proofpoint

RAPPORT

EMAIL FRAUD THREAT REPORT

BILAN DE L'ANNÉE

RAPPORT SUR LA FRAUDE À LA MESSAGERIE

proofpoint.com

La fraude à la messagerie, également appelée Piratage de la messagerie en entreprise (BEC), est aujourd'hui l'une des plus grandes cyber-menaces. Ces attaques d'ingénierie sociale cherchent davantage à exploiter la nature humaine que la technologie. Très ciblées et envoyées en faible nombre, elles usurpent l'identité de personnes en position d'autorité.

La fraude à la messagerie exploite entre autres les faiblesses de la nature humaine, la peur et le désir de plaire pour soutirer de l'argent ou de précieuses informations aux employés, clients et partenaires commerciaux.

Proofpoint a analysé plus de 160 milliards de courriers électroniques adressés à plus de 2 400 sociétés réparties dans 150 pays.

Voici nos conclusions pour l'année 2017.

FRAUDE À LA MESSAGERIE
Lors d'une attaque par fraude à la messagerie, un e-mail (ou une série d'e-mails), supposé provenir d'un cadre dirigeant ou d'une société partenaire, demande au destinataire d'effectuer un virement financier ou de transmettre des informations sensibles. N'utilisant ni pièce jointe ni URL, ces attaques sont difficiles à détecter et à intercepter.

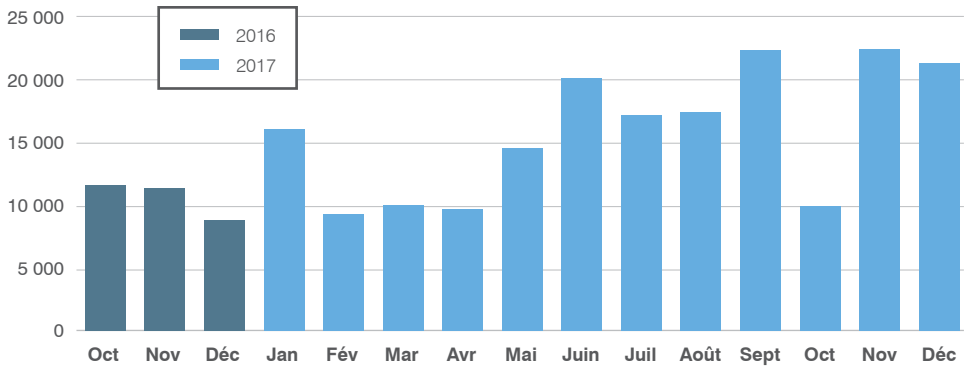
FRAUDE À LA MESSAGERIE : UNE CROISSANCE CONTINUE

LA FRAUDE À LA MESSAGERIE a été omniprésente en 2017. Bien que la menace reste très ciblée, les attaques ont visé davantage d'organisations et plus fréquemment qu'en 2016.

Le pourcentage d'entreprises visées par une telle attaque au moins est en progression constante et a atteint un nouveau sommet au 4e trimestre (88,8 %), soit une hausse de 13,8 pourcent par rapport au même trimestre l'an dernier (75 % des organisations).

En moyenne, 18,5 e-mails frauduleux ont ciblé les entreprises chaque trimestre, une augmentation de 17 % par rapport à l'année précédente. En termes de volume, l'année s'est terminée sur deux des trois trimestres records jamais enregistrés à ce jour pour la fraude à la messagerie.

Attaques par piratage de la messagerie en entreprise (BEC) détectées et bloquées par Proofpoint
Les 3e et 4e trimestres ont connu deux des trois chiffres records jamais enregistrés à ce jour pour le nombre de fraudes à la messagerie.



LES FRAUDEURS NE SE LIMITENT PLUS AU SOMMET DE L'ORGANIGRAMME !

Les cybercriminels abandonnent les escroqueries au PDG/Directeur financier à mesure qu'ils étendent leur rayon d'action dans les organisations.

Multiplication des usurpations d'identité

Après être resté stable tout au long des trois premiers trimestres de l'année, le nombre moyen d'identités usurpées par organisation a plus que doublé au 4e trimestre (10 identités environ).

Cette évolution est logique. En effet, à mesure que les équipes en charge de la sécurité redoublent d'efforts pour sensibiliser les employés aux risques d'usurpation de l'identité du PDG, les « méchants » se tournent vers d'autres figures d'autorité à usurper. Dans près de la moitié des organisations (47 %), plus de cinq identités ont été usurpées au 4e trimestre, presque le double par rapport au trimestre précédent.

Éventail plus large de rôles ciblés

Au sein d'une organisation donnée, le nombre moyen d'individus ciblés se stabilise au 4e trimestre (13 environ). Cependant, les cybercriminels ne se limitent plus au sommet de l'organigramme ni à certains groupes dans l'entreprise tels que le département des ressources humaines et le service comptable. Dans la plupart des cas, l'ingénierie sociale et les informations publiquement disponibles sur les employés sur Internet et les réseaux sociaux leur permettent de rédiger un e-mail très convaincant.

À mesure que les cybercriminels sont descendus dans l'organigramme au 4e trimestre, 41 % des entreprises visées ont fait face à des attaques usurpant plus que cinq identités et visant plus de cinq employés.

ATTAQUES UN À UN

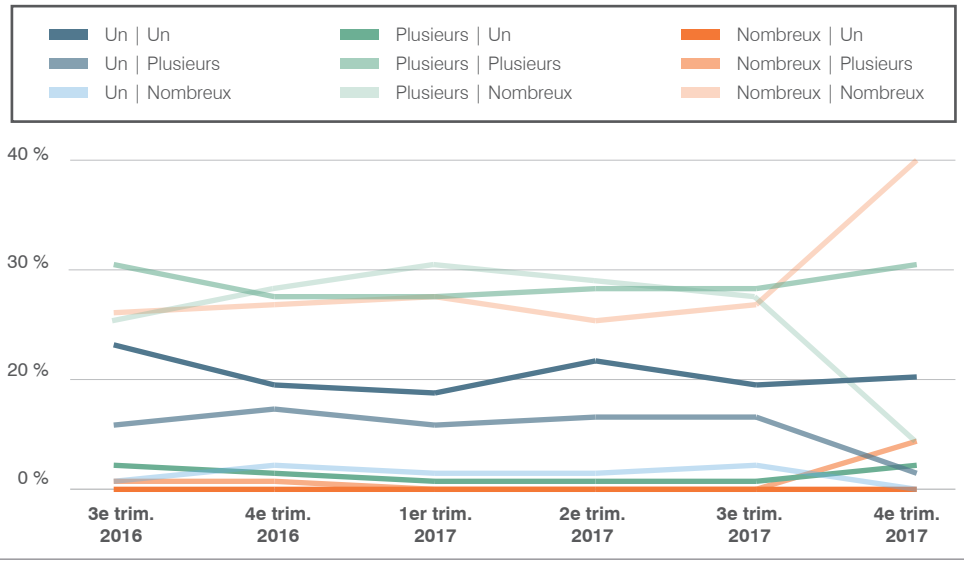
Dans le cas de la fraude à la messagerie dite « un à un », un cybercriminel usurpe une seule identité (généralement celle du PDG) et cible un seul destinataire (en général, le directeur financier).

ATTAQUES DE NOMBREUX À NOMBREUX

Lors des attaques dites de « nombreux à nombreux », les fraudeurs usurpent diverses identités de cadre dirigeant et visent plusieurs destinataires. Le cybercriminel peut par exemple essayer de se faire passer pour différents responsables et cibler toute l'équipe du service financier de l'entreprise.

Comparaison entre les usurpations d'identité et les e-mails envoyés

Les fraudeurs délaissent peu à peu les attaques simples de type **un à un**, se tournent vers l'usurpation d'identités d'acteurs plus influents et visent davantage de personnes au sein de l'organisation. Ces attaques sont dites de **nombreux à nombreux**.



POUR LE CYBERCRIMINEL, LA TAILLE N'A PAS D'IMPORTANCE !

