Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2004
N° CERTA-2004-ACT-021

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N21

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2004-ACT-021

Gestion du document

Référence	CERTA-2004-ACT-021
Titre	Bulletin d'actualité N21
Date de la première version	08 octobre 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

Durant la semaine du 23 au 30 septembre 2004, les paquets à destination des ports 135/tcp, 445/tcp et 137/udp ont constitué la majeure partie des rejets observés sur deux dispositifs de filtrage.

Une machine compromise nous a été signalée par un de nos correspondants. Cette machine, dont le profil est un serveur http sous Linux RedHat 9, est en cours d'analyse par le CERTA.

port	pourcentage
135/tcp	27,33
445/tcp	20,41
137/udp	19,07
139/tcp	5,53
5554/tcp	3,79
80/tcp	3,44
1433/tcp	2,92
1026/udp	2,31
1080/tcp	2,27
9898/tcp	2,04
1023/tcp	1,74
1027/udp	1,70
1434/udp	1,55
21/tcp	1,01
2745/tcp	0,84
4899/tcp	0,79
3127/tcp	0,78
6129/tcp	0,57
22/tcp	0,50
443/tcp	0,43
23/tcp	0,36
111/tcp	0,20
3389/tcp	0,14
5000/tcp	0,13
3128/tcp	0,10
6112/tcp	0,05

TAB. 2 – *Paquets rejetés*

3 Analyse d'un ver inconnu

Le CERTA a été contacté à propos d'une machine infectée par un ver a priori non reconnu par certains antivirus à la date de l'étude. Ce ver a fait l'objet d'une analyse comprenant plusieurs étapes.

3.1 Vérification du format du ver

Le ver se présente sous la forme d'un fichier d'extension .zip. Il s'agit d'un fichier de type `zip` possédant une structure valide et contenant un fichier d'extension `.exe` de nom `winole.exe`. Cet exécutable n'est pas reconnu par la plupart des antivirus au moment de l'étude du ver par le CERTA. En regardant plus en détail le type du fichier, il s'agit bien d'un fichier exécutable au format PE (Portable Executable), format standard en environnement Microsoft Windows.

3.2 Analyse des chaînes de caractères

Une analyse rapide des chaînes de caractères contenues dans l'exécutable ne révéle a priori rien de classique (pas de fonctions relatives à une activité réseau, pas de manipulation de messages électroniques ...). Le fichier est compressé avec l'outil de compression ("packer") Molebox. Cet outil permet, en plus de la compression d'un exécutable, le chiffrement de son contenu.

3.3 Installation du ver dans un environnement isolé

Dans un environnement de test déconnecté de tout réseau, le CERTA procède ensuite à l'analyse comportementale du ver. Lors du lancement de l'exécutable, des outils de surveillance d'un certain nombre de points clefs d'un système Windows sont utilisés.

La première chose constatée est la création d'un exécutable dont la chaîne de caractères est aléatoire. Il s'agit du ver qui sera résident dans la machine. Chaque ver est ainsi "unique", créé à la volée sur la machine. Il est important de noter ce point dans le cas où certains pensent que le nom de l'exécutable est toujours une donnée unique pour un ver ou un virus. Il en est de même pour la taille ainsi que le contenu de l'exécutable et donc des données dérivées telles les empreintes MD5 ou SHA-1 qui peuvent ainsi changer pour un même virus ou ver. L'observation de la base de registre Microsoft Windows montre la modification, entre autre, des clefs suivantes :

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

Ces clefs de registre sont des endroits classiques (mais ce ne sont pas les seuls) où un ver écrit afin de survivre aux prochains redémarrages.

3.4 Analyse du trafic réseau

Après quelques jours de surveillance, une activité réseau "légère" est confirmée. Il s'agit de recherches des partages au sens Microsoft, probablement pour en exploiter les vulnérabilités classiques.

Le CERTA n'a pu confirmer une activité de type IRC. En pareil situation, une activité IRC permet en général de pousser l'analyse plus loin, dans le cas où les machines concernées sont des machines relevant de notre communauté. Pourtant, l'analyse des chaînes de caractères de l'exécutable décompressé laissait supposer que le fonctionnement du ver reposait, en partie, sur l'IRC.

3.5 Conclusion

Une telle analyse, bien que très succinte, permet de se faire une idée globale sur un exécutable et d'avoir des pistes dans le cas où l'on désire pousser plus loin l'analyse.

Ce ver utilise les partages réseau pour se propager, mais il est possible qu'il ait d'autres fonctionnalités (défectueuses ou impossibles à mettre en évidence dans notre environnement).

Seul un désassemblage et une analyse du code assembleur permet de comprendre en profondeur tous les comportements du ver. Plusieurs outils sont disponibles pour réaliser ceci, de solides bases en assembleur sont le prérequis minimum.

Il est important de souligner que ce genre d'analyse doit-être effectuée dans un environnement dédié, déconnecté de tout autre réseau (Internet, Intranet ...). Le comportement du ver ou du virus n'étant jamais connu à l'avance, les conséquences sont toujours imprévisibles et peuvent être graves.

4 Actions suggérées

4.1 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.

4.2 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.

4.3 Appliquer les correctifs de sécurité

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

4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. Unpare-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.

4.5 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.

4.6 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 Rappel des avis et des mises à jour émis

Durant la semaine du 27 septembre au 01 octobre, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-327 : Multiples vulnérabilités dans JRUN Server
- CERTA-2004-AVI-328 : Vulnérabilité dans Sendmail avec SASL
- CERTA-2004-AVI-329 : Vulnérabilité dans Subversion

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

- CERTA-2004-AVI-325-001 : Vulnérabilités de XFree86 et de libXpm (ajout du bulletin Gentoo)
- CERTA-2004-AVI-294-002 : Vulnérabilité de lha (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2004-AVI-295-005 : Vulnérabilité dans ImageMagick (ajout de la référence au bulletin FreeBSD et à la mise-à-jour NetBSD)

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-21 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
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-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-14 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-09 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-30 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-03 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
1023	TCP	–	Serveur ftp de Sasser.E	–
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-15
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	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-21
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*

– CERTA-2004-AVI-319-004 : Multiples vulnérabilités dans gdk-pixbuf (ajout référence au bulletin de sécurité de NetBSD)
– CERTA-2004-AVI-318-001 : Vulnérabilité d'OpenOffice et StarOffice (ajout référence au bulletin de sécurité de Mandrake)

6 Documentation

Liste des tableaux

Gestion détaillée du document

08 octobre 2004 version initiale.