Acronis

Rapport 2020

Rapport d'Acronis sur les cybermenaces 2020

Les tendances de cybersécurité en 2021, l'année de l'extorsion

Acronis
Rapport sur les cybermenaces 2020

Sommaire

AUTEURS :

Alexander Ivanyuk

Directeur du positionnement des produits et des technologies, Acronis

Candid Wuest

Vice-président de la recherche sur la cyberprotection, Acronis

Introduction et résumé

Acronis a été la première entreprise à implémenter une cyberprotection complète et intégrée pour protéger toutes les données, toutes les applications et tous les systèmes. La cyberprotection exige de mener des recherches sur les menaces, de les surveiller, mais aussi de respecter les cinq éléments de la cyberprotection — fiabilité, accessibilité, confidentialité, authenticité et sécurité. Dans le cadre de cette stratégie, nous avons mis en place trois centres d'opérations de cyberprotection (CPOC) dans le monde afin de surveiller et d'étudier les cybermenaces 24 heures sur 24 et 7 jours sur 7.

Nous avons également mis à niveau nos produits phares : Acronis Cyber Protect Cloud, lequel fait partie de la plate-forme Acronis Cyber Cloud destinée aux fournisseurs de services, et Acronis Cyber Protect 15, une solution sur site. Avant de lancer ces nouvelles éditions, Acronis était déjà l'un des leaders du marché de la cyberprotection grâce à sa technologie anti-ransomware innovante Acronis Active Protection, sans cesse améliorée pour démontrer le savoir-faire unique d'Acronis en matière de neutralisation des menaces ciblant les données. Il faut souligner également que les technologies basées sur l'intelligence artificielle et l'analyse comportementale développées par Acronis en 2016 ont évolué afin de détecter et de neutraliser toutes les formes de malwares et autres menaces potentielles.

Ce rapport s'intéresse au paysage des menaces observées par nos capteurs et analystes en 2020.

Les données sur les malwares présentées dans ce rapport ont été collectées entre juin et octobre 2020, après le lancement d'Acronis Cyber Protect en mai 2020, et reflètent les menaces ciblant les terminaux détectées au cours de ces derniers mois.

Ce rapport offre une vue globale des menaces et se fonde sur les données recueillies auprès de plus de 100 000 terminaux disséminés dans le monde entier. Seules les menaces ciblant les systèmes d'exploitation Windows sont présentées dans ce rapport, car leur prévalence est de loin supérieure aux menaces visant les systèmes macOS. Nous continuerons de surveiller de près l'évolution de la situation et, au besoin, nous inclurons des données sur les menaces macOS dans le rapport de l'année prochaine.

LES 5 CHIFFRES CLÉS DE L'ANNÉE 2020 :

- **31 %** des multinationales ont été attaquées par des cybercriminels au moins une fois par jour.
- Le ransomware Maze est impliqué dans près de **50 %** de toutes les attaques par ransomware ayant été détectées.
- Plus de **1 000** entreprises ont constaté des fuites de données après des attaques par ransomware.
- Microsoft a corrigé quelque **1 000** vulnérabilités dans ses produits en l'espace de neuf mois.
- La durée de vie moyenne d'un échantillon de malware est de **3,4** jours.

PRINCIPALES TENDANCES DE CYBERSÉCURITÉ EN 2021 :

- Les attaques visant les collaborateurs en télétravail ne feront qu'augmenter.
- L'exfiltration de données va supplanter le chiffrement de données.
- Les attaques contre les fournisseurs de services managés, les petites entreprises et le Cloud vont se multiplier.
- Les ransomwares se chercheront de nouvelles cibles.
- Les cybercriminels vont se tourner davantage vers l'automatisation et le nombre d'échantillons de malware va augmenter.

THÈMES ABORDÉS DANS CE RAPPORT :

- Principales tendances observées en 2020 en matière de sécurité et de menaces
- Statistiques sur les malwares et aperçu des principales familles
- Statistiques sur les ransomwares accompagnées d'une analyse approfondie des menaces les plus dangereuses
- Raisons pour lesquelles la divulgation de données confidentielles représente la deuxième étape des attaques par ransomware les plus fructueuses
- Principales vulnérabilités contribuant à la réussite des attaques
- Raisons pour lesquelles les fournisseurs de services managés sont de plus en plus ciblés
- Nos prévisions et recommandations pour 2021

1re partie

Principales cybermenaces et tendances de 2020

1. Exploitations sur le thème de la COVID-19
2. Le télétravail en ligne de mire
3. Les fournisseurs de services managés, nouvelle cible de choix des cybercriminels
4. Les ransomwares toujours en tête du classement des menaces
5. Les simples solutions de sauvegarde et de sécurité ne suffisent plus

La pandémie de COVID-19, apparue à la toute fin de l'année 2019, a eu des conséquences dramatiques sur la vie de tous les habitants de la planète. Outre les dangers flagrants posés à la santé humaine et l'impact économique majeur de cette pandémie, celle-ci a bouleversé le monde numérique, nos habitudes de travail et nos activités de loisir en ligne.

Avec l'arrêt des voyages, la plupart des entreprises et des services ont été obligés de passer aux opérations en ligne. Ceux qui avaient déjà une présence en ligne ont dû développer leur infrastructure, tandis que d'autres ont dû mettre en place de tout nouveaux processus. Qu'il s'agisse des administrations publiques, du secteur médical ou des sociétés de services, tous se sont vus contraints d'adopter un nouvelle approche afin de satisfaire les besoins quotidiens.

Les réunions de travail ont migré vers des applications de télécommunication telles que Zoom, Webex et Microsoft Teams, qui sont devenues la nouvelle norme. Les collaborateurs ont été renvoyés dans leurs foyers, souvent dans l'urgence et sans le support approprié, et ont dû, dans de nombreux cas, avoir recours à leur propre matériel pour effectuer leur travail.

Malheureusement, les cybercriminels ont vu dans ces nouveaux défis une magnifique aubaine dont ils n'ont pas hésité à profiter pour multiplier leurs attaques, au mépris de toute compassion humaine.

1. Exploitations sur le thème de la COVID-19

Comme il fallait s'y attendre, les gens se sont précipités sur leurs terminaux pour avoir des informations en ligne sur la pandémie : les mesures à prendre pour s'en prémunir, les dernières nouvelles, l'assistance sur laquelle ils peuvent compter, etc. Cet intérêt a donné lieu à une multitude d'arnaques et autres exploits.

Les cybercriminels continuent d'user et d'abuser des mêmes vieilles méthodes pour exploiter le thème de la COVID-19 dans leurs cyberattaques, en incitant les victimes à communiquer leurs identifiants ou informations personnelles sur une page Web de phishing, ou en incorporant des charges actives malveillantes dans des documents censés contenir des renseignements essentiels sur la pandémie. D'autres arnaques notables sur le thème de la COVID-19 ont connu un beau succès. En voici quelques exemples.

Faux tests gratuits

La dernière version du malware Trickbot/Qakbot/Qbot s'est propagée via de nombreux e-mails de phishing proposant des tests COVID-19 gratuits. Les victimes étaient invitées à compléter un formulaire joint qui était en réalité un faux document incorporant un script malveillant. Pour éviter de révéler sa charge active lors de l'analyse antimalware en sandbox, le script ne commençait à la télécharger qu'après un certain délai.

Le document de leurre utilise un subterfuge standard pour inciter les utilisateurs à cliquer sur l'option d'activation de contenu, laquelle permet l'exécution du script VBA malveillant incorporé.

Aide financière fallacieuse

Dans de nombreux cas, les cyberattaques sont restées locales selon la gravité de la pandémie de COVID-19 dans le pays. Par exemple, le Land de Rhénanie-du-Nord-Westphalie en Allemagne a été victime d'une campagne de phishing. Les cyberpirates ont créé des copies factices du site Web du ministère de l'Économie dédié aux demandes d'aide financière liées à la COVID-19. Les cyberescrocs ont collecté les données à caractère personnel soumises par les victimes, puis ont envoyé leurs propres demandes via le site Web légitime en utilisant les informations des victimes, mais leur propre compte bancaire.

Les autorités du Land allemand ont admis avoir donné suite à près de 4 000 fausses demandes, et les escrocs sont repartis avec un butin de quelque 109 millions de dollars.

Arnaques liées à l'enseignement à distance

Les cybercriminels ont également cherché à exploiter l'enseignement à distance. Un nouvel e-mail de phishing sur le thème de la pandémie a distribué un cheval de Troie FormBook incorporé dans une fausse application de notation destinée aux enseignants. FormBook est un type de malware conçu pour voler des informations (infostealer) et capable de capturer des identifiants de connexion à partir de navigateurs Internet. Il est proposé sur les forums de piratage depuis février 2016.

Il est intéressant de noter que les cybercriminels ont employé plusieurs techniques destinées à contrer l'analyse et la détection, notamment la détection en environnement sandbox, la détection des machines virtuelles, la stéganographie et le chiffrement XOR, pour masquer la charge active et donc échapper à la vigilance de Windows Defender.

Les criminels à l'origine des campagnes FormBook s'en sont également pris aux sociétés biomédicales pour voler des ressources financières, des données à caractère personnel sensibles et du capital intellectuel.

Faux certificats médicaux

La campagne Trickbot a également exploité les craintes liées à la pandémie de COVID-19 pour distribuer un document malveillant intitulé : « Family and Medical Leave of Act 22.04.doc » (SHA256 : 875d0b66ab7252cf8fe6ab23e31926 b43c1af6dfad6d196f311e64ed65e7c0ce).

La vraie loi FMLA (Family Medical Leave Act) donne aux collaborateurs le droit de bénéficier de congés pour raisons médicales et familiales. Toutefois, dès que l'utilisateur active la macro dans ces documents frauduleux, un script malveillant commence à télécharger d'autres malwares sur l'ordinateur.

Un nouveau type de sextorsion

Nous avons observé une nouvelle forme de sextorsion. Les cybercriminels utilisent un mot de passe précédemment piraté pour convaincre leur victime, sauf que cette fois, ils menacent non pas de publier une vidéo enregistrée, mais bien la vie de l'utilisateur. Ils prétendent connaître l'adresse exacte et les habitudes de la victime. Ils déclarent en outre pouvoir « infecter toute la famille avec le coronavirus ». Pour ne pas mettre leurs menaces à exécution, ils exigent le versement de 4 000 dollars en bitcoins.

Ce n'est pas la première fois que des cyberescrocs menacent la vie des utilisateurs. Il nous est arrivé de rencontrer des cas où ils menaçaient d'envoyer des voyous pour passer les victimes à tabac, mais la menace d'infection par la COVID-19 hisse ce type d'extorsion vers de nouveaux sommets.

La plupart de ces e-mails sont envoyés depuis des adresses usurpées aléatoires ou des comptes de messagerie légitimes. Naturellement, ce type même de message constitue un indice clair qu'il s'agit d'une arnaque et qu'il vous suffit de le supprimer.

La chasse aux secrets des gouvernements et des sociétés privées concernant la COVID-19

Certaines données de valeur en rapport avec la pandémie de COVID-19 et soupçonnées par certains analystes d'avoir été gardées secrètes par le gouvernement chinois attirent les cyberpirates du monde entier. Par exemple, le groupe à la solde de l'État vietnamien APT32 (également appelé OceanLotus) aurait attaqué des organisations étatiques chinoises dans l'espoir de s'emparer des mesures de lutte contre le virus, des recherches médicales et des statistiques révélant le nombre d'infections qui n'auraient pas été divulguées par la Chine. Le Vietnam est un voisin de la Chine. Son intérêt s'explique en partie par son désir de contrôler la propagation de la pandémie dans la région.

