APOGEE *Communications*

Rapport de Veille Technologique Sécurité N°70

Mai 2004

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: mailing-lists, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:


Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.


Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

La diffusion de ce document est restreinte aux clients des services VTS-RAPPORT et VTS-ENTREPRISE

APOGEE Communications
15, Avenue du Cap Horn
ZA de Courtaboeuf
91940 Les ULIS

Pour tous renseignements
Offre de veille: http://www.apogee-com.fr/veille
Informations: vts-info@apogee-com.fr

Au sommaire de ce rapport ...

PRODUITS ET TECHNOLOGIES 6
LES PRODUITS 6
JOURNALISATION 6
MICROSOFT – LOGPARSER V2.1 6
SYSTÈMES D'EXPLOITATION 9
LINUX – COMPARAISON DES DISTRIBUTIONS MAJEURES 9
LES TECHNOLOGIES 11
COMPROMISSION ELECTROMAGNÉTIQUE 11
TEMPEST ACOUSTIQUE 11
INFORMATIONS ET LÉGISLATION 12
LES INFORMATIONS 12
CERTIFICATION 12
ICSA LABS – 30 NOUVEAUX PRODUITS ÉVALUÉS 12
ICSALABS – CERTIFICATIONS SSL/TLS 13
DCSSI – CATALOGUE DES PRODUITS QUALIFIÉS 13
CRYPTOGRAPHIE 14
ECC2-109 – DÉFI REMPORTÉ 14
CONFÉRENCES 15
CANSECWEST 2004 – PREMIER VOLET 15
NEW METHODS IN OS FINGERPRINTING / TCP STACK TESTING 15
YOUR NETWORK IS TALKING, ARE YOU LISTENING 16
EXPLOIT MITIGATING TECHNIQUES 17
OPPORTUNISTIC ENCRYPTION USING IPSEC / IKE 17
SLIPPING IN THE WINDOW : TCP RESET ATTACKS 18
SHELLFORGE V2 – SHELLCODES FOR EVERYBODY AND EVERY PLATFORM 19
RELIABLE WINDOWS HEAP EXPLOITS 19
WHY HONEYPOTS SUCKS 20
BLUETOOTH : RED FANG, BLUE FANG 20
MÉTHODES 21
NIST – SP800-58 / SECURITY CONSIDERATIONS FOR VOICE OVER IP SYSTEMS 21
NIST – ETAT DES GUIDES DE LA SÉRIE SP800 22
TENDANCES 23
GOOGLE ET L'ENREGISTREMENT DES NOMS DE DOMAINE 23
LA LÉGISLATION 24
DROITS DE L'INTERNET 24
FR – LE DROIT SUR L'INTERNET EXPLIQUÉ À TOUS 24
GOUVERNANCE DE L'INTERNET 24
FR – OUVERTURE DU '.FR' 24
EU – LA LONGUE ROUTE VERS LA CRÉATION DU TLD 'EU' 25
LOGICIELS LIBRES 27
LES SERVICES DE BASE 27
LES OUTILS 27
NORMES ET STANDARDS 29
LES PUBLICATIONS DE L'IETF 29
LES RFC 29
LES DRAFTS 29
NOS COMMENTAIRES 33
LES DRAFTS 33
DRAFT-AZCORRA-TCPM-TCP-BLIND-ACK-DOS-00 33
ALERTES ET ATTAQUES 34
ALERTES 34
GUIDE DE LECTURE 34
FORMAT DE LA PRÉSENTATION 35
SYNTHÈSE MENSUELLE 35
ALERTES DÉTAILLÉES 36
AVIS OFFICIELS 36

APACHE 36
APPLE 36
BEA 36
BLUECOAT 36
CHECKPOINT 37
CITRIX 37
CVS 37
ETHEREAL 37
EXIM 37
GNU 37
HEIMDAL 37
HP 38
IBM 38
KDE 38
LINKSYS 38
LINUX 38
LINUX DEBIAN 39
LINUX REDHAT 39
LINUX SUSE 39
MICROSOFT 40
MCAFEE 40
OPENBSD 40
PROFTPD 40
QUALCOMM 40
SAMBA/RSYNC 40
SAMBAR 40
SCO 41
SGI 41
SIDEWINDER 41
SUN 41
SYMANTEC 41
WIFI 42
XINE/MPLAYER 42
ALERTES NON CONFIRMÉES 42
3COM 42
ACTIVESTATE 42
AGNITUM 42
ALLEGRO 42
ALT-N 42
APPLE 42
BSD 43
BUSINESSOBJECT 43
CPANEL 43
DELEGATE 43
F5 SOFTWARE 43
F-SECURE 43
FIREBIRD 43
GNU 43
KAME 44
KINESPHERE 44
LIFERAY 44
LINUX 44
MAILENABLE 44
MICROSOFT 45
MOLLENSOFT 46
NETAPP 46
NETGEAR 46
NETWIN 46
OMNICRON 46
OPERA 46
PANDORA 47
PHP 47
QUALCOMM 47
RHINOSOFT 47
SMC 47
SQUID 47
SQUIRRELMAIL 47
SUBVERSION 48
TRENDMICRO 48
UCD-SNMP 48
VERITAS 48
VERITY 48
VOCALTEC 48
VSFTPD 48
ZONEMINDER 48
AUTRES INFORMATIONS 49
REPRISES D'AVIS ET CORRECTIFS 49
CIAC 49
FREEBSD 51
HP 51

IBM 51
LINUX DEBIAN 52
LINUX FEDORA 52
LINUX MANDRAKE 52
LINUX REDHAT 53
MICROSOFT 53
ORACLE 53
SAMBA 53
SCO 53
SGI 53
SUN 54
CODES D'EXPLOITATION 54
CVS 54
MICROSOFT 54
SYMANTEC 54
TCP 54
VIRUS 55
BULLETINS ET NOTES 55
CISCO 55
VIRUS 55
ATTAQUES 56
TECHNIQUES 56
PHISHING 56

Le mot de la rédaction …

Le rapport définitif portant sur les causes du 'blackout' électrique subit en août dernier par certains Américains et une province Canadienne confirme que rien ne permet de prouver « *que les vers et virus circulant sur l'Internet au moment de l'interruption aient pu avoir un effet sur les systèmes de fourniture d'électricité* ». Une nouvelle qu'il faut analyser à la lumière des dégâts récemment occasionnés par le ver 'Sasser' et qui ne doit pas conduire à minimiser le risque posé par les menaces virales sur les systèmes de traitements automatisés ou 'SCADA' dans le jargon.

https://reports.energy.gov/BlackoutFinal-Web.pdf

Nous n'avions pas relevé le défi lancé le mois dernier par le groupe '**HoneyNet**' contrairement à notre habitude. Fort heureusement, Frank MeerKoetter, l'un des challengers, nous propose une analyse remarquable tant sur le plan du fond que de la forme. Nous recommandons sa lecture ainsi que celle de l'analyse proposée par l'auteur du défi. Ce dernier précise que l'adresse du 'proxy ouvert', objet du défi, a été publiée sans qu'il en ait été informé à la suite d'un test de validation effectué à l'aide d'un outil proposé sur un site russe. Les attaques et l'utilisation abusive du service ont commencé sitôt après …

http://project.honeynet.org/scans/scan31/sub/frank_meerkoetter/report_scan31_frank_meerkoetter.pdf

Pour terminer, nous recommandons la lecture de l'étude de 76 pages publiée par l'ART portant sur les enjeux de la messagerie instantanée en environnement fixe mais aussi et surtout mobile avec l'essor du GPRS.

http://www.art-telecom.fr/communiques/communiques/2004/index-c240504.htm

L'équipe de Veille Technologique

PRODUITS ET TECHNOLOGIES

LES PRODUITS

JOURNALISATION

MICROSOFT – LOGPARSER V2.1

- **Description**

Nombreux sont les outils écrits par les équipes de développement afin de les assister dans le test et le déboguage des applications qui sont ensuite remisés au placard.

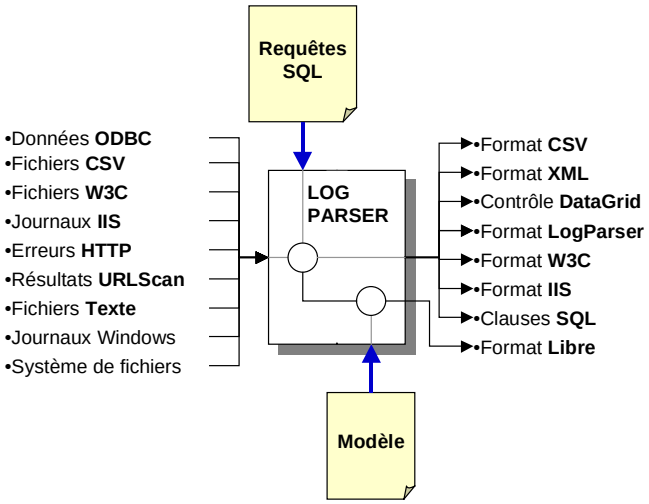
Il arrive pourtant que certains de ces outils soient diffusés, et bien que non officiellement maintenus fassent l'objet d'un réel intérêt de la part des spécialistes. Ce fut le cas de l'extraordinaire outil d'aide à la documentation '**AutoDuck**' diffusé dans les années 1994 sous la forme d'un exemple de programmation livré avec le compilateur '**C**' de Microsoft.

C'est aussi le cas du non moins extraordinaire outil d'analyse des journaux dénommé '**LogParser**' dont la première version était livrée par Microsoft noyée dans le kit de développement de l'application **IIS** avant d'être mis en évidence à la suite du succès rencontré.

Cet outil permet en effet d'analyser la quasi-totalité des journaux produits par les systèmes d'exploitation Windows mais aussi par l'application phare **IIS**, et ce, par le biais de requêtes formulées en '**SQL**', l'outil pouvant être activé depuis une interface console mais aussi de manière programmatique en activant l'objet **Active/X** associé.

Dans sa version 2.1, l'utilitaire '**LogParser**' est à même de traiter les données contenues dans quelques 14 formats de journalisation différents :

- **IIS Centralized Binary Log Format** dit 'BIN',
- **IIS Log format** dit 'IIS',
- **IIS W3C Extended Log Format** dit 'IISW3C',
- **IIS Log Format with MSID Filter fields** dit 'IISMSID',
- **HttpError Log Format** dit 'HTTPERR',
- **NCSA Common Log Format** dit 'NCSA',
- **Generic W3C Log Format** dit 'W3C',
- **ODBC log Format** dit 'ODBC',
- **URLScan Log Format** dit 'URLSCAN',
- **Event Logger Format** dit 'EVT',
- **TextLine Log Format** dit 'TEXTLINE',
- **TextWord Log Format** dit 'TEXTWORD',
- **FileSystem Crawler Format** dit 'FS',
- **Comma Separated Format** dit 'CSV'.



Les traitements qui seront appliqués aux structures spécifiques à chacun des formats d'entrée supportés sont spécifiés sous la forme de clauses '**SQL**' agrémentées de quelques 42 fonctions de conversion fort utiles. On notera la présence des indispensables fonctions de manipulation des chaînes de caractères mais aussi d'une fonction de résolution d'une adresse IP ou encore d'un identifiant système dit '**SID**'.

Les résultats peuvent être générés dans l'un des neufs formats de sortie reconnus. Parmi ceux-ci, trois formats apparaissent particulièrement intéressants :

- le format dit '**TPL**' permettant une présentation des résultats en intégrant ceux-ci dans un quelconque modèle de présentation. Ce format est particulièrement adapté à la production de résultats au format **HTML** exploitables par le biais d'un navigateur,
- le format dit '**SQL**' autorisant l'injection directe des résultats dans la table d'une base de données, l'utilitaire assurant la connexion à celle-ci moyennant la fourniture des paramètres de connexion dans la ligne de commande,
- le format dit '**DataGrid**' pour lequel les données seront présentées dans un objet de type '**DataGrid**', un tableur minimaliste offrant une présentation similaire à celle proposée par le tableau Excel.

La structure de cet utilitaire rend celui-ci extrêmement intéressant comme outil d'extraction sélective et conditionnelle de données mais aussi comme outil de conversion de format. Cette dernière fonctionnalité est simplifiée par l'existence de six fonctions de conversion activables par le biais de l'option '**-c**'.

Il est ainsi possible de convertir l'un des quatre formats d'entrée présentés dans le tableau ci-contre en une seule ligne de commande. Cette option n'est pas exclusive et peut parfaitement être utilisée conjointement avec une clause '**SQL**' !

BIN	W3C	IIS	MSID	*vers*
⇒		⇒	⇒	W3C
⇒	⇒			IIS
			⇒	MSID

La commande suivante permet ainsi de convertir le format **IIS** propriétaire en format **W3C** reconnu par la majorité des

outils d'analyse en ne conservant que les enregistrements pour lesquels le champ '**ComputerName**' est renseigné.

```
logparser –c –i:BIN –o:W3C input.bin output.log "ComputerName IS NOT NULL"
```

La liste des champs définis pour chacun des formats d'entrée reconnus est documentée dans le manuel d'utilisation livré avec la version 2.0. Elle peut aussi être obtenue par le biais de l'option d'aide '**-h –i:NomDuFormat**'. Nous en proposons une synthèse ci-dessous:

		BIN	IIS	IisMsid	NCSA	ODBC
BytesReceived	I	X	X	X		
BytesRecvd	I					X
BytesSent	I	X	X	X	X	X
ClientIP	S					
ClientIpAddress	S	X				
ComputerName	S	X				
Date	T		X	X		
DateTime	T	X			X	
GUID	S			X		
HostName	S		X	X		
LogFilename	S	X	X	X	X	X
LogRow	I		X	X	X	X
LogTime	T					X
Machine	S					X
Method	S	X				
Operation	S					X
Parameters	S		X	X		X
PartnerID	S			X		
PassPortID	S			X		
ProcessingTime	I					X
ProtocolStatus	I	X				
ProtocolVersion	S	X				
RecordNumber	I	X				
Referrer	S			X		
RemoteHostName	S				X	
RemoteLogName	S				X	
Request	S				X	
RequestType	S		X	X		
ServerIP	S		X	X		X
ServerIpAddress	S	X				
ServerPort	I	X				
Service	S					X
ServiceInstance	S		X	X		
ServiceStatus	I					X
SiteID	I	X				
SiteInstance	S					
StatusCode	I		X	X	X	
SubStatus	I	X				
Target	S		X	X		X
Time	T		X	X		
TimeTaken	I	X	X	X		
UriQuery	S	X				
UriStem	S	X				
UserAgent	S			X		
UserIP	S		X	X		
UserName	S	X	X	X	X	
Win32Status	I	X				X
Win32StatusCode	I		X	X		

		EVT	NTFS	UrlScan	HttpErr
EventLog	S	X			
RecordNumber	I	X			
TimeGenerated	T	X			
TimeWritten	T	X			
EventID	I	X			
EventType	I	X			
EventTypeName	S	X			
EventCategory	I	X			
SourceName	S	X			
Strings	S	X			
ComputerName	S	X			
SID	S	X			
Message	S	X			
Path	S		X		
Name	S		X		
Size	I		X		
Attributes	S		X		
CreationTime	T		X		
LastAccessTime	T		X		
LastWriteTime	T		X		
ClientIP	S			X	
Comment	S			X	
Date	T			X	
LogFilename	S			X	
LogRow	I			X	
SiteInstance	S			X	
URL	S			X	
date	**T**				X
time	**T**				X
cs-method	**S**				X
sc-status	**I**				X
src-ip	**S**				X
src-port	**I**				X
dst-ip	**S**				X
dst-port	**I**				X
cs-url	**S**				X
sc-status	**I**				X
s-site	**S**				X
s-reason	**S**				X

avec
S -> STRING
I -> INTEGER
T -> TIME

On regrettera que l'auteur de ce logiciel ait choisi de conserver le nom des champs tels que définis dans les spécifications du format sans tenter de regrouper sur un nom identique les champs de même signification et de même type, tels les champs 'Win32Status' et 'Win32StatusCode' ou encore '**ServerIP**' et '**ServerIPAddress**' …

Quelques exemples simples permettront de mieux appréhender la puissance de cet utilitaire dont il ne faudrait surtout pas restreindre l'utilisation aux seules tâches d'administration d'un serveur **WEB IIS** même s'il a été initialement conçu pour cela.

Système de fichier NTFS

L'utilitaire '**LogParser**' peut être utilisé sur le système de fichier en spécifiant le format '**FS**' ici considéré comme une table contenant les 7 principaux attributs d'un fichier: chemin, nom, taille, attributs spécifiques, dates de création, de modification et de dernier accès.

Ce mode d'accès permet de créer simplement et rapidement des requêtes répondant aux besoins quotidiens de l'exploitant à l'identique de l'indispensable fonction '**find**' en environnement UNIX.

La requête suivante recherche ainsi tous les fichiers temporaires créés sur le volume 'C:' la veille et délivre les résultats dans un objet de type grille:

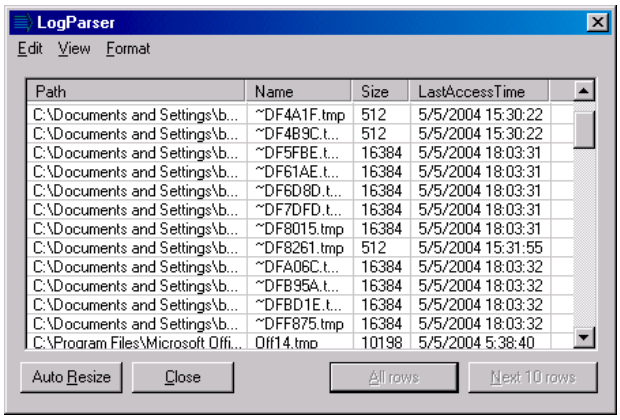
```
logparser -i:FS -o:datagrid "SELECT Name, Size FROM C:\* WHERE Name LIKE '%TMP' AND
TO_DATE(LastAccessTime) = TO_DATE(SUB(SYSTEM_TIMESTAMP(), TO_TIMESTAMP('01-02', 'MM-dd')))"
```

Cette syntaxe requiert quelques explications:

- la fonction '**SYSTEM_TIMESTAMP()**' délivre la date du système ensuite réduite par la fonction '**TO_DATE()**' à une date exprimée sous la forme 'MM-JJ-AAAA',
- la date recherchée est obtenue en soustrayant à cette date via la fonction '**SUB**', un horodatage correspondant à une journée écoulée obtenu par utilisation de la fonction '**TO_TIMESTAMP('01-02','MM-dd')**'.

Les résultats, ici délivrés sous la forme d'un tableau, auraient parfaitement pu être générés dans un format exploitable par un script, tel le format 'CSV'.

On pourrait même parfaitement envisager d'automatiser entièrement l'opération par le biais d'un script Visual Basic ou .NET en s'appuyant sur la librairie dynamique 'LogParser' et sa multitude de fonctions.



Journal d'évènement Windows

Les événements journalisés en environnement Windows et sauvegardés dans un fichier au format '**EVT**' peuvent être traités sous la forme d'une table contenant les 13 champs constituant un enregistrement. La requête suivante permet d'extraire à l'écran les évènements significatifs d'une erreur (EventType = 1).

```
logparser -i:EVT "SELECT TO_DATE(TimeGenerated) AS Time, SourceName, ComputerName FROM
C:\temp\events.evt WHERE EventType = 1"
 Time     SourceName   ComputerName
 -------- ------------ ------------
 5/3/2004 MsiInstaller PORTXXX
 5/3/2004 MsiInstaller PORTXXX
 5/3/2004 MsiInstaller PORTXXX
 Statistics:
 -----------
 Elements processed: 31
 Elements output:    3
 Execution time:     0.06 seconds
```

Fichier Texte quelconque

Les formats d'entrée 'TEXTLINE' et 'TEXTWORD' permettent d'envisager pouvoir utiliser '**LogParser**' sur des fichiers de journalisation quelconques. L'exemple suivant utilise le format d'extraction ligne à ligne pour filtrer les requêtes GET dans un fichier de journalisation Apache.

```
logparser -i:TEXTLINE "SELECT SUBSTR(Text,53) FROM C:\temp\httpd.log WHERE Text Like
'% \"GET'"
SUBSTR(Text,53)
---------------------------------------------------------------
GET /ressources/menu.css HTTP/1.1" 200 172 "https://veille/menu.html"
GET /ressources/header.css HTTP/1.1" 200 675 "https://veille/header.htm
GET /ressources/style.css HTTP/1.1" 304 - "https://veille/home.html"
GET /ressources/search.gif HTTP/1.1" 200 42580 "https://veille/header.h
GET /ressources/leg.gif HTTP/1.1" 200 159 "https://veille/home.html"
GET /ressources/new.gif HTTP/1.1" 200 157 "https://veille/home.html"
 Statistics:
 -----------
 Elements processed: 393
 Elements output:    393
 Execution time:     3.61 seconds
```

Dans bien des cas cependant, un script écrit en '**Perl**' sera plus performant et plus efficace !

Pour conclure cette rapide présentation, tout serait parfait si l'absence d'une documentation réellement exploitable ne se faisait cruellement et rapidement sentir, et ce malgré la mise à disposition par Microsoft d'un manuel d'utilisation de plus de 46 pages. Fort heureusement, plusieurs ressources externes viendront au secours de l'utilisateur dont le site '**www.logparser.com**' entièrement consacré à cet outil. Par ailleurs, de nombreuses informations pratiques peuvent être obtenues en utilisant les différentes combinaisons de l'option '-h' donnant accès à l'aide en ligne.

Nous conseillons à ce propos d'imprimer ces informations dont la grammaire SQL (option '-h 1') et de les garder à porter de main.

```
Microsoft (R) Log Parser Version 2.1
Copyright (C) 2002 Microsoft Corporation. All rights reserved.
 Usage:
  LogParser   [-i:<input_format>] [-o:<output_format>] <SQL query> | file:<query_filename>
              [<input_format_options>] [<output_format_options>]
              [-q[:ON|OFF]] [-e:<max_errors>] [-iw[:ON|OFF]] [-stats[:ON|OFF]]
  LogParser -c -i:<input_format>   -o:<output_format> <from_entity> <to_entity> [<where_clause>]
              [<input_format_options>] [<output_format_options>]
              [-q[:ON|OFF]] [-e:<max_errors>] [-iw[:ON|OFF]] [-stats[:ON|OFF]
              [-multisite[:ON|OFF]
  -i:<input_format>  : one of IISW3C, NCSA, IIS, ODBC, BIN, IISMSID, HTTPERR, URLSCAN, CSV, W3C,
                       EVT, TEXTLINE, TEXTWORD, FS (if omitted, will guess from the FROM clause)
  -o:<output_format> : one of CSV, XML, NAT, W3C, IIS, SQL, TPL, NULL (if omitted, will guess
```

```
                        from the TO clause)
  -q[:ON|OFF]         : quiet mode; default is OFF
  -e:<max_errors>     : max # of parse errors before aborting; default is -1 (ignore all)
  -iw[:ON|OFF]        : ignore warnings; default is OFF
  -stats[:ON|OFF]     : dump stats after executing query; default is ON
  -c                  : use built-in conversion query
  -multisite[:ON|OFF]: send BIN conversion output to multiple files depending on the SiteID
                        value; default is OFF
Examples:
  LogParser "SELECT date, REVERSEDNS(c-ip) AS Client, COUNT(*) FROM file.log
             WHERE sc-status<>200 GROUP BY date, Client" -e:10
  LogParser -c -i:BIN -o:W3C file1.log file2.log "ComputerName IS NOT NULL"
Help:
  -h 1                  : SQL Language Grammar
  -h 2 [ <function> ]   : Functions Syntax
  -h 3                  : Example queries
  -h -i:<input_format>  : Help on <input_format>
  -h -o:<output_format> : Help on <output_format>
  -h -c                 : Conversion help
```

Le paquetage d'installation contient l'outil sous la forme d'un exécutable (LogParser.exe – 598Ko), sous la forme d'une librairie dynamique enregistrée en tant que composant Active/X durant le processus d'installation (LogParser.dll – 564Ko), le manuel au format Word dans le cas du paquetage V2.0 ainsi qu'un ensemble de fichiers d'exemple forts utiles.

Si la version 2.0 est accessible sous la forme d'un paquetage autonome pouvant être installé sur tout système Windows, la version 2.1 est intégrée au ressource kit **IIS 6.0** dont l'installation doit obligatoirement être effectuée sur un **Windows XP professional** ou un **Windows Server 2003** sauf à utiliser les options '/V/a' en argument de la commande d'installation du ressource kit 'iis60rkt.exe'.

- **Complément d'information**

http://www.microsoft.com/downloads/details.aspx?familyid=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en
http://www.microsoft.com/technet/community/scriptcenter/logs/logparser/default.mspx - Présentation de l'outil
http://www.logparser.com - Le site 'LogParser' non officiel
http://www.logparser.com/instantforum33/messages.aspx?ForumID=1 - Forum dédié à l'outil LogParser

SYSTEMES D'EXPLOITATION

LINUX – COMPARAISON DES DISTRIBUTIONS MAJEURES

- **Description**

La belle épopée d'un système d'exploitation conçu par tous et utilisable par chacun, non commercial et libre de tout droit est en passe d'être révolue. Cette utopie moderne n'aura pas résisté aux contraintes pratiques du marché lequel, s'il acceptera un système 'libre', n'en exigera pas moins les services d'accompagnement traditionnels: support technique, packaging, internationalisation, distributions prêtes à l'emploi, …

Autant de services qui ne peuvent raisonnablement tous être délivrés dans le cadre du modèle communautaire à l'origine du succès LINUX conduisant ainsi à la prolifération d'éditeurs – commerciaux ou associations de volontaires - reprenant à leur compte ces services sans lesquels LINUX n'aurait jamais dépassé le cadre d'un système conçu par des spécialistes pour des spécialistes.

A l'origine, chaque grande distribution disposait de caractéristiques propres répondant aux besoins de groupes d'utilisateurs, tous passionnés et disposant des moyens requis pour charger tout ou partie de ces distributions depuis l'Internet et recompiler celles-ci pour les optimiser en fonction des matériels utilisés.

Apparaissaient ainsi courant 1992, les trois distributions fondamentales que furent '**SLS**', '**SlackWare**' et '**Debian**'. Fondamentales car offrant pour la première fois un paquetage réellement exploitable contenant le cœur du système d'exploitation – le noyau – par ailleurs disponible sous forme de sources mais aussi l'ensemble des utilitaires et applications formant un vrai système d'exploitation. D'un noyau unique, le vrai 'LINUX', émergeront plusieurs variations d'un système d'exploitation dont les caractéristiques seront pilotées par le choix de ces utilitaires, de ces applications d'accompagnement mais surtout par la conception de l'environnement d'administration et d'installation.

Ces trois distributions marqueront de leur empreinte les distributions suivantes qui reprendront tout ou partie des concepts et choix de conception dont:

- '**SuSE**' distribution proposée par la société allemande **SuSE** fondée en 1992 (dernièrement rachetée par **Novell**). Cette distribution s'appuiera sur la distribution '**SLS**' puis sur la distribution '**SlackWare**' pour enfin intégrer le mécanisme de gestion des paquetages de la distribution '**RedHat**',
- '**RedHat**' société fondée en 1993 proposant une distribution du même nom dont le facteur de succès aura été l'introduction en 1995 d'un mécanisme facilitant la gestion des paquetages dit '**RPM**', une fonctionnalité indispensable dans le cadre de la fourniture d'une distribution commerciale,
- '**Caldera**' distribution éditée fin 1994 par la société **Caldera Systems** qui rachetait en 2000 le célèbre éditeur '**SCO**' et les droits que celui-ci possédait sur le système UNIX System V.
- '**Mandrake**' distribution française mise sur la marché en 1998 puis ensuite éditée par la société **MandrakeSoft**.

Les dernières années auront vu un repositionnement des acteurs commerciaux qui proposent une gamme de produits adaptés aux différents segments du marché: bureautique, serveur d'entrée et gros serveurs tout en conservant une distribution librement accessible mais non maintenue.

L'éditeur **Red-Hat** a ainsi dernièrement annoncé l'arrêt du support de sa distribution 'Linux Red-Hat V9.0' au profit de la distribution **Fedora** dont tout laisse à penser qu'elle servira de plate-forme de test pour les prochaines évolutions des versions commerciales.

Distributions

Face à la multiplicité des distributions proposées par chaque éditeur, nous proposons ci-après un tableau récapitulatif des distributions proposées par trois éditeurs commerciaux en y intégrant la distribution '**Debian**' produite et gérée par un groupe de volontaires.

Editeur	Distribution	Version	Processeurs	Prix	Libre	Utilisation
Debian	Debian GNU/LINUX	3.0r2 woody	i386, ia64, Alpha, HPPA, Arm, m68k, Mips, PPC, s390,Sparc	-	OUI	Usage personnel, Bureautique Trois niveaux de validation
Mandrake	Discovery	10	i586	$50	OUI	Usage personnel
	PowerPack	10	i586	$80	NON	Bureautique
	PowerPack+	10	i586	$199	NON	Serveurs de milieu de gamme Support IBM DB2 8.1
	Corporate Serveur	2.1	i586, AMD64	$799	NON	Serveurs critiques
RedHat	Linux	9.0	i386	$40	OUI	Usage personnel N'est plus supportée
	Fedora	Core1 yarrow	i386, AMD64	gratuit	OUI	Usage personnel Durée de vie limité: 4 à 6 mois
	Professional WS	3	bi-CPU i386	-	NON	Non encore disponible
	Enterprise Linux WS	3	i386, AMD64, ia64	$190 $984	NON	Bureautique Support : Basic ou Standard
	Enterprise Linux ES	3	i386	$349 $991	NON	Serveurs de milieu de gamme Support : Basic ou Standard
	Enterprise Linux AS	3	i386, AMD64, ia64, PPC, s390, s390x	$1499 $3190	NON	Serveurs critiques Support : Basic ou Standard
SuSE	Personnal	9.1	i586	$30	OUI	Usage personnel
	Professional	9.1	i586, AMD64	$90	NON	Bureautique
	Enterprise	8	i586, AMD64, ia64, s390	$749 $1405	NON	Serveurs de milieu de gamme Pack d'extension Lotus Domino

La colonne 'Libre' indique si la distribution concernée peut être librement et gratuitement téléchargée sur le site de l'éditeur. Si tel est la cas, le prix indiqué en regard correspond au coût de la distribution livrée sur support conventionnel.

