ÉVOLUTION DES CYBER ATTAQUES AU 1ER SEMESTRE 2020

F-Secure

SOMMAIRE

INTRODUCTION

Virus. Quarantaine. Epidémie. Ces mots nous étaient particulièrement familiers du point de vue de la sécurité numérique. En 2020, ils ont aussi pris une toute autre connotation, plus médicale. La pandémie COVID-19 a éclaté, affectant tous les secteurs, y compris la cyber sécurité. Les entreprises ont été contraintes de s'adapter au home office et les équipes informatiques ont dû gérer ces brusques changements.[1] Les technologies favorisant le travail à distance ont connu un développement exponentiel... et leur défauts de sécurité ont été mis en évidence.[2] Parallèlement, des pirates informatiques associés à l'État-nation russe ont commencé à cibler la propriété intellectuelle d'organisations engagées dans la recherche et le développement de vaccins.[3]

Avec le passage au home office, les réseaux professionnels sont devenus plus poreux et leur surface d'attaque a augmenté de manière exponentielle. Des volumes de données colossaux sont désormais physiquement détenus ou accessibles en dehors des frontières traditionnelles des entreprises. Les employés travaillant à distance sont plus susceptibles d'utiliser des appareils et réseaux peu sécurisés. Ils disposent également d'un moindre accès aux équipes de sécurité informatique.[4]

Les pirates informatiques ont su rapidement tirer profit du mot d'ordre « restez chez-vous ». Le secteur a connu une augmentation du phishing pour les identifiants en ligne, un bombardement constant d'e-mails sur le thème de COVID et des niveaux élevés de trafic malveillant vers les ports de bureaux distants. C'est dans ce contexte que nous présentons notre rapport semestriel sur l'évolution des cyber menaces. Ce document présente les malware et les opérations de phishing ciblant les individus et les entreprises.Il fait également le point sur le trafic enregistré par notre réseau mondial de honeypots.

MALWARE : LES DERNIÈRES TENDANCES

Les créateurs de malware sont sans cesse à la recherche de nouvelles stratégies pour contourner les contrôles de sécurité, de manière à passer inaperçus. Ce constat reste valable en 2020 et la crise du COVID-19 a offert aux pirates informatiques de nouvelles opportunités d'attaques.

Méthodes d'infection

La méthode de diffusion de malware la plus courante reste le spam, qui n'a fait que progresser : à ce jour, pour 2020, les e-mails ont représenté 51 % des tentatives d'infection, contre 43 % l'année dernière. La crise du coronavirus a joué un rôle-clé dans cette augmentation : les hackers ont en effet tiré profit de l'inquiétude généralisée en envoyant des spams à ce sujet. Ils ont par ailleurs joué sur l'ingénierie sociale, en s'en prenant à des employés qui, débutant dans le home office, se trouvaient souvent débordés et utilisaient des appareils moins sécurisés. Cette augmentation des spams est sans doute également liée au fait que certains malware, notamment les ransomware, ciblent désormais les entreprises plutôt que les particuliers.

Compte tenu des restrictions organisationnelles courantes (installation gérée des logiciels, accès bloqué à certains sites web), l. Les cracks logiciels contournent les contrôles de licence ou d'autres exigences habituelles. Les applications en pack, comme nous les appelons, sont des applications potentiellement indésirables packagées avec des logiciels légitimes. Alors que ces deux catégories de fichiers représentaient 10% des tentatives d'infection l'année dernière, elles n'ont représenté que 5% pour 2020, jusqu'à ce jour.

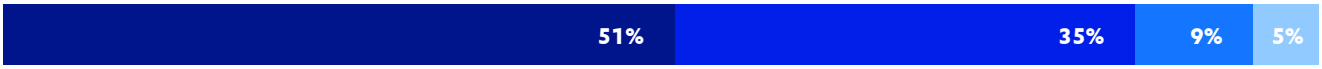
L'utilisation des kits d'exploitation n'a que légèrement diminué, passant de 10 % en 2019 à 9 % cette année. Comparé aux e-mails, l'implémentation des exploits nécessite plus d'efforts de la part des cyber criminels et débouche sur des taux d'infection moindres. Toutefois, dans la mesure où les entreprises ne veillent pas toujours à mettre en place des mesures de correction rapides des vulnérabilités, les exploits continuent de faire partie de la panoplie d'outils des hackers.

35 % des malware (contre 24 % l'année dernière) ont été téléchargés via une charge utile secondaire ou installée manuellement : ces malware ont donc été installés soit par l'utilisateur, soit par le pirate informatique. Cette augmentation peut être liée au fait que les cyber criminels créent des milliers de faux domaines « Zoom » pour tromper les utilisateurs et les amener à télécharger des malware déguisés en logiciels de vidéoconférence. Autre explication : des pirates informatiques installent manuellement un ransomware comme charge utile secondaire après s'être implantés sur le réseau de l'entreprise par le biais d'un port RDP non-sécurisé. Selon plusieurs rapports, les ports RDP vulnérables se sont multipliés lors du passage au home office.

Méthodes de diffusion des malware :

E-mail
Installation manuelle/ Charge utile secondaire
Kit d'exploit / Exploitation de logiciels / Publicité malveillante / Téléchargement Drive-by
Crack logiciels / Applications en pack

1er semestre 2020



Menaces par e-mails

Les cyber criminels ont tout fait pour capitaliser sur la peur et l'incertitude générées par la crise du COVID-19. Spams, tentatives de phishing, pièces jointes malveillantes... Nous avons assisté à un véritable bombardement d'e-mails de différentes natures sur cette thématique.
Nous avons remarqué que, géographiquement parlant, la diffusion des e-mails COVID-19 suivait de près la propagation du virus. Les cyber criminels ont en effet envoyé des e-mails prétendant contenir des informations ou des conseils sur le virus à des utilisateurs se trouvant dans des régions nouvellement touchées.
L'une des premières campagnes d'e-mails malveillants de ce type a été Emotet : celle-ci a visé le le Japon en janvier, après que le pays eut confirmé sa première infection. L'e-mail, supposé provenir d'une autorité de santé publique japonaise, comportait en pièce jointe un guide de prévention. Nous avons ensuite observé des campagnes similaires se propager de manière localisée, là où apparaissait le virus : Lokibot au Vietnam, Remcos à Hong Kong, puis d'autres campagnes ciblant des pays occidentaux comme l'Italie.

