SOPHOS
Cybersecurity evolved.

RAPPORT SOPHOS 2021 SUR LES MENACES

Gouvernance de la cybersécurité face à un monde incertain

Par les équipes **SophosLabs, Sophos Managed Threat Response, Sophos Rapid Response Sophos AI et Cloud Security**

TABLE DES MATIÈRES

LA PUISSANCE DU PARTAGE

Joe Levy, Directeur technique de Sophos

« Si tu veux aller vite, marche seul ; mais si tu veux aller loin, marchons ensemble. »

Ce proverbe africain ne saurait mieux s'appliquer à l'industrie de la cybersécurité. En travaillant de manière collective, avec un sens aigu du travail d'équipe, nous pouvons atteindre de bien meilleurs résultats dans la lutte contre la cybercriminalité qu'en tant que fournisseurs individuels.

Mais ce n'est qu'en améliorant notre approche, en partageant notre intelligence sur les menaces de manière plus globale, mais aussi en élargissant le nombre de participants qui contribuent à ce partage et à cette collaboration (et qui en bénéficient), que les acteurs de la cybersécurité pourront alourdir les coûts pour les attaquants et changer la donne de façon durable.

C'est dans cet esprit que Sophos a rejoint en 2017 la ***Cyber Threat Alliance***, une organisation visant à éliminer les barrières qui, pendant des années, ont entravé toute tentative de collaboration entre les concurrents du secteur de la sécurité de l'information. La CTA a réussi bien au-delà de son objectif initial, à savoir de servir de référentiel pour le partage de l'intelligence sur les menaces et d'espace de résolution des différends, pour devenir une sorte d'ONU consacrée à l'industrie de la cybersécurité.

Grâce à ce partenariat avec la CTA, Sophos reçoit des alertes précoces et bénéficie d'échanges de données entre fournisseurs qui lui permettent de mieux protéger ses clients. Sophos partage également la charge de protéger les clients des autres fournisseurs en partageant sa propre veille sur les menaces.

En mars 2020, alors qu'une partie du monde se retrouvait confinée pour limiter la propagation du Covid-19, le directeur scientifique de Sophos, Joshua Saxe, a lancé un appel sur Twitter. Affligés par le fait que des groupes malveillants commençaient à incorporer des références au Covid-19 dans une vague de cyber campagnes criminelles, plus de 4 000 analystes de la sécurité de l'information ont riposté en se regroupant au sein de la coalition « COVID-19 Cyber Threat Coalition (CCTC) » sur un canal Slack créé le même jour. Ce canal, qui crée un « terrain commun » durable que la communauté pourra exploiter en temps de crise, est sur le point d'obtenir le statut d'organisme à but non lucratif sous les auspices de la CTA.

Finalement, ces exemples de partage de l'intelligence sur les menaces nous révèlent bien plus que des informations sur les organisations elles-mêmes. Comme nous le rappelle la fable de l'aveugle et de l'éléphant, aucun éditeur ne peut fournir une vérité complète ou absolue de par sa seule expérience subjective. C'est la mise en commun de nos expériences qui fait émerger la nature réelle des choses complexes. C'est grâce à ce genre d'initiatives collectives que des millions de personnes ont pu échapper aux cybercriminels, mais ce n'est pas ***l'unique raison***. Elles ont réussi aussi parce que la principale motivation de leurs membres et de leurs fondateurs a été, en premier lieu, de protéger toute personne susceptible d'être exposée à un danger. L'objectif d'une telle action n'était pas le profit, mais simplement l'envie de défendre des personnes en situation vulnérable face à leurs agresseurs.

Cet exemple montre que ce modèle collaboratif fonctionne et comble des failles critiques dans la couverture qu'aucun d'entre nous ne pouvait générer à lui seul. Mais ensemble, c'est possible. En tant qu'industrie, nous pouvons donc envisager à l'avenir de partager des modèles de Machine Learning ou des bases de données pour la formation, tout comme nous partageons aujourd'hui des listes de blocage ou des règles Yara. Nous pourrions également contribuer et renforcer des normes émergentes telles que le protocole STIX ou la matrice ATT&CK. Et nous pourrions participer aux normes ISAC et ISAO spécifiques à l'industrie.

Un avenir plus connecté est synonyme d'une meilleure sécurité pour tous.

RÉSUMÉ

Le rapport sur les menaces 2021 de Sophos couvre tous les domaines sur lesquels Sophos a concentré ses efforts au cours des douze derniers mois. Il intègre le travail d'analyse des SophosLabs sur les malwares et le spam, mais aussi des équipes Sophos Rapid Response, Cloud Security et Data Science. Ces aspects de notre travail quotidien donnent une vision claire du panorama des menaces qui guide les professionnels de la sécurité informatique et de la réponse aux incidents sur la direction à prendre pour mieux défendre les réseaux et les systèmes d'extrémité au cours de la prochaine année.

Le rapport se divise en quatre parties : Tout d'abord, il explique la transformation des ransomwares et la direction que prend actuellement cette menace ; puis il analyse les attaques les plus fréquentes visant les grandes entreprises et pourquoi ces menaces, tels des « canaris dans une mine de charbon » restent significatives ; il montre ensuite comment l'émergence d'une pandémie a affecté la sécurité des données en 2020 ; et enfin, il évalue l'ampleur des attaques ciblant les plates-formes qui habituellement ne font pas partie de la surface d'attaque des entreprises.

Pour résumer les points du rapport à retenir :

Ransomware

- Les acteurs de ransomware continuent d'innover à un rythme effréné à la fois dans leur technologie et dans leur modes opératoires
- De plus en plus de groupes spécialisés dans les ransomwares volent désormais les données dans le but d'extorquer les cibles en les menaçant de divulguer leurs données privées sensibles
- Les groupes de ransomware redoublent d'efforts dans leurs attaques actives contre les grandes organisations et les rançons exigées ont augmenté de manière fulgurante
- Différents groupes d'acteurs impliqués dans des attaques de ransomwares semblent désormais collaborer plus étroitement avec leurs confrères criminels, se comportant davantage comme de véritables cartels de la cybercriminalité que comme des groupes indépendants
- Les attaques de ransomware qui auparavant prenaient des semaines ou des jours peuvent maintenant se réaliser en quelques heures

Menaces classiques

- Les plates-formes de serveur Windows et Linux ont été lourdement ciblées et exploitées pour attaquer les organisations de l'intérieur
- Les services courants comme les concentrateurs VPN et RDP restent des points centraux pour les attaques sur le périmètre réseau, et les cybercriminels utilisent également le RDP pour se déplacer latéralement au sein des réseaux corrompus
- Même les malwares basiques « bas de gamme » peuvent engendrer des violations importantes, car de plus en plus de familles se transforment en « réseaux de distribution de contenu » pour d'autres malwares
- Négliger un ou plusieurs aspects de base de la sécurité s'est avéré être à l'origine d'un grand nombre des attaques les plus dommageables sur lesquelles nous avons enquêté

COVID-19

- Le télétravail génère de nouveaux défis, en étendant le périmètre de sécurité de l'entreprise à des milliers de réseaux domestiques protégés par des niveaux de sécurité extrêmement variables
- Le Cloud Computing a réussi à amortir le choc et à répondre aux nombreux besoins des entreprises en matière d'environnements informatiques sécurisés, mais il présente toujours ses propres défis uniques, par rapport à ceux d'un réseau d'entreprise traditionnel
- Les cybercriminels ont tenté de blanchir leur réputation en promettant de ne pas cibler les organismes de santé œuvrant à sauver des vies, mais ces promesses ont vite été oubliées
- Les entreprises criminelles se sont transformées en une véritable économie de services facilitant l'entrée de nouveaux acteurs
- Les professionnels de la cybersécurité du monde entier se sont rapidement organisés en 2020 au sein d'une coalition réactive pour combattre les menaces d'ingénierie sociale qui exploitent les craintes liées au Coronavirus

Plates-formes non traditionnelles

- Les attaquants profitent désormais de la richesse des outils et des utilitaires « Red Team » mis au point par les testeurs d'intrusion dans le cadre d'attaques actives en direct
- Malgré les efforts des opérateurs de plates-formes mobiles pour surveiller les applications à la recherche de codes malveillants, les attaquants poursuivent leur travail en développant des techniques pour contourner ces scanners de code
- Les logiciels autrefois classés comme « potentiellement indésirables » parce qu'ils diffusaient une pléthore de publicités (bien qu'en soi non malveillantes) sont utilisés dans des tactiques de plus en plus difficiles à distinguer des véritables malwares
- Pour combler les failles dans la détection, les spécialistes de la Data Science ont appliqué des approches empruntées au monde de l'épidémiologie biologique aux attaques de spam et aux charges utiles de malwares.

L'AVENIR DES RANSOMWARES

Les attaques de ransomware lancées tout au long de l'année 2020 sont venues aggraver les circonstances d'une population déjà très inquiète et fatiguée. En plus de la pandémie qui a bouleversé nos vies et nos modes de vie, s'est ajoutée une famille de ransomwares dont les efforts n'ont pas cessé de cibler les secteurs de la santé et de l'éducation, alors même que les hôpitaux devenaient des champs de bataille contre le Covid-19 et que les écoles ont dû inventer une toute nouvelle façon d'enseigner aux enfants à partir de mars et au-delà.

En temps de pandémie, une tombola ne suffira jamais à récolter assez d'argent pour payer une rançon, mais certaines écoles ont réussi à se remettre d'attaques qui semblaient ciblées dès le premier jour d'école, en ayant gardé des sauvegardes sécurisées.

Les auteurs de ransomwares ont mis au point de nouveaux moyens d'échapper aux produits de sécurité informatique et de se propager rapidement. Ils ont même trouvé une solution au problème (de leur point de vue) des individus ou entreprises qui avaient de bonnes sauvegardes, stockées en toute sécurité là où les ransomwares ne pourraient les atteindre.

Mais il semblerait que cette large variété de ransomwares ne soit pas si variée que cela. Au fil du temps, et en étudiant un nombre croissant d'attaques, les analystes de Sophos ont découvert que certains codes de ransomwares semblaient avoir été partagés entre les familles, et que certains des groupes travaillaient en collaboration plutôt qu'en concurrence.

Dans ce contexte, il est impossible de prédire avec certitude ce que les cybercriminels préparent pour la suite. Les auteurs et les opérateurs de ransomwares ont consacré beaucoup de temps et d'efforts à se défendre contre les produits de sécurité Endpoint. Nous contrecarrons leurs contre-mesures. Ils font preuve de créativité et d'adaptabilité pour concevoir leurs nouvelles tactiques. Notre devoir est de faire preuve de ténacité pour analyser ce qu'ils font et trouver des moyens intelligents de les bloquer.

Le vol de données crée un marché d'extorsion secondaire

Jusqu'à cette année, l'approche conventionnelle des éditeurs de sécurité qui avaient une quelconque expérience des ransomwares était assez uniforme : Verrouiller les méthodes d'infiltration évidentes, comme les ports RDP connectés à Internet, effectuer de bonnes sauvegardes hors ligne et traiter rapidement les infections des petits malwares inoffensifs tels que Dridex ou Emotet, avant qu'ils ne puissent livrer la charge utile malveillante.

Plusieurs attaques de ransomware qui ont fait du bruit aux États-Unis, comme celles visant des « school districts » (ou collectivités), ont échoué au moins en partie parce que les responsables informatiques avaient conservé une sauvegarde intacte des données critiques.

Pour contrecarrer la bonne préparation de leurs victimes, plusieurs familles de ransomware ont mis les bouchées doubles en augmentant la pression sur leurs victimes pour qu'elles paient la rançon — même si chaque sauvegarde avec des données critiques était sécurisée. Non seulement elles ont pris les machines en otage, mais elles ont volé les données qu'elles contenaient et menacé de les divulguer au monde entier si leurs cibles refusaient de payer.

Selon les observations de Sophos sur les six derniers mois, les cybercriminels ont décidé de mettre en commun toute une série d'outils (qui se développe lentement) qu'ils utilisent pour exfiltrer les données du réseau de la victime. Cet ensemble d'outils connus et légitimes, que quiconque pourrait utiliser, n'est pas détecté par les produits de sécurité Endpoint. La liste des familles de ransomware qui se livrent à cette pratique ne cesse de s'allonger, et inclut entre autres Doppelpaymer, REvil, Clop, DarkSide, Netwalker, Ragnar Locker et Conti. Les attaquants exploitent des sites de « fuites », où ils rendent publiques les données qu'ils ont volées. REvIL, par exemple, permet à n'importe qui d'acheter ces données directement sur son site.

Ces outils permettent aux criminels de copier les informations internes sensibles, de les compresser dans une archive et de les transférer hors du réseau — et hors de portée de la victime. Voici quelques exemples d'outils dont nous avons observé l'utilisation jusqu'à aujourd'hui :

- Total Commander (gestionnaire de fichiers avec client FTP intégré)
- 7zip (logiciel de création d'archives)
- WinRAR (logiciel de création d'archives)
- psftp (client SFTP de PuTTY)
- Windows cURL

Lorsqu'il s'agit de voler des données, les attaquants sont beaucoup moins pointilleux et exfiltrent des dossiers entiers, quels que soient les types de fichiers qu'ils contiennent. (Généralement, les ransomwares priorisent le chiffrement des types de fichiers clés et en excluent beaucoup d'autres.)

La taille des fichiers n'a aucune importance. Ils se préoccupent pas de la quantité de données qui va être exfiltrée. Les structures de répertoires sont propres à chaque entreprise et certains types de fichiers peuvent être mieux compressés que d'autres. Nous avons vu des données compressées de tailles très variables — de seulement 5 Go jusqu'à 400 Go — être volées aux victimes avant le déploiement du ransomware.

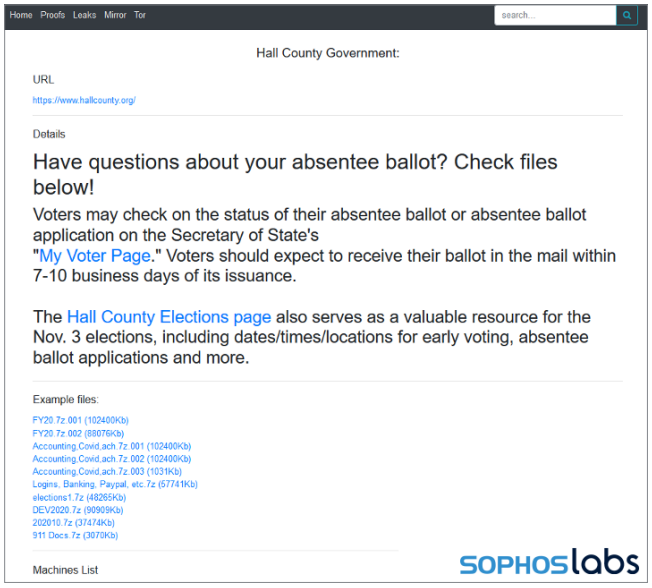


Fig.1. En octobre 2020, le site des fuites du ransomware Doppelpaymer a révélé que les attaquants avaient frappé les réseaux du comté de Hall, en Géorgie (États-Unis). La fuite contenait une référence à un fichier nommé « élections » qui comprenait de nombreuses données sensibles dont des échantillons de bulletins de vote pour les élections primaires de l'État en 2020, ainsi que des listes de membres du bureau de vote avec leurs numéros de téléphone datant des élections de 2018. L'agence de presse Associated Press a rapporté que le ransomware avait chiffré la base de données de vérification des signatures utilisée par le comté pour valider les bulletins de vote. Source : SophosLabs.

Ensuite, les criminels envoient généralement les données exfiltrées à des services légitimes de stockage dans le Cloud, ce qui en fait une opération difficile à repérer, puisqu'il s'agit d'une destination courante et ordinaire du trafic réseau. Selon nos observations, voici les trois services de stockage dans le Cloud les plus utilisés par les attaquants pour stocker les données exfiltrées :

- Google Drive
- Amazon S3 (Simple Storage Service)
- Mega.nz
- Serveurs FTP privés

Dans leur dernier élan de destruction, les auteurs de ransomware traquent de plus en plus les serveurs locaux qui contiennent des sauvegardes de données critiques et, lorsqu'ils les trouvent, ils suppriment ces sauvegardes (ou les chiffrent indépendamment) juste avant de chiffrer l'ensemble du réseau.

Il est donc plus important que jamais d'avoir une sauvegarde de vos données stockée hors ligne. S'ils parviennent à les trouver, les criminels n'hésiteront pas à les détruire.

Les attaques sont en hausse, les rançons aussi

Difficile de croire qu'il y a tout juste deux ans, les analystes de Sophos s'émerveillaient du butin de 6 millions de dollars rapporté par le ransomware SamSam. En 2020, lors d'une attaque à laquelle Sophos a répondu, les exploitants du ransomware ont ouvert leurs négociations à un montant plus de deux fois supérieur à ce que le gang SamSam avait gagné en 32 mois d'activité.

