

**Chaque JOUR**, le site [www.bichard.com](http://www.bichard.com)  
Chaque vendredi [NetCost&Security HEBDO](#)  
sur votre Email et *Palm™ Pilot* avec les liens HTML

4 offres pour recevoir [NetCost&Security](#)

*NetCost&Security Hebdo #26 : 2000-05-05*

1	- CONFIDENTIEL : <a href="#">JEAN-PHILIPPE BICHARD / NETCOST&amp;SECURITY</a> .....	1
2	- ABONNEMENT : 4 OFFRES POUR RECEVOIR <a href="#">NETCOST&amp;SECURITY</a> .....	2
3	- L'INFO DE LA SEMAINE : SPÉCIAL VIRUS ILOVEYOU.....	3
4	- LES INDISCRÉTIONS DE NETCOST&SECURITY : .....	6
5	- ANALYSE : COMPTE-RENDU DE LA CONFÉRENCE SANS 2000 PAR HERVÉ SCHAUER, DENIS DUCAMP ET GILLES GUIOT .....	7
6	- VEILLE ATTAQUES : <a href="#">OLIVIER CALEFF / APOGEE COMMUNICATIONS</a> ..	12
7	- ACTUALITÉS .....	13
8	- SOLUTIONS : LES OFFRES SÉLECTIONNÉES PAR LA RÉDACTION .....	13

[1 - CONFIDENTIEL : Jean-Philippe Bichard / NetCost&Security](#)

**EDITO : Jean-Philippe Bichard**

**Cybercrime : peu de chiffres mais beaucoup de menaces**

Le ministère de l'Intérieur a rendu public cette semaine son analyse touchant aux infractions et délits recensés en 1999 par la Direction centrale de la police judiciaire (DCPJ) qui s'appuie sur les chiffres de la Police Judiciaire et ceux de la Gendarmerie Nationale. Quel crédit accorder à ces données ? Ainsi, le piratage informatique ne représente que 9% de l'ensemble des délits. Certes les principaux délits ne sont pas connus, donc pas recensés. Reste que la mise en place des réformes en matière de cybercriminalité promises par le Premier Ministre est attendue avec impatience par certains services officiels. Le traditionnel discours de Hourtin durant l'été devrait faire avancer les choses...

*[Jean-Philippe Bichard](#)*  
*[netcost@bichard.com](mailto:netcost@bichard.com)*

**2 - ABONNEMENT : 4 offres pour recevoir NetCost&Security**

**Des offres personnalisées pour bénéficier d'une veille SECUR en français**

- Je souscris un abonnement COMPLET pour un an (soit 40 numéros NetCost&Security HEBDO sur mon Email + 4 suppléments papiers trimestriels NetCost&Security MAGAZINE au prix de 3900 FRF TTC
- Je souhaite recevoir UNIQUEMENT NetCost&Security HEBDO par **Émail** (Acrobat/PDF & PalmPilot™/iSilo) au prix de 3000 FRF TTC :
- Je souhaite recevoir UNIQUEMENT les 4 numéros trimestriels NetCost&Security MAGAZINE au prix de 900 FRF TTC :
- Je souhaite recevoir 1 numéro trimestriel au prix de 250 FRF TTC :

**DEMANDE D'ABONNEMENT NetCost&Security**

Nom - Prénom : .....  
Fonction : .....  
Société ou organisme : .....  
Activité : .....  
Adresse : .....  
Code postal : ..... Ville : .....  
Tél. : ..... Email : .....@.....

- Je paie par chèque bancaire ci-joint à l'ordre de **Bichard Corp.** : .....
- Adressez-moi une facture acquittée : .....
- Je règle à réception de votre facture : .....

