F-Secure

APERÇU DES CYBER ATTAQUES AU PREMIER SEMESTRE 2018

INTRODUCTION

Au cours du premier semestre 2018, des changements notables ont été observés concernant les cyber menaces. Les tendances enregistrées diffèrent sensiblement des années précédentes. Grâce au renforcement de la sécurité des systèmes et au renforcement des technologies antivirus, l'impact des exploits logiciels a été clairement limité et les menaces standards ont pu être efficacement bloquées. Résultat : les pirates ont été contraints de se tourner vers un vecteur d'infection plus ancien : le spam, qui a opéré son grand retour. Jusqu'à récemment, les ransomware - ou logiciels rançon - constituaient les cyber menaces les plus sérieuses pour les entreprises. Ces attaques restent bien présentes mais leur domination semble appartenir au passé. Elles ont été supplantées par le piratage cryptographique, qui tire profit de la popularité actuelle des cryptomonnaies.

Les cyber attaques observées sur notre réseau mondial de honeypots ont, elles aussi, évolué : la Russie, habituellement premier pays source d'attaques, a cédé sa place au Royaume-Uni. Il s'agit d'une première : depuis 2016 - année à laquelle nous avons commencé à publier nos observations -, la Russie dominait systématiquement le classement. Le nombre total de cyber attaques observées au niveau mondial a quant à lui reculé par rapport aux deux semestres précédents.

TRAFIC DES CYBER ATTAQUES AU NIVEAU MONDIAL : LES OBSERVATIONS DE NOTRE RÉSEAU DE HONEYPOTS

En termes simples, un honeypot - ou « pot de miel » - peut être considéré comme un piège à destination des pirates. Les honeypots simulent des services populaires tels que SSH, HTTP, et SMB, de manière à éveiller leur intérêt. Les honeypots les plus efficaces sont comparables à des labyrinthes : ils permettent aux analystes d'observer le comportement des pirates à leur insu. Les honeypots permettent de recueillir des informations précieuses sur les stratégies des pirates, ainsi que sur les choix qu'ils opèrent concernant leurs victimes. Ces honeypots peuvent être par ailleurs une source d'échantillons de malware et de scripts shell.

Les honeypots sont des leurres : une connexion entrante enregistrée par un honeypot est soit le résultat d'une erreur (quelqu'un tapant une mauvaise adresse IP, ce qui est peu probable), soit le résultat d'un balayage d'internet ou d'un réseau par un pirate. C'est en effectuant ce type de balayage que les pirates découvrent des services potentiellement vulnérables.

L'observation de cette activité de balayage fournit des informations sur le type de services attirant particulièrement l'attention des pirates. Les évolutions observées concernant ces tendances correspondent souvent à des cyber événements d'envergure mondiale. Nous avons par exemple observé, il y a plusieurs mois, des pics d'activité liés au protocole Samba (port 445) : ces derniers étaient liés à l'utilisation de l'exploit EthernalBlue par les malware WannaCry et NotPetya, ainsi qu'au lancement par Microsoft du serveur MSSQL pour Linux.

Lorsque le pirate trouve un honeypot au cours de son balayage, il tente d'en obtenir l'accès. Les honeypots sont délibérément configurés pour permettre au hacker d'accéder facilement aux services qu'ils fournissent. Par exemple, ils requièrent des mots de passe faciles à deviner, ou finissent par accepter n'importe quel mot de passe, après un certain nombre de tentatives.

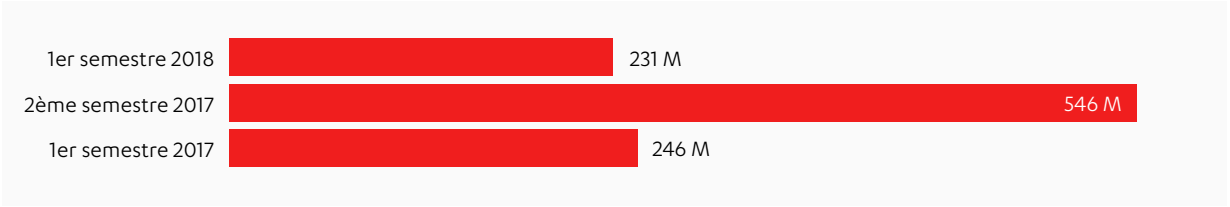
Une fois que le pirate a accédé au honyepot, ses actions sont enregistrées : ses tentatives de connexion, sa progression, les logiciels malveillants qu'il installe et les outils qu'il télécharge... jusqu'à ce qu'il réalise qu'il s'agit d'un honeypot et qu'il prenne la fuite.

Les honeypots les plus efficaces sont réalisés sur mesure, de manière à offrir davantage de réalisme. Ils donnent l'impression de suivre un objectif spécifique, ou d'appartenir à une organisation. Un honeypot bien conçu peut tromper les hackers les plus chevronnés. En 2013, un chercheur en sécurité a notamment piégé un collectif de pirates chinois (connu sous le nom d'APT1 ou Comment Crew) avec un honeypot imitant un système municipal de contrôle des eaux.

Les honeypots font partie intégrante du service de détection et d'intervention rapide de F-Secure. Ils peuvent être conçus pour imiter des serveurs Windows, des postes de travail, des serveurs de fichiers et même des serveurs VOIP. Ils permettent de détecter les intrus avec précision, même dans les couches inférieures de la communication réseau. F-Secure déploie des honeypots sur ses environnements clients mais aussi sur internet, et dispose de serveurs de leurre installés dans le monde entier.

Ce rapport présente les cyber attaques visant les honeypots et les catégorise par pays. Il convient de prendre en compte le fait que le pays apparaissant comme le pays-source n'est pas nécessairement celui d'où l'attaque a été réellement lancée. En effet, pour échapper aux autorités, les pirates passent par de multiples proxys. Ils utilisent des VPN, TOR, voire des infrastructures ou des ordinateurs préalablement corrompus.

