Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 décembre 2005
N° CERTA-2005-ACT-049

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-49

Gestion du document

Référence	CERTA-2005-ACT-049
Titre	Bulletin d'actualité n° 2005-49
Date de la première version	09 décembre 2005
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 Activité en cours

1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 01 et le 08 décembre 2005.

1.2 Incidents traités

1.2.1 Défigurations de site

Le CERTA a traité deux cas de défiguration de site web. Dans le premier cas, la faille exploitée est une vulnérabilité de `phpBB`. Les forums reposant sur `phpBB` sont très nombreux, et sont parfois installés à l'insu des administrateurs.Dans l'autre cas, c'est une faille de type « injection ASP » qui a été exploitée.

1.2.2 Compromissions

Le CERTA a analysé un serveur web compromis par l'exploitation d'une faille de `awstats.pl` (à noter qu'un forum reposant sur une version vulnérable de `phpBB` était également présent). La compromission a été très limitée par l'existence d'un filtrage en sortie, ce qui a bloqué les tentatives d'utilisation de la commande `wget` par le pirate. Ce dernier, n'ayant pas réussi à installer ses outils, a abandonné la machine.

D'autre part, le CERTA a été informé de la probable compromission d'un serveur, celui-ci ayant scanné de nombreuses classes d'adresses sur le port 22/tcp (ssh).

2 Logiciel de protection Sony

Plusieurs utilisateurs ont remonté au CERTA depuis plusieurs semaines, les journaux de leur serveur de résolution de noms. Ces journaux montrent des requêtes provenant de la même adresse IP, ayant les mêmes ID et port et portant sur les noms de domaine `connected.sonymusic.com`, `license.sunncomm2.com`, `updates.xcp-aurora.com`... Ces requêtes sont effectuées par des programmes executés depuis un laboratoire de recherche qui tente de connaître l'étendue de la propagation du cheval de Troie présent dans le logiciel de protection de Sony. Cette étude est réalisée à partir des réponses retournées par les serveurs cache de noms qui sont configurés de façon à accepter des requêtes depuis l'extérieur. Les résultats de cette étude peuvent être trouvés sur le site du laboratoire de recherche à l'adresse suivante :

http://www.doxpara.com?q=sony

La carte semble présenter une plus faible diffusion dans notre pays, qui n'est pas forcément caractéristique d'une moindre prolifération : les caches en France peuvent juste être moins nombreux à appliquer une politique de restriction des interrogations.

Pour savoir si votre ordinateur est compromis il suffit de visualiser si le service `XCP CD Proxy` est démarré sur votre ordinateur. Dans ce cas, il est probable que le cheval de Troie soit également installé sur votre ordinateur. Des outils de désinfection ont été fournis par certains éditeurs d'antivirus pour supprimer ce cheval de troie.

3 Liens utiles

- Note d'information pour limiter l'impact du SPAM ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
  http://www.auscert.org.au/render.html?it=1935

4 Rappel des avis et mises à jour émis

Durant la période du 02 au 08 décembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-477 : Vulnérabilité de Citrix
- CERTA-2005-AVI-478 : Vulnérabilité dans Webmin/Usermin
- CERTA-2005-AVI-479 : Vulnérabilité dans DotClear
- CERTA-2005-AVI-480 : Vulnérabilité dans Helix Player
- CERTA-2005-AVI-481 : Vulnérabilité du serveur HTTP de CISCO IOS
- CERTA-2005-AVI-482 : Vulnérabilité de cURL/libcURL
- CERTA-2005-AVI-483 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées
- CERTA-2005-AVI-484 : Vulnérabilité dans phpMyAdmin

