proofpoint

RAPPORT

RAPPORT TRIMESTRIEL SUR LES MENACES

3E TRIM. 2017

proofpoint.com/fr

Le *rapport trimestriel sur les menaces de Proofpoint* met en lumière les menaces, les tendances et les principaux points à retenir que nous avons observés au sein de notre vaste clientèle et dans le paysage des menaces de manière plus générale.

Chaque jour, nous analysons plus d'un milliard d'e-mails, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malware afin de protéger les entreprises du monde entier contre les menaces avancées. Nous suivons constamment de près les trois principaux vecteurs de propagation des menaces sophistiquées, à savoir la messagerie électronique, les médias sociaux et les technologies mobiles. Nous bénéficions ainsi d'une perspective unique pour identifier et analyser les tactiques, les outils et les cibles des cyberattaques en vogue aujourd'hui.

Ce rapport vise à vous doter de renseignements directement exploitables que vous pourrez utiliser pour mieux lutter contre les attaques actuelles, anticiper les tendances émergentes et gérer votre approche en matière de sécurité. En plus de tirer des conclusions, ce rapport recommande une série de mesures à prendre pour protéger vos collaborateurs, vos données et votre marque.

SOMMAIRE

PRINCIPAUX POINTS À RETENIR : RETOUR VERS LE FUTUR

Ces dernières années, le troisième trimestre est devenu un point névralgique pour les chercheurs en menaces. En effet, il enregistre des niveaux record en termes de volume de messages et offre un aperçu des outils et techniques que les cybercriminels utiliseront dans les mois à venir. Le troisième trimestre de cette année ne déroge pas à cette règle.

Les e-mails recourant à des URL malveillantes ont littéralement explosé et sont parvenus, en à peine plus de deux ans, à représenter la majeure partie des attaques par e-mail (par opposition à celles utilisant des pièces jointes). Les ransomwares et les chevaux de Troie demeurent les charges actives de prédilection.

Les techniques d'ingénierie sociale et de ciblage ont quant à elles évolué en fraudes par e-mail et en attaques sur les médias sociaux.

Par ailleurs, notre première analyse publique des domaines similaires utilisés pour mener une série d'attaques et de fraudes révèle que les cybercriminels sont en train de remporter la course à l'enregistrement des domaines. Pour chaque enregistrement « défensif » d'une entreprise agissant de manière proactive, nous avons épinglé vingt enregistrements de domaines similaires suspects.

Voici les principaux points à retenir pour ce trimestre.

MESSAGERIE ÉLECTRONIQUE

Le volume de messages malveillants a augmenté de 85 % par rapport au trimestre précédent, sous l'impulsion des nombreuses attaques recourant à des URL malveillantes.
Le volume de messages contenant des URL malveillantes pointant vers des malwares hébergés a grimpé de près de 600 % par rapport au trimestre précédent, et de plus de 2 200 % par rapport au même trimestre de l'année précédente. Cette montée en puissance a accentué une tendance observée au premier semestre : ces messages représentent désormais la majorité des attaques par e-mail (par opposition à celles utilisant des pièces jointes) identifiées depuis 2014. Les campagnes de grande envergure recourant à des pièces jointes malveillantes ont cependant également contribué à cette hausse, grâce à des malwares dissimulés dans des fichiers d'archive compressés.

Les ransomwares restent en tête des catégories de malwares.
Les ransomwares représentent près de 64 % de toutes les tentatives de distribution d'e-mails malveillants au sein de notre clientèle mondiale. De nouvelles souches de ransomwares voient quotidiennement le jour, mais Locky demeure la principale charge active. Cette menace représente près de 55 % du volume total de messages et plus de 86 % du nombre de ransomwares. Parallèlement, des souches connues sous le nom de Philadelphia et GlobeImposter ont évolué, passant du rang de petites variantes circonscrites au niveau régional en menaces mondiales, grâce à quelques campagnes de grande envergure menées par le même individu.

CHEVAUX DE TROIE BANCAIRES
Ce type de malware a pour but de dérober des identifiants bancaires, généralement en redirigeant le navigateur des victimes vers une version factice du site Web de leur banque ou en injectant de faux formulaires de connexion sur le site réel.

ETERNALBLUE
EternalBlue est un outil de piratage puissant qui exploite une faille d'un composant de partage de fichiers de Windows. Dérobé à la NSA, il a été dévoilé publiquement début 2017.

LES CHEVAUX DE TROIE BANCAIRES représentent 24 % du nombre total de messages malveillants, The Trick étant à lui seul responsable de 70 % de ce volume.
Soutenu par des attaques massives menées par un cybercriminel, The Trick a détrôné la souche Dridex en tant que principal cheval de Troie bancaire. (Après une accalmie qui avait perduré quasiment tout le premier trimestre, Dridex avait refait son apparition dans de vastes campagnes au deuxième trimestre.) Aux côtés d'Ursnif, de Bancos et de Zloader, Dridex a poursuivi son travail de sape dans des campagnes ciblant des régions spécifiques. Une nouvelle version de Retefe a également fait son apparition. Celle-ci s'est propagée via **ETERNALBLUE**, un exploit développé par la NSA qui avait été mis au jour par un groupe de pirates.

Les fraudes par e-mail ont augmenté de 29 % par rapport au trimestre précédent.
La fréquence des attaques s'est également intensifiée : les tentatives de fraude par e-mail par entreprise ciblée sont en hausse de 12 % par rapport au trimestre précédent et de 32 % par rapport au même trimestre de l'année précédente. Bien que ce type de fraude ne fasse pas de discrimination selon la taille des entreprises, celles aux chaînes d'approvisionnement plus complexes sont davantage ciblées.

KITS D'EXPLOIT
Exécutés sur le Web, ces kits détectent et exploitent les failles des ordinateurs qui s'y connectent. Bien souvent vendus sous la forme de services aux auteurs d'attaques, ils permettent d'infecter facilement des ordinateurs à l'aide de téléchargements de malware à l'insu de l'utilisateur (drive-by).

KITS D'EXPLOIT ET ATTAQUES WEB

Le trafic associé aux KITS D'EXPLOIT est resté stable, mais à 10 % seulement du pic observé en 2016.
Le kit d'exploit RIG représente à lui seul 76 % de toute l'activité due à ce type d'attaque. Les cybercriminels associent aujourd'hui divers stratagèmes d'ingénierie sociale à leurs campagnes de kit d'exploit. Cette tendance suggère qu'ils n'entendent pas se limiter aux seuls exploits, de plus en plus difficiles à obtenir.

ENREGISTREMENT DÉFENSIF
Pratique recommandée consistant à acheter des domaines Internet susceptibles d'être confondus avec les vôtres avant que des cybercriminels ne le fassent. Les domaines similaires peuvent être utilisés pour tromper les clients et les partenaires commerciaux au moyen de faux sites Web ou d'e-mails frauduleux semblant émaner de votre entreprise.