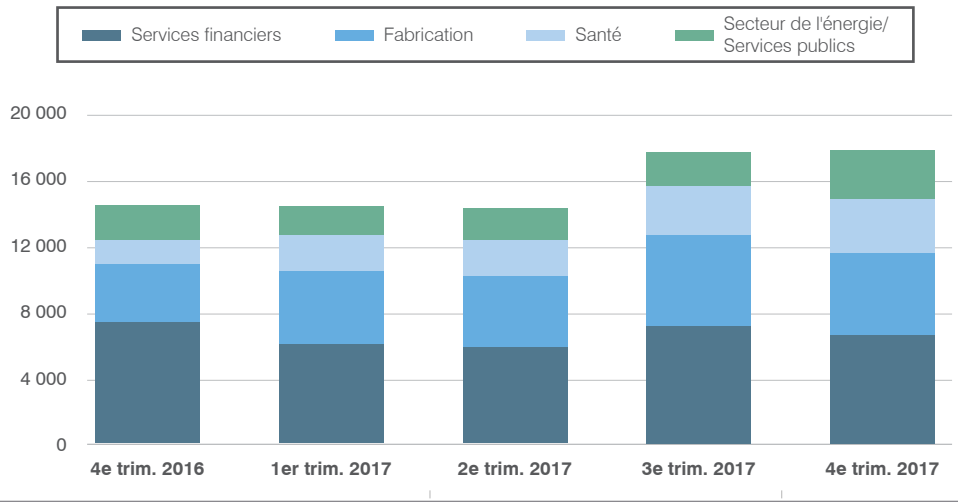
Les fraudeurs visent toutes les organisations, quelle que soit leur taille. Ils sont également opportunistes et ciblent tous les secteurs.

Les attaques ciblent les sociétés de toutes tailles

Depuis le tout début de notre suivi de ces données en 2016, nous n'avons encore pu établir aucun lien ou presque entre la taille de la société et la fréquence des attaques par fraude à la messagerie. Seul le 2e trimestre 2017 montre une certaine corrélation : les cybercriminels ayant laissé apparaître une légère préférence pour les cibles de taille plus importante.

Les cybercriminels ciblent de nombreux secteurs

Les secteurs des services financiers et de la fabrication sont les plus souvent visés, mais la fraude à la messagerie se répand dans tous les secteurs d'activité.



Que les attaques visent uniformément les petites et les grandes entreprises peut sembler surprenant. Du point de vue du cybercriminel toutefois, cela paraît logique. Les grandes entreprises peuvent sembler plus fortunées, mais les entités plus petites sont souvent plus vulnérables à ces attaques avancées.

Les cybercriminels ciblent de nombreux secteurs

Nos recherches antérieures révélaient une répartition presque uniforme des tentatives de fraude à la messagerie dans tous les secteurs. (Bien que les secteurs des services financiers, de la fabrication, de la santé et de l'énergie et des services publics aient été visés légèrement plus fréquemment.)

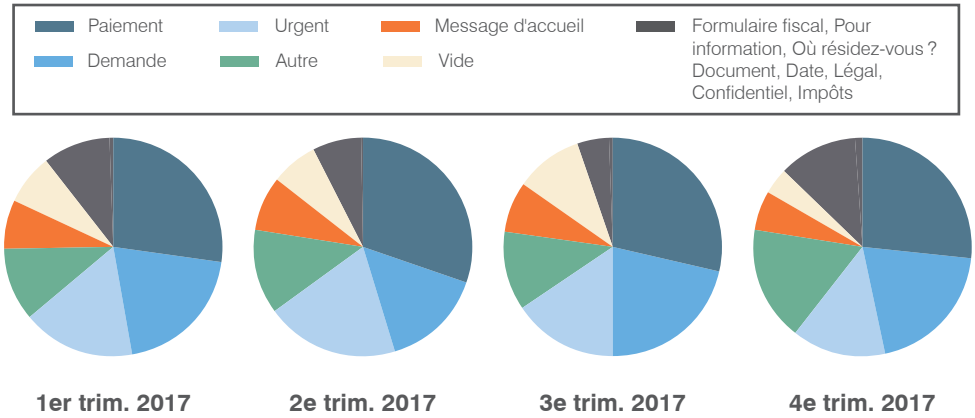
Au 4e trimestre, les cybercriminels ont ciblé de nouveaux secteurs. Le domaine de l'immobilier est pour eux un nouveau moyen de monétiser les transactions d'une valeur élevée. De même, le secteur de l'enseignement connaît une hausse de 77 % des attaques par rapport au trimestre précédent et de 120 % par rapport à la même période l'an dernier.

FRAUDE À LA MESSAGERIE : CHANGEMENT DE TACTIQUE

Pour échapper à la surveillance des outils traditionnels et atteindre leurs victimes, les fraudeurs font sans cesse évoluer leurs techniques.

Lignes d'objet employées dans les tentatives de fraude à la messagerie

Les lignes d'objet « Paiement », « Demande » et « Urgent » restent les plus courantes, mais les objets associés au contexte juridique ont connu un pic au 4e trimestre.



Fraude au virement

LA FRAUDE PAR VIREMENT BANCAIRE reste la forme la plus fréquente pour la messagerie (près de 27 % du volume des e-mails frauduleux). Les différentes catégories d'objet des e-mails reprennent généralement des variantes du mot « paiement ».

Arnaques aux impôts

LE NOMBRE D'ESCROQUERIES VIA LES FORMULAIRES FISCAUX augmente chaque année depuis deux ans aux premiers trimestres, probablement du fait de l'approche du délai de présentation des déclarations de revenus aux États-Unis et en Europe. Une hausse de 3,408 % est par exemple constatée au 1er trimestre par rapport au précédent. Au 2e trimestre, après expiration de ce délai de déclaration, le volume d'attaques diminue puis se stabilise.

Changement d'identités ou de lignes d'objet

Pour se faire passer pour une autorité officielle, les cybercriminels endossent l'identité d'un large éventail d'identités. Tout au long de l'année 2017, les attaques par fraude à la messagerie ont permuté les catégories d'objet reprenant les termes « urgent » et « demande ».

« Urgent » et « Demande »

Les messages associés à la catégorie « Urgent » sont généralement plus directs et concis. Ceux dont la ligne d'objet utilise le terme « Demande » adoptent généralement une approche plus progressive. Ils établissent un certain nombre d'échanges avant de demander les précieuses informations recherchées.

« Légal »

Deux autres catégories d'objet sont montées en flèche au 4e trimestre : celles qui reprenaient une date et celles qui reprenaient le terme « Légal ».

Bien qu'encore faible en termes absolus, le volume d'attaques adoptant l'angle « légal » augmente de 1,850 % par rapport à l'année précédente. Parmi ces attaques, la plus répandue utilisait la ligne d'objet « Appel de l'avocat ».

FRAUDE PAR VIREMENT BANCAIRE

Dans le cas de la fraude par virement bancaire, le cybercriminel envoie un e-mail dans lequel il se fait passer pour un cadre supérieur. L'objet de cet e-mail est de leurrer le destinataire afin de l'inciter à effectuer un virement bancaire qu'il fait passer pour une opération commerciale habituelle ou pour une affaire essentielle exigeant discrétion.

ESCROQUERIES AU FORMULAIRE FISCAL

Dans le cas de cette arnaque, quelqu'un se fait passer pour un cadre dirigeant et demande au service financier de lui transmettre les dossiers des employés. Ces dossiers servent ensuite à voler des identités pour d'autres attaques. Le nom de cette arnaque découle du formulaire fiscal W2 utilisé par les employeurs américains pour déclarer les salaires de leurs employés.

Lors de ces attaques, le fraudeur tente généralement de passer des e-mails au transfert bancaire par téléphone. Ce type d'attaque fonctionne, car le cybercriminel se fait passer pour une personne influente, mais avec laquelle la victime n'est généralement pas en relation. De plus, comme le contact se fait en majorité hors ligne, les équipes en charge de la sécurité ont du mal à la détecter et l'intercepter.

Faux historiques d'e-mails

Les tentatives de fraude reprenant de faux historiques d'e-maile augmentent d'un trimestre à l'autre tout au long de 2017.

Cette technique reprend les termes « Re: » ou « Tr: » dans la ligne d'objet, un faux historique d'e-mails, voire les deux. Plutôt réaliste, l'historique des échanges inséré dans la fausse chaîne d'e-mails laisse entendre que la demande a déjà été approuvée par les intervenants autorisés.

Au 4e trimestre, plus de 11 % de toutes les attaques par e-mail reprenaient une version de cette technique, contre 7,3 % au même trimestre l'année dernière.

DES TECHNIQUES DOMINÉES PAR L'USURPATION DU NOM DE DOMAINE/D'AFFICHAGE

Tout au long de l'année 2017, les messages frauduleux ont combiné les usurpations de noms de domaine, de noms d'affichage, et les attaques par sosie de nom de domaine (domaine cousin).

Usurpation du nom de domaine

L'USURPATION DU NOM DE DOMAINE, attaque au cours de laquelle des criminels détournent les domaines de messagerie de confiance de l'organisation, représente encore une grande part de la fraude à la messagerie. Au 4e trimestre, 69 % des organisations visées par la fraude à la messagerie ont subi une attaque par usurpation de nom de domaine au moins. Sur l'année 2017, près de 93 % d'entre elles ont subi une telle attaque.

Usurpation du nom d'affichage

L'USURPATION DU NOM D'AFFICHAGE au travers des services de messagerie de type Web représente près de 40 % des attaques de fraude à la messagerie au 4e trimestre. Les domaines aol.com et gmail.com se sont révélés les domaines d'expédition privilégiés par ces menaces, même si les cybercriminels en utilisent bien d'autres.

Adoption de la norme DMARC

Pour éviter les attaques par fraude à la messagerie, il est possible d'implémenter la norme d'authentification des e-mails **DMARC**. La multiplication des projets d'adoption de la norme DMARC en 2017 n'a donc rien de surprenant.

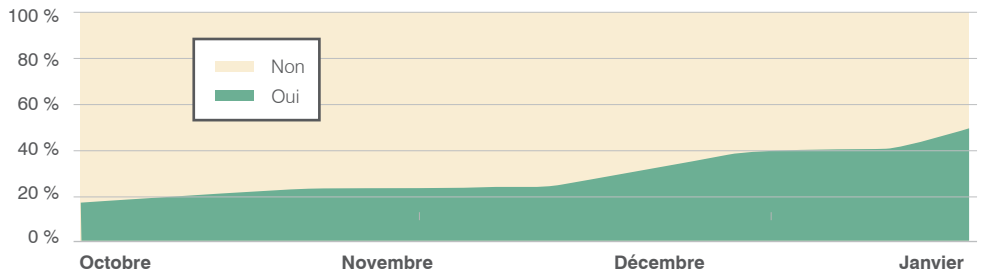
Au mois d'octobre, le Ministère américain de la sécurité intérieure a publié la Directive opérationnelle exécutoire 18-01. Cette directive vise à mieux protéger les destinataires des e-mails envoyés par les organismes fédéraux et ceux qui consultent un site Web fédéral. L'un des éléments essentiels de cette directive prévoit que tous les organismes civils fédéraux déploient rapidement la norme DMARC.

Lorsque cette directive a été annoncée, près d'un e-mail sur huit envoyés à partir du domaine .gov était frauduleux. Seuls 17 % des organismes environ avaient alors adopté la norme DMARC.

90 jours environ après le démarrage du projet, ce pourcentage avait plus que triplé. Près de 52 % des organismes ont respecté la première échéance DMARC.

Déploiement de la norme DMARC dans les administrations

Suite à la directive fédérale, davantage d'agences gouvernementales déploient l'authentification des e-mails. Près de la moitié n'a toutefois pas encore terminé la première étape.



USURPATION DE NOM DE DOMAINE

L'usurpation consiste à se faire passer pour un collègue ou un contact de confiance en faisant en sorte que l'e-mail semble provenir de l'adresse attendue et légitime.

USURPATION DU NOM D'AFFICHAGE

L'usurpation du nom d'affichage consiste à placer une adresse électronique et un nom familiers dans le champ de l'expéditeur (DE :) que voit l'utilisateur. Lorsque le destinataire répond, son message est alors envoyé à l'adresse indiquée dans l'en-tête « Répondre à : » de l'e-mail.

DMARC

La norme DMARC, qui vient de l'anglais « Domain-based Message Authentication, Reporting and Conformance », est un protocole d'authentification des e-mails capable d'éviter la plupart des attaques par fraude à la messagerie.

Peu de temps après l'annonce de la directive, le NH-ISAC (National Health Information Sharing and Analysis Center), groupe industriel qui soutient le partage d'informations entre les fournisseurs de services médicaux, a demandé à ses membres de s'engager à déployer la norme DMARC en 2018.

LES SOSIES DE DOMAINE AU MICROSCOPE

USURPATION PAR SOSIE DE NOM DE DOMAINE
Lors d'une usurpation par sosie de nom de domaine, les cybercriminels procèdent à l'enregistrement de domaines trompeusement similaires à ceux d'enseignes renommées.

L'USURPATION PAR SOSIE DE NOM DE DOMAINE, qui consiste pour le cybercriminel à enregistrer un nom de domaine confusément similaire à celui d'un domaine fiable, est une autre tactique efficace. Les cybercriminels incitent alors certaines personnes à divulguer de précieuses informations par le biais d'e-mails dont l'expéditeur semble familier.

Pour façonner ces domaines trompeurs, les cybercriminels modifient légèrement l'orthographe du nom de domaine authentique. Ils peuvent échanger certains caractères, par exemple remplacer la lettre O par le chiffre 0. Ils peuvent insérer des caractères, par exemple, ajouter un S à la fin du nom de domaine.

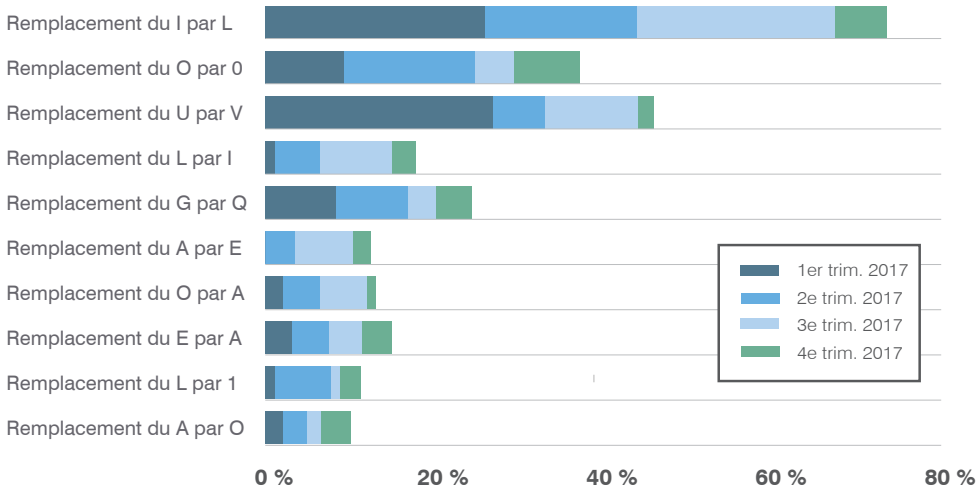
Le volume d'attaques par sosie de nom de domaine n'est pas aussi important que celui associé à l'usurpation des noms d'affichage et de domaine. Cela découle probablement du fait que la technique implique que le cybercriminel procède à l'enregistrement d'un nom de domaine et que cette opération a un coût. Cependant, comme le nombre de variantes orthographiques d'un unique nom de domaine fiable est sans limite, les cybercriminels disposent de très nombreuses possibilités.

Échanges de caractères

Comme les autres tactiques de fraude à la messagerie, les techniques de sosie de nom de domaine changent tous les trimestres. Pour l'année 2017 dans son ensemble, l'échange de caractères individuels a été le plus répandu, avec une fréquence atteignant près de 38 %. Les échanges les plus courants ont été les suivants :

- Remplacement du I par un L (17,4 %)
- Remplacement de la lettre O par le chiffre 0 (8,7 %)
- Remplacement du U par un V (8 %)

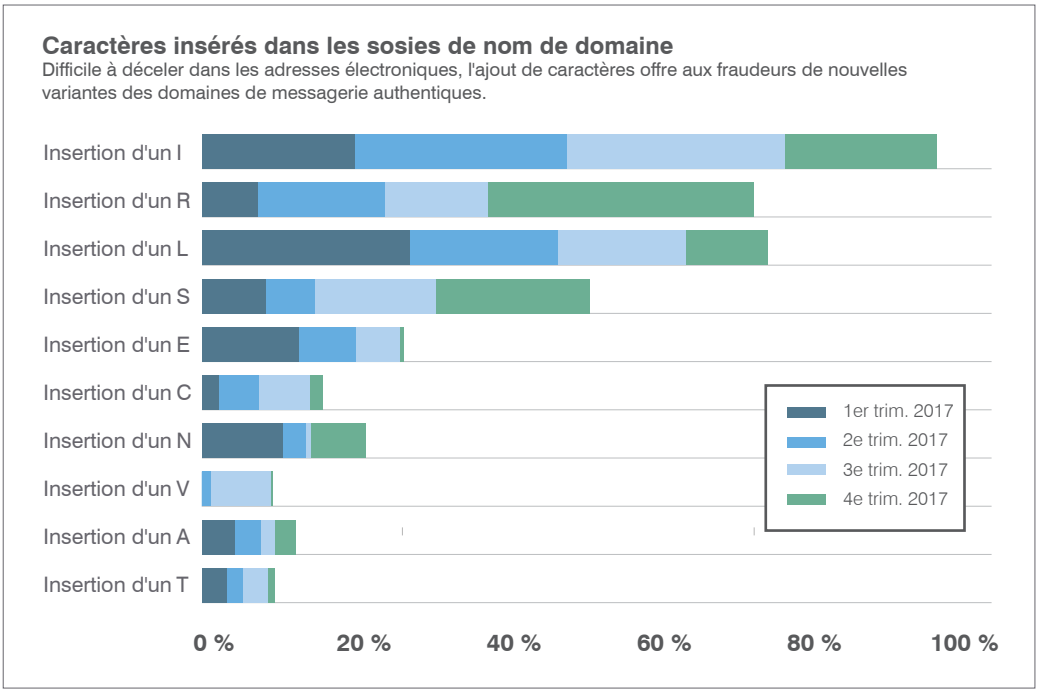
Remplacement de caractères dans les sosies de nom de domaine
Comme certains caractères se ressemblent, les fraudeurs n'ont que l'embarras du choix pour créer des domaines ressemblant aux vôtres.



Insertion de caractères

Les noms de domaine trompeurs, dans lesquels un caractère supplémentaire est inséré, atteignent près de 34 % sur l'année. Les insertions les plus courantes ont été les suivantes :

- Lettre I (23,7 %)
- Lettre R (19,3 %)
- Lettre L (15,4 %)



Autres techniques

Une autre technique répandue consiste à ajouter ou supprimer un caractère de début ou de fin dans le nom de domaine. Cette approche représente près de 13 % des sosies de nom de domaine enregistrés.

Les autres tactiques d'usurpation par sosie de nom de domaine comprennent :

- Insertion d'un trait d'union
- Suppression de caractères
- Typographie et **HOMOGRAPHIE**

