RAPPORT

proofpoint®

RAPPORT TRIMESTRIEL SUR LES MENACES

4E TRIM. 2017

proofpoint.com/fr

Le *rapport trimestriel sur les menaces de Proofpoint* met en lumière les tendances ainsi que les principales leçons à tirer des attaques observées au sein de notre 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 applications de cloud. 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 : LES MINEURS DE CRYPTOMONNAIE ET LES RANSOMWARES SONT PARTOUT

Voici les principaux points à retenir pour ce dernier trimestre 2017.

MESSAGERIE ÉLECTRONIQUE

Le volume de messages contenant des pièces jointes malveillantes a triplé.
Ce trafic est essentiellement dû à des campagnes d'attaque de grande envergure exploitant le protocole **DYNAMIC DATA EXCHANGE (DDE)** de Microsoft ainsi que l'ingénierie sociale.

Les RANSOMWARES sont restés la principale charge active distribuée par les messages malveillants.
Ce type d'attaque représente 57 % du volume total de messages malveillants.

Le nombre de demandes de rançon payables en bitcoins a chuté de 73 % en raison des importantes fluctuations de la CRYPTOMONNAIE.
De plus en plus, les cybercriminels réclament des rançons en dollars américains ou en devise locale (même si le paiement en soi continue généralement de se faire en cryptomonnaie).

THE TRICK est le cheval de Troie bancaire le plus utilisé au 4e trimestre.
Il représente à lui seul 84 % de tous les messages de spam contenant un cheval de Troie bancaire.

Les domaines similaires et TYPOSQUATTÉS ont été utilisés dans un large éventail d'attaques.
La permutation de caractères est la principale technique utilisée pour créer des domaines susceptibles d'être confondus avec ceux d'une société ou d'une enseigne connue et légitime.

KITS D'EXPLOIT ET ATTAQUES WEB

Les techniques d'ingénierie sociale se sont multipliées alors que l'utilisation d'exploits de navigateur a diminué dans les campagnes d'attaque Web relayées par les médias.
Le trafic lié aux **KITS D'EXPLOIT** a baissé de 31 % par rapport au trimestre précédent. Le plus utilisé a été le kit d'exploit RIG.

MÉDIAS SOCIAUX

Le nombre de comptes d'assistance à la clientèle frauduleux sur les médias sociaux a augmenté de 30 %.
En même temps, les liens de phishing sur les réseaux sociaux ont progressé de 70 % par rapport au 3e trimestre.

DYNAMIC DATA EXCHANGE
Dynamic Data Exchange (DDE) est un protocole de communication de Microsoft Windows vieux de 20 ans qui permet d'extraire des informations d'autres documents. Cette technique a été largement remplacée par des protocoles plus récents mais elle est toujours prise en charge par Windows.

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.

CRYPTOMONNAIE
Forme de monnaie numérique conçue pour être sûre et anonyme, ce qui en fait la solution idéale pour le paiement des rançons puisqu'il est impossible de remonter au cybercriminel.

THE TRICK
The Trick, également appelé TrickBot, est un cheval de Troie bancaire étroitement lié à Dyre. Bien que les responsables de sa propagation aient été arrêtés par les autorités russes en 2015, il est réapparu en 2017.

TYPOSQUATTAGE
Utilisation de domaines enregistrés qui sont des variantes légèrement déformées de domaines légitimes. L'objectif est de leurrer les internautes qui font des fautes de frappe en tapant une URL ou ne prêtent pas suffisamment d'attention aux en-têtes des e-mails.

KIT D'EXPLOITS
Exécutés sur le Web, ces kits détectent et exploitent les failles des ordinateurs qui accèdent à des sites compromis, à des publicités malveillantes ou à des pages de renvoi sous le contrôle d'un cyberpirate. 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). Ils sont aussi de plus en plus souvent utilisés pour distribuer des attaques par ingénierie sociale qui ne reposent pas sur des exploits actifs.

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

GLOBEIMPOSTER
Cette variante de ransomware, également appelée Fake Globe, imite une souche plus ancienne, Globe, à laquelle elle doit d'ailleurs son nom. Au départ utilisée dans de petites campagnes régionales, GlobeImposter est devenue une menace mondiale lorsque le cybercriminel TA505, très actif, a commencé à l'utiliser dans des campagnes de plus grande envergure.

E-MAIL : LES DOCUMENTS MALVEILLANTS PRENNENT LE PAS SUR LES URL

Chiffre clé : le volume de messages contenant des pièces jointes malveillantes a progressé de 300 % par rapport au trimestre précédent.

Le volume total de messages contenant des pièces jointes malveillantes a plus que triplé par rapport au trimestre précédent. Envoyés dans le cadre de campagnes de grande envergure menées par le cybercriminel **TA505**, ces messages distribuaient souvent le cheval de Troie bancaire The Trick ou diverses souches de ransomware, dont **LOCKY** et **GLOBEIMPOSTER**.

Plusieurs cyberpirates ont profité de la divulgation au grand jour d'une technique d'exploitation du protocole DDE (Dynamic Data Exchange) de Microsoft pour distribuer des malwares dans le cadre de campagnes de petite et grande envergure.

Dès la fin octobre, les cybercriminels avaient pour la plupart abandonné cette technique pour revenir à leurs méthodes habituelles d'exploitation de macros malveillantes et à d'autres formes de code incorporé. Malgré tout, on a observé quelques campagnes sporadiques exploitant DDE en novembre et en décembre, cette technique faisant désormais partie de l'arsenal d'outils des cyberpirates.

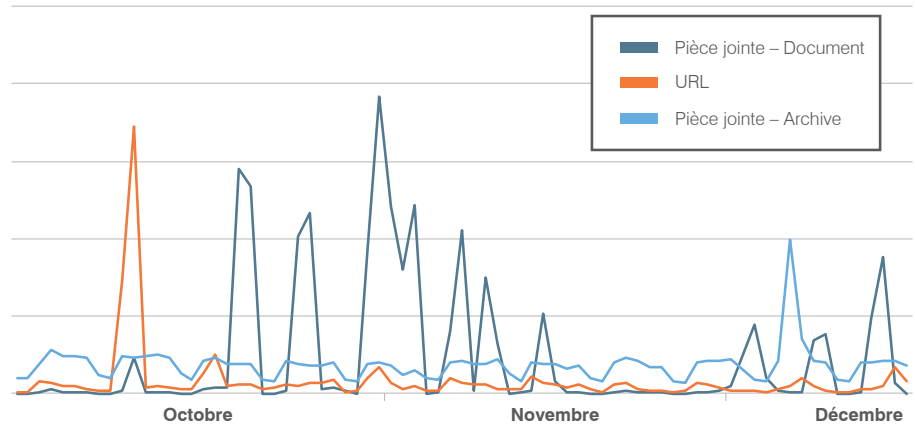

Figure 1. Volumes indexés par type d'attaque, tendances d'octobre à décembre 2017 (77 jours)

À l'inverse, les URL malveillantes ont chuté. Les volumes exceptionnellement élevés observés au troisième trimestre n'étaient finalement qu'une simple anomalie. Quoi qu'il en soit, toutes les techniques d'attaques trouvent leur place au sein de la vaste communauté de cybercriminels.

La figure 1 illustre les fluctuations importantes du volume de messages malveillants utilisant des URL, des pièces jointes et des fichiers d'archive (ZIP ou 7-Zip, par exemple) malveillants. Ces fluctuations constantes soulignent la flexibilité des cybercriminels, qui ne cessent de varier les types d'attaque, les charges actives et les méthodes d'infection pour gagner en efficacité et multiplier leurs profits.

CHEVAL DE TROIE BANCAIRE
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.

ZEUS PANDA
Également appelé Panda Banker, ce cheval de Troie bancaire est lié à Zeus, un des tout premiers chevaux de Troie bancaires.