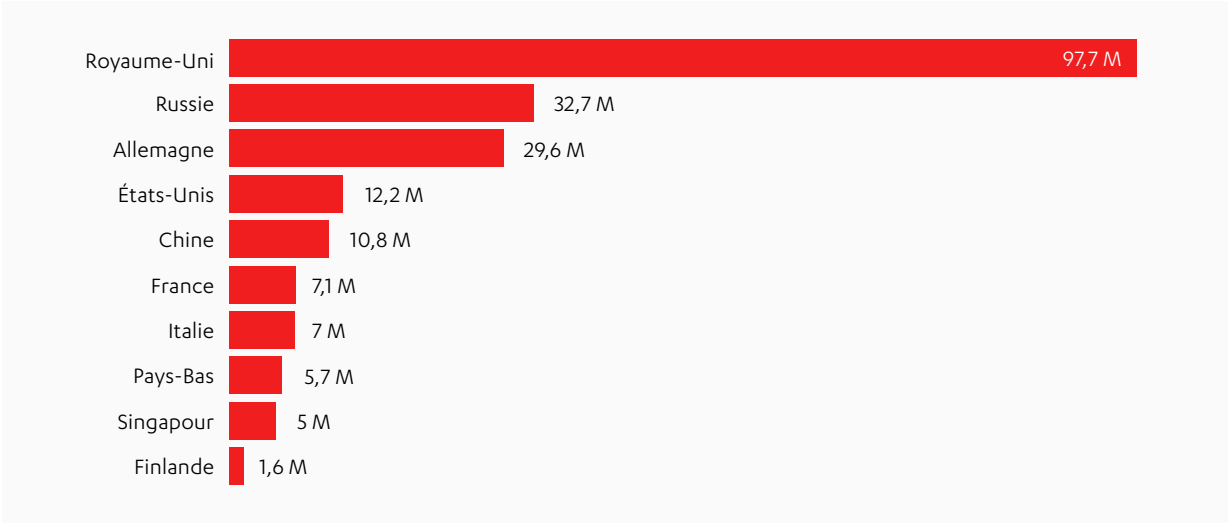
NOMBRE TOTAL DE CYBER ATTAQUES VISANT LES HONEYPOTS, PAR SEMESTRE



Les six premiers mois de l'année ont été marqués par un ralentissement des attaques par rapport aux semestres précédents. Au second semestre 2017, le trafic avait été particulièrement important, avec des opérations d'envergure provenant de la Russie et ciblant le protocole SSH. Le calme relatif de la Russie durant ce premier trimestre explique une grande partie de l'accalmie observée.

Ce ralentissement peut s'expliquer, dans une moindre mesure, par le recul de WannaCry. Au deuxième semestre 2017, les périphériques infectés par WannaCry continuaient de sonder des ports SMB ouverts et potentiellement vulnérables. Certes, WannaCry reste l'un des principaux programmes malveillants détectés par F-Secure : les périphériques infectés tentent toujours de parcourir le web à la recherche de périphériques potentiellement vulnérables mais, en 2018, davantage de systèmes ont été mis à jour et les solutions de protection des postes de travail parviennent désormais à stopper les infections, réduisant le nombre de dispositifs infectés et donc le nombre de tentatives de connexion au premier semestre. Le port 445 reste le port le plus prisé, mais la majorité de ce trafic provient de quelques campagnes d'attaques agressives en provenance du Royaume-Uni. Lorsque ces campagnes ne sont pas prises en compte, le port 445 présente un trafic inférieur à celui observé précédemment.

PRINCIPAUX PAYS-SOURCES

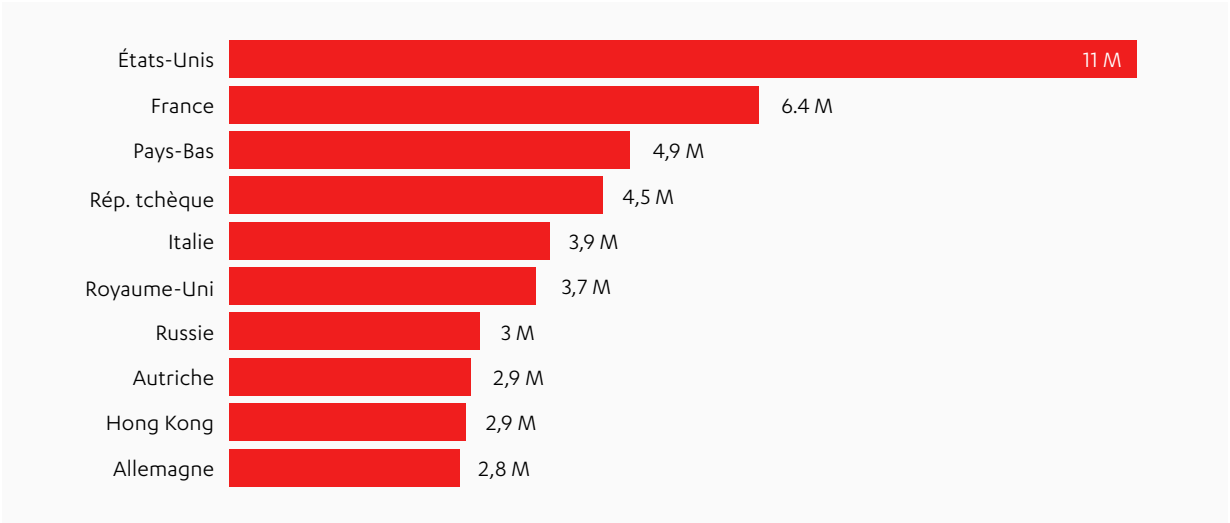


Le Royaume-Uni a détrôné la Russie de sa première place, à la faveur de quelques campagnes d'attaques d'envergure. 99 % du trafic en provenance du Royaume-Uni a concerné le port 445.

Pour la première fois, la Finlande figure dans ce classement.

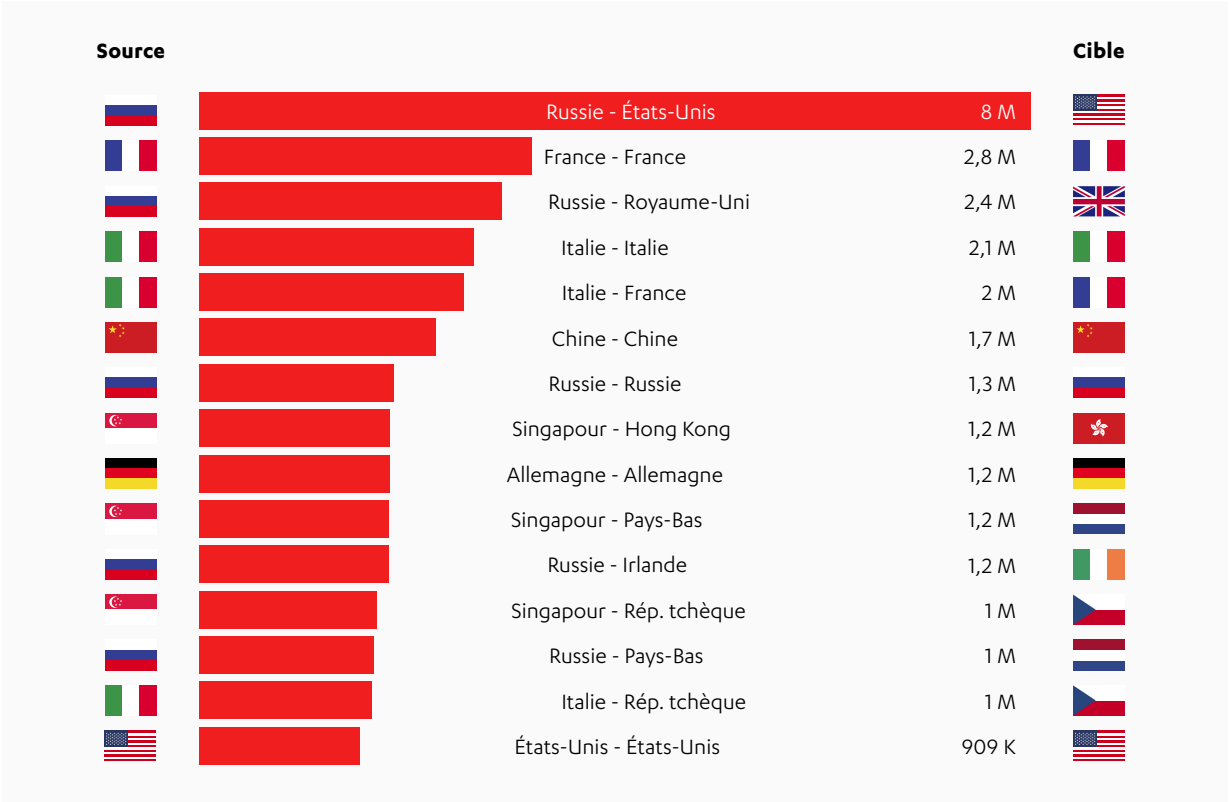
Concernant la Russie, une relative accalmie a été observée : 33 millions d'attaques ont été observées ce semestre. 108 millions d'attaques avaient été observées au premier semestre 2017, 146 millions au second.

