

BILAN DU 4E TRIMESTRE ET DE L'ANNÉE 2016

RÉCAPITULATIF DES MENACES

Le rapport trimestriel de Proofpoint expose les menaces, les tendances et les transformations observées au sein de notre base de clients et sur le marché de la sécurité au sens large. Chaque jour, nous analysons plus d'un milliard de messages électroniques, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de code malveillants afin de protéger les entreprises contre les menaces avancées. Nous disposons ainsi d'un point d'observation unique qui permet de voir les données et les tendances à l'échelle du paysage global des menaces.

Analyser l'évolution de ces menaces entre deux trimestres permet de déceler les tendances majeures, et de fournir aux entreprises des renseignements exploitables et des conseils pour la gestion de leur stratégie de sécurité. Les menaces sophistiquées associées aux trois principaux vecteurs de propagation (messagerie électronique, réseaux sociaux et appareils mobiles) se maintiennent.

TABLE DES MATIÈRES

Points clés : Plus gros, plus rapides, plus nombreux.....	3
Messagerie et kits d'exploit	3
Appareils mobiles.....	3
Réseaux sociaux	4
Points clés du 4e trimestre	4
Menaces liées aux programmes malveillants et au courrier électronique	4
Tendances des volumes et techniques associées aux menaces du 4e trimestre	4
Techniques	6
Piratage de la messagerie en entreprise (BEC)	7
Aperçu des kits d'exploit	8
Appareils mobiles.....	9
Réseaux sociaux	9
Bilan de l'année 2016	11
Principaux événements de 2016.....	11
Volume et diversité	11
Reprise des ransomware	12
Bifurcation des campagnes de malware par e-mail.....	13
Convergence du spam, du phishing et des malware.....	13
Piratage de la messagerie en entreprise (BEC)	14
Kits d'exploit	15
Amélioration du ciblage	16
Réseaux sociaux	16
Menaces liées aux appareils mobiles.....	17
Le point sur la recherche 2016	18
Menaces persistantes avancées	18
Trojans bancaires, Chevaux de Troie bancaires et voleurs.....	18
Piratage de la messagerie en entreprise (BEC)	18
Propagation et techniques.....	18
Kits d'exploit et malvertising.....	18
Contexte	19
Appareils mobiles.....	19
Ransomware	19
Réseaux sociaux	19
Spam	19
Vulnérabilités inédites et autres	19
Nos recommandations.....	20

POINTS CLÉS : PLUS GROS, PLUS RAPIDES, PLUS NOMBREUX

Les tendances observées en 2016 montrent qu'au 4e trimestre, les cybercriminels ont changé de techniques et d'approches afin de rentabiliser au maximum les malware et l'infrastructure. Le volume des messages associés à des campagnes malveillantes a augmenté de façon spectaculaire. Les tactiques employées pour échapper aux outils de cybersécurité ont gagné en complexité. Les attaques par piratage de la messagerie en entreprise (BEC, Business Email Compromise) ont évolué à mesure que les pirates inventaient de nouvelles manières d'usurper l'identité des dirigeants et de leurrer leurs victimes pour les inciter à transférer de l'argent ou à transmettre des données sensibles. Le marché des kits d'exploit (outils conviviaux qui permettent d'exploiter les vulnérabilités des systèmes) a lui imposé lorsque les pirates ont multiplié les opérations d'exploitation de la nature humaine et d'ingénierie sociale.

Les attaques associées aux kits d'exploit (EK) traditionnels se sont stabilisées en fin d'année, et le niveau d'activité du 4e trimestre est très inférieur à celui du 1er. Mais les kits d'exploit qui visent les appareils mobiles et l'Internet des objets (IoT) tels que les **routeurs Internet des particuliers** ont fait leur apparition, révélant la disponibilité accrue des vulnérabilités exploitables au sein de ce nouvel espace. Sur les réseaux sociaux, l'activité malveillante associée aux événements majeurs et aux grandes tendances a également connu une recrudescence, comme le contenu négatif, nuisible et malveillant dont le volume a augmenté de façon drastique sur ces réseaux. Cette activité inclut le « phishing Angler », terme par lequel nous désignons les attaques impliquant de faux comptes d'assistance à la clientèle, destinés à leurrer les utilisateurs qui recherchent de l'aide pour les inciter à communiquer leurs identifiants de connexion et autres informations. Pour les pirates, toutes ces menaces se traduisent par une forte rentabilisation.

Voici les principales conclusions de ce dernier trimestre, ainsi qu'un aperçu général de l'année 2016.

MESSAGERIE ET KITS D'EXPLOIT

La plus grande campagne d'e-mails malveillants du 4e trimestre a été 6,7 fois plus importante que la plus grande du 3e trimestre. Toutes deux impliquaient la famille de ransomware Locky et passaient par l'envoi de fichiers et de code JavaScript malveillants compressés. Elles marquent une nette augmentation de ces tactiques par rapport aux campagnes précédentes, qui passaient par des pièces jointes comportant des macros malveillantes.

Les pièces jointes JavaScript malveillantes ont régulièrement dépassé en nombre (de quatre à six fois) le volume de messages avec document joint. Les pirates ont également utilisé d'autres types de script (par exemple, .vbs et .wsf) dans le but d'échapper à toute détection.

L'activité globale des kits d'exploit est restée stable au 4e trimestre, à 93 % de son niveau record du 1er trimestre. Une partie de l'activité susceptible d'utiliser le fameux kit d'exploit Angler passe désormais par les kits RIG et Neutrino. Le kit d'exploit Angler (qui n'a rien à voir avec le phishing Angler sur les réseaux sociaux) a disparu à la fin du 2e trimestre. D'une manière générale, le marché des kits d'exploit a été en grande partie relégué aux opérateurs de malvertising de niveau intermédiaire et aux publicités en ligne incorporant du code malveillant pour exploiter les vulnérabilités des navigateurs.

Les escroqueries au PDG ciblant le Directeur financier ont chuté de 28 % entre les mois d'août (où elles représentaient alors 39 % des e-mails de pirates se faisant passer pour le PDG) et de décembre. L'adoption de la norme DMARC a connu un essor de 33 % entre les 3e et 4e trimestres. Face au phishing par piratage de la messagerie en entreprise (BEC), les organisations deviennent plus agressives. Mais les auteurs d'attaques BEC s'adaptent également et améliorent désormais leurs techniques en envoyant des e-mails aux employés subalternes.

Le nombre de nouvelles variantes de ransomware atteint près de 30 fois celui de ce même trimestre l'année dernière. La plus grande partie du volume de ransomware était associée à Locky, mais le nombre de variantes continue de croître rapidement. Parmi ces dernières, Cerber et CryptXXX, qui ont été propagées par e-mail et kit d'exploit, se démarquent.

APPAREILS MOBILES

Le kit d'exploit DNSChanger a potentiellement exposé des centaines de milliers d'appareils mobiles à des attaques redirigeant les utilisateurs vers des sites Web malveillants. Utilisant la technique dite de redirection DNS, ces attaques potentielles incluaient du malvertising et de la redirection de publicité. Ce kit n'exploite pas les vulnérabilités des appareils mobiles, mais les lacunes des routeurs réseau qu'utilisent les particuliers et les petites entreprises pour connecter les appareils mobiles à Internet.

APPAREILS MOBILES (SUITE)

4 500 applis mobiles liées aux Jeux Olympiques d'été et aux marques des sponsors étaient douteuses ou malveillantes. Les menaces qui ciblent les mobiles et les réseaux sociaux exploitent souvent les grands événements et les tendances majeures. Les applis douteuses susceptibles de voler des données sont monnaie courante sur les principales plateformes mobiles.

RÉSEAUX SOCIAUX

Le nombre de comptes de réseau social frauduleux a doublé entre les 3e et 4e trimestres. Ces comptes peuvent ensuite être utilisés pour du phishing, des escroqueries, la propagation de programmes malveillants, etc.

Les attaques par phishing sur réseau social ont quintuplé cette année. Cela inclut le phishing Angler qui détourne les services d'assistance client sur les réseaux sociaux.

POINTS FORTS DU 4E TRIMESTRE

Le 4e trimestre de 2016 a enregistré de fortes variations quant aux charges utiles, au chronométrage et aux techniques employés pour diffuser des malware et attaquer les entreprises et les consommateurs. Le volume et la diversité de ces attaques dépassent de loin ceux que nous avons pu observer tout au long de l'année 2016. De l'ampleur sans précédent des campagnes Locky aux attaques des routeurs à domicile via le malvertising, les cybercriminels ont continué à innover et à expérimenter.

MENACES LIÉES AUX PROGRAMMES MALVEILLANTS ET AU COURRIER ÉLECTRONIQUE

L'e-mail est resté le principal vecteur de propagation des programmes malveillants, tandis que les kits d'exploit ont poursuivi leur déclin et que les fournisseurs ont rapidement corrigé les vulnérabilités Zero Day et limité l'efficacité des kits d'exploit. Plusieurs facteurs sont venus compliquer les efforts de détection, au niveau de l'utilisateur comme de l'antivirus :

- Ingénierie sociale
- Volume élevé de spam
- Ciblage et personnalisation d'ampleur limitée
- Augmentation continue du nombre de pièces-jointes aux e-mails n'utilisant pas les formats Microsoft Word et Excel (ex. : JavaScript, archives RAR, etc.)
- Propagation d'URL par le biais de plateformes de confiance telles que Microsoft SharePoint ou de variations intentionnellement mal orthographiées (typosquattage) d'URL apparemment fiables

Les malware eux-mêmes poursuivent également leur évolution, avec l'apparition des éléments associés aux réseaux sociaux **dans l'espace des ransomware** et des macros malveillantes plus sophistiquées.

TENDANCES DES VOLUMES ET TECHNIQUES ASSOCIÉES AUX MENACES DU 4E TRIMESTRE

En fin d'année 2016, l'importance du volume est restée essentielle dans le paysage des menaces associées aux e-mails.

Le ransomware Locky en particulier a été propagé par la plus vaste campagne de spam jamais observée et a dominé le trafic des messages malveillants tout au long du trimestre.

Statistique clé : la plus vaste campagne d'e-mails propageant le ransomware Locky a été de 35 % supérieure à la plus grande campagne du 3e trimestre, lui-même record.

