Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 01 juin 2004
N° CERTA-2004-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N3

Gestion du document

Référence	CERTA-2004-ACT-003
Titre	Bulletin d'actualité N3
Date de la première version	01 juin 2004
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

2 Activité en cours

Le tableau des paquets rejetés (cf. table 2) montre l'activité entrante refusée sur deux pare-feux configurés pour tout bloquer par défaut et n'autoriser que quelques services sur quelques serveurs. Les ports présents dans ce tableau ont été choisis pour leur fréquence d'apparition ou pour leur caractère dangereux constaté dans des incidents traités par le CERTA.

Il s'agit de déterminer à quoi correspondent ces paquets rejetés et quels sont les enseignements pragmatiques en termes d'administration quotidienne de la sécurité que l'on peut retirer de l'observation de ces rejets de paquets.

port	pourcentage
$135/tcp$	34,84
$445/tcp$	29,55
$80/tcp$	10,30
$137/udp$	8,77
$2745/tcp$	3,99
$139/tcp$	3,70
$1433/tcp$	1,42
$3127/tcp$	1,41
$1434/udp$	1,16
$5000/tcp$	0,89
$6129/tcp$	0,85
$4899/tcp$	0,76
$5554/tcp$	0,56
$9898/tcp$	0,43
$21/tcp$	0,39
$1080/tcp$	0,33
$443/tcp$	0,21
$3128/tcp$	0,17
$23/tcp$	0,12
$3389/tcp$	0,07
$111/tcp$	0,04
$22/tcp$	0,03
$10080/tcp$	0,01

TAB. 2 – *Paquets rejetés*

Durant la période du 20 mai 2004 au 27 mai 2004, l'activité a été marquée par un net recul de la propagation des vers bien connus. Les ports 135/tcp et 445/tcp sont toujours les ports les plus recherchés, et représentent près des deux tiers des rejets.

L'activité des vers de la famille `Phatbot` a fortement diminué. Les vers de cette famille se caractérisent par des scans simultanés sur les ports 6129/tcp, 2745/tcp et 3127/tcp. Ces scans émanent généralement de machines compromises. Toutefois, en fonction des règles de filtrage actuellement mises en œuvre pour ces machines compromises, il est possible de ne voir qu'une partie de ces scans.

L'activité sur le port 5000/tcp attribué aux vers `Kibuv` et `Bobax` a chuté mais n'est pas nulle.

3 Activité particulière

Les vers `Bobax` et `Kibuv`, découverts à la mi-mai 2004, ont eu une activité en forte baisse durant la période du 20 mai 2004 au 27 mai 2004. Ces vers se caractérisaient par un scan sur le port 5000/tcp, probablement dans le but d'identifier des machines fonctionnant sous Windows XP. Cette caractéristique a probablement limité la propagation de ces vers, puisqu'ils ne tentent de se propager qu'après avoir reçu une réponse positive du scan sur le port 5000/tcp. De plus, ces vers tentent d'exploiter une faille du service `lsass`, qui a été largement exploitée par le ver `Sasser`. La mise en place des filtres sur le port 445/tcp par certains fournisseurs d'accès, ainsi que l'application des correctifs de Microsoft pour Windows ont contribué à limiter la propagation des vers `Bobax` et `Kibuv`.

4 Retour d'expérience sur les incidents

Nous profitons de ce bulletin d'actualité pour vous rappeler les dangers de l'écriture des programmes *CGI* (Commom Gateway Interface), notamment ceux en PHP.

Le CERTA a déjà publié en 2003 une alerte traitant de l'exploitation de la vulnérabilité "include PHP" (CERTA-2003-ALE-003).