Paquetages

Le tableau suivant précise la version des différents paquetages classiquement livrés avec les principales distributions de LINUX.

Paquetage	Linux 3.0	Fedora Core 1	Debian 3.0r2	SuSE 9.1	Mandrake 10
kernel	2.4.21	2.4.22	2.2.20	2.6.4	2.6.3
apache			1.3.26		1.3.29
apache 2	2.0.46	2.0.47		2.0.49	2.0.48
bind	9.2.2	9.2.2p3	8.3.3	9.2.3	9.2.3
iptable	1.2.8	1.2.8	1.2.6a	1.2.9	1.2.9
mysql	3.23.58	3.23.58	3.23.29	4.0.18	4.0.17
openssh	3.6.1p1	3.6.1p2	3.4p1	3.8p1	3.6.1p2
openssl	0.9.7a	0.9.7a	0.9.6c	0.9.7d	0.9.7c
perl	5.8. 0	5.8.1	5.6.1	5.8.3	5.8.3
postfix	2.0.11	2.0.11	1.1.11	2.0.19	2.0.18
postgresql		7.3.4	7.2.1	7.4.2	7.4.1
rpm	4.2.1	4.2.1	4.0.3	4.1.1	4.2.2
samba	3.0.0	3.0.0	2.2.3a	3.0.2a	3.0.2
sendmail	8.12.10	8.12.10	8.12.3	8.12.10	8.12.11
Xfree-86	4.3.0	4.3.0	4.1.0	4.3.99.902	4.3.0
xinetd	2.3.12	2.3.12	2.3.4	2.3.13	2.3.12

On notera les écarts existant entre certaines versions actuellement livrées et la dernière version disponible. Ce problème endémique de toute distribution logicielle est ici amplifié par la grande quantité d'applications de toutes sortes livrées avec chaque distribution. Il met en évidence l'intérêt de disposer d'un excellent système de mise à jour – et c'est l'une des forces de la distribution '**Debian**' - mais aussi de composants spécialisés n'intégrant que les paquetages requis pour la fonction rendue.

▪**Complément d'information**

http://digital-domain.net/lug/unix-linux-history.html - La véritable histoire de LINUX
http://www.debian.org/ - Distribution 'Debian'
http://www.mandrakesoft.com/ - Distribution 'Mandrake'
http://fedora.redhat.com/about/history/ - Distribution 'RedHat'
http://www.suse.com/us/index.html - Distribution 'SuSE'

LES TECHNOLOGIES

COMPROMISSION ELECTROMAGNETIQUE

TEMPEST ACOUSTIQUE

▪Description

Si les effets des émissions électromagnétiques indésirables sur la sécurité des systèmes d'information sont bien connus (Rapport N°69 – Avril 2003), il n'en va pas de même avec les signaux acoustiques qui doivent pourtant être considérés comme des signaux compromettants. Telle est du moins la conclusion d'une pré-étude publiée par deux célèbres 'touche-à-tout' dans le domaine de la cryptographie: **Adi Shamir** et **Eran** Tromer du non moins célèbre '**WeizMann Institute**'.

Une première synthèse de cette pré-étude a été diffusée sous le titre '**Acoustic Cryptanalysis: On nosy people and noisy machines**' à l'occasion de la conférence **EuroCrypt 2004** qui s'est tenue du 2 au 6 mai dernier en Suisse.

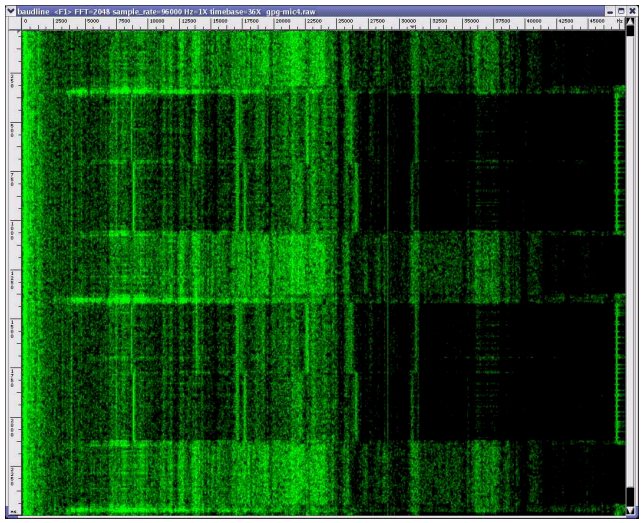
L'hypothèse développée par ces deux chercheurs est que le bruit généré par un matériel informatique, dans le cas présent un ordinateur, peut être corrélé avec l'activité du processeur et ainsi fournir une information suffisamment fiable et précise pour être exploitable dans le domaine de la cryptanalyse.

Une pré-étude menée pour valider cette hypothèse a permis de mettre en évidence l'existence de motifs acoustiques spécifiques à certaines activités, et en particulier, la présence de séquences significatives du changement d'état d'un processeur de type INTEL provoqué par l'instruction '**HALT**'.

Cette instruction est couramment utilisée pour positionner le processeur, et les périphériques partageant son bus d'instruction, dans un mode d'attente à faible consommation électrique, mode dont il sera réveillé par une interruption matérielle signalant généralement la disponibilité de données sur un quelconque périphérique d'entrée/sortie.

Le résultat observé par les auteurs n'est donc pas si étonnant si l'on tient compte que tout changement d'activité aussi minime soit-il aura une répercussion sur la consommation d'énergie, et par conséquence sur le bruit acoustique généré par tous les composants positionnés dans la chaîne: ventilateur de refroidissement bien entendu mais aussi toutes les selfs et capacités intervenant dans la régulation des niveaux d'alimentation.

La constitution physique de ces deux derniers composants laisse supposer que les appels de courants dus aux variations d'activité puissent se traduire par la génération d'une onde acoustique détectable: vibration des armatures de condensateurs de régulation de très forte capacité, résonance des ferrites des selfs d'apport d'énergie, ...



Le spectrogramme, extrait de l'article et présenté ci-contre, met en évidence l'apparition du phénomène durant une signature **GnuPG** effectuée sur un PC standard.

On y distingue nettement deux types de motifs: un motif correspondant à un bruit à large spectre répété trois fois correspondant à l'état d'attente du processeur dans lequel s'insère un motif spécifique correspondant à la phase dite 'd'exponentiation modulo' effectuée deux fois – modulo puis modulo q - dans le cas d'une implémentation utilisant la technique 'des restes chinois'.

Les auteurs ont confirmé que la source compromettante trouve son origine dans le bloc de condensateurs assurant la régulation de l'alimentation du processeur en refroidissant ceux-ci et en constatant la disparition totale du phénomène. Une expérience similaire menée sur un ordinateur portable a permis de reproduire à l'identique les résultats en notant cependant une variation notable dans le niveau d'émission acoustique liée au mode d'alimentation: batterie ou secteur.

Nous laisserons au lecteur le soin de parcourir cette fort intéressante pré-étude de tout au plus quinze pages HTML et d'écouter les enregistrements sonores disponibles en ligne.

▪Complément d'information

http://www.wisdom.weizmann.ac.il/~tromer/acoustic/ - Pré-étude
http://www.zurich.ibm.com/eurocrypt2004/ - Eurocrypt 2004

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

CERTIFICATION

ICSA LABS – 30 NOUVEAUX PRODUITS EVALUES

- **Description**

Fin Avril, **ICSALabs** a annoncé avoir mené à bien la 'certification' de 30 produits de sécurité dans les catégories **Pare-Feu**, **IPSec** et **IDS** sur le premier trimestre de l'année.

Cette branche de la société **TruSecure** s'est notamment spécialisée dans l'évaluation des produits de sécurité et la délivrance d'un label garantissant la conformité de ceux-ci vis à vis d'un ensemble de critères techniques non normalisés mais représentatifs des exigences minimales attendues de ce type de produits.

A ce jour, les produits peuvent faire l'objet d'une évaluation dans les catégories – non exclusives – suivantes:

Catégorie	Sous-catégorie	2003	2004	Remarques
Antivirus	**Antivirus scanner détection**	**17**	16	
	Anti-Virus Scanner Cleaning	7	7	
	Products for Internet Gateway	6	**9**	
	Products for Microsoft Exchange Server	5	**7**	
	Product for Lotus Notes Certification	4	**6**	
	Product for Security Service Providers	1	1	
	On-Line Anti-Virus Scanners	1	1	
Pare-Feu	**Critères V3.0a**	15	**27**	Critères désormais obsolètes
	Critères V4.0	**25**	12	
IDS	**Critères NIDS**	3	2	
	Critères T1	2	2	
IPSec	**Niveau 1.0b**	22	**23**	Critères désormais obsolètes
	Niveau 1.1	3	**5**	
Pare-Feu personnels		3	1	
Filtrage de contenu		1	1	
SSL/TLS		**6**	-	Nouvelle catégorie
WLAN		**-**	**-**	Aucun produit évalué

Nous proposons, ci-dessous, le tableau de synthèse que nous avons établi concernant les produits certifiés **ICSA** dans les catégories '**Détection d'intrusion**' (colonne '**IDS**'), '**IPSec**' et '**Pare-Feux**'. Les produits annoncés certifiés durant le premier trimestre 2004 sont annotés dans la colonne 'Q1'.

Editeur	Produit	Crypto	IDS		FW		IPSEC		Q1
Allied Telesyn	AR450S	X			X	4.0	X	1.0B	**X**
Check Point	NG FireWall-1 Linux				X	4.0			
Cisco	NID 4235		X	NIDS					**X**
	Cisco PIX Firewall	X			X	4.0	X	1.0B	
	Cisco 806	X					X	1.0B	
	IOS 1700, 2600, 3600, 3700, 7200	X					X	1.0B	
CA	eTrust Firewall for Windows 2000				X	3.0a			
CoSine Comm.	IPSX Product Family				X	3.0a			
CyberGuard Corp.	CyberGuard Premium Firewall				X	4.0			
Efficient Net	Efficient Router Family				X	3.0a			
Enterasys	XSR - Security Routers, XSR-1805	X					X	1.0B	**X**
eSoft	EX Firewall Policy Manager				X	3.0a			
Fortinet	Fortigate-300	X	X	NIDS/T1					**X**
	Antivirus Firewalls				X	4.0	X	1.0B	**X**
Global Technology	GTA Firewall Family				X	4.0			
Inkra Networks	Inkra 4000 Virtual Service Switch				X	4.0			
Intoto, Inc.	iGateway	X			X	4.0	X	1.1	
Juniper	M-Series Router Family				X	4.0			**X**
Kerio	WinRoute Firewall				X	4.0			
Linksys	Router BEFVP41 V2	X					X	1.0B	
Lucent	Access Point Family	X			X	3.0a	X	1.0B	
Lucent	Lucent VPN Firewall Family	X			X	4.0	X	1.0B	
Microsoft	ISA Server 2000				X	4.0			**X**
NETASQ	NETASQ F100-3				X	3.0a			
NetContinuum	NC-1000 Web Security Gateway				X	4.0			
Netgear	Prosafe Firewall FR114P				X	4.0			

	Firewall Router FVL328				X	4.0			**X**
Netopia	Cayman 3300-ENT				X	4.0			**X**
NetScreen	NetScreen Family	X			X	4.0	X	1.1	
NetWolves	WolfPac Security Platform SG2020				X	4.0			
Nokia	Nokia IP Series Routers	X			X	3.0a	X	1.0B	
Nortel Networks	Alteon Switched Firewall Family				X	4.0			
Novell	BorderManager				X	4.0			
Permeo	Application Security Platform	X							
RIAS Corporation	GreatSpeed GS-1540G				X	4.0			
Secure Computing	Sidewinder G2 Firewall	X					X	1.1	
ServGate	ServGate Security Gateways				X	3.0a			
SnapGear Inc.	SnapGear SME550				X	4.0			
SonicWALL Inc.	SonicWALL Pro 4060	X			X	3.0a	X	1.0B	
Sourcefire	Network Sensor 2000		X	NIDS					
	Snort 1.8.6		X	T1					
Stonesoft	StoneGate	X			X	4.0	X	1.0B	**X**
Symantec	Enterprise Firewall for NT, Solaris	X			X	3.0a			
	Enterprise VPN NT, Solaris	X					X	1.0B	
	Gateway Security 5420	X					X	1.0B	**X**
Thomson	SpeedTouch 610 POTS, 610i	X					X	1.0B	
VarioSecure	VarioSecure				X	4.0			
WatchGuard	Firebox System Family	X			X	4.0	X	1.0B	**X**
ZyXel	ZyWALL Series	X			X	3.0a	X	1.0B	

Le lecteur souhaitant obtenir plus d'informations pourra se reporter aux listes proposées sur le site de laboratoire de l'ICSA et aux fiches d'évaluation renseignées pour chacun des produits.

Chaque fiche, d'une dizaine de pages au format PDF, détaille les conditions de test – plates-formes matérielles et logicielles, documentation fournie, configuration d'installation, … - et les résultats de chacun des essais effectués conformément à la méthodologie développée pour la catégorie pour laquelle est demandée la certification.

- **Complément d'information**

http://www.trusecure.com/company/press/pr_20040419.shtml - Annonce de presse
http://www.icsalabs.com/html/communities/firewalls/newsite/cert2.shtml - Certification Pare-feux V4.0
http://www.icsalabs.com/html/communities/ipsec/certification/certified_products/1.1index.shtml - Certification IPSec V1.1
http://www.icsalabs.com/html/communities/ipsec/certification/certified_products/index.shtml - Certification IPSec V1.0B
http://www.icsalabs.com/html/communities/ids/index.shtml - Certification IDS

ICSALABS – CERTIFICATIONS SSL / TLS

- **Description**

Le 26 avril dernier, **ICSALabs** annonçait la certification d'une première série de six équipements **VPN** dans le cadre du programme de certification **TLS / SSL** engagé fin 2003.

Contrairement aux autres programmes de certification et aux engagements pris par **ICSALabs**, force est de constater que les critères de tests et de validation applicables au test des équipements **TLS / SSL** n'ont pas toujours été publiés. Il est difficile de juger de la pertinence de cette certification dans ces conditions.

Les produits certifiés sont les suivants :

Editeur	Produit	Version
Aventail Corp.	EX-1500 SSL VPN Appliance	7.02 Patch 3
F5 Networks	Firepass 1000 and Firepass 4000	4.0.2
Netilla Networks	Netilla Security Platform (E-Class)	4.0 build 5531
NetScaler	NetScaler 9400	4.0.2.1p2
NetScreen	NetScreen Family	5.1 build 34.9
PortWise AB	PortWise mVPN	3.5.4

- **Complément d'information**

http://www.trusecure.com/company/press/pr_20040426.shtml - Annonce de presse
http://www.icsalabs.com/html/communities/ssl-tls/index.shtml - Certification SSL/TLS

DCSSI – CATALOGUE DES PRODUITS QUALIFIES

- **Description**

La **DCSSI** vient de publier une première version de son 'catalogue des produits qualifiés'. Celui-ci regroupe les différentes attestations de sécurité ayant été délivrées par la **DCSSI** correspondant soit à une certification de type 'Critère Communs', soit à une qualification établie en référence à l'un des trois niveaux définis par la DCSSI (standard, renforcé ou élevé), soit encore à un agrément ou une caution jugeant de l'aptitude à assurer la protection d'informations classifiées ou d'informations sensibles.

La version actuelle – V1.1 Avril 2004 – de ce catalogue ne recense que les produits dits 'd'usage général' qualifiés ou en cours de qualification. La liste des produits certifiés au titre du décret 2002-535 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est publiée séparément sur le site du **SSI**.

Rappelons que le processus de qualification s'inscrit en complément du processus d'évaluation et de certification. Il se

positionne selon les définitions du document de référence 'N°001591/SGDN/DCSSI/SDR' décrivant le processus de qualification au niveau standard:

- en amont du processus d'évaluation et de certification « pour accepter la cible de sécurité (ou 'TOE') du produit à évaluer »,
- en aval du processus d'évaluation et de certification pour « vérifier que la certification n'a pas induit de modifications de la cible de sécurité préalablement acceptée, qui seraient de nature à remettre en cause la qualification ».

Le catalogue est accessible en ligne sur le site de la **DCSSI** mais peut aussi être téléchargé sous la forme d'un fichier d'archive de 16Mo contenant une version exploitable en local par le biais d'un quelconque navigateur WEB, soit quelques 187 fichiers principalement aux formats **HTML** et **PDF**.

Les sections 'Accueil', 'Références', 'Certification', 'Qualification' fournissent toutes les informations concernant l'organisation du catalogue, son contenu mais aussi sur les principes, les normes et les méthodes utilisés dans le cadre de la certification et de la qualification des produits recensés.

Les produits sont classés en six catégories fonctionnelles allant de la téléphonie à la signature électronique.

Pour chaque produit sont indiquées les informations suivantes: le fournisseur, la désignation du produit, l'attestation de sécurité délivrée ou visée dans le cas d'un produit en cours de qualification. Les produits recensés dans la version actuelle du catalogue sont au nombre de 15 répartis comme suit:

Catégorie	Produits certifiés	Produits qualifiés	Produits en cours de qualification
Téléphonie			1
Infrastructures de Gestion des Clefs			2
Ressources Cryptographiques			2
Chiffrement IP		**1**	2
Firewall	**2**		3
Signature électronique			2
	=2	**=1**	**=12**

▪ **Complément d'information**

http://www.ssi.gouv.fr/fr/politique_produit/catalogue/index.html	- Présentation du catalogue
http://www.ssi.gouv.fr/fr/politique_produit/catalogue/catalogue.zip	- Catalogue Version 1.1
http://www.ssi.gouv.fr/fr/confiance/certificats.html	- Produits certifiés Critère Communs
http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/Qualification.standardv1.pdf	- Qualification niveau Standard
http://www.ssi.gouv.fr/fr/politique_produit/catalogue/decret2002-535.html	- Décret 2002-535

CRYPTOGRAPHIE

ECC2-109 – DEFI REMPORTE

▪ **Description**

Le 27 avril dernier, la société **CertiCom** a révélé que **Chris Monico** et son équipe de l'université **Texas Tech** avaient remporté le second défi cryptographique de la série '**ECC-109**'. Ce défi fait partie d'une première série de défis lancés en 1997 destinés à démontrer la robustesse de la technologie cryptographique dite à courbes elliptiques ou **ECC** (Elliptic Curve Cryptosystem). Il s'agit de calculer une clef privée de respectivement 109 et 131 bits en ayant simplement connaissance de la clef privée et des paramètres ECC associés.

Pour chaque longueur de clef, deux défis sont proposés, l'un dans le corps '**Fp**' (classe des défis **ECCp**), l'autre dans le corps '**F2m**' (classe des défis **ECC2**). Une seconde série de défis infiniment plus difficile porte sur des tailles de clefs privées de 163, 191, 239 et 359 bits.

La liste complète des défis, et des solutions actuelles, est résumée dans la table ci-dessous:

	Classe 'Fp' – Nombres premiers			Classe 'F2m' – Modulo 2		
Taille	**Nom**	**Calcul estimé (jours)**	**Solutions**	**Nom**	**Calcul estimé (jours)**	**Solutions**
79	*ECC2-79*	*352*	*12/1997*	*ECCp-79*	*146*	*12/1997*
89	*ECC2-89*	*11278*	*02/1998*	*ECCp-89*	*4360*	*01/1998*
95	*ECC2K-95*	*8637*	*05/1998*			
97	*ECC2-97*	*180448*	*09/1999*	*ECCp-97*	*71982*	*03/1998*

109	*ECC2K-108*	*1.3 10^6*	*04/2000*			
	ECC2-109	**2.1 10^7**	04/2004	*ECCp-109*	*9 10^7*	*11/2002*
131	ECC2K-130	2.7 10^9	-			
	ECC2-131	6.6 10^{10}	-	ECCp-131	2.3 10^{10}	
163	ECC2-163	2.9 10^{15}	-	ECCp-163	2.3 10^{15}	
	ECC2K-163	4.6 10^{14}	-			
191	ECC2-191	1.4 10^{20}	-	ECCp-191	4.8 10^{19}	
239	ECC2-238	3.0 10^{27}	-	ECCp-239	1.4 10^{27}	
	ECC2K-238	1.3 10^{26}	-			
359	ECC2-353	1.4 10^{45}	-	ECCp-259	3.7 10^{45}	
	ECC2K-358	2.8 10^{44}	-			

Le défi précédent, **ECCp-109**, avait été solutionné par une équipe de l'école Notre-Dame (Ontario) menée à l'époque par **Chris Monico** moyennant l'utilisation d'un environnement de calcul distribué faisant intervenir 10482 utilisateurs ayant contribué pour un total cumulé de quelques 7092 années de calcul ininterrompu sur un système de type **Pentium** II à 400Mhz. La résolution du défi **ECC2-109** aura demandé un effort distribué équivalent à 1200 années de calcul sur un processeur de type **Athlon** fonctionnant à 3.2Ghz.

Les systèmes commerciaux basés sur la technologie ECC utilisent un espace de 163 bits, ce qui laisse une marge plus que raisonnable contre toute attaque menée en force comme l'ont été toutes les approches ayant permis de solutionner les défis.

- **Complément d'information**

http://www.certicom.com/about/pr/02/021106_ecc_winner.html - Annonce officielle ECCp-109
http://www.certicom.com/index.php?action=company,press_archive&view=307 - Annonce officielle challenge ECCp-109
http://www.nd.edu/~cmonico/eccp109/ - Challenge ECCp-109
http://ecompute.org/ecc2/ - Challenge ECC2-109

CONFERENCES

CANSECWEST 2004 – PREMIER VOLET

- **Description**

L'édition **2004** de la célèbre conférence '**CanSecWest**' s'est tenue du 21 au 23 Avril dernier à **Vancouver**. Les textes des présentations sont partiellement accessibles sur le site officiel.

Nous proposons ci-après au lecteur une présentation synthétique des quelques thèmes ayant attiré notre attention parmi les 19 présentations effectuées. Rendez-vous le mois prochain pour une synthèse de la suite des présentations.

New methods in OS fingerprinting / TCP stack testing — Greg Taleck

L'auteur de la présentation, **Greg Taleck**, travaille pour la société **NFR Security**, société qui s'est fait connaître en 1996 avec son produit de détection d'intrusion 'Network Flight Recorder'. Le thème abordé est celui de '**l'OS Fingerprinting**' ou reconnaissance d'empreintes réseaux, c'est à dire l'identification d'un système d'exploitation à partir des seules caractéristiques des paquets échangés lors de l'ouverture d'une connexion **TCP/IP** vers ce système.

L'idée même de l'existence d'une signature réseau révélatrice de l'identité de l'équipement distant peut apparaître surprenante au premier abord, les piles réseaux étant théoriquement censées toutes répondrent à la même spécification et donc ne pas faire apparaître de comportements caractéristiques. Dans la pratique, mille et un facteurs conduisent à faire apparaître de subtiles différences dans les implémentations: choix fonctionnels laissés au libre arbitre du concepteur (les fameux SHOULD, MUST, MAY des Request for Comments de l'IETF) mais aussi caractéristiques intrinsèques de la plate-forme.

Le concept d'identification **active** ou **passive** par reconnaissance d'empreintes n'est pas récent. Ainsi, la faisabilité d'une identification active avait été démontrée dès 1997 par **Fyodor** et son remarquable outil '**nmap**'. Courant 2000, **Michael Zalewski** démontrait avec '**p0f**', son outil d'analyse passive, que dans certaines conditions le seul paquet '**SYN**' transmis lors d'une demande de connexion révélait assez d'informations caractéristiques pour identifier de nombreux systèmes et équipements. Enfin, **Ofir Arkin** étendait le concept d'identification active en 2001 en substituant le protocole **ICMP** au protocole **TCP/IP**.

Remarquablement performants, les outils d'identification **active** ont cependant un défaut commun qui est de ne pas être suffisamment flexibles pour s'adapter aux différentes situations rencontrées, notamment sur le plan de la configuration des requêtes transmises vers le système cible.

Avec son utilitaire d'identification active '**SynScan**', **Greg Taleck** se propose de palier à ce défaut en offrant un environnement hautement configurable et modulaire. Il est ainsi possible de spécifier la forme et le séquencement des requêtes alimentant en données les modules d'analyse, et ce, que ce soit au niveau d'un service – **HTTP** par exemple – ou plus simplement d'une session **TCP**.

Dans la version actuelle, seize modules élémentaires d'analyse sont proposés qui correspondent chacun à un paramètre significatif:

- Module '**DF**': Détermination du comportement de la pile vis à vis de la fragmentation,
- Module '**SN**': Détermination du comportement de la pile vis à vis de la gestion des numéros de séquence,
- Module '**MS**': Détermination de la taille minimale d'un segment (champ MSS),
- Module '**TL**': Détermination de la durée de vie d'un paquet (champ TTL),

- Module '**HZ**': Détermination de la résolution de l'horodatage,
- Module '**ID**': Détermination de l'algorithme utilisé pour renseigner le champ ID,
- Module '**FP**': Détermination du comportement en cas de fragments se recouvrant,
- Module '**F8**': Détermination de la taille minimale d'un fragment,
- Module '**TP**': Détermination du comportement en cas de paquets se recouvrant,
- Module '**RT**': Détermination de l'algorithme de retransmission d'un paquet SYN,
- Module '**FT**': Détermination de l'algorithme de retransmission d'un paquet FINACK,
- Module '**PT**': Détermination de l'algorithme de retransmission d'un paquet SYNACK,
- Module '**CC**': Détermination du modèle de gestion du contrôle de congestion,
- Module '**CW**': Détermination de la taille de la fenêtre d'acquittement,
- Module '**TO**': Détermination des options 'TCP',
- Module '**WS**': Détermination de la taille initiale de la fenêtre TCP.

La combinaison de chacun de ces paramètres formera le modèle d'une signature tel que le modèle suivant correspondant à un système 'Windows NT, 2K ou XP':

```
fingerprint "Microsoft Windows NT/ 2K/ XP" {
        CC= newreno;
        CW= 3;
        DF= 1;
        HZ= 10;
        ID= R;
        F8= Y;
        FP= last;
        FT= 3,6,12;
        MS= 536;
        PT= 3,6,12;
        RT= 3,6,12,24,48;
        SN= RI( 500000);
        TL= 128;
        TP= first;
        TO= M( 1460)[ NW( 0)][ NNT( N)][ NNS];
        WS= 65535;
};
```

La base de signatures fournie avec la version actuelle de '**synscan**' contient les 25 signatures suivantes:

AIX	3.X
	4.X
	5.X
BSD/OS	4.X
FreeBSD	3.X
	4.X
	5.X
IRIX	6.X

Linux	2.0.X
	2.2.X
	2.4.X
MacOs	X 10.X
	7-9
OpenBSD	3.2
	3.3
	3.4

Solaris	2.X
	7
	8 (2 signatures)
	9
SunOS	4.1.1
Windows	95/98/ME
	NT/2K/XP
	2003/.NET

Les performances de cette approche ont été mesurées par l'auteur en testant '**synscan**', '**nmap**' et '**xprobe2**' sur 4516 systèmes tirés aléatoirement par le biais des services de '**Yahoo!**'. Les résultats de ce test comparatif, extraits de la présentation originale, sont présentés ci-après.

Résultats unitaires	**Cibles**	
Nmap v3.48	2968/4516	65.7%
Xprobe2 v0.2	3218/4516	71.2%
Synscan v0.1	4504/4516	99.7%

Résultats identiques	**Cibles**	
Nmap = Xprobe	1543/2232	69.1%
SynScan = Nmap	1835/2965	61.9%
SynScan = Xprobe	1655/3213	51.5%
SynScan = Xprobe = Nmap	1314/2232	59.0%

http://cansecwest.com/csw04/csw04-Taleck.pdf
http://synscan.sourceforge.net/

Your Network is Talking, Are you listening — Martin Roesch

Martin Roesch, le créateur du célèbre outil de détection d'intrusion '**Snort**', est aussi le directeur technique de la société **SourceFire** qu'il a fondée il y a quelques années pour développer une gamme de produits commerciaux basés sur le moteur de 'snort'.

Intitulée 'Your network is talking, Are you listing', la présentation de **Martin Roesch** vise à démontrer, exemples à l'appui, l'intérêt de combiner l'approche classique jusqu'alors utilisée par les systèmes de détection d'intrusion avec une approche de type '**PNDS**' – **P**assive **N**etwork **D**iscovery **S**ystems'. Cette dernière permet d'automatiser l'établissement d'une cartographie de l'environnement de manière purement passive, c'est à dire par simple écoute et analyse du trafic sur le réseau.

Les données ainsi collectées doivent permettre d'optimiser les fonctionnements des sondes de détection d'intrusion et de réduire en conséquence le nombre de fausses alertes remontées sur les consoles d'administration. L'identification automatique des différentes ressources présentes à un instant donné sur le réseau permettrait par exemple d'éviter la génération d'alertes portant sur un évènement ne nécessitant aucunement une intervention urgente (une tentative d'attaque d'une cible **LINUX** par un ver Windows) quand d'autres évènements critiques seront ignorés (la compromission d'un système via un service actif mais totalement ignoré des exploitants).

Cette présentation, quoique qu'intéressante car présentant notamment deux exemples concrets peu connus de mise en défaut d'un **IDS** classique (diapositives 13 et 14), n'en reste pas moins un plaidoyer commercial en faveur de la technologie '**RNA**' (Real-Time Network Awereness™) annoncée par '**SourceFire**' en août 2003 (Rapport N°64 – 8 Novembre 2003).

http://cansecwest.com/csw04/csw04-Roesch.ppt

Exploit mitigating techniques — Theo de Raadt

Sous titrée '**In OpenBSD, of course**', cette présentation effectuée par l'irrascible '**Theo de Raadt**' s'ouvre sur un dessin représentant le poisson-lune emblématique du système **OpenBSD** déguisé en Robin des bois. Doit-on y voir une allégorie de l'esprit animant l'auteur, détenteur de la seule vérité concernant **OpenBSD** et pourfendeur de tous les hérétiques qui osent prétendre que ce système peut lui aussi être pris en défaut ?

