

Un livre blanc des  
**TrendLabs**

# À L'AFFÛT DES EMAILS MALVEILLANTS

COMMENT DÉJOUER L'ENSEMBLE DES MENACES LIÉES A L'EMAIL?



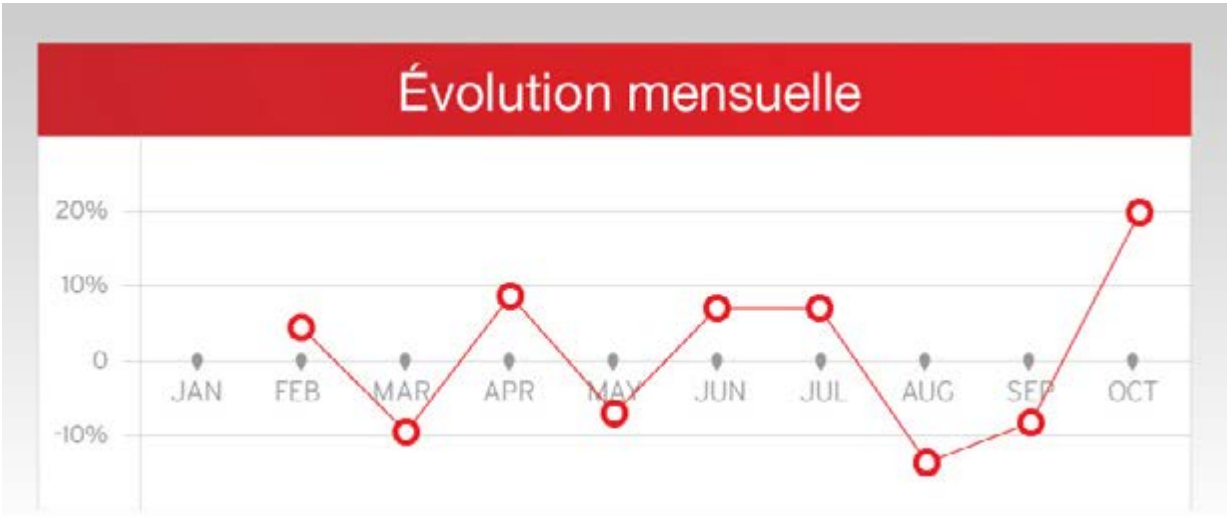
# Des emails malveillants au coeur de l'entreprise

Les cybercriminels capitalisent sur l'email pour s'immiscer dans des réseaux d'entreprise. En effet, l'omniprésence de l'email dans le milieu professionnel, en fait une passerelle idéale pour les attaques.

Trend Micro a mené l'enquête en 2012, et révèle que le nombre d'emails malveillants reçus par les entreprises ne semble guère fléchir.<sup>1</sup> Nos sources indiquent que les entreprises reçoivent plus de 20 milliards d'emails malveillants par trimestre. En outre, environ 450 milliards de liens malveillants ont été bloqués sur la période étudiée (de janvier à octobre 2012). L'évolution mensuelle (voir schéma 1) montre que le nombre d'emails malveillants fluctue, avec un taux de variation de -13% à 20%.

Les entreprises reçoivent plus de 20 milliards d'emails malveillants par trimestre.

Schéma 1 : Évolution mensuelle du nombre d'emails malveillants reçus par les entreprises



1 Étude interne réalisée à partir de Trend Micro™ Smart Protection Network™, de janvier à octobre 2012.

# Des attaques initiées par des liens inclus dans les emails

Les emails constituent des portes d'entrée pour les logiciels malveillants (malware) qui sévissent sous deux formes : pièces jointes et liens URL. Les attaques réussies peuvent résulter d'un téléchargement de malware ou d'un phishing, et induire une perte de données, des risques en matière de conformité ou des dommages financiers.

Schéma 2 : Exemple d'email imitant ceux de LinkedIn



## Les attaques menées via le Blackhole Exploit Kit

- Cet outil de piratage revisite la notion de phishing.<sup>2</sup> Le phishing traditionnel invite les utilisateurs à saisir leurs informations personnelles. Désormais, ces derniers sont simplement invités à ouvrir un email et à cliquer sur le lien qui y est affiché.
- Les cybercriminels imitent des emails officiels provenant de sites tels que LinkedIn, Citibank, AT&T ou Verizon, et remplacent les liens d'origine par des liens malveillants.<sup>3</sup> Les emails paraissent donc sérieux et inoffensifs, bien que les liens soient, en réalité, malveillants.
- Ce kit de piratage a la particularité de modifier constamment les liens inclus dans les emails envoyés aux victimes, pour éviter de se faire repérer par les outils antispam ou de filtrage d'URL.<sup>4</sup>
- Au-delà de l'analyse de la vulnérabilité des logiciels installés sur un poste client, ce kit détecte le navigateur utilisé, la version de système d'exploitation, ainsi que la localisation de l'utilisateur.<sup>5</sup>

## Des attaques ciblées

- Les emails liés aux attaques ciblées parviennent souvent avec un document PDF, Microsoft Word, Excel ou PowerPoint en tant que pièce jointe, bien que cela ne soit pas toujours le cas.
- L'étude de Trend Micro révèle que 91% des attaques ciblées se basent sur des emails de spear phishing. Les attaques de spear phishing, dans leur majorité, tentent d'identifier des vulnérabilités logicielles, mais de faux liens ont été identifiés dans 6% des échantillons d'emails étudiés.<sup>6</sup>
- Ces attaques ciblent souvent des organisations non gouvernementales et commerciales, qui disposent de collaborateurs distants ou itinérants.

2 <http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-exploit-kit-transforms-phishing/>  
3 <http://blog.trendmicro.com/trendlabs-security-intelligence/same-operation-diversification-of-targets-being-spoofed-current-black-hole-exploit-kit-spam-runs/>  
4 <http://blog.trendmicro.com/trendlabs-security-intelligence/protecting-customers-from-black-hole-exploit-kit-spam-runs/>  
5 [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_blackhole-exploit-kit.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf)  
6 <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf>

**Les principaux avantages du BYOD selon les dirigeants d'entreprise :**

- Davantage de mobilité (43,1%)
- Évite d'avoir à transporter ou gérer de multiples équipements (13,6%)
- Perception que le BYOD constitue un avantage pour le collaborateur (10,5%)

*SOURCE:  
Mobile Consumerization Trends & Perceptions: IT Executive  
and CEO Survey, 2012*

Les équipes de sécurité informatique tentent de prévenir les menaces qui prolifèrent par email, et notamment au sein des organisations qui se sont mises à la page du BYOD (utilisation d'équipements personnels par les collaborateurs) ou dont les collaborateurs travaillent à distance. Le lieu de travail s'étend désormais au-delà du traditionnel bureau, et l'utilisation de l'email est plus que jamais une nécessité dans ce contexte de télétravail. Selon une étude de Decisive Analytics LLC commanditée par Trend Micro, seul un petit nombre d'entreprises ayant déploré une violation de données, ont mis un terme à leur programme de BYOD.<sup>7</sup> Les entreprises considèrent en effet que les avantages du BYOD l'emportent sur les risques. Reste à en connaître exactement les risques, et les pratiques qui y sont associées.

**Utilisation d'un équipement mobile**

- Consulter les emails professionnels en dehors du réseau d'entreprise, ces emails n'étant pas forcément analysés par la passerelle de sécurité email
- Lire ses emails professionnels avec un équipement mobile dont le logiciel de sécurité est obsolète ou utiliser un équipement qui ne peut procéder à la mise à jour de sécurité que s'il est connecté au réseau d'entreprise
- Envoyer des liens au lieu de pièces jointes par email qui peuvent, elles, être analysées par un antivirus

**Le BYOD**

- Autoriser l'utilisation d'équipements personnels, mobiles ou portatifs. La sécurité est moindre car gérée par l'utilisateur et non par l'infrastructure de sécurité de l'entreprise

**Utiliser des méthodes traditionnelles d'antispam**

- Services de solutions de sécurité sommaires qui ne bloquent que les emails non sollicités ou n'analysent que les pièces jointes. Le réseau d'entreprise reste vulnérable aux autres types de menaces
- Absence d'analyse des malwares à partir de liens contenus dans les messages. Le réseau n'est que partiellement protégé

**Les entreprises ont besoin d'outils de sécurité dotés d'une fonction de protection email efficace, capable de détecter à la fois les pièces jointes suspectes et les liens malveillants.**

# Sécuriser les emails dans un contexte de mobilité et d'attaques ciblées

Face au phénomène du BYOD et à la multiplication des plateformes mobiles, des systèmes d'exploitation et des équipements nomades, les entreprises doivent adopter une stratégie multicouche et proactive pour protéger leurs informations propriétaires et confidentielles, ainsi que leurs applications critiques.

