



RAPPORT SUR LES DONNÉES DE SÉCURITÉ MICROSOFT

VOLUME 24
JANVIER – DÉCEMBRE 2018

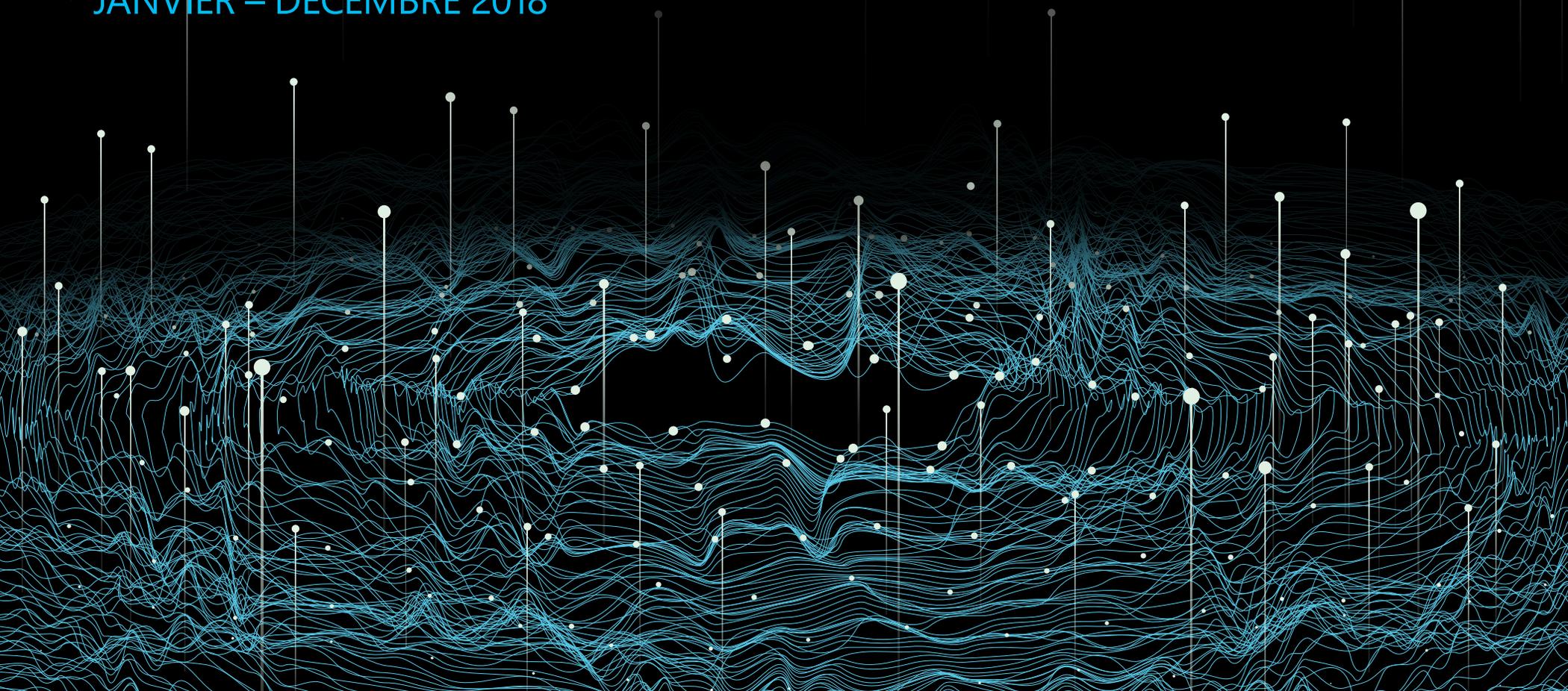


Table des matières

Le présent document est proposé à titre informatif uniquement. MICROSOFT N'ATTESTE NI NE GARANTIT, DE MANIÈRE EXPRESSE OU IMPLICITE, LES INFORMATIONS PRÉSENTÉES DANS CE DOCUMENT.

Le présent document est fourni en l'état. Les informations et les points de vue exprimés dans le présent document, y compris les URL et autres références à des sites web, sont susceptibles d'être modifiés sans préavis. Vous assumez les risques associés à son utilisation.

Copyright © 2019 Microsoft Corporation. Tous droits réservés.

Les noms des sociétés et des produits mentionnés dans le présent document peuvent être des marques commerciales de leurs détenteurs respectifs.

Auteurs et contributeurs

Abhishek Agrawal

Protection de l'information

David Fantham

Protection de l'information

Debraj Ghosh

Microsoft Security Marketing

Diana Kelley

Groupe de solutions de cybersécurité

Elia Florio

Windows Active Defense

Eric Avena

Équipe de recherche de Windows Defender

Eric Douglas

Équipe de recherche de Windows Defender

Francis Tan Seng

Équipe de recherche de Windows Defender

Jonathan Trull

Groupe de solutions de cybersécurité

Joram Borenstein

Groupe de solutions de cybersécurité

Karthik Selvaraj

Équipe de recherche de Windows Defender

Kasia Kaplinska

Microsoft Security Marketing

Kristina Laidler

Réponse aux incidents de sécurité

Matt Duncan

Ingénierie et analyse des données Windows Active Defense

Mark Simos

Groupe de solutions de cybersécurité

Paul Henry

Wadeware LLC

Pragya Pandey

Microsoft Security Marketing

Ram Pliskin

Azure Security

Ryan McGee

Microsoft Security Marketing

Seema Kathuria

Groupe de solutions de cybersécurité

Steve Wacker

Wadeware LLC

Tanmay Ganacharya

Équipe de recherche de Windows Defender

Volv Grebennikov

Bing

Yaniv Zohar

Azure Security

Avant-propos

Bonjour et bienvenue dans la 24e édition du rapport sur les données de sécurité Microsoft (SIR). En tant que praticienne et architecte de la sécurité, j'ai lu des rapports comme celui-ci dans l'espoir de comprendre un peu mieux le paysage et d'en tirer des conseils pratiques sur la façon d'utiliser ces connaissances pour défendre et protéger plus efficacement les organisations.

L'équipe SIR apporte à ce rapport l'esprit d'éducation en vue d'améliorer la cyber-résilience et a passé au crible une année de données pour distiller les leçons les plus importantes.

Ce que vous lisez sont des informations sélectionnées parmi une année d'analyse de données de sécurité et de leçons pratiques apprises. Les données analysées incluent les 6,5 mille milliards de signaux de menace qui traversent le cloud de Microsoft chaque jour, ainsi que les expériences de recherche et concrètes issues de nos milliers de chercheurs et d'intervenants en matière de sécurité dans le monde entier. En 2018, les attaquants ont utilisé diverses entourloupes, à la fois nouvelles (minage de cryptomonnaie) et anciennes (hameçonnage), dans leur quête continue pour voler des données et des ressources à des clients et des organisations. Les attaques hybrides, comme la campagne Ursnif, ont mélangé des approches sociales et techniques. À mesure que l'intelligence des défenseurs s'est développée contre les ransomwares, une forme d'attaque forte et perturbatrice, les criminels sont passés aux mineurs de cryptomonnaie, plus «furtifs», mais qui demeurent rentables.

Ce « passage » peut sembler frustrant, comme si les attaquants avaient toujours une longueur d'avance. Mais, vue sous une optique différente, l'histoire est ici positive. Des défenseurs et des professionnels de la cybersécurité comme vous ont mis en œuvre des techniques défensives qui ont obligé les attaquants à changer leurs charges utiles préférées et à renoncer aux ransomwares.

Un autre domaine où les cyber-criminels ont accru leur activité est la chaîne d'approvisionnement. L'une des plus notables, l'épidémie de mineur de cryptomonnaie Dofail, qui a frappé le 6 mars 2018, a été lancée par une application d'égal à égal empoisonnée. Les préoccupations en termes de chaîne d'approvisionnement sont allées au-delà des applications, jusque dans le cloud et comprenaient des extensions de navigateur malveillantes, des référentiels Linux compromis et plusieurs instances de modules avec une porte dérobée. Pour gérer cette menace, les organisations adoptent un modèle de chaîne d'approvisionnement transparent et fiable.

Si les données sont très utiles, il est parfois important de découvrir ce qu'il s'est réellement passé dans une organisation. C'est pourquoi nous avons inclus les leçons apprises dans le domaine par notre équipe de détection et d'intervention (DART). Il s'agit notamment de la façon dont une grande entreprise de fabrication a été en mesure d'installer des contrôles pour bloquer une campagne de hameçonnage en plusieurs phases dont elle a été la proie pendant des mois, et d'organisations de services financiers qui ont finalement été en mesure d'éradiquer les acteurs de la menace de leurs systèmes en utilisant une surveillance des points de terminaison et des outils d'investigation avancés.

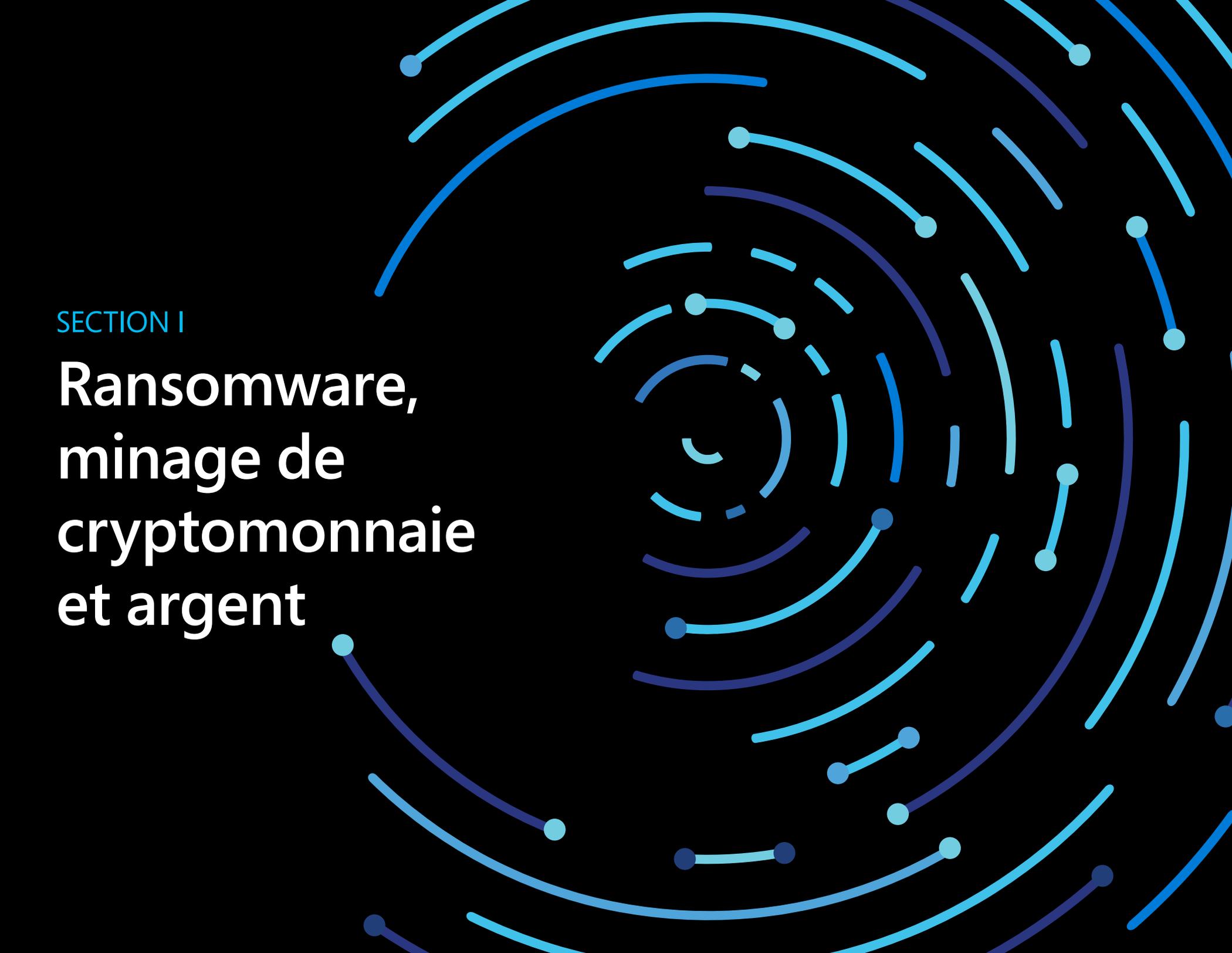
Enfin, les clics de hameçonnage ont continué à augmenter, mais les modèles de Machine Learning parviennent de mieux en mieux à identifier le hameçonnage avant qu'il ne frappe les boîtes de réception des utilisateurs et, dans le cas contraire, à prévenir les dommages après le clic. D'autres bonnes nouvelles ? Un nombre croissant d'entreprises installent des solutions multifacteur pour limiter le succès des e-mails de hameçonnage visant à voler des informations d'identification.

