SOPHOS
Cybersecurity delivered.

Active Adversary Playbook 2022

Comportements, tactiques et outils des cyberattaquants observés par des experts en réponse aux incidents en 2021

Par **John Shier**, Senior Security Advisor, CTO Office

Un livre blanc Sophos Juin 2022

Introduction

Défendre une organisation contre des cybermenaces qui évoluent rapidement et sont de plus en plus complexes peut représenter un défi considérable. Les adversaires adaptent et font évoluer en permanence leur comportement et leurs outils, exploitent de nouvelles vulnérabilités et abusent des outils informatiques courants pour échapper à la détection et garder une longueur d'avance sur les équipes de sécurité.

Il peut être difficile pour les professionnels de l'informatique et des opérations de sécurité de se tenir au courant des dernières approches utilisées par les attaquants. En particulier lorsqu'il s'agit d'attaques ciblées et actives qui impliquent plusieurs acteurs malveillants, comme un courtier d'accès initial (Initial Access Broker) qui s'introduit dans l'environnement d'une cible et vend ensuite cet accès à des gangs de ransomware qui l'utiliseront dans leurs attaques.

Ce présent rapport « Active Adversary Playbook 2022 » passe en revue les principaux attaquants, outils et comportements d'attaques observés en situation réelle en 2021 par les experts en réponse aux incidents de Sophos. Il fait suite au rapport « Active Adversary Playbook 2021 » et montre comment le paysage des attaques continue d'évoluer.

L'objectif est d'aider les équipes de sécurité à comprendre ce que les adversaires font pendant une attaque et comment repérer et se défendre contre une telle activité sur leur réseau.

Les résultats sont basés sur les données des incidents investigués par l'équipe Sophos Rapid Response en 2021. Lorsque cela est possible, les données sont comparées aux résultats décrits dans le rapport Active Adversary Playbook 2021.

Profil démographique de la réponse aux incidents en 2021

Le rapport est basé sur 144 incidents de sécurité ciblant des organisations de toutes tailles, dans un large éventail de secteurs industriels, et situés aux États-Unis, Canada, Royaume-Uni, Allemagne, Italie, Espagne, France, Suisse, Belgique, Pays-Bas, Autriche, Émirats arabes unis, Arabie saoudite, Philippines, Bahamas, Angola et Japon.

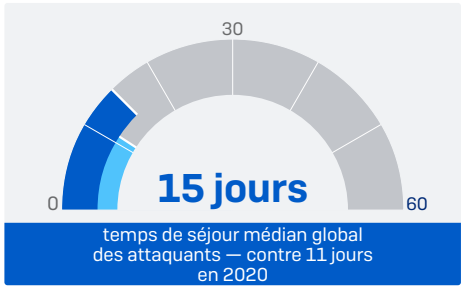
Les secteurs les plus représentés sont l'industrie manufacturière (17 % des interventions concernaient ce secteur), suivie par le retail (14 %), la santé (13 %), l'informatique (9 %), la construction (8 %) et l'éducation (6 %). Des informations supplémentaires sur les profils sont disponibles dans les tableaux de données à la fin de ce rapport.

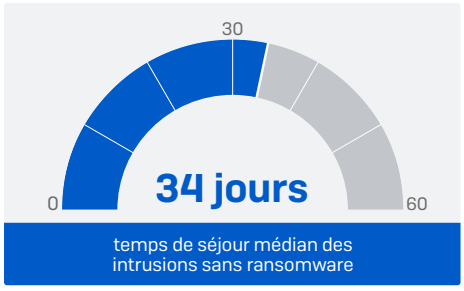
Tableau de bord : L'anatomie des attaques actives en 2021

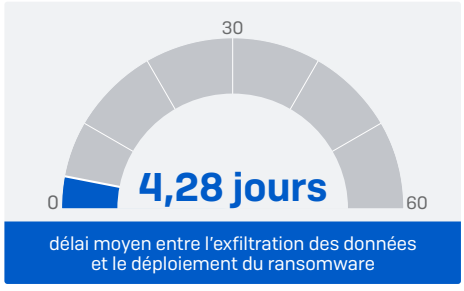
Deux des développements de cybersécurité les plus marquants de l'année se sont produits en mars et en août 2021, avec le signalement des vulnérabilités ProxyLogon et ProxyShell dans les serveurs Microsoft Exchange. Comme l'ont noté récemment le CISA (Cybersecurity and Infrastructure Security Agency) et d'autres agences de sécurité gouvernementales américaines, les bugs ProxyLogon/ProxyShell ont été largement exploités par les attaquants. Il n'est donc pas surprenant qu'ils figurent dans un nombre significatif d'incidents investigués par Sophos en 2021.

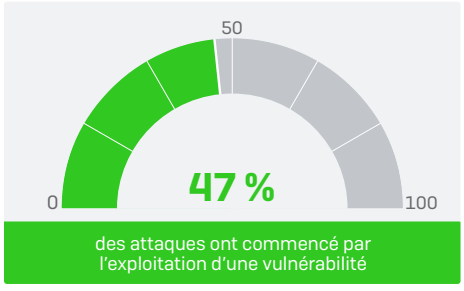
Tableau de bord : Anatomie des attaques actives en 2021

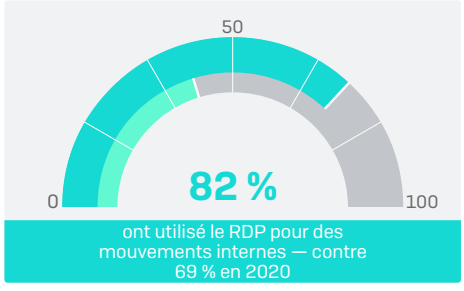
Principales conclusions des investigations réalisées dans le cadre de la réponse aux incidents