PHISHING ANGLER
Cette forme de phishing consiste à créer des comptes d'assistance à la clientèle factices sur les médias sociaux. Le but est d'attirer les clients et abonnés en quête d'aide sur un site de phishing ou de leur soutirer des informations de connexion.

TA505
Motivé par l'appât du gain, ce cybercriminel est à l'origine de quelques-unes des plus grandes campagnes d'attaque par e-mail observées, dont celles ayant contribué à diffuser les chevaux de Troie bancaires Dridex et The Trick, les ransomwares Locky et Jaff, et bien d'autres encore.

LOCKY
Cette souche de ransomware la plus courante dans les e-mails malveillants chiffre les données de la victime et les garde « en otage » jusqu'à ce que celle-ci paie la rançon pour pouvoir les récupérer. Durant une bonne partie de l'année 2016 et quelques mois de l'année 2017, Locky a été responsable de la majorité du trafic lié aux e-mails malveillants.

DOMAINES

Les enregistrements de domaines suspects l'ont largement emporté sur les ENREGISTREMENTS DÉFENSIFS, avec un rapport de 20 pour 1.
Si certaines entreprises enregistrent des domaines à tout-va pour lutter contre le typosquattage et l'usurpation de domaines, ce n'est pas le cas de la majorité d'entre elles. Les enregistrements défensifs de domaines appartenant aux marques ont chuté de 20 % par rapport à la même période l'année précédente, tandis que les enregistrements de domaines suspects ont augmenté de 20 %.

MÉDIAS SOCIAUX

Les comptes d'assistance factices, utilisés pour des attaques dites de PHISHING ANGLER, ont doublé par rapport au même trimestre de l'année précédente.
Le nombre de comptes d'assistance à la clientèle factices a augmenté de 5 % par rapport au trimestre précédent, tandis que le volume de liens de phishing sur les canaux sociaux des enseignes a enregistré une hausse de 10 %.

TENDANCES EN MATIÈRE DE MENACES PROPAGÉES PAR E-MAIL

Chiffres clés : Les campagnes de propagation de malwares par e-mail ont augmenté de près de 600 % par rapport au trimestre précédent, et de plus de 2 200 % par rapport à la même période de l'année précédente.

Le volume de messages frauduleux distribuant des malwares au moyen d'URL malveillantes a fortement augmenté. **TA505**, un cybercriminel particulièrement prolifique connu pour ses campagnes massives de propagation de Locky, est l'un des principaux responsables de cette hausse. Il a en effet délaissé les pièces jointes au profit des URL pour assurer la diffusion du ransomware. Il est également à l'origine de la diffusion des ransomwares Philadelphia et GlobeImposter et du cheval de Troie bancaire The Trick dans des volumes tels qu'il est parvenu à faire la différence.

Ce bond a contribué à faire grimper le volume total de messages malveillants de 85 % par rapport au trimestre précédent, et ce malgré une chute de 74 % du volume d'e-mails contenant des pièces jointes malveillantes.

Les pièces jointes malveillantes n'en demeurent pas moins un moyen de diffusion essentiel. Les cybercriminels ont notamment lancé plusieurs campagnes par e-mail avec pièce jointe malveillante, quoique dans une mesure plus limitée, de même que quelques campagnes de très grande envergure dissimulant du code malveillant dans des fichiers d'archive compressés. Ces campagnes font appel à des formats de fichiers d'archive RAR et 7-Zip, contenant généralement des scripts JavaScript ou VBScript malveillants. En cas d'exécution, ces derniers téléchargent et installent le ransomware **LOCKY**.

Comme le montrent les figures 1 et 2, les messages contenant des URL malveillantes représentent désormais 64 % du volume total de messages. Un tel pourcentage n'avait plus été atteint depuis 2014, dernière année où les messages contenant des URL malveillantes avaient constitué la majorité des campagnes d'attaque par e-mail. Au bout du compte, ces deux approches tendaient vers des objectifs similaires : que la distribution soit assurée par des URL ou des pièces jointes, Locky constituait la charge active de la majorité de ces campagnes massives.

Volumes quotidiens indexés de messages malveillants par type d'attaque, depuis le début de l'année 2017

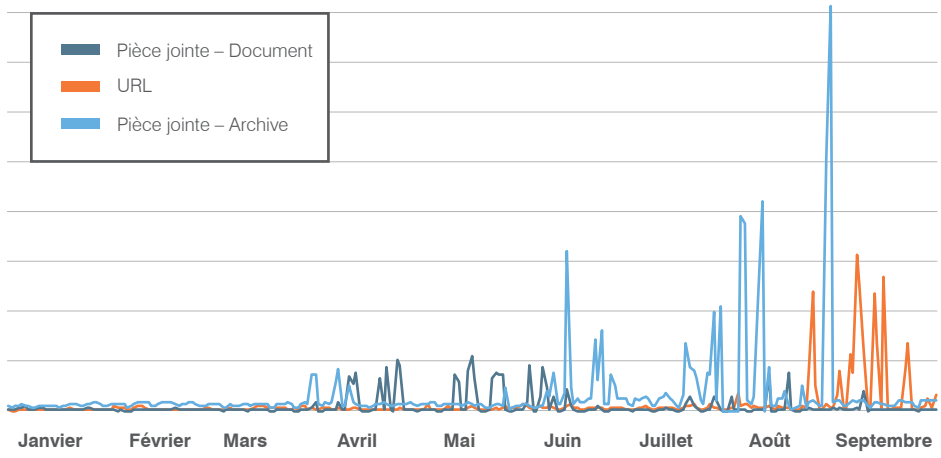

Figure 1. Volumes indexés par type d'attaque, tendances de janvier 2017 à septembre 2017 (273 jours)

Comparaison de volumes quotidiens indexés de messages malveillants par type d'attaque, 3e trimestre 2017

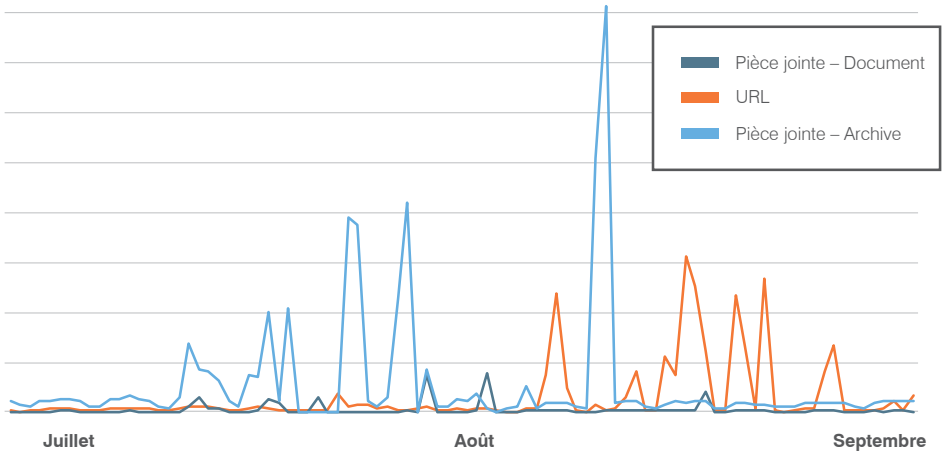

Figure 2. Volumes indexés par type d'attaque, tendances de juillet 2017 à septembre 2017 (92 jours)

La figure 3 illustre la prédominance continue des ransomwares, en particulier Locky. Quelques campagnes de grande envergure ayant pour but de diffuser le cheval de Troie bancaire **THE TRICK** ont enregistré des pics en fin de trimestre.