Analyse : l'activité erratique des campagnes de mi-2016 a repris au 4e trimestre. Le spam Locky a connu trois grandes interruptions : deux semaines en octobre, une semaine en novembre et, comme pour les dernières vacances de l'année précédente, la dernière semaine de décembre. Les volumes sont toutefois restés très élevés, l'activité restant essentiellement liée à la propagation de charges utiles Locky par le biais de code JavaScript joint et compressé. Les plus grosses campagnes du 4e trimestre ont surpassé de 35 % les volumes des plus grosses campagnes du 3e trimestre.

Outre les campagnes de grande ampleur propageant Locky à travers les pièces jointes JavaScript, nous avons également constaté que de vastes campagnes Locky utilisaient :

- Des documents joints Microsoft Word et Excel incluant des macros malveillantes
- Des URL conduisant à des fichiers JavaScript compressés et autres documents malveillants
- Des fichiers VBScript compressés

Au 4e trimestre, la principale différence provient de la combinaison de ces techniques. Alors que, de février à septembre, les campagnes Locky de grande ampleur passaient par un seul type de pièce jointe, nous avons à plusieurs reprises observé que deux ou trois de ces techniques étaient réunies dans une même campagne au 4e trimestre.

Les derniers mois de 2016 sont également marqués par une reprise des URL. Ces adresses conduisent toutefois davantage à des charges utiles malveillantes qu'aux kits d'exploit qui caractérisaient les campagnes de 2013 et 2014. Relativement rare en 2016, l'utilisation d'URL malveillantes dans les campagnes d'e-mails a rebondi en novembre, alimentée pour l'essentiel par un pirate propageant le cheval de Troie Vawtrak par le biais de campagnes ciblant les États-Unis. Les URL étaient généralement liées à du code JavaScript ou autres documents malveillants hébergés sur des serveurs dédiés ou conduisant à des liens SharePoint contenant du code JavaScript compressé.

Parmi ces campagnes de grande ampleur, la plus importante provenait d'un pirate propageant Vawtrak. Ces URL conduisaient à des téléchargements de documents malveillants, parfois combinés à des documents joints malveillants. Jusque-là, cet escroc organisait seulement des campagnes d'e-mails avec documents joints. Comme bon nombre de pirates que nous surveillons, il semble vouloir expérimenter de nouvelles méthodes de diffusion avant d'opter en dernier ressort pour l'utilisation de liens avec encodage en base 64 des adresses e-mail des destinataires dans l'URL.

La chronologie ci-dessous retrace l'évolution de ces campagnes :

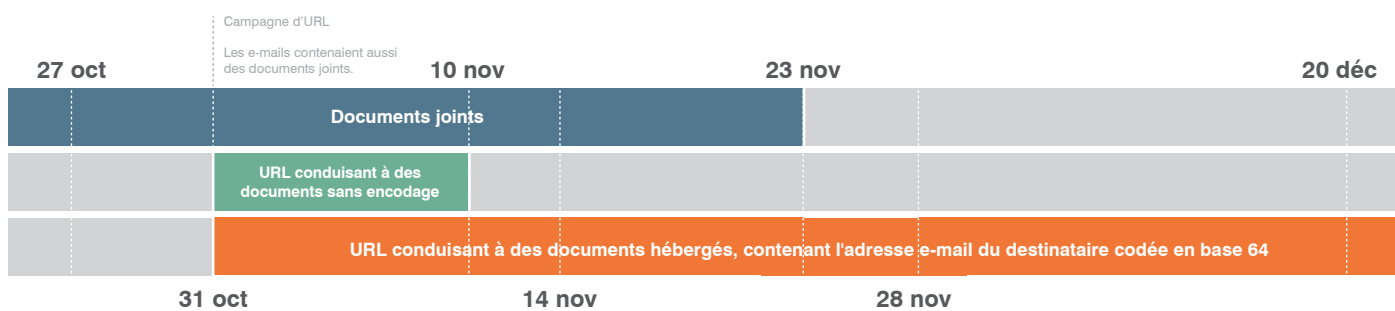


Figure 1 : Chronologie de l'évolution des campagnes Vawtrak

Outre ces campagnes Vawtrak et les quelques campagnes Ursnif qui utilisaient des liens Microsoft SharePoint, l'emploi d'URL dans les e-mails malveillants semble avoir retrouvé un niveau d'activité « normal », relativement faible, en décembre.

Le graphique ci-dessous montre le volume relatif de campagnes par document joint et URL, observées au cours du trimestre. Notez que les variations des fichiers JavaScript joints étaient de loin les plus courantes, la plupart de ces e-mails s'appuyant sur le ransomware Locky. Le retour d'une offensive plus équilibrée en décembre se voit d'ailleurs dans la hausse du volume de documents malveillants, presque équivalente à la baisse du volume de scripts joints compressés.

Volume indexé de messages malveillants par type d'attaque, Octobre - Décembre 2016

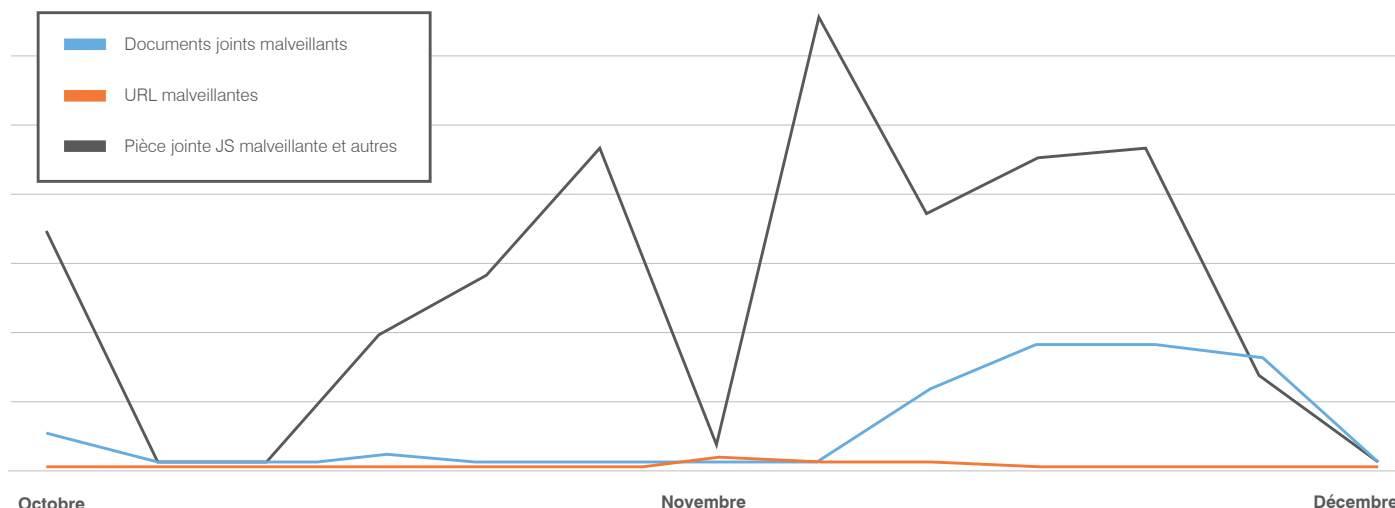


Figure 2 : Volume indexé de messages malveillants par type d'attaques

Comme nous l'avons constaté fin 2015 et début 2016, les vacances de Noël dans les pays occidentaux et les fêtes de Noël orthodoxes en Russie se sont traduites par une pause durable dans la propagation de la plupart des chevaux de Troie bancaires ; l'activité du ransomware Locky s'est également interrompue fin 2016.

TECHNIQUES

Durant les trois derniers mois de 2016, les cybercriminels ont redoublé d'efforts pour contourner ou déjouer d'une manière ou d'une autre les mises en sandbox automatiques et autres formes d'analyses dynamiques automatisées. Par exemple, nous avons décelé des documents joints malveillants dans lesquels des objets VBScript et LNK incorporés remplaçaient les macros malveillantes. D'autres pirates ont commencé à utiliser des documents joints chiffrés ou protégés par un mot de passe inclus dans le corps de l'e-mail. Ces méthodes renforcent la crédibilité du message tout en réduisant les risques de mise en sandbox de ces documents. Nous avons pu observer cette technique dans des campagnes propageant le ransomware Cerber et le cheval de Troie bancaire Ursnif, ou encore dans des campagnes de phishing d'identifiants de connexion.

Statistique clé : les destinations des e-mails contenant des URL malveillantes sont désormais presque exclusivement des pages de phishing dédiées ; au mois de décembre, 1 % seulement des liens inclus dans les e-mails malveillants conduisaient à des pages de kit d'exploit.

Analyse : le phishing d'identifiants, qui reste une menace d'ampleur propice et notable, va des attaques sophistiquées de phishing par harponnage (spear phishing) aux campagnes plus ordinaires de phishing d'identifiants Gmail, Office 365 et autres services Cloud. Ces attaques de phishing se propagent généralement par des liens inclus dans les e-mails et, comme le montre la Figure 3, les URL conduisant directement à des pages de phishing dédiées ont largement remplacé les liens vers les kits d'exploit, beaucoup plus nombreux en 2014 et 2015. À la fin du 4e trimestre, les kits d'exploit représentaient seulement 1 % des liens présents dans les e-mails malveillants. Les changements de destination des URL concordent avec le recul global de l'activité des kits d'exploit de cette année.