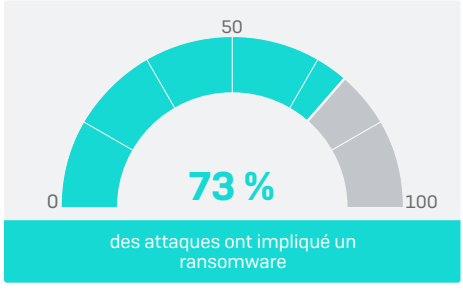


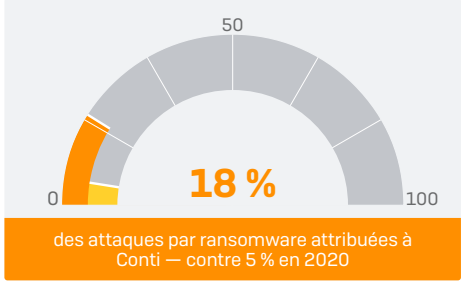


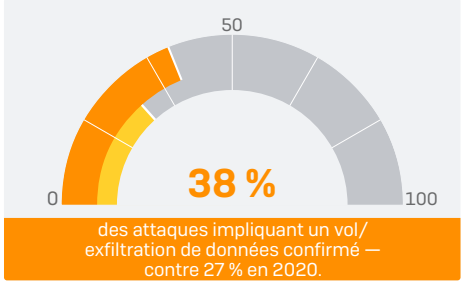












Il est probable que de nombreuses violations ProxyLogon/ProxyShell soient encore inconnues à l'heure actuelle, où des webshells (codes encoquillés) et des portes dérobées installés chez les victimes attendent sagement que cet accès soit utilisé ou vendu.

Cela nous amène à une autre évolution majeure qui a façonné le paysage des cybermenaces en 2021 : l'influence et le pouvoir croissants des courtiers d'accès initial (IAB).

Le succès des IAB dépend de leur capacité à être les premiers à infiltrer une cible et à ouvrir un accès qu'ils pourront revendre. C'est pourquoi les IAB font souvent leur apparition lorsque des bugs viennent tout juste d'être signalés, dans l'espoir de compromettre les cibles avant que les correctifs ne soient appliqués. Leur objectif est de s'implanter dans l'environnement d'une victime et, éventuellement, d'effectuer quelques mouvements exploratoires initiaux pour se faire une idée de la valeur de l'actif — avant de le vendre à d'autres adversaires, tels que des opérateurs de ransomware, pour l'utiliser dans des attaques, parfois des mois après l'intrusion initiale.

Comme le souligne le Rapport Sophos 2022 sur les menaces, l'essor des IAB reflète la « professionnalisation » croissante des attaques sur un marché des cybermenaces qui compte un nombre croissant de fournisseurs de services spécialisés. L'industrie florissante du Ransomware as a Service (RaaS) est un autre exemple de cette tendance.

Dernier point, mais non le moindre, des preuves post-mortem découvertes en 2021 au cours d'investigations ont révélé des cas où de multiples adversaires, y compris des IAB, des gangs de ransomware, des cryptomineurs et parfois même de multiples opérateurs de ransomware, ciblaient la même organisation simultanément. Il s'agit d'une évolution qui continuera à façonner le paysage des cybermenaces en 2022 et au-delà.

La durée passée par les intrus dans les réseaux des victimes augmente, probablement en raison de cette activité. Parmi les autres attaquants qui s'implantent durablement dans les réseaux des victimes, parfois simultanément, figurent les créateurs de botnets et les plateformes de diffusion de logiciels malveillants ou « droppers ».

Ces évolutions sont examinées plus en détail ci-dessous.

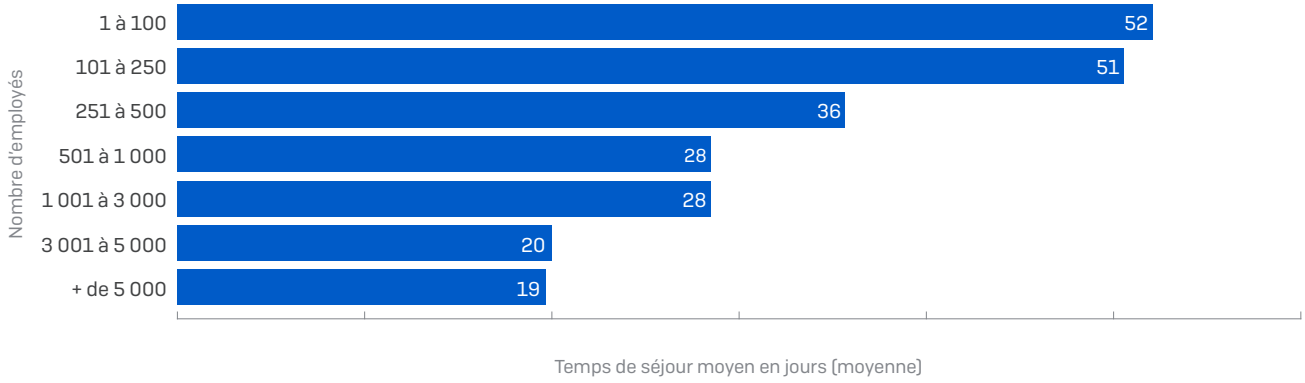
Les intrus invisibles

Les données sur les incidents montrent que la durée médiane du temps de séjour des acteurs malveillants a augmenté d'environ un tiers entre 2020 et 2021, passant de 11 à 15 jours. Des variations considérables ont été observées : des attaques aboutissant à un ransomware ont eu des durées de séjour plus courtes, en moyenne autour de 11 jours (contre 18 jours en 2020) et d'autres intrusions ont duré beaucoup plus longtemps, avec une durée de séjour médiane de 34 jours.

Variation de la durée moyenne de séjour des intrus (médiane)

Comme nous l'avons suggéré ci-dessus, des temps de séjour plus longs peuvent refléter l'implication d'un IAB. Pour les petites entreprises ou les secteurs industriels tels que l'éducation (temps de séjour moyen des intrus : 34 jours), les durées de séjour plus longues reflètent également la difficulté pour le personnel de sécurité informatique interne de chasser, d'investiguer et de répondre de manière proactive aux alertes suspectes et aux menaces potentielles.