THE TRICK
Également connu sous le nom de Trickbot, The Trick est un cheval de Troie bancaire étroitement lié à Dyre. Bien que les responsables de la propagation de Dyre aient été arrêtés par les autorités russes en 2015, le malware a connu une résurgence en 2017.

Ransomwares, chevaux de Troie bancaires et autres malwares

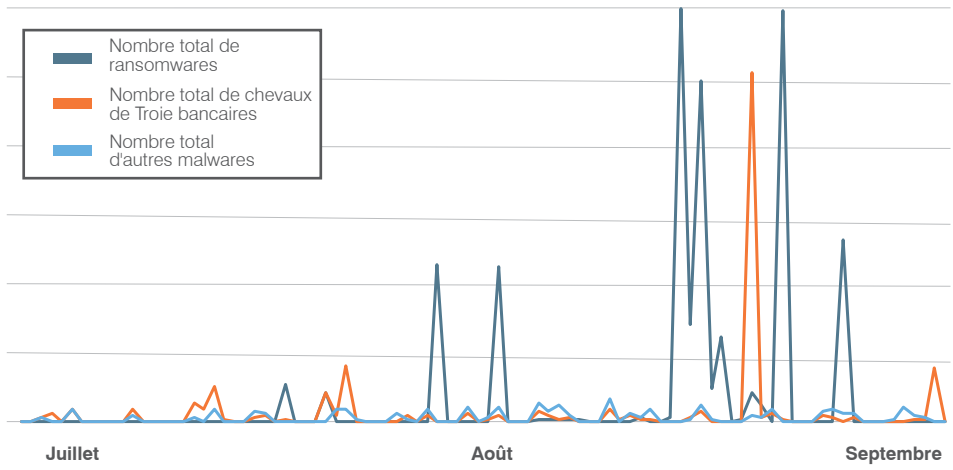

Figure 3. Juillet 2017 à septembre 2017 (92 jours)

CHEVAUX DE TROIE BANCAIRES : DE NOUVELLES TENDANCES POUR DES ACTEURS DE LONGUE DATE

Chiffres clés : The Trick représente à lui seul 70 % de tous les messages visant à distribuer des chevaux de Troie bancaires.

La majorité de ces e-mails malveillants sont le fait de TA505, déjà à l'origine des campagnes par e-mail massives de distribution du ransomware Locky et du cheval de Troie bancaire Dridex.

Délaissé par TA505 au profit de The Trick, **DRIDEX** a enregistré une forte baisse de son trafic. L'activité associée à **ZLOADER** est quant à elle restée stable une bonne partie du trimestre, quoique à des niveaux inférieurs à ceux du deuxième trimestre. Zeus Panda, Emotet et URLZone ont quant à eux fait leur apparition dans de vastes campagnes ciblées sur des régions spécifiques.

Certains chevaux de Troie bancaires tels que **RETEFE** et The Trick se sont associés à l'exploit EternalBlue, ce qui laisse entrevoir des possibilités de développement plus avant, dans la mesure où ils peuvent se propager sans aide au sein de réseaux internes après l'infection initiale de la messagerie. Retefe, qui ciblait principalement des banques suisses au moyen de leurres en allemand, n'a jamais atteint le niveau de Dridex ou de Zeus, que ce soit en termes de volume ou de portée. Ces « ricochets » de l'attaque **WANNACRY** — qui s'est également fondée sur EternalBlue — laissent toutefois entrevoir une tendance potentielle pour 2018. Les cybercriminels pourraient être plus nombreux à profiter des failles de sécurité mises au jour par WannaCry et NotPetya.

La figure 4 illustre les différents chevaux de Troie bancaires identifiés au quotidien. Les pics de trafic associé à The Trick ponctuent ce trimestre, en éclipsant les bonds plus limités essentiellement dus à Zloader et à Panda Banker.

DRIDEX
Dridex est un cheval de Troie bancaire très répandu distribué par le biais de divers vecteurs, principalement la messagerie électronique, afin d'infecter les victimes et de faire main basse sur des identifiants bancaires.

ZLOADER
Également connu sous le nom de Terdot, Zloader est un programme de téléchargement souvent utilisé en combinaison avec le cheval de Troie bancaire Zbot et d'autres variantes de malware.

RETEFE
Ce cheval de Troie bancaire a essentiellement ciblé certaines régions d'Europe. Plutôt que d'injecter de faux formulaires de connexion sur des sites Web bancaires légitimes (à l'instar de nombreux chevaux de Troie bancaires), il redirige l'utilisateur vers une version factice du site par le biais d'une série de serveurs proxy.

WANNACRY
Ce ransomware a infecté des dizaines de milliers de systèmes dans plus de 150 pays à travers le monde en mai dernier, dans le cadre de l'une des plus vastes cyberattaques à ce jour. Il s'est propagé via une faille d'un composant de partage de fichiers de Microsoft Windows.

Principaux chevaux de Troie bancaires — Volumes quotidiens indexés par type d'attaque, tendances au 3e trimestre 2017

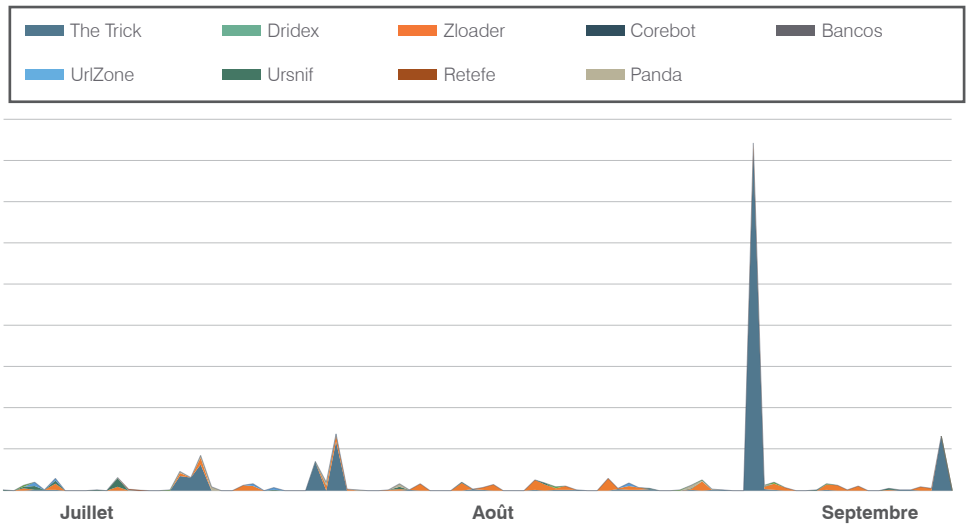

Figure 4. Volumes quotidiens indexés de messages pour les principales souches de chevaux de Troie bancaires, de juillet à septembre 2017

RANSOMWARE : INTENSIFICATION DES CAMPAGNES LOCKY ET PROGRESSION DES RANSOMWARES DESTRUCTEURS

Chiffres clés : Les tentatives de distribution de ransomwares représentent près de 64 % du volume total de messages malveillants au sein de notre clientèle mondiale.