Il semblerait que la société chinoise Huiying Medical, qui aurait développé une intelligence artificielle capable de diagnostiquer la COVID-19 par tomodensitométrie (TDM) avec une précision de 96 %, ait été victime d'un piratage. D'après la société de cybersécurité Cyble, un pirate baptisé « THE0TIME » a mis les données de Huiying Medical en vente sur le Dark Web avec des informations sur les utilisateurs, le code source et des rapports sur les tests, au prix de 4 bitcoins (environ 30 000 dollars à l'époque).

D'autres groupes cybercriminels ont lancé des attaques contre des sociétés pharmaceutiques et des laboratoires de vaccination pour s'emparer des données sur la COVID-19.

2. Le télétravail en ligne de mire

La pandémie de COVID-19 a bouleversé le paysage des menaces et mis en lumière les nombreux risques de sécurité et de confidentialité associés au télétravail, notamment l'accès distant aux serveurs d'entreprise internes, les vidéoconférences et les formations de sécurité au sein du personnel.

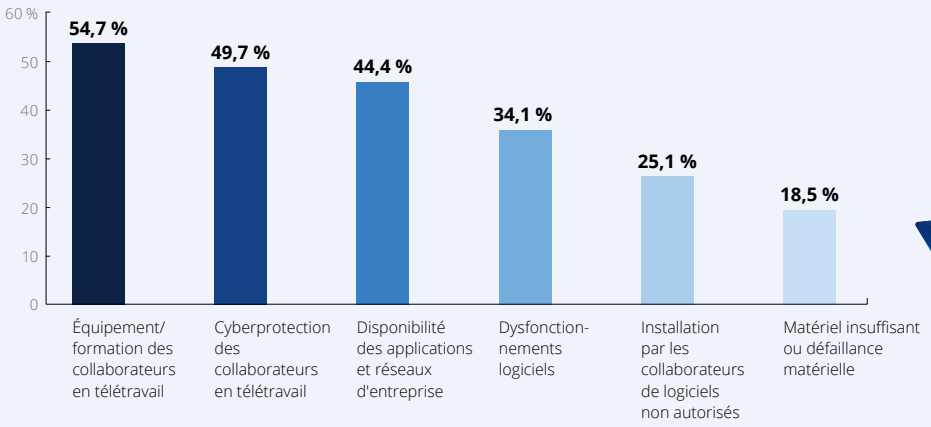
Pour évaluer la capacité des équipes informatiques à faire face à la situation, notamment les entreprises les plus aptes à migrer vers les environnements à distance et celles pouvant nettement s'améliorer, nous avons élaboré notre tout premier rapport sur la cyberpréparation. Pour les besoins de ce rapport, nous avons interrogé 3 400 entreprises et collaborateurs en télétravail partout dans le monde en juin et juillet 2020 à propos des menaces, défis et tendances qu'ils avaient remarqués depuis leur passage au télétravail. Les résultats sont alarmants :

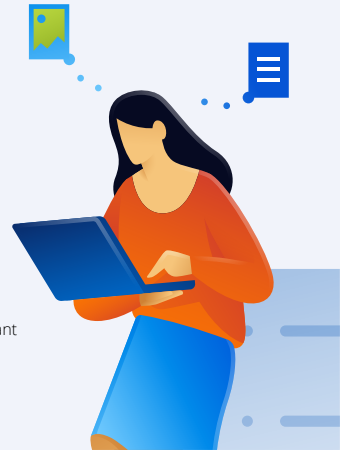
- Près de la moitié de tous les responsables informatiques ont peiné à former les collaborateurs en télétravail et à assurer leur sécurité.
- 31 % des multinationales ont été attaquées par des cybercriminels au moins une fois par jour. Les types d'attaques les plus courants ont été les tentatives de phishing, les attaques par déni de service distribué et les attaques contre les outils de vidéoconférence.
- 92 % des entreprises internationales ont dû adopter de nouvelles technologies pour passer au télétravail. En conséquence, 72 % d'entre elles ont constaté une augmentation de leurs coûts informatiques pendant la pandémie.
- Les attaques fructueuses restent fréquentes en dépit des investissements technologiques, car les entreprises ne priorisent pas correctement leurs capacités défensives.
- 39 % des entreprises ont signalé des attaques contre leurs outils de vidéoconférence pendant la pandémie.

Le défi majeur des responsables informatiques : la formation du personnel aux bonnes pratiques de télétravail

Q1. Quels sont les principaux défis techniques auxquels vous avez dû faire face pour gérer l'augmentation du nombre de collaborateurs en télétravail du fait de la pandémie ?

Acronis
Rapport sur la cyberpréparation 2020





Augmentation des attaques contre Zoom pendant la pandémie

Le début de la pandémie de COVID-19 a marqué un regain d'intérêt des cybercriminels pour la plate-forme de vidéoconférence Zoom. Compte tenu de l'augmentation massive des utilisateurs, un nombre croissant de personnes ont commencé à analyser le code de Zoom pour identifier les failles et signaler les problèmes de confidentialité.

Par exemple, Vice.com a indiqué que deux vulnérabilités jour zéro, c.-à-d. des failles de sécurité dont les éditeurs ne sont pas conscients et pour lesquelles ils ne possèdent pas de correctifs, étaient disponibles sur le Dark Web : l'une pour Windows et l'autre pour macOS. L'exploit Zoom Windows RCE (Remote Code Execution) a été mis en vente pour la somme de 500 000 dollars.

Par ailleurs, Zoom a été la cible d'une campagne de phishing visant à s'emparer d'identifiants du service. Les e-mails de phishing ont été distribués dans plus de 50 000 boîtes aux lettres. Ils ciblaient les utilisateurs de Microsoft 365 en leur envoyant une fausse invitation à une future réunion Zoom avec le service des ressources humaines afin de discuter d'une évaluation des performances (un sujet toujours stressant pour la victime et qui peut lui faire oublier la prudence de mise vis-à-vis de tels e-mails). Ces attaques de phishing, combinées aux attaques de type « credential stuffing » (recyclage d'identifiants), où les cybercriminels vérifient si l'utilisateur a employé le même mot de passe pour plusieurs services, ont conduit à la mise en vente de plus de 500 000 identifiants utilisateur Zoom sur des forums clandestins.

Un autre facteur intéressant pour les cybercriminels était l'absence de mot de passe défini pour de nombreuses vidéoconférences Zoom. Ils ont donc essayé tous les ID de réunion possibles jusqu'à trouver une session en cours. Ils ont alors rejoint la session et perturbé les participants en insérant des vidéos, du contenu musical bruyant ou simplement inapproprié. Ces intrusions ont conduit de nombreux établissements scolaires à mettre un terme à leurs programmes d'enseignement à distance.

Zoom n'est pas le seul : les utilisateurs de Microsoft 365 sont eux aussi sous le feu des attaques

Il est clair que Zoom n'a pas été le seul outil de collaboration à être pris pour cible. Des attaques similaires ont été lancées contre Microsoft Teams et Webex. Par exemple, quelque 50 000 utilisateurs de Microsoft 365 ont été attaqués en l'espace d'une semaine avec des e-mails de

phishing contenant des fausses notifications Microsoft Teams qui redirigeaient les victimes vers une page de connexion Microsoft 365 factice.

Les services de partage de fichiers Microsoft tels que Sway, SharePoint et OneNote ont eux aussi fait l'objet d'attaques au moyen de plusieurs campagnes de phishing de petite envergure ciblant des sociétés de services financiers, des cabinets juridiques et des groupes immobiliers. Une de ces attaques, baptisée PerSwaysion du fait de son exploitation des services Sway, a été exécutée en trois étapes. Elle envoie dans un premier temps des e-mails de phishing qui contiennent une pièce jointe PDF malveillante. Il s'agit d'une notification de partage de fichiers Microsoft 365 incluant un lien hypertexte « Read Now » (Lire). Lorsqu'un utilisateur clique sur le lien, ce dernier ouvre un autre document factice dans les services de partage de fichiers Microsoft (principalement Sway) avec un autre lien « Read Now » qui dirige la victime vers une fausse page de connexion Microsoft destinée à voler ses identifiants.

Manque de sécurité pour le personnel en télétravail

Maintenant que certaines personnes travaillent de leur domicile sur leur propre ordinateur, les menaces de sécurité sont omniprésentes. D'une part, ces machines personnelles ne bénéficient pas toujours d'une cyberprotection digne de ce nom et d'autre part, de nombreux utilisateurs n'appliquent pas régulièrement les derniers correctifs de sécurité pour leur système d'exploitation et les logiciels tiers populaires, ce qui expose leurs ordinateurs à de nombreux risques. Une large part de ces ordinateurs personnels ne sont pas gérés par le service informatique et échappent aux règles d'entreprise.

La résolution de ces vulnérabilités et des problèmes de gestion des correctifs à la périphérie du réseau est devenue un véritable casse-tête pour les administrateurs et les techniciens chargés d'assurer le support informatique pour aider les petites entreprises à survivre à la crise sanitaire.

En outre, les réseaux domestiques sont souvent exposés à d'autres terminaux non protégés, notamment ceux des enfants et des autres membres de la famille. Enfin, le routeur est souvent obsolète, ce qui permet aux cyberpirates de le pirater et de rediriger un trafic spécifique.

3. Les fournisseurs de services managés, nouvelle cible de choix des cybercriminels

Comme un nombre croissant de PME externalisent certains services et les confient à des fournisseurs de services managés (MSP), bon nombre de ceux-ci ont été victimes de cyberattaques. La logique est simple : au lieu de chercher à infiltrer 100 entreprises différentes, les cybercriminels n'ont qu'à pirater un MSP pour avoir accès à 100 clients. Les attaques observées en 2020 révèlent que les compromissions s'appuient sur une multitude de techniques, les logiciels d'accès à distance mal configurés représentant l'un des principaux vecteurs d'attaque. Les cybercriminels exploitent les vulnérabilités, l'absence d'authentification à deux facteurs et le phishing pour accéder aux outils de gestion des MSP et via ceux-ci aux machines de leurs clients.

Le fournisseur international de solutions et services informatiques DXC Technology a révélé une attaque par ransomware contre les systèmes de sa filiale Xchanging, par exemple. Xchanging offre principalement ses services aux compagnies d'assurance, mais sa clientèle inclut des entreprises d'autres secteurs : services financiers, aérospatial, défense, automobile, enseignement, produits de grande consommation,

santé et fabrication. Le MSP canadien Pivot Technology Solutions, dont l'infrastructure informatique a été la cible d'une cyberattaque, en est un autre exemple. Pivot Technology Solutions a été victime d'une compromission de données après une attaque par ransomware. L'incident est susceptible d'avoir affecté les informations personnelles des clients. Ce ne sont que deux exemples parmi tant d'autres des incidents survenus en 2020, et tout porte à croire qu'il vont se multiplier.

4. Les ransomwares toujours en tête du classement des menaces

Il est clair que 2020 a été l'année des ransomwares. Elle a été caractérisée par un nombre plus élevé d'attaques, des pertes plus importantes et l'implémentation de nouvelles techniques d'extorsion par les cybercriminels. De nouveaux incidents sont annoncés au public pratiquement chaque semaine. D'après un rapport publié par Coalition, un des plus importants acteurs du marché de la cyberassurance en Amérique du Nord, les attaques par ransomware représentent 41 % des déclarations de sinistre introduites au cours du premier semestre 2020. « Les ransomwares peuvent frapper tous les secteurs. Nous avons constaté une augmentation des demandes de rançon dans la plupart des secteurs que nous servons », a indiqué Coalition. C'est également ce que constate Acronis.

Pour obtenir des statistiques détaillées, consultez les données de nos centres d'opérations de cyberprotection (CPOC) dans d'autres sections de ce rapport. Ici, nous nous contentons de présenter les grandes tendances (peu réjouissantes) observées.