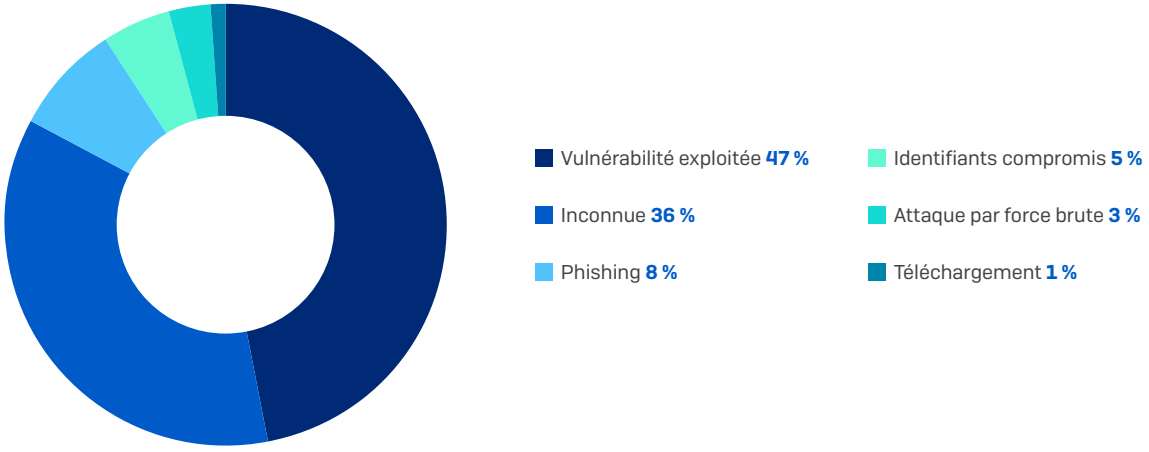
Temps de séjour des intrus par taille d'entreprise (moyenne)



Les causes initiales des attaques

Il n'est pas toujours possible, ou facile, d'identifier la cause initiale d'une attaque. Parfois, les attaquants ont intentionnellement supprimé les preuves de leur activité et parfois l'équipe de sécurité informatique a déjà effacé ou réimagé les machines compromises au moment où les experts en réponse commencent leur intervention. Malgré cela, les données montrent que parmi les incidents analysés par Sophos, l'exploitation de vulnérabilités non corrigées (telles que ProxyLogon ou ProxyShell) a été la cause première de près de la moitié (47 %) des cyber incidents de 2021.

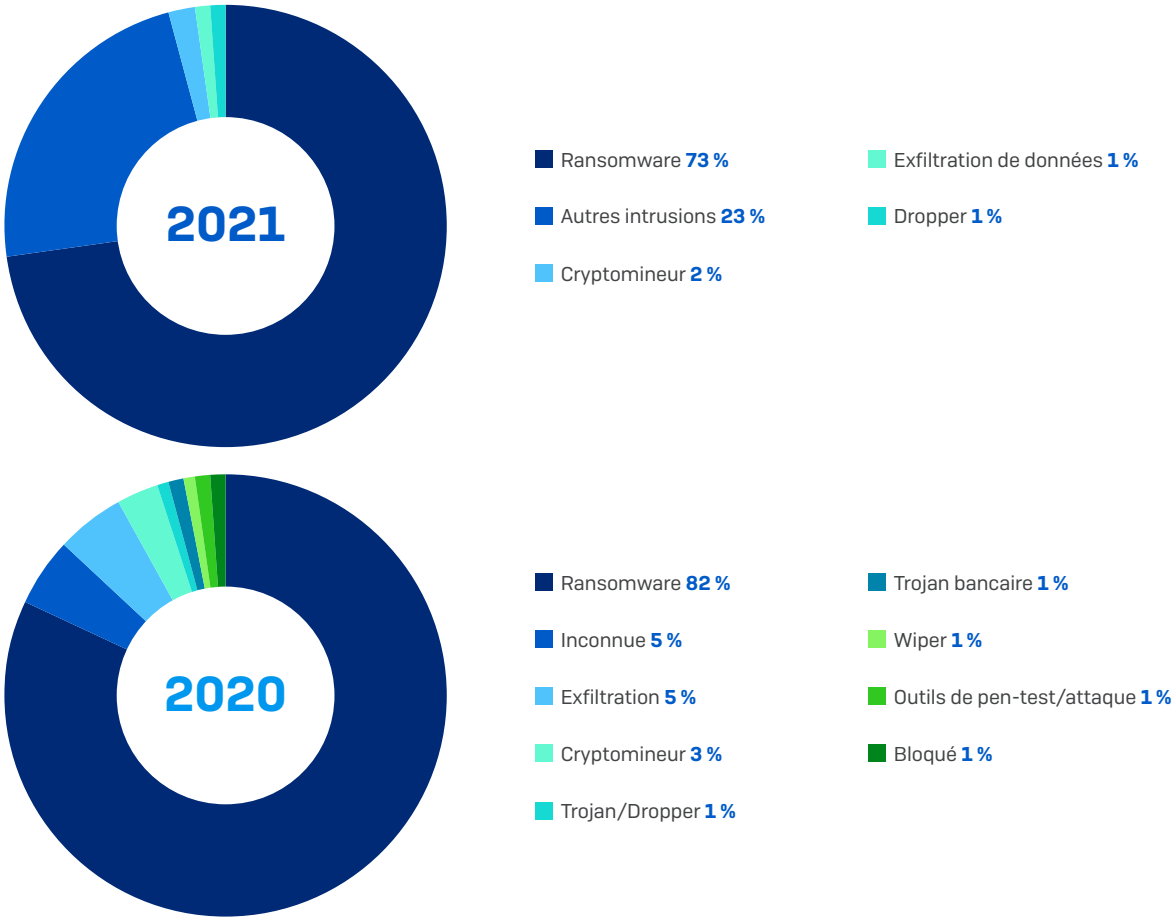
Causes initiales des attaques



Les principaux types d'attaque

L'offensive d'un ransomware est malheureusement souvent le moment où l'attaque devient visible aux yeux de l'équipe de sécurité informatique. Il n'est donc pas surprenant que 73 % des incidents auxquels Sophos a répondu en 2021 impliquent un ransomware. Les ransomwares étaient également le type d'attaque le plus répandu en 2020, à hauteur de 82 % (ce chiffre élevé reflétant probablement un plus petit ensemble de données). Dans le cas de l'exfiltration de données, qui représente 1 % des incidents, les experts en réponse aux incidents pensent que ces attaques se seraient probablement terminées par un ransomware si elles n'avaient pas été identifiées et neutralisées à temps.