Aujourd'hui, les ransomwares se déclinent en plusieurs catégories : les poids lourds qui s'attaquent aux réseaux des grandes entreprises, les poids welters qui ciblent la société civile (gouvernement local et sécurité publique) et les petites et moyennes entreprises, et les poids plume qui visent les utilisateurs à domicile et les ordinateurs privés. Bien que la distinction douteuse d'être le poids lourd le plus lourd semble impressionnante, il n'est pas juste de comparer les demandes de rançon élevées à celles qui se trouvant en bas de l'échelle.

Sophos dispose d'une équipe dédiée qui analyse et travaille souvent avec des victimes d'attaques de ransomware. Cette équipe est capable de reconstituer en détail les événements d'une attaque après coup, voire d'interrompre les attaques alors qu'elles sont encore en cours. L'équipe Sophos Rapid Response intervient dans les cas où il existe une chance d'arrêter ou de limiter les dommages. Mais parfois l'attaque se déroule si vite qu'elle ne peut rien faire, et la cible doit alors décider de payer la rançon ou non, et dans ce cas, Sophos n'est plus impliqué.

C'est là que des entreprises comme Coveware entrent en jeu. Cette société qui représente les entreprises victimes de ransomwares intervient en tant que négociateur de haut niveau avec les attaquants. Le directeur technique de Coveware, Alex Holdtman, a confirmé nos soupçons, à savoir que les poids lourds sont les principaux acteurs derrière les demandes de rançons astronomiques.

Montant moyen des rançons, par trimestre

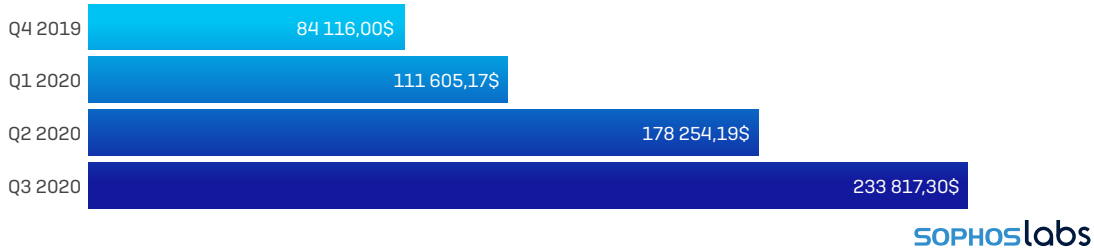


Fig.2. Les montants moyens des demandes de rançon ont augmenté de 21 % au dernier trimestre et ont presque triplé en un an. Source : Coveware.

Au cours du dernier trimestre seulement, le total des rançons versées a augmenté de 21 %. Mais selon Coveware, ces moyennes peuvent être faussées si elles incluent une ou deux sommes très élevées. La moyenne des sommes versées pour le trimestre écoulé équivaut aujourd'hui à 233 817,30 $ en cryptomonnaie. Il y a un an, elle était de 84 116 $ seulement.

Les cybercriminels savent que les interruptions peuvent être très coûteuses et n'ont de cesse de tester la limite maximale de ce qu'ils peuvent extraire avec une attaque.

Plusieurs familles de ransomware se sont spécialisées dans l'extorsion afin de conclure l'affaire plus rapidement. En effet, comme nous l'avons déjà mentionné, des groupes tels que Netwalker ont recours à cette tactique. Ainsi, même si l'organisation visée dispose de sauvegardes parfaitement récupérables, elle peut se retrouver obligée de payer si elle ne veut pas voir ses données internes divulguées au monde entier.

Tout en bas de l'échelle des rançons, les demandes ont augmenté, mais d'après Holdtman, elles n'ont rien à voir avec « les gros poissons ». En effet, beaucoup de petites entreprises et de particuliers sont touchés, mais dans leur cas, les demandes de rançon n'ont pas vraiment évolué.

Dans la vie d'un service de réponse rapide aux ransomwares

Lorsqu'une organisation a été victime du ransomware Maze, alors encore actif, elle a fait appel à l'équipe Sophos Rapid Response. Nous sommes intervenus et avons réussi à contrecarrer activement l'attaque alors qu'elle était encore en cours. Voici le résumé de son déroulement jours après jour :

Avant le Jour 1
À un moment donné avant que l'attaque ne devienne active, les opérateurs compromettent un ordinateur du réseau de la cible.

Cet ordinateur est alors utilisé comme une « tête de pont » sur le réseau. À partir de là, l'attaquant se connectera à plusieurs reprises à d'autres ordinateurs via le protocole RDP (Remote Desktop Protocol).

Jour 1
La première preuve d'activité malveillante apparaît lorsqu'une balise Cobalt Strike SMB est installée comme service sur un contrôleur de domaine (DC) non protégé. Les attaquants sont capables de contrôler le DC depuis l'ordinateur compromis en premier, en exploitant un compte d'administration de domaine avec un mot de passe faible.

Jour 2
Les attaquants créent, exécutent puis suppriment une série de tâches planifiées et de scripts de commandes. D'après les preuves recueillies par les chercheurs, les tâches étaient similaires à une technique utilisée par la suite pour déployer les attaques de ransomwares. Il est possible que les attaquants testent la méthode qu'ils prévoient d'utiliser.

En utilisant le compte d'administration du domaine compromis et l'accès RDP, les attaquants se déplacent latéralement sur le réseau vers d'autres serveurs critiques.

Ils utilisent Advanced IP Scanner, l'outil légitime d'analyse réseau, pour commencer à cartographier le réseau et établir des listes d'adresses IP sur lesquelles les ransomwares seront ensuite déployés. Les attaquants créent une liste distincte d'adresses IP, appartenant aux ordinateurs utilisés par les administrateurs IT de la cible.

Ensuite, ils utilisent l'outil Microsoft ntdsutil pour supprimer la base de données d'identifiants hachée d'Active Directory.

Ils exécutent diverses commandes WMI pour recueillir des informations sur les machines compromises, puis ils passent à l'exfiltration des données : Ils identifient un serveur de fichiers et, avec le compte de l'administrateur de domaine compromis, y accèdent à distance via le RDP. Ils commencent à compresser les dossiers qui s'y trouvent.

Puis ils déplacent les archives vers le contrôleur de domaine, et essaient d'installer l'application de stockage Cloud Mega sur le DC. Celle-ci est bloquée par la sécurité, alors ils passent à la version web et téléchargent les fichiers compressés.

Jour 3
L'exfiltration des données vers Mega se poursuit tout au long de la journée.

Jour 4 et 5
Aucune activité malveillante n'est observée pendant cette période. Lors d'incidents précédents, nous avons vu que les attaquants pouvaient attendre le weekend ou un jour férié, pour lancer l'attaque, lorsque l'équipe de sécurité ne travaille pas ou relâche son attention sur les activités du réseau.

Jour 6
Un dimanche. La première attaque de ransomware Maze est lancée, via le compte d'administration de domaine compromis et les listes d'adresses IP qui ont été identifiées. Plus de 700 ordinateurs sont visés par l'attaque, qui est rapidement détectée et bloquée par la sécurité. Soit les attaquants ne se rendent pas compte que l'attaque a été empêchée, soit ils espèrent encore pouvoir faire chanter la victime avec les données volées, car c'est le moment où ils émettent une demande de rançon de 15 millions de dollars.

Jour 7
L'équipe de sécurité installe une protection supplémentaire et assure une surveillance des menaces 24 h/24, 7 j/7. L'investigation sur la réponse à l'incident commence, en identifiant rapidement le compte administrateur compromis, en recherchant plusieurs fichiers malveillants et en bloquant la communication entre l'attaquant et les machines infectées.

Jour 8
D'autres outils et techniques utilisés par les criminels sont découverts, ainsi que des preuves relatives à l'exfiltration de données. D'autres fichiers et comptes sont bloqués.

Jour 9
Malgré l'activité défensive, les attaquants maintiennent leur accès au réseau et à un autre compte compromis, et lancent une deuxième attaque. Cette attaque est similaire à la première : elle exécute des commandes sur un DC, en bouclant les listes d'adresses IP contenues dans les fichiers txt.

L'attaque est rapidement identifiée. Le ransomware est automatiquement détecté et aussi bien le compte compromis que la charge utile sont désactivés et supprimés. Aucun fichier n'est chiffré.

Les criminels, qui ne sont manifestement pas prêts à abandonner, essaient de nouveau. La troisième tentative se produit quelques heures après la deuxième attaque.

Là, ils semblent désespérés, car cette attaque ne vise plus qu'un seul ordinateur. Il s'agit du principal serveur de fichiers sur lequel les données ont été exfiltrées.

Les attaquants changent d'approche et déploient une copie complète d'une machine virtuelle (VM) et un installateur d'hyperviseur VirtualBox, une attaque détaillée sur SophosLabs Uncut en septembre 2020.

Le résultat de la troisième tentative est le même : l'équipe Sophos Rapid Response parvient à détecter et à déjouer l'attaque, sans aucun chiffrement des fichiers. Sophos a réussi à verrouiller le groupe criminel, qui se retrouve dans l'impossibilité de poursuivre l'attaque.

LES MENACES QUOTIDIENNES, DES CANARIS DANS UNE MINE DE CHARBON

Si tout ce que vous savez sur les cyberattaques provient des médias, vous pourriez penser que le ciel vous tombe sur la tête ! Tous les jours les grandes entreprises sont la cible d'attaques, mais elles ne sont pas toutes extrême, comme un vol majeur de données, susceptible de ruiner une entreprise (ou faire chuter le cours de ses actions) et d'anéantir sa réputation. En fait, bon nombre d'attaques sont plutôt banales et impliquent des malwares que l'équipe des SophosLabs traque dans une liste de « Usual Suspects » les plus recherchés.

Mais bien que faciles à comprendre et à maîtriser, ces attaques, et certains des malwares qu'elles diffusent peuvent vite empirer si elles ne sont pas stoppées rapidement et efficacement. Pour reprendre la métaphore utilisée dans le titre, ces attaques routinières sont tels des canaris dans une mine de charbon, autrement dit l'alerte préliminaire d'une présence toxique qui pourrait rapidement échapper à tout contrôle.

Attaques visant les serveurs Windows et Linux

Alors que la grande majorité des incidents de sécurité auxquels nous avons répondu en 2020 concernaient des ordinateurs portables ou de bureau opérant sous des variantes de Windows, nous avons constaté une hausse constante des attaques sur les serveurs Windows et non Windows. En fait, les serveurs sont depuis longtemps des cibles très intéressantes pour diverses raisons : Ils opèrent souvent pendant de longues périodes sans surveillance ; ils ont souvent une plus grande capacité de processeur et de mémoire que les ordinateurs portables personnels ; et ils peuvent occuper un espace privilégié sur le réseau, ayant souvent accès aux données les plus sensibles et les plus précieuses de l'organisation. Ils constituent donc un point d'ancrage intéressant pour les attaquants. Ce constat ne changera pas en 2021 et Sophos prévoit que le nombre des attaques visant les serveurs continuera de croître.

La plupart des attaques ciblant les serveurs correspondent à l'un des trois profils suivants : ransomwares, cryptomineurs et exfiltration de données, chacun utilisant un ensemble de tactiques et de techniques propre. Les bonnes pratiques pour les administrateurs de serveurs consistent à éviter d'installer des applications classiques de bureau, de type client de messagerie ou navigateur web, sur le serveur pour bloquer toute infection, ce qui oblige les attaques ciblant les serveurs à changer de tactique.

Les serveurs en ligne sous Windows subissent une avalanche interminable de tentatives d'attaque RDP par force brute, une tactique d'attaque qui, depuis au moins trois ans, est le plus souvent associée et prédictive d'attaques de ransomwares. D'après les observations de l'équipe Sophos Rapid Response, la cause première des attaques de ransomwares sur lesquelles elle enquête consiste souvent à d'abord accéder au réseau cible via des connexions RDP, puis à utiliser ces machines pour pénétrer au sein du réseau et contrôler les serveurs DC, qui permettront de piloter le reste de l'attaque.

Les attaques de cryptojacking, en revanche, ont tendance à viser un plus large éventail de vulnérabilités dans Windows et dans les applications normalement exécutées sur serveurs, comme les logiciels de base de données.

Par exemple, l'une des méthodes utilisées par le cryptomineur Lemon_Duck consiste en une attaque par force brute contre des serveurs connectés à Internet et opérants sous Microsoft SQL Server. Dès que les attaquants ont deviné le mot de passe de la base de données, ils utilisent cette même base de données pour reconstituer la charge utile du cryptojacker, l'écrire sur le système de fichiers du serveur et l'exécuter. La machine infectée tente alors d'exploiter les vulnérabilités EternalBlue ou SMBGhost dans le but de propager le cryptojacker.

Lemon_Duck est une attaque qui procède de la même manière pour infecter les serveurs Linux. Le malware tente de forcer des mots de passe SSH issus d'une liste relativement courte. En cas de succès, les attaquants uploadent un shellcode malveillant pour établir ensuite la persistance en exploitant les failles d'un service appelé Redis. Le cryptojacker peut également se dissimuler en exécutant les commandes pour se lancer depuis des clusters Hadoop.

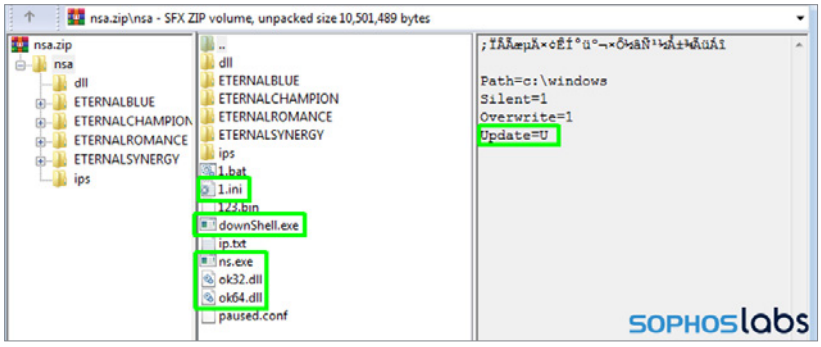


Fig.3. L'un des cryptojackers les plus prolifiques, appelé MyKings, a distribué les composants responsables de l'installation du botnet (surligné en vert) dans une archive Zip ainsi que plusieurs des exploits divulgués par les Shadow Brokers de la NSA. Source : SophosLabs.

Parfois, les attaquants ciblent les serveurs parce que, plutôt que de recevoir une somme fixe ou de se faire payer au compte-gouttes en cryptomonnaie, ils préfèrent voler les données de valeur qui y sont stockées. En 2020, Sophos a identifié un attaquant qui ciblait les serveurs Linux en utilisant un malware que nous avons appelé Cloud Snooper. Les serveurs en question étaient hébergés dans un cluster du Cloud et ont échappé à la détection en créant un système intelligent de relais de messages et en transposant leurs messages C&C sur des connexions HTTP de routine.

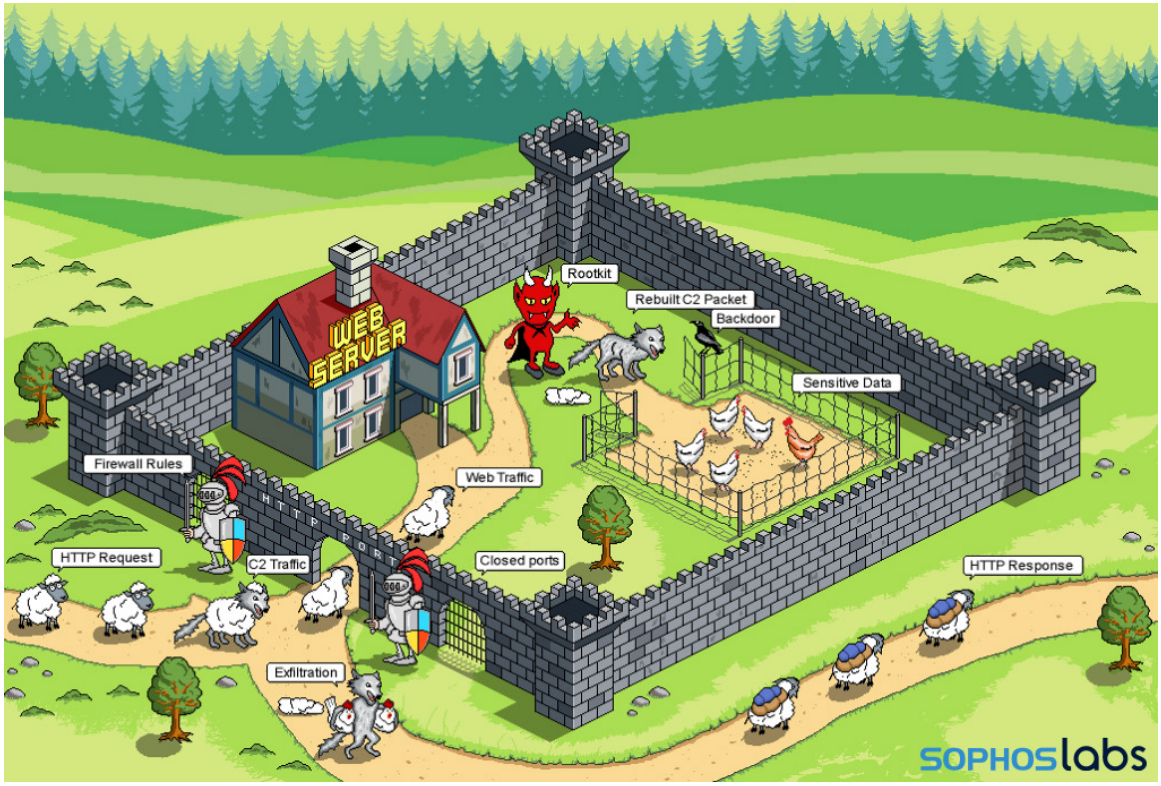


Fig.4. Illustration de la métaphore du « loup déguisé en agneau » : le malware APT Cloud Snooper dissimulait ses commandes et exfiltrait des données sous la forme de requêtes et de réponses HTTP classiques, à l'aide d'un outil qui surveillait le trafic réseau et réécrivait les paquets TCP/IP en temps réel. Source : SophosLabs.