Des cibles majeures pour des profits décuplés

Le 18 juillet, le plus grand opérateur de télécommunications d'Argentine a été la cible d'une attaque par ransomware, probablement lancée par le groupe Sodinokibi, qui exigeait une rançon de 7,5 millions de dollars. Comme c'est souvent le cas dans le chef de cybercriminels cherchant à forcer la main aux victimes, cette demande était censée doubler si le paiement n'était pas effectué dans les 48 heures. Le ransomware avait apparemment infecté plus de 18 000 postes de travail, y compris des terminaux hébergeant des données extrêmement sensibles.

Garmin, l'une des plus importantes sociétés d'accessoires connectés, a confirmé que l'interruption de services majeure ayant débuté le 24 juillet était due à une attaque du ransomware WastedLocker. Cette attaque a contraint Garmin à suspendre toute communication avec le centre d'opérations, Garmin Connect, et même avec les lignes de production à Taïwan. Avec un chiffre d'affaires annuel estimé à 4 milliards de dollars, Garmin représente sans conteste une cible de choix. Le montant de la rançon demandée s'élevait apparemment à 10 millions de dollars. D'autres attaques WastedLocker récentes ont exigé des sommes allant de 500 000 à plusieurs millions de dollars.

La liste des victimes est longue. En février, le FBI a publié des estimations des bénéfices engrangés par certains groupes de ransomwares. Selon cette liste, des groupes comme Ryuk ont gagné près de 3 millions de dollars par mois en 2019. Avec de telles sommes, il est peu probable de voir la menace disparaître dans un avenir proche.

De plus, les familles de ransomwares actuelles exigent non seulement une rançon pour déchiffrer les données, mais aussi pour ne pas divulguer les données confidentielles volées au public, ce qui augmente encore les chances de paiement.

Demande de rançon pour éviter la divulgation des données

Le groupe de ransomwares REvil/Sodinokibi a annoncé le 14 août avoir compromis la société Brown-Forman du Kentucky — la société mère de marques de whisky telles que Jack Daniels, Old Forester, The Glendronach, ainsi que d'autres vins et spiritueux. Compte tenu des chiffres publiés dans son bilan 2020 (plus de 2 milliards de dollars de bénéfices bruts et un revenu net de 872 millions), Brown-Forman est incontestablement une cible très prisée des opérateurs de ransomwares.

Le groupe REvil a prétendu avoir volé plus d'un téraoctet de données, y compris des informations confidentielles sur les collaborateurs, des données financières, des communications internes et des contrats commerciaux. Les images publiées sur son site indiquent qu'ils sont en possession de données remontant à 2009 au moins.

Canon, la société multinationale spécialisée dans les produits optiques et d'imagerie, a été victime d'une attaque par le ransomware Maze. Celle-ci a impacté son système de messagerie, Microsoft Teams, son site Web américain et d'autres applications internes. Les opérateurs du ransomware Maze ont déclaré avoir volé plus de 10 téraoctets de données de Canon, dont certaines bases de données privées. Canon a admis avoir été victime d'une attaque dans un message interne adressé à son personnel.

CWT, l'une des plus importantes sociétés mondiales de voyages et d'organisation d'événements, a été compromise par le ransomware Ragnar Locker. Les cyberpirates se seraient emparés de 2 téraoctets de données d'entreprise sensibles et prétendent avoir compromis plus de 30 000 systèmes. Alors que les cybercriminels demandaient au départ une rançon de 10 millions de dollars pour la restitution des données volées, CWT a entamé des négociations et a finalement accepté de payer la somme de 414 bitcoins, soit plus de 4 millions de dollars à l'heure de la rédaction de ce rapport.

Conti, un nouveau service RaaS (Ransomware-as-a-Service) et le successeur de la célèbre variante Ryuk, a mis en service un site Web de publication de données dans le cadre de sa stratégie d'extorsion visant à contraindre les victimes de payer une rançon. Bien que l'activité de Conti remonte à plusieurs mois, ce n'est que récemment que les cybercriminels ont mis en service un site de divulgation de données public où ils menacent de publier les données volées en cas de non-paiement de la rançon. « Conti.News » recense actuellement 112 victimes, dont quelques grandes sociétés très en vue.

Au total, près de 20 groupes de ransomwares différents ont créé des pages dédiées pour les fuites de données, hébergées sur le réseau clandestin Tor. Plus de 700 entreprises ont ainsi vu leurs données publiées — 37 % des fuites résultant des infections par le ransomware Maze, 15 % par Conti et 12 % par Sodinokibi.

Ces compromissions de données peuvent avoir des conséquences dramatiques, notamment une atteinte à la réputation, des attaques de suivi et diverses amendes. De plus, la divulgation des données clients peut être punie par la loi en vertu de diverses réglementations sur la protection des données à caractère personnel, comme le RGPD ou la loi CCPA, et le paiement d'une rançon peut constituer un délit selon la réglementation de l'OFAC, l'organisme de contrôle financier des États-Unis.

5. Les simples solutions de sauvegarde et de sécurité ne suffisent plus

Depuis 2016, nous prédisons des attaques par ransomware contre les solutions de sauvegarde. Cette prévision résulte de projets tels que « No More Ransom », dont Acronis est membre depuis 2017 et qui encourage les individus et les entreprises à ne plus verser de rançon, mais plutôt à protéger correctement leurs machines contre les ransomwares. En effet, si vous disposez d'une sauvegarde, vous n'avez pas besoin de payer de rançon, puisqu'il vous suffit de restaurer votre système. C'était en tout cas le principe initial, mais les cybercriminels se sont rapidement adaptés. Depuis 2017, quasiment toutes les souches de ransomware ont commencé à supprimer ou à désactiver les clichés instantanés de volumes Windows et tenté de désactiver les solutions de sauvegarde classiques. Comme bon nombre de ces solutions ne disposent que de fonctions d'autoprotection limitées, voire inexistantes, cela ne leur a posé aucun problème. Le test réalisé par NioGuard, un laboratoire membre de l'organisation AMTSO, reflète cette situation alarmante.

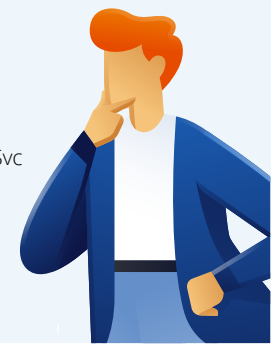
Examinons quelques exemples de ransomwares récents.

RANSOMWARE CONTI :

- Ce ransomware exige généralement des rançons inférieures à 100 000 dollars.
- Il utilise le Gestionnaire de redémarrage Windows pour fermer tous les fichiers ouverts ou non enregistrés avant le chiffrement.
- Il contient plus de 250 routines de déchiffrement de chaînes et environ 150 services qu'il est capable d'arrêter.
- Il effectue un chiffrement de fichiers rapide dans 32 threads simultanés à l'aide des ports de terminaison d'E/S Windows.
- Il suit la tendance actuelle et a récemment lancé un site de publication de données « Conti.News ».

Par ailleurs, le ransomware supprime les clichés instantanés des fichiers et redimensionne les volumes de stockage de clichés instantanés C: à H:, ce qui peut également entraîner la disparition des clichés instantanés. Il arrête également des services appartenant à SQL, aux antivirus et autres solutions de sauvegarde et de cybersécurité, tels que BackupExec et Veeam. Il tente également d'interrompre la solution Acronis Cyber Protect, mais notre fonction d'autoprotection l'en empêche. La liste contient près de 150 services, dont les suivants :

Acronis VSS Provider	BackupExecRPCService	VeeamDeploySvc
Veeam Backup Catalog Data Service	BackupExecVSSProvider	VeeamEnterpriseManagerSvc
AcronisAgent	EPSecurityService	VeeamMountSvc
AcrSch2Svc	EPUpdateService	VeeamNFSSvc
Antivirus	mozyprobackup	VeeamRESTSvc
BackupExecAgentAccelerator	VeeamBackupSvc	VeeamTransportSvc
BackupExecAgentBrowser	VeeamBrokerSvc	VeeamHvIntegrationSvc
BackupExecDeviceMediaService	VeeamCatalogSvc	Zoolz 2 Service
BackupExecJobEngine	VeeamCloudSvc	AVP
BackupExecManagementService	VeeamDeploymentService	



RANSOMWARE NETWALKER :

NetWalker est un autre exemple de ransomware découvert en août 2019. Il implémente le modèle RaaS et cible les entreprises comme les particuliers. Depuis mars 2020, le groupe a réussi à extorquer environ 25 millions de dollars. La caractéristique de la version la plus récente de NetWalker est l'utilisation d'un chargeur PowerShell parfaitement masqué qui démarre le ransomware sur un système infecté. L'utilisation d'un script PowerShell ou, en général, l'exploitation des outils préinstallés sans laisser d'empreinte (« living-off-the-land »), reste une pratique répandue au sein de la communauté cybercriminelle.

À l'instar de nombreuses autres souches de ransomware, NetWalker supprime les clichés instantanés des fichiers Windows.

```
Get-Wmiobject Win32_Shadowcopy | ForEach-Object {$_.Delete();} | Out-Null
```

NetWalker tente également d'arrêter les services de sauvegarde qui commencent par les chaînes suivantes afin d'empêcher toute restauration :

veeam*	ShadowProtectSvc	StorageCraft ImageManager
backup*	AcronisAgent	acrsch2svc*
backup	AcrSch2Svc	

2e partie

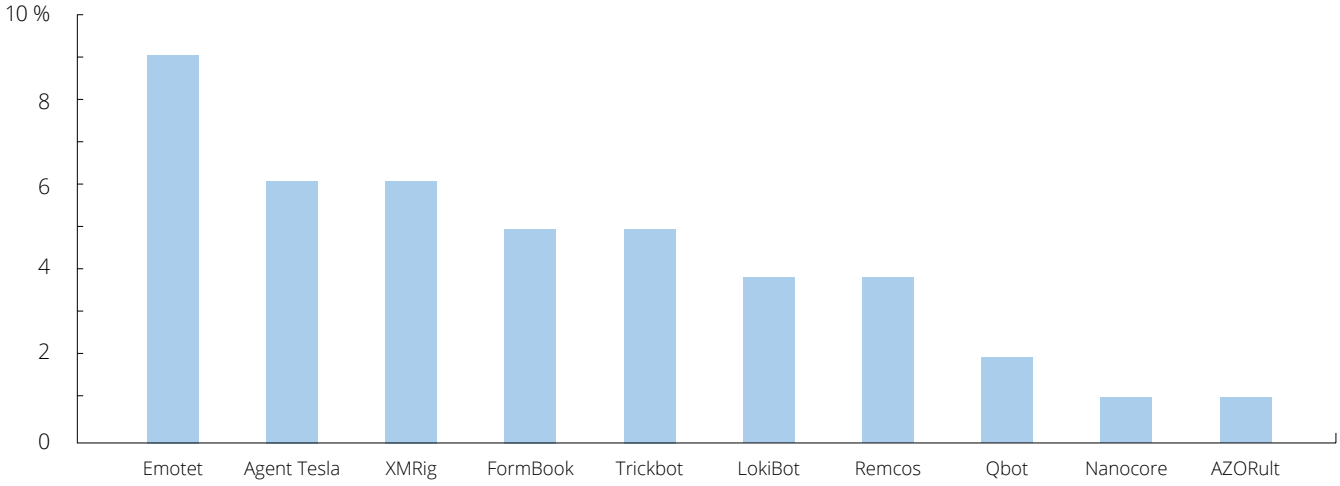
Menace posée par les malwares en général

Au cours du 3e trimestre 2020, environ 11 % de nos clients ont été victimes d'au moins une attaque par malware qu'ils ont réussi à bloquer. Les chiffres sont revenus progressivement à la normale depuis le début de la pandémie. En juillet, ils étaient 14,7 % à avoir été victimes d'une attaque, 10,1 % en août, 8,9 % en septembre et 6,7 % en octobre.