**Réception par Email** : Adresse de messagerie sur Internet :  
.....@.....

- Bulletin à compléter et à retourner à :**
- NetCost&Security, 3<sup>ter</sup> rue Georges Bizet, 78380 Bougival, France
  - ou par fax au : + 33 (0) 01 39 69 06 16
  - ou par Email à : netcost@bichard.com

© Copyright Bichard Corp. 2000 - tous droits réservés.  
*Pour joindre la rédaction en cas d'urgence ! 06 09 61 84 68*

**Bonne lecture "SECUR"**  
**Prochain numéro Hebdo sur votre Email : Vendredi 12 Mai 2000**  
**Chaque trimestre, la revue NetCost&Security MAGAZINE :**  
**analyses, reportages, marchés, solutions, projets SECUR...**  
**prochain numéro Mai 2000**

**3 - L'info de la semaine : spécial virus ILOVEYOU**

**Jeudi 4 mai, jour du bouclage de *NetCost&Security* HEBDO, le virus ILOVEYOU endommage de nombreux sites. *NetCost&Security* a immédiatement produit un numéro spécial pour informer ces lecteurs vers 19 h 30 jeudi soir. Nous développons dans cette rubrique l'essentiel sur ce virus avec plusieurs éditeurs de solutions anti-virales.**

ILOVEYOU est un ver en Script VB, d'une taille de 10Ko (10337 Bytes), susceptible de provenir des Philippines.

Le virus infecte les applications : Microsoft Outlook, miRC, Internet explorer, et les fichiers .vbs, .js, .jse, .css, .wsh, .sct .hta, .jpg, .jpeg, .mp3 ou .mp2

Il se déploie par un mail sous OUTLOOK :

Sujet : ILOVEYOU

Corps : 'kindly check the attached LOVELETTER coming from me'

(*nous vous saurions gré de contrôler le LOVELETTER ci-joint venant de moi.*)

Pièce jointe : LOVE-LETTER-FOR-YOU.TXT.VBS

Si vous n'utilisez pas Outlook, le virus se comportera comme un Ver mIRC.

Pour éviter l'infection ne pas ouvrir le fichier attaché.

Protégez-vous en désactivant l'option d'activation des scripts de Internet Explorer.

**INFECTION:**

Le virus crée dans le dossier : *windows\system* :

- MSKernel32.vbs - LOVE-LETTER-FOR-YOU.TXT.vbs

et dans le dossier *Windows*:

- Win32DLL.vbs

Puis il ajoute dans la base de registre, les clefs :

*HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32*

*HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL*

Le ver remplace la page de démarrage d'Internet Explorer par un lien qui le dirige sur le site *http://www.skyinet.net/* d'où il télécharge un programme exécutable, "*WIN-BUGSFIX.exe*"

Lors du téléchargement, le ver modifie la base des registres:

*HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX*

(Exécuté au prochain démarrage du système)

*HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\Start Page", "about:blank"*  
(Page blanche au démarrage d'Internet explorer)

Le ver crée un fichier HTML, "*LOVE-LETTER-FOR-YOU.HTM*" qui contient le ver, dans *WINDOWS\SYSTEM*  
Il s'autoenvoie en utilisant mIRC lors des utilisations du canal IRC par un *send DCC* en joignant *LOVE-LETTER-FOR-YOU.HTM*.

Le ver s'auto-envoie à toutes les adresses du carnet d'adresses de OUTLOOK.

Le message est :

*Objet: ILOVEYOU*

*Body: kindly check the attached LOVELETTER coming from me.*

*Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs*

Le ver envoie le courrier une seule fois à chaque destinataire.  
Lorsque le courrier est envoyé, un repère est ajouté dans la base des registres pour éviter une réexpédition.

Le virus recherche des fichiers dans tous les dossiers locaux et réseaux.  
Les fichiers avec l'extension "vbs" or "vbe" sont effacées.  
Les fichiers avec les extensions : ".js", ".jse", ".css", ".wsh", ".sct" et ".hta",  
Le virus crée un nouveau fichier avec le même nom, mais en utilisant l'extension "vbs".  
Le fichier initial est effacé.  
La double extension permet de ne pas supprimer les associations.  
Le virus localise les fichiers .jpg, .jpeg, .mp3, .mpeg et .mp2.  
Il ajoute un nouveau fichier et efface le fichier initial.  
Par exemple, une image nommée "pics.jpg " causera un nouveau fichier appelé "pics.jpg.vbs" et l'effacement de pics.jpg.

LoveLetter a été détecté le 4 mai, 2000.