Types d'attaque



Le deuxième type d'attaque le plus courant est la catégorie générale des « autres intrusions », qui représente 23 % des incidents. Pour les besoins de ce rapport, les « autres intrusions » sont définies comme des intrusions qui n'ont pas abouti à un ransomware ou à tout autre type d'attaque traquée.

Une intrusion est souvent le résultat de l'exploitation d'une vulnérabilité non corrigée, telle que ProxyLogon et ProxyShell, mais elle peut également résulter de l'utilisation abusive de services d'accès à distance ou de VPN non sécurisés, du vol d'identifiants de connexion ou de négligences en matière de sécurité (comme le fait de laisser des points d'entrée ouverts sur Internet).

L'essentiel est que les intrusions aient été détectées et neutralisées avant qu'une charge utile malveillante importante ne soit livrée sur la cible. On peut supposer que certaines, voire la plupart, de ces intrusions étaient des surplus appartenant aux IAB : des accès « mis en réserve » qui n'avaient pas encore été vendus à un autre acteur malveillant. Si les intrusions n'avaient pas été détectées, il est probable qu'un nombre important d'entre elles se seraient terminées par une attaque de ransomware.

Les cryptomonnaies étaient le principal type d'attaque dans 2 % des incidents investigués. La présence de cryptomineurs malveillants est souvent détectée grâce à leur impact sur les performances du système, car le minage illégal de cryptomonnaies consomme énormément de puissance de traitement sur les ordinateurs. Il peut être tentant de considérer les cryptomineurs comme une menace de bas niveau, mais le fait qu'ils soient présents sur le réseau prouve qu'il existe un point d'entrée vulnérable quelque part. Ils peuvent être le signe avant-coureur de menaces bien plus graves.

Il en va de même pour les droppers et les systèmes de livraison de logiciels malveillants en général, qui sont conçus pour livrer, charger ou installer d'autres charges utiles malveillantes sur un système cible. Ce sont des catalyseurs pour une attaque en cours, offrant une plateforme pour des modules malveillants supplémentaires, tels que des portes dérobées ou des ransomwares. Les défenseurs doivent donc traiter la présence de droppers et de systèmes de diffusion de logiciels malveillants, dont Trickbot, Emotet et d'autres, avec le même sérieux qu'un grand groupe de ransomwares, car ils sont souvent les précurseurs d'attaques plus importantes.

Un terrain de jeu bondé

Les types d'attaques ne s'excluent pas mutuellement. Comme nous l'avons mentionné plus haut, plusieurs attaquants, y compris des IAB, des gangs de ransomware et des cryptomineurs, peuvent se trouver en même temps dans un même réseau cible.

Par exemple, alors que les cryptomineurs étaient le principal type d'attaque dans seulement 2 % des incidents, ils étaient également présents dans 7 % des incidents de ransomware. Les cryptomineurs recherchent et suppriment souvent d'autres mineurs dans les réseaux infectés, mais ils peuvent coexister sans problème avec d'autres menaces, comme les ransomwares.

Les attaques simultanées identifiées par Sophos en 2021 comprennent une attaque impliquant le ransomware Atom Silo en compagnie de deux cryptomineurs, ainsi qu'une double attaque de ransomware impliquant Netwalker et REvil. Et cette tendance se poursuit en 2022.

La boite à outils des attaquants

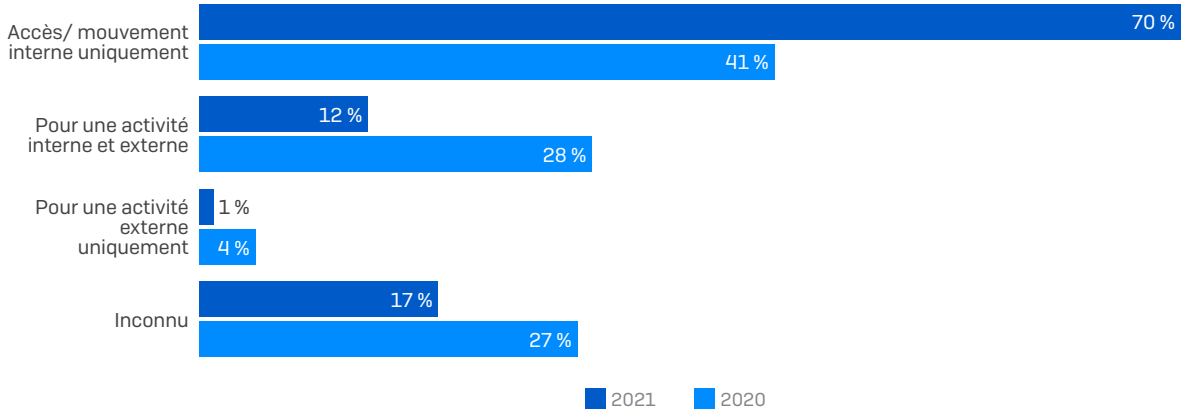
Les services de bureau à distance constituent une menace interne majeure

Le RDP (Remote Desktop Protocol) a joué un rôle dans au moins 83 % des attaques, en augmentation par rapport à 2020 où il était identifié dans 73 % des attaques. Une utilisation interne du RDP était identifiée dans 82 % des cas et une utilisation externe dans 13 % des cas. Ces chiffres étaient respectivement de 69 % et 32 % en 2020.

Toutefois, la manière dont les attaquants ont utilisé le RDP mérite d'être soulignée. Dans moins de trois quarts (70 %) des incidents impliquant le RDP, l'outil a été utilisé *uniquement* pour un accès interne et des mouvements latéraux, ce qui représente une augmentation significative par rapport aux 41 % de 2020.

Le RDP a été utilisé pour un accès externe *uniquement* dans 1 % des cas, contre 4 % en 2020. Et seulement 12 % des attaques ont montré que les attaquants utilisaient le RDP à la fois pour un accès externe et le mouvement interne, soit moins de la moitié de ce qui avait été observé en 2020 (qui était 28 %).

Utilisation du RDP (Remote Desktop Protocol) par les attaquants



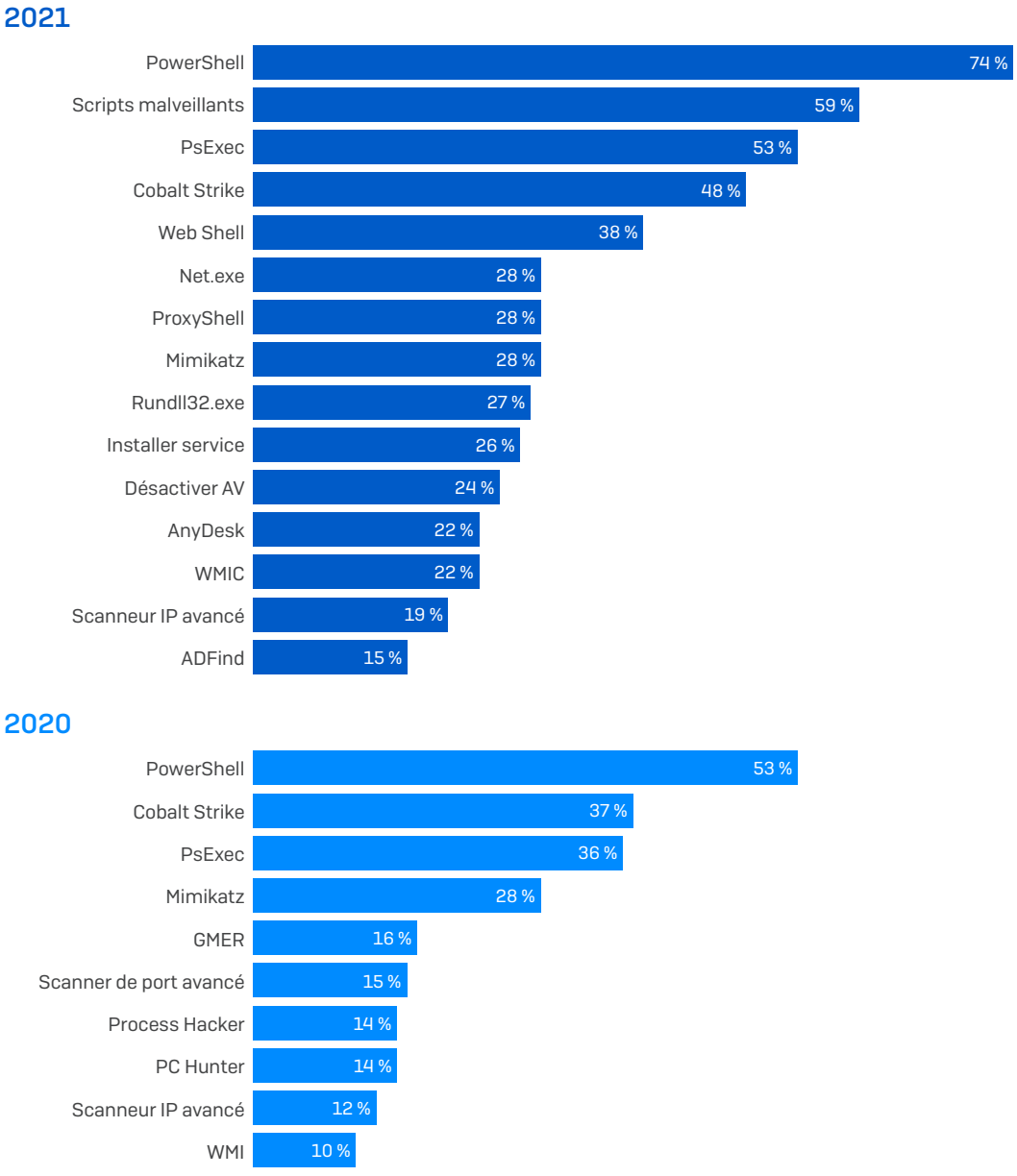
Le déclin de l'utilisation du RDP pour un accès externe est probablement le reflet d'une amélioration de la sécurité, notamment par la désactivation du service. Cependant, le RDP reste largement accessible à l'intérieur du périmètre, et le durcissement de cet accès doit être une priorité pour les équipes de sécurité.

Les outils d'attaque en 2021

Le tableau ci-dessous montre les « artefacts », notamment les outils, les techniques et les services, les plus susceptibles de se trouver dans la panoplie d'outils d'un attaquant en 2021. Nombre d'entre eux peuvent également être utilisés par les professionnels de l'informatique à des fins totalement bénignes. Ils sont populaires auprès des attaquants, car ils leur permettent de mener des activités telles que le vol d'identifiants, la découverte, le mouvement latéral et l'exécution de logiciels malveillants, et plus encore, tout en se faisant passer pour une activité informatique quotidienne inoffensive.

Le nombre et la nature des artéfacts mettent en évidence l'ampleur du défi auquel les défenseurs sont confrontés pour différencier les activités malveillantes des activités légitimes sur le réseau.

Principaux artéfacts utilisés dans les attaques



Un examen plus approfondi des éléments les plus populaires utilisés dans les attaques révèle le playbook typique des cyberattaques en 2021.

Les artéfacts qui composent les boites à outils

Les artéfacts identifiés lors des investigations sur les incidents peuvent être divisés en 3 catégories : outils légitimes et de piratage, binaires Microsoft, et artéfacts supplémentaires (scripts, techniques, services, etc.).

Les investigations ont permis de trouver 525 artéfacts différents, contre 132 en 2020 (bien que la taille de l'échantillon de base était également plus importante), dont 209 outils légitimes et de piratage, 107 binaires Microsoft et 209 artéfacts supplémentaires.