Nous invitons nos lecteurs à aller découvrir de ce pas la page d'accueil du site '**www.openBSD.org**' mise à jour pour l'annonce de la toute nouvelle version **OpenBSD 3.5**, page dans laquelle il est rappelé :

Only one remote hole in the default install, in more than 8 years!

Comme ce fût le cas de la présentation effectuée en 2003 à l'occasion de la même conférence, **Theo de Raadt** dresse un bilan des développements et améliorations fondamentales ayant été intégrés au système **OpenBSD** dans l'optique d'en renforcer son niveau de sécurité sans toutefois casser la compatibilité avec les standards dont POSIX.

- L'intégration du mécanisme de gestion des exceptions de pile '**ProPolice**' dans le compilateur **GCC** dans la version précédente aura été un succès tout comme l'intégration progressive du mécanisme dit '**W^X**' permettant de s'assurer qu'un segment autorisé à l'exécution ne le soit pas à l'écriture. Ce mécanisme a été implémenté sur la majorité des architectures (i386, sparc, sparc64, alpha, m88k, hppa, amd64, ia64) à l'exception du powerpc.
- La mise en œuvre des principes de '**séparation des privilèges**' engagée avec la version 3.3 sur quelques services s'est prolongée avec la refonte des services '**pglogd**', '**bgpd**', '**tcpdump**'. La séparation des privilèges pour les services '**httpd**' et '**isakmp**' est encore en cours d'étude.
- Les fonctions d'allocation mémoire '**malloc()**' et de pagination '**mmap()**' retournent une référence sur un bloc sélectionné aléatoirement. Un pointeur différent sera délivré à chaque appel, à chaque exécution cassant ainsi certaines attaques basées sur la prédictibilité de l'adresse d'allocation. Un mécanisme de pages de garde (dont l'activation est optionnelle) a été mis en œuvre dans ces deux fonctions destiné à détecter les accès effectués en dehors des limites.
- Un nouveau mécanisme de protection en écriture dit '**!W**' est implémenté qui permet de protéger en écriture la liste chaînée de pointeurs de fonctions utilisée par la fonction '_atexit()' lors de la terminaison d'un programme. Cette liste pouvait être utilisée pour insérer un fonction illicite.

Le rythme des évolutions semble s'être ralenti cette année, phénomène qui est peut être corrélé à l'arrêt du financement d'une partie des développements par le **DARPA**. Le système **OpenBSD** n'en reste pas moins la plate-forme Open Source de référence en matière de sécurité, et certainement le seul environnement à considérer la sécurité non pas au sens absolu du terme mais d'un point de vue bien plus pratique et tangible visant en priorité à complexifier le travail d'un éventuel agresseur.

http://cansecwest.com/csw04/csw04-DeRaadt.tgz

Opportunistic Encryption Using IPSec/IKE — Michael Richardson

Plusieurs implémentations des protocoles **IPSec** (chiffrement et authentification des flux IP) et **IKE** (mise à la clef) sont disponibles librement dont la remarquable distribution LINUX proposée par le projet '**FreeS/Wan**'. L'équipe fondatrice annonçait hélas fin avril la fin des développements avec la publication de la toute dernière version, la distribution **FreeSwan 2.06**.

Cet arrêt inattendu trouve officiellement son origine dans le manque de succès du mécanisme dénommé '**O**pportunistic **E**ncryption' - '**OE**' – permettant d'automatiser l'établissement de tunnels **IPSec** avec tout site ayant publié les données requises. On peut cependant imaginer que l'intégration des composants **IPSec** dans la version 2.6 du noyau LINUX et le manque de finances ont pu peser sur cette décision.

Rappelons que l'objectif initial de ce projet était essentiellement politique. Les fondateurs estimaient en effet que la mise à disposition de tous d'un protocole de chiffrement, performant et ne nécessitant aucune configuration, permettrait de garantir la liberté des échanges sans tomber sous la coupe des lois de régulations fleurissant à l'époque notamment aux Etats-Unis.

La situation n'est cependant pas désespérée. Le projet '**OpenSwan**' - fondé à la suite d'une divergence d'opinion avec les membres fondateurs de **FreeS/Wan** – continue en effet de faire vivre une branche dérivée du code initial. Ce nouveau paquetage dispose même d'un support commercial assuré par la société '**Xelerance**' fondée par d'anciens membres du projet **FreeS/Wan** dont **Michael Richardson** l'auteur de la présentation. La boucle est bouclée …

Ce dernier nous propose une très intéressante synthèse des problématiques rencontrées durant le développement de ce qui pourrait passer pour une pure '**utopie**': établir des tunnels sécurisés entre des entités ne se connaissant absolument pas et n'ayant donc aucune raison de se faire confiance, et ce, sur la simple base des données publiées sur un service publique, dans le cas présent, le DNS.

La conclusion de cette présentation est pourtant très positive: '**O**pportunistic **E**ncryption' n'est pas une vue de l'esprit et peut d'ores et déjà être mis en œuvre aussi bien par les clients de bout en bout que par les fournisseurs d'accès. La seule réserve qui puisse être formulée à ce sujet reste celle de la nécessité d'utiliser des DNS sécurisés. Et l'auteur de conclure sur l'excellente protection offerte par **O**pportunistic **E**ncryption'. On le voit, le volet politique n'a pas totalement disparu des revendications de l'équipe 'OpenSwan' !

Diffusé en mars dernier, le paquetage '**OpenSwan V2.1.1**' intègre nombre des fonctionnalités évoluées présentées dont le support du mécanisme 'X-AUTH' et le 'NAT-Traversal' autorisant l'établissement de tunnels à travers des équipements implémentant un mécanisme de translation d'adresse.

Le lecture désireux d'approfondir le sujet pourra se référer avec intérêt à la proposition de standard '**Opportunistic Encryption using The Internet Key Exchange**' – 53 pages - co-éditée par **M.Richardson** et **D.Redelmeier**.

http://cansecwest.com/csw04/csw04-Richardson.pdf

ftp://ftp.nordu.net/internet-drafts/draft-richardson-ipsec-opportunistic-15.txt

Slipping in the Window : TCP Reset attacks — Paul Watson

Cette présentation a fait couler beaucoup d'encre avant même que la conférence **CanSecWest** ne soit ouverte. Les vulnérabilités qui sont détaillées étaient en effet suffisamment critiques pour ne pas pouvoir être divulguées avant que les éditeurs aient été avertis, que les correctifs nécessaires aient été validés et qu'une modification viable du protocole **TCP** ait été étudié (Rapport N°69 – Avril 2004).

Autant dire que le lièvre levé par **Paul Watson** était important: la conception même du protocole **TCP** autorise la mise en œuvre d'une attaque en déni de service d'une redoutable efficacité car permettant de rompre une connexion TCP établie sur un quelconque équipement. Sont potentiellement impactés la totalité des serveurs WEB accessibles depuis l'Internet, de nombreux systèmes personnels sans oublier les innombrables équipements réseaux.

A l'origine de ce problème, les conditions régissant la gestion des drapeaux **RST** et **SYN**, conditions décrites dans le **RFC793** qui stipule que :

> "In all states except SYN-SENT, all reset (RST) segments are validated by checking their SEQ-fields [sequence numbers]. **A reset is valid if its sequence number is in the window**. In the SYN-SENT state (a RST received in response to an initial SYN), the RST is acceptable if the ACK field acknowledges the SYN."

et que

> un paquet '**RST**' destiné à rompre la session sera transmis au cas où un paquet '**SYN**' serait reçu avec un numéro de séquence valide dans la fenêtre d'acquittement.

Ces deux paragraphes, lisibles par tout un chacun, indiquent la méthode à suivre pour casser une connexion en ayant connaissance des adresses IP et des numéros de port de la source et de la destination de cette connexion: il suffit de transmettre un paquet **RST** (ou **SYN**) contenant un numéro de séquence valide dans la fenêtre d'acquittement courante.

Cette technique est couramment utilisée par les dispositifs de sécurité disposant d'une fonction permettant de rompre une connexion active mais détectée comme étant non conforme à la politique de sécurité. Etant à l'écoute du trafic réseau, le dispositif dispose de tous les éléments nécessaires pour transmettre un paquet **RST** forgé de toute pièce mais parfaitement valide.

En faisant abstraction de la notion de fenêtre d'acquittement, un agresseur désireux de forger un paquet **TCP** valide devra obtenir le numéro de séquence qui sera valide pour son paquet. Plusieurs méthodes lui permettront d'optimiser cette recherche notamment dans le cas d'équipements utilisant un procédé de génération de la valeur initiale du numéro de séquence ou '**ISN**' prédictible. Au pire, il lui faudra générer et tester toutes les valeurs possibles, et ce dans un laps de temps très court.

Paul Watson cite ainsi les résultats d'une analyse publiée il y a moins d'un an par deux ingénieurs de la société CISCO à propos des rumeurs concernant la vulnérabilité du protocole '**BGP**':

> Une attaque en aveugle permettrait d'obtenir le bon numéro de séquence en moins de 30mn en transmettant 1 million de paquets par seconde. En tenant compte du caractère aléatoire du numéro de port source, et d'un débit raisonnable de 62500 paquets par seconde, il faudra 142 ans pour déterminer la bonne combinaison.

Ce raisonnement est exact mais il ne tient pas compte de cette fameuse fenêtre d'acquittement dont la taille maximale peut atteindre 65525 paquets voire même dans certaines conditions exceptionnelles 1Go. En pratique, les tailles de fenêtre couramment utilisées vont de 4192 à 16 384 octets.

On conçoit alors que le nombre d'essais requis pour déterminer la bonne combinaison – à savoir un numéro de séquence valide dans une fenêtre – en sera d'autant réduit comme le montre le tableau suivant établi par **Paul Watson** à partir des paramètres standards de quelques équipements classiques:

Equipement	Taille de la fenêtre initiale	Nombre de paquets requis
Efficient Network 5861 DSL router	4096	1 048575
Linux 2.4.18	5840	735439
Nokia IPSO 3.6-FCS6	16384	262143
Cisco IOS 12.2(8)	16384	262143
Cisco IOS 12.1(5)	16384	262143
Cisco IOS 12.0(7)	16384	262143
Cisco IOS 12.0(8)	16384	262143
Windows 2000 5.00.2195 SP1	16384	262143
Windows 2000 5.00.2195 SP3	16384	262143
HP-UX 11	32768	131071
Windows 2000 5.00.2195 SP4	64512	66576
Windows XP Home Edition SP1	64240	66858

Les résultats publiés par l'équipe de **CISCO** dans l'étude intitulée '**BGP Vulnerability Testing: Separating Fact from FUD**' doivent alors être revus avec pour conséquence de réduire le temps d'exploration de 142 ans à seulement 1.6s avec les conséquences qui s'ensuivent.

D'aucuns argumenteront que le problème de la prédiction du numéro de port source reste entier conduisant à accroître la difficulté d'un facteur de 2^{15}. Hélas, il n'en est rien puisque l'algorithme de sélection du prochain numéro de port à allouer est prédictible: incrémentation d'une unité dans le cas des systèmes Windows, LINUX et de 512 unités dans le cas de certaines versions de l'IOS **Cisco**.

Dans la seconde partie de sa présentation, **Paul Watson** décrit l'analyse de vulnérabilité qu'il a menée à la lumière des résultats précédents sur quelques protocoles (**BGP**, **SSL**, **DNS**, **IRC**) ainsi que l'impact du débit utile de la connectivité Internet sur la durée de l'attaque.

Cette analyse ayant - hélas - été confirmée par une série de tests, un processus de notification des organismes d'alertes et des éditeurs a dû être engagé avec des résultats variables mais qui ont conduit certains éditeurs à modifier immédiatement le comportement de la pile **TCP** de leurs équipements. De son coté, l'IETF a entamé une réflexion sur les modifications devant être rapidement apportées au protocole **TCP** dans l'optique de réduire son degré d'exposition à ce genre d'attaques.

http://cansecwest.com/csw04/csw04-Watson.doc

http://www.nanog.org/mtg-0306/pdf/franz.pdf

ftp://ftp.nordu.net/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt

http://www.uniras.gov.uk/vuls/2004/236929/index.htm

ShellForge V2 – Shellcodes for everybody and every platform — Philippe Biondi

En août dernier **Philippe Biondi**, un français, publiait '**ShellForge**' un outil écrit en langage Python permettant d'automatiser la création d'un '**ShellCode**' LINUX, c'est à dire le programme qui sera transféré puis exécuté lors de l'exploitation d'un débordement de buffer survenant dans un quelconque service ou application (Rapport N°62 – Septembre 2003).

Le mode opératoire de cet outil était on ne peut plus simple :

1- Ecrire le code actif du '**ShellCode**' en langage '**C**',

2- Activer le script '**ShellForge**' en indiquant le nom du source '**C**' en paramètre,

3- Assembler le source généré et vérifier son bon fonctionnement en local,

4- Intégrer la table de données générée dans le programme vecteur.

Le '**ShellCode**' ainsi obtenu ne fonctionnera qu'à la condition que l'environnement cible soit identique à l'environnement sur lequel il aura été généré tant au niveau du système d'exploitation qu'au niveau de la **CPU**, la génération finale étant effectuée dans un langage non portable, l'assembleur.

La nouvelle version de l'outil '**ShellCode**', dévoilée à l'occasion de la conférence **CanSecWest**, corrige ce problème et autorise la production d'un code adapté à de multiples plates-formes, à ce jour **i386**, **ARM**, **PA-Risc**, **Sparc**, **Mips** et sous peu **Alpha**, **PowerPC**, **68000** et **S390**.

Cette fonctionnalité a été rendue possible par l'utilisation d'une librairie spécifique, la '**SFLib**', regroupant tous les appels systèmes sous la forme d'autant de macro fonctions, chacune d'entres-elles étant déclinée sur chacun des processeurs supportés. Comme le précise l'auteur, la '**SFLib**' est le pendant 'anémique' de la '**libC**', la librairie contenant tous les appels systèmes et fonctions spécifiques à l'environnement. Utilisée avec un cross compilateur tel 'gcc', cette librairie permettra de générer un binaire adapté au processeur et contenant les appels systèmes ad'hoc.

Plusieurs transformations sont effectuées sur le code assembleur pour obscurcir celui-ci, puis sur le binaire généré afin de rendre celui compatible avec les exigences du protocole utilisé pour transférer le programme vecteur et son shellcode. Le détail de celles-ci pourra être trouvé dans la présentation de **Philippe Biondi**.

http://cansecwest.com/csw04/csw04-Biondi.pdf

Reliable Windows Heap Exploits — Connever & Horovitz

De nombreuses vulnérabilités, pour ne pas dire la majorité des vulnérabilités, trouvent leur origine dans une erreur de programmation liée aux caractéristiques de certains langages dont en particulier le langage '**C**'.

Remarquablement souple, ce langage autorise divers modes d'accès aux données et tableaux de données, notamment par le biais d'une référence à l'adresse de stockage de celle-ci ou 'pointeur'. L'absence de tout mécanisme de contrôle du domaine de validité durant la phase de compilation mais aussi d'exécution conduit à maintenir dans le code final de multiples erreurs de programmation qui pourront rester longtemps non détectées.

Citons parmi les erreurs les plus courantes, les deux erreurs à l'origine de failles les plus régulièrement exploitées:

- Confusion dans les types de données signées / non signées conduisant à utiliser un index de type 'integer' (entier signé) sur la plage de variation d'un entier non signé. Ici encore cette erreur de programmation pourra donner lieu à une vulnérabilité de sécurité si la valeur dudit index peut être modifiée depuis un flux d'entrée de l'application pour prendre une valeur négative.
- Erreur dans l'allocation statique ou dynamique d'un tableau de données, déclaré en indiquant sa taille 'n' et accédé de la position '0' à la position 'n-1'. Cette erreur de programmation conduira à un débordement de pile (données stockées dans la pile) ou de tas (données stockées dans une zone allouée dynamiquement) qui s'il peut être provoqué via l'un des flux d'entrée de l'application pourra conduire à un déni de service, voire à l'exécution d'un code malicieux.

Si les techniques d'exploitation des débordements dans la pile sont légions et désormais parfaitement maîtrisées, il n'en va pas de même avec les débordements dans le tas dont l'exploitation requiert une connaissance approfondie des mécanismes de gestion du tas et du contexte d'exécution de l'application. Ainsi, et à ce jour, aucun code d'exploitation générique d'un débordement dans le tas en environnement WIN32 n'a jamais été publié.

Après avoir étudié en détail les mécanismes de gestion du tas en environnement WIN32, **Matt Connever** de la société **Symantec** (le fondateur du groupe 'W00w00') et **Oded Horovitz** de la société **NAI** ont mis au point un procédé complexe mais efficace permettant d'exploiter un débordement dans le tas sans aucun des inconvénients des procédés précédents.

Il apparaît désormais possible d'envisager disposer de codes d'exploitation de débordements dans le tas fonctionnels sur un système **WIN32** quelque soit son niveau de mise à jour. Fort heureusement, les auteurs de cette présentation annoncent que leur procédé ne fonctionnera pas en environnement **XP SP2**, du moins à la lumière des informations actuellement disponibles sur les modifications apportées par cette nouvelle version dans les mécanismes de gestion du tas.

Le support de présentation contient l'impressionnante et très technique analyse du mécanisme de gestion du tas en environnement WIN32 ainsi qu'un intéressant comparatif de différents procédés d'exploitation à ce jour divulgués. Une présentation à réserver aux passionnés du sujet étant donnée la technicité de celui-ci …

http://cansecwest.com/csw04/csw04-Oded+Connover.ppt

http://www.w00w00.org/files/articles/heaptut.txt

Why honeypots sucks — Lance Spitzner

Présentée par **Lance Spitzner**, un spécialiste de la sécurité et en particulier des pare-feux CheckPoint, cette conférence traite des aspects négatifs de l'utilisation des pièges et leurres dénommés 'pots de miel' ou 'honeypots' dans le jargon. Une fois identifiés, ces dispositifs peuvent en effet être retournés contre leurs utilisateurs et devenir de redoutables outils de désinformation.

Trois classes de problèmes sont ici identifiées:

- La mise à disposition des sources de la majorité des implémentations conduisant à dévoiler certaines caractéristiques et spécificités fort utiles pour lever le doute et identifier sans risque d'erreur un pot de miel,
- Les vulnérabilités susceptibles d'être exploitées pour prendre le contrôle du pot de miel, et éventuellement identifier les autres composantes actives dans le cas d'un réseau de pots de miel ou 'honeynet',
- La qualité de la 'récolte' dont idéalement celle-ci devrait permettre d'identifier de nouvelles techniques ou encore de mettre en évidence l'existence de réseaux organisés mais qui bien souvent ne permet de ferrer que du menu fretin.

http://cansecwest.com/csw04/csw04-Spitzner.ppt

Bluetooth : Red Fang, Blue Fang — Ollie Whitehouse

Avec cette présentation, l'une des équipes de la société '@Stake' s'attaque à démontrer la vulnérabilité de la seconde grande famille d'équipements sans fil, à savoir les dispositifs 'BlueTooth'.

Les quatre attaques connues à ce jour sont tout d'abord détaillées:

- Recherche des dispositifs activés en mode discret (non discoverable) par interrogation active sur toute la plage d'adressage **BlueTooth** soit tout au plus 2^{48} essais. L'outil '**RedFang**', développé par **@Stake** a fait l'objet d'une mise à jour récente permettant d'accélérer cette recherche.
- Recherche des services actifs mais cachés par parcours systématique des ports sans passer par l'annuaire des services **SDP** (Service Protocol Discovery). A ce jour, aucun service caché n'a pu être découvert.
- Transfert d'informations depuis certains équipements mal configurés dont des cartes de visite ou encore des images via le protocole **OBEX** en mode **PUSH**,
- Récupération depuis certains équipements mal configurés d'informations variées (dont la liste dépend du fournisseur de l'équipement) via le protocole **OBEX** en mode **PULL**.

Les auteurs dévoilent ensuite une toute nouvelle série d'attaques cryptographiques basées sur les caractéristiques de la version 1.2 du protocole BlueeTooth. Ces attaques permettent de récupérer les deux secrets requis pour régénérer la clef de session et par conséquent pour déchiffrer hors ligne certains échanges **BlueTooth**.

Les deux premières attaques permettent de révéler le code d'accès du dispositif ou '**PIN**' :

- soit en ligne par recherche systématique de celui-ci s'il est codé en dur dans le dispositif en changeant l'adresse utilisée pour l'attaque à chaque essai dans le but de contourner le délai de réponse incrémenté à chaque erreur sur le code présenté par un même dispositif.
- soit hors ligne en capturant les données échangées durant la phase d'authentification puis en testant tous les codes confidentiels possibles sur un programme de simulation jusqu'à obtenir les données acquises. Les performances annoncées conduisent à pouvoir envisager de révéler un code de 6 chiffres en moins de 12 secondes mais il faudra plus de 4000 ans dans le cas d'un code de 16 chiffres.

Ce dernier procédé permet aussi de recouvrir la clef de liaison '**Kc**'. On notera cependant que la capture des échanges nécessite de disposer d'un matériel spécifique, les dispositifs BlueTooth n'offrant aucune fonction d'acquisition contrairement aux dispositifs dits 'WiFi'. Les auteurs recommandent cependant de mettre en place les contre-mesures suivantes:

- ne jamais engager d'association dans un contexte potentiellement hostile, c'est à dire non maîtrisé,
- utiliser, lorsque cela est possible, le plus long code confidentiel autorisé par le dispositif.

La présentation se clôt sur une recette permettant de modifier un dispositif **BlueTooth** en lui adjoignant une antenne à haut gain dans l'optique d'augmenter la portée. En utilisant une antenne Yagi offrant un gain de 14dB, les auteurs ont pu étendre celle-ci à quelque 150m, une distance amplement suffisante pour assurer la plus grande discrétion.

http://cansecwest.com/csw04/csw04-Whitehouse.pdf

http://www.thebunker.net/release-bluestumbler.htm

▪**Complément d'information**

http://www.cansecwest.com/resources.html - Accès aux présentations de CanSecWest 2004

METHODES

NIST – SP800-58 / SECURITY CONSIDERATIONS FOR VOICE OVER IP SYSTEMS

- **Description**

Le '**NIST**' propose à la relecture le document **SP800-58** intitulé '**Security Considerations for Voice Over IP Systems**' qui prend la forme d'un mémorandum traitant de la sécurité des protocoles et systèmes assurant le transport de la voix sur les réseaux **IP**.

SIP, **H323**, **H245**, **MegaCo**, **MGCP**, **GateKeeper**, … autant de sigles et acronymes traitant d'un seul et unique sujet: l'établissement d'une communication vocale entre deux intervenants dont l'un au moins utilise un dispositif connecté à un réseau **IP**, équipement dont la mobilité conduira à devoir considérer le problème de la localisation au même titre que celui de la sécurité.

Si la sécurisation des communications téléphoniques et la protection des équipements associés pouvaient être traitées en toute indépendance il y a quelques années de par l'utilisation de réseaux spécifiques et dédiés, l'avènement du tout digital a notablement modifié la donne à la fin des années 90 avec l'arrivée de technologies pouvant être considérées comme matures et performantes. Il n'est ainsi plus possible d'envisager pouvoir continuer à maintenir la séparation entre voix et données sur le plan physique mais aussi sur le plan logique ouvrant la porte à une nouvelle classe de problèmes de sécurité.

En 2002, un article intitulé '**How VoIP is changing the network security equation**' mettait en garde contre les risques engendrés par ces technologies pour lesquelles la sécurité n'était considérée que du point de vue réseaux sans prendre en compte les spécificités des flux de données transportées. Mais il aura fallu l'apparition d'utilitaires capables de restituer sur une simple carte son le contenu de paquets interceptés sur le réseau sans aucun a priori sur le format utilisé – dont **VOMIT** publié dès décembre 2001 - pour déclencher une réelle prise de conscience.

Le mémorandum publié par le **NIST** vient à point en offrant à la fois une très didactique introduction aux technologies phares et une excellente synthèse des solutions de sécurisation et de protection susceptibles d'être mises en place.

La première moitié de ce document de 91 pages est ainsi entièrement consacrée à une comparaison détaillée des avantages et inconvénients des deux protocoles leaders (**H323** et **SIP)** sur le plan de la sémantique des échanges et de l'impact de celle-ci sur les mécanismes de filtrage et leur performance. Un chapitre est en plus spécialement consacré aux protocoles '**Megaco**' et '**MGCP**' employés entre les passerelles d'accès dites '**Media Gateway**' et leurs contrôleurs.

La seconde moitié du document traite des problématiques rencontrées avec les équipements de filtrage et de sécurité classiques qui pour des raisons principalement de performance n'interprètent que très partiellement les protocoles qu'ils sont chargés de surveiller. Etendre les fonctionnalités de filtrage et les traitements liés aux mécanismes de translation d'adresse conduirait à devoir analyser l'intégralité du protocole, et par conséquent à implémenter les fonctions de décodage ad'hoc avec pour conséquence de dégrader la qualité de service en modifiant notamment le temps de latence d'un paquet. Il en va de même avec les mécanismes de chiffrement et les dispositifs cryptographiques qui, en l'absence d'un mécanisme de gestion des priorités, introduisent des variations de débits et des temps de transit impactant fortement la qualité de service.

La solution à de nombreux problèmes est très certainement dans l'utilisation d'une infrastructure s'appuyant sur le protocole 'SRTP' – Secure Real Time Protocol – pour assurer le transport des données multi-média (voix et vidéo) et privilégiant l'utilisation de réseaux privés établis de bout en bout par les équipements d'accès multi-média.

La table des matières de ce guide est reproduite ci-dessous :

1 Introduction
2 Overview of VOIP
2.1 VOIP Equipment
2.2 Overview of VOIP Data Handling
2.3 Cost
2.4 Speed and Quality
2.5 VOIP Security Issues
3 Quality of Service Issues
3.1 Latency
3.2 Jitter
3.3 Packet Loss
3.4 Bandwidth & Effective Bandwidth
3.5 The Need for Speed
4 H.323
4.1 H.323 Architecture
4.2 H.235 Security Profiles
4.2.1 H.235v2
4.2.2 H.235v3
4.2.3 H.323 Annex J
4.2.4 H.323 Security Issues
5 SIP
5.1 SIP Architecture
5.2 Existing Security Features within the SIP Protocol
5.2.1 Authentication of Signaling Data using HTTP Digest Authentication
5.2.2 S/MIME Usage within SIP
5.2.3 Confidentiality of Media Data

5.2.4 TLS usage within SIP
5.2.5 Ipsec usage within SIP
5.2.6 Security Enhancements for SIP
5.2.7 SIP Security Issues
6 Gateway Decomposition
6.1 MGCP
6.1.1 Overview
6.1.2 System Architecture
6.1.3 Security Considerations
6.2 Megaco/H.248
6.2.1 Overview
6.2.2 System Architecture
6.2.3 Security Considerations
7 Firewalls, Address Translation, and Call Establishment
7.1 Firewalls
7.1.1 Stateful Firewalls
7.1.2 VOIP specific Firewall Needs
7.4 Network Address Translation
7.5 Firewalls, NATs, and VOIP Issues
7.5.1 Incoming Calls
7.5.2 Firewalls, NATs, and QoS
7.5.3 Firewalls and NATs
7.6 Call Setup Considerations with NATs and Firewalls
7.6.1 Application Level Gateways
7.6.2 Firewall Control Proxies and Middleboxes
7.6.3 Proxies – Internal & External
7.7 Mechanisms to solve the NAT problem
7.8 Virtual Private Networks and Firewalls
8 Encryption & Ipsec
8.1 Ipsec
8.2 The Role of Ipsec in VOIP
8.3 Local VPN Tunnels
8.4 Difficulties Arising from VOIPsec
8.5 Encryption / Decryption Latency
8.6 Scheduling and the Lack of QoS in the Crypto-Engine
8.7 Expanded Packet Size
8.8 Ipsec and NAT Incompatibility
9 Solutions to the VOIPsec Issues
9.1 Encryption at the End Points
9.2 Secure Real Time Protocol (SRTP)
9.3 Key Management for SRTP – MIKEY
9.4 Better Scheduling Schemes
9.5 Compression of Packet Size
9.6 Resolving NAT/Ipsec Incompatibilities
10 Planning for VOIP Deployment
References
A Appendix: VOIP Risks, Threats, and Vulnerabilities
A.1 Confidentiality and Privacy
A.2 Integrity Issues
A.3 Availability and Denial of Service
B Appendix: VOIP Frequently Asked Questions
C Appendix: VOIP Terms

Le document **SP800-58** est très certainement amené à devenir un document de référence qui occupera une place de premier choix dans la bibliothèque du responsable de sécurité et de tout intervenant amené à travailler dans le domaine de la téléphonie sur IP.

L'annexe 'A' contient une intéressante synthèse des risques, menaces et vulnérabilités touchant les réseaux **VoIP** sur le plan de l'intégrité, de la confidentialité et de la disponibilité. Cette lecture pourra être complétée par la très intéressante étude intitulée '**Sécurité Analysis: Traditional Telephony and IP Telephony**' publiée dans la salle de lecture virtuelle du Sans Institute.

- **Complément d'information**

http://csrc.nist.gov/publications/drafts/NIST_SP800-58-040502.pdf	- Guide SP800-58
http://www.eetimes.com/story/OEG20021014S0072	- Article de P.Bednarz
http://www.sans.org/rr/papers/index.php?id=924	- Etude du SANS
http://vomit.xtdnet.nl/	- VOMIT, l'outil d'acquisition et de restitution

NIST – ETAT DES GUIDES DE LA SERIE SP800

- **Description**

La publication pour commentaire des guides **SP800-58 'Security Considerations for Voice Over IP Systems'** et SP800-66 '**An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule**' nous amène à proposer une mise à jour du tableau récapitulatif des publications récentes de la série spéciale '**SP800**'.

