommateurs afin de voler leurs données personnelles. Nous avons observé d'importantes augmentations des exploitations de vulnérabilité par des ransomwares ainsi que des tentatives de piratage sophistiquées ciblant les hôpitaux, les organisations de santé et les entreprises contribuant à la fabrication et l'expédition des vaccins essentiels à la lutte contre la COVID-19.

En décembre, nous avons vu d'importantes attaques de type Sunburst qui ciblaient des milliers d'organisations gouvernementales et privées spécialisées dans la technologie du monde entier via une porte dérobée intégrée dans leur logiciel de gestion de réseau SolarWinds. Check Point avait prédit pour la première fois il y a deux ans ces types d'attaques de génération V à grande échelle, à vecteurs multiples et à évolution rapide, et elles frappent les organisations du monde entier plus fréquemment que jamais auparavant. Toutes ces attaques et menaces augmentent encore aujourd'hui. Cette cyber pandémie croissante pourrait détruire la nouvelle normalité que nous avons façonnée au cours de l'année passée.

La COVID-19 a certes été à l'origine de sombres jours dans le monde, mais il y a de fortes chances que nous sortions bientôt de cette crise. La plus grande campagne de vaccination au monde est actuellement déployée afin de protéger les populations contre l'infection. Cela permettra ensuite de réduire les restrictions et nous permettra de tirer pleinement parti des fantastiques avancées numériques que nous avons réalisées en 2020.

Mais pour ce faire, nous devons agir maintenant afin d'arrêter la propagation incontrôlée de la cyber pandémie. De la même façon que le déploiement mondial du vaccin permettra aux populations de mettre fin aux confinements en toute sécurité, nous devons également vacciner nos réseaux hyperconnectés afin d'éviter les cyberattaques et les menaces nuisibles qui mettent en péril la sécurité de tous.

Dans ce rapport sur la cybersécurité de 2021, nous allons passer en revue les cybermenaces, attaques et événements importants de 2020 ainsi que leur impact sur les organisations du monde entier. Nous nous pencherons également sur ce que nous attendons du cyberespace en 2021, afin d'aider les organisations à se préparer pour la suite et de montrer comment elles peuvent mettre en place la meilleure posture de sécurité possible. En empêchant les cyberattaques majeures, la sécurité est un catalyseur qui libère l'innovation et aide à protéger l'avenir, pour le bien de tous.

Dr Dorit Dor

Vice-présidente des produits
Check Point Software Technologies

PLUS DE **22 MILLIARDS** DE DOSSIERS ONT ÉTÉ EXPOSÉS À DES FUITES DE DONNÉES DANS LE MONDE EN 2020, POUR 730 FUITES DIVULGUÉES PUBLIQUEMENT

— Rapport rétrospectif de Tenable sur le contexte de la menace de 2020

2 CHRONOLOGIE DES PRINCIPAUX ÉVÉNEMENTS EN LIGNE DE 2020

JAN

01

Les opérations de Travelex, une société de change basée à Londres, ont été paralysées pendant des semaines en raison d'une attaque par ransomware du groupe Sodinokibi (également appelé REvil). Travelex a entamé des négociations avec le groupe, mais a refusé de payer la demande de rançon de 6 millions de dollars en échange des clés de décryptage. En représailles, les attaquants ont menacé de publier 5 Go d'informations personnelles de clients qui avaient été volées et exfiltrées avant le chiffrement. Il s'agissait de l'une des attaques par un ransomware à double extorsion les plus médiatisées, dans laquelle les attaquants pénètrent dans les réseaux d'entreprise, volent des fichiers sensibles, puis chiffrent les données et demandent une rançon pour les décrypter, et menacent de publier des données si la demande de rançon n'est pas satisfaite, pour exercer une pression supplémentaire sur les victimes.

Travelex

FÉV

02

Estée Lauder, le géant des cosmétiques basé à New York, a accidentellement exposé 440 millions documents internes à l'Internet public, y compris des e-mails, rapports et documents internes. Cependant, il n'y avait aucune preuve que les dossiers des clients ou les informations de paiement étaient mis en péril.

ESTĒE LAUDER

MAR

03

Le groupe Marriott Hotels a divulgué une nouvelle fuite de données affectant 5,2 millions de clients de l'hôtel. La chaîne hôtelière a découvert qu'un pirate avait utilisé les identifiants de connexion de deux employés de l'un de ses établissements franchisés pour accéder aux informations des clients à partir des systèmes backend de l'application. La société a informé les clients par e-mail et fourni des services de surveillance des informations personnelles aux personnes affectées par cette fuite de données.

Marriott

SOLARWINDS INDIQUE QUE JUSQU'À **18 000** DE SES CLIENTS DANS LE MONDE ONT ÉTÉ AFFECTÉS PAR LA VIOLATION DE SES SYSTÈMES. LES DONNÉES INDIQUENT QUE LA VIOLATION DES SYSTÈMES A ÉTÉ EFFECTUÉE AU MOINS UN AN AVANT SA DÉCOUVERTE

AVR

04

Alors que les pays du monde entier ont commencé à mettre en œuvre des confinements et des restrictions pour ralentir la propagation de la Covid-19, une enquête de Check Point a montré que 71 % des professionnels de la sécurité ont signalé une augmentation des menaces et des attaques de sécurité depuis le début de l'épidémie de coronavirus. La menace principale citée était les tentatives de phishing (citées par 55 % des personnes interrogées), suivies par les sites Web malveillants prétendant offrir des informations ou des conseils sur la pandémie (32 %), suivis par l'augmentation des malwares (28 %) et des ransomwares (19 %).

Microsoft a averti les utilisateurs de Kubernetes d'une campagne de piratage à grande échelle qui cible Kubeflow, une boîte à outils de machine learning. La campagne vise à infecter les instances de Kubernetes en ligne et à les utiliser pour l'extraction cryptographique aux frais des victimes, en utilisant le logiciel de minage malveillant XMRig.

Microsoft

MAI

05

La compagnie aérienne EasyJet a été piratée, touchant 9 millions de clients et exposant les informations de plus de 2 000 cartes de crédit et de débit. EasyJet a déclaré avoir été la cible d'une attaque « très sophistiquée », qui a permis de consulter et de voler les adresses e-mail et les informations de voyage des clients.

easyJet

JUN

06

L'université de Californie a payé 1 million de dollars de rançon pour déchiffrer les données de recherche sur la COVID-19 après avoir été victime d'un ransomware. L'attaque a eu un impact sur l'école de médecine de l'université, chiffrant les données sur un « nombre limité de serveurs », selon une déclaration de l'UCSF. Bien qu'elle pense qu'aucun dossier de patient n'a été exposé par l'attaque du ransomware Netwalker, l'université a ajouté : « Nous avons pris la décision difficile de payer une partie de la rançon, environ 1,14 million de dollars, aux individus derrière l'attaque du malware en échange d'un outil pour déverrouiller les données chiffrées et le retour des données qu'ils avaient obtenues ».

UCSF

JUL

07

Microsoft a corrigé l'exploitation de vulnérabilité SIGRed vieille de 17 ans qui pouvait être utilisée pour pirater des serveurs Microsoft Windows. La vulnérabilité, découverte par Check Point Research (CPR) et corrigée dans le cycle régulier Patch Tuesday de Microsoft, a obtenu le niveau de gravité le plus élevé de 10,0. La vulnérabilité est d'une grande importance pour les entreprises, car elle peut se propager d'elle-même. Elle est ainsi capable de passer à travers des machines vulnérables sans aucune interaction avec l'utilisateur, ce qui peut potentiellement compromettre l'ensemble du réseau d'ordinateurs d'une organisation, la rendant aussi importante que la vulnérabilité EternalBlue de 2017, qui a conduit aux cyberattaques mondiales de WannaCry et NotPetya.

SIGRed

AOU

08

Les opérateurs du ransomware Maze ont publié des dizaines de gigaoctets de données internes provenant des réseaux des géants de l'industrie LG et Xerox suite à deux tentatives d'extorsion infructueuses. Les pirates ont divulgué 50,2 Go de données qu'ils affirment avoir volées sur les réseaux internes de LG, et 25,8 Go de données de Xerox. Cet exemple souligne la menace très réelle posée par les ransomwares à double extorsion.

LG

xerox

SEP

09

Un patient d'un hôpital en Allemagne est décédé après avoir été redirigé d'un hôpital qui avait été touché par une attaque par un ransomware. Le patient, qui avait besoin de soins médicaux d'urgence, est décédé après avoir été redirigé vers un hôpital de la ville de Wuppertal, à plus de 30 km de sa destination initiale, l'hôpital universitaire de Düsseldorf, qui avait été frappé par l'attaque. L'Agence fédérale allemande pour la sécurité des technologies de l'information a déclaré que les pirates ont attaqué l'hôpital en exploitant une vulnérabilité dans le logiciel Citrix qui n'avait pas fait l'objet de correctifs, alors que le correctif était disponible depuis plusieurs mois.

CITRIX

OCT

10

Le prestataire de soins de santé UHS (Universal Health Services), comptant plus de 400 établissements aux États-Unis, au Royaume-Uni et à Porto Rico, a été touché par le ransomware Ryuk. L'attaque a paralysé l'ensemble de son infrastructure informatique et de son système téléphonique aux États-Unis, entraînant une transition vers des systèmes entièrement papier.

Une base de données d'électeurs à Hall Country, dans l'état de Géorgie, utilisée pour vérifier les signatures des électeurs, a été piratée par un ransomware, ainsi que d'autres systèmes gouvernementaux, ce qui en fait peut-être la première ressource électorale officielle à être touchée par un ransomware. Le groupe « DoppelPaymer » a revendiqué cette attaque.

NOV

11

La CISA (Cybersecurity and Infrastructure Security Agency), le FBI (Federal Bureau of Investigation) et le département américain de la Santé et des Services sociaux (HHS) ont publié une mise en garde contre une augmentation des attaques du ransomware Ryuk sur les hôpitaux américains. Check Point Research a montré que le secteur de la santé était le plus ciblé aux États-Unis, avec une augmentation de 71 % des attaques en novembre par rapport au mois précédent. Les attaques ont de nouveau augmenté en décembre 2020.

DÉC

12

La semaine du 13 décembre, les bureaux du gouvernement américain ont révélé qu'ils avaient été visés par une série de cyberattaques de grande ampleur, prétendument liées à des organisations de la menace financées des gouvernements. Les attaques ciblaient de nombreuses organisations technologiques gouvernementales et du secteur privé dans le monde entier. Cette série d'attaques, baptisée « Sunburst », a été rendue possible lorsque les pirates ont pu intégrer une porte dérobée dans le logiciel de gestion de réseau SolarWinds. Plus de 18 000 entreprises et bureaux gouvernementaux ont téléchargé ce qui semblait être une mise à jour logicielle ordinaire sur leurs ordinateurs, alors qu'il s'agissait d'un cheval de Troie. En exploitant les pratiques informatiques courantes des mises à jour logicielles pour intégrer des malwares aux réseaux des organisations, les attaquants ont utilisé la porte dérobée pour compromettre les ressources des victimes, à la fois sur le cloud et sur site, leur permettant d'espionner le trafic du réseau et d'accéder à ses données.

SUNBURST

CHAQUE JOUR, LE MONDE DOIT FAIRE FACE À PLUS DE **100 000** SITES MALVEILLANTS ET **10 000** FICHIERS MALVEILLANTS, TOUS CHERCHANT À VOLER, À ENTRAÎNER DES PERTURBATIONS OU À CAUSER DES DOMMAGES

87 % DES ORGANISATIONS ONT CONNU DES TENTATIVES D'EXPLOITATION D'UNE VULNÉRABILITÉ EXISTANTE ET DÉJÀ CONNUE

DES ENVIRONNEMENTS SUR SITE AUX ENVIRONNEMENTS CLOUD : L'ATTAQUE SUR LA CHAÎNE D'APPROVISIONNEMENT DE SOLARWINDS

En décembre 2020, juste au moment où nous pensions que l'année ne pouvait plus empirer davantage, l'attaque de SolarWinds a été découverte et a rapidement remporté le titre de cyber-attaque la plus importante de l'année. Le premier signe de l'attaque a été sa divulgation, le 8 décembre par la société de cybersécurité FireEye, qui a rendu public le fait qu'un groupe APT (Advanced Persistent Threat) hautement compétent avait ouvert une brèche, au cours de laquelle les outils d'évaluation en ligne de la FireEye Red Team ont été volés.

L'ampleur de cette attaque a été révélée quelques jours plus tard, lorsque Microsoft, FireEye, SolarWinds et le gouvernement américain ont admis avoir subi une attaque rendue possible à cause du piratage du logiciel de gestion informatique de base de SolarWinds. Une enquête plus approfondie a révélé que les attaquants ont ajouté une porte dérobée, appelée « Sunburst », à un composant du système SolarWinds Orion, qui s'est ensuite propagée aux clients SolarWinds via une mise à jour logicielle automatique. Cela a permis un accès à distance à plusieurs organisations de premier plan, ce qui en fait l'une des attaques de chaîne d'approvisionnement les plus réussies jamais observées.

46 % DES ORGANISATIONS ONT VU AU MOINS UN EMPLOYÉ TÉLÉCHARGER UNE APPLICATION MOBILE MALVEILLANTE QUI MENACE LEURS RÉSEAUX ET LEURS DONNÉES.

AVI REMBAUM
Vice-président,
Solutions
de sécurité

« Les attaques de chaîne d'approvisionnement, comme celles impliquant SolarWinds, montrent l'impact potentiel de vecteurs de menace inconnus auparavant. Les pratiques de sécurité de base, telles que le principe du moindre privilège et la segmentation, restent essentielles pour limiter la probabilité de violation initiale ainsi que le potentiel d'expansion latérale.

La caractère inédit de l'incident récent nous informe également de la nécessité d'envisager de nouvelles approches en matière de cybersécurité. Les développeurs d'applications doivent envisager des moyens d'adopter les méthodologies DevSecOps et d'intégrer des contrôles de sécurité dans le code ainsi que le cycle de vie du développement logiciel. Les professionnels de la sécurité doivent explorer les possibilités de mise en œuvre de protections automatisées en temps réel pour les exploitations de vulnérabilité identifiées, et étendre les capacités de détection et de prévention des menaces à tous les environnements : réseau, postes, cloud et mobile. »

L'ampleur de l'attaque est énorme : les documents fournis par SolarWinds à la SEC (Securities and Exchange Commission) américaine révèlent qu'environ 18 000 clients ont téléchargé la mise à jour compromise du logiciel Orion, parmi lesquels 425 entreprises figurant sur la liste du Fortune 500. Évidemment, les clients qui ont reçu la mise à jour compromise ne sont pas tous devenus des cibles actives. Les attaquants n'ont choisi que les entités de grande valeur dont le réseau et les données étaient compromis. Il semble que les acteurs de la menace se soient principalement concentrés sur les entreprises technologiques, les agences gouvernementales et les sociétés de conseil aux États-Unis, en Europe, en Asie et au Moyen-Orient. La liste des victimes comprend les départements américains de l'État, de l'Énergie (DOE) et de la Sécurité intérieure (DHS), les Instituts nationaux de la santé (NIH), Cisco et Microsoft, parmi beaucoup d'autres.

Les acteurs de l'attaque, supposés être d'origine russe et avoir des liens avec les services de renseignement russes, ont fait preuve de capacités remarquables. Nous ne savons certes pas exactement comment SolarWinds a été infecté en premier lieu, mais nous soupçonnons que la sécurité de l'entreprise a été violée via ses comptes Office 365. Les attaquants ont réussi à contrefaire un jeton d'authentification d'un compte hautement privilégié d'Azure Active Directory et à obtenir des privilèges d'administration grâce aux identifiants compromis. En quelques mots, l'attaquant a obtenu un accès important au réseau sur site des clients SolarWinds via la mise à jour compromise, puis s'est déplacé de manière latérale vers l'environnement cloud afin de faciliter un accès sur le long terme à la victime et de récupérer des informations telles que des fichiers de messagerie volés via Microsoft Office 365.

« Les attaques de vishing représentent une cybermenace croissante. Elles donnent à l'attaquant le contrôle du canal d'information et exercent une pression psychologique supplémentaire sur la cible. Pour cette raison, nous constatons que de plus en plus de cyberattaques multi-étapes intègrent des appels de vishing dans leurs chaînes d'infection. Les organisations doivent sensibiliser leurs employés à ne pas communiquer de manière inappropriée des informations sensibles telles que les identifiants ou les coordonnées bancaires, et à vérifier l'authenticité de la personne avec qui ils se trouvent au téléphone. »

LOTEM FINKELSTEEN
Responsable du renseignement sur les menaces

Une innovation clé de cette attaque est la façon dont les attaquants ont obtenu l'accès aux services basés sur le cloud. Il semble que les services basés sur le cloud aient été un objectif majeur dans cette attaque de la chaîne d'approvisionnement, et l'accès à ceux-ci a été obtenu via des systèmes d'authentification sur les réseaux compromis, ce qui leur a permis de pénétrer ces services sans éveiller de soupçons. Ce vecteur d'attaque est parfaitement adapté aux environnements cloud hybrides sur site, courants de nos jours.

Les organisations souhaitant se défendre de l'attaque doivent examiner à la fois leur réseau sur site et leurs services basés sur le cloud et prendre les mesures nécessaires pour protéger leur infrastructure d'authentification et établir des procédures de surveillance pour détecter de telles attaques.

LE VISHING, LA NOUVELLE MÉTHODE À L'ANCIENNE

En 2020, nous avons assisté au retour malheureux d'une ancienne méthode d'ingénierie sociale sous une nouvelle forme, un concept bien adapté à l'aménagement dynamique du travail dans la situation actuelle. L'hameçonnage par téléphone, ou vishing, est une tentative d'accès à des informations ou systèmes privés ou d'entreprise par le biais d'appels vocaux frauduleux. Pendant l'appel téléphonique, l'attaquant utilise des techniques d'ingénierie sociale afin d'inciter la victime à ouvrir un document malveillant, partager des informations sensibles ou donner à l'appelant l'accès à des appareils privés.