MINEURS DE CRYPTOMONNAIE
La cryptomonnaie est créée à l'aide d'un processus de « minage » qui utilise les ressources de traitement des ordinateurs pour résoudre des problèmes mathématiques complexes. Les mineurs de cryptomonnaie sont des souches de malware qui piratent les systèmes infectés dans ce but, générant ainsi de la cryptomonnaie pour le cybercriminel distribuant le malware.

WEBINJECT
Technique destinée à modifier les pages Web lorsqu'elles s'affichent sur l'écran des utilisateurs. Les cyberpirates utilisent du code WebInject pour ajouter des formulaires non sécurisés à des sites Web qui devraient logiquement être sûrs. Lorsque les utilisateurs complètent les formulaires (par exemple avec leurs identifiants bancaires), ces informations sont envoyées au pirate et non à la banque.

CHEVAUX DE TROIE BANCAIRES : PAS SEULEMENT LIMITÉS AU SECTEUR BANCAIRE

Chiffre clé : les messages distribuant The Trick représentaient 84 % du volume total des messages contenant un CHEVAL DE TROIE BANCAIRE.

The Trick est resté le premier cheval de Troie bancaire en termes de volume total de messages. Sa prévalence dans les messages est six fois supérieure à celles de tous les autres chevaux de Troie bancaires confondus. On est loin des chiffres de 2016, où The Trick se limitait essentiellement à de petites campagnes très localisées et où Dridex et Vawtrak se taillaient la part du lion.

En plus de la menace The Trick, **ZEUS PANDA** (alias Panda Banker) et Emotet sont également apparus de manière assez fréquente dans les campagnes du 4e trimestre. Plusieurs pirates assez actifs ont par ailleurs rapidement adopté un nouveau cheval de Troie appelé IcedID.

Certains chevaux de Troie bancaires — surtout The Trick — incorporent désormais des robots ou des modules de minage de cryptomonnaie. D'autres campagnes du même type ont ajouté des **MINEURS DE CRYTPOMONNAIE** en tant que charges actives intervenant lors d'une phase ultérieure, une tendance déjà constatée au troisième trimestre et qui semble se développer.

Ces dernières années, on a souvent observé une plus grande variété dans les cibles des chevaux de Troie bancaires en automne. Le 4e trimestre 2017 n'a pas dérogé à cette règle. Les campagnes Zeus Panda ont complété et étendu les fichiers **WEBINJECT** bancaires habituels du robot par des injections de code ciblant les sites d'achat en ligne de plusieurs enseignes connues.

Cette évolution nous rappelle que les chevaux de Troie bancaires ne se limitent pas aux seuls clients des sociétés de services financiers. Les clients en ligne de *n'importe quel* service ou entreprise représentent autant de cibles potentielles.

RANSOMWARE : LA VOLATILITÉ DU BITCOIN PERTURBE LES AFFAIRES

Chiffre clé : l'utilisation du bitcoin pour les demandes de rançon a chuté de 73 %.

En dépit d'un pic dans le volume des messages contenant un cheval de Troie bancaire — largement dû aux grandes campagnes basées sur The Trick et menées par un pirate unique — les ransomwares sont restés la principale charge active malveillante des campagnes e-mail. Ils représentent en effet plus de 57 % de tous les messages malveillants, comme illustré à la figure 2.

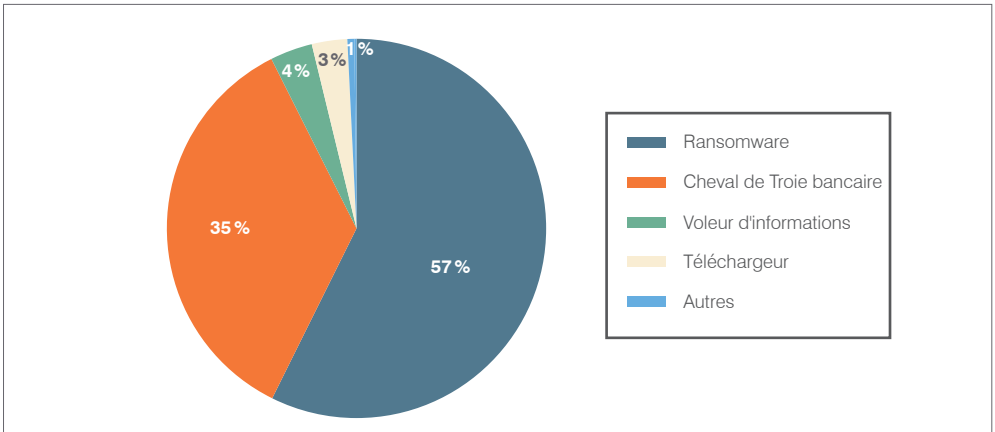

Figure 2. Part du volume global de messages malveillants par famille de malware, 4e trimestre 2017