SP800-26	Security Self-Assessment Guide for Information Technology Systems	[F]	11/2001
SP800-27	Engineering Principles for Information Technology Security – Rev A	[R]	01/2004
SP800-28	Guidelines on Active Content and Mobile Code	[F]	10/2001

SP800-29	Comparison of Security Reqs for Cryptographic Modules in FIPS 140-1 & 140-2	[F]	10/2001
SP800-30	Underlying Technical Models for Information Technology Security – Rev A	[R]	01/2004
SP800-31	Intrusion Detection Systems	[F]	11/2001
SP800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	[F]	02/2001
SP800-33	Underlying Technical Models for Information Technology Security	[F]	12/2001
SP800-34	Contingency Planning Guide for Information Technology Systems	[F]	06/2002
SP800-35	Guide to Selecting IT Security Products	[*]	10/2003
SP800-36	Guide to IT Security Services	[*]	10/2003
SP800-37	Guidelines for the Security C&A of Federal Information Technology Systems	[R]	04/2004
SP800-38	Recommendation for Block Cipher Modes of Operation	[F]	12/2001
SP800-40	Applying Security Patches	[F]	09/2002
SP800-41	Guidelines on Firewalls and Firewall Policy	[F]	01/2002
SP800-42	Guidelines on Network Security testing	[*]	10/2003
SP800-43	System Administration Guidance for Windows2000	[R]	01/2002
SP800-44	Guidelines on Securing Public Web Servers	[F]	09/2002
SP800-45	Guide On Electronic Mail Security	[F]	09/2002
SP800-46	Security for Telecommuting and Broadband Communications	[F]	09/2002
SP800-47	Security Guide for Interconnecting Information Technology Systems	[F]	09/2002
SP800-48	Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices	[R]	07/2002
SP800-49	Federal S/MIME V3 Client Profile	[R]	11/2002
SP800-50	Building an Information Technology Security Awareness & Training Program	[F]	03/2003
SP800-51	Use of the Common Vulnerabilities and Exposures Vulnerability Naming Scheme	[F]	09/2002
SP800-53	Minimum Security Controls For Federal Information Technology Systems	[D]	
SP800-53a	Techniques & Procedures for the verification of Security Controls in Fed. ITS	[D]	
SP800-55	Security Metrics Guide for Information Technology Systems	[F]	07/2003
SP800-56	Recommendation on Key Establishment Schemes	[D]	01/2003
SP800-57	Recommendation on Key Management	[D]	01/2003
SP800-58	Security Considerations for Voice Over IP Systems	[D]	05/2004
SP800-59	Guideline for Identifying an Information System as a National Security System	[F]	08/2003
SP800-61	Computer Security Incident Handling Guide	[F]	01/2004
SP800-60	Guide for Mapping Types of Information & Information Systems to Security Categories	[R]	03/2004
SP800-63	Recommendation for Electronic Authentication	[R]	01/2004
SP800-64	Security Considerations in the Information System Development Life Cycle	[F]	10/2003
SP800-65	Recommended Common Criteria Assurance Levels	[D]	02/2004
SP800-66	An Introductory Resource Guide for Implementing the HIPAA Security Rule	[D]	05/2004
SP800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	[D]	04/2004

[F] Finalisé
[*] Récemment finalisé
[R] Pour commentaire et relecture
[D] En cours de développement

- **Complément d'information**

http://csrc.nist.gov/publications/nistpubs/index.html

TENDANCES

GOOGLE ET L'ENREGISTREMENT DES NOMS DE DOMAINE

- **Description**

L'annonce de l'introduction de **Google** en Bourse a inspiré de nombreuses personnes. En avril, on a recensé l'enregistrement de plus de 469 noms de domaines contenant la chaîne de caractères "google", dont un "francegoogle.com", mais aucun n'émanait de la société **Google** !

En mai il y a eu 492 enregistrements dont 8 par la société **Google**, un par la société **Yahoo** (yahoo-backdoor.com) et un "googlefrance.com". On notera à ce propos l'enregistrement de certains noms de domaine qui font clairement penser à du "typo-squatting".

Les statistiques par extension donnent ainsi:

extensions	Avril 2004	Mai 2004	Total	Pourcentage
".biz"	12 noms	4 noms	16 noms	1,7 %
".com"	342 noms	404 noms	746 noms	78,4 %
".info"	18 noms	4 noms	22 noms	2,3 %
".net"	67 noms	44 noms	111 noms	11,7 %
".org"	17 noms	19 noms	36 noms	3,8 %
".us"	13 noms	5 noms	18 noms	1,9 %
".ws"	-	2 noms	2 noms	0,2 %
Total	469 noms	483 noms	952 noms	100 %

Ce phénomène n'est pas nouveau, puisque le nom de la société **Microsoft** et de ses produits sont régulièrement déposés sous différentes formes. Les décisions de l'**OMPI** en font état quasiment tous les mois.

Année	Exemples de noms de domaines contestés

2000	wwwmicrosoft.com, microsof.com, microsoft.org, microsofthome.com, microsoftnetwork.com
2001	microosoft.com, microsofthealth.com
2002	microesoft.com, microsoftsite.com, microsoftcertified.com, microsoftcertified.info
2003	microsoftcorp.com
2004	micorosft.com, microsoftcorporation.com, microsoftmail.com, microsftmall.com, microsoftbasics.com, microsoft-com.com, msnmall.com

▪**Complément d'information**

http://www.resourceshelf.com/2004/google_names_1.htm - Nom en '*google*.*' enregistrés en avril 2004

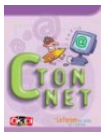
http://www.resourceshelf.com/2004/google_names_2.html - Nom en '*google*.*' enregistrés en mai 2004

LA LEGISLATION

DROITS DE L'INTERNET

FR – LE DROIT SUR L'INTERNET EXPLIQUE A TOUS

▪**Description**



En association avec plusieurs partenaires dont la revue **Okapi**, l'**UNAF**, **Wanadoo** et les Ministères de la Famille et de la Recherche et des Nouvelles Technologies, le **Forum des Droits sur l'Internet** publie deux remarquables brochures destinées à informer les jeunes – mais aussi les moins jeunes – des règles et des lois qui régissent cet espace ouvert qu'est l'Internet.

Disponible au format 'PDF', la brochure '**C Ton NET**' s'adresse au public des adolescents voire même des plus jeunes dans une forme simple, graphique et percutante par l'utilisation d'un vocabulaire quelques fois très direct et d'exemples adaptés. Un Quiz permet d'introduire les concepts techniques élémentaires utilisés par la suite: 'cookie', 'spam', 'e-mail', 'lien', 'moteur de recherche', 'forum', … Les problématiques liées à l'utilisation de l'Internet sont ensuite abordées autour des six thèmes suivants:

- Les **discussions** et les problèmes associés à l'anonymat, à la confidentialité des échanges, à la teneur de ceux-ci et aux principes de bonne conduite et règles de politesse régissant toutes les formes de sociétés y compris les sociétés 'virtuelles',
- La **musique** et les infractions susceptibles d'être commises par l'intermédiaire des réseaux d'échanges et autres pratiques frauduleuses,
- L'**image** et l'atteinte au droit à l'image, voire plus largement l'utilisation abusive de tout document protégé par le droit d'auteur,
- Le **risque**, qu'il soit d'ordre technique avec les problèmes générés par les virus et autres codes malicieux, d'ordre moral avec les traumatismes susceptibles d'être provoqués par la violence de certains contenus notamment pornographiques pourtant parfaitement légaux ou encore d'ordre économique avec les offres de toutes sortes associées à l'obtention d'un identifiant via des numéros surfacturés,
- La **confidentialité** avec les nuisances provoquées par l'utilisation abusive des adresses de messagerie ou d'informations collectées par le biais de formulaires divers et variés,
- La **désinformation** provoquée par les fausses informations, canulars ou 'hoax', régulièrement transmises à tout propos: virus, blagues, chaînes de solidarités, …

La brochure '**Parents, l'internet est à vous**' reprend la même thématique en insistant plus particulièrement sur les risques encourus dans le cas de délits accomplis par des mineurs. On en retiendra l'absolue nécessité d'un accompagnement éducatif des jeunes destiné à inculquer les principes et règles de base dans un environnement virtuel dans lequel les biens immatériels et intangibles n'apparaissent pas toujours être soumis aux obligations et contraintes du monde réel.

Nous ne pouvons que recommander la lecture de ces deux brochures dont nous espérons qu'elles seront largement diffusées au sein des familles mais aussi en milieu scolaire.

▪**Complément d'information**

http://www.droitdunet.fr/telechargements/ctnet_hd_ados.pdf - Brochure destinées adolescents

http://www.droitdunet.fr/telechargements/ctnet_hd_parents.pdf - Brochure destinées parents

GOUVERNANCE DE L'INTERNET

FR – OUVERTURE DU '.FR'

▪**Description**

La gestion de l'extension de domaine '**.fr**' est en phase de migration d'un mode régulé par une autorité centrale, l'AFNIC, à un mode plus libéral à l'instar des domaines '.com', '.net' ou de nombreuses extensions nationales.

La règle à terme sera celle du 'premier arrivé, premier servi', comme celle qui a cours pour les principaux domaines génériques ('.com', '.net', '.org' ...). Il s'agit donc de la fin d'une autre 'exception culturelle française' avec cet abandon du 'droit au nom'. Toute personne pourra ainsi demander l'enregistrement d'un nom de domaine en '.fr' sans avoir à justifier d'un droit de propriété sur le nom demandé.

Cette 'phase d'ouverture', pour reprendre le terme utilisé par l'AFNIC, s'effectue en deux étapes:

- La première a démarré le 11 mai dernier, date à partir de laquelle toutes les personnes identifiables en ligne sur des bases de données publiques et nationales (entreprises, artisans, associations immatriculées à l'INSEE, détenteurs de marques...) pouvaient obtenir le nom de domaine qu'elles souhaitaient sans que ce dernier figure sur quelque document que ce soit.

  Afin de pouvoir gérer correctement l'afflux attendu de demandes, la phase initiale d'enregistrement s'est étalée sur 4 jours, du 11 au 14 mai :

  - 11 mai: les noms de domaine commençant par les lettres 'a' et 'b' ainsi que par les chiffres '0' à '9',
  - 12 mai: extension aux noms de domaine commençant par les lettres 'c' à 'f',
  - 13 mai: extension aux noms de domaine commençant par les lettres 'g' à 'n',
  - 14 mai: extension aux noms de domaine commençant par les lettres 'o' à 'z',

  Avec 49 716 demandes de dépôts de noms cette semaine, cela correspond à une croissance de près de 25 % du domaine français puisque l'on passera de 190.500 domaines gérés par l'AFNIC à plus de 242.000.

  Voici les chiffres fournis par l'AFNIC :

Messages reçus	de 9h00 à 9h05	de 9h00 à 9h15	dans la journée	Noms distincts	Noms les plus demandés
11 mai	33 994	46 362	52 365	6 685	avion.fr, bio.fr, assurance-auto.fr, blague.fr, appareil-photo.fr
12 mai	31 249	39 437	52 319	12 768	cheveux.fr, email.fr, e-commerce.fr, emploi.fr, charme.fr
13 mai	40 281	46 714	62 347	16 219	montagne.fr, maisons.fr, internet.fr, lille.fr, luxe.fr
14 mai	44 104	55 148	64 463	18 419	robot.fr, site-internet.fr, portes.fr, surveillance.fr, patron.fr
sur 4 jours	149 628	187 661	231 302	49 716	

- La seconde étape se déroulera début 2005, les nouvelles conditions pour l'enregistrement en '.fr' étant alors étendues aux particuliers, aux associations non immatriculées à l'INSEE ... bref, à tout le monde.

L'AFNIC a publié plusieurs documents et communiqués traitant aussi des litiges qui ne manqueront pas d'être soulevés. Ainsi, les procédures alternatives de résolution des litiges (PARL) pour les noms de domaine '.fr' sont gérées par deux centres de médiation :

- le **CMAP** (Centre de Médiation et d'Arbitrage de Paris — http://www.cmap.asso.fr/),
- le Centre d'arbitrage et de médiation de l'**OMPI** (Organisation Mondiale de la Propriété Intellectuelle).

Trois critères principaux ont été pris en considération pour effectuer ce choix :

- des délais courts, entre un et deux mois maximum pour traiter un litige,
- des coûts réduits, inférieurs à 1.500 Euros,
- la possibilité de pouvoir faire appel des avis rendus devant les tribunaux.

La protection des noms et des marques est plus que jamais à prendre en considération. On ne peut que conseiller de s'intéresser (de nouveau) à cette problématique, aujourd'hui pour le domaine français ou les autres extensions génériques ou nationales, et d'ici à la fin de l'année pour l'extension européenne '**.eu**'.

▪Complément d'information

http://www.afnic.fr/actu/nouvelles/nommage /CP20040120 - Annonce de janvier 2004 sur la phase d'ouverture

http://www.afnic.fr/doc/ref/juridique/parl - Communiqué sur les procédures alternatives

http://www.afnic.fr/data/chartes/charte310304_V4.pdf - Nouvelle charte de nommage '.fr' au format PDF

EU – LA LONGUE ROUTE VERS LA CREATION DU TLD 'EU'

▪Description

C'est en 2000 que l'annonce de la création d'une extension de domaine européen '.eu' sur Internet a été faite. Puis le 25 mars 2002, le Conseil des Ministres Européen avait approuvé le règlement sur le ccTLD '**.eu**', par la résolution 733/2002. Le registre ne devait cependant être ouvert qu'après l'appel à manifestation d'intérêt publié au Journal Officiel dans le courant de l'été 2002.

Dans le rapport mensuel N°47 de juin 2002, nous faisions alors état des risques d'abus sur la réservation des noms de domaines en '**.eu**'. En effet, aucune société ne pouvait alors prétendre faire une quelconque réservation de nom de domaine en '**.eu**' et l'**AFNIC** avait publié un avertissement sur le site Gouvernance de l'Internet.

En février 2004, la Commission Européenne annonçait enfin que les sociétés et les particuliers de pays membres de l'Union Européenne, pourraient commencer à utiliser les noms de domaines en '**.eu**' à partir de novembre 2004, après une période de pré-enregistrement qui devait commencer en septembre 2004.

Le 10 mars 2004, le 'Communications Committee' de la Communauté Européenne approuvait un document de travail de la Commission de Régulation qui spécifie les règles ('**PPR**' ou 'Public Policy Rules') concernant l'implémentation et les fonctions du 'Top Level Domain' pour le domaine '**.eu**'.

Enfin, le 28 avril 2004, la Commission des Communautés Européennes publiait le règlement numéro 874/2004 établissant les règles de politique d'intérêt général relatives à la mise en œuvre et aux fonctions du domaine de

premier niveau '.eu' et les principes applicables en matière d'enregistrement.

Les négociations de l'EURid (the European Registry of Internet Domain names) avec l'ICANN pour mettre en place ce domaine '.eu' sont donc désormais possibles.

Le nouveau planning prévisionnel "remis à jour", consultable sur le site de l'EURid, est le suivant :

- mai et juin 2004: préparation et traduction des documents,
- juin et juillet 2004 : choix de registrars pour le domaine '.eu',
- aux environs de décembre 2004 : début de la période de pré-enregistrement,
- aux environs d'avril 2005: ouverture du domaine '.eu'.

Il reste donc encore 6 à 8 mois avant de pouvoir faire des pré-enregistrements, et presque 1 an avant que ce domaine ne voit vraiment le jour. Les entreprises disposent donc encore de quelques mois pour se positionner et faire un choix stratégique quant à leur visibilité sur l'Internet Européen.

D'ici là, on peut s'attendre à recevoir de nombreuses sollicitations pour pré-réserver, pré-enregistrer, pré-valider, ... bref, pour soit-disant "préserver" nos chances d'être visibles en 'Europe', et particulièrement en France, où la "libéralisation" bien que préparée et contrôlée a plus ressemblé à un sprint matinal qu'à une course d'endurance (voir article sur le domaine '.fr').

▪Complément d'information

http://www.eurid.org/Information/timetable.html - Calendrier prévisionnel
http://europa.eu.int/eur-lex/pri/fr/oj/dat/2004/l_162/l_16220040430fr00400050.pdf - Texte de la Commission Européenne
http://europa.eu.int/eur-lex/en/archive/2002/l_11320020430en.html - Annonce de la création de l'extension '.eu'
http://europa.eu.int/eur-lex/pri/fr/oj/dat/2002/l_113/l_11320020430fr00010005.pdf - Résolution 733/2002
http://europa.eu.int/information_society/topics/telecoms/internet/eu_domain/index_en.htm
http://europa.eu.int/information_society/topics/.../index_en.htm#pre-register

LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RÉSEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.2.3	23/10/03	http://www.isc.org/
		8.4.4	25/01/04	
DHCP	Serveur d'adresse	3.0p2	15/01/03	http://www.isc.org/
NTP4	Serveur de temps	4.2.0	15/10/03	http://www.ntp.org/downloads.html
WU-FTP	Serveur de fichiers	2.6.2**p**	28/08/03	http://www.wu-ftpd.org

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2004	10/05/04	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.5	13/03/03	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
POPA3D	Relevé courrier	0.6.4	17/11/03	http://www.openwall.com/popa3d/
SENDMAIL	Serveur de courrier	8.12.11	18/01/04	ftp://ftp.sendmail.org/pub/sendmail/RELEASE_NOTES

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.31	11/05/04	http://httpd.apache.org/dist
		2.0.49	18/03/04	
ModSSL	API SSL Apache 1.3.31	2.8.17	11/05/04	http://www.modssl.org
MySQL	Base SQL	3.23.58	11/09/03	http://dev.mysql.com/doc/mysql/en/News-3.23.x.html
		4.0.20	17/05/04	
SQUID	Cache WEB	2.5s5	01/03/04	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
INN	Gestion des news	2.4.1	07/01/04	http://www.isc.org/
MAJORDOMO	Gestion des listes	1.94.5	15/01/00	http://www.greatcircle.com/majordomo
OpenCA	Gestion de certificats	0.9.1.8	16/03/04	http://www.openca.org/openca/download-releases.shtml
OpenLDAP	Gestion de l'annuaire	2.2.11	21/04/04	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/
OpenReg	Gestion DNS	1.0.2	22/03/04	http://www.isc.org/sw/openreg/

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
SPLINT	Analyse de code	3.1.1	25/05/03	http://lclint.cs.virginia.edu
Perl	Scripting	5.8.4	22/04/04	http://www.cpan.org/src/index.html
PHP	WEB Dynamique	4.3.6	15/04/04	http://www.php.net/downloads.php
		5.0rc2	25/04/04	

ANALYSE RÉSEAU

Nom	Fonction	Ver.	Date	Source
Big Brother	Visualisateur snmp	1.9^{e}	02/01/04	http://bb4.com/
Dsniff	Boite à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.6.b	03/07/03	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.10.4	13/0(/04	http://www.ethereal.com
IP Traf	Statistiques IP	2.7.0	19/05/02	http://cebu.mozcom.com/riker/iptraf/
Nstreams	Générateur de règles	1.0.3	06/08/02	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boite à outils	1.14	10/12/99	http://www.samspade.org/ssw/
TcpDump	Analyse multiprotocole	3.8.3	30/03/04	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.8.3	30/03/04	http://www.tcpdump.org/
TcpFlow	Collecte données	0.21	07/08/03	http://www.circlemud.org/~jelson/software/tcpflow/
TcpShow	Collecte données	1.81	21/03/00	http://ftp7.usa.openbsd.org/pub/tools/unix/sysutils/tcpshow

🗁	**WinPCap**	Acquisition Trame	3.1b3	15/05/04	http://winpcap.polito.it/news.htm

ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	5.32	23/03/03	http://www.analog.cx
fwLogWatch	Analyse log	1.0.0	25/04/04	http://cert.uni-stuttgart.de/projects/fwlogwatch/
SnortSnarf	Analyse Snort	021111	02/11/02	http://www.silicondefense.com/software/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SÉCURITÉ

Nom	Fonction	Ver.	Date	Source
FIRE	Boite à outils	0.4a	14/05/03	http://sourceforge.net/projects/biatchux/
curl	Analyse http et https	7.11.2	26/04/04	http://curl.haxx.se/
Nessus	Vulnérabilité réseau	2.0.10	22/01/04	http://www.nessus.org
Nikto	Analyse http et https	1.32	17/12/03	http://www.cirt.net/nikto/UPDATES/1.32/CHANGES.txt
Nmap	Vulnérabilité réseau	3.50	18/01/04	http://www.insecure.org/nmap/nmap_download.html
Pandora	Vulnérabilité Netware	4.0b2.1	12/02/99	http://www.packetfactory.net/projects/pandora/
🗁 **Saint**	Vulnérabilité réseau	5.4	17/05/04	http://www.saintcorporation.com/updates.html
🗁 **Sara**	Vulnérabilité réseau	5.0.5b	25/05/04	http://www.www-arc.com/sara/downloads/
Tara (tiger)	Vulnérabilité système	3.0.3	15/08/02	http://www-arc.com/tara
Trinux	Boite à outils	0.89	02/08/03	http://sourceforge.net/projects/trinux/
Whisker	LibWhisker	2.0	27/02/03	http://www.wiretrip.net/rfp/p/doc.asp?id=21

CONFIDENTIALITÉ

Nom	Fonction	Ver.	Date	Source
OpenPGP	Signature/Chiffrement			http://www.openpgp.org
GPG	Signature/Chiffrement	1.2.4	24/12/03	http://www.gnupg.org

CONTRÔLE D'ACCÈS

Nom	Fonction	Ver.	Date	Source
TCP Wrapper	Accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers
Xinetd	Inetd amélioré	2.3.13	01/02/04	http://synack.net/xinetd/

CONTRÔLE D'INTÉGRITÉ

Nom	Fonction	Ver.	Date	Source
Tripwire	Intégrité LINUX	2.3.47	15/08/00	http://www.tripwire.org/downloads/index.php
ChkRootKit	Compromission UNIX	0.43	27/12/03	http://www.chkrootkit.org/

DÉTECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
Deception TK	Pot de miel	19990818	18/08/99	http://all.net/dtk/index.html
LLNL NID	IDS Réseau	2.6	10/10/02	http://ciac.llnl.gov/cstc/nid/nid.html
Snort	IDS Réseau	2.1.3rc1	21/04/04	http://www.snort.org/dl/
Shadow	IDS Réseau	1.8	30/04/03	http://www.nswc.navy.mil/ISSEC/CID/

GÉNÉRATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
Elza	Requêtes HTTP	1.4.5	01/04/00	http://www.stoev.org/elza/project-news.html
FireWalk	Analyse filtres	5.0	20/10/02	http://www.packetfactory.net/firewalk
IPSend	Paquets IP	2.1a	19/09/97	ftp://coombs.anu.edu.au/pub/net/misc
IDSWakeUp	Détection d'intrusion	1.0	13/10/00	http://www.hsc.fr/ressources/outils/idswakeup/download/
UdpProbe	Paquets UDP	1.2	13/02/96	http://sites.inka.de/sites/bigred/sw/udpprobe.txt

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	3.1	19/04/00	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	4.1.1	11/03/04	http://coombs.anu.edu.au/ipfilter/ip-filter.html
NetFilter	Pare-Feu IpTables	1.2.9	02/11/03	http://www.netfilter.org/downloads.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.5.4	29/06/01	http://sites.inka.de/sites/bigred/devel/cipe.html
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httptunnel.html
OpenSSL	Pile SSL	0.9.7d	17/03/04	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	3.8.1p1	19/04/04	http://www.openssh.com/
🗁 **OpenSwan**	Pile IPSec	2.1.2	19/05/04	http://www.openswan.org/code/
		1.0.4	17/05/04	http://www.openswan.org/code/
Stunnel	Proxy https	4.05	14/02/03	http://www.stunnel.org
TeraTerm Pro	Terminal SSH2	3.1.3	08/10/02	http://www.ayera.com/teraterm/
Zebedee	Tunnel TCP/UDP	2.4.1	29/05/02	http://www.winton.org.uk/zebedee/

NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du **28/04/2003** au **26/05/2004**, **16 RFC** ont été publiés dont 5 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
CRYPTO	3713	04/04	Inf	A Description of the Camellia Encryption Algorithm
IPV6	3756	05/04	Inf	IPv6 Neighbor Discovery (ND) Trust Models and Threats
SSL	3749	05/04	Pst	Transport Layer Security Protocol Compression Methods
WEBDAV	3744	05/04	Pst	Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol
WLAN	3770	05/04	Pst	Certificate Extensions & Attributes Supporting Authentication in PPP and WLAN

RFC TRAITANT DE DOMAINES CONNEXES À LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
SCTP	3758	05/04	Pst	Stream Control Transmission Protocol (SCTP) Partial Reliability Extension

AUTRES RFC

Thème	Num	Date	Etat	Titre
ENUM	3761	04/04	Pst	The E.164 to URI Dynamic Delegation Discovery System (DDDS) Application (ENUM)
	3762	04/04	Pst	Telephone Number Mapping (ENUM) Service Registration for H.323
IETF	3774	05/04	Inf	IETF Problem Statement
MDN	3798	05/04	Dft	Message Disposition Notification
OWAMP	3763	04/04	Inf	One-way Active Measurement Protocol (OWAMP) Requirements
SCSI	3783	05/04	Inf	Small Computer Systems Interface (SCSI) Command Ordering Considerations with iSCSI
SCTP	3758	05/04	Pst	Stream Control Transmission Protocol (SCTP) Partial Reliability Extension
SIP	3764	04/04	Pst	enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record
SMI	3780	05/04	Exp	SMIng - Next Generation Structure of Management Information
	3781	05/04	Exp	Next Generation Structure of Management Information (SMIng) Mappings to SNMP

LES DRAFTS

Du **28/04/2003**au **26/05/2004**, 212 drafts ont été publiés: **151** drafts mis à jour, **61** nouveaux drafts, dont **20** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
AAA	draft-mariblanca-aaa-eap-lla-00	24/05	EAP lower layer attributes for AAA protocols
CRYPTO	draft-haddad-mip6-cga-bub-00	19/05	Applying Cryptographically Generated Addresses to BUB (BUB+)
DNS	draft-stjohns-dnssec-trustupdate-00	11/05	Automated Updates of DNSSEC Trust Anchors
EAP	draft-badra-eap-double-tls-00	18/05	EAP-Double-TLS Authentication Protocol
	draft-adrangi-eap-network-discovery-00	24/04	Mediating Network Discovery in EAP
EMAIL	draft-delany-domainkeys-base-00	18/05	Domain-based Email Authentication Using PK Advertised in DNS
ETHERNET	draft-keri-local-anon-00	17/05	Privacy Enhanced Local Ethernet Net with Protocol Anonymization
GSS	draft-williams-gssapi-stackable-pseudo-me-00	20/05	Stackable Generic Security Service Pseudo-Mechanisms
IKE	draft-nir-ikev2-auth-lt-00	12/05	Repeated Authentication in IKEv2
NNTP	draft-ietf-nntpext-authinfo-00	30/04	NNTP Extension for Authentication
PKIX	draft-gerck-pkix-revocation-00	24/05	Certificate Revocation Revisited Internet X.509 PKI
RADIUS	draft-decnodder-radext-dynauth-ser-mib-00	30/04	RADIUS Dynamic Authorization Server MIB
	draft-zorn-radius-err-msg-00	10/05	RADIUS Error Messages
SIMPLE	draft-sharma-simple-multicast-source-auth-00	11/05	A Simple Approach to Data Source Auth. for Multicast Security
SOBGP	draft-white-sobgparchitecture-00	12/05	Architecture and Deployment Considerations for soBGP
	draft-white-sobgp-architecture-00	12/05	Architecture and Deployment Considerations for soBGP
	draft-ng-sobgp-bgpextensions-00	12/05	Extensions to BGP Transport soBGP Certificates
SPAM	draft-bonatti-generic-antispam-00	12/05	A Mechanism for Control of Unwanted Application Communications
TCP	draft-azcorra-tcpm-tcp-blind-ack-dos-00	11/05	DoS vulnerability of TCP by acknowledging not received segments
TLS	draft-salowey-tls-ticket-00	20/05	A TLS Hello Extension for Ticket Based Pre-Shared Keys

MISE À JOUR DE DRAFTS TRAITANT DE LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
DHCP	draft-ietf-dhc-v4-threat-analysis-02	29/04	DHCP v4) Threat Analysis
DNS	draft-ietf-dnsext-dnssec-intro-10	17/05	DNS Security Introduction and Requirements
	draft-ietf-dnsext-dnssec-records-08	17/05	Resource Records for the DNS Security Extensions
	draft-ietf-dnsext-dnssec-protocol-06	17/05	Protocol Modifications for the DNS Security Extensions
	draft-ietf-dnsext-nsec-rdata-06	14/05	DNSSEC NSEC RDATA Format
	draft-ietf-dnsop-dnssec-operational-pract-01	14/05	DNSSEC Operational Practices
GSSAPI	draft-williams-gssapi-store-deleg-creds-01	20/05	GSS-APIv2 Extension for Storing Delegated Credentials
GTSM	draft-ietf-rtgwg-rfc3682bis-02	30/04	The Generalized TTL Security Mechanism (GTSM)
HEALTH	draft-marshall-security-audit-12	20/05	Security Audit & Access Acc. Msg. XML Data Def. for Healthcare
IEEE802	draft-walker-ieee802-req-01	13/05	EAP Method Requirements for Wireless LANs
MBONE	draft-ietf-mboned-mroutesec-01	19/05	PIM-SM Multicast Routing Security Issues and Enhancements
MIPV4	draft-ietf-mip4-aaa-key-05	11/05	AAA Registration Keys for Mobile IPv4
MIPV6	draft-haddad-mip6-cga-omipv6-01	14/05	Applying Cryptographically Generated Addresses to OMIPv6
MPLS	draft-behringer-mpls-security-07	19/05	Analysis of the Security of BGP/MPLS IP VPNs
PANA	draft-ietf-pana-pana-04	11/05	Protocol for Carrying Authentication for Network Access (PANA)
PKIX	draft-ietf-pkix-certstore-http-07	21/05	X.509 PKI Operational Protocols: Certificate Store Access via HTTP
RADIUS	draft-zorn-radius-logoff-02	13/05	User Session Tracking in RADIUS
SASL	draft-newman-sasl-c-api-03	12/05	Simple Authentication and Security Layer C API
	draft-ietf-sasl-saslprep-09	29/04	SASLprep: Stringprep profile for user names and passwords
SECURE	draft-sharma-secure-mobility-dimensions-01	10/05	Secure Mobility Dimensions
SIP	draft-jennings-sipping-certs-03	18/05	Certificate Management Service for SIP
	draft-ono-sipping-end2middle-security-02	17/05	End-to-middle security in the Session Initiation Protocol(SIP)
	draft-ietf-sip-identity-02	17/05	Enhancements for Authenticated Identity Management in SIP
	draft-ietf-sipping-kpml-03	20/05	A Session Initiation Protocol (SIP) Event Package for KPML
	draft-ietf-sipping-e2m-sec-reqs-02	12/05	Requirements for End-to-middle Security for SIP
SMIME	draft-ietf-smime-rfc2632bis-06	10/05	S/MIME Version 3.1 Certificate Handling
SSH	draft-ietf-secsh-userauth-19	20/05	SSH Authentication Protocol
TESLA	draft-ietf-msec-tesla-intro-02	12/05	TESLA: Multicast Source Authentication Transform Introduction
VLAN	draft-sanjib-private-vlan-01	11/05	Addressing vlan scalability & security issues in a multi-client env.
TLS	draft-ietf-tls-ecc-06	20/05	ECC Cipher Suites For TLS