Les attaquants cherchent des opportunités. Ainsi, plus nous en savons sur leurs techniques et leur savoir-faire, mieux nous serons préparés pour construire des défenses et réagir rapidement. De petites étapes importantes peuvent faire une énorme différence dans l'intégrité globale de la cybersécurité d'une organisation. C'est pourquoi, en plus des informations approfondies sur le paysage changeant de programmes malveillants et d'attaques, vous trouverez dans ce rapport des recommandations d'étapes et d'autres conseils de bonnes pratiques. Parce que quand j'étais intervenante, c'est exactement ce dont j'avais besoin dans ma lutte contre les méchants. Nous espérons que c'est ce dont vous avez besoin vous aussi.

Diana Kelley

Directrice technique Microsoft Cybersecurity

P.S. Nous cherchons toujours à améliorer le SIR. Si vous avez des commentaires, merci de nous contacter pour évaluer notre prestation.



SECTION I

Ransomware, minage de cryptomonnaie et argent

Les grandes histoires de sécurité de 2017 ont principalement impliqué les ransomwares. Des apparitions importantes dans le monde entier de WannaCrypt et de Petya ont imposé le ransomware (un type de programme malveillant qui verrouille ou chiffre les ordinateurs, puis exige de l'argent pour rétablir l'accès) dans la conscience générale, et beaucoup avaient avancé que ce problème ne ferait qu'augmenter à l'avenir. Au lieu de cela, **les attaques de ransomware ont nettement diminué en 2018.**

La baisse des attaques de ransomware a été due en partie à l'amélioration de la détection et de l'éducation car il est ainsi devenu plus difficile pour les attaquants d'en tirer profit. En conséquence, les attaquants ont commencé à se détourner du ransomware pour favoriser des approches telles que le minage de cryptomonnaie, qui utilisent les ressources informatiques des victimes pour faire de l'argent numérique pour les attaquants. Le changement démontre la nature fondamentalement opportuniste de la plupart des cybercriminels axés sur le profit : ils ont tendance à rechercher l'argent le plus facilement disponible, et quand l'économie de la cybercriminalité change, ils sont prompts à s'adapter.

LES ATTAQUES DE RANSOMWARE SUR LE DÉCLIN

Il y a plus d'une décennie, les pirates et les farceurs qui dominaient les premiers programmes malveillants souterrains ont été supplantés par le crime organisé et d'autres intérêts axés sur le profit. Alors que les premières flambées de programmes malveillants étaient souvent voyantes et évidentes, les programmes malveillants axés sur le profit étaient beaucoup plus susceptibles de fonctionner en silence et d'éviter d'attirer l'attention, afin de continuer à remplir leur fonction : envoyer des spams, voler des informations sensibles, mener des attaques par déni de service et d'autres activités malveillantes, aussi longtemps que possible.

Les ransomwares ont résisté à cette tendance. Au lieu d'essayer de rester inaperçus, le ransomware refuse ouvertement aux victimes l'accès à leurs ordinateurs

et à des fichiers importants jusqu'à ce qu'elles paient la rançon (et il n'est pas rare non plus que les attaquants n'arrêtent pas leur contrôle des ordinateurs même après que la rançon soit payée). Comme les ransomwares ont pris de l'ampleur en 2017, il semblait que ce style d'attaque ouverte pourrait représenter une nouvelle phase dans les techniques des attaquants. Mais des données plus récentes suggèrent que le ransomware pourrait être sur le déclin, avec des attaquants revenant de plus en plus au mode de fonctionnement plus furtif qu'ils ont employé dans le passé, cherchant à passer inaperçus afin de mener plus efficacement des attaques telles que le minage de cryptomonnaie. Bien qu'il y ait eu une baisse du taux d'attaques de ransomware, cela ne signifie pas nécessairement que la sévérité de ces dernières ait diminué.

Taux d'attaques de ransomware

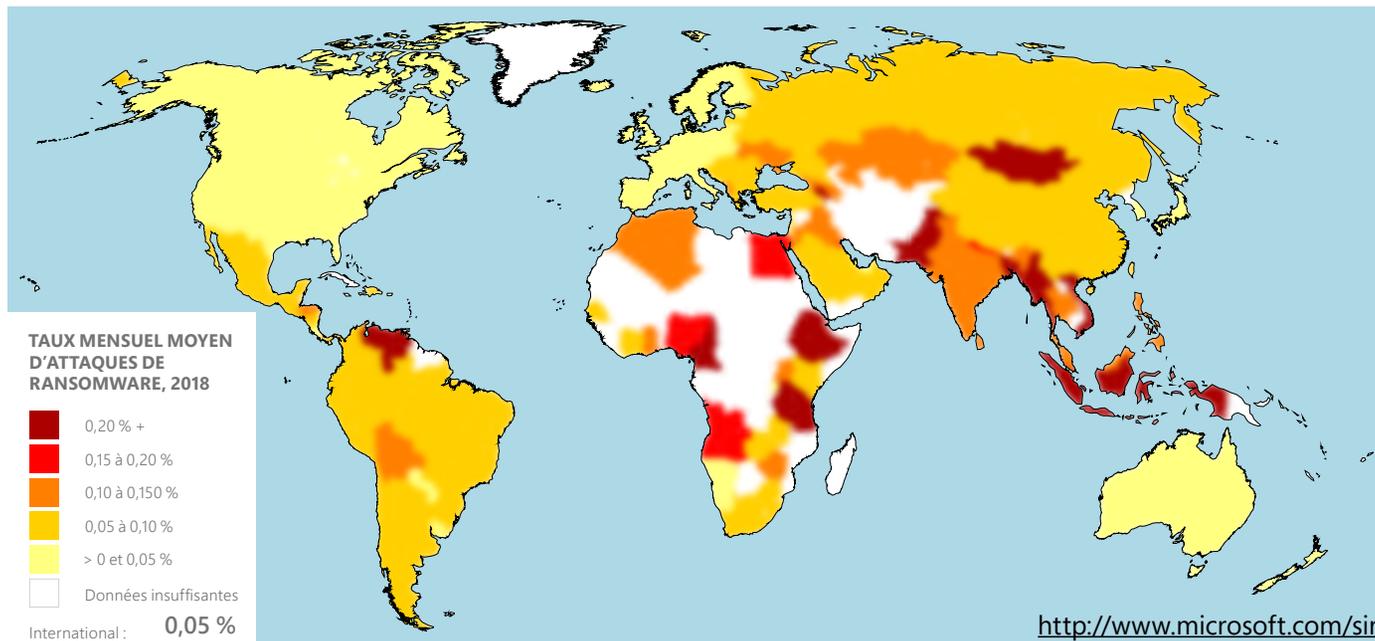


Les taux d'attaques de ransomware **ont diminué d'environ 60 %** entre mars 2017 et décembre 2018, avec des augmentations intermittentes au cours de cette période.

▲ **FIGURE 1.**

Attaques de ransomware entre mars 2017 et décembre 2018

Les causes de ce déclin global sont sans doute multiples, bien que les chercheurs de sécurité de Microsoft soupçonnent qu'un facteur principal repose sur le fait que tant les utilisateurs que les organisations deviennent plus conscients des menaces de ransomware et les traitent plus intelligemment, notamment en se montrant plus prudents et en sauvegardant les fichiers importants afin qu'ils puissent être restaurés s'ils sont chiffrés par un ransomware. En outre, comme décrit précédemment, les cybercriminels sont opportunistes.



◀ **FIGURE 2.**

Moyenne mensuelle des taux d'attaques de ransomware dans le monde entier par pays/région en 2018

PAYS LE PLUS IMPACTÉ PAR LES RANSOMWARES : ÉTHIOPIE



Taux mensuel moyen d'attaques :

0,77 %

Les cinq endroits avec le taux mensuel moyen d'attaques de ransomware le plus élevé en 2018 ont été l'Éthiopie (0,77 % de taux mensuel moyen d'attaques de ransomware), la Mongolie (0,46), le Cameroun (0,41), le Myanmar (0,33) et le Venezuela (0,31), chacun ayant un taux mensuel moyen d'attaques de ransomware de 0,31 % ou plus au cours de la période.¹ Il y a quelques années, les attaques de ransomware se regroupaient généralement dans les pays et régions riches d'Europe et d'Amérique du Nord, mais avec le déclin du ransomware auprès des attaquants, le modèle d'attaque a de plus en plus ressemblé à celui des logiciels malveillants dans leur ensemble.

Les emplacements avec les plus bas taux d'attaques de ransomware en 2018 étaient l'Irlande (0,01), le Japon (0,01), les États-Unis (0,02), le Royaume-Uni (0,02) et la Suède (0,02 %), chacun ayant un taux mensuel moyen d'attaques de ransomware de 0,02 % ou moins pendant la même période. Les endroits où les taux d'attaques sont faibles disposent généralement d'infrastructures de cybersécurité matures et de programmes bien établis pour protéger les infrastructures critiques et communiquer avec leurs citoyens en matière de sécurité de base.

NOTE DE BAS DE PAGE

¹ Le taux d'attaque correspond au pourcentage d'ordinateurs exécutant des produits Microsoft de sécurité en temps réel qui signalent une attaque de programme malveillant. Une telle menace d'attaque ne signifie pas que l'ordinateur a été infecté. Seuls les ordinateurs dont les utilisateurs ont accepté de fournir des données à Microsoft sont pris en compte dans le calcul des taux d'attaques.

LE MINAGE DE CRYPTOMONNAIE A LE VENT EN POUPE

La cryptomonnaie est l'argent virtuel qui peut être utilisé pour acheter et vendre anonymement des biens et des services, à la fois en ligne et dans le monde physique. Beaucoup de différents types de cryptomonnaies existent, mais ils sont tous basés sur la technologie blockchain impliquant que chaque transaction soit enregistrée dans un registre distribué tenu à jour par des milliers ou des millions d'ordinateurs dans le monde entier. De nouvelles pièces sont créées, ou « minées », par des ordinateurs réalisant des calculs complexes qui servent également à vérifier les transactions blockchain.

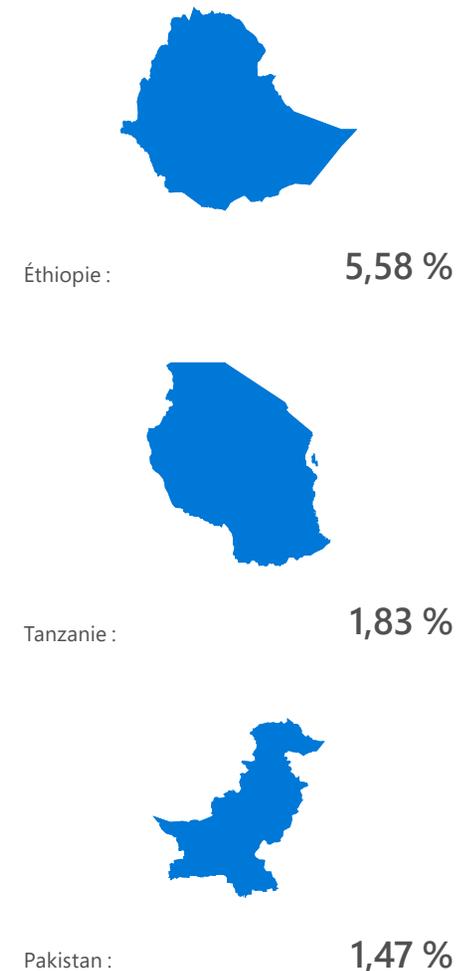
Le minage de cryptomonnaie peut être très lucratif.