En 2020, l'augmentation des attaques réussies

MAYA HOROWITZ
Directrice, Renseignement et recherche sur les menaces

« Les attaques par des ransomwares ont de nouveau augmenté en 2020, la technique de double extorsion exerçant une pression accrue sur les organisations pour répondre aux demandes des pirates informatiques. On estime que les ransomwares ont coûté aux entreprises 20 milliards de dollars à l'échelle mondiale en 2020, contre 11,5 milliards de dollars en 2019. Pour éviter d'être victime d'un ransomware, les organisations doivent adopter une stratégie de prévention des menaces et ne pas s'appuyer uniquement sur la détection ou les mesures correctives. Celles-ci doivent déployer des solutions dédiées "antiransomware", appliquer virtuellement des correctifs sur les vulnérabilités telles que le RDP et informer les employés des risques relatifs aux e-mails malveillants qui peuvent représenter un danger. »

ayant recours au phishing par téléphone a révélé que ces attaques ne se limitaient plus à de simples escroqueries de support technique qui sont facilement détectables par des personnes sensibilisées aux cybermenaces. Les attaques de ce type peuvent être sophistiquées, adaptées à la victime et à son travail. Avec quelques recherches et un appelant possédant de bonnes compétences linguistiques, le vishing peut être utilisé pour obtenir l'accès à un réseau d'entreprise.

Un article récent a révélé qu'un groupe de cybercriminels professionnels proposait leurs services pour donner accès à des entreprises spécifiques grâce au vishing. Ces attaques ciblent les employés qui travaillent à domicile en cherchant à obtenir leurs identifiants VPN afin d'accéder au réseau de l'entreprise. Les appels téléphoniques personnalisés donnent de la crédibilité au criminel, celui-ci se faisant passer pour un employé du service d'assistance et démontrant sa connaissance de l'entreprise et du poste de l'employé. En août 2020, la CISA (Cybersecurity and Infrastructure Security Agency) et le FBI ont publié un bulletin d'alerte commun concernant une vague d'attaques de type vishing ciblant les entreprises du secteur privé américain, incitant les employés à fournir leurs identifiants d'entreprise.

Tandis que des attaquants indépendants ou des petits groupes de cybercriminels peuvent être à l'origine de telles attaques, nous avons récemment constaté que des groupes APT intégraient le vishing à leur arsenal. Selon les rapports, des entités comme le groupe iranien Charming Kitten et le groupe nord-coréen Lazarus utilisent le vishing dans le cadre de stratagèmes de phishing complexes. Des groupes de cybercriminalité sophistiqués, tels

que Evilnum, motivés par l'appât du gain, ont également adopté le vishing comme tactique plus efficace et contrôlée pour assurer le succès de la phase de phishing.

Le vishing peut également être utilisé pour contourner le mécanisme de sécurité d'authentification à deux fauteurs (2FA). Dans certains cas, les attaquants ont utilisé le téléphone de la victime pour l'authentification afin d'accéder à un compte privé.
Ils ont ensuite demandé le code 2FA de l'utilisateur lors d'un appel téléphonique, prétendant être un représentant du support technique. Le code donnait à l'attaquant un accès total au compte. Cette technique a récemment été utilisée dans une campagne de piratage de comptes WhatsApp afin d'utiliser le compte de la victime pour cibler tous ses contacts.

Un exemple éloquent est l'attaque sur Twitter en juillet 2020, lors de laquelle les pirates ont obtenu l'accès à des dizaines de comptes Twitter très en vue, dont ceux de Joe Biden et de Jeff Bezos, et ont tweeté des demandes de rançon en bitcoin qui ont rapporté plus de 100 000 dollars en quelques heures. Il a été découvert plus tard que l'attaque avait débuté par un vishing, ce qui avait incité les employés de Twitter à donner l'accès à des outils internes. En novembre, une attaque similaire a frappé GoDaddy, le plus grand registraire de nom de domaine au monde.

Ces attaques donnent une idée de la nature de la vague actuelle d'attaques de phishing : sophistiquées, bien planifiées et ciblant des utilisateurs spécifiques dans des organisations de premier plan. Un travail de reconnaissance approfondi est probablement effectué en amont pour choisir les employés les plus susceptibles de coopérer, recueillir des données personnelles les concernant et obtenir leurs numéros de téléphone. Nous pouvons bientôt nous attendre à ce que les attaques de vishing intègrent des techniques de « deep phishing » telles que le deepfake, qui permet au pirate de choisir la voix utilisée lors de l'appel et d'imiter toute personne d'intérêt, ou même le visage utilisé dans une vidéoconférence. Imaginez-vous recevoir un appel qui semble provenir du PDG de votre entreprise qui vous relance sur un accord commercial et qui vous demande même d'effectuer une transaction.

LES RANSOMWARES À DOUBLE EXTORSION SE MULTIPLIENT

Alors que les ransomwares conventionnels continuent de déstabiliser les organisations du monde entier, les acteurs de la menace ont inventé une nouvelle tactique fin 2019 : la double extorsion. Il s'agit d'une attaque par un ransomware à plusieurs étapes qui associe le chiffrement traditionnel des fichiers de la victime avec une exfiltration des données. L'attaquant menace alors de divulguer publiquement les données volées à moins de recevoir une rançon dans un certain délai. Cela fait office de pression supplémentaire sur les victimes qui doivent répondre aux demandes de l'attaquant, tout en exposant la victime à des sanctions imposées par l'entité de surveillance de données, ainsi qu'à la nécessité d'alerter les clients, partenaires et consommateurs concernés dont les données ont été piratées.

DES RECHERCHES MONTRENT QU'AU **TROISIÈME TRIMESTRE 2020**, PRÈS DE LA MOITIÉ DES SCÉNARIOS DE RANSOMWARE COMPRENAIENT LA MENACE DE DIVULGUER LES DONNÉES VOLÉES, ET LE PAIEMENT MOYEN DE RANÇON ÉTAIT DE **233 817 DOLLARS, SOIT UNE AUGMENTATION DE 30 %** PAR RAPPORT AU **DEUXIÈME TRIMESTRE 2020.**

En 2020, les attaques à double extorsion ont augmenté. Le géant des centres de données Equinix a été victime du ransomware Netwalker. L'auteur de cette attaque était également responsable de l'attaque contre K-Electric, le plus grand fournisseur d'électricité au Pakistan, demandant 4,5 millions de dollars en bitcoin pour les clés de décryptage et empêcher la divulgation des données piratées. Le modèle commercial des attaques à double extorsion s'est avéré si efficace que les techniques traditionnelles des ransomwares ne sont rien à côté.

Parmi les autres entreprises connues pour avoir subi de telles attaques, citons la société française de conseil en systèmes et logiciels Sopra Steria, qui compte d'importants clients du secteur de la finance et de la santé ; le développeur de jeux japonais Capcom ; l'entreprise italienne de spiritueux Campari Group ; le fournisseur de missiles militaires américain Westech ; le groupe mondial d'ingénierie aérospatiale et électronique ST Engineering ; le géant de la gestion des voyages CWT, qui a payé aux opérateurs du ransomware Ragnar Locker 4,5 millions de dollars en bitcoin ; et le géant des services aux entreprises Conduent, qui a été attaqué par le ransomware Maze, sans doute via un serveur Citrix vulnérable.

Et ce n'est que la valeur moyenne d'une rançon. Lors d'une attaque récente utilisant le ransomware Ryuk, la victime a payé la coûteuse rançon de 34 millions USD, soit 2 200 bitcoins. Et évidemment, même si vous vous pliez aux demandes de rançon, vous n'avez quand même aucune garantie que les attaquants honoreront leur promesse de libérer les fichiers.

Les attaquants affinent également les techniques de double extorsion pour accentuer la pression sur les entreprises qui ne veulent pas payer. Le groupe de ransomwares Ragnar Locker, par exemple, utilise des comptes piratés pour lancer des campagnes publicitaires sur Facebook, déclarant que de nombreuses données client sensibles ont en effet été collectées, réfutant les déclarations souvent publiées par les entreprises ciblées.

Avec le temps, certains attaquants se sont rendu compte que la menace de fuite des données pourrait être encore plus grande que l'étape de la demande de rançon et ont donc tout simplement sauté cette étape, comme ce fut le cas avec Vastaamo, une clinique de psychothérapie finlandaise comptant plus de 40 000 patients. Pendant plus d'un an, les pirates ont réussi à recueillir des informations appartenant à des dizaines de milliers de patients. Contre toute attente, les pirates ont envoyé un e-mail directement à la clinique et aux patients, menaçant de divulguer les données. Environ 530 000 USD en bitcoin ont été demandés au prestataire de soins de santé tandis qu'une somme entre 200 et 500 USD en Bitcoin a été demandée aux patients pour empêcher la publication des notes de session de leur thérapeute. Les dossiers médicaux de 300 patients ont été publiés pour accélérer le paiement. Impliquer les clients dans le processus d'extorsion garantit une divulgation rapide de l'incident au grand public, ce qui exerce une pression supplémentaire sur l'organisation victime, l'obligeant à suivre les réglementations et à alerter les organismes d'application de la loi ainsi que le personnel affecté.

« HELLCARE » : LES ATTAQUES SUR LE SECTEUR DE LA SANTÉ SONT-ELLES ALLÉES TROP LOIN ?

En mars 2020, lorsque l'ampleur et la gravité de la pandémie mondiale de COVID-19 sont devenues évidentes, plusieurs groupes de cybercriminels, dont Maze et DoppelPaymer, se sont engagés à ne pas attaquer les établissements de santé, qui avaient des difficultés à faire face à la charge de travail croissante, à effectuer des recherches sur le virus et à traiter le nombre accablant de patients. Certains groupes sont même allés jusqu'à promettre de fournir des services de décryptage gratuits aux institutions attaquées par erreur. Parmi ces groupes figurait le célèbre groupe de ransomwares Maze, qui s'est engagé à respecter la déclaration suivante : *« Nous arrêtons également toute activité contre toutes sortes d'organisations médicales jusqu'à la stabilisation de la situation liée au virus. »*

Au cours de l'année 2020, il est devenu de plus en plus évident que de telles promesses étaient mensongères. En réalité, en 2020, les attaques ciblant les établissements de santé, les institutions médicales et les centres de recherche pharmaceutique se sont intensifiées à un rythme sans précédent. Début avril, Hammersmith Medicines Research Ltd. (HMR), un centre de recherche qui attendait à l'époque d'effectuer des tests sur les vaccins pour la COVID-19 chez l'homme, a été victime d'une fuite de données causée par le ransomware Maze. L'enquête a révélé que la fuite s'est produite le 14 mars, presque en même temps que la promesse du groupe Maze. Comme HMR a décidé de ne pas payer la rançon, les données ont été publiées sur le site de Maze.

Peu de temps après, nous avons observé une augmentation des attaques sur le secteur de la santé, car les attaquants ont commencé à se concentrer sur les établissements médicaux cherchant à ralentir la propagation du coronavirus ainsi que sur les institutions

CYBERATTAQUES MENSUELLES PAR ORGANISATION DE SOINS DE SANTÉ, JANVIER 2020 À JANVIER 2021

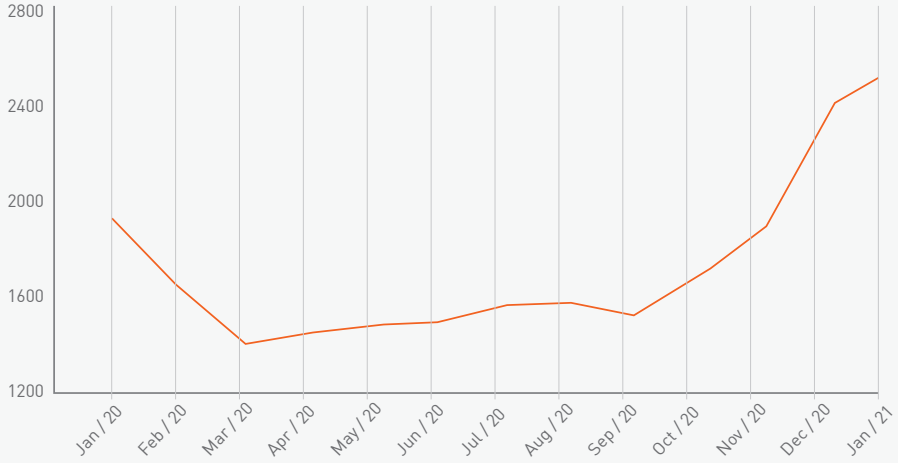


Figure 1 : en mars 2020, les groupes de ransomwares se sont engagés à éviter d'attaquer les établissements de santé. En réalité, les attaques sur ces établissements ont fortement augmenté vers la fin de l'année.

pharmaceutiques travaillant sur le développement d'un vaccin. Ces attaques se sont poursuivies tout au long de l'année 2020.

Une étude récente de Check Point Research en octobre montre que les services de santé sont actuellement l'industrie la plus ciblée aux États-Unis, avec une augmentation de 71 % des attaques par rapport à septembre. Le graphique ci-dessus montre l'augmentation radicale des attaques sur le secteur de la santé par rapport à l'augmentation mondiale. En novembre et décembre 2020, une augmentation de plus de 45 % des attaques ciblant les organisations de services de santé à l'échelle mondiale a été constatée, soit le double de l'augmentation mondiale des attaques observées au cours de la même période dans tous les secteurs d'activité (22 %). Ce graphique montre l'augmentation du taux d'attaque par organisation de services de santé tout au long de l'année 2020 et au début de l'année 2021.

Vers la fin du mois d'octobre, le CISA, le FBI et le département de la Santé et des Services sociaux des États-Unis (HHS) ont publié une alerte concernant une augmentation des attaques du ransomware Ryuk sur les hôpitaux américains en mentionnant le malware polyvalent Trickbot, utilisé pour déployer Ryuk dans le réseau de la victime.

Nous avons également observé des groupes APT soutenus par leurs pays, dont le groupe nord-coréen Lazarus et le groupe russe Fancy Bear, ciblant les institutions impliquées dans le développement de traitements et de vaccins contre la COVID-19. Le phishing ciblé basé sur des thèmes liés à la pandémie est la tactique utilisée la plus courante. Il semble que les pirates et les groupes liés aux États, cherchant

« Les cyberattaques contre le secteur mondial de la santé échappent à tout contrôle, car les criminels considèrent que les hôpitaux sont plus disposés à répondre à leurs demandes et à payer des rançons. Les événements de 2020 le prouvent. L'utilisation de Ryuk met l'accent sur la tendance des attaques par ransomware plus ciblées et personnalisées, plutôt que d'utiliser une campagne de spam massive, ce qui permet aux attaquants de s'assurer qu'ils touchent les parties les plus critiques de l'organisation et ont une plus grande chance de faire payer la rançon. »

OMER DEMBINSKY
Responsable de la recherche sur les données

à promouvoir leurs intérêts nationaux et à avoir un impact mondial, aient décidé de se concentrer sur les institutions promouvant la lutte mondiale contre la pandémie, mettant ainsi les citoyens des pays en première ligne de leurs attaques.

LE DÉTOURNEMENT DE FILS DE DISCUSSIONS E-MAIL : VOS PROPRES E-MAILS POURRAIENT ÊTRE UTILISÉS CONTRE VOUS

Aujourd'hui, l'un des éléments clés d'une bonne sécurité est la formation de sensibilisation à la cybersécurité pour les employés d'une entreprise. Elle doit inclure une liste complète de choses à faire et à ne pas faire dans un environnement professionnel. Une règle d'or courante consiste à faire attention aux pièces jointes d'e-mails qui n'ont pas été envoyés par vos collègues ou partenaires de confiance. Mais que se passe-t-il lorsque vous recevez une réponse à un ancien fil de discussion d'entreprise avec un nouveau fichier joint ? L'ouvrez-vous sans vous poser de question ou devriez-vous vous méfier ?

Emotet, à l'origine un malware pour le secteur bancaire et aujourd'hui l'un des plus grands botnets du cyberespace, a systématiquement atteint le premier rang aux classements des malwares de Check Point Research pendant plusieurs mois, après avoir ciblé près de 20 % des organisations mondiales au cours de l'année dernière.

L'une des raisons clés du succès stupéfiant des campagnes de spam d'Emotet est une technique de phishing simple mais sophistiquée appelée le détournement de

EMOTET, À L'ORIGINE UN MALWARE POUR LE SECTEUR BANCAIRE ET AUJOURD'HUI L'UN DES PLUS GRANDS BOTNETS DU CYBERESPACE, A SYSTÉMATIQUEMENT ATTEINT LE PREMIER RANG AUX CLASSEMENTS DES MALWARES DE CHECK POINT RESEARCH PENDANT PLUSIEURS MOIS, APRÈS AVOIR CIBLÉ PRÈS DE **20 %** DES ORGANISATIONS MONDIALES AU COURS DE L'ANNÉE DERNIÈRE

fils de discussion. Une fois qu'une victime est infectée, les attaquants exploitent les anciennes conversations par e-mail de cette personne pour distribuer des malwares, en transférant le dernier e-mail du fil de discussion et en ajoutant des fichiers malveillants en pièces jointes. Il est ainsi plus facile de piéger de nouvelles victimes qui sont dans l'entourage social et professionnel de la victime puisque de leur point de vue, elles reçoivent un e-mail d'un collègue de confiance concernant un sujet connu.

En ce qui concerne Emotet, les fils de discussion par e-mails, souvent choisis pour leur lien avec un virement bancaire ou des renseignements exclusifs sensibles, sont détournés par les attaquants et envoyés à leurs serveurs C&C. Les attaquants se font ensuite passer pour l'une des adresses e-mail utilisées dans le fil de discussion et inventent une réponse à l'e-mail détourné. Les utilisateurs ciblés peuvent faire partie de la conversation initiale, mais aussi être de nouveaux utilisateurs au sein de l'organisation. Parfois, des fichiers légitimes volés du réseau sont joints à l'e-mail de phishing en plus du fichier malveillant. La technique du détournement de fils de discussion a même été utilisée lors d'une attaque d'Emotet ciblant le ministère de la Justice du Québec et a réussi à infecter des dizaines d'utilisateurs. Cette technique, associée à la grande diffusion d'Emotet, s'est avérée si efficace que le ministère de l'Intérieur français a réagi en interdisant tous les documents Office (.doc) d'être envoyés par e-mail.