Auparavant, les administrateurs de serveurs n'installaient pas de protection Endpoint sur les serveurs, mais avec l'arrivée de ce type d'attaques, la donne a changé.

Sous-estimer les malwares « de base », à ses risques et périls

Tout le monde n'est pas affecté par une vulnérabilité de type Zero Day due à une menace persistante avancée (Advanced Persistent Threat). La plupart des attaques sont le fruit de malwares ordinaires diffusés par des moyens conventionnels, c'est à dire généralement un email de spam, une pièce jointe ou un lien d'apparence inoffensive, mais très persuasive pour inciter la cible à les ouvrir. Sophos reçoit chaque mois des milliers de résultats télémétriques portant sur ces malwares courants, signe habituellement qu'un ordinateur protégé par l'un de nos produits a bloqué l'attaque.

Sur les ordinateurs non protégés, où il peut s'exécuter pleinement, le malware établit le profil de l'ordinateur de la cible ; il extrait tous les identifiants de connexion ou les mots de passe enregistrés pour les sites web qui donnent accès des données confidentielles (en général les comptes bancaires ou autres services financiers, mais pas seulement) ; puis il renvoie ces informations à ses opérateurs et attend de nouvelles instructions, qui peuvent arriver quelques secondes ou quelques jours plus tard.

Mais ne vous laissez pas berner par le fait que ces familles de malwares ne soient que de simples *menaces ordinaires*, ce qui vous donnerait un faux sentiment de sécurité. Ce sont de véritables bourreaux de travail malveillants, qui peuvent causer d'énormes problèmes si on les laisse persister. Comme nous l'avons déjà évoqué, l'équipe des SophosLabs tient une liste des malwares les plus recherchés et dispose d'analystes dédiés à ces familles persistantes. Voici ci-dessous une brève présentation des plus importants.

Dridex et Zloader

L'un des types de malwares les plus courants est le « loader » ou chargeur. Les chargeurs ont pour fonction de livrer une autre charge utile de malware au nom de leurs opérateurs ou d'individus qui ont un contrat avec leurs opérateurs. Les familles de malwares Dridex et Zloader sont toutes deux des plates-formes de chargeurs bien établies. Les attaquants utilisent à la fois Dridex et Zloader pour collecter des informations sur le système cible et les renvoyer aux criminels, qui peuvent décider quels composants ou charges utiles ils livreront, en fonction des informations que le bot leur renvoie.

Le but principal du chargeur Dridex est de contacter son serveur C&C (C2), de récupérer une ou plusieurs charges utiles chiffrées et de les déployer. Il est très difficile pour les analystes d'obtenir ces charges utiles, car les opérateurs ne les distribuent qu'en fonction des besoins, dans le cas par ex. d'un VNC (système de contrôle à distance) caché ou d'un proxy SOCKS. Ces charges utiles donnent aux attaquants la possibilité d'effectuer des opérations au niveau du périphérique de l'utilisateur. Elles permettent également aux criminels d'accéder aux ressources sur le système de la victime, qu'ils ne peuvent pas atteindre directement depuis leur propre système.

La logique côté serveur qui définit ce qui se passe lors d'une infection peut être insondable, mais nous pouvons en déduire certaines règles, car les bots n'infectent pas les ordinateurs utilisés par les analystes de malwares. Le bot envoie à ses opérateurs une liste des programmes installés ; s'il y a des outils d'analyse ou des composants de machines virtuelles, les bots n'envoient pas de charge utile à cette machine. Dans le cas de Zloader, les opérateurs diffusent le malware par un message de spam ; si vous mettez trop de temps à infecter votre ordinateur (dans les huit à douze heures suivant l'envoi du spam), ils cessent d'envoyer des charges utiles.

De plus, la machine doit être propre, mais pas trop on plus. Une installation basique de Windows ne déclenchera rien, mais un ordinateur ultra chargé avec beaucoup d'outils non plus.

Agent Tesla et RATicate, infostealers et RAT

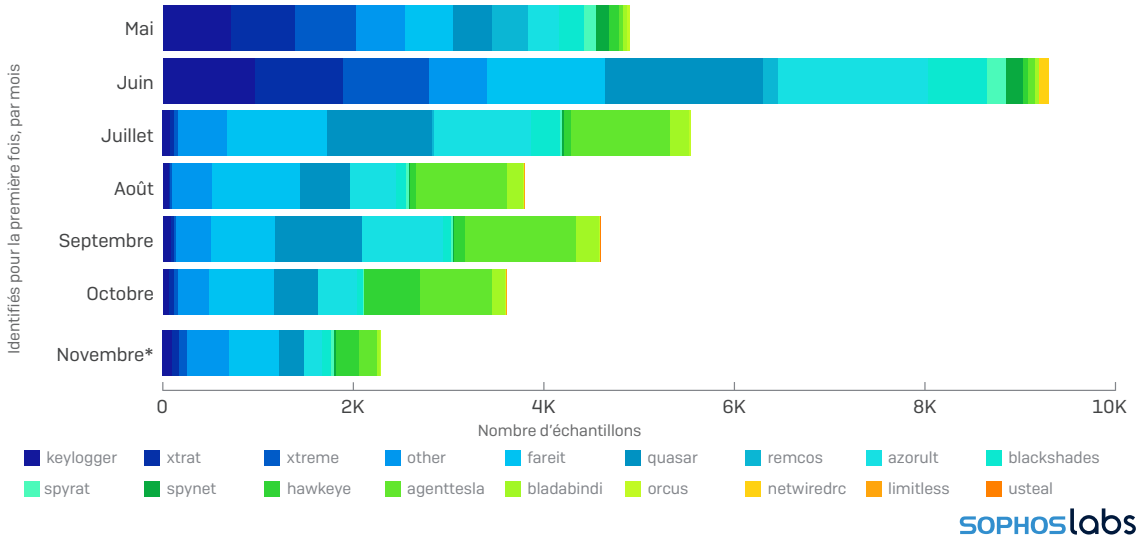


Fig.5. Nous analysons tous les échantillons de malwares de type RAT récemment découverts via notre système interne de sandboxing. Ce tableau illustre le nombre de nouveaux échantillons uniques que nous avons identifiés sur une période de sept mois et que nous avons ensuite classés dans l'une des 18 familles de RAT les plus courantes, en fonction des noms de famille. * Données partielles sur le mois Source : SophosLabs.

Les chevaux de Troie d'administration à distance ou RAT (Remote Access Trojan) et les infostealers comptent parmi les formes les plus anciennes de malwares. Comme leur nom l'indique, les RAT donnent à l'attaquant la possibilité de contrôler l'ordinateur infecté à distance. Les infostealers, littéralement « voleurs d'infos », sont des trojans conçus pour collecter et exfiltrer des informations précieuses comme les identifiants, les certificats et autres données sensibles. Deux des familles de notre liste les « plus recherchées » que nous avons rencontrées au cours de cette année sont l'Agent Tesla (un infostealeur) et RATicate (un RAT).

Comme les chargeurs, les RAT disposent généralement d'un mécanisme leur permettant de livrer des charges utiles supplémentaires, et notamment des mises à jour d'elles-mêmes. Selon nos observations, le RATicate peut distribuer d'autres malwares, y compris l'Agent Tesla. Nous avons également vu ces familles de RAT être diffusées à partir des mêmes adresses IP ou serveurs, ou communiquer avec eux, ce qui laisse supposer un partage entre des groupes normalement non apparentés.

Démantèlement de Trickbot

Depuis quatre ans au moins, Trickbot est connu pour être un malware persistant. Ce botnet, malheureusement célèbre, est à l'origine de nombreux comportements et caractéristiques devenus courants aujourd'hui, par exemple, le fait de communiquer avec son infrastructure C2 en utilisant le protocole TLS. Impliqué dans plusieurs attaques de ransomwares qui ont fait parler d'elles, c'est un voleur d'identifiants très compétent.

```
    "type"   :  "TEXT",
    "size"   :  101
  },
  "controllers"   :  [   {
    "url"   :  "https://127.0.0.1.1"
  }  ],
  "controllers"   :  {
```

SOPHOSlabs

Fig.6. Trickbot a été démantelé par une seule ligne de code. Source : SophosLabs.

En octobre 2020, alors que nous préparions ce rapport, Microsoft et le ministère américain de la justice ont annoncé qu'ils avaient saisi plusieurs serveurs et envoyé une commande via le système C&C du botnet, qui empêchait celui-ci de communiquer (d'environ 90 %) avec le centre C&C.

Les enquêteurs ont réussi à uploader une configuration « empoisonnée » dans l'infrastructure de Trickbot que chaque bot a ensuite téléchargée. La configuration a fait croire au botnet que son principal serveur de C&C était la machine infectée sur laquelle il fonctionnait. Le botnet a alors perdu le contact avec les véritables serveurs C2 et ne pouvait plus récupérer les charges utiles ou les instructions.

Ce succès a eu un fort impact sur l'opérateur de Trickbot, mais on s'attend à ce qu'il revienne, lentement mais surement, à un fonctionnement normal.

Mécanismes de diffusion

Pour atteindre une machine cible ou pénétrer un réseau, les malwares ou les attaquants ont en fait un nombre limité de moyens. La plupart des attaques reposent sur des méthodes bien connues, comme l'utilisation d'un email contenant des liens ou des pièces jointes d'un fichier malveillant. L'attaquant peut aussi jouer un rôle plus actif en ciblant le RDP ou un autre service vulnérable hébergé sur le périmètre réseau connecté à Internet.

RDP, le premier vecteur d'attaque pour les ransomwares

Le protocole RDP ou Remote Desktop Protocol est un service standard disponible dans toutes les versions actuelles de Windows. Moyennant très peu d'efforts, le RDP permet aux administrateurs ou aux utilisateurs de se connecter à un ordinateur lorsqu'ils ne sont pas physiquement en présence de ce celui-ci, ce qui est très utile en cas de pandémie où tout le monde est soudainement obligé de télétravailler. Malheureusement, depuis trois ans, les acteurs de ransomwares abusent (à un rythme effréné) de cette même plate-forme d'accès à distance pour causer des dommages à grande échelle, extorquant au passage des sommes de plus en plus énormes aux grandes entreprises ciblées.

Tentatives de connexion au RDP par honeypot

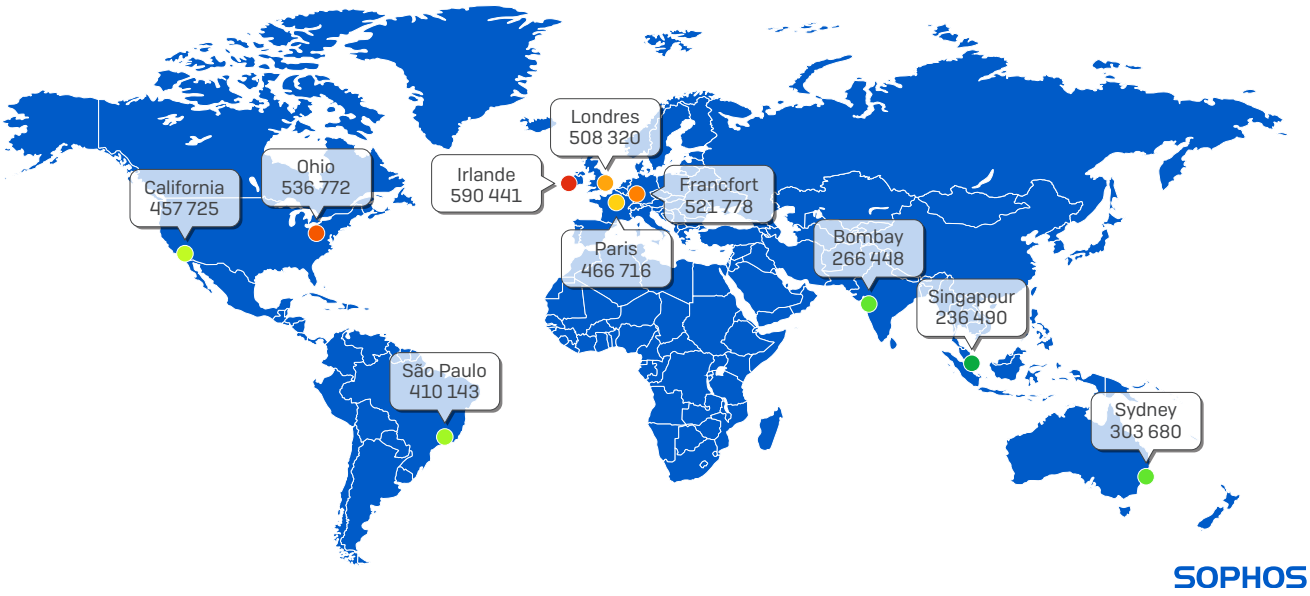


Fig.7. Nous avons distribué des honeypots (pots de miel) aux data centers du monde entier et avons laisser les criminels attaquer par force brute. Les machines pots de miel ont été découvertes de manière « organique », sans aucune publicité. Cette carte illustre le nombre d'attaques reçues par chaque pot de miel sur un mois de test.

Le phénomène de confinement dû au Covid-19 ne fait qu'exacerber le problème, car un nombre croissant d'organisations et de travailleurs sont contraints de recourir au RDP pour rester opérationnels. Le principal problème est que le RDP n'a jamais été conçu pour faire face au type d'attaques qu'il peut recevoir d'Internet. Si le mot de passe RDP est faible, facile à deviner ou forcé par des tentatives de connexion automatisées, l'attaquant peut pénétrer le réseau et l'exploiter à sa guise.

Selon l'équipe Sophos qui gère la réponse aux incidents majeurs, le RDP reste l'une des principales causes des incidents de ransomwares qu'elle doit traiter. Les conseils aux responsables informatiques restent les mêmes : D'une part, le RDP ne doit jamais être connecté à Internet, mais plutôt être placé derrière un pare-feu obligeant les utilisateurs à se connecter d'abord via un VPN ou un autre dispositif Zero Trust (confiance zéro). D'autre part, les administrateurs doivent renforcer les politiques de mots de passe Windows avec des mots de passe plus longs et un token (jeton) ou une application d'authentification multifacteurs.

Dans le cadre d'une recherche menée avant l'entrée en vigueur du confinement, Sophos a installé des honeypots dans dix data centers à travers le monde pour mieux évaluer l'ampleur du problème. Sur une période de 30 jours, les honeypots ont reçu une moyenne de 467 000 tentatives de connexion RDP, soit environ 600 par heure sur chaque site. Les analyses montrent que ces tentatives ont été lancées sur chaque pot de miel avec une fréquence et un acharnement en augmentation constante jusqu'à ce que Sophos mette fin à l'opération.

Top 5 des noms d'utilisateur utilisés dans tous les échecs de connexion

NOM D'UTILISATEUR	ÉCHECS DE TENTATIVES DE CONNEXION
administrateur	2 647 428
admin	376 206
utilisateur	79 384
ssm-user	53 447
test	42 117

Fig.8. Les tentatives d'attaques par force brute sur le bureau distant visent les noms d'utilisateur Windows les plus courants, notamment le compte par défaut « administrateur ».

Source : SophosLabs.