Après l'annonce de la première infection COVID au Japon, ce spam Emotet a tiré profit de la situation.

Il peut être intéressant de diviser ces spams COVID-19 en deux catégories : ceux avec et sans pièce jointe. Les e-mails sans pièce jointe sont, pour la plupart, du pur spam sans élément de code malveillant. Il peut s'agir de tentatives de vente de produits douteux ou de masques qui ne seront jamais réellement livrés après commande.

Les e-mails avec pièces jointes, quant à eux, contiennent souvent des documents prétendument importants relatifs au COVID-19, alors qu'il s'agit en réalité de fichiers contenant un code malveillant destiné à télécharger et exécuter des malware. Compte tenu de la crise qu'a connu l'Italie au premier semestre, l'e-mail malveillant que nous avons observé le plus fréquemment sur la thématique du COVID-19 était en italien.

Principaux intitulés des e-mails sur la thématique du COVID sans pièce jointe

1. Informations urgentes concernant sécurité
2. Thermomètre infrarouge sans contact
3. Mesure de la température corporelle : visez le front
4. Masques médicaux dès 0,4 â - 0,5 â'
5. Thermomètre numérique multi-fonctionnel sans contact
6. Suivi de votre température corporelle
7. Le CoronaVirus fait peur ! Respirez plus facilement avec SafeMask
8. Un thermomètre révolutionnaire utilisé par le personnel médical dans le monde entier est désormais accessible au public
9. ALERTE AU CORONAVIRUS : Masques respiratoires gratuits pour les États-Unis
10. Testez vos connaissances pour obtenir 2 cours gratuits sur la santé

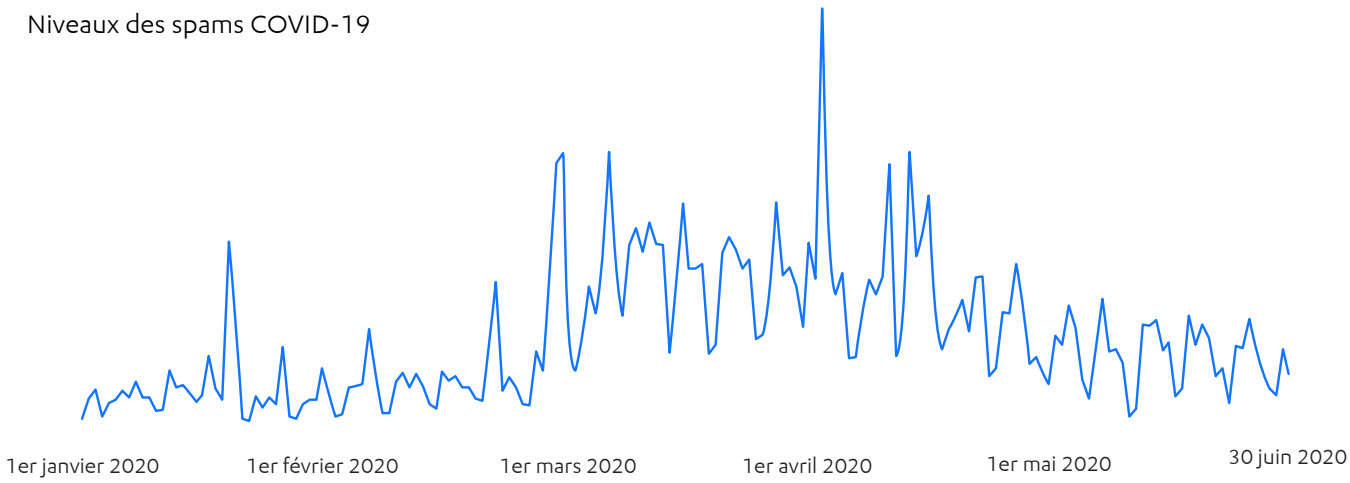
Principaux intitulés des e-mails sur la thématique du COVID avec pièce jointe

1. Coronavirus: Informazioni importanti su precauzioni
   (« Coronavirus : Informations importantes sur les précautions à prendre »)
2. Standard Bank : Fonds d'allègement des paiements COVID-19 approuvé
3. Fonds de secours d'urgence en ligne Absa
4. MISE À JOUR COVID-19 - NSL Analytical Services
5. Coronavirus : information importante concernant les précautions à prendre pour les entreprises
6. Soutien d'urgence en ligne Absa
7. Réponse du gouvernement au coronavirus COVID-19
8. Coronavirus (COVID-19)
9. Relevés eStatements Absa.pdf
10. COVID-19 USA

75 % des pièces jointes des e-mails observés diffusaient soit Lokibot, soit Formbook. Ces infostealers ont été retrouvés dans 38 % et 37 % des pièces jointes COVID respectivement. Les campagnes de spams avec pièce jointe contenaient généralement des fichiers .doc, .zip et .pdf. Cependant, suivant une tendance déjà initiée en 2019, nous avons remarqué un pourcentage faible mais constant de malware déguisés en fichiers ISO ou IMG qui, à leur tour, démarraient un fichier exécutable. Agent Tesla, par exemple, est un RAT se propageant via un fichier ISO joint à un e-mail de demande de devis.

Nous avons également observé des fichiers d'archive et de compression atypiques, tels que .gz et .ace, utilisés pour contourner les passerelles de messagerie capables de détecter les exécutables malveillants contenus dans des formats plus conventionnels de type .zip.

Niveaux des spams COVID-19



C'est en mars, avril et début mai que les niveaux de spams COVID-19 ont été les plus élevés, ce après quoi la tendance s'est poursuivie à un rythme plus modéré. Les utilisateurs ont gagné en vigilance face aux fraudes liés à la pandémie et les hackers en sont revenus à leurs spams de prédilection : les faux e-mails relatifs aux livraisons et aux factures. En juin, nous avons également observé certains spams capitalisant sur le mouvement Black Lives Matter pour diffuser Trickbot.