PRINCIPAUX PAYS-CIBLES



Comme c'est le cas régulièrement, les États-Unis ont été la première cible des attaques observées. Toutefois, l'Allemagne, positionnée d'ordinaire dans le Top 5, a reculé à la 10ème place.

QUEL PAYS CIBLE QUEL PAYS ? CLASSEMENT PAR PAYS-SOURCE - PAYS-CIBLE



Le premier couple pays-source - pays-cible reste la Russie ciblant les États-Unis. Toutefois, le volume de ces cyber attaques russes visant les Etats-Unis a nettement diminué, tombant à 8 millions. Au second semestre 2016, près de 27 millions d'attaques issues de la Russie visaient les États-Unis. Au premier comme au second semestre 2017, le nombre de ces attaques approchait les 70 millions.

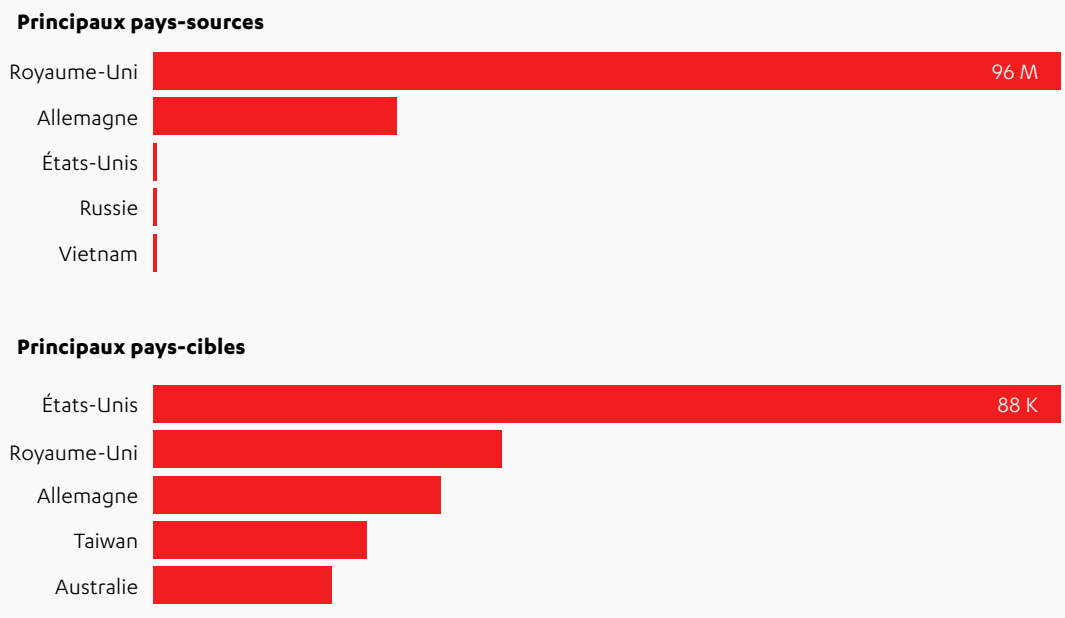
Bien que le Royaume-Uni ait enregistré le plus grand nombre de cyber attaques, il n'apparaît pas sur cette liste comme un pays-source important car les cyber attaques menées ont été très largement réparties : elles ont concerné un grand nombre de pays. Le principal pays-cible de ces campagnes a été l'Autriche, avec seulement 39 000 attaques.

PRINCIPAUX PORTS TCP SONDÉS

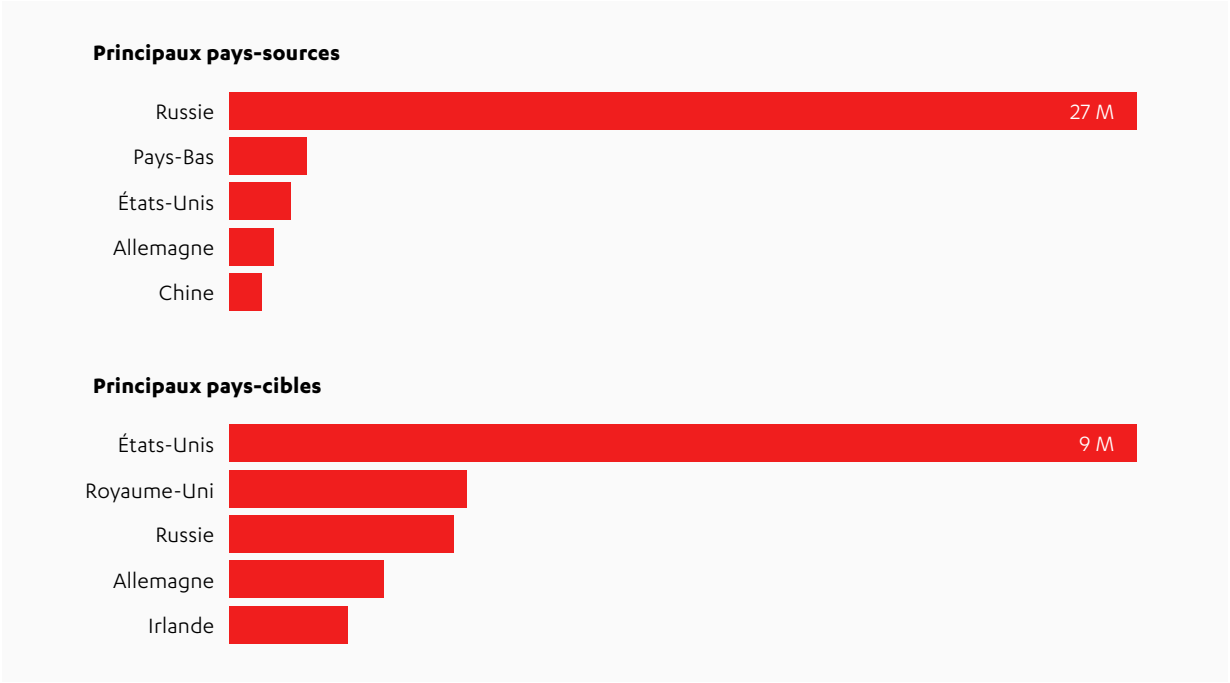
Port	Protocole	Nombre d'attaques
445	SMB	127 M
22	SSH	
25	SMTP	
3306	MySQL	
80	HTTP	
1433	MSSQL	
7547	CWMP	
179	BGP	
21	FTP	
8291	Winbox	

L'activité importante détectée sur le port 445 en provenance du Royaume-Uni est la principale variable expliquant la présence du protocole SMB en tête de cette liste. Un tel score peut indiquer l'utilisation persistante d'exploits comme EternalBlue et de vers SMB. Plusieurs autres logiciels malveillants se servent de ce port comme stratégie d'infection complémentaire : c'est le cas des cryptomineurs et de certains chevaux de Troie, principalement à des fins de déplacement latéral sur les réseaux.

RÉPARTITION DES CYBER ATTAQUES CONCERNANT LE PROTOCOLE SMB



RÉPARTITION DES CYBER ATTAQUES CONCERNANT LE PROTOCOLE SSH



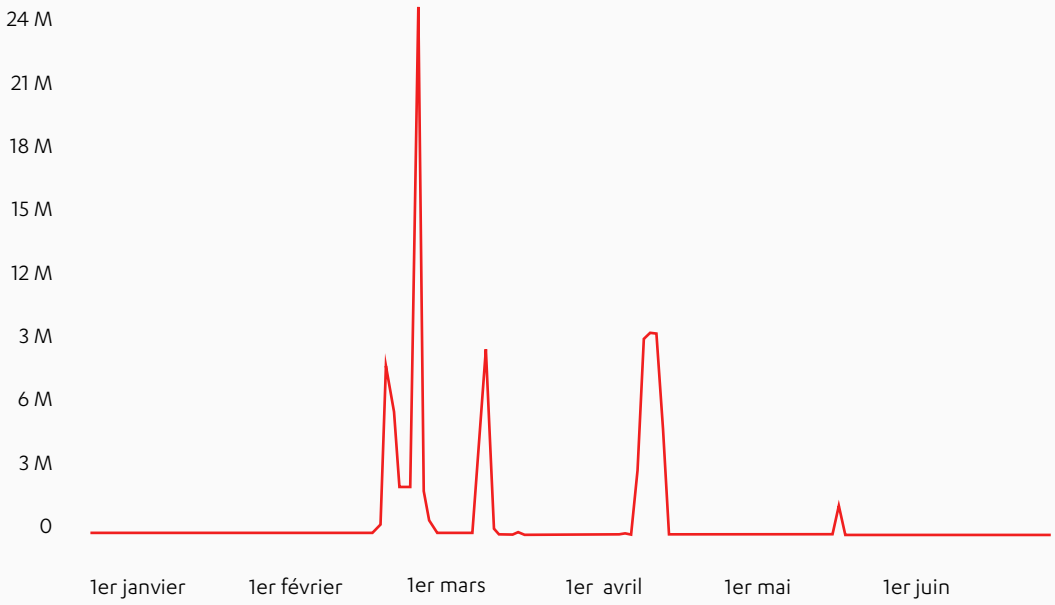
Les attaques SSH indiquent des tentatives d'accès à distance, en tant que root ou administrateur. La Russie reste le principal pays-source du trafic SSH.

ANALYSE PAR PAYS

Il est intéressant d'examiner l'activité de certains pays au cours de ce premier semestre. Plusieurs d'entre eux présentent une activité significative en janvier, suivie d'une accalmie relative, avant une reprise à la mi-avril. Le Royaume-Uni fait exception à cette tendance, tout comme le Danemark.

ROYAUME-UNI

Comme nous pouvons le constater, le Royaume-Uni doit sa première place à quelques campagnes d'envergure, menées tout au long du semestre. La plus importante a eu lieu au début du mois de mars, avec près de 24 millions de ports sondés.



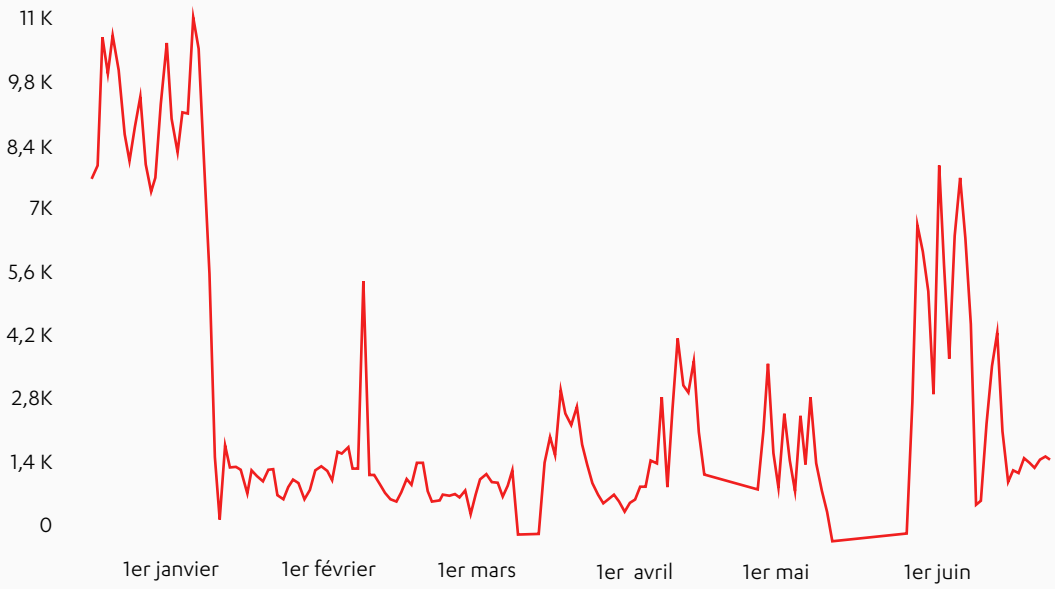
Nombre total d'évènements observés : 97 680 746.

Principaux pays-cibles

Principal port utilisé : 445

ÉTATS-UNIS

Le trafic en provenance des États-Unis a été particulièrement significatif durant les mois de janvier et de juin.