Récemment, une autre variante connue d'un malware a ajouté le détournement de fils de discussion à son arsenal : le malware bancaire Qbot, également appelé Qakbot. La nouvelle version du malware, publiée à la fin du mois de juillet et analysée par Check Point Research, comporte un module appelé « collecteur d'e-mails » capable de détourner les fils de discussions de messagerie Microsoft Outlook. Le module extrait toutes les conversations par e-mail du client de la victime, les met en ligne sur un serveur à distance et les utilise dans des campagnes de spam malveillantes. Les e-mails volés observés comprennent des sujets liés à la COVID-19, des rappels de paiement d'impôts et des affaires de recrutement. La campagne Qbot a été distribuée dans le monde entier mais s'est concentrée sur les utilisateurs américains et sur les secteurs gouvernementaux et militaires.

YANIV BALMAS
Responsable de la recherche sur la cybernétique

« Même les anciennes formes de malwares peuvent être mises à jour avec de nouvelles fonctionnalités pour en faire une menace dangereuse et persistante. Les acteurs de la menace derrière Qbot et Emotet investissent massivement dans le développement pour permettre le vol de données à grande échelle par des organisations et des individus. Nous recommandons vivement aux organisations d'éduquer les employés à surveiller attentivement leurs e-mails afin de détecter les signes indiquant une tentative de phishing, même lorsque l'e-mail semble provenir d'une source fiable. Ils doivent également utiliser une solution de sécurité de la messagerie électronique. »

Une mise en pratique créative de la technique de détournement de fils de discussion a également été observée cette année. Check Point Research a récemment constaté un incident durant lequel des pirates avaient réussi à accéder au compte WhatsApp d'un utilisateur et à distribuer des malwares aux contacts de la victime en répondant aux correspondances WhatsApp existantes. Les attaquants ont utilisé le vishing pour obtenir le mot de passe 2FA fourni à la victime par SMS.

Emotet et Qbot sont bien plus que des malwares connus du cyberespace. Leur succès continu les a transformés en lanceurs de tendances. Nous estimons donc que la technique de détournement de fils de discussion sera rapidement adoptée par d'autres acteurs de la menace dans le domaine, des groupes d'espionnage soutenus par leurs pays aux pirates motivés par l'appât du gain.

VULNÉRABILITÉS D'ACCÈS À DISTANCE

Avec la propagation du coronavirus dans le monde, les politiques de distanciation sociale adoptées en raison de la pandémie ont forcé un nombre important d'employés qui travaillaient dans des bureaux d'entreprise à se tourner vers le télétravail. Les administrateurs réseau ont dû s'adapter rapidement aux exigences de travail à distance et mettre en œuvre des plateformes d'accès à distance au sein de leurs organisations. Malheureusement, cela a souvent entraîné des défauts de configuration et des connexions vulnérables, permettant aux attaquants d'exploiter ces failles pour accéder aux informations de l'entreprise.

En conséquence, le premier semestre de 2020 a connu une augmentation des attaques contre les technologies d'accès à distance telles que le RDP (Remote Desktop Protocol) et le VPN,

« Les pirates chercheront toujours des organisations qui ont des systèmes vulnérables et non corrigés afin d'obtenir un accès facile, comme un voleur de voiture à la recherche d'une voiture déverrouillée. Pour éviter de faciliter la tâche aux pirates, nous recommandons vivement aux utilisateurs d'appliquer régulièrement des correctifs aux serveurs afin d'éviter l'exploitation de ces vulnérabilités. IPS empêche les tentatives d'exploitation de vulnérabilités des systèmes ou des applications vulnérables, vous protégeant du risque d'exploitation de la dernière menace, et une protection complète des postes est cruciale pour éviter les failles de sécurité. »

ADI IKAN
Groupe de recherche et de protection du réseau

ainsi qu'une forte hausse des attaques par force brute sur les serveurs RDP. Plusieurs chercheurs ont d'ailleurs découvert qu'au cours du premier semestre de cette année, le RDP était le vecteur d'intrusion le plus répandu, ainsi que la plus grande plateforme de diffusion de ransomwares, surpassant alors les e-mails de phishing. Un autre rapport a conclu que, pendant les premiers mois de la pandémie, près d'un million de tentatives d'attaque contre les connexions RDP ont été observées chaque jour.

Au cours du deuxième semestre, les attaquants ont adopté une approche mieux calculée, visant à s'assurer que, même après que les organisations ont correctement mis en œuvre leurs plateformes d'accès à distance et minimisé les incidents de configuration, les services de connexion à distance peuvent toujours être victimes d'attaques d'entreprise.

Au lieu de chercher des serveurs mal configurés, ils ont commencé à exploiter les vulnérabilités des services d'accès à distance grâce à de nombreuses vulnérabilités récemment révélées dans les appareils de périmètre et d'accès à distance. Cette liste comprend IBM WebSphere Application Server, Oracle WebLogic, Microsoft Remote Desktop Gateway, Citrix NetScaler Gateway, Citrix ADC, Cisco ASA et Firepower, Oracle iPlanet Web Server et d'autres encore.

Cette multitude de nouvelles vulnérabilités est le résultat direct de l'adoption croissante de ces appareils dans le contexte de la « nouvelle normalité » liée à la pandémie de COVID-19 et de l'intérêt accru des chercheurs en sécurité pour les plateformes d'accès à distance.
Les groupes de menaces soutenus par les gouvernements qui mènent des opérations d'espionnage à long terme ont également

AUGMENTATION DES ATTAQUES EXPLOITANT DES VULNÉRABILITÉS DANS LES PRODUITS D'ACCÈS À DISTANCE 2019-2020

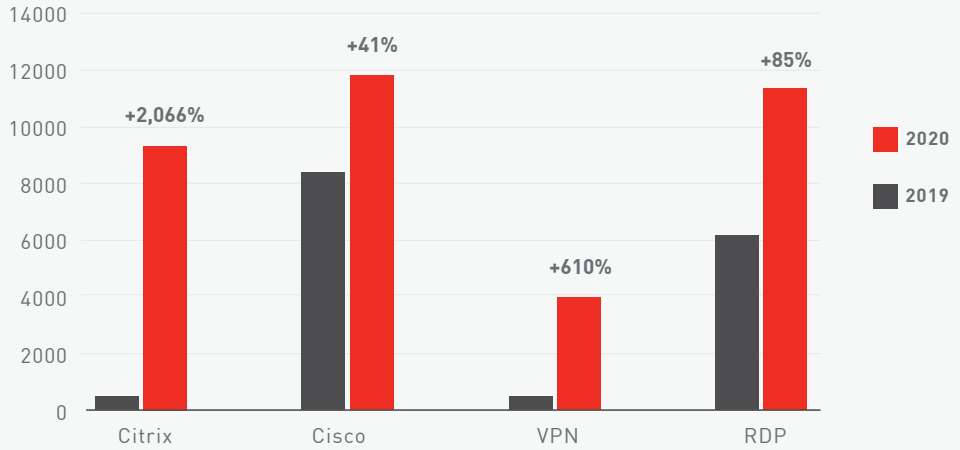


Figure 2 : les groupes APT intègrent des vulnérabilités d'accès à distance nouvelles et anciennes pour s'implanter.

exploité des vulnérabilités d'accès à distance, anciennes et récentes, pour s'implanter dans leurs réseaux cibles.

Le groupe iranien Fox Kitten, qui a pris pour cible ces trois dernières années des organisations du secteur du pétrole et du gaz, de l'aviation, de l'informatique gouvernementale et de la sécurité, exploite les vulnérabilités connues des systèmes dont le principal vecteur d'infection reste les services VPN et RDP sans correctifs. Le groupe APT 41, affilié à la Chine, a exploité les vulnérabilités des applications Cisco et Citrix dans le cadre d'une campagne axée sur les secteurs industriels, financiers ainsi que ceux de la télécommunication et de la santé.

En octobre 2020, la NSA a publié un rapport détaillé énumérant les 25 principales vulnérabilités actuellement utilisées et exploitées par les acteurs de la menace chinois. Les failles qui figuraient sur la liste ont été exploitées sept fois plus souvent que d'autres vulnérabilités en 2020. Le graphique ci-dessus montre l'augmentation des attaques exploitant des vulnérabilités des produits de connexion à distance.

La liste des 20 vulnérabilités les plus exploitées de Check Point Research, comme le montre notre réseau de capteurs du système de prévention des intrusions (IPS), comprend huit vulnérabilités pour les dispositifs d'accès à distance. Parmi ces vulnérabilités, citons **Cisco Unified IP Conference Station 7937G Denial of Service (CVE-2020-16139), Citrix XenMobile Server Directory Traversal (CVE-2020-8209)** et **Citrix ADC Reflected Cross Site Scripting (CVE-2020-8191).**

ISAAC DVIR
Directeur, Solutions mobile

« Alors que nous comptons davantage sur nos appareils mobiles pour rester connectés et gérer nos vies, les attaquants les ciblent de plus en plus via des malwares sophistiqués et des applications malveillantes, et tentent d'exploiter les vulnérabilités. Les entreprises doivent adopter une sécurité mobile capable de protéger en toute transparence les appareils non gérés contre ces cybermenaces avancées, et les utilisateurs doivent veiller à n'utiliser que les applications des boutiques d'applications officielles pour minimiser les risques. »

Alors que les chercheurs continuaient à enquêter et à identifier les vulnérabilités des plateformes d'accès à distance, les attaquants, qu'ils soient expérimentés ou non, utilisaient le délai entre la divulgation des vulnérabilités et l'application réelle de correctifs aux systèmes pour déclencher des attaques et renforcer leur emprise sur les cibles corporatives dans le monde entier.

MOBILE : DE LA COVID-19 AUX ATTAQUES DE TYPE « ZERO-CLICK »

La COVID-19, comme pour tous les autres aspects de la vie, a dominé le paysage des cybermenaces mobiles en 2020. Outre l'introduction de plusieurs applications malveillantes se faisant passer pour des applications légitimes liées au coronavirus, des inquiétudes croissantes ont été exprimées concernant des problèmes de confidentialité des données dans les applications officielles de suivi développées par les gouvernements.

L'augmentation de l'utilisation d'appareils mobiles dans le contexte du confinement et de la distanciation sociale peut également expliquer le développement important des familles de malwares de type cheval de Troie bancaire. L'acteur de la menace Guildma a créé Ghimob, capable d'effectuer des transactions sur des comptes d'institutions financières au Brésil, au Paraguay, au Pérou, au Portugal, en Allemagne, en Angola et au Mozambique. L'EventBot, récemment découvert, se concentre sur des cibles aux États-Unis et en Europe, tandis que le ThiefBot vise les utilisateurs turcs. La liste continue avec BlackRock, Wroba, TrickMo et autres, qui montrent tous l'augmentation des attaques de type cheval de Troie bancaire.

« Le CloudGuard de Check Point a été essentiel pour nous permettre d'ajouter de nouvelles charges de travail et de nouveaux services sur le cloud sans devoir analyser ou déployer constamment de nouvelles infrastructures de sécurité. Cela signifie que nous pouvons nous concentrer sur les tâches publiques critiques où nous pouvons ajouter une valeur réelle. Nous construisons actuellement nos systèmes de gestion de la vaccination, et notre approche axée sur le cloud nous donne l'agilité et l'évolutivité dont nous avons besoin pour les déployer au niveau national tout en nous assurant que les données et les services sont sécurisés. »

DERYCK MITCHELSON
Responsable de la sécurité de l'information, Ministère de la Santé écossais

NHS SCOTLAND

Les activités de menace persistante avancée (APT) via les appareils mobiles se sont poursuivies, propageant les outils d'accès à distance mobiles (MRAT) et affinant sans cesse leurs capacités. Dans certains cas, comme celui de l'APT iranien Rampant Kitten, l'acteur de la menace a utilisé une combinaison de fausses applications mobiles, d'infostealers Windows et de pages de phishing Telegram pour se servir des codes d'authentification à deux facteurs (2FA) volés afin d'espionner les citoyens iraniens expatriés. Les mécanismes d'authentification à facteurs multiples sont l'un des principaux objectifs des groupes d'espionnage et des groupes à motivation financière dans le cadre de leur activité de surveillance.

Les vulnérabilités majeures signalées cette année dans le matériel mobile et les applications populaires peuvent marquer un changement dans les stratégies d'attaque, qui sont actuellement basées sur des applications malveillantes déguisées ou des vulnérabilités du système d'exploitation. Auparavant, dans la plupart des cas, les attaquants parvenaient à s'implanter grâce à des applications malveillantes ou des failles du système d'exploitation, mais en 2020, nous avons constaté une augmentation des rapports de vulnérabilités dans le matériel mobile et les applications populaires.

La famille de vulnérabilités Achilles a révélé plus de 400 faiblesses dans une puce Qualcomm qui touche une grande partie de l'ensemble du marché mobile. Zimperium a fait remarquer des faiblesses supplémentaires dans le matériel des téléphones Android qui peuvent être exploitées et entraîner une prise de contrôle totale. Il a été constaté que les applications les plus

TSION (TJ) GONEN
Responsable de la ligne de produits cloud

« Le taux de migrations et de déploiements cloud a dépassé les capacités des équipes de sécurité à se défendre contre les attaques et les violations. Plus de 80 % des entreprises déclarent que leurs solutions de sécurité traditionnelles ne fonctionnent pas du tout, ou ne fournissent que des fonctions limitées dans les environnements cloud, créant ainsi une excellente opportunité pour les attaquants ciblant le cloud. Pour combler ces failles de sécurité, les entreprises doivent bénéficier d'une visibilité holistique sur tous leurs environnements de cloud public et déployer des protections unifiées et automatisées natives du cloud. De cette façon, ils peuvent suivre le rythme des demandes commerciales tout en garantissant une sécurité et une conformité continues. »

utilisées exposent leurs utilisateurs à de potentielles exploitations de vulnérabilités. Instagram aurait une vulnérabilité RCE de type zero click dans son décodeur JPEG. La vulnérabilité du système de connexion Apple peut permettre aux attaquants à distance de contourner l'authentification et de pirater certains comptes ciblés. Des vulnérabilités supplémentaires ont été détectées sur WhatsApp, Facebook et d'autres encore.

ESCALADE DES PRIVILÈGES SUR LE CLOUD

La pandémie de COVID-19 a entraîné un changement systématique de l'architecture du réseau d'entreprise. Le besoin urgent en réseaux souples et évolutifs gérés à distance a accéléré le passage à une infrastructure cloud qui permet une flexibilité en termes d'échelle et de gestion des ressources et qui est accessible depuis n'importe où. Une étude récente montre que le marché du cloud a augmenté de près de 40 % au premier trimestre 2020 et révèle l'utilisation croissante des réseaux cloud hybrides. D'ici 2025, il est prévu que le marché sera supérieur au double de sa valeur actuelle.

Les pirates ont remarqué cette migration massive vers les technologies cloud hybrides. Dark Halo, l'acteur de la menace derrière la tristement célèbre scandale de la chaîne d'approvisionnement SolarWinds à l'origine de la violation de plus de 18 000 organisations, s'est fortement appuyé sur le modèle de cloud hybride pour accéder aux informations sensibles et mettre en place une persistance sur les organisations ciblées. Une fois qu'une organisation est compromise, l'attaquant

passe latéralement du serveur SolarWinds de l'organisation au serveur Active Directory Federation Services (ADFS) sur site, un service responsable de l'authentification unique de l'organisation pour accéder aux services cloud comme Office 365. À ce stade, l'attaquant utilise une technique précédemment publiée pour créer un « Golden SAML » qui donne à l'attaquant un accès complet, persistant et difficile à détecter aux services cloud de la victime.

Dans l'ensemble, nous avons constaté l'année dernière un changement dans la nature des erreurs de configuration du cloud, leurs causes profondes et leurs conséquences lorsque les erreurs de configuration de la gestion des identités et des accès (GIA) ont commencé à faire la une des journaux. Ces attaques ciblées de comptes cloud, parfois causées par des failles dans les autorisations du fournisseur ou la logique derrière la politique de confiance, pourraient permettre à un attaquant d'obtenir une escalade des privilèges et de se déplacer latéralement dans l'environnement cloud de l'entreprise, obtenant ainsi des clés privées de certificat, des informations sensibles et des identifiants de base de données.

Il y a essentiellement une tendance à s'attaquer aux comptes sur le cloud plutôt qu'aux ressources sur le cloud. Cette nouvelle façon d'utiliser le cloud a ouvert la porte à des vecteurs d'attaque basés sur la prise en charge du rôle (la capacité d'obtenir des autorisations à court terme pour des ressources), ce qui permet souvent de vastes opérations au sein de l'environnement, y compris le vol de données. Selon des chercheurs, les rôles de gestion des identités et des accès (GIA) peuvent être utilisés de manière abusive par 22 API réparties dans 16 services Amazon. Les exploitations de vulnérabilité d'escalade de privilège basées sur les paramètres d'autorisation peuvent également être trouvées sur Salesforce qui, contrairement à AWS, est un SaaS (Software as a Service).

Cette nouvelle classe d'attaques d'escalade de privilèges, qui exploite les composants structurels de l'infrastructure cloud, peut souvent être obtenue en enchaînant plusieurs vulnérabilités et erreurs de configuration. L'accès initial peut être obtenu via une application vulnérable hébergée sur le cloud, et utilisé par les attaquants pour se procurer le jeton nécessaire pour obtenir des autorisations importantes et se déplacer latéralement dans les différents segments de l'environnement, augmentant progressivement les privilèges. Ces attaques s'appuient sur la compréhension des composants, de l'architecture et de la politique de confiance des fournisseurs IaaS (Infrastructure-as-a-Service, comme Amazon) et SaaS pour élaborer des attaques sophistiquées en plusieurs étapes, contrairement aux violations de données autrefois courantes, qui s'appuyaient principalement sur des paramètres mal configurés tels que les compartiments S3 exposés publiquement.

BIEN QUE 2020 AIT ÉTÉ UNE ANNÉE QUE BEAUCOUP PRÉFÉRERAIENT OUBLIER, NOUS AVONS ÉGALEMENT VU DE NOMBREUSES ACTIONS RÉUSSIES DES ORGANISATIONS MONDIALES D'APPLICATION DE LA LOI, SOUTENUES PAR LA COMMUNAUTÉ DE LA CYBERSÉCURITÉ, DANS LE SUIVI ET L'INCULPATION DE NOMBREUSES PERSONNES ET GROUPES DE LA MENACE IMPLIQUÉS DANS LA CYBERCRIMINALITÉ DANS LE MONDE ENTIER.