Pour en savoir plus :

<http://2.digital.cnet.com/cgi-bin2/flo?x=dAEuAuBmmKwKhAhuK>

<http://2.digital.cnet.com/cgi-bin2/flo?x=dAEuAuBmmKwKhAKuB>

<http://www.trendmicro.fr/presse>

TREND MICRO ANNONCE LA DECOUVERTE DE L'ANTIDOTE POUR LE VIRUS I LOVE YOU

Trend Micro, spécialiste international sur le marché des logiciels de protection virale pour réseaux, messageries électroniques, Internet et intranet annonce la

disponibilité d'une protection contre le nouveau virus ILOVEYOU qui à la manière de Melissa est un mass-mailer mais à diffusion beaucoup plus rapide que celle de Melissa.

En effet, Trend Micro a reçu de très nombreux appels provenant de clients infectés par ce nouveau virus et à la suite de la réception du premier échantillon aujourd'hui à 11 heures, le laboratoire de Trend Micro France a trouvé un antidote à 11h15. Cet antidote est disponible pour tous sur le site Internet : [www.trendmicro.fr](http://www.trendmicro.fr).

Le virus se présente sous la forme d'une pièce attachée à un mail au titre évocateur : ILOVEYOU. La pièce jointe s'appelle : LOVE-LETTER-FOR-YOU.TXT.vbs. Le texte joint : Kindly check the attached LOVELETTER coming from me.

Dans ce contexte, Trend Micro recommande donc à l'ensemble de ses clients de mettre à jour leurs logiciels avec le nouveau fichier de signatures virales appelé : 4may2k\_REDALERT\_03.zip

### **Comment réduire les risques d'infection**

Trend Micro recommande aux utilisateurs d'être très prudents lors de l'ouverture des fichiers joints dont l'objet est « ILOVEYOU ».

Symantec conseille pour sa part :

COMMENT REPARER LE VIRUS ?

1. Supprimer tous les fichiers infectés.
2. Supprimer la clef de la base de registre suivante :

HKLM/software/Microsoft/Windows/Current Version/Run/WIN-BUGSFIX

COMMENT SE PROTEGER ?

Les utilisateurs de Norton Anti-Virus sont protégés contre ce virus depuis le 4 mai 2000.

NORTON ANTI VIRUS UNE MISE A JOUR RAPIDE ET PERMANENTE

Les utilisateurs de Norton Anti-Virus peuvent mettre à jour leur logiciel Anti Virus rapidement et simplement via modem ou Internet d'un simple clic sur la fonction LiveUpdate. Les définitions seront récupérées et installées automatiquement. Il est recommandé d'effectuer cette opération au moins une fois par semaine.

Les utilisateurs peuvent aussi récupérer manuellement la définition sur le site FTP suivant :

[ftp://ftp.symantec.com/public/english\\_us\\_Canada/antivirus\\_definitions/norton\\_antivirus/specdef](ftp://ftp.symantec.com/public/english_us_Canada/antivirus_definitions/norton_antivirus/specdef)

**Fin de notre rubrique SPECIAL ILOVEYOU**

**4 - Les indiscretions de NetCost&Security :****▪ Fin d'une histoire entre Compaq Corp et Apogée Communications**

Compaq Corporate et Apogée Communications ne se sentent plus des âmes de jeunes mariés. Le mariage annoncé fin mars ne se fera pas officiellement "pour raisons techniques". Quelles raisons ? Quelles techniques ? Mécanismes financiers, mésentente des managers, problèmes avec les partenaires ? Difficile à savoir. Les deux parties ayant décidé de communiquer par le ... silence ! Pourquoi pas ? Les télécoms n'ont rien à voir avec le show-business bien que... En revanche, le flirt persiste entre Apogée Communications et la filiale française de Compaq. La Corporate bien qu'officiellement informée semble dépassée par cette "love story française" dédiée au marché du "Professional Service".

**▪ Accord Compaq et IBM**

La société d'investissement Safeguard Scientifics Inc a annoncé lundi 1<sup>er</sup> mai avoir reçu 50 millions de dollars de Compaq Computer Corp et d'International Business Machines Corp avec qui elle a noué des relations stratégiques.