Les ransomwares continuent de dominer le paysage des menaces. De nouvelles variantes apparaissent chaque jour, le développement de ransomwares destructeurs persiste et les attaques ciblées se multiplient.

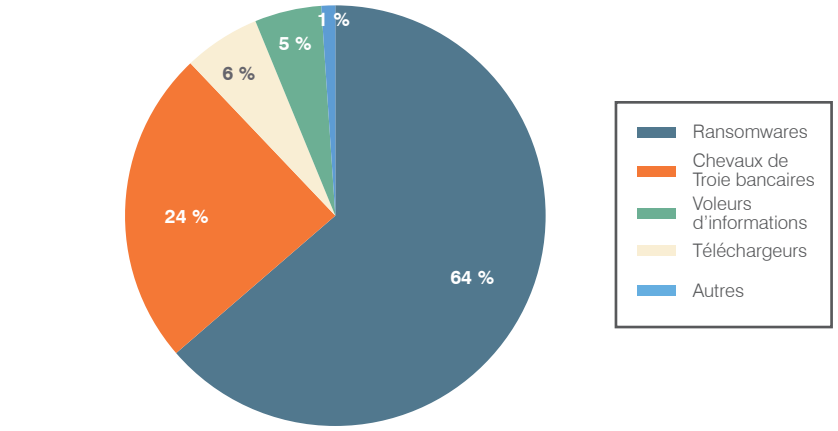

Figure 5. Comparaison du volume de messages global au cours du trimestre

La plupart des ransomwares sont apparus dans des campagnes de propagation de Locky de très grande envergure orchestrées par TA505. Le pirate n'en est cependant pas resté là, puisqu'il est également à l'origine de la diffusion des variantes GlobeImposter et Philadelphia du ransomware. Une de ces souches contenait notamment une version « hors ligne » de Locky qui ne nécessitait aucune infrastructure centrale de commande et contrôle pour chiffrer les fichiers des victimes de l'attaque.

D'autres cyberpirates ont délaissé les campagnes massives menées au hasard au profit d'attaques plus ciblées. L'un d'eux a notamment introduit la souche de ransomware Defray dans des attaques à petite échelle qui ont ciblé les secteurs des soins de santé et de l'éducation en août dernier. D'autres cybercriminels leur ont emboîté le pas. Ainsi, plusieurs nouveaux **ID D'AFFILIATION** propres à Locky sont apparus dans des campagnes visant principalement des établissements d'enseignement supérieur et de soins de santé. Au moins l'un d'entre eux (Affid=36) a distribué la version hors ligne de Locky.

D'autres souches ont émergé dans la foulée des attaques WannaCry et Petya en Ukraine à la fin du deuxième trimestre. Hell (découvert en juillet) et IsraByte (identifié en août) ne sont pas parvenus à s'imposer ni à attirer la publicité souhaitée. Mais à l'instar de **NOTPETYA** et de WannaCry, ils semblaient avoir davantage pour but de détruire que d'engranger des profits.

Comme le montre la figure 6, les auteurs de campagnes de grande envergure se sont rassemblés autour d'un nombre plus restreint de souches de ransomware au troisième trimestre, malgré l'apparition de nouvelles souches et utilisations. Sous l'impulsion de TA505, Locky, GlobeImposter et Philadelphia ont occupé le devant de la scène, tandis que de nouveaux distributeurs de Locky sont venus grossir les rangs. Certaines souches telles que SAGE et TorrentLocker ont pratiquement disparu.

ID D'AFFILIATION
Il arrive souvent que les auteurs de malwares engagent des affiliés pour qu'ils se chargent de la propagation contre rémunération. Ces affiliés reçoivent chacun un ID qui est codé en dur dans les versions du malware et qui désigne sans équivoque l'auteur d'une infection, lequel peut ainsi percevoir la rétribution.

NOTPETYA
Cette souche de malware qui se fait passer pour le ransomware Petya serait en fait un outil commandité par un État conçu pour semer la pagaille plutôt qu'obtenir une rançon.

Principales souches de ransomwares — Volumes quotidiens indexés, tendances au 3e trimestre 2017

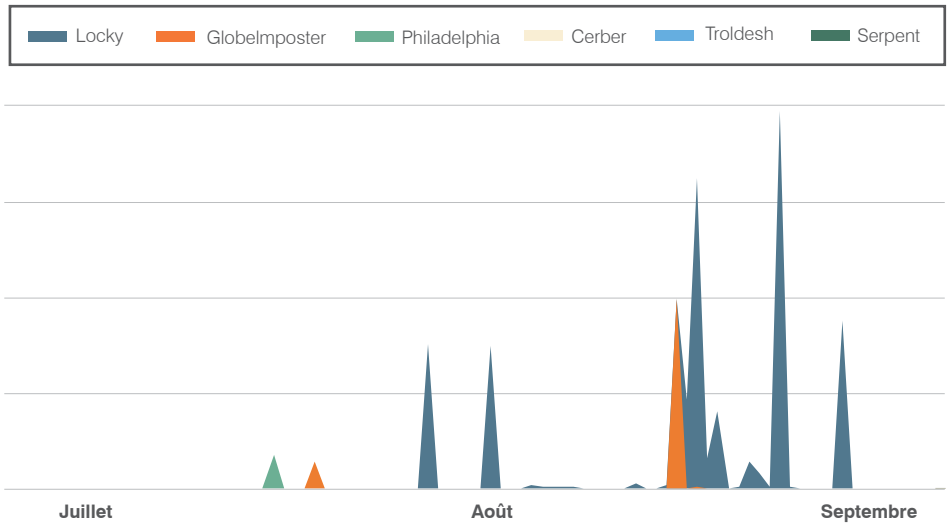

Figure 6. Volumes quotidiens indexés de messages pour les principales souches de ransomware, de juillet à septembre 2017

RANSOMWARE
Ce type de malware prend en otage les données de ses victimes en les chiffrant, puis exige le paiement d'une rançon pour les déverrouiller.

La croissance quasiment exponentielle des nouvelles souches de **RANSOMWARE** tout au long de l'année dernière semble finalement ralentir quelque peu — mais en aucun cas à cause d'un fléchissement de la menace.

En moyenne, 1,4 nouvelle souche de ransomware est apparue chaque jour, soit une baisse par rapport au trimestre précédent (1,8 nouvelle souche par jour). Cette diminution est probablement imputable à un déclin des souches de type « projet mineur », validation de concept (PoC) et expérimental ou générées par des « script kiddies », qui avaient contribué à gonfler les chiffres antérieurs.

En d'autres termes, ce fléchissement ne reflète nullement une baisse de la menace associée aux ransomwares. Il suggère plutôt que les cybercriminels se concentrent désormais sur un nombre restreint de souches plus efficaces pour développer de nouvelles méthodes d'utilisation des ransomwares et ainsi gagner en sophistication (figure 7).

Nouvelles souches signalées

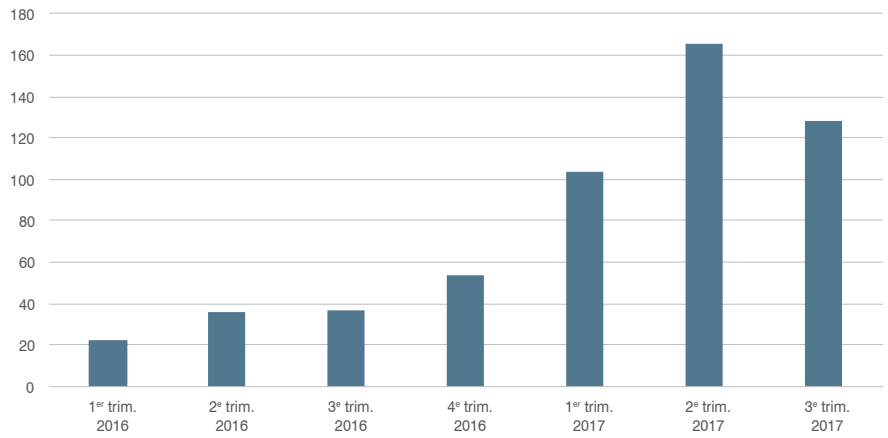

Figure 7. Nouvelles souches de ransomwares signalées par trimestre, 2016 et 2017 (jusqu'au moment de la rédaction)

DES MINEURS MALVEILLANTS

Les malwares mineurs de **CRYPTOMONNAIE** utilisent les ressources système des machines qu'ils infectent pour générer de l'argent électronique au profit de pirates. Les cryptomonnaies telles que Bitcoin et Litecoin possèdent des mécanismes intégrés qui préservent la rareté de la devise et en garantissent la valeur. Ces protections compliquent fortement les calculs nécessaires pour « miner » (générer) de nouvelles unités. Le minage de la cryptomonnaie la plus connue et largement répandue, Bitcoin, nécessite désormais une puissance de calcul énorme, proche de celle des superordinateurs. Toutefois, d'autres cryptomonnaies telles que Litecoin et Monero peuvent encore être minées à l'aide d'un ordinateur de bureau... ou en siphonnant la puissance de calcul d'un grand nombre de systèmes clients.

Dès lors les malwares de minage pour ces cryptomonnaies sont en expansion. Ils sont propagés via des kits d'exploit, des stratagèmes d'ingénierie sociale et même des exploits de la NSA tels que EternalBlue. The Pirate Bay a fait les gros titres récemment lorsque ce site s'est mis à exploiter la puissance processeur des systèmes de ses visiteurs pour miner Monero.

Ces menaces présentent de nombreuses facettes. Certaines attaques exploitent des vulnérabilités Web côté serveur. Ainsi, elles insèrent des scripts qui déploient des malwares de minage afin de tirer parti des ressources processeur des navigateurs consultant les sites infectés. D'autres attaques, qui ratissent large et prennent de l'importance à l'heure actuelle, recourent au phishing pour voler les identifiants permettant d'accéder aux portefeuilles de cryptomonnaie. D'autres encore utilisent des malwares pour transformer les ordinateurs de leurs cibles en mineurs à leur solde.

Quelle que soit leur méthode, les cybercriminels ne manqueront pas d'explorer de nouvelles pistes. Jusqu'à ce que les cryptodevises moins importantes atteignent les taux de saturation de Bitcoin, leur exploitation illicite restera extrêmement lucrative. L'appât du gain a toujours été et restera une motivation très forte des cyberpirates.

CRYPTOMONNAIE
Une monnaie électronique conçue pour être sûre et anonyme. Elle peut être utilisée pour acheter et vendre des biens ou échangée contre une devise émise par un pays. Elle est créée par une opération de « minage » nécessitant la puissance de calcul d'un ordinateur pour résoudre des problèmes mathématiques complexes.

USURPATION DE DOMAINES
L'usurpation de domaines consiste à emprunter frauduleusement l'identité d'un contact ou d'un collègue par l'emploi d'une adresse e-mail qui semble légitime en apparence. Dans certains cas, elle utilise des noms de domaines très similaires aux domaines usurpés.

LA FRAUDE PAR E-MAIL PROGRESSE GRÂCE AU PERFECTIONNEMENT DES TECHNIQUES D'ATTAQUE

Chiffres clés : Les tentatives de fraude par e-mail ont grimpé de 29 % par rapport au trimestre précédent au sein de notre clientèle mondiale.

En même temps que leur nombre total, la fréquence des attaques ciblées de ce type est en hausse elle aussi. Ainsi, elles ont progressé de 12 % par rapport au trimestre précédent et de 32 % par rapport au même trimestre de l'année précédente.

L'USURPATION DE DOMAINES, une technique courante en matière de fraude par e-mail, s'est également intensifiée. Les attaques qui prennent cette forme particulière peuvent toutes être bloquées grâce à l'authentification des e-mails. Pourtant, 89 % des entreprises ont subi au moins une attaque par usurpation de domaine au cours du trimestre.

Secteurs ciblés

Tous les secteurs sont visés par la fraude par e-mail. Les pirates semblent toutefois privilégier les secteurs aux chaînes d'approvisionnement plus complexes, comme nous l'avons déjà constaté au cours des trimestres précédents. La fabrication, par exemple, est une fois encore le secteur le plus souvent ciblé. La figure 8 illustre la fréquence relative des cibles d'attaques par secteur d'activité. Elle compare le 3e trimestre 2017, le 2e trimestre 2017 et le même trimestre de l'an dernier, révélant des relations similaires.