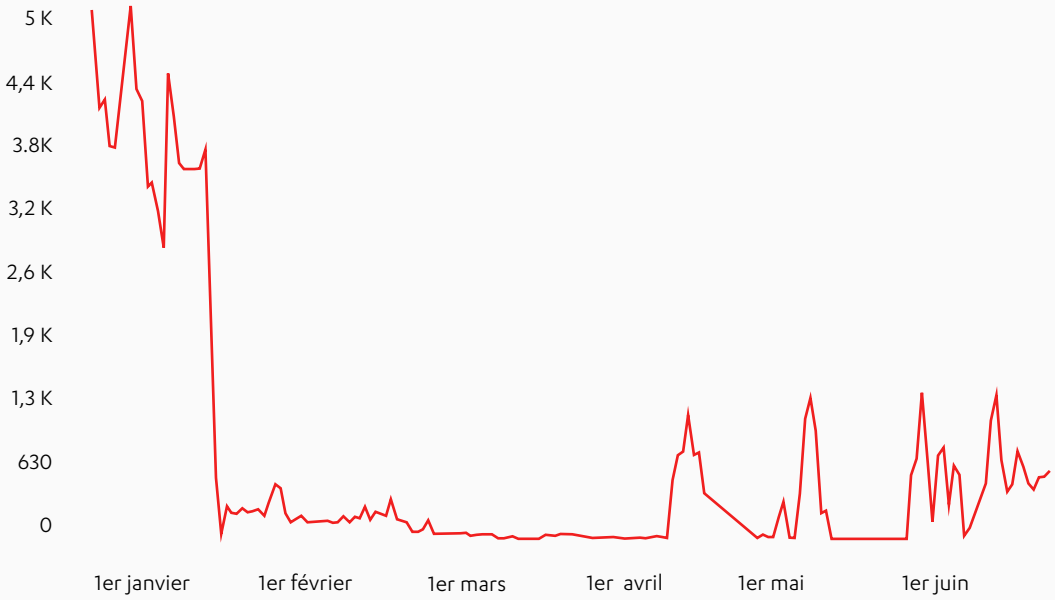
Nombre total d'évènements : 12 185 768

Principaux pays-cibles

Principal port utilisé : 22

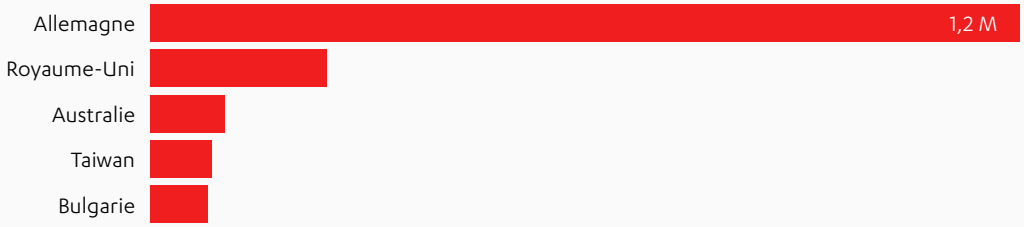
ALLEMAGNE

Tout comme les États-Unis, l'Allemagne a présenté un pic d'activité durant le mois de janvier.



Nombre total d'évènements enregistrés : 29 574 191

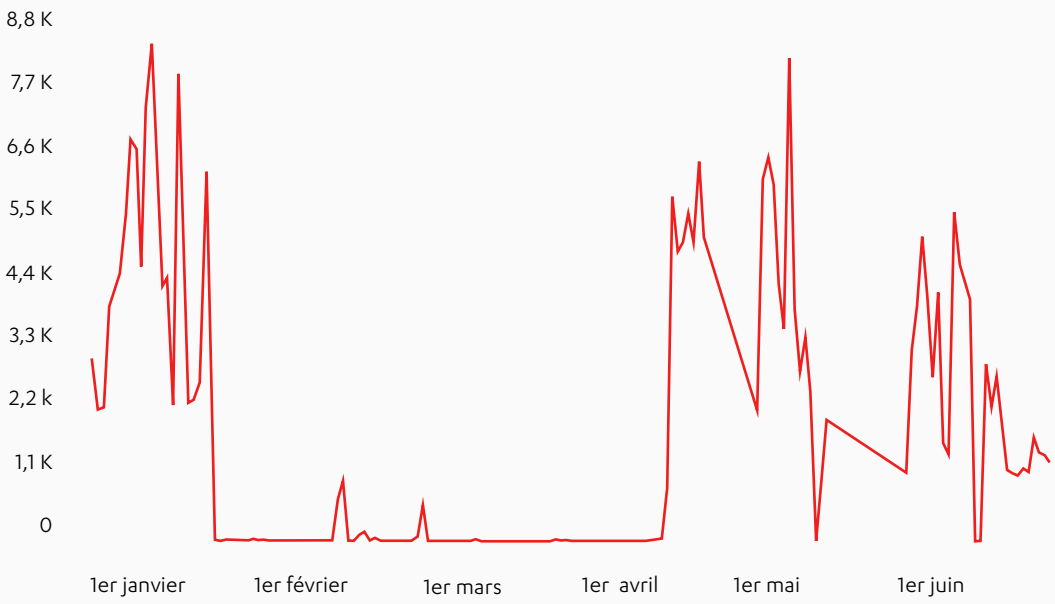
Principaux pays-cibles



Principal port utilisé : 445

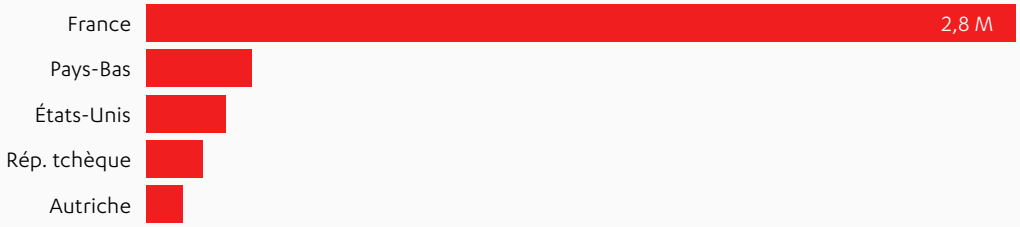
FRANCE

La France a présenté une activité significative en janvier et à partir de la mi-avril.



Nombre total d'évènements : 7 131 905

Principaux pays-cibles



Principal port utilié : 22

FINLANDE

La Finlande, qui fait son apparition dans le top 10, présente des pics d'activité similaires à ceux de la France.

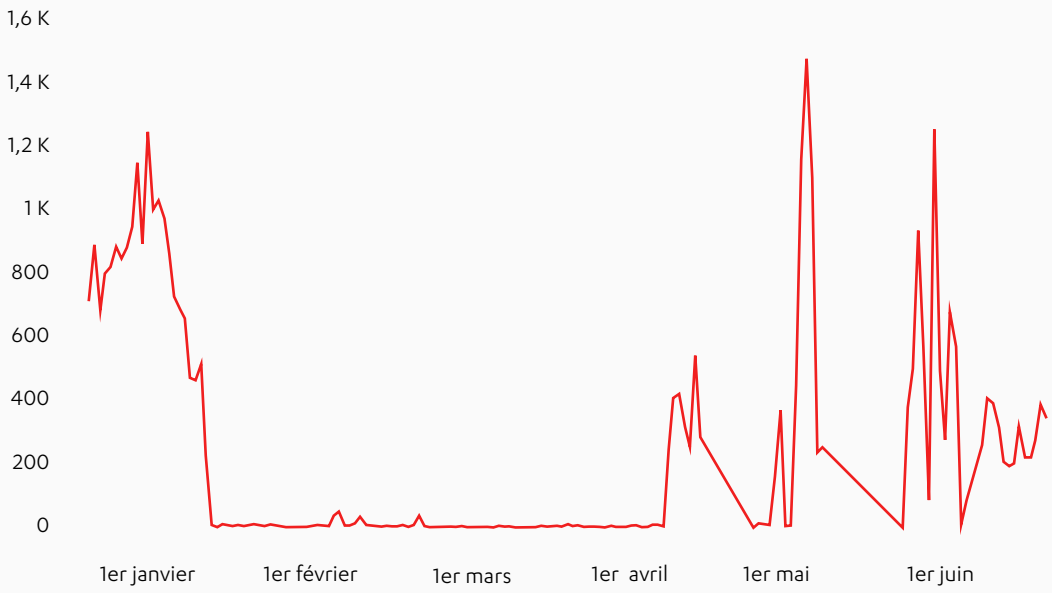
Nombre total d'évènements observés : 1 593 790

Pays-cibles

Principal port utilisé : 22

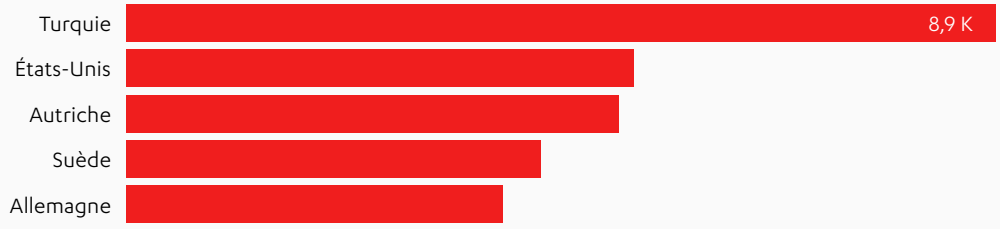
JAPON

Le trafic du Japon suit la tendance observée dans d'autres pays.



Nombre total d'évènements observés : 837 873

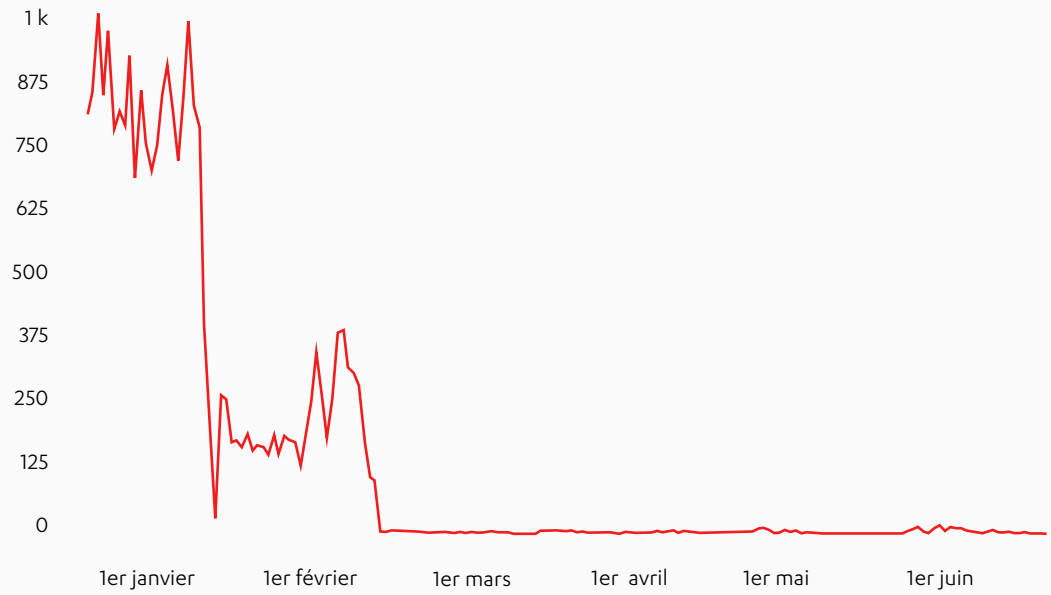
Pays-cibles



Principal port utilisé : 80

DANEMARK

Le Danemark a connu un mois de janvier particulièrement actif, mais contrairement à d'autres pays, cette activité n'a pas repris en avril.



Nombre total d'évènements observés : 60 9315

Pays-cibles

Principal port utilisé : 22

L'ENVIRONNEMENT CLIENT

Lorsqu'un honeypot est visité, nous savons qu'un pirate est actif sur le réseau. Mais que faire si le pirate opère au sein de l'environnement informatique d'un client, sans jamais toucher au honeypot ? Repérer un comportement malveillant parmi tous les autres revient à trouver une aiguille dans une botte de foin.

Dans le cadre de notre service de détection et d'intervention rapide déjà évoqué précédemment, nous déployons des capteurs discrets au sein des environnements informatiques de nos clients afin de leur permettre de détecter les signes d'une éventuelle intrusion. Déployés sur plusieurs ordinateurs à travers l'organisation, ces capteurs sont conçus pour collecter et communiquer les événements bruts à nos systèmes. Nos outils d'intelligence artificielle recherchent ensuite les anomalies comportementales, puis ces détections sont analysées par nos spécialistes afin d'éliminer les faux-positifs. Les menaces réelles, quant à elles, sont signalées au client, à qui nous prodiguons des conseils lui permettant de remédier au problème.

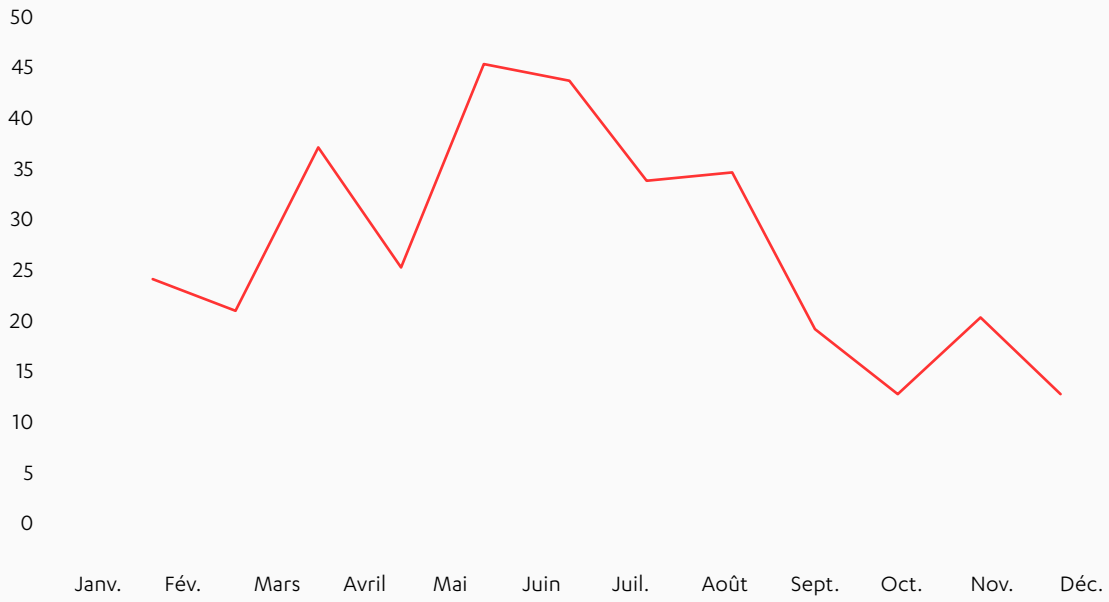
Au cours de ce premier semestre, plusieurs centaines de milliards d'évènements bruts ont été collectés auprès de nos clients. Après analyse des données brutes par notre système back-end, des dizaines de millions d'événements ont été signalés comme suspects. Nos mécanismes de détection, associés à une analyse menée au peigne fin par nos spécialistes, ont permis d'éliminer 99,96 % d'entre eux, évitant ainsi à nos clients de faire face à plusieurs millions de faux-positifs. En fin de compte, seulement 0,003 % des événements suspects, soit quelques centaines pour l'ensemble de notre clientèle, ont été confirmés comme étant des menaces réelles.