Outils légitimes et de piratage

Il s'agit de logiciels qui ont été utilisés pour faciliter une attaque. Cobalt Strike (48 %) et Mimikatz (28 %) conservent les deux premières places obtenues en 2020, suivis de AnyDesk (22 %), Advanced IP Scanner (19 %) et ADFind (15 %). Par rapport à 2020, Cobalt Strike a augmenté sa part (partant de 37 %), Mimikatz est resté stable (se maintenant à 28 %), et trois nouveaux outils ont fait irruption dans le top 5.

Cobalt Strike est une suite d'outils d'exploitation produite commercialement et conçue pour aider les équipes de sécurité à recréer un large éventail de scénarios d'attaque. Les attaquants tentent d'établir une porte dérobée « balise » Cobalt Strike sur une machine infectée. Les balises peuvent être configurées pour exécuter des commandes, télécharger et exécuter des logiciels supplémentaires, relayer des commandes à d'autres balises installées sur un réseau ciblé et communiquer avec le serveur Cobalt Strike. Toute détection de Cobalt Strike sur le réseau doit être immédiatement investiguée.

Le deuxième outil le plus répandu, **Mimikatz**, a également été conçu à l'origine comme un outil de sécurité offensif, et peut voler des mots de passe et d'autres identifiants de connexion pour les utiliser dans une attaque.

Des scanners de réseau légitimes, tels que **Advanced Port Scanner** ou **IP Scanner**, sont utilisés pour générer une liste d'adresses IP et de noms de périphériques, pour permettre aux attaquants de cibler les machines et les infrastructures informatiques les plus critiques de l'organisation ciblée.

L'utilisation abusive de l'outil de gestion informatique légitime **AnyDesk** est de plus en plus courante, car il offre aux attaquants un contrôle direct de l'ordinateur cible, y compris le contrôle de la souris/du clavier et la possibilité de voir l'écran. Les services d'accès à distance légitimes tels que **TeamViewer**, **Screen Connect**, **Atera RMM** et **Splashtop** étaient également très populaires en 2021.

Process Hacker, **PCHunter** et **GMER** sont tous des outils légitimes qui incluent des pilotes de noyau. Si un attaquant parvient à installer le bon pilote de noyau, il peut souvent désactiver les produits de sécurité.

Binaires Microsoft

Séparer les outils Microsoft des outils génériques montre comment les attaquants exploitent les ressources qui sont déjà disponibles, ou ce qu'on appelle en anglais : « living off the land ». Ces outils sont tous signés numériquement par Microsoft. Sans surprise, **PowerShell** (74 %) arrive en tête de liste, suivi de **PsExec** (53 %), de "**net.exe**" (28 %), de "**rundll32.exe**" (27 %) et de l'outil de **Ligne de commande WMI** (WMIC) (22 %). L'utilisation de PowerShell, PsExec et WMIC a augmenté en 2021 par rapport à 2020.

L'outil "net.exe" a été utilisé dans de nombreuses phases d'une attaque, le plus souvent comme outil de découverte, tandis que "rundll32.exe" a été largement utilisé pour l'exécution et le contournement des défenses.

Les autres outils Microsoft qui pourraient indiquer la présence d'un attaquant sur le réseau sont "**whoami.exe**", le **Planificateur de tâches** (pour maintenir la persistance) et "**schtasks.exe**" (pour exécuter un code malveillant). L'utilisation de ces outils doit être étroitement surveillée.

Artéfacts supplémentaires

Cette catégorie comprend à la fois les outils et les techniques, comme la tentative de désactiver la protection, les vulnérabilités telles que ProxyShell, l'utilisation de services Cloud tels que **Mega.io**, les logiciels malveillants supplémentaires trouvés, les infections secondaires et les protocoles de transport utilisés.

Des **scripts malveillants** (hors PowerShell) ont été observés dans 59 % des incidents investigués. Les scripts malveillants sont des codes logiciels qui permettent une activité malveillante. Parmi les exemples de scripts utilisés à mauvais escient par les attaquants figurent les scripts DOS/CMD en mode batch et en ligne de commande, les scripts Python (une collection de commandes dans un fichier à exécuter comme un programme) et les VBScripts (scripts Visual Basic pouvant être exécutés dans Windows ou dans l'Explorateur Windows).

Les webshells constituent le deuxième type de menace le plus courant (observés dans 38 % des incidents), avec ProxyShell (28 %) et ProxyLogon (11 %). L'installation de services, la désactivation de la protection, le vidage de LSASS, la création de comptes pirates, la modification du registre et l'effacement des journaux complètent le top 10.

Exfiltration de données

En 2021, **Rclone** a fait son entrée sur la liste des principaux artéfacts utilisés pour l'exfiltration de données. Rclone est un outil de ligne de commande qui se connecte à une grande variété de fournisseurs de stockage dans le Cloud, comme Mega. Il était en 2021 l'outil le plus utilisé dans l'exfiltration de données. Parmi les autres fournisseurs de stockage Cloud figurant dans les investigations de 2021 figurent **Dropbox**, **DropMeFiles**, **M247**, **pCloud** et **Sendspace**.

En plus de Rclone, les outils découverts au cours des investigations dont l'activité a permis d'exfiltrer des données incluent **Megasync**, **FileZilla**, **Handy Backup**, **StealBit**, **WinSCP** et **Ngrok**.

L'apparition d'outils d'exfiltration dans le top 10 en 2021 n'est pas surprenante si l'on considère que 38 % de tous les incidents investigués impliquaient une exfiltration de données, contre 27 % en 2020. Un certain nombre d'autres incidents (8 % au total) ont montré des signes de collecte de données et de préparation en vue d'une éventuelle exfiltration. Dans les cas où l'exfiltration a eu lieu, les preuves suggèrent que les informations volées ont ensuite été divulguées dans 46 % des incidents.

Les attaquants suppriment généralement les informations juste avant de déployer le ransomware. L'analyse des incidents par Sophos montre qu'en 2021, le laps de temps médian entre l'exfiltration des données et le déploiement d'un ransomware était d'environ 44 heures. Le délai moyen était d'un peu plus de 4 jours (4,28 jours) et le délai médian était inférieur à 2 jours (1,84 jour).