**Adopter une sécurité multicouche**

Chaque outil de sécurité a une fonction distincte dans la protection de l'infrastructure d'une entreprise. Une stratégie de défense intégrant des technologies telles que la réputation des sites, l'authentification des emails et la réputation IP, est sans doute le moyen le plus efficace de protéger l'entreprise contre les nouvelles menaces polymorphes. Lorsqu'une solution de sécurité exhaustive est déployée, il est important d'identifier les types d'utilisateurs présents dans l'entreprise, les collaborateurs ayant chacun des contraintes et besoins différents.

**Utiliser une solution de sécurité optimale pour le serveur de messagerie**

Face au développement rapide des nouvelles menaces, une technologie de réputation associée à une gestion intelligente des menaces protège mieux les ressources d'entreprise. Les solutions de sécurité qui n'analysent que les pièces jointes et qui négligent les liens présents dans un email, ne sont pas suffisantes, car ce sont ces deux vecteurs potentiels d'infection qui doivent être surveillés. Les attaques sophistiquées peuvent utiliser des milliers d'URL internet différentes lors d'une seule campagne. Les antispams traditionnels, qui ne sont mis à jour que périodiquement, ne sont pas efficaces.

**Intégrer la sécurité email aux lignes de défense des entreprises**

Les entreprises doivent se rendre compte que les cybercriminels utilisent les emails pour perpétrer leurs attaques de manière efficace. Il est difficile de faire la différence entre des documents associés à des attaques ciblées et des documents légitimes. Une solution capable de déceler des attaques connues et de type "zero-day" dans des fichiers joints Adobe PDF, Microsoft® Office®, etc., renforce la protection. Le nombre d'emails contenant des liens qui redirigent vers des sites malveillants est également en hausse.<sup>8</sup> Les entreprises doivent intégrer une solution de sécurité email dans leur stratégie de défense, pour être moins vulnérables face à de nouvelles menaces toujours plus virulentes. Trend Micro™ Smart Protection Network™, technologie évoluée et analytique de réputation web est un moyen de neutraliser les menaces les plus récentes. De surcroît, une protection étendue est proposée aux entreprises par des solutions telles que Trend Micro™ ScanMail™ Suite.

Dans un contexte de forte mobilité et d'attaques ciblées, les entreprises doivent prendre en considération toutes les communications par email, en particulier celles contenant des pièces jointes et des liens malveillants. Une solution de sécurité pour les serveurs email, comme ScanMail™ Suite for Microsoft® Exchange™, neutralise à la fois les liens et les documents joints malveillants dans les emails, et protège les organisations au-delà des menaces email traditionnelles.

<sup>7</sup> [http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp\\_decisive-analytics-consumerization-surveys.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf)

<sup>8</sup> <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Blackhole+Exploit+Kit+Spam+Runs%3A+A+Threat+Vortex%3F>



## TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), spécialiste de la sécurité du cloud, sécurise les échanges numériques pour les entreprises et le grand public, grâce à ses solutions de sécurité des contenus Internet et de gestion des menaces. Pionnier de la sécurité des serveurs depuis plus de 20 ans, Trend Micro propose une offre complète de sécurité pour postes clients, serveurs et en mode Cloud, pour neutraliser les nouvelles menaces plus rapidement et protéger les données en environnements physiques, virtuels ou Cloud. Optimisés par l'infrastructure Trend Micro Smart Protection Network, les technologies, produits et services Trend Micro dédiés aux environnements Cloud neutralisent toutes les menaces à la source sur Internet et s'appuient sur un réseau mondial de plus d'un million d'experts. [www.trendmicro.fr](http://www.trendmicro.fr)



Securing Your Journey  
to the Cloud

## TRENDLABS

Les TrendLabs constituent l'infrastructure mondiale des centres de recherche, de développement et de support, dédiée, en 24x7, à la surveillance sur les menaces, la prévention des attaques et au bon fonctionnement des solutions de sécurité. Regroupant plus de 1 000 experts et ingénieurs supports, les Trend Labs sont disséminés aux quatre coins de la planète. Les Trend Labs permettent à Trend Micro d'assurer une veille permanente sur les menaces dans le monde, de fournir des données en temps réel pour détecter et neutraliser les menaces, d'étudier et analyser de nouvelles technologies pour déjouer les menaces, de répondre en temps réel aux menaces cibles et d'aider nos clients à minimiser les dommages, à alléger leurs coûts et à assurer la continuité de leur activité.