Les États-Unis étaient le pays affichant le pourcentage le plus élevé de détections de malwares au 3e trimestre 2020 avec 27,9 %, suivis par l'Allemagne (16,7 %) et le Royaume-Uni (6,1 %).

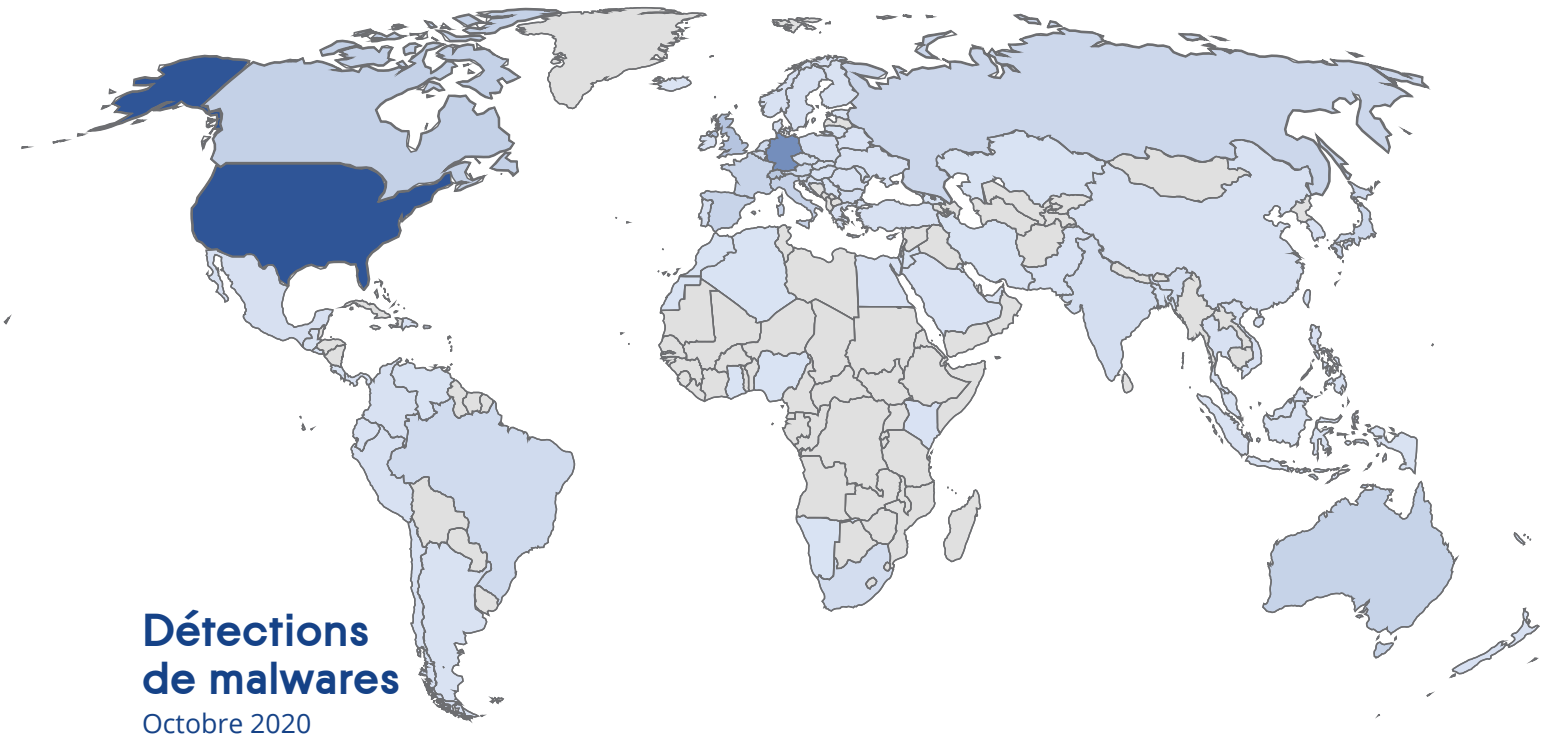
Le laboratoire indépendant AV-Test a recensé 400 000 nouveaux échantillons de malware par jour au 3e trimestre 2020, ce qui montre clairement que les cybercriminels automatisent leurs processus et génèrent une multitude de nouvelles menaces liées aux malwares. Toutefois, la plupart d'entre elles sont utilisées pour quelques attaques seulement et sur une période très courte. Parmi les échantillons que nous avons recensés, 19 % ont été observés une seule fois. La durée de vie moyenne d'un échantillon malveillant est de 3,4 jours, avant de disparaître à jamais.

Voici les 10 principales familles de malwares recensées et suivies en 2020 :



Pourcentage mensuel des détections globales par pays

PAYS	OCT. 2020	SEPT. 2020	AOÛT 2020	JUILLET 2020
États-Unis	27,5 %	27,9 %	29,3 %	16,4 %
Allemagne	18,4 %	16,7 %	16,8 %	4,3 %
Suisse	7,2 %	5,4 %	3,6 %	3,2 %
Royaume-Uni	5,9 %	6,1 %	6,4 %	4,5 %
Canada	3,0 %	3,6 %	3,6 %	1,5 %
France	3,0 %	2,9 %	3,3 %	2,3 %
Italie	3,0 %	3,2 %	3,3 %	1,7 %
Australie	3,0 %	3,3 %	3,1 %	2,0 %
Espagne	2,6 %	3,0 %	2,8 %	4,2 %
Japon	2,0 %	2,3 %	3,2 %	15,7 %



Détections de malwares

Octobre 2020

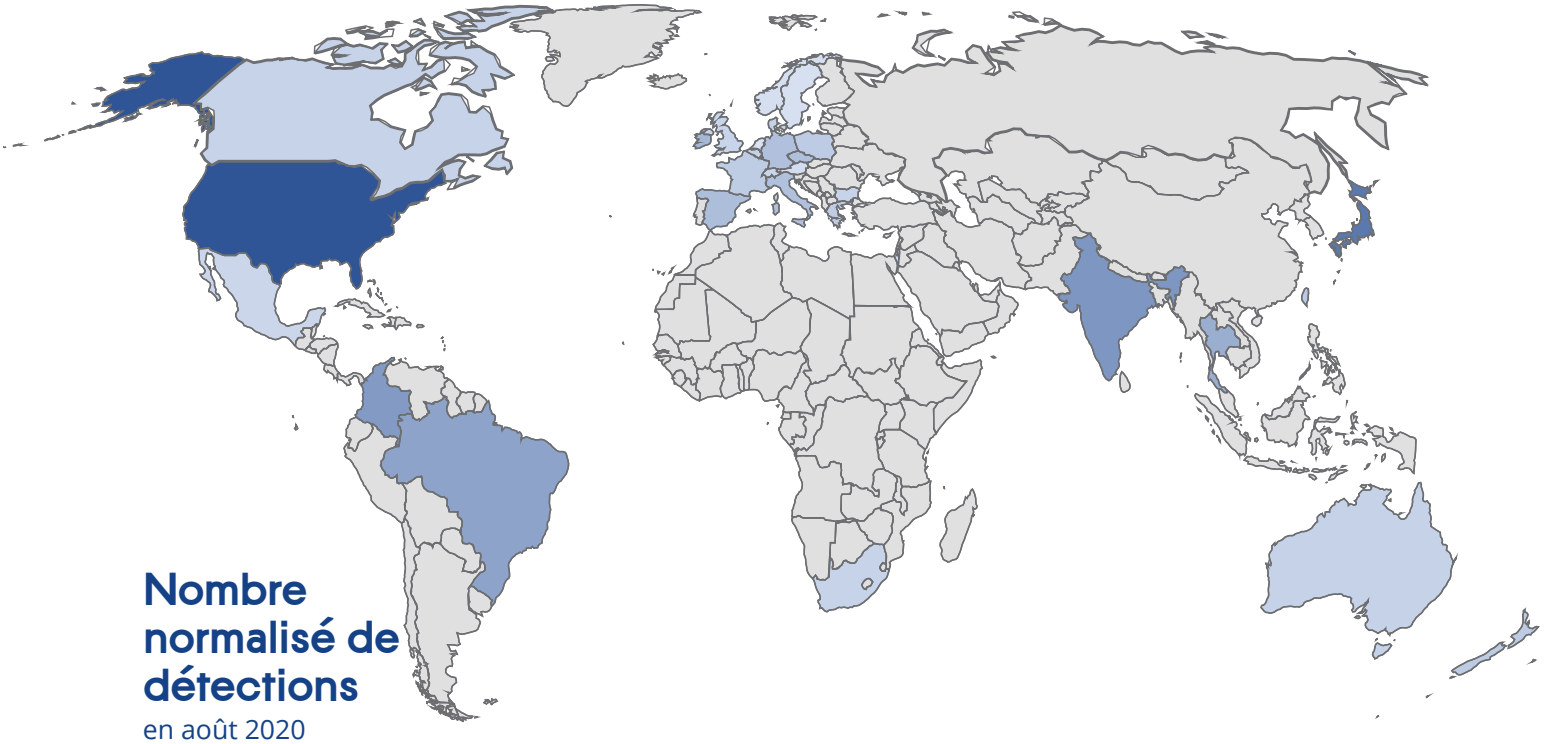
Pourcentage

0 % 0,27 %

Si nous normalisons le nombre de détections par client actif et par pays, la distribution est légèrement différente. Le tableau suivant illustre le nombre de détections recensées pour 1 000 clients par pays. Il montre clairement que les cybermenaces sont un phénomène planétaire.

CLASSEMENT	PAYS	DÉTECTIONS DE MALWARES pour 1 000 clients en août
1	États-Unis	2 059
2	Japon	1 571
3	Inde	1 168
4	Colombie	1 123
5	Brésil	994
6	Thaïlande	856
7	Irlande	729
8	Espagne	634
9	République tchèque	611
10	Allemagne	601
11	Italie	589

CLASSEMENT	PAYS	DÉTECTIONS DE MALWARES pour 1 000 clients en août
12	Hong Kong	518
13	Taïwan	480
14	Nouvelle-Zélande	462
15	Pologne	453
16	France	444
17	Grèce	437
18	Danemark	375
19	Australie	361
20	Belgique	358
21	Afrique du Sud	351
22	Bulgarie	351
23	Canada	347
24	Royaume-Uni	329
25	Suisse	311



Nombre normalisé de détections
en août 2020

Nombre de détections pour 1 000 clients

131 2 059

Menace posée par les ransomwares

Comme nous l'avons déjà mentionné dans la section consacrée aux principales tendances, les ransomwares restent en tête du classement des cybermenaces pesant sur les entreprises. Même si nous avons commencé à observer des ransomwares en 2017 lors du développement initial d'Acronis Active Protection, cette section se concentre sur les données collectées entre le 1er janvier et le 31 octobre 2020.