Business Email Compromise et Business Email Spoofing

Business Email Compromise ou BEC (Compromission de courrier électronique professionnel) est le nom officiel d'un type de spam qui a pour but une demande d'argent frauduleuse. Dans une attaque BEC classique, un spammeur envoie un message à un salarié, qui semble provenir d'un cadre hiérarchique, en lui demandant d'effectuer un transfert financier ou de réaliser un achat important en son nom. Pour ce faire, l'attaquant peut par exemple usurper l'apparence des emails internes à la société (tactique du Business Email Spoofing) ou essayer de prendre le contrôle des comptes sur le propre serveur de messagerie de l'organisation, et utiliser ce compte pour envoyer la demande frauduleuse.

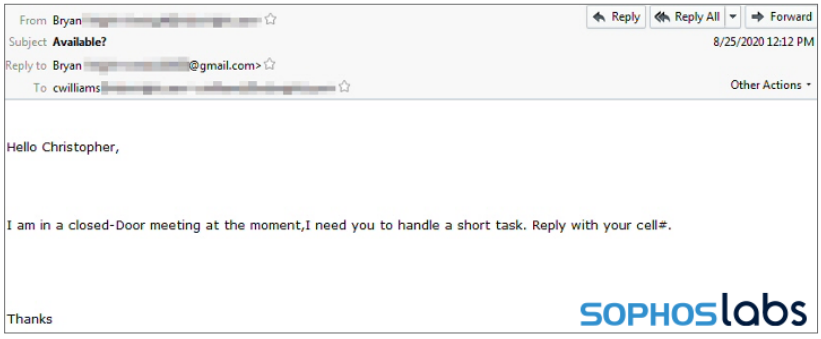


Fig.9. Dans cet exemple BEC de la vie réelle, le fraudeur se faisant passer pour un cadre hiérarchique, demande à un employé de répondre à une demande urgente. L'email a une adresse de réponse (vers un compte Gmail) différente de celle de l'en-tête « From », ce qui laisse supposer quelque chose de louche — si la cible est capable de le remarquer. Source : SophosLabs.

L'attaquant, se faisant passer pour un supérieur hiérarchique, peut demander à l'employé visé d'acheter des cartes-cadeaux coûteuses ou d'accélérer une transaction financière quelconque. Les attaques sont généralement parfaitement adaptées à l'individu ou à l'organisation visés. Les emails BEC ne ressemblent en rien à du spam malveillant, car ils ne suivent pas les mêmes schémas. Souvent, ils ne contiennent pas de pièce jointe ou de lien malveillant et ils donnent l'impression de provenir de l'organisation cible, incorporant même parfois des « signatures » typiques de l'entreprise ou d'autres éléments familiers pour les employés, afin de les rendre plus convaincants à leurs yeux.

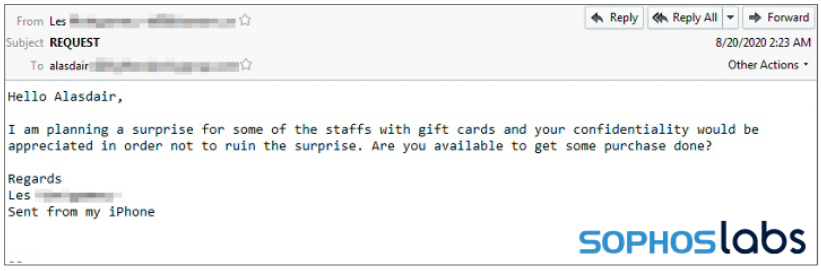


Fig. 10. Dès que la cible accuse réception de la demande initiale, le fraudeur fait sa demande, avec un prétexte qui semble plausible. Source : SophosLabs.

Les BEC reposent sur une double condition : que la cible (l'employé) soit physiquement distante de l'objet de l'escroquerie (le supérieur hiérarchique) et qu'elle agisse rapidement, avant que quiconque ne puisse comprendre ce qui se passe et l'empêche d'effectuer l'opération demandée. L'escroc peut rédiger son email lorsqu'il sait que le cadre est absent ou en déplacement pour affaires.

Ce type de demande frauduleuse implique souvent un échange de messages entre l'attaquant et la cible. L'attaquant peut commencer par solliciter un simple accusé de réception de la part de la cible, puis, après un échange de quelques emails, finir par lui demander d'effectuer un achat en prétextant une excuse plausible.

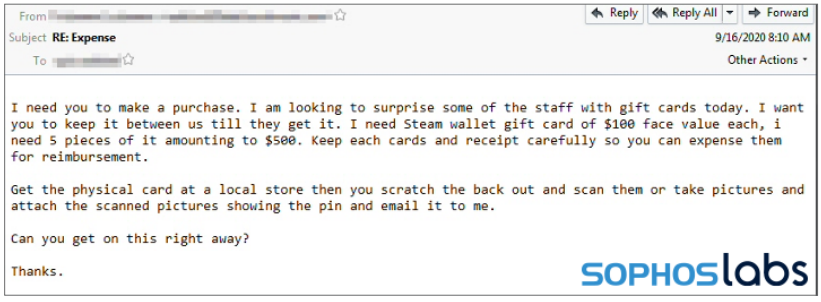


Fig.11. À un moment donné de l'attaque, le scammeur va faire une demande totalement inattendue et opportune, comme celle de faire un virement bancaire urgent vers un compte inconnu de la cible. Ce qui amène l'employé méfiant à remettre en question la nature de la demande : pourquoi ce supérieur aurait-il besoin d'une photo du dos de la carte cadeau avec le code PIN découvert alors qu'elle va être donnée en cadeau ? Source : SophosLabs.

Lorsque la plupart d'entre nous travaillent encore en présentiel, la proximité physique entre la cible et le sujet aurait rendu l'escroquerie tout de suite évidente. Mais avec le contexte de télétravail actuel, où les deux protagonistes ne sont probablement pas dans le même bureau, l'employé a moins de chances de se déplacer auprès de son supérieur pour lui demander de confirmer sa demande.

Les scams de ce type existaient bien avant l'avènement du Covid-19, mais comme de plus en plus d'individus travaillent à distance, les auteurs de BEC profitent de la situation. C'est une attaque plutôt perverse dans un sens, car elle exploite la nature humaine qui tend tout simplement à être aimable et serviable. Si vous êtes confronté à ce genre d'emails, fiez-vous à votre instinct et, si possible, n'hésitez à contacter directement l'expéditeur ou demander conseil à une autre personne si vous ne pouvez pas le joindre. Plus l'employé s'implique dans la gestion de ces demandes, plus il est probable que le scam soit découvert avant que le mal ne soit fait.

Science obscure, l'ancien bug Office frappe à nouveau

En ce qui concerne les fichiers Office malveillants (maldocs) et les exploits qu'ils tentent de déployer, on observe beaucoup de recyclage. Le problème disparaît dès lors que Microsoft sort une nouvelle mise à jour et puis, parfois, il refait surface. Depuis des années, les SophosLabs suivent la façon dont les attaquants intègrent leurs exploits divers et variés dans les maldocs. Les vulnérabilités récentes sont souvent exploitées par les criminels qui utilisent les maldocs comme vecteurs pour diffuser des charges utiles. En effet, tout le monde n'installe pas immédiatement les correctifs et parfois les éditeurs de sécurité prennent un peu de temps pour mettre en place une réponse efficace, basée sur le comportement ou d'autres caractéristiques d'un nouveau vecteur.

La plupart des maldocs que nous avons observés cette dernière année ont été conçus avec des outils appelés « builders ». Ces derniers offrent aux attaquants un système de menu de type « pointer-cliquer » qui leur permet de décider exactement quel(s) exploit(s) intégrer dans le document malveillant. Mais alors qu'on améliore les outils de sécurité Endpoint pour identifier ces exploits plus modernes, ce qui implique généralement un script intégré au document, les auteurs de maldocs n'abandonnent pas. Ils semblent avoir creusé encore davantage pour trouver un très vieux bug, aidant à dissimuler les macros ou d'autres contenus malveillants dans les documents.

Ce bug est familièrement connu sous le nom d'exploit **VelvetSweatshop**, même s'il ne s'agit pas vraiment d'un exploit. En fait, VelvetSweatshop a été introduit par Microsoft dans Microsoft Office 2003, bien qu'il n'ait été utilisé qu'en 2013, lorsque les classeurs Excel exploitant la vulnérabilité CVE-2012-0158 ont été dissimulés par le bug. Une feuille de calcul Excel ou un fichier Word .doc indiqué « en lecture seule » n'est qu'un document protégé par un mot de passe avec un mot de passe de base provenant, vous l'aurez deviné, de VelvetSweatshop.

Nous avons vu circuler beaucoup de feuilles de calcul Excel malveillantes cette année, qui utilisaient cette technique comme moyen d'échapper à la détection avancée des menaces. Avec le chiffrement, le véritable contenu malveillant est caché derrière une forte cryptographie, impossible à identifier ou déchiffrer par les scanners à moins de prendre en charge le dernier algorithme utilisé par les attaquants. En utilisant le mot de passe par défaut, Excel ouvre le contenu décodé sans demander le mot de passe de sorte que, au niveau de l'exécution, le chiffrement est transparent. Les programmes de sécurité Endpoint ont ajouté la prise en charge du chiffrement et du mot de passe par défaut, mais les criminels continuent de trouver des algorithmes cryptographiques supplémentaires qui ont la même caractéristique et ne sont pas (encore) mis en œuvre par les contrôles antivirus.

Nous avons même découvert un bug si obsolète que, transposé à l'âge humain, il aurait déjà terminé toute sa scolarité ! Mais après tout, il n'est pas surprenant que les auteurs de documents malveillants tentent d'en tirer profit.

Sécurité des données : une rétrospective sur 20 ans

Si ce rapport annuel nous donne l'occasion de revenir sur les événements importants de l'année écoulée, nous avons pensé qu'une rétrospective plus étalée, sur les deux dernières décennies, nous permettrait de mieux appréhender comment nous sommes arrivés au contexte actuel. Le tournant du millénaire a marqué une étape importante, lorsque la sécurité des informations est devenue une discipline et une industrie en soi. Cette chronologie des menaces et des événements montre les moments significatifs et représentatifs de l'évolution du comportement des menaces.

Alors qu'à la fois les entreprises et les particuliers adoptaient Internet pour les affaires et les loisirs, les grands réseaux sont devenus des cibles mûres pour l'émergence de vers prolifiques : les malwares auto-propagateurs. Au total, les vers auront infecté des dizaines de millions de systèmes dans le monde entier et ont coûté plus de cent milliards de dollars en dommages et en coûts de correction.

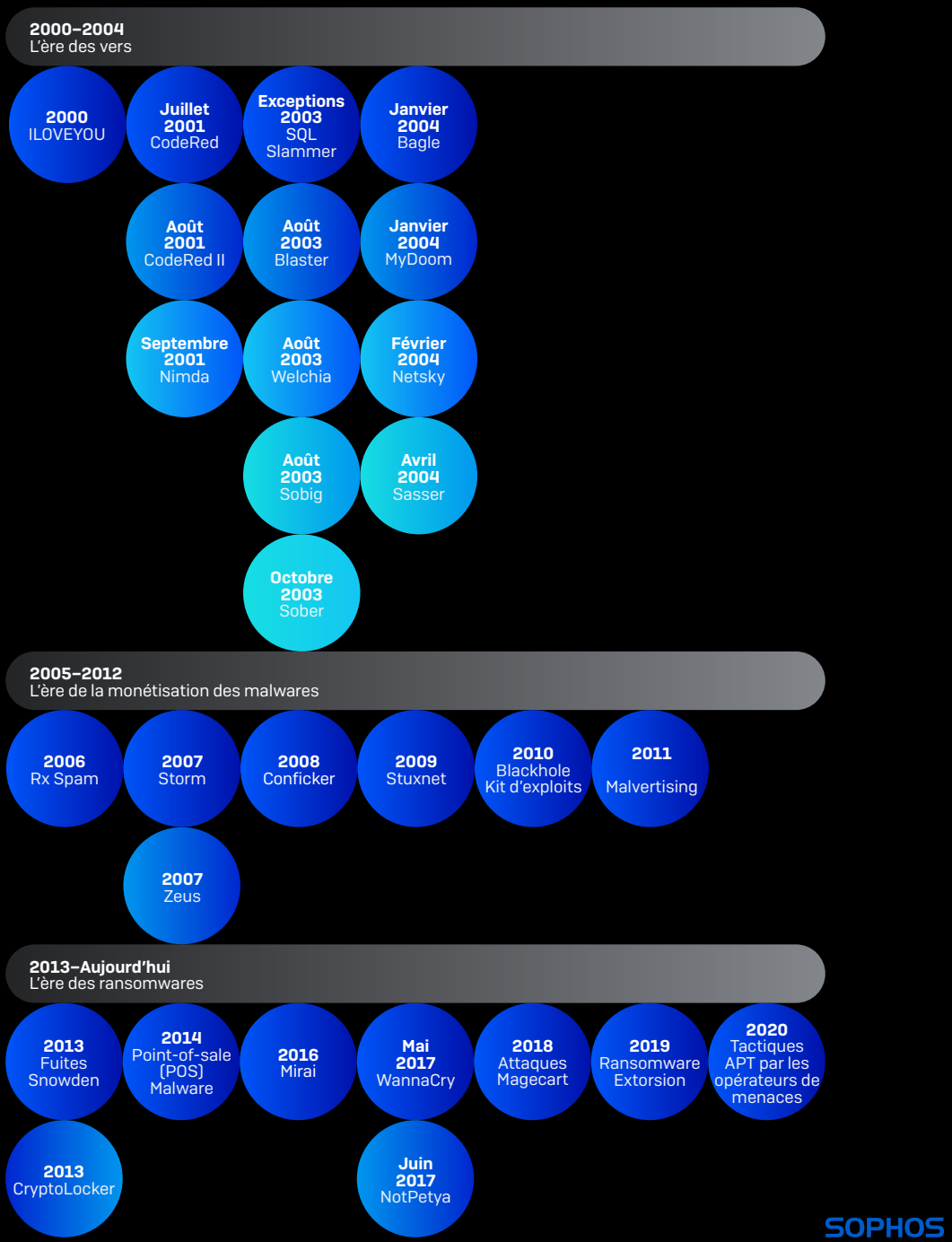


Fig.12. Source : Sophos

2000-2004 - L'ère des vers

2000 - ILOVEYOU
Le ver ILOVEYOU a utilisé une tactique d'ingénierie sociale qui persiste encore aujourd'hui : Arrivant sous la forme d'une pièce jointe à un spam, il infecte environ 10 % de tous les ordinateurs Windows connectés à Internet.

Juillet 2001 - CodeRed
Tirant son nom de la boisson américaine Mountain Dew que ses auteurs buvaient à l'époque, CodeRed a utilisé une vulnérabilité de dépassement de la mémoire tampon dans IIS pour se propager et dégrader des sites web. Un mois plus tard, il a été suivi par une version actualisée qui a installé une porte dérobée sur les ordinateurs en réseau.

Août 2001 - CodeRed II

Septembre 2001 - Nimda

Janvier 2003 - SQL Slammer
Avec seulement 376 octets, Slammer a su exploiter un dépassement de la mémoire tampon dans les applications de base de données de Microsoft. Doublant ses infections toutes les 8,5 secondes, il a anéanti de larges portions d'Internet en seulement 15 minutes.

Août 2003 - Blaster
Blaster a été créé par rétro-ingénierie d'un correctif Microsoft quelques mois avant le premier Patch Tuesday. Il a exploité une vulnérabilité de dépassement de la mémoire tampon dans le service RPC des systèmes Windows XP et 2000 et a lancé une attaque DDoS contre windowsupdate.com si le jour du mois était supérieur au 15 ou si le mois était septembre ou après.

Août 2003 - Welchia

Août 2003 - Sobig

Octobre 2003 - Sober

Janvier 2004 - Bagle

Janvier 2004 - MyDoom
On estime que 25 % de tous les emails envoyés en 2004 provenaient du ver MyDoom, envoyé en masse à de nouvelles victimes et impliqué dans une attaque par déni de service (DDoS).

Février 2004 - Netsky

Avril 2004 - Sasser

2005-2012 - L'ère de la monétisation des malwares
Jusqu'en 2005 environ, les incidents dus aux malwares suscitaient la curiosité, ne causant que de « simples perturbations ». Les malwares de type botnet, discrets, mais lucratifs, dominaient. Cette époque a également vu le début du « spam pharmaceutique ». Les exploits contre les vulnérabilités logicielles sont devenus des éléments clés des malwares, ce qui a permis le développement du malvertising. Partout où il y avait un potentiel de gain financier, les cybercriminels ont exploité ces opportunités.