**▪ Alain Tingaud va introduire InfoVista simultanément sur les bourses américaines et européennes**

MSP : manager service provider, c'est la nouvelle vogue venue des US. Alain Tingaud, P-DG fondateurs de plusieurs Start-up (Arche Communication, InfoVista) se lance dans une nouvelle aventure avec Clariteam (qualité de service). Il vient d'installer simultanément en Grande Bretagne, France, et Allemagne ces filiales. Le service "operating center" est opérationnel GB. Selon Alain Tingaud, de nouveaux services s'imposent tels que l'administration d'indicateurs de qualité de service à distance vus de l'application. Exemple : les brokers on line. Quelles performances pour quels services vu de l'utilisateur ? Et quelles solutions proposées pour optimiser ces services ?

Coté Infovista qui revend des solutions aux entreprises, c'est l'actualité financière qui occupe la scène avec une prochaine introduction en bourse simultanément sur le Nasdaq et en Europe. InfoVista réalise 40% de son chiffre d'affaires aux États-Unis et va ouvrir une filiale à Singapour. Près de 60% du chiffre d'affaires est réalisé par les ventes aux ISP et Telco. La société est passée de 30 à 140 collaborateurs en un an. Alain Tingaud met l'accent sur les partenariats à l'échelle mondiale et notamment avec CISCO autour du protocole NetFlow (retour d'analyse à partir des protocoles CISCO) et SAA intégrés dans les routes pour la gestion des applications. En juin d'autres accords seront annoncés.

**▪ ODS devient Intrusion.com en migrant de l'ATM vers la sécurité**

ODS Network se baptise désormais Intrusion.com et se positionne sur la détection d'intrusion avec sa plate forme SECUR COM dédiées aux ISP. Signature avec RISC techno, Newlink et Softway prochainement affirme Marius

Bratan, P-DG Europe de la nouvelle structure. Il vise 1 milliard de dollars de capitalisation avec un CA de 60 millions de dollars en sécurité sur 80 millions de dollars au total. L'Europe devrait réaliser au moins 20% de ce chiffre d'affaires sur ce nouveau marché SECUR. Au catalogue d'Intrusion.com, des outils de détection d'intrusion : KSE (Kane Security Entreprise) et d'analyse de vulnérabilité (NT Netware Unix à venir) avec Kane Security Analyst.

## **5 - Analyse : compte-rendu de la conférence SANS 2000 par Hervé Schauer, Denis Ducamp et Gilles Guiot**

La conférence SANS : System Administration, Networking & Security (<http://www.sans.org>) qui s'est déroulée du 21 au 28 Mars 2000 à Orlando en Floride a bénéficié d'une affluence record, avec plus de 2400 participants et 59 exposants. Une affluence internationale aussi puisque pas moins de 36 pays étaient représentés.

### ▪ **Détection d'Intrusion**

L'ensemble des instructeurs restent focalisés sur la détection d'intrusion sur les réseaux, même si SANS couvre aussi bien la sécurité Unix que Windows, ainsi que les réseaux en général, de la commutation à Sendmail en passant par le DNS.

Il demeure cependant un fossé entre les spécialistes des réseaux comme Allan Leinwand et ceux de la sécurité : Les premiers ont du mal à accepter la sécurité comme étant une fonction intrinsèque du réseau, et la perçoivent comme une facteur de dégradation des performances du réseau.

Avec la version actualisée de son tutoriel "IP for Intrusion Detection" Stephen Northcutt a fait salle comble. Succès mérité puisque ses transparents étaient d'une grande qualité, notamment dans les explications sur la fragmentation.

La préoccupation majeure des participants semblait être les IDS réseaux, et la détection de tous les types de scans et d'attaques. Certains comme Steve Schall et Richard Bejtlich se démarquaient en rappelant les qualités des IDS systèmes et en fournissant une définition d'un véritable scan.

### ▪ **Le logiciel SNORT (<http://www.clark.net/~roesch/security.html>)**

Snort (<http://www.clark.net/~roesch/security.html>), écrit par Martin Roesch <roesch@clark.net> est le logiciel de détection d'intrusion open source le plus léger. Il repose sur l'utilisation d'une base de signatures.