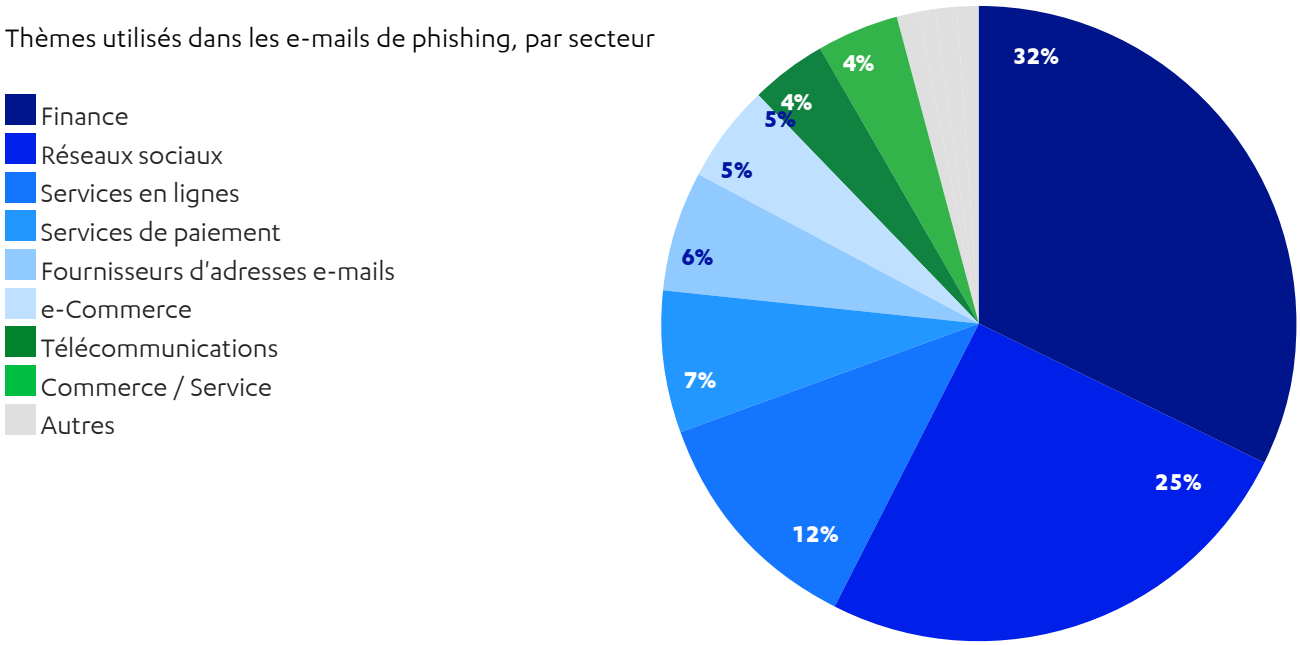
Phishing

Les e-mails de phishing prétendent provenir d'une source de confiance. Ils visent à convaincre l'utilisateur de fournir des informations personnelles ou de cliquer sur un lien ou une pièce jointe malveillante. Parmi les e-mails de phishing reçus par nos instruments de mesure durant cette période, la majorité (19 %) imitait Facebook. Les sociétés financières ont elles aussi été la cible de ces usurpations d'identité : plusieurs banques ont ainsi représenté, ensemble, 32% des usurpations.

Entreprises dont l'identité a été usurpée dans les attaques de phishing

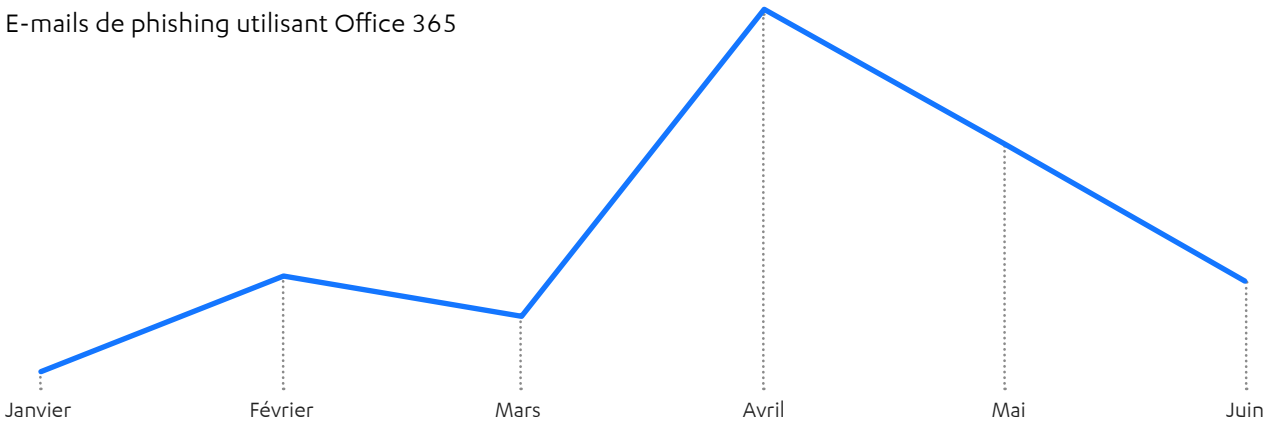
Facebook, Inc.	19%
Chase Personal Banking	11%
Microsoft Office365	6%
PayPal Inc.	6%
Bank of America	5%
WhatsApp	4%
Webmail Providers	3%
Wells Fargo & Company	3%
Amazon.com Inc.	2%
Apple Inc.	2%
eBay Inc.	2%
Itau Unibanco S.A	2%
Netflix Inc.	2%
Adobe Inc.	1%
Alibaba	1%
Americanas.com S/A Comercio Electronico	1%
Bancolombia	1%
Canadian Imperial Bank of Commerce	1%
DHL Airways, Inc.	1%
Google Inc.	1%
LinkedIn Corporation	1%
Orange	1%
Outlook	1%
Steam	1%
Autres	23%

