



Panorama de la cybercriminalité

Année 2003



Objectifs du panorama

Apprécier l'émergence de nouveaux risques et les tendances de risques déjà connus

Relativiser ou mettre en perspective des incidents qui ont défrayé la chronique

Englober la criminalité haute technologie, comme des atteintes plus « rustiques »

Sélection réalisée par un groupe de travail pluriel (assureur, avocat, consultant, journaliste, officier de gendarmerie et police, RSSI).

Sélection des événements médias

Illustration

- d'une émergence,
- d'une tendance,
- d'un volume d'incidents.

Cas particulier

- Impact ou enjeux,
- Cas d'école.

Les images sont droits réservés

Les informations utilisées proviennent de sources ouvertes, quelques références d'URL en annexe

Les entreprises sont parfois citées par souci de précision et parce que leur nom a été communiqué dans les médias

Retour sur le panorama 2002

- Vote électronique

- Intrusions sur les réseaux d'entreprises spécialisées (eVote)
 - www.cnn.com/2003/TECH/biztech/12/29/voting.hack.ap/index.html
 - <http://www.msnbc.msn.com/id/3825143/>

- Données personnelles - vol d'identité - fraude

- Vols massifs de fichiers
 - <http://news.bbc.co.uk/1/hi/uk/3228040.stm>
 - <http://news.zdnet.co.uk/internet/0,39020369,2137915,00.htm>
 - <http://news.zdnet.co.uk/internet/0,39020369,2131593,00.htm>

Retour sur le panorama 2002

- Chantage-Extorsion

- Extorsion et arrestation, laboratoire au Pôle Sud

- <http://www.southpolestation.com/news/news.html>
- <http://www.thepoles.com/story/HackAttackontheSouthPoleStationOct192003.shtml>
- <http://www.mail-archive.com/isn@attrition.org/msg01811.html>

- Dangers des réseaux sans fil

- Intrusion via hot spot

- <http://cryptome.org/att-spam.htm>
- <http://www.theregister.com/content/69/34144.html>

- Yescard 2G

- Utilisation de la Valeur de Signature d'un porteur

- AFP, 06/11/03, Créteil
- AFP, 2/12/03, Mulhouse

Retour sur le panorama 2002

La fraude aux cartes bancaires prend une nouvelle dimension internationale et technologique : fausse goulotte pour lire la piste magnétique, caméra pour enregistrer la composition du code...



Retour sur le panorama 2002



Quelques références

AFP, 17/02/03, Nîmes

AFP, 09/04/03, Nice

AFP, 19/12/03, Meaux

Panorama 2003

- 💣 Logiciel Libre : une sécurité surestimée ?
- 💣 Téléchargements illicites : les risques pour l'entreprise
- 💣 Virus : professionnalisation et recherche de gain
- 💣 Ripostes judiciaires : objectif dissuasion
- 💣 La riposte anti-spam s'affirme
- 💣 Phishing : la triple imposture
- 💣 Nouvelles opportunités d'espionnage *hi-tech*

Logiciel Libre : une sécurité surestimée ?

Les faits

Plusieurs événements de l'année 2003 semblent altérer la réputation de sécurité des systèmes d'exploitation OpenSource :

- Vulnérabilité du serveur de gestion CVS.
- Cheval de Troie sur un serveur FTP GNU.
- Faille serveur Debian.
- Mise en évidence de failles dans différents noyaux pendant defcon11 (réunion de hackers à Las Vegas).
- Tentative de corruption de la version 2.6 du prochain Linux.

Logiciel Libre : une sécurité surestimée ?

Chronologie et détails

21/01/2003 : détection d'une vulnérabilité dans le gestionnaire de versions CVS (concurrent versions system), utilisé par la majorité des projets OpenSource. Cette faille dans le serveur CVS permet pour un attaquant d'obtenir des privilèges (éventuellement root suivant l'état du serveur) qui peut alors modifier les données (et donc les versions des sources) stockées sur le serveur.

fin juillet 2003 : un cheval de Troie est découvert sur un serveur racine FTP du projet GNU. L'attaque exploite une faille de l'appel système ptrace (permettant à un processus parent de contrôler l'exécution d'un processus fils, utilisé notamment pour le débogage). Le cheval de Troie aurait été déposé à la fin du mois de mars 2003. Les responsables du projet conseillent de contrôler systématiquement l'intégrité des sources téléchargées.

Logiciel Libre : une sécurité surestimée ?

Chronologie et détails

01 au 03 août 2003 : au cours de la réunion de hackers defcon11 organisée à LAS VEGAS, un audit de code mené sur plusieurs OS OpenSource (Linux, FreeBSD, NetBSD, OpenBSD) met en évidence la présence de nombreux défauts. La présentation montre que les 3 mois d'audit ont pu révéler une centaine de failles, des débordements de mémoire portant surtout sur les drivers et les appels système dans les sources des OS. Selon l'auteur, l'exploitation de ces vulnérabilités n'est pas forcément très difficile, contrairement à ce qui est généralement annoncé pour ce type de systèmes.

Logiciel Libre : une sécurité surestimée ?

Chronologie et détails

06/11/2003 : tentative de corruption de la nouvelle version du noyau Linux (2.6). Accédant à la plateforme gérant les versions des sources du futur Linux en usurpant l'identité d'un développeur, un attaquant y dépose un cheval de Troie. L'objectif était de donner l'accès root au pirate sur toutes les machines qui auraient exécuté ce noyau ! Le problème est rapidement décelé et éradiqué lors du contrôle d'intégrité des données.

Novembre 2003 : le projet de développement de la distribution DEBIAN est victime d'une intrusion (compromission de 4 serveurs). Cette attaque utilise une faille du noyau (version 2.4.22) découverte en septembre 2003 : débordement de mémoire dans la fonction `do_brk()` qui permet d'augmenter les privilèges (de passer root) pour un processus utilisateur.

Logiciel Libre : une sécurité surestimée ?

Enjeux et conséquences

(Re)pose le problème de la sécurité des projets OpenSource, plus que jamais important compte tenu du succès croissant des systèmes d'exploitation issus du monde libre, notamment dans les milieux professionnels : serveurs, systèmes embarqués...

- Problème de l'introduction d'une faille intentionnelle dans les sources d'un OS : soit depuis l'extérieur par un pirate n'appartenant pas au projet, soit par un développeur malveillant participant au projet. L'exploitation de cette faille permet la prise de contrôle de la machine sur laquelle s'exécute le système d'exploitation.

La multiplication des projets et l'intérêt grandissant pour le libre peuvent-ils être des facteurs aggravant la sécurité des systèmes ?

Logiciel Libre : une sécurité surestimée ?

Enjeux et conséquences

- Les arguments souvent avancés de meilleure sécurité pour les OS libres semblent maintenant plus discutés : les systèmes d'exploitation libres ne sont pas forcément écrits par des experts sécurité, contiennent des failles (souvent de type débordement de mémoire) qui peuvent être exploitées relativement (?) aisément et permettre à des pirates de prendre le contrôle de machines exécutant ces OS.

La sécurité des OS OpenSource a-t-elle tendance à être surestimée ?

Logiciel Libre : une sécurité surestimée ?

Enjeux et conséquences

La gestion des failles et des correctifs devient un domaine de plus en plus lourd à gérer pour les équipes d'administration des entreprises. Ce travail est devenu un enjeu important pour la sécurité des systèmes d'information. Les systèmes d'exploitation OpenSource n'échappent pas à cette logique.

La gestion des correctifs peut-elle devenir un facteur important dans le déploiement des OS libres?

Logiciel Libre : une sécurité surestimée

Quelques références

- <http://www.cert.org/advisories/CA-2003-02.html>
- <http://www.cert.org/advisories/CA-2003-21.html>
- <http://computerworld.com/securitytopics/security/hacking/story/0,10801,87516,00.html>
- <http://www.kb.cert.org/vuls/id/301156>
- <http://www.defcon.org/html/links/defcon-media-archives.html#defcon-11>
- <http://www.newsfactor.com/perl/story/22748.html>
- <http://www.zdnet.fr/actualites/technologie/0,39020809,39129006,00.htm>

Téléchargements illicites : les risques pour l'entreprise

Les faits

Les thèmes du détournement des moyens informatiques de l'entreprise à des fins illégales et de sa responsabilité civile par rapport à ses employés continuent de faire l'actualité pendant l'année 2003 : condamnation de Lucent Technologies, arrêt du conseil d'Etat suite à l'utilisation abusive d'une adresse électronique professionnelle, décision d'une cour d'appel dans une affaire de saisie de disquettes lors d'un licenciement.



Téléchargements illicites : les risques pour l'entreprise

Chronologie et détails

Jugement TGI Marseille du 11/06/03 : Un employé de Lucent Technologies conçoit un site personnel dénonçant les abus (selon lui) de la société Escota. Il met en ligne ce site depuis son poste de travail. Le tribunal de grande instance de Marseille condamne l'auteur de ce site mais aussi sa société en considérant que la faute a été commise dans l'exercice de ses fonctions (article 1384 du code civil).

Décision du conseil d'Etat du 15/10/03 : le conseil d'Etat confirme l'exclusion temporaire d'un adjoint technique de recherche. Cet employé avait utilisé l'adresse électronique de son directeur de laboratoire pour communiquer sur le site d'une secte. L'entreprise a été avertie de ce problème par un autre salarié et a à priori constaté le fait sur le site sans prendre connaissance du contenu de mails.

Téléchargements illicites : les risques pour l'entreprise

Chronologie et détails

Arrêt de la cour d'appel de bordeaux du 29/10/03 :
Une société licencie une salariée pour faute lourde en utilisant le contenu de disquettes pour prouver son activité parallèle pendant son temps de travail. Le tribunal considère cette preuve comme valide et ne retient pas l'argument d'atteinte à la vie privée, rien n'indiquant le caractère personnel de ces disquettes.

Téléchargements illicites : les risques pour l'entreprise

Contexte

- La responsabilité pénale des employés est engagée en cas d'utilisation illicite de moyens informatiques de l'entreprise : droit d'auteur et des marques pour téléchargement de logiciels pirates, documents audio ou films (MP3, DIVX...), loi Godfrain (code pénal : 323.1, .323.2 et 323.3) pour les tentatives d'intrusion et d'altération d'un système.
- La responsabilité civile des entreprises peut aussi être établie si les tribunaux considèrent que l'employé en faute était « dans l'exercice de ses fonctions » en s'appuyant sur l'article 1384 du code civil (ou responsabilité du commettant du fait du préposé)

Téléchargements illicites : les risques pour l'entreprise

Enjeux et conséquences

- Surveillance des employés : les entreprises sont partagées entre la volonté d'exercer un contrôle de l'utilisation des moyens informatiques mis à disposition des salariés et le respect de l'intimité de leur vie privée (confirmé notamment par l'arrêt NIKON du 02/10/2001 de la Cour de cassation). Quels moyens pour protéger l'entreprise (chartes...) ?
- Responsabilité civile de l'entreprise : en cas d'utilisation illicite des moyens informatiques, quels sont les cas où le salarié est considéré comme étant dans l'exercice de ses fonctions ?
- Ces tendances peuvent-elles entraîner une diminution des moyens mis à disposition des salariés ?