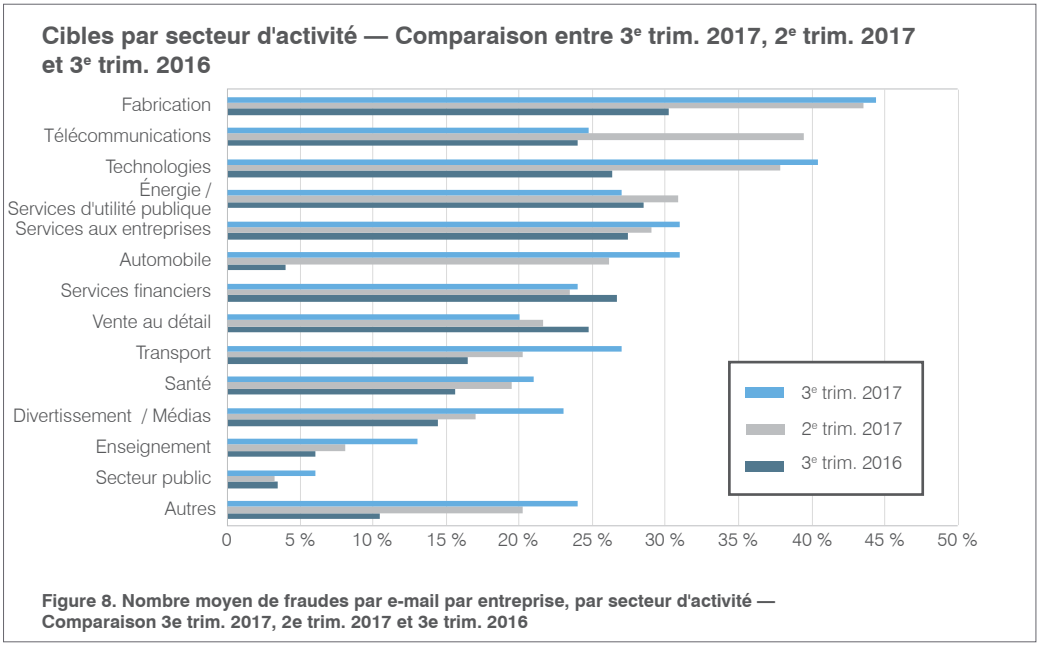

Figure 8. Nombre moyen de fraudes par e-mail par entreprise, par secteur d'activité — Comparaison 3e trim. 2017, 2e trim. 2017 et 3e trim. 2016

FRAUDE PAR E-MAIL
Ces attaques utilisent un e-mail qui semble provenir d'un cadre supérieur de l'entreprise et enjoint au destinataire de transférer une somme d'argent ou de communiquer des informations sensibles. Elles ne comportent ni pièces jointes ni URL, de sorte qu'il est difficile de les détecter et de les neutraliser.

Notre analyse de la **FRAUDE PAR E-MAIL** n'a identifié aucune corrélation entre la taille de l'entreprise et la fréquence de ces attaques. Nous avons constaté qu'au 2e trimestre, certains cybercriminels semblaient privilégier les entreprises de plus grande taille, mais sans que cette observation ne revête une réelle importance statistique. Au cours du 3e trimestre, en revanche, aucune relation apparente n'est apparue. Les entreprises ont été ciblées de manière uniforme, indépendamment de leur taille.

Un ciblage individuel optimisé

Par nature, la fraude par e-mail se concentre sur des cibles précises. Cette hypothèse est largement corroborée par le fait que les pirates ont utilisé davantage d'identités usurpées et ciblé un plus grand nombre de collaborateurs par entreprise. Dans près de 3/4 des cas, les attaques ont emprunté plusieurs identités et visé plusieurs collaborateurs au sein de la même entreprise. Les attaques utilisant l'adresse e-mail d'un cadre dirigeant pour en cibler un autre sont toujours monnaie courante. (Ce type d'attaque est baptisé « whaling », ou chasse à la baleine, en référence au statut de leurs cibles. Il est représenté à la figure 9 sous l'appellation d'attaque « un à un ».) Toutefois, les cybercriminels étendent désormais leur terrain de chasse et diversifient leurs cibles au sein des entreprises.

Identités usurpées par nombre de collaborateurs ciblés — Comparaison 3e trim. 2017, 2e trim. 2017 et 3e trim. 2016

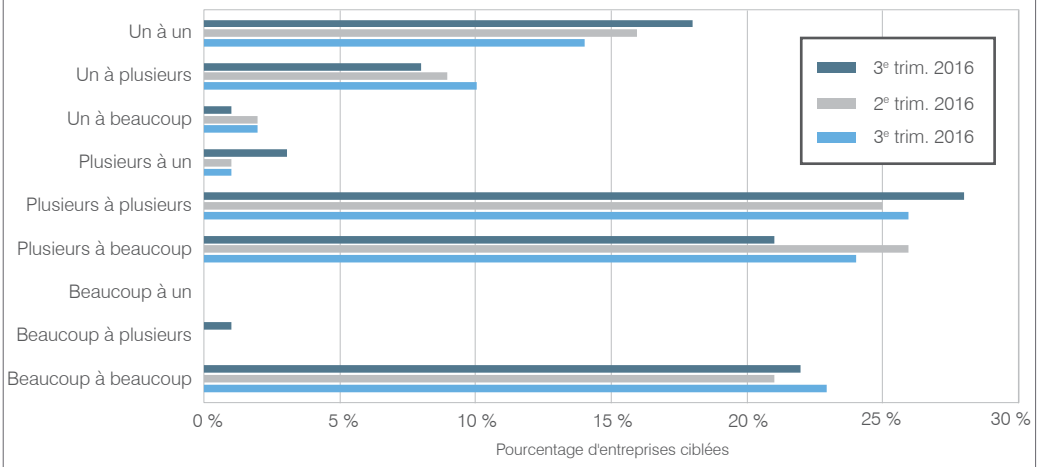

Figure 9. Types d'attaques par nombre d'identités de dirigeants usurpées, comparé au nombre de collaborateurs ciblés. Exemple : une fraude par e-mail contre une entreprise qui usurpe 4 identités de cadres dirigeants et cible 10 membres du département financier sera classée comme une attaque « plusieurs à beaucoup ».

Les pirates continuent à utiliser des chaînes d'e-mails frauduleux pour rendre leurs messages plus convaincants. Environ 10 % des fraudes par e-mail ont eu recours à cette tactique au 3e trimestre.

KITS D'EXPLOIT : EN BAISSE MAIS PAS HORS COURSE

RIG
Après la disparition d'Angler à la suite de l'arrestation en juin 2016 des responsables de sa propagation, RIG est devenu le kit d'exploit le plus en vogue.

Chiffres clés : 73 % des activités liées aux exploits au 3e trimestre impliquaient le kit d'exploit RIG.
Les kits d'exploit ont connu un déclin spectaculaire et très médiatisé, après avoir atteint un niveau record au début de l'année 2016. De fait, si cette activité stagne à seulement 10 % du pic de 2016, les kits d'exploit constituent toujours une composante importante du paysage des menaces. C'est particulièrement vrai dans des régions où les logiciels pirates sont fréquents, ce qui empêche l'application régulière de correctifs.