Thèmes utilisés dans les e-mails de phishing, par secteur

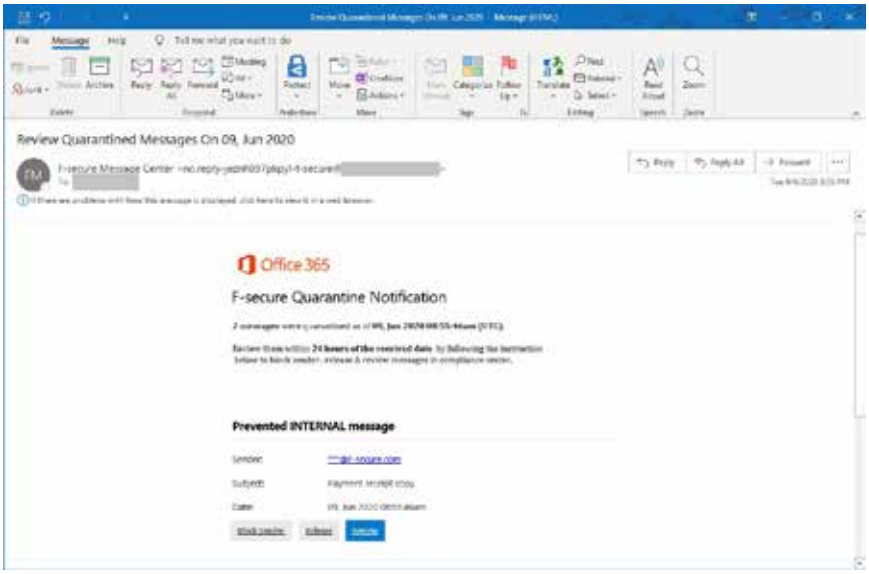


Au cours de l'année passée, le secteur a connu une augmentation globale des attaques utilisant les fournisseurs de messagerie cloud tels que Microsoft Office 365. Les cyber criminels font évoluer leurs méthodes de phishing et de vol d'identifiants pour s'adapter à la migration généralisée vers les services en ligne. Cette évolution du phishing ne devrait que se confirmer, à mesure que cette migration cloud s'accélérera pour répondre aux besoins des travailleurs à distance.

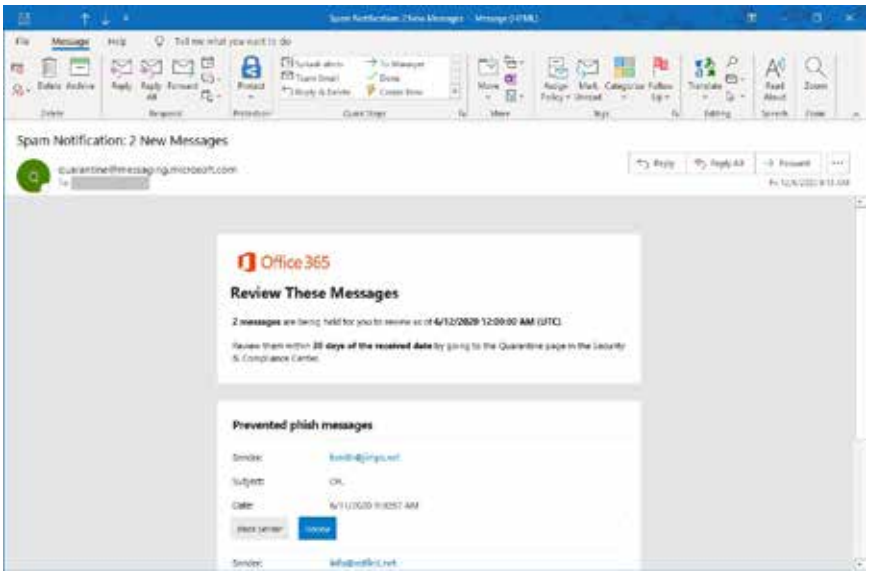
E-mails de phishing utilisant Office 365



Les campagnes de phishing ciblant les services cloud comme Office 365 sont efficaces car les utilisateurs sont habitués à recevoir des notifications de la part de ces services, surtout s'ils font partie de l'infrastructure logicielle de l'organisation. Les fausses notifications envoyées par les cyber criminels concernent généralement des échecs de livraison, des alertes de dépassement des limites de stockage, des notifications de quarantaine, des demandes de réactivation ou des e-mails de « mise à jour de votre mot de passe ».



Faux e-mail d'examen de la quarantaine



E-mail d'examen de la quarantaine Office 365 authentique

À l'origine, les attaques de phishing ont été créées avec un objectif : tromper l'utilisateur final pour offrir au hacker un accès illimité au compte de messagerie ciblé et aux services auxquels la victime est autorisée à accéder. Désormais, pour obtenir un accès encore plus large, les cyber criminels lancent de plus en plus fréquemment des attaques ciblées de spear phishing à l'encontre des administrateurs de Microsoft Office 365. Ces attaques, si elles réussissent, permettent au au pirate informatique d'obtenir un contrôle administratif total sur le domaine et sur tous les comptes Office 365 de l'entreprise.

Des attaques de phishing similaires ont été observées contre d'autres services de messagerie cloud, comme Gmail et G-Suite de Google. Compte-tenu de la prévalence des comptes Google et de la façon dont ils sont utilisés pour se connecter à divers sites web, il n'est pas surprenant qu'ils soient aussi la cible d'attaques de phishing spécifiques.

Familles de menaces

Notre classement des principales menaces se base sur des données provenant à la fois de nos instruments de détection et de flux de menaces externes. Les infostealers et les chevaux de Troie d'accès à distance (RAT) occupent une place prépondérante dans ce top 20. Ils doivent notamment leur « succès » aux e-mails sur le thème du coronavirus. Les deux infostealers les plus fréquemment rencontrés ont été Lokibot et Formbook. Les RAT les plus répandus ont été Remcos et Ave Maria.

Emotet continue à jouer un rôle de premier plan. Après avoir débuté comme cheval de Troie bancaire, ce malware a évolué en menace beaucoup plus modulaire intégrant des capacités de botnet. Aujourd'hui, nous voyons Emotet se déployer en malware primaire : il est distribué principalement par le biais de pièces jointes, dans le cadre de campagnes de spams d'envergure. Emotet est connu pour introduire des chevaux de Troie bancaires tels que Trickbot et Qakbot, et des ransomware tels que Ryuk.

