



HORNETSECURITY

CYBERTHREAT REPORT

2ND EDITION 2020

L'année 2020 nous a confronté à plusieurs défis: aussi bien d'un point de vue sanitaire qu'économique. La pandémie du coronavirus a mis à l'épreuve l'humanité, le mouvement «black lives matter» a permis une nouvelle sensibilisation politique de la société et de nouvelles menaces sont apparues dans le monde digital.

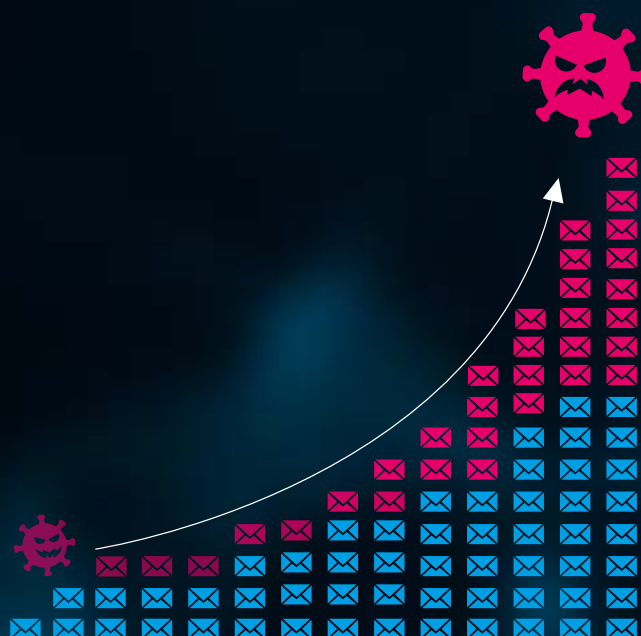
Dans le **Cyberthreat Report 2nd Edition 2020**, les experts informatiques d'Hornetsecurity s'intéressent de plus près à la **porte d'entrée qu'est la communication par e-mail** et analysent les outils et méthodes les plus récents et fréquents des cybercriminels. Quels nouveaux dangers sont apparus en 2020 et à quoi doivent se préparer les entreprises dans le futur lors de l'ouverture de leur boîte de réception?

Risque de cybersécurité: la communication par e-mail

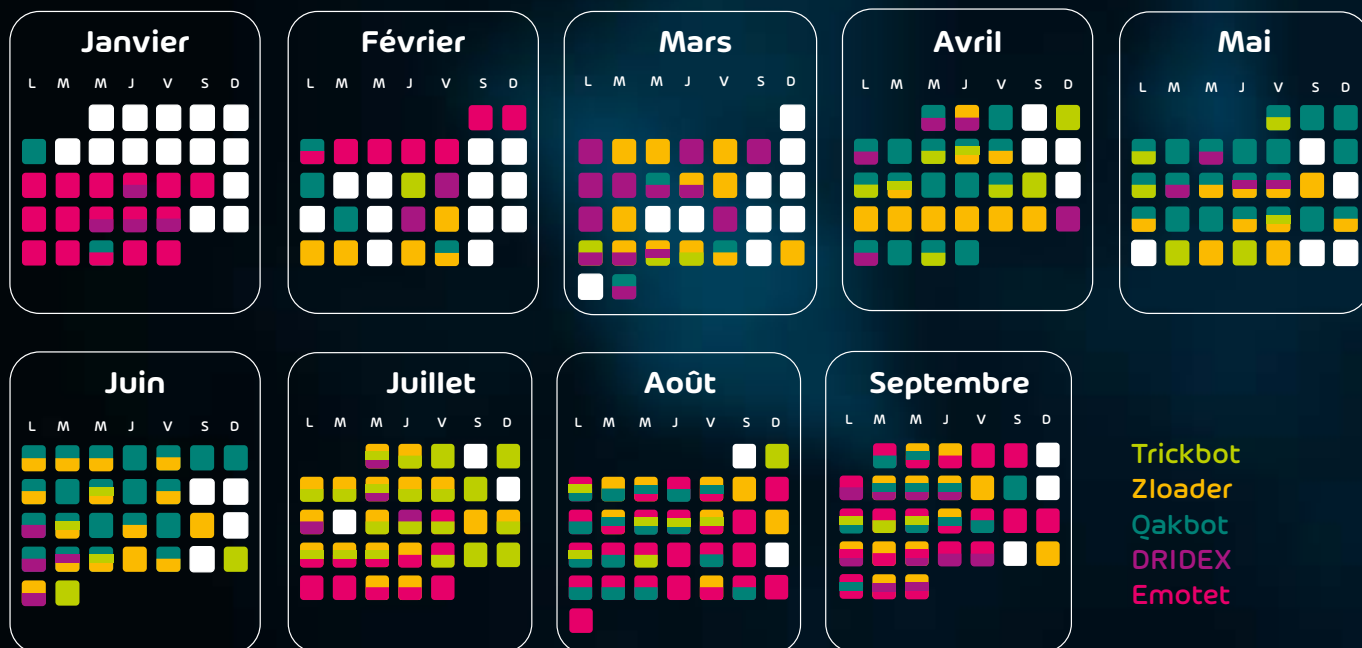
La communication par e-mail reste la porte d'entrée principale des cyberattaques. Dans son étude relative aux cyberattaques contre les entreprises de taille moyenne, le «Gesamtverband der deutschen Versicherer» est arrivé à la conclusion que **deux tiers des attaques réussies pénétraient dans les systèmes des entreprises via les e-mails**. Par des méthodes perfides, les hackers entraînent le destinataire à ouvrir des pièces-jointes dangereuses, à cliquer sur des liens inconnus ou même à effectuer des transactions financières.¹



III. 1: part des logiciels malveillants dans l'ensemble du trafic analysé des e-mails



Les logiciels malveillants constituent, qu'on le veuille ou non, la cybermenace la plus redoutée. Ces dernières années, WannaCry, Petya et Emotet ont clairement montré que les logiciels malveillants étaient tout à fait en mesure **d'échapper aux mesures de sécurité des entreprises**. Dans certains cas, les cyberattaques ont des conséquences dramatiques: de l'interruption de l'activité à la faillite.



III. 2: diffusions de logiciels malveillants durant la période entre janvier et septembre 2020

Les analystes Security d'Hornetsecurity ont analysé des e-mails réceptionnés et catégorisés comme malveillants pendant une période allant de janvier et septembre 2020. Ils ont identifié les logiciels malveillants les plus connus actuellement comme Emotet, Zloader, Dridex, Qakbot et Trickbot. Nous allons nous y intéresser brièvement dans ce qui suit:

Emotet: le grand comeback

Le cheval de Troie tristement célèbre Emotet est réputé pour des **attaques de hackers particulièrement graves sur des entreprises** – le BSI l'a même désigné comme le «logiciel malveillant le plus dangereux au monde». Les techniques d'attaques de ce cheval de Troie s'étendent de l'hijacking de conversations par e-mail aux modifications du shell Web en passant par les pièces-jointes chiffrées en malspam. Des menaces que les filtres antivirus usuels repoussent généralement avec succès.

Le groupe cybercriminel à l'origine d'Emotet a stoppé sa diffusion le 7 février de cette année. Ce n'est pas inhabituel, car depuis l'identification du programme malveillant en 2014, il y a eu plusieurs périodes durant lesquelles aucun spam malicieux Emotet n'a été envoyé. Pendant la période d'inactivité, les analystes Security ont enregistré les modifications du loader d'Emotet et sur cette base, le Hornetsecurity Security Lab a pronostiqué le retour imminent du logiciel malveillant. Ces prévisions se sont vérifiées le 17 juillet et le botnet Emotet a repris ses activités.²

ZLoader:

Zloader est issu d'une scission avec le cheval de Troie bancaire Zeus. Les premières versions ont été découvertes en novembre 2019. Cette année, les cybercriminels ayant créé Zoader ont réutilisé une ancienne technique d'attaque redécouverte, les **macros XLM**, et ont diffusé ainsi ce maliciel. Le Hornetsecurity Security Lab a été l'un des premiers à identifier cette nouvelle opération de diffusion de Zloader utilisant des macros XLM à grande échelle. Alors que la diffusion a débuté doucement, des spams malicieux sont désormais envoyés quotidiennement. Les acteurs à l'origine du logiciel malveillant Zloader arrivent à créer régulièrement des documents Excel malicieux **qui ne sont reconnus par aucun logiciel antivirus**.