Ces deux dernières années, les rançons demandées par les cybercriminels ont été principalement libellées en bitcoins. Le montant demandé est exprimé sous la forme d'un certain nombre de bitcoins, soit un entier, soit une fraction, par exemple 0,5 ou 0,15.

La flambée du bitcoin est une aubaine pour celui qui en possède. Mais elle est beaucoup plus problématique pour celui qui tente de fixer le prix de son produit ou service en bitcoins, y compris les cybercriminels.

Au 4e trimestre, les nouvelles souches de ransomware l'ont, semble-t-il, pris en compte. Le ransomware Sigma, apparu pour la première fois à la mi-novembre, exigeait un paiement libellé en dollars américains.

Libeller les rançons en devise émise par un gouvernement — même si le paiement en soi reste en bitcoins — présente deux grands avantages pour un cyberpirate. Cela lui permet de garantir la stabilité des prix et de continuer à accepter des paiements de façon anonyme, qui plus est dans une devise dont la valeur ne cesse actuellement d'augmenter.

L'analyse des demandes de rançon de la mi-septembre à la mi-décembre révèle que le changement de devise s'inscrit dans une tendance générale (figure 3).

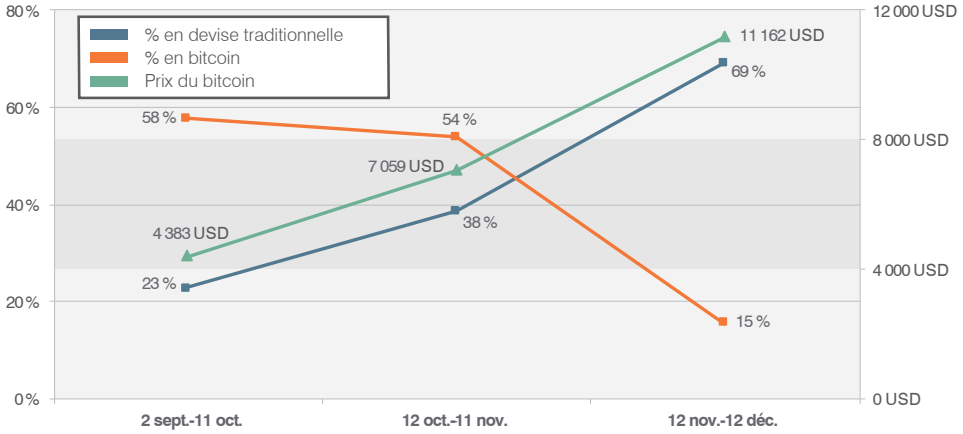

Figure 3. Rançons de ransomware libellées en bitcoins et en devise traditionnelle, tendance sur 90 jours

Le libellé de ces demandes de rançon dans une devise traditionnelle au lieu ou en plus du bitcoin est clairement lié à la valorisation de cette cryptomonnaie. L'appréciation du bitcoin résulterait en fait de ce changement de devise.

La tendance pourrait s'inverser si le prix du bitcoin chutait. Quoi qu'il en soit, cette corrélation est une preuve supplémentaire de la motivation financière des cybercriminels. Ils adoptent les outils et les techniques qui servent le mieux leurs intérêts financiers.