Destinations des URL : Pages de phishing d'identifiants par rapport aux kits d'exploit

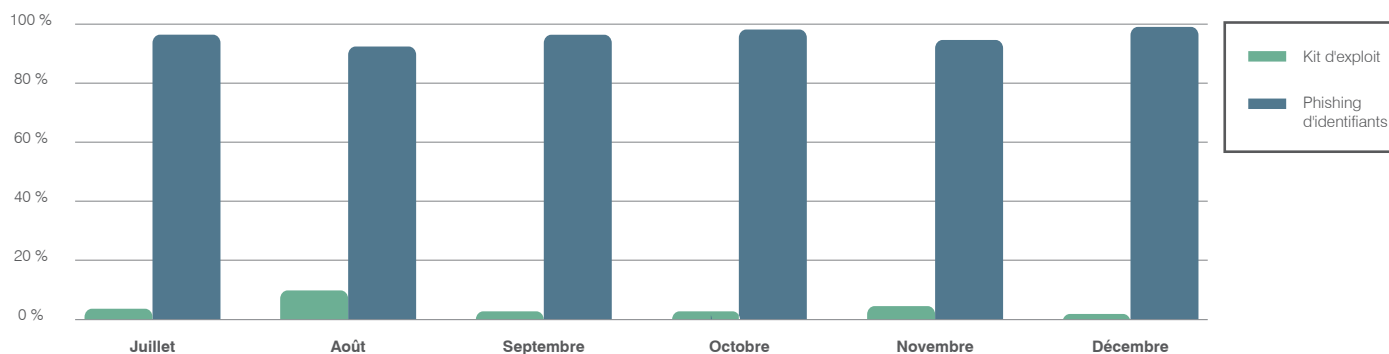


Figure 3 : Comparaison de l'utilisation d'URL dans les e-mails et de liens vers des kits d'exploit

Outre l'apparition de faux sites Web de plus en plus élaborés et destinés au phishing, les techniques employées dans les campagnes de programmes malveillants ont également évolué. Par exemple, nous avons constaté une augmentation constante de l'emploi de PowerShell dans les documents malveillants ces quelques derniers mois. Généralement combiné à des macros malveillantes dans des documents Microsoft Office, PowerShell présente plusieurs avantages pour les cybercriminels par rapport à la seule utilisation de macros pour installer ou télécharger les malware :

- **Parade à la détection :** bien que certains sandbox génèrent des faux négatifs lorsque PowerShell n'est pas installé, cet avantage ne devrait pas durer et disparaîtra dès que les outils et fournisseurs de sécurité combleront leur retard. Le plus gros avantage est que PowerShell permet d'installer des charges utiles malveillantes sans fichier, donc en général d'échapper à la détection.
- **Flexibilité :** plus sophistiqué que les seules macros, PowerShell peut exécuter davantage d'actions. Pour l'instant, son usage se limite au téléchargement et à l'exécution de charges utiles .EXE, mais ce comportement évoluera certainement dès que les cybercriminels recourront davantage à cet outil, en exploitant notamment les malware et outils déjà écrits en PowerShell.

Pour finir, les cybercriminels continuent de perfectionner et d'exploiter les **techniques de personnalisation** déjà observées en début d'année. Combinées à une ingénierie sociale sophistiquée, ces techniques démontrent l'efficacité immuable de l'exploitation du facteur humain, ainsi que la rentabilité potentielle que recherchent les cybercriminels à travers les malware et les nouveaux modes de propagation.

PIRATAGE DE LA MESSAGERIE EN ENTREPRISE (BEC)

La plupart des grandes organisations ont déjà commencé à implémenter les règles et procédures nécessaires pour éviter les pertes massives associées au piratage de la messagerie en entreprise. Les attaques BEC sont des campagnes d'ingénierie sociale soigneusement planifiées, qui commencent par des e-mails ciblés avant de passer à d'autres formes de communication hors bande les rendant difficiles à déceler et à éviter.

Les organisations ont toutefois commencé à adopter des solutions technologiques qui permettent de mieux identifier les e-mails frauduleux à la base des attaques BEC. Les normes SPF, DKIM et DMARC se combinent à un nombre restreint de solutions de fournisseur pour intercepter les e-mails BEC avant qu'ils n'atteignent leurs destinataires.

Statistique clé : les escroqueries au PDG destinées au Directeur financier ont chuté de 28 % entre les mois d'août, où elles représentaient alors 39 %, et de décembre. L'adoption de la norme DMARC a connu un essor de 33 % par rapport au 3e trimestre 2016.

Analyse : comme le montre la Figure 4, il est évident qu'à la fin du trimestre dernier, les auteurs d'attaques BEC ont compris que, lorsqu'ils usurpaient l'identité du PDG dans un e-mail, il était plus efficace de s'adresser aux subalternes qu'au Directeur financier. Les escroqueries au PDG adressées au Directeur financier ont chuté de 28 % entre les mois d'août, où elles représentaient alors 39 %, et de décembre.

Escroqueries au PDG visant le Directeur financier au 2e semestre 2016

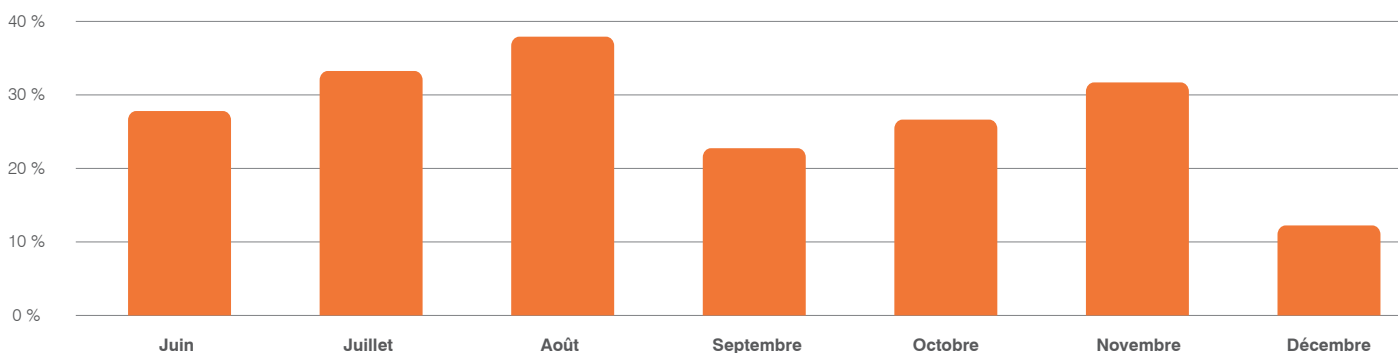


Figure 4 : Pourcentage total d'e-mails BEC du PDG enregistrés au premier semestre 2016 et spécifiquement adressés au Directeur financier

Types d'usurpation observés au 4e trimestre



Figure 5 : Informations complémentaires sur la nature des attaques BEC et les techniques d'usurpation d'identité sous-jacentes observées au 4e trimestre 2016

Par ailleurs, les taux d'adoption de la norme DMARC (Figure 6 ci-après) d'une année à l'autre par les organisations que nous surveillons laissent entendre que, bien que cette adoption soit large, bon nombre d'organisations doivent encore mettre vraiment en œuvre ces technologies.

Taux d'adoption de la norme DMARC par secteur - 4e trim. 2016

Secteur	Adoption de DMARC au 4e trimestre 2016	Adoption de DMARC au 4e trimestre 2015	Progression annuelle
Banques	36 %	27 %	33 %
Santé	28 %	16 %	75 %
Télécommunications	29 %	21 %	36 %
Logistique	50 %	41 %	22 %
Services de paiement	44 %	32 %	36 %
Administrations	50 %	25 %	100 %
Distribution/eCommerce/Jeux	33 %	25 %	30 %
Réseaux sociaux	63 %	59 %	36 %
Technologie	61 %	51 %	6 %
Voyages	39 %	31 %	26 %
TOTAL	38 %	33 %	17 %

Figure 6 : Taux d'adoption de la norme DMARC par secteur d'activité

APERÇU DES KITS D'EXPLOIT

À la fin de l'année 2016, l'activité des kits d'exploit (EK) reste au même niveau qu'au 3e trimestre. Globalement, les kits d'exploit n'ont pas récupéré le terrain perdu au premier semestre de 2016 en tant que vecteur de propagation, et les **tendances montrent** même qu'ils n'ont guère de chance d'y parvenir. L'activité des kits d'exploit enregistrée au 4e trimestre, essentiellement liée au malvertising, reste néanmoins importante. Si le kit Angler, auparavant dominant, n'a pas fait sa réapparition, le kit RIG et ses variantes constituent désormais le plus gros du trafic de kit d'exploit.

Statistique clé : au 4e trimestre, l'activité des kits d'exploit demeure à 93 % du sommet atteint en janvier et ne montre aucun signe d'augmentation future.

Activité des kits d'exploit : échantillons collectés au 4e trimestre 2016

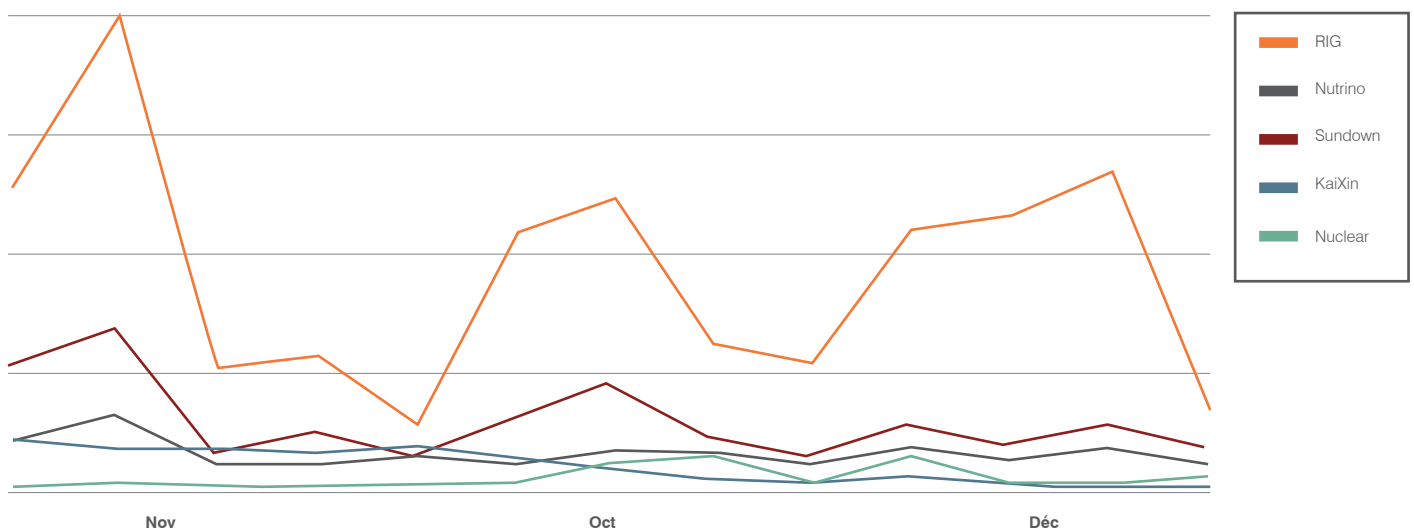


Figure 7 : Activité des kits d'exploit au 4e trimestre 2016

Analyse : cette baisse d'activité des kits d'exploit par rapport à 2015 devient la « nouvelle norme », mais ne signifie pas pour autant que cet élément essentiel de l'infrastructure des cyber-menaces soit en stagnation. Le **kit d'exploit DNSChanger** démontre que, dans le secteur des kits d'exploit, l'innovation est permanente. Le kit DNSChanger, qui passe surtout par le malvertising, peut attaquer les routeurs SOHO à travers les navigateurs pour Windows et Android. Les terminaux eux-mêmes ne sont pas infectés, mais une fois les routeurs compromis, leurs enregistrements DNS sont alors remplacés et, quel que soit leur système d'exploitation, tous les appareils deviennent vulnérables aux attaques de malvertising, aux fenêtres contextuelles indésirables et autres. L'utilisation massive du kit DNSChanger enregistrée au mois de décembre nous laisse penser qu'il pourrait s'agir d'une nouvelle orientation dans l'emploi de kits d'exploit standard rapidement modifiables par les fournisseurs pour compromettre les PC, transformant les appareils tels que les routeurs et les terminaux IoT en cibles privilégiées.

APPAREILS MOBILES

Au 4e trimestre, le paysage des menaces visant les appareils mobiles a continué à évoluer rapidement. Les applis dangereuses et malveillantes et les clones d'appli ont fait leur apparition, tandis que les kits d'attaque des mobiles et les kits d'exploit IoT offrent de nouvelles possibilités aux cybercriminels sur les systèmes d'exploitation mobiles.

Statistique clé : des centaines de milliers d'appareils mobiles ont été soumis au malvertising, à des attaques potentielles, etc.

Analyse : les appareils mobiles ont non seulement été affectés par les actions du kit DNSChanger, mais sont également devenus un vecteur intéressant via lequel ce même kit pourrait infecter les routeurs des particuliers et des petites entreprises. Les chercheurs de Proofpoint ont confirmé que tous ceux qui utilisent Chrome pour accéder à Internet sur Android sont susceptibles d'infecter les routeurs SOHO vulnérables par lesquels passe leur connexion. Il est intéressant de noter que la vulnérabilité n'était pas inhérente à Chrome ou Android, mais aux communications normales entre l'appareil mobile et le routeur ; le kit d'exploit DNSChanger utilise l'appareil mobile pour modifier les enregistrements DNS du routeur, mais ne compromet pas l'appareil lui-même. Pour autant, une fois le routeur compromis, tous les appareils mobiles et de bureau sont alors soumis à la redirection de navigateur, au malvertising, aux fenêtres contextuelles, etc., quel que soit leur système d'exploitation (iOS et Android compris).

RÉSEAUX SOCIAUX

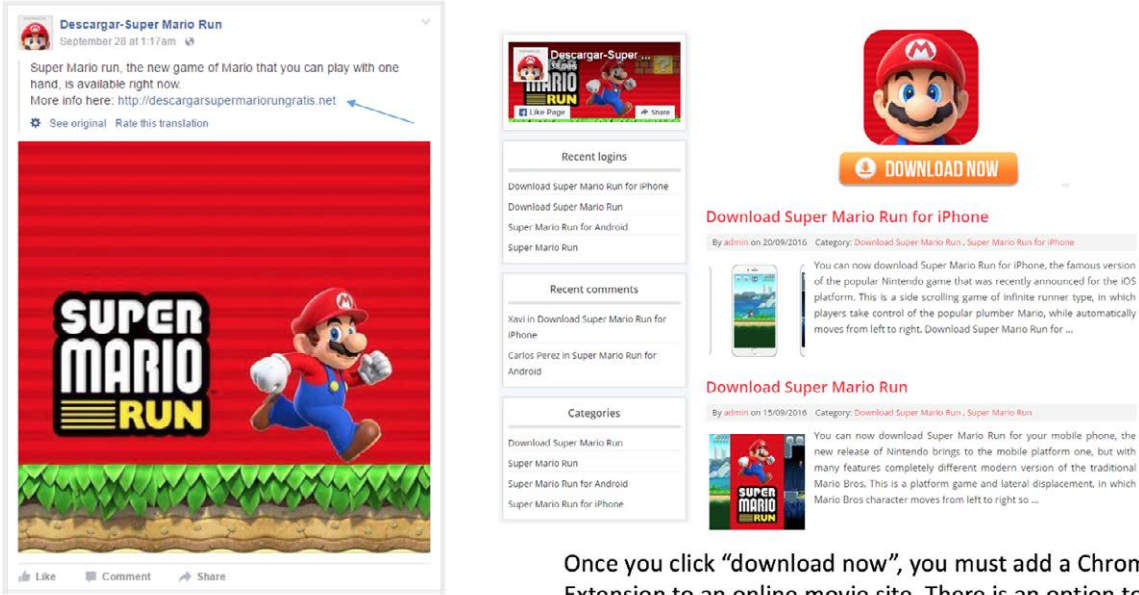
L'utilisation des réseaux sociaux en tant que vitrine des marques a poursuivi son essor rapide au 4e trimestre ; dans le même temps, les cybercriminels ont profité de cette croissance pour étendre leurs activités. Un certain degré de contagion entre les réseaux sociaux, les mobiles et les malware a également été observé.

Statistique clé : l'utilisation de faux comptes de réseau social a augmenté de 100 % entre les 3e et 4e trimestres 2016.

Analyse : nous avons constaté que l'utilisation de comptes frauduleux a globalement doublé entre les mois de septembre et octobre 2016. Du courrier indésirable au « **phishing Angler** », ces faux comptes ont été largement exploités. À cet égard, les chercheurs de Proofpoint ont observé une augmentation de 20 % du contenu indésirable sur Facebook et Twitter d'un trimestre à l'autre. Le 4e trimestre enregistre le second record de 2016 en termes de volume de spam (le 1er trimestre était le premier).

Les comptes Twitter légitimes d'assistance ont envoyé plus de messages privés que jamais, les messages directs envoyés au 4e trimestre augmentant de plus de 25 % par rapport au 3e. Toutefois, les comptes d'assistance envoyant davantage de messages et les clients s'habituant peu à peu à interagir directement avec leurs marques favorites, le phishing Angler devient plus facile et les clients probablement moins soupçonneux. Au 4e trimestre, le phishing Angler a été le plus courant sur les comptes de services financiers et de divertissement.

Comme le montre la multitude de pages « Super Mario Run » apparues au 4e trimestre, avant et après la sortie très attendue de ce jeu pour mobile, les cybercriminels ont continué d'exploiter les sujets d'actualité via leurs comptes frauduleux. Comme pour le jeu **Pokemon Go**, de nombreux comptes de réseaux sociaux ont proposé des liens permettant de « télécharger » le jeu. Ces liens conduisaient en réalité à des malware ou à des enquêtes telles que celle ci-dessous (Fig. 8).



The image shows a Facebook post on the left and a website on the right. The Facebook post is from a page named 'Descargar-Super Mario Run' and contains text about downloading the game for free. The website on the right has a 'DOWNLOAD NOW' button and several articles with titles like 'Download Super Mario Run for iPhone' and 'Download Super Mario Run'. A blue arrow in the Facebook post points to a link in the text.

<https://www.facebook.com/descargarsupermariorun/>

Once you click “download now”, you must add a Chrome Extension to an online movie site. There is an option to register to the website.

Figure 8 : Faux téléchargements du jeu Super Mario Run

Soulignant les interactions croissantes entre malware et réseaux sociaux, les chercheurs de Proofpoint ont également détecté le logiciel de verrouillage de poste de travail **Ransoc**. Le logiciel Ransoc, qui reflète une tendance grandissante appelée « doxware », scrute les profils sur Skype et les réseaux sociaux pour y dénicher des informations personnelles, et analyse les fichiers et les dossiers Torrent pour y trouver d'éventuelles données sensibles. Toutefois, et contrairement au ransomware de cryptage plus notoire qui s'était imposé en 2016, Ransoc menace les victimes de fausses procédures légales s'ils ne paient pas la rançon lorsqu'il détecte du contenu contestable voire illégal.

BILAN DE L'ANNÉE 2016

En 2016, le paysage des menaces s'est caractérisé par les extrêmes et a laissé peu de place au juste milieu :

- Campagnes massives de centaines de millions de messages propageant le ransomware Locky
- Campagnes plus ciblées et de moindre ampleur passant par le cheval de Troie bancaire Dridex, principal malware de messagerie de 2015
- Interruption quasi-totale de Locky et Dridex lors de la panne du botnet Necurs qui a duré un mois
- Hausse sans précédent du trafic des kits d'exploit en début d'année, suivie d'une baisse spectaculaire jusqu'au nouveau niveau actuel, bien inférieur
- Vastes campagnes soutenues de malvertising passant par les kits d'exploit et ciblage et filtrage plus élaborés affectant des millions d'utilisateurs
- Croissance rapide et ininterrompue des menaces sur les réseaux sociaux et les mobiles, du phishing Angler aux kits d'exploit pour mobiles

Pour savoir ce que nos experts prévoient en 2017 en matière de menaces, consultez notre blog Threat Insight et découvrez nos [Prévisions 2017 en matière de cybersécurité](#).

PRINCIPAUX ÉVÉNEMENTS DE 2016

En 2016, le paysage des menaces a radicalement changé, en entamant une forte transition vers des campagnes de grande ampleur dans les secteurs des kits d'exploit et de la messagerie. Le repli marqué de l'activité des kits d'exploit a été compensé par les vastes campagnes de malvertising, tandis que les ransomware, en pleine expansion, ont dominé l'espace qu'occupaient auparavant les chevaux de Troie bancaire.

Volume et diversité

Statistiques clés :

- Par rapport à 2015, le volume de documents joints malveillants a augmenté de 600 %.
- Le volume total de pièces jointes JavaScript et leurs variantes (négligeable en 2015) atteint au total 2,5 fois celui de tous les documents joints malveillants.
- Même les messages à URL malveillantes (une petite portion du volume total de messages malveillants) ont augmenté de plus de 300 % par rapport à 2015.

Les volumes d'e-mails malveillants ont dramatiquement augmenté tout au long de l'année 2016. Alors que nous mesurons les « campagnes de grande ampleur » en centaines de milliers de messages en 2015, puis en millions de messages au premier trimestre 2016, au sein de la base de clients Proofpoint, ces campagnes atteignaient régulièrement des centaines de millions de messages fin 2016. Dans le même temps, ces vastes campagnes ont progressivement cessé d'utiliser les documents avec macros propageant des charges utiles de chevaux de Troie bancaires (en général, Dridex) pour se tourner vers des pièces jointes JavaScript malveillantes propageant le ransomware Locky. Le graphique ci-dessous souligne à la fois la croissance des campagnes et l'évolution des vecteurs de propagation tout au long de 2016.

