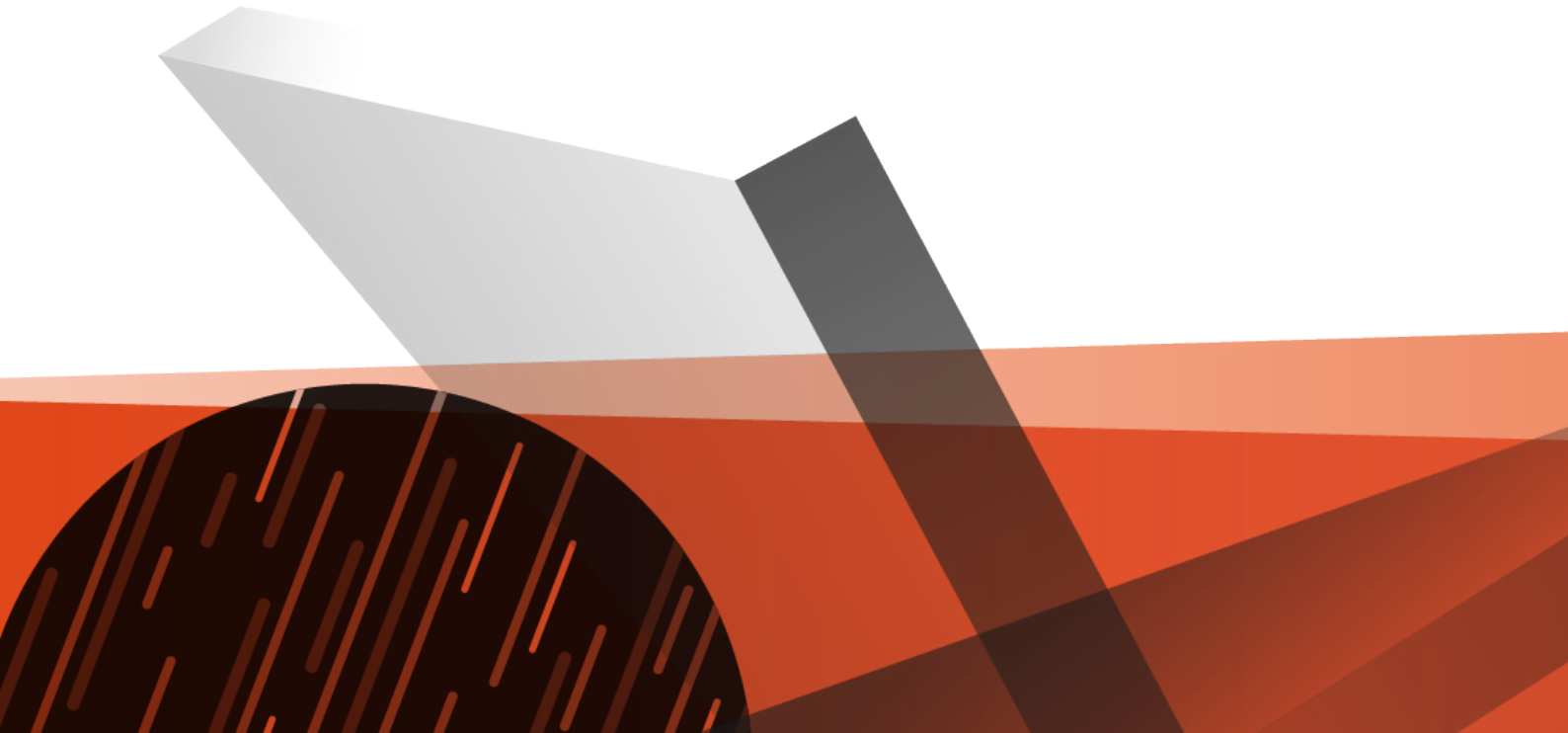
FIREEYE | MANDIANT

RAPPORT DE SYNTHÈSE



Un éclairage instructif sur les réalités des cyberattaques

En 2020, le monde de la cybersécurité s'est frotté à des enjeux dont l'envergure et le caractère inédits ont poussé les entreprises en territoire inconnu. Alors même que les attaques par ransomware se sont multipliées à l'encontre des administrations publiques, des collectivités locales, des services de santé et des établissements d'enseignement, les mesures de lutte contre la pandémie de COVID-19 ont contraint la majeure partie de l'économie à basculer vers des modèles de télétravail. Dans l'urgence, les entreprises ont dû adopter de nouvelles technologies tout en bousculant leurs plans de croissance initiaux pour s'adapter à cette nouvelle « normalité ».

Quelques mois plus tard, UNC2452, un groupe soupçonné d'être à la solde d'un État, a mené l'une des campagnes de cyberespionnage les plus sophistiquées des dernières années. Face à l'ampleur de la menace, les équipes de sécurité informatique ont dû suspendre le grand chantier du télétravail pour se recentrer sur la lutte contre ce type d'attaque dissimulée dans une plateforme de confiance.

Cyberespionnage étatique des laboratoires travaillant sur un vaccin, alliance des attaquants autour d'offensives coordonnées, exploitation de nouvelles vulnérabilités liées au télétravail, dangers de compromission de la supply chain… Les incidents observés en 2020 sont appelés à redessiner les contours des politiques de sécurité pour les années à venir.

Voici un résumé des constatations relatées dans l'édition 2021 du rapport M-Trends :

- 59 % des intrusions analysées par Mandiant au cours des douze derniers mois ont été détectées en interne par les entreprises, soit une amélioration de 12 % sur un an.
- Le ransomware prend la forme d'un système d'extorsion protéiforme : les attaquants ne se contentent plus de chiffrer les données de leurs victimes mais emploient à présent divers moyens de pression pour forcer les victimes à accéder à leurs demandes.
- Un groupe à visée financière récemment nommé FIN11 par Mandiant a mené des campagnes de phishing à grande échelle dans le cadre d'opérations de double extorsion.
- La durée médiane de présence continue de baisser en raison d'une forte recrudescence d'attaques par ransomware capitalisant sur la crise sanitaire et l'évolution des modes de travail.

- UNC2452, un groupe suspecté d'appartenir à une filière étatique, a mené une campagne d'espionnage massive consistant à injecter un DLL malveillant dans la chaîne de développement de la plateforme SolarWinds Orion. Mandiant a identifié cette offensive et collaboré avec les pouvoirs judiciaires et les acteurs de la cybersécurité pour organiser la riposte et protéger les entreprises.
- Les investigations de Mandiant montrent que les cybercriminels ont utilisé 63 % des techniques MITRE ATT&CK et que près d'un tiers des méthodes observées ont été employées dans plus de 5 % des intrusions.
- Les attaquants ont ciblé l'infrastructure sous-tendant le télétravail en mettant l'accent sur les exploits de vulnérabilités.

L'une des tendances les plus marquantes observées sur la période du 1er octobre 2019 au 30 septembre 2020 est la réduction significative de la durée médiane de présence à l'échelle mondiale : pour la première fois, celle-ci passe sous la barre d'un mois (24 jours). Ce bon résultat s'explique par l'amélioration de la visibilité et des capacités de réponse des entreprises, mais aussi par la montée en puissance des attaques par ransomware, qui tendent à raccourcir le délai entre l'infection initiale et la détection.

Le rapport 2021 ajoute à ces observations de nouveaux indicateurs et chiffres clés, un portrait du groupe cybercriminel nouvellement nommé FIN11, ainsi que de nouvelles études de cas. Cette édition du M-Trends poursuit donc sa mission essentielle de transparence au service des professionnels de la cybersécurité. Les informations présentées dans ce document ont été anonymisées afin de protéger les identités des victimes et leurs données.

LES CHIFFRES CLÉS

Les investigations FireEye Mandiant nous livrent leurs données

Les indicateurs présentés dans le rapport M-Trends 2021 s'appuient sur les investigations menées par FireEye Mandiant dans le cadre d'attaques ciblées, perpétrées entre le 1er octobre 2019 et le 30 septembre 2020.

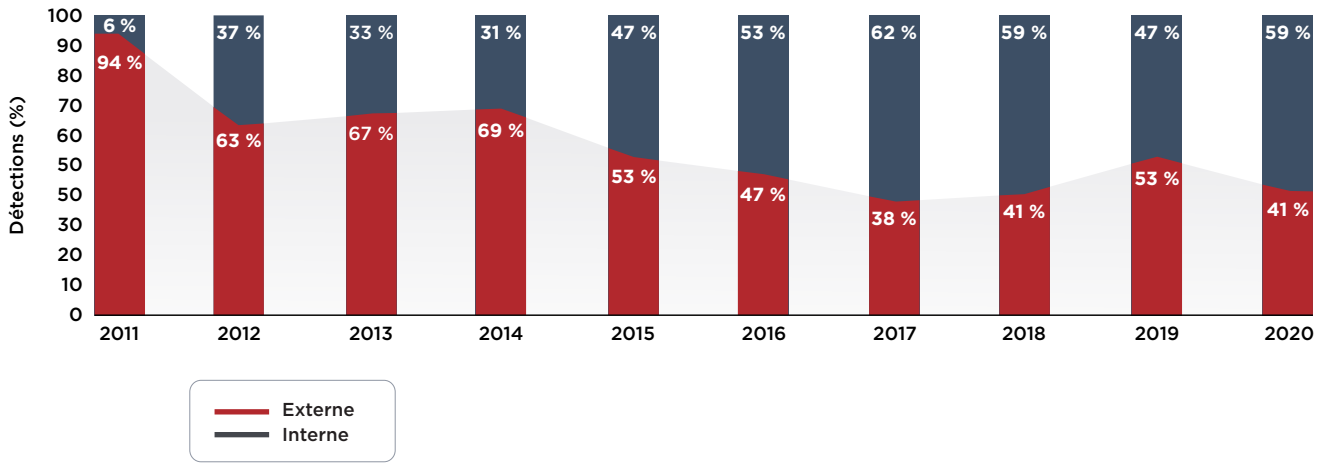
Détection par source

Les entreprises continuent d'améliorer leurs capacités de détection des compromissions au sein de leurs environnements. Alors que notre précédent rapport notait une baisse des notifications internes pour l'année 2019, les chiffres 2020 montrent que les entreprises reprennent la main en repérant par elles-mêmes la majorité des incidents de sécurité dont elles sont victimes. La part des cas de détection interne atteint 59 %, soit une augmentation de 12 points par rapport à 2019. Ce résultat marque donc un retour à la tendance générale des dix dernières années. D'une part, il traduit l'engagement continu des entreprises à élargir et renforcer leurs capacités organiques de détection et de réponse. De l'autre, il est une conséquence directe de l'essor des campagnes de ransomware.

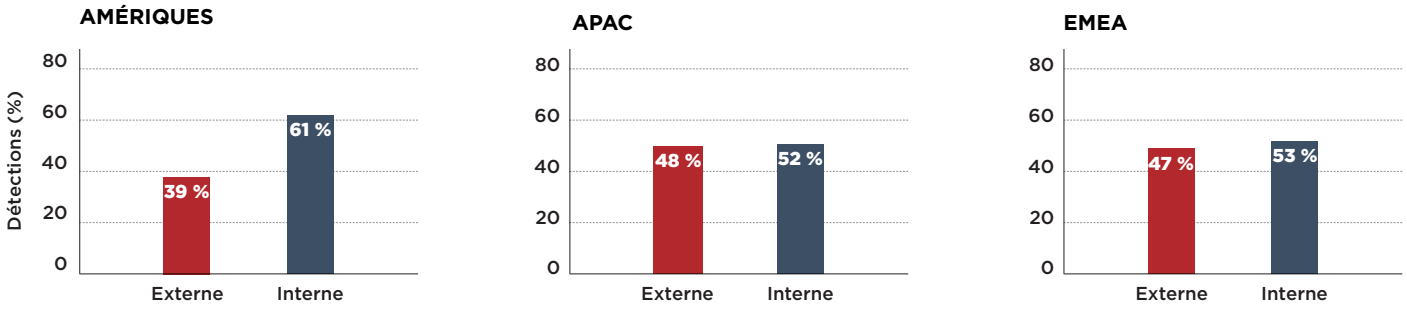
La **détection interne** désigne les cas de compromission découverts par les entreprises victimes elles-mêmes.

Une **notification externe** est un cas dans lequel une entité tierce informe une entreprise qu'elle a été compromise.

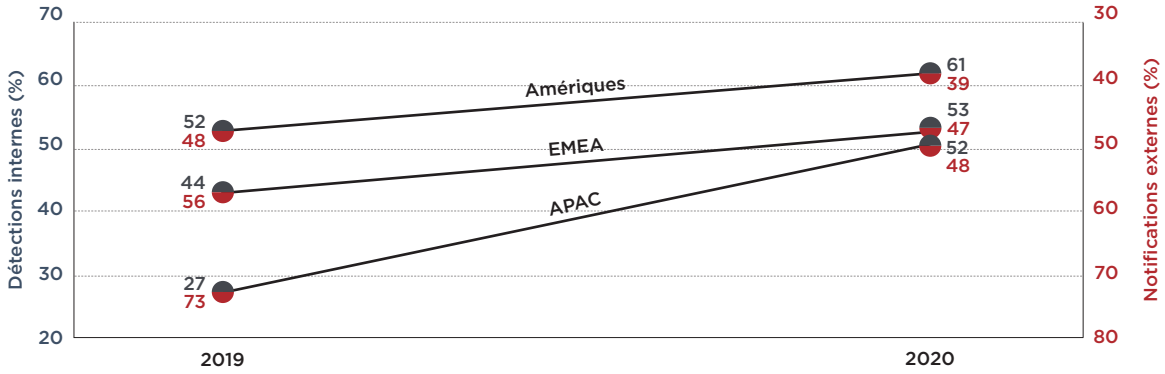
DÉTECTION PAR SOURCE – 2011 À 2020



DÉTECTION PAR SOURCE ET PAR RÉGION – 2020



DÉTECTION PAR SOURCE ET PAR RÉGION – COMPARATIF 2019-2020



La **durée de présence** correspond au nombre de jours d'implantation d'un attaquant dans le réseau d'une victime avant sa détection. Une valeur médiane permet de diviser un ensemble de données en deux parties égales.

Durée de présence

Les entreprises repèrent et endiguent les menaces de plus en plus rapidement. Au cours des dix dernières années, on note une réduction significative de la durée médiane de présence, passant d'un an en 2011 à tout juste moins d'un mois en 2020.

Durée médiane de présence

416 JOURS EN 2011 ➤ **24** JOURS EN 2020

Durée de présence à l'échelle mondiale

En 2020, la durée médiane de présence dans le monde a chuté pour la première fois sous la barre d'un mois : les entreprises détectent les incidents en seulement 24 jours, soit deux fois plus vite qu'en 2019. D'après nos observations, les progrès sont généraux, indépendamment de la source de notification. Pour les incidents détectés en interne, la durée médiane de présence à l'échelle mondiale passe à 12 jours, contre 73 jours pour les notifications externes.

DURÉE MÉDIANE DE PRÉSENCE DANS LE MONDE – 2011 À 2020

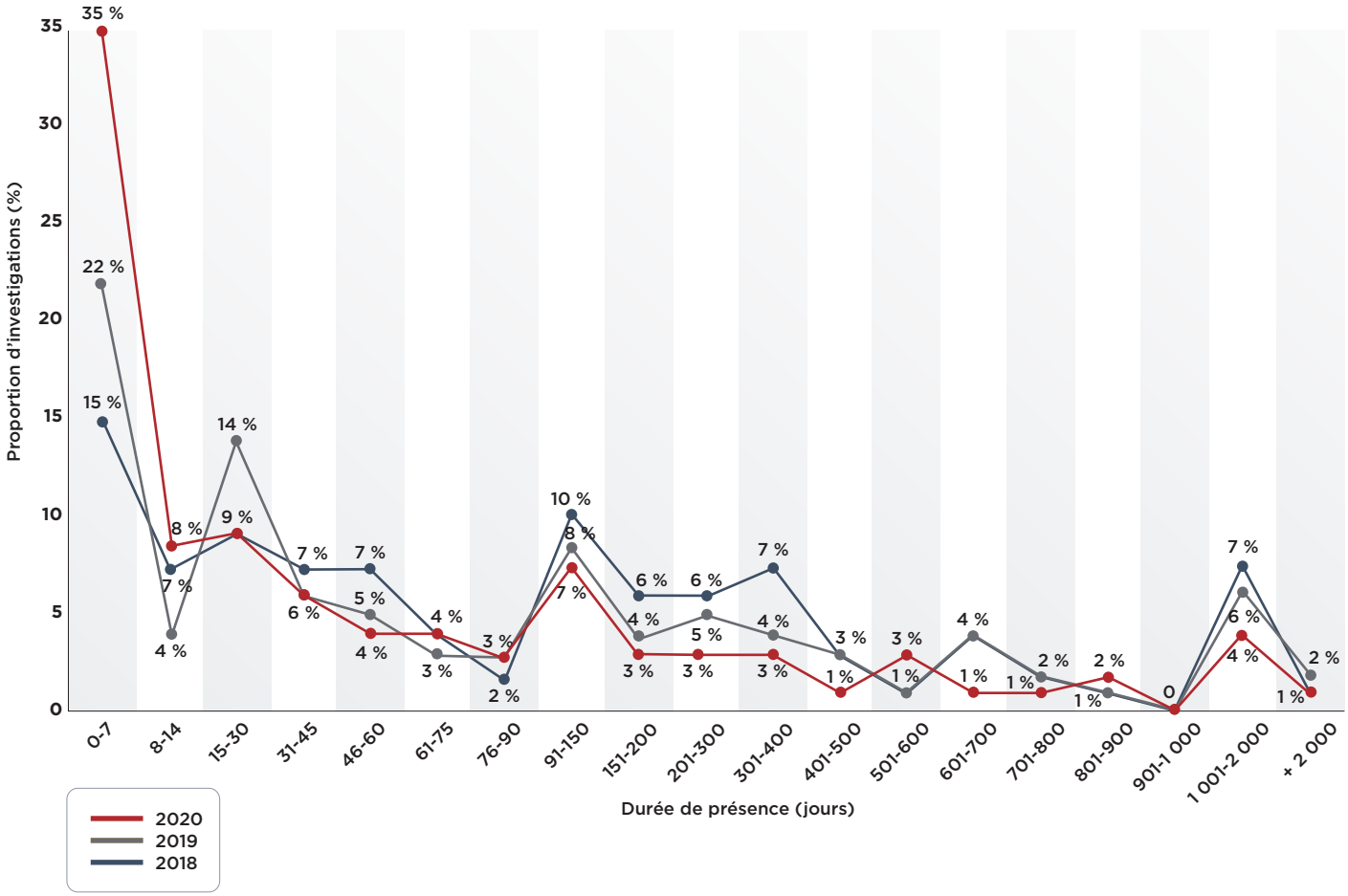
Notifications de compromissions	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Tout	416	243	229	205	146	99	101	78	56	24
Notification externe	–	–	–	–	320	107	186	184	141	73
Détection interne	–	–	–	–	56	80	57,5	50,5	30	12

Répartition de la durée médiane de présence à l'échelle mondiale

Par rapport aux années précédentes, les entreprises détectent globalement plus d'incidents au cours des 30 premiers jours d'une intrusion et moins lorsque la présence dépasse les 700 jours. La répartition des données mondiales montre une augmentation continue de la part d'incidents associés à une durée de présence de 30 jours ou moins : celle-ci passe de 31 % en 2018, à 41 % en 2019 puis 52 % en 2020. On note également quelques améliorations à l'autre extrémité de la plage de valeurs, puisque les experts Mandiant observent une réduction de 3 % des investigations impliquant une durée de présence supérieure à 700 jours.

La tendance générale de ces trois dernières années peut s'expliquer par le développement et l'amélioration continus des capacités de détection interne des entreprises, ainsi que par l'évolution du champ des menaces.

RÉPARTITION DE LA DURÉE MÉDIANE DE PRÉSENCE DANS LE MONDE – 2018 À 2020

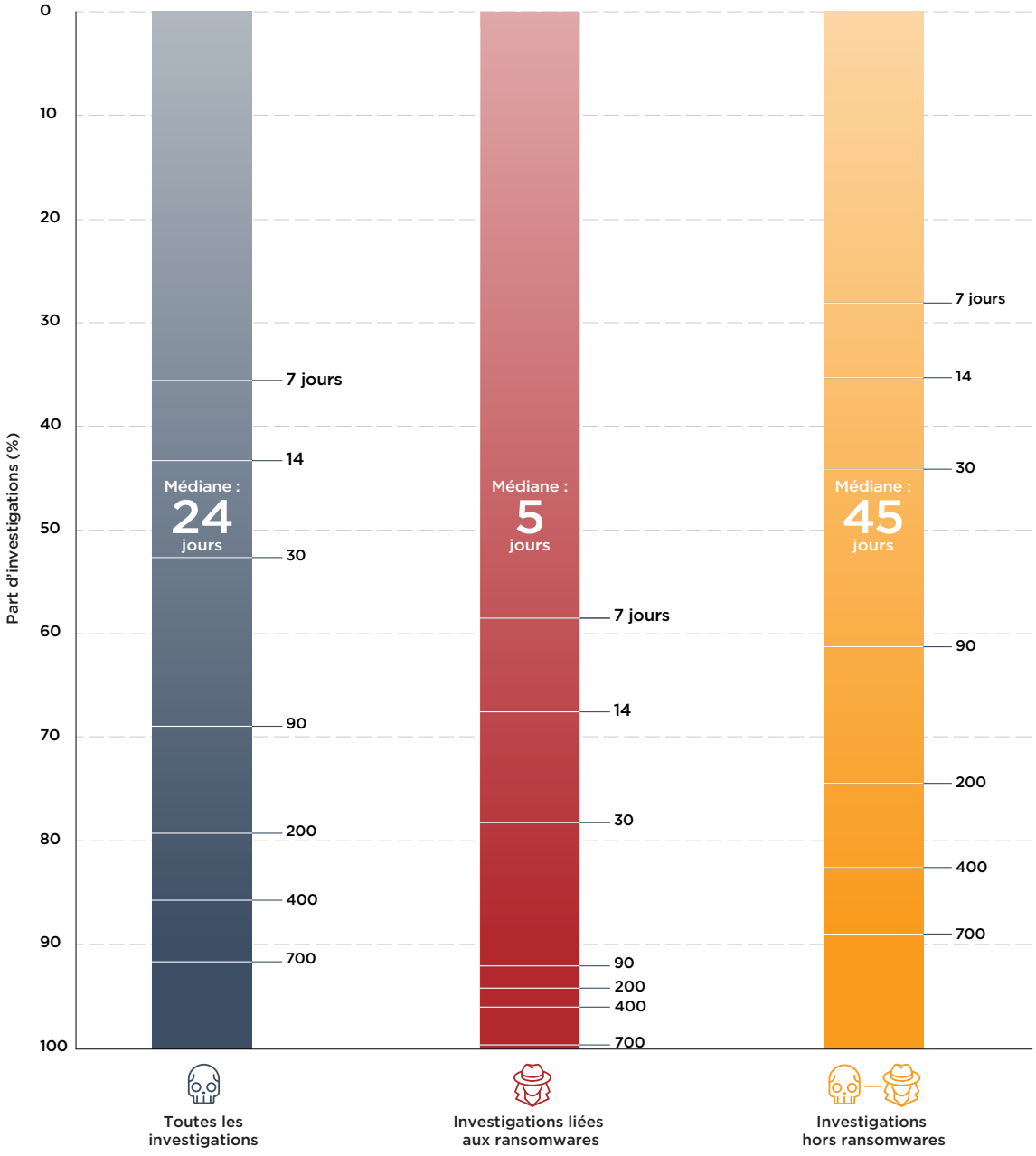


Investigations impliquant un ransomware

14 % EN 2019 ➤ **25** % EN 2020

Le raccourcissement de la durée de présence s'explique notamment par la hausse continue de la proportion d'investigations impliquant des ransomwares, qui passe de 14 % en 2019 à 25 % en 2020. Concrètement, 78 % des intrusions de ce type sont détectées en 30 jours ou moins, contre 44 % pour les autres attaques. De même, les experts Mandiant notent que seulement 1 % des campagnes de ransomware ont une durée de présence de 700 jours ou plus, contre 11 % pour le reste.

DURÉE DE PRÉSENCE DANS LE MONDE PAR TYPE D'INVESTIGATION – 2020



Évolution de la durée médiane de présence en zone Amériques

60 ➤ **17**

JOURS EN 2019 **JOURS EN 2020**

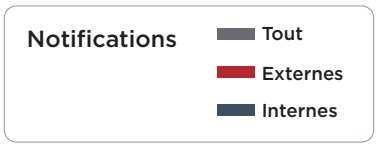
Durée médiane de présence en zone Amériques

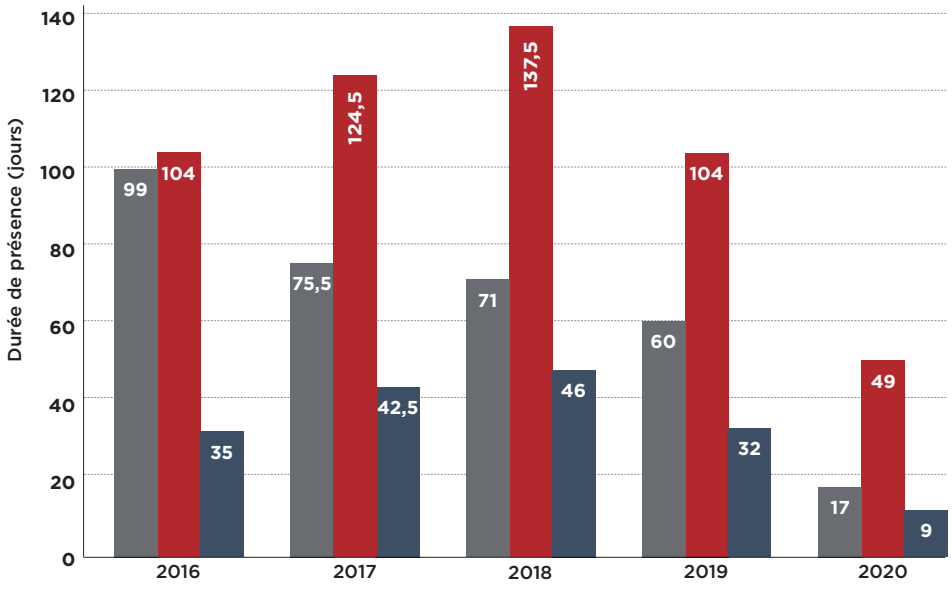
Le continent américain enregistre à nouveau une baisse de la durée médiane de présence en 2020. Les cas de détection interne enregistrent les plus forts progrès, puisque ce délai passe de 32 à 9 jours, tombant ainsi pour la première fois sous la barre des 10 jours au sein d'une même région.

La durée médiane de présence est 3,5 fois plus courte en 2020 qu'en 2019. Cette accélération se vérifie pour les cas de détection interne comme pour les notifications externes de compromission, dont les délais sont respectivement 3,6 et 2,1 fois plus courts que l'an passé.

En 2020, 27,5 % des investigations de sécurité de la zone Amériques ont impliqué un ransomware. Cette part élevée contribue sans aucun doute à la réduction de la durée médiane de présence, puisque les attaques par ransomware sont détectées en seulement 3 jours et comptent pour 41 % des incidents impliquant une durée de présence inférieure ou égale à 14 jours.

DURÉE MÉDIANE DE PRÉSENCE – AMÉRIQUES – 2016 À 2020





Évolution de la durée médiane de présence en zone APAC

54 ➤ **76**

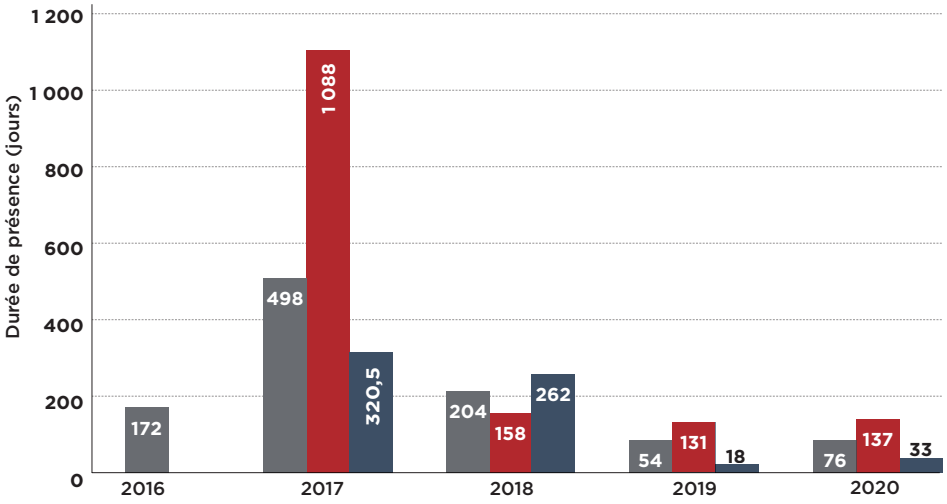
JOURS EN 2019 **JOURS EN 2020**

Durée médiane de présence en zone APAC

Dans la région APAC, la durée médiane de présence passe de 54 jours en 2019 à 76 jours en 2020. On assiste par ailleurs à une réduction du nombre de compromissions impliquant un ransomware, qui passent de 18 % des incidents de sécurité en 2019 à 12,5 % en 2020. Ceci peut expliquer en partie la hausse globale de la durée médiane de présence constatée dans la région.

On note également que les attaquants continuent de s'implanter durablement au sein des environnements compromis : 10 % des investigations enregistrent une durée de présence de plus de trois ans et 4 % de plus de neuf ans, ce qui confirme les observations du dernier rapport.

DURÉE MÉDIANE DE PRÉSENCE – APAC – 2016 À 2020



Évolution de la durée médiane de présence en zone EMEA

54 ➤ 66

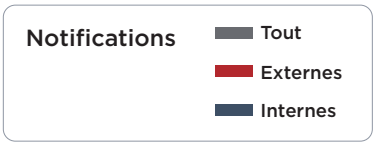
JOURS EN 2019 **JOURS EN 2020**

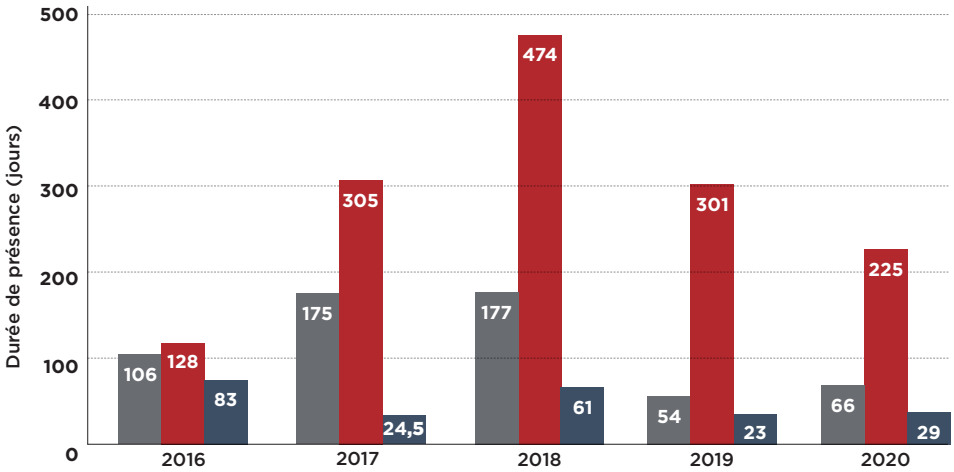
Durée médiane de présence en zone EMEA

Dans la région EMEA, la durée médiane de présence est passée de 54 jours en 2019 à 66 jours en 2020. Les experts Mandiant rapportent que 28 % des incidents de sécurité en EMEA affichent une durée de présence d'une semaine ou moins, tandis qu'à l'autre bout du spectre, 8 % des incidents sont détectés après trois ans. Les entreprises de la région EMEA continuent donc de répondre aux intrusions longue durée tout en étant aux prises avec des attaques à plus forte vélocité, à commencer par les ransomwares.

On note une tendance différente selon la source de détection, puisque la durée médiane de présence augmente pour les incidents découverts en interne mais diminue pour les notifications externes. En effet, les cas détectés par les victimes elles-mêmes passent d'une présence de 23 jours en 2019 à 29 jours en 2020, soit une hausse de 20 %. À l'inverse, les compromissions notifiées par un acteur externe enregistrent une baisse de 25 % de la durée médiane de présence – de 301 jours en 2019 à 225 jours en 2020.

DURÉE MÉDIANE DE PRÉSENCE – EMEA – 2016 À 2020





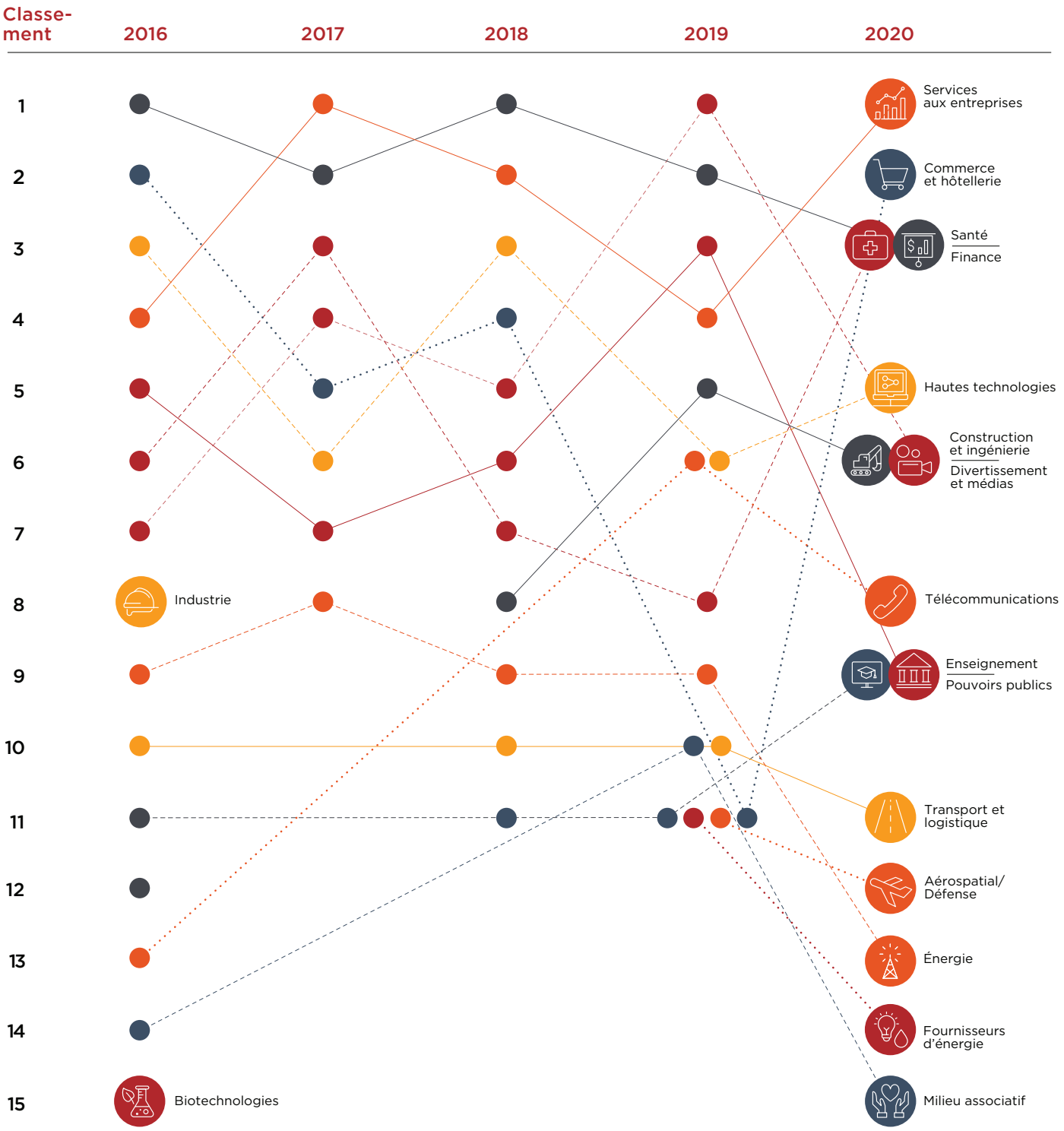
Secteurs d'activité ciblés

Les données recueillies par Mandiant en 2020 montrent que le ciblage sectoriel s'inscrit dans la tendance générale des années passées. Les domaines d'activité les plus visés sont, dans l'ordre : les services aux entreprises, le retail et l'hôtellerie, la finance, la santé et les hautes technologies. Notons que les services aux entreprises et les services financiers ont toujours figuré dans le top 5 des secteurs les plus attaqués au cours des dix dernières années. Globalement, ce classement évolue peu, même si l'ordre est relativement fluctuant.

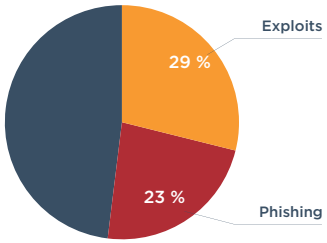
Changements notables

Les chiffres 2020 montrent une forte hausse des attaques à l'encontre des entreprises du retail et de l'hôtellerie : ce secteur arrive en deuxième position, alors qu'il n'était que onzième en 2019. La santé, huitième en 2019, figure désormais en troisième position. À l'inverse, les experts Mandiant notent une nette diminution des offensives à l'encontre d'industrie du divertissement et des médias, qui décroche à la sixième position alors qu'elle était la plus ciblée en 2019.

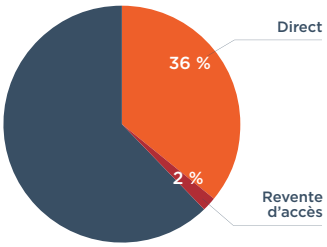
SECTEURS D'ACTIVITÉ CIBLÉS – 2016 À 2020



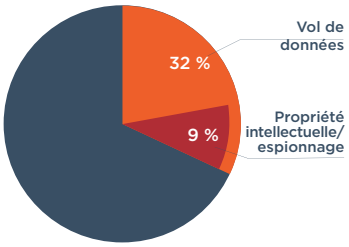
Vecteur d'infection initiale
(cas identifiés)



Objectif : gain financier



Objectif : vol de données



Détection de plusieurs groupes
(par environnement)

15 ➤ **29**
% en 2019 **% en 2020**

Attaques ciblées

Le volume et la variété des cas d'intrusion analysés par Mandiant en 2020 permettent d'obtenir une bonne perspective des vecteurs d'infection initiale, des objectifs des cybercriminels et des environnements infectés.

Vecteur d'infection initiale

Bien que le phishing reste une arme de compromission efficace, les attaquants ont exprimé un goût prononcé pour les exploits de vulnérabilités en 2020. Ainsi, dans les cas où le vecteur de compromission initiale a pu être identifié, les exploits représentent 29 % des intrusions, contre 23 % pour le phishing. Les investigations de Mandiant montrent par ailleurs que le vol d'identifiants ou les attaques par force brute constituent le vecteur initial dans 19 % des incidents. Les cas de compromission antérieure comptent quant à eux pour 12 % des intrusions dont l'infection initiale a pu être identifiée.

Objectifs des cybercriminels

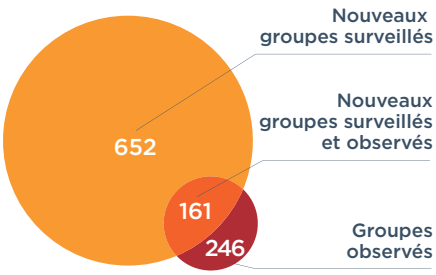
L'appât du gain reste la motivation première des attaquants. Quant aux méthodes utilisées, elles vont de l'extorsion au vol de carte de paiement, en passant par les demandes de rançon et les transferts illicites. Nos investigations montrent que 36 % des attaques visent un gain financier direct, tandis que 2 % sont motivées par la revente d'accès.

En 2020, le vol de données est resté l'un des objectifs principaux des cybercriminels avec 32 % du total des intrusions analysées. Dans 29 % de ces cas (soit 9 % des incidents totaux), la finalité de l'attaque était liée à de l'espionnage ou du vol de propriété intellectuelle.

Près de 3 % des intrusions ne sont a priori qu'un moyen de compromettre l'architecture en préparation à de futures attaques. Enfin, les menaces internes restent rares et comptent pour moins de 1 % des cas.

Environnement

Dans 29 % des cas, les experts Mandiant ont détecté la présence de plusieurs groupes cybercriminels dans l'environnement de la victime – soit près de deux fois plus qu'en 2019.

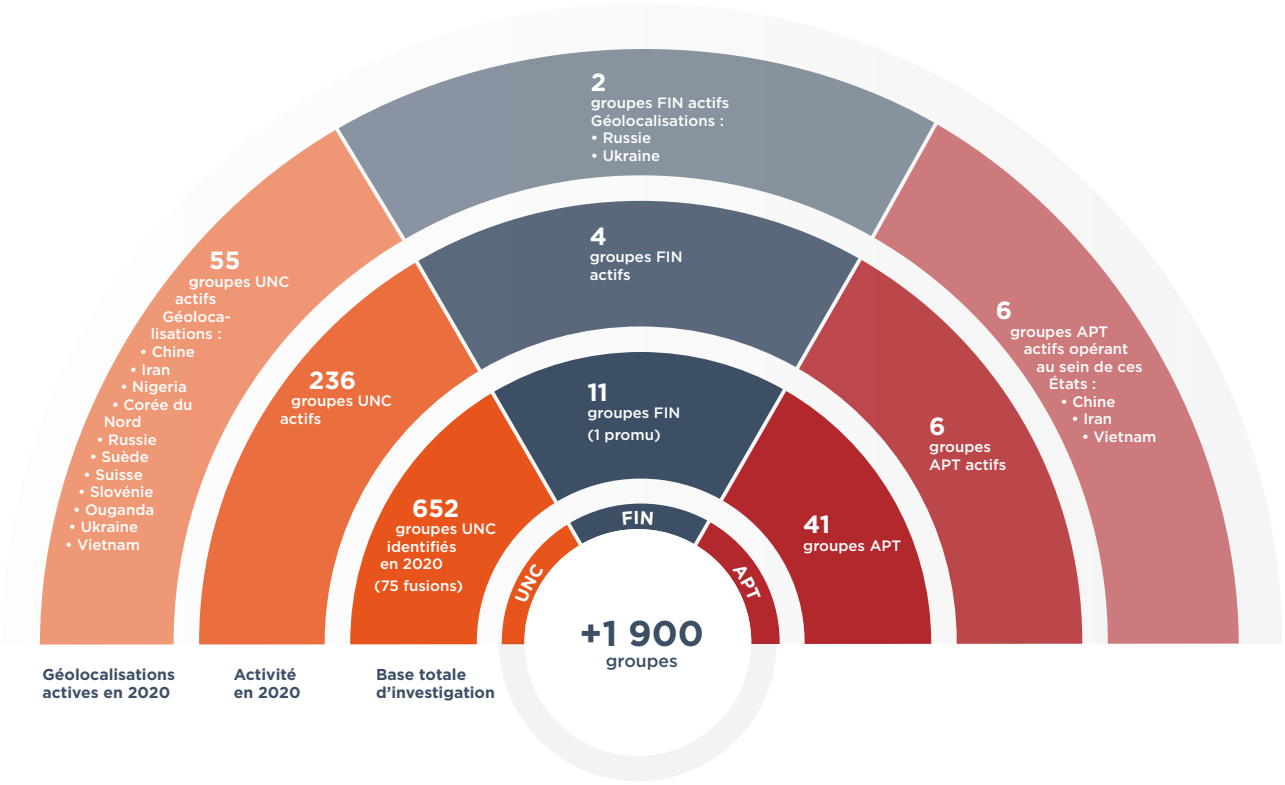


Groupes cybercriminels

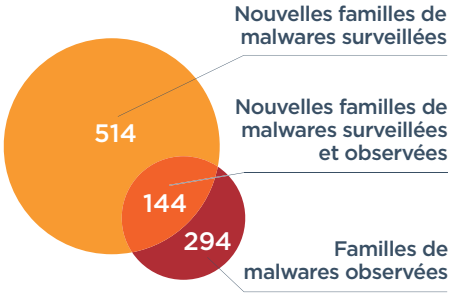
Depuis sa création, Mandiant a suivi les faits et gestes de quelque 2 400 groupes cybercriminels, dont plus de 650 nouveaux acteurs rien qu'en 2020. Au fil des ans, certains de ces groupes ont fusionné ou disparu de la circulation, ce qui nous donne à l'heure actuelle plus de 1 900 groupes distincts sous surveillance. Mandiant mobilise, affine et développe sa vaste base de connaissances au gré de ses missions d'investigation. En 2020, l'équipe a ainsi pu nommer un nouveau groupe et en fusionner 75 autres sur la base d'études approfondies des chevauchements et recoupements d'activités. Pour tout savoir sur le traitement des groupes non classés (UNC), veuillez consulter l'article « How Mandiant Tracks Uncategorized Threat Actors »[1] sur le blog de FireEye (en anglais).

Les intrusions analysées en 2020 impliquent au total 246 acteurs distincts. Les entreprises ont été victimes de 4 groupes à visée financière (FIN), 6 groupes de menace persistante avancée (APT) – certains à la solde de la Chine, de l'Iran et du Vietnam – ainsi que 236 groupes non classés (UNC). Sur les 246 groupes observés en 2020, 161 font leur entrée sur la liste des acteurs sous surveillance.

GROUPES CYBERCRIMINELS – 2020



1. FireEye (17 décembre 2020). « DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors ».



Une **famille de malware** désigne un type ou un ensemble de programmes malveillants dont la ressemblance du code permet de les classer dans un même groupe. Le terme de « famille » élargit donc le périmètre d'un malware unique, celui-ci pouvant être transformé au fil du temps tout en conservant son appartenance fondamentale à un même groupe.

Malwares

Mandiant continue d'enrichir sa base de connaissances des malwares à partir de données issues de ses propres investigations, de rapports publics, du partage d'informations et d'autres études. En 2020, l'équipe a effectué un suivi de plus de 500 nouvelles familles de malware – un chiffre sensiblement égal à celui de 2019.

Mandiant intervient chaque année dans le cadre de centaines d'intrusions, chacune présentant ses propres défis. En 2020, l'étude des environnements compromis fait ressortir 294 familles de malware distinctes. Parmi celles-ci, 144 correspondent à des menaces que Mandiant a commencé à surveiller au cours de la même année. Cela prouve à quel point les attaquants ne cessent de se réinventer et de s'adapter à l'environnement de leurs victimes.

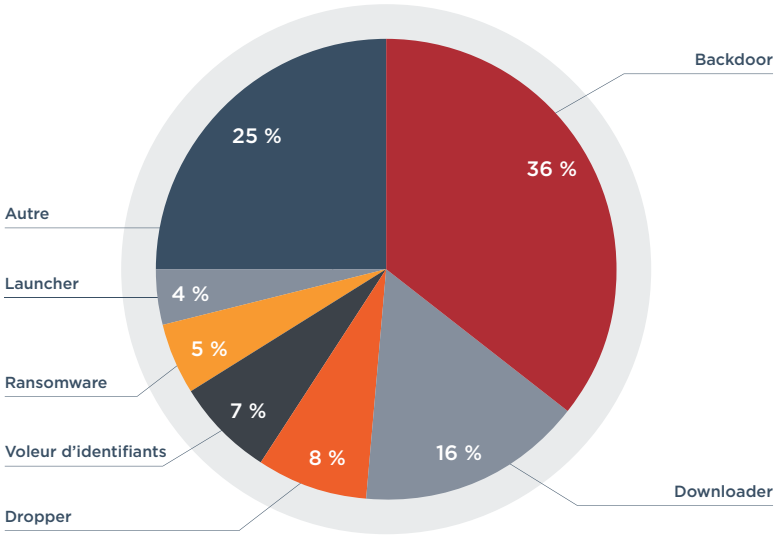
Une **catégorie** décrit l'objectif principal d'une famille de malware donnée, chacune étant affectée à la catégorie qui correspond le mieux à sa finalité, ce même si ses fonctionnalités la vouent à plus d'une catégorie.

Familles de malware par catégorie

Nos dernières investigations montrent une relative stabilité sur le plan de la répartition des malwares par catégorie. Les 514 nouvelles familles de malware surveillées en 2020 appartiennent à ces cinq catégories principales : backdoors (portes dérobées) (36 %), downloaders (téléchargeurs) (16 %), droppers (injecteurs) (8 %), launchers (lanceurs) (7 %) et ransomwares (5 %).

Catégorie de malware	Objectif principal
Backdoor	Un programme permettant l'exécution interactive de commandes sur le système infecté.
Voleur d'identifiants	Un utilitaire facilitant la consultation, la copie ou le vol d'informations d'identification.
Downloader	Un programme dont le seul but est de télécharger (voire lancer) un fichier à partir d'une adresse spécifique, sans autre fonctionnalité ni support de commandes interactives.
Dropper	Un programme utilisé pour extraire, installer et potentiellement lancer ou exécuter un ou plusieurs fichiers.
Launcher	Un programme dont le rôle premier est de lancer un ou plusieurs fichiers. À la différence d'un dropper ou d'un installateur, il ne contient ni ne configure les fichiers en question : il se contente de les exécuter ou de les charger.
Ransomware	Un programme malveillant utilisé notamment pour chiffrer les données d'une victime et lui en redonner l'accès contre le paiement d'une rançon.
Autres	Comprend toutes les autres catégories de malware comme les utilitaires, les enregistreurs de saisies clavier, les malwares de terminaux PDV (point de vente), les tunnelers et les dataminers.

NOUVELLES FAMILLES DE MALWARE SURVEILLÉES PAR CATÉGORIE – 2020

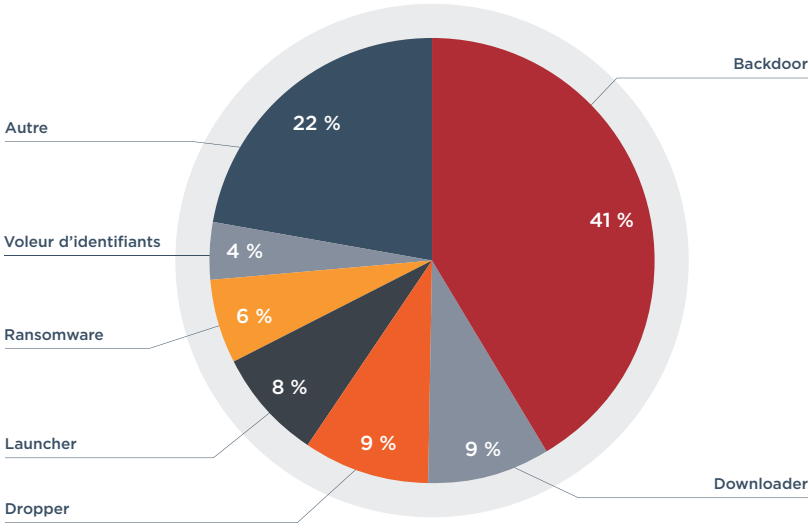


Une **famille de malware observée** correspond à une famille identifiée au cours des investigations menées par les experts Mandiant.

Familles de malware observées par catégorie

Les backdoors restent un grand classique et représentent la plus grande catégorie de malware observée lors des investigations. Les données récoltées par Mandiant montrent que les attaquants ont déployé au moins une backdoor dans plus de la moitié des cas d'intrusion. Les 294 familles de malware observées en 2020 appartiennent à cinq catégories principales : les backdoors (41 %), les downloaders (9 %), les droppers (9 %), les ransomwares (8 %) et les launchers (6 %).

FAMILLES DE MALWARE OBSERVÉES PAR CATÉGORIE – 2020



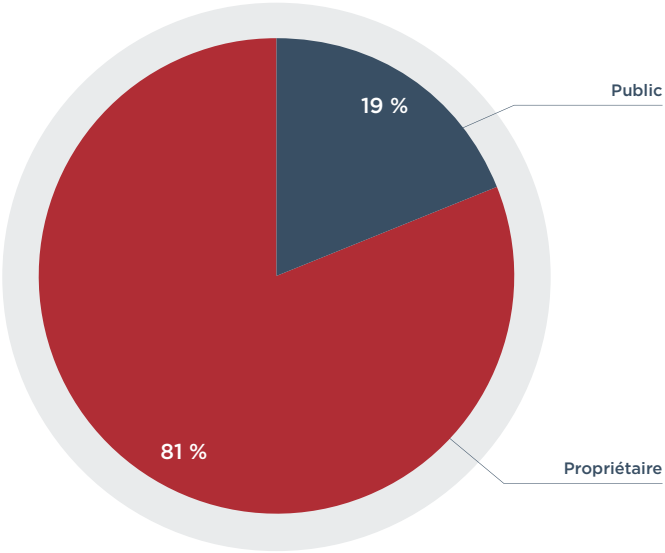
Nouvelles familles de malware surveillées par disponibilité

L'étude des experts Mandiant montre que 81 % des nouvelles familles de malware surveillées sont des programmes propriétaires et que 19 % sont des malwares publics. Bien que les cybercriminels utilisent des outils et du code librement accessibles, la majorité des familles de malware surveillées semblent être développées en privé ou ne sont distribuées que de façon limitée.

NOUVELLES FAMILLES DE MALWARE SURVEILLÉES PAR NIVEAU DE DISPONIBILITÉ – 2020

Un **outil ou une famille de code publiquement disponible** est accessible sans restriction. Cela comprend les outils téléchargeables gratuitement sur Internet, ainsi que ceux disponibles à la vente ou à l'achat, tant que la transaction est ouverte à tous.

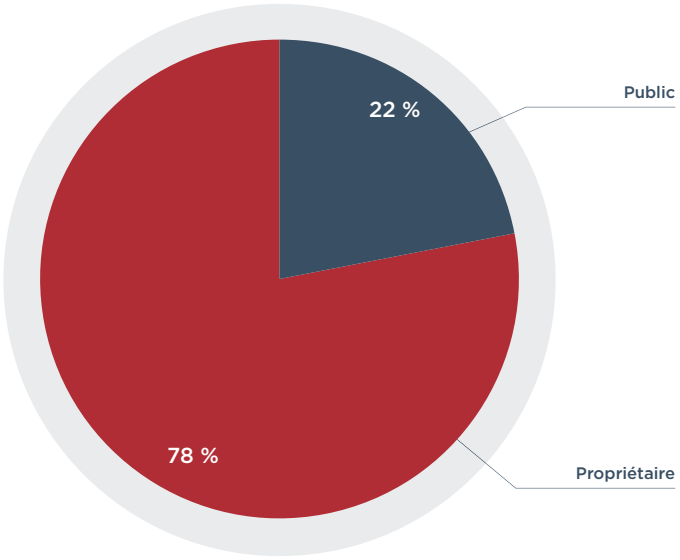
Un **outil ou une famille de code propriétaire** n'est, à notre connaissance, pas disponible publiquement (que ce soit gratuitement ou à l'achat). Cela peut comprendre les outils développés, détenus ou utilisés en privé, ou bien partagés ou vendus auprès d'une clientèle restreinte.



Familles de malware observées par niveau de disponibilité

Les experts Mandiant constatent que 78 % des familles de malware utilisées par les attaquants sont propriétaires, contre 22 % disponibles publiquement. Ces chiffres reflètent donc une tendance en phase avec les familles de malware nouvellement ajoutées à la liste de surveillance.

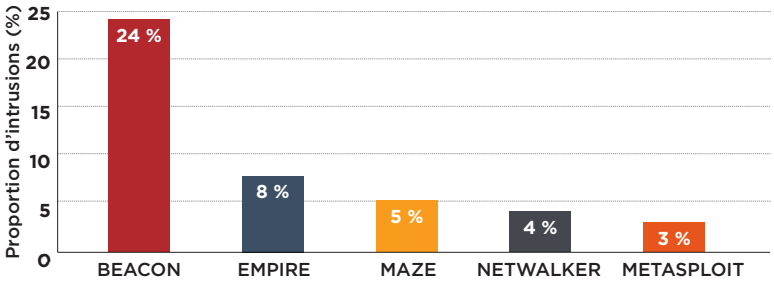
FAMILLES DE MALWARE OBSERVÉES PAR NIVEAU DE DISPONIBILITÉ – 2020



Familles de malware les plus observées

Les cinq familles de malware les plus observées en 2020 sont BEACON, EMPIRE, MAZE, NETWALKER et METASPLOIT. Notons que BEACON domine largement ce classement, avec près d'un quart des intrusions analysées par Mandiant en 2020. Les données recueillies montrent également qu'un même malware est rarement utilisé dans plus d'une attaque : **seules 3,4 % des familles de malware ont été observées dans 10 incidents de sécurité ou plus, tandis que 70 % n'ont été utilisées que dans un seul cas d'intrusion.**

FAMILLES DE MALWARE LES PLUS OBSERVÉES – 2020



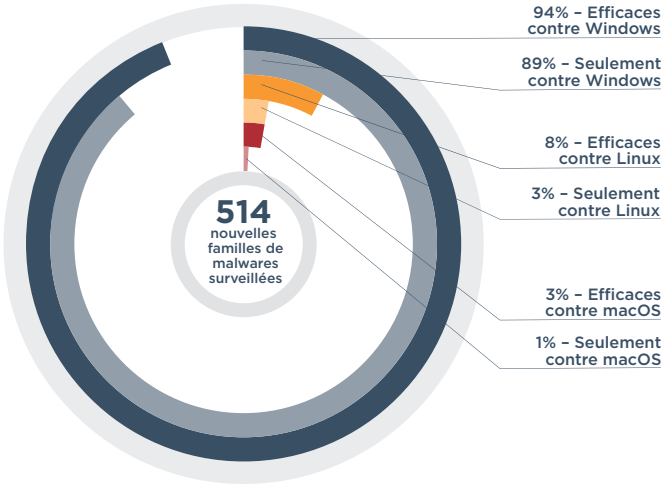
- **BEACON** est un malware de type backdoor disponible à l'achat. Celui-ci fait partie intégrante de la plateforme logicielle de tests d'intrusion Cobalt Strike. Parmi ses fonctionnalités : l'injection et l'exécution de code arbitraire, le chargement et le téléchargement de fichiers, ou encore l'exécution de commandes shell. Les investigations de Mandiant montrent que BEACON est utilisé par plusieurs groupes cybercriminels comme APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9 et FIN11, ainsi que près de 300 clusters non classés (UNC).
- **EMPIRE** est un framework de post-exploitation PowerShell publiquement disponible, qui permet à ses utilisateurs d'exécuter des agents PowerShell sans powershell.exe. Les attaquants s'en servent également pour exécuter différents types de modules post-exploitation et adapter leurs communications afin de contourner les systèmes de détection. Les experts Mandiant surveillent actuellement 90 groupes cybercriminels ayant déjà utilisé EMPIRE, dont APT19, APT33, FIN10, FIN11 et 86 clusters non classés (UNC).
- **MAZE** est une famille de ransomware visant à chiffrer les fichiers locaux ainsi que les données stockées sur les plateformes de partage réseau. MAZE peut être configuré dans le but d'infecter les disques distants et amovibles, ainsi que pour envoyer des informations système de base via HTTP. Mandiant a observé une dizaine de groupes FIN distincts utilisant ce ransomware.
- **NETWALKER** est une famille de ransomware capable de supprimer les snapshots de volumes compromis et de chiffrer les fichiers présents sur l'hôte infecté et les lecteurs réseau mappés. Il recourt pour cela à une combinaison d'algorithmes SALSA20 et Curve25519 dédiés. Mandiant surveille actuellement huit groupes cybercriminels ayant utilisé le ransomware NETWALKER dans le cadre d'activités crapuleuses de demande de rançon.
- **METASPLOIT** est une plateforme de test d'intrusion permettant à ses utilisateurs d'identifier, d'exploiter et de valider des vulnérabilités. Mandiant a constaté que APT40, APT41, FIN6, FIN7, FIN11 et 40 clusters non classés (UNC) utilisaient METASPLOIT, les objectifs allant du cyberespionnage au gain financier, en passant par les tests d'intrusion.

L'**efficacité contre les systèmes d'exploitation** permet de déterminer les OS les plus vulnérables à une famille de malware donnée.

Efficacité contre les systèmes d'exploitation

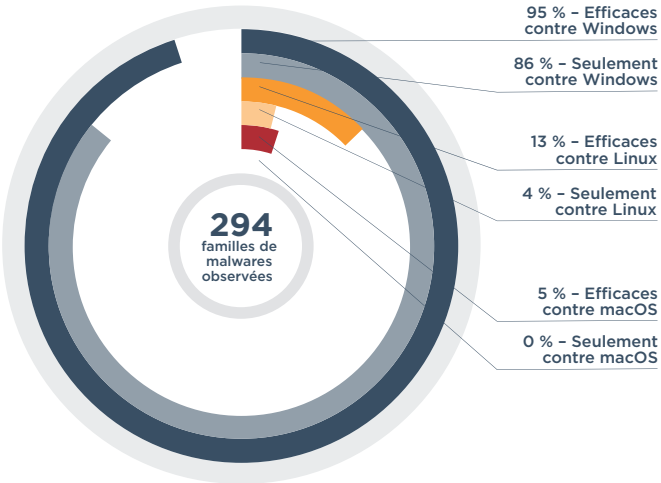
Dans la continuité des tendances passées, Windows est l'OS le plus vulnérable aux nouvelles familles de malware sous surveillance. En comparaison, seules 8 % et 3 % d'entre elles sont parvenues à infecter des systèmes Linux et macOS, respectivement.

EFFICACITÉ DES NOUVELLES FAMILLES DE MALWARE SURVEILLÉES PAR OS – 2020



La majorité des familles de malware observées au cours des investigations de Mandiant sont efficaces contre Windows. Les plateformes Linux et macOS ont quant à elles été infectées par seulement 13 % et 5 % de ces familles, respectivement.

EFFICACITÉ DES FAMILLES DE MALWARE OBSERVÉES PAR OS – 2020



MITRE ATT&CK® est une base de connaissances ouverte qui liste les tactiques et techniques d'attaque observées sur le terrain. Elle fournit un cadre de référence aux structures publiques et privées, ainsi qu'à l'ensemble de la communauté de la cybersécurité, pour le développement de modèles de menaces et de méthodologies spécifiques.

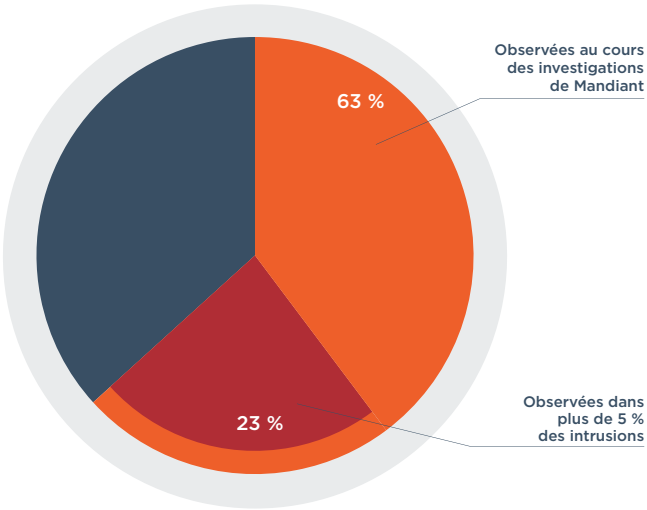
Techniques d'attaque

Mandiant apporte une contribution active à la communauté de la cybersécurité en alignant ses découvertes et conclusions sur MITRE ATT&CK. Ce framework a d'ailleurs fait l'objet de changements significatifs en 2020, avec l'introduction des sous-techniques et l'inclusion de PRE-ATT&CK dans la matrice Enterprise. L'évolution du framework et l'enrichissement continu du modèle data de Mandiant lui permettent désormais de recouper plus de 1 800 techniques avec le référentiel MITRE ATT&CK.

Dans le domaine de la cybersécurité, un bon processus décisionnel doit prendre en compte les probabilités d'utilisation des différentes techniques d'intrusion. Les investigations de Mandiant montrent qu'en 2020, les attaquants ont utilisé 63 % de techniques et 24 % de sous-techniques référencées dans le framework MITRE ATT&CK. Toutefois, seules 37 % des méthodes observées (23 % de l'ensemble des techniques) sont déployées dans plus de 5 % des intrusions.

Plus de la moitié des incidents analysés en 2020 impliquent l'obscurcissement de fichiers ou d'informations, tant par le biais du chiffrement que de l'encodage, le but étant de rendre la détection et l'analyse plus difficiles (T1027). Les attaquants ont fréquemment recours à un interpréteur de scripts ou de commandes à des fins d'infiltration plus approfondie (T1059). Dans 80 % des cas, il s'agit de PowerShell (T1059.001). Avec 31 % des intrusions, le détournement de services système (T1569) reste également une méthode très répandue. Notons que seuls les services Windows (T1569.002) ont été visés. Les attaquants s'en prennent également aux services distants (T1021) : 88 % des intrusions impliquent l'utilisation du protocole RDP (Remote Desktop Protocol) (T1021.001). Pour résumer, les cybercriminels tendent à exploiter les systèmes natifs de l'environnement des victimes, en particulier PowerShell, les services Windows et le protocole RDP.

TECHNIQUES MITRE ATT&CK LES PLUS UTILISÉES – 2020



TECHNOLOGIES FRÉQUEMMENT CIBLÉES – 2020

88 % – Protocole RDP (T1021.001) dans les intrusions exploitant les **services distants (T1021)**

Utilisation dans 25 % des intrusions

100 % – Services Windows (T1569.002) dans les intrusions exploitant les **services système (T1569)**

Utilisation dans 31 % des intrusions

80 % – PowerShell (T1059.001) dans les intrusions exploitant un **interpréteur de scripts ou de commandes (T1059)**

Utilisation dans 41 % des intrusions

TECHNIQUES MITRE ATT&CK DANS LE CYCLE D'ATTAQUE – 2020

Reconnaissance initiale

Reconnaissance

T1595 : scan actif	0,2 %

Développement de ressources

T1588 : obtention de fonctionnalités	21,3 %	T1588.003 : certificats de signature de code	21,0 %
T1583 : acquisition d'infrastructure	7,8 %	T1583.003 : serveur privé virtuel	7,8 %
T1584 : compromission d'infrastructure	5,1 %		
T1587 : développement de fonctionnalités	1,2 %	T1587.003 : certificats numériques	1,2 %

Compromission initiale

Accès initial

T1190 : exploitation d'application publique	21,0 %		
T1566 : phishing	14,2 %	T1566.001 : pièce jointe d'e-mail de spear-phishing	8,1 %
		T1566.002 : lien d'e-mail de spear-phishing	7,1 %
		T1566.003 : spear-phishing via un service	0,5 %
T1133 : services distants externes	11,5 %		
T1078 : comptes valides	6,8 %		
T1199 : relation de confiance	3,2 %		
T1189 : compromission par téléchargement furtif (drive-by)	1,5 %		
T1091 : réplication via support amovible	0,5 %		
T1195 : compromission de supply chain	0,5 %	T1195.002 : compromission de supply chain logicielle	0,5 %
T1200 : ajout de matériel	0,5 %		

Cycle d'attaque Mandiant

Framework MITRE ATT&CK

- **+ 20 %**
- **10 % à 19,99 %**
- **5 % à 9,99 %**
- **2 % à 4,99 %**
- **0 % à 1,99 %**

Implantation

Persistance

T1053 : tâche/job programmé	15,2 %	T1053.005 : tâche planifiée	6,6 %
T1505 : composant logiciel serveur	12,2 %	T1505.003 : Web Shell	12,2 %
T1133 : services distants externes	11,5 %		
T1098 : manipulation de compte	9,0 %		
T1543 : création ou modification de processus système	9,0 %	T1543.003 : service Windows	9,0 %
T1078 : comptes valides	6,8 %		
T1136 : création de compte	6,1 %	T1136.001 : compte local	0,2 %
		T1136.002 : compte de domaine	0,2 %
T1547 : exécution automatique au démarrage ou à la connexion	4,2 %	T1547.001 : clés de registre Run/dossier de démarrage	4,2 %
		T1547.009 : modification de raccourci	0,2 %
T1546 : exécution déclenchée par un évènement	3,2 %	T1546.008 : fonctionnalités d'accessibilité	1,2 %
		T1546.011 : exploitation de shim applicatif	1,2 %
		T1546.003 : souscription aux événements Windows Management Instrumentation	0,7 %
T1574 : détournement de flux d'exécution	3,2 %	T1574.001 : détournement d'ordre de recherche DLL	2,4 %
		T1574.002 : chargement latéral de DLL	2,4 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1197 : jobs BITS	0,7 %		
T1542 : démarrage pré-OS	0,2 %	T1542.003 : bootkit	0,2 %

Élévation des privilèges

Élévation des privilèges

T1055 : injection de code dans un processus	18,1 %	T1055.003 : détournement d'exécution de thread	1,0 %
		T1055.012 : Process Hollowing	0,5 %
T1053 : tâche/job programmé	15,2 %	T1053.005 : tâche planifiée	6,6 %
T1543 : création ou modification de processus système	9,0 %	T1543.003 : service Windows	9,0 %
T1078 : comptes valides	6,8 %		
T1134 : manipulation de jeton d'accès	5,9 %	T1134.001 : usurpation/ vol de jeton	0,2 %
T1547 : exécution automatique au démarrage ou à la connexion	4,2 %	T1547.001 : clés de registre Run/dossier de démarrage	4,2 %
		T1547.009 : modification de raccourci	0,2 %
T1546 : exécution déclenchée par un évènement	3,2 %	T1546.008 : fonctionnalités d'accessibilité	1,2 %
		T1546.011 : exploitation de shim applicatif	1,2 %
		T1546.003 : souscription aux événements Windows Management Instrumentation	0,7 %
T1574 : détournement de flux d'exécution	3,2 %	T1574.001 : détournement d'ordre de recherche DLL	2,4 %
		T1574.002 : chargement latéral de DLL	2,4 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1548 : abus des mécanismes de contrôle d'élévation des privilèges	0,7 %	T1548.002 : contournement du contrôle des comptes utilisateurs	0,5 %
		T1548.001 : setuid et setgid	0,2 %
T1068 : exploitation pour l'élévation des privilèges	0,2 %		
T1484 : modification de politique de domaine	0,2 %	T1484.001 : modification de politique de groupe	0,2 %

Reconnaissance interne

Découverte

T1082 : découverte d'informations système	24,2 %		
T1083 : découverte de fichiers et répertoires	21,8 %		
T1012 : interrogation du registre	13,0 %		
T1016 : découverte de configurations réseau système	13,0 %		
T1497 : contournement des environnements sandbox et de virtualisation	12,7 %	T1497.001 : contrôles système	1,5 %
T1057 : découverte de processus	12,0 %		
T1518 : découverte de logiciels	11,5 %		
T1033 : découverte d'utilisateurs/ propriétaires système	9,8 %		
T1049 : découverte de connexions réseau système	5,4 %		
T1007 : découverte de services système	4,9 %		
T1482 : découverte de relations de confiance entre domaines	4,9 %		
T1087 : découverte de comptes	4,2 %	T1087.004 : compte cloud	0,2 %
		T1087.002 : compte de domaine	0,2 %
T1010 : découverte de fenêtres applicatives	2,4 %		
T1069 : découverte de groupes d'autorisations	2,4 %	T1069.003 : groupes cloud	0,2 %
T1046 : scan de services réseau	1,7 %		
T1124 : découverte de l'heure système	1,0 %		
T1018 : découverte de systèmes distants	0,2 %		
T1135 : découverte de partages réseau	0,2 %		
T1217 : découverte de favoris de navigateur	0,2 %		
T1538 : tableau de bord de service cloud	0,2 %		
T1580 : découverte d'infrastructure cloud	0,2 %		

Déplacement latéral

Déplacement latéral

T1021 : services distants	28,4 %	T1021.001 : protocole RDP	24,9 %
		T1021.002 : partages administratifs Windows/SMB	3,9 %
		T1021.004 : SSH	3,2 %
		T1021.006 : Gestion à distance de Windows	1,0 %
		T1021.003 : modèle DCOM (Distributed Component Object Model)	0,2 %
T1091 : réplication via support amovible	0,5 %		
T1550 : utilisation d'un moyen d'authentification alternatif	0,5 %	T1550.002 : Pass the Hash	0,2 %
		T1550.003 : Pass the Ticket	0,2 %
T1563 : détournement de sessions de services distants	0,5 %	T1563.002 : détournement de RDP	0,2 %
T1534 : spear-phishing interne	0,2 %		

Maintien de la persistance

Persistance

T1053 : tâche/job programmé	15,2 %	T1053.005 : tâche planifiée	6,6 %
T1505 : composant logiciel serveur	12,2 %	T1505.003 : Web Shell	12,2 %
T1133 : services distants externes	11,5 %		
T1098 : manipulation de compte	9,0 %		
T1543 : création ou modification de processus système	9,0 %	T1543.003 : service Windows	9,0 %
T1078 : comptes valides	6,8 %		
T1136 : création de compte	6,1 %	T1136.001 : compte local	0,2 %
		T1136.002 : compte de domaine	0,2 %
T1547 : exécution automatique au démarrage ou à la connexion	4,2 %	T1547.001 : clés de registre Run/dossier de démarrage	4,2 %
		T1547.009 : modification de raccourci	0,2 %
T1546 : exécution déclenchée par un évènement	3,2 %	T1546.008 : fonctionnalités d'accessibilité	1,2 %
		T1546.011 : exploitation de shim applicatif	1,2 %
		T1546.003 : souscription aux événements Windows Management Instrumentation	0,7 %
T1574 : détournement de flux d'exécution	3,2 %	T1574.001 : détournement d'ordre de recherche DLL	2,4 %
		T1574.002 : chargement latéral de DLL	2,4 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1197 : jobs BITS	0,7 %		
T1542 : démarrage pré-OS	0,2 %	T1542.003 : bootkit	0,2 %

Exécution de la mission

Collecte

T1560 : archivage des données collectées	15,2 %	T1560.001 : archivage via un utilitaire	3,4 %
		T1560.002 : archivage via une bibliothèque	1,5 %
T1056 : capture de données de saisie	4,9 %	T1056.001 : enregistrement de saisies clavier	4,9 %
T1213 : données de référentiels d'informations	4,2 %	T1213.002 : SharePoint	0,2 %
T1113 : capture d'écran	3,2 %		
T1114 : collecte d'e-mails	3,2 %	T1114.003 : règle de transfert d'e-mails	1,5 %
T1115 : données du presse-papiers	2,7 %		
T1530 : données d'un objet de stockage cloud	0,5 %		
T1074 : enregistrement provisoire des données	0,2 %		
T1123 : capture audio	0,2 %		
T1125 : capture vidéo	0,2 %		

exfiltration

T1567 : exfiltration via un service web	0,2 %		

Impact

T1489 : interruption de service	13,4 %		
T1529 : arrêt/redémarrage système	3,2 %		
T1490 : blocage de la récupération système	2,7 %		
T1486 : chiffrement de données stratégiques	2,2 %		
T1496 : détournement de ressources	2,0 %		
T1565 : manipulation de données	1,7 %	T1565.001 : manipulation de données stockées	1,7 %
T1531 : interdiction d'accès aux comptes	1,0 %		
T1491 : défiguration	0,7 %	T1491.002 : défiguration externe	0,7 %

Tout au long du cycle d'attaque

Accès aux identifiants

T1003 : extraction d'identifiants via l'OS	8,8 %	T1003.001 : mémoire LSASS	4,4 %		
		T1003.003 : NTDS	3,4 %		
		T1003.002 : Gestionnaire de comptes de sécurité	0,7 %		
		T1003.006 : DCSync	0,2 %		
		T1003.008 : /etc/passwd et /etc/shadow	0,2 %		
T1110 : force brute	6,1 %	T1110.003 : password spraying	2,0 %		
		T1110.001 : supposition de mot de passe	1,2 %		
T1056 : capture de données de saisie	4,9 %	T1056.001 : enregistrement de saisies clavier	4,9 %		
T1555 : identifiants issus de magasins de mots de passe	1,7 %	T1555.003 : identifiants issus de navigateurs web	1,0 %		
T1552 : identifiants non sécurisés	1,0 %	T1552.004 : clés privées	0,5 %		
		T1552.001 : identifiants stockés dans des fichiers	0,2 %		
T1111 : interception des facteurs d'authentification	0,7 %				
T1558 : vol ou falsification de tickets Kerberos	0,7 %	T1558.003 : Kerberoasting	0,2 %		
T1187 : authentification forcée	0,2 %				
T1539 : vol de cookie de session web	0,2 %				

Commande et contrôle

T1105 : transfert d'outils externes	24,2 %				
T1573 : canal chiffré	15,9 %	T1573.002 : chiffrement asymétrique	15,9 %		
T1095 : protocole hors couche applicative	13,0 %				
T1071 : protocole sur la couche applicative	9,5 %	T1071.001 : protocoles web	7,6 %		
		T1071.004 : DNS	1,7 %		
		T1071.003 : protocoles de courrier électronique	0,5 %		
		T1071.002 : protocoles FTP	0,2 %		
T1572 : tunnelisation de protocole	5,4 %				
T1090 : proxy	4,9 %	T1090.003 : chaîne de proxys	3,2 %		
		T1090.004 : dissimulation du domaine de destination	0,2 %		
T1102 : service web	1,0 %				
T1219 : logiciel d'accès à distance	0,7 %				
T1001 : obscurcissement de données	0,2 %				
T1568 : résolution dynamique	0,2 %	T1568.002 : algorithmes de génération de noms de domaines	0,2 %		
T1571 : port non-standard	0,2 %				

Exécution

T1059 : interpréteur de scripts et de commandes	51,3 %	T1059.001 : PowerShell	40,8 %		
		T1059.003 : interface de commande Windows	15,4 %		
		T1059.005 : Visual Basic	5,9 %		
		T1059.007 : JavaScript/JScript	2,7 %		
		T1059.006 : Python	1,0 %		
T1569 : services système	30,6 %	T1569.002 : exécution de service	30,6 %		
T1053 : tâche/job programmé	15,2 %	T1053.005 : tâche planifiée	6,6 %		
T1204 : exécution par un utilisateur	11,5 %	T1204.001 : lien malveillant	7,3 %		
		T1204.002 : fichier malveillant	4,2 %		
T1203 : exploitation pour l'exécution côté client	4,9 %				
T1047 : Windows Management Instrumentation	2,7 %				
T1106 : API native	0,2 %				

Tout au long du cycle d'attaque

Contournement des défenses

T1027 : obscurcissement de fichiers ou données	52,6 %	T1027.001 : remplissage de fichiers binaires	0,2 %	T1140 : désobscurcissement/ décodage de fichiers ou d'informations	2,7 %		
		T1027.004 : compilation post-distribution	0,2 %	T1218 : exécution par l'intermédiaire de fichiers binaires signés	2,4 %	T1218.010 : Regsvr32	1,0 %
		T1027.005 : suppression d'indicateurs de compromission des outils	1,0 %			T1218.002 : panneau de configuration	0,5 %
		T1027.002 : compression/ chiffrement de logiciels	8,1 %			T1218.005 : mshta	0,5 %
		T1027.003 : stéganographie	0,5 %			T1218.003 : CMSTP	0,2 %
T1070 : suppression d'indicateurs de compromission sur l'hôte	24,4 %	T1070.004 : suppression de fichiers	18,1 %			T1218.011 : rundll32	0,2 %
		T1070.006 : falsification d'horodatage	5,9 %	T1564 : masquage d'artefacts	2,2 %	T1564.003 : masquage de fenêtre	2,0 %
		T1070.001 : effacement des journaux d'événements Windows	4,2 %			T1564.004 : attributs de fichiers NTFS	0,2 %
		T1070.005 : suppression de connexion de partage réseau	1,2 %	T1036 : camouflage	1,5 %	T1036.003 : modification du nom d'utilitaire système	0,7 %
T1553 : corruption des contrôles de sécurité	21,3 %	T1553.002 : signature de code	21,0 %			T1036.001 : signature de code non valide	0,5 %
T1055 : injection de code dans un processus	18,1 %	T1055.003 : détournement d'exécution de thread	1,0 %			T1036.005 : utilisation de noms ou d'emplacements légitimes	0,2 %
		T1055.012 : Process Hollowing	0,5 %	T1480 : exécution conditionnelle	1,5 %		
T1112 : modification de registre	15,6 %			T1197 : jobs BITS	0,7 %		
T1497 : contournement des environnements sandbox et de virtualisation	12,7 %	T1497.001 : contrôles système	1,5 %	T1548 : abus des mécanismes de contrôle d'élévation des privilèges	0,7 %	T1548.002 : contournement du contrôle des comptes utilisateurs	0,5 %
T1562 : perturbation des défenses	9,8 %	T1562.001 : désactivation ou modification d'outils de sécurité	5,9 %			T1548.001 : setuid et setgid	0,2 %
		T1562.004 : désactivation ou modification du pare-feu système	5,1 %	T1578 : modification d'infrastructure cloud	0,5 %	T1578.002 : création d'instance cloud	0,5 %
		T1562.007 : désactivation ou modification du pare-feu cloud	0,2 %			T1578.003 : suppression d'instance cloud	0,2 %
T1078 : comptes valides	6,8 %			T1550 : utilisation d'un moyen d'authentification alternatif	0,5 %	T1550.002 : Pass the Hash	0,2 %
T1134 : manipulation de jeton d'accès	5,9 %	T1134.001 : usurpation/ vol de jeton	0,2 %			T1550.003 : Pass the Ticket	0,2 %
T1202 : exécution indirecte de commandes	3,7 %			T1127 : exécution via des utilitaires de développement de confiance	0,2 %	T1127.001 : MSBuild	0,2 %
T1574 : détournement de flux d'exécution	3,2 %	T1574.001 : détournement d'ordre de recherche DLL	2,4 %	T1211 : exploitation pour le contournement des défenses	0,2 %		
		T1574.002 : chargement latéral de DLL	2,4 %	T1484 : modification de politique de domaine	0,2 %	T1484.001 : modification de politique de groupe	0,2 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %	T1542 : démarrage pré-OS	0,2 %	T1542.003 : bootkit	0,2 %

CONCLUSION

Les bonnes pratiques vont de pair avec un effort de sensibilisation

L'année 2020 aura au moins eu le mérite de nous rappeler à quel point la cybersécurité peut être affectée par les événements du monde qui nous entoure. Dans les précédents rapports M-Trends, nous soulignions déjà les répercussions des enjeux géopolitiques sur la nature et la physionomie des menaces. Ainsi, au cours des douze derniers mois, une crise sanitaire mondiale a rebattu les cartes et bouleversé l'activité des entreprises, redéfinissant par là même leur surface d'attaque et leur profil de risque. Résultat : les équipes de sécurité ont dû s'adapter dans l'urgence à cette nouvelle normalité tout en s'efforçant de se protéger contre des groupes cyber tentant de profiter de la situation.

Dans un autre registre, nous avons pu à nouveau constater toute la complexité et l'impact des attaques de la supply chain, évoquées pour la première fois dans le rapport M-Trends de 2013. Nous relations alors la manière dont les attaquants avaient utilisé des fournisseurs de services tiers pour compromettre leurs victimes. Bien que la plupart des tendances observées en 2020 ne soient pas nouvelles, celles-ci ont atteint des niveaux jamais vus en matière d'ampleur et de sophistication.

Nous avons par ailleurs observé l'évolution des attaques par ransomware, qui adoptent un système d'extorsion de plus en plus protéiforme, notamment par le recours à des sites de divulgation de données visant à tenir la réputation des entreprises victimes si elles refusent d'accéder aux demandes des cybercriminels. Enfin, les attaquants ont su tirer parti de l'infrastructure sous-tendant les nouvelles pratiques de télétravail en exploitant des vulnérabilités nouvelles ou connues. Ces tendances soulignent donc l'importance des aspects fondamentaux de la cybersécurité, comme la gestion des failles et des correctifs, le principe du moindre privilège et les stratégies de sécurisation renforcée.

Les équipes de sécurité doivent continuer à renforcer leurs défenses face à la montée en puissance des cybercriminels, tout en gérant et en s'adaptant aux changements à l'œuvre dans leur environnement et sur leur surface d'attaque. Si les modes opératoires restent en partie les mêmes, l'omniprésence et la progression des cybermenaces appellent à toute la vigilance, à l'évolution et à l'adaptabilité de l'écosystème de sécurité.

Pour en savoir plus sur FireEye, rendez-vous sur **www.fireeye.fr**
Pour en savoir plus sur Mandiant Solutions, rendez-vous sur **www.fireeye.fr/mandiant**

FireEye, France
Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle,
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26 | france@fireeye.com
FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
+1 408 321 6300 | info@fireeye.com

À propos de FireEye
Chez FireEye, notre mission est de placer nos technologies innovantes, notre Threat Intelligence et notre expertise de terrain au service d'une protection sans relâche des entreprises face aux cyberattaques. Découvrez comment sur www.fireeye.fr.

À propos de Mandiant Solutions
Mandiant Solutions base sa validation continue des systèmes de sécurité sur une CTI leader et des données issues directement de son expertise de première ligne. Les entreprises disposent ainsi des outils dont elles ont besoin pour augmenter l'efficacité de leur sécurité et réduire le risque métier.