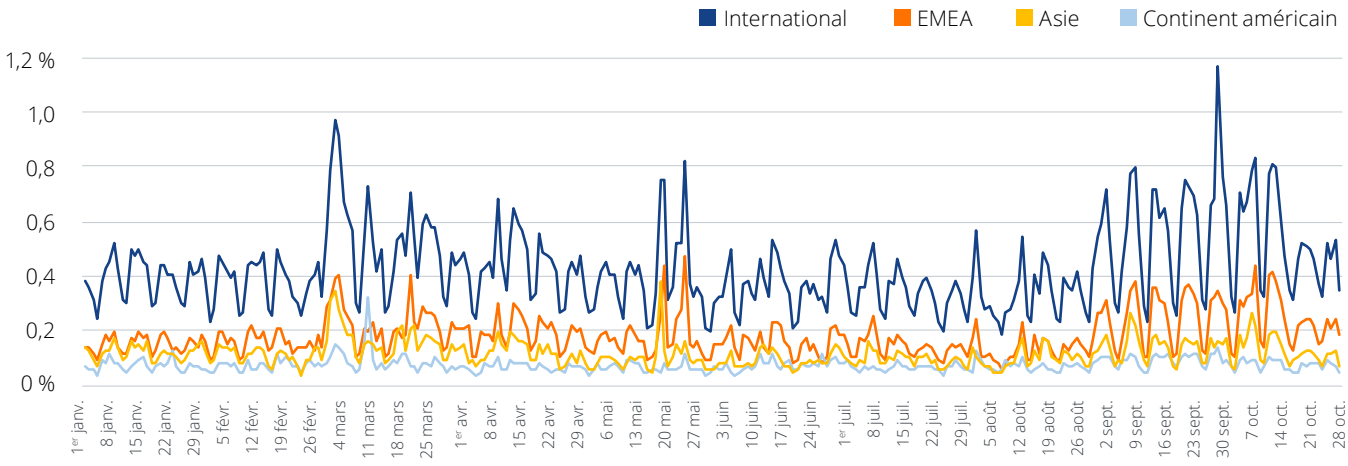
Voici les 10 principales familles de ransomwares recensées et suivies en 2020. Rappelez-vous que certains groupes tentent d'infecter autant d'utilisateurs finaux que possible par le biais d'une attaque de grande envergure, tandis que d'autres se concentrent sur les cibles de valeur et ne cherchent à infecter qu'un nombre limité de victimes beaucoup plus rentables. Dès lors, le volume de détections d'une menace à lui seul n'est pas représentatif du danger présenté par celle-ci.

1. Maze
2. REvil/Sodinokibi
3. SNAKE (EKANS)
4. Nemty
5. NetWalker (également appelé Mailto)
6. Ragnar Locker
7. MegaCortex
8. CLOP
9. DoppelPaymer
10. Thanos

Ces neuf derniers mois, nous avons observé l'émergence d'une cinquantaine de nouvelles familles de ransomwares. Il s'agit pour certaines de groupes plus petits qui se concentrent sur les particuliers, mais la tendance des nouvelles familles comme Avaddon, Mount Locker et SunCrypt est de cibler les entreprises plus rentables. Un nombre croissant de ces groupes sont actifs dans le secteur du RaaS et jouent le rôle de redistributeurs de menaces préétablies. Cela donne lieu à un taux de distribution encore plus élevé de ransomwares connus.

Détections quotidiennes de ransomwares

Cette année, nous avons constaté une hausse très nette partout dans le monde au début du confinement dû à la COVID-19 en mars. Depuis lors, l'activité des ransomwares est restée plus élevée qu'en temps normal. En ce qui concerne les zones géographiques ou les secteurs les plus ciblés, nous n'avons observé aucune exception : tous les secteurs sont visés par des attaques. En septembre, nous avons commencé à observer une autre vague d'attaques par ransomware, surtout à l'encontre des secteurs de l'enseignement et de la fabrication en Amérique du Nord.



10 pays les plus touchés : détections de ransomwares par région

Asie :

PAYS	% de détections de ransomwares par région au 3e trim. 2020
Japon	17,7 %
Philippines	13,3 %
Taïwan	9,6 %
Chine	8,6 %
Inde	7,8 %
Turquie	5,4 %
Iran	5,3 %
Corée du Sud	3,9 %
Indonésie	3,7 %
Thaïlande	3,6 %

EMEA :

PAYS	% de détections de ransomwares par région au 3e trim. 2020
Allemagne	17,7 %
France	13,3 %
Italie	9,6 %
Royaume-Uni	8,6 %
Suisse	7,8 %
Espagne	5,4 %
Autriche	5,3 %
Pays-Bas	3,9 %
Belgique	3,7 %
République tchèque	3,6 %

Continent américain :

PAYS	% de détections de ransomwares par région au 3e trim. 2020
États-Unis	67,3 %
Canada	15,9 %
Chili	4,7 %
Brésil	3,0 %
Mexique	2,7 %
Colombie	1,7 %
Pérou	1,0 %
Argentine	0,8 %
Bolivie	0,4 %
Équateur	0,3 %

Les groupes de ransomwares les plus en vue

Le ransomware Maze furtif chiffre et vole des téraoctets de données privées dans le cadre d'attaques ciblées.

Le ransomware Maze a été au centre de plusieurs attaques ciblées, et ce depuis mai 2019 au moins. Il serait responsable de la dernière attaque contre Canon le 30 juillet 2020, qui s'est traduite par une panne du service de stockage Cloud « image.canon ». Qui plus est, l'opérateur du ransomware Maze prétend s'être emparé de 10 téraoctets de données privées au cours de l'attaque contre Canon. Il a déjà publié les données des entreprises Xerox et LG volées lors d'une attaque en juin 2020, comme les sociétés refusaient de payer la rançon.

- **Le ransomware ne se contente pas de chiffrer les données. Il les vole également pour les publier ultérieurement en cas de non-paiement de la rançon.**
- **Canon, Xerox et LG font partie des plus importantes victimes de Maze.**
- **Il a recours à des techniques destinées à contrer le désassemblage et le débogage.**
- **Il ne chiffre pas les systèmes avec des paramètres régionaux russes par défaut.**
- **L'appel wmic.exe pour supprimer les clichés instantanés est masqué.**
- **Il envoie une demande de connexion (check-in) HTTP à un serveur C&C situé sur le réseau 91.218.114.0 à Moscou en Russie.**
- **Il utilise les outils de piratage Mimikatz, ProcDump et Cobalt Strike pour se propager.**

Le ransomware Maze est généralement distribué dans le cadre d'une attaque ciblée contre une entreprise qui commence par l'envoi d'un e-mail de spear-phishing (harponnage), l'obtention d'un accès via une connexion RDP ou VDI compromise (les identifiants sont généralement achetés sur le Dark Web), et l'exploitation de vulnérabilités dans les réseaux VPN.

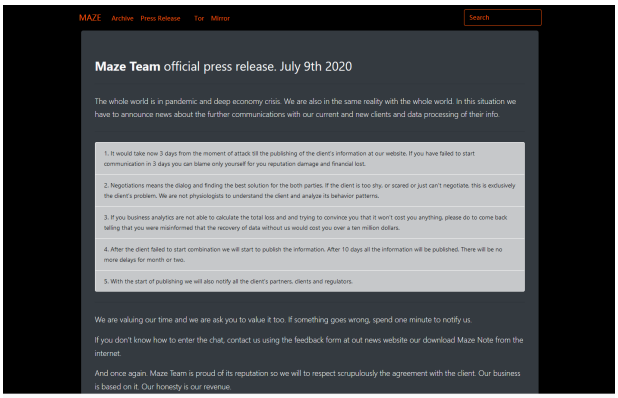
Dès que l'opérateur obtient l'accès au réseau interne de l'entreprise, Maze exécute Mimikatz et ProcDump pour collecter les mots de passe stockés en mémoire et passe à l'étape de reconnaissance à l'aide de l'outil Cobalt Strike (utilisé par les Red Teams dans les tests de cybersécurité).

Maze utilise des techniques destinées à empêcher le désassemblage pour compliquer l'analyse de code dans un désassembleur.

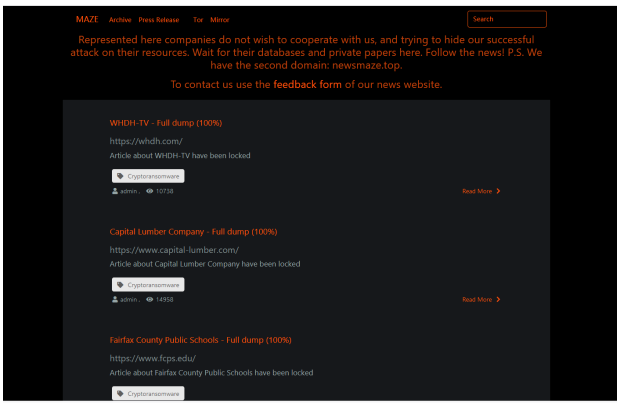
Les techniques de dissimulation incluent les suivantes :

1. **Sauts conditionnels qui redirigent vers le même emplacement et remplacent les sauts absolus**
2. **Suivi des appels par l'envoi (push) de l'adresse de retour à la pile et par un saut jusqu'à l'adresse de l'appelant**

En outre, Maze peut détecter si son code est soumis à un débogage. Il vérifie l'indicateur « BeingDebugged » dans la structure PEB si le processus est exécuté sous un débogueur. Si c'est le cas, le code tourne en boucle infinie et ne procède à aucun chiffrement. De plus, Maze arrête les processus des outils bureautiques et d'analyse antimalware par le hachage des noms des processus.



Le ransomware Maze est similaire aux souches récentes de ransomware telles que WastedLocker, NetWalker et REvil en cela qu'il ne se contente pas



de chiffrer les données, mais les vole aussi. Il utilise l'utilitaire 7-Zip pour compresser les données collectées et exfiltrer les archives vers le serveur FTP du cyberpirate à l'aide du client WinSCP. Dans certains incidents, les données exfiltrées auraient été codées en Base64.

Toutes ces caractéristiques font de Maze l'un des ransomwares les plus dangereux de 2020.

Le ransomware DarkSide n'attaque pas les hôpitaux, les établissements scolaires ni les services publics.

DarkSide est une nouvelle souche de ransomware. Les attaques ont commencé au début du mois d'août 2020. Elles auraient été lancées par les anciens affiliés d'autres campagnes de ransomware qui, après s'être enrichis dans le marché de l'extorsion, ont décidé de développer leur propre code. D'après les incidents rapportés, la rançon demandée varie entre 200 000 et 2 millions de dollars. À l'instar d'autres ransomwares utilisés dans des attaques ciblées, DarkSide ne se limite pas à chiffrer les données utilisateur, mais exfiltre aussi les données des serveurs compromis.

Toutefois, à la différence de Maze qui s'en est pris à des écoles du district scolaire de Newhall et du comté de Fairfax, le code de conduite de DarkSide lui interdit d'attaquer les hôpitaux, les établissements scolaires et les services publics.