De nouveaux stratagèmes d'ingénierie sociale sont également utilisés conjointement aux kits d'exploit pour rendre ces derniers plus efficaces ; de ce fait, les pirates n'ont pas nécessairement besoin de nouveaux exploits. Nous observons également un accroissement de l'activité des « traffers », des réseaux conçus pour diriger le trafic vers les pages de renvoi des kits d'exploit. Cette nouvelle tendance laisse présager une possible résurgence de l'activité des kits d'exploit dans les mois à venir.

À l'heure actuelle, RIG reste le kit d'exploit dominant, puisqu'il représente à lui seul 73 % de toute l'activité due à ce type d'attaque. À la fin du trimestre, le trafic déjà modeste associé au kit d'exploit Angler avait pratiquement disparu. Même Neutrino, qui a fait jeu égal avec RIG à certains moments au cours du trimestre, a presque entièrement cédé la place à celui-ci au terme de cette période. La figure 10 illustre le trafic correspondant aux principaux kits d'exploit.

Activité des kits d'exploit – Répartition des échantillons collectés au 3e trim. 2017

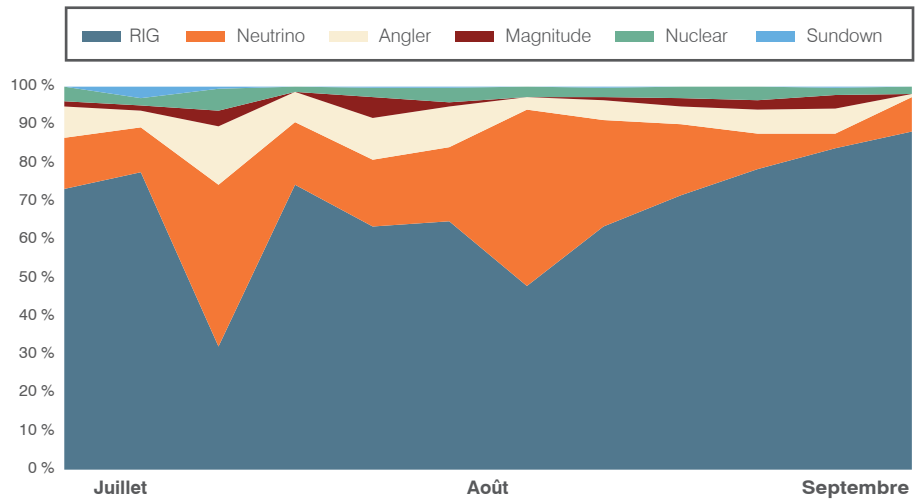

Figure 10. Trafic lié aux principaux kits d'exploit (pourcentage par rapport au total), d'avril à mai 2017

TENDANCES EN MATIÈRE DE DOMAINES

Chiffres clés : Les enregistrements de domaines suspects ont été 20 fois plus nombreux que les enregistrements défensifs. Le fossé se creuse entre les entreprises qui cherchent à protéger leurs marques et les pirates qui tentent de les exploiter à des fins illicites.

Au 3e trimestre, nous avons élargi le champ de nos recherches et étudié l'enregistrement de domaines suspects pour les grandes entreprises du Fortune 50. Le terme « domaines suspects » se réfère ici aux noms de domaines susceptibles d'être exploités lors d'attaques par **TYPOSQUATTAGE** ou usurpation d'identité.

TYPOSQUATTAGE
L'utilisation de domaines enregistrés qui sont des variantes légèrement déformées de domaines légitimes. L'objectif est de leurrer les internautes qui feraient des fautes de frappe en tapant une URL ou ne seraient pas attentifs aux en-têtes d'un e-mail frauduleux.

À compter du début de l'année 2015 jusqu'à la fin du mois d'août 2017, les enregistrements défensifs de domaines appartenant aux marques ont diminué, alors qu'à l'inverse, les enregistrements suspects par des tiers ont progressé (figure 11). De janvier à août 2017, les enregistrements suspects ont connu une hausse de 20 % par rapport à la même période l'année précédente, tandis qu'à l'inverse, les enregistrements défensifs des marques ont chuté de 20 %.

Malgré les enregistrements défensifs, les domaines suspects sont toujours largement majoritaires par rapport aux domaines appartenant aux marques légitimes. En 2016, pour chaque enregistrement défensif, nous avions identifié 10 enregistrements de domaines similaires suspects. Cette année, le rapport est de 20 pour 1.

De plus, les pics dans les enregistrements défensifs correspondent généralement à un événement ponctuel affectant la marque, comme le lancement d'un produit, plutôt qu'à une stratégie de défense continue.

Comparaison des enregistrements de domaines suspects et des enregistrements défensifs par des marques, depuis le début de l'année 2017

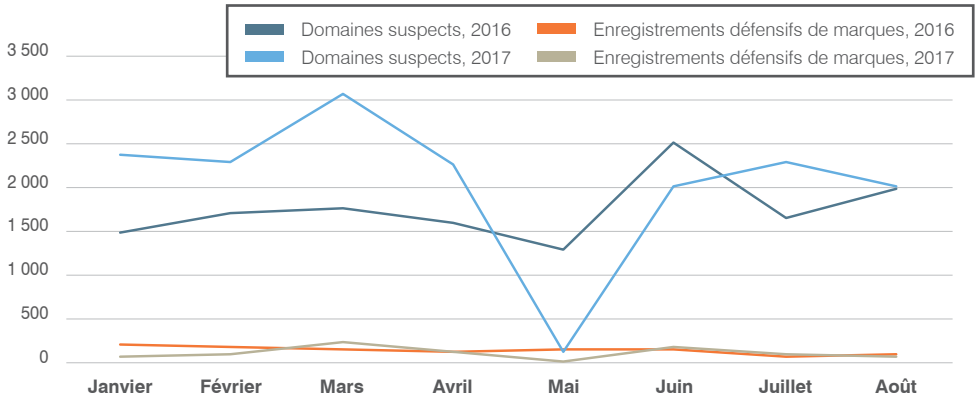

Figure 11. Comparaison par année (1er au 3e trim 2016 et 2017) des enregistrements de domaines suspects et des enregistrements défensifs par les marques pour les entreprises du Fortune 50

TENDANCES EN MATIÈRE DE MÉDIAS SOCIAUX

Chiffres clés : Les comptes d'assistance à la clientèle factices ont doublé par rapport au même trimestre de l'année précédente.

Sur les médias sociaux, les menaces sont à la fois nombreuses et variées, allant des malwares aux fraudes. Nous y surveillons deux principales catégories :

- Les comptes d'assistance factices, utilisés pour des attaques de phishing Angler
- Les liens de phishing plus classiques, qui mènent à des pages servant à capturer des identifiants de connexion et des informations personnelles

Le nombre de faux comptes d'assistance a augmenté de 5 % par rapport au trimestre précédent et doublé par rapport à la période correspondante l'an dernier. Les liens de phishing sur les comptes de médias sociaux d'une marque ont progressé de 10 % par rapport au trimestre précédent (figure 12). Leur nombre est globalement stable comparé à l'année précédente.