DRAFTS TRAITANT DE DOMAINES CONNEXES À LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-aaa-diameter-cc-05	14/05	Diameter Credit-control Application
CTP	draft-singh-capwap-ctp-00	14/05	CAPWAP Tunneling Protocol (CTP)
DNS	draft-ymbk-dns-choices-00	14/05	Design Choices When Expanding DNS
ECML	draft-ietf-trade-ecml2-spec-09	29/04	ECML:Version 2 Specification
IGP	draft-ietf-rtgwg-igp-shortcut-01	24/05	Calculating IGP Routes Over Traffic Engineering Tunnels
IP	draft-liumin-v6ops-silkroad-01	11/05	Tunneling IPv6 with private IPv4 addresses behind NAT devices
	draft-bryant-ipfrr-tunnels-00	20/05	IP Fast Reroute using tunnels
L3VPN	draft-ietf-l3vpn-bgpvpn-auto-04	13/05	Using BGP as an Auto-Discovery Mechanism for L3 and L2 VPNs
	draft-ietf-l3vpn-as2547-05	11/05	Applicability Statement for BGP/MPLS IP VPNs
LDAP	draft-ietf-ldapbis-protocol-24	11/05	LDAP: The Protocol
	draft-pauzies-ldap-schema-nonascii-mr-00	12/05	LDAP: Additional Matching Rules
MPLS	draft-ietf-mpls-rsvp-lsp-fastreroute-05	11/05	Fast Reroute Extensions to RSVP-TE for LSP Tunnels
RPSLNG	draft-blunk-rpslng-05	13/05	Routing Policy Specification Language next generation (RPSLng)
SIP	draft-khartabil-sip-policy-uri-call-info-pur-01	18/05	Conveying a Conference Policy URI in SIP
SNMP	draft-ietf-snmpconf-pm-15	21/05	Policy Based Management MIB
SPF	draft-mengwong-spf-01	17/05	A Convention to Describe Hosts Authorized to Send SMTP Traffic
SYSLOG	draft-ietf-syslog-protocol-04	29/04	The syslog Protocol
	draft-ietf-syslog-transport-udp-01	12/05	Transmission of syslog messages over UDP
VPN	draft-ouldbrahim-ppvpn-gvpn-bgpgmpls-05	13/05	Generalized VPN Services using BGP and GMPLS Toolkit
XCON	draft-niemi-xcon-cpcp-rules-00	18/05	Conference Policy Authorization Rules

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
AD	draft-ietf-proto-ad-comments-pilot-02	11/05	Workgroup Chair Followup of AD Evaluation Comments
BFCP	draft-camarillo-xcon-bfcp-00	12/05	The Binary Floor Control Protocol (BFCP)
BFD	draft-katz-ward-bfd-v4v6-1hop-01	19/05	BFD for IPv4 and IPv6 (Single Hop)
BGP	draft-ietf-grow-bgp-med-considerations-01	18/05	BGP MED Considerations
	draft-ietf-idr-bgp4-experience-protocol-04	19/05	Experience with the BGP-4 Protocol
	draft-ietf-idr-rfc3065bis-02	19/05	Autonomous System Confederations for BGP
	draft-ietf-idr-rfc2796bis-01	12/05	BGP Route Reflection - An Alternative to Full Mesh IBGP
	draft-ietf-idr-avoid-transition-00	19/05	Avoid BGP Best Path Transitions from One External to Another
	draft-chen-bgp-prefix-orf-07	10/05	Address Prefix Based Outbound Route Filter for BGP-4
	draft-chavali-bgp-prefixlimit-02	29/04	Peer Prefix Limits Exchange in BGP
	draft-chen-bgp-rfc2796bis-survey-00	10/05	BGP Route Reflection - Implementation Report
CALLERID	draft-atkinson-callerid-00	20/05	Caller ID for E-mail
CAP	draft-ietf-calsch-cap-13	24/05	Calendar Access Protocol (CAP)
CPL	draft-ietf-iptel-cpl-09	29/04	CPL: A Language for User Control of Internet Telephony Services

DHCP	draft-ietf-dhc-vendor-02	18/05	Vendor-Identifying Vendor Options for DHCPv4
	draft-ietf-dhc-rapid-commit-opt-03	13/05	Rapid Commit Option for DHCPv4
DNS	draft-ietf-dnsop-ipv6-dns-issues-07	13/05	Operational Considerations and Issues with IPv6 DNS
	draft-danisch-dns-rr-smtp-04	21/05	RMX DNS RR & method for lightweight SMTP sender authorization
	draft-dougotis-srv-caa-00	17/05	DNS Extension for SRV-Client Address Authorization (SRV-CAA)
DOS	draft-iab-dos-01	11/05	Internet Denial of Service Considerations
	draft-zinin-rtg-dos-01	13/05	Internet Routing Infrastructure from Outsider CPU Attacks
DSTM	draft-bound-dstm-exp-01	30/04	Dual Stack Transition Mechanism
EMAIL	draft-crocker-email-arch-00	17/05	Internet Mail Architecture
ENUM	draft-ietf-enum-pres-01	21/05	Enumservice Registration for Presence Services
ETS	draft-carlberg-ets-mip-00	14/05	Requirements for MIPv4 Mobility Agents Support of ETS
FTP	draft-preston-ftpext-deflate-01	11/05	Deflate transmission mode for FTP
H350	draft-johnson-h350-directory-serv-02	12/05	H.350 Directory Services
HTTP	draft-dusseault-http-patch-02	17/05	Partial Document Changes (PATCH Method) for HTTP
iCAL	draft-hare-xcalendar-00	20/05	Guideline for use of XML with iCalendar elements
IDMR	draft-ietf-idmr-dvmrp-v3-as-01	12/05	Distance Vector Multicast Routing Protocol Applicability Statement
IDN	draft-klensin-idn-tld-03	24/05	National and Local Characters in DNS TLD Names
	draft-klensin-reg-guidelines-03	30/04	Registration of IDN: Overview and Method
IDR	draft-savola-idr-rfc1863-historic-00	20/05	Request to Move RFC 1863 to Historic
IETF	draft-iab-research-funding-03	11/05	IAB Concerns & Recom. Regarding Internet Research & Evolution
	draft-iab-model-01	24/05	Writing Protocol Models
	draft-dawkins-pstmt-twostage-02	21/05	Two Stage Standardization Approach
	draft-alvestrand-ietf-mission-01	30/04	A Mission Statement for the IETF
	draft-klensin-newtrk-antiques-00	24/05	Valuable Antique Documents: A Model for Advancement
IIALP	draft-davey-iialp-01	19/05	Iowa Internet Annoyance Logging Protocol pronounced I'-alp
IMAP	draft-ietf-imapext-sort-17	24/05	IMAP - SORT AND THREAD EXTENSION
	draft-ietf-imapext-list-extensions-06	17/05	IMAP4 LIST Command Extensions
	draft-maes-lemonade-p-imap-02	12/05	Push Extensions to the IMAP Protocol (P-IMAP)
IP	draft-ietf-ipdvb-ule-01	21/05	ULE for transmission of IP datagrams over MPEG-2/DVB networks
	draft-klensin-ip-service-terms-01	24/05	Terminology for Describing Internet Connectivivy
	draft-shand-ipfrr-framework-00	21/05	IP Fast Reroute Framework
IPPM	draft-ietf-ippm-metrics-registry-06	19/05	IPPM metrics registry
IPV4	draft-dreibholz-ipv4-flowlabel-02	24/05	An IPv4 Flowlabel Option
IPV6	draft-ietf-ipv6-node-requirements-09	24/05	IPv6 Node Requirements
	draft-ietf-ipv6-rfc2011-update-10	24/05	Management Information Base for the Internet Protocol (IP)
	draft-hain-ipv6-pi-addr-use-06	14/05	the IPv6 Provider Independent Global Unicast Address Format
	draft-arunt-prefix-delegation-using-icmpv6-00	29/04	IPv6 Prefix Delegation Using ICMPv6
	draft-ietf-v6ops-unmaneval-02	20/05	Evaluation of Transition Mechanisms for Unmanaged Networks
	draft-ietf-v6ops-ent-scenarios-02	11/05	IPv6 Enterprise Network Scenarios
	draft-ietf-v6ops-v6onbydefault-02	11/05	Issues with Dual Stack IPv6 on by Default
	draft-ietf-v6ops-onlinkassumption-02	11/05	IPv6 Neighbor Discovery On-Link Assumption Considered Harmful
IRI	draft-duerst-iri-07	11/05	Internationalized Resource Identifiers (IRIs)
ISATAP	draft-templin-v6ops-iemmei-01	10/05	ISATAP Extensions for Mobility, Multihoming and Efficiency Impro.
ISER	draft-murphy-iser-telnet-02	21/05	iSeries Telnet Enhancements
JXTA	draft-duigou-jxta-protocols-04	11/05	JXTA v1.0 Protocols Specification
L2VPN	draft-ietf-l2vpn-vpls-bgp-02	18/05	Virtual Private LAN Service
	draft-holness-network-l2vpsp-02	20/05	The Nortel Networks Ethernet Layer 2 VP Service Protocol
L3VPN	draft-ietf-l3vpn-mpls-vpn-mib-03	14/05	MPLS/BGP Layer 3 VPN Management Information Base
LDAP	draft-ietf-ldapbis-syntaxes-08	21/05	LDAP: Syntaxes and Matching Rules
	draft-melnikov-ldap-krb-authzid-00	17/05	Authorization identity syntax for Kerberos-aware Directories
LTP	draft-irtf-dtnrg-ltp-00	12/05	Licklider Transmission Protocol
LWAPP	draft-ohara-capwap-lwapp-00	11/05	Light Weight Access Point Protocol (LWAPP)
MBONE	draft-ietf-mboned-embeddedrp-04	29/04	Embedding the RP Address in an IPv6 Multicast Address
MIB	draft-ietf-hubmib-efm-epon-mib-01	12/05	Managed Objects for the Ethernet Passive Optical Networks
MIDCOM	draft-ietf-midcom-mib-01	11/05	Definitions of Managed Objects for Middlebox Communication
MIME	draft-klyne-hdrreg-mail-05	11/05	Registration of mail and MIME header fields
MIPV4	draft-sgundave-mip4-identity-ext-00	14/05	Mobility Agent Identity Extension for Mobile IPv4
MIPV6	draft-ietf-mip6-mipv6-mib-02	17/05	A Management Information Base for Mobile IPv6
	draft-vogt-mipv6-credit-based-authoriza-00	21/05	Credit-Based Authorization for Mobile IPv6 Early Binding Updates
	draft-arkko-mipv6-binding-lifetime-extensi-00	21/05	Credit-Based Authorization for Binding Lifetime Extension
MIXMAST	draft-sassaman-mixmaster-01	19/05	Mixmaster Protocol Version 2
MMUSIC	draft-ietf-mmusic-sdp-comedia-06	14/05	Connection-Oriented Media Transport in SDP
MPLS	draft-ietf-ccamp-gmpls-egress-control-02	11/05	GMPLS Signaling Procedure For Egress Control
	draft-ietf-ccamp-gmpls-recovery-e2e-sig-01	12/05	RSVP-TE Ext in support of End-to-End GMPLS-based Recovery
	draft-ietf-mpls-telink-mib-07	17/05	Traffic Engineering Link Management Information Base
	draft-deoliveira-diff-te-preemption-03	21/05	LSP Preemption policies for Diff-Serv-aware MPLS Traffic Enginee.
	draft-xushao-ipo-mplsovergmpls-02	13/05	Requirements for MPLS over GMPLS-based Optical Networks
	draft-farrel-ccamp-inter-domain-frame-00	30/04	A Framework for Inter-Domain MPLS Traffic Engineering
	draft-dimitri-ccamp-gmpls-rsvp-te-bundled-00	14/05	GMPLS RSVP-TE signaling using Bundled TE Links
	draft-ietf-speechsc-mrcpv2-03	13/05	Media Resource Control Protocol Version 2(MRCPv2)
MSGHEAD	draft-newman-msgheader-originfo-05	28/05	Originator-Info Message Header
MSRP	draft-ietf-simple-msrp-relays-00	18/05	Relay Extensions for Message Sessions Relay Protocol (MSRP)
NEMO	draft-na-nemo-path-control-header-00	30/04	Route Optimization Scheme based on Path Control Header
	draft-thubert-tree-discovery-00	12/05	Nested Nemo Tree Discovery
NNTP	draft-ietf-usefor-article-13	17/05	News Article Format and Transmission
NOMAD	draft-nomadhoc-manet-filters-01	10/05	Filters for Mobile Ad hoc Networks (NOMADHOC)
NSIS	draft-luu-ntlp-con-imp-01	24/05	NSIS Transport Layer Protocol Considerations and Implementation

	draft-ietf-nsis-qos-nslp-03	12/05	NSLP for Quality-of-Service signaling
	draft-ietf-nsis-nslp-natfw-02	21/05	A NAT/Firewall NSIS Signaling Layer Protocol (NSLP)
OSPF	draft-spagnolo-manet-ospf-wireless-interf-01	19/05	OSPFv2 Wireless Interface Type
	draft-lindem-ospfv3-dest-filter-02	19/05	OSPFv3 Destination Address Filter
PIM	draft-farinacci-pim-pop-count-00	18/05	Population Count Extensions to PIM
	draft-ietf-pim-anycast-rp-01	24/05	Anycast-RP using PIM
POSTING	draft-bambenek-posting-guidelines-03	17/05	Reply Posting Guidelines in One to Many Communications
PWE3	draft-rosen-pwe3-congestion-01	12/05	PWE3 Congestion Control Framework
	draft-ietf-pwe3-tdm-requirements-05	29/04	Reqs for Edge-to-Edge Emulation of TDM Circuits over PSN
	draft-ietf-pwe3-fcs-retention-01	20/05	PWE3 Frame Check Sequence Retention
	draft-ietf-pwe3-satop-mib-00	20/05	Managed Objects for Structure-Agnostic TDM over Packet Network
	draft-ietf-pwe3-tdm-mib-00	20/05	Managed Objects for TDM over Packet Switched Network (PSN)
ROHC	draft-ietf-rohc-udp-lite-03	17/05	RObust Header Compression (ROHC):Profiles for UDP-Lite
RSVP	draft-kompella-rsvp-change-02	18/05	Procedures for Modifying RSVP
RTP	draft-ietf-avt-rtp-h264-06	17/05	RTP payload Format for H.264 Video
	draft-ietf-avt-rtp-midi-format-04	29/04	RTP Payload Format for MIDI
	draft-ietf-avt-rtp-midi-guidelines-04	29/04	An Implementation Guide for RTP MIDI
	draft-ietf-avt-text-red-05	20/05	Registration of the text/red MIME Sub-Type
	draft-ietf-avt-rtp-3gpp-timed-text-01	11/05	RTP Payload Format for 3GPP Timed Text
	draft-ahmadi-avt-rtp-vmr-wb-02	18/05	RTP Payload & File Storage Formats for the VMR-WB Audio Codec
SEAMOBY	draft-ietf-seamoby-ctp-09	14/05	Context Transfer Protocol
	draft-ietf-seamoby-iana-01	21/05	Instructions for Seamoby Experimental Protocol IANA Allocations
SIMPLE	draft-lonnfors-simple-partial-publish-01	17/05	Partial Publication of Presence Information
	draft-ietf-simple-message-sessions-06	18/05	The Message Session Relay Protocol
	draft-ietf-simple-prescaps-ext-01	10/05	User agent capability presence status extension
	draft-ietf-simple-iscomposing-01	17/05	Indication of Message Composition for Instant Messaging
	draft-ietf-simple-xcap-pidf-manipul-usage-00	13/05	XML XCAP Usage for Manipulating Presence Document Contents
SIP	draft-camarillo-sipping-exploders-03	14/05	Requirements for SIP Exploder Invocation
	draft-hilt-sipping-session-indep-policy-01	17/05	Session-Independent Policies for the Session Initiation Protocol
	draft-procter-sipping-call-park-extension-00	30/04	An approach to Call Park/Retrieve using SIP
	draft-garcia-sipping-message-exploder-00	12/05	Multiple recipient MESSAGE requests in SIP
	draft-elwell-sipping-redirection-reason-00	14/05	Indicating redirection reasons in SIP
	draft-hilt-sipping-consider-policy-00	14/05	Considerations for Session-specific SIP Session Policies
	draft-dolly-sipping-config-content-00	20/05	Data Content for SIP User Agent Profile Delivery
	draft-ietf-sip-session-timer-14	19/05	Session Timers in the Session Initiation Protocol (SIP)
	draft-ietf-sipping-conference-package-04	24/05	A SIP Event Package for Conference State
	draft-ietf-sipping-config-framework-03	18/05	A Framework for SIP User Agent Profile Delivery
SMTP	draft-motonori-dualstack-smtp-req-01	11/05	SMTP Operational Experience in Mixed IPv4/v6 Environments
	draft-dougotis-smtp-caa-00	19/05	SMTP Client Address Authorization (SMTP-CAA)
SNMP	draft-black-snmp-uri-05	17/05	Uniform Resource Identifier (URI) Scheme for SNMP
SOAP	draft-baker-soap-media-reg-06	18/05	The 'application/soap+xml' media type
SONET	draft-malis-sonet-ces-mpls-06	19/05	SONET/SDH Circuit Emulation Service Over MPLS Encapsulation
STACK	draft-venkataraman-stack-00	20/05	Stack Aware Architectures for Mobile Ad hoc Networks
STREAM	draft-flundberg-basestream-03	30/04	BaseStream - A Simple Typed Stream Format
TCP	draft-gont-tcpm-tcp-auto-option-00	19/05	TCP Adaptive User TimeOut (AUTO) Option
WARD	draft-katz-ward-bfd-02	19/05	Bidirectional Forwarding Detection
WEBDAV	draft-reschke-webdav-locking-00	21/05	WebDAV Locking Protocol
XML	draft-legg-xed-protocols-02	24/05	The XML Enabled Directory: Protocols
	draft-legg-xed-rxer-01	24/05	Robust XML Encoding Rules for ASN.1 Types
XMPP	draft-saintandre-xmpp-simple-01	29/04	Interoperability between XMPP and SIP Extensions for IMP
	draft-ietf-xmpp-core-24	10/05	Extensible Messaging and Presence Protocol (XMPP): Core

NOS COMMENTAIRES

LES DRAFTS

DRAFT-AZCORRA-TCPM-TCP-BLIND-ACK-DOS-00

DoS vulnerability of TCP by acknowledging not received segments

Cette proposition de standard décrit un aménagement du protocole **TCP** permettant de contrer une attaque connue et susceptible de provoquer un déni de service. Initialement présentée dans l'analyse de sécurité du mécanisme 'MultiHoming' en environnement IP V6 publiée en octobre dernier, et re-décrite dans cette proposition de standard, cette attaque se positionne dans la même lignée que la série d'attaques mises en évidence fin avril par **Paul Watson** (Rapport N°69 – Avril 2004) en utilisant elles aussi un effet de bord dans la spécification du protocole **TCP**.

L'une des attaques développées par Erik Nordmark et Tony Li tire parti du mécanisme de contrôle de congestion mis en œuvre dans le protocole **TCP**, mécanisme coopératif qui ne peut fonctionner que si les deux correspondants respectent les mêmes règles. Dans un monde utopique, cette spécificité ne doit pas poser de problème. Dans le monde réel, le non respect des règles de gestion de la congestion par l'un des correspondants peut conduire à l'effondrement d'une partie du réseau.

L'un des mécanismes de contrôle de congestion spécifiés par le **RFC2581** consiste à définir une valeur de régulation dite '**Congestion Windows**' intervenant dans la définition du plus grand numéro de séquence acceptable pour le prochain paquet devant être transmis. En cas de détection d'un problème de congestion, cette valeur est augmentée réduisant le nombre de paquets non acquittés transmis donc le débit de transmission, et par conséquent, l'impact du système sur la congestion du réseau.

Ce **RFC** stipule notamment :

> In some situations it may be beneficial for a **TCP** sender to be more conservative than the algorithms allow, however **a TCP MUST NOT be more aggressive** than the following algorithms allow (that is, **MUST NOT** send data when the value of cwnd computed by the following algorithms would not allow the data to be sent).

L'algorithme utilisé pour la détermination du numéro de séquence maximal conduit hélas à une situation dangereuse dans l'hypothèse où le destinataire d'un paquet acquitterait celui-ci avant même de l'avoir reçu. La fenêtre de congestion de l'émetteur est ainsi artificiellement réduite autorisant une augmentation du débit de transmission de sa part pouvant mener à une éventuelle saturation du destinataire mais aussi du réseau. Cette situation n'a théoriquement aucune raison d'exister, chaque intervenant respectant les spécifications du **RFC2581** sauf à être provoquée par un système agressif dans l'unique but de provoquer un déni de service.

Le risque est accentué par la relative facilité de prédiction du numéro de séquence du prochain paquet transmis et par les implémentations courantes qui ignorent purement et simplement un numéro d'acquittement correspondant à un paquet non transmis. Une attaque en aveugle peut alors aisément être engagée.

ftp://ftp.nordu.net/internet-drafts/draft-azcorra-tcpm-tcp-blind-ack-dos-00.txt - Aménagement du protocole TCP

ftp://ftp.nordu.net/internet-drafts/draft-nordmark-multi6-threats-01.txt - Description de l'attaque (non disponible)

http://www.join.uni-muenster.de/Dokumente/drafts/draft-nordmark-multi6-threats-00.txt

ALERTES ET ATTAQUES

ALERTES

GUIDE DE LECTURE

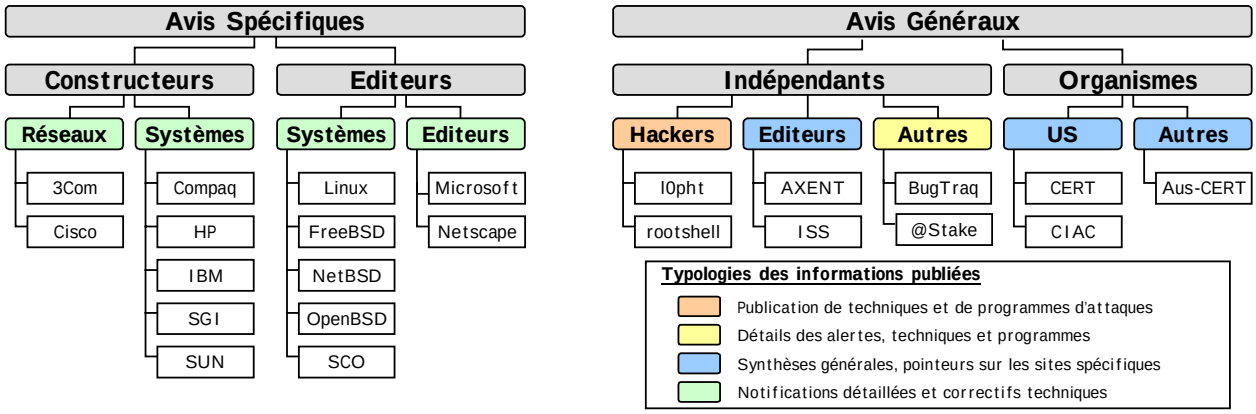
La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,

Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

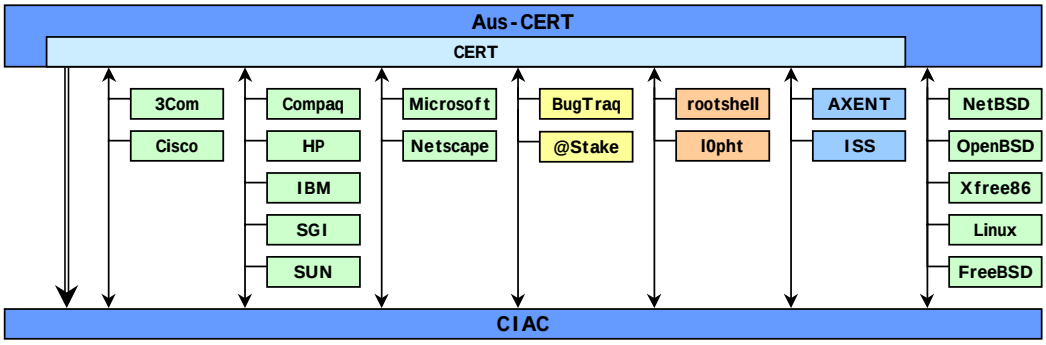
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.



L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

Recherche d'informations générales et de tendances :	Lecture des avis du CERT et du CIAC
Maintenance des systèmes :	Lecture des avis constructeurs associés
Compréhension et anticipation des menaces :	Lecture des avis des groupes indépendants



FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

Présentation des Alertes

EDITEUR			
TITRE			
Description sommaire			
Gravité	Date	Informations concernant la plate-forme impactée	
Correction		Produit visé par la vulnérabilité	Description rapide de la source du problème
Référence		URL pointant sur la source la plus pertinente	
Référence(s) CVE si définie(s)			

Présentation des Informations

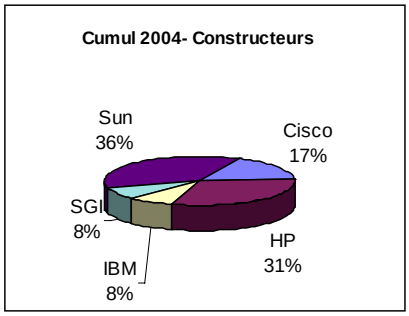
SOURCE
TITRE
Description sommaire
URL pointant sur la source d'information
Référence(s) CVE si définie(s)

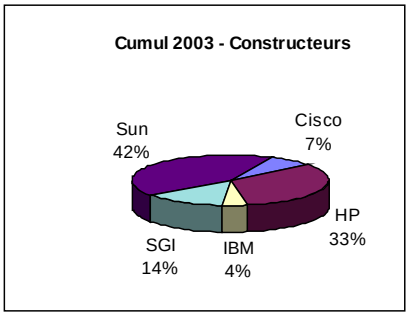
SYNTHESE MENSUELLE

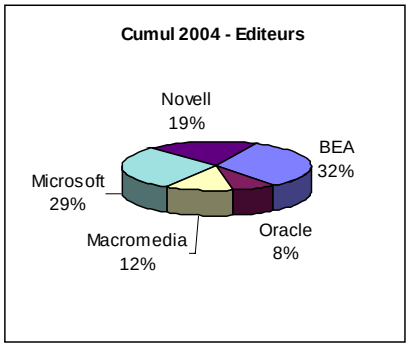
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

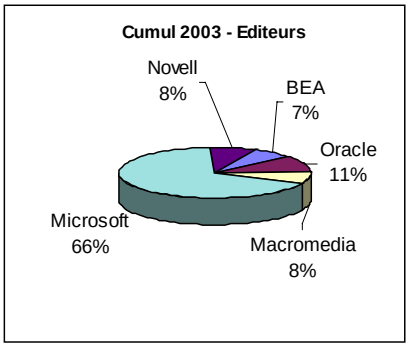
Période du **28/04/2003** au **26/05/2004**

		Cumul	
	Période	2004	2003
Organisme	**22**	**126**	**181**
US-CERT	0	12	28
CERT-IN	0	2	4
CIAC	22	112	149
Constructeurs	**14**	**88**	**284**
Cisco	0	15	21
HP	3	27	93
IBM	3	7	12
SGI	3	7	40
Sun	5	32	118
Editeurs	**3**	**52**	**76**
BEA	2	17	5
Oracle	0	4	8
Macromedia	0	6	6
Microsoft	1	15	51
Novell	0	10	6
Unix libres	**62**	**280**	**444**
Linux RedHat	15	62	122
Linux Fedora	18	47	
Linux Debian	13	103	190
Linux Mandr.	13	50	106
FreeBSD	3	18	26
Autres	**8**	**28**	**48**
@Stake	1	5	28
eEye	6	19	9
X-Force	1	4	11









ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

APACHE

Défaut de configuration dans Apache			
Un défaut de configuration affecte Apache dans le module 'mod_usertrack'.			
Moyenne	13/05	Apache 1.3.29 et 2.0.48 et inférieures	
Palliatif proposé		Module 'mod_usertrack'	Défaut de configuration
Apache		http://nagoya.apache.org/bugzilla/show_bug.cgi?id=24483	
CAN-2003-0987, CAN-2003-0020, CAN-2004-0174, CAN-2003-0993,CAN-2004-0113			

APPLE

Multiples vulnérabilités dans MacOS X			
Apple Mac OS X est sensible à de multiples vulnérabilités.			
Forte	03/05	Apple Mac OS X Client et Server versions 10.3.3 et inférieures	
Correctif existant		Cf avis original	Multiples vulnérabilités
Apple 61798		http://docs.info.apple.com/article.html?artnum=61798	
a050304-1		http://www.atstake.com/research/advisories/2004/a050304-1.txt	
CAN-2004-0430, CAN-2003-0020, CAN-2004-0113, CAN-2004-0174,CAN-2004-0428, CAN-2004-0155, CAN-2004-0403, CAN-2004-0429,CAN-2004-0431			

Exécution de code arbitraire dans MacOS X			
L'association de plusieurs vulnérabilités permet à un site web malicieux de provoquer l'exécution distante de code arbitraire.			
Forte	22/05	Navigateurs et applications MacOS X gérant les URI 'disk://'	
Aucun correctif		URI 'disk://'	Erreur de conception
CERT-US 210606		http://www.kb.cert.org/vuls/id/210606	
Apple 61798		http://docs.info.apple.com/article.html?artnum=61798	
Secunia 11622		http://secunia.com/advisories/11622	
Secunia 11689		http://secunia.com/advisories/11689	
CAN-2004-0486			

Deux vulnérabilités dans Mac OS X			
Deux vulnérabilités affectent Mac OS X.			
Forte	24/05	Apple Mac OS X versions 10.2.8 et 10.3.3	
Correctif existant		'Terminal', 'HelpViewer'	Mauvaise gestion des zones de sécurité
Apple 61798		http://docs.info.apple.com/article.html?artnum=61798	
CAN-2004-0485, CAN-2004-0486			

BEA

Accès non autorisé aux applications web du serveur			
Une mauvaise gestion du fichier 'weblogic.xml' permet d'accéder aux applications web du serveur WebLogic.			
Forte	11/05	BEA WebLogic Server et Express 7.0 jusqu'au SP5 inclus, 8.1 jusqu'au SP2 inclus	
Correctif existant		WebLogic Builder	Mauvaise gestion des rôles dans 'weblogic.xml'
BEA BEA04-59.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_59.00.jsp	

Arrêt non autorisé à des serveurs WebLogic			
Un utilisateur possédant un rôle 'Admin' ou 'Operator' peut arrêter le serveur WebLogic.			
Moyenne	11/05	BEA WebLogic Server et Express 7.0 jusqu'au SP5 inclus, 8.1 jusqu'au SP2 inclus	
Correctif existant		WebLogic	Non application des règles
BEA BEA04-60.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_60.00.jsp	

BLUECOAT

Exposition d'informations sensibles via SGOS			
Une vulnérabilité dans l'interface web d'administratio peut conduire à l'exposition de données sensibles.			
Forte	17/05	BlueCoat Security Gateway SG 3.x	
Correctif existant		Interface web d'administration	Stockage en clair de données sensibles
BlueCoat		http://www.bluecoat.com/support/knowledge/advisory_private_key_compromise.html	

CHECKPOINT

Débordement de buffer dans VPN-1

Les produits VPN-1 de Check Point sont sensibles à un débordement de buffer.