Top 20 des principaux malware

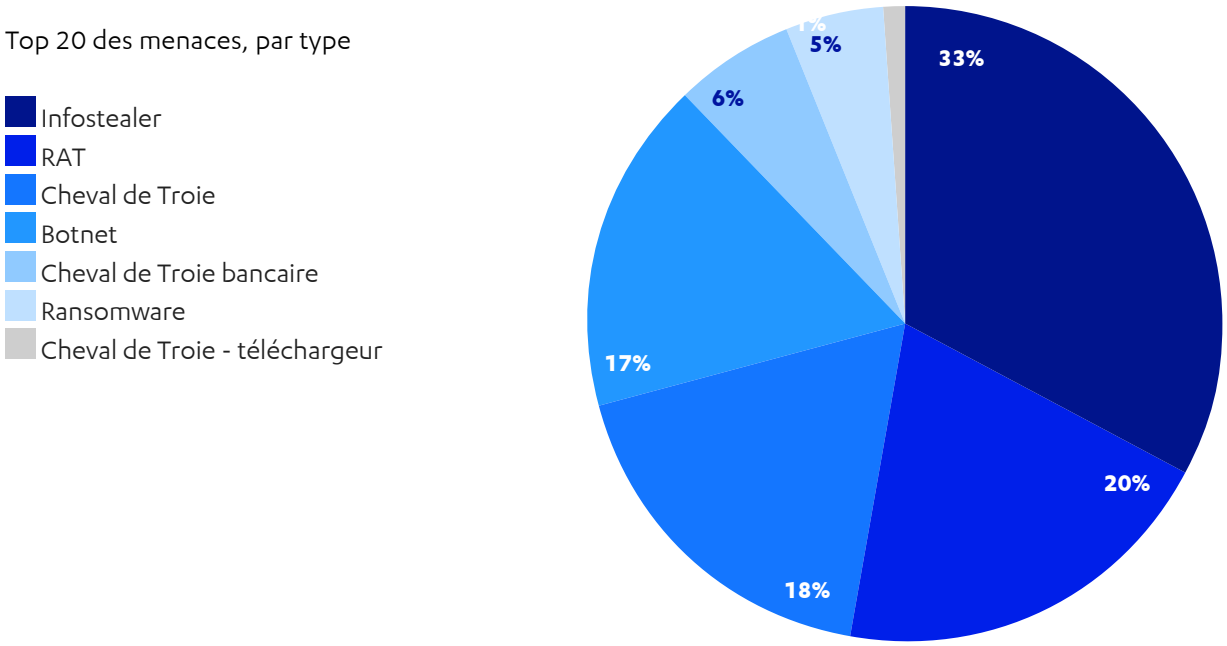
NOM		TYPE
1.	Lokibot	Infostealer
2.	Emotet	Botnet
3.	Generic behavior*	Cheval de Troie
4.	Formbook	Infostealer
5.	Remcos	RAT
6.	Ave Maria	RAT
7.	Ransomware	Ransomware
8.	Agent Tesla	RAT
9.	Trickbot	Ch. de Troie bancaire
10.	Qakbot	Ch. de Troie bancaire
11.	NanoCore	RAT
12.	Netwire	RAT
13.	Raccoon	Infostealer
14.	Ursnif	Ch. de Troie bancaire
15.	AZORult	Infostealer
16.	GULoader	Ch. Troie téléchargeur
17.	IcedID	Cheval de Troie
18.	Malicious Packer	Cheval de Troie
19.	njRAT	RAT
20.	DarkComet	RAT

* « Comportement générique » fait référence aux malware ne correspondant pas directement à une famille de menaces connues mais qui affichent un comportement malveillant typique tel que le dépôt de fichiers supplémentaires, la modification des clés de registre ou la connexion à internet pour télécharger d'autres fichiers.

MALWARE : GLOSSAIRE

Botnet : Ensemble des appareils infectés par un programme de bot, qui permet à un pirate informatique de contrôler chaque appareil individuellement, ou de piloter collectivement tous les appareils infectés.
Exploit : Programme tirant profit d'une vulnérabilité présente sur une application ou un système d'exploitation pour exécuter une action non-autorisée telle que la livraison d'une charge utile malveillante.
Infostealer : Programme conçu pour voler des informations sensibles et confidentielles telles que des identifiants et des mots de passe à partir d'un système infecté.
Ransomware : Logiciel malveillant prenant le contrôle des données ou de l'appareil de l'utilisateur. Le hacker exige ensuite une rançon.
Cheval de Troie d'accès à distance : Programme permettant à un hacker de contrôler le système d'une victime à distance et d'exécuter des commandes.
Cheval de Troie : Fichier ou programme en apparence inoffensif mais qui effectue secrètement des actions pouvant nuire à votre appareil, à vos données ou à votre vie privée.
Cheval de Troie bancaire : Cheval de Troie utilisant diverses techniques telles que le vol d'identifiants pour surveiller ou intercepter les sessions bancaires en ligne.
Cheval de Troie téléchargeur : Cheval de Troie contactant un serveur distant pour télécharger d'autres programmes malveillants.

Top 20 des menaces, par type



Les ransomware n'ont représenté que 5 % des familles de notre top 20 des familles de menaces, un chiffre trompeur qui s'explique par la manière dont ces logiciels malveillants se diffusent. Plutôt que de les utiliser comme charge utile primaire, les pirates informatiques injectent généralement les ransomware dans un second temps, après avoir introduit un malware primaire comme Emotet. Comme nos technologies de protection des endpoints détectent et bloquent la charge utile primaire, le ransomware qui aurait suivi n'est jamais téléchargé ni exécuté : de ce fait, ces incidents n'apparaissent pas dans nos mesures.

Certaines familles de menaces exploitent des vulnérabilités logicielles pour s'implanter sur les réseaux. Black Kingdom utilise par exemple un exploit pour cibler les organisations ayant omis de corriger la récente vulnérabilité de Pulse Secure VPN. Les ransomware Nefilim et Sodinokibi/REvil ciblent quant à eux les vulnérabilités des serveurs Citrix. D'autres familles de ransomware, enfin, utilisent des RDP non-sécurisés pour accéder aux réseaux des entreprises.

En 2020, les hackers recourant aux ransomware procèdent comme suit : ils s'infiltrent un réseau, exfiltrent le plus de données possible et, enfin, déploient un ransomware pour chiffrer les données. Pour les entreprises, la prise en otage des données n'est alors plus le seul risque : les pirates peuvent également menacer de publier ces données, ce qui constitue un moyen de pression supplémentaire pour le paiement de la rançon. Si les entreprises refusent de payer la rançon, elles seront tout de même confrontées à des problèmes financiers, du fait de poursuites judiciaires émanant des clients ou des amendes du RGPD résultant de fuites de données.

En dehors de ce top 20, les principales menaces relevées sont des chevaux de Troie génériques ou des menaces dont le volume n'est pas significatif.