Téléchargements illicites : les risques pour l'entreprise

- Quelques références

- www.legalis.net/jnet/2003/actualite_07_2003.htm

Virus : professionnalisation et recherche de gain

Des objectifs technologiques

- Savoir se mettre à jour :
 - W95/Babylonia@M (1999)
 - W32/Hybris@MM (2000)
 - W32/Sobig@MM (2003)
- S'affranchir de l'utilisateur, Gagner en vitesse, diminuer en taille :
 - W32/CodeRed.worm (2001)
 - W32/SQLSlammer.worm (2003)
- Intégrer de multiples techniques de propagation, cibler le particulier et l'entreprise :
 - W32/Nimda@MM (2001)
 - W32/Cayam.worm!p2p (2003)
- Être anonyme, séduire l'utilisateur ou s'en affranchir :
 - W32/BugBear@MM (2003)
 - W32/Sobig@MM (2003)
- Tirer avantage des nombreuses vulnérabilités découvertes :
 - W32/Lovsan.A.worm (2003)

Virus : professionnalisation et recherche de gain

- **Des objectifs pragmatiques, ciblés et fonctionnels**

- Ouvrir la voie à d'autres formes d'attaques :
 - [W32/Sobig@MM \(2003\)](#)
- Distribuer une porte dérobée :
 - [W32/Bugbear.B@MM \(2003\)](#)
- Porter atteinte à la confidentialité :
 - [W32/Sircam@MM \(2001\)](#)
 - [W32/Klez.H@MM \(2002\)](#)
- Collecter des informations diverses et des mots de passe :
 - [W32/Bugbear@MM \(2003\)](#)
 - [W32/Mimail.I@MM \(2003\)](#)
- Distribuer des mini-serveurs relais afin de faciliter l'envoi de courriers non-sollicités :
 - [W32/Sobig@MM \(2003\)](#)

Virus : professionnalisation et recherche de gain

W32/BUGBEAR.B@MM

- Le virus contient une TRES LONGUE liste de domaines liés au monde bancaire (France, Grande Bretagne, Allemagne, Australie, Italie, Grèce, Danemark, Nouvelle-Zélande, Espagne, Brésil, Roumanie, Pologne, Argentine, Suisse, Finlande, Taiwan, Turquie, Islande, Slovaquie, Corée, Etats-Unis, Afrique du Sud, Républiques Baltes, Autriche, Hongrie, Norvège, Tchécoslovaquie).
- Au démarrage de la machine, si celle-ci appartient à l'un des domaines cibles, la clé de registre responsable du processus de numérotation téléphonique automatique est désactivée.
- Le virus recherche alors les mots de passe présents dans la mémoire cache et les envoient à une adresse prédéfinie choisie aléatoirement dans une liste.
- Une fois ce travail effectué, le virus restaure la clé de registre.

banquepopulaire.fr
bics.fr
bpic.fr
bpnord.fr
bred.fr
ca-alpesprovence.fr
ca-alsace-vosges.fr
ca-midi.fr
ca-normand.fr ccbonline.com
ccf.fr
cin.fr
covefi.fr
cpr.fr
credit-agricole.fr
credit-du-nord.fr
creditleyonnais.fr
creditmutuel.fr
-epargne.fr
eurocardmastercard.tm.fr
nxbp.fr
smc.fr
transat.tm.fr

Virus 2003 : professionnalisation et recherche de gain

W32/BUGBEAR.B@MM cible plus de 1300 domaines bancaires

lnatbanker.com lnationalbank.com lstbk.com lstfed.com lstfederal.com lstnatbank.com
lstnationalbank.com lstnb.com lstnewrichmond.com lstsecuritybank.com lstsource.com
365online.com 53.com abbeynational.co.uk abbybank.com abingtonbank.com abnamro.be
abramsbank.com abtbank.com accbank.ie acommunitybk.com adirondacktrust.com advance.com.au
advance-bank.de advancefinancial.com aea-bank.com afbank.com affinbank.com.my agfirst.com
agrobresciano.it ahli.com aib.ie aibusa.com aigprivatebank.com ain.hangseng.com
alettibank.it allbank.com allbank.de allegiantbank.com alliancebank.com alliance-bank.com
alpbank.com alpha.gr alpinebank.com altapd.it amagerbanken.dk ambfinancial.com amcore.com
ameribank.com american-bank.com americanbankmn.com americanbankmontana.com
americanexpress.com americanfsb.com americannationalbank.com americantrust.com amgb.com
amsouth.com anb.com.sa anb.portalvault.com anbcleveland.com anbfinancial.com anbnet.com
anchorbank.com anchornetbank.com antonveneta.it anz.com.au arabank.com arjil-associes.com
arvest.com asbbank.co.nz asbonline.com ashefederal.com askbm.co.uk assbank.it assocbank.com
atlanticcentral.com auburndalecoop.com avbpgh.com avsb.com axa.be azzoaglio.it ba-ca.com
baldwinfnb.com baltcosavings.com balticbankinggroup.com banamex.com bancaakros.webbank.it
bancadibologna.it bancadipiaccenza.it bancadirimini.it bancadisassari.it bancaetruria.it
bancaintesa.it bancamarch.es bancamediolanum.it bancaprofilo.it bancaucb.com bancavalle.it
bancfirst.com bancoatlantico.es bancobrascan.com.br bancocuscatlan.com bancodisicilia.it
Etc., etc., etc.

Virus : professionnalisation et recherche de gain

La famille W32/SOBIG@MM

- Des expériences qui ne doivent pas interférer les unes avec les autres.
- Au travers de mécanismes complexes, Sobig installe sur les machines cibles, des renifleurs de clavier, des portes dérobées et des mini-serveurs proxy.

VARIANTE	DATE DE DECOUVERTE	DATE DE FIN DE VIE PROGRAMMEE ET REMARQUES
Découverte de l'existence d'étranges serveurs proxy.	Août 2002	
W32/Sobig.A	9 janvier 2003	Automatique dès l'installation du cheval de Troie
B	18 mai 2003	31 mai 2003 (liée à l'horloge interne du PC)
C	31 mai 2003	8 juin 2003 (liée à des serveurs NTP)
D	18 juin 2003	2 juillet 2003 Fin de la dépendance Geocities. Les serveurs secrets sont derrière des modems câble. Même si l'adresse IP n'est pas fixe, elle est conservée suffisamment longtemps pour l'utilisation qui en est faite.
E	25 juin 2003	14 juillet 2003 // avant la date via le cheval de Troie
F	18 août 2003	10 septembre 2003 La « stratégie SOBIG » ayant été mise à jour, c'est un échec. L'auteur va devoir changer de tactique.

Virus : professionnalisation et recherche de gain

W32/SOBIG@MM fait évoluer le spamming

- Avant :
 - Utilisation de comptes temporaires, on l'ouvre le vendredi, on l'abandonne le lundi. Inconvénient : on laisse sa trace chez l'ISP (carte de crédit).
 - Utilisation de serveurs relais SMTP ouverts. Inconvénient : on laisse sa trace, ils peuvent être « blacklistés ».
 - Utilisation de la technique du « tunneling » avec serveurs proxy HTTP/SOCKS non sécurisés. Inconvénients : les ports TCP ou UDP peuvent être « blacklistés ».
- Sobig entre en scène :
 - Distribution de serveurs proxy invisibles et utilisant des ports non standards (Wingate – serveur proxy légitime détourné).
 - Le paramétrage est modifié à chaque nouvelle version (ports utilisés).
- Aujourd'hui, 2/3 du spam se fait par le biais de serveurs proxy créés par les virus (source MessageLabs)

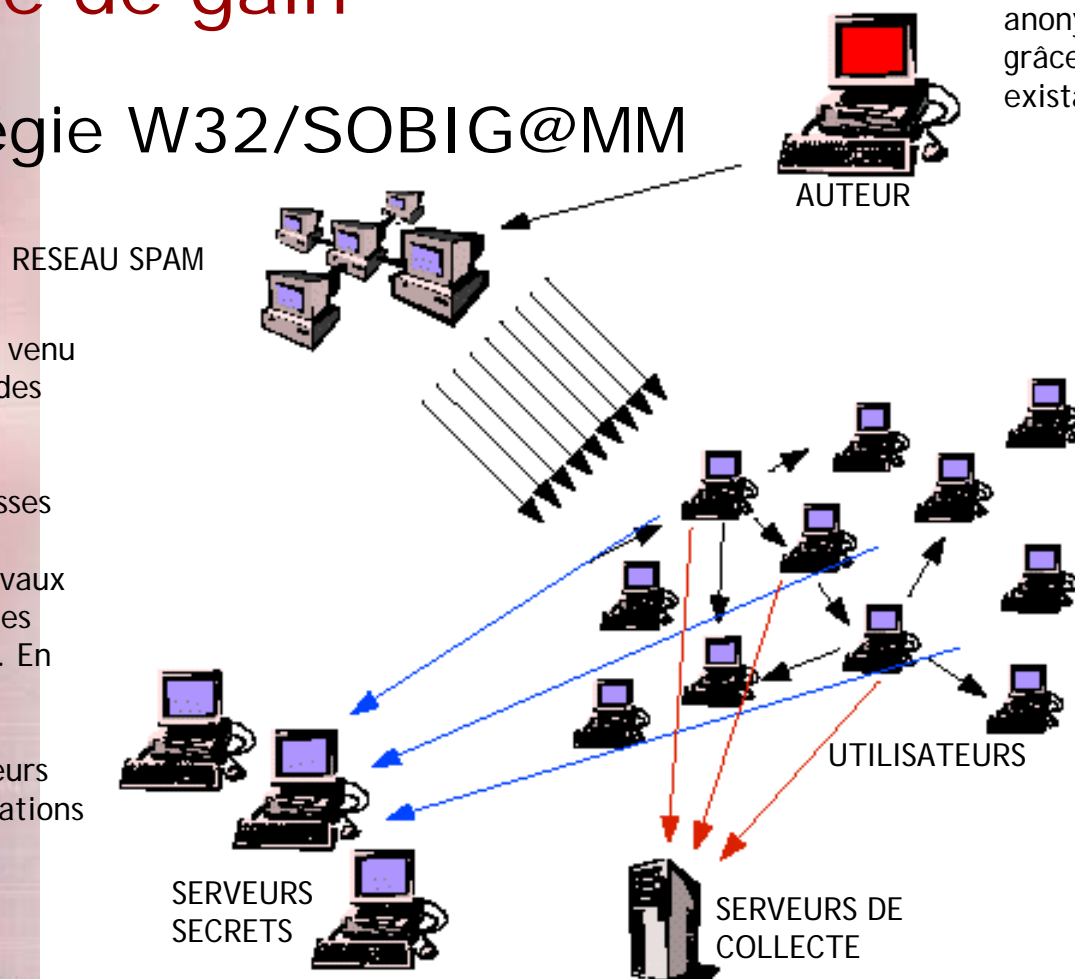
Virus : professionnalisation et recherche de gain

W32/SOBIG@MM s'intéresse au monde bancaire

- Activation du renifleur de clavier si des chaînes de caractères spécifiques sont détectées au travers d'Internet Explorer :
 - W32/Sobig.A@MM (Lala.A)
 - PayPal, paypal, iFriend, E-Bullion, EZCardinc, gold, Gold, Account Access, orders, Nettler, Chase, Evocash, Intimate Friends Network, Bank, My eBay, WebMoney, Washington Mutual, LloydsTSB online, My Online Accounts, Web Money, compte, Compte, banque, Banque, Rekeningnummer, rekeningnumber, bank
 - W32/Sobig.E@MM (Lala.E)
 - e-gold Account Access, Account Access, Bank, My eBay, Online Service, bank, E*TRADE Financial, PayPal – Log In
- Capture des cookies correspondants
- Expédition des données capturées vers l'auteur du virus.