Étant peu gourmand en ressources, un Pentium 83 suffit pour faire fonctionner simultanément trois occurrences du logiciel, et permettre ainsi la surveillance d'une LS modeste. SNORT autorise également la surveillance d'un réseau 100Mbit fonctionnant au maximum de ses capacités à condition de désactiver la détection de scans de ports.

Ces qualités ont incité un grand nombre de testeurs et de développeurs très actifs tels que Martin Roesh, Fyodor (CyberPsychotic), Patrick Mullen et tant d'autres à le porter sous de nombreux systèmes tels que : Linux, OpenBSD, FreeBSD, NetBSD, Solaris, SunOS 4.1.X, HP-UX, AIX, IRIX, Tru64 ou encore MacOS X Server.

SNORT bénéficie d'une architecture modulaire comprenant :

- . Les modules preprocessors, en charge de l'examen et de la manipulation des paquets
- . Les modules de détection : chacun ne fait qu'un test simple sur un paramètre précis d'un paquet (TTL, ID, Flags, Ack, Seq, ..., content, ...)
- . Les modules de sortie : fichier alerte, syslog, tcpdump, Winpopup SMB

Le fichier de configuration est composé de règles, chacune d'entre elles comportant deux parties :

- . L'entête : spécifie les filtrages sur les adresses, les ports sources et destinations, ainsi que la direction et l'action (alert, pass, log)
- . Une combinaison de modules de détection

Parmi les pré-processeurs qui sont aujourd'hui en standard :

- . détection de scans de ports
- . normalisation du protocole HTTP (%41 -> A)
- . détection de fragments (trop) petits

En cours de développement :

- . défragmentation IP
- . analyse de trafic ICMP pour détecter les canaux cachés
- . activation / désactivation dynamique de règles
- . changement d'identité et restriction dans une cage (chroot)

Un module de réponse active est disponible mais n'est à utiliser qu'avec beaucoup d'attention. Il a par ailleurs déjà prouvé son efficacité contre la détection d'OS par nmap.

Si les bibliothèques fournies en standard sont un très bon point de départ, d'autres sont disponibles sur :

- . la base arachNIDS par Max Vision : <http://dev.whitehats.com/ids/>
- . la base rapidnet par Jim Foster : <http://snort.rapidnet.com/>

Il est vrai que les possibilités de fausses alertes sont nombreuses, mais les NIDS ne sont que des "antivirus réseaux" et n'ont encore que peu d'années d'expériences.

Au final, s'il manque encore quelques fonctionnalités comme la reconstruction de flux TCP, SNORT se révèle cependant excellent à l'accomplissement de toutes les tâches pour lesquelles il a été conçu.

**▪ Sécurité réseau distribuée (Distributed Network Security)**

La sécurité réseau distribuée représente l'avenir de la sécurité des réseaux. Telle était la thèse défendue par Hervé Schauer, qui offrait de nombreux arguments à l'appui :

- Demain, chaque utilisateur aura une adresse IP : filtrer les adresses IP aujourd'hui permettra demain de faire de la sécurité au niveau des utilisateurs.
- Les IDS ne peuvent empêcher les dénis de service. Quand l'IDS s'aperçoit qu'un paquet malicieux arrive, il est déjà passé...
- L'impact sur les utilisateurs est nul, seuls les pirates auront conscience des restrictions.
- Il est irréaliste de vouloir sécuriser plusieurs centaines de serveurs parfaitement, seuls les serveurs les plus sensibles peuvent être réellement sécurisés.
- Les routeurs utilisés aujourd'hui n'ont pas toujours les possibilités de filtrage et les ressources nécessaires, mais les routeurs et commutateurs récents savent filtrer à des débits élevés sans dégradation de performance.
- Il n'est pas nécessaire de sécuriser tous les routeurs, 5 bien choisis peuvent suffire à assurer un filtrage efficace. Il devient alors possible d'utiliser des interfaces de configuration semblables à celle de FW-1.
- Aucun logiciel n'est capable de gérer des centaines de routeurs, notamment à cause des problèmes d'antispoofing et des chargements de configurations.
- Le filtrage IP est à la base de la sécurité des réseaux ; C'est sur cette base que s'appuient les VPN chiffrés et la sécurité au niveau des individus. Le filtrage a cet avantage sur l'IDS qu'il va refuser les paquets interdits alors que l'IDS ne pourra détecter un paquet "erroné" qu'après son passage, et les modifications de la configuration du Firewall induites par l'IDS ouvrent la porte aux dénis de service.
- Un atout de l'IDS est la détection des attaques sur des ports autorisés.