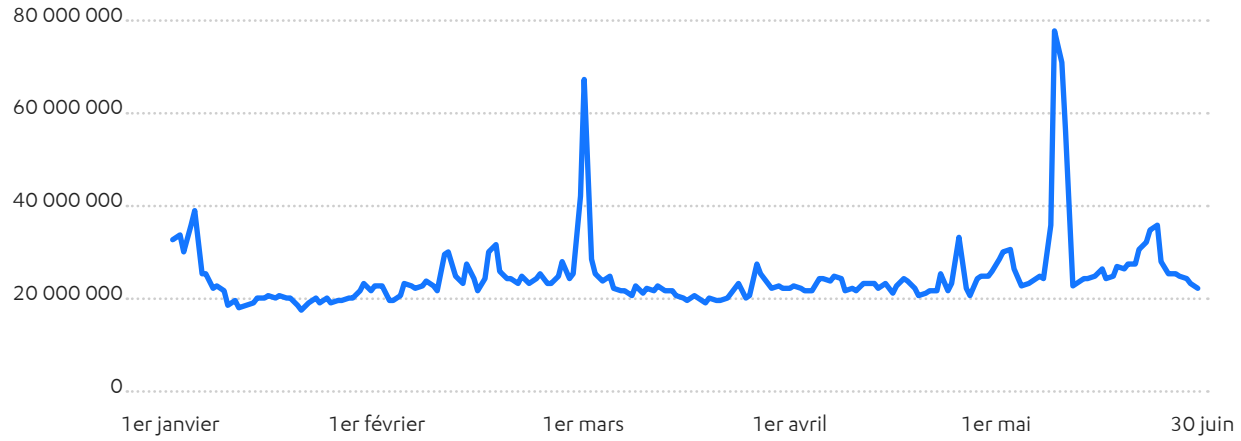
HONEYPOTS : QUI ATTAQUE QUI ?

Les malware et les attaques de phishing ciblent les systèmes-clients. Notre réseau mondial de honeypots, lui, nous permet de porter nos observations au niveau du trafic réseau, pour couvrir un large éventail d'activités. Ce réseau enregistre les actions des hackers qui recherchent des postes de travail vulnérables sur l'internet ouvert. Il scrute les tentatives d'intrusion et de piratage de ces systèmes.

Nos honeypots ont enregistré des niveaux de trafic presque identiques à ceux de l'année dernière. Au total, le réseau a enregistré plus de 2,8 milliards de visites au cours du premier semestre de cette année, contre 2,9 milliards au premier semestre de l'année dernière et 2,8 milliards au second semestre 2019. En temps normal comme en temps de pandémie, les hackers n'hésitent donc pas à poursuivre leurs activités.

Tout au long du semestre, l'activité est restée presque constante. Des pics importants ont toutefois été relevés à la mi-mars et au début du mois de juin, avec des campagnes DDoS par réflexion ciblant le port UDP 1900, qui est le port par défaut des protocoles d'identification des périphériques réseau UPnP et SSDP. Une grande partie de ces attaques ont frappé la Chine, et la majorité d'entre elles provenaient des espaces IP chinois, brésilien, américain et singapourien.

Trafic de honeypot au premier semestre



Parmi les pays dont les espaces IP ont généré les niveaux de trafic les plus élevés vers nos honeypots, nous trouvons la Chine, les États-Unis et la Russie. Viennent ensuite les Pays-Bas, Hong Kong, le Brésil, l'Allemagne, l'Ukraine et Singapour. Tous ces pays s'avèrent être des sources de trafic habituelles. L'Irlande, à l'inverse, présente un trafic inhabituellement élevé et se place en troisième position.Le trafic provenant de l'espace IP irlandais a principalement ciblé le SSH. Il a été constant tout au long de la période et s'est réparti sur plusieurs pays-cibles.

QU'EST-CE QU'UN HONEYPOT ?

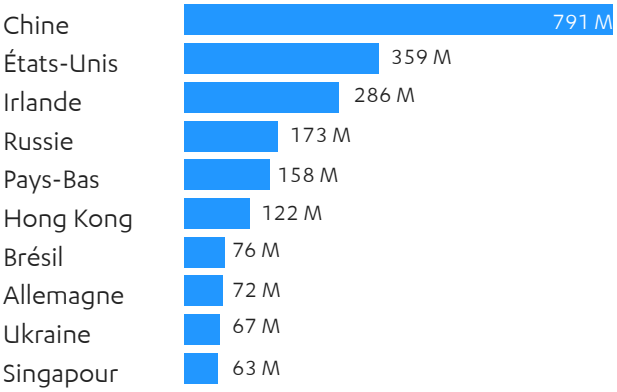
Nos honeypots sont des serveurs actifs dans le monde entier et destinés à leurrer les pirates informatiques pour mieux les connaître. Ces serveurs cherchent plus précisement à mesurer les activités potentiellement malveillantes. Toute connexion entrante enregistrée par un honeypot est considérée comme suspecte car elle résulte probablement de scans d'internet par un pirate informatique. Cela étant, de rares adresses IP mal saisies peuvent également déclencher l'enregistrement d'une connexion.

Plus de 99 % du trafic vers nos honeypots est un trafic automatisé provenant de bots, puisque ces derniers peuvent effectuer des tâches secondaires de manière répétée. Les interactions enregistrées peuvent provenir de n'importe quel type de dispositif connecté infecté comme un ordinateur traditionnel, une montre intelligente ou encore une brosse à dents connectée.

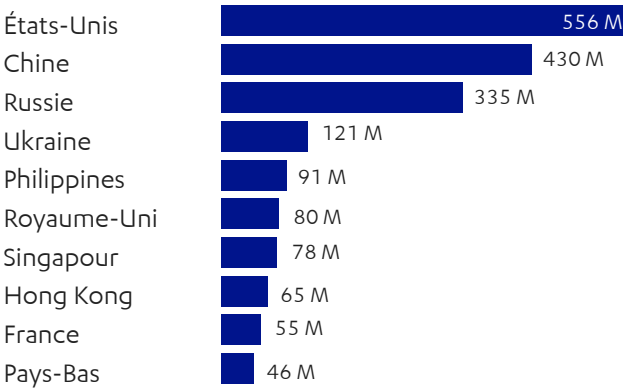
Nos honeypots enregistrent tout type d'interactions, qu'il s'agisse d'un simple ping exploratoire ou d'un accès complet au service.