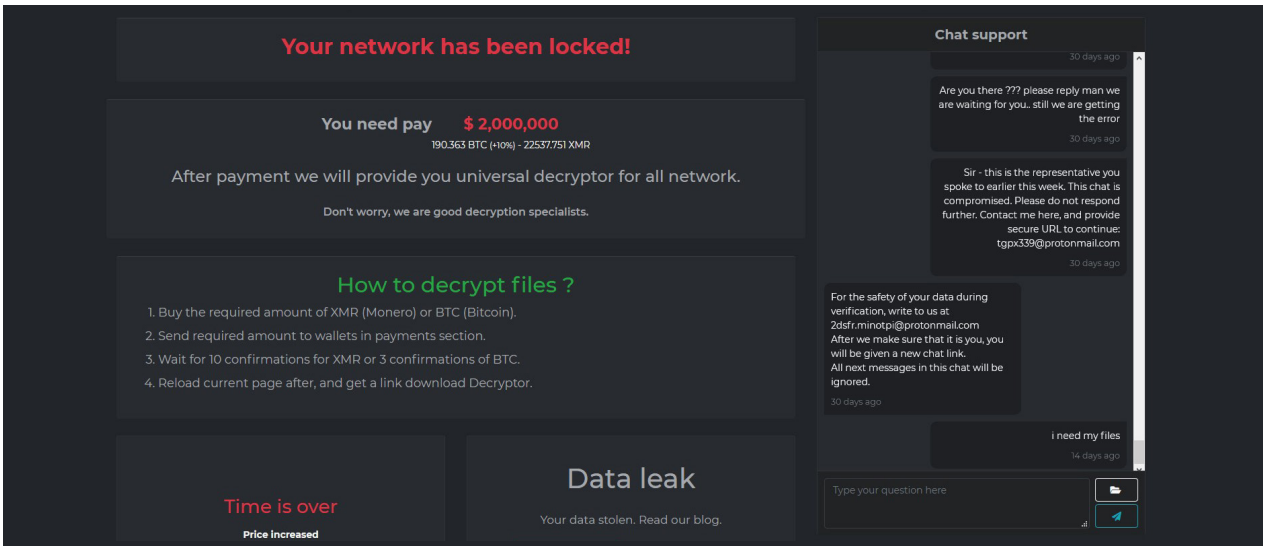
- **DarkSide a été découvert en août 2020.**
- **Il cible uniquement les pays anglophones et évite les pays de l'ancien bloc soviétique.**
- **Il ne s'en prend pas aux hôpitaux, aux maisons de repos, aux établissements scolaires, aux universités, aux organisations sans but lucratif ni au secteur public.**
- **Il utilise les algorithmes de chiffrement RSA-1024 et Salsa20 avec une matrice personnalisée.**
- **Les rançons varient entre 200 000 et 2 millions de dollars.**

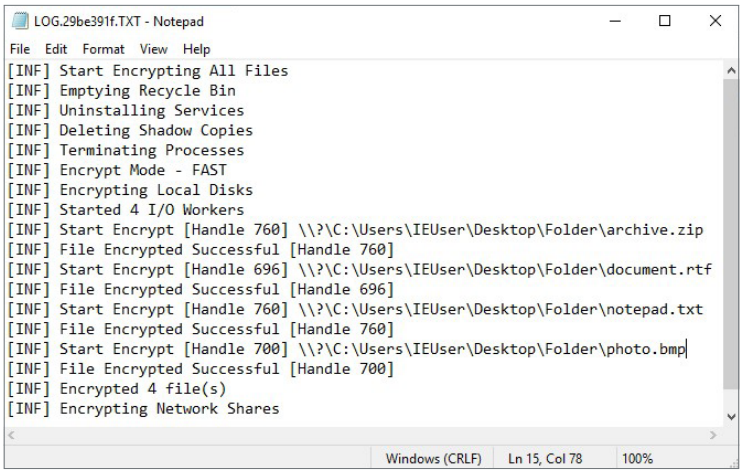
Pour être plus furtif, le ransomware vide la Corbeille sans utiliser la fonction SHEmptyRecycleBinA(). Au lieu de cela, il supprime un à un les fichiers et dossiers placés dans la Corbeille.

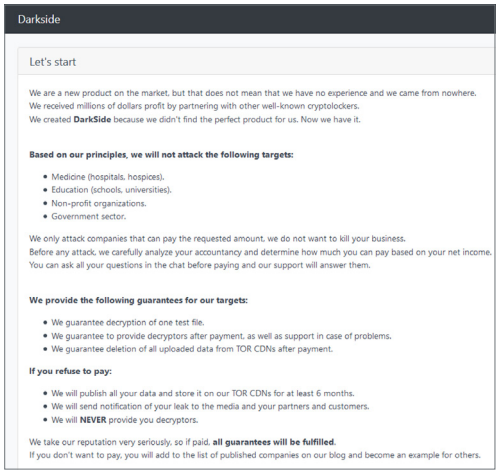
DarkSide désinstalle les services suivants associés aux solutions de sécurité et de sauvegarde :

Après avoir désinstallé le service de cliché instantané des volumes (VSS), le ransomware supprime les clichés instantanés en exécutant un script PowerShell masqué. DarkSide spécifie aussi une clé qui doit être entrée sur le premier site. Il semblerait que la clé ne soit pas propre à un utilisateur mais à un échantillon, étant donné que sa valeur est codée en dur et chiffrée dans le fichier exécutable.

La conclusion est la même ici : les nouvelles familles de ransomwares, même relativement simples, attaquent par défaut les sauvegardes. C'est malheureusement devenu la norme.







Sites Web malveillants

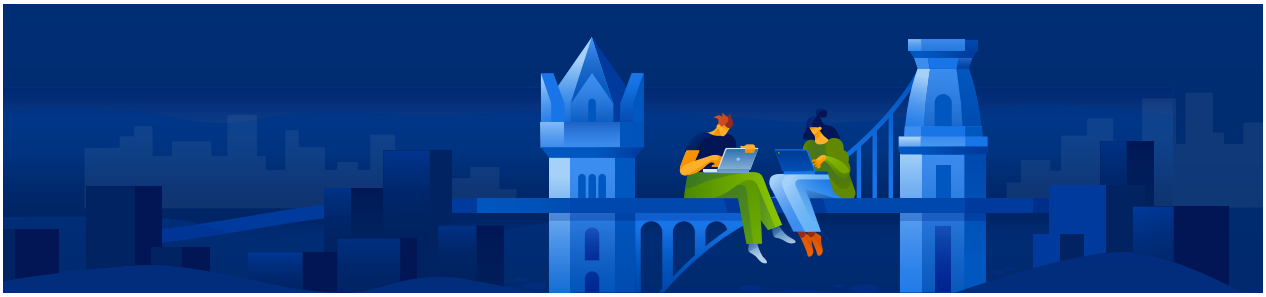
Au cours de la pandémie, nous avons assisté à une augmentation des attaques de phishing, surtout contre les outils de collaboration et les services de partage de fichiers dont l'utilisation s'est généralisée avec l'adoption croissante du télétravail. Après le pic initial de mars, nous avons observé un retour à la normale des attaques de phishing. Certains groupes cybercriminels semblent être revenus aux pièces jointes malveillantes. Même le tristement célèbre Emotet a fait son retour après cinq mois d'absence en envoyant à nouveau des documents Office malveillants.

MOIS	% D'UTILISATEURS ayant cliqué sur des URL malveillantes
Juin	5,5 %
Juillet	5,1 %
Août	2,3 %
Septembre	2,7 %
Octobre	3,4 %

C'est aux États-Unis que l'on a recensé le plus haut pourcentage d'URL malveillantes bloquées au 3e trimestre 2020, soit 16,4 %. L'Allemagne et la République tchèque les suivent de près avec respectivement 14,1 % et 10,4 %. Toutefois, 51 % des URL bloquées étaient des adresses HTTPS chiffrées, ce qui a compliqué leur filtrage sur le réseau. D'après nos observations, un nombre croissant de groupes tentent aussi d'obtenir des jetons 2FA et de les utiliser immédiatement avec un script pour se connecter. Pour compliquer la détection de ces pages de phishing, celles-ci sont généralement hébergées sur les domaines de fournisseurs de services Cloud réputés, comme Azure ou Google. Certains cyberpirates ajoutent même une page CAPTCHA qui doit être résolue avant que l'utilisateur n'atteigne la dernière page de phishing — une tactique qui peut empêcher les solutions d'analyse automatisée de détecter et de bloquer le site Web de phishing.

20 pays comptant le plus grand nombre d'URL bloquées au 3e trimestre

CLASSEMENT	PAYS	% D'URL BLOQUÉES AU 3E TRIM. 2020
1	États-Unis	16,4 %
2	Allemagne	14,1 %
3	République tchèque	10,4 %
4	Espagne	8,3 %
5	Royaume-Uni	6,7 %
6	Chine	5,8 %
7	Afrique du Sud	5,2 %
8	Hong Kong	3,6 %
9	Italie	3,4 %
10	Australie	2,4 %
11	France	2,1 %
12	Canada	2,0 %
13	Pérou	1,9 %
14	Norvège	1,9 %
15	Pays-Bas	1,8 %
16	Japon	1,6 %
17	Suisse	1,6 %
18	Bulgarie	0,9 %
19	Singapour	0,8 %
20	Autriche	0,7 %



3e partie

Vulnérabilités des logiciels et du système d'exploitation Windows

1 Vulnérabilité et exploitation croissante des applications tierces par les cyberpirates

2 Applications les plus exploitées dans le monde

Le nombre de vulnérabilités identifiées et de correctifs distribués a explosé en 2020. L'équipe VulnDB de la société Risk Based Security a agrégé 11 121 vulnérabilités identifiées au cours du premier semestre 2020.

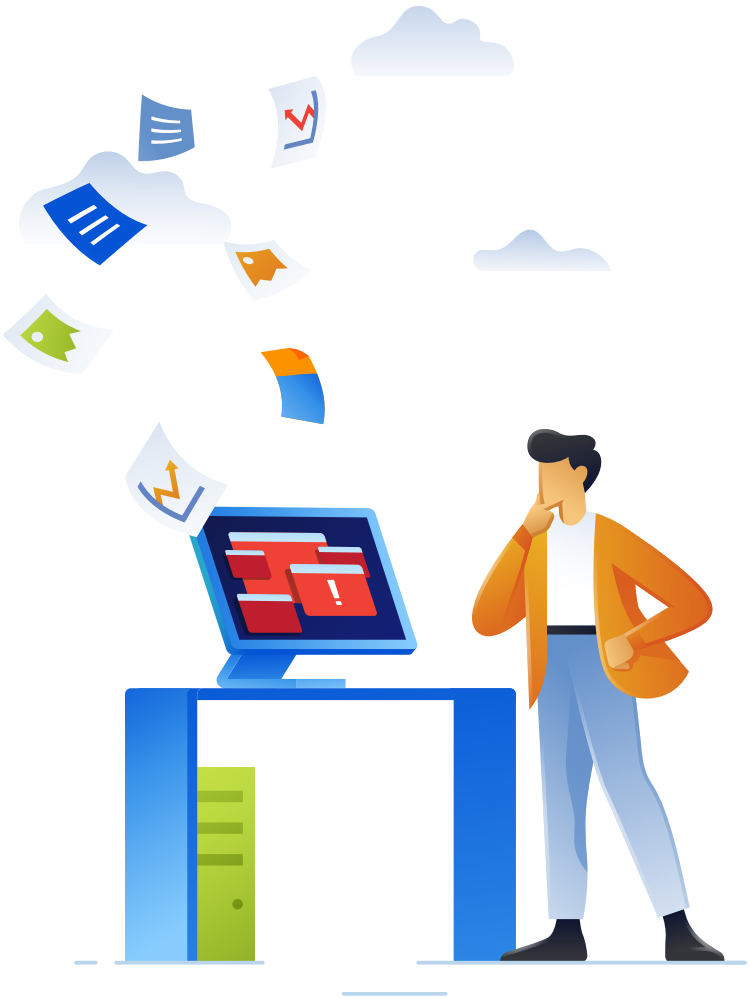
Dans le dernier correctif publié par Microsoft en septembre, la société a signalé 129 vulnérabilités de sécurité corrigées, dont 23 étaient susceptibles d'être exploitées par un malware pour prendre le contrôle total des ordinateurs Windows sans intervention, sinon minime, des utilisateurs. C'est le septième mois consécutif où Microsoft distribue des correctifs pour plus de 100 vulnérabilités dans ses produits, et le quatrième mois consécutif que la société en corrige plus de 120.

Malheureusement, le problème n'est pas nouveau : même si un éditeur distribue rapidement un correctif, cela ne signifie pas pour autant qu'il a été appliqué sur toutes les machines. Par exemple, la vulnérabilité CVE-2020-0796, plus connue sous le nom SMBGhost, serait tellement dangereuse si elle était exploitée qu'elle a obtenu le score de vulnérabilité CVSS le plus élevé : 10. Microsoft a publié un correctif d'urgence « hors bande » en quelques jours. Mais les sociétés de cybersécurité du monde entier, dont Acronis, ont continué d'observer l'utilisation de cette vulnérabilité.