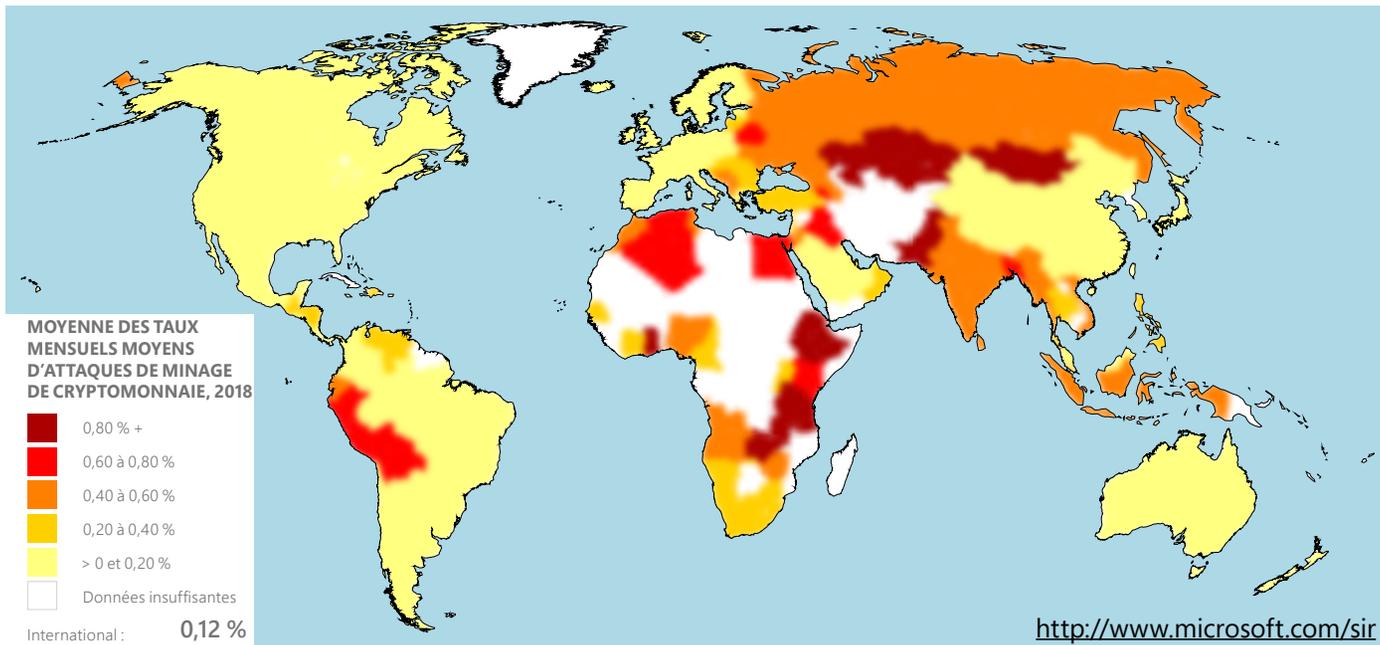
En 2018, une seule pièce de Bitcoin, la cryptomonnaie la plus ancienne et la plus populaire, valait plusieurs milliers de dollars américains, mais l'exécution des calculs nécessaires peut être très exigeante en termes de ressources et le devient plus encore chaque fois qu'une nouvelle pièce est minée. Pour les monnaies populaires telles que Bitcoin, le minage rentable de cryptomonnaie est presque impossible sans accès à des ressources informatiques immenses qui sont largement hors de portée pour la plupart des individus et des petits groupes. C'est pourquoi les attaquants cherchant des profits illicites se sont de plus en plus tournés vers les programmes malveillants qui leur permettent d'utiliser les ordinateurs des victimes pour les aider à miner des pièces de cryptomonnaie. Cette approche leur permet de tirer profit de la puissance de traitement de centaines de milliers d'ordinateurs au lieu d'un ou de deux. Même lorsqu'une infection mineure est découverte, la nature anonyme de la cryptomonnaie complique les efforts pour traquer les parties responsables.

En 2018, le taux mensuel moyen mondial d'attaques liées à un minage de pièces de cryptomonnaie était de 0,12 pour cent, comparativement à seulement 0,05 pour cent pour le ransomware. De nombreux facteurs contribuent à la popularité accrue du minage comme une charge utile pour les programmes malveillants. Contrairement au ransomware, le minage de cryptomonnaie ne nécessite pas d'intervention de l'utilisateur : il fonctionne en arrière-plan pendant que l'utilisateur effectue d'autres tâches ou est loin de l'ordinateur, et il peut passer complètement inaperçu s'il ne dégrade pas notablement les performances de l'ordinateur. En conséquence, les utilisateurs sont moins susceptibles de prendre toute mesure pour supprimer la menace, et le minage peut se poursuivre au profit de l'attaquant pendant une longue période de temps.

La disponibilité de produits « du commerce » pour le minage secret de nombreuses cryptomonnaies est un autre moteur de la tendance. Il y a peu d'obstacles en raison de la grande disponibilité des logiciels de minage de cryptomonnaie que les cybercriminels reconditionnent en tant que programme malveillant pour les installer sur les ordinateurs d'utilisateurs qui ne se doutent de rien. Les mineurs armés sont ensuite distribués aux victimes à l'aide de plusieurs des mêmes techniques que celles utilisées par les attaquants pour fournir d'autres menaces, telles que le piratage psychologique, les codes malveillants exploitant une faille de sécurité et les téléchargements furtifs. Une fois le logiciel de minage installé, il s'exécute en arrière-plan sur les ordinateurs des victimes pour effectuer les calculs de blockchain, et c'est l'attaquant qui en récolte les fruits.

TAUX MENSUEL MOYEN D'ATTAQUES DES PAYS LES PLUS TOUCHÉS PAR LE MINAGE DE CRYPTOMONNAIE





◀ **FIGURE 3.**

Moyenne des taux mensuels moyens d'attaques de mineurs de cryptomonnaie dans le monde entier par pays/région en 2018

TAUX MENSUEL MOYEN D'ATTAQUES DES PAYS LES MOINS TOUCHÉS PAR LE MINAGE DE CRYPTOMONNAIE



Les cinq emplacements avec les taux d'attaques les plus élevés de minage de cryptomonnaie en 2018 étaient l'Éthiopie (5,58), la Tanzanie (1,83), le Pakistan (1,47), le Kazakhstan (1,24) et la Zambie (1,13), avec pour chacun un taux mensuel moyen d'attaques de minage de cryptomonnaie d'environ 1,13 % ou plus au cours de la période. Les emplacements avec les taux d'attaques les plus bas de minage de cryptomonnaie en 2018 étaient l'Irlande, le Japon, les États-Unis et la Chine, chacun ayant un taux mensuel moyen d'attaques de minage de cryptomonnaie d'environ 0,02 % au cours de la période.

MINEURS DE CRYPTOMONNAIE BASÉS SUR NAVIGATEUR : UN NOUVEAU TYPE DE MENACE

Les statistiques présentées dans cette section impliquent des mineurs de cryptomonnaie malveillants qui sont conçus pour être installés sur les ordinateurs des victimes comme des programmes malveillants. Mais certaines des menaces les plus significatives de minage de cryptomonnaie sont basées entièrement dans les navigateurs web et ne nécessitent jamais aucune installation. Un certain nombre de services annoncent un minage de cryptomonnaie basé sur navigateur comme un moyen pour les propriétaires de sites web de monétiser le trafic vers leurs sites sans s'appuyer sur la publicité. Les propriétaires de site doivent ajouter du code JavaScript à leurs pages qui mine la cryptomonnaie en arrière-plan pendant qu'un utilisateur visite le site, avec la répartition des revenus entre le propriétaire du site et le service.

Taux d'attaques Brocoiner



Malheureusement, les attaquants ont été prompts à profiter de ces services pour miner la cryptomonnaie sans obtenir le consentement des utilisateurs, souvent en compromettant des sites web légitimes et en insérant de façon malveillante le code de minage dans leur code source. Ces mineurs basés sur le navigateur ne nécessitent aucune compromission de l'ordinateur de l'utilisateur et s'exécuteront sur n'importe quelle plateforme avec un navigateur web compatible avec JavaScript. Comme les chevaux de Troie de minage de cryptomonnaie, les mineurs basés sur navigateur peuvent dégrader considérablement les performances de l'ordinateur et gaspiller l'électricité pendant qu'un utilisateur visite une page web concernée.

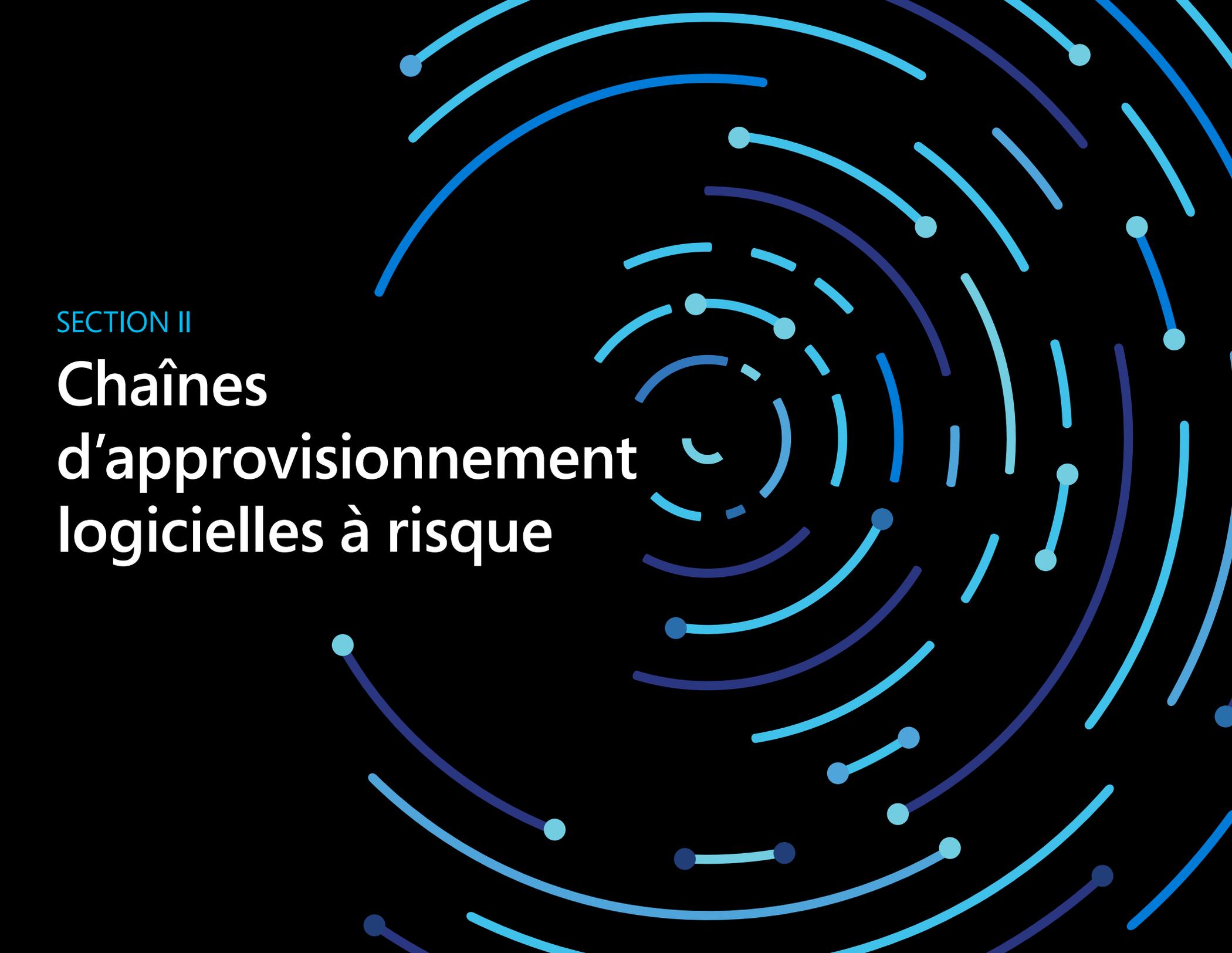
◀ FIGURE 4.

Taux d'attaques pour Brocoiner, le mineur de cryptomonnaie basé sur navigateur le plus répandu

L'IMPACT D'UN MINAGE DE CRYPTOMONNAIE NON SOLlicitÉ

La menace la plus évidente rencontrée par les victimes du minage de cryptomonnaie malveillant est la consommation de ressources informatiques, qui peut gaspiller de l'électricité et dégrader significativement les performances de l'ordinateur. Les utilisateurs et les organisations sont également confrontés à d'autres risques liés au minage de cryptomonnaie, notamment :

- ! **S'introduire pour faire plus de dégâts à l'avenir.**
Comme d'autres formes de programmes malveillants, le minage de cryptomonnaie peut être un point d'entrée pour les attaquants. Pendant que l'ordinateur est occupé au minage de cryptomonnaie en arrière-plan, les cybercriminels peuvent obtenir des informations sur l'environnement et peut-être découvrir des lacunes dans la sécurité à exploiter à d'autres fins.
- ! **Les appareils connectés à Internet peuvent être compromis et transformés en robots pour le minage de cryptomonnaie.**
Beaucoup de ces appareils manquent de sécurité intégrée telle que la détection de menace de programme malveillant, ce qui peut en faire des cibles séduisantes pour des attaquants.
- ! **Endommager des machines.**
Le logiciel de minage de cryptomonnaie fonctionnant en continu pendant des mois ou plus peut nuire aux performances, et la chaleur générée par la consommation d'énergie et l'utilisation de l'UC excessives peut endommager les ordinateurs.