Critique	04/05	VPN-1/FireWall-1 NG AI versions inférieures à R54 HFA-410, à R55 HFA-03 et à HFA-325, VSX NG, VSX 2.01, GX 2.0, SecuRemote/SecureClient NG AI versions inférieures à R56	
Correctif existant		Protocole 'ISAKMP'	Débordement de buffer
Check Point		http://www.checkpoint.com/techsupport/alerts/ike_vpn.html	

CITRIX

Accès non autorisé aux volumes d'un utilisateur

Une vulnérabilité peut autoriser un utilisateur distant à avoir accès aux volumes logiques d'un autre utilisateur.

Faible	26/04	Citrix MetaFrame XP Presentation Server 1.0 pour plate-forme Microsoft, Citrix MetaFrame 1.8	
Correctif existant		Citrix	Non disponible
Citrix CTX103763		http://support.citrix.com/kb/entry.jspa?entryID=4289&categoryID=118	

CVS

Débordement de buffer dans 'cvs'

Un débordement de buffer dans le serveur 'cvs' peut autoriser l'exécution de code arbitraire.

Forte	19/05	Red Hat, Debian Linux 3.0 (woody)	
Correctif existant		Paquetage 'cvs'	Débordement de buffer
RHSA-04:190-14		https://rhn.redhat.com/errata/RHSA-2004-190.html	
DSA-505-1		http://www.debian.org/security/2004/dsa-505	
e-matters 07/04		http://security.e-matters.de/advisories/072004.html	
CAN-2004-0396			

ETHEREAL

Vulnérabilité dans plusieurs dissecteurs

Une vulnérabilité existe dans plusieurs dissecteurs utilisés par Ethereal.

Critique	13/05	Ethereal versions 0.9.8 à 0.10.3 inclus	
Correctif existant		SIP, AIM, SPNEGO et MMSE	Mauvaise gestion des paquets, Débordement de buffer
enpa-sa-00014		http://www.ethereal.com/appnotes/enpa-sa-00014.html	

EXIM

Débordements de buffer dans Exim

Exim est sensible à deux débordements de buffer.

Forte	06/05	Exim version 3.35, Exim version 4.32	
Correctif existant		'verify.c' et 'accept.c'	Débordement de buffer
Guninski 68		http://www.guninski.com/exim1.html	
DSA-501-1		http://www.debian.org/security/2004/dsa-501	
CAN-2004-0399, CAN-2004-0400			

GNU

Multiples vulnérabilités dans Midnight Commander

De multiples vulnérabilités affectent l'explorateur de fichiers Midnight Commander.

Forte	29/04	GNU Midnight Commander	
Correctif existant		Non disponible	Débordements de buffer, Création non sécurisée de fichiers et répertoires temporaires, Formatage non sécurisé de chaînes de caractères
DSA-497-1		http://www.debian.org/security/2004/dsa-497	
CAN-2004-0226, CAN-2004-0231, CAN-2004-0232			

Exposition d'informations sensibles dans Mailman

Une vulnérabilité dans GNU Mailman permet de récupérer les mots de passe d'autres utilisateurs.

Forte	15/05	GNU Mailman versions inférieures à 2.1.5	
Correctif existant		Non disponible	Non disponible
GNU 000072		http://mail.python.org/pipermail/mailman-announce/2004-May/000072.html	
CAN-2004-0412			

HEIMDAL

Débordement de tas dans 'kadmind'

Un débordement de tas dans 'kadmind', et par extension dans 'k5admind', permet l'exécution de code arbitraire.

Forte	06/05	Heimdal kadmind version 0.6.1 et inférieures, FreeBSD 4 et 5 avec Kerberos 4 et Kerberos 5	
Palliatif proposé		Module 'crypto_heimdal'	Débordement de tas
SA-04:09		ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:09.kadmind.asc	
Heimdal 04-05-06		http://www.pdc.kth.se/heimdal/advisory/2004-05-06/	
CAN-2004-0434			

HP

Vulnérabilité dans HP OpenView Select Access

Une vulnérabilité dans HP OpenView Select Access permet à un utilisateur distant d'acquérir un accès non autorisé.

Forte	24/05	HP OpenView Select Access versions 5.0 patch 4, 5.1 patch1, 5.2 et 6.0	
Correctif existant		OpenView Select Access	Mauvaise gestion des caractères encodés
HP HPSBMA01045		http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01045	

Déni de service dans HP iLO

Une vulnérabilité dans les produits HP integrated Lights Out (iLO) peut entraîner un déni de service.

Forte	24/05	HP iLO avec firmware versions 1.10 à 1.55 non inclus	
Correctif existant		Integrated Light Out (iLO)	Erreur de conception
HP HPSBMA01046		http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01046	

Permissions laxistes dans les sources de GTK+

Les fichiers sources de GTK+ fournis par Hewlett-Packard ont des droits d'accès trop permissifs.

Moyenne	10/05	HP-UX B.11.00 et B.11.11 avec le paquetage B6848AB installé	
Correctif existant		bibliothèques GTK+	Droits d'accès trop permissifs
HPSBUX01034		http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01034	

IBM

Elévation de privilèges dans IBM Parallel Environment

Deux vulnérabilités permettent d'exécuter du code avec les privilèges de l'utilisateur 'root'.

Forte	10/05	IBM Parallel Environment 3.2, IBM Parallel Environment 4.1	
Correctif existant		Code de démonstration	Vulnérabilités non spécifiées dans le code de démonstration des APIs
IBM		https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs?mode=18&ID=312	

Vulnérabilité dans des commandes console sur AIX

Plusieurs commandes console sur IBM AIX sont localement vulnérables à des attaques par lien symbolique.

Forte	28/04	IBM AIX versions 5.1 et 5.2	
Correctif existant		'bos.rte.console' et 'bos.rte.serv_aid'	Vulnérabilité de type lien symbolique
IBM		http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0543.2	

Deux vulnérabilités dans des commandes LVM sur AIX

Des commandes sont vulnérables localement à des attaques par lien symbolique et à un débordement de buffer.

Forte	30/04	IBM AIX versions 5.1 et 5.2	
Correctif existant		Paquetage 'bos.rte.lvm'	Vulnérabilité de type lien symbolique, Débordement de buffer
IBM		http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2004.0544.2	

KDE

Vulnérabilité dans KDE

Une mauvaise vérification de l'adresse fournie dans une URL permet d'écraser un fichier arbitraire ou d'exécuter du code arbitraire.

Forte	17/05	KDE version 3.2.2 et inférieures, Red Hat	
Correctif existant		KDE	Mauvaise vérification des URLs
KDE		http://www.kde.org/info/security/advisory-20040517-1.txt	
RHSA-04:222-11		https://rhn.redhat.com/errata/RHSA-2004-222.html#Other	
CAN-2004-0411			

LINKSYS

Vulnérabilité du serveur DHCP sur routeurs Linksys

Une vulnérabilité exploitable à distance affecte le serveur DHCP des routeurs Linksys.

Forte	14/05	Linksys routeurs BEFSR41 et BEFW11S4	
Correctif existant		Serveur DHCP	Mauvais traitement des paquets BOOTP
Linksys		http://www.linksys.com/download/vertxt/Befsr41v3ver.txt	
Jon Hart		http://spoofed.org/files/linksys-dhcp-exploit.c	

LINUX

Vulnérabilité dans la bibliothèque 'libpng'

Une vulnérabilité dans les bibliothèques 'libpng2' et 'libpng3' peut entraîner un déni de service dans les applications utilisant celles-ci.

Forte	30/04	Debian Linux 3.0 (woody), Red Hat Linux 9, Paquetages 'libpng2' et 'libpng3'	
Correctif existant		Routine de traitement d'erreur	Erreur de conception
DSA-498-1		http://www.debian.org/security/2004/dsa-498	
RHSA-04:181-03		http://rhn.redhat.com/errata/RHSA-2004-181.html	
CAN-2004-0421			

Débordement de buffer dans la bibliothèque 'neon'			
La bibliothèque WebDAV 'neon', intégrée par exemple dans le paquetage 'cadaver', est sensible à un débordement de buffer permettant ainsi l'exécution de code arbitraire.			
Forte	19/05	Red Hat, Debian Linux 3.0 (woody) , Paquetage 'cadaver'	
Correctif existant		Routine de formatage de date	Débordement de buffer
RHSA-04:191-06		https://rhn.redhat.com/errata/RHSA-2004-191.html	
DSA-506-1		http://www.debian.org/security/2004/dsa-506	
CAN-2004-0398			

Vulnérabilité dans le démon 'sysklogd'			
Une vulnérabilité conduisant à un déni de service affecte 'sysklogd'.			
Moyenne	29/04	Sysklogd version 1.4.1-14 et inférieures	
Correctif existant		Fichier 'syslogd.c'	Erreur de code
Red Hat 120453		http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=120453	

LINUX DEBIAN

Vulnérabilités dans l'émulateur de terminal 'eterm'			
Le traitement des séquences d'échappement par 'eterm' permet l'exécution de code arbitraire.			
Forte	29/04	'eterm' version 0.9.1 et précédentes	
Correctif existant		Paquetage 'eterm'	Absence de contrôle des séquences d'échappement
DSA-496-1		http://www.debian.org/security/2004/dsa-496	
BR 244808		http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=244808	
CAN-2003-0068			

Création non sécurisée de fichiers dans 'flim'			
Le paquetage 'flim', une bibliothèque pour emacs, crée de manière non sécurisée des fichiers temporaires.			
Forte	01/05	Debian Linux 3.0 (woody), Paquetage 'flim'	
Correctif existant		Paquetage 'flim'	Création non sécurisée de fichiers temporaires
DSA-500-1		http://www.debian.org/security/2004/dsa-500	
CAN-2004-0422			

Déni de service distant dans 'mah-jong'			
Une erreur de codage permet de provoquer l'arrêt brutal du serveur 'mah-jong' dans Debian Linux.			
Forte	13/05	Debian Linux 3.0 (woody)	
Correctif existant		Paquetage 'mah-jong'	Erreur de codage
DSA-503.1		http://www.debian.org/security/2004/dsa-503	
CAN-2004-0458			

Débordement de buffer dans Heimdal			
Un débordement de buffer affecte le paquetage Heimdal.			
Forte	18/05	Debian Linux 3.0 (woody)	
Correctif existant		Composant Kerberos 4	Débordement de buffer
DSA-504-1		http://www.debian.org/security/2004/dsa-504	
CAN-2004-0472			

Débordement de buffer dans le paquetage 'xpcd'			
Un débordement de buffer affecte un composant du paquetage 'xpcd'.			
Moyenne	22/05	Debian Linux 3.0 (woody), Paquetage 'xpcd'	
Correctif existant		Paquetage 'xpcd', 'xpcd-svga'	Débordement de buffer
DSA-508-1		http://www.debian.org/security/2004/dsa-508	
CAN-2004-0402			

LINUX REDHAT

Multiples vulnérabilités dans le paquetage 'lha'			
Le paquetage 'lha', outil de compression au format LHarc, est sensible à plusieurs débordements de buffer ainsi qu'à des attaques par saut de répertoires.			
Forte	30/04	Red Hat Linux 9.0, Paquetage 'lha'	
Correctif existant		Paquetage 'lha'	Deux débordement de buffer, Saut de répertoires
RHSA-04:179-03		https://rhn.redhat.com/errata/RHSA-2004-179.html	
CAN-2004-0234, CAN-2004-0235			

LINUX SuSE

Acquisition des droits 'root' à distance sur Live CD			
Une erreur de configuration dans Live CD permet d'acquérir les droits 'root' à distance.			
Critique	07/05	SuSE Linux 9.1 Personal Edition Live CD	
Correctif existant		Live CD	Absence de mot de passe pour l'utilisateur 'root'
SuSE-SA:04:011		http://www.securityfocus.com/advisories/6673	

MICROSOFT

Exécution de code distant dans Help and Support Center			
Une nouvelle vulnérabilité affecte la fonction HSC (Help and Support Center) et permet d'exécuter un code arbitraire à distance.			
Forte	11/05	XP et XP SP1, XP 64-Bit Edition SP1, XP 64-Bit Edition version 2003, Server 2003, Server 2003 64-Bit Edition	
Correctif existant		Help and Support Center (HSC)	Mauvaise validation des données fournies par l'utilisateur
MS04-015		http://www.microsoft.com/technet/security/bulletin/ms04-015.mspx	
EXPL-A-2003-027		http://www.exploitlabs.com/files/advisories/EXPL-A-2003-027-helpctr.txt	
CERT VU#484814		http://www.kb.cert.org/vuls/id/484814	
CAN-2004-0199			

McAFEE

Exécution de code arbitraire dans ePolicy Orchestrator			
Une vulnérabilité affectant McAfee ePolicy Orchestrator (ePO) peut entraîner l'exécution distante de code arbitraire.			
Critique	10/05	McAfee ePolicy Orchestrator 2.5.0, 2.5.1 inférieur à Patch 14, 3.0 inférieur à Patch 4 pour 3.0 SP2A Les versions antérieures peuvent aussi être affectées	
Correctif existant		Gestionnaire 'spipe'	Acceptation des requêtes HTTP 'POST' illicites
ISS X-Force 173		http://xforce.iss.net/xforce/alerts/id/173	
SF 10200		http://www.securityfocus.com/bid/10200	
ISS X-Force14166		http://xforce.iss.net/xforce/xfdb/14166	
CAN-2004-0038			

OPENBSD

Exposition d'informations du noyau via 'procfs'			
Des problèmes de débordement d'entier dans 'procfs' autorisent l'accès à certaines zones mémoire du noyau.			
Forte	13/05	OpenBSD 3.4 et 3.5	
Correctif existant		Système de fichiers 'procfs'	Débordements d'entier
OpenBSD		http://www.openbsd.org/security.html	

PROFTPD

Contournement des listes d'accès dans 'ProFTPD'			
Une vulnérabilité peut autoriser un utilisateur distant à contourner les restrictions d'accès.			
Forte	30/04	ProFTPD version inférieure à 1.2.10rc1	
Correctif existant		'dirtree.c'	Erreur de conception
ProFTPD		http://bugs.proftpd.org/show_bug.cgi?id=2267	

QUALCOMM

Débordement de buffer dans Eudora			
Un débordement de buffer dans la gestion des en-têtes de courrier permet potentiellement de provoquer un déni de service ou l'exécution de code arbitraire.			
Forte	21/05	Qualcomm Eudora versions 6.1 et inférieures	
Correctif existant		Gestion du champ 'To:'	Débordement de buffer
Qualcomm		http://www.eudora.com/download/eudora/windows/6.1.1/RelNotes.txt	

SAMBA / RSYNC

Vulnérabilité dans 'rsync'			
Une vulnérabilité dans 'rsync' peut entraîner la corruption de fichiers arbitraires.			
Forte	01/05	Samba 'rsync' versions inférieures à 2.6.1, Debian Linux 3.0 (woody)	
Palliatif proposé		Paquetage 'rsync'	Mauvaise gestion des chemins soumis par les utilisateurs
'rsync' apr04		http://rsync.samba.org/#security_apr04	
DSA-499-1		http://www.debian.org/security/2004/dsa-499	
CAN-2004-0426			

SAMBAR

Multiples vulnérabilités dans Sambar Server 5.x			
Des vulnérabilités permettent d'exposer des informations sensibles et d'exécuter du code arbitraire.			
Forte	30/04	Sambar Server 5 toutes versions	
Correctif existant		Non disponible	Validation insuffisante de l'adresse IP du client, des données en entrée, Chiffrement réversible des mots de passe, Erreurs de conception diverses
Bugtraq 361846		http://www.securityfocus.com/archive/1/361846	
SF10256		http://www.securityfocus.com/bid/10256/discussion/	
Sambar		http://www.sambar.com/security.htm	

SCO

Accès non autorisé à une session X11 sur OpenServer 5

Un utilisateur distant peut obtenir un accès non autorisé à une session X11 sur OpenServer 5.

Forte	12/05	SCO OpenServer 5.0.5, 5.0.6 et 5.0.7	
Correctif existant		Méthode d'accès à une session	Utilisation d'une méthode non sécurisée
SCOSA-2004.5		ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2004.5/SCOSA-2004.5.txt	
CAN-2004-0390			

SGI

Vulnérabilités réseau dans IRIX

Quatre vulnérabilités réseau ont été rendues publiques par SGI.

Forte	05/05	SGI IRIX versions 6.5 à 6.5.22m	
Correctif existant		Non disponible	Validation insuffisante d'en-tête de paquets TCP, Erreur de codage
SGI 040502-02-P		ftp://patches.sgi.com/support/free/security/advisories/20040502-02-P.asc	

Déni de service dans le service 'rpc.mountd'

Le service 'rpc.mountd' est sensible à un déni de service.

Forte	17/05	SGI IRIX 6.5.24	
Correctif existant		Service 'rpc.mountd'	Non disponible
SGI 040503-01-P		ftp://patches.sgi.com/support/free/security/advisories/20040503-01-P.asc	

SIDEWINDER

Multiples dénis de service dans Sidewinder G2

De multiples vulnérabilités dans le pare-feu Sidewinder G2 peuvent entraîner un déni de service.

Forte	18/05	Sidewinder G2 Firewall et Enterprise Manager version 6.1	
Correctif existant		Non disponible	Multiples vulnérabilités
Secure Comp.		http://www.securecomputing.com/pdf/SW61002Rel_Notes_0512.pdf	

SUN

Déni de service dans Java Runtime Environment

Une vulnérabilité dans Java Runtime Environment peur conduire à un déni de service distant.

Forte	06/05	Sun SDK et JRE 1.4.2 à 1.4.2_03 (Windows, Solaris, Linux)	
Correctif existant		Java JRE/SDK	Non disponible
Sun 57555		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57555	

Mauvaise validation de certificat dans JSSE

Le composant Java JSSE de Sun ne valide pas correctement le certificat d'un serveur Web.

Forte	17/05	Sun Java Secure Socket Extension versions 1.0.3, 1.0.3_01 et 1.0.3_02 pour Windows, Solaris et Linux	
Correctif existant		Java Secure Socket Extension	Mauvaise validation d'un certificat serveur
Sun 57560		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57560	

Vulnérabilité dans Solaris Management Console

La réponse à une requête envoyée à SMC permet de déterminer si le fichier ou répertoire pointé existe bien.

Faible	13/05	Sun Solaris 8 et 9 (Sparc et Intel)	
Correctif existant		Solaris Management Console	Saut de répertoires, Réponse explicite
Sun 57559		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57559	

SYMANTEC

Exécution de code distant privilégié sur Symantec

Une vulnérabilité critique affecte de nombreux produits Symantec et permet l'exécution de code distant sous des droits privilégiés.

Critique	12/05	Symantec Norton Internet Security 2002, 2003, 2004, Security Professional 2002, 2003, 2004 Personal Firewall 2002, 2003, 2004, Client Firewall 5.01, 5.1.1, Client Security 1.0, 1.1, 2.0(SCF 7.1) Norton AntiSpam 2004	
Correctif existant		Pilote 'SYMDNS.SYS'	Mauvaise validation des paquets NetBIOS Name Service (NBNS) et DNS
2004.05.12		http://securityresponse.symantec.com/avcenter/security/Content/2004.05.12.html	
eEye AD040512A		http://www.eeye.com/html/Research/Advisories/AD20040512A.html	
CAN-2004-0444, CAN 2004-0445			

Vulnérabilité dans Norton AntiVirus 2004

Une vulnérabilité dans un composant ActiveX peut autoriser l'exécution de commandes arbitraires ou entraîner un déni de service.

Forte	20/05	Symantec Norton AntiVirus 2004	
Correctif existant		Composant ActiveX	Mauvaise vérification des paramètres
SYM04-009		http://www.sarc.com/avcenter/security/Content/2004.05.20.html	

WIFI

Déni de service dans le protocole sans fil IEEE 802.11			
Le protocole sans fil IEEE 802.11 est vulnérable à des attaques par déni de service.			
Forte	13/05	Protocole IEEE 802.11 avec couche physique DSSS, Dispositifs IEEE 802.11, 802.11b et 802.11g en vitesse basse inférieure à 20Mbps	
Aucun correctif		Algorithme CCA	Retard de transmission
CERT VU#106678		http://www.kb.cert.org/vuls/id/106678	
AA-2004.02		http://www.auscert.org.au/render.html?it=4091	
CAN-2004-0459			

XINE/MPLAYER

Débordements de buffer dans les clients xine et MPlayer			
Plusieurs débordements de buffer exploitables à distance affectent les clients xine et MPlayer.			
Forte	25/04	MPlayer version 1.0pre1-pre3try2xine-lib version 1-beta1 à 1-rc3c	
Correctif existant		Clients RTPS	Débordement de buffer
Xine XSA-2004-3		http://xinehq.de/index.php/security/XSA-2004-3	

ALERTES NON CONFIRMEES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

3COM

Déni de service dans les solutions de téléphonie sur IP			
Une vulnérabilité permet de provoquer un déni de service à distance sur deux produits 3Com.			
Forte	30/04	3Com SuperStack 3 NBX, 3Com NBX 100	
Aucun correctif		Firmware NBX version 4.2.7	Validation insuffisante des données en entrée
SECNAP		http://www.secnap.net/security/20040420.html	

ACTIVESTATE

Débordement de buffer dans ActivePerl			
Un débordement de buffer affecte ActivePerl lors de l'utilisation de la fonction 'system()'.			
Forte	17/05	ActiveState ActivePerl version 5.8.3 et inférieures, Perl version 5.6.1 pour Cygwin	
Aucun correctif		Fonction 'system()'	Débordement de buffer
Oliver Karow		http://www.oliverkarow.de/research/ActivePerlSystemBOF.txt	

AGNITUM

Déni de service dans Outpost Pro Firewall			
Le maintien d'une liste de tous les nouveaux paquets entrants peut conduire à un déni de service.			
Forte	13/05	Agnitum Outpost Pro Firewall version 2.1	
Palliatif proposé		Liste des paquets entrants	Saturation des ressources
Securiteam		http://www.securiteam.com/windowsntfocus/5FP0E0KCUW.html	

ALLEGRO

Déni de service dans RomPager 2.10			
Il est possible de provoquer un déni de service distant avec une requête HTTP spécialement formatée.			
Forte	24/05	Allegro RomPager 2.10	
Correctif existant		Gestion des requêtes HTTP	Débordement de buffer
SF 1290		http://www.securityfocus.com/bid/1290	
Bugtraq 364071		http://www.securityfocus.com/archive/1/364071	

ALT-N

Débordement de buffer dans Mdaemon			
Un débordement de buffer existe dans le composant IMAP de Mdaemon.			
Moyenne	12/05	ALT-N Mdaemon 7.0.1	
Aucun correctif		Composant IMAP	Débordement de buffer
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-May/021279.html	

APPLE

Vulnérabilité dans Safari et Internet Explorer pour Mac			
Une fonction dans Apple permet d'exécuter localement des scripts ou des applications depuis le système d'aide.			
Forte	18/05	Apple Safari version 1.2 et inférieures, Microsoft Internet Explorer 5.2 pour Mac	
Palliatif proposé		Système d'aide	Mauvaise gestion des zones de sécurité
Bugtraq		http://www.securityfocus.com/archive/1/363551	

Execution de code arbitraire dans QuickTime et iTunes			
Une vulnérabilité présente permet l'exécution de code arbitraire via un fichier vidéo spécialement construit.			
Forte	02/05	Apple QuickTime 6.5, iTunes 4.2.0.72	
Correctif existant		Bibliothèque 'QuickTime.qts'	Débordement d'entier
EEye AD040502		http://www.eeye.com/html/Research/Advisories/AD20040502.html	
BugTraq 361883		http://www.securityfocus.com/archive/1/361883	
CAN-2004-0431			

BSD

Elévation de privileges grâce à 'systrace'			
Une erreur de conception dans 'systrace' permet à un utilisateur local d'obtenir les droits de l'utilisateur 'root'.			
Forte	11/05	NetBSD avec support de 'systrace' daté d'avant 09/04/2004, FreeBSD avec le portage de Vladimir Kotal	
Correctif existant		'syscall_fancy()' et 'trace_exit()'	Erreur de conception
e-matters 042004		http://security.e-matters.de/advisories/042004.html	

BUSINESSOBJECT

Multiples vulnérabilités dans Crystal Reports			
Plusieurs vulnérabilités dans Crystal Reports permettent de voler et supprimer des fichiers sensibles, et de provoquer un déni de service.			
Forte	03/05	BusinessObject Crystal Reports	
Aucun correctif		Non disponible	Non disponible
SC 20040503-000		http://www.security-corporation.com/articles-20040503-000.html	

CPANEL

Exécution de code arbitraire dans cPanel			
Une erreur de configuration autorise un utilisateur distant à exécuter du code arbitraire sur le serveur.			
Forte	24/05	cPanel versions antérieures au 15/04/2004	
Correctif existant		Module 'mod_phpsuexec'	Mauvaises options de compilation
Bugtraq 364112		http://www.securityfocus.com/archive/1/364112	

DELEGATE

Exécution de code arbitraire dans DeleGate			
Un débordement de buffer distant affecte DeleGate.			
Forte	05/05	DeleGate version 8.9.2 et inférieures (SSL-filter)	
Correctif existant		Filtre SSLway	Débordement de buffer
Bad Coded 0401		http://0xbadc0ded.org/advisories/0401.txt	
Delagate 2605		http://www.delegate.org/mail-lists/delegate-en/2605	

F5 SOFTWARE

Déni de service dans les switches BIG-IP			
Une vulnérabilité dans le noyau logiciel des switches BIG-IP les rend vulnérables à une attaque en déni de service.			
Forte	21/05	F5 BigIP 4.5 et 4.5.10	
Correctif existant		Gestion des 'syncookies'	Conflit d'accès au ressources (race condition)
SF10388		http://www.securityfocus.com/bid/10388	

F-SECURE

Vulnérabilité dans F-Secure Anti-Virus			
Un problème dans F-Secure Anti-Virus conduit à ne pas détecter les virus Sober.D et Sober.G.			
Forte	25/05	F-Secure Anti-Virus Client Security V 5.50, 5.52, Workstations V 5.41, 5.42, Serveurs de fichiers V 5.41, 5.42	
Correctif existant		F-Secure Anti-Virus	Non disponible
Secunia		http://secunia.com/advisories/11699/	

FIREBIRD

Débordement de pile dans la base de données FireBird			
Un débordement de pile dans Firebird 1.0 permet de provoquer un déni de service à distance.			
Forte	23/05	Firebird Database 1.0	
Correctif existant		Firebird Database 1.0	Débordement de pile
Securiteam		http://www.securiteam.com/unixfocus/5AP0P0UCUO.html	

GNU

Attaque par lien symbolique dans 'wget'			
'wget' ne verrouille pas les fichiers qu'il sauvegarde localement, autorisant une attaque par lien symbolique.			
Forte	16/05	GNU 'wget' 1.8.2, 1.9 et 1.9.1	
Aucun correctif		Utilitaire 'wget'	Absence de verrouillage de fichier
Bugtraq 363537		http://www.securityfocus.com/archive/1/363537	

Vulnérabilité dans une bibliothèque du projet GnuTLS			
Une vulnérabilité existe dans le traitement des règles d'encodage DER du format ASN.1.			
Non	14/05	GNU tASN.1 0.1 versions inférieures à 0.1.2, tASN.1 0.2 versions inférieures à 0.2.7	
Correctif existant		Bibliothèque 'tASN.1'	Non spécifié
ST 1010159		http://www.securitytracker.com/alerts/2004/May/1010159.html	
CAN-2004-0401			

KAME

Déni de service distant dans Racoon			
Un attaquant peut provoquer un déni de service distant via un message IKE spécialement construit.			
Forte	05/05	KAME Racoon versions 20040407b et inférieures	
Correctif existant		Démon Racoon	Validation insuffisante des données en entrée
KAME fbsd4/555		http://orange.kame.net/dev/query-pr.cgi?pr=555	
CAN-2004-0392			

KINESPHERE

Débordement de buffer dans eXchange POP3			
Un débordement de buffer dans eXchange POP3 est exploitable via un email spécialement formaté.			
Forte	20/04	Kinesphere eXchange POP3 4.0 toutes versions, POP3 5.0 versions inférieures à 5.0.1629	
Correctif existant		Proxy 'eXchange POP3'	Débordement de buffer
SF 10180		http://www.securityfocus.com/bid/10180	
Bugtraq 360765		http://www.securityfocus.com/archive/1/360765	

LIFERAY

Multiples vulnérabilités dans Enterprise portal			
Enterprise Portal est vulnérable à plusieurs vulnérabilités de type cross-site scripting et injection de code HTML.			
Forte	22/05	Liferay Enterprise Portal	
Aucun correctif		Liferay Enterprise Portal	Validation insuffisante des données en entrée
Bugtraq 364073		http://www.securityfocus.com/archive/1/364073	

LINUX

Débordement d'entier dans la gestion du protocole SCTP			
Un débordement d'entier dans le protocole SCTP permet l'écrasement de la mémoire du noyau Linux.			
Forte	11/05	Linux noyau 2.4.25 et inférieurs	
Correctif existant		SCTP_SOCKOPT_DEBUG_NAME	Débordement d'entier
Bugtraq 362953		http://www.securityfocus.com/archive/1/362953	

Elévation de privilèges dans les noyaux Linux 2.6			
Une erreur de conception permet à tout processus du système d'hériter de certains droits d'un processus qui vient de se terminer.			
Forte	07/05	Linux noyau 2.6 toutes versions	
Aucun correctif		Appel système 'exit_thread()'	Erreur de conception
Linux Kernel		http://www.ussg.iu.edu/hypermail/linux/kernel/0405.0/1265.html	
Linux Kernel		http://www.ussg.iu.edu/hypermail/linux/kernel/0405.0/1242.html	

Vulnérabilité dans la fonction 'do_fork' du noyau			
Une vulnérabilité dans la fonction 'do_fork' du noyau peut entraîner un déni de service.			
Moyenne	02/05	Linux noyau versions 2.4 et 2.6	
Correctif existant		Fonction 'do_fork()'	Erreur de conception
Linux Kernel		http://marc.theaimsgroup.com/?l=linux-kernel&m=108139073506983&w=2	
CAN-2004-0427			

Déni de service dans le noyau Linux			
Une utilisation incorrecte de la fonction 'fb_copy_cmap()' permet de provoquer localement un déni de service.			
Moyenne	29/04	Linux noyau versions 2.4 et 2.6	
Correctif existant		Fonction 'fb_copy_cmap()'	Utilisation incorrecte de la fonction
Security Tracker		http://www.securitytracker.com/alerts/2004/Apr/1009961.html	
CAN-2004-0229			

MAILENABLE

Débordement de tas dans Messaging Services			
Un débordement de tas permet à un utilisateur distant de provoquer un déni de service ou l'exécution de code avec des droits privilégiés.			
Forte	09/05	MailEnable Professional Edition versions 1.5 à 1.7	
Correctif existant		Interface web 'HTTPMail'	Débordement de tas
Hat-Squad 0071		http://www.hat-squad.com/en/000071.html	

MICROSOFT

Usurpation de certificat grâce à Internet Explorer

Une vulnérabilité permet de dérober le certificat SSL d'un autre site, et d'obtenir ainsi la confiance du visiteur.