LES BONS CÔTÉS DE 2021

En octobre, la tristement célèbre infrastructure de cybercriminalité « Trickbot », qui compte plus d'un million de machines infectées à l'échelle mondiale, a été démantelée dans le cadre d'une action coordonnée par les fournisseurs et les forces de l'ordre. Cet exemple et d'autres montrent comment une collaboration étroite entre les chercheurs en sécurité, les fournisseurs de logiciels, les forces de l'ordre et les organismes gouvernementaux peut réduire et même éliminer les cybermenaces et attaques majeures qui peuvent avoir un impact sur nos vies. Sur la base de cette réussite, nous envisageons avec optimisme que 2021 offrira de nombreux autres exemples positifs de la manière dont les cybermenaces peuvent être vaincues.

Les pays ont coopéré en extradant les cybercriminels pour comparaître en justice à l'étranger, atteignant des niveaux élevés de coopération internationale. Europol a dirigé plusieurs de ces enquêtes, notamment l'opération DisrupTor au cours de laquelle 179 vendeurs de biens illicites sur les forums du Dark Web ont été arrêtés. Des stocks de marchandises illégales ont été saisis, notamment de la drogue, de l'argent liquide et des devises cryptographiques, ainsi que des armes.

Des actions contre des pirates individuels ont entraîné différentes arrestations, comme dans le cas du résident de la Floride âgé de 17 ans, derrière le célèbre piratage Twitter de célébrités. Un rapport Check Point Research aux autorités juridiques brésiliennes révélant l'identité de « VandaTheGod », qui a mené pendant sept ans une campagne de dégradation de sites Internet et de vol d'informations à l'encontre des gouvernements du monde entier, a abouti à son arrestation. Le membre de GandCrab qui a utilisé le célèbre MaaS pour extorquer des victimes dans plus de 100 pays a été arrêté en Biélorussie.

L'effort mondial visant à exposer les individus derrière les APT et les activités de cybercriminalité de l'État s'est poursuivi. L'Allemagne a émis des mandats d'arrestation pour un officier de renseignement militaire russe suspecté de pirater des serveurs du parlement allemand. Les autorités américaines ont arrêté un membre du groupe de piratage Fin7, qui était lié au vol de plus d'un milliard de dollars. Six ressortissants russes, membres de la GRU, ont été accusés d'avoir orchestré les attaques de type Sandworm sur des infrastructures

ukrainiennes et les élections françaises, ainsi que la diffusion du ransomware NotPetya et l'attaque Olympic Destroyer.

Le gouvernement américain a également porté plainte contre cinq ressortissants chinois, faisant partie du groupe chinois APT41, pour le piratage de plus de 100 sociétés. Deux hommes d'affaires malaisiens ont été arrêtés par les autorités locales pour avoir coopéré dans les activités d'APT41. En conclusion d'une enquête de trois ans, le département de la Justice des États-Unis a inculpé quatre pirates informatiques soutenus par l'armée chinoise dans l'affaire Equifax, qui a touché près de la moitié des Américains.

Ce ne sont pas seulement des groupes et des acteurs de la menace individuels qui ont été poursuivis. Dans de nombreux cas, les organismes de cybercriminalité ont ciblé et réussi à démanteler les infrastructures des opérations criminelles. En octobre, Microsoft, de concert avec différents organismes gouvernementaux, a démantelé les infrastructures derrière le botnet Trickbot. Connu pour ses activités malveillantes avec d'autres groupes de malwares, qui se sont souvent traduits par le déploiement de ransomwares, il a été désigné comme une menace majeure pour les élections américaines de 2020. Ce n'était pas le premier effort de l'année mené par Microsoft. En mars, l'entreprise a engagé une action contre le botnet Necurs, rompant son mécanisme DGA et bloquant les futurs enregistrements de domaine.

La COVID-19 a incité différents acteurs à s'unir pour lutter contre les cyberattaques. Le NCSC (National Cyber Security Centre) britannique a augmenté les capacités de son service de démantèlement et a mobilisé le grand public afin de mettre un terme aux escroqueries liées au coronavirus, ce qui a permis de démanteler plus de 22 000 URL malveillantes liées à la COVID-19. La pandémie a rassemblé des initiatives telles que la Cyber Threat Coalition (CTC), unissant les efforts de milliers de professionnels de la sécurité pour recueillir, analyser et partager les IoC liés à la COVID-19. La CTI League a mis en place une communauté mondiale de bénévoles pour protéger les secteurs liés à la pandémie et susceptibles de sauver des vies.

Les gouvernements analysent activement les réseaux à la recherche de faiblesses et alertent les CISO en conséquence. La NCSC britannique a signalé avoir analysé un million d'adresses IP du NHS (National Health Service) avec 51 000 IoC partagés.

Les rapports de vulnérabilité et le partage d'informations, en particulier les enquêtes « zero-day », constituent un autre domaine qui affiche des résultats positifs. Les exploitations de vulnérabilité zero-day sont inconnues des fournisseurs de logiciels et peuvent donc être exploitées par des personnes malveillantes. Check Point Research a trouvé et signalé une vulnérabilité de score CVE de 10,0 dans Microsoft Azure, permettant à Microsoft de la corriger et de protéger les utilisateurs contre les prises de contrôle malveillantes du cloud. De même, Check Point Research a signalé SIGRed, une vulnérabilité de score 10,0 sur les serveurs DNS Windows. Les alertes intersectorielles ont favorisé l'application de correctifs contre la vulnérabilité VPN Pulse Secure, l'exploitation F5 BIG-IP et plus encore. Les malwares eux-mêmes ne sont pas exempts de vulnérabilités et un bogue de dépassement de buffer chez Emotet a agi comme un coupe-circuit et a permis aux chercheurs d'arrêter son activité pendant une période de six mois en 2020.

Cette pause dans l'activité d'Emotet a été suivie en janvier 2021 par l'annonce qu'une opération internationale de la police dans plusieurs pays avait réussi à faire tomber le botnet Emotet qui, depuis de nombreuses années, était considéré comme l'une des variantes de malwares les plus dangereuses au monde.

Cet exemple et d'autres montrent comment une collaboration étroite entre les chercheurs en sécurité, les fournisseurs de logiciels, les forces de l'ordre et les organismes gouvernementaux peut réduire et même éliminer les cybermenaces et attaques majeures qui peuvent avoir un impact sur nos vies. Sur la base de cette réussite, nous envisageons avec optimisme que 2021 offrira de nombreux autres exemples positifs de la manière dont les cybermenaces peuvent être vaincues.

LES DONNÉES PRÉSENTÉES DANS LES SECTIONS SUIVANTES DE CE RAPPORT SONT BASÉES SUR LES RÉSULTATS TIRÉS DE LA CARTE DES CYBERMENACES DE CHECK POINT THREATCLOUD ENTRE LE 1ER JANVIER ET LE 31 DÉCEMBRE 2020.

5 STATISTIQUES MONDIALES SUR LES MALWARES

CATÉGORIES DE CYBERATTAQUES PAR RÉGION

À L'ÉCHELLE MONDIALE

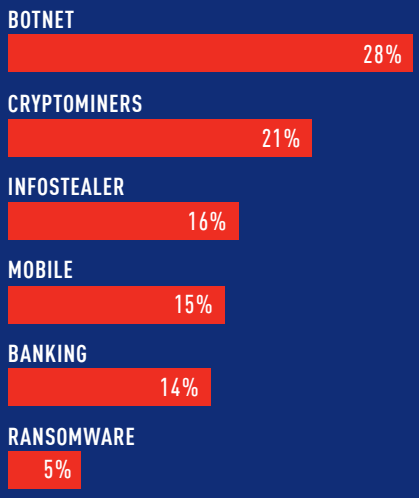


Figure 3 : pourcentage de réseaux d'entreprise attaqués par type de malware.

AMÉRIQUES

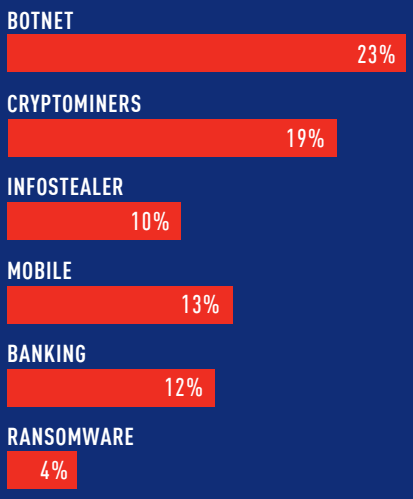


Figure 4 : pourcentage de réseaux d'entreprise attaqués par type de malware.

CATÉGORIES DE CYBERATTAQUES PAR RÉGION

EMEA

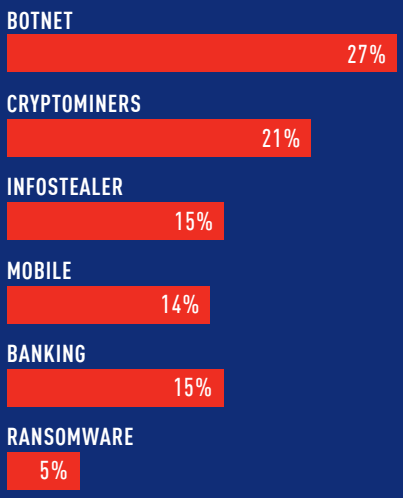


Figure 5 : pourcentage de réseaux d'entreprise attaqués par type de malware.

APAC

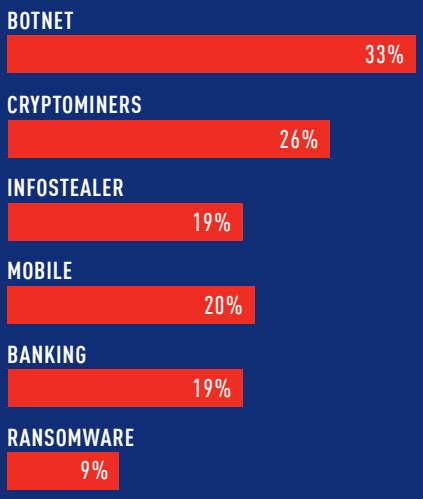
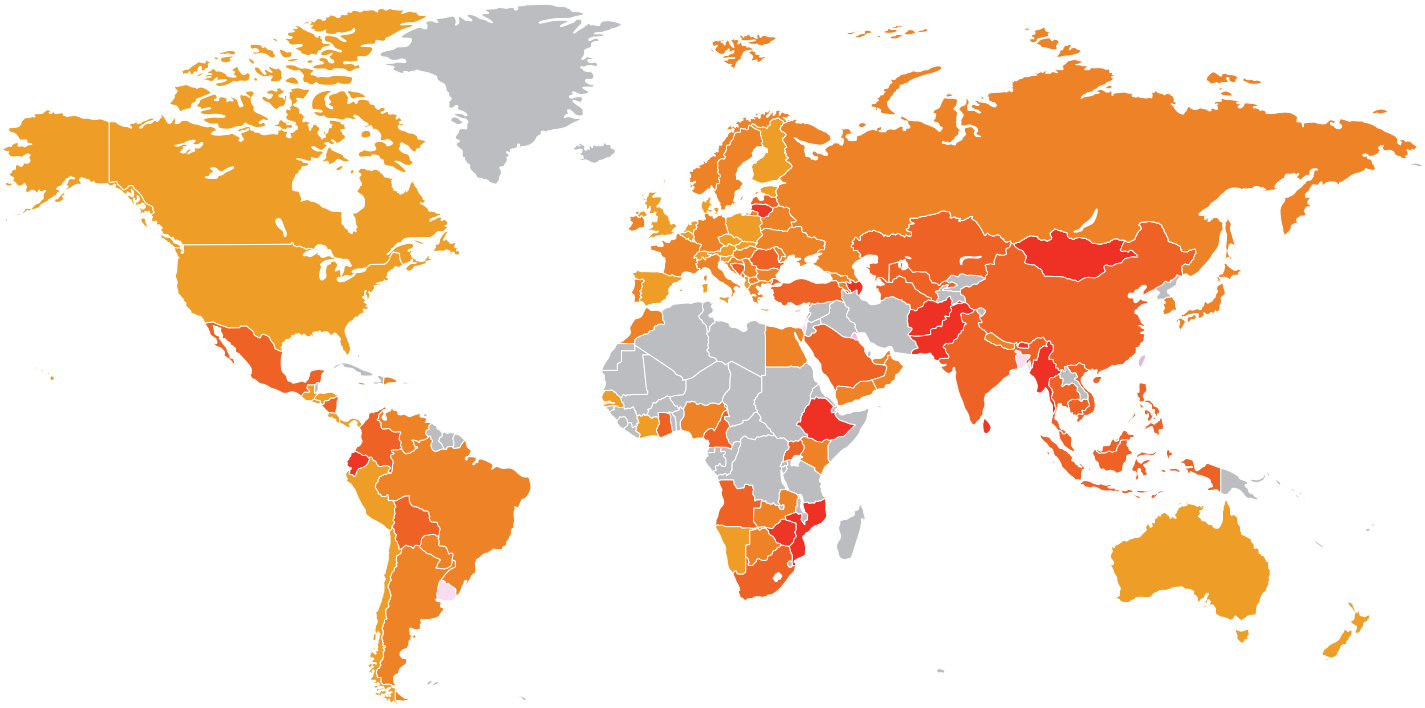


Figure 6 : pourcentage de réseaux d'entreprise attaqués par type de malware.

CARTE DE L'INDICE MONDIAL DES MENACES

La carte affiche l'indice de risque de cybermenace à l'échelle mondiale, présentant les principales zones à risque dans le monde.*



* Rouge plus foncé = Risque plus élevé
Gris = Données insuffisantes

Figure 7.

PRINCIPAUX TYPES DE FICHIERS MALVEILLANTS – WEB ET E-MAIL

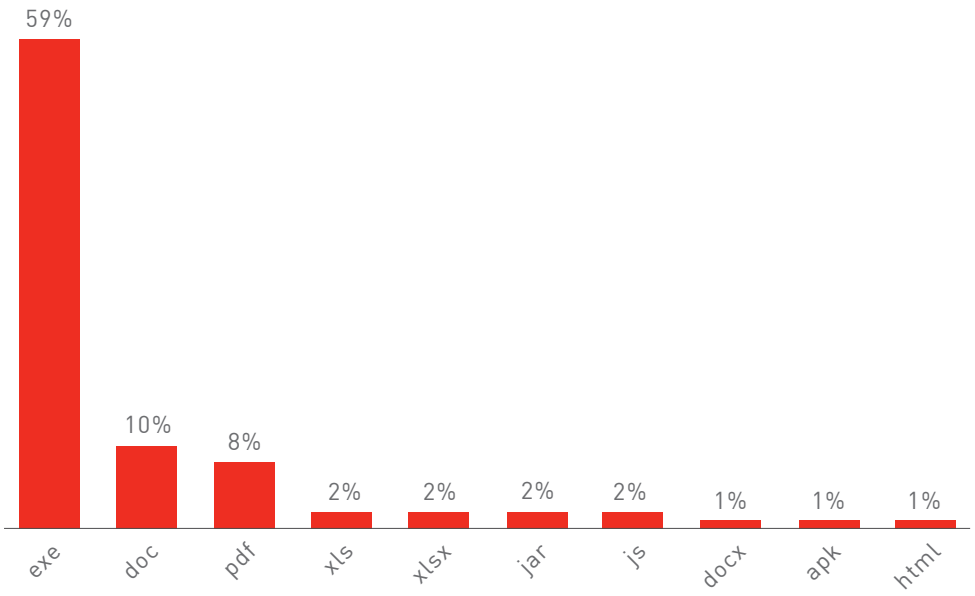


Figure 8 : les principaux types de fichiers malveillants sur Internet.

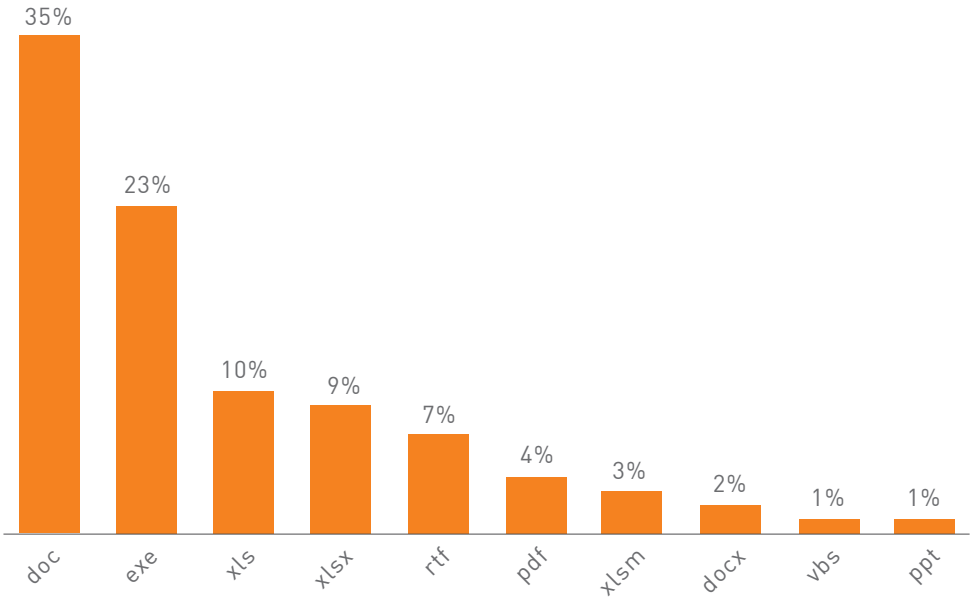


Figure 9 : les principaux types de fichiers malveillants par e-mail.

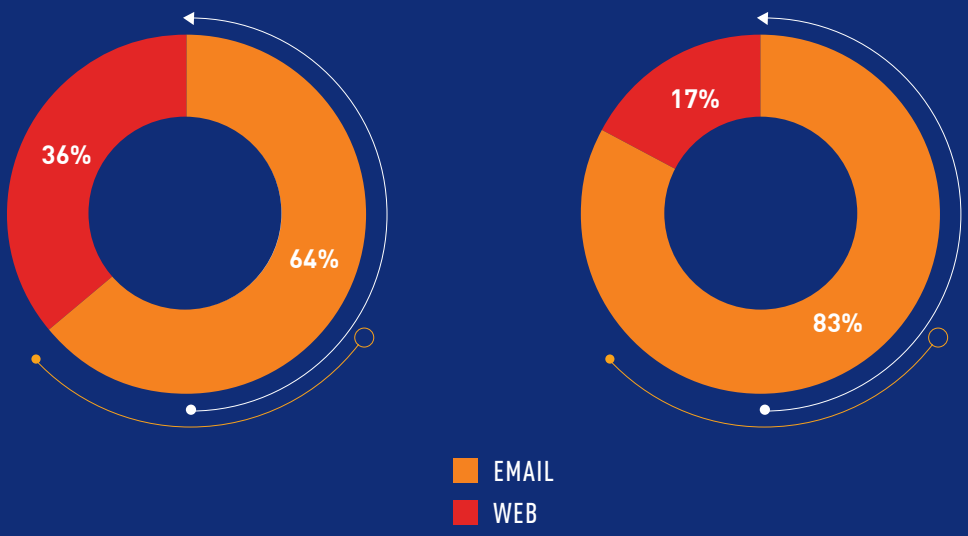


Figure 10 : protocoles de distribution – Vecteurs d'attaques par e-mail et sur Internet en 2019 et 2020.