Les principaux pays-sources figurent dans ce classement pour plusieurs raisons. De manière générale, ils occupent une présence importante sur internet. Les pirates informatiques ont par ailleurs tendance à utiliser des hôtes dans des pays autres que celui où ils se trouvent, avec des lois moins strictes ou moins efficaces en matière de cyber criminalité, pour courir moins de risques d'être retrouvés ou poursuivis. Les hackers tendent également à cibler des serveurs situés dans des régions dans lesquelles le matériel et les logiciels informatiques sont perçus comme plus vulnérables, de manière à faciliter les piratages et la propagation des attaques.

Principaux pays-sources - 1er semestre 2020



Principaux pays-sources - 2nd semestre 2019

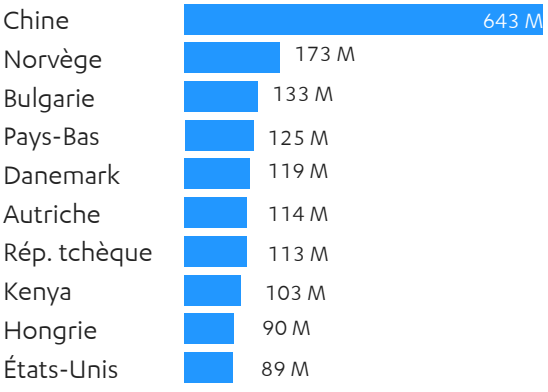


Une portion significative du trafic issu des principaux pays-sources (notamment la Chine elle-même) ciblait l'espace IP chinois. La Chine a été le premier pays-cible des attaques ; la Norvège, le second.

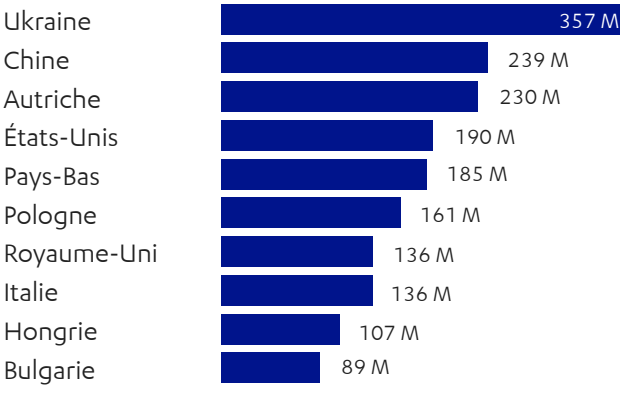
> La liste des pays-sources doit être considérée avec beaucoup de précaution, car les pirates informatiques peuvent faire passer leurs attaques via des proxys dans d'autres pays, afin d'éviter d'être identifiés par les autorités. Nous ne cherchons pas non plus à insinuer que ces activités relèvent des États-nations eux-mêmes. La majorité de ces attaques sont lancées par des cyber criminels menant des attaques DDoS et diffusant des malware dans un but lucratif.

Pour mieux comprendre pourquoi l'espace IP norvégien est aussi visé, il peut être utile de noter que le pays a récemment connu plusieurs piratages très médiatisés : celui de Norsk Hydro en 2019 et ceux du constructeur naval VARD, du revendeur de pièces automobiles MECA/Mekonomen et du fonds d'investissement Norfund en 2020. Cette augmentation du trafic est donc peut-être une coïncidence, ou bien le résultat d'une exposition médiatique accrue.

Principaux pays-cibles - 1er semestre 2020



Principaux pays-cibles - 2nd semestre 2019

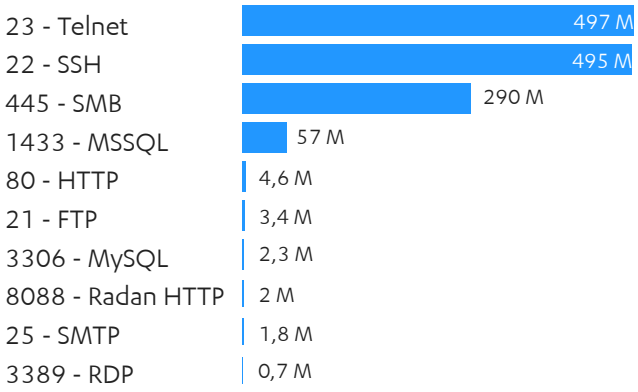


Ports et protocoles

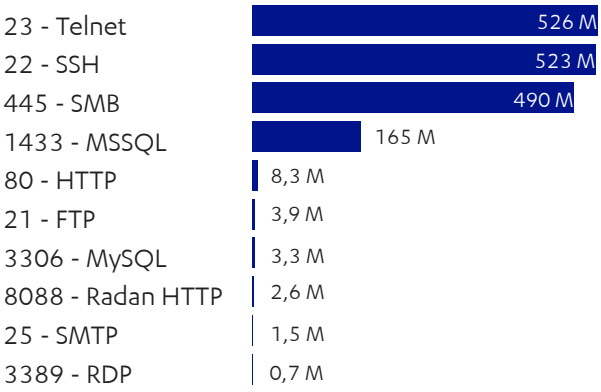
Dans leur grande majorité, les principaux ports ciblés au premier semestre 2020 sont les mêmes qu'au second semestre 2019. Les deux principaux ports concernés, les ports 23 et 22, renvoient respectivement à des tentatives d'accès distant au serveur via le protocole Telnet non-chiffré et via le protocole SSH, plus sécurisé. Les versions les plus courantes des attaques Telnet et SSH reposaient sur des tentatives d'authentification en tant qu'utilisateur local, via des combinaisons de noms d'utilisateurs et de mots de passe répandus.

Même s'il reste encore trop largement utilisé, notamment sur les serveurs et les objets connectés, le protocole Telnet est en recul par rapport à 2019. Une grande partie du trafic Telnet est liée à Mirai, dont les variantes ont constitué la grande majorité des malware répertoriés par nos honeypots.

Principaux ports TCP ciblés au 1er semestre 2020



Principaux ports TCP ciblés au 2nd semestre 2019



En troisième position sur la liste, se trouve le port 445 qui correspond aux connexions SMB. Ce trafic se trouve également à un niveau inférieur à celui de 2019. Le trafic SMB concerne les tentatives d'upload de données malveillantes à des fins d'exploitation ainsi que les tentatives d'exfiltration de données. Une partie de ce trafic continue à capitaliser sur la vulnérabilité EternalBlue. Quelques autres vulnérabilités liées au protocole SMB ont été révélées cette année, comme SMBGhost et SMBleed. Il est donc probable que les vulnérabilités SMB restent activement ciblées.