Quelle que soit la moyenne utilisée, le message important est qu'après l'exfiltration, les défenseurs disposent d'une possible fenêtre d'opportunité pour empêcher la phase finale la plus dommageable de l'attaque de se produire. Toute détection d'outils réputés pour être utilisés dans l'exfiltration de données doit donc être investiguée en priorité.

Combinaisons d'outils

Les investigations des incidents ont permis de révéler un schéma de combinaisons d'outils utilisés sur les réseaux des victimes qui constitue un puissant signal d'alerte pour les équipes de sécurité informatique (des données comparatives pour 2020 étaient disponibles dans certains cas) :

- En 2021, PowerShell et des scripts malveillants non-PS ont été observés ensemble dans 64 % des cas
- PowerShell et Cobalt Strike ont été combinés dans 56 % des cas, contre 58 % en 2020
- PowerShell et PsExec ont été trouvés dans 51 % des cas, contre 49 % en 2020
- PowerShell, des scripts malveillants et Cobalt Strike ont été détectés dans 42 % des cas
- PowerShell, des scripts malveillants et PsExec ont été observés dans 38 % des cas
- PowerShell, Cobalt Strike et PsExec sont présents dans 33 % des incidents, contre 12 % en 2020
- Cobalt Strike et Mimikatz ont été vus ensemble dans 16 % des cas

Ces corrélations restent aussi importantes cette année que l'année dernière, car leur détection peut être un signe avant-coureur d'une attaque imminente ou confirmer la présence d'une attaque active.

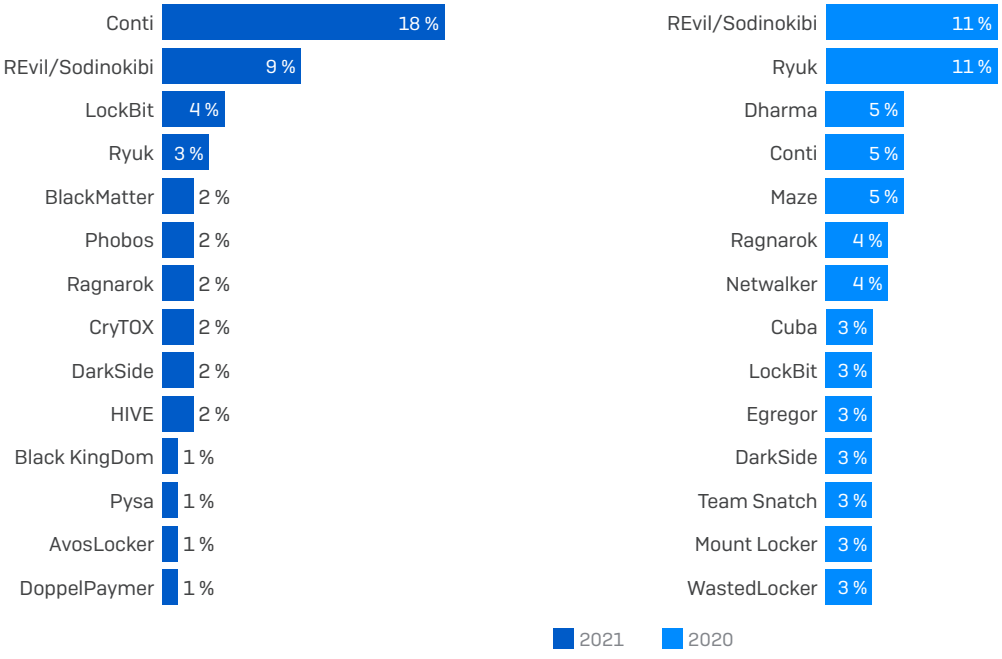
Les principaux acteurs de ransomware en 2021

41 acteurs de ransomware différents ont été identifiés dans les 144 incidents inclus dans l'analyse. Parmi ceux-ci, environ deux tiers (28) étaient de nouveaux groupes signalés pour la première fois en 2021. 18 groupes de ransomwares identifiés dans des incidents en 2020 ont disparu de la liste en 2021. Cela montre clairement à quel point le paysage des cybermenaces est devenu dense, dynamique et complexe, et combien cela peut compliquer la vie des défenseurs.

À bien des égards, l'année 2021 a « appartenu » à Conti, un opérateur RaaS prolifique qui est à l'origine d'un peu moins d'un incident sur cinq (18 %) investigué par Sophos. Il convient toutefois de noter que le ransomware REvil est à l'origine d'un incident sur dix, bien qu'il ait apparemment cessé ses activités en juillet 2021 (il est réapparu brièvement en septembre 2021, puis en 2022).

Parmi les autres familles de ransomware les plus répandues en 2021, citons DarkSide, le RaaS à l'origine de la fameuse attaque contre Colonial Pipeline aux États-Unis, et Black KingDom, l'une des « nouvelles » familles de ransomware apparues en mars 2021 à la suite de la vulnérabilité ProxyLogon.

Attribution : principaux acteurs de ransomware



Environ un quart (24 %) des incidents en 2021, et 25 % en 2020, ont été attribués à d'autres groupes de ransomware, tandis que le reste des incidents n'a pu être attribué avec certitude à aucun groupe connu.

Sophos a publié de nombreux articles sur le ransomware Conti. Une liste complète d'articles sur Conti et d'autres familles de ransomware communes, y compris LockBit, Ryuk, et plus encore, peut être trouvée dans le Centre de renseignements sur les menaces de ransomware de Sophos.

Conclusion

Chaque organisation est une cible potentielle pour un adversaire à un moment donné, et, de plus en plus, elle peut être visée par plusieurs acteurs malveillants Qu'il s'agisse de phishing, de fraude financière, de création de réseaux de zombies, de plateformes de diffusion de logiciels malveillants, de cryptomonnaies, d'IAB, de vol de données, d'espionnage d'entreprise, de ransomware, etc., s'il existe un point d'entrée vulnérable dans un réseau, il y a de fortes chances que des attaquants le recherchent et finissent par le trouver et l'exploiter.

Jusqu'à ce que le point d'entrée exposé soit traité et que tout ce que les attaquants ont mis en place pour établir et conserver l'accès soit complètement éradiqué, à peu près n'importe qui peut entrer grâce au travail réalisé par ces derniers. Et ce sera probablement le cas.