Virus : professionnalisation et recherche de gain

La stratégie W32/SOBIG@MM



Étape 1: L'auteur diffuse anonymement un e-mail infecté grâce aux serveurs proxy existants.

Étape 2: Les utilisateurs imprudents cliquent sur la pièce jointe, s'infectent et propagent le virus à toute adresse trouvée dans les fichiers .TXT et .HTML.

Étape 4: Si l'utilisateur tente de joindre un site bancaire, le cheval de Troie s'active, les informations sont capturés et retransmise vers des serveurs de collecte.

Étape 3: Le moment venu (gâchette calée sur des serveurs NTP), les ordinateurs infectés contactent des adresses IP secrètes et téléchargent les chevaux de Troie et la liste des serveurs de collecte. En dehors du créneau horaire, et s'ils sont interrogés, ces serveurs délivrent des informations erronées.

Étape 5: De nouveaux serveurs proxy se mettent en place. Ils pourront être utilisés par l'auteur du virus ou par d'autres spammeurs. Le moment venu, une nouvelle version de Sobig est diffusée pour optimiser le processus.


D'après l'étude LURHQ

Virus : professionnalisation et recherche de gain

W32/MIMAIL.I@MM
W32/MIMAIL.J@MM

Simulation d'écrans sécurisés de saisie et renvoi des informations collectées vers un compte tiers.

PayPal Secure Application



PayPal.com Authorization, step 1 of 2
Please fill all the fields below:

Credit Card Number:	<input type="text"/>
PIN: Please provide us with your correct PIN number so that we are able to cross check your credit card with your bank account	<input type="text"/>
CVV Code: 3 digit number that appears to the right of your card number	<input type="text"/>
Expire date:	<input type="text" value="01"/> <input type="text" value="2003"/>

I confirm that the above information is correct.

Virus : professionnalisation et recherche de gain

W32/MIMAIL.I@MM
W32/MIMAIL.J@MM

Simulation d'écrans sécurisés de saisie et renvoi des informations collectées vers un compte tiers.

PayPal Secure Application

PayPal[®]

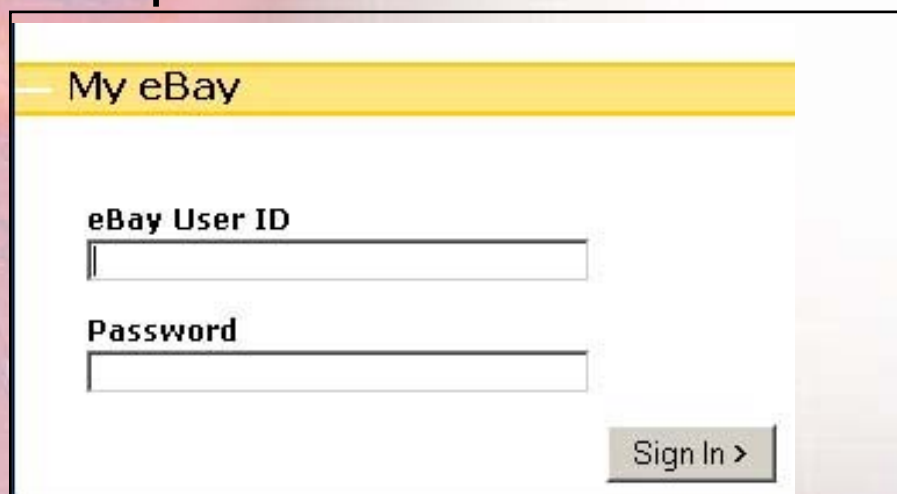
PayPal.com Authorization, step 2 of 2
Please fill all the fields below:

First, Middle, Last Name:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Date of Birth:	<input type="text"/>	01 - Jan <input type="text"/>	<input type="text"/>
Country:	<input type="text"/>		
State:	Alabama <input type="text"/>		
Zip code:	<input type="text"/>		
City:	<input type="text"/>		
Address line 1:	<input type="text"/>		
Address line 2:	<input type="text"/>		
Social security number:	<input type="text"/>		

Virus : professionnalisation et recherche de gain

W32/CAYAM.worm!p2p

Simulation d'écrans sécurisés de saisie et renvoi des informations collectées vers un compte tiers.



The image shows a simulated login form for eBay. At the top, there is a yellow header bar with the text "My eBay". Below this, there are two input fields: "eBay User ID" and "Password". A "Sign In >" button is located at the bottom right of the form.

Sujet: Verify your eBay account information

Corps du Message:

Dear Ebay user,
Dear valued eBay member, It has come to our attention that your eBay Billing Information records are out of date. That requires you to update the Billing Information If you could please take 5-10 minutes out of your online experience and update your billing records, you will not run into any future problems with eBay's online service. However, failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

Please open attachment to update your billing records.

Thank you for your time!

Marry Kimmel,

Attachement: eBayVerify.exe

Virus : professionnalisation et recherche de gain

W32/CAYAM.worm!p2p

Simulation
d'écrans sécurisés
de saisie et renvoi
des informations
collectées vers un
compte tiers.


Verify your eBay account information

Hello *user*

<p>Billing Address</p> <p>Full Name: <input type="text"/></p> <p>Street Address: <input type="text"/></p> <p>Home Phone: <input type="text"/></p> <p>Work Phone: <input type="text"/></p> <p>City: <input type="text"/></p> <p>State: <input type="text"/></p> <p>Zip Code: <input type="text"/></p> <p>Country: <input type="text"/></p>	<p>Credit Card Information</p> <p>Credit Card Number: <input type="text"/></p> <p>Expiration Date: Day: <input type="text"/> Month: <input type="text"/> Year: <input type="text"/></p> <p>Cvv2: <input type="text"/> >> This number is printed on your MasterCard, Visa, Amex cards in the signature area of the back of the card. (It is the last 3 or 4 digits AFTER the credit card number in the signature area of the card)</p> <p>Pin Code: <input type="text"/></p> <p>Card Type: <input type="text"/></p> <p>Bank Name: <input type="text"/></p>
<p>Identity Verification</p> <p>Social Security Number: <input type="text"/> - <input type="text"/> - <input type="text"/></p> <p>Date Of Birth: <input type="text"/></p> <p>Mother's Maiden Name: <input type="text"/></p> <p>Driver License Number: <input type="text"/></p> <p>Driver License State: <input type="text"/></p>	<p>Checking account information</p> <p>Checking Account Number: <input type="text"/></p> <p>Bank Routing Number: <input type="text"/></p> <p>Bank Name: <input type="text"/></p> <p>PayPal Account Information</p> <p>PayPal Login (Optional): <input type="text"/></p> <p>PayPal Password (Optional): <input type="text"/></p>

Virus : professionnalisation et recherche de gain

Les récents événements semblent annoncer une nouvelle destinée pour les virus

- Le but actuel des virus n'est pas la destruction massive sans discernement, il est beaucoup plus réfléchi,
- Le virus transporte des outils dédiés à des tâches indéliques et frauduleuses,
- Des liens se sont établis entre auteurs de virus et acteurs de la criminalité informatique,
- Il n'est plus incongru de penser qu'à moyen terme certains virus soient utilisés dans des buts criminels en lien avec une idéologie totalitaire ou un certain banditisme en col blanc,
- Bugbear, Sobig, Mimap et Cayam s'intéressent aux domaines financiers,
- Certains états ne cachent plus leur intérêt pour le développement et l'utilisation des nouvelles technologies dans un but offensif.

Virus : professionnalisation et recherche de gain

Références

- Relais de Messagerie / Relais Ouvert :
<http://www.easynet.fr/support/netiquette/relais.asp>
- Tous les détails sur Sobig :
<http://www.lurhq.com/sobig.html>
<http://www.lurhq.com/sobig-e.html>
<http://www.lurhq.com/sobig-f.html>
- Spam and Viruses Hit All Time Highs in 2003
<http://www.message-labs.com/news/virusnews/detail/default.asp?contentItemId=613®ion=emea>
- Les domaines bancaires liés à W32/Bugbear.B@MM
http://vil.nai.com/vil/content/v_100358.htm
http://www.f-secure.com/v-descs/bugbear_b.shtml
- Le virus W32/Mimail@MM (variantes I et J)
http://vil.nai.com/vil/content/v_100822.htm
http://vil.nai.com/vil/content/v_100825.htm
- Le virus W32/Cayam.worm!p2p
http://vil.nai.com/vil/content/v_100903.htm

Virus : le ver Internet va-t-il détrôner le « mass-mailer » ?