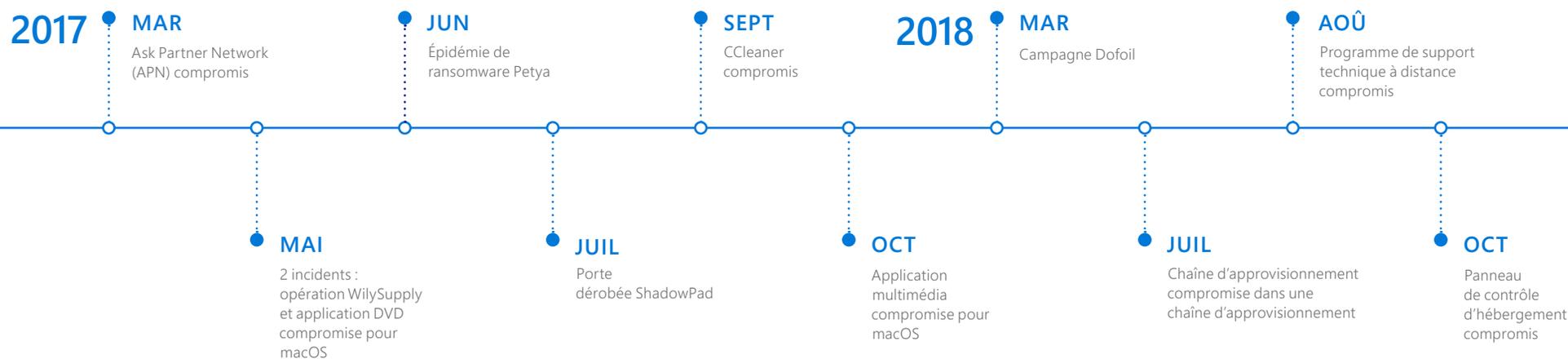


SECTION II

Chaînes d'approvisionnement logicielles à risque

Depuis des années, Microsoft suit les auteurs de menaces qui utilisent [a mise en péril de la chaîne d'approvisionnement](#) comme point d'entrée pour les attaques. Dans une attaque de chaîne d'approvisionnement, l'attaquant se concentre sur la mise en péril du processus de développement ou de mise à jour d'un éditeur de logiciels légitime.

En cas de réussite, l'attaquant peut intégrer un composant compromis dans un package de mise à jour ou d'application légitime qui est ensuite distribué aux utilisateurs du logiciel. Le code malveillant s'exécute alors avec la même confiance et les mêmes autorisations que le logiciel. Le [nombre accru d'attaques de chaînes d'approvisionnement de logiciels au cours des dernières années](#) est devenu un sujet important dans de nombreuses conversations de cybersécurité et est une source principale de préoccupation dans bien des départements informatiques.



ATTAQUES DE CHAÎNES D'APPROVISIONNEMENT LOGICIELLES MAJEURES EN 2017 ET 2018

En 2017, les attaques de chaînes d'approvisionnement ont été responsables d'un certain nombre d'incidents de haut niveau, notamment [l'épidémie de ransomware Petya](#) en juin, qui a été attribuée à des infections initiales d'un processus de mise à jour compromis pour une application de comptabilité fiscale populaire en Ukraine. En mai, [Operation WilySupply](#) a compromis le programme de mise à jour logicielle d'un éditeur de texte pour installer une porte dérobée sur des organisations cibles dans les secteurs financier et informatique. En juillet, une porte dérobée appelée [ShadowPad](#) a été cachée dans un package logiciel de gestion de serveur, et a permis aux attaquants d'installer des charges utiles de programmes malveillants supplémentaires pour le vol de données et d'autres activités malveillantes. En septembre, l'infrastructure de l'outil gratuit populaire CCleaner a été compromise et une [version avec porte dérobée](#) a été livrée à son parc d'utilisateurs.

▲ FIGURE 5.

Attaques de chaînes d'approvisionnement logicielles en 2017 et 2018

ATTAQUES DE CHAÎNE D'APPROVISIONNEMENT DE LOGICIELS EN 2018 - CAUSES PROFONDES ET IMPACT

Le premier incident majeur d'attaque de chaîne d'approvisionnement de logiciel en 2018 a eu lieu le 6 mars, quand Windows Defender ATP a bloqué une campagne massive pour livrer le cheval de Troie Dofail (également connu sous le nom de Smoke Loader). La campagne massive de programme malveillant a été localisée à sa source dans une application d'égal à égal empoisonnée. Le package de mise à jour de l'application a été remplacé par un programme malveillant qui a téléchargé le code compromis, puis a installé le programme malveillant Dofail. Le cheval de Troie sophistiqué portait une charge utile de minage de pièces et présentait des mécanismes de persistance, des méthodes de sortie et des techniques d'injection interprocessus avancés.

▼ FIGURE 6.

Les tendances des attaques de Dofail (Smoke Loader) en 2018 affichent des pics d'instances bloquées en mars

Taux d'attaques Dofail



Dans les 12 premières heures de la campagne, l'antivirus Windows Defender a bloqué plus de 400 000 tentatives d'infection dans le monde entier. La Russie représentait 73 % des attaques mondiales, la Turquie et l'Ukraine enregistrant respectivement 18 % et 4 %.

Plusieurs autres attaques ont été détectées en utilisant des chaînes d’approvisionnement logicielles compromises en tant que mécanismes de livraison en 2018, y compris les éléments mentionnés dans le tableau suivant :

Période	Attaque	Description	Logiciel affecté
Mars 2018	Campagne de minage de pièces Dofoil (signalée par Microsoft).	Les attaquants ont empoisonné le processus de mise à jour d’une application d’égal à égal pour installer Dofoil, qui à son tour a installé des programmes malveillants de minage de pièces.	Application d’égal à égal
Juillet 2018	Chaîne d’approvisionnement compromise dans une chaîne d’approvisionnement (signalée par Microsoft).	Les attaquants ont compromis l’infrastructure partagée entre un fournisseur d’applications de l’éditeur PDF et l’un de ses partenaires fournisseurs de logiciels.	Application de l’éditeur PDF et fournisseur de partenaires tiers.
Août 2018	Programme de support technique à distance compromis (opération Red Signature, signalée par Trend Micro et IssueMakersLab).	Le serveur de mise à jour d’un fournisseur de solutions de support technique à distance a été compromis pour fournir un outil d’accès distant appelé 9002 RAT.	Programme de support technique à distance.
Octobre 2018	Solution de panneau de configuration d’hébergement compromise (signalée par ESET).	Le script d’installation d’une solution de panneau de configuration d’hébergement a été modifié pour voler des informations d’identification.	Solution de panneau de configuration d’hébergement.

◀ FIGURE 7.

Autres attaques de chaînes d’approvisionnement logicielles en 2018

LA CONFIANCE EN PÉRIL

Les attaques de chaîne d’approvisionnement sont insidieuses parce qu’elles tirent profit de la confiance que les utilisateurs et les départements informatiques placent dans le logiciel qu’ils utilisent. Le logiciel compromis est souvent signé et certifié par le fournisseur, et peut ne donner aucune indication que quelque chose ne va pas. Il est ainsi bien plus difficile de détecter l’infection. Ces attaques peuvent mettre à mal la relation entre les chaînes d’approvisionnement et leurs clients, que ces derniers soient des professionnels ou des particuliers. En empoisonnant les logiciels et en sapant les infrastructures de livraison ou de mise à jour, les attaques de chaîne d’approvisionnement peuvent nuire à l’intégrité et à la sécurité des biens et des services fournis par les organisations.

Les attaques de chaîne d’approvisionnement ont affecté un large éventail de logiciels et ciblé des organisations dans différents secteurs et emplacements géographiques. La menace des attaques de chaîne d’approvisionnement est un problème à l’échelle de l’industrie qui nécessite l’attention de plusieurs parties prenantes, y compris les développeurs et les fournisseurs de logiciels qui écrivent le code, les administrateurs système qui gèrent les installations logicielles, et la communauté de sécurité de l’information qui trouve ces attaques et crée des solutions pour protéger les personnes et les logiciels.

AU-DELÀ DU LOGICIEL : COMPROMISSION DE LA CHAÎNE D'APPROVISIONNEMENT PAR DES OBJETS CLOUD

La capacité des attaques de chaîne d'approvisionnement à saper la confiance est amplifiée et rendue encore plus complexe dans le cloud. Plusieurs incidents d'infrastructure, de services et d'objets cloud compromis en 2018 soulignent cette complexité :

- Extensions Chrome empoisonnées qui ont installé des programmes malveillants de fraude au clic (signalées par [ICEBRG](#))
- Divers dépôts Linux compromis (signalés dans quelques forums en ligne)
- Plug-ins malveillants WordPress utilisés pour diverses activités malveillantes, y compris permettre aux attaquants de publier du contenu sur des sites WordPress (signalés par [Wordfence](#))
- Images Docker malveillantes qui contenaient un script pour télécharger un programme malveillant de minage de cryptomonnaie et se sont téléchargées sur le compte Docker Hub (signalées par [Fortinet](#) et [Kromtech](#))
- Un package malveillant de typosquattage dans le dépôt Python officiel ; le package contenait un script malveillant qui télécharge des programmes malveillants utilisés pour modifier des adresses de minage de pièces dans le presse-papiers (signalé sur [Medium](#))
- Script compromis dans StatCounter qui permettait aux attaquants d'injecter un script malveillant dans des sites web qui utilisent StatCounter (signalé par [ESET](#))

- Plusieurs incidents de modules npm avec porte dérobée ([The npm Blog](#), [Medium](#)) qui, en cas d'exploitation, pourrait entraîner des situations telles que, par exemple, un attaquant en mesure d'entrer un code arbitraire dans un serveur en cours d'exécution et de l'exécuter.

Ces incidents démontrent comment le compromis de la chaîne d'approvisionnement peut élargir immensément une surface d'attaque. S'ils ne sont pas sécurisés, les objets cloud peuvent être des vecteurs d'entrée inattendus. Par exemple, l'incident du Docker Hub impliquait un compte malveillant qui chargeait des images Docker contenant une porte dérobée cachée de minage de pièces. Les images Docker ont été hébergées sur Docker Hub pendant près d'un an et ont été téléchargées des millions de fois et utilisées par des administrateurs et des utilisateurs qui ne se doutent de rien.

Les risques liés à la chaîne d'approvisionnement s'étendent au code dans le Cloud, à l'open source, aux bibliothèques web, aux conteneurs et à d'autres objets dans le Cloud. Ces risques, couplés au degré élevé de variation entre la chaîne d'approvisionnement logicielle et matérielle, compromettent les incidents qui ont été mis en évidence, font des attaques de chaîne d'approvisionnement une ample catégorie de menace. Bien qu'il n'existe pas de solution unique pour l'ensemble de ces types d'attaques, les organisations doivent renforcer [la protection préventive et la détection post-violation](#) des attaques de la chaîne d'approvisionnement provenant de fournisseurs de matériel et de logiciels compromis, de fournisseurs de logiciels open source, ou de services cloud et de fournisseurs d'infrastructure.

Enquêter sur les cyberincidents avec DART

L'équipe de détection et d'intervention (DART) est une équipe mondiale d'intervenants en cas d'incident et d'experts en cybersécurité qui aide les organisations à détecter les incidents de cybersécurité, enquêter sur ces derniers et y réagir. Cette section met en évidence certains des cas de clients que DART a traité au cours de l'année passée. Elle illustre les tendances courantes des attaquants et la façon dont Microsoft et ses clients ont pu les contrecarrer.



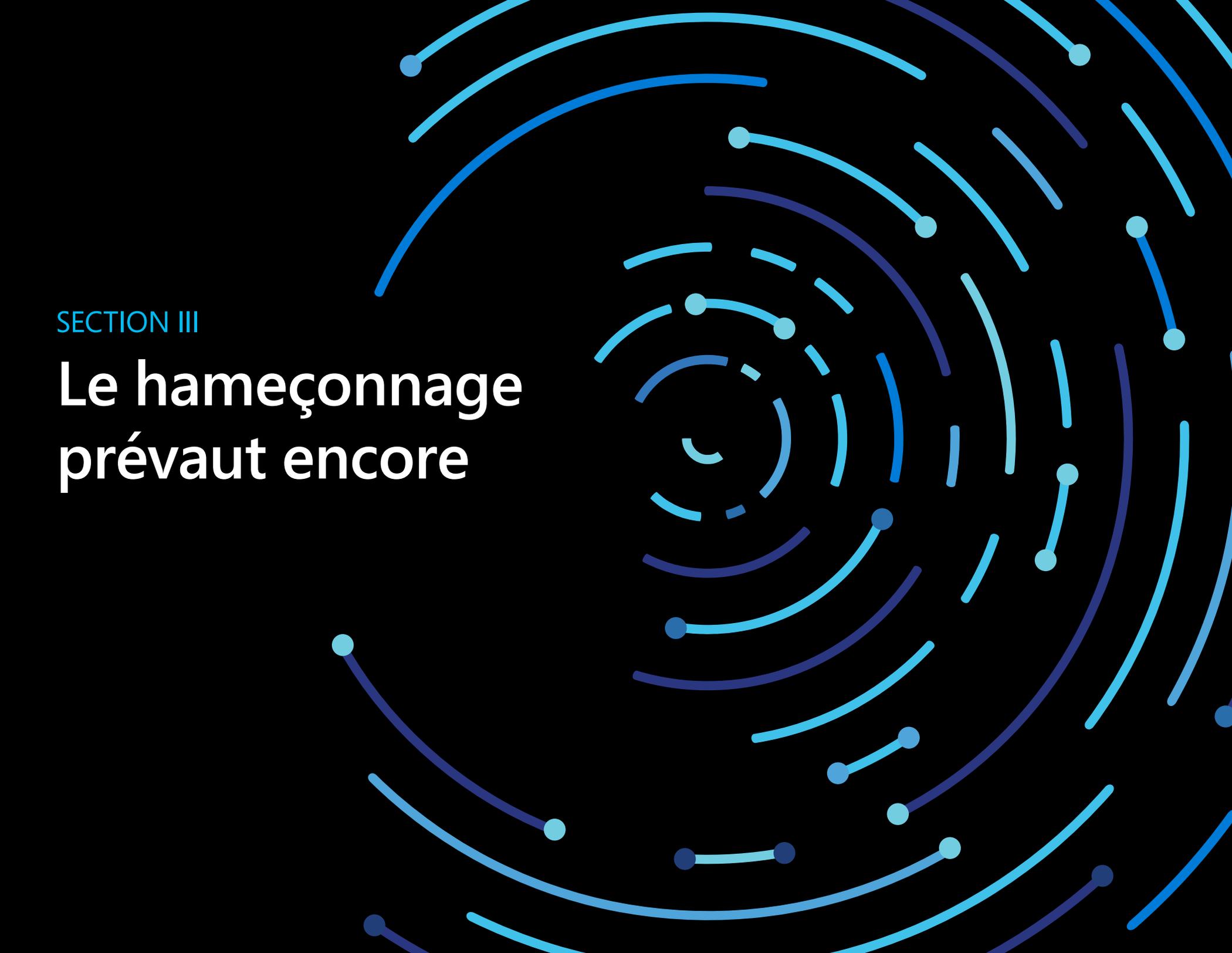
UNE ORGANISATION DE SERVICES PROFESSIONNELS A CONNU UNE ATTAQUE ÉTATIQUE QUI A EXFILTRÉ DES DONNÉES