[Digression] Les macros XLM: faire du neuf avec du vieux?

Les macros XLM sont un langage macro présenté pour la première fois dans Excel 4 en 1997. En février 2020, le Security Lab a découvert une mystérieuse campagne de spam révélant l'utilisation de ces macros. Les hackers envoient des e-mails avec des archives Zip en fichier-joint. Lors de la décompression du document, une boîte de dialogue s'ouvre sur l'ordinateur de la victime «Nous avons trouvé un problème avec le

contenu. Voulez-vous essayer d'en récupérer autant que possible?» Si l'utilisateur clique sur «OK», le document utilise une Excel Web Query afin de télécharger un code macro. Ce code macro télécharge à son tour un fichier exécutable qui lance l'application « calculatrice » de Windows. Dans ce cas, le Security Lab part du principe que le démarrage de la calculatrice a été intégré en tant que technique de contournement de l'analyse ou en tant qu'erreur intentionnelle, afin que le logiciel malveillant devant être introduit via les macros Excel 4, reste invisible pendant aussi longtemps que possible.

Dridex:

Ce cheval de Troie a été découvert pour la première fois en 2011. Cependant, son pic d'activité a été enregistré par les analystes en mars 2020: la forte hausse de ses activités est due à plusieurs campagnes de spams malveillants contenant un fichier Excel (.xlsm) frauduleux en pièce-jointe. L'objectif primaire de Dridex est **d'infiltrer les ordinateurs et de dérober les données bancaires** afin d'effectuer des virements aux hackers responsables.³

Qakbot:

Qakbot est un «Information Stealer» modulaire également connu sous le nom «Qbot» et «Pinksliipbot». Il est actif déjà depuis 2007. Cependant, à l'origine, il s'agissait d'un cheval de Troie bancaire. Dès que Qakbot a infecté le système de sa victime, les exploitants du maliciel peuvent **lancer des logiciels malveillants supplémentaires**. Depuis avril, le Security Lab a remarqué une diffusion plus importante de Qakbot via des spams malicieux contenant un lien frauduleux entraînant le téléchargement d'une archive ZIP comprenant elle-même un VBScript et installant finalement Qakbot sur le système concerné. Depuis mars 2020, Qakbot installe le ransomware ProLock. Le FBI et les CERT mettent en gardent contre cette combinaison dangereuse.⁴

Trickbot:

Au plus tard depuis l'apparition du dangereux trio Emotet, Trickbot et Ryuk, TrickBot est sorti de son anonymat relatif. À l'origine, il s'agissait d'un cheval de Troie bancaire réunissant cependant des fonctionnalités modulaires. Dans la plupart des cas, il s'introduit dans les réseaux informatiques via Emotet. Ensuite, tous les **programmes de protection sont tout d'abord désactivés et Trickbot récupère les droits d'administration**. Des exemples d'envois de TrickBot durant le deuxième semestre de cette année sont les campagnes de maliciels en lien avec le coronavirus⁵ ainsi qu'ensuite le mouvement «black lives matter».⁶

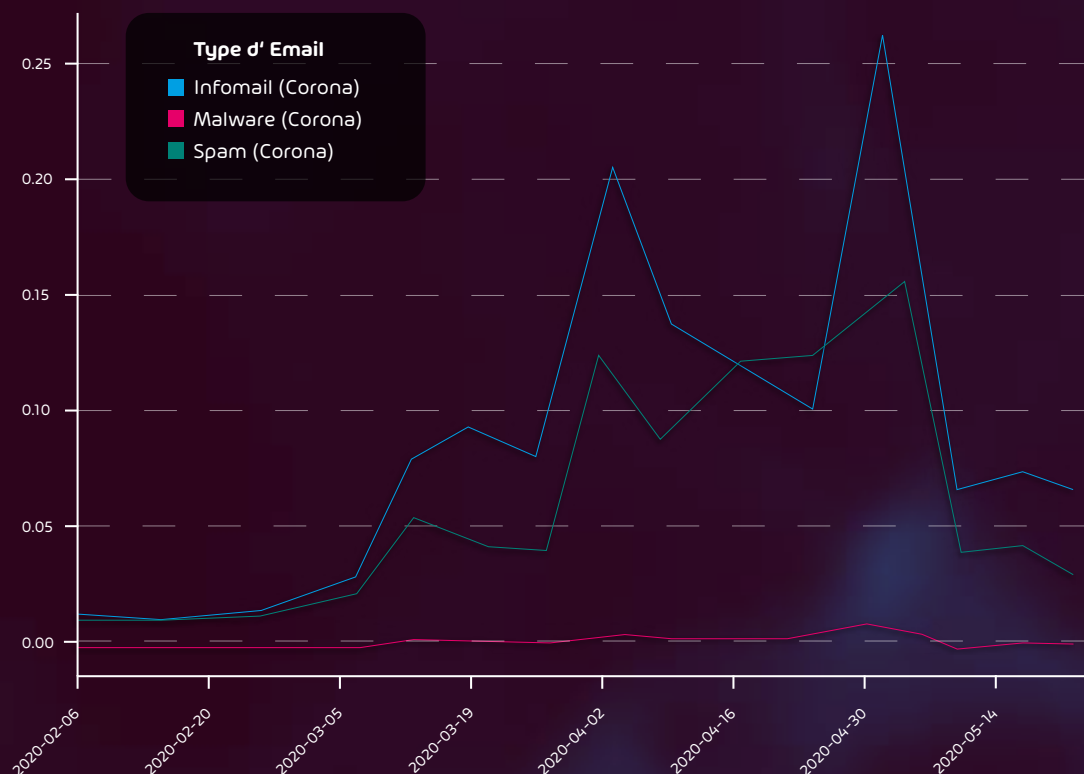
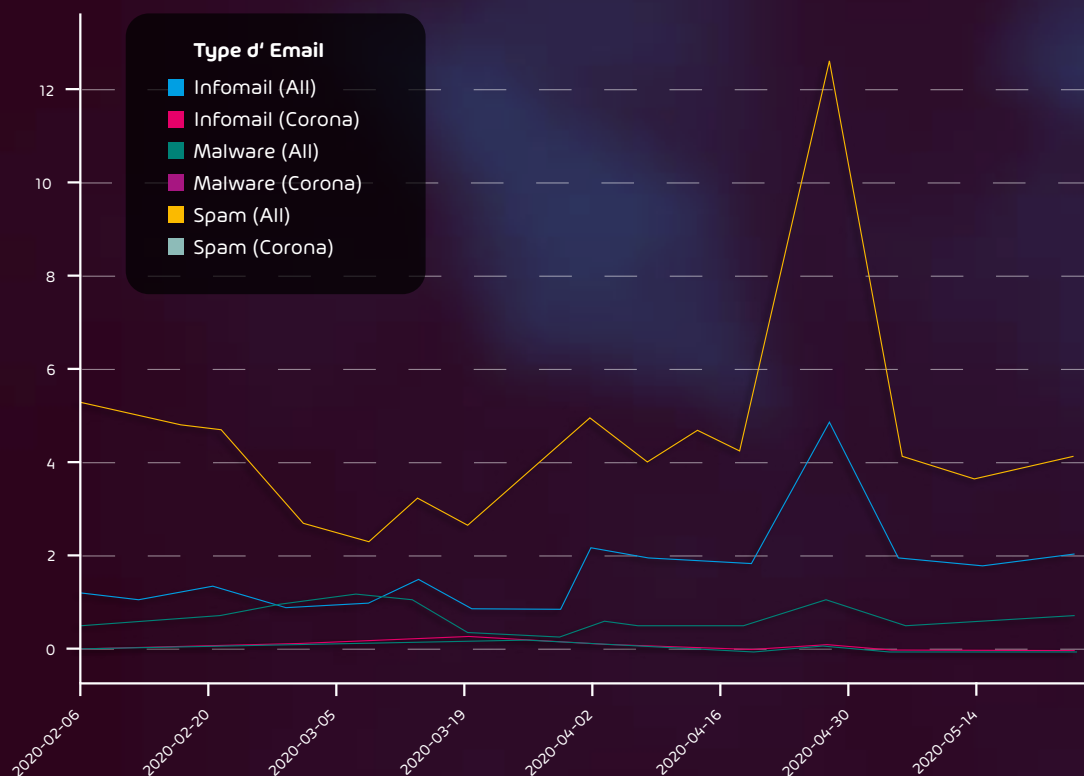
THREAT TREND:

Le Covid-19 et les autres évènements actuels: des aubaines pour la cybercriminalité?

L'année 2020 a été marquée par des événements marquants: «coronavirus» ou «Covid-19», «télétravail» et «black-lives-matter» ont été des termes utilisés plusieurs millions de fois dans les moteurs de recherche.

Les cybercriminels utilisent ces thèmes médiatiques et tentent par exemple d'accéder à des données confidentielles ou d'introduire des logiciels malveillants dans les systèmes via des e-mails de phishing en rapport avec ces sujets. En raison de la sensibilisation et de la crainte de passer à côté d'informations importantes, la probabilité que le destinataire ouvre de tels e-mails est plus élevée.

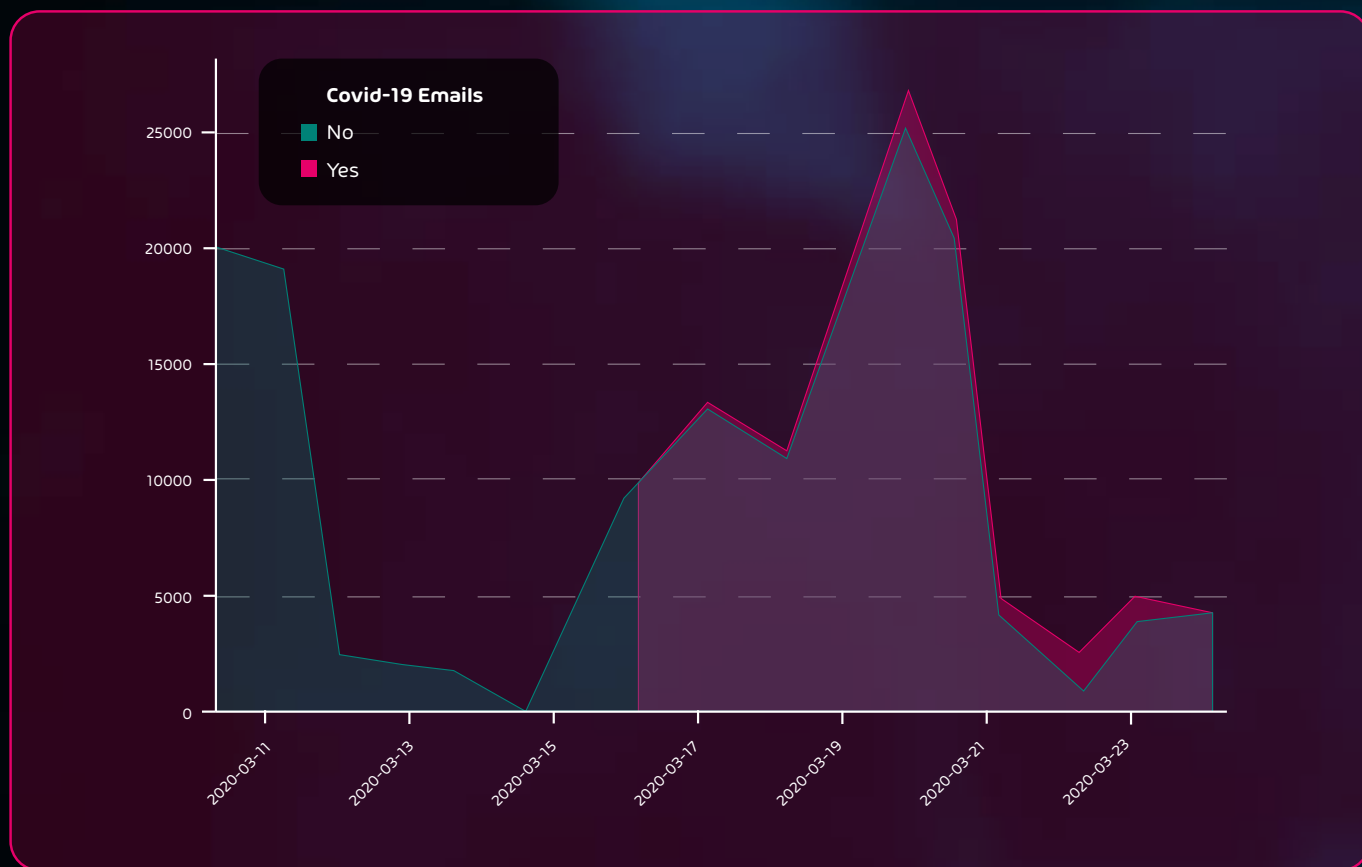
Pendant la crise du coronavirus, les analystes Security d'Hornetsecurity ont pu observer très souvent **l'exploitation d'évènements actuels, futurs ou critiques**:



III. 3: nombre de types d'e-mails malveillants en se basant sur l'exemple de la pandémie de coronavirus

Certains incidents relatifs au coronavirus peuvent vraisemblablement être mis en lien avec le nombre élevé de spams et d'e-mails avec des pièces-jointes nuisibles: ainsi sur les 15 premiers jours de mars 2020, les e-mails de spam envoyés au nom de l'Organisation mondiale de la santé (OMS) se sont multipliés après que celle-ci ait officiellement déclaré la propagation du coronavirus comme étant une pandémie.

Les e-mails frauduleux contiennent des liens vers des sites web compromis ou des pièces-jointes infectées. Dans le texte de l'e-mail, le destinataire est invité à les ouvrir, car ils contiendraient des informations relatives aux mesures protégeant de l'infection par le virus. Si cette requête est suivie, il est très probable que des logiciels malveillants soient installés de manière invisible sur le système d'information interne. Les analystes Security ont pu observer un lien clair avec la situation actuelle en ce qui concerne la diffusion de logiciels malveillants:



III. 4 : diffusion de logiciels Malveillants en rapport avec le Covid-19



Les analystes Security ont pu identifier des activités particulières des types de logiciels malveillants comme «AgentTesla», «Lokibot» et «Formbook» qui ont été diffusés dans différents types de fichiers d'archive (Zip, Rar, Iso et xls) via des e-mails malintentionnés. À partir du 15/16 mars, les termes «Covid-19» ou «coronavirus» ont été de plus en plus présents dans l'objet ou le titre des pièces-jointes de ces e-mails. Après l'introduction du port du masque dans différents pays, le volume total d'e-mails de spam a logiquement augmenté au moment de l'entrée en vigueur de la loi (Autriche, 1er avril 2020, Allemagne, 30 avril 2020). Une grande partie concernait du spam avec de la publicité pour des masques de protection.