Le graphique ci-dessus montre une augmentation significative de près de 20 % de la distribution des attaques par e-mail par rapport aux vecteurs d'attaque Web. Le pic correspond à la chronologie des événements de 2020 et à la fin de vie de Flash Player qui a rendu les kits d'exploitation de vulnérabilité moins efficaces. La seule pandémie de COVID-19, qui a été exploitée de manière créative par les attaquants depuis sa création, a entraîné une augmentation de 220 % du taux d'attaque par e-mail de phishing.

Les autres événements actuels qui ont été lourdement exploités par les cybercriminels et les groupes de menaces comprennent Black Lives Matters, l'élection présidentielle de 2020 et les journées commerciales de shopping.

STATISTIQUES MONDIALES SUR LES MALWARES

Les données présentées dans les sections suivantes de ce rapport sont basées sur les données tirées de la carte des cybermenaces de Check Point ThreatCloud entre janvier et le décembre 2020.

Pour chacune des régions ci-dessous, nous présentons le malware le plus répandu.

LES PRINCIPALES FAMILLES DE MALWARES

À L'ÉCHELLE MONDIALE

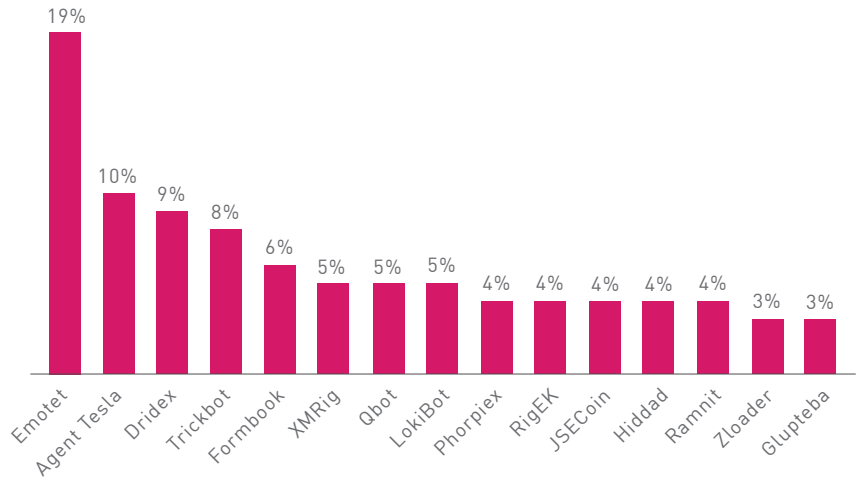


Figure 11 : les malwares les plus répandus à l'échelle mondiale.
Pourcentage de réseaux d'entreprise attaqués par famille de malware.

AMÉRIQUES

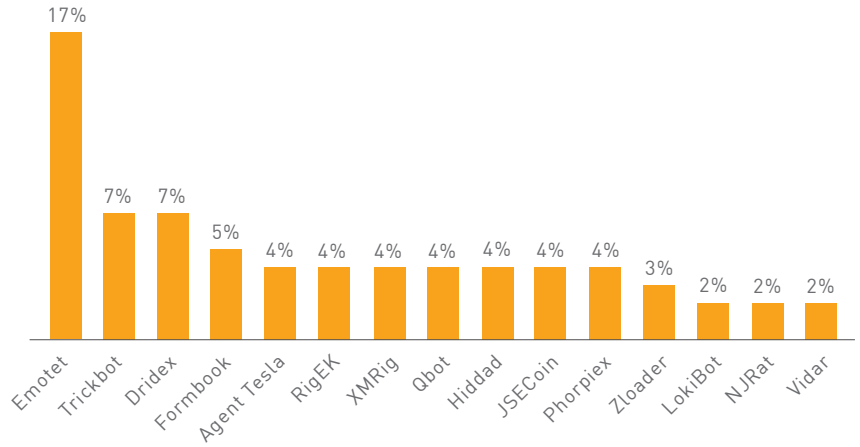


Figure 12 : les malwares les plus répandus aux Amériques.

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)

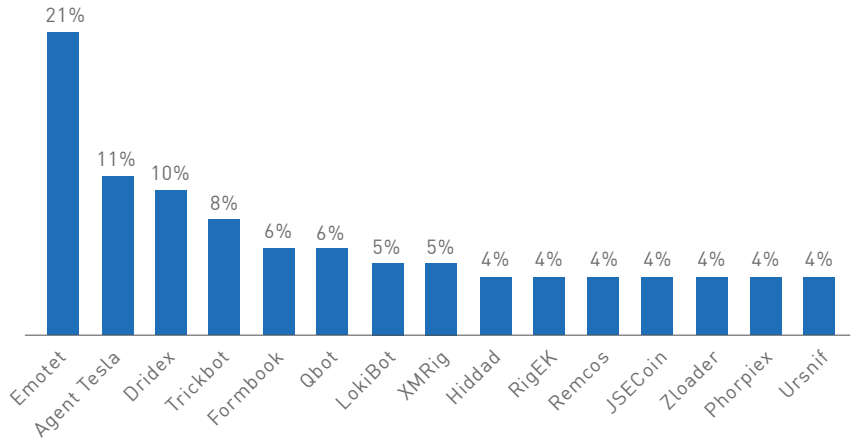


Figure 13 : les malwares les plus répandus dans la région EMEA.

ASIE-PACIFIQUE (APAC)

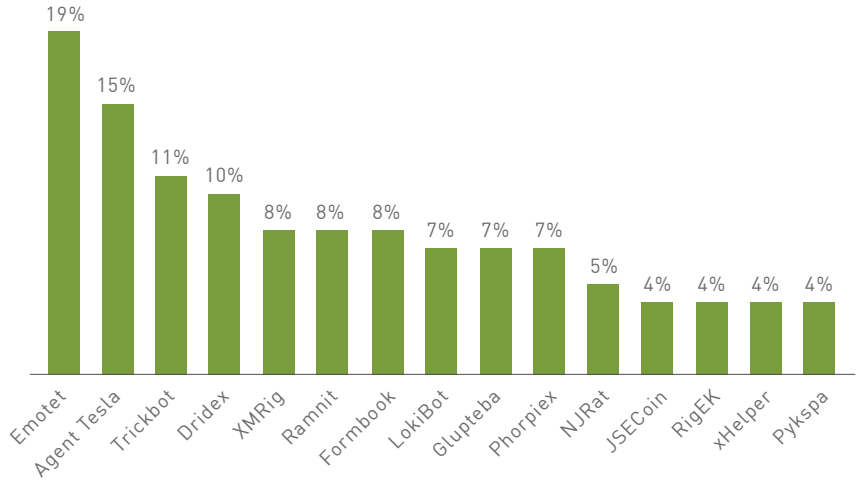


Figure 14 : les malwares les plus répandus dans la région APAC.

AU COURS DE LA DERNIÈRE SEMAINE DE JANVIER 2021, LES AGENCES INTERNATIONALES D'APPLICATION DE LA LOI ONT PRIS LE CONTRÔLE DE L'INFRASTRUCTURE EMOTET, ET LE DÉMANTÈLEMENT EST EN COURS : UNE VICTOIRE MAJEURE DANS LA LUTTE CONTINUE CONTRE LES MALWARES.

ANALYSE MONDIALE DES PRINCIPAUX MALWARES

De nombreuses familles de malwares ont pu maintenir leur rang mondial de 2019, avec seulement de légères montées ou descentes de rang. Agent Tesla et Formbook, deux infostealers largement répandus, sont passés des rangs inférieurs aux cinq premiers. Les cryptomineurs de type « drive-by » comme Cryptoloot sont descendus de rang ou sont sortis du top 10.

Emotet, un botnet à l'origine de la diffusion de Trickbot, Qbot et d'autres encore, entraînant dans certains cas une attaque par ransomware, constituait la famille de malwares la plus largement distribuée en 2019 et en 2020. Les statistiques annuelles reflètent la part importante du botnet dans le paysage des menaces, malgré des interruptions périodiques de l'activité sur plusieurs mois. La pause la plus longue a eu lieu entre février et juillet 2020 et a réduit l'impact d'Emotet sur le premier semestre de l'année.

Emotet a également tiré parti des élections présidentielles des États-Unis en 2020 avec une campagne de spam distribuant des lettres supposées provenir de l'initiative Team Blue de la Convention nationale démocrate. Pendant sa pause, Emotet a raté l'opportunité des premiers mois du début de la pandémie, mais son retour en juillet lui a tout de même permis de tirer pleinement profit de la situation. Après une autre pause de deux mois, Emotet a repris ses attaques le jour du réveillon de Noël lors d'une campagne ciblant plus de 100 000 utilisateurs par jour. Le botnet a mis à jour ses charges utiles, amélioré ses capacités de contournement de la détection et modifié son document macro malveillant pour dissimuler le flux d'installation de la charge utile.

LES PRINCIPAUX MALWARES MOBILES

À L'ÉCHELLE MONDIALE

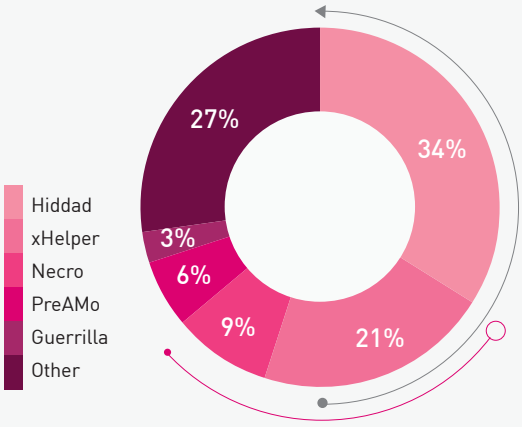


Figure 15 : les principaux malwares mobiles à l'échelle mondiale

AMÉRIQUES

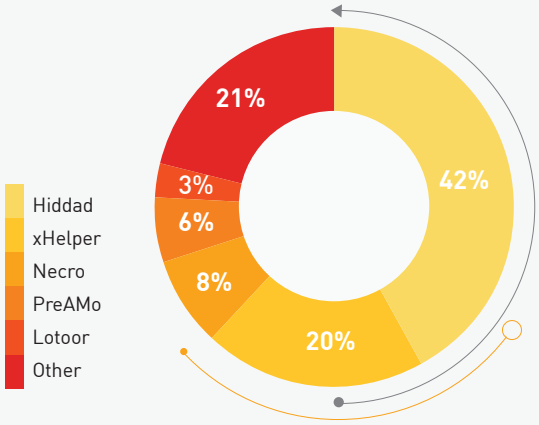


Figure 16 : les principaux malwares mobiles aux Amériques

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)

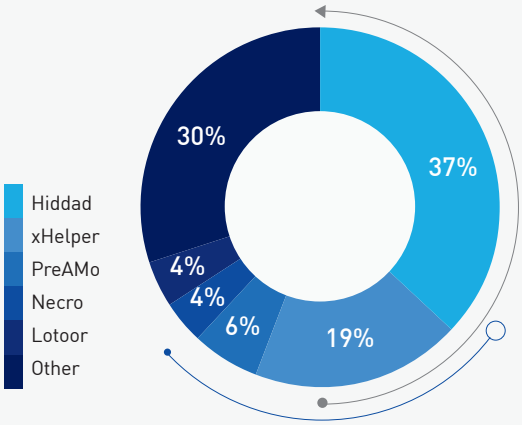


Figure 17 : les principaux malwares mobiles dans la région EMEA

ASIE-PACIFIQUE (APAC)

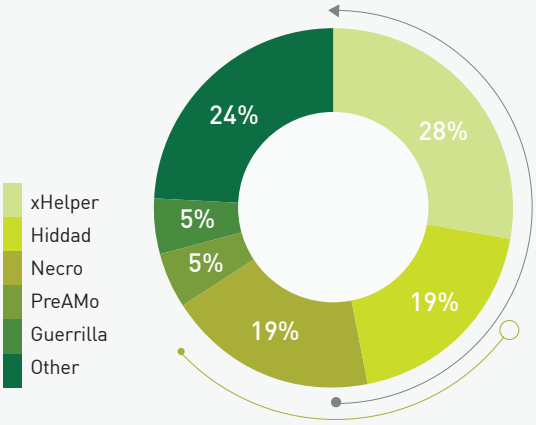


Figure 18 : les principaux malwares mobiles dans la région APAC

ANALYSE MONDIALE DES MALWARES MOBILES

Hiddad, l'abréviation de « Hidden Ad », est passé de la quatrième place en 2019 à la tête du classement mondial cette année. Le malware, conçu pour afficher des publicités et collecter des informations système, dispose de moyens simples, mais intelligents, pour rester sur l'appareil de la victime. Il masque son icône du lanceur d'applications et se fait passer pour d'autres applications après l'installation, telles que « Google Play Service » et « Google Play Store ». Cette année, le malware a rejoint la tendance COVID-19 et s'est fait passer pour une application d'information sur le coronavirus pour les personnes arabophones. Après l'infection, le malware affichait en temps voulu de volumineuses publicités en plein écran.

LES PRINCIPAUX BOTNETS

À L'ÉCHELLE MONDIALE

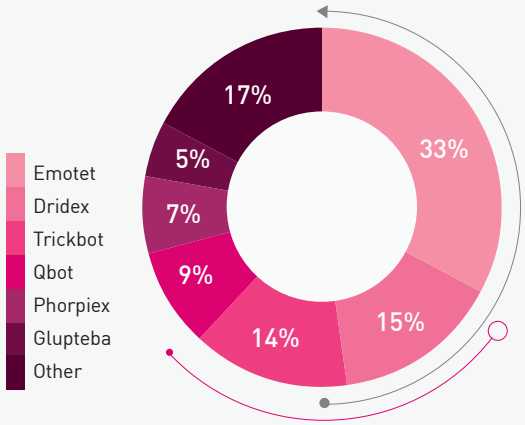


Figure 19 : les botnets les plus répandus à l'échelle mondiale

AMÉRIQUES

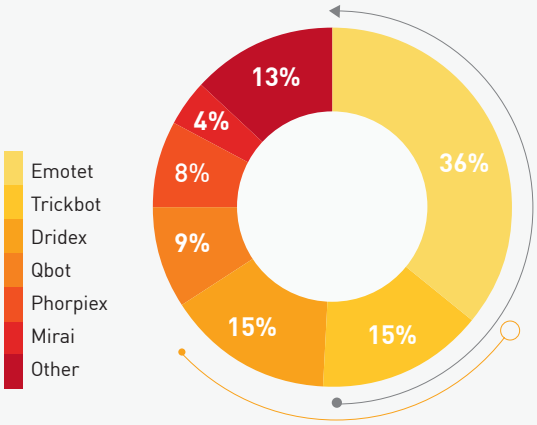


Figure 20 : les botnets les plus répandus aux Amériques

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)

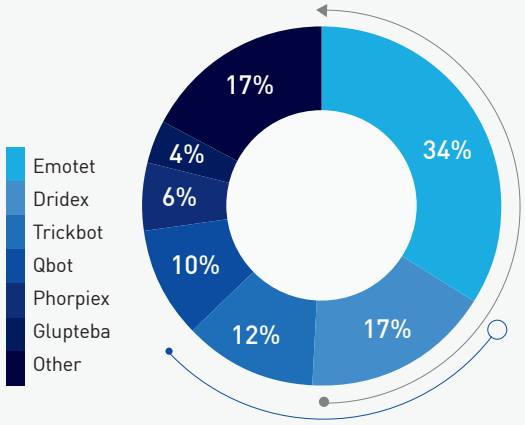


Figure 21 : les botnets les plus répandus dans la région EMEA

ASIE-PACIFIQUE (APAC)

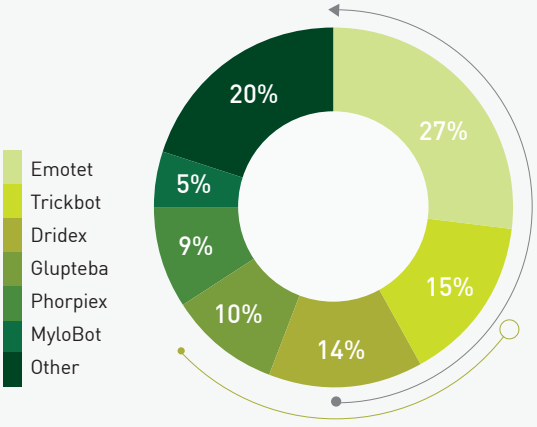


Figure 22 : les botnets les plus répandus dans la région APAC

ANALYSE MONDIALE DES BOTNETS

L'arène des botnets reste sous le contrôle de plusieurs botnets majeurs, notamment les variantes basées sur Emotet, Trickbot et Mirai. Cette année, contrairement à 2019, Dridex est entré dans nos premiers rangs, alimenté par de nombreuses campagnes de spam. Dridex est apparu la première fois comme cheval de Troie bancaire en 2012 et a gagné en visibilité en 2015 en raison de ses capacités de vol d'identifiants. Vers 2016, le malware a commencé à opérer comme un botnet, distribuant des malwares visibles tels que le ransomware Locky. Aujourd'hui, il alimente des attaques ciblées à l'aide du ransomware DoppelPaymer.

En septembre, Emotet et Trickbot ont participé à l'une des attaques les plus mémorables de 2020, attestant de la force et du potentiel de la collaboration de botnets avec l'incident d'UHS (Universal Health Services). UHS est l'un des plus grands prestataires de soins de santé aux États-Unis, avec plus de 400 établissements situés principalement aux États-Unis et au Royaume-Uni, et traite 3,5 millions de patients par an.