W32/SQLSlammer.worm

- 25 janvier 2003
- Les leçons apprises n'ont pas servi. Le patch bloquant la faille était connu depuis juillet 2002 mais n'avait pas été appliqué.
- *« Le ver le plus rapide de l'histoire »*

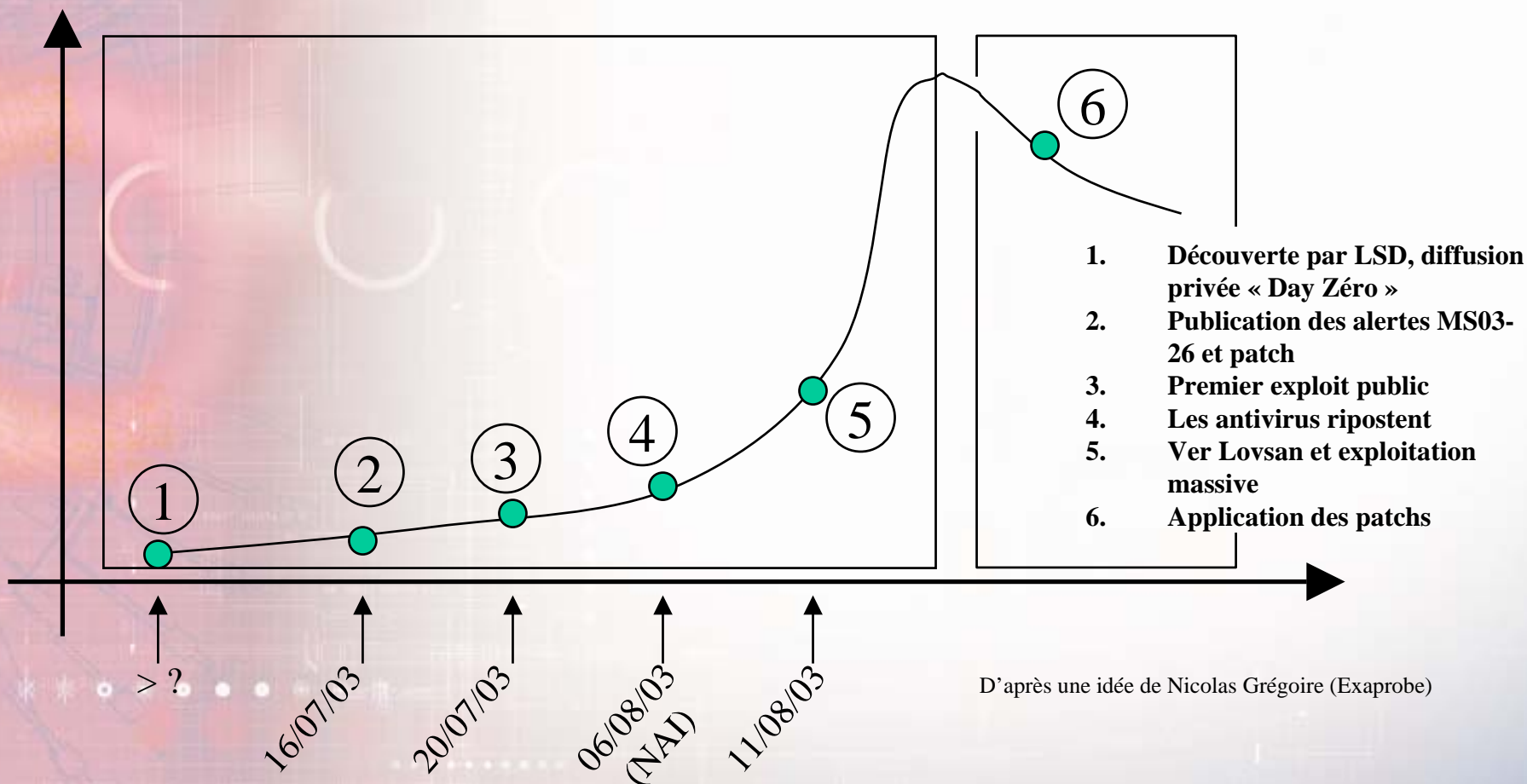
Virus : le ver Internet va-t-il détrôner le « mass-mailer » ?

W32/SQLSlammer.worm

- *« Le ver le plus rapide de l'histoire »*
- En 3 minutes, le ver a atteint son niveau maximal d'activité. Il effectue alors 55 millions de « scan » à la seconde. En moins de 10 minutes, 90% des machines vulnérables étaient atteintes.
- La rapidité de propagation fut aussi un point fort de cette histoire. Le taux de propagation de Slammer doublait toutes les 8,5 secondes. En Juillet 2001, celui de CodeRed.A doublait toutes les 37 minutes et la majorité de ses cibles potentielles furent atteintes en 20 heures (10 minutes pour Slammer)
- Cette différence s'explique par un mode de fonctionnement différent :
 - CodeRed transmettait des paquets TCP-SYN : sa propagation était limitée par le temps de latence nécessaire avant que n'arrive les réponses de la cible.
 - Slammer ne transmettait qu'un seul paquet UDP (*) sans rien attendre en retour. C'est la bande passante disponible qui limitait sa vitesse de propagation. (*) pas de place pour un « payload »

Virus : le ver Internet va-t-il détrôner le « mass-mailer » ?

W32/LOVSAN.A.worm : un autre cas d'école !



D'après une idée de Nicolas Grégoire (Exaprobe)

Virus 2003 : le ver Internet va-t-il détrôner le « mass-mailer » ?

La grande majorité des virus mis en exergue depuis l'an 2000 sont des « mass-mailers ». L'inflexion de tendance au profit des vers (.worm) n'est pas franchement décelable. Elle semble pourtant s'annoncer. Après Codered en 2001, Slammer, puis Lovsan et Nachi en sont les premiers exemples.

VIRUS AYANT ENTRAINES UNE ALERTE NOTABLE	ANNEE	1999	2000	2001	2002	2003 Q1-2-3
MASS-MAILERS	MACRO-VIRUS	4	1			
	VIRUS DE SCRIPT	1	5	3		
	VIRUS PRG (W95/W32)	3	3	8	10	14
.WORM		1	2	2		3
AUTRES	Non mass-mailer, non .worm	12	1	4	1	

Virus 2003 : le ver Internet va-t-il détrôner le « mass-mailer » ?

Références

- CAIDA Analysis of Code-Red
<http://www.caida.org/analysis/security/code-red/>
- Analysis of the Sapphire Worm - A joint effort of CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE
<http://www.caida.org/analysis/security/sapphire/>
- Le ver Internet va t'il détrôner le « mass-mailer » ?
Tableau réalisé après compilation des virus ayant, un moment, entraîné une alerte entre « Médium » et « High » chez Network Associates

Ripostes judiciaires : objectif dissuasion

L'année 2003 est marquée par des actions judiciaires significatives, qui manifestent une volonté de dissuasion.

Ces actions ont une valeur démonstrative : envoi de signes forts à l'adresse des criminels, délinquants et fraudeurs du Net, qu'ils soient des entreprises ou de simples particuliers.

De nouvelles lois se mettent en place

Mais...

Ripostes judiciaires : objectif dissuasion

Dispositifs législatifs

2003 : la France continue à examiner les textes de lois sur l'Economie Numérique.

L'Assemblée Nationale et le Sénat se sont déjà accordés pour durcir les peines et doubler le montant des amendes pour les actes de contrefaçon.

Juillet 2003 : la Californie se dote d'une loi anti-spam.

Octobre 2003 : la Directive européenne sur la vie privée et les communications électroniques entre en vigueur. Les Etats-membres doivent la transposer.

• • • • • Décembre 2003 : Décembre 2003 : Promulgation de la loi anti-spam pour tout le territoire des Etats-Unis.

Ripostes judiciaires : objectif dissuasion

Actions contre les diffuseurs de virus

Janvier 2003 : Simon Vallor, 23 ans, alias « Gobo », auteur des vers GOKAR, REDESI et ADMIRER est condamné à deux ans de prison en Grande Bretagne.

Juin 2003 : Le FBI ouvre une enquête sur le ver BUGBEAR.B

Le ver comporte dans son code une liste de plus d'un millier de banques.

Août 2003 : arrestation de Jeffrey Lee Parson, âgé de 18 ans, à Minneapolis, Minnesota (Etas-Unis). Il est inculpé d'avoir codé et diffusé une variante du ver BLASTER : BLASTER.B.

Ripostes judiciaires : objectif dissuasion

Septembre 2003 : deuxième arrestation en liaison avec la diffusion d'une variante de BLASTER : RPCSDBOT .II s'agit d'un mineur de moins de 18 ans, son nom n'est pas révélé par le FBI ni le lieu de son arrestation.

Septembre 2003 : un jeune homme de 24 ans, est suspecté par la police roumaine d'être l'auteur d'une autre variante du ver BLASTER : BLASTER.F. Les traces laissées dans le code du ver, son pseudonyme « "Enbiei" » et un message en roumain sur un ancien de ses professeurs, ont donné des indices aux enquêteurs.

Ripostes judiciaires : objectif dissuasion

Novembre 2003 : Microsoft annonce qu'il offrira une récompense à toute personne qui pourra donner des informations permettant d'arrêter et d'inculper des auteurs de virus, et consacre une enveloppe de 5 millions de dollars pour ce programme international. Sur cette somme :
250 000 dollars pour l'arrestation de l'auteur de BLASTER.A (alias LOVESAN), et 250 000 dollars pour l'auteur de SOBIG.
Le FBI, le Secret Service et INTERPOL sont associés à ce programme.

Novembre 2003 : arrestation en Espagne de l'auteur présumé du ver RALEKA. Le jeune homme de 23 ans, au pseudonyme « 900K » est également soupçonné d'être le chef du groupe de « phreakers » AKELARRE.

Ripostes judiciaires : objectif dissuasion

Fraudes sur Internet : opérations significatives

Le nombre de plaintes de consommateurs victimes de fraudes sur Internet s'accroît, des autorités gouvernementales lancent des opérations significatives.

Opération contre les escroqueries sur les sites d'enchères

30 avril 2003 – Vaste opération à travers plusieurs Etats américains lancée à la demande de la FTC (Commission Fédérale du Commerce), suite au nombre important de plaintes de consommateurs victimes d'escroqueries sur les sites de vente aux enchères sur Internet. Selon la FTC, 51.000 plaintes rapportées à ses services sont liées à une escroquerie survenue lors d'enchères.

Ripostes judiciaires : objectif dissuasion

Operation E-Con

16 mai 2003 – 130 personnes sont arrêtées et 17 millions de dollars ont été saisis lors d'une vaste opération menée par le FBI dans plusieurs Etats américains, contre diverses fraudes, escroqueries et autres délits commis via Internet : escroqueries aux sites d'enchères, fausses rencontres, contrefaçons de logiciel, etc.

Opération Cyber Sweep

1^{er} octobre 2003 – Opération « Cyber Sweep », présentée comme la plus vaste opération jamais lancée pour lutter contre les fraudeurs agissant sur le réseau Internet. Opération FBI contre escrocs à la carte bancaire, vente de produits contrefaits, etc.

Ripostes judiciaires : objectif dissuasion

Le nombre de plaintes relatives à des fraudes sur Internet était de 53.392 pour les neuf premiers mois de l'année 2003, avant le début de l'opération « Cyber Sweep », contre 48.000 pour les douze mois de l'année précédente, selon les chiffres donnés par le IFCC (The Internet Fraud Complaint Center) qui dépend à la fois du FBI et du National White-Collar Crime aux Etats-Unis.

Lutte anti-spam

Décembre 2003 : Le numéro 8 de la liste des plus gros spammeurs du monde, Jeremy Jaynes est arrêté et mis en examen en Virginie (Etats-Unis) pour fraude afin de transmettre des messages non sollicités.

Ripostes judiciaires : objectif dissuasion

Actions significatives à la demande d'organisations professionnelles

Pour défendre la propriété intellectuelle et les droits des auteurs, les industriels, les organismes représentatifs de producteurs de musique, de films, de l'audiovisuel, des sociétés d'auteurs déposent des plaintes.

Sont visés par les poursuites aussi bien des professionnels (entreprises éditrices de logiciels ou des sites de commerce) que des simples particuliers.