III. 5: exemple de campagne de spams après l'entrée en vigueur du port du masque



Un groupe de hackers habituellement connu pour ses activités de sextorsion a saisi l'opportunité de cette situation particulière pour ses agissements frauduleux. Lors de la sextorsion, la victime est extorquée par les hackers qui affirment l'avoir filmée lors de sa visite de sites web pornographiques. Ils menacent de publier la vidéo si aucune rançon (généralement sous forme de bitcoins) n'est payée. Cependant, au cours de la pandémie du coronavirus, le groupe de hackers a changé de procédé et a affirmé dans ses e-mails être membre de l'OMS. Ainsi, le groupe demandait des dons aux destinataires afin d'aider les pays aux systèmes de santé fragiles à se préparer à la pandémie. En particulier autour du 24/25 mars, le Security Lab a pu **filtrer plus de 1000 e-mails de ce type par heure**.⁷

D'une manière générale, les cybercriminels continuent d'utiliser les mêmes schémas et processus, déjà connus de la plupart des utilisateurs, lors de leurs attaques. Cependant, comme la crise du coro-



III. 6: exemple d'un e-mail de phishing au nom de l'OMS

navirus a été un sujet particulièrement fort émotionnellement, la probabilité que certains destinataires tombent quand même dans la combine était plus élevée. Par conséquent, la manipulation psychique par les cybercriminels demeure une menace à prendre au sérieux.

THREAT TREND: Ransomeleaks et Ranshameware

Les ransomwares constituent l'un des types de maliciels les plus craints et avec la croissance la plus rapide au monde. Chaque année, les logiciels malveillants de chiffrement causent des dommages toujours plus importants aux entreprises concernées. Selon les estimations, **en 2020, les pertes financières causées par les attaques de ransomware s'élèveront à environ 17 milliards de dollars**.⁸ Ce montant comprend non seulement la rançon exigée, mais également les coûts entraînés par l'interruption de l'exploitation et les données perdues.

Selon les experts Security, le logiciel Malveillant va également continuer à l'avenir d'être responsable de coûts croissants en raison de la cybercriminalité: c'est ce que montre d'une part l'évolution des dernières années en matière de diffusion de ransomware et d'autre part le montant des rançons exigées par les hackers afin de débloquer les fichiers chiffrés.

Jusqu'en 2015, les campagnes de logiciels d'extorsion ont été principalement menées par des groupes de hackers organisés qui développaient leurs propres codes source.⁹ Alors qu'en 2016, environ 70 différents types de ransomware étaient connus, le site web id-ransomware.malewarehunterteam.com a **enregistré 944 différents types de logiciels ransomwares en octobre 2020**¹⁰— et des nouveaux logiciels sont identifiés quasiment chaque jour. Conti, Maze, RagnarLocker ou NetWalker constituent quelques types de ransomware connus.

Jusqu'à présent, la rançon la plus élevée a été versée aux exploitants du logiciel de ransomwares RagnarLocker: ceux-ci ont chiffrés environ 30 000 ordinateurs de l'agence de voyage américaine CWT et ont exigé 10 millions de dollars pour son déchiffrement. Après des négociations avec les hackers, l'entreprise a finalement versé 4,5 millions de dollars (414 bitcoins).¹¹

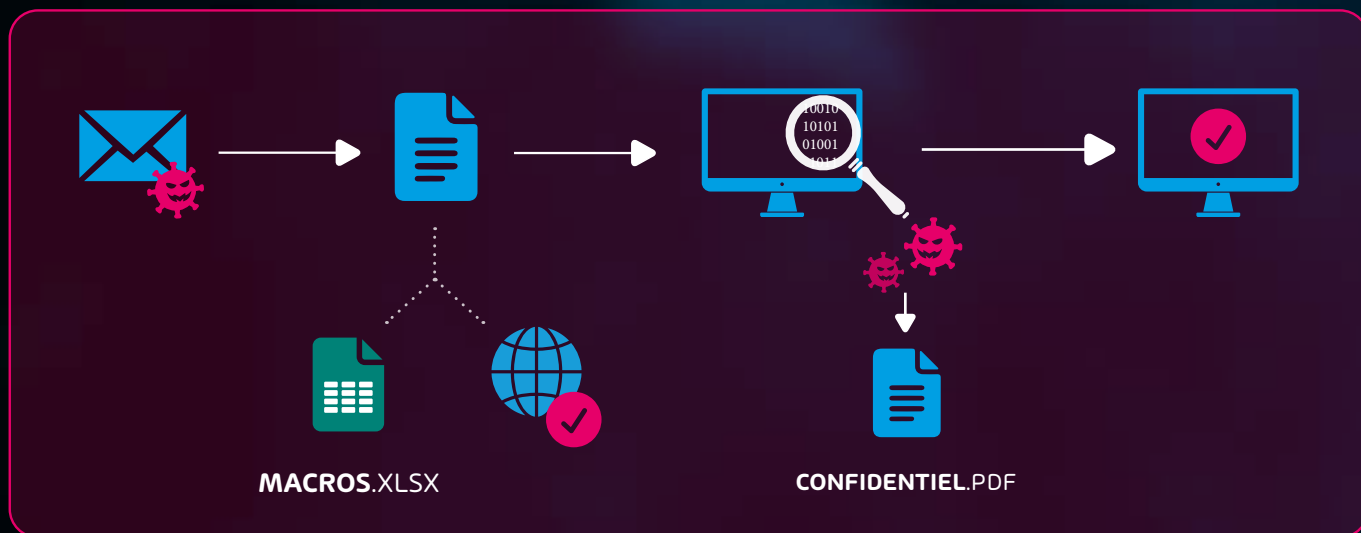
Une autre raison de la menace croissance par les ransomware est une évolution que les analystes Security ont remarqué principalement ces dernières années: sur de nombreuses places de marché criminelles en ligne, le **Ransomware-as-a-Service (RaaS)** devient de plus en plus populaire et remplace peu à peu l'offre de toolkits de logiciels malveillants avec lesquels les hackers acceptent des missions pour des campagnes de ransomwares ciblées. Le fait que les auteurs rendent le code de leurs ransomware accessible à d'autres cybercriminels permet d'augmenter considérablement leur portée et leur diffusion. En échange, les fournisseurs reçoivent soit une part

de la rançon versée ou bien exigent un paiement préalable.¹²

Cela signifie que fondamentalement, toute personne ayant accès à de tels services et à la possibilité de diffusion peut utiliser des e-mails de phishing avec des logiciels de ransomwares. Et tant que les victimes acceptent les demandes de rançon, la popularité de ces méthodes va continuer à augmenter.