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2005-AVI-474-001 : Multiples vulnérabilités dans la machine virtuelle Java de Sun
  (ajout de la référence au bulletin de sécurité Apple)
- CERTA-2005-AVI-400-003 : Faiblesse dans OpenSSL 0.9.x
  (ajout de la référence à l'avis de sécurité Cisco)
- CERTA-2005-AVI-457-001 : Déni de service sur SpamAssassin
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-478-001 : Vulnérabilité dans Webmin/Usermin
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-383-003 : Vulnérabilité dans UW-imapd
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:850)
- CERTA-2005-AVI-474-002 : Multiples vulnérabilités dans la machine virtuelle Java de Sun
  (corrections et précisions sur les versions impactées)
- CERTA-2005-AVI-478-002 : Vulnérabilité dans Webmin/Usermin
  (ajout des références aux bulletins de sécurité Gentoo et DYAD Security)

5 Actions suggérées

5.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

5.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

5.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

5.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines 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 correct d'un pare-feu.

5.5 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 afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

5.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

5.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

6 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.

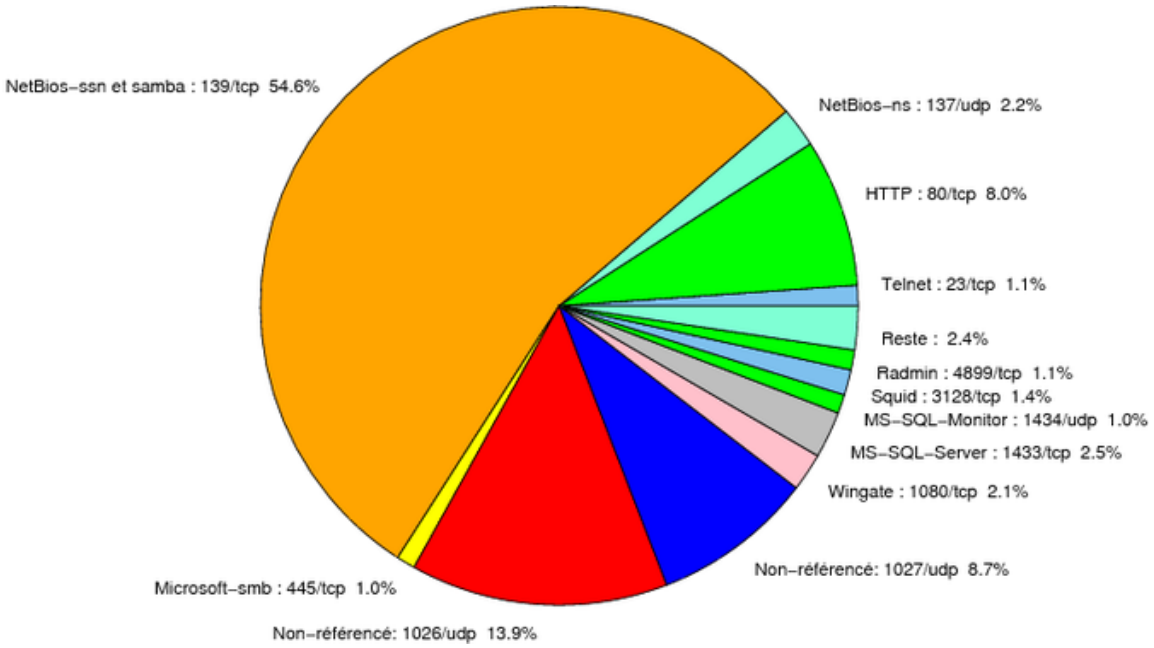

FIG. 1: Répartition relative des ports pour la semaine du 01.12.2005 au 08.12.2005

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT

111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CER
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
139/tcp	54,64
1026/udp	13,93
1027/udp	8,72
80/tcp	8
1433/tcp	2,52
137/udp	2,16
1080/tcp	2,05
3128/tcp	1,37
23/tcp	1,1
4899/tcp	1,08
1434/udp	1,02
445/tcp	1,01
10000/tcp	0,66
15118/tcp	0,4
22/tcp	0,34
6129/tcp	0,21
3306/tcp	0,18
25/tcp	0,14
2100/tcp	0,09
21/tcp	0,07
3127/tcp	0,06
5554/tcp	0,03
9898/tcp	0,02
11768/tcp	0,01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

09 décembre 2005 version initiale.