2006 - Rx Spam
Ce qui au départ n'était qu'un moyen de propager des vers est devenu un commerce lucratif, utilisant du spam publicitaire pour vendre principalement des médicaments sur ordonnance contrefaits. On estime que les spammeurs pharmaceutiques ont gagné des milliards de dollars avec ces médicaments que la plupart des gens pouvaient obtenir en allant simplement chez leur médecin.

2007 - Storm

2007 - Zeus

2008 - Conficker
Conficker a infecté des millions d'ordinateurs dans le monde entier, mais n'a pas causé beaucoup de dommages. Nous ne connaissons toujours pas le véritable objectif du ver, mais des milliers d'hôtes restent infectés à ce jour, et le trafic de Conficker est régulièrement détecté comme « un fond diffus » d'Internet.

2009 - Stuxnet
Stuxnet a été l'une des premières armes numériques à cibler un système physique : des centrifugeuses nucléaires utilisées par l'Iran pour enrichir l'uranium. L'héritage de Stuxnet est d'avoir ouvert la porte de manière permanente à l'utilisation de malwares par les États comme outil de guerre.

2010 - Kit d'exploits Blackhole
Les kits d'exploits — des boîtes à outils ciblant les vulnérabilités des logiciels — ont réuni différentes parties de l'écosystème de la cybercriminalité. Le crimeware « as a service » est né lorsque les créateurs du kit d'exploits Blackhole ont commencé à proposer leurs services.

2011 - Malvertising

2013 à aujourd'hui - L'ère du ransomware
Ce sont les ransomwares qui marquent le plus cette période. Alors que les vers, les chevaux de Troie bancaires, le malvertising et le spam persistent, aucune autre menace n'est venue rivaliser avec la force destructrice des ransomwares. Les dommages causés par les attaques de ransomwares au cours des sept dernières années s'évaluent en trillions de dollars. Ils sont aussi très probablement la première forme de malware liée à une mort humaine. En fait, de nombreuses menaces actuelles finissent par diffuser des ransomwares et, comme les kits d'exploits, elles ont donné le turbo à un écosystème cybercriminel déjà florissant.

2013 - Fuites Snowden leaks

2013 - CryptoLocker
Au cours de sa courte existence, CryptoLocker a fourni aux futurs criminels une combinaison gagnante en associant deux technologies existantes : le chiffrement et les cryptomonnaies. CryptoLocker a changé à jamais le panorama des menaces et ses répercussions se font encore sentir aujourd'hui. Trois mois après son lancement, le portefeuille de bitcoin utilisé par CryptoLocker contenait près de 30 millions de dollars.

2014 - Malware POS (Point-of-sale)

2016 - Mirai

May 2017 - WannaCry
WannaCry, l'hybride ver-ransomware le plus répandu, a démontré (une fois de plus) qu'une défaillance dans l'application des correctifs peut avoir des conséquences désastreuses. Il a utilisé des exploits volés à la NSA et rendus publics par The Shadow Brokers. Ces attaques ont forcé Microsoft à publier des mises à jour hors bande pour des produits non pris en charge.

Juin 2017 - NotPetya
NotPetya a paralysé certaines des plus grandes sociétés de transport et de logistique du monde, et aurait causé plus de 10 milliards de dollars de dommages. Certaines entreprises touchées ne se sont pas encore totalement remises de cette catastrophe.

2018 - Attaques Magecart

2019 - Ransomware Extorsion
Lors d'une attaque contre la ville de Johannesburg, en Afrique du Sud, les criminels derrière le ransomware Maze ont été les premiers à utiliser l'extorsion. Après avoir chiffré et volé des données, ils ont également menacé de publier les données volées si les entreprises ne payaient pas. Cette tactique a été reprise par de nombreux autres gangs de criminels pour se prémunir face aux cibles ayant de bonnes sauvegardes.

2020 - Tactiques APT par les opérateurs de menaces
L'adoption des outils et des tactiques par les États, qui a débuté au cours des deux dernières années, s'est généralisée en 2020. Les gangs professionnels utilisent des outils sophistiqués comme Cobalt Strike qui ont un effet dévastateur, alors que d'autres groupes (Dharma) en font des kits d'outils « point-and-shoot » à l'intention des novices.

L'EFFET DÉMULTIPLICATEUR DU COVID-19 SUR LES ATTAQUES

Le coronavirus Covid-19 a eu un impact considérable sur tous les aspects de la cybersécurité. Les attaquants se sont sentis enhardis à cibler la nouvelle vague de télétravailleurs. La vague de peur et d'anxiété généralisée au sein de la population mondiale s'est vue exacerbée par les campagnes de spam, les ransomwares visant des institutions affaiblies ou brisées, mais aussi la société civile déjà sous pression financière, et toutes sortes de fraudes lucratives, avec recherche de profits tirés de la rareté de tout, des masques jusqu'au papier toilette.

La maison, le nouveau périmètre

Notre « normalité » a complètement basculé en mars 2020 lorsque, aussi bien les salariés que les élèves et étudiants de tous niveaux se sont vus renvoyés chez eux dans une course effrénée pour stopper la propagation du Covid-19 et soulager la pression sur les hôpitaux surchargés. Soudain, nous ne savions plus trop si nous travaillions à la maison ou vivions au travail !

Beaucoup de gens ont eu du mal à trouver une nouvelle « normalité » sans avoir à se rendre au bureau. La demande d'accès aux VPN et aux services d'authentification multifacteurs a explosé. Les Chromebooks sont devenus une denrée rare. En deux mois, Zoom a connu une croissance évolutive d'une dizaine d'années. Et pendant toute cette période, Microsoft, Adobe, Apple et Google n'ont cessé de publier des mises à jour et des correctifs de maintenance pour une multitude de plates-formes.

Covid-19 et arnaques par email en hausse

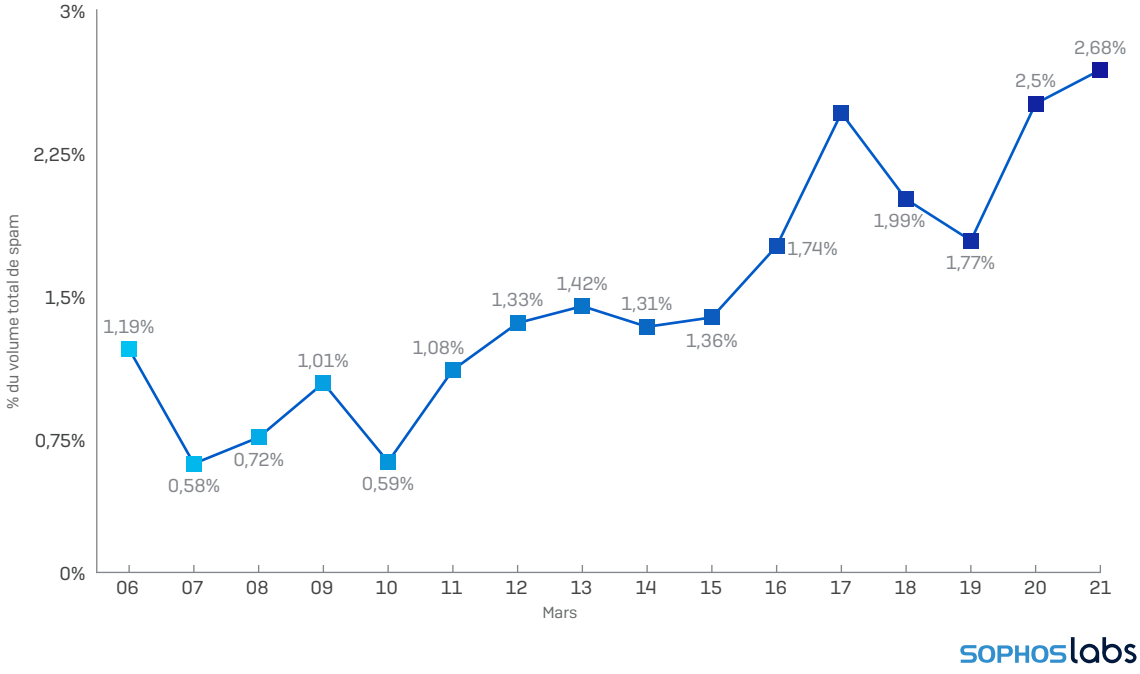


Fig.13. À l'échelle mondiale, une grande partie des spams contenait le terme Covid-19 ou Coronavirus dans les semaines suivant le confinement. Source : SophosLabs.

Avec le Covid-19, nous avons dû nous improviser informaticiens, devant gérer les correctifs, les mises à jour de sécurité et les problèmes de connectivité qui nous empêchaient d'assister aux réunions ou aux cours virtuels des enfants. La demande pour les casques, les microphones, un meilleur éclairage ou une meilleure sécurité a grimpé en flèche, aussi bien pour les postes de travail que pour les réseaux. Il a donc fallu donner aux enfants un cours accéléré sur le phishing, le spam, les fraudes en ligne, la cyber-intimidation et les malwares, déguisé en votre jeu préféré, prêt à l'emploi.

Cela n'a pas été facile, et on ne fonctionne toujours pas comme en février 2020, mais pour beaucoup d'individus, la nouvelle normalité pourrait, d'une certaine manière, constituer une amélioration. En effet, de nombreuses entreprises ont décidé de continuer à autoriser le travail à distance même après la fin du confinement et le fait que les salariés pouvaient retourner au travail, et cela pourrait présenter des avantages considérables tant pour leur qualité de vie que pour l'environnement.

Comme les périmètres de travail s'élargissent pour englober davantage d'individus sur leurs sites distants, nous devons reconsidérer avec bien plus de sérieux le rôle des réseaux domestiques qui sont désormais la dernière ligne de défense. Le modem planqué sous l'escalier ou dans le coin du salon constitue aujourd'hui le nouveau périmètre réseau. Et nous devons repenser complètement notre façon de le sécuriser.

Crimeware as a service

Les créateurs de malwares fonctionnent en quelque sorte comme des start-up. Au début, ils rencontrent des difficultés puis ils finissent par fidéliser des clients. Et il peut y avoir autant de business models que dans le cas des logiciels légitimes.

Le terme « crimeware » est volontairement vague. Certains auteurs de malwares, ou d'outils permettant de diffuser facilement des malwares ou de les enrichir de nouvelles fonctionnalités, ne vendent pas directement leur produit, mais le cèdent sous forme de licence comme vous pourriez acheter une licence annuelle de la suite Adobe Creative. Nous avons appelé cette catégorie de business model « crimeware-as-a-service » (CaaS) et d'après nos observations, elle pourrait devenir la nouvelle norme.

L'un des exemples les plus notoires de ce type de malware est Emotet. Ce cheval de Troie diffusé par spam existe depuis des années et semble offrir une expérience sans heurts pour le criminel en puissance. Emotet fait partie de cette catégorie de malwares que les chercheurs en sécurité appellent communément des « loaders ». L'objectif principal d'Emotet est de diffuser d'autres malwares sur l'ordinateur de la cible. Il accomplit cette tâche à l'aide d'un réseau sophistiqué qui distribue des spams à un grand nombre de cibles.

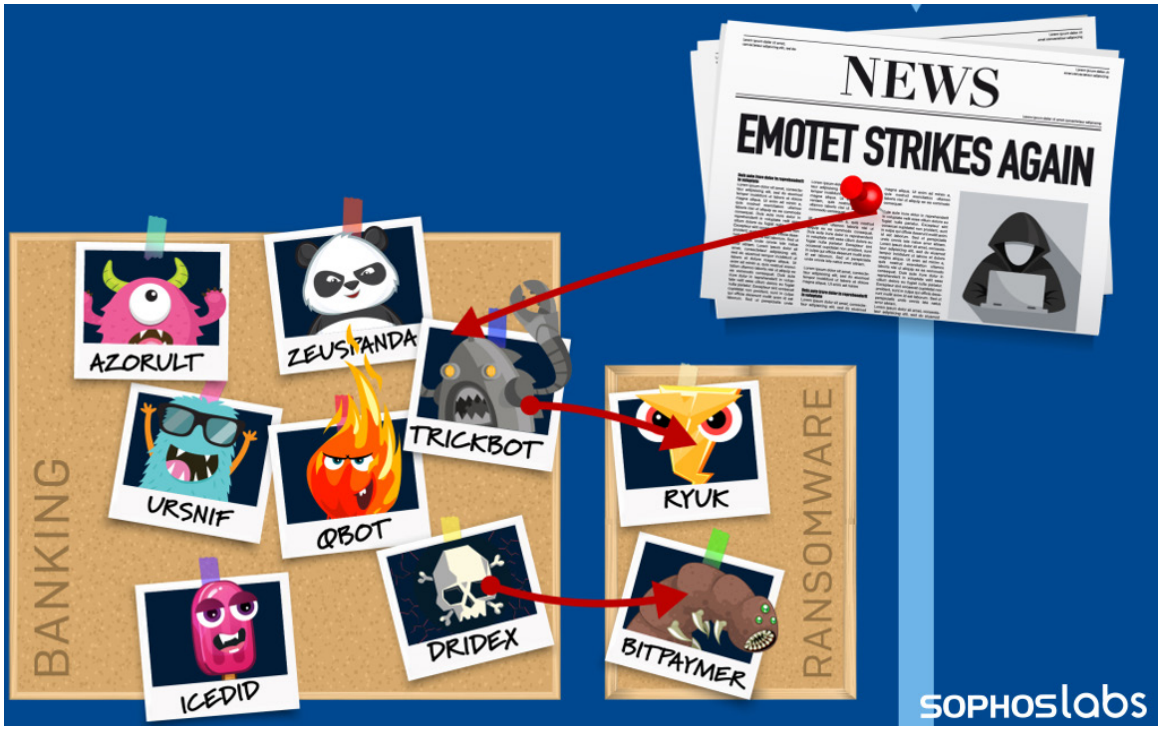


Fig.14. Source : SophosLabs.

Emotet a toutefois connu deux périodes sombres cette année. Le malware est resté en communication avec ses serveurs C2 pendant près de cinq mois, au cours desquels les courriers indésirables qui livraient normalement les attaques se sont complètement évaporés. Les spams diffusant Emotet ont mystérieusement repris en juillet.

Autre malware CaaS digne d'intérêt, le ransomware Dharma. Contrairement à ses confrères plus exigeants, Dharma maintient une rançon fixe et relativement modique. La raison s'explique par son business model. C'est un ransomware doté de « stabilisateurs » pour les criminels en herbe qui ont besoin d'apprendre les ficelles du métier. En substance, ces criminels paient un abonnement qui leur permet d'obtenir des charges utiles des auteurs de Dharma et ils se partagent entre eux le profit tiré de leurs attaques.

Comme les attaquants sont classés par spécialités voire par sous-spécialités, le business model utilisé par les criminels pour travailler avec des entrepreneurs indépendants et autres affiliés n'est pas prêt de disparaître.

Spam, scams, et promesses non tenus

Le confinement généralisé qui a touché la population mondiale s'est accompagné d'un flot d'escroqueries favorisées par le spam. Dans le meilleur des cas, les campagnes de spam les plus efficaces rajoutent un sentiment d'urgence en exigeant du destinataire qu'il donne suite au message. Il s'agit là d'une astuce psychologique bien connue, car si vous prenez quelques instants pour réfléchir au contenu du message de spam, vous vous rendrez probablement compte qu'il s'agit d'un faux. Mais si le spammeur déclenche une réaction de peur, vous agissez avant de réfléchir, et vous vous faites prendre au piège.

Le Covid-19 avait déjà mis tout le monde sous tension, si bien que les spammeurs n'ont même pas eu à faire d'efforts particuliers.

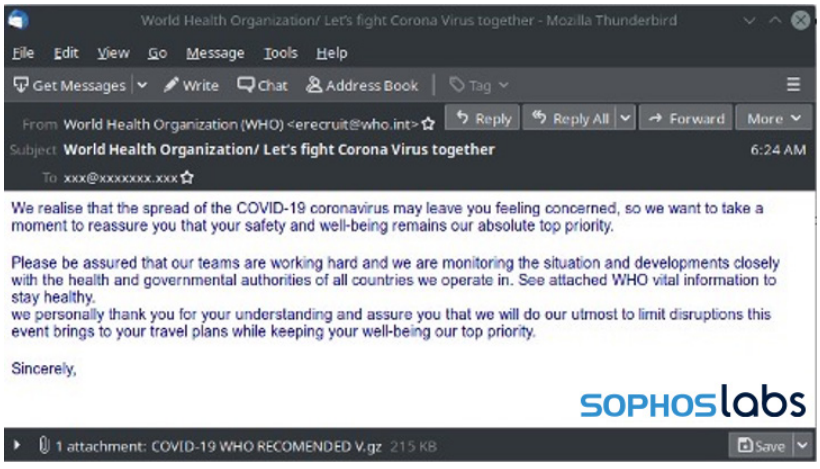


Fig.15. Source : SophosLabs.

