



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 novembre 2008
N° CERTA-2008-ACT-047

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-47

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047>

Gestion du document

Référence	CERTA-2008-ACT-047
Titre	Bulletin d'actualité 2008-47
Date de la première version	21 novembre 2008
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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047/>

1 Quand l'USB est le vecteur de l'infection

1.1 Présentation

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un réseau de l'administration par un virus. Malgré un cloisonnement physique des réseaux ayant un niveau de sécurité différent, l'utilisation de supports de stockage USB était autorisée entre les différents réseaux. Une clef USB semble être le vecteur de la première infection. Le virus, qui n'était pas encore reconnu par les antivirus pourtant à jour, s'est ensuite répandu dans tout le réseau.

A cette étape de l'analyse, le CERTA rappelle que des règles de cloisonnement strictes doivent être mises en oeuvre pour éviter de pouvoir contourner les mesures de sécurité mises en place (ici l'isolement des machines en libre-service).

Le CERTA indique également qu'il existe plusieurs méthodes pour désactiver l'exécution automatique des périphériques USB :

- une technique radicale consiste à désactiver le support USB, comme décrite dans la note d'information CERTA-2006-INF-006. Cela peut gêner l'utilisation de périphériques comme des claviers ou des souris ;

- la base de connaissances de *Microsoft* (cf article 823732) indique comment désactiver l'utilisation des dispositifs de stockage USB ;
- une autre technique plus modérée consiste à modifier le comportement de *Windows* à l'égard des fichiers `autorun.inf`. Il est en effet possible de désactiver l'exécution automatique de ce fichier via une clef de registre :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies
\Explorer\NoDriveTypeAutorun
```

Par exemple, la valeur `0xFF` désactive cette fonctionnalité sur tous les supports.

1.2 Documentation

- Article 823732 de la base de connaissance de microsoft :
<http://support.microsoft.com/kb/823732>
- Note d'information du CERTA CERTA-2006-INF-006 du 09 novembre 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>

2 Modification malveillante des résolutions DNS

2.1 Présentation

Le CERTA traite actuellement la recrudescence d'infections d'ordinateurs par un code malveillant modifiant les résolutions DNS des machines victimes. Ce code malveillant modifie la configuration DNS des ordinateurs compromis. Ces derniers lancent alors de nombreuses requêtes DNS directement vers des serveurs DNS situés à l'étranger. Ces serveurs DNS suspects résolvent certaines requêtes de manière anormale en dirigeant les victimes vers des adresses incorrectes.

Ces infections proviennent souvent de la navigation sur des sites malveillants proposant de fausses vidéos ou des (faux) outils de protection gratuits (antivirus, antispyware, ...) ou faisant croire à l'installation de mises à jour.

Pour détecter si des ordinateurs sont compromis, il est recommandé de :

- surveiller le flux DNS et vérifier qu'il s'adresse aux serveurs définis dans l'architecture DNS ;
- vérifier la configuration DNS des postes et le respect de l'architecture DNS comme préconisé dans CERTA-2008-INF-002 ;
- rechercher dans les journaux des antivirus des signalements d'infections par des virus portant de noms tels que : (les versions peuvent évoluer) :
 - Trojan.Win32.DNSChanger.ef (Kaspersky Lab)
 - DNSChanger.a (McAfee)
 - TROJ_DNSCHAN.SUB (Trend Micro)
 - Troj/DNSBust-O (Sophos)
 - Trojan:Win32/Alureon.A (Microsoft)
 - Trojan.Win32.DNSChanger (Ikarus)

Pour se protéger des effets de tels codes malveillants, il est recommandé de :

- mettre en place une architecture DNS n'autorisant les requêtes DNS sur des serveurs extérieurs que dans des cas exceptionnels (nomades) ;
- vérifier l'application de cette architecture (configuration des postes, surveillance du trafic DNS) ;
- rappeler les utilisateurs à la vigilance : ne pas télécharger des fichiers (images, codecs, exécutables, documents) depuis des sources non sûres.

2.2 Références

- Note d'information « Du bon usage du DNS » (section 3.4) :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/>
- Bulletin d'actualité CERTA-2007-ACT-044, « Les modifications de configuration DNS » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-044.pdf>

- Bulletin d'actualité CERTA-2007-ACT-052, « Modification des fichiers » : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-052.pdf>
- Bulletin d'actualité CERTA-2008-ACT-008, « Surveiller le trafic DNS, une nécessité » : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-008.pdf>

3 OpenBSD et correctifs de fiabilité