Une organisation de services professionnels a été affectée par une menace persistante avancée (APT) soutenue par un État qui a obtenu l'accès à des informations d'identification privilégiées de l'organisation. Les attaquants ont obtenu l'accès au réseau en utilisant une attaque par pulvérisation de mots de passe dans laquelle ils ont utilisé un petit nombre de mots de passe faibles ou largement utilisés (tels que « p@ssword » ou « 123456 ») pour cibler un grand nombre de comptes d'utilisateurs et obtenir des informations d'identification d'administration Office 365. (Les attaques par pulvérisation de mots de passe sont utilisées pour éviter la détection en limitant le nombre de tentatives de connexion pour chaque compte.) Après avoir infiltré le réseau, l'APT a procédé à une exfiltration élaborée et automatisée des données des boîtes aux lettres des collaborateurs. En dépit de multiples tentatives en interne pour les supprimer, l'adversaire est

resté dans le réseau pendant plus de 200 jours. Dans le cadre de l'attaque, l'adversaire a exploité le logiciel de la chaîne d'approvisionnement de l'organisation et automatisé l'exfiltration des données.

Suite à une suspicion de violation de ses données client, l'organisation a engagé l'équipe DART pour enquêter et aider à prévenir d'autres dommages. L'équipe DART a identifié des recherches ciblées de boîtes aux lettres Office 365, des comptes compromis ainsi que des canaux de contrôle et de commande de l'attaquant. Les principales leçons client tirées de cet incident étaient de déployer des contrôles pour protéger les services cloud contre les attaquants et les menaces basées sur l'identité. L'organisation a adopté l'authentification multifacteur (MFA), des stratégies d'accès conditionnel pour certaines applications cloud et la journalisation Office 365. Pour se protéger davantage contre des

menaces similaires à l'avenir, l'organisation peut également adopter une solution de détection des menaces et d'intervention de point de terminaison (EDR) pour détecter les attaquants susceptibles d'essayer d'exploiter son réseau. En outre, nous avons recommandé que cette organisation nomme un organisme de gouvernance du cloud ou une équipe d'identité mondiale qui gèrera et appliquera les stratégies d'authentification utilisateur appropriées, afin que l'organisation surveille sa position de sécurité et puisse atténuer plus efficacement les risques.



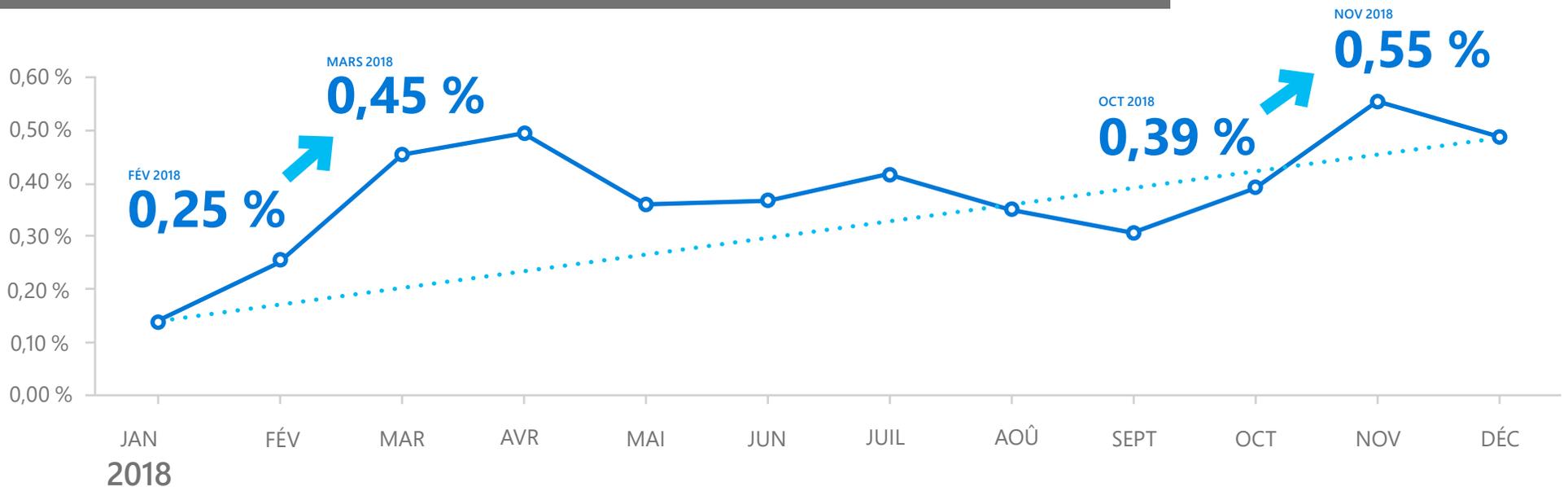
SECTION III

Le hameçonnage prévaut encore

En 2018, les analystes Microsoft des menaces ont vu des preuves que **les attaquants continuent à utiliser le hameçonnage comme méthode d'attaque préférée.**

Le hameçonnage promet de demeurer un problème dans un avenir prévisible car il implique des décisions humaines et un jugement face aux efforts persistants des cybercriminels pour attirer les victimes dans leurs pièges.

Les taux de hameçonnage demeurent en hausse Pourcentage du total des e-mails entrants qui sont des e-mails de hameçonnage



LE HAMEÇONNAGE CONTINUE D'ÊTRE UN VECTEUR D'ATTAQUE PRÉFÉRÉ EN 2018

Microsoft analyse et scanne dans Office 365 plus de 470 milliards d'e-mails par mois pour le hameçonnage et les programmes malveillants, ce qui fournit aux analystes un aperçu considérable des tendances et des techniques des attaquants. La part des e-mails entrants qui étaient des messages de hameçonnage **a augmenté de 250 %** entre janvier et décembre 2018. Le hameçonnage reste l'un des vecteurs d'attaque les plus utilisés pour fournir des charges utiles zero-day malveillantes aux utilisateurs, et Microsoft a continué à durcir le ton contre ces attaques avec des capacités supplémentaires de réaction, d'investigation, de détection et de protection anti-hameçonnage pour contribuer à sécuriser les utilisateurs.

▲ FIGURE 8.

E-mails de hameçonnage en 2018

Évolution des méthodes d'attaque par hameçonnage

À mesure que les outils et les techniques utilisés pour protéger les personnes contre le hameçonnage gagnent en sophistication, les attaquants sont contraints de s'adapter eux-mêmes. Les attaques de hameçonnage sont devenues de plus en plus polymorphes, ce qui signifie que les attaquants n'utilisent pas une URL, un domaine ou une adresse IP unique pour envoyer du courrier, mais qu'ils ont recours à une infrastructure variée avec plusieurs points d'attaque. La nature des attaques elles-mêmes a également évolué, avec des campagnes de hameçonnage modernes allant d'attaques à courte portée qui sont actives pendant seulement quelques minutes, à des campagnes d'un volume bien supérieur. D'autres sont des variantes d'attaques en série dans lesquelles les attaquants envoient un court volume de courrier sur plusieurs jours successifs.

En outre, Microsoft a observé une tendance des attaquants à utiliser une infrastructure hébergée et d'autres infrastructures de cloud public, ce qui permet d'éviter plus facilement la détection en se cachant parmi des ressources et des sites légitimes. Par exemple, les attaquants se servent de plus en plus de services et de sites de collaboration et de partage de documents populaires pour distribuer des charges utiles malveillantes et de faux formulaires de connexion utilisés pour voler des informations d'identification d'utilisateurs. Il y a également eu une augmentation de l'utilisation de comptes compromis pour ensuite distribuer des e-mails malveillants à l'intérieur et à l'extérieur d'une organisation.

Les campagnes de hameçonnage varient de ciblées à vastes

Comme avec la distribution de programmes malveillants en général, les campagnes de hameçonnage varient, allant d'attaques ciblées à larges, génériques. Bien que les attaques hautement sophistiquées génèrent plus de gains monétaires par compte hameçonné, les attaques plus génériques génèrent moins d'argent par compte compromis, mais ciblent un ensemble plus large d'utilisateurs.

Un exemple de campagne sophistiquée et ciblée est [Ursnif](#) qui implique que les attaquants localisent le nom de fichier du document comme étant spécifique à une organisation familière ou à l'industrie de la cible. De telles attaques sont assez différentes des campagnes de grande envergure et apparaissent comme étant plus légitimes et dignes de confiance.

Certaines des campagnes de grande envergure en 2018 ont été liées à Business Email Compromise (BEC) et à l'emprunt d'identité de marques, de domaines ou d'utilisateurs connus au sein des organisations cibles et de campagnes d'usurpation sophistiquées. L'emprunt d'identité de domaine est une tactique d'attaque courante utilisée pour inciter les organisations à croire que l'e-mail est digne de confiance et doit être ouvert.

Les leurres du hameçonnage prennent de nombreuses formes

Les chercheurs de Microsoft ont constaté que de nombreux types différents de leurres de hameçonnage ou de charges utiles sont utilisés dans des campagnes, dont les suivantes :

- **Usurpation de domaine** (le domaine de message électronique et le nom de domaine d'origine sont identiques))
- **Emprunt d'identité de domaine** (le domaine du message électronique ressemble au nom de domaine d'origine)²
- **Emprunt d'identité d'utilisateur** (le message électronique semble provenir d'une personne en qui vous avez confiance)
- **Leurres de textes** (le message écrit semble provenir d'une source légitime telle qu'une banque, un organisme gouvernemental ou une autre société pour donner une certaine légitimité aux revendications et il est généralement demandé à la victime de fournir des informations sensibles telles que les suivantes : noms d'utilisateur, mots de passe ou données financières sensibles)

- **Liens de hameçonnage d'informations d'identification** (le message électronique contient un lien vers une page qui ressemble à une page de connexion pour un site légitime, afin que les utilisateurs saisissent leurs identifiants d'identification)
- **Pièces jointes de hameçonnage** (le message électronique contient une pièce jointe de fichier malveillant que l'expéditeur incite la victime à ouvrir)
- **Liens vers de faux emplacements de stockage dans le cloud** (le message électronique semble provenir d'une source légitime et incite l'utilisateur à donner une autorisation et/ou à saisir des informations personnelles telles que des identifiants en échange d'un accès à un faux emplacement de stockage dans le cloud)

Cette variété de leurres qui pourraient potentiellement être employée par les attaquants augmente la complexité des menaces de hameçonnage auxquelles les organisations doivent faire face.

NOTE DE BAS DE PAGE

² L'emprunt d'identité de domaine peut ressembler à l'usurpation de domaine (correspondance exacte avec le nom de domaine d'origine) dans le cas exceptionnel où le domaine apparaît dans le nom complet d'affichage d'adresse de messagerie).