Quelques semaines après le confinement, nous avons décidé d'examiner de plus près un autre phénomène en pleine croissance : les enregistrements de domaines. En quelques semaines, on a vu se créer chaque jour des milliers de nouveaux noms de domaine contenant une combinaison des chaînes *Covid-19*, *Corona* ou *virus*.

Domain	First Seen	Nameserver	Ns Ip
coronavirusshaquilleoneal.com	2020-03-14 07:00:38	ns-cloud-b1.googledomains.com	216.239.32.107

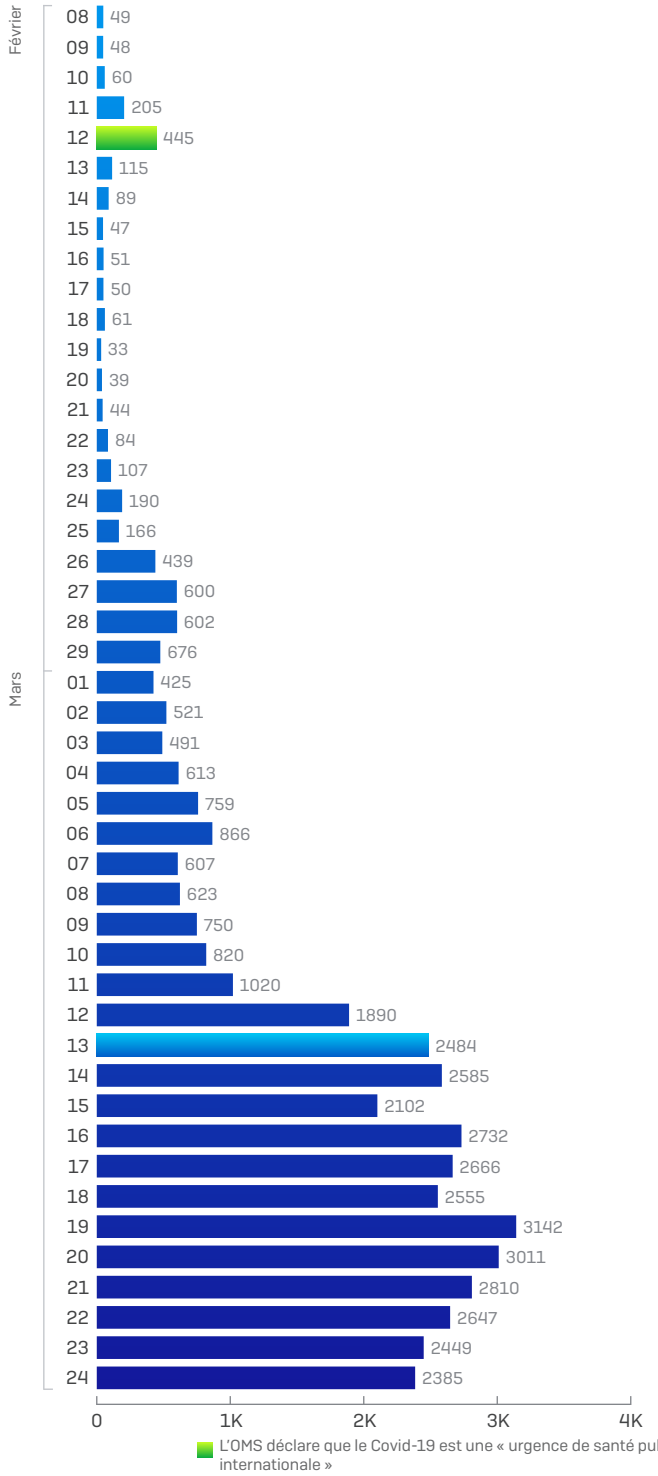
SOPHOSlabs

Fig.16. Source : SophosLabs.

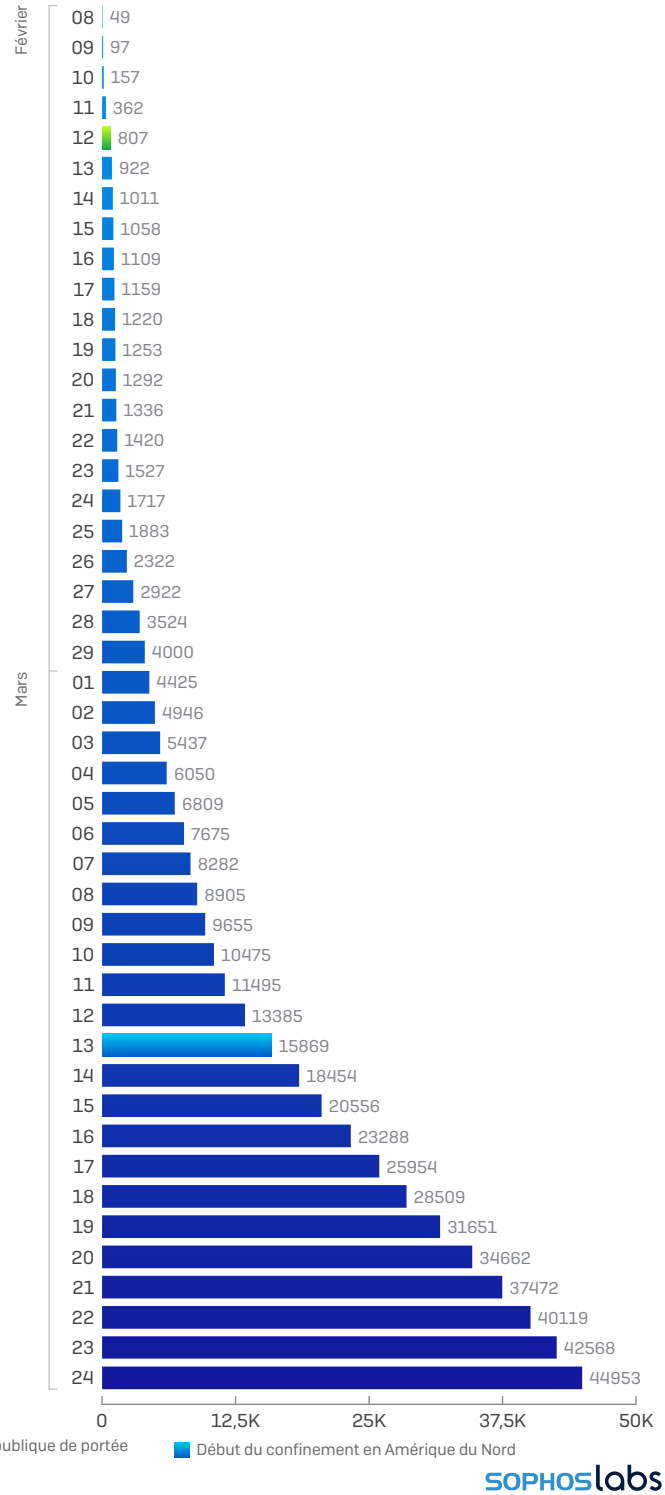
Certains de ces sites étaient de véritables canulars, mais d'autres ressemblaient de façon déroutante à ceux utilisés par les autorités sanitaires légitimes, régionales ou nationales.

Nous avons également recherché les domaines et sous-domaines liés au Covid-19 dans les journaux de transparence des certificats TLS. Les journaux de transparence des certificats sont utiles pour suivre les sous-domaines qui ont leurs propres certificats TLS — des informations qui n'apparaissent pas dans les données brutes d'enregistrement des domaines — et les noms de domaine.

Nouveaux enregistrements de domaines COVID, par jour



Total des nouveaux noms de domaines COVID, à ce jour



SOPHOSlabs

Fig.17. Au cours des premiers mois de la crise sanitaire, on a enregistré des milliers de domaines et cédé au moins autant de licences de certificats TLS chaque jour, dont les noms contenaient la chaîne « Covid-19 » ou « corona ». Source : SophosLabs.

Nouveaux certificats TLS par mois avec le nom d'hôte « Covid-19 » ou « Corona »

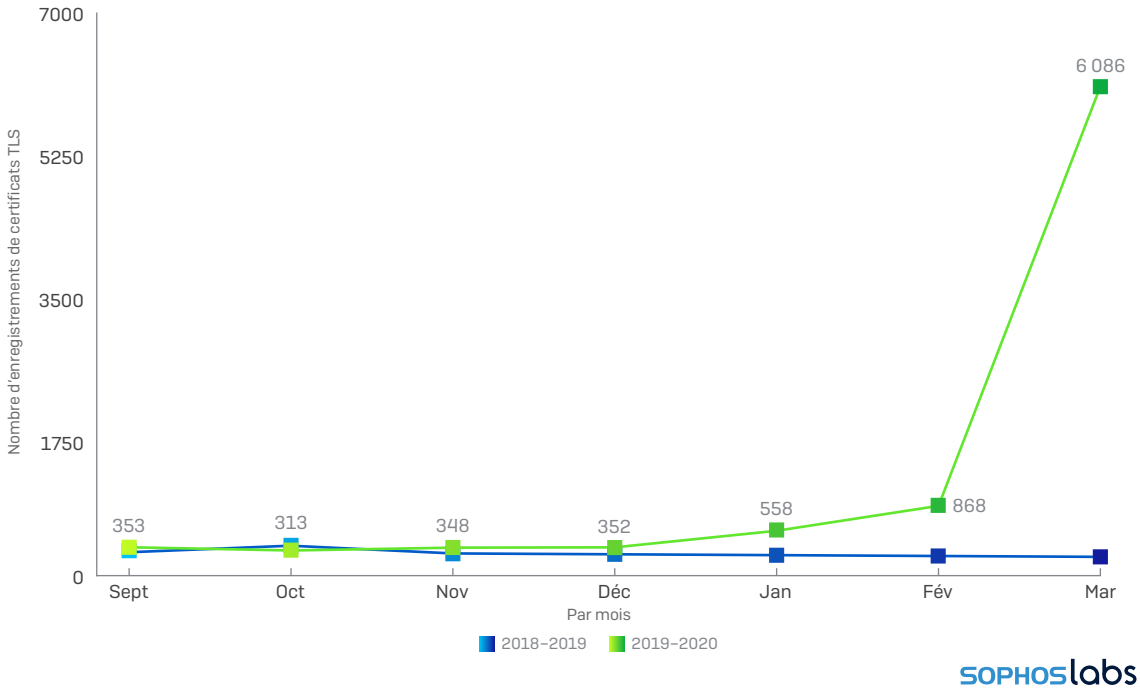


Fig.18. Les enregistrements de certificats TLS faisant référence à la pandémie ont connu un pic à peu près au même moment que les enregistrements de domaines. Source : SophosLabs.

En moyenne, nous avons observé plus de 200 demandes de certificats pour des domaines Covid-19 par jour en mars, et ce taux a continué à grimper dans les mois suivants. En juin, il était en moyenne de 625 par jour et en octobre, il a connu un pic de à 951 par jour.

La plupart de ces domaines restent légitimes ou bénins, mais beaucoup restent en attente et n'ont aucun contenu - signe potentiel que le titulaire du domaine le fasse vieillir (domain aging) et le mette de côté pour de futurs contrôles de réputation.

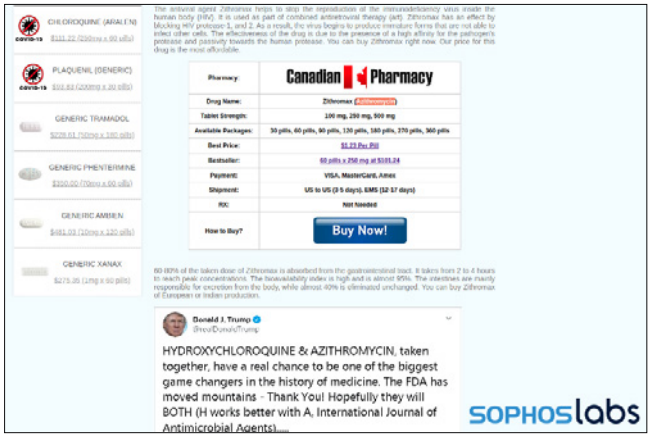


Fig.19. Même les praticiens escrocs n'ont pas pu résister à tirer profit du dernier remède miracle mentionné sur Twitter et ont même posté des tweets dans leurs annonces.

Source : SophosLabs.

Seul un très faible pourcentage (inférieur à un pour cent) a été identifié comme étant associé au phishing ou à du malware. Beaucoup sont éphémères, avec des noms d'hôtes qui ne peuvent plus être résolus après seulement une journée.

Le télétravail soulève l'importance de sécuriser le Cloud

Lorsque le confinement a été mis en place en mars 2020, les organisations publiques et privées et l'ensemble des individus qui y participent ont entamé une transition rapide et sans précédent qui se poursuit encore aujourd'hui. Notre façon de travailler, d'aller à l'école, de nous divertir, d'assister à des réunions, des événements ou encore des conférences a peut-être changé à jamais… Le Cloud Computing a été un élément essentiel de cette évolution, mais il doit faire face à de nombreux défis.

Les abus d'autorisation d'accès, la visibilité limitée sur les ressources et l'absence d'audit, tout cela a accru la vulnérabilité des environnements Cloud aux cybermenaces et les malwares ne sont pas moins dangereux dans le Cloud que partout ailleurs. C'est le cas par exemple du cryptojacking, un problème croissant. Les processus des cryptomineurs, lourds en cycles informatiques, sont déjà mauvais lorsqu'ils fonctionnent sur des machines physiques et font grimper la facture d'électricité ; mais sur des instances du Cloud, ils ont des effets secondaires encore plus marqués. La cible est facturée par le fournisseur de Cloud pour les cycles de CPU consommés par ses stations de travail virtuelles qui effectuent les calculs lourds nécessaires pour fournir quelques centimes de cryptomonnaie.

En outre, de nombreux télétravailleurs ont été victimes d'attaques de ransomwares, les criminels ayant verrouillé l'infrastructure du Cloud de la même manière qu'ils ont ciblé les machines physiques. Après tout, les ransomwares peuvent chiffrer un disque dur virtuel ou un object storage (stockage d'objets) tout aussi facilement que le stockage physique. Les organisations dont l'infrastructure dans le Cloud est attaquée par un ransomware peuvent se retrouver non seulement à payer une rançon, mais aussi une facture pour les cycles consacrés au chiffrement des données.

Entreprises ayant connu un incident de sécurité au cours de l'année passée

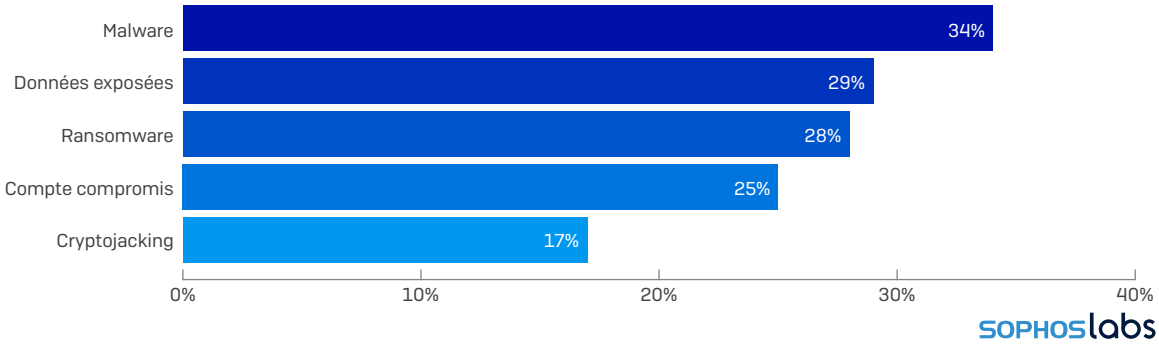


Fig.20. Dans son rapport 2020 sur la sécurité du Cloud, Sophos a interrogé plus de 3 500 professionnels IT sur leur expérience d'utilisation du Cloud et a constaté que de nombreux problèmes de sécurité affectant les réseaux physiques se répercutaient aussi sur les réseaux virtuels. Source : SophosLabs.

En cas de confinement, les services informatiques ont besoin d'un moyen d'assurer un service d'assistance virtuel comme s'il s'agissait d'un service réel. Le Covid-19 a exigé de grands changements, qui se sont déroulés en trois vagues.

Dans les premières semaines qui ont suivi le début du confinement, on a d'abord assisté à une vague d'accès. Comme des millions de télétravailleurs, se retrouvant coincés chez eux, devaient accéder aux ressources de leur organisation, la demande croissante d'accès à des réseaux privés virtuels (VPN) ou à d'autres dispositifs Zero Trust a littéralement submergé les ressources existantes. En plus des VPN, les entreprises ont dû ajouter de nouveaux pare-feu, mais aussi d'autres dispositifs de sécurité. Les déploiements de systèmes modernes de gestion unifiée des menaces sont venus compléter les pare-feu rudimentaires de type L3 fournis par les services de Cloud.