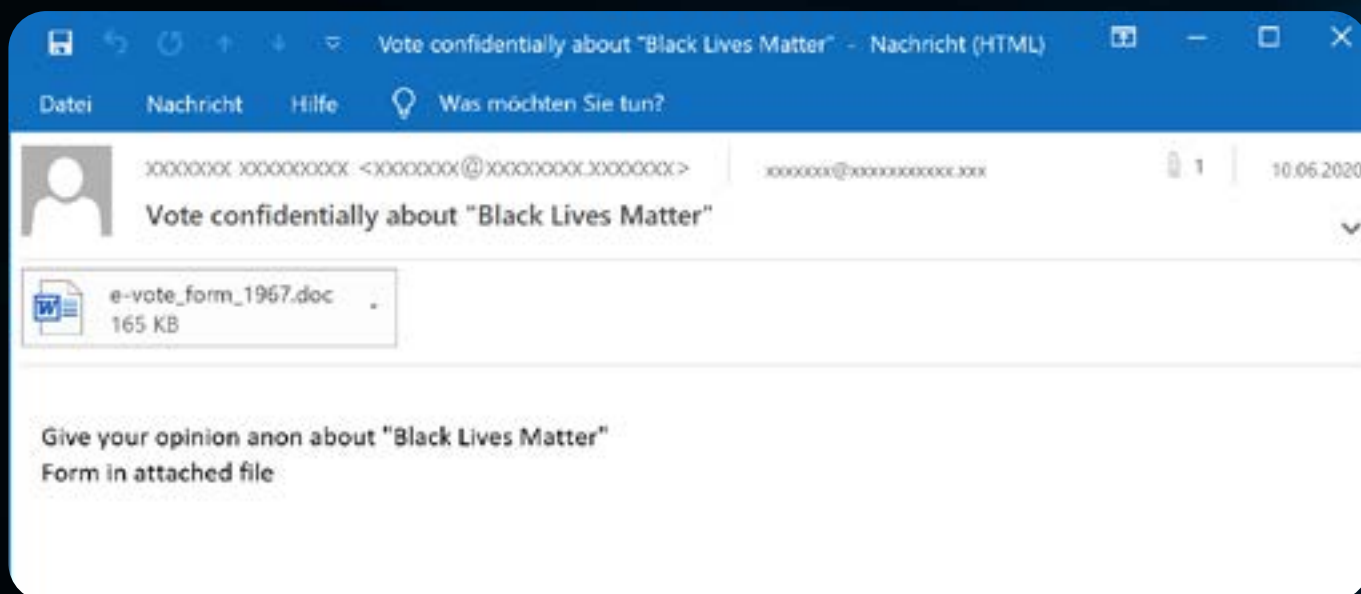
Le mode opératoire des logiciels de ransomwares

Dans la plupart des cas, les logiciels de ransomwares sont installés sur le système concerné via d'autres logiciels malveillants eux-mêmes dissimulés derrière des pièces-jointes d'e-mails ou des liens de téléchargement incorporés.



III. 7: les logiciels malveillants se cachent derrière des pièces-jointes d'e-mails ou des liens de téléchargement frauduleux

Le logiciel malveillant de chiffrement «Ryuk» constitue un exemple connu: le ransomwares accède au système via un e-mail Emotet en combinaison avec le cheval de Troie bancaire Trickbot avant de chiffrer tous les fichiers se trouvant dans le système. Le montant exigé de la rançon s'oriente selon l'évaluation des acteurs de Trickbot des disponibilités financières actuelles de l'entreprise.



III. 8: exemple d'e-mail frauduleux qui utilise le mouvement «black lives matter» en tant qu'accroche pour la distribution d'un logiciel de ransomwares

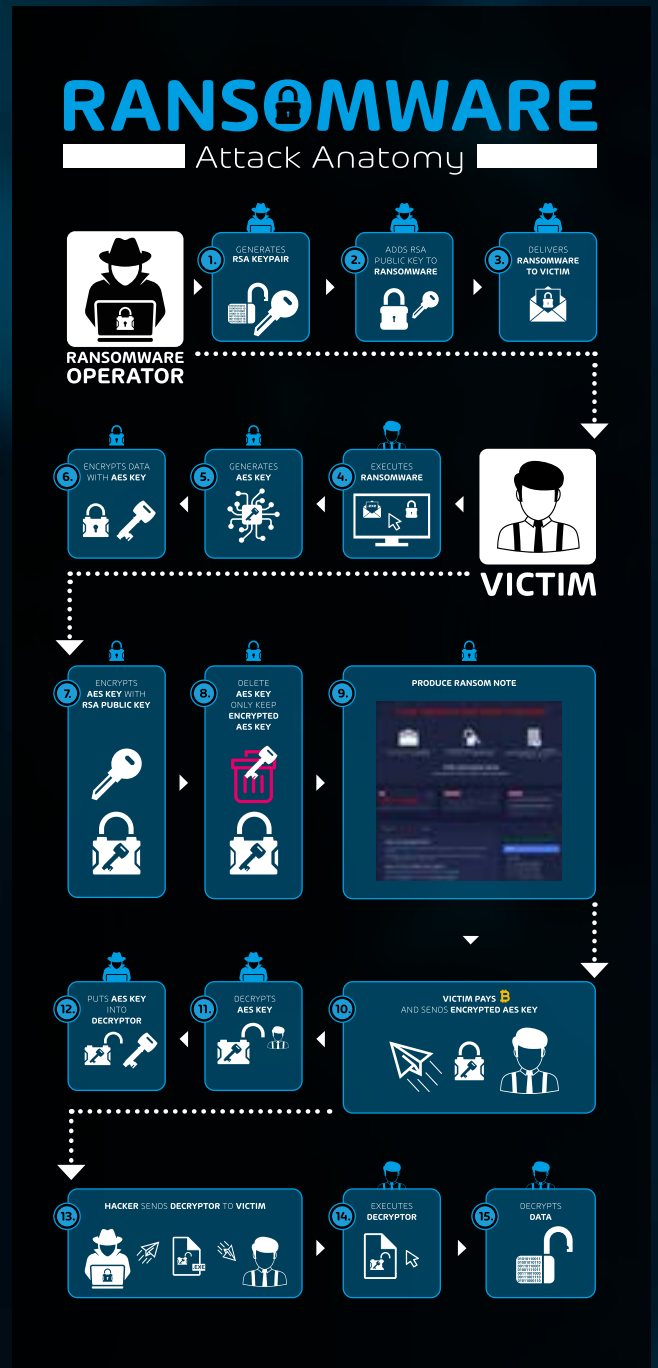
Après que le ransomware ait pénétré dans le réseau de l'entreprise, il explore les données se trouvant sur le système et les chiffre. Ensuite, la victime est prévenue du chiffrement des données et doit verser une certaine rançon afin de pouvoir récupérer les données. Mais le déchiffrement n'est pas garanti après le paiement.

Depuis peu, les analystes Security d'Hornetsecurity observent une nouvelle tendance qui accompagne la demande initiale de rançon via une attaque ultérieure d'une pression supplémentaire.

Le mode opératoire des RANSOMWARES

Certains groupes de hackers ne misent plus seulement sur le chiffrement de données via des logiciels de ransomwares mais élargissent leurs stratégies d'extorsion: **avant que les données des victimes soient chiffrées sur les ordinateurs compromis, le ransomware copie les données sur les serveurs des hackers** qui menacent ensuite de publier ces informations sensibles sur des pages «public shaming». Cette technique d'attaque, une combinaison de ransomwares et de «public shaming» est appelée **«Ranshameware»** par les analystes Security d'Hornetsecurity. Les créateurs de Maze ont lancé la première attaque de ce type en décembre 2019. Ensuite, de nombreux autres groupes de logiciels de ransomwares ont suivi. En outre, certains exploitants de logiciels de ransomwares s'adressent aux partenaires commerciaux ou aux clients de la victime. En effet, leurs informations font souvent partie des fichiers à publier et cela permet d'augmenter la pression sur les personnes concernées. Ainsi, les créateurs du ransomware Clop sont tristement célèbres pour cela.

III. 9: déroulement classique d'une attaque de logiciel de ransomwares



La publication de données permet d'augmenter la pression

Dans le cadre de l'évolution de cette technique d'attaque, les analystes ont constaté que les gangs de logiciels de ransomwares se regroupent de plus en plus souvent: ainsi, les créateurs du ransomware Maze coopèrent avec d'autres groupes cybercriminels afin de pouvoir menacer de publier les données des victimes avec une portée encore plus grande sur des plateformes de leak supplémentaires. Cela confère aux groupes un moyen de pression plus important et de potentiels bénéfices plus élevés. Selon les médias, LockBit et RagnarLocker font partie du «cartel Maze». Cependant, il n'est pas possible d'affirmer actuellement que cette coopération perdure. Avec environ 240 ensembles de données, la page leak de Maze compte le plus grand nombre de victimes jusqu'à présent. Cependant, il s'agit «seulement» des publications des victimes qui n'ont pas accepté les demandes de rançon.