Volume hebdomadaire indexé de messages malveillants par type d'attaques en 2016

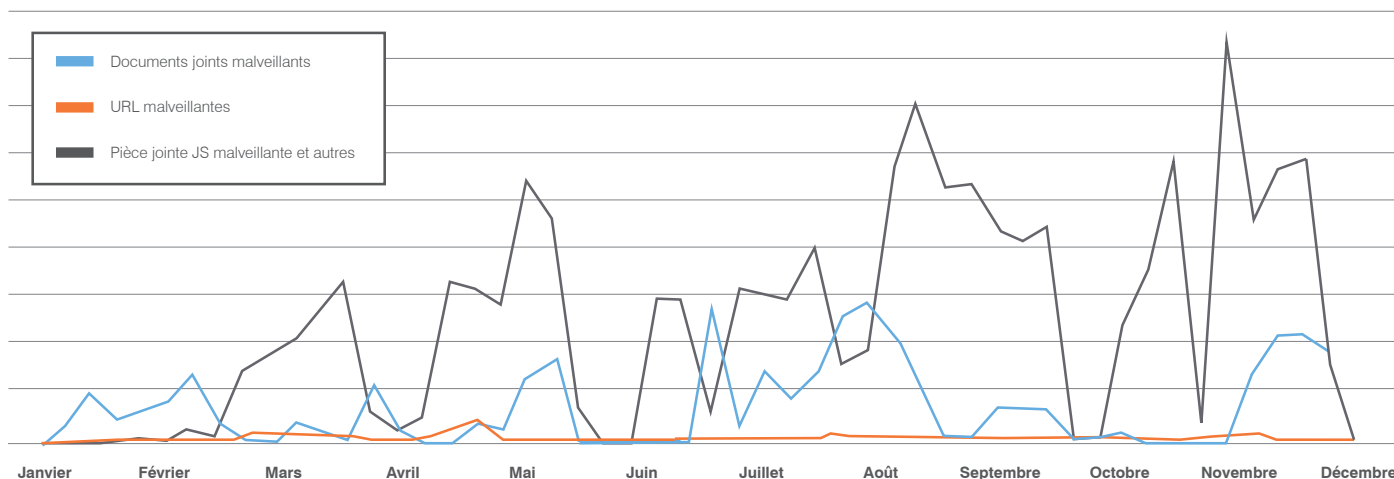
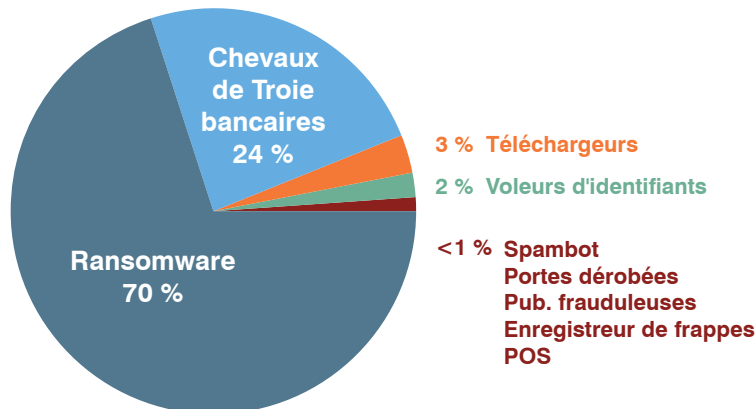


Figure 9 : Volume relatif de messages par type d'attaques

Bien qu'en 2016, le principal type de programme malveillant propagé par e-mail au sein de la base de clients Proofpoint ait été le ransomware, les chevaux de Troie bancaires représentent encore près d'un quart des malware passant par les e-mails. Parmi ces messages électroniques, un nombre disproportionné a été envoyé durant le premier trimestre 2016, avant que les cybercriminels qui propageaient Dridex ne se tournent vers le ransomware Locky, que les chercheurs de Proofpoint **ont découvert en février 2016**. Un pourcentage bien inférieur de malware globalement liés aux e-mails (Fig. 10) propageait des téléchargeurs intermédiaires, des voleurs d'identifiants, des robots de spam (spambot) et autres charges utiles.

Catégories de programmes malveillants : Janvier-Octobre 2016**Figure 10 : Catégories de malware propagées par e-mail entre les mois de janvier et d'octobre**

L'ampleur exceptionnellement élevée des campagnes propageant Locky n'a toutefois pas empêché les cybercriminels et autres escrocs d'innover dans d'autres secteurs. Les nouveaux chevaux de Troie bancaires comme **Panda Banker**, les voleurs d'informations comme **August Stealer**, les téléchargeurs comme **RockLoader**, voire même les nouveaux malware POS (Point-of-Sale) ont tous contribué à cet éventail considérable de logiciels malveillants, et ce malgré le battage médiatique autour du ransomware Locky.

Par ailleurs, les familles de malware bien établies comme les chevaux de Troie bancaires Vawtrak et **Ursnif** ont été largement exploitées, en particulier dans les campagnes dites « personnalisées » ou géographiquement ciblées.

REPRISE DES RANSOMWARE

Statistique clé : le nombre de variantes de ransomware en vigueur a presque été multiplié par 30, même si la grande majorité concernait le ransomware Locky.

Bien que le ransomware Locky, avec ses vastes campagnes d'e-mails et son utilisation encore sans précédent des pièces jointes JavaScript, ait été le plus répandu de cette année, l'essor global des ransomware en 2016 est significatif. Par rapport au nombre de variantes de ransomware en circulation fin 2015 (un nombre relativement stable au fil des ans), nous avons observé que ce nombre avait augmenté de plus de 30 fois fin 2016. La plupart d'entre elles n'ont pas atteint la visibilité ni la large distribution des variantes telles que CryptXXX ou Cerber, mais le nombre de variantes et la facilité avec laquelle les cybercriminels peuvent désormais créer et propager ce type de malware, nous conduisent à désigner les ransomware comme le nouveau « **Bonjour, la compagnie !** » des **malware modernes**.

Évolution des variantes de ransomware depuis décembre 2015

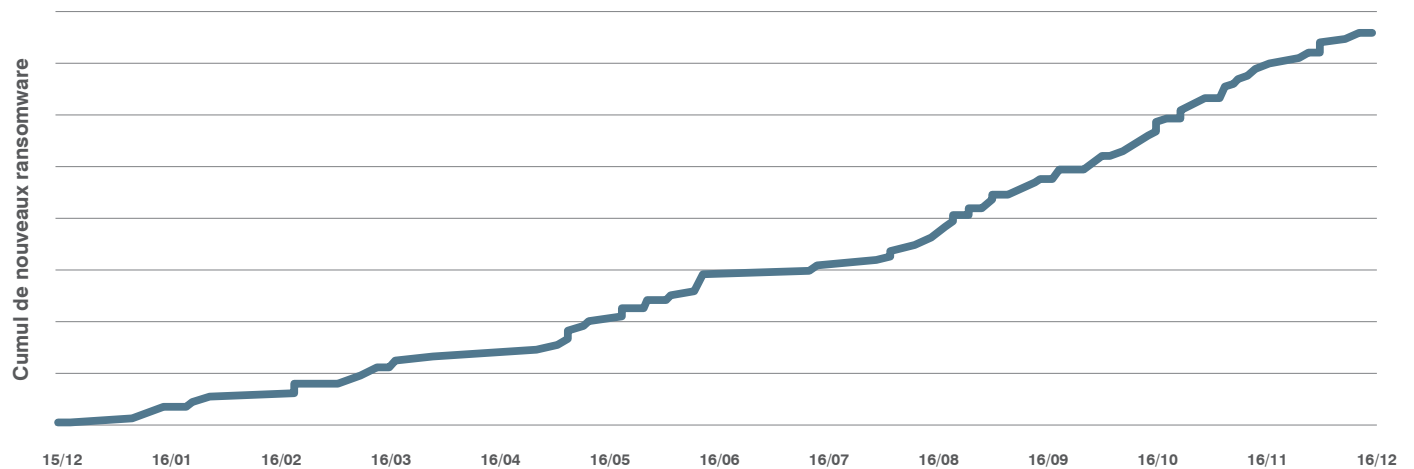


Figure 11 : Croissance cumulée des variantes de ransomware

L'évolution des programmes malveillants à « problème instantané » ne s'est pas limitée aux ransomware de cryptage des fichiers. Par exemple, outre les types de ransomware classiques, nous avons constaté que les verrouilleurs de poste de travail étaient également en augmentation. Au lieu de crypter les fichiers stockés dans les PC, ces malware interdisent simplement l'accès à l'ordinateur via une application ou une page Web affichée en plein écran et exigent le versement d'une rançon pour rétablir cet accès. Comme nous l'avons vu précédemment, l'instance la plus élaborée des « doxware » (les logiciels de verrouillage de poste de travail Ransoc) a démontré que l'innovation était constante pour ce type de malware, et laisse entrevoir de nombreuses possibilités encore inexploitées dans la catégorie des malware à 'problème immédiat'.

D'une manière générale, cette évolution traduit la propension des campagnes de grande ampleur à opter pour des logiciels faciles à rentabiliser, par opposition aux chevaux de Troie bancaires, enregistreurs de frappe, RAT et autres programmes malveillants qui exigent bien plus de préparation et de maintenance et ne sont pas forcément rentables pour les cybercriminels.

BIFURCATION DES CAMPAGNES DE MALWARE PAR E-MAIL

En 2016, les campagnes de malware par e-mail ont connu une certaine dichotomie. Alors que le courrier indésirable s'appuyait jusque-là sur des campagnes de grande ampleur de style « en rafales », les campagnes Dridex de 2015 et Locky de 2016 ont exploité cette même technique pour la propagation des malware. Fin 2016, les cybercriminels qui distribuaient notamment le ransomware Locky ont placé très haut la barre de la propagation des malware par e-mail à grande échelle. Bien qu'éclipsé par les campagnes Locky, le ransomware Cerber s'est également fortement répandu au second semestre 2016. Les ransomware se prêtent bien à ce type de distribution puisqu'ils n'exigent pas le même niveau de personnalisation selon les régions que les chevaux de Troie bancaires, à savoir les injections Web à saisir selon les différentes banques.

Il semble que les cybercriminels soient parvenus à la même conclusion en 2016, et aient peu à peu réservé les chevaux de Troie bancaires, RAT, enregistreurs de frappe et autres voleurs d'informations aux campagnes ciblées de plus faible envergure. Les campagnes de chevaux de Troie bancaires sont devenues plus ciblées, en termes de régions comme de secteurs ; Dridex, par exemple, qui a fait sa réapparition en août après un silence quasi-total en juin et juillet, ciblait les banques suisses. De même, un auteur d'e-mails non sollicités connu pour la forte personnalisation de ses campagnes a régulièrement propagé les chevaux de Troie bancaires Ursnif et Nymaim par le biais d'attaques ciblées tout au long des trois derniers trimestres de 2016.

Ces campagnes de moindre ampleur laissent toute la liberté nécessaire aux cybercriminels pour imaginer des offensives plus lucratives et mieux exploiter les informations volées, tandis que les vastes campagnes de ransomware maximisent les profits, bien que les taux de conversion soient plus faibles.

CONVERGENCE DU SPAM, DU PHISHING ET DES MALWARE

D'une manière générale, les cybercriminels ont tendance à se spécialiser : les spammeurs distribuent du courrier indésirable, les adeptes du phishing s'intéressent aux identifiants de connexion et aux données personnelles, et les auteurs de malware atteignent leurs buts à l'aide de logiciels malveillants. En 2016, toutefois, d'autres convergences sont apparues entre les diverses menaces associées aux e-mails. Les vecteurs et les méthodes de propagation ont eux-mêmes évolué, à mesure que les cybercriminels s'adaptent au changement de contexte.

En décembre par exemple, les chercheurs de Proofpoint ont décrit une campagne d'e-mails lancée par un auteur de phishing connu qui utilisait des documents joints protégés par mot de passe. Cette technique avait déjà été employée par les cybercriminels propageant le ransomware Cerber et autres malware pour échapper à la détection et donner un caractère plus urgent et plus crédible à leurs e-mails. L'usage de cette approche pour le phishing d'identifiants (la page de hameçonnage prenant la forme d'un fichier joint protégé par un mot de passe) met en évidence le processus d'hybridation de ces techniques pour garder une longueur d'avance sur les systèmes de défense en amélioration constante.

Depuis sa découverte au mois d'avril, et contrairement à Locky et Cerber, le ransomware CryptXXX s'est essentiellement propagé à travers les kits d'exploit. Au mois de juillet, les chercheurs de Proofpoint ont ensuite constaté que ce programme malveillant était également présent dans des campagnes de messagerie. Le calendrier coïncide avec la baisse de 96 % du trafic des kits d'exploit entre les mois d'avril et juin, laissant supposer que les cybercriminels ont tenté de s'adapter à ces nouvelles conditions en se détournant peu à peu des techniques de distribution en perte d'efficacité pour adopter des méthodes au bon rapport coût/efficacité.

Cette adaptation et cet ajustement permanents s'appliquent autant aux charges utiles qu'aux techniques de distribution et d'esquive. Par exemple, les cybercriminels à l'origine de Dridex (malware « à succès » de 2015) ont réellement accéléré l'effet boule de neige des ransomware en début d'année 2016 avec Locky. En parallèle, et à mesure que les ransomware reprenaient leur activité à travers des campagnes de grande ampleur, les fonctionnalités des chevaux de Troie bancaires ont également multiplié leurs capacités de vol et d'établissement du profil des applications et services installés, voire se sont transformées en chargeurs intermédiaires. Cela traduit la capacité des cybercriminels à optimiser encore l'efficacité des charges utiles à succès : celles à « problème immédiat » comme les ransomware n'ont pas vraiment besoin d'échapper à la détection après infection initiale, et la furtivité des chevaux de Troie bancaires en fait des candidats idéaux pour de nombreux usages, de l'enregistrement de frappes au téléchargement de malware POS et autres charges utiles.

PIRATAGE DE LA MESSAGERIE EN ENTREPRISE (BEC)

Bien que le FBI ait déjà déclaré que le piratage de la messagerie en entreprise se chiffrait déjà en milliards, la menace n'est pas réservée aux très grandes entreprises. En réalité, près de 15 % des attaques BEC concernent les entreprises de moins de 5 000 employés, soit plus que n'importe quel groupe présent dans nos données.

Si les grandes organisations ont éventuellement plus d'argent et sont donc de meilleures cibles pour les auteurs d'attaques BEC, les sociétés plus petites ont elles moins de ressources à allouer à leur protection contre ces attaques. Quelle que soit leur taille, toutefois, les organisations examinent diverses solutions électroniques. Comme nous l'avons vu au 4e trimestre, la mise en œuvre et l'application des normes SPF, DKIM et DMARC améliorent la lutte contre les attaques BEC, notamment là où elles commencent, à savoir dans les e-mails frauduleux avec usurpation d'identité. En réalité, 2016 a été « l'année de la norme DMARC », qui enregistre une forte adoption, notamment au sein du secteur public où son utilisation a doublé par rapport à 2015.

Implémentation de la norme DMARC par secteur en 2016

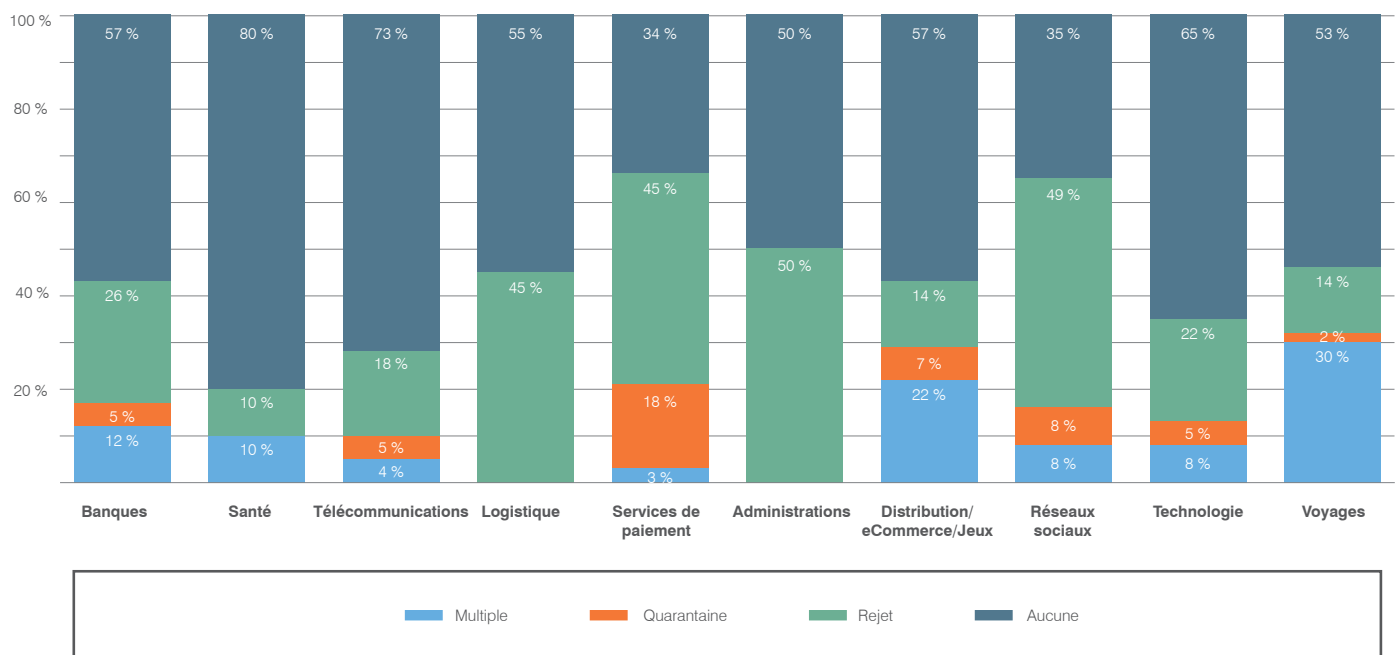


Figure 12 : Implémentation de la norme DMARC par secteur

2016 a été l'année de la norme DMARC La large reconnaissance des attaques BEC en tant que véritable menace pesant sur un grand nombre d'organisations s'est manifestée à travers l'adoption de la norme DMARC dans une multitude de secteurs. Globalement, 38 % des sociétés interrogées par Proofpoint publient actuellement un enregistrement DMARC (en hausse de 29 % sur l'année précédente et de 22 % par rapport à 2014). Alors que les régions EMOA (Europe, Moyen-Orient et Afrique), l'Australie et la Nouvelle-Zélande connaissent encore un certain retard par rapport aux autres parties du monde en termes d'adoption globale (avec respectivement 25 % et 27 %), leur augmentation par rapport au même mois de l'année précédente représente le double de celle que connaît l'Amérique du Nord. Ces deux dernières années, le taux d'adoption le plus rapide de la norme DMARC a été enregistré en Amérique Latine, mais l'Amérique du Nord reste en tête pour son utilisation, avec un taux d'adoption de 51 %, soit une hausse de 42 % sur un an.

KITS D'EXPLOIT

L'un des changements les plus saisissants de 2016 a été le déclin rapide du trafic des kits d'exploit après leur niveau record au premier trimestre. Le kit Angler, jusque-là dominant dans cet espace, a fortement chuté au 2e trimestre après l'arrestation très médiatisée de quelques acteurs clés.