Ripostes judiciaires : objectif dissuasion

Musique : La RIAA dépose plainte contre des particuliers

Le 8 septembre 2003, la RIAA (l'association américaine du disque) annonce qu'elle a déposé 261 plaintes au civil contre des particuliers, pour avoir diffusé en moyenne 1.000 fichiers musicaux *via* les réseaux d'échange Peer To Peer, au mépris des droits des labels et des auteurs.

C'est la première fois que l'industrie du disque s'en prend directement à des particuliers pour défendre la propriété intellectuelle des labels et des artistes.

Ripostes judiciaires : objectif dissuasion

Films, CD et DVD : interpellations et décisions en France et en Espagne

En Espagne, le 18 janvier 2003 : dans une opération présentée comme étant la plus grande opération de ce type en Europe, 40 personnes sont arrêtées à Madrid. La police saisit 250 000 CD et le matériel permettant de reproduire plus de 60 millions de DVD et CD par an.

Grande-Bretagne, janvier 2003 : la chaîne de cybercafés EasyInternet Café est reconnue responsable d'avoir permis à ses clients de télécharger des fichiers musicaux et de les graver sur des CD.

Ripostes judiciaires : objectif dissuasion

En France : février 2003, arrestation d'un jeune homme en région parisienne suite à une plainte de la Fédération des Distributeurs de Films. Il est soupçonné de vendre sur Internet 630 films piratés, dont certains ne sont même pas encore vendus sur le marché.

En Espagne : en juillet 2003, un cabinet d'avocat annonce qu'il va entamer poursuivre 4000 internautes pour échanges de films, musiques et logiciels protégés par le droit d'auteur.

En France : novembre 2003, suite à une plainte de la SACEM, interpellation d'une quinzaine de personnes. Des sociétés écrans vendent sur Internet à des prix très bas des CD et DVD vierges venant d'Asie sans acquitter la taxe SACEM.

Ripostes judiciaires : objectif dissuasion

En décembre 2003, l'ALPA (Association de lutte contre la piraterie audiovisuelle) annonce que le site Internet STPBEAM a été fermé et trois personnes ont été interpellées à Rennes, Strasbourg et Mulhouse.

Le site aurait permis de télécharger 2 000 films récents et constamment renouvelés à travers un réseau d'échange Peer-to-Peer. Plus de 600 films sur CD-R ont été saisis aux domiciles des personnes interpellées.

Ripostes judiciaires : objectif dissuasion

Logiciels d'échanges Peer-To-Peer

Fin avril 2003 : La plainte de plusieurs majors du disque et de l'industrie cinématographique est rejetée par une décision du District Central de la Cour de Californie qui estime que l'entreprise australienne Streamcast Networks exploitant les logiciels de Peer To Peer Grokster et Streamcast (Morphéus) ne peut être reconnue coupable des actes de leurs utilisateurs.

Protection des DVD

Décembre 2003 : La MPAA (Motion Picture Association of America) perd son procès contre Jon Lech Johansen devant la Cour d'Appel de Norvège, poursuivi pour son programme permettant de lire les DVD sous Linux.

Il avait créé le programme DeCSS et vient de contourner la protection des fichiers musicaux de iTunes de Apple.

La riposte anti-Spam s'affirme

Le spam concerne aussi bien les courriers électroniques que les messages SMS.

L'année 2003 est marquée par :

- la forte croissance du spam, l'accroissement des coûts occasionnés,
- la convergence de plus en plus affirmée entre SPAM + PHISHING + VERS,
- les combats entre spammeurs, aidés d'auteurs de virus, et anti-spammeurs,
- la mise en place de mesures législatives aux Etats-Unis et en Europe,
- des arrestations et jugements de spammeurs.

La riposte anti-Spam s'affirme

Utilisation de spam pour la promotion de produits et services :

Viagra, zyban, xanax, Améliorez votre vie sexuelle
Désendettez-vous, Passez un diplôme en ligne, Travaillez à domicile, XXX, porn.

Quand les spams ne proviennent pas de sociétés commerciales ayant pignon sur rue, les spammeurs se servent de méthodes de falsification d'adresses email d'origine ainsi que de sujets de messages trompeurs pour déjouer la méfiance des utilisateurs.

Ainsi, des messages titrés innocemment « Did you see my mother ? » ou « new cartoons », une fois ouverts, affichent des images pornographiques particulièrement explicites.

La riposte anti-Spam s'affirme

Utilisation de spam à des fins malveillantes

Décembre 2003 : En Angleterre, un email de la société Huntington Mail Order reçu par des internautes les informe qu'une somme de 399 livres va leur être débitée pour l'achat d'un d'un lecteur numérique portable IPOD et procure un numéro de téléphone en cas de contestation de l'achat.

En réalité, la société Huntington Mail Order n'existe pas, et le numéro de téléphone fourni est celui d'un commissariat de police, qui voit son standard téléphonique submergé d'appels de réclamations, 500 appels par heure. Quelques heures plus tard, un jeune homme de 21 ans suspecté d'être l'auteur de cet acte de malveillance est arrêté.

La riposte anti-Spam s'affirme

Novembre 2003 : un français est condamné à 10 mois de prison avec sursis et à payer plus de 34 000 euros de dommages et intérêts pour avoir envoyé 700 000 messages à des dirigeants et salariés du groupe pharmaceutique Smith & Nephew (S&N).

Messages dénigrants, pendant plus de deux ans, où il affirme que ses produits sont défectueux ou mortels et ses dirigeants corrompus.

Pour envoyer ses nombreux emails, il adopte un mode opératoire particulier : il envoie les messages depuis une multitude de sites web qui ont une rubrique "envoyez cet article à un ami", usurpe des adresses emails d'expéditeur et trouve le moyen d'envoyer jusqu'à 10.000 messages par heure.

La riposte anti-spam s'affirme

Spams préparatoires à des escroqueries (phishing)

Il s'agit de courriers électroniques non sollicités réalisés dans le but de commettre des escroqueries.

(voir infra Panorama de la Cybercriminalité : Phishing).

Spams déclenchés par des vers informatiques utilisés pour relais de spam et/ ou attaque de sites anti-spam

2003 : Convergence spam+phishing+vers.

(voir infra Panorama de la Cybercriminalité : Virus)

La riposte anti-Spam s'affirme

Spam à des fins commerciales

- En octobre 2003 : la société PW Marketing et ses deux dirigeants sont condamnés en Californie (Etats-Unis) à deux millions de dollars d'amende pour avoir envoyé des millions d'emails publicitaires, sous des noms fictifs. Les millions de spams envoyés faisaient la promotion d'un guide du spam...
- Décembre 2003 : Le numéro 8 de la liste des plus gros spammeurs du monde, Jeremy Jaynes est arrêté et mis en examen en Virginie (Etats-Unis) pour fraude afin de transmettre des messages non sollicités.

La riposte anti -Spam s'affirme

Enjeux et coûts

- Le spam est devenu un gros problème (gêne, nuisance, coûts, possibilité d'actions malveillantes).
- AOL affirme avoir filtré 500 milliards de spam en 2003
- Le spam coûte cher aux entreprises.
- Le coût du spam en 2003 pour les entreprises européennes est estimé à 2,5 milliards par le cabinet Ferris Research et 8,9 milliards pour les entreprises américaines, auquel il faut ajouter 500 millions d'investissement des fournisseurs d'accès pour tenter de faire barrage au spam.

La riposte anti-Spam s'affirme

Sécurité

- Prévention contre les spams porteurs de virus, sensibilisation du personnel aux risques, etc.
- Problème d'atteinte à la vie privée (collecte et utilisation d'adresses emails) et risques d'escroqueries.
- Contenus illicites.
- Atteintes aux mineurs (pornographie, etc.)
- Effets collatéraux : Entraves pour autrui : les noms de domaine empruntés abusivement par des spammeurs qui usurpent des adresses emails d'expéditeurs sont signalés sur une liste noire et les possesseurs légitimes de ces adresses emails usurpées ne peuvent plus envoyer leurs emails sans qu'ils se voient rejetés.

La riposte anti-spam s'affirme

Les spammeurs

- Les destinataires du spam sont ceux qui supportent les plus gros frais, le spam coûte plus cher aux spammés qu'aux spammeurs.

- Le spam rapporte gros aux spammeurs.

Sur des centaines de milliers de messages envoyés, même un faible pourcentage de commandes sont rentables.

- Pour les spammeurs l'investissement est quasiment nul : listes d'adresses emails vendues pas cher : 25 millions d'adresses email pour 25 euros, CD proposés avec plus de 100 millions d'adresses emails pour moins de 100 euros.

La riposte anti-spam s'affirme

Le spam a ses professionnels

Environ 200 personnes seraient à l'origine de 90 % du spam.

Ils peuvent provenir de particuliers ou de sociétés qui ont trouvé là une activité rapidement lucrative.

Ils oeuvrent pour certains sous de faux noms, et se servent de toutes les ressources d'Internet pour rester à l'abri.

Mais il n'est pas impossible de les identifier et d'agir.

La riposte anti-spam s'affirme

Riposte anti-spam

- Initiatives individuelles :

En Russie : en juillet 2003, Andrei Korotkov, Ministre adjoint à la Communication de Russie, à l'initiative d'une mesure gouvernementale pour inciter la population à l'usage d'Internet, devient la cible d'une quarantaine de spams par jour venant de l'école American Language Center, école de formation en anglais à Moscou. Il leur demande de cesser mais les spams continuent. Il décide alors de riposter et de spammer le spammeur. Avec un système d'appel téléphonique automatique, il fait appeler l'école 1000 fois en une matinée et leur diffuse un message pré-enregistré qui leur demande d'arrêter. En retour, il reçoit un e.mail, qui lui répond que les lignes téléphoniques de l'école sont indisponibles mais qu'elle peut être jointe via ICQ.

La riposte anti-spam s'affirme

- Riposte associations d'utilisateurs :

Le site anti-spam Caspam publie une liste de noire d'adresses email spammeuses.

Fin décembre 2003, le site de l'association anti-spam spamhaus a publié une liste noire des plus gros spammeurs du monde : le numéro 1 de la liste détiendrait le record de 70 millions d'emails envoyés en une seule journée. Spamhaus publie aussi la liste des serveurs-relais de spam les plus utilisés, et les pays où ils sont situés, et une liste de moyens techniques utilisés par les spammeurs.