Enquêter sur les cyberincidents avec DART

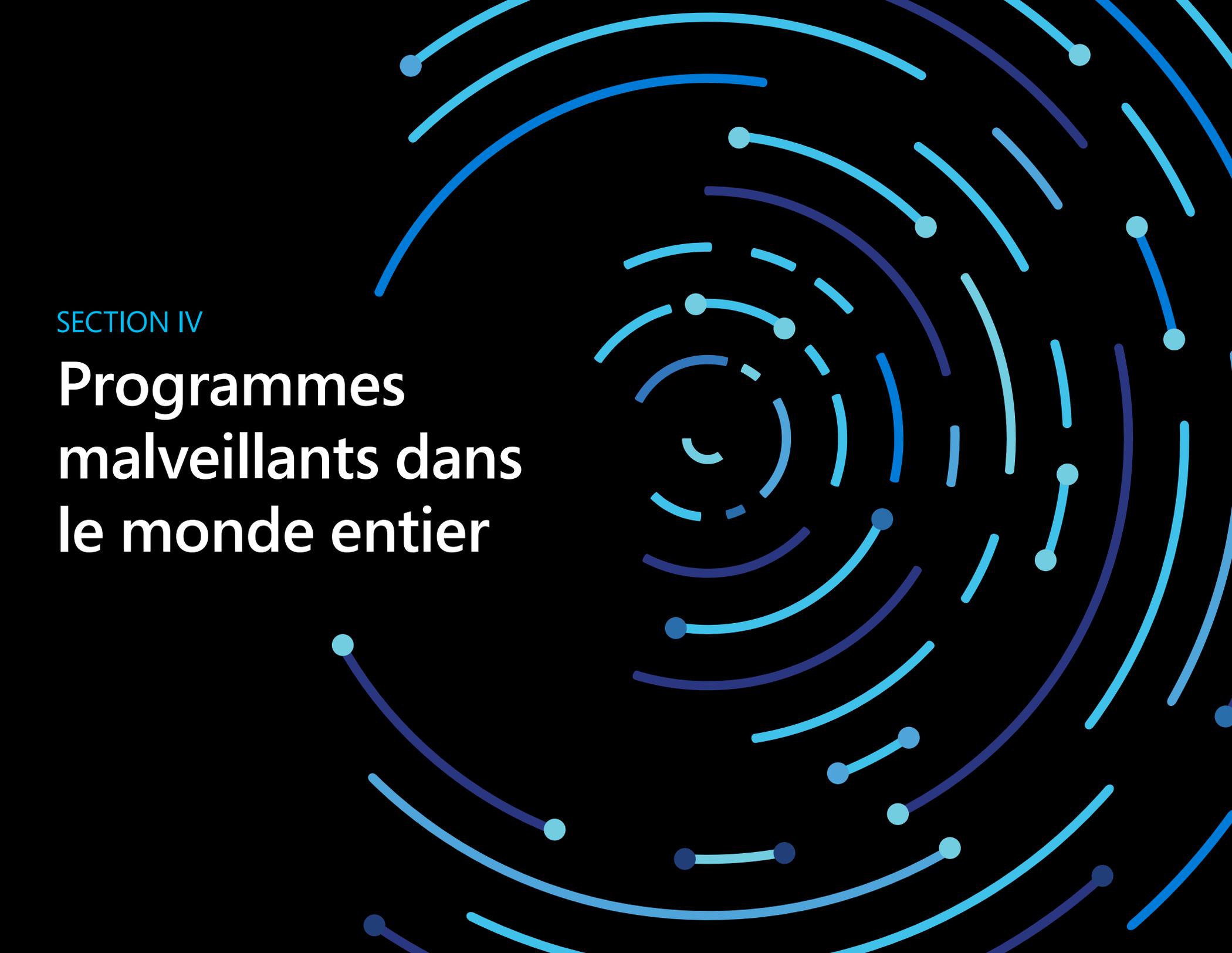
GRANDE ORGANISATION DE FABRICATION TOUCHÉE PAR DES INCIDENTS DE HAMEÇONNAGE CIBLÉS

Une organisation de fabrication a été la cible d'une campagne de hameçonnage en plusieurs phases sur une période de quelques mois. Cette approche n'est pas inhabituelle. Au cours de la première phase, l'attaquant effectue une reconnaissance et, lors de la deuxième phase, il cible les actifs de grande valeur. La première phase de cette campagne a exploité une escroquerie de hameçonnage bien connue qui était basée sur un lien de page web inclus dans un e-mail envoyé à un petit groupe ciblé au sein de l'organisation. L'e-mail affirmait que la cible avait un document électronique important en attente de révision et que tout ce que le destinataire avait à faire était de s'authentifier avec ses informations d'identification du domaine pour obtenir l'accès. Cette fausse page de destination mise en place pour permettre à la cible d'examiner le soi-disant « document important » a en réalité récolté les informations d'identification et permis à l'attaquant d'accéder à des comptes Office 365 à partir de n'importe où dans le monde. La deuxième phase de la campagne de hameçonnage visait à envoyer des courriels de hameçonnage similaires à des actifs de grande valeur à l'intérieur de l'organisation de fabrication cible, dans l'espoir d'accéder à des données plus précieuses. Microsoft s'est impliquée aux côtés de ce client pendant la deuxième phase de la campagne de hameçonnage. Les leçons client clés de cet incident ont été les suivantes : le hameçonnage demeure une des méthodes d'attaque les plus efficaces et les utilisateurs

sont encore le lien le plus faible. Former les utilisateurs à se méfier des escroqueries par hameçonnage, avoir des outils en place pour identifier les attaquants et agir, ainsi qu'appliquer régulièrement des correctifs aux systèmes sont toutes des opérations importantes ; si l'organisation ne met pas en place au moins l'une d'elles, elle peut être vulnérable.

Dans ce cas, la préoccupation la plus importante du client était un besoin immédiat de bloquer l'accès aux comptes compromis. En partenariat avec les équipes Azure Identity et Office 365, DART a conçu un plan pour éradiquer l'attaquant du réseau et surveiller tout trafic vers le canal de commande et de contrôle à l'aide de la solution Log Analytics de Microsoft Azure nouvellement déployée. L'équipe a été en mesure d'aider à résoudre la situation en seulement trois heures. L'accès de l'attaquant a été bloqué et l'organisation a pu porter son attention sur la récupération et l'évaluation des dommages. DART a utilisé les outils Log Analytics d'Azure pour rechercher le comportement de l'attaquant, ce qui a permis de découvrir de nombreux défis de configuration pour l'organisation. Par exemple, DART a identifié des lacunes dans le correctif sur les serveurs critiques, découverts des ordinateurs sur le réseau communiquant avec des hôtes incorrects connus sur Internet, et également trouvé plusieurs serveurs importants sans protection contre les programmes malveillants.



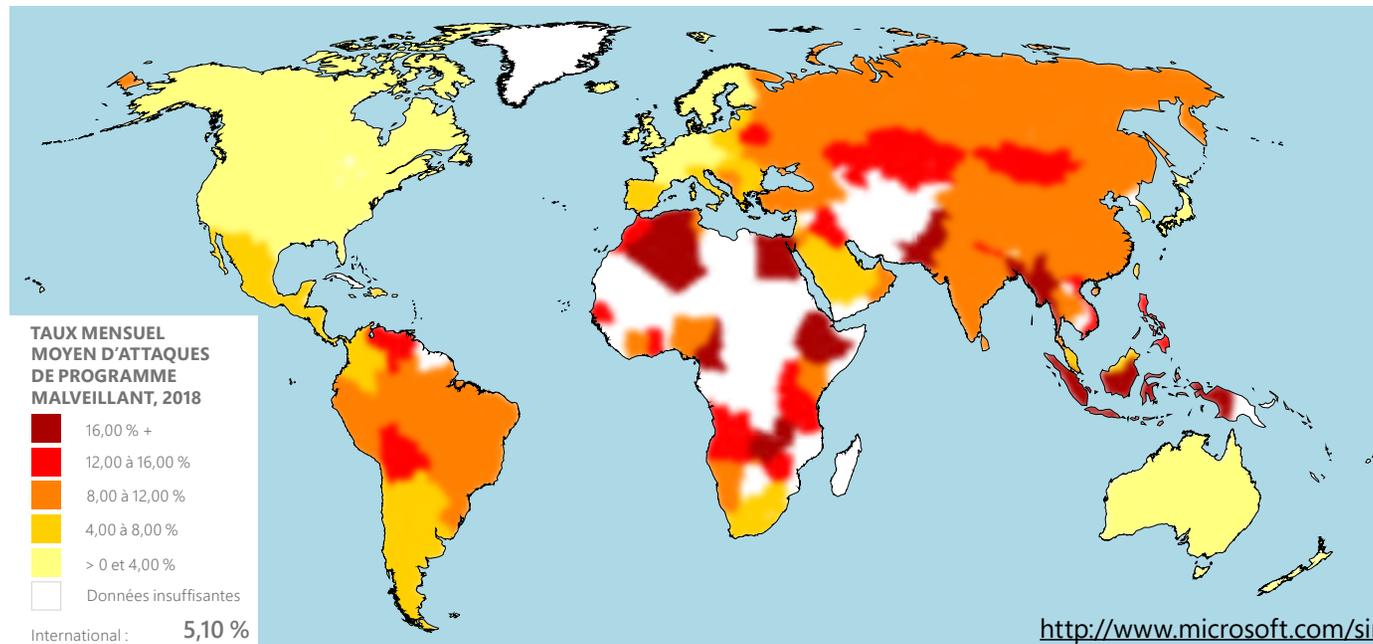


SECTION IV

Programmes malveillants dans le monde entier

Les programmes malveillants représentent un risque pour les organisations et les individus sous la forme d'une utilisation altérée, de perte de données, de vol de propriété intellectuelle, de perte monétaire, de détresse émotionnelle, et peuvent même mettre la vie humaine en danger. Microsoft utilise un large éventail d'outils et de techniques pour identifier, bloquer et éradiquer les infections de programmes malveillants où qu'ils se trouvent.

En 2017, les taux d'attaques des programmes malveillants allaient d'environ 5 % à plus de 7 %. Au début de 2018, ils ont augmenté avant de diminuer pendant la majeure partie de l'année pour arriver juste au-dessus de 4 %. Certaines raisons potentielles de la [diminution globale des taux d'attaques des programmes malveillants en 2018](#) sont la croissance de l'adoption de Windows 10 et l'utilisation accrue de Windows Defender pour la protection. Le taux d'attaques correspond au pourcentage d'ordinateurs exécutant l'antivirus Windows Defender ayant signalé avoir rencontré des programmes malveillants pendant le mois, y compris des tentatives d'infection que Defender a bloquées.



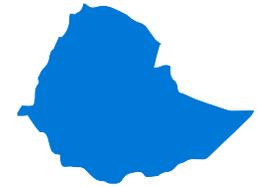
◀ **FIGURE 9.**

Moyenne mensuelle des taux d'attaques de programme malveillant dans le monde entier par pays/région en 2018

Les cinq sites présentant les taux d'attaques les plus élevés de programmes malveillants durant la période de janvier à décembre 2018 étaient l'Éthiopie (26,33 % de taux mensuel moyen d'attaques), le Pakistan (18,94), les Territoires palestiniens (17,50), le Bangladesh (16,95) et l'Indonésie (16,59), tous ayant un taux mensuel moyen d'attaques d'environ 16,59 % ou plus au cours de la période. Les taux d'infection tendent à corrélérer fortement avec les facteurs de développement humain et le niveau de technologie au sein d'une société. Tous les emplacements avec les taux d'attaques les plus élevés en 2018 ont été classés dans les premiers 40 % des pays et des régions de l'indice Technologies de l'information et de la communication (TIC) de 2017, publié par l'Union internationale des télécommunications (UIT) des Nations Unies.

Les cinq emplacements avec les taux d'attaques les plus bas de programme malveillant pendant cette même période étaient l'Irlande (1,26), le Japon (1,51), la Finlande (1,74), la Norvège (1,79) et les Pays-Bas (1,82), tous ayant un taux mensuel moyen d'attaques de 1,82 % ou moins au cours de la période. Ces emplacements disposent généralement d'infrastructures de cybersécurité matures et de programmes bien établis pour protéger les infrastructures critiques et communiquer avec leurs citoyens en matière de sécurité de base.

TAUX MENSUEL MOYEN D'ATTAQUES DES PAYS LES PLUS TOUCHÉS PAR LES PROGRAMMES MALVEILLANTS



Éthiopie : **26,33 %**



Pakistan : **18,94 %**



Territoires palestiniens : **17,50 %**

Enquêter sur les cyberincidents avec DART

PLUSIEURS ORGANISMES DE SERVICES FINANCIERS ONT CONNU DES ATTAQUES ÉTATIQUES QUI ONT PERTURBÉ LES OPÉRATIONS

Dans l'un des incidents les plus destructeurs que DART a pu observer, plusieurs organismes de services financiers ont été la cible d'une APT parrainée par un État (un groupe différent de celui qui ciblait l'organisation de services professionnels mentionnée plus tôt) qui s'est déroulée d'une manière similaire.

Cette APT a obtenu un accès administratif après avoir infecté une machine patient zéro en implantant une porte dérobée hautement ciblée et obscurcie, sans doute livrée via un e-mail de harponnage. Par la suite, l'APT a exécuté plusieurs transactions frauduleuses, transférant de grosses sommes d'argent sur des comptes bancaires étrangers. Dans certains cas, l'attaquant est demeuré indétecté pendant plus de 100 jours. Après que l'attaquant s'est rendu compte qu'il avait été détecté, il a rapidement déployé une attaque préinstallée, délivrant un programme malveillant destructeur à plus de la moitié des systèmes dans l'environnement ; les opérations de ces clients ont été fermées pendant plusieurs jours.

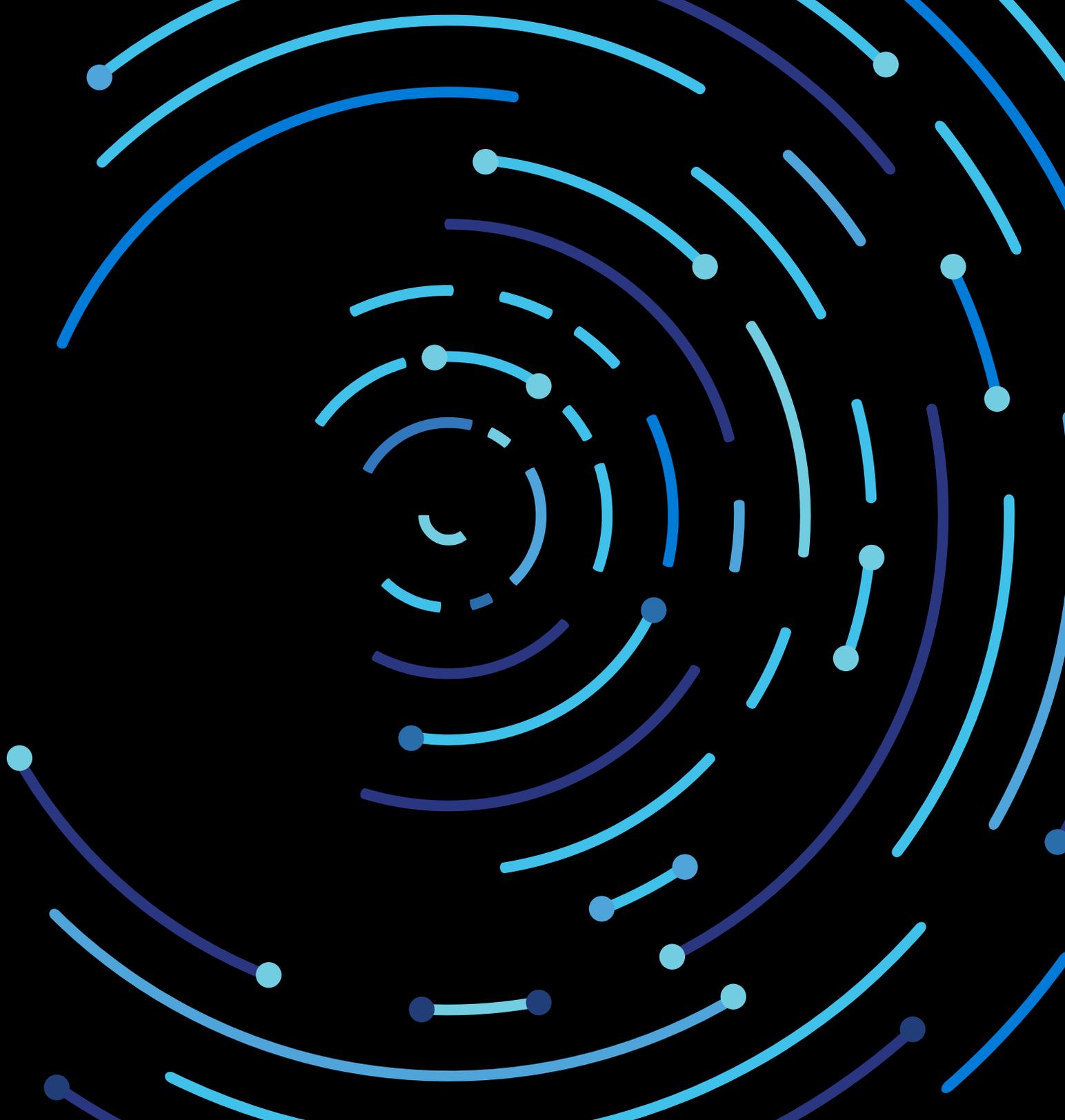
Quelques leçons client clés ont été tirées de ces incidents. La première était que la gestion du cycle de vie des logiciels est particulièrement importante, ce qui inclut la mise à jour (systèmes d'exploitation et sécurité), la correction et la vérification régulières des systèmes.

Dans un cas, l'environnement système Linux d'une organisation sur lequel un nombre exceptionnellement élevé de charges de travail s'exécutait était entièrement non géré, ce qui le place face à un risque d'attaque remarquablement élevé. La deuxième leçon a été qu'il est important de conserver des sauvegardes des données système dans un emplacement hors connexion dans l'éventualité où les données principales seraient perdues. Une autre leçon a été que les solutions antivirus traditionnelles peuvent ne pas suffire si vous avez besoin de connaître l'activité de l'adversaire.

Le retour au mode de fonctionnement normal était la plus haute priorité pour ces organisations. DART a aidé à restaurer les services en examinant d'abord l'impact, puis en entreprenant les actions d'atténuation nécessaires, telles qu'éliminer les programmes malveillants des systèmes concernés et restaurer l'intégrité de l'état de ces derniers. L'équipe a également formé des clients sur la façon d'utiliser les outils d'examen des menaces Microsoft, y compris EDR et d'autres, afin qu'ils puissent rechercher l'activité de l'attaquant et le comportement anormal dans leur réseau. DART a insisté sur le fait que la surveillance des points de terminaison est essentielle pour la défense contre les attaques sophistiquées et ciblées qui peuvent ne pas être détectées par des solutions antivirus traditionnelles.



Conseils



Conseils

L'instauration d'une résilience organisationnelle et d'une réduction significative des risques nécessite une approche sécuritaire qui inclut la prévention ainsi que la détection et l'intervention. Nous avons organisé les suggestions suivantes de contrôles et de meilleures pratiques de sécurité dans ces catégories.

PRÉVENTION :

Les contrôles préventifs jouent un rôle clé dans une stratégie de défense globale car les bons investissements peuvent augmenter le coût des attaques pour les cybercriminels et soutenir ces coûts d'attaque accrus sur la durée (sans exiger qu'un expert analyste doive surveiller et interpréter les résultats). Les investissements en matière de contrôle préventif devraient viser les techniques de coûts les plus bas pour éliminer progressivement les techniques d'attaque efficaces et bon marché.

Quatre points à considérer pour la prévention sont les suivants :

1. L'hygiène de sécurité est essentielle. Comme on le voit dans certains des cyberincidents partagés dans ce rapport, les problèmes d'hygiène courants peuvent saper les capacités de sécurité avancées, de sorte que suivre ces conseils peut aider à atténuer les risques :

- Évitez d'utiliser des logiciels libres et/ou piratés inconnus. Utilisez uniquement des logiciels provenant de sources fiables.
- Réduisez les risques de vol d'informations d'identification, notamment en sécurisant les comptes d'administrateur privilégiés. Pour

découvrir comment procéder, lisez ce [blog](#) qui décrit certains principes et outils que Microsoft a utilisés pour guider et améliorer notre propre posture de sécurité et certaines feuilles de route prescriptives pour vous aider à planifier vos propres initiatives.

- Appliquez des lignes de base de configuration sécurisées fournies par vos éditeurs de logiciels.
- Tenez les machines à jour en appliquant rapidement les dernières mises à jour à vos systèmes d'exploitation et applications, et déployez immédiatement des mises à jour de sécurité critiques pour le système d'exploitation, les navigateurs et les e-mails. Isolez (ou mettez hors service) les machines qui ne peuvent pas être mises à jour ou corrigées.
- Installez des protections avancées d'e-mails et de navigateurs. Déployez une passerelle de messagerie sécurisée dotée de fonctionnalités avancées de protection contre les menaces pour vous défendre contre les variantes de hameçonnage modernes.
- Activez les défenses anti-programme malveillant et réseau de l'hôte pour obtenir des interventions de blocage en quasi temps réel à partir du cloud (si disponible dans votre solution).

2. Installez des contrôles d'accès. Envisagez les éléments suivants :

- Appliquez le principe du privilège minimum qui inclut l'installation de la segmentation du réseau, la suppression des privilèges d'administrateur local des utilisateurs et l'effort de prudence lors de l'octroi de toutes autorisations aux applications s'exécutant sur l'ordinateur.
- Limitez le téléchargement des applications uniquement à celles provenant de sources fiables (un magasin d'applications officiel).
- Déployez des stratégies d'intégrité de code forte, notamment en limitant les applications que les utilisateurs peuvent exécuter. Si possible, adoptez une solution de sécurité qui limitera le code qui s'exécute dans le noyau du système et peut bloquer les scripts non signés et d'autres formes de code non fiable. Utilisez la mise en liste blanche d'applications.
- Pour en savoir plus sur les attaques de chaîne d'approvisionnement de logiciels et la manière de se protéger contre elles, consultez ce blog de chercheurs Microsoft.

3. Conservez des sauvegardes.

- Créez des sauvegardes indestructibles de vos systèmes et données critiques.
- Utilisez des services de stockage cloud pour la sauvegarde automatique des données en ligne. Pour les données qui sont sur site, sauvegardez régulièrement les données importantes à l'aide de la règle 3-2-1. Conservez trois sauvegardes de vos données, sur deux types de stockage différents et au moins une hors site.

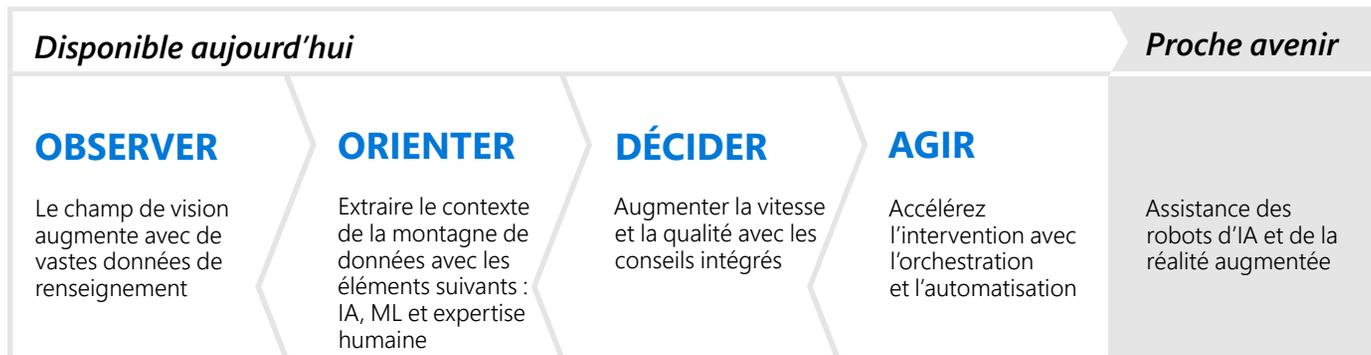
4. En cas de doute, soyez vigilant et agissez.

- Apprenez aux collaborateurs à se méfier des communications suspectes qui demandent des informations sensibles et comment réagir et les signaler à l'équipe des opérations de sécurité de l'organisation immédiatement. La formation peut également aider à atténuer les attaques de harponnage et de piratage psychologique.
- Soyez prudent lorsque vous cliquez sur des liens Web. La pratique d'habitudes de navigation web sécurisée et l'utilisation de solutions qui fournissent des avertissements ou qui bloquent l'accès à des sites non sécurisés peuvent contribuer à réduire la probabilité de rencontrer des sites web associés au minage de cryptomonnaie.
- Si un ordinateur est exceptionnellement lent, recherchez tous les fichiers suspects en cours d'exécution et n'hésitez pas à soumettre un échantillon au fournisseur du système d'exploitation. Vous pouvez soumettre des fichiers pour l'analyse de programme malveillant à l'adresse suivante : <https://www.microsoft.com/wdsi/filesubmission>.

DÉTECTION ET INTERVENTION :

La détection et l'intervention contribuent à la résilience en limitant le temps d'accès d'un attaquant à vos ressources. Cela diminue le retour sur investissement de l'attaquant à la fois en augmentant le coût de l'attaquant (ils doivent réessayer ou modifier leurs opérations) et en diminuant le rendement (limite la probabilité d'atteindre leur objectif).

La même technologie de cloud qui permet aux organisations professionnelles de mieux répondre aux besoins du marché peut également aider les opérations de sécurité à mieux lutter contre les attaquants.



◀ **FIGURE 10.**

Trajectoire d'évolution des SOC

Alors que nous examinons la trajectoire de l'évolution des centres d'opérations de sécurité (SOC), nous voyons que la technologie augmente continuellement la rapidité et la qualité des décisions et des actions de ces derniers. Bon nombre de ces innovations peuvent être cartographiées à chaque étape de la « boucle » OODA (Observer, Orienter, Décider et Agir) qui a été documentée par le colonel John Boyd de l'USAF.³

OBSERVER – Les SOC peuvent puiser dans la vaste veille de sécurité disponible (de Microsoft et d'autres sources) augmentant considérablement leur champ de vision au sein de l'organisation et de l'environnement externe.