Le 1er novembre 2020, le groupe Maze a publié sur sa page un communiqué de presse annonçant l'interruption de ses activités.

En juin 2020, le groupe de logiciels de ransomwares Revil (Sodinokibi) a vendu aux enchères des données volées via une vente en ligne. Cependant, le site web sur lequel la vente a eu lieu n'expliquait pas comment on pouvait

enchérir en tant qu'acheteur potentiel. On peut donc logiquement penser qu'avec ce mode opératoire, les cybercriminels envisageaient principalement d'apeurer leurs victimes et d'attirer l'attention des médias sur eux.



III. 10: page de leak du groupe Maze



III. 11: page de leak du groupe de logiciels de ransomwares Revil

Afin de se protéger de ce nouveau mode opératoire, il est important de savoir comment les ransomware et les autres programmes malveillants peuvent accéder aux réseaux des entreprises. Comme déjà indiqué, la communication par e-mail constitue la principale porte d'entrée à la diffusion. Lors de leurs analyses, les analystes Security du Hornetsecurity Security Lab sont arrivés à la conclusion que c'étaient principalement les **pièces-jointes d'e-mails frauduleux** qui jouaient ici un rôle important.

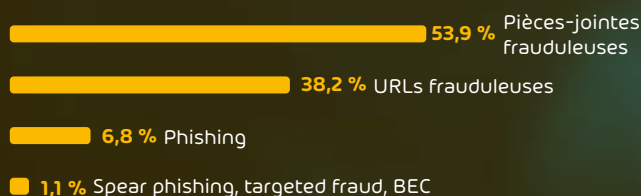
Pièces-jointes frauduleuses: le type de menace numéro 1 (premier semestre 2020)

Pour le premier semestre 2020, les analystes Security d'Hornetsecurity ont analysé les méthodes d'attaque les plus utilisées par les cybercriminels lors de l'envoi d'e-mails frauduleux.

Les experts ont abouti aux résultats suivants: avec **53,9 %** les pièces-jointes malveillantes se classent à la première place des attaques les plus fréquentes. Avec une part de **38,2 %**, les liens frauduleux constituent également une méthode d'attaque courante et se classent en deuxième position. Le phishing, avec une part de **6,8%**, s'établit à la troisième place, suivi par des menaces ciblées comme le spear phishing, les fraudes ciblées et BEC avec une part de **1,1 %**.

Mais pourquoi est-ce que les liens et pièces-jointes sont tellement appréciés des cybercriminels? Les hackers essaient ainsi d'introduire des logiciels malveillants dans les systèmes de leurs victimes. Contrairement aux techniques d'ingénierie sociale et aux méthodes d'attaque ciblées, il est possible d'automatiser l'ajout **de pièces-jointes aux fichiers et liens dans les e-mails**. Par conséquent, ce procédé est bien plus fréquent. Les pièces-jointes malveillantes peuvent également être dangereuses après la réception de l'e-mail pour les utilisateurs, car en cas de doute, elles peuvent rester longtemps dans la boîte de réception. Par contre, les URLs dépendent d'une infrastructure qui fonctionne. Les URLs frauduleuses sont souvent bloquées, ce qui permet d'éliminer généralement plus vite le danger dans ce cas.

Les attaques ciblées comme le spear phishing et la targeted fraud sont dangereuses pour les utilisateurs, car elles peuvent entraîner d'énormes dégâts financiers. Cependant, ces attaques nécessitent une préparation complexe, car les cybercriminels doivent récupérer à l'avance de nombreuses informations pour réussir leur attaque.



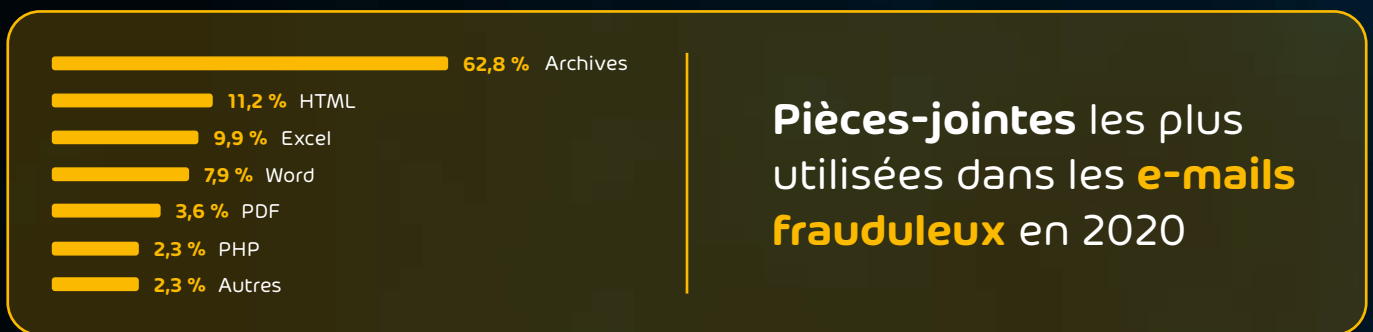
Types d'attaques
les plus **utilisées**
en 2020

III. 12 : types d'attaques les plus fréquentes en 2020

Archives: la pièce-jointe frauduleuse la plus utilisée

Comme dans le paragraphe précédent, les pièces-jointes des e-mails constituent le type d'attaque le plus répandu. Les experts du Hornetsecurity Security Lab ont analysé ces pièces-jointes et sont arrivés à la conclusion suivante: 62,8 % des e-mails avec des pièces-jointes frauduleuses contenaient des archives, 11 % étaient des pièces-jointes HTML, environ 10 % des fichiers Excel et 8 % des fichiers Word. L'utilisation d'archives afin d'introduire des fichiers malveillants dans les boîtes de réception est très répandue, car elle empêche la vérification directe des différents fichiers par les programmes antispam et antivirus.

Un antivirus doit d'abord extraire la pièce-jointe contenue dans le fichier archivé afin de l'analyser. Certes, de nombreux filtres bloquent au préalable les programmes exécutables comme .exe., .vbs., .com, .scr, .bat et .js, mais dans certains cas uniquement lorsque les fichiers sont directement joints à l'e-mail. La dissimulation des fichiers frauduleux offre donc une certaine protection aux cybercriminels, ce qui augmente **le taux de réussite des attaques.**



III. 13: pièces-jointes les plus fréquemment utilisées dans les e-mails frauduleux

Phishing HTML:


Lors de l'phishing HTML, les cybercriminels envoient un site web de phishing sous forme de pièce-jointe d'un e-mail à la victime. L'e-mail demande par exemple au destinataire d'actualiser son profil d'utilisateur. Si l'utilisateur clique sur la pièce-jointe, il est redirigé vers un formulaire sur lequel il doit saisir différentes informations personnelles. Dès que les données ont été saisies et que la victime clique sur «Envoyer», une demande HTTP-POST est envoyée et celle-ci transfère les données saisies vers un serveur. Par le biais de ce schéma, les cybercriminels évitent qu'un site web de phishing soit placé sur une liste noire. En effet, la victime ouvre la page via la pièce-jointe HTML, localement dans le navigateur, et ne peut être prévenu par des systèmes de détection précoce, comme par exemple Safebrowsing de Google.¹³




Diffusion de logiciels malveillants via HTML:

Des logiciels malveillants peuvent également être diffusés via les pièces-jointes HTML. À ce sujet, les experts du Hornetsecurity Security Lab ont représenté la chaîne d'infection du ransomware Clop. Les cybercriminels envoient à la victime un e-mail avec une pièce-jointe HTML malveillante. Celle-ci redirige la victime vers un document XLS contenant le loader Get2 qui installe à son tour un cheval de Troie Remote Access. Celui-ci permet de préparer le réseau à l'utilisation du ransomware Clop.

 **EXE [in archive]** 78.0160889310551%

 **VBS [in archive]** 5.293661058470925%

 **.com [in archive]** 2.8011246124065057%

fichiers malveillants
dans des archives
Top 3

III. 14: Fichiers malveillants dans les archives: top 3

Dans les archives, les cybercriminels utilisent principalement des fichiers .exe avec une part supérieure à 78 %. «exe» signifie «executable» (exécutable) et il s'agit d'une application pour les systèmes fonctionnant avec Windows. Les fichiers Visual Basic Script suivent avec environ 5 %. Ici, il s'agit d'un langage de script développé par Microsoft. Les fichiers COM occupent la troisième place avec presque 3 %.

Portrait des différentes familles: Agent Tesla, GuLoader, Formbook et Loki

En plus des types d'attaques et de fichiers, les experts Security d'Hornetsecurity ont aussi analysé les types de logiciels malveillants qui ont été envoyés en tant que fichiers exécutables dans des archives par e-mail. AgentTesla a été le maliciel le plus diffusé, suivi par GuLoader, Formbook et Loki. Dans ce qui suit, nous allons nous intéresser de plus près aux caractéristiques des différentes familles de logiciels malveillants.

AgentTesla:

AgentTesla est un cheval de Troie de type RAT (Remote Access Tool) permettant de commander des ordinateurs à distance. AgentTesla circule depuis 2014 et est en mesure d'enregistrer les saisies de clavier d'un ordinateur compromis.¹⁴

GuLoader:

GuLoader, également appelé CloudEyE, est un VB5/6 Downloader. Les cybercriminels utilisent GuLoader afin d'infecter des ordinateurs avec des programmes malveillants, comme par exemple AgentTesla, qui peuvent alors notamment être utilisés pour dérober des informations confidentielles.

Formbook:

Formbook est un cheval de Troie de type « Infostealer » qui peut être acheté sur Internet en tant que MaaS (Malware as a Service). Ce logiciel malveillant contient des fonctionnalités innovantes pouvant également être utilisées par des hackers possédant peu de connaissances techniques.

Loki:

Loki est également un logiciel malveillant de type « Infostealer » ayant été découvert pour la première fois en 2015 dans des forums clandestins où il est vendu. Il est conçu pour dérober les données des ordinateurs infectés avant de les transmettre à un serveur C2 via HTTP POST. Ces données sont en première ligne des mots de passe sauvegardés et des données de connexion de navigateurs web.¹⁵

NanoCore:

MassLogger:

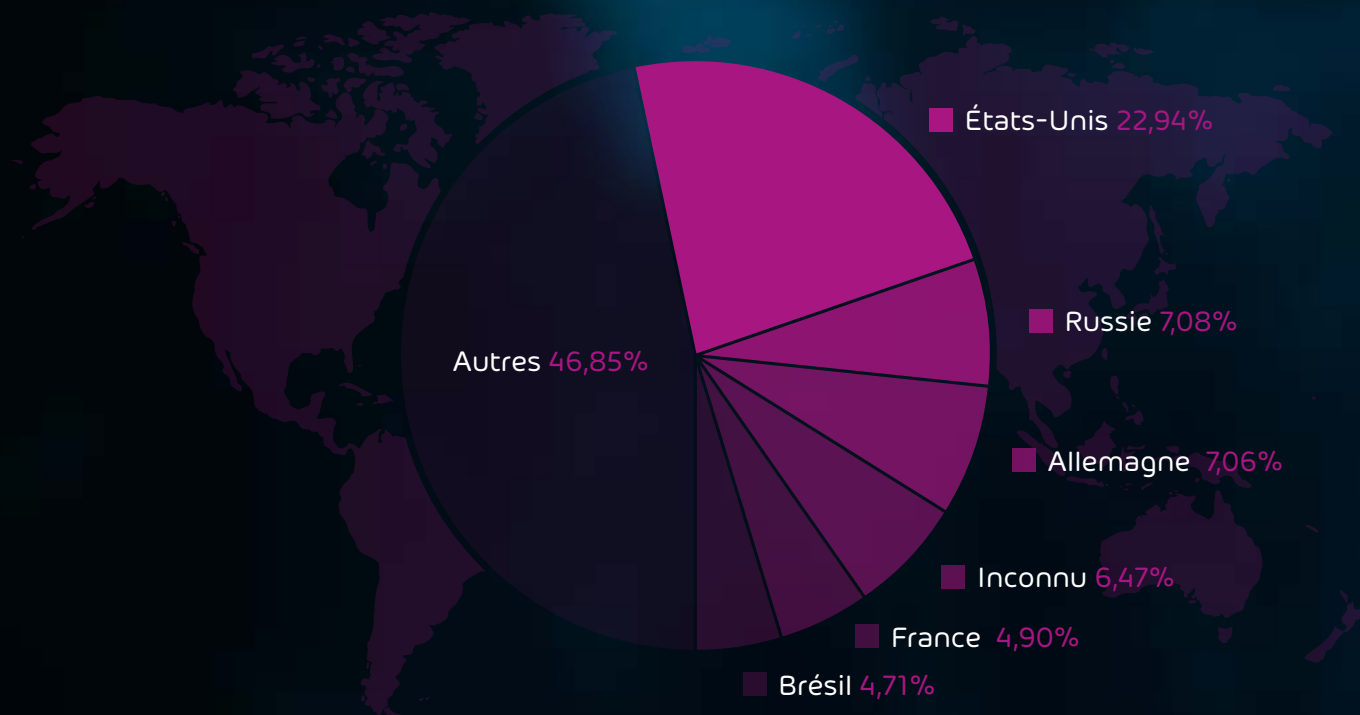
RemcosRAT:

HawkEye:

III. 14: maliciel diffusé dans les archives en tant que fichier exécutable

L'origine géographique des attaques de logiciels malveillants

Mais d'où proviennent les nombreux e-mails que les cybercriminels utilisent pour l'envoi de leurs attaques de maliciels ? Le graphique suivant permet de visualiser les origines géographiques analysées par le Hornetsecurity Security Lab avec les parts les plus élevées d'envois de maliciels.



III. 16: origine géographique des envois de logiciels malveillants

Avec une part de 22,94 %, la plupart des diffusions de logiciels malveillants proviennent de grands fournisseurs d'hébergement connus aux États-Unis. «En outre, nous observons une **utilisation abusive croissante d'outils d'envoi** comme SendGrid qui sont utilisés pour la **diffusion d'e-mails frauduleux**», explique un analyste Security d'Hornetsecurity.

La Russie se classe deuxième avec une part de 7,08 %. La majorité des adresses IP des expéditeurs proviennent du fournisseur Ufanet. Les analystes estiment que l'utilisation du «Bulletproof Hosting» pourrait constituer la cause de cette part élevée. Ici, les cybercriminels utilisent des serveurs dont les exploitants ne réagissent pas aux plaintes relatives à un abus et qui, d'une manière générale, ne s'occupent pas de ce qu'il se passe avec les serveurs qu'ils mettent à disposition. Cela facilite l'envoi par les hackers de spams en grande quantité. Le fait que l'Allemagne représente également une part importante de l'origine des envois est lié à l'utilisation croissante de «freemailers» (comme par exemple mail.com ou gmx.de) qui sont fréquemment utilisés pour des campagnes de malspam.

Perspectives: à quoi doivent s'attendre les entreprises à l'avenir?