Le trafic ciblant le port 1433, MSSQ, apparaît en quatrième position. Ce port correspond aux attaques de base de données (comme les injections SQL), au cryptomining, aux backdoors d'accès à distance et aux ransomware. Le trafic MSSQL est également inférieur à celui enregistré en 2019.

Les attaques ciblant le protocole HTTP concernent plusieurs activités parmi lesquelles : le scraping de fichiers sensibles ou de pages de sites web qui auraient dû être restreintes ou supprimées ; l'upload de fichiers malveillants pour s'implanter sur un serveur ; l'énumération des partages réseau cachés ; le flooding des ressources de serveur ; l'injection de commandes et les attaques par réflexion.

Les attaques basées sur le protocole FTP téléchargent divers fichiers malveillants, dont des cryptominers. Ces attaques sont également souvent associées à des commandes d'accès à distance intégrées à des scripts automatisés.

Dans le cas des attaques ciblant la messagerie (SMTP), nous avons le plus souvent observé des tentatives de distribution de charges utiles malveillantes et d'énumération des utilisateurs, ainsi que diverses tentatives de spam ou de phishing.

Le travail à distance se généralise dans le monde entier et les entreprises font tout pour s'adapter rapidement.[1] Malheureusement, plusieurss rapports font état d'une augmentation des attaques RDP. Ces attaques ciblant les connexions vulnérables du protocole RDP (Remote Desktop Protocol) sont souvent des tentatives de connexion par force brute utilisant des identifiants obtenus sur le dark web. La vulnérabilité BlueKeep, révélée à la fin du printemps 2019, est probablement liée à une partie du trafic RDP observé ici.[2]

Le port UDP 1900 a connu un trafic important avec près de 85 millions de visites. Ce trafic a majoritairement eu lieu durant les campagnes de mars et juin mentionnées précédemment. Le port 1900 est utilisé à la fois par les protocoles SSDP et UPnP, qui permettent aux appareils et aux services de s'identifier les uns les autres et de communiquer sans configuration préalable. Ces protocoles permettent le partage des données ainsi que les communications et la diffusion en continu sur un réseau donné. Largement destinés aux petits environnements domicile et bureau, les protocoles SSDP et UPnP sont extrêmement répandus et exécutés sur des millions d'appareils dans le monde entier, notamment les routeurs, les imprimantes et les objets connectés. Malheureusement, en raison de leur faible degré de sécurité intrinsèque et de l'utilisation du routage multicast où un seul paquet réseau peut être transmis simultanément vers plusieurs destinations, ces deux protocoles sont souvent utilisés pour mener des attaques de piratage à grande échelle, comme celles subies par Amazon Web Services et par Akamai[2], le fournisseur mondial de CDN, au cours du premier semestre 2020.

1 https://www.rapid7.com/research/report/nicer-2020/
2 https://blogs.akamai.com/2020/06/akamai-mitigates-sophisticated-144-tbps-and-385-mpps-ddos-attack.html

CONCLUSION

Les hackers ont capitalisé sur le virus du COVID-19. Ils n'ont pas hésité à tirer profit des craintes liées à cette pandémie pour maximiser leurs revenus. Les cyber menaces observées au premier semestre 2020 en sont la preuve. Et ils n'entendent pas s'arrêter là. Ils développent actuellement leurs programmes d'affiliation et mènent des campagnes de recrutement[3]. Reste à voir quels vecteurs d'attaque ils entendent utiliser en ce second semestre.

Les pirates informatiques sont capables de s'adapter à de nouvelles situations en adaptant sans cesse leurs stratégies aux thématiques d'actualité. Malheureusement, le secteur de la santé n'a pas été épargné et continue de faire face à des cyber attaques alors même qu'il se bat en première ligne.[4] Il est toutefois rassurant de noter que des bénévoles du secteur de la cyber sécurité se portent volontaires pour aider à sécuriser les établissements de santé en cette période de crise. [5]

Pour se protéger des menaces, les entreprises doivent adhérer aux bonnes pratiques et aux recommandations générales fournies par les professionnels de la cyber sécurité : installer les mises à jour et correctifs, verrouiller les services vulnérables, tenter de séparer l'environnement informatique professionnel des employés de leur environnement personnel, rester toujours vigilant face aux campagnes de spams ou de phishing et, enfin, sensibiliser les employés sur ces campagnes. Les entreprises trouveront des conseils plus détaillés pour sécuriser le travail à distance dans les guides spécifiques au COVID.

Les professionnels de la cyber sécurité doivent s'efforcer de réduire le taux de réussite des attaques par e-mails en optimisant les technologies, en amenant les entreprises à faire évoluer leur stratégie et en favorisant la formation. Nous avons beaucoup à faire pour sensibiliser le monde aux dangers omniprésents des cyber menaces. Mais l'avenir n'a pour autant rien de morose : si la pandémie du COVID-19 nous a appris quelque chose, c'est bien que chacun peut jouer un rôle pour rendre le cyber monde plus sûr.

3 https://www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/
4 https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic
5 https://www.csoonline.com/article/3539319/legions-of-cybersecurity-volunteers-rally-to-protect-hospitals-during-covid-19-crisis.html

À PROPOS DE F-SECURE

Fondée en 1988, F-Secure est une entreprise finlandaise spécialisée en cyber sécurité, cotée au NASDAQ OMX Helsinki Ltd. Depuis plus de trente ans, nous protégeons des dizaines de milliers d'entreprises et des millions de particuliers grâce à notre réseau de partenaires de distribution, et plus de 200 fournisseurs de services. Des solutions de protection des postes de travail à la détection et réponses aux menaces avancées, nous veillons à ce que nos utilisateurs puissent compter sur une cyber sécurité de haut-niveau. L'alliance unique de l'expertise humaine, de solutions logicielles et d'intelligence artificielle nous permet d'être reconnu comme un acteur incontournable du marché européen.

f-secure.com/fr_FR/ | **twitter.com/fsecurefrance** | **linkedin.com/company/f-secure-corporation**

F-Secure