Activité des kits d'exploit : échantillons collectés en 2016

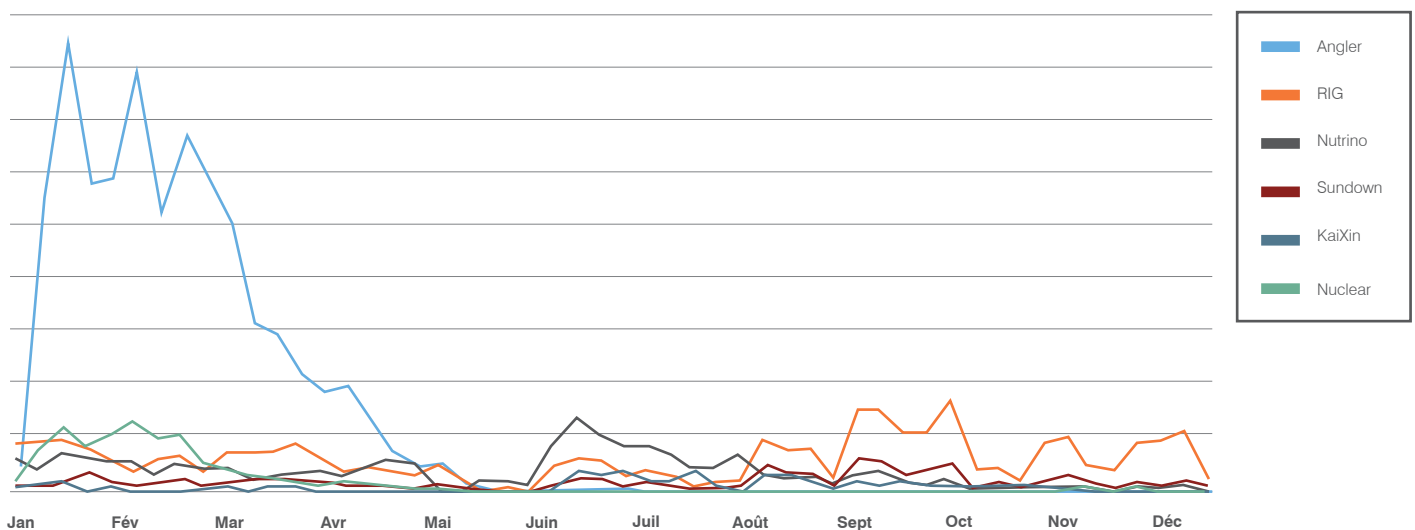


Figure 13 : Volumes relatifs globaux du trafic EK en 2016

Activité des kits d'exploit : Proportion des échantillons collectés en 2016

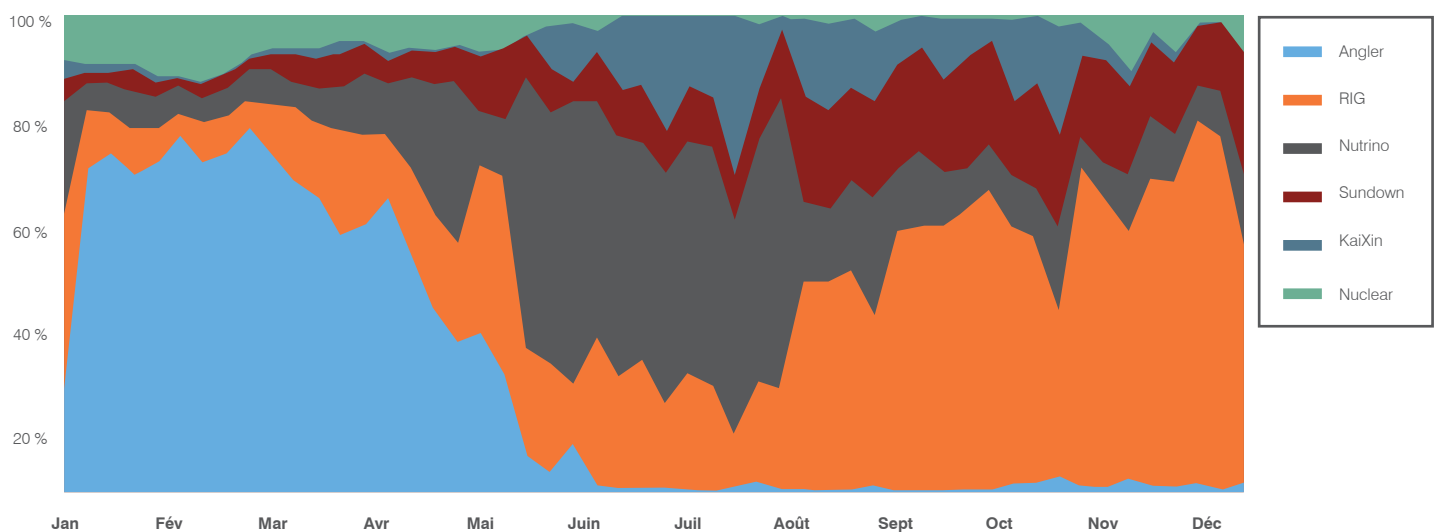


Figure 14 : Activité hebdomadaire des 6 principaux kits d'exploit en pourcentage du total, 2016

Comme le montrent les Figures 13 et 14, bien qu'aucun kit d'exploit n'ait réellement remplacé le kit Angler en termes de volume, les kits Neutrino, Sundown et RIG ont enregistré une hausse relativement importante à mesure que les cybercriminels recherchaient des alternatives. Le trafic global de kits d'exploit atteint néanmoins 93 % des niveaux enregistrés au 1^{er} trimestre tout au long ou presque du second semestre.

Les experts de Proofpoint attribuent ce changement à la baisse des taux de conversion associés aux kits d'exploit, qui montre que les cybercriminels ont de plus en plus de mal à dénicher des visiteurs exploitables. Notre couverture du [groupe AdGholas](#) a illustré la fin de « l'âge d'or » des kits d'exploit en tant qu'outils privilégiés des cybercriminels. Le groupe AdGholas utilisait :

- Un filtrage très complexe pour identifier les utilisateurs de qualité potentiellement les plus vulnérables et exclure la communauté des spécialistes de la sécurité
- Des vulnérabilités de faible niveau qui échappaient à tous les radars, et autorisaient la présentation d'impressions publicitaires malveillantes à des millions d'utilisateurs par jour pour les campagnes les plus vastes

Plus récemment, nous avons constaté que le kit « DNSChanger » ciblait les routeurs SOHO (Small Office/Home Office, ou PME/indépendant). Ce kit n'exploite pas les vulnérabilités des navigateurs ou des systèmes, pour lesquels l'application de correctifs est désormais si rapide que, pour les cybercriminels, les attaques dites Zero Day se révèlent bien moins utiles qu'auparavant, mais sur celles des routeurs et de l'Internet des objets (IoT), bien plus courantes et plus faciles à exploiter.

Cette évolution a conduit les principaux groupes de cybercriminels à totalement abandonner les kits d'exploit, alors que les escrocs moins ambitieux continuent de s'en servir à plus petite échelle. L'innovation se poursuit toutefois dans ce domaine, les vulnérabilités des appareils mobiles et de l'IoT offrant un terrain fertile à de nouvelles campagnes, d'ampleur malgré tout plus limitée.

AMÉLIORATION DU CIBLAGE

Bien que cette année, les gros titres ont surtout mis en avant l'incroyable ampleur des attaques, notamment dans le cas du ransomware Locky, les grandes améliorations apportées au ciblage et à l'automatisation (via les réseaux sociaux, les e-mails ou le trafic associé aux kits d'exploit et aux sites Web compromis) représentent le plus grand risque pour les utilisateurs. Les leurres d'ingénierie sociale, le contenu personnalisé et les différents modes de communication dans le cas des attaques BEC exploitent tous le facteur humain par un biais que les attaques génériques à grande échelle ne permettent pas.

Par exemple, l'un des spammeurs les plus prolifiques que nous surveillons utilise des données recueillies entre autres sur LinkedIn pour [créer des e-mails personnalisés à grande échelle](#) et propager les malware à travers des messages leurres très efficaces. De manière plus limitée (mais avec un impact potentiellement plus important), nous observons toujours une certaine activité des menaces persistantes avancées (APT) associées à un ciblage extrême. Si l'accord signé en août entre les États-Unis et la Chine semble avoir entraîné une baisse mesurable des menaces APT provenant de la Chine contre les intérêts américains, nous avons observé un grand nombre d'opérations APT à travers le monde, notamment issues de la Russie, où les auteurs de menaces APT se sont montrés extrêmement actifs durant le second semestre 2016.

Dans le même temps, comme nous l'avons vu, les campagnes de malvertising organisées par le groupe AdGholas les six premiers mois de l'année ont fait preuve d'une efficacité et d'une précision redoutables dans le ciblage et le filtrage des utilisateurs potentiellement vulnérables. Face à la perte d'efficacité des kits d'exploit et à la baisse des taux de conversion, un filtrage soigné du trafic se révèle indispensable pour rentabiliser au maximum l'utilisation restante des kits d'exploit.

Quel que soit le vecteur ou support, et outre les campagnes massives de Locky ou de vaste malvertising observées en début d'année, les attaques démontrent que le nouvel Eldorado sera les campagnes d'ampleur limitée, et qu'un filtrage soigné permettra aux cybercriminels de rentabiliser au maximum leur investissement.

RÉSEAUX SOCIAUX

Les réseaux sociaux ont poursuivi leur forte croissance tout au long de l'année 2016, autant en tant que plateforme destinée aux particuliers que comme outil professionnel. Les attaques ciblant ces plateformes ont enregistré une croissance tout aussi rapide, tandis que les techniques d'attaque exploitant ces réseaux comme vecteur ont évolué parallèlement. Les attaques de réseaux sociaux assurant un retour sur investissement bien plus important, cette importante hausse n'est pas une surprise et devrait se poursuivre parallèlement à l'évolution des plateformes et des attaques elles-mêmes.

Outre cet essor, quelques autres tendances ont également fait leur apparition cette année. En particulier, nous avons pu constater que les attaques coïncidaient généralement avec les grands événements tels que les [Jeux Olympiques d'été](#). Les applis frauduleuses que proposent les fausses pages de réseau social tirent parti de l'attention que suscitent de tels événements ; les Jeux Olympiques ont donné lieu à des milliers d'applis liées à l'événement, ainsi qu'à une hausse de 60 % du contenu dangereux sur les réseaux sociaux. Les jeux Pokemon GO et Super Mario Run, les élections présidentielles, les vacances et les grands événements sportifs sont tous des exemples d'occasions ou de manifestations entraînant une augmentation de l'activité malveillante sur les réseaux sociaux.

Le phishing Angler a également fait son apparition en tant que menace significative, et cible à la fois les consommateurs et les enseignes. Les adeptes du phishing Angler tirent systématiquement parti des périodes de repos, des domaines d'aspect identique et de l'ingénierie sociale pour récupérer des identifiants de connexion au nom des grandes marques.