Cette semaine, le projet OpenBSD a fourni un ensemble de correctifs pour son système d'exploitation homonyme dans sa dernière version (OpenBSD 4.4 mentionné dans le bulletin d'actualité CERTA-2008-ACT-046) :

- un premier concernant le comportement anormal de la pile IPv4 dans certaines conditions ;
- un second relatif au *mod_proxy* du serveur HTTP intégré qui peut présenter des dysfonctionnements sur les systèmes *64-bit* ;
- un troisième concerne un bogue entraînant une consommation excessive de la mémoire lors de la manipulation de tableaux dans des applications ;
- la dernière concerne un problème de non-interopérabilité du serveur DHCP avec certains clients comme ceux de OpenSolaris ou Solaris.

D'après l'éditeur, ces correctifs ne présentent pas un caractère de sécurité. Mais, dans la mesure où ils touchent des composants utilisés relativement fréquemment et que les erreurs peuvent mettre en jeu la disponibilité du système, il est conseillé d'appliquer ces correctifs.

4 Retour sur la vulnérabilité TKIP

4.1 Présentation

Le CERTA avait mentionné dans son bulletin d'actualité CERTA-2008-ACT-045 (section 3) une possible vulnérabilité concernant le protocole TKIP (*Temporal Key Integrity Protocol*).

Les intervenants ont effectivement présenté récemment une méthode d'attaque qui combine plusieurs points :

- la réadaptation d'une attaque détaillée pour le WEP, prénommée *chopchop* ;
- la possibilité d'utiliser différentes files de priorité, comme spécifié dans le standard pour la qualité de service 802.11e, afin de pouvoir réutiliser des *keystreams* ;
- l'exploitation de l'algorithme MIC ou Michael servant au contrôle d'intégrité.

L'attaque concerne aussi bien WPA que WPA2 dans la mesure où TKIP est utilisé, indépendamment de la méthode d'authentification mise en place (PSK ou 802.1X/EAP).

L'exploitation complète de cette vulnérabilité conduit actuellement une personne quelconque qui se trouve à portée des échanges :

- à déchiffrer des paquets arbitraires émis par un point d'accès à destination d'un poste. Comme le déchiffrement actuel de l'attaque est assez lent (un octet par minute), la technique s'applique essentiellement à peu de trames ou des trames de petites tailles et de contenu assez prévisible.
- à injecter des trames arbitraires, avec une limitation imposée principalement par le nombre de files de priorité possibles. L'injection ne doit pas dépasser l'ordre d'une dizaine de trames.

Cette attaque s'appuie par ailleurs sur une technique active, *chopchop*. Il faut donc la lancer sur du trafic réel et non un simple rejeu. Si le poste client se désassocie du point d'accès, l'attaque échoue.

L'attaque a été déployée dans certains outils publics.

4.2 Recommandations

Les recommandations sont inchangées par rapport à celles citées dans CERTA-2008-ACT-045. Nous pouvons cependant apporter quelques précisions quant au renouvellement fréquent des clés avec TKIP. Une clé changée toutes les minutes permet de récupérer un octet. Une rotation de deux minutes peut donc être un bon contournement provisoire. Les points d'accès de type Aruba ("*timer mkey-rotation-period*") et Cisco ("*broadcast-key change*", "*devshell dot1xUpdateBroadcastRekeyTimer*") permettent par exemple de modifier ce paramètre (cf. la documentation).

Ce changement doit être fait avec prudence afin de vérifier qu'il ne génère aucun désagrément pour l'architecture sans-fil.

Cette attaque nécessite également l'interprétation de la qualité de service (802.11e).

Enfin, il est important d'avoir une politique de chiffrement claire mise en place au niveau du point d'accès. Il faut choisir clairement l'option CCMP/AES. Certains points d'accès laissent la possibilité d'être configurés en mode "TKIP+AES". Ce mode hybride est dangereux, car il risque d'imposer le chiffrement le plus faible à tous les postes, même si le mode TKIP est exigé par un seul d'entre eux.

Les tentatives d'attaques peuvent laisser des traces. Il ne faut donc pas négliger l'analyse régulière des journaux du point d'accès. Des erreurs de type `MIC Failure report from the station` peuvent apparaître.

Enfin, certains constructeurs feront éventuellement des mises à jour pour leurs produits. Il faut donc également suivre le support de ces derniers.

4.3 Conclusions

D'autres améliorations à cette attaque sont envisageables dans les prochains mois.

La vulnérabilité ne peut être exploitée qu'avec certaines contraintes. Elle permet néanmoins de mettre en oeuvre des attaques non négligeables, comme la redirection de trafic.

Cette vulnérabilité permet de rappeler que TKIP n'est qu'une solution de sécurité partielle et que les mises en oeuvre doivent tendre vers du chiffrement plus robuste, avec AES/CCMP.

Il est donc important de penser dès à présent à sensibiliser les utilