

TABLE DES MATIERES

- [Vulnérabilités / Incidents](#)
- [Veille Technologique / Tools](#)
- [Informations Fournisseurs](#)
- [Sites d'intérêt](#)
- [Informations / News Navixia](#)

Vulnérabilités / Incidents

Social engineering et malware : savoir ouvrir l'oeil !

La tendance se confirme : les pirates jouent toujours plus sur les sentiments des utilisateurs pour faire circuler les malware. Deux exemples récents :

Les hackers ont tiré parti de l'émotion entourant les catastrophes naturelles comme le [tremblement de terre au Chili](#). Websense constate d'ailleurs que [plus de 13%](#) des recherches concernant des sujets d'actualité récents aboutissent

- à des liens malveillants. La société [donne ici l'exemple](#) d'une page html concernant le tsunami frappant Hawaii, « déguisée » en PDF pour augmenter sa crédibilité (c'est nouveau), et destinée à infecter le visiteur.
- Par ailleurs, et bien qu'il soit déjà en circulation depuis plusieurs mois, un ver virulent nommé Palevo [infecte les messageries](#) ces jours-ci. Il incite le destinataire à visualiser la galerie photo d'un ami. En cliquant sur un fichier JPG, l'utilisateur se fait infecter par le ver [Worm.P2P.Palevo.DP](#), capable d'intercepter des mots de passe et d'autres données sensibles saisies dans les navigateurs web Firefox et Internet Explorer.

« Jedi Packet Trick » : peut-on se fier aux cartes réseaux ?

Pendant la récente [CanSecWest](#) (Applied Security Conference) de Vancouver, [Arrigo Triulzi](#) a démontré dans sa présentation « [Jedi Packet Trick](#) » comment un attaquant pouvait prendre le contrôle à distance de [certaines cartes réseaux](#) de Broadcom (CVE-2010-0104). Un groupe de chercheurs français a par ailleurs simulé [une autre attaque à distance](#) de cartes réseaux et montré ce faisant que le firmware des NIC joue un plus grand rôle que ce que l'on croit (présentation [ici](#)). L'avenir serait à des NIC plus simples et à des drivers plus petits, garants d'une meilleure sûreté. Plus d'infos sur l'ensemble de la conférence, [en images](#) et en [blog](#).

Veille Technologique / Tools

Dernier rapport MELANI : intéressante lecture

Le [10^{ème} rapport](#) de la centrale d'enregistrement et d'analyse pour la sûreté de l'information [MELANI](#) vient de paraître. Il est consacré aux vols d'informations, aux attaques à connotation politique et au chantage, sous la menace d'attaques de type déni de services, durant le 2^{ème} semestre 2009. Là aussi, on voit clairement que les hackers s'appuient sur le social engineering dans beaucoup des attaques récentes... [A lire ici](#).

Scanner de vulnérabilités web

Le spécialiste en sécurité bien connu [Michal Zalewski](#) vient de développer pour Google un tool gratuit baptisé [skipfish](#). Il s'agit d'un scanner open source particulièrement rapide qui permet d'auditer la sécurité des sites et des applications web.

Sécurité sur Windows 7 – panorama

[Windows 7](#) a été [bien accueilli et rapidement adopté](#) par les entreprises – ce qui a eu pour conséquence de confronter, parfois douloureusement, beaucoup d'administrateurs réseau avec les nouvelles caractéristiques sécurité de la plate-forme. Windows 7 introduit non seulement des changements au contrôle des utilisateurs (User Account Control), au BitLocker et à d'autres

éléments hérités de Vista, mais aussi une série d'**éléments nouveaux** dont il est intéressant de découvrir le détail.

Nouvelles du BlackHat Barcelone

La conférence **BlackHat**, qui a eu lieu à Barcelone du 12 au 15 avril dernier et qui rassemble les plus grands noms de la sécurité informatique dans le monde, a traité les problématiques les plus chaudes du moment réparties en trois thèmes principaux : la sécurité des applications, celle du hardware, et des sujets généraux critiques (« big picture security issues »). Tous les supports sont consultables [ici](#), y compris la présentation de **maltego 3**, l'application d'information forensique open source révolutionnaire développée par **Roelof Temmingh**, qui permet de retrouver et d'agrèger les traces les plus infimes d'un internaute sur la toile pour retracer son profil en ligne.