USURPATION PAR HOMOGRAPHIE

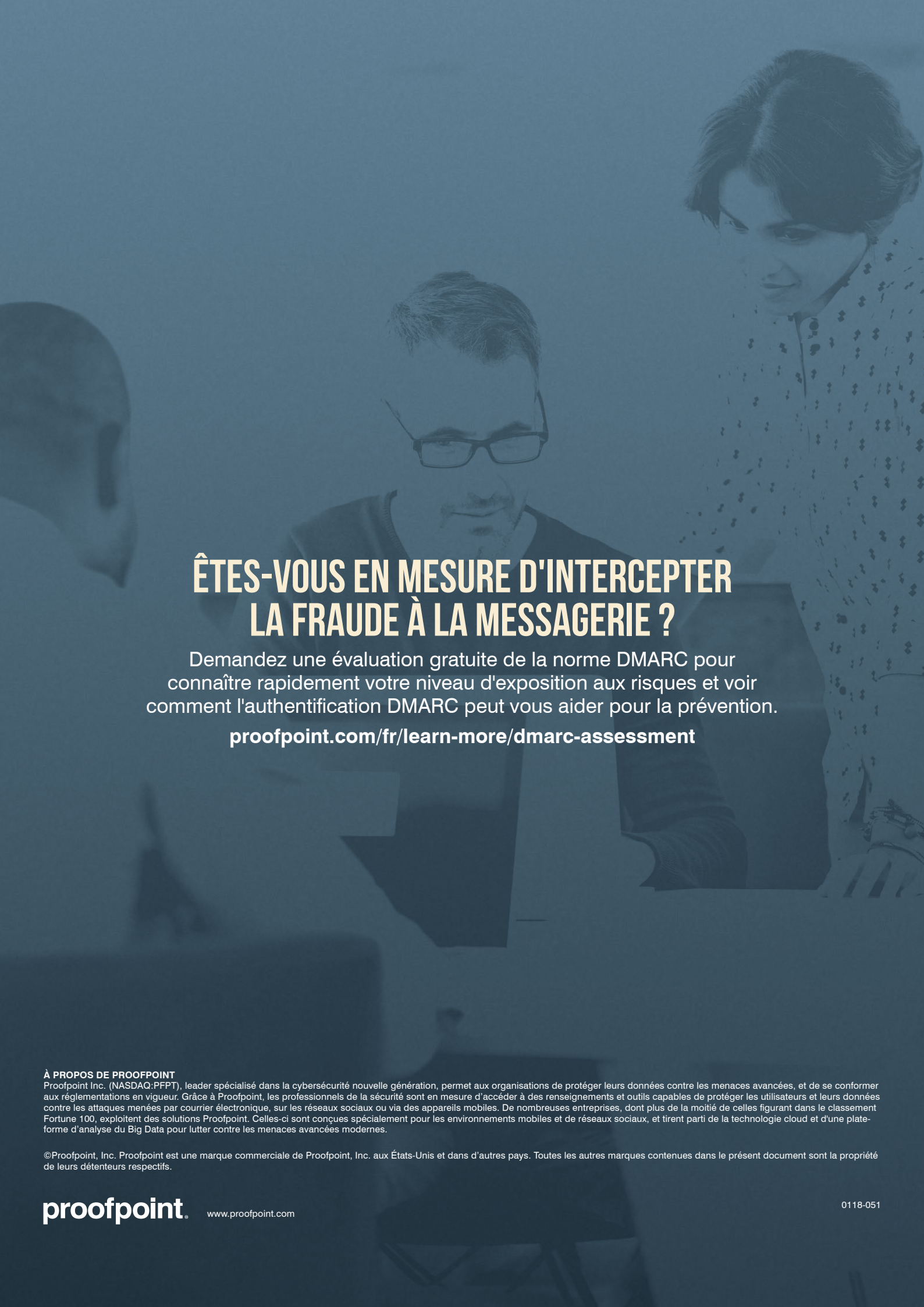
L'usurpation par homographie consiste à combiner des jeux de caractères de différentes langues afin de créer un sosie de nom de domaine que l'utilisateur ne distingue pas du véritable, contrairement à l'ordinateur. Par exemple, un domaine risqué utilisant le caractère A cyrillique et un domaine authentique utilisant le caractère A latin sembleront identiques.

CONCLUSION ET RECOMMANDATIONS

En dépit des investissements substantiels déjà réalisés par les organisations en matière de sécurité, la fraude à la messagerie est en hausse. Les cybercriminels se perfectionnent sans cesse. Ils parviennent à échapper aux solutions de sécurité classiques, laissant les employés comme dernière ligne de défense.

Les tactiques de fraude à la messagerie ne cessent d'évoluer. Voilà pourquoi il vous faut une protection à plusieurs couches, qui comprenne les capacités suivantes :

1. **Authentification des e-mails via la norme DMARC** : bloquez toutes les attaques usurpant des domaines de messagerie de confiance.
2. **Classification dynamique** : analysez le contenu et le contexte de chaque e-mail afin d'intercepter toute tactique d'usurpation du nom d'affichage et de domaine cousin au niveau de la passerelle de messagerie.
3. **Détection des sosies de nom de domaine :** identifiez et désignez comme potentiellement suspects les domaines enregistrés par des tiers.
4. **Prévention des pertes de données :** assurez-vous d'empêcher toute fuite d'informations sensibles (formulaires fiscaux, par exemple) à partir de votre environnement.



ÊTES-VOUS EN MESURE D'INTERCEPTER LA FRAUDE À LA MESSAGERIE ?

Demandez une évaluation gratuite de la norme DMARC pour connaître rapidement votre niveau d'exposition aux risques et voir comment l'authentification DMARC peut vous aider pour la prévention.

proofpoint.com/fr/learn-more/dmarc-assessment

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 plate-forme d'analyse du Big Data pour lutter contre les menaces avancées modernes.

proofpoint. www.proofpoint.com