Chaque environnement client est unique. Au début de chaque collaboration, plusieurs mois sont donc nécessaires pour déterminer quelles détections restent acceptables sur un réseau donné, et lesquelles constituent une menace. Durant cette période transitoire, nous communiquons plus volontiers avec eux au sujet des détections réalisées, de manière à distinguer les faux-positifs des véritables menaces. Nous devenons ensuite en mesure de procurer une détection extrêmement précise des comportements malveillants. Grâce à nos rapports, nos clients apprennent beaucoup sur leur propre environnement.

LOGICIELS MALVEILLANTS : TENDANCES

Les ransomware, qui dominaient en 2016, sont en recul depuis le second semestre 2017. Ce déclin s'est poursuivi au premier semestre 2018. Les ransomware constituent néanmoins toujours une menace sérieuse : il reste nécessaire de se montrer vigilant et de prendre les précautions qui s'imposent.

Nombre de familles/variantes uniques de ransomware observées par mois, en 2017



Plusieurs facteurs peuvent expliquer cette évolution. Tout d'abord, les victimes de ransomware sont moins disposées à payer la rançon exigée. Des campagnes de sensibilisation comme le projet No More Ransom ont permis de sensibiliser le public. De nombreux utilisateurs ont, de ce fait, effectué des sauvegardes leur permettant de rester protégés. Par ailleurs, l'industrie du ransomware a payé les conséquences des campagnes NotPetya et WannaCry, au cours desquelles les victimes n'ont pas toujours été en mesure de récupérer les fichiers chiffrés après paiement de la rançon. Comme en témoigne notre étude « L'expérience utilisateur des victimes de ransomware » datant de 2016, les pirates spécialistes du ransomware étaient parvenus jusque-là à se forger une réputation de probité, instaurant une confiance relative et incitant les victimes à payer la rançon. Malheureusement pour eux, ces deux campagnes d'attaques ont ruiné leurs efforts.

Le recul des ransomware peut également être attribué aux performances des antivirus, capables de bloquer efficacement les menaces standards répandues. Pour contourner ces mesures de protection, les pirates envoient des spams contenant des pièces jointes particulières : des macro-documents protégés par un mot de passe dévoilé dans le corps de l'e-mail. Ce procédé empêche les détections antivirus car le fichier ne s'exécute qu'une fois le mot de passe entré. Le spam constitue toutefois l'une des formes d'ingénierie sociale les moins efficaces : le fait que les pirates en viennent à utiliser ce type de stratégies est révélateur de l'efficacité des antivirus : sans recours aux mots de passe, les fichiers infectés sont bel et bien neutralisés.

L'abandon des ransomware implique inévitablement l'émergence d'autres menaces. Durant ce premier semestre 2018, le cryptojacking et les « arnaques à la romance » sont venus occuper l'espace laissé vacant. Le piratage cryptographique, ou l'utilisation non-autorisée de l'ordinateur d'une victime pour extraire de la cryptomonnaie (principalement Monero), a émergé mi-2017 et connaît depuis une popularité croissante. Les scripts de cryptomining se déplacent désormais latéralement sur les réseaux d'entreprise à l'aide d'exploits comme EternalBlue, en association avec des techniques d'acquisition de certificats de type Mimikatz.

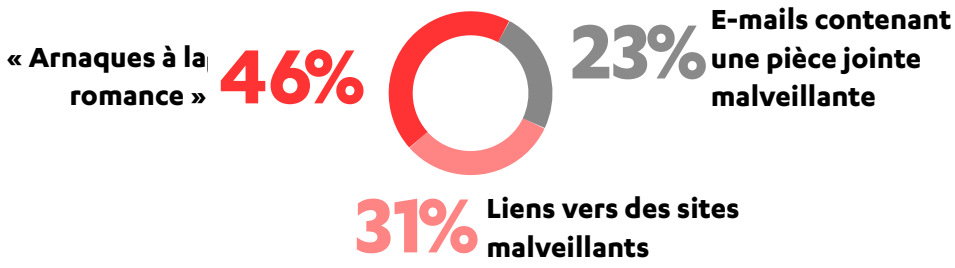
Les objets connectés continuent de susciter l'intérêt des pirates en quête de bots. En témoigne le malware le plus commun observé à partir de nos honeypots : PNScan, un cheval de Troie Linux qui infecte les appareils connectés et les routeurs Linux mal sécurisés. Linux n'a jamais été un système d'exploitation très populaire mais il a su séduire les pirates contrôleurs de bots. Cette tendance peut s'expliquer par l'amélioration continue de la sécurité des PC, ou par le fait que les PC potentiellement exploitables sont déjà utilisés par d'autres botnets.

La cyber menace bancaire la plus marquante au premier semestre 2018 a été Trickbot. Trickbot, qui a sévi en particulier en Scandinavie, a émergé en 2016. Progressivement, de nouvelles fonctionnalités y ont été intégrées par les hackers. Sur la liste des victimes, figurent plus de 400 banques : parmi elles, on retrouve la plupart des grandes banques scandinaves, ainsi que de grandes banques américaines et européennes. Trickbot utilise d'abord EternalBlue pour infecter les systèmes Windows non-patchés, puis Mimikatz pour récupérer des identifiants et s'en servir sur des systèmes déjà patchés. Une version de Trickbot a également intégré XMRig, module d'extraction capable de miner des cryptomonnaies, comme source alternative de revenus.

LE SPAM RESTE UN PUISSANT OUTIL

Les e-mails de spam contenant des URL et des pièces jointes malveillantes ont constitué la première méthode d'infection utilisée par les pirates au premier semestre 2018. 31 % de ces spams comportaient des liens vers des sites web malveillants, tandis que 23 % d'entre eux contenaient une pièce jointe infectée. 85 % des pièces jointes en question présentaient les extensions suivantes : 7Z, DOC, PDF, XLS et ZIP. La plupart renfermaient des infostealers, des RAT ou des chevaux de Troie bancaires.

Les « arnaques à la romance » opèrent un retour en force : elles représentent les 46% de spams restants. Ces e-mails font croire au destinataire qu'il lui est possible de communiquer avec une personne célibataire et disponible, de manière à en tirer profit. Il peut simplement s'agir de convaincre la victime de s'inscrire à un site de rencontre payant. Dans d'autres cas, l'individu mal intentionné utilise un canular tristement familier qui consiste à faire tomber sa victime amoureuse, pour lui soutirer ensuite de l'argent.