MENACES LIÉES AUX APPAREILS MOBILES

Comme pour les réseaux sociaux, 2016 a été une année marquante quant aux menaces visant les appareils mobiles. Outre l'évolution des malware destinés aux plateformes mobiles, qui s'est poursuivie de plus belle, plusieurs risques importants ont fait leur apparition :

- Risques dus aux clones malveillants de certaines applis populaires comme **Pokémon GO**
- Utilisation accrue du chargement latéral (sideloading) pour propager des applis non autorisées
- Mise à disposition d'outils capables de cibler les appareils mobiles tels que **Pegasus**

Si les failles Zero Day qui affectent les PC Windows et les kits d'exploit traditionnels destinés aux postes de travail ont connu une baisse en 2016, les vulnérabilités Zero Day des mobiles et les kits d'attaque ont gagné en importance. Les attaques passant par des réseaux WiFi douteux deviennent plus faciles que jamais à mettre en œuvre, et les principaux systèmes d'exploitation pour mobiles ont démontré leurs lacunes.

Le kit d'exploit DNSChanger a même réussi à attaquer indirectement les appareils mobiles en modifiant les enregistrements DNS des routeurs à domicile et en exposant tous les appareils connectés aux fenêtres contextuelles, malvertising et autres compromissions potentielles, quel que soit le système d'exploitation.

Nous voyons là encore que les vecteurs appareils mobiles/réseaux sociaux se combinent aux applis malveillantes qui se propagent via ces réseaux. Là encore, ces attaques coïncidaient généralement avec de grandes occasions ou manifestations. Les Jeux Olympiques ont par exemple engendré plus de 4 500 applis mobiles douteuses ou malveillantes associées à ce thème et aux marques des sponsors.

LE POINT SUR LA RECHERCHE 2016

Des découvertes Zero Day à l'examen des nouvelles macros qui propagent les malware, les chercheurs de Proofpoint ont surveillé un large éventail de menaces tout au long de l'année 2016. Vous trouverez ci-dessous les principaux posts publiés sur notre blog Threat Insight pour 2016, de même qu'une visite guidée des évolutions et innovations majeures qu'a connu le secteur de la cybersécurité en 2016.

MENACES PERSISTANTES AVANCÉES

Operation Transparent Tribe : Des menaces APT visant les intérêts diplomatiques et militaires indiens

Cambriolage de banques : les banques du Moyen-Orient et des États-Unis visées par de nouvelles attaques du groupe Carbanak

La menace APT NetTraveler cible les intérêts russes et européens

TROJANS BANCAIRES, CHEVAUX DE TROIE BANCAIRES ET VOLEURS

Après mise à jour, le cheval de Troie bancaire Blackmoon se concentre sur les clients des banques sud-coréennes

Dridex, JavaScript et Porta Johns

Les chevaux de Troie bancaires Vawtrak et UrlZone ciblent le Japon

Aux portes de la mort : le cheval de Troie Thanatos/Alphabot fait son apparition sur le marché

Panda Banker : Un nouveau cheval de Troie bancaire affecte le marché

Reprise de l'activité Dridex dans des attaques plus ciblées et de plus faible envergure

Cauchemar à Tor Street : la variante Ursnif Dreambot intègre des fonctionnalités Tor

Le cheval de Troie bancaire Kronos servait à propager de nouveaux malware POS

Août en novembre : De nouveaux voleurs d'informations entrent en scène

PIRATAGE DE LA MESSAGERIE EN ENTREPRISE (BEC)

Au-delà du phishing Vanilla : Les menaces associées aux e-mails frauduleux arrivent à maturité

Les cyber-escrocs exploitent la tentative de coup d'État en Turquie à travers des leurres BEC très opportuns

PROPAGATION ET TECHNIQUES

Au nez et à la barbe de tous : techniques d'obfuscation des attaques de phishing

« .om » n'est pas « .com » : les cybercriminels font une utilisation accrue du typosquattage

Phishing à grande échelle : un cybercriminel combine les e-mails personnalisés et l'éventail de malware pour cibler les dirigeants d'entreprise

Attention à JavaScript : explosion des campagnes avec pièces jointes .js

Les macros malveillantes intègrent des techniques d'esquive du sandbox pour propager le nouveau Dridex

Les cybercriminels utilisent de vrais comptes PayPal pour propager le cheval de Troie bancaire Chthonic

La campagne du cheval de Troie bancaire Ursnif passe au niveau supérieur grâce à de nouvelles techniques d'esquive du sandbox

L'art de chercher des problèmes : La plateforme de résolution des problèmes Windows utilisée pour propager des malware

Montée en flèche du malware de publicité frauduleuse Kovter via les astuces de macro

Veil-Framework infecte les victimes d'une attaque de phishing OWA ciblée

KITS D'EXPLOIT ET MALVERTISING

Le malvertising vidéo à l'origine de nouveaux risques pour les sites à grande visibilité

Kit d'exploit déjà vu : Des campagnes d'e-mails massives propagent Dridex via Angler

Le kit d'exploit Angler nourrit-il les poissons ? Le kit d'exploit Neutrino propage désormais la plupart des ransomware CryptXXX.

KITS D'EXPLOIT ET MALVERTISING (SUITE)

Reprise du botnet Necurs et, dans son sillage, d'une nouvelle version du ransomware Locky

Les campagnes massives du groupe de malvertising AdGholas exploitent la stéganographie et la mise en liste blanche des fichiers pour disparaître aux yeux de tous

CONTEXTE

Deux menaces pour le prix d'une : le phishing d'identifiants conduit à l'enregistreur de frappes iSpy

Tout est calme... trop calme : la coupure du botnet Necurs interrompt la propagation de Dridex et Locky

Le trafic des malware POS ZeusPOS et NewPOSThings quadruple pendant le « Black Friday »

Ostap Bender : 400 façons d'obliger la population à mettre la main à la poche

MOBILE

DroidJack exploite le sideloading... et se révèle super efficace ! Détection d'une porte dérobée dans l'appli Android Pokemon GO

RANSOMWARE

Les auteurs de Dridex se tournent vers le ransomware avec « Locky »

Nouveau ransomware : vos données nous appartiennent

CryptXXX : nouveau ransomware des auteurs de Reveton, propagé via Angler

L'explosion des ransomware se poursuit : détection de CryptFile2, BrLock et MM Locker

Les auteurs du ransomware Locky se tournent vers XORed JavaScript pour échapper aux systèmes de défense classiques

Le ransomware de verrouillage de poste de travail Ransoc pille les fichiers locaux et les profils de réseau social

RÉSEAUX SOCIAUX

Les fans et les sponsors des Jeux Olympiques de Rio 2016 visés par les applis malveillantes et les escroqueries par réseau social

Les faux comptes de réseau social poursuivent le phishing d'identifiants bancaires

Les menaces liées à l'appli mobile Pokémon GO passent aussi par les réseaux sociaux

Pas de vérification miracle : les escroqueries de phishing par vérification des comptes de réseau social volent les identifiants et les numéros de carte bancaire

SPAM

Du courrier indésirable désormais parallèle au ransomware CryptXXX !

Spam et phishing liés aux élections à l'approche du mois de novembre

Le spam lié aux élections devient bipartisan

VULNÉRABILITÉS ZERO DAY ET AUTRES

Étouffer une attaque Zero Day dans l'œuf : Adobe CVE-2016-1019

Les correctifs Microsoft CVE-2016-3351 Zero Day exploités par les groupes de malvertising AdGholas et GooNky

Des jumeaux : Correctifs Microsoft pour la référence CVE-2016-3298, seconde vulnérabilité de divulgation d'informations Zero Day, utilisée dans les campagnes publicitaires malveillantes et dans le kit d'exploit Neutrino

Microsoft Word Intruder 8 : Nouvelle prise en charge de la vulnérabilité CVE-2016-4117 dans Flash

Les appareils Windows et Android sont ciblés par des logiciels publicitaires malveillants via les routeurs domestiques

RECOMMANDATIONS DE PROOFPOINT

Ce rapport révèle d'importantes informations sur l'évolution du paysage des risques qui menacent votre stratégie de cybersécurité. Voici les principales recommandations à suivre pour protéger votre société et votre marque en 2017.

Partez du principe que vos utilisateurs se laisseront piéger. L'exploitation de l'ingénierie sociale en tant que déclencheur d'attaques par e-mails se répand, et les techniques des criminels évoluent rapidement. Optez pour une solution à la fois capable d'identifier et de mettre en quarantaine les e-mails entrants qui menacent vos employés et les menaces sortantes qui ciblent vos consommateurs avant même qu'elles n'atteignent leur boîte aux lettres.

Élaborez un solide système de défense contre les attaques BEC. Extrêmement ciblées et de faible envergure, les escroqueries par piratage de la messagerie en entreprise (BEC) ne présentent généralement aucune charge utile et sont de ce fait plus difficiles à déceler. Investissez dans une solution dotée de fonctions de classification dynamique simplifiant la mise en œuvre de politiques de mise en quarantaine et de blocage.

Protégez votre réputation et vos clients. Lutte contre les attaques qui ciblent vos clients sur les réseaux sociaux et dans le courrier électronique et les appareils mobiles, et notamment contre les comptes frauduleux qui détournent l'image de votre marque. Recherchez une solide solution de sécurité pour les réseaux sociaux, capable d'analyser l'ensemble des réseaux et de signaler toute activité frauduleuse.

Verrouillez les environnements d'applications mobiles. Les environnements mobiles multiplient les risques que des applis non autorisées dérobent des données sensibles pour votre entreprise. Investissez dans une solution orientée données et capable de collaborer avec votre propre système de gestion des appareils mobiles (MDM, Mobile Device Management) pour analyser le comportement des applis au sein de votre environnement, et notamment d'identifier les données auxquelles elles ont accès.

Choisissez un fournisseur de renseignements sur les menaces comme partenaire. Les attaques de faible ampleur mais plus ciblées exigent de précieux renseignements sur les menaces. Optez pour une solution combinant les techniques statiques et dynamiques, capable de détecter toutes les nouveautés (outils, tactiques et cibles), puis d'en tirer les enseignements nécessaires.

À PROPOS DE PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT), leader spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger leurs données contre les menaces avancées, et de se conformer aux réglementations en vigueur. Grâce à Proofpoint, les professionnels de la sécurité sont en mesure d'accéder à des renseignements et outils capables de protéger les utilisateurs et leurs données contre les attaques menées par courrier électronique, sur les réseaux sociaux ou via des appareils mobiles. De nombreuses entreprises, dont plus de la moitié de celles figurant dans le classement Fortune 100, exploitent des solutions Proofpoint. Celles-ci sont conçues spécialement pour les environnements mobiles et de réseaux sociaux, et tirent parti de la technologie cloud et d'une plateforme d'analyse du Big Data pour lutter contre les menaces avancées modernes.