De même, les vulnérabilités CVE-2020-1425 et CVE-2020-1457, deux failles d'exécution de code à distance (RCE), ont été respectivement classées « critique » et « importante » en termes de gravité. Les deux sont liées à la bibliothèque de codecs Microsoft Windows qui gère les objets en mémoire. Un cyberpirate capable d'exploiter la vulnérabilité CVE-2020-1425 « pourrait obtenir des informations pour compromettre davantage le système de l'utilisateur », selon Microsoft. L'exploitation réussie de la seconde faille, quant à elle, pourrait permettre aux cybercriminels d'exécuter un code arbitraire sur la machine ciblée. Chaque faille a reçu la note « Exploitation moins probable » selon l'indice d'exploitabilité Microsoft.

Certaines de ces vulnérabilités sont activement exploitées, comme nous pouvons le constater dans nos données : CVE-2020-1020 et CVE-2020-0938. Comme nous l'avons signalé le 23 mars, Microsoft a confirmé que ces vulnérabilités Windows sans correctif étaient activement exploitées par les cybercriminels. Les utilisateurs de Windows 10 qui n'ont pas appliqué le correctif au moment de sa publication par Microsoft s'exposent potentiellement à l'installation de programmes, à la consultation ou modification de leurs données et à la création de nouveaux comptes.

La vulnérabilité d'usurpation Windows CVE-2020-1464 est également massivement attaquée. La faille est liée à la validation incorrecte des signatures de fichiers par Windows. Un cyberpirate qui parvient à exploiter cette vulnérabilité pourrait utiliser une signature usurpée jointe à un fichier exécutable malveillant pour charger n'importe quel fichier et amener le système d'exploitation à considérer ce fichier comme étant légitime. Cette vulnérabilité affecte toutes les versions de Windows prises en charge et, si le correctif n'est pas appliqué, représente un problème majeur.



Vulnérabilité et exploitation croissante des applications tierces par les cyberpirates

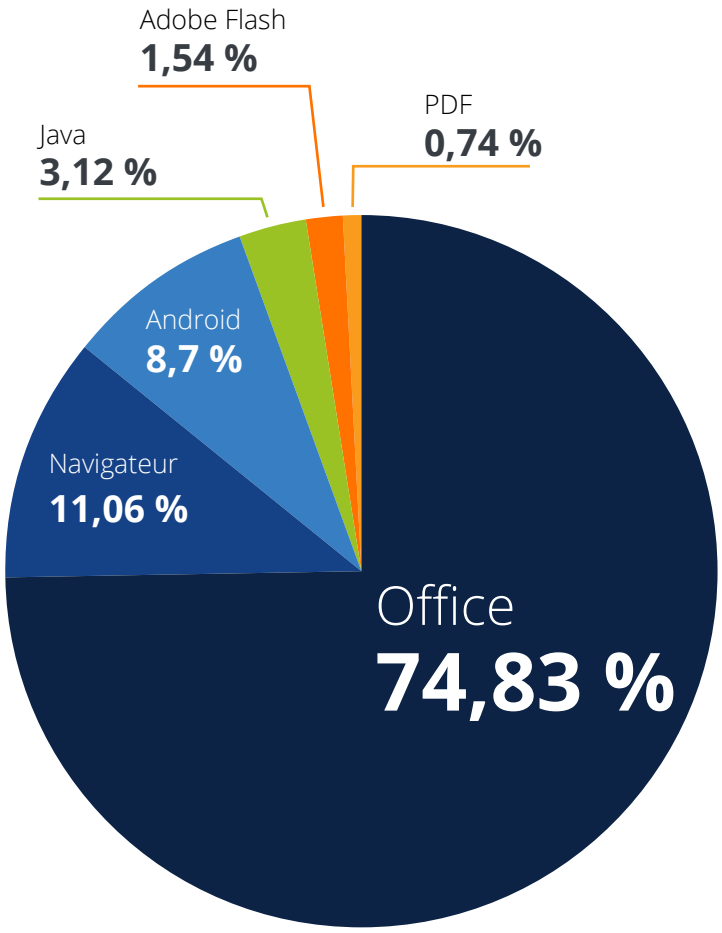
Il va de soi que Microsoft n'est pas le seul éditeur dont les logiciels présentent des vulnérabilités. Les vulnérabilités suivantes ont également été identifiées et exploitées en 2020.

Adobe distribue régulièrement des correctifs de sécurité pour ses produits et a publié une mise à jour de sécurité d'urgence « hors bande » pour Photoshop, Prelude et Bridge en juillet. Une semaine après avoir distribué sa mise à jour de sécurité mensuelle habituelle, Adobe a publié des avis de sécurité recensant 13 vulnérabilités, dont 12 considérées comme critiques. Si elles étaient exploitées, elles pourraient conduire à l'exécution de code arbitraire.

En août, Adobe a publié des correctifs pour 26 vulnérabilités identifiées dans Adobe Acrobat et Adobe Reader, dont 11 jugées critiques. Les failles critiques pourraient être exploitées pour contourner les contrôles de sécurité, neuf d'entre elles permettant l'exécution de code arbitraire à distance.

Les logiciels Windows ne sont pas les seuls à présenter des vulnérabilités. Les cybercriminels ciblent de plus en plus les vulnérabilités VPN non corrigées. Une vulnérabilité permettant l'exécution de code arbitraire des appliances VPN Citrix, appelée CVE-2019-19781, a été détectée dans plusieurs exploits. Une vulnérabilité de lecture de fichier arbitraire des serveurs VPN Pulse Secure, appelée CVE-2019-11510, reste une cible de choix pour les cybercriminels.

Applications les plus exploitées dans le monde



4e partie

À surveiller en 2021

Recommandations d'Acronis pour rester protégé dans le paysage des menaces d'aujourd'hui et de demain

Augmentation attendue des attaques visant les collaborateurs en télétravail

Avec l'augmentation rapide des taux d'infection par la COVID-19, il est difficile d'imaginer que la pandémie prendra fin cette année. Selon toute probabilité, la distribution mondiale d'un vaccin risque de prendre au moins un an, voire de se prolonger jusqu'en 2022. En d'autres termes, le télétravail et tous les risques qu'il présente risquent de perdurer. En 2020, les cybercriminels ont pris conscience que le phishing reste efficace et que les collaborateurs sont un parfait vecteur d'accès aux données des entreprises. Selon nos prévisions, les attaques contre les collaborateurs en télétravail vont se multiplier et gagner en sophistication, puisque les cybercriminels seront de plus en plus nombreux à tenter d'accéder aux données et aux systèmes d'entreprise hébergés dans les centres de données et les bureaux vides.

Délaissement du chiffrement de données au profit de l'exfiltration de données

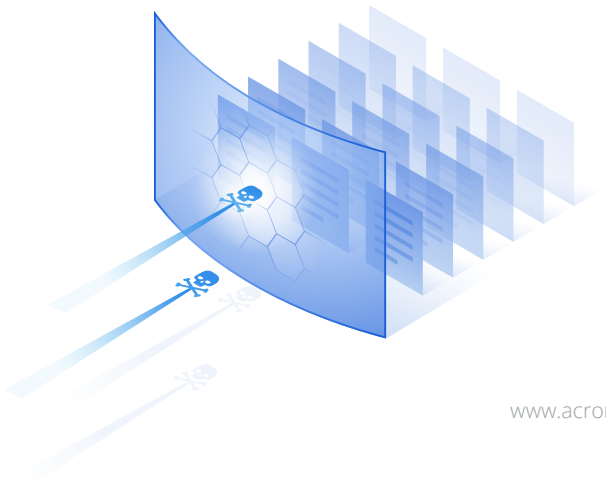
Les récents cas de ransomware ont montré que les cybercriminels cherchent à monétiser chaque attaque. Pire encore, ils ont constaté que l'extorsion associée au vol de données confidentielles fonctionne très bien, peut-être même mieux que le simple chiffrement de ces données. C'est pourquoi nous nous attendons à ce que l'objectif principal de chaque attaque par ransomware soit l'exfiltration de données. Les solutions de protection des données et de prévention des fuites de données vont jouer un rôle important au cours de l'année à venir. En effet, même si nous observons une diminution du nombre de nouvelles familles, les ransomwares actifs seront très efficaces et provoqueront des dommages considérables. Il faut donc s'attendre à ce que les ransomwares restent en tête du classement des menaces pesant sur les entreprises l'année prochaine.

Multiplication des attaques contre les fournisseurs de services managés et les petites entreprises

Le recours croissant des PME aux fournisseurs MSP et MSSP ouvre grand la porte aux attaques des cybercriminels. En 2019 et en 2020, les cyberpirates se sont rendu compte que les attaques ciblant les MSP sont très efficaces, en particulier si elles visent des sociétés de plus petite envergure, parfois mal préparées. En ciblant les MSP, ils ont aussi accès à leurs clients et peuvent récolter davantage d'argent au moyen d'infections par ransomware ou de chevaux de Troie bancaires. En outre, les cybercriminels peuvent tirer parti d'outils à l'efficacité démontrée, tels que les utilitaires d'accès à distance et de distribution de logiciels. Ces types d'attaques vont probablement se multiplier et gagner toutes les régions, dans la mesure où les petites entreprises et les MSP ne sont pas suffisamment préparés pour contrer des attaques bien menées et ont toujours les moyens de payer une rançon raisonnable.

Le Cloud en ligne de mire

Pendant le confinement, de nombreuses entreprises ont migré leurs services vers le Cloud. Malheureusement, la configuration laisse souvent à désirer et n'est pas parfaitement sécurisée, exposant services de données et applications Cloud aux risques d'Internet. Un tel scénario offre aux cyberpirates la possibilité d'accéder aux données et de les exfiltrer, comme nous l'avons constaté avec les compromissions de données sur les compartiments S3 et les bases de données Elasticsearch. En outre, la gestion des identités et des accès est encore trop souvent négligée, même si les identités s'imposent progressivement comme le nouveau périmètre. Cette situation conduira à une adoption accrue des solutions d'analyse du comportement des utilisateurs et des entités ainsi que des contrôles d'accès dynamiques.



Les futures cibles des ransomwares

Les attaques par ransomware ne se contentent plus de cibler les postes de travail Windows et Mac. Les cybercriminels tentent de s'infiltrer dans l'environnement Cloud, car les conteneurs et bases de données Cloud représentent des cibles très lucratives. Au sein des entreprises, les systèmes de contrôle industriels, toujours plus exposés, représentent une autre cible de choix pour les tentatives d'extorsion. Pour les particuliers, l'adoption croissante de l'Internet des objets (IoT), surtout en rapport avec la 5G, peut favoriser l'émergence de nouveaux vecteurs d'infection, si ce n'est que pour générer des attaques par déni de service distribué afin d'inciter les victimes à payer les rançons.

Adoption croissante de l'automatisation par les cybercriminels et augmentation du nombre d'échantillons de malware

Les cybercriminels tentent d'automatiser leurs processus autant que possible. Les outils d'analyse des Big Data et l'apprentissage automatique leur permettent d'identifier de nouvelles victimes et de générer des messages de spam personnalisés. Les services CaaS (Crimeware-as-a-Service) et les programmes affiliés accélèrent encore ces processus automatisés. Toutefois, après la phase d'accès et d'exécution initiale, la plupart des groupes continuent d'utiliser des méthodes manuelles pour propager leurs malwares au sein des réseaux d'entreprise. Quoi qu'il en soit, nous allons assister à une utilisation plus fréquente des méthodes d'attaque connues, avec des degrés variables de personnalisation.