La riposte anti-spam s'affirme

Top 10 ROKSO Spammers

December 2003

- 1 [Alan Ralsky](#)
- 2 [Damon DeCrescenzo - Docdrugs](#)
- 3 [wholesalebandwidth.com](#)
- 4 [Alexey Panov - ckync.com](#)
- 5 [Eddy Marin - Oneroute](#)
- 6 [Eric Reinertsen](#)
- 7 [Juan Garavaglia aka Super-Zonda](#)
- 8 [Scott Richter - Saverealbig.com](#)
- 9 [Webfinity/Dynamic Pipe](#)
- 10 [Angelo Tirico](#)

Source : spamhaus.org

La riposte anti-spam s'affirme

Source : spamhaus.org

Top 10 Spam Countries December 2003

1	<u>United States</u>
2	<u>China</u>
3	<u>South Korea</u>
4	<u>Brazil</u>
5	<u>Argentina</u>
6	<u>Canada</u>
7	<u>Taiwan</u>
8	<u>Russia</u>
9	<u>Italy</u>
10	<u>United Kingdom</u>

Top 10 Worst Spam ISPs December 2003

1	<u>ARIN (direct allocations)</u>
2	<u>uu.net</u>
3	<u>kornet.net</u>
4	<u>telesp.net.br</u>
5	<u>level3.net</u>
6	<u>chinanet-qd</u>
7	<u>above.net</u>
8	<u>chinanet-fj</u>
9	<u>exodus.net</u>
10	<u>interbusiness.it</u>

La riposte anti-spam s'affirme

Riposte juridique

Les sociétés montent au créneau et portent plainte. Plusieurs fournisseurs d'accès internet, comme AOL et EarthLink, ont porté plainte contre des spammeurs. En mai 2003 : au Etats-Unis, le « spammeur de Buffalo », Howard. Carmack est condamné à payer 16,4 millions de dollars de dommages intérêts au fournisseur d'accès EarthLink pour avoir envoyé 825 millions de messages électroniques non sollicités.

En décembre 2003, la société Microsoft a engagé des poursuites contre des sociétés et des personnes qui seraient à l'origine de plusieurs milliards d'envois de spam, notamment les sociétés Synergy6, et Optinrealbig, laquelle serait responsable de l'envoi de 250 millions de spams par jour.

La riposte anti-spam s'affirme

Le dispositif légal se renforce

- Europe : Octobre 2003 : la directive européenne sur la vie privée et les communications électroniques entre en application. Les états membres doivent la transposer dans leur pays.
- Spams : excepté les communications s'inscrivant dans le cadre limité de relations client-fournisseur existantes - la prospection commerciale par courrier électronique n'est autorisée qu'avec le consentement préalable des abonnés (Opt-In). Concerne également les messages SMS et les autres messages électroniques envoyés à des terminaux mobiles et fixes. Il est interdit de camoufler l'identité de l'émetteur ou d'indiquer une adresse d'expédition non valable. Les États membres peuvent aussi interdire l'envoi de messages électroniques non sollicités à des entreprises.

La riposte anti-spam s'affirme

Décembre 2003 : aux Etats-Unis, la première loi nationale anti-spam est promulguée. Elle interdit certaines formes de mails indésirables et prévoit des peines de prison et des amendes de plusieurs millions de dollars pour les contrevenants. Certains Etats avaient déjà des dispositifs et la Californie et la Virginie avaient mis en place des lois anti-spams au cours de l'année 2003.

La loi nationale américaine anti-spam permet néanmoins aux entreprises d'envoyer des messages à n'importe quel titulaire d'une adresse e-mail, tant que ces sociétés s'identifient clairement et cessent de solliciter les consommateurs qui ne le veulent pas (système de l'Opt-Out).

La riposte anti-spam s'affirme

Quelques références

Magazine Expertises.

Agence France Presse , Reuters, Associated Press, Virus Informatique

<http://spamhaus.org>

<http://caspam.org>

<http://pourriel.ca>

http://caspam.org/docs/spam_telus.pdf

http://www.caspam.org/cas_blacklist.php

http://europa.eu.int/information_society

[http://www.zdnet.fr/actualites/technologie/0,39020809,39115493,00.htm?
feed](http://www.zdnet.fr/actualites/technologie/0,39020809,39115493,00.htm?feed)

<http://www.zdnet.fr/actualites/technologie/0,39020809,39135585,00.htm>

<http://www.foruminternet.org/texte/actualites/lire.phtml?id=574&>

<http://vnunet.com/News/1151399>



Phishing : la triple imposture

Les données personnelles et bancaires sont des informations très convoitées par les escrocs. Elles peuvent être obtenues en soudoyant du personnel d'entreprises ou en piratant des bases de données.

Mais une autre méthode permet de les recueillir directement auprès des individus.

C'est la méthode du PHISHING.

Les cas de PHISHING se sont démultipliés en 2003 et font des milliers de victimes.

Phishing : la triple imposture

Phishing : veut dire « fishing » (pêcher) écrit avec le « ph » comme dans le jargon pirate (« phreaking »).

C'est une opération malveillante d'escroquerie qui consiste à lancer un filet – le plus souvent via l'envoi massif d'emails non sollicités et la mise en place de faux sites web - pour aller à la pêche aux données personnelles et financières.

But : obtenir les données sensibles d'autrui, coordonnées de comptes bancaires, cartes bancaires, données personnelles des internautes, afin de commettre des impostures à l'identité et des escroqueries financières.

Le but est le plus souvent lucratif : appât du gain.

Phishing : la triple imposture

Mode opératoire et stratagèmes employés

Le PHISHING joue sur l'illusion et les apparences.

Principe du phishing : une imposture à triple détente.

Première imposture : se faire passer pour qui on n'est pas (une entreprise connue) pour solliciter les données convoitées auprès des internautes.

Deuxième imposture : présenter des contenus fallacieux qui font illusion (motifs évoqués, faux liens, fausses pages web, etc.)

Troisième imposture : une fois les données convoitées recueillies, se faire passer pour qui on n'est pas (les internautes escroqués) pour se procurer des services ou des biens (argent, marchandises, papiers d'identité et autres documents administratifs).

Phishing : la triple imposture

Lancement du filet

Le plus souvent, le phishing s'effectue via le « spam » : envoi massif d'emails non sollicités.

Mais aussi, on assiste à des dissémination par des vers informatiques.

Il est réalisé également via de faux sites web, mis en place pour l'occasion.

Tromper les victimes

Tromperie sur l'expéditeur des emails :

Noms d'expéditeurs faux ou usurpés et usurpation de noms de sociétés connues.

Phishing : la triple imposture

Tromper sur l'émetteur

L'appât du gain étant le principal mobile, les emails prétendent provenir d'entreprises connues et surtout d'établissements bancaires :

EBAY, YAHOO, MSN, HOTMAIL, EARTHLINK et des organismes financiers et bancaires tels que PAYBAL, BARCLAYS, LLYODS TSB, CITIBANK, VISA, BANQUE D'ANGLETERRE, HALIFAX, NATWEST, NATIONWIDE, WESTPAC etc.

Tromper sur le motif - Sujet des emails

Mise à jour de sécurité, changez votre mot de passe, information utilisateur, confirmez vos informations d'enregistrement, réactivez votre compte, etc.

Phishing : la triple imposture

Tromper sur le contenu

Il donne les prétextes et apparences pour inciter les destinataires naïfs à donner tous les renseignements attendus par les escrocs.

Association avec pages web truquées

Ces emails frauduleux sont souvent associés à des pages web truquées , empruntant l'apparence des vrais sites Allant jusqu'à reproduire trait pour trait le graphisme, les logos, la typographie, les interfaces

L'URL des faux sites induisent en erreur (nom ressemblant, nom de l'entreprise inséré, etc.)

Mystification d'URL : URL présentée identique à celle du site web original, alors qu'en réalité la page web présentée est frauduleuse (par exploitation de la faille Microsoft IE6 de décembre 2003 « input validation error »).

Phishing : la triple imposture

Association avec vers informatiques et chevaux de Troie

Amorcé en 2002 avec le ver FISHLET.A, on observe en 2003 que les vers et les chevaux de Troie affirment une tendance forte à jouer un rôle dans les activités de spam et phishing.

Récolte d'adresses emails, localisation de cibles plus précises comme des établissements financiers, utilisation de machines infectées comme relais, présentation de faux écrans de formulaires de récolte de données dans les emails portés par les virus, sont des particularités très significatives qui montrent une convergence entre auteurs de virus, phisseurs et spammers.

Phishing : la triple imposture

Spams préparatoires à des escroqueries (phishing)

Il s'agit de courriers électroniques non sollicités et frauduleux, qui usurpent l'identité de sociétés bien connues, le plus souvent des établissements financiers ou sites d'enchères, pour collecter des données sensibles : renseignements personnels et coordonnées bancaires, dans le but de commettre des escroqueries. De nombreux cas d'envois de spam à but de phishing ont eu lieu en 2003, avec des victimes abusées qui ont vu leurs comptes bancaires débités.

(cf. infra Panorama Cybercriminalité 2003: Spam).

Phishing : la triple imposture

Vers informatiques utilisés pour relais de spam et/ ou attaques de sites anti-spam

2003 : Convergence spam+phishing+vers +chevaux de Troie

- Le ver MIMAIL confirme une prétendue commande de photos pornographiques. L'internaute est avisé qu'il peut contester cette commande en envoyant un mail à un service de réclamation, dont l'adresse n'est autre que celle de sites Internet anti-spam qui se sont vus paralysés suite à cette attaque.
- D'autres variantes de MIMAIL, MIMAIL E et MIMAIL-L déclenchent une attaque pour inonder plusieurs sites anti-spam : Spamhaus.org, SpamCop.net, Spews.org.

(voir infra Panorama de la Cybercriminalité : Virus 2003)

Phishing : la triple imposture

Vers informatiques utilisés pour relais de spam et/ ou attaques de sites anti-spam

2003 : Convergence spam+phishing+vers +chevaux de Troie

- SOBIG.F prépare les machines infectées à devenir des relais d'envois d'emails massifs.
- MIMAIL.I et J contiennent un faux écran de PAYPAL pour collecter les données et les renvoyer à un compte escroc, - -CAYAM affiche un faux écran EBAY, les chevaux de Troie MIGMAF et QHOST peuvent transformer les machines compromises en paravents de sites web escrocs.

(voir infra Panorama de la Cybercriminalité : Virus 2003)

Phishing : la triple imposture

Organisation de la fuite

La page web présentée à l'utilisateur peut être soit hébergée sur serveur dans le pays ou à l'étranger.

Les noms de domaines sont enregistrés sous de faux noms et adresses.

Ou la page web frauduleuse est présentée via un serveur détourné pour l'occasion.

En février 2003, un pirate a utilisé un serveur de l'Université de Caroline du Nord aux Etats-Unis pour envoyer des emails frauduleux se faisant pour EBAY qui demanderait la vérification d'informations personnelles. Il a collecté des données personnelles et sur des cartes bancaires pendant un peu plus de deux heures avant que les techniciens de l'Université remarquent quelque chose d'anormal dans le système informatique et ferme ce serveur.

Phishing : la triple imposture

Où des ordinateurs victimes sont utilisés à leur insu comme relais et paravents, par exemple s'ils ont été préalablement compromis par des chevaux de Troie de type MIGMAF ou QHOST. En effectuant un traceroute pour vérifier la localisation de la page web frauduleuse, la recherche renvoie sur une localisation, quelques secondes plus tard, la même requête donne une autre origine et ainsi de suite. L'enquêteur est balloté à travers un labyrinthe sans fin.