Les cyberattaques sont devenues l'une des principales menaces pour les entreprises en général. L'Internet des objets, l'utilisation de l'intelligence artificielle et le stockage croissant de données sensibles sur le cloud vont entraîner la poursuite de cette tendance.¹⁶ Ainsi, les résultats du Global Risk Report montrent qu'en 2020, 76,1 % des sondés s'attendent à une hausse des attaques sur les infrastructures critiques ainsi qu'à une augmentation du danger de vol des données et des fraudes (75 %).¹⁷

Les analystes Security du Hornetsecurity Security Lab prévoient également que certaines tendances déjà mentionnées pourraient devenir les **nouveaux standards pour les groupements cybercriminels**. «Nous remarquons de plus en plus que les criminels utilisent le modèle du «ranshameware». Ils introduisent ainsi des logiciels de ransomwares dans les entreprises, dérobent et chiffrent les données sensibles avant d'extorquer l'entreprise en menaçant de publier ces contenus», explique le Security Lab. «En outre, depuis le début de l'année, il existe certains groupes qui utilisent des macros XLM dans leurs documents frauduleux et rendent ainsi l'identification par les

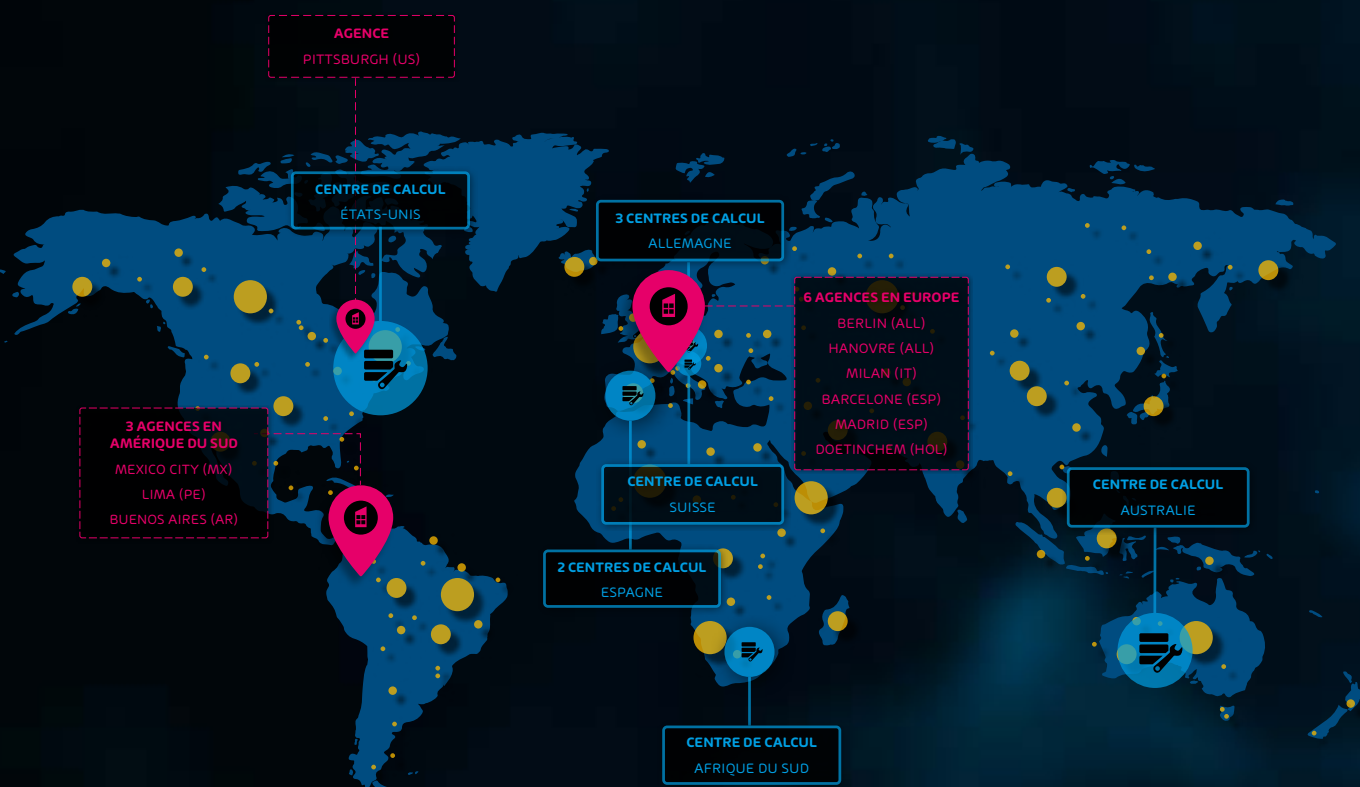
programmes de sécurité toujours plus compliquée. Ici, nous observons une tendance claire suivie désormais également par des acteurs aux connaissances techniques moins importantes», explique un analyste Security d'Hornetsecurity.

Le danger des cyberattaques ne diminue pas, les hackers vont plutôt continuer à se professionnaliser. **Les entreprises doivent être conscientes de cette évolution** afin de pouvoir se protéger à temps des risques grâce à des services de sécurité sophistiqués. En particulier au vu de l'utilisation croissante de thème médiatisés en tant qu'appât, il est d'autant plus important de rester vigilant et de garantir une gestion appropriée de la sécurité.

À propos de Hornetsecurity

Hornetsecurity est le principal fournisseur européen Cloud Security pour les e-mails et protège infrastructure informatique, la communication numérique ainsi que les données d'entreprises et organisations de toutes tailles. Le spécialiste de sécurité informatique d'Hanovre fournit ses services via neuf centres de calcul internationaux sécurisés par des moyens redondants. Le portefeuille de produits englobe des solutions dans les domaines de la sécurité des e-mails, du web et des fichiers. Tous les services de l'entreprise peuvent être rapidement implémentés et sont disponibles 24 heures sur 24. Hornetsecurity emploie environ 200 collaborateurs sur dix sites internationaux. Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA et Claas font notamment partie des clients.

Hornetsecurity international



10 SITES D'AGENCES
DANS LE MONDE, DONT 6 EN EUROPE



9 CENTRES DE CALCUL
DANS LE MONDE, DONT 3 EN EUROPE



40 000 ENTREPRISES
SONT PROTÉGÉES PAR NOS SERVICES

Sources

- (1) <https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberisiken-im-mittelstand-2019-pdf-data.pdf>, S. 10
- (2) <https://www.hornetsecurity.com/de/security-informationen/emotet-ist-zurueck/>
- (3) <https://www.checkpoint.com/press/2020/march-2020s-most-wanted-malware-dridex-banking-trojan-ranks-on-top-malware-list-for-first-time-2/>
- (4) <https://www.hornetsecurity.com/de/security-informationen/der-malspam-qakbot-verbreitet-prolock/>
- (5) <https://www.hornetsecurity.com/de/security-informationen/corona-malware-kampagne-mit-trickbot-im-gepaeck/>
- (6) <https://www.hornetsecurity.com/de/security-informationen/trickbot-malspam-nutzt-black-lives-matter-aus/>
- (7) <https://www.hornetsecurity.com/de/security-informationen/corona-opportunisten-wie-cyberkriminelle-die-krise-ausnutzen/>
- (8) <https://de.safetymalware.com/blog/ransomware-fakten-trends-statistiken/>
- (9) https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email
- (10) <https://id-ransomware.malwarehunterteam.com/index.php>
- (11) <https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W>
- (12) https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email
- (13) <https://www.hornetsecurity.com/de/security-informationen/html-phishing-mit-doppelter-passwort-abfrage/>
- (14) <https://www.pcrisk.de/ratgeber-zum-entfernen/9166-agent-tesla-rat#:~:text=Agent%20Tesla%20ist%20ein%20Fernzugriffstool,verschiedene%20pers%C3%B6nliche%20Daten%20zu%20stehlen.>
- (15) <https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws>
- (16) Global Risk Report, S. 7
- (17) Global Risk Report, S. 11