Kirillos et l'histoire des comptes Facebook

La nouvelle a créé un **buzz** sur la toile : fin avril, **iDefense**, la division de surveillance hacking de Verisign, annonçait qu'un hacker nommé Kirillos proposait à la vente 1,5 million de comptes Facebook (soit un utilisateur sur 300) sur un forum underground à des prix **particulièrement bas**. Le vol et la revente d'identifiants ne sont pas rares dans le monde des hackers, mais l'attention des investigateurs a été éveillée par le volume inhabituel de l'offre et par l'origine apparemment russe du hacker, surprenante car jusqu'ici les hackers russophones limitaient plutôt leurs activités à leurs réseaux sociaux régionaux. Avec quelques jours de recul, et un travail d'investigation poussé de VeriSign et de Facebook, il semble que le buzz se soit dégonflé : le hacker – un naïf ? un débutant ? – n'aurait en réalité détenu que **quelques centaines de comptes**, dont il aurait créé une grande partie lui-même. Facebook, qui a d'ailleurs fini par remonter la trace du hacker et **identifier le coupable**, a maintenant porté plainte contre lui.

Botnets plus ou moins insidieux

W32.Qakbot est un ver en circulation **depuis plus d'une année**, qui se propage via le javascript de pages web malveillantes. Il **transfère certaines informations** - et pas n'importe lesquelles - de l'ordinateur infecté sur des serveurs FTP: des logins utilisateurs, des certificats du système. Malgré cela, il reste considéré comme peu dangereux, car pour éviter d'éveiller l'attention, il se propage très lentement et prudemment. Mais il gagne du momentum : Symantec a récemment annoncé, après avoir analysé pendant deux semaines deux serveurs FTP utilisés par Qakbot, que le botnet parvient à uploader plus de **2GB de données sensibles par semaine** (logins e-banking, données de cartes de crédit, logins de comptes de réseaux sociaux, logins de comptes e-mail, historiques internet, etc.) lui permettant de retracer un portrait très complet des habitudes de consommation des utilisateurs des ordinateurs contaminés. Garder ses antivirus constamment à jour reste la meilleure parade pour éviter les intrusions indésirables.

Informations Fournisseurs

Consécration pour Clearswift

En remportant le trophée du "Best Content Security 2010" décerné par le **SC Magazine**, Clearswift s'est vu attribuer l'un des prix les plus convoités de l'industrie de la sécurité. **Clearswift** est réputé pour ses solutions efficaces de sécurisation de la messagerie et d'internet. Plus d'infos sur les concurrents et sur les résultats de l'édition 2010 [ici](#).

Websense : conformité PCI assurée

Ce document montre comment le **Data Security Suite** de Websense permet de sécuriser les informations de l'entreprise pour les mettre en conformité avec les **normes très strictes** de sécurité des cartes de crédit (PCI DSS). **Websense** y parvient en particulier en protégeant les données contre les risques de pertes et de fraude, qu'ils soient d'origine interne ou externe.

Des nouveautés chez Check Point

Check Point a annoncé au mois de mars la sortie de deux nouvelles solutions :

- **Abra, le bureau virtuel**, permet à l'aide d'une clé USB cryptée de travailler de manière sécurisée avec vos données d'entreprise sur n'importe quel ordinateur dans un espace de travail virtuel séparé. Le cryptage intégré protège les données pendant le travail ou le déplacement. Plus d'infos [ici](#).
- **Data Loss Prevention (DLP)** est une solution de prévention des fuites de données. Elle permet d'assurer de manière préventive une protection contre la perte involontaire de données sensibles. Plus d'info [ici](#).

Magic Quadrant de Gartner pour les firewalls d'entreprise

Gartner a publié en mars [son analyse](#) du marché des principaux concepteurs de firewalls. Check Point y figure comme un leader du marché. Selon cette analyse, Provider-1 est particulièrement apprécié par ses utilisateurs et la version R70 a apporté un nombre significatif d'améliorations qui distinguent Check Point sur le marché. La console de management SmartCenter est considérée comme étant de grande qualité. Check Point est vu comme un fabricant solide, dont les solutions sont appropriées aux entreprises de toutes tailles.

Dernières versions software

La liste des dernières versions utilisées dans nos produits se trouve [ici](#).

Sites d'intérêt

Etat d'internet en temps réel

[Akamai](#) fournit en temps réel l'analyse du trafic internet dans le monde entier : nombre d'attaques en cours, temps de latence les plus élevés et densité du trafic.

Géolocalisation par Wifi

Vous utilisez Firefox, et vous êtes connecté à internet à travers un réseau Wifi ? Alors testez [ce site](#), qui vous géolocalise quasiment à l'immeuble près sur Google maps. Et voilà pourquoi Google utilise également un sniffer Wifi sur les voitures qui prennent les photos pour StreetView ! Qui aurait pensé que les MAC-adresses de nos points d'accès serviraient un jour ?...

La manière dont les informations privées sont exploitées par Google crée, on le sait, [un certain malaise](#) au niveau des instances de [protection des données](#). Pour contrer la polémique liée à l'affaire des sniffers Wifi, Google a d'ailleurs annoncé vendredi que, dès la semaine prochaine, Google search sera [disponible en mode crypté](#).

Trafic aérien en direct

Clin d'œil aux récentes fermetures des espaces aériens en Europe : voici un site au graphisme très réussi qui donne la [position des avions](#) en temps réel (éviter Internet Explorer, problème de script).

Informations / News Navixia

L'exemple des autres...

Comment assurer la traçabilité et le contrôle des accès privilégiés aux infrastructures de sécurité de l'entreprise ? Pour les institutions qui traitent des informations confidentielles, savoir qui accède aux ressources, à quel moment et dans quel but est une nécessité. [Découvrez ici](#) comment une banque privée internationale à Genève a trouvé une réponse efficace à ce problème.

D'autres témoignages vous intéressent ? [Ceux de nos clients](#) qui acceptent de faire part de leurs expériences vous offrent un outil de référence précieux. Merci à eux, et profitez bien de ces lectures...

Nouveau web Navixia

Notre site internet a fait peau neuve ! Prenez le temps d'y [jeter un coup d'œil](#).

« Techno Digest » & Croissants

Notre prochain rendez-vous aura lieu à la fin de juin. Cette fois, nous rompons avec la tradition des séances d'informations générales. En effet, en raison de la quantité et de la complexité des nombreuses nouveautés proposées par Check Point dans le domaine de la sécurité étendue, il nous a paru nécessaire d'organiser une séance spéciale « digest » pour vous expliquer de manière condensée et vous démontrer concrètement l'essentiel des nouvelles fonctionnalités proposées. Attention : certaines démonstrations seront des premières mondiales !

Vous pourrez entre 08:30 et 10:00 vous informer de manière compacte tout en dégustant café et croissants. Un gain de temps considérable. Plus d'infos et inscriptions [sur notre site](#).

Formation en sécurité: réservez votre place à temps !

Pensez à votre formation en sécurité ! Une nouvelle session de cours de haut niveau vous attend à la fin de septembre 2010. Attention, le nombre de places est limité.

- Les [cours HBN](#) sont donnés en collaboration avec la société Sensepost. Vous avez le choix entre différents niveaux de cours spécialisés portant sur la sécurisation de votre réseau: niveau initiation ([Bootcamp Edition](#)), niveau expert ([Combat Edition](#)). Vous pouvez [voir ici](#) la description générale des cours, accéder à tous les détails du programme et lire les commentaires des participants.
- Nous offrons aussi des [cours de sensibilisation](#) à la sécurité destinés à tout le personnel non technique. Ces cours s'organisent dans vos locaux à votre convenance.

Vous pouvez [télécharger notre prospectus de cours](#) (en français), et nous sommes [à votre disposition](#) pour toute question.

Avez-vous un commentaire ou souhaitez-vous réagir à un article de cette newsletter ? [Cliquez ici](#).

Vous recevez la newsletter de Navixia parce que vous en avez fait la demande spécifique. Si toutefois vous souhaitez vous désinscrire, il vous suffit de [cliquer sur ce lien](#)