ÉMERGENCE DE CYBERCRIMINELS PRIVILÉGIANT LES ATTAQUES CIBLÉES

Bon nombre des campagnes observées par nos chercheurs au cours du 4e trimestre étaient des charges actives malveillantes de base distribuées à grande échelle. Mais nous avons également analysé et relevé des activités menées par plusieurs cyberpirates privilégiant une approche plus ciblée, dont Lazarus Group, APT28 et un nouveau groupe que nous avons appelé Leviathan.

Les e-mails et les documents utilisés dans ces attaques sont souvent personnalisés et adaptés aux centres d'intérêt et aux activités du destinataire. Ils utilisent des documents publics et des signes distinctifs des marques qu'ils ont dérobés. Ils s'appuient également sur des domaines similaires ou typosquattés pour inciter les destinataires à cliquer sur des liens ou à télécharger des fichiers.

FRAUDES PAR E-MAIL : LE POINT SUR LES PRATIQUES D'ENREGISTREMENT DE NOMS DE DOMAINE FRAUDULEUX

ENREGISTREMENT DE DOMAINES DÉFENSIF
Pratique recommandée consistant à acheter des domaines Internet susceptibles d'être confondus avec ceux des marques légitimes avant que les cybercriminels ne le fassent. Les domaines similaires peuvent servir à tromper les clients et les partenaires commerciaux en créant des sites Web factices et des e-mails frauduleux qui semblent émaner d'une entreprise légitime.

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.

Chiffre clé : le nombre moyen d'ENREGISTREMENTS DE DOMAINE DÉFENSIFS s'élève à 300. Pour les grandes entreprises, les enregistrements de domaine suspects peuvent être 20 fois plus nombreux que les domaines enregistrés par les marques elles-mêmes.

D'après nos recherches, il semble que les cybercriminels dépassent largement les marques si l'on compare les enregistrements de domaine suspects aux enregistrements défensifs. Un tel écart laisse les marques vulnérables à la fraude, au phishing, à l'usurpation d'identité et à bien d'autres menaces.

Pour se protéger, les entreprises ne doivent pas nécessairement enregistrer chaque permutation possible de leur(s) domaine(s). Il est plus intéressant d'analyser les modifications et les substitutions les plus courantes afin de prioriser leurs enregistrements défensifs et de gérer un nombre plus raisonnable de domaines typosquattés potentiels.

Les domaines similaires représentent un peu plus de 3 % de l'ensemble des tentatives de fraude par e-mail. En revanche, ils représentent un nombre extrêmement élevé de domaines utilisés dans la fraude par e-mail, le phishing, le **PHISHING ANGLER** et d'autres attaques.

Même si certains chercheurs accordent aujourd'hui une plus grande attention aux enregistrements frauduleux dans des domaines de premier niveau inhabituels ou nouveaux, les enregistrements suspects dans la catégorie standard « .com » restent de loin les plus répandus.

Près de 82 % de ces enregistrements utilisent « .com ». De plus, près de 90 % des enregistrements suspects utilisent le même domaine de premier niveau que la marque dont ils usurpent l'identité. Les fraudeurs utilisent souvent de simples variations des noms de domaine légitimes dans le domaine de premier niveau de la marque dont ils cherchent à usurper l'identité.

La figure 4 présente les variations orthographiques les plus courantes dans les enregistrements de domaine suspects.

Type de domaine cousin	Domaine de 1er niveau différent	Domaine de 1er niveau identique	Total général
Permutation d'un seul caractère	3,49 %	37,60 %	41,09 %
Insertion d'un caractère supplémentaire	0,97 %	31,15 %	32,12 %
Ajout ou suppression de caractères de début/fin	0,73 %	12,51 %	13,25 %
Suppression d'un caractère	0,41 %	5,10 %	5,51 %
Correspondance exacte avec trait d'union	1,23 %	3,40 %	4,63 %
Correspondance exacte	3,40 %	0,00 %	3,40 %
Total général	**10,23 %**	**89,77 %**	**100 %**

Figure 4. Techniques de typosquattage

La permutation de caractères individuels d'un nom de marque dans le même domaine de premier niveau est la technique de typosquattage la plus courante. La figure 5 propose une représentation graphique des permutations de lettres spécifiques.