Dans le monde pré-Covid-19, les VPN n'étaient pas beaucoup utilisés puisque les employés en présentiel étaient beaucoup plus nombreux que ceux en déplacement ou en distantiel. Lorsque le confinement s'est prolongé de mars à mai puis à juin, le VPN est devenu pour ces travailleurs un outil vital (en réalité le plus important) qui a permis aux organisations de continuer à fonctionner.

Mais rapidement, les entreprises ont aussi réalisé que les employés ne devaient pas utiliser leurs appareils personnels depuis leur domicile pour accéder au VPN ; du coup, la baisse du nombre d'ordinateurs portables disponibles a créé un nouveau défi pour les organisations déjà confrontées aux besoins IT d'un personnel distribué. Faute de machines physiques suffisantes, les organisations se sont pour l'instant tournées vers la ressource apparemment illimitée que constituent les machines virtuelles pour répondre à ce besoin d'avoir un outil de travail sécurisé. C'est là que la deuxième vague a commencé : la vague des bureaux virtuels.

Alors que de plus en plus d'employés se sont tournés vers l'utilisation d'un bureau virtuel, l'hébergement de ces bureaux dans le Cloud s'est avéré pratique et économique, mais il fallait quand même les protéger.

Soudain, les services informatiques se sont donc retrouvés à prendre en charge des centaines ou des milliers de machines virtuelles d'employés, et ont eu besoin d'outils de visibilité pour pouvoir inventorier et configurer en toute sécurité le parc croissant de serveurs virtuels, de bureaux virtuels et de services dans le Cloud…. la troisième vague, celle de la gestion dans le Cloud.

Chronologie de l'attaque

Fig.21. Selon une attaque de cryptojacking que nous avons investiguée, un développeur a intégré par accident ses identifiants Cloud dans le code d'un dépôt public.

Le criminel découvre et utilise ces identifiants pour attaquer, en utilisant les API du fournisseur de Cloud natif et en faisant tourner des centaines d'instances de MV pour exploiter Bitcoin. Dans le même temps, il automatise des fonctionnalités sur ces instances pour les rendre plus difficiles à arrêter. Ensuite, il révoque l'accès à d'autres utilisateurs légitimes.

Source : SophosLabs.

L'ère du Covid-19 marque de grandes transformations dans tous les aspects de la vie humaine et, pour beaucoup, dans notre façon de travailler. Dans une récente enquête de Reuters, 97 % des PDG et directeurs techniques interrogés ont déclaré que le confinement avait accéléré leur transition vers les nouvelles technologies. Mais en période de restrictions budgétaires et d'incertitude, près d'un directeur technique (CTO) sur trois a déclaré que son devoir était de mettre en œuvre ces changements de la manière la plus rentable possible.

Dans le dernier rapport de Sophos sur la sécurité du Cloud, nous avons constaté que la majorité des incidents de sécurité liés au Cloud computing relevait de deux causes principales : le vol ou le phishing d'identifiants, ou des violations de données résultant de mauvaises configurations. Sur les 3 700 professionnels de l'informatique interrogés pour le rapport, sept sur dix ont affirmé que leur infrastructure de Cloud avait subi une brèche dans les 12 mois précédant l'enquête.

Comment la CCTC peut apporter une réponse rapide aux menaces à grande échelle

Fig.22. Source : Sophos.

Environ une semaine après le début du confinement, le responsable scientifique de Sophos, Joshua Saxe, a lancé un appel aux volontaires du monde entier. Cette brigade virtuelle est rapidement devenue la « Covid-19 Cyber Threat Coalition » (CCTC), une organisation comptant plus de 4 000 membres au service d'un même objectif : s'efforcer de contrer tout type de menace ou d'ingénierie sociale qui tenterait d'exploiter la peur du public par rapport au Covid-19, par nom ou par inférence.

« Je ne suis pas pompier, donc je ne saurais pas comment lutter contre un incendie, mais je peux aider une équipe à renforcer les défenses de ses infrastructures critiques, comme les hôpitaux », déclare Nick Espinosa, analyste de la sécurité et podcasteur au CCTC, basé à Chicago.

Cette initiative était vraiment nécessaire. Dès le tout début du confinement, les attaquants en ont profité pour diffuser des spams, des malwares et autres types de malwares, faisant référence, sous une forme ou une autre, au jargon terrifiant de la nouvelle pandémie. Comme nous l'avons mentionné dans ce rapport, à un moment donné, les gens enregistraient chaque jour des milliers de nouveaux domaines avec les mots Covid-19, corona ou CoV. Sophos a retracé les domaines connectés aux certificats TLS, avec ces mêmes chaînes de texte dans les données du certificat, et en a trouvé des milliers d'autres.

Augmentation du nombre des membres de la « Covid-19 Cyber Threat Coalition »

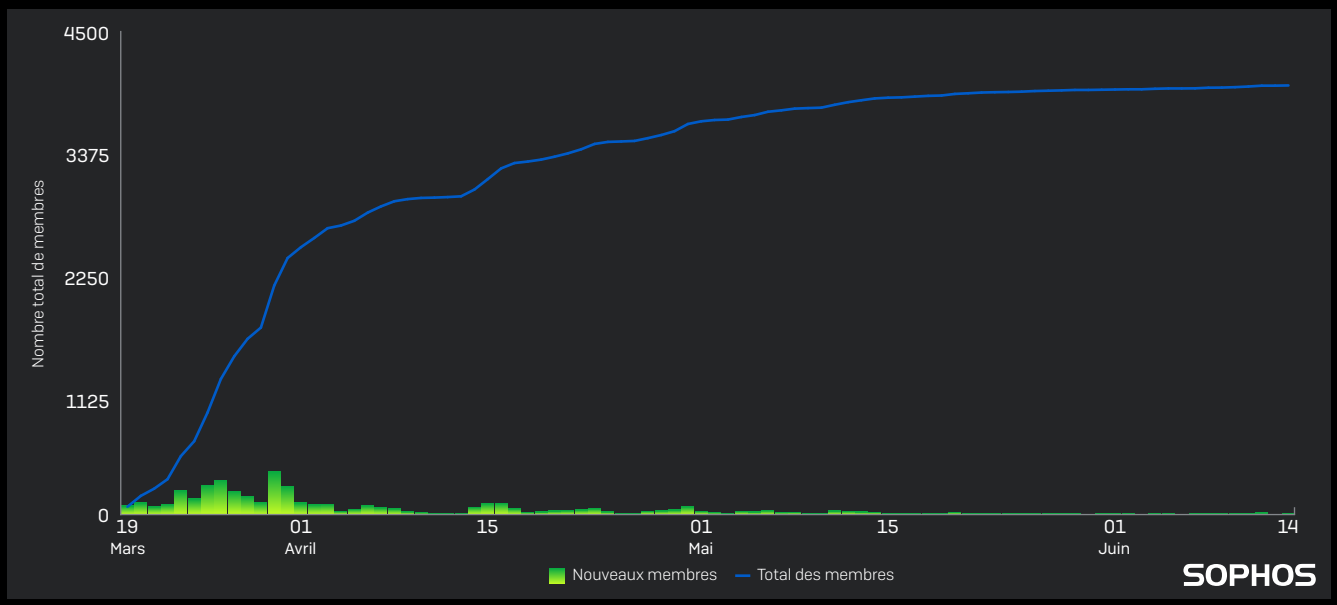


Fig.23. Source : Sophos.

En raison du caractère unique du Covid-19, le spam malveillant qui abuse de la crise mondiale représente une menace particulièrement flagrante et offensive. « Nous avons assisté à une explosion du piratage criminel utilisant le Covid-19 comme appât », a déclaré Espinosa. Les campagnes de spam se sont multipliées, les spammeurs déguisant leurs messages comme des communiqués officiels de l'OMS, du CDC aux États-Unis, du NHS au Royaume-Uni, ou toute autre autorité sanitaire des autres pays.

Les analystes ont également vu des références au Covid-19 dans des chaînes de binaires, utilisées comme variables dans des scripts LOL (living off-the-land).

Les membres de la CCTC ont partagé des échantillons et des renseignements sur toutes sortes d'incidents grâce à un canal Slack créé à la hâte. Chaotique au début, l'organisation s'est rapidement transformée en une structure rudimentaire. « Beaucoup de gens se sont rassemblés et n'ont pas cessé d'échanger des informations », explique Espinosa.

Le produit de la CCTC, le résultat de la collecte, c'est son flux de renseignements qui répertorie tous les nouveaux indicateurs de compromission. Le flux est libre d'utilisation, par n'importe qui. Ces IoC complètent les technologies défensives déjà en place, d'une manière neutre pour le fournisseur. Lorsque la CCTC a formé un partenariat avec la Cyber Threat Alliance, les fournisseurs de sécurité participant à la CTA ont amplifié l'effet protecteur de la veille sur les menaces de la CCTC en ingérant ces menaces et en protégeant contre elles.

La rapide cohésion des professionnels de la sécurité, partageant un objectif commun, nous a encouragés, conclut Espinosa. « Au départ, c'était la confusion totale, mais le groupe a su rapidement s'organiser ». Avec la plate-forme de partage de la CCTC, toute personne qui pourrait avoir besoin de répondre à une pandémie de type Covid-19 dans le futur n'aura pas à réinventer la roue ; elle sera davantage préparée à répondre à la menace, de même que son système immunitaire.

MENACES ET PLATES-FORMES NON TRADITIONNELLES : RESTER VIGILANT

Nous vivons dans un monde où nous sommes entourés d'appareils informatiques qui n'ont rien à voir avec un ordinateur ou un serveur : routeurs, téléphones portables, pare-feu, smart TV, box de streaming, boîtes VoIP, caméras et sonnettes de porte, stockage en réseau, certaines marques d'appareils électroménagers, etc.

Mais ce n'est pas parce qu'ils n'ont pas l'apparence d'un ordinateur classique qu'ils ne peuvent pas être utilisés ou exploités de la même manière.

Le malware Joker sur Android gagne en volume

Les utilisateurs d'Android se retrouvent au milieu d'une « course aux armements » entre Google (détenteur de la plate-forme Android et de Google Play Store) et les créateurs de malwares qui veulent que leurs logiciels soient téléchargeables sur le Google Play Store. Google a consacré des années à un système conçu pour inspecter le code source des applications Android demandant à figurer sur le Google Play Store, à la recherche de parties de code susceptibles d'aboutir à un résultat malveillant ou indésirable pour les utilisateurs Android. Les développeurs de malwares ont donc dû travailler dur pour échapper aux contrôles de code du Google Play Store.

Joker, alias Bread, est une application de fraude à la facturation par SMS, l'un des exemples les plus réussis d'une famille de malwares qui a évolué pour échapper à ces contrôles de code. Depuis qu'elles ont été découvertes pour la première fois l'année dernière, Google a supprimé du Google Play Store des milliers de ces applications malveillantes modifiées par Joker. Mais malgré tous ces efforts pour s'en débarrasser, elles continuent de rebondir.

Joker se présente sous la forme d'un large éventail d'applications diverses et variées : utilitaires, outils, fonds d'écran, traducteurs, services de messagerie — autant de clones d'applications très populaires. Rqppelons que Joker peut parfaitement être intégré à une application qui ressemble et fonctionne exactement comme la version originale. En fait, une application Joker ne contient qu'un tout petit morceau de code malveillant en plus, enfoui dans l'une des bibliothèques tierces que les créateurs d'applications compilent régulièrement dans leurs applications pour diverses raisons légitimes.

Plusieurs raisons expliquent donc pourquoi Joker a pu échapper aux contrôles de code de sécurité du Google Play Store à maintes reprises :

1. Ces applis malveillantes utilisent l'obfuscation, allant de la simple substitution de chaîne aux packers complexes, pour ralentir l'analyse et tromper le Google Play Store.
2. Lorsque le « développeur » Joker lance l'application, celle-ci ne contient absolument aucun code malveillant. Ainsi, lorsque l'application arrive dans le Google Play Store, son historique est vierge. Ce n'est que plus tard que le code malveillant apparaît dans l'application, après une mise à jour.
3. L'application déchiffre sa charge utile au moment de l'exécution ou la télécharge plus tard de façon dynamique.

Le malware Joker utilise le code natif (JNI) au lieu du DEX, plus courant. Le code natif utilise le C pour la programmation, ce qui ralentit l'analyse du code malveillant. En comparaison, DEX, une variation du code Java, est beaucoup plus facile à décompiler en quelque chose de lisible par l'homme. Le malware utilise ce code JNI pour envoyer des messages SMS, pour gagner de l'argent et comme moyen de contacter son réseau C&C. L'utilisation de JNI et du signal hors bande sur le réseau téléphonique plutôt que sur Internet peut aider Joker à échapper aux scanners dex automatisés qui ne décodent pas le JNI.

Joker a développé une longueur d'avance dans la bataille contre Google et son contrôle automatisé de code sur les nouvelles applications, et aucun signe ne nous laisse supposer que cette tendance va ralentir en 2021. Certains concurrents pourraient même rejoindre la bataille d'ici peu.

Les pubs et les PUA, difficiles à distinguer des malwares

Les publicités malveillantes (malvertising) restent une source majeure de menaces pour toute une série de périphériques. Récemment, nous avons examiné deux tendances en matière de publicité malveillante qui ne font pas partie des malwares : l'arnaque au faux support technique qui utilise des pages web « verrouillant le navigateur » et des publicités ciblant les mobiles, liées à des applications frauduleuses ou « fleeceware ». Sophos les classe dans la catégorie des « fausses alertes », à savoir du malverting qui a pour but d'effrayer la cible et de l'inciter à effectuer des actions qui profitent aux escrocs.

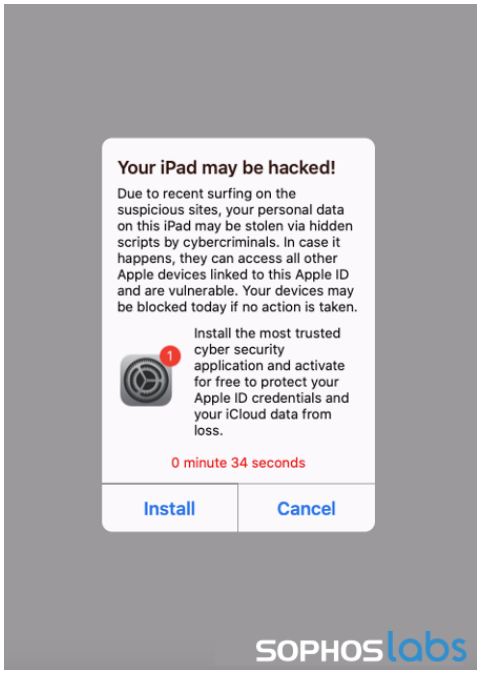


Fig. 24. Source : SophosLabs.

Les arnaques au faux support IT vise généralement à inciter la cible à fournir un accès à distance à son ordinateur, puis à la convaincre soit d'acheter des logiciels et des services d'assistance technique à des prix exorbitants, soit à donner les coordonnées de sa carte bancaire à des fins frauduleuses. Alors qu'avant, la plupart de ces escroqueries reposaient sur les appels de télémarketing direct, aujourd'hui un grand nombre d'opérateurs de scam sont passés à un modèle « pull » ou inversé. Ils exploitent des publicités malveillantes sur Internet qui tentent de convaincre l'utilisateur que son ordinateur a été verrouillé pour des raisons de sécurité, et lui demandent d'appeler lui-même le faux support.

Pour y parvenir, ils déploient des kits de sites Internet contenant des scripts conçus pour perturber la navigation et la rendre difficile, avec par exemple des variantes du « curseur maudit » (le curseur pointe au mauvais endroit ou il devient invisible) ou des attaques de « téléchargement interminable » qui assaillent le navigateur tout en se faisant passer pour une alerte de Microsoft ou d'Apple. Certains des kits que nous avons trouvés exploitaient un bug que l'équipe des SophosLabs avait découvert dans Firefox au début de l'année, tandis que d'autres exécutaient des attaques similaires sur d'autres navigateurs — toutes diffusées par des annonces intrusives malveillantes de type « pop-under ».