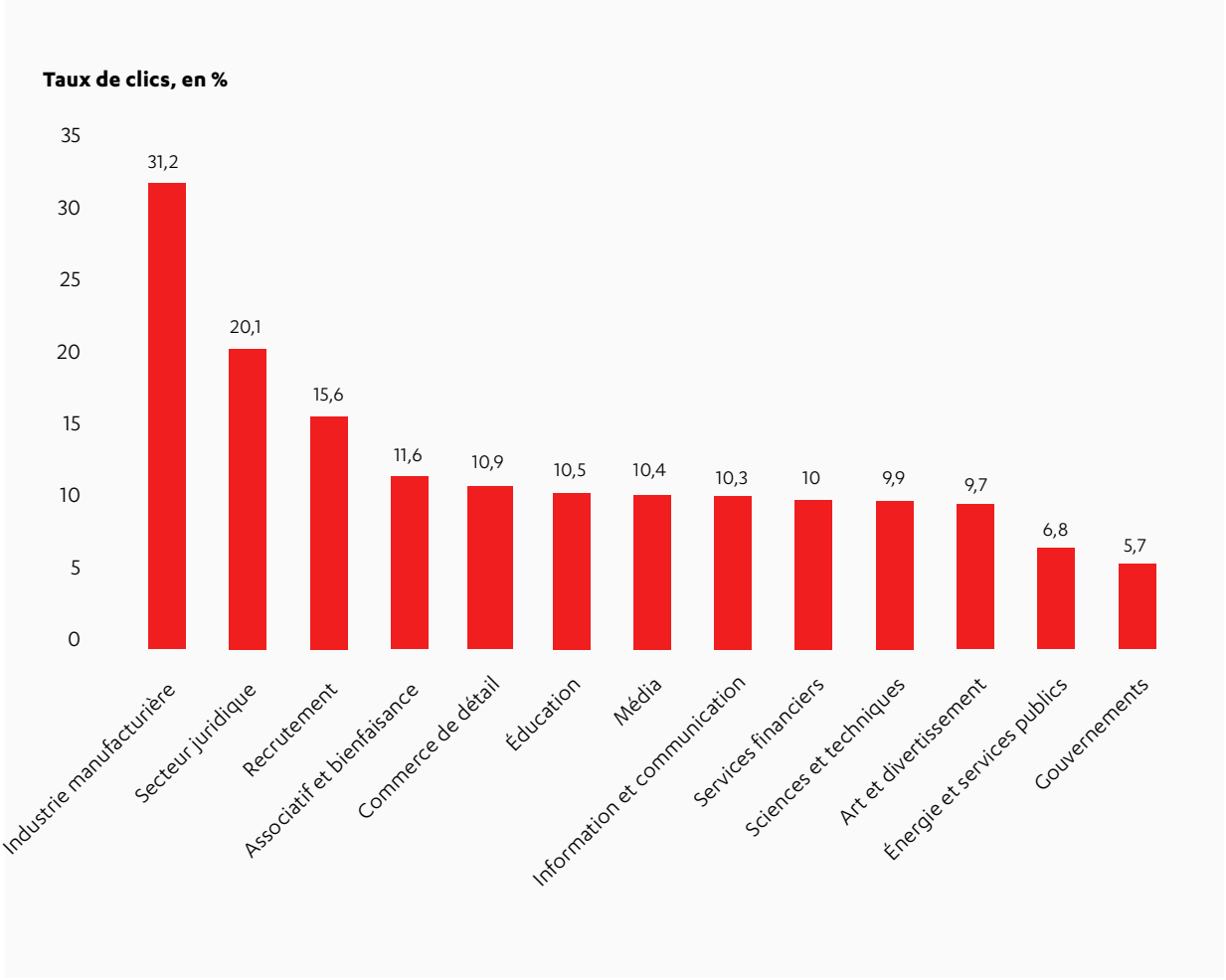


Échantillons de spams au printemps 2018

Les données de phishd, plateforme d'évaluation du phishing de MWR Infosecurity, confirment l'efficacité croissante du spam. Le taux de clics sur les e-mails envoyés aux organisations clientes via la plateforme est passé de 13,4 % au deuxième semestre de 2017 à 14,2 % en 2018.

Cette recrudescence du spam peut être attribuée à l'amélioration de la sécurité des systèmes contre d'autres menaces. La prise en charge désormais marginale de Flash Player par les navigateurs, qui permettait aux pirates d'exécuter facilement des kits d'exploits, a par exemple joué un rôle majeur dans le déclin de ce type de malware. Les hackers se sont trouvés contraints de recourir à nouveau à leur plus vieil outil, le spam. Toutefois, les utilisateurs ont été sensibilisés et les attaques d'hier ne fonctionnent plus aujourd'hui. Le spam a donc dû évoluer pour rester efficace.

Par ailleurs, internet stimule notre attention de manière parfois exagérée, si bien que notre vigilance s'en trouve altérée. Il nous arrive de cliquer sans réfléchir. À l'instar de tout utilisateur, les cadres sont susceptibles d'être victimes d'attaques de spam, car leur boîte de réception est souvent si saturée qu'il leur est difficile d'évaluer la légitimité de chaque e-mail.



Taux de clics des spams, par secteur d'activité, tels que recueillis par la plateforme phishd au cours des cinq dernières années.

Les recherches de MWR Infosecurity révèlent les nouvelles caractéristiques que revêt le spam pour devenir plus efficace :

Un expéditeur prétendument connu
Le facteur le plus influent sur le taux de clic est la provenance apparente du spam. Lorsque ce dernier prétend provenir d'un expéditeur connu, il obtient un taux de clics de +12%.

Aucune faute d'orthographe dans l'objet.
L'objet de l'e-mail est un élément-clé du succès d'un spam. Il doit être crédible, et donc exempt d'erreur. Un objet sans faute de grammaire ou d'orthographe améliore le taux de succès du spam de 4,5%.

Une urgence subtile, plutôt que trop explicite.
Lorsque les spams font état d'une urgence implicite plutôt qu'absolue, ils obtiennent un taux de clic d'1% supérieur. « Des informations supplémentaires sont nécessaires pour compléter votre commande » aura davantage de succès que « RÉPONDEZ MAINTENANT OU VOTRE COMMANDE SERA ANNULÉE ! ».

CONCLUSION

La cyber sécurité n'a qu'une seule constante : le changement. Ce constat reste valable en 2018. Nous n'avons de cesse d'améliorer la sécurité des systèmes et de sensibiliser les utilisateurs. Progressivement, les logiciels les plus vulnérables sont abandonnés. Mais malheureusement, les pirates s'adaptent : ils ajustent leurs stratégies afin de continuer à sévir. Le piratage cryptographique émerge comme nouvelle tendance et, parallèlement, des outils vieux comme le monde, comme le spam ou les arnaques à la romance, s'offrent une nouvelle jeunesse et opèrent un retour en force. Dans le même temps, de nouveaux pays se hissent en haut du classement des pays-sources de cyber attaques. Une certitude : l'immobilisme n'a pas sa place dans la course qui nous oppose au côté obscur du monde connecté.