Cependant le futur de l'IDS tel qu'implémenté actuellement est hypothéqué par le recours croissant aux commutateurs dans les réseaux. L'IDS devra alors être mis en place au sein des routeurs/commutateurs, à l'instar du sous-ensemble de NetRanger fourni par Cisco dans ses routeurs.

Enfin, la mise en place d'un filtrage IP n'est pas synonyme de machines coûteuses : Si les vieux routeurs dont vous disposez n'offrent pas de fonctionnalités de filtrage, un PC de base doté de Linux/IPChains ou d'OpenBSD/IPFilter les remplacera avantageusement. L'examen des sources vous dévoilera la qualité du filtrage IP ainsi mis en place, supérieur à celui de bien des Firewalls commerciaux. Enfin, il faut tenir compte du contexte : dans le cadre de la sécurisation d'un réseau d'entreprises, les adresses IP sont beaucoup plus fiables que dans une perspective Internet.

**▪ Autres sujets des cours et conférences**

Le Dr. Matt Bishop présentait un cours intéressant sur les méthodes d'attaque de programmes et son pendant, les règles à respecter pour l'écriture de programmes sécurisés.

De la même façon, Crispin Cowan présentait les différentes attaques en débordement de buffers et les différentes méthodes pour s'en prémunir.

Du cours de John Green, on retiendra plus particulièrement quelques recommandations : l'utilisation régulière de nmap afin de surveiller les serveurs et les services disponibles sur son réseau, ainsi que celle de Nessus, \*le\* logiciel de tests de vulnérabilités (<http://www.nessus.org>).

Il cite également les logiciels capables de tester le filtrage IP d'un équipement, qui sont également utiles : nmap, tcpdump et filterrules (<http://www.hsc.fr/cabinet/produits/#filterrules>) de Renaud Deraison.

A noter également Chris Benton, qui donnait des indications précieuses sur les méthodes d'audit régulier de systèmes NT. Quant au cours de Simple Nomad (Paranoid Network), si son sujet était digne d'intérêt (sécurisation de système et durcissement de noyau) les exemples pratiques et références étaient trop rares. Cette tendance se retrouvait dans de nombreux autres cours, qui faisaient une part trop importante aux généralités et à la théorie.

En ce qui concerne les réseaux, Steve Acheson de Cisco remettait quelque peu en cause la rentabilité des VPN aux USA. En effet, le coût analytique moyen d'une liaison Frame Relay t1 (1,5 Mb) entre un bureau distant et Cisco est de \$3000 par mois, alors que la même chose avec un accès Internet T1 et un VPN revient à \$6000 par mois. Parallèlement, il confirmait la tendance au remplacement progressif des serveurs d'authentification TACACS et RADIUS par des serveurs LDAP.

Une évolution de la sécurité qu'il appuyait en rappelant que certains réseaux câblés subissent plus de scans que le réseau de Cisco.

Toujours dans le domaine de la sécurité, Jeffrey Hunker, Senior Director for Critical Infrastructure National Security Council ([www.ciao.gov](http://www.ciao.gov)) présentait les axes du combat mené par le gouvernement américain contre la cyber-criminalité, comme lors des éditions précédentes.

**▪ Infogérance de la sécurité**

Fritz Nelsonn, éditeur en chef de la revue américaine Network Computing ([www.networkcomputing.com](http://www.networkcomputing.com)) proposait une présentation-débat sur l'infogérance de la sécurité.

Entre autres informations, les résultats d'une enquête réalisée auprès de 500 lecteurs étaient présentés :

	Utilisent déjà	Planifient d'utiliser
Anti-virus	94%	3%
Firewall	88%	13%
VPNs(tout types, y compris accès distants)	46%	37%
Chiffrement au niveau applicatif	42%	24%
Logiciels de détection d'intrusion	30%	42%
Logiciels de tests de vulnérabilités	21%	33%
Authentification forte	18%	23%
Infrastructure de clés	10%	25%

La conclusion de la présentation indique que l'infogérance de sa sécurité est un choix discutable, car parfois imputable à un excès de confiance...