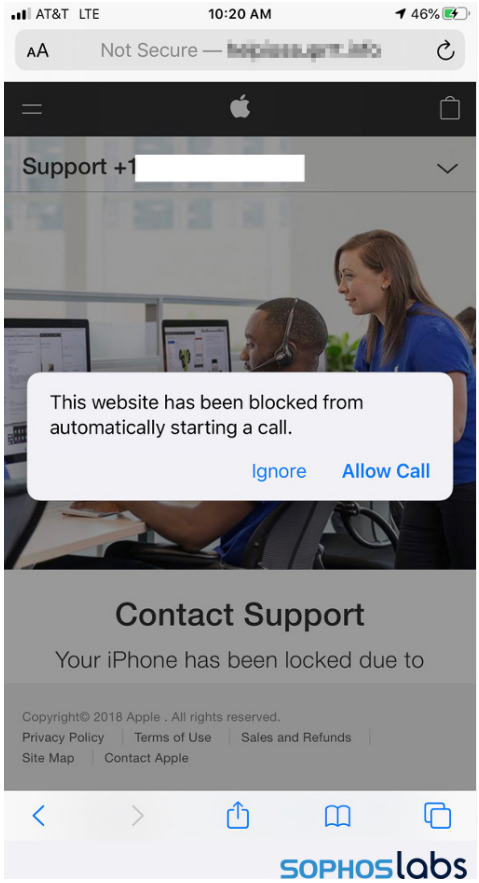


Fig. 25. Source : SophosLabs

La même infrastructure de réseau qui prend en charge ces attaques sur les navigateurs PC et Mac sert aussi pour les arnaques au faux support technique et aux fausses alertes en renvoyant à des applications mobiles potentiellement indésirables. C'est le cas par exemple des applis qui prétendent être des services VPN ou des outils de « nettoyage » supposés éliminer les malwares, et qui s'accompagnent de frais d'abonnement intégrés (et dans certains cas, de véritables malwares Android). Sophos a trouvé une série de serveurs diffusant ces campagnes publicitaires, qui utilisait un logiciel commercial créé par un développeur russe, spécialement conçu pour la réalisation de telles campagnes.

Utiliser vos propres ressources contre vous : l'abus criminel des outils de sécurité

Certaines attaques n'impliquent pas du tout de malwares ou attendent la fin de l'attaque pour en diffuser. À la place, elles utilisent uniquement les outils déjà présents sur les systèmes d'exploitation des ordinateurs du réseau. Certains criminels exploitent le potentiel offert par deux outils utilisés dans l'industrie de la sécurité des données : les outils de réponse aux incidents et les testeurs de pénétration.

La communauté de la sécurité des informations a défini le genre d'attaques qui impliquent peu ou pas de malwares, mais qui exploitent les composants existants du système d'exploitation ou des progiciels populaires, comme « living off-the-land » (LOL), c'est-à-dire vivant des ressources existantes. Ces attaques impliquent généralement une ou plusieurs formes d'automatisation sous la forme de scripts natifs tels que PowerShell, fichiers batch ou scripts VBScript, communément appelés LOLscripts. Ces derniers sont utilisés par les attaquants pour exécuter des séquences de commandes à l'aide d'applications binaires (applications) LOL appelés LOLbins.

Les logiciels conçus à l'origine pour le segment Red Team de l'industrie incluent des méthodes d'attaque basées sur le « bring your own ». Les attaquants, dans ce cas, déploient et utilisent des outils de sécurité prêts à l'emploi qui sont couramment utilisés par les administrateurs réseau et les testeurs d'intrusion. C'est le cas par exemple de Cobalt Strike ou d'éléments du Metasploit framework, conçus pour évaluer les vulnérabilités de sécurité et effectuer des tests techniques.

Outils pour les opérateurs de la menace Netwalker sur la matrice ATT&CK

ACCÈS INITIAL	EXÉCUTION	ÉLÉVATION DES PRIVILÈGES	CONTOURNEMENT DE LA DÉFENSE	ACCÈS AUX IDENTIFIANTS	DÉTECTION	MOUVEMENT LATÉRAL	IMPACT
Exploit Tomcat	Scripts PowerShell	CVE-2020-0796	Chargement sans fichier	mimikatz	Contrôleur de réseau SoftPerfect	psexec	Ransomware Netwalker
Exploit Weblogic	psexec	CVE-2019-1458	Outil AV Eset	Mimidogz	NLBrute	Teamviewer	Ransomware Zeppelin
Email de phishing		CVE-2017-0213	Récupération de mots de passe Eset de Gordon	Mimikittenz		Anydesk	Ransomware Smaug
		CVE-2015-1701	Outil de désinstallation de l'agent de sécurité Trend Micro	Éditeur des identifiants Windows			Exfiltration de données
			Désinstallation du client de sécurité Microsoft	pwdump			
				NLBrute			
				LaZagne			
				WinPwn			

SOPHOSlabs

Fig. 26. L'ensemble d'outils utilisés par l'opérateur de la menace impliqué dans les attaques de ransomware de Netwalker comprenait une série de freeware et d'utilitaires open source, à différents moments de l'attaque. Source : SophosLabs.

Ces outils sont précieux pour les attaquants pour plusieurs raisons : Comme ils sont souvent utilisés à titre légitime (pour évaluer ou améliorer la sécurité du système), ces outils ou leurs activités peuvent être difficiles à détecter pour les solutions antivirus/de sécurité. C'est pourquoi Sophos doit s'appuyer davantage sur l'analyse du comportement des LOLscripts pour identifier les activités malveillantes potentielles. Et évidemment, il est plus facile d'utiliser un outil qui existe déjà que de créer ses propres outils à partir de zéro.

Même si l'utilisation des LOLscripts et des reverse shells ne date pas de l'année dernière, ils sont devenus en 2020 un élément omniprésent des attaques complexes et manuelles de ransomwares. En fait, aussi bien la quantité que la variété des outils d'attaque que nous avons observés semblent avoir augmenté.

La kill chain (chaîne de frappe) des outils d'attaque de Dharma RaaS

ACCÈS INITIAL	EXÉCUTION	ÉLÉVATION DES PRIVILÈGES	CONTOURNEMENT DE LA DÉFENSE	ACCÈS AUX IDENTIFIANTS	DÉTECTION	MOUVEMENT LATÉRAL	EXFILTRATION	IMPACT
Bourrage d'identifiants RDP	PowerShell	CVE-2019-1388	Désactivation de la protection anti-malware	mimikatz	PCHunter	Objets des politiques de groupe	Email de screenshot PowerShell	Ransomware Dharma
Vol d'identifiants RDP	WMI	CVE-2018-8120	Outil de désinstallation Revo	Remote Desktop Passview	Process Hacker	Remote Desktop	TOR	
	AutoIT	CVE-2017-0213	Outil de désinstallation IOBit	LaZagne	GMER	Gestion à distance de WinRM	dropmefiles[.]com	
	RDP/Ligne de commande			NLBrute	Scanneur IP avancé			
				Outils Hash Suite	NS2.EXE			

SOPHOSlabs

Fig.27. Source : SophosLabs.

Les outils d'attaque sont d'une grande variété, allant des applications disponibles sur le marché aux dépositaires GitHub open source, avec des fonctionnalités pouvant inclure :

- Centres de commande et de contrôle de type botnets
- Génération de shellcodes et obfuscation
- Contournement de l'AV et détection du sandboxing
- Extraction des mots de passe ou identifiants
- Kerberoasting (maintient la persistance des privilèges de l'administrateur de domaine)
- Possibilité de forcer les mots de passe utilisés par divers services
- Exfiltration des données du système

La plupart de ces outils ne contiennent pas ou peu de charge utile (bénigne) dans leur état « prêt à l'emploi », mais dans le passé, nous avons pu détecter un grand nombre de ces outils se livrer à des activités malveillantes grâce aux informations contextuelles acquises par nos technologies de détection comportementale.

Selon notre télémétrie, les dix outils d'attaque que nous avons vus le plus souvent utilisés sont (par ordre de fréquence d'utilisation) : Metasploit, BloodHound, mimikatz, PowerShell Empire, Cobalt Strike, Veil Evasion, Hydra THC, Enigma, Nishang et Shellter. Metasploit est de loin l'outil le plus courant, utilisé environ deux fois plus souvent que le suivant, BloodHound.

Actuellement, Sophos suit l'utilisation de 99 outils d'attaque différents… ; il semble peu probable que l'on assiste à un sursis de la part des attaquants qui continueront à en profiter en 2021.

Épidémiologie digitale

Quel est le pourcentage des systèmes informatiques infectés par des malwares qui ne sont pas détectés ? Quel est le pourcentage des exécutions en ligne de commande effectuées par des pirates non détectés ? Quel est le pourcentage d'emails de phishing ciblés qui ne sont pas détectés ? Comment tous ces chiffres évoluent-ils en fonction du secteur d'activité, de la géolocalisation et du statut du réseau ?

Poser de telles questions revient à se demander « quel est le pourcentage de personnes infectées par le Covid-19 ? », dans un contexte où de nombreuses personnes pourraient ne jamais être testées, les tests effectués peuvent avoir des taux de faux positifs et de faux négatifs importants.

Autrement dit, c'est une situation complexe.

Malgré ces défis, les épidémiologistes parviennent à répondre quotidiennement à des questions cruciales sur le Covid-19. Mais ce n'est pas le cas pour les chercheurs en cybersécurité vis-à-vis des cyberattaques. En effet, nous accusons un retard sur les épidémiologistes en ce qui concerne les outils, techniques et procédures que nous avons mis au point pour avancer dans cette incertitude. Nous n'avons pas d'excuse ; il est temps de concevoir nos propres outils pour mieux appréhender la nature de la menace à laquelle nous sommes confrontés, pour signaler les risques à ceux que nous défendons de manière précise et pour prendre les bonnes décisions pour mieux orienter nos efforts.

Pour nous aider dans cette mission, Sophos AI s'est lancé dans un projet de conception d'un ensemble de modèles statistiques inspirés de l'épidémiologie pour estimer la prévalence totale des infections par malwares. Nous associons un solide pipeline de collecte de données portant sur 100 millions de postes à un ensemble de méthodes statistiques bayésiennes, ce qui nous permet d'aborder ces questions difficiles pour bâtir une vision complète des performances de nos modèles « sur le terrain ».

Par exemple, examinons la question : « Quel est le volume de malware affectant véritablement nos clients d'une semaine à l'autre, et quel pourcentage détectons-nous vraiment ?

Si, pour tous les fichiers, nous savions déjà lesquels sont des malwares et lesquels sont bénins, nous aurions déjà répondu ! Malheureusement, nous avons face à nous deux problèmes.

1. Nous ne connaissons pas toute la vérité sur chaque fichier donné. Certains malwares échapperont toujours aux produits Endpoint, quels qu'ils soient, et les cas de faux positif (un fichier normal signalé comme malware) sont inévitables.
2. Dans la réalité, l'équilibre entre les fichiers bénins et malveillants penche massivement en faveur des fichiers bénins, si bien que nous ne pouvons probablement pas le déterminer par une analyse manuelle. Il nous faut effectuer une analyse approfondie des milliers de fichiers, définis comme bénins par notre produit Endpoint, pour trouver un seul fichier malveillant.

Pour résoudre ces problèmes, nous nous tournons vers les statistiques bayésiennes. En termes extrêmement simples, nous construisons un modèle « génératif » des données : un programme mathématique qui peut faire des suppositions sur les paramètres (« combien de malwares y a-t-il réellement ? »), et transformer ces suppositions en simulations du nombre de détections sur des postes que nous pourrions voir. Ensuite, nous essayons différentes suppositions, voyons quelles simulations correspondent à la réalité observée et travaillons à rebours pour trouver des valeurs plausibles du paramètre qui nous intéresse.

Par exemple, imaginez que nous ayons pour une semaine donnée 2 000 détections sur des postes et une bonne estimation des taux de vrais et de faux positifs du modèle. Nous pouvons simuler des environnements avec des taux de malware de 0 %, 2 %, 5 %, etc., et voir ce que la simulation prévoit pour les détections sur les postes. Si nous voyons près de 2 000 détections pour certains taux de malwares, alors c'est (peut-être) une valeur plausible.

Fig. 28. Simulez un taux de malware, échantillonnez, voyez si la simulation correspond à la réalité observée, comptez les détections réelles et répétez. Source : SophosAI.

Ce processus peut être répété des millions de fois pour bâtir une distribution de valeurs plausibles pour le taux de malware et, comme nous utilisons une approche bayésienne, les barres d'erreur sont « intégrées » à l'estimation. Dans notre exemple, le modèle pense que la valeur la plus probable pour « quel pourcentage de fichiers sont des malwares » est légèrement supérieure à 3 %, mais nous pourrions tout à fait avoir une valeur comprise entre 2,75 % et 3,35 %.

Et dès que nous avons une bonne estimation de ce chiffre (pourcentage de fichiers susceptibles d'être des malwares sur les systèmes Endpoint des clients), les détections manquées et les faux positifs deviennent assez simples à estimer. Si nous examinons les données de notre système de détection des malwares basé sur le ML, qui a été utilisé pendant une semaine en mai (sans aucune option basée sur la signature, le comportement ou l'heuristique), nous pouvons élaborer une matrice complète de vrais et faux positifs et négatifs, et finaliser notre tableau des performances du modèle. Dans ce cas, nous constatons que même si nous avons quelques faux négatifs, le nombre de faux positifs est faible et tend vers zéro, tandis que le nombre de vrais positifs est élevé et tend vers 161 000 (le nombre total de résultats positifs dans l'échantillon). D'après l'échelle, nous pouvons voir que ces trois quantités sont éclipsées par le nombre de vrais négatifs, c'est-à-dire des fichiers inoffensifs que notre ML a qualifiés de bénins.

Notre outil inspiré de l'épidémiologie nous a donc permis d'estimer, voire de trouver, les aiguilles dans notre botte de foin de fichiers PE.

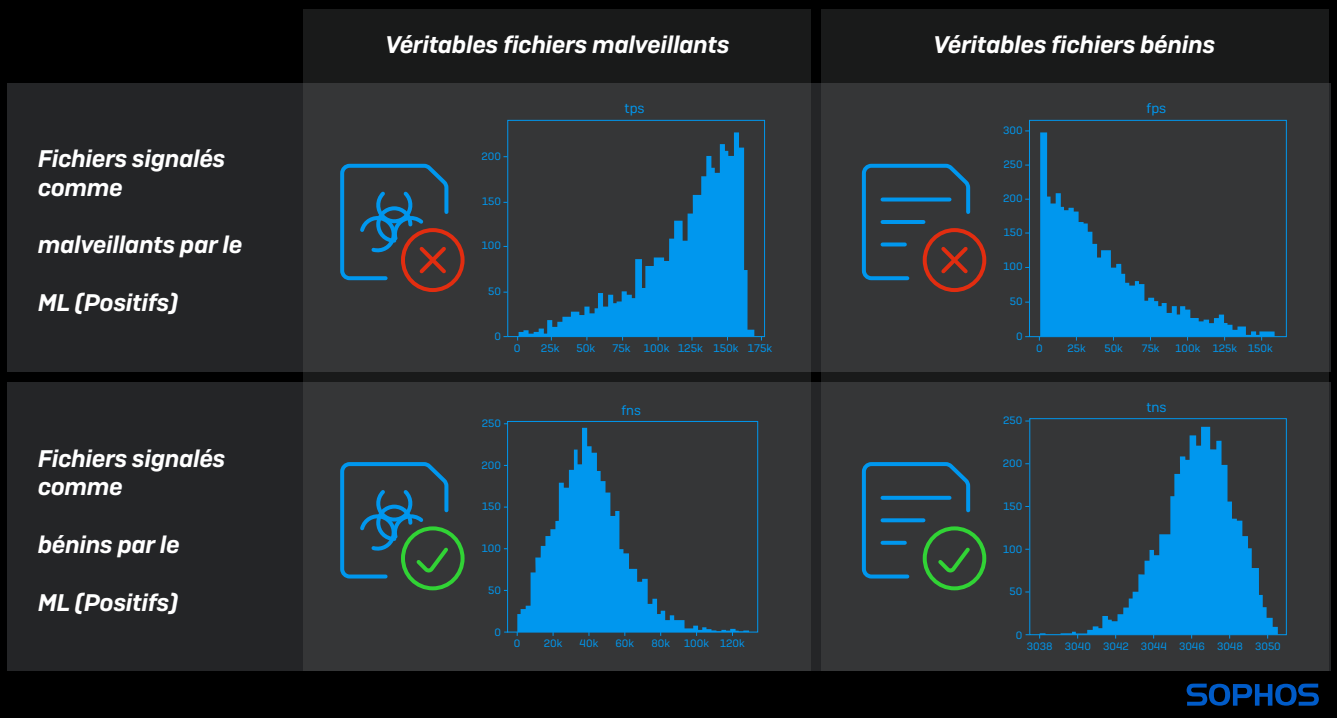


Fig. 29. Analyse des vrais et faux positifs du modèle de ML au début du mois de mai 2020. Source : SophosAI.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : partners@sophos.fr

20-11-01 FR (DD)

SOPHOS