Recommandations d'Acronis pour rester protégé dans le paysage des menaces d'aujourd'hui et de demain

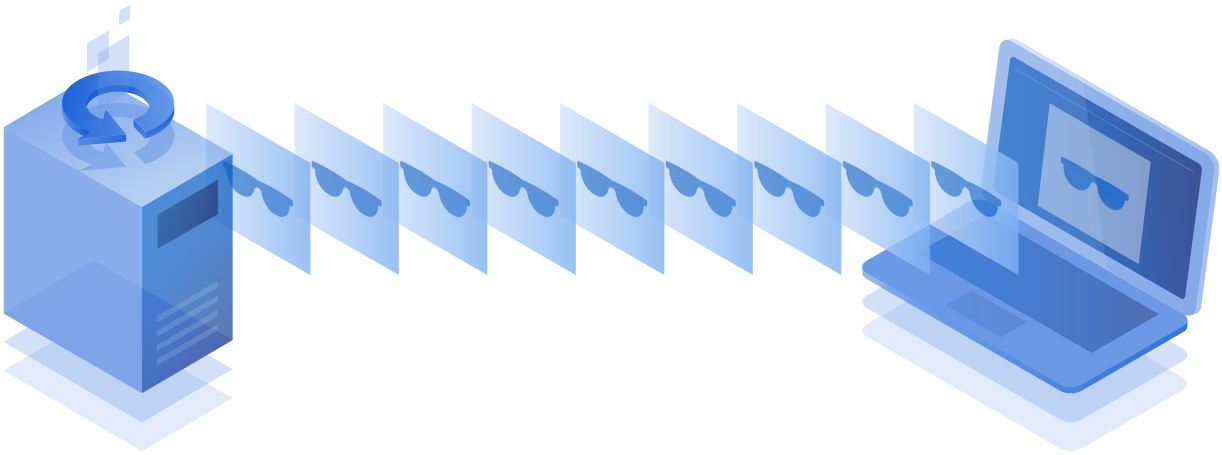
Face aux nouvelles cyberattaques, fuites de données et infections par ransomware, le constat est amer : la cybersécurité perd du terrain. La raison est simple : des technologies inefficaces et des erreurs humaines provoquées par une ingénierie sociale très habile. Dans les cas où une solution de sauvegarde fonctionne bien et n'est pas compromise, il faut généralement plusieurs heures voire quelques jours pour restaurer les systèmes (et les données) à un état opérationnel. La sauvegarde est essentielle lorsque les solutions de cybersécurité sont mises en échec. Cela étant, les solutions de sauvegarde peuvent elles aussi être compromises, désactivées ou ralenties, ce qui entraîne des interruptions d'activité et, au bout du compte, des pertes financières importantes pour les entreprises.

Pour résoudre ces problèmes, nous recommandons une solution de cyberprotection intégrée comme Acronis Cyber Protect, qui combine de nombreuses fonctionnalités — antimalware, évaluation des vulnérabilités, gestion des correctifs, gestion et surveillance à distance et sauvegarde — au sein d'un seul agent exécuté sous divers systèmes d'exploitation Windows. Cette intégration vous permet de garantir des performances optimales, d'éliminer les problèmes de compatibilité et d'assurer une restauration rapide. Si une menace passe entre les mailles du filet pendant la modification de vos données, l'agent peut immédiatement restaurer les données non modifiées à partir d'une sauvegarde.

Ce type de reprise automatisée est impossible avec un simple agent antimalware. La solution antimalware peut certes bloquer la menace, mais vous risquez entretemps de perdre certaines données. L'agent de sauvegarde n'en sera pas automatiquement informé et les données seront restaurées lentement, voire pas du tout.

Bien entendu, Acronis Cyber Protect Cloud fera tout pour éviter d'avoir recours à la récupération des données, en détectant et en éliminant les menaces avant qu'elles ne puissent endommager les systèmes de votre environnement. Un tel niveau de défense est possible grâce à nos fonctionnalités de cybersécurité multiniveau optimisées.

Quoi qu'il en soit, les entreprises et les particuliers ne devraient jamais oublier les règles de sécurité élémentaires, même s'ils utilisent des solutions de dernière génération comme Acronis Cyber Protect.



Appliquez des correctifs à vos systèmes d'exploitation et à vos applications

Il est impératif d'appliquer des correctifs dans la mesure où de nombreuses attaques aboutissent à cause de vulnérabilités non corrigées. Avec une solution comme Acronis Cyber Protect, vous êtes protégé par des fonctionnalités intégrées d'évaluation des vulnérabilités et de gestion des correctifs. Nous assurons le suivi de toutes les vulnérabilités identifiées et des correctifs distribués et permettons aux administrateurs ou aux techniciens d'appliquer facilement des correctifs à tous les terminaux grâce à une configuration flexible et à des rapports détaillés. Acronis Cyber Protect prend non seulement en charge toutes les applications Windows embarquées, mais aussi plus d'une centaine d'applications tierces populaires, notamment les outils de télécommunication Zoom et Slack, ainsi que les clients VPN les plus utilisés dans le cadre du télétravail. Veillez à corriger d'abord les vulnérabilités les plus graves et à consulter le rapport d'exécution pour vérifier si les correctifs ont été correctement appliqués.

Si vous ne possédez pas Acronis Cyber Protect et/ou que vous n'utilisez pas de logiciel de gestion des correctifs, la tâche sera bien plus complexe. Assurez-vous au moins d'installer toutes les mises à jour requises de Windows, et ce dans les meilleurs délais. Les utilisateurs ont tendance à ignorer les messages système, surtout lorsque Windows les invite à effectuer un redémarrage, ce qui est une grave erreur. Pensez à activer les mises à jour automatiques des éditeurs et des applications les plus répandus, tels qu'Adobe et Acrobat Reader.

Anticipez les tentatives de phishing et ne cliquez pas sur les liens suspects

La COVID-19 est désormais un thème récurrent de nombreuses attaques de phishing, mais ce type d'activités malveillantes ne va cesser d'augmenter. Tous les collaborateurs en télétravail devraient donc s'y préparer. Chaque jour voit apparaître de nouveaux sites Web malveillants et tentatives de phishing sur les thèmes du moment. En général, ceux-ci sont filtrés par le navigateur, mais avec des solutions de cyberprotection comme Acronis Cyber Protect, vous bénéficiez en plus de fonctions de filtrage d'URL dédiées. Des fonctionnalités identiques sont disponibles dans les solutions de protection des terminaux. Toutefois, Acronis Cyber Protect possède une catégorie spéciale liée aux thèmes de santé publique, qui est mise à jour en priorité. Les liens malveillants peuvent émaner de n'importe quelle source : e-mails, messages de forum et applications de messagerie instantanée.

Ne cliquez pas sur des liens dont vous n'avez pas besoin ou que vous ne vous attendiez pas à recevoir.

Le phishing et les pièces jointes malveillantes peuvent être véhiculés par e-mail, au même titre que les liens dangereux précités. En ce qui concerne les pièces jointes, vérifiez toujours leur provenance et demandez-vous s'il est normal que vous les receviez. Dans tous les cas, avant d'ouvrir une pièce jointe, celle-ci doit être analysée par votre solution antimalware.

Utilisez un VPN lorsque vous manipulez des données d'entreprise

Que vous vous connectiez aux sources et services distants de l'entreprise ou que vous consultiez des ressources sur Internet et employiez des outils de télécommunication, utilisez systématiquement un réseau privé virtuel (VPN). Un VPN permet de chiffrer tout le trafic et le sécurise dans le cas où un cyberpirate tenterait de capturer vos données en transit. Si votre entreprise prévoit l'utilisation d'un VPN, vous recevrez sans doute des instructions de votre administrateur ou du technicien de votre MSP. Si vous êtes responsable de la sécurisation de votre lieu de travail, utilisez des services et des applications VPN connus et recommandés, disponibles sur les marketplaces de logiciels ou directement auprès des fournisseurs.

Vérifiez que votre solution de cybersécurité fonctionne bien

Acronis Cyber Protect possède de nombreuses technologies de sécurité bien équilibrées et optimisées, y compris plusieurs moteurs de détection, qui sont préférables à une solution Windows intégrée.

Mais la mise en place d'une solution antimalware ne suffit pas, il faut également la configurer correctement. En d'autres termes :

- **Il faut effectuer une analyse complète une fois par jour au moins.**
- **Les produits doivent être mis à jour toutes les heures ou tous les jours, selon la fréquence de publication.**
- **Le produit doit être connecté à ses mécanismes de détection Cloud — dans le cas d'Acronis Cyber Protect, à Acronis Cloud Brain. Cette base de données de réputation est activée par défaut, mais vous devez vérifier qu'Internet est disponible et que son accès n'est pas accidentellement bloqué par un logiciel antimalware.**
- **Les analyses à la demande et à l'accès (en temps réel) doivent être activées et réagir à chaque tentative d'installation ou d'exécution d'un nouveau logiciel.**

En outre, ne négligez pas les messages émanant de votre solution antimalware. Lisez-les attentivement et vérifiez que la licence est légitime si vous utilisez une version payante de votre fournisseur de sécurité.

Protégez correctement vos mots de passe et votre espace de travail

Dernier conseil de sécurité : veillez à ce que vos mots de passe et ceux de vos collaborateurs soient privés et forts. Ne communiquez jamais vos mots de passe à qui que ce soit. Configurez des mots de passe longs et différents pour chaque service utilisé. Pour vous aider à vous en souvenir, utilisez un gestionnaire de mots de passe. Pour configurer des mots de passe forts, la méthode la plus simple consiste à créer une série de longues phrases faciles à mémoriser. De nos jours, il est très facile de craquer les mots de passe à huit caractères avec des attaques en force.

Un produit sécurisé comme Acronis Cyber Cloud ou Acronis Cyber Backup ne stocke jamais les mots de passe, ce qui empêche tout accès non autorisé à vos données.

Enfin, n'oubliez pas de verrouiller votre ordinateur portable ou de bureau et d'en limiter l'accès, même lorsque vous travaillez de votre domicile. Il est arrivé bien souvent que des informations sensibles soient volées sur un PC non verrouillé, même à distance.

Ressources supplémentaires

Webinaire à la demande : Cybersecurity 2021 – The Expected Threat Landscape (Cybersécurité 2021 – Paysage des menaces attendu)

Livre blanc : Rapport d'Acronis sur la cyberpréparation

Outil gratuit : Questionnaire d'évaluation de la cybersécurité

Acronis

À propos d'Acronis

Acronis unifie la protection des données et la cybersécurité pour délivrer une approche de cyberprotection intégrée et automatisée réunissant les conditions SAPAS de fiabilité des données, d'accessibilité, de confidentialité, d'authenticité et de sécurité. Par ses modèles de déploiement flexibles adaptés au fonctionnement des fournisseurs de services et des professionnels IT, Acronis garantit la cyberprotection supérieure des données, applications et systèmes avec des solutions antivirus de nouvelle génération, de sauvegarde, de reprise après sinistre et de gestion de la protection des terminaux. Grâce à ses technologies primées d'authentification par la blockchain et de lutte contre les malwares à base d'IA, Acronis protège n'importe quel environnement, Cloud, hybride, sur site, pour un coût prévisible et abordable.

Société fondée à Singapour en 2003 et enregistrée en Suisse en 2008, Acronis compte à présent plus de 1 500 salariés sur 33 sites dans 18 pays. Plus de 5,5 millions de particuliers et 500 000 entreprises font confiance aux solutions Acronis, dont 100 % du classement Fortune 1000, ainsi que de grandes équipes sportives professionnelles. Les produits Acronis sont distribués par un réseau de 50 000 partenaires et fournisseurs de services, couvrant plus de 150 pays dans plus de 40 langues. Pour plus d'informations, consultez notre site www.acronis.com