ORIENTER – Au fur et à mesure que ces nouvelles sources de données deviennent disponibles pour les SOC déjà surchargés, le Machine learning (un sous-ensemble de l'intelligence artificielle) devient un outil essentiel pour raisonner sur ces jeux de données massifs et identifier les anomalies qui méritent d'être étudiées. Les fournisseurs de sécurité (y compris Microsoft) ont adopté la technologie de Machine learning pour hiérarchiser rapidement les événements (et aider à fusionner ces événements individuels en incidents globaux).

DÉCIDER – Du fait que la complexité et le volume d'attaque peuvent rapidement surcharger un SOC, les analystes et les intervenants en cas d'incident doivent

prendre de nombreuses décisions et agir rapidement en réponse aux alertes et aux détections. Microsoft et d'autres fournisseurs ont intégré des capacités d'investigation automatisées ainsi que des conseils pour aider les analystes à prendre rapidement de bonnes décisions (pour isoler des appareils potentiellement infectés ou compromis, par exemple). Pour le moment, l'automatisation se concentre sur la résolution rapide des incidents à faible priorité, de sorte que les compétences spécialisées puissent être appliquées à des problèmes plus complexes.

AGIR – L'intervention nécessite une exécution rapide et précise sur de nombreuses technologies et plateformes, ce que permettent les technologies d'automatisation des réactions et d'orchestration de sécurité. Microsoft et beaucoup d'autres continuent d'investir dans ces technologies, y compris la détection des menaces modernes et les solutions de réaction automatisée.

NOTE DE BAS DE PAGE

³<http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/>

D'autres tendances qui s'appliquent à un SOC moderne sont les suivantes :

- **Qualité par rapport à la quantité de flux d'alerte**
– Les organisations passant de la gestion des « informations insuffisantes », à celle de « trop d'informations », le temps et l'attention des analystes de SOC hautement spécialisés deviennent de plus en plus précieux. Cela entraîne un besoin accru de qualité dans les alertes qui requièrent l'engagement d'analystes de niveaux 1 et 2. Alors que les flux de données supplémentaires sont toujours utiles pour les enquêtes et le repérage proactif, le Corporate IT SOC de Microsoft mesure le taux positif réel des flux d'alerte nécessitant une réponse d'analyste (et exigeant actuellement 90 % ou plus de taux positif vrai).
- **Gravité des données** – L'analyse de données sur les grands ensembles (y compris les données de sécurité) est difficile à réaliser sans accès aux données brutes sous-jacentes. À mesure que des données de sécurité supplémentaires sont disponibles, il devient plus économique et plus pratique d'effectuer les analyses de sécurité dans le cloud par rapport à un retour de ces données vers un système local. Cela conduira probablement à l'évolution des architectures SIEM et SOC qui peuvent inclure des approches SIEM hybrides ou l'adoption du cloud natif SIEM en tant que service.
- **Contexte élevé** – Ces types de détections sont beaucoup plus utiles en raison de leur capacité à corréliser les jeux de données plus efficacement. Bien que les détections basées sur le trafic réseau traditionnel continuent de fournir une certaine

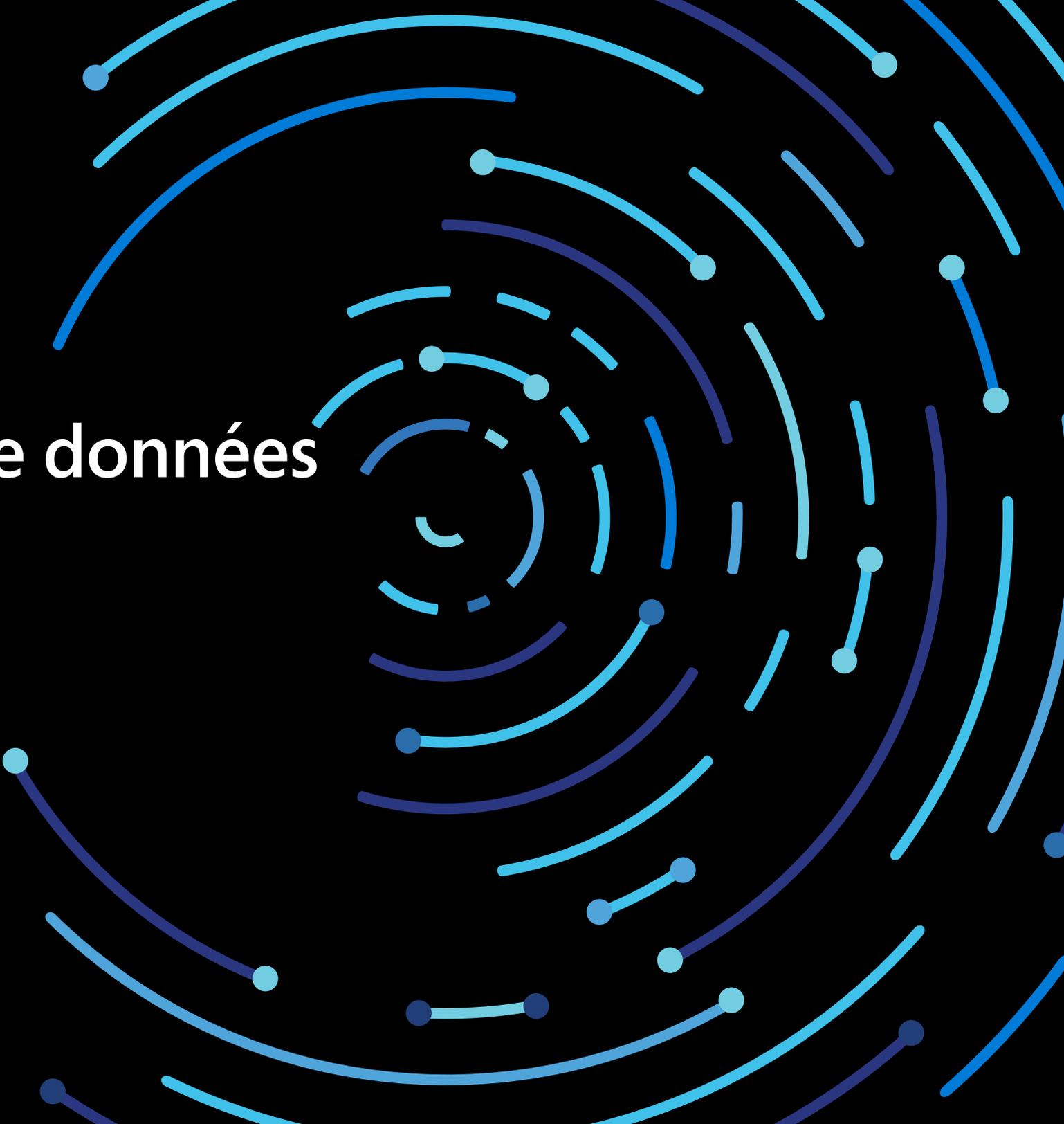
valeur de sécurité, le trafic réseau brut manque généralement de contexte pour différencier l'activité légitime et l'activité anormale. Nous voyons les SOC retirer beaucoup plus de valeur de détections riches en contexte comme les suivantes :

- **Solutions EDR (Endpoint Detection and Response, Détection et intervention au niveau des points terminaux)** qui ont un contexte profond sur l'activité de l'hôte
- Détections basées sur l'identité qui incluent des informations sur les modèles d'authentification utilisateur normaux (emplacements, heures, services accédés, etc.) et appliquent l'analyse comportementale

Les adversaires ont plus de mal à contourner ces détections riches en contexte parce qu'ils doivent imiter une opération beaucoup plus complexe (par rapport à quelques attributs techniques du trafic IP).

Une autre leçon que nous avons tirée des violations majeures chez les clients a été la difficulté de réagir rapidement aux incidents lorsque les fonctions informatiques sont partiellement ou entièrement externalisées. Nous vous recommandons d'examiner vos contrats d'externalisation informatique et vos contrats de niveau de service (SLA), ainsi que les fournisseurs de chaînes d'approvisionnement pour vous assurer qu'ils sont compatibles avec une réponse rapide aux problèmes de sécurité. Pour plus d'enseignements tirés de nos enquêtes sur les incidents chez les clients, consultez l'IRRG (Incident Response Reference Guide - Guide de référence de la réponse aux incidents) à l'adresse suivante : <https://aka.ms/IRRG>.

Sources de données



Sources de données

Microsoft a collecté les données incluses dans le Security Intelligence Report de Microsoft dans le cadre de la fourniture d'une large gamme de produits et de services Microsoft, comme indiqué dans la [Déclaration de confidentialité Microsoft](#). Ces données nous fournissent des informations précieuses sur la sécurité et les opérations de nos produits et services, ainsi que des aperçus sur le paysage de menace de cybersécurité en général. Ces données comprennent des analyses des sources suivantes.⁴

- [Azure Security Center](#) est un service qui permet aux entreprises de prévenir, de détecter et de traiter les menaces en offrant une visibilité accrue sur la sécurité des charges de travail dans le cloud et en intégrant les analytiques avancées et les renseignements sur les menaces afin de détecter les attaques.
- [Bing](#) est le moteur de recherche et de décision qui analyse des milliards de pages web par an afin de déceler les contenus malveillants. Une fois ces contenus détectés, Bing affiche des avertissements aux utilisateurs pour aider à prévenir l'infection.
- [Exchange Online](#) est le service de productivité et de messagerie hébergé par Microsoft. Les services anti-malware et antispam d'Exchange Online analysent chaque année des milliards de messages pour identifier et bloquer le spam et les logiciels malveillants.
- [L'outil de suppression de logiciels malveillants](#) (MSRT) est un outil gratuit, conçu par Microsoft, pour identifier et éliminer certaines familles spécifiques courantes de programmes malveillants sur les ordinateurs des clients. Le MSRT est principalement publié sous la forme de mise à jour importante via Windows Update, Microsoft Update et les mises à jour automatiques. Une version de l'outil est également disponible à partir du Centre de téléchargement Microsoft. Le MSRT ne vient pas remplacer une solution antivirus à jour en temps réel.
- Le [Scanner de sécurité Microsoft](#) est un outil de sécurité gratuit à télécharger, qui fournit des analyses à la demande et élimine les programmes et autres logiciels malveillants. Le Microsoft Safety Scanner ne constitue en aucun cas un outil de remplacement pour une solution antivirus à jour. En effet, il n'offre pas de protection en temps réel et ne peut pas empêcher l'infection d'un ordinateur.

NOTE DE BAS DE PAGE

⁴Il est important de noter que ces données sont toujours soumises à des limites strictes de confidentialité et de conformité avant d'être utilisées pour la sécurité.

- **Microsoft Security Essentials** est un produit gratuit de protection en temps réel, facile à télécharger, qui offre une protection basique mais efficace contre les virus et les logiciels anti-espions pour Windows Vista et Windows 7.
- **Microsoft System Center Endpoint Protection** (anciennement Forefront Client Security et Forefront Endpoint Protection) est un produit unifié de protection contre les programmes malveillants et les logiciels indésirables pour les systèmes d'exploitation des serveurs, des ordinateurs portables et des ordinateurs de bureau en entreprise. Il utilise Microsoft Malware Protection Engine et la base de données de signature de l'antivirus Microsoft pour fournir une protection en temps réel, planifiée et à la demande.
- **Office 365** est le service d'abonnement à Microsoft Office pour les entreprises et les particuliers. Certains plans d'abonnement incluent l'accès à Office 365 - Protection avancée contre les menaces.
- **Sécurité Windows** dans Windows 10 fournit l'analyse en temps réel et la suppression des programmes malveillants et des logiciels indésirables. En outre, la dernière version de Windows exploite des données contextuelles riches telles que la [configuration de la machine](#), les performances et l'intégrité de l'appareil, ainsi que d'autres informations de ce type pour améliorer la sécurité des clients. Dans le même temps, nous permettons aux clients d'être mieux informés sur leur confidentialité dans Windows 10. Lisez [ce blog](#) pour en savoir plus sur certaines méthodes utilisées par Microsoft dans ce domaine.
- **Windows Defender Advanced Threat Protection** est un service intégré à la Mise à jour anniversaire Windows 10, et versions ultérieures, qui permet aux entreprises de détecter, d'analyser et d'éliminer les menaces persistantes avancées et les violations de données sur leurs réseaux.
- **Windows Defender hors ligne** est un outil à télécharger qui permet de créer un CD, un DVD ou une clé USB de démarrage pour analyser un ordinateur et y rechercher les éventuels programmes malveillants et autres menaces. Il n'offre pas de protection en temps réel et n'est pas un substitut à une solution anti-programme malveillant à jour.
- **Windows Defender SmartScreen**, une fonctionnalité disponible dans Microsoft Edge et Internet Explorer, offre aux utilisateurs une protection contre les sites de hameçonnage et les sites hébergeant des programmes malveillants. Microsoft tient à jour une base des sites de phishing et d'hébergement de logiciels malveillants signalés par les utilisateurs de Microsoft Edge, d'Internet Explorer et d'autres produits et services Microsoft. Lorsqu'un utilisateur tente de visiter un site figurant dans cette base de données avec le filtre activé, le navigateur affiche un avertissement et bloque la navigation vers la page.