UHS a subi une attaque du ransomware Ryuk, entraînant le verrouillage des ordinateurs, des bases de données et des systèmes téléphoniques dans tous les établissements UHS aux États-Unis pendant près d'un mois. Les employés et le personnel médical ont reçu comme consigne de travailler uniquement avec des documents papier. Des rapports ont affirmé que les hôpitaux ont été obligés de rediriger toutes les ambulances vers des centres plus petits et que les traitements étaient retardés car les résultats de laboratoire ne pouvaient pas être livrés au personnel.

Les enquêteurs ont découvert qu'Emotet et Trickbot étaient tous deux impliqués dans l'attaque. Emotet a probablement obtenu l'accès au réseau d'UHS grâce à une pièce jointe malveillante d'un e-mail de phishing. Emotet a ensuite installé Trickbot afin de détecter et de récupérer des informations précieuses du système, puis a diffusé le ransomware Ryuk.

LES PRINCIPAUX MALWARES INFOSTEALERS

À L'ÉCHELLE MONDIALE

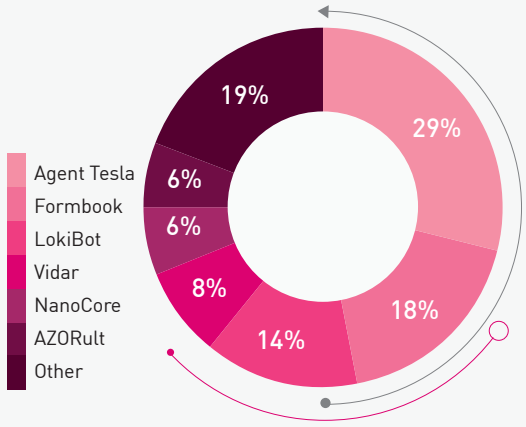


Figure 23 : les principaux malwares mobiles à l'échelle mondiale

AMÉRIQUES

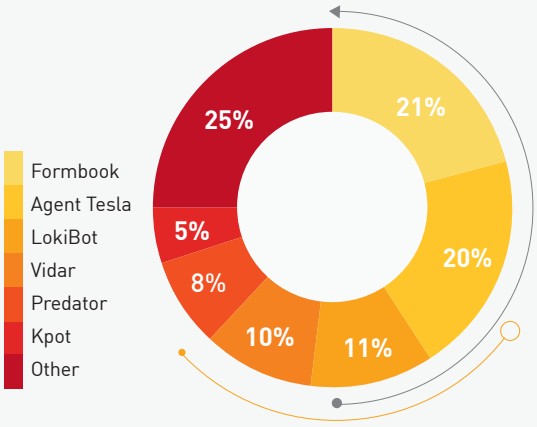


Figure 24 : les principaux malwares mobiles aux Amériques

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)

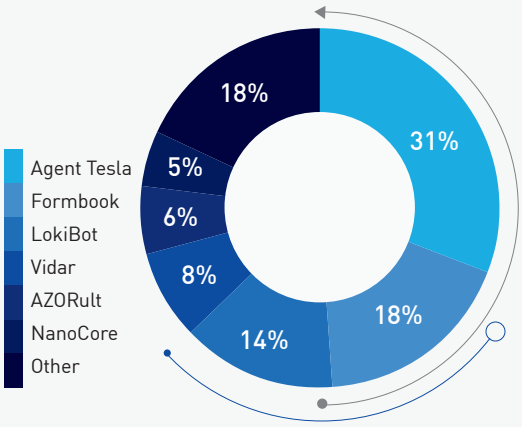


Figure 25 : les principaux malwares mobiles dans la région EMEA

ASIE-PACIFIQUE (APAC)

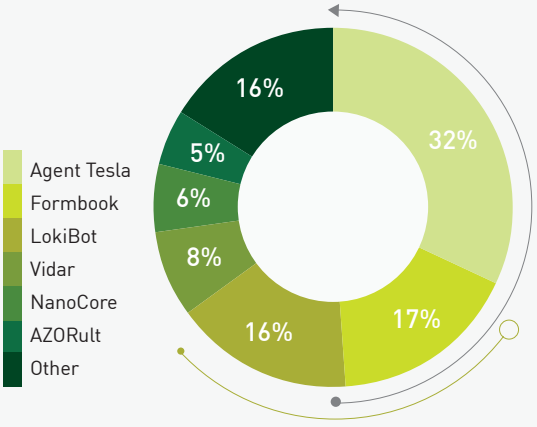


Figure 26 : les principaux malwares mobiles dans la région APAC

ANALYSE GLOBALE DES MALWARES INFOSTEALER

Le classement des meilleurs infostealers n'a pas connu de changements significatifs depuis l'année dernière. L'arène des infostealers est dominée par trois grandes familles de malwares : Agent Tesla, LokiBot et Formbook. Les malwares largement répandus, disponibles à l'achat ou au téléchargement, sont souvent alimentés par des campagnes de spam de masse qui peuvent être exploitées par des attaquants moins qualifiés. Le NanoCore RAT, qui n'était pas présent dans les classements au cours du premier semestre de l'année, est également un malware de ce type.

Les attaquants qui utilisent ces familles de malwares ont toujours recours à de nouvelles astuces pour éviter la détection, comme la migration de leur infrastructure vers le cloud et l'hébergement de ses charges utiles sur des services cloud connus tels que Dropbox et Google Drive via des comptes en apparence légitimes. En avril, une campagne LokiBot tirant parti de la pandémie a ciblé des utilisateurs aux États-Unis, en Turquie, au Portugal, en Allemagne et en Autriche. AZORult est un autre infostealer à avoir exploité l'épidémie de COVID-19. En mars, AZORult a été distribué via une application de carte des points chauds du coronavirus. Pendant que l'application affichait la carte, l'infostealer collectait des informations en arrière-plan.

LES PRINCIPAUX CHEVAUX DE TROIE BANCAIRES

À L'ÉCHELLE MONDIALE

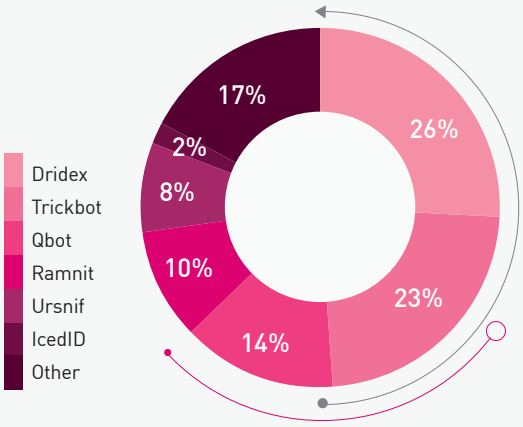


Figure 27 : les chevaux de Troie bancaires les plus répandus à l'échelle mondiale

AMÉRIQUES

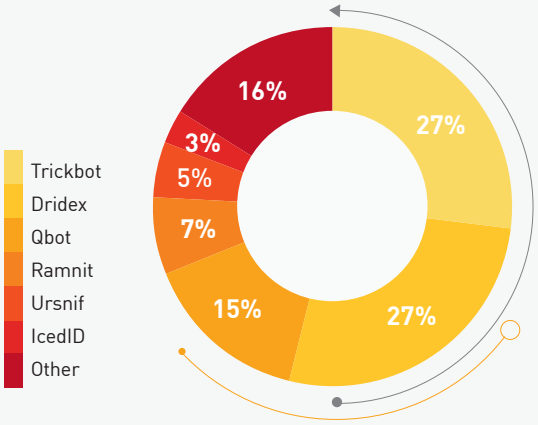


Figure 28 : les chevaux de Troie bancaires les plus répandus aux Amériques

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)

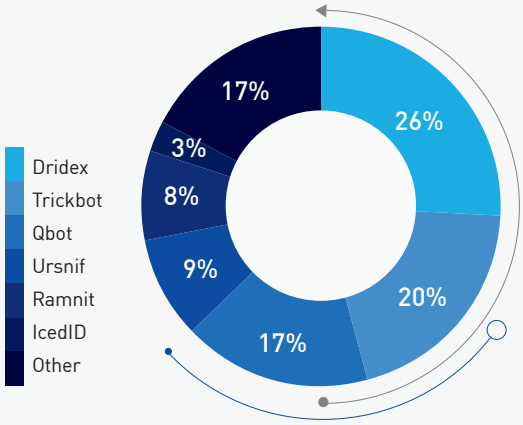


Figure 29 : les chevaux de Troie bancaires les plus répandus dans la région EMEA

ASIE-PACIFIQUE (APAC)

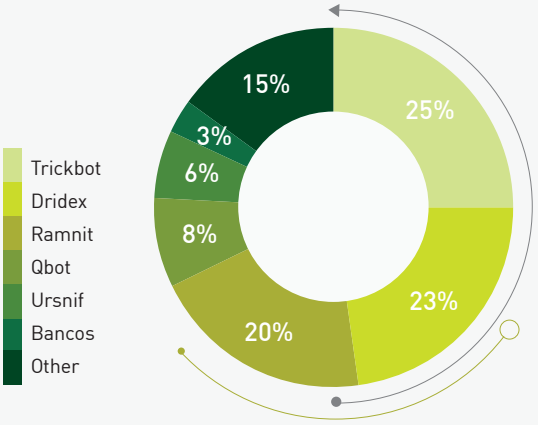


Figure 30 : les chevaux de Troie bancaires les plus répandus dans la région APAC

ANALYSE MONDIALE DES CHEVAUX DE TROIE BANCAIRES

Dridex et Trickbot continuent à dominer l'arène du secteur bancaire. Les institutions financières ont signalé une augmentation significative du nombre d'e-mails de phishing qui prétendent être envoyés par des banques connues. Nombre de ces campagnes tirent parti des changements provoqués par la crise de COVID-19, à savoir les difficultés financières, l'évolution du marché du travail et le travail solitaire à distance. Les e-mails de phishing prétendent offrir un soutien financier, des prêts flexibles et des reports de crédit.

Qbot a fait son apparition dans le classement des principaux malwares bancaires de cette année. Le malware est apparu pour la première fois en 2008, et a été conçu pour voler les identifiants bancaires et imiter les frappes de clavier des utilisateurs et se propager principalement par le biais de campagnes de spam par e-mail. Cependant, Qbot est un malware en constante évolution, disposant constamment de nouvelles fonctionnalités et capacités, tant pour l'exfiltration des données que pour la discrétion. Sa première campagne en 2020 s'est déroulée entre mars et la fin du mois de juin, et a été suivie d'un bref arrêt pour développement ultérieur. Qbot a rapidement repris son activité en juillet, aux côtés d'Emotet, et a été installé par Emotet dans plusieurs campagnes de spam. La dernière corde à son arc est le détournement de fils de discussion.

IcedID, un autre cheval de Troie bancaire en plein essor qui ciblait fortement la région des Amériques, a également réussi à se placer en tête du classement des malwares bancaires de la région. Relativement nouveau, IcedID a été révélé pour la première fois en 2017, et ciblait des banques, des sociétés de cartes de crédit, des services de paie et des sites d'e-commerce, principalement aux États-Unis. En 2020, sa dernière version comportait de nombreux outils d'évasion, des tactiques d'injection de code modifiées et la stéganographie.

LES PRINCIPAUX MALWARES DE CRYPTOMINING

À L'ÉCHELLE MONDIALE

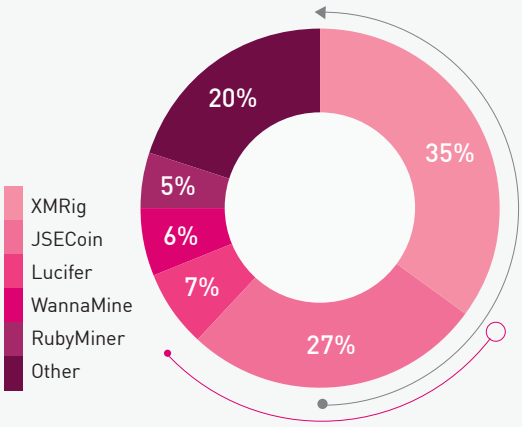


Figure 31 : les principaux malwares de cryptomining à l'échelle mondiale

AMÉRIQUES

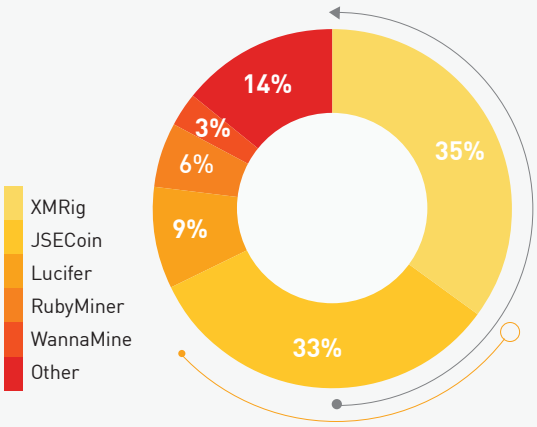


Figure 32 : les principaux malwares de cryptomining des Amériques

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)

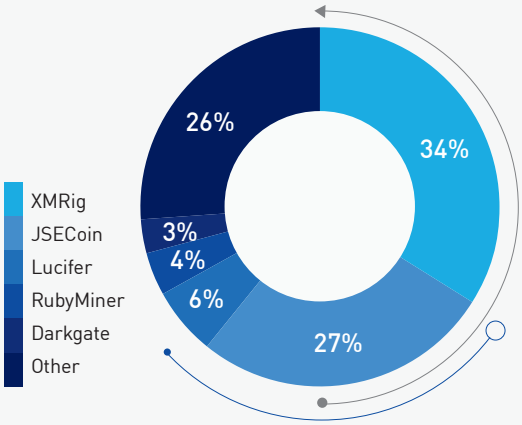


Figure 33 : les principaux malwares de cryptomining dans la région EMEA

ASIE-PACIFIQUE (APAC)

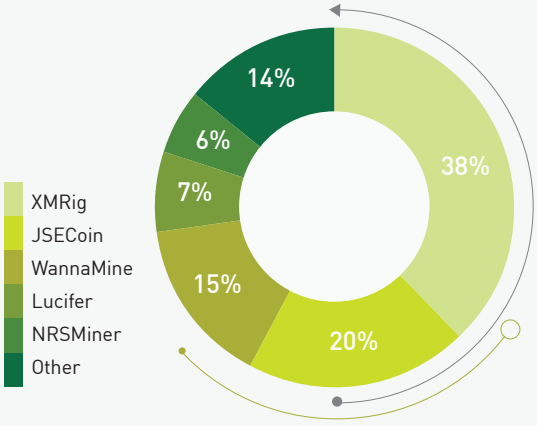


Figure 34 : les principaux malwares de cryptomining dans la région APAC

ANALYSE GLOBALE DES CRYPTOMINEURS

À l'origine, XMRig, un outil d'extraction légitime en open source utilisé par des attaquants à des fins malveillantes, se trouve désormais en haut du classement des cryptomineurs, malgré une baisse sur l'année de 46 % (au premier semestre) à 35 %. Depuis 2019, nous assistons à un déclin constant des cryptomineurs de type « drive-by », qui étaient le type dominant au cours des dernières années. Cette baisse, qui est alignée sur la valeur décroissante de la rentabilité de l'extraction drive-by, a été accélérée par la fermeture de Coinhive en mars 2019 et de JSECoin en avril 2020.

Lucifer est une famille de cryptomineurs en pleine ascension qui a fait sa première apparition dans le classement. Lucifer est un malware multiplateforme auto-propagateur qui cible les appareils Linux et IdO, ainsi que les serveurs web Windows. Il est intéressant de noter qu'il s'agit également d'un malware hybride, intégrant plusieurs types d'attaques DDoS, de téléchargements de malwares, d'exécution de code à distance et d'extraction de la cryptomonnaie Monero.

LA LISTE SUIVANTE DES PRINCIPALES VULNÉRABILITÉS EST BASÉE SUR LES DONNÉES COLLECTÉES PAR LE SYSTÈME DE PRÉVENTION DES INTRUSIONS (IPS) DE CHECK POINT ET DÉTAILLE CERTAINES DES TECHNIQUES D'ATTAQUE ET DES EXPLOITATIONS DE VULNÉRABILITÉ LES PLUS RÉPANDUES ET INTÉRESSANTES OBSERVÉES PAR **LES CHERCHEURS DE CHECK POINT EN 2020**

INJECTION DE COMMANDE DRAYTEK VIGOR (CVE-2020-8515)

Draytek est un fabricant taïwanais d'équipements réseau et de systèmes de gestion tels que des pare-feu, des périphériques VPN et des routeurs. Draytek Vigor est une série de routeurs VPN conçus pour construire un VPN site à site avec d'autres routeurs et s'intégrer dans l'infrastructure réseau d'une organisation. En janvier, la gamme de routeurs Draytek Vigor s'est avérée exposée à une vulnérabilité critique d'exécution de code à distance, qui permet à un pirate non authentifié d'exécuter un code arbitraire en tant que racine via des métacaractères shell. Cette vulnérabilité de premier plan a été répertoriée dans les 25 principales vulnérabilités de la NSA dans la nature exploitées par des acteurs de la menace parrainés par l'État chinois. Elle a également été fortement exploitée par les cybercriminels : **selon Check Point Research, environ 27 % des organisations ont été affectées par des tentatives d'exploitation de la vulnérabilité de Draytek Vigor en 2020.**

EXÉCUTION DE CODE À DISTANCE F5 BIG-IP (CVE-2020-5902)

Le BIG-IP de F5 est un appareil réseau polyvalent populaire conçu autour de solutions de disponibilité d'applications, de contrôle d'accès et de sécurité. En juin, un défaut critique a été découvert dans l'interface utilisateur de gestion du trafic (TMUI), également appelée utilitaire de configuration, de plusieurs versions des périphériques BIG-IP de F5. Cette vulnérabilité d'exécution de code à distance permet à tout utilisateur disposant d'un accès à distance à l'interface TMUI d'exécuter des commandes système et d'obtenir un contrôle complet sur un système vulnérable. Les attaquants peuvent facilement accéder à l'interface TMUI si elle est exposée à Internet. Les chercheurs ont rapidement mis en ligne une solution pour la faille, et bien qu'une mise à jour ait été diffusée un mois après l'exposition, les attaquants ont rapidement réagi en ciblant des appareils sans correctifs. Cette vulnérabilité a été exploitée pour installer des malwares et des cryptomineurs de l'IdO ; l'US-CERT a exhorté les organisations à installer le correctif, car la faille est probablement toujours exploitée par les cybercriminels. La vulnérabilité a été répertoriée dans les 25 principales vulnérabilités de la NSA dans la nature exploitées par des acteurs de la menace parrainés par l'État chinois.