URLs :

<http://www.nwc.com/core/core8.html>

<http://www.nwc.com/consensus/>

<http://img.cmpnet.com/nc/1105/graphics/f22.pdf>

#### ▪ Exposition

L'exposition comprenait 59 exposants dans le seul domaine de la sécurité, dont une seule société française présente avec Solsoft NP (<http://www.solsoft.fr/>), leader de policy-based managment pour la sécurité.

La société américaine Hiverworld, <http://www.hiverworld.com>, réputée pour ses conseils en sécurité, et travaillant principalement pour la défense américaine, se transforme en fournisseur d'un système de tests de vulnérabilités. Le système proposé n'est ni la vente d'un logiciel de tests de vulnérabilités comme le propose Fidji ([www.fidji-rd.com](http://www.fidji-rd.com)), ni la vente d'un service de tests de vulnérabilités, comme le propose Qualys ([www.secmanage.com](http://www.secmanage.com)), mais une combinaison des deux modèles. Hiverworld propose à la vente ou la location des boîtiers : "Hivermute", un PC avec une carte Ethernet 100MB carrossé en boîtier rackable, que l'on place dans son réseau privé. Les boîtiers dialoguent avec Hiverworld en utilisant un tunnel propriétaire utilisant blowfish. Les boîtier effectuent des tests de vulnérabilités en permanence sur le réseau. Sur le serveur web d'Hiverworld, le système ARMS (Adaptive Risks Managment System), permet d'obtenir statistiques et rapports en PDF.

Hiverworld annonce plus de 500 signatures reconnues, fruit d'une expérience de 8 ans en conseil en sécurité. Il va de soi qu'un tel service d'infogérance de ses tests de vulnérabilités, avec des boîtiers étrangers sur son réseau, ne conviendra qu'aux entreprises prêtes à faire confiance à un tiers pour la sécurité de leur réseau privé.

La société "e-security" proposait elle un logiciel de surveillance de divers logiciels et firewalls, dans une vue topologie graphique de son réseau similaire à celle utilisée par Solsoft NP.

SANS demeure la manifestation la plus large et la plus complète pour se former et s'informer en sécurité.

<http://www.hsc.fr>

## **6 - Veille Attaques : Olivier Caleff / APOGEE Communications**

### 6.1 - Les Organismes Officiels

Le [CERT](#) a publié deux avis. L'avis [CA-2000-03](#) rappelle que de nombreux serveurs DNS utilisent toujours une version du BIND qui est vulnérable aux attaques décrites dans l'alerte [CA-99-14](#), bien que la publication de cette dernière date de plus de 6 mois !

- <http://www.cert.org/advisories/CA-2000-03.html>
- <http://www.cert.org/advisories/CA-99-14-bind.html>

D'autre part, le CERT a publié l'avis d'incident [IN-2000-05](#) sur *mstream*, un outil de déni de service réparti, qui a été analysé par David Dittrich.

- [http://www.cert.org/incident\\_notes/IN-2000-05.html](http://www.cert.org/incident_notes/IN-2000-05.html)
- <http://staff.washington.edu/dittrich/misc/mstream.analysis.txt>

Le [CIAC](#) a publié l'avis [K-034](#), reprise de celui de Cisco intitulé 'Catalyst Enable Password Bypass Vulnerability', et l'avis [K-035](#), reprise de l'avis Red Hat sur une vulnérabilité de *LVS (Linux Virtual Server)* dans le package *piranha*.

- <http://www.ciac.org/ciac/bulletins/k-034.shtml>
- <http://www.ciac.org/ciac/bulletins/k-035.shtml>

### 6.2 - Environnement Microsoft

[Microsoft](#) a publié 2 avis depuis le dernier numéro de *Netcost&Security HEBDO*. Juste après la clôture de l'édition précédente, [Microsoft](#) a publié l'avis [MS00-027](#), qui est intitulé 'Patch Available for "Malformed Environment Variable" Vulnerability'. Il s'agit de variables d'environnement trop longues qui provoquent une réservation abusive d'espace mémoire qui n'est plus libérée ultérieurement. C'est plus particulièrement l'interpréteur *cmd.exe* qui est visé.