Forte	30/04	Microsoft Internet Explorer version 6.0 et 6.0 SP1	
Aucun correctif		'meta http-equiv= "REFRESH"' 'BODY onUnload=...'	Usurpation d'identité
Bugtraq 361860		http://www.securityfocus.com/archive/1/361860	
SF 10148		http://www.securityfocus.com/bid/10248/discussion/	

Déni de service dans Internet Explorer

Il est possible de provoquer l'arrêt brutal d'Internet Explorer à distance avec du code XML spécialement formaté.

Forte	10/05	Internet Explorer version 6.0.2600.0	
Correctif existant		Bibliothèque 'msxml3.dll'	Erreur de codage
SF10318		http://www.securityfocus.com/bid/10318	
Bugtraq 362770		http://www.securityfocus.com/archive/1/362770	

Exécution de code arbitraire dans Outlook 2003

Il est possible de provoquer l'exécution de code arbitraire à distance dans Microsoft Outlook 2003.

Forte	17/05	Microsoft Outlook 2003 (Windows XP)	
Aucun correctif		Microsoft Outlook 2003	Erreur de conception
Bugtraq 363596		http://www.securityfocus.com/archive/1/363596	

Exécution de code arbitraire dans Windows

Il est possible de créer dans Windows de faux répertoires dont l'ouverture déclenchera l'exécution de code arbitraire.

Forte	17/05	Windows 2000 toutes versions, Windows XP toutes versions	
Aucun correctif		'explorer.exe' et 'iexplore.exe'	Validation insuffisante des données en entrée
Bugtraq 363590		http://www.securityfocus.com/archive/1/363590	
Secunia SA11633		http://secunia.com/advisories/11633	

Déni de service dans Internet Explorer

Une vulnérabilité dans le traitement des feuilles de style CSS permet de provoquer l'arrêt brutal d'Internet Explorer à distance.

Forte	18/05	Microsoft Internet Explorer 6.0.2800.1106 (Windows XP Familiale SP1 et 2000 SP4)	
Aucun correctif		Bibliothèque 'mshtml.dll'	Non spécifié
Bugtraq 363666		http://www.securityfocus.com/archive/1/363666	

Déni de service dans Internet Explorer

Le navigateur Internet Explorer est sensible à un déni de service via les méthodes 'onLoad' et 'window.location'.

Forte	07/05	Microsoft Internet Explorer 6.0.2800, Microsoft MSN Messenger	
Aucun correctif		Internet Explorer	Corruption des registres ECX, EDX et EDI
Kellinis 07-05-04		http://www.cipher.org.uk/index.php?p=advisories/Remote_DoS_IE_Memory_Access_Violation_7....advisory	

Exécution de script arbitraire dans Outlook 2003

Deux vulnérabilités permettent d'exécuter des scripts arbitraires et d'usurper une URL dans un message.

Forte	08/05	Microsoft Outlook 2003, Microsoft Internet Explorer Microsoft Outlook Express	
Aucun correctif		Outlook 2003	Sauvegarde locale de fichiers issus d'un tiers, Usurpation d'URL
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-May/021116.html	

Exposition de mots de passe dans Outlook Express

La fonction "dépannage" appliquée au courrier dans Outlook Express peut provoquer la recopie de noms d'utilisateurs SMTP et de mots de passe dans son fichier de journalisation.

Forte	18/05	Microsoft Outlook Express 5 et 6	
Aucun correctif		Fonction de dépannage	Erreur de conception
Kurczaba0405131		http://www.kurczaba.com/securityadvisories/0405131.htm	

Déni de service dans Internet Explorer

Une erreur de codage permet à une page HTML contenant un code spécifique de provoquer l'arrêt brutal d'Internet Explorer.

Forte	14/05	Microsoft Internet Explorer 6.0 SP1	
Aucun correctif		Bibliothèque 'mshtml.dll'	Déréférencement de pointeur NULL
SFVuln363396		http://www.securityfocus.com/archive/82/363396	

Débordement de buffer dans Visual Basic

Un débordement de buffer affecte la commande 'print' de Visual Basic.

Moyenne	18/05	Microsoft Visual Basic 6.0 version 8176	
Aucun correctif		Commande 'print'	Débordement de buffer
Dr_insane		http://members.lycos.co.uk/r34ct/main/ms-vb/MS-vb.txt	

Validation d'adresse de messagerie dans Outlook 2003		
Un message au format HTML visualisé dans Outlook 2003 permet d'informer l'émetteur que le message a été lu.		
Moyenne 12/05	Microsoft Outlook 2003	
Aucun correctif	Outlook 2003	Accès non sollicité à une source externe
Full Disclosure	http://lists.netsys.com/pipermail/full-disclosure/2004-May/021207.html	

Exposition d'informations via ASP sur IIS		
Certaines valeur de cookies conduisent les serveurs IIS à exposer des informations au travers de scripts ASP.		
Faible 05/05	Microsoft applications développées Active Server Pages sur Internet Information Server (IIS)	
Palliatif proposé	Moteur Active Server Pages	Gestion des données fournies par l'utilisateur, Message d'erreur explicite
App Sec 05-01	http://www.appsecinc.com/resources/alerts/general/05-0001.html	

MOLLENSOFT

Déni de service dans Lightweight FTP Server		
Un débordement de buffer permet à un utilisateur distant de provoquer un déni de service du serveur FTP.		
Forte 24/05	Mollensoft Lightweight FTP Server 3.6	
Aucun correctif	Commande FTP 'CWD'	Débordement de buffer
Securiteam	http://www.securiteam.com/windowsntfocus/5RP0L15CUM.html	

NETAPP

Déni de service dans Data ONTAP et NetCache		
Les produits Data ONTAP et NetCache sont vulnérables à des attaques par déni de service.		
Forte 03/05	Network Appliance Data ONTAP 6.x, Appliance NetCache 5.x	
Correctif existant	Data ONTAP et NetCache	Non disponible
Secunia	http://secunia.com/advisories/11516/	

NETGEAR

Contournement des filtres dans Netgear RP114		
Une vulnérabilité dans les routeurs Netgear RP114 autorise le contournement du module de filtrage des URLs.		
Moyenne 24/05	Netgear RP114	
Correctif existant	RP114	Erreur de conception
Bugtraq	http://www.securityfocus.com/archive/1/364113	

NETWIN

Contournement de l'authentification dans SurgeLDAP		
Une erreur de conception dans SurgeLDAP permet d'obtenir les droits d'administration du produit.		
Forte 05/05	Netwin SurgeLDAP 1.0 versions "a" à "g"	
Aucun correctif	Erreur de conception	Contournement du modèle de sécurité
ST 1010068	http://www.securitytracker.com/alerts/2004/May/1010068.html	
SF10294	http://www.securityfocus.com/bid/10294/	

OMNICRON

Exécution de code arbitraire dans OmniHTTPd		
Un débordement de buffer permet de provoquer l'exécution de code arbitraire à distance.		
Forte 18/05	Omnicron OmniHTTPd versions 3.0a et inférieures	
Aucun correctif	Serveur 'omnihttpd'	Débordement de buffer
Bugtraq 363651	http://www.securityfocus.com/archive/1/363651	

OPERA

Usurpation d'URL		
Il est possible de tromper un utilisateur d'Opera sur l'identité du site web réellement affiché.		
Moyenne 13/05	Opera 7.23 (Windows et Linux)	
Correctif existant	Barre d'adresse d'Opera	Erreur de conception
Secunia SA11532	http://secunia.com/advisories/11532/	

Ecrasement de fichier arbitraire via Opera		
Une mauvaise vérification de l'adresse fournie dans une URL permet d'écraser un fichier arbitraire.		
Moyenne 14/05	Opera version 7.23 et inférieures (Windows, Mac, Linux)	
Palliatif proposé	Navigateur Opera	Mauvaise vérification des URLs
iDefense 104	http://www.idefense.com/application/poi/display?id=104&type=vulnerabilities	

PANDORA

Création non sécurisée de fichiers dans 'ipmenu'

L'interface 'ipmenu' crée des fichiers temporaires de manière non sécurisée.

Forte	06/05	Pandora ipmenu version 0.0.3 et inférieures	
Aucun correctif		Interface 'ipmenu'	Création non sécurisée de fichiers temporaires
Security Tracker		http://www.securitytracker.com/alerts/2004/May/1010064.html	

PHP

Déni de service d'Apache provoqué par PHP

Il est possible de provoquer un déni de service avec un script PHP spécialement construit.

Moyenne	23/05	PHP sur Apache	
Aucun correctif		Fonctions de téléchargement	Erreur de conception
Securiteam		http://www.securiteam.com/unixfocus/5ZP0O0UCUO.html	

QUALCOMM

Débordement de buffer dans Eudora

Le client de messagerie Eudora est sensible à un débordement de buffer.

Forte	07/05	Qualcomm Eudora versions 6.1, 6.0.3 et 5.2.1	
Correctif existant		Non disponible	Débordement de buffer
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-May/021059.html	

Dissimulation d'URL malveillante dans Eudora

Il est possible de corrompre l'affichage de la barre d'état d'Eudora pour tromper le lecteur sur la destination d'un lien HTML.

Faible	08/05	Qualcomm Eudora	
Aucun correctif		Qualcomm Eudora	Erreur de conception
Bugtraq 362599		http://www.securityfocus.com/archive/1/362599	

RHINOSOFT

Débordement de pile dans Serv-U

Le serveur FTP RhinoSoft Serv-U est vulnérable à un débordement de pile exploitable à distance.

Critique	20/05	RhinoSoft Serv-U 3.0 et 3.1, Serv-U 4.0.0.4, 4.1, 4.1.0.11 et 4.2	
Correctif existant		Commande FTP 'MDTM'	Débordement de pile
Bugtraq 355367		http://www.securityfocus.com/archive/1/355367	
SF9751		http://www.securityfocus.com/bid/9751	

SMC

Accès à l'interface d'administration des routeurs SMC

L'interface d'administration de certains routeurs SMC sont accessibles depuis l'extérieur sans mot de passe.

Moyenne	01/05	SMC routeur 7008ABR (950.7814 avec firmware 1.032) SMC routeur 7004VBR version 1 (firmware 1.231)	
Palliatif proposé		Interface d'administration	Absence de mot de passe
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2004-April/020580.html	

SQUID

Contournement des règles d'accès

Il est possible de contourner les règles d'accès de Squid pour atteindre des sites web normalement interdits.

Moyenne	10/05	Squid 2.3.STABLE5	
Aucun correctif		Proxy 'squid'	Validation insuffisante des données en entrée
Bugtraq 362691		http://www.securityfocus.com/archive/1/362691	
SF10315		http://www.securityfocus.com/bid/10315	

SQUIRRELMAIL

Vulnérabilité de type Cross-Site Scripting

Une vulnérabilité de type Cross-Site Scripting affecte le service de mail par interface web SquirrelMail.

Forte	02/05	SquirrelMail version 1.4.2 et inférieures	
Correctif existant		Script 'compose.php'	Cross-Site Scripting
Securiteam		http://www.securiteam.com/unixfocus/5SP080KCUC.html	

Injection de code SQL dans SquirrelMail

SquirrelMail est vulnérable à une attaque par injection de code SQL pouvant endommager la base de données.

Forte	21/05	SquirrelMail versions 1.4.2 et inférieures	
Correctif existant		SquirrelMail	Validation insuffisante des données en entrée
SF10397		http://www.securityfocus.com/bid/10397	

SUBVERSION

Débordement de buffer

Une vulnérabilité dans une fonction de Subversion permet de compromettre un serveur depuis un client malicieux.

Forte	19/05	Subversion versions 1.0.2 et inférieures	
Correctif existant		Fonction de conversion de date	Débordement de pile
E-Matters 082004		http://security.e-matters.de/advisories/082004.html	
CAN-2004-0397			

TRENDMICRO

Déni de service dans Trend OfficeScan

Le service d'antivirus OfficeScan peut être désactivé par la suppression de clés de registre ou de fichiers dans le répertoire d'installation.

Forte	10/05	TrendMicro Trend OfficeScan 3.0 à 5.58	
Correctif existant		Clés de registre	Permissions laxistes
Bugtraq		http://www.securityfocus.com/archive/1/362523	

UCD-SNMP

Exécution de code arbitraire dans 'snmpd'

Une vulnérabilité dans l'interprétation de la ligne de commande permet l'exécution de code arbitraire avec les privilèges du démon 'snmpd'

Forte	21/05	UCD-SNMP versions 4.2.6 et inférieures	
Aucun correctif		Démon 'snmpd'	Débordement de buffer
SF10396		http://www.securityfocus.com/bid/10396	

VERITAS

Multiples vulnérabilités dans NetBackup

De multiples vulnérabilités autorisent un utilisateur local à acquérir les privilèges de l'utilisateur 'root'.

Forte	01/05	Veritas NetBackup	
Aucun correctif		Non disponible	Débordements de buffer, Validation insuffisante des données en entrée
Security Tracker		http://www.securitytracker.com/alerts/2004/Apr/1010011.html	
SF 10226		http://www.securityfocus.com/bid/10226	

VERITY

Exposition d'information dans Ultraseek

Certains messages d'erreur de Verity Ultraseek révèlent une information sur sa configuration.

Faible	05/05	Verity Ultraseek versions 5.2.1 et inférieures	
Correctif existant		Message d'erreur mal conçu	Erreur de conception
c040113-001		http://www.corsaire.com/advisories/c040113-001.txt	
CAN-2004-0050			

VOCALTEC

Déni de service dans les VocalTec Telephony Gateway

Une vulnérabilité dans deux passerelles de téléphonie VocalTec permet de provoquer un déni de service à distance.

Forte	24/05	VocalTec Telephony Gateway VTG120 et VTG480	
Aucun correctif		Protocoles H.323 et H.225	Non disponible
SecurityLab		http://www.securitylab.ru/_Exploits/2004/05/killvoc-small.c	
SL 45401		http://www.securitylab.ru/45401.html	
ST 1010268		http://www.securitytracker.com/alerts/2004/May/1010268.html	

VSFTPD

Déni de service dans le serveur 'vsftpd'

Le serveur FTP 'vsftpd' est sensible à un déni de service.

Forte	21/05	vsftpd versions inférieures à 1.2.2	
Correctif existant		Non disponible	Non disponible
vsftpd		ftp://vsftpd.beasts.org/users/cevans/untar/vsftpd-1.2.2/Changelog	

ZONEMINDER

Débordement de buffer dans le script 'zms'

Un débordement de buffer permet d'exécuter du code à distance sur un serveur ZoneMinder.

Forte	12/05	ZoneMinder versions 1.19.1 et inférieures	
Correctif existant		Script 'zms'	Débordement de buffer
ST 1010140		http://www.securitytracker.com/alerts/2004/May/1010140.html	

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme, ou ont donné lieu à la fourniture d'un correctif :

CIAC

Reprise de l'avis Symantec SYM04-008

Le CIAC a repris, sous la référence O-141, l'avis Symantec SYM04-008 à propos des multiples vulnérabilités affectant de nombreux produits Symantec, et permettant ainsi d'exécuter du code arbitraire distant et de provoquer un déni de service.

http://www.ciac.org/ciac/bulletins/o-141.shtml

CAN-2004-0444, CAN-2004-0445

Reprise de l'avis HP HPSBUX01038

Le CIAC a repris, sous la référence O-142, l'avis HP HPSBUX01038 au sujet d'une vulnérabilité dans 'dtlogin', autorisant l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/o-142.shtml

CAN-2004-0368

Reprise de l'avis HP HPSBUX01034

Le CIAC a repris, sous la référence O-143, l'avis HP HPSBUX01034 au sujet d'une vulnérabilité dans les bibliothèques GTK+ fournies par Hewlett-Packard. Des droits d'accès trop permissifs sur les fichiers sources de ces bibliothèques peuvent permettre la corruption d'informations critiques.

http://www.ciac.org/ciac/bulletins/o-143.shtml

Reprise de l'avis Sun 57554

Le CIAC a repris, sous la référence O-144, l'avis Sun 57554 au sujet du retrait de certains correctifs pour Solaris 9. Ils peuvent entraîner l'exposition d'informations sensibles pouvant être exploitée par un utilisateur local ou distant.

http://www.ciac.org/ciac/bulletins/o-144.shtml

Reprise de l'avis Red Hat RHSA-2004:188-14

Le CIAC a repris, sous la référence O-145, l'avis Red Hat RHSA-2004:188-14 concernant la disponibilité des correctifs pour le noyau Linux pour Red Hat Enterprise Linux AS, ES et WS version 3. Ils corrigent de multiples vulnérabilités affectant le descripteur '/proc/tty/driver/serial', la fonction noyau 'strncpy()', les pilotes RTC (Real Time Clock) et DRI (Direct Render Infrastructure) ainsi que la fonction 'ncp_lookup()'.

http://www.ciac.org/ciac/bulletins/o-145.shtml

CAN-2003-0461, CAN-2003-0465, CAN-2003-0984, CAN-2004-0003, CAN-2004-0010

Reprise de l'avis Red Hat RHSA-2004:222-11

Le CIAC a repris, sous la référence O-146, l'avis Red Hat RHSA-2004:222-11 à propos une vulnérabilité dans la gestion des URLs permettant ainsi d'écraser un fichier arbitraire ou d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/o-146.shtml

CAN-2004-0411

Reprise de l'avis Debian DSA-505-1

Le CIAC a repris, sous la référence O-147, l'avis Debian DSA-505-1 au sujet d'un débordement de buffer dans le serveur 'cvs' pouvant autoriser l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/o-147.shtml

CAN-2004-0396

Reprise des avis Debian DSA-506-1 et DSA-507-1

Le CIAC a repris, sous la référence O-148, les avis Debian DSA-506-1 et DSA-507-1 au sujet d'un débordement de buffer affectant la bibliothèque 'neon'.

http://www.ciac.org/ciac/bulletins/o-148.shtml

CAN-2004-0398

Reprise de l'avis ISS 15732

Le CIAC a repris, sous la référence O-130, l'avis ISS 15732 concernant un débordement de buffer dans la fonction 'win32_stat' des interpréteurs Perl et ActivePerl.

http://www.ciac.org/ciac/bulletins/o-130.shtml

CAN-2004-0377

Reprise de l'avis Symantec SYM04-009

Le CIAC a repris, sous la référence O-149, le bulletin Symantec SYM04-009 au sujet d'une vulnérabilité dans un composant ActiveX de Norton AntiVirus 2004. Cette vulnérabilité peut autoriser l'exécution de commandes arbitraires ou entraîner un déni de service de l'application.

http://www.ciac.org/ciac/bulletins/o-149.shtml

Reprise de l'avis Ethereal enpa-sa-00014

Le CIAC a repris, sous la référence O-150, l'avis Ethereal enpa-sa-00014 au sujet d'une vulnérabilité dans quatre dissecteurs, pouvant conduire à un déni de service ou à l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/o-150.shtml

Reprise de l'avis CERT-US VU#578798

Le CIAC a repris, sous la référence O-151, l'avis du CERT-US VU#578798 au sujet d'une vulnérabilité dans le système d'aide de MacOS X. Cette vulnérabilité permet l'exécution à distance de commandes arbitraires.

http://www.ciac.org/ciac/bulletins/o-151.shtml

CVE-2004-0486

Reprise de l'avis IBM MSS-OAR-E01-2004.0544.2

Le CIAC a repris, sous la référence O-131, l'avis IBM MSS-OAR-E01-2004.0544.2 concernant deux vulnérabilités dans des commandes LVM sur AIX. Ces vulnérabilités peuvent entraîner la corruption de données, un déni de service ou l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/o-131.shtml

Reprise de l'avis BEA BEA04_54.00

Le CIAC a repris, sous la référence O-132, l'avis BEA BEA04_54.00 concernant une mauvaise validation des chaînes de certificats dans WebLogic Server et Express.

http://www.ciac.org/ciac/bulletins/o-132.shtml

Reprise de l'avis Red Hat RHSA-2004:175-05

Le CIAC a repris, sous la référence O-133, l'avis Red Hat RHSA-2004:175-05 concernant une vulnérabilité dans le paquetage 'utempter' pouvant entraîner l'écrasement de fichiers arbitraires.

http://www.ciac.org/ciac/bulletins/o-133.shtml

CAN-2004-0233

Reprise de l'avis Debian DSA-499-1

Le CIAC a repris, sous la référence O-134, l'avis Debian DSA-499-1 concernant une vulnérabilité dans le paquetage 'rsync', pouvant être exploitée afin de corrompre des fichiers arbitraires.

http://www.ciac.org/ciac/bulletins/o-134.shtml

CAN-2004-0426

Reprise de l'avis Cert VU#179804

Le CIAC a repris, sous la référence O-129, l'avis Cert VU#179804 concernant une vulnérabilité dans 'dtlogin' autorisant l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/o-129.shtml

CAN-2004-0368

Reprise de l'avis US-CERT VU#782958 sur QuickTime

Le CIAC a repris, sous la référence O-135, l'avis US-CERT VU#782958 au sujet d'une vulnérabilité dans QuickTime et iTunes permettant l'exécution de code arbitraire via un fichier vidéo spécialement construit. Cette vulnérabilité avait initialement été découverte par eEye.

http://www.ciac.org/ciac/bulletins/o-135.shtml

http://www.kb.cert.org/vuls/id/782958

CAN-2004-0431

Reprise de l'avis ISS X-Force #15989 sur HP JetAdmin

Le CIAC a repris, sous la référence O-136, l'avis ISS X-Force #15989 au sujet de nombreuses vulnérabilités dans HP Web JetAdmin pouvant conduire à l'acquisition distante des droits 'root'. Ces failles avaient été rapportées par le groupe Phenoelit.

http://www.ciac.org/ciac/bulletins/o-136.shtml

Reprise de l'avis SGI 20040502-02-P

Le CIAC a repris, sous la référence O-137, l'avis SGI 20040502-02-P au sujet de quatre vulnérabilités réseau dans IRIX conduisant à un déni de service, à l'établissement d'une connexion TCP non autorisée et à l'impossibilité de désactiver le service ARP. Le numéro d'avis SGI 20050502-01-P est en fait erroné.

http://www.ciac.org/ciac/bulletins/o-137.shtml

Reprise de l'avis @stake a050304-1

Le CIAC a repris, sous la référence O-138, l'avis @stake a050304-1 au sujet de multiples vulnérabilités dans Apple Mac OS X Jaguar (10.2.8) et Panther (10.3.3).

http://www.ciac.org/ciac/bulletins/o-138.shtml

CAN-2004-0430, CAN-2003-0020, CAN-2004-0113, CAN-2004-0174, CAN-2004-0428,CAN-2004-0155, CAN-2004-0403, CAN-2004-0429, CAN-2004-0431

Reprise de l'avis US-CERT VU#648406

Le CIAC a repris, sous la référence O-139, l'avis US-CERT VU#648406 traitant d'une vulnérabilité spécifique à AppleFileServer sur Mac OS X et décrite dans l'avis @stake a050304-1 repris par ailleurs.

http://www.ciac.org/ciac/bulletins/o-139.shtml

CAN-2004-0430

Reprise de l'avis Microsoft MS04-015

Le CIAC a repris, sous la référence O-140, l'avis Microsoft MS04-015 au sujet d'une nouvelle vulnérabilité dans la fonction HSC (Help and Support Center) permettant d'exécuter un code arbitraire à distance.

http://www.ciac.org/ciac/bulletins/o-140.shtml

CAN-2004-0199

FREEBSD

Disponibilité de plusieurs correctifs

FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

heimdal	*FreeBSD-SA-04:08*
heimdal	*FreeBSD-SA-04:09*
cvs	*FreeBSD-SA-04:10*

http://www.linuxsecurity.com/advisories/freebsd.html

HP

Correctif 'mozilla'

HP a annoncé dans l'avis HPSBUX01036 la disponibilité du correctif pour Mozilla sur les plate-formes HP-UX B.11.00, B.11.11, et B.11.22. Il corrige trois vulnérabilités pouvant entraîner un déni de service, l'exposition d'informations sensibles, l'exécution de code arbitraire et la possibilité de mener des attaques de type Cross-Site Scripting.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01036

CAN-2003-0564, CAN-2003-0594, CAN-2004-0191

Correctifs 'dtlogin'

HP a annoncé la disponibilité des correctifs pour 'dtlogin' pour HP-UX B.11.00, B.11.04, B.11.11, B.11.22, et B.11.23, corrigeant une vulnérabilité autorisant l'exécution de code arbitraire.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01038

CAN-2004-0368

Correctif 'mozilla'

HP a annoncé la disponibilité du correctif pour Mozilla sur les plate-formes HP Tru64 UNIX v5.1A PK6, v5.1B PK2 et v5.1B PK3. Il corrige trois vulnérabilités pouvant entraîner un déni de service, l'exposition d'informations sensibles, l'exécution de code arbitraire et la possibilité de mener des attaques de type Cross-Site Scripting.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01021

CAN-2003-0564, CAN-2003-0594, CAN-2004-0191

Publication de l'avis HPSBPI01026

HP a publié, sous la référence HPSBPI01026, un bulletin d'information concernant les douze récentes vulnérabilités affectant HP Web JetAdmin, et indique que la version 7.5 corrige ces vulnérabilités.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBPI01026

Parade pour HP ProCurve

HP a annoncé que les produits HP ProCurve Routing Switch 9315M, 9308M, 9304M et tous les dispositifs HP EtherTwist, HP AdvanceStack et HP ProCurve sont vulnérables à la faille découverte dans l'implémentation TCP pouvant conduire à un déni de service distant. HP recommande, pour les dispositifs HP ProCurve Routing Switch 9315M, 9308M et 9304M, d'utiliser la fonction de protection par condensé MD5 dans le cadre du protocole BGP.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBGN01041

CAN-2004-0230

Correctifs pour le Java Runtime Environment

HP annonce dans le bulletin HPSBUX01044 la disponibilité de correctifs pour les versions 1.4.2 à 1.4.2.02 et précédentes du JRE sur HP-UX B.11.00, B.11.11, B.11.22, et B.11.23. Ils corrigent une vulnérabilité permettant un déni de service distant.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01044