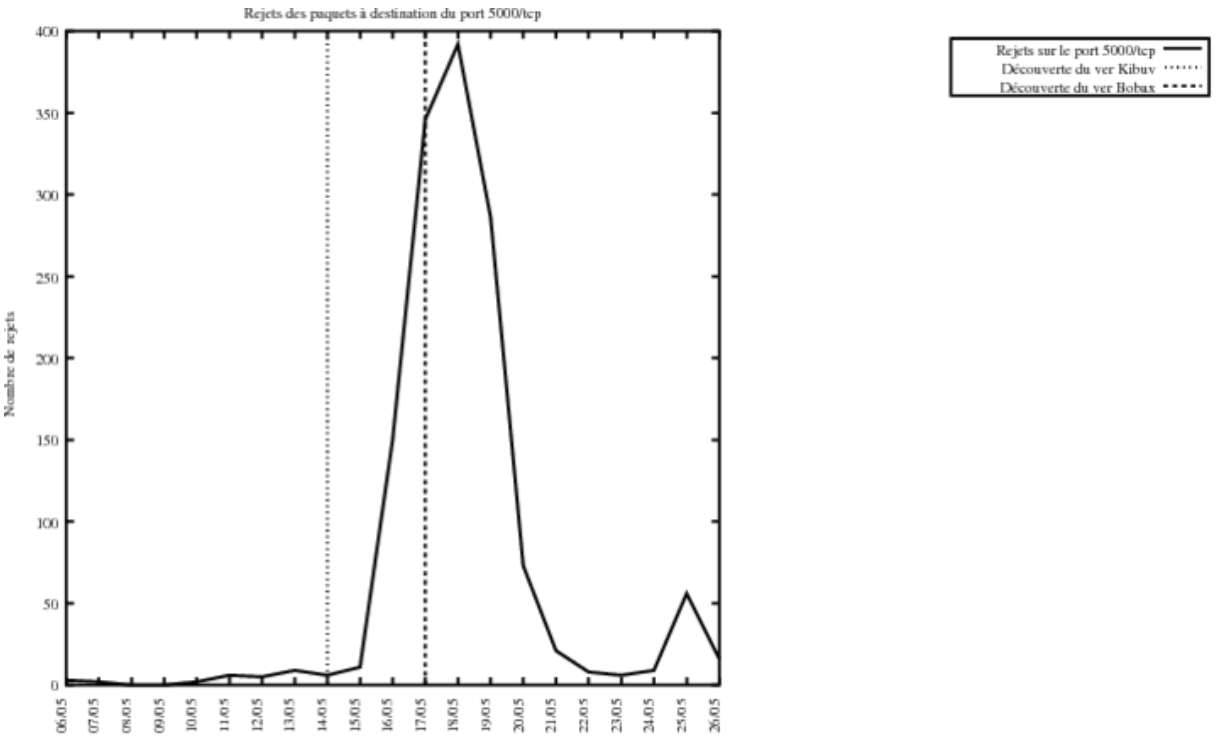

FIG. 1 – *Historique des rejets de paquets sur le port recherché par les vers Bobax et Kibuv*

Nous avons traité ces derniers temps plusieurs incidents relatifs à des gestionnaires de contenus développés en PHP.
Les vulnérabilités exploitées proviennent d'erreurs de programmation, comme par exemple des chaînes de caractères renseignées par l'utilisateur, dont le contenu n'est pas correctement vérifié.

Il existe de nombreux logiciels permettant aux éditeurs de site web en PHP de développer plus rapidement les différents scripts (*PHP-nuke*, *phpBB*, etc...). Ces logiciels incluent des modules de base, qui peuvent être réutilisées dans les sites.

De nombreux problèmes sont apparus à cause d'erreurs directement incluses dans ces briques. Les développeurs de sites ne prenant pas toujours le temps de relire le code source des modules qui leur sont fournis.

Il est donc primordial de vérifier le code des programmes *CGI*, et de se tenir informé des vulnérabilités et des correctifs concernant ces différents programmes.
Voici un site recensant les vulnérabilités relatifs à différents scripts PHP :
http://www.phpsecure.info
Les administrateurs de sites rédigés avec *PHP-nuke* (ou tout autre outil PHP) sont invités à prendre contact avec le CERTA.

5 Actions suggérées

5.1 Respecter la politique de sécurité

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document.

5.2 Appliquer les correctifs de sécurité

La table 3 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-066 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-064 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-132
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-152
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-209 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-179 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-131
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-050
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-052
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-00 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-111 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-031
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-168 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-144 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-045 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-102 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-068 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-041 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-004 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-156
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-095 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-053 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-105 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-038 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-062
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-165
5554	TCP	–	Serveur ftp de Sasser	–
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–

TAB. 3: Correctifs correspondant aux ports destination des paquets rejetés

5.3 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. Un pare-feu correctement configuré peut retenir les attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée.. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage d'un pare-feu.

5.4 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement de sorte à découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

5.5 Réagir aux incidents de sécurité

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

Liste des tableaux

Gestion détaillée du document

01 juin 2004 version initiale.