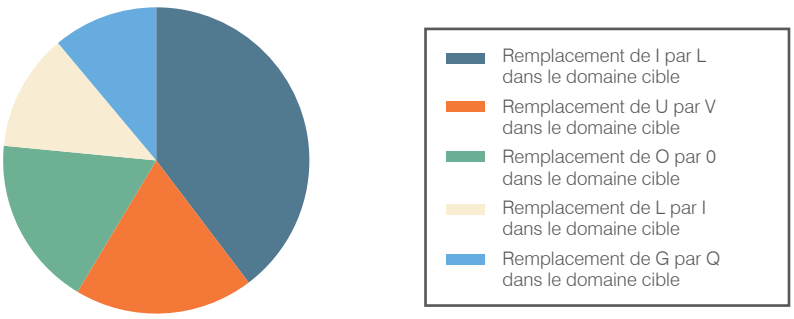

Figure 5. Modes de substitution de caractères dans le typosquattage de domaines suspects

MENACES WEB : CONSOLIDATION ET INGÉNIERIE SOCIALE

Chiffre clé : le trafic lié aux kits d'exploit a diminué de 31 % par rapport au 3e trimestre.

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

Déjà modeste, le trafic lié aux kits d'exploit, qui s'est maintenu pendant plusieurs trimestres à environ 10 % de son pic de 2016, a encore chuté au 4e trimestre. Le **KIT D'EXPLOIT RIG** représente près de 98 % du trafic lié aux kits d'exploit au dernier trimestre 2017. Mais sa part de trafic a diminué en fin de trimestre face à une poussée tardive du kit d'exploit Magnitude (figure 6).

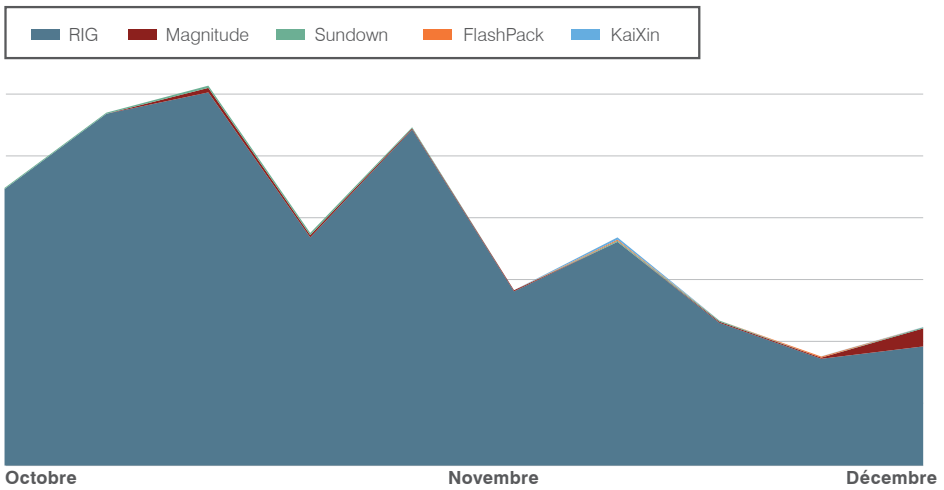

Figure 6. Trafic lié aux principaux kits d'exploit (pourcentage par rapport au total), d'octobre à décembre 2017

BAD RABBIT
Cette souche de ransomware, apparue pour la première fois en octobre, cible la population russe et ukrainienne. Elle ressemble beaucoup au ransomware NotPetya. Sous le couvert d'une « mise à jour » d'Adobe Flash, le ransomware infecte les systèmes par un téléchargement à l'insu de l'utilisateur, mais pour arriver à ses fins, il doit être exécuté par la victime.

On a beaucoup entendu parler d'une vaste campagne publicitaire malveillante très sophistiquée qui ciblait les utilisateurs d'un site connu de vidéos pour adultes. Au lieu d'exploiter les failles techniques du navigateur Web des utilisateurs, l'attaque incitait ces derniers à installer eux-mêmes le malware. Les cybercriminels ont eu recours à un filtrage avancé pour cibler leurs victimes par zone géographique et fournisseur d'accès Internet. Les internautes pris pour cible voyaient s'afficher une page Web leur demandant de télécharger une mise à jour de leur navigateur ou d'Adobe Flash. Ils téléchargeaient à la place Kovter, un malware exploitant des publicités frauduleuses, une technique déjà observée dans l'attaque du ransomware **BAD RABBIT** en octobre dernier.