CONTOURNEMENT DE L'AUTHENTIFICATION CITRIX ADC (CVE-2020-8193)

Une vulnérabilité de premier plan a été découverte dans plusieurs produits Citrix et a été grandement exploitée par des cybercriminels en raison de sa grande pertinence pour la nouvelle normalité professionnelle due à la pandémie de COVID-19. Les produits Citrix permettent aux employés d'entreprise de collaborer à distance, quel que soit le réseau ou l'appareil. Le bogue est le résultat d'un contrôle d'accès et d'une validation des entrées incorrects, et il permet un accès non authentifié à certains points de terminaison d'URL ainsi que la divulgation d'informations aux utilisateurs à faible niveau de privilège. Citrix a publié un correctif pour remédier à ce problème et les chercheurs ont publié un scanner pour les exploitations de vulnérabilité qui se trouvent dans la nature. La vulnérabilité a été exploitée par des pirates seulement un jour après sa divulgation. Elle a également fait partie des 25 principales vulnérabilités exploitées par des acteurs de la menace parrainés par l'État chinois.

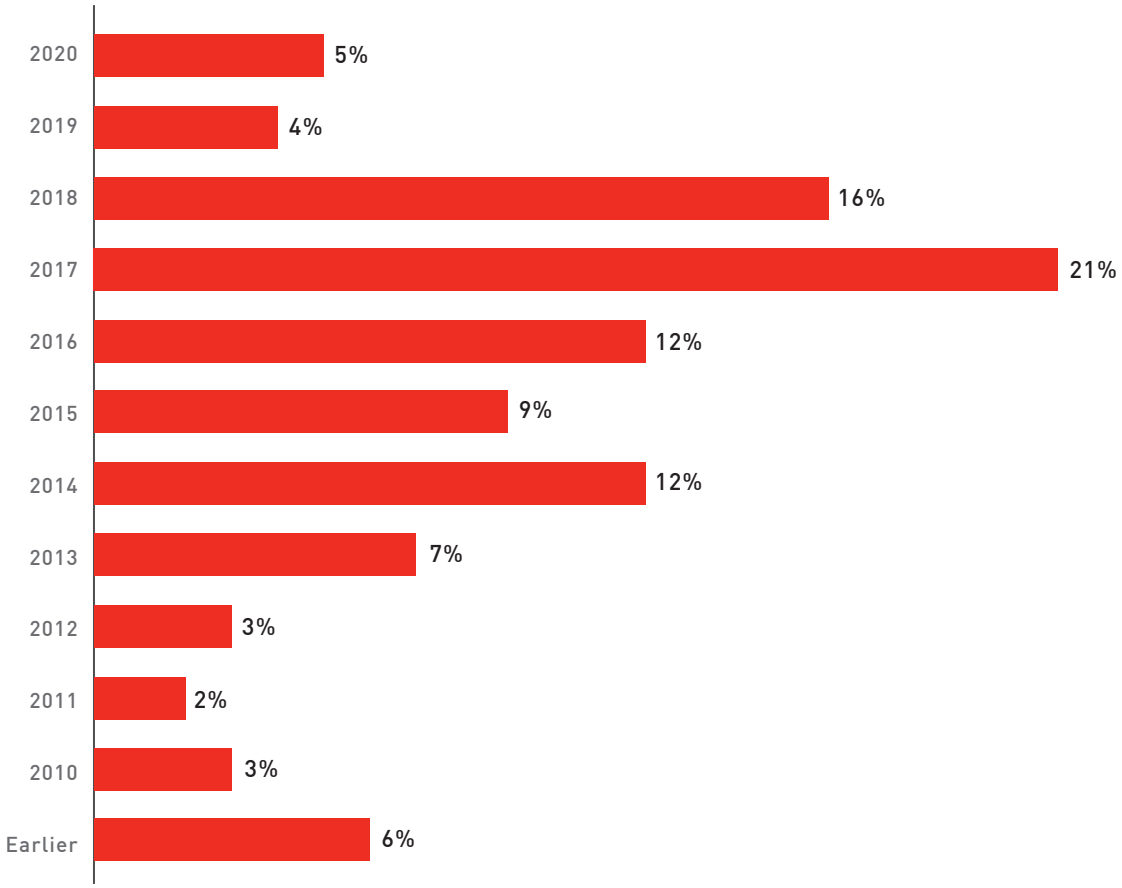


Figure 35 : pourcentage d'attaques tirant parti des vulnérabilités par année de divulgation en 2020.

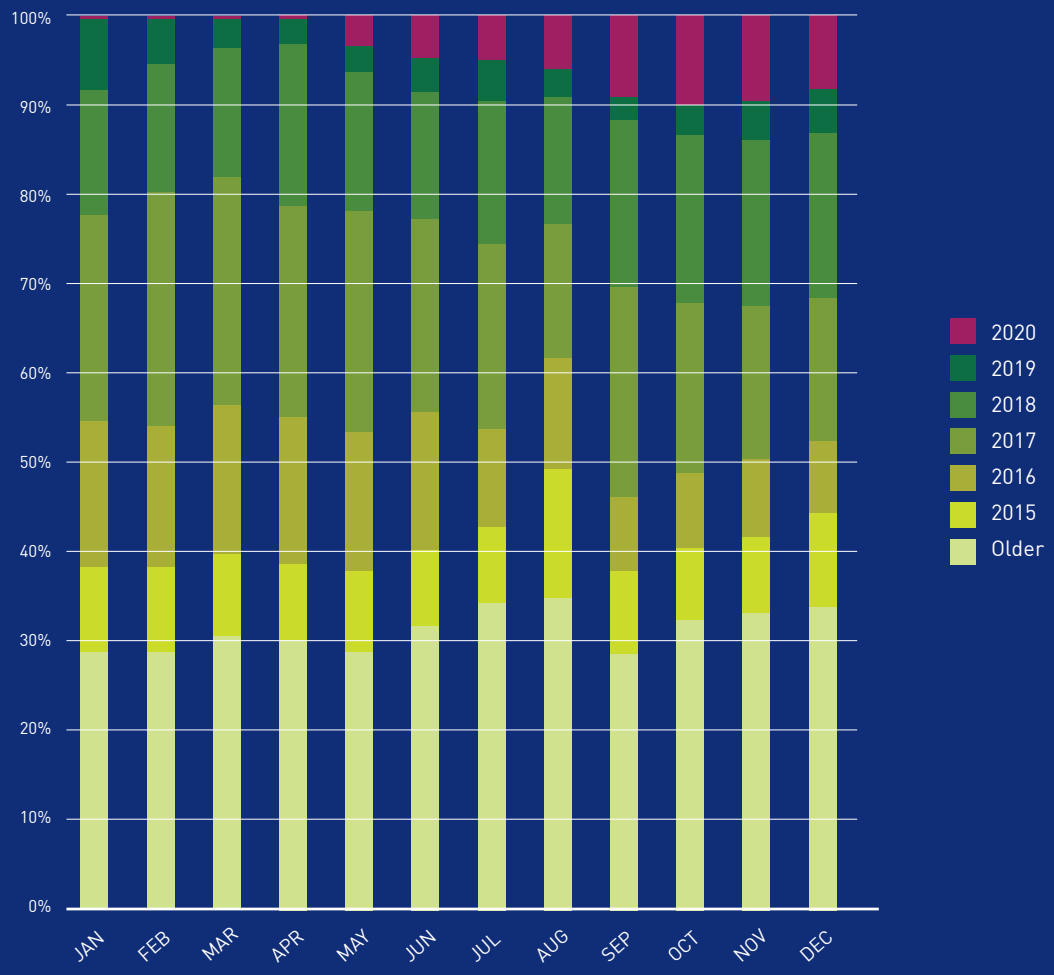


Figure 36 : pourcentage d'attaques tirant parti des vulnérabilités par année de divulgation et par mois.

Le graphique ci-dessus montre l'intégration de nouvelles vulnérabilités dans les chaînes d'exploitation au cours de l'année, et révèle comment les CVE de 2020 ont été de plus en plus exploitées par les attaquants tout au long de l'année.

Environ 80 % des attaques observées tout au long de l'année 2020 ont eu recours à des vulnérabilités signalées et enregistrées en 2017 et avant. L'année la plus importante du graphique est 2017, au cours de laquelle 21 % des vulnérabilités exploitées cette année ont été révélées. Cela nous conduit à la conclusion qu'en moyenne, il faut trois ans à une vulnérabilité pour atteindre son exploitation maximale. Alors que de nombreuses exploitations de vulnérabilités sont développées par des acteurs ou des groupes de la menace qualifiés pour un usage personnel, les vulnérabilités les plus exploitées sont celles qui ont un code de démonstration de faisabilité facilement disponible ou qui ont été intégrées dans une boîte à outils d'exploitation de vulnérabilité populaire et proposées à la vente ou à la location sur des forums clandestins.

EN 2020, LE TEMPS MOYEN NÉCESSAIRE POUR IDENTIFIER ET ENDIGUER UNE BRÈCHE INFORMATIQUE ÉTAIT DE **280 JOURS**, ET LE COÛT MOYEN D'UNE VIOLATION EN TERMES DE PERTES ET DE MESURES CORRECTIVES ÉTAIT DE PRÈS DE **4 MILLIONS USD**.

C'EST POURQUOI LA PRÉVENTION EST PRÉFÉRABLE À LA DÉTECTION.

7 RECOMMANDATIONS POUR EMPÊCHER LA PROCHAINE CYBERPANDÉMIE

Par Jony Fischbein,
CISO pour Check Point Software

PRÉVENTION EN TEMPS RÉEL

Comme nous l'avons appris dans le domaine des soins de santé, la vaccination pour empêcher l'infection est nettement plus efficace que le traitement après l'infection. Il en va de même pour votre cybersécurité. La prévention en temps réel place votre organisation dans une meilleure position pour se défendre contre la prochaine cyberpandémie.

Les organisations qui mettent l'accent sur la prévention des menaces inconnues et zero-day ont la possibilité de gagner la bataille de la cybersécurité. Les attaques provenant de menaces inconnues présentent des risques critiques pour les entreprises et, malheureusement, elles sont également les plus difficiles à contrecarrer. C'est pourquoi de nombreuses entreprises ont recours à la protection par détection uniquement. Certaines comptent sur la surveillance et la traque des menaces par les équipes du centre de sécurité des opérations pour détecter les événements une fois qu'ils ont pénétré le système. Mais il s'agit d'une stratégie beaucoup moins efficace. L'impératif stratégique pour les organisations est de prévenir les cyberattaques avant qu'elles ne contaminent les systèmes de l'entreprise.

SÉCURISEZ VOTRE ENSEMBLE

Chaque partie de la chaîne compte. La nouvelle norme introduite par la COVID-19 exige que vous repensiez et vérifiiez le niveau de sécurité et la pertinence de toutes les infrastructures et processus de votre réseau, ainsi que la conformité des appareils mobiles et des postes connectés, de même que votre flotte grandissante d'appareils de l'IdO.

L'utilisation accrue du cloud exige également un niveau de sécurité accru, en particulier dans les technologies qui sécurisent les charges de travail, les conteneurs et les applications sans serveur dans les environnements multi-cloud et hybrides.

CONSOLIDATION ET VISIBILITÉ

Les changements spectaculaires dans l'infrastructure de votre entreprise représentent une opportunité unique d'évaluer vos investissements en sécurité. Trouvez-vous vraiment ce dont vous avez besoin et vos solutions de terminaison protègent-elles les bons éléments ? Y a-t-il des domaines que vous avez négligés ?

Le plus haut niveau de visibilité sur l'ensemble de votre réseau que permet la consolidation, vous garantit l'efficacité de la sécurité nécessaire pour prévenir les cyberattaques sophistiquées. Une gestion unifiée et une visibilité des risques complètent votre architecture de sécurité. Cela peut être réalisé en réduisant vos solutions et fournisseurs de produits de terminaison, ainsi que vos coûts globaux.

SÉCURITÉ ABSOLUE ZERO-TRUST »

Avec les cybermenaces existantes à l'intérieur et à l'extérieur du périmètre de sécurité, il est devenu essentiel d'adopter une approche de type zero-trust afin de préserver la sécurité des données de l'entreprise, où qu'elles se trouvent. Dans l'ensemble du secteur, les professionnels de la sécurité passent à un mode de pensée zero-trust : par défaut, aucun appareil, utilisateur, charge de travail ou système ne peut être considéré comme fiable, que ce soit à l'intérieur ou à l'extérieur du périmètre de sécurité.

Cependant, le fait de concevoir ou de reconstruire votre infrastructure de sécurité autour de cette approche zero-trust en utilisant des solutions de terminaison, entraîne souvent des complexités dans le déploiement et la gestion, ainsi que des failles de sécurité inhérentes. Construisez une solution pratique et holistique pour mettre en œuvre l'approche zero-trust, basée sur une architecture de cybersécurité consolidée et unique qui regroupe un large éventail de fonctions et de solutions de sécurité vous permettant de déployer les sept principes du modèle de sécurité élargie zero-trust : réseaux, charges de travail, personnes, données, appareils, visibilité et analyses, automatisation et orchestration.

MAINTENEZ VOS RENSEIGNEMENTS SUR LES MENACES À JOUR

Les malwares évoluent constamment, faisant des renseignements sur les menaces un outil essentiel pour presque toutes les entreprises. Lorsqu'une organisation dispose de ressources financières, personnelles, intellectuelles ou nationales, une approche plus globale de la sécurité est la seule façon de se protéger contre les attaques de nos jours. L'une des solutions de sécurité proactives les plus efficaces disponibles aujourd'hui est le renseignement sur les menaces. Le renseignement combine des informations provenant de plusieurs sources, offrant ainsi un écran de protection plus efficace pour votre réseau. Les organisations comprennent rapidement la nécessité d'adopter un outil tel que le renseignement sur les menaces dans leur architecture de sécurité.

Pour prévenir les attaques zero-day, les organisations ont d'abord besoin d'informations incisives et en temps réel sur les menaces, qui fournissent des informations à jour sur les vecteurs d'attaque et les moyens de piratage les plus récents. Le renseignement sur les menaces doit englober toutes les surfaces d'attaque, y compris le cloud, le mobile, le réseau, les postes et l'IdO, car ces vecteurs sont courants dans une entreprise. Pour maintenir les opérations commerciales, vous avez besoin d'un renseignement complet qui stoppe de manière proactive les menaces, d'une gestion des services de sécurité pour surveiller votre réseau et d'une réponse aux incidents pour répondre rapidement aux attaques et les résoudre. Les malwares évoluent constamment, faisant des renseignements sur les menaces un outil essentiel pour presque toutes les entreprises afin de mieux se protéger.

ANNEXE

DESCRIPTIONS DES FAMILLES DE MALWARES

Agent Tesla

Actif depuis 2014, l'Agent Tesla est un cheval de Troie d'accès à distance (RAT) avancé qui fonctionne comme un enregistreur de frappes et un voleur de mot de passe. L'Agent Tesla peut surveiller et collecter la saisie du clavier et le presse-papiers du système de la victime, et peut enregistrer des captures d'écran et exfiltrer des identifiants pour une variété de logiciels installés sur la machine de la victime (y compris Google Chrome, Mozilla Firefox et le client de messagerie Microsoft Outlook). L'agent Tesla est vendu sur diverses places de marché en ligne et forums de piratage.

AZORult

AZORult est un cheval de Troie qui recueille et exfiltre des données du système infecté. Lorsque le logiciel malveillant est installé sur un système, il peut envoyer des mots de passe enregistrés, des fichiers locaux, des crypto-portefeuilles et des informations sur le profil de l'ordinateur à un serveur C&C à distance. Le générateur Gazorp, disponible sur le Dark Web, permet à quiconque d'héberger un serveur C&C AZORult avec relativement peu d'efforts.

Cerberus

Sa première apparition datant de juin 2019, Cerberus est un cheval de Troie d'accès à distance (RAT) avec des fonctions de superposition d'écran bancaire spécifiques pour les appareils Android. Cerberus opère selon un modèle de Malware-as-a-Service (MaaS), remplaçant les systèmes abandonnés comme Anubis et Exobot. Ses fonctionnalités comprennent le contrôle de SMS, l'enregistrement de frappes, l'enregistrement audio, le suivi de localisation et plus encore.

Clop

Clop est un ransomware qui a été découvert pour la première fois début 2019 et qui cible principalement les grandes entreprises. Il a été utilisé dans une attaque contre l'université néerlandaise de Maastricht, pour laquelle certains chercheurs ont établi un lien avec le groupe russe de cybercriminalité TA505. En 2020, Clop a commencé à exercer une stratégie de double extorsion où, en plus de chiffrer les données de la victime, les attaquants ont également menacé de publier des informations volées, sauf si les demandes de rançon étaient satisfaites.

Coinhive

Coinhive est un service d'extraction de cryptomonnaie, aujourd'hui abandonné mais autrefois populaire, conçu pour effectuer une extraction en ligne non autorisée de la cryptomonnaie Monero lorsqu'un utilisateur visite une page Web spécifique. Le JavaScript implanté utilise une grande quantité des ressources informatiques des machines de l'utilisateur final, ce qui a un impact sur les performances.

Danabot

Danabot est un cheval de Troie bancaire modulaire écrit en Delphi qui cible la plateforme Windows. Le malware, qui a été observé pour la première fois en 2018, est diffusé via des e-mails de spam. Une fois qu'un appareil est infecté, le logiciel malveillant télécharge le code de configuration mis à jour et d'autres modules à partir du serveur C&C. Les modules disponibles comprennent un « sniffer » pour intercepter les identifiants, un « stealer » pour voler des mots de passe à partir d'applications populaires, un module « VNC » pour le contrôle à distance, et plus encore.

DarkGate

DarkGate est un malware multifonction actif depuis décembre 2017, qui combine des capacités de ransomware, de vol d'identifiants, de RAT et d'extraction de cryptomonnaie. Ciblant principalement le système d'exploitation Windows, DarkGate emploie une variété de techniques d'évasion.