Les équipes de sécurité peuvent défendre leur organisation en surveillant et en enquêtant sur les activités suspectes. La différence entre inoffensif et malveillant n'est pas toujours facile à repérer. La technologie, quel que soit l'environnement concerné, qu'il soit de type cyber ou physique, peut faire beaucoup, mais elle ne suffit pas à elle seule. L'expérience, les compétences humaines ainsi que les capacités en matière de réponse sont des éléments essentiels de toute solution de sécurité.

Les principales leçons à tirer en matière de réponse aux incidents de 2021 concernent véritablement la rapidité et l'ampleur avec lesquelles les vulnérabilités courantes et faciles à exploiter sont utilisées par les adversaires, permettant ainsi de mettre en œuvre des intrusions plus longues avec l'implication de multiples adversaires. Pour les défenseurs, ces leçons signifient que détecter, investiguer et répondre aux signaux d'alerte concernant les outils et techniques connus de l'adversaire n'a jamais été aussi important.

Sophos Rapid Response

Les conclusions de ce rapport sont basées sur des données provenant d'incidents investigués par Sophos Rapid Response, une équipe d'expert en réponse aux incidents et en neutralisation des menaces. Le service Sophos Rapid Response est disponible à la fois pour les clients Sophos actuels, mais aussi pour les clients non Sophos.

Si vous êtes confronté à un incident actif et que vous souhaitez parler avec l'équipe Rapid Response, appelez les numéros ci-dessous à tout moment :

Allemagne : +49 611 711 86 766

Australie : +61 272 084 454

Canada : +1 778 589 7255

États-Unis : +1 408 746 1064

France : +33 1 86 53 98 80

Italie : +39 02 873 17993

Royaume-Uni : +44 1235 635 329

Suède : +46 858 400 610

Tableaux de données supplémentaires

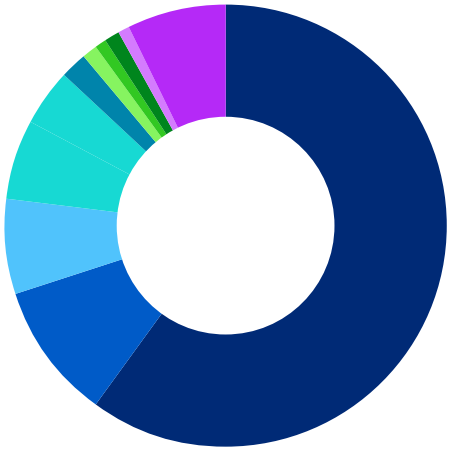
Artéfacts des investigations des incidents mis en correspondance avec la chaîne d'attaque de MITRE

Les outils, techniques et autres artéfacts observés lors de l'investigation des incidents ont été mis en correspondance avec le cadre ATT&CK de MITRE. Des détails supplémentaires seront publiés dans un article complémentaire sur Sophos News.

Étapes de MITRE Attack											
Accès initial	Exécution	Persistance	Élévation des privilèges	Contourne-ment de la défense	Accès aux identifiants	Détection	Mouvement latéral	Collecte	Command and Control	Exfiltration	Impact
Artéfacts											
Services à distance	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Scanneur IP avancé	RDP	Navigation sur le réseau	Cobalt Strike	Rclone	Données chiffrées
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Network Breach

Profil démographique de la réponse aux incidents en 2021

Nombre d'incidents par pays

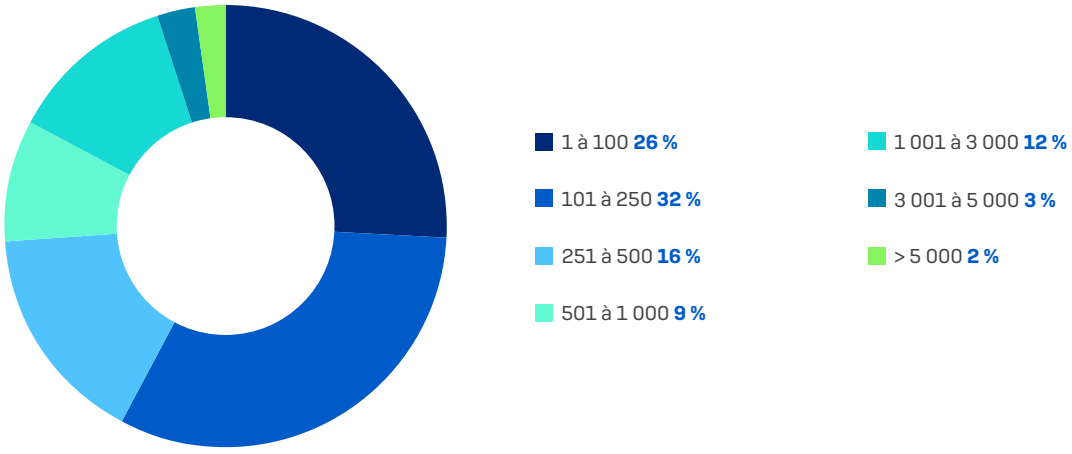


- US **60 %**
- Allemagne **10 %**
- R.U. **7 %**
- Canada **6 %**
- Italie **4 %**
- Espagne **2 %**
- France **1 %**
- Suisse **1 %**
- Belgique **1 %**
- Philippines **1 %**
- Autre **7 %** (Pays-Bas, Autriche, Émirats arabes unis, Arabie saoudite, Bahamas, Angola, Japon)

Nombre d'incidents par secteur

- Manufacturier **17 %**
- Retail **14 %**
- Santé **12 %**
- Informatique **9 %**
- Construction **8 %**
- Éducation **6 %**
- Alimentaire **4 %**
- Logistique **4 %**
- Finance **4 %**
- Divertissement **3 %**
- Services **3 %**
- Médias **3 %**
- Autre **13 %** (Transport, Pharmaceutique, MSP/Hébergement, Non lucratif, Gouvernement, Hôtellerie, Juridique, Agriculture, Énergie, Immobilier)

Nombre d'incidents par taille de l'organisation (Nb d'employés)



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

2022-05-25 FR (DD)

SOPHOS