Les cybercriminels manquent en effet d'exploits de navigateur Web viables et sont confrontés aux limitations des exploits en tant que technique d'infection. Comme certaines attaques de fin 2016 le laissaient présager, ils recourent désormais à des techniques axées sur l'ingénierie sociale, similaires à celles utilisées dans les attaques par e-mail et souvent beaucoup plus efficaces.

LES FLUCTUATIONS DES MALWARES POUR POINTS DE VENTE

En 2016, à l'occasion du week-end du Black Friday, nous avions enregistré un trafic de malwares pour points de vente (POS) spécifiques quatre fois supérieur à la normale. Ces pics ont été moins marqués en 2017. Une série de souches majeures sont restées actives à différentes périodes de l'année et pas seulement aux alentours du Black Friday (figure 7).

Par exemple, FindPOS a été actif en mars, puis son activité a ralenti pendant l'été pour reprendre à la fin du mois d'octobre. Cette reprise est survenue à peu près au moment où l'activité de MagikPOS a connu un déclin, ce qui laisse penser que l'attaque est le fait d'un cyberpirate isolé qui a simplement changé d'outil. En revanche, le trafic associé à NewPosThings, à l'exception d'un pic en juin, est resté faible et constant la majeure partie de l'année.

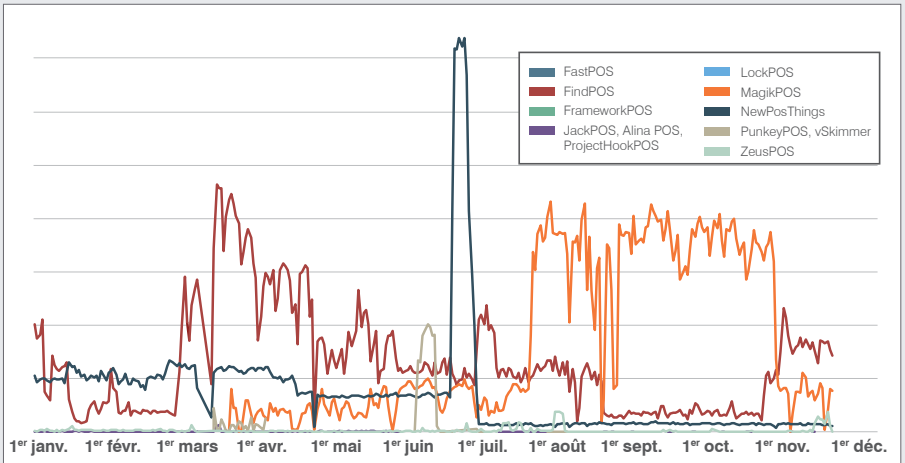

Figure 7. Trafic de malwares pour points de vente, de janvier à novembre 2017

Ce qu'il faut en retenir ? On peut supposer que la généralisation de l'utilisation de cartes à puce avec un code PIN a un impact non négligeable sur ce type de malwares et limite le succès potentiel des campagnes saisonnières à l'origine des pics de trafic. Mais il nous faudra étudier plus en détail les tendances cycliques des malwares pour points de vente afin de déterminer si et comment le paysage des menaces peut se polariser sur des variantes nouvelles et existantes.

MULTIPLICATION DES ATTAQUES SUR LES MÉDIAS SOCIAUX : UNE TENDANCE QUI DEVRAIT SE POURSUIVRE EN 2018

Chiffre clé : les comptes d'assistance à la clientèle frauduleux sur les médias sociaux ont progressé de 30 % par rapport au trimestre précédent et à la même période l'année dernière.