Ces diverses données laissent entrevoir un large revirement en matière d'attaques sur les médias sociaux. Les cyberpirates continuent à tirer parti d'événements et de tendances saisonnières comme le fait le phishing conventionnel. Cela étant, ils se tournent de plus en plus vers le phishing Angler, plus lucratif.

Certes, le phishing conventionnel exploitant les médias sociaux pour le vol d'identifiant est plus facile à mettre en œuvre. Le phishing Angler, cependant, est souvent plus efficace car il paraît légitime ; il est en effet bien plus proche d'une interaction humaine que les liens aléatoires insérés dans les commentaires des pages de réseaux sociaux.

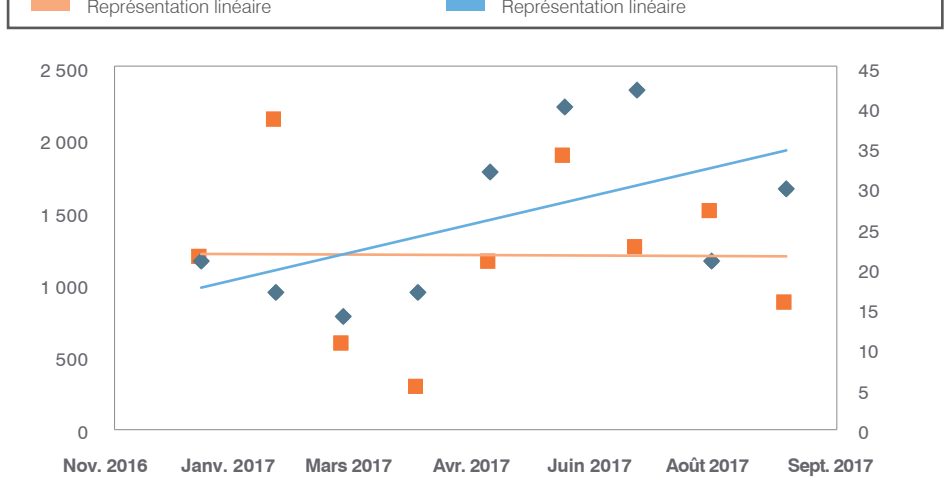

Figure 12. Comparaison entre l'activité mensuelle liée à la distribution de liens vers des pages de phishing via les médias sociaux et celle associée à des comptes d'assistance à la clientèle factices

RECOMMANDATIONS

Ce rapport apporte un éclairage sur l'évolution du paysage des menaces à la fois pertinent et précieux pour parfaire votre stratégie de cybersécurité. Voici nos principales recommandations sur les mesures à prendre pour protéger vos données, vos collaborateurs et votre marque au cours des mois à venir.

Luttez contre le typosquattage sur le Web.
L'enregistrement défensif de domaines est une mesure simple et efficace pour empêcher les pirates de créer des noms de domaines similaires au vôtre et de les exploiter dans le cadre de fraudes par e-mail ou de phishing d'identifiants. En collaboration avec des dirigeants de l'entreprise, définissez une liste de noms similaires et enregistrez les domaines correspondants. N'oubliez pas les sites Web de vos campagnes marketing ou de vos conférences, qui sont des cibles fréquentes.

Appliquez l'authentification des e-mails pour bloquer les techniques d'usurpation de domaines qu'utilise la fraude par e-mail.
Les protocoles d'authentification tels que DMARC (Domain-based Message Authentication, Reporting & Conformance) empêchent les imposteurs d'exploiter votre domaine de messagerie à des fins malveillantes. De plus, votre solution doit pouvoir identifier tous les domaines susceptibles d'être confondus avec le vôtre et permettre la collaboration avec des prestataires externes afin de démanteler les usurpateurs.

Protégez vos utilisateurs contre tous les types d'attaques par e-mail.
Vos dispositifs de protection des e-mails doivent couvrir l'éventail le plus large possible de menaces propagées par la messagerie électronique — qu'il s'agisse de pièces jointes infectées, d'URL malveillantes ou de tentatives de fraude par ingénierie sociale. Cette protection fiable doit comprendre des fonctions d'analyse performantes, capables d'identifier et d'isoler de manière préventive les URL et pièces jointes suspectes. Vos mesures de sécurité doivent inclure une analyse multiniveau en environnement sandbox permettant de détecter les pièces jointes et URL dangereuses, à la fois au point d'entrée et lors du clic sur l'élément malveillant. Elles doivent également identifier et bloquer les menaces autres que les malwares, comme les e-mails frauduleux d'imposteurs demandant l'exécution de transferts financiers ou l'envoi d'informations confidentielles.

Collaborez avec un fournisseur spécialisé dans la cyberveille.
Pour faire face aux attaques de faible ampleur et plus ciblées, vous avez besoin de renseignements pointus sur les menaces. La solution choisie doit répondre à trois critères : associer une analyse des données avec des informations sur les menaces ; combiner des techniques statiques et dynamiques pour détecter les nouvelles attaques (au travers de leurs outils, tactiques et cibles) ; être en mesure de tirer les enseignements nécessaires de toutes ces données. En recoupant les résultats des analyses avec les données de cyberveille reçues, il est possible d'identifier et de bloquer les e-mails malveillants difficiles à détecter avant qu'ils atteignent les utilisateurs.

Protégez votre marque contre les imposteurs sur les médias sociaux.
Utilisez une solution de sécurité qui signale les comptes de médias sociaux d'imposteurs, particulièrement lorsqu'ils offrent des pseudo-services d'assistance frauduleux. Elle doit non seulement détecter les comptes illégitimes, mais collaborer avec les prestataires assurant leur démantèlement, pour empêcher qu'ils ne flouent vos clients et partenaires.

Pour plus d'informations sur les menaces et leurs tendances, consultez le blog Proofpoint Threat Insight à l'adresse **proofpoint.com/fr/threat-insight**

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ : PFPT), société spécialisée dans les solutions de cybersécurité de nouvelle génération, permet aux entreprises de barrer la route aux menaces avancées de façon à garantir à leur personnel un environnement de travail sûr, tout en écartant les risques de non-conformité. Grâce à Proofpoint, les responsables de la cybersécurité peuvent protéger leurs utilisateurs contre les attaques avancées (qu'elles utilisent comme vecteur la messagerie électronique, les applications mobiles ou les médias sociaux) et sécuriser les informations critiques créées au sein de l'entreprise. De plus, leurs équipes disposent des outils et renseignements adéquats pour réagir rapidement en cas d'incident. Des entreprises de renom et de toutes tailles, dont plus de la moitié de celles figurant au classement Fortune 100, ont adopté les solutions Proofpoint. Ces dernières sont conçues pour les environnements informatiques d'aujourd'hui, tournés vers les applications mobiles et les médias sociaux, et s'appuient sur de puissantes technologies cloud ainsi que sur une plate-forme analytique orientée Big Data pour lutter contre les menaces sophistiquées, même les plus récentes.

proofpoint.

www.proofpoint.com/fr