DoppelPaymer

DoppelPaymer est une variante du ransomware BitPaymer découvert en 2019. Il a été impliqué dans plusieurs attaques ciblées de haut niveau, notamment des attaques contre la ville de Florence, l'Alabama et Bretagne Télécom. Il est généralement utilisé comme étape finale après une intrusion réussie dans le réseau des victimes. DoppelPaymer cible principalement les moyennes et grandes entreprises et exige des rançons élevées. En 2020, les opérateurs de DoppelPaymer ont commencé à exercer une stratégie de double extorsion où, en plus de chiffrer les données de la victime, les attaquants ont également menacé de publier des informations volées, sauf si les demandes de rançon étaient satisfaites.

Dridex

Dridex est un cheval de Troie bancaire qui cible la plateforme Windows. Il est utilisé lors de campagnes de spam et d'exploitations de vulnérabilité, et s'appuie sur WebInjects pour intercepter et rediriger les identifiants bancaires vers un serveur contrôlé par un attaquant. Dridex contacte un serveur distant, envoie des informations sur le système infecté et peut également télécharger et exécuter des modules supplémentaires pour le contrôler à distance.

Emotet

Emotet est un cheval de Troie avancé, auto-propagateur et modulaire. Emotet était autrefois utilisé comme cheval de Troie bancaire et est maintenant utilisé comme distributeur pour d'autres campagnes ou malwares. Il utilise diverses méthodes pour maintenir les techniques de persistance et d'évasion afin d'éviter la détection. En outre, Emotet peut également être diffusé par le biais de spams de phishing contenant des pièces jointes ou des liens malveillants.

Formbook

Formbook est un infostealer ciblant le système d'exploitation Windows et a été détecté pour la première fois en 2016. Il est commercialisé sous le nom de Malware-as-a-Service (MaaS) dans des forums de piratage clandestins pour ses techniques d'évasion puissantes et son prix relativement bas. Formbook récolte les identifiants à partir de divers navigateurs, collecte des captures d'écran, surveille et consigne les frappes clavier, et peut télécharger et exécuter des fichiers selon les ordres de son C&C.

Glupteba

Connue depuis 2011, Glupteba est une porte dérobée qui a progressivement évolué pour devenir un botnet. En 2019, elle comprenait un mécanisme de mise à jour de l'adresse C&C via des listes de bitcoin publiques, une capacité de vol de navigateur intégrée et un exploiteur de routeur.

Guerrilla

Guerrilla est un cheval de Troie Android intégré à plusieurs applications légitimes et capable de télécharger des charges utiles malveillantes supplémentaires. Guerrilla génère des revenus publicitaires frauduleux pour les développeurs d'applications.

Hawkeye

Hawkeye est un logiciel malveillant infostealer pour Windows, actif depuis 2013, conçu principalement pour voler les identifiants des utilisateurs sur les appareils infectés et les distribuer à un serveur C&C. Au cours des dernières années, Hawkeye a acquis la capacité de prendre des captures d'écran, propagées via USB, en plus de ses fonctions originales de vol de mots de passe par e-mail et navigateur et d'enregistrement de frappes. Hawkeye est souvent vendu en tant que MaaS (Malware-as-a-Service).

Hiddad

Malware Android qui reconditionne les applications légitimes, puis les publie dans une boutique tierce. Sa fonction principale est d'afficher des publicités, mais elle peut également accéder aux détails de sécurité clés intégrés au système d'exploitation.

IcedID

IcedID est un cheval de Troie bancaire qui a émergé pour la première fois en septembre 2017. Il se propage par des campagnes de spam et utilise souvent d'autres malwares comme Emotet pour mieux proliférer. IcedID utilise des techniques d'évasion telles que l'injection dans les processus et la stéganographie, et vole les données financières des utilisateurs via des attaques de redirection (installation d'un proxy local pour rediriger les utilisateurs vers de faux sites clonés) et des attaques par injection sur le Web.

JSECoin

Cryptomineur basé sur le Web conçu pour effectuer une extraction non autorisée de la cryptomonnaie Monero lorsqu'un utilisateur visite une page Web spécifique. Le JavaScript implanté utilise une grande quantité de ressources informatiques des machines des utilisateurs finaux pour extraire la monnaie, ce qui a un impact sur les performances du système. JSECoin ne fonctionne plus depuis avril 2020.

KPOT

KPOT est un cheval de Troie qui cible la plateforme Windows. Ce malware vole des informations personnelles provenant de diverses sources telles que les navigateurs Web, les comptes Microsoft, les messageries instantanées, les FTP, les e-mails, les VPN, le RDP, la cryptomonnaie et les logiciels de jeu, et envoie les informations collectées au serveur distant. De plus, ce malware prend des captures d'écran et récupère les informations système de l'ordinateur infecté et les envoie à un serveur distant.

Les rapports de fin 2020 indiquent que le code source de KPOT a été acquis par le groupe de ransomwares REvil lors d'une vente aux enchères organisée sur un forum de pirates informatiques.

LokiBot

LokiBot est un infostealer largement répandu pour Windows. Il collecte des identifiants à partir d'une variété d'applications, de navigateurs, de clients de messagerie, d'outils d'administration informatique tels que PuTTY, et plus encore. LokiBot a été vendu sur des forums de piratage et on pense qu'il a divulgué son code source, permettant ainsi l'apparition d'une gamme de variantes. Il a été identifié pour la première fois en février 2016.

Lotoor

Lotoor est un outil de piratage qui exploite les vulnérabilités du système d'exploitation Android pour obtenir des privilèges racine sur les appareils mobiles compromis.

Lucifer

Lucifer est un malware hybride cryptomineur et DDOS qui exploite les vulnérabilités Windows. Le malware utilise également des attaques par force brute pour obtenir des identifiants de connexion et infecter les serveurs Windows et les PC.

Lucifer avait initialement pour cible le système Windows, mais a récemment évolué en un malware multi-plateforme et multi-architecture ciblant les appareils Linux et IdO, et dispose de versions ARM et MIPS distinctes.

Maze

Maze est un ransomware observé pour la première fois vers juin 2019 et a été le premier ransomware à appliquer la stratégie de double extorsion. Les opérateurs Maze ont ouvert une page Web dédiée où, en plus de chiffrer les données de leurs victimes, ils ont commencé à publier des informations sensibles volées aux victimes qui ont refusé de payer la rançon. De nombreux autres groupes de menaces ont suivi cette stratégie.

Mirai

Mirai est un malware bien connu de l'Internet des objets (IdO) qui suit les appareils IdO vulnérables, tels que les webcams, les modems et les routeurs, et les transforme en bots. Le botnet est utilisé par ses opérateurs pour mener des attaques massives par déni de service distribué (DDoS). Le botnet Mirai est apparu pour la première fois en septembre 2016 et a rapidement fait la une des journaux en raison de certaines attaques à grande échelle, y compris une attaque massive par déni de service DDoS utilisée pour mettre hors ligne l'ensemble du Libéria, et une attaque par déni de service DDoS contre l'entreprise d'infrastructure Internet Dyn, qui fournit une partie importante de l'infrastructure Internet des États-Unis.

MyloBot

MyloBot est un botnet sophistiqué qui a émergé pour la première fois en juin 2018 et qui est équipé de techniques d'évasion complexes, notamment des techniques anti-VM, anti-bac à sable et anti-débogage. Le botnet permet à un pirate de prendre le contrôle complet du système de l'utilisateur, en téléchargeant toute charge utile supplémentaire à partir de son C&C.

NanoCore

NanoCore est un cheval de Troie d'accès à distance qui cible les utilisateurs du système d'exploitation Windows et qui a été observé pour la première fois dans la nature en 2013. Toutes les versions du RAT contiennent des plug-ins et des fonctionnalités de base tels que la capture d'écran, l'extraction de la cryptomonnaie, le contrôle à distance du bureau et le vol de session de webcam.

Necro

Necro est un cheval de Troie compte-gouttes Android. Il peut télécharger d'autres malwares, afficher des publicités intrusives et facturer des abonnements payants de manière frauduleuse.

NRSMiner

NRSMiner est un cryptomineur qui a émergé vers novembre 2018 et qui s'est principalement propagé en Asie, en particulier au Vietnam, en Chine, au Japon et en Équateur. Après l'infection initiale, il utilise la célèbre exploitation de vulnérabilité EternalBlue SMB pour se propager à d'autres ordinateurs vulnérables dans les réseaux internes et finalement commencer à extraire la cryptomonnaie Monero (XMR).

Phorpiex

Phorpiex est un botnet (appelé Trik) qui est actif depuis 2010 et qui, au plus fort de ses activités, a contrôlé plus d'un million d'hôtes infectés. Il est connu pour diffuser d'autres familles de malwares via des campagnes de spam, ainsi que pour alimenter des campagnes de spam et de sextorsion à grande échelle.

PreAMO

PreAMo est un malware de type « clicker » pour les appareils Android, signalé pour la première fois en avril 2019. PreAMo génère des revenus en imitant l'utilisateur et en cliquant sur des publicités à son insu. Découvert sur Google Play, le malware a été téléchargé plus de 90 millions de fois sur six applications mobiles différentes.

Predator the Thief

Predator the Thief est un infostealer sophistiqué qui a été identifié au milieu de l'année 2018. Initialement conçu comme expérimentation de codage dans le développement de malwares, il s'est ensuite transformé en une menace à part entière. Predator peut extraire des mots de passe, accéder à l'appareil photo de la victime et voler des informations de portefeuilles de cryptomonnaie.

Pykspa

Un ver qui se propage en envoyant des messages instantanés aux contacts sur Skype. Il extrait les informations personnelles de l'utilisateur de la machine et communique avec les serveurs distants à l'aide d'un algorithme de génération de domaine.

Qbot

Qbot, appelé aussi Qakbot, est un cheval de Troie bancaire qui est apparu pour la première fois en 2008. Il a été conçu pour voler les identifiants bancaires et les frappes clavier d'un utilisateur.Souvent diffusé par des e-mails de spam, Qbot utilise plusieurs techniques anti-VM, anti-débogage et anti-bac à sable pour empêcher l'analyse et échapper à la détection.

Ragnar Locker

Ragnar Locker est un ransomware observé pour la première fois en décembre 2019. Il utilise des techniques d'évasion sophistiquées, dont le déploiement en tant que machine virtuelle sur des systèmes ciblés pour masquer son activité. Ragnar a été utilisé dans une attaque contre la compagnie nationale d'électricité du Portugal dans un acte de double extorsion durant laquelle les attaquants ont publié des données sensibles volées à la victime.

Ramnit

Ramnit est un cheval de Troie bancaire modulaire découvert pour la première fois en 2010. Ramnit vole des informations de session, donnant à ses opérateurs la possibilité de voler des identifiants de compte pour tous les services utilisés par la victime, y compris les comptes bancaires, les comptes d'entreprise et les comptes de réseaux sociaux. Le cheval de Troie utilise à la fois des domaines codés en dur et des domaines générés par un algorithme de génération de domaine (DGA) pour contacter le serveur C&C et télécharger des modules supplémentaires.

Remcos

Remcos est un cheval de Troie de type RAT qui est apparu pour la première fois dans la nature en 2016. Remcos se diffuse lui-même via des documents Microsoft Office malveillants, qui sont joints aux e-mails de spam, et est conçu pour contourner la sécurité UAC de Microsoft Windows et exécuter des malwares avec des privilèges de haut niveau.

RigEK

RigEK, le plus ancien et le plus connu des kits d'exploitation de vulnérabilité actuellement en service, existe depuis le milieu de l'année 2014. Ses services sont proposés à la vente sur des forums de piratage et le réseau TOR. Certains « entrepreneurs » revendent même des infections à faible volume pour les développeurs de malwares qui ne sont pas encore suffisamment importants pour se permettre d'accéder à l'intégralité du service. RigEK a évolué au fil des années pour fournir divers malwares, d'AZORult à Dridex, en passant par des ransomwares et des cryptomineurs peu connus.

RubyMiner

RubyMiner a été vu pour la première fois dans la nature en janvier 2018 et cible à la fois les serveurs Windows et Linux. RubyMiner recherche des serveurs Web vulnérables (tels que PHP, Microsoft IIS et Ruby on Rails) à utiliser pour l'extraction de cryptomonnaie, à l'aide de l'extracteur open source XMRig pour la cryptomonnaie Monero.

Ryuk

Ryuk est un ransomware utilisé par le groupe Trickbot dans des attaques ciblées et bien planifiées contre différentes organisations à travers le monde. Ce logiciel provenait à l'origine du ransomware Hermes, dont les capacités techniques sont relativement faibles, et comprend un compte-gouttes de base et un schéma de chiffrement simple. Néanmoins, Ryuk a été en mesure de causer de graves dommages aux organisations ciblées, les obligeant à payer des rançons extrêmement élevées en bitcoin. Contrairement aux ransomwares courants, systématiquement diffusés via des campagnes massives de spam et des kits d'exploitation de vulnérabilité, Ryuk est utilisé exclusivement pour des attaques personnalisées.

Sodinokibi

Sodinokibi est un Ransomware-as-a-Service qui exploite un programme « d'affiliation » et a été repéré pour la première fois dans la nature en 2019. Sodinokibi chiffre les données dans le répertoire de l'utilisateur et supprime les sauvegardes de copies fantômes pour complexifier la récupération des données. En outre, les affiliés de Sodinokibi utilisent diverses tactiques pour la diffusion, notamment par le biais de spams et d'exploitations de vulnérabilité de serveurs, ainsi que par le piratage des backends des fournisseurs de services gérés (MSP), et par le biais de campagnes publicitaires malveillantes qui redirigent vers le kit d'exploitation de vulnérabilités RIG.

Trickbot

Trickbot est un cheval de Troie bancaire modulaire qui cible la plateforme Windows et est principalement diffusé via des campagnes de spam ou d'autres familles de malwares comme Emotet. Trickbot envoie des informations sur le système infecté et peut également télécharger et exécuter des modules arbitraires à partir d'un large éventail de modules disponibles, y compris un module VNC pour le contrôle à distance et un module SMB pour la propagation dans un réseau compromis. Une fois qu'une machine est infectée, les acteurs de la menace derrière ce malware utilisent ce large éventail de modules non seulement pour voler des identifiants bancaires sur le PC ciblé, mais aussi pour le déplacement latéral et la reconnaissance de l'organisation ciblée, avant de lancer une attaque par ransomware à l'échelle de l'entreprise.

Ursnif

Ursnif est une variante du cheval de Troie bancaire Gozi pour Windows, dont le code source a été divulgué en ligne. Il dispose de capacités « man-in-the-browser » pour voler des informations bancaires et des identifiants pour les services en ligne populaires. En outre, il peut voler des informations à des clients de messagerie locaux, des navigateurs et des portefeuilles de cryptomonnaie. Enfin, il peut télécharger et exécuter des fichiers supplémentaires sur le système infecté.

Valak

Connu depuis 2019, Valak était à l'origine un logiciel compte-gouttes malveillant qui a été amélioré pour inclure des capacités de vol d'informations. Le malware se propage par le biais de campagnes de spam, souvent en répondant aux fils de discussion par e-mails avec un compte compromis. Valak est souvent diffusé avec d'autres malwares tels qu'Ursnif.

Vidar

Vidar est un infostealer qui cible les systèmes d'exploitation Windows. Détecté pour la première fois fin 2018, il est conçu pour voler des mots de passe, des données de cartes de crédit et d'autres informations sensibles dans divers navigateurs Web et portefeuilles numériques. Vidar est vendu sur divers forums en ligne et utilisé comme compte-gouttes pour télécharger le ransomware GandCrab en tant que charge utile secondaire.

WannaMine

WannaMine est un ver sophistiqué d'extraction de la cryptomonnaie Monero qui propage l'exploitation de vulnérabilité EternalBlue. WannaMine implémente un mécanisme de propagation et des techniques de persistance en exploitant les abonnements aux événements permanents WMI (Windows Management Instrumentation).

xHelper

xHelper est un malware Android qui affiche principalement des publicités contextuelles intrusives et des spams de notification. Il est très difficile à supprimer une fois installé, en raison de ses capacités de réinstallation. Observé pour la première fois en mars 2019, xHelper a maintenant infecté plus de 45 000 appareils.

XMRig

XMRig est un logiciel open source d'extraction de processeur utilisé pour extraire la cryptomonnaie Monero. Les acteurs de la menace abusent souvent de ce logiciel open source en l'intégrant à leur malware pour mener des activités d'extraction illégales sur les appareils des victimes.

Zeus

Zeus est un cheval de Troie Windows largement diffusé qui est principalement utilisé pour voler des informations bancaires. Lorsqu'une machine est compromise, le logiciel malveillant envoie des informations telles que les identifiants de compte aux attaquants à l'aide d'une chaîne de serveurs C&C.

Zloader

Zloader est un malware bancaire qui utilise des injections Web pour voler des identifiants et des informations privées, et qui peut extraire des mots de passe et des cookies du navigateur de la victime. Il télécharge le VNC qui permet aux pirates de se connecter au système de la victime et d'effectuer des transactions financières à partir de l'appareil de l'utilisateur. Repéré pour la première fois en 2016, le cheval de Troie est basé sur une fuite de code du malware Zeus de 2011. En 2020, ce malware était très populaire parmi les pirates et comprenait de nombreuses variantes.

L'indice global d'impact des menaces de Check Point et sa carte ThreatCloud s'appuient sur les renseignements ThreatCloud de Check Point, le plus grand réseau collaboratif de lutte contre la cybercriminalité qui fournit des données sur les menaces et les tendances des attaques à partir d'un réseau mondial de capteurs de menaces. La base de données ThreatCloud inspecte plus de 3 milliards de sites Internet et 600 millions de fichiers par jour, et identifie plus de 250 millions d'activités de malwares chaque jour.

cp<r>
CHECK POINT RESEARCH

CONTACTEZ-NOUS

SIÈGE SOCIAL MONDIAL

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

SIÈGE SOCIAL AUX ÉTATS-UNIS

959 Skyway Road, Suite 300, San Carlos, Californie 94070
Tél. : +1 800 429 4391 | +1 650 628 2000 | Fax : +1 650 654 4233

VOUS ÊTES ATTAQUÉS ?

Contactez notre équipe de réponse aux incidents :
emergency-response@checkpoint.com

PODCAST CHECK POINT RESEARCH

Connectez-vous à cp<radio> pour découvrir les dernières recherches de CPR, ainsi que les coulisses et d'autres contenus exclusifs.
Rendez-nous visite sur https://research.checkpoint.com/category/cpradio/

WWW.CHECKPOINT.COM