Les attaques sur les médias sociaux ont fortement progressé au cours du dernier trimestre. Le nombre de comptes d'assistance à la clientèle factices a augmenté de 30 % par rapport au 3e trimestre et à la même période en 2016.

Après avoir stagné une grande partie de l'année 2017, les liens de phishing sur les médias sociaux ont également connu une forte hausse au 4e trimestre, avec une progression de près de 70 % par rapport au 3e trimestre (figure 8).

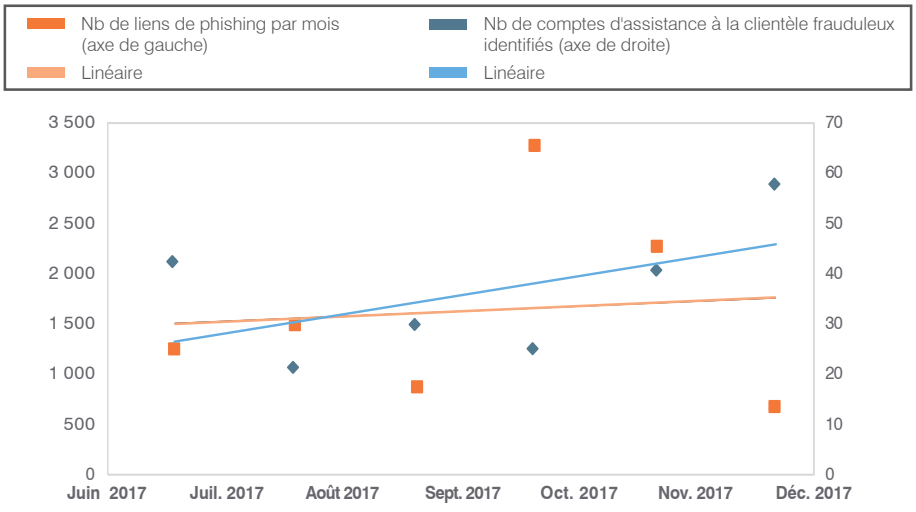

Figure 8. Comparaison entre l'activité mensuelle liée à la distribution de liens vers des pages de phishing via les médias sociaux et celle associée à des comptes d'assistance à la clientèle frauduleux

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 votre entreprise et votre marque au cours des mois à venir.

Partez du principe que vos utilisateurs se laisseront piéger. La préférence accordée à l'ingénierie sociale pour mener des attaques par e-mail est de plus en plus marquée, et les cybercriminels sont perpétuellement à la recherche de nouvelles techniques pour exploiter le facteur humain. Déployez une solution capable d'identifier et de mettre en quarantaine tant les e-mails entrants visant vos employés que les messages sortants qui ciblent vos clients, et ce avant qu'ils n'atteignent la boîte de réception.

Mettez en place un dispositif de défense robuste contre les attaques par e-mail. Extrêmement ciblées et de faible envergure, ces escroqueries ne recourent que très rarement à une charge active et sont par conséquent difficiles à déceler. Investissez dans une solution dotée de fonctions de classification dynamique afin de pouvoir définir des règles de mise en quarantaine et de blocage.

Protégez la réputation de votre marque et vos clients. Luttez contre les attaques ciblant vos clients par l'intermédiaire des médias sociaux, des e-mails et des appareils mobiles, en particulier celles qui recourent à des comptes frauduleux qui « phagocytent » votre marque. Recherchez une solution de sécurité complète pour les médias sociaux, à même d'analyser l'ensemble des réseaux sociaux et de signaler toute activité frauduleuse.

Faites appel à un fournisseur spécialisé dans la cyberveille comme partenaire. Pour faire face aux attaques de faible ampleur et davantage ciblées, vous avez besoin de renseignements pointus sur les menaces. Appuyez-vous sur une solution combinant des techniques statiques et dynamiques pour détecter les nouvelles caractéristiques des attaques (c'est-à-dire leurs outils, tactiques et cibles) et des menaces en constante évolution, et qui soit en mesure d'en tirer les enseignements nécessaires.

Pour consulter les dernières recherches sur les menaces et des recommandations concernant les menaces avancées et les risques numériques, consultez la page **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