Les correctifs sont disponibles pour Windows NT 4.0 et Windows 2000.

- <http://www.microsoft.com/technet/security/bulletin/ms00-027.asp>

L'avis [MS00-028](#) est intitulé 'Patch Available for "Server-Side Image Map Components" Vulnerability'. Il s'agit d'un *buffer overflow* dans des extensions de Frontpage qui permettent l'exécution de code non sollicité. Les composants impactés sont *Frontpage Server 97* et *98*, *IIS 4.0* et *Personal Web Server 4.0*. Les modules plus particulièrement en cause sont *htimage.exe* et *imagemap.exe*.

- <http://www.microsoft.com/technet/security/bulletin/ms00-028.asp>

## **7 - Actualités**

### ▪ **Les services secrets britanniques veulent intercepter les e-mails**

Selon notre confrère Sunday, les services secrets britanniques (MI5) seraient sur le point de monter un centre d'interception des courriers électroniques qui arrivent ou partent du Royaume-Uni en collaboration avec les ISP.

<http://www.securityservice.gov.uk/>

Lire aussi dans notre dernière édition (NetCost&Security HEBDO numéro 25 : le FBI concurrence Echelon

<http://search.washingtonpost.com/wp-srv/WPlate/2000-04/06/3081-040600-idx.html>

Outils de détection d'intrusion :

### ▪ Nessus Project

<http://www.nessus.org/>

### ▪ ISSO Intrusion Detection and Security Tools Database V1.1

[http://www.nswc.navy.mil/ISSEC/CID/id\\_tools.mdb](http://www.nswc.navy.mil/ISSEC/CID/id_tools.mdb)

## **8 - Solutions : les offres sélectionnées par la rédaction**

**MyCIO Corp**, l'initiative de partenariat lancée par myCIO.com, a pour mission de mettre ses services de protection des infrastructures à la disposition d'un large éventail de sociétés Web. MyCIO Corps se compose de trois programmes : Admiral, Captain et Affiliate.

Tous les participants à ces programmes bénéficient de l'appui des centres opérationnels de myCIO.com du monde entier, avec des liens directs vers plus de 300 experts en sécurité, de sorte que leurs solutions sont actualisées 24 heures sur 24, 7 jours sur 7 en fonction de l'apparition de nouveaux virus, hoax et menaces pour la sécurité.

[www.myCIO.com](http://www.myCIO.com).

### ▪ **Une intégration technologique transparente pour click2send**

Cclick2send.com, le réseau global de transmission de fichiers électroniques, intègre la technologie de protection antivirus administrée de myCIO.com au sein de son système de stockage et de transfert de fichiers, qui est opérationnel 24h/24 et 7j/7. Cette solution assurera la protection de la base de données de click2send.com contre les menaces virales et les attaques malveillantes.

Grâce à la protection antivirus administrée de myCIO.com, les clients de click2send.com bénéficieront en permanence d'une protection rapide et transparente contre les risques d'infection virale.

Par cet accord, myCIO.com devient le fournisseur exclusif de services de protection virale de click2send.com. Click2send.com déploiera cette protection antivirus au sein de son infrastructure de transmission sous forme de service administré afin de garantir l'intégrité de ses propres applications et des fichiers de ses clients. Ce service administré couvre l'ensemble des documents qui pénètrent dans les systèmes de passerelle et de courrier électronique de click2send.com. Les alertes concernant les mises à jour automatiques et l'actualisation des signatures de virus via Internet sont transmises click2send.com afin d'en protéger l'infrastructure contre les nouveaux virus.

<http://www.myCIO.com>

- **Safe Data System annonce la disponibilité et la gratuité de SDS Access One.**

Safe Data Access One est un serveur Radius et Tacacs+ d'authentification permettant de gérer, de contrôler et de vérifier l'identité des utilisateurs distants qui souhaitent se connecter aux différents systèmes d'information de l'entreprise.

De plus, Safe Data System propose une version gratuite de son produit Safe Data Access One (version 100 utilisateurs). Ce logiciel est disponible et downloadable sur le site [www.safedata.com](http://www.safedata.com)