Ces méthodes permettent aux escrocs d'esquiver le retraceage vers eux et noyer les investigations.

Pour entraver les investigations et s'esquiver, les escrocs jouent la montre, en arrêtant le faux site web assez vite, et en en faisant renaître un autre à une autre adresse, et ainsi de suite.

Phishing : la triple imposture

Tout au long de l'année 2003, de très nombreux emails frauduleux prétendus provenir de EBAY sont apparus : Plus d'une soixantaine.

Certains mois, il en arrive une version différente tous les deux jours !

Exemples de titres de ces emails escrocs :

ACCOUNT UPDATE

SECURITY UPDATE

SECURITY MEASURES

OFFICIAL NOTICE

USER ACCOUNT PROTECTION

CONTACT INFORMATION VERIFICATION

UPDATE REGISTRATION INFORMATION

YOUR ACCOUNT WILL BE SUSPENDED

YOUR CREDIT CARD HAS BEEN CHARGED

CHANGE YOUR PASSWORD

CONFIRM YOUR REGISTRATION INFORMATION

Phishing : la triple imposture

Quand ils ne présentent pas directement dans le corps de l'email frauduleux un faux écran de formulaire EBAY, PAYPAL ou autre établissement financier, nombre d'emails de phishing renvoient sur une fausse page web qui imite un formulaire de EBAY.

Une version de cette escroquerie apparue début octobre demande par email au destinataire

- sous prétexte de prévenir la fraude -

de se rendre sur une page web de EBAY, en réalité, une fausse page où se trouve un formulaire en tous points similaire à celui utilisé par la vraie société EBAY et d'y entrer toutes ses coordonnées personnelles.

Phishing : la triple imposture

Dear eBay user.

At 10.09.2003 the eBay company has blocked a number of accounts in the system connected with money laundering and credit card fraud activity. The information in regards to those accounts has been passed to our corresponded banks, local and international authorities.

Due to database operations some accounts can be lost. We are insisting to our clients to update their account's information.

If you will find any presence of fraudulent activities at your account - let us know immediately at e-mail anti-fraud@ebay.com
Don't wait until criminals will steal your money - help the authorities to block their accounts.

To update your account's information please click on the link below. Thank you.

<https://cgi.ebay.com/saw-cgi/eBay/SAPI.dll?UpdateInformation>

Phishing : la triple imposture



Dear valued costumer,

eBay's acquisition of PayPal was completed on August 3, 2003. As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website , we are undertaking a period review of our member accounts. You are requested to visit our site by following the link given below ,


<https://cgi4.ebay.com/aw-cgi/eBayISAPI.dll?UserVerify>

This message was sent to you courtesy of eBay's computerized e-mail system. Please do not send a reply to this message, as it will vanish into the mysterious electronic void. If you have a question or some input, and would like a response from a live, caring human being, please e-mail us at info@eBay.com.

Copyright © 1995-2003 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

Phishing : la triple imposture

Address <http://verify.us.ebay.com/Secure-Signin/ebay/SAFtdllUse/Verify/verify-account.dll/index.html>



[Browse](#) | [Sell](#) | [Services](#) | [Search](#) | [Help](#) | [Community](#)

1 Verify your identity

Your credit/debit card and bank account information along with your personal information will be verified instantly. All the data is protected by the industry standard [SSL](#) encryption. All information is required and is kept confidential in accordance with [eBay's Privacy Policy](#).

- Your credit/debit card and checking account information is used to verify your identity.

Enter Your Ebay Information

Ebay User ID

Password

PayPal Password

Email Address

Enter Your Credit Card/Debit Card Information

Credit card/debit card number Credit Card: Visa, MasterCard, American Express, Discover.
Debit Card: Visa, MasterCard.

Expiration date **Month:** **Day:** **Year:**
Leave day as --, if day on credit/debit card is not listed

CVV Code 3 Digit code at the back of your card; next to signature

Your name on card

Please enter your billing address as it appears on your credit card bill statement:

Billing address

Primary telephone ()

Secondary telephone ()

City

State/province

Phishing : la triple imposture

Dans l'un des emails frauduleux, L'URL qui apparaît dans la barre d'adresses quand on se rend sur le faux site est n'appartient pas à EBAY, mais est enregistrée sous le nom d'un particulier aux Etats-Unis à Plaquemine, Los Angeles et hébergée par YAHOO.COM.

Contrairement à ce qu'en disent certains spécialistes, il n'est pas du tout évident pour tout un chacun de se rendre compte que cette URL prétendue être celle d'un service EBAY est fausse.

Phishing : la triple imposture

Décembre 2003 :

Email qui prétend provenir de la Banque Llyod TSB et demande au destinataire de redonner ses coordonnées en invoquant une mise à jour ou un changement des mesures de sécurité.

L'email procure un lien qui mène à un faux site web prétendu être celui de la banque.

En réalité, le serveur qui héberge ce faux site est situé au Japon.

Phishing : la triple imposture



Lloyds TSB online for business

Dear Valued Customer,

- our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.
- Due to technical update we recommend you to reactivate your account.

Click on the link below to login and begin using your updated Lloyds account.

To log into your account, please visit the Lloyds online Banking <https://online.lloydstsb.co.uk/>

For business banking login here <https://online-business.lloydstsb.co.uk/customer.ibc>

If you have questions about your online statement, please send us a Bank Mail or call us at 0846 600 2323 (outside the UK dial +44 247 686 2063).

We appreciate your business. It's truly our pleasure to serve you.

Lloyds Customer Care

This email is for notification only. To contact us, please log into your account and send a Bank Mail.

Phishing : la triple imposture

Fin Octobre 2003 :

Méthode très vicieuse :

Email « Verification » en anglais prétend venir de la **Barclay's Bank**, adresse expéditeur :

affirme vouloir vérifier l'adresse email du destinataire – client ,

contient un lien truqué vers le vrai site de la Barclays qui affiche un pop up par dessus la page du site de la Banque.

Le pop-up demande le numéro de membre de la Banque, le mot de passe.

Lorsque le destinataire naif a rempli et validé les informations qu'il a entrées dans le pop-up, les données sont envoyées au compte email escroc géré par un serveur en Russie.

Dans d'autres cas, les données sont envoyées à autre adresse de serveur aux Etats Unis.

Phishing : la triple imposture

Address <http://www.personal.barclays.co.uk/BRC1/jsp/brocontrol?site=pls>

Barclays.com | Important Info | Privacy Policy | Security | Site Map | Contact Us | Accessibility | Help

Home

Personal Banking

Browse & buy
 Current accounts
 Savings & investments
 Loans & borrowing
 Barclaycard
 Mortgages
 Openplan
 Insurance
 Protection & pensions
 Platinum Banking
 Students & graduates

Focus on
 Buying a home
 Travel services

Access our services
 Online Banking
 Other ways to bank

Need help?
 Info Centre
 Ask the Expert
 Glossary

Welcome to Barclays Internet Banking

Please enter your Surname:

Please enter your membership number: 2010

Please enter your five-digit passcode:

Please enter your memorable word:

Get a personal loan at a personal rate: Rates from as low as 7.9% (typical APR 9.9%) [Apply for a Barclayloan](#)

Debit & credit cards are changing: How Chip & PIN is [fighting the fraudsters](#)

A great package in our Additions account with [£544 of benefits](#)

Phishing : la triple imposture

La même méthode est employée en novembre 2003 pour emails prétenus provenir de CITIBANK :



Address <http://www.citibank.com/us/index.htm>

sign on • open account • contact us • search

citi PRODUCTS & SERVICES PLANNING & TOOLS INVESTING & MARKETS HELP DESK

Welcome to Citibank

Ready to remodel? A Home Equity Line of Credit

sign on to your Citibank

Choose or

learn / take a t

apply / open an

Jump to

Small Bus

Corporate

select a cos

United Sts

There are r

Apply for a

look for a product or service

Choose one

learn at

Choose

smartdeals

Introducing the new Citibank® Access Account

No checks, no hassles. Just more online convenience.

details

Bank

sign on to Citibank with your Citibank® Banking Card

Full Debit Card Number

PIN (4-6 digits, ~ ATM PIN)

Card Expiration Date (mm/yyyy)

sign on

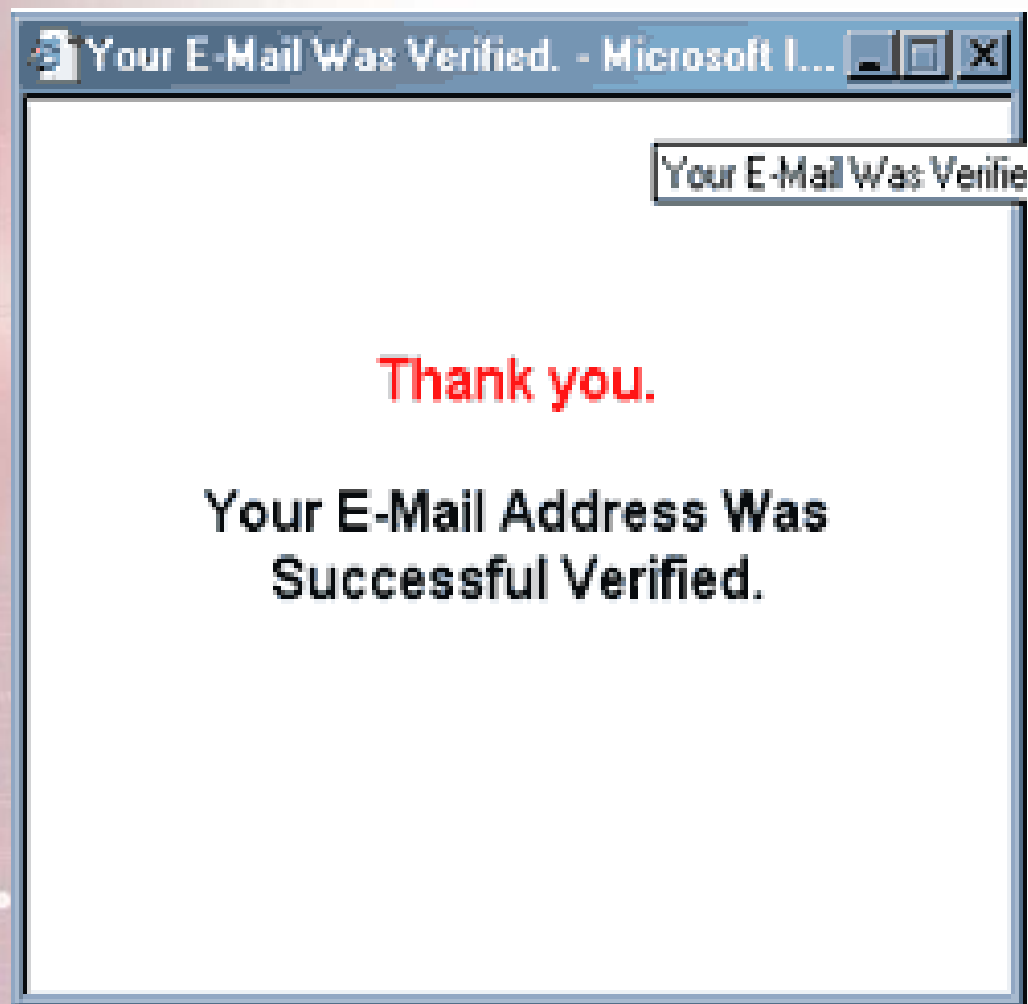
Welcome

[about e-mail fraud](#) | [about us](#) | [careers](#)

Citi.com is the source of information about domestic financial services provided by the Citigroup family of companies N.A., Citibank (West), FSB, Citibank, F.S.B. Member FDIC.

citi Citi.com

Phishing : la triple imposture



Phishing : la triple imposture

Novembre 2003 :

Emails frauduleux prétendus venir de **MSN** et **HOTMAIL**

Pour inciter le destinataire à fournir ses informations personnelles, le texte de l'email prétend que quelqu'un a essayé de corrompre le compte utilisateur du destinataire, et qu'il lui est donc demandé de redonner ses informations personnelles, en remplissant le formulaire situé à l'adresse du lien fourni dans l'email.