Correctifs pour HP 'WBEM Services'

HP a annoncé la disponibilité des correctifs pour 'WBEM Services' pour les plate-formes HP HP-UX versions B.11.00, B.11.11 et B.11.23 et Red Hat Enterprise Linux. Ils corrigent deux vulnérabilités dans OpenSSL qui peuvent entraîner un déni de service distant.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01037

CAN-2004-0079, CAN-2004-0112

IBM

Correctifs 'dtlogin'

IBM a annoncé la disponibilité des correctifs pour 'dtlogin' pour IBM AIX 4.3, 5.1 et 5.2. Ils corrigent une vulnérabilité permettant d'exécuter du code arbitraire ou de provoquer un déni de service.

https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs?mode=18&ID=284

CAN-2004-0368

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

eterm	*DSA-496*
mc	*DSA-497*
libpng	*DSA-498*
rsync	*DSA-499*
flim	*DSA-500*
exim	*DSA-501*
exim-tls	*DSA-502*
mah-jong	*DSA-503*
heimdal	*DSA-504*
cvs	*DSA-505*
neon	*DSA-506*
cadaver	*DSA-507*
xpcd	*DSA-508*

http://www.debian.org/security/2004/

LINUX FEDORA

Disponibilité de nombreux correctifs

Fedora annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

mc	*FEDORA-2004:112*	
libpng1.2.2	*FEDORA-2004:105*	
libpng1.0.13	*FEDORA-2004:106*	
iproute	*FEDORA-2004:115*	
lha	*FEDORA-2004:119*	
neon	*FEDORA-2004:103*	
cvs	*FEDORA-2004:110*	
kdelibs	*FEDORA-2004:121*	
tcpdump	*FEDORA-2004:120*	*1*
kdelibs	*FEDORA-2004:122*	*2*
cvs	*FEDORA-2004:131*	*1 / 2*
neon	*FEDORA-2004:130*	*1 / 2*
subversion	*FEDORA-2004:128*	*1 / 2*
ipsec	*FEDORA-2004:132*	*2*
kdepim	*FEDORA-2004:133*	*1*
httpd	*FEDORA-2004:117*	*1*
OpenSSL	*FEDORA-FLSA:1395*	
Utempter	*FEDORA-FLSA:1546*	

http://www.linuxsecurity.com/advisories/fedora.html

LINUX MANDRAKE

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

syslogkd	*MDKSA-2004:038*	*9.1 / 9.2/ 10.0 / CS 2.1 / MNF 8.2*
mc	*MDKSA-2004:039*	*9.1 / 9.2/ 10.0 / CS 2.1*
linpng	*MDKSA-2004:040*	*9.1 / 9.2/ 10.0 / CS 2.1 / MNF 8.2*
proftpd	*MDKSA-2004:041*	*10.0*
rsync	*MDKSA-2004:042*	*9.1 / 9.2/ 10.0 / CS 2.1 / MNF 8.2*
apache2	*MDKSA-2004:043*	*9.1 / 9.2/ 10.0*
linuser	*MDKSA-2004:044*	*9.1 / 9.2/ 10.0 / CS 2.1*
passwd	*MDKSA-2004:045*	*9.1 / 9.2/ 10.0 / CS 2.1 / MNF 8.2*
apache	*MDKSA-2004:046*	*9.1 / 9.2/ 10.0 / CS 2.1 / MNF 8.2*
kdelibs	*MDKSA-2004:047*	*9.2/ 10.0*
cvs	*MDKSA-2004:048*	*9.1 / 9.2/ 10.0 / CS 2.1*
libneon	*MDKSA-2004:049*	*9.2/ 10.0*
kernel	*MDKSA-2004:050*	*9.2/ 10.0*

http://www.linux-mandrake.com/en/security/

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

xchat	*RHSA-2004:177-01*	*9.0*
lha	*RHSA-2004:179-01*	*9.0*
httpd	*RHSA-2004:182-01*	*9.0*
utempter	*RHSA-2004:175-01*	*9.0*
libpng	*RHSA-2004:181-01*	*9.0*
OpenOffice	*RHSA-2004:163-01*	*9.0*
mc	*RHSA-2004:173-01*	*9.0*
kernel	*RHSA-2004:188-01*	*AS.ES.WS 3*
ipsec	*RHSA-2004:165-01*	*AS.ES.WS 3*
kdelibs	*RHSA-2004:222-01*	*AS.ES.WS 2.1 / AS.ES.WS 3*
cvs	*RHSA-2004:190-01*	*AS.ES.WS 2.1 / AS.ES.WS 3*
cadaver	*RHSA-2004:191-01*	*AS.ES.WS 2.1*
mc	*RHSA-2004:172-01*	*AS.ES.WS 2.1*
libpng	*RHSA-2004:180-01*	*AS.ES.WS 2.1 / AS.ES.WS 3*
rsync	*RHSA-2004:192-01*	*AS.ES.WS 2.1 / AS.ES.WS 3*

http://www.linuxsecurity.com/advisories/redhat.html

MICROSOFT

Problèmes suite à l'installation du correctif MS04-011

Microsoft annonce que l'installation du correctif MS04-011 sur Windows 2000 peut engendrer des problèmes conduisant à un déni de service lorsque les pilotes 'Ipsecw2k.sys', 'Imcide.sys' ou 'Dlttape.sys' sont installés. Microsoft confirme ce problème si le client VPN Nortel Networks est installé et que le service IPSec Policy Agent est utilisé. Une parade spécifique est fournie et consiste à désactiver le service.

http://support.microsoft.com/default.aspx?scid=kb;EN-US;841382

Révision du bulletin MS01-052 sur RDP

Microsoft a révisé le bulletin MS01-052 au sujet d'une vulnérabilité dans l'implémentation du protocole RDP (Remote Data Protocol) de Windows NT 4.0 et Windows 2000. Le correctif pour Windows NT Server 4.0 Terminal Server Edition a été mis à jour. http://www.microsoft.com/downloads/details.aspx?FamilyId=485658CB-49F0-4AF5-B3DD-C98CB36C0520&displaylang=en

http://www.microsoft.com/technet/security/bulletin/ms01-052.mspx

CAN-2001-0663

Révision du bulletin MS04-014 sur Jet Database Engine

Microsoft a révisé le bulletin MS04-014 au sujet d'un débordement de buffer exploitable à distance dans Jet Database Engine. Le correctif pour Windows XP contient les messages d'erreur conformes à la langue sélectionnée.

http://www.microsoft.com/technet/security/bulletin/ms04-014.mspx

CAN-2004-0197

ORACLE

Révision du bulletin Oracle 64

Oracle a révisé son bulletin 64 au sujet de multiples vulnérabilités dans Oracle9i Database Server, entraînant un déni de service ou la capture d'une session utilisateur. Il indique la vulnérabilité de la version 9.0.1.5 d'Oracle9i Database Server Release 1, ainsi que la disponibilité du correctif associé.

http://otn.oracle.com/deploy/security/pdf/2004alert64.pdf

SAMBA

Disponibilité de Samba 3.0.4 et 2.2.9

Samba annonce la disponibilité de Samba versions 3.0.4 et 2.2.9. Elles corrigent de nombreuses vulnérabilités et notamment l'impossibilité de changer de mot de passe après l'application du correctif Microsoft KB828741 discuté dans le bulletin MS04-012.

http://us1.samba.org/samba/whatsnew/samba-3.0.4.html

http://us1.samba.org/samba/whatsnew/samba-2.2.9.html

SCO

Correctif pour 'Apache'

SCO a annoncé la disponibilité d'un correctif 'Apache' pour SCO UnixWare versions 7.1.1 et 7.1.3 et SCO Open UNIX version 8.0.0, corrigeant ainsi de multiples vulnérabilités.

ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.6/SCOSA-2004.6.txt

CAN-2003-0192, CAN-2003-0542

SGI

Correctif cumulatif

SGI a annoncé la disponibilité du correctif cumulatif 10069 pour SGI ProPack v2.4. Il corrige de multiples vulnérabilités dans les paquetages 'wu-ftpd', 'xfree86' et 'util-linux'.

http://lists.netsys.com/pipermail/full-disclosure/2004-April/020619.html

CAN-2004-0093, CAN-2004-0094, CAN-2004-0080

Le service ESP et le ver Sasser utilisent le même port

Bien que non vulnérable aux attaques du ver Sasser, le serveur web ESP (Embedded Support Partner) de SGI peut être impacté. Il utilise en effet le même port tcp/5554 que celui utilisé par le serveur FTP ouvert par le virus. Le service web est activé par défaut sur les systèmes IRIX et Altix. Il est donc recommandé de s'assurer de la nature du service ouvert sur ce port.

ftp://patches.sgi.com/support/free/security/advisories/20040501-01-I.asc

SUN

Révision du bulletin Sun 57554

Sun a révisé son bulletin 57554 pour annoncé la disponibilité des correctifs finaux pour Sun Solaris 9. L'installation de certains correctifs entraînait l'exposition d'informations sensibles.

Solaris 9 (Sparc) http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=113579&rev=06
Solaris 9 (x86) http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=114342&rev=06

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57554

Retrait de correctifs pour Sun Solaris 9

Sun a retiré les correctifs 113579-02 à 113579-05 (pour Sparc) et 114342-02 à 114342-05 (pour x86). L'installation de ces correctifs peut entraîner l'exposition d'informations sensibles pouvant être exploitée par un utilisateur local ou distant. Sun fournit des correctifs temporaires T113579-06 (pour Sparc) et T114342-06 (pour x86).

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57554

Correctif pour Samba sur Sun Cobalt Qube3

Sun a annoncé la disponibilité des correctifs pour la vulnérabilité présente sur Samba versions inférieures à 2.2.8 pour les serveurs Sun Cobalt Qube3.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/53924http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/53924

CAN-2003-0085

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

CVS

Deux codes d'exploitation pour la faille 'cvs'

Deux codes d'exploitation concernant le débordement de buffer dans le serveur 'cvs' ont été publiés. Le premier code cible les serveurs fonctionnant sur plate-forme Solaris, et le second sur les plate-formes Linux et FreeBSD. Ils permettent d'obtenir un interpréteur de commandes à distance.

http://www.k-otik.com/exploits/05212004.CVS_Solaris.c.php
http://www.k-otik.com/exploits/05212004.CVS_Linux.c.php

CAN-2004-0396

MICROSOFT

Code d'exploitation universel pour une faille MS04-011

Un nouveau code d'exploitation concernant le débordement de buffer dans la bibliothèque 'lsasrv.dll' a été publié. Ce code est universel et cible les systèmes Windows XP et Windows 2000. Il permet théoriquement une prise de main à distance sur le système cible mais nous n'avons pu le vérifier lors de nos tests. Il est fort probable de voir apparaître prochainement un ver utilisant ce code. Au regard de ces risques, nous vous conseillons l'installation du correctif MS04-011, tout en gardant à l'esprit les

http://www.securitylab.ru/_Exploits/2004/04/HOD-ms04011-lsasrv-expl.c

SYMANTEC

Code d'exploitation pour la vulnérabilité DNS

Un code d'exploitation pour la vulnérabilité découverte dans le traitement des paquets DNS par de nombreux produits Symantec a été publié. Il ne permet pas d'obtenir un interpréteur de commandes mais conduit à un déni de service du dispositif attaqué.

http://www.securiteam.com/exploits/5KP0D1PCUI.html

CAN-2004-0445

TCP

Code d'exploitation pour la vulnérabilité TCP

Un nouveau code exploitant la vulnérabilité dans le protocole TCP a été diffusé. ***autoRST*** *est un outil utilisant les bibliothèques Winpcap afin de scruter le trafic réseau dans l'optique d'exploiter cette faille. Il construit des paquets RST en calculant le numéro de séquence approprié et usurpe l'adresse MAC correspondante. Ce code semble bien plus performant que le précédent.*

http://www.securiteam.com/exploits/5YP0915CUI.html

VIRUS

Code d'exploitation pour le ver Sasser

Le ver Sasser ouvre un serveur FTP lors l'infection. Celui-ci est vulnérable à un débordement de buffer. Il est donc possible d'exploiter le ver afin d'obtenir un interpréteur de commandes à distance sous des droits privilégiés. Par ailleurs, on apprend que les nouvelles versions de Sasser utilisent le port tcp/1022 afin d'accéder à un interpréteur de commande et ouvrent le serveur FTP sur le port tcp/1023.

http://www.k-otik.com/exploits/05102004.sasserftpd.c.php
http://vil.nai.com/vil/content/v_125091.htm

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :

CISCO

Vol du code source de IOS 12.3

Un pirate a annoncé le 15/05/2004 avoir volé le code source de CISCO IOS 12.3. La validité des preuves fournies reste cependant à confirmer, ainsi que le fait qu'il aurait bien réussi à subtiliser 800 Mo de code source comme il le prétend. Si tel était le cas, il est à craindre que nombreuses nouvelles vulnérabilités soient découvertes dans les jours à venir. Elles pourraient faire l'objet d'exploitations systématiques comme cela fût le cas lors de la divulgation du code source de Windows. Nous recommandons en conséquence de porter une grande attention aux événements journalisés par les différents équipements réseaux et de sécurité.

http://www.securitylab.ru/45221.html
http://www.zone-h.org/en/news/read/id=4235/
http://news.com.com/2100-7349_3-5213724.html

VIRUS

Complément d'informations sur le virus Sasser

Plusieurs éditeurs diffusent des informations utiles au sujet du ver Sasser. ISS rapporte que le serveur FTP ouvert par le virus sur le port tcp/5554 contient une vulnérabilité ! Il est donc possible d'exploiter ce ver afin d'obtenir un accès sur le système affecté. Par ailleurs, il est conseillé de filtrer les ports udp/135, udp/137, udp/138, udp/445, ainsi que tcp/135, tcp/139, tcp/445 et tcp/593 afin de limiter la propagation. Il est aussi nécessaire de bloquer les ports tcp/5554 et tcp/9996 utilisés suite à l'infection.

http://xforce.iss.net/xforce/alerts/id/172
http://www.lurhq.com/sasser.html
http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-007/index.html
http://www.securitytracker.com/alerts/2004/May/1010030.html
CAN-2003-0533

Apparition des virus 'Kibuv' et 'Bobax'

Deux nouveaux vers se propagent actuellement sur Internet. Kibuv exploite la vulnérabilité dans LSASS ainsi que celle affectant DCOM RPC. Bobax exploite aussi la vulnérabilité LSASS et tente d'injecter un fichier DLL dans l'espace mémoire du processus 'explorer.exe'. Il ouvre plusieurs ports sur la machine infectée afin de la transformer en relais de mails. http://www.lurhq.com/bobax.html

http://securityresponse.symantec.com/avcenter/venc/data/w32.kibuv.worm.html
http://securityresponse.symantec.com/avcenter/venc/data/w32.bobax.a.html
CAN-2003-0533, CAN-2003-0352

Le ver Dabber exploite la faille laissée par Sasser

Le ver Dabber est apparu sur Internet. Il exploite la faille laissée dans le serveur FTP ouvert par Sasser. Lorsqu'il s'exécute, Dabber s'installe dans une clé portant la valeur 'package.exe' et supprime de nombreuses entrées dans la base de registre, principalement dans les applications et services installés par Sasser et par d'autres virus. Il ouvre un serveur TFTP lui permettant de se propager et ouvre une porte dérobée sur le port tcp/9898. Le ver repère les systèmes affectés en se connectant au port tcp/5554. Dabber est bien plus dangereux que le ver Sasser qu'il exploite. Maintenez vos signatures d'antivirus régulièrement à jour.

http://www.lurhq.com/dabber.html

ATTAQUES

TECHNIQUES

PHISHING

▪ **Description**

Deux études ont été publiées simultanément par le '**Gartner Group**' et la société '**MessageLabs**' ce mois qui portent sur ce nouveau fléau désigné par le nom imagé de '**Phishing**'. Ce nom résulte de la contraction des termes américains '**Phreak**' et '**Fishing**', le premier désignant les fraudeurs à la taxe téléphonique – **Phone Freak** - et le second tout simplement l'action de pécher.

Le terme '**Phishing**' ainsi se traduire en 'pèche à la fraude informatisée' puisqu'il s'agit de ratisser sans préjuger du moyen utilisé – message électronique, site WEB piégé, virus … - une population a priori crédule dans l'optique de collecter un maximum d'informations sensibles car ouvrant l'accès à des biens personnels: comptes bancaires, numéro de cartes de crédit, codes d'accès à divers services, …

On trouvera une première trace de ce procédé dans les années 90 avec l'apparition de messages électroniques censés provenir de la Maison Blanche – '**whitehouse.gov**' – mais forgés de toutes pièces. On ne pouvait alors réellement parler d'escroquerie mais plutôt de manipulation politique, l'objectif étant alors de jeter le discrédit sur l'administration Américaine.

Dans la même période est apparue l'une des plus remarquables escroqueries jamais réalisées par le biais d'un support moderne tel que le fax puis quelques années plus tard, la messagerie électronique, escroquerie désormais désignée par le terme de '**lettre Nigérienne**' ou '**Nigerian 4.1.9 SCAM**' du nom du pays à l'origine des premières lettres.

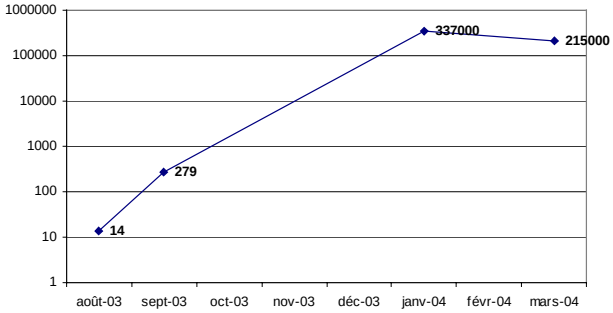
Le point d'orgue en matière d'escroquerie organisée a très certainement été atteint fin 2003 avec la mise en place de procédés délictueux de collecte d'informations personnelles performants, remarquablement fiables, totalement automatisables, bref industrialisables à très grande échelle pour être opérés par des associations de malfaiteurs.

Les deux études précédemment mentionnées mettent en évidence un taux d'augmentation phénoménal des tentatives de collectes utilisant les procédés de '**Phishing**' sur les 6 derniers mois.

L'étude publiée par la société '**MessageLabs**' spécialisée dans le traitement, l'analyse et le routage de messages électroniques pour les grandes entreprises annonce ainsi avoir détecté 215000 messages piégés en mars dernier contre seulement 279 en septembre 2003.

Cette société annonce analyser quelques 45 millions de messages par jour pour ses 8500 clients répartis de par le monde.

Les chiffres publiés doivent en conséquence être pris avec le plus grand sérieux car résultant d'une analyse effectuée sur une base de référence conséquente et représentative en matière de clientèle.



En autres résultats, cette étude met en évidence un premier point commun à toutes les sociétés servant d'appât: elles ont toutes une présence signifiante en matière de service en ligne. Sont ainsi prioritairement touchés les acteurs de premier plan dans le domaine de la banque et de l'assurance mais aussi les services de vente aux enchères, …

La mondialisation de la langue anglo-saxonne fait des services disponibles dans cette langue une cible particulièrement appréciée des fraudeurs. Les campagnes d'attaques ont ainsi particulièrement visé les clients des **banques TD Canada**, **CitiBank**, **Ebay PayPal** et **Visa** sur le continent **Nord Américain**, **Barclays**, **NatWest**, **Lloyds TSB** et **Halifax** en Angleterre ou encore **ANZ**, **WestPac**, **National**, **Commonwealth** en Australie.

Le phénomène ne semble pas avoir encore atteint la France, du moins à l'échelle observée dans les pays anglo-saxons, mais tout laisse à penser que cela n'est hélas que temporaire. La majorité des banques Françaises disposant d'un service en ligne ont d'ailleurs anticipé ce risque en informant leurs clients des bonnes pratiques à respecter.

Les statistiques publiées mensuellement par le groupe de travail '**AWG**' – Anti-Phishing Working Group – et reproduites ci-après reflètent l'étendue des dégâts sur les grandes sociétés. Ainsi et pour le seul mois de mars dernier, les clients de la société **e-Bay** étaient en première ligne avec 110 messages spécialement créés à leur attention, suivis de près par les clients de la **CitiBank** (98 messages différents), de **PayPal** (63 messages) et de la **Fleet Bank** (23 messages).

Fait remarquable, la société **AOL** longtemps positionnée en troisième position semble ne plus autant attirer les escrocs.

Les auteurs de l'analyse accompagnant ces statistiques font remarquer que le mois de Mars aura été particulièrement fertile en nouveautés puisque le seuil de 100 messages différents par semaine aura été dépassé 2 fois.

On en déduira que les escrocs à l'origine des ces délits ont les mêmes contraintes que les professionnels du marketing et doivent renouveler leurs méthodes et leur messages régulièrement !

	Métier	03/04	02/04	01/04	12/04	11/04
eBay	Service	110	104	51	33	6
CitiBank	Banque	98	58	35	17	6
PayPal	Banque	63	42	10	6	4
Fleet Bank	Banque	23	9	2	2	1
Barclays	Banque	11	6	1	1	-
AOL	ASP	10	10	34	16	4
Westpac	Banque	10	-	2	2	1
Visa	Banque	7	8	2	2	1
BankOne	Banque	5	3	-	-	-
Earthlink	ISP	5	8	9	4	2
Microsoft	ASP	5	1	3	3	1

ANZ	Banque	4	-	2	2	1
HSBC	Banque	4	-	-	-	-
Lloyds	Banque	4	-	1	1	-
US Bank	Banque	4	-	1	1	-
Yahoo !	ASP	3	4	2	1	-
AT&T	ISP	2	-	1	1	-
Chase	Banque	2	-	-	-	-
e-Gold	Banque	2	2	1	1	-

De son coté, l'étude projective menée par le **Gartner Group** met en évidence le très fort taux de succès de ce procédé relativement nouveau puisqu'elle estime qu'environ 19% des américains ayant reçu un mail de 'Phishing' – soit quelques 11 millions d'utilisateurs adultes – auront suivi le lien HTML aboutissant sur le site de collecte. **Gartner Group** considère que 3% des ces personnes auront dévoilé aux escrocs des informations sensibles d'ordre privées ou financières par ce biais.

Sur le plan purement technique, toutes les analyses concourent à démontrer que les attaques de ce type ne sont plus l'œuvre d'individus isolés mais bien le fait de groupes mafieux organisés comme une véritable industrie disposant de tous les moyens logistiques et financiers nécessaires: développement des sites de collecte, des programmes piégés installés sous la forme de chevaux de Troie sur les systèmes de victimes mais aussi mise en œuvre et gestion de serveurs **DNS** permettant l'enregistrement de domaines valides pour la durée d'une arnaque, et dans ce monde électronique, tout va très vite.

Le site 'Codephish.info' fait état de l'arrestation d'un groupe d'une douzaine d'hommes de paille – ou 'electronic mules' dans le jargon - des pays de l'Est œuvrant pour une organisation mafieuse et de la possible relation de cause à effet liant ces arrestations à la diminution du nombre d'attaques à destination de l'Australie constatée peu de temps après. Cette analyse est à prendre avec toutes les précautions nécessaires mais elle ne semble pas dénuée de sens.

Nous conseillons à ce sujet la lecture des analyses de code publiées sur le site '**CodeFish.org**' et en particulier, l'étude de l'incroyable attaque ayant visé les clients des quatre principales banques Australiennes sous le titre '**The "Bank DDoS Attack" trojan**' par un 'Dawnstar', un australien spécialiste du domaine.

Le taux de réussite de ces procédés purement probabilistes– il faut ici réellement considérer que les arnaqueurs lancent un hameçon auquel ne mordront que quelques poissons – est directement lié à la représentativité de la clientèle de la société prise comme appât dans la population recevant le courrier piégé. Nombres de facteurs influencerons probablement le résultat de la campagne de pèche dont la qualité de la liste de diffusion mais aussi la dimension de la société dans le tissus économique du pays.

Une campagne de 'Phishing' ciblant les clients de quelques grandes entreprises Françaises par le biais de messages rédigés en Français et transmis sur des adresses de messagerie collectées dans le domaine '.fr' pourrait ainsi avoir un taux de succès bien supérieur à celui des campagnes actuellement engagées vers les pays anglo-saxons.

Sur le plan pratique, les techniques de '**Phishing**' peuvent utiliser plusieurs supports – messages électroniques, sites WEB compromis, … mais elles partagent toutes la même caractéristique: amener le 'pigeon' à fournir tous les renseignements souhaités en toute bonne fois et sans que l'arnaque ne puisse être immédiatement détectée.

Les bonnes vieilles recettes des arnaqueurs d'antan sont toujours valables dans le monde du virtuel et de l'intangible: il faut endormir la méfiance du client par tous les moyens possibles en lui présentant l' environnement rassurant qu'il est en droit d'attendre.

L'approche la plus usitée consiste à informer le 'pigeon' par courrier électronique, avec doigté et toute la forme nécessaire, d'un quelconque problème nécessitant de sa part une action ou une réponse immédiate en lui recommandant d'utiliser directement le lien fourni dans le courrier plutôt que de répondre à celui-ci. La réussite de l'opération dépendra pour une bonne part du fond et de la forme du message qui devra avoir l'aspect le plus officiel possible mais aussi des moyens mis en œuvre pour masquer les traces de la manipulation fondamentale, à savoir l'aiguillage du client vers un site tiers n'ayant rien à voir avec le site de la société censée être à l'origine de la demande.

C'est à ce niveau qu'entrent en jeux les milles et unes techniques de manipulation destinées à semer la confusion dans les principaux navigateurs WEB dont les moteurs de présentation sont utilisés par les clients de messageries voire à implanter de manière permanente dans ceux-ci quelques lignes de code destinées à intercepter les entrées clavier et masquer certains liens.

L'objectif reste cependant toujours le même: masquer l'URL du site réellement accédé par une URL rassurante. Plusieurs procédés peuvent être ici utilisés qui tirent toujours parti du format de la balise '**A**' (Anchor ou Ancre), laquelle autorise l'association d'un descriptif avec le lien référencé par l'attribut '**HREF**'.

Soit dans sa forme la plus simple:

```
<A HREF "http://www.mysite.com/mypage.html" > Un lien vers ma page </A>
```

Référence du LIEN (une URL) — Description

Le procédé le plus simple reste celui consistant à encoder une référence n'ayant rien à voir avec la description. Moyennant l'utilisation de couleurs ad'hoc, la chaîne correspondant à la description pourra se fondre avec l'URL associée.

```
<A HREF="http://www.mysite.com/index.html">http://www.mybank.com/index.html
```

Un utilisateur averti découvrira cependant la supercherie en se référant à l'information présentée dans la barre d'état du navigateur ou encore dans une bulle pour certains clients de messagerie.

Plus astucieux est le procédé consistant à remplir l'URL de caractères non interprétés mais cependant représentés à l'écran de manière à déplacer à l'extrême droite de la fenêtre, si possible en dehors de l'espace réservé dans la barre d'état, la partie réellement utile de l'URL. Rappelons en effet que la forme normale d'une URL autorise l'utilisation du caractère '@' comme séparateur de champ, la partie précédant ce caractère étant alors censée contenir un nom d'utilisateur et optionnellement un authentifiant.

```
http:// user:password @ www.mysite.com/mypage.html
```

Données — URL d'accès à la ressource

Il est donc parfaitement légal du point de vue syntaxique de présenter une URL constituée de la chaîne que l'on

souhaite faire apparaître dans la barre d'état, suivie d'une grande quantité de caractères ' ' en utilisant l'encodage HTML et terminée par le caractère '@' précédant l'URL du site vers lequel le navigateur sera dirigé.

```
<A HREF="http://www.mybank.com&#32&#32 ... &#32@http://www.mysite.com/index.html">http://www.mybank.com/index.html
```

Ce procédé – publié le 8 mai dernier - n'est pas sans rappeler celui utilisé un temps par les auteurs de virus qui consistait à utiliser un nom de fichier en attachement comportant une extension jugée sans risque suivie d'une grande quantité d'espaces et de la véritable extension. Seuls les quelques dizaines de premiers caractères étaient affichés dans la fenêtre de travail du client de messagerie persuadant l'utilisateur qu'il avait à faire à un attachement inoffensif.

Un procédé alternatif tirant partie d'une vulnérabilité de conception présente dans Internet Explorer et fort heureusement corrigée par le correctif '**MS04-004**' consistait à insérer le caractère '%00' (dit NULL), voire le caractère '%01', immédiatement avant le caractère '@'.

```
<A HREF="http://www.mybank.com%00@http://www.mysite.com/index.html">http://www.mybank.com/index.html
```

Les moyens employés évoluent de jour en jour au grès de la découverte de nouvelles vulnérabilités, voire simplement d'erreurs d'implémentation, dans les moteurs de présentation HTML mais aussi de l'astuce des arnaqueurs. N'a-t-on pas vu poindre dernièrement un procédé consistant purement et simplement à remplacer la barre d'adresse du navigateur Internet Explorer par une copie conforme programmée en JavaScript !

La solution imparable reste encore celle de l'inspection visuelle du code source de la page et plus particulièrement de toutes les URL associées aux balises '**A**' ou à l'attribut '**HREF**'. Encore faut-il que le volume de données à inspecter soit raisonnable et que celles-ci soient présentées de manière intelligible ce qui est hélas rarement le cas dans les exemples de 'Phishing', obscurcis à souhait !

On recommandera la consultation régulière du site '**antiphishing.org**' en passe de devenir aussi célèbre que son homologue '**hoaxbuster.com**' consacré aux canulars et autres mystifications de toutes sortes.

▪Complément d'information

http://www.messagelabs.com/microsites/phishing/phishing.pdf	- Analyse de la société MessageLabs
http://www4.gartner.com/5_about/press_releases/asset_71087_11.jsp	- Projection du Gartner Group
http://www.antiphishing.org/APWG_Phishing_Attack_Report-Mar2004.pdf	- Statistiques de l'AWG
http://www.codephish.info/	- Site d'information
http://assiste.free.fr/p/frameset/06_42.php	- Excellente présentation