Phishing : la triple imposture

: Dear MSN User,

It has become noticeable that another party has been trying to corrupt your MSN account and has violated our User Agreement policy listed:

1. PERSONAL AND NON-COMMERCIAL USE LIMITATION

Unless otherwise specified, the MSN Sites/Services are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, or sell any information, software, products or services obtained from the MSN Sites/Services.

You received this notice from MSN because a website was bought fraudulently and it has come to our attention that your account may cause interruptions with other MSN members and MSN requires immediate verification for your account. Please verify your account or the account may become disabled. please [Click here to verify](#)

Sincerely,

Mike Jones

MSN Fraud Department

Case Number :NL1FB0

Phishing : la triple imposture

Lien qui renvoie vers une URL :

[http:// beam.to/MSNSecurity](http://beam.to/MSNSecurity)

fausse page MSN, hébergée sur des serveurs en Chine, mais qui présente un formulaire de MSN lui ressemblant trait pour trait, copie complète du formulaire original.

S'il cède au message, l'utilisateur va ainsi fournir son nom, adresse, numéro de carte bancaire, son numéro de sécurité sociale, le nom de jeune fille de sa mère, son numéro de permis de conduire etc etc.

Ces informations sont transmises aux escrocs via le formulaire de service email neveru.nl pendant que l'utilisateur est détourné vers une authentique page MSN et HOTMAIL.

Phishing : la triple imposture

Décembre 2003 : un email prétendu venir de **VISA INTERNATIONAL Service** affirme que VISA a mis en place un nouveau système de sécurité pour « vous aider à éviter les actions frauduleuses » et invite l'utilisateur à cliquer sur un lien pour « réactiver votre compte ».

Le lien renvoie sur l'adresse du site officiel de VISA INTERNATIONAL.

En apparence seulement, car en réalité, le lien est codé de manière à pointer sur une adresse qui n'appartient pas à VISA. Le site frauduleux a été fermé, mais il n'est pas écarté qu'il en ressurgisse d'autres ailleurs.

Phishing : la triple imposture

PHISHING : Une forme d'escroquerie de plus en plus répandue

Cette forme de malveillance est de plus en plus répandue et pose de gros problèmes.

Le vol d'identité prend des proportions colossales : le chiffre de 17 millions d'identités volées est avancé en ce moment rien qu'aux Etats-Unis.

La convergence observée des techniques SPAM+ PHISHING + VERS INFORMATIQUES + CHEVAUX DE TROIE est de nature à démultiplier le potentiel du risque.

Les emails frauduleux de PHISHING ont des apparences convaincantes et un contenu également convaincant susceptibles de duper de très nombreuses personnes.

40 % des destinataires de l'email prétendu venir de la CITIBANK seraient tombés dans le panneau.

Phishing : la triple imposture

Le phénomène pose le problème de la responsabilité de l'utilisateur qui va donner lui-même les informations sensibles pour se voir escroqué par la suite.

En Australie et en Nouvelle Zelande, la banque **WESTPAC** visée par une opération de phishing en décembre 2003, a émis un communiqué pour dire que les victimes étaient responsables parce que c'était elles-mêmes qui avaient donné les informations sensibles.

Le phishing est coûteux pour les victimes, particuliers et banques.

En octobre 2003, la Banque **HALIFAX** a dû interrompre l'activité de son site web à cause d'une opération de phishing visant ses clients. HALIFAX aurait identifié la réplique pirate de son site web en Russie.

Phishing : la triple imposture

- Le phishing est rentable pour les escrocs : sur plusieurs millions d'emails envoyés, il suffit d'une très faible proportion d'internautes qui tombent dans le piège pour rentabiliser l'opération.
- Pour les escrocs, le phishing est relativement facile à mettre en place.
Ils se servent de toutes les ressources d'Internet pour opérer.
- Le phishing repose sur l'imposture et est le prélude à d'autres impostures et escroqueries.
- Le phishing s'appuie sur la crédulité des internautes.
- Il se sert des possibilités techniques d'illusion et d'évasion sur Internet.

Phishing : la triple imposture

- La prévention par la sensibilisation à ce risque est la plus importante mesure à prendre.
- Il est nécessaire de signaler le plus rapidement possible la tentative d'escroquerie ou l'escroquerie, en conservant les emails frauduleux avec toutes leurs en-têtes techniques.
- **La Bank of America Corporation** victime d'une opération de phishing en mai 2003 a réagi assez vite en informant ses clients de la présence d'un " mouchard " frauduleux sur son propre site. Des emails frauduleux incitaient les utilisateurs à se connecter à un faux site ressemblant à l'original. Le site frauduleux a pu être fermé 13 heures après la découverte de son existence et seul un faible nombre de comptes auraient été touchés dans l'opération.

Phishing : la triple imposture

- En juillet 2003, un jeune homme de 17 ans résidant à Washington a été arrêté pour avoir effectué une opération de phishing, dans laquelle il est soupçonné de s'être procuré les données personnelles de tiers sous prétexte d'une demande de mise à jour des informations de comptes utilisateurs par AOL.
- En septembre 2003, un homme a été arrêté en Roumanie pour une escroquerie utilisant le phishing qui a coûté 500.000 dollars aux utilisateurs de comptes du site d'enchères EBAY.
- le FBI dit recevoir 9 000 plaintes par mois pour des faux emails et faux sites web.

Phishing : la triple imposture

Quelques références

Agence France Presse, Reuters

<http://www.millersmiles.co.uk/identitytheft/spoof-email-hoax-scam-archive-1.php>

Nouvelles opportunités d'espionnage *hi-tech*

Disque dur des photocopieurs

- Décembre 2003 : une société norvégienne, spécialisée dans la récupération des données, publie une enquête qui souligne la vulnérabilité des informations stockées sur les copieurs et machine multifonction. L'affaire commence par un salarié indélicat qui récupérait les informations d'un copieur numérique pour les passer à une société concurrente. De plus en plus de copieurs sont ainsi exposés. Toutefois, différentes solutions sont proposées : disque amovible, effacement (mais pas surécriture...) des données après photocopie ou numérisation, emploi d'algorithmes propriétaires de traitement (mais cela ne signifie pas chiffrement...), etc.

Nouvelles opportunités d'espionnage *hi-tech*

Extension de la problématique : sécurité des périphériques (imprimantes, photocopieurs)

- Janvier 2003 : étude du MIT sur l'absence d'effacement des informations sur les supports revendus d'occasion. Budget de 1 000 dollars pour acheter des supports d'occasion sur un site d'enchères. 158 disques achetés, seulement 12 correctement effacés. Un disque, vraisemblablement utilisé dans un distributeur de billets (Illinois), contenait 5 000 numéros de cartes de crédit.

Nouvelles opportunités d'espionnage *hi-tech*

Extension de la problématique : sécurité des périphériques (imprimantes, photocopieurs)

- Spécialisation de hackers dans l'attaque des « embedded systems ». Le groupe *Phenoelit* fait régulièrement des présentations et démonstrations sur les opportunités de compromission des imprimantes et des périphériques numériques.

D'une part en raison des informations accessibles et d'autre part, pour les opportunités d'exploitations des ressources TCP/IP dans le cadre du périphérique mis en réseau.

Plusieurs virus, dont CodeRed, se sont appuyés sur de telles ressources pour leur propagation.

Nouvelles opportunités d'espionnage *hi-tech*

Supports de stockage portables (clef USB, iPOD, lecteur MP3)

- Février 2002 : un adolescent utilise son iPOD pour «aspirer» un logiciel Office pour MacOS X dans une boutique (Dallas, E-U). La technologie FireWire lui permet de réaliser sa copie en quelques minutes. La vitesse de transmission sur une clef USB est inférieure mais l'emploi de cet équipement est déjà évoqué lors de conférences de hackers pour installer des programmes ou récupérer des informations.

Nouvelles opportunités d'espionnage *hi-tech*

GSM-appareil photo

- Juillet 2003 : les nouvelles générations de téléphones GSM permettent la prise de vue et son envoi. Problématique de confidentialité, dans un contexte professionnelle, ou d'atteinte à la vie privée (gymnases, écoles, musées, kiosques à journaux, etc.)

Face à cette menace, plusieurs solutions sont évoquées : interdiction d'emploi sur certains lieux (de l'entreprise), y compris par les salariés; appareils générant un son particulier lors de la prise de vue.

Nouvelles opportunités d'espionnage *hi-tech*

Conclusions

Il est normal d'utiliser une ressource (performante) donc, pas de catastrophisme ! Il faut prendre en considération la spécificité de l'équipement.

Toute nouvelle ressource peut (va) générer un emploi malveillant (détournement d'usage, effet de bord)

Toute nouvelle ressource porte un risque intrinsèque

- Par exemple, pour la messagerie électronique :
 - Perte de hiérarchie
 - Risque de *bombing* (saturation ou déni de service sur le courrier électronique)
 - Divulgation accidentelle (CC et *reply-to*, affaire M. Lewinsky)

Nouvelles opportunités d'espionnage *hi-tech*

Quelques références

- <http://www.01net.com/article/224701.html>
- <http://www.zdnet.fr/actualites/technologie/0,39020809,39133986,00.htm>
- <http://web.mit.edu/newsoffice/nr/2003/diskdrives.html>
- <http://www.silicon.fr/getarticle.asp?ID=1752>
- <http://www2.canoe.com/techno/nouvelles/archives/2003/12/20031229-095518.html>
- <http://www.defcon.org/html/links/defcon-media-archives.html#defcon-11>

Pour terminer

Nous aurions aussi aimé évoquer...

- Nouvelles extorsions
- Impact économique des attaques contre la NGage
- Cyber-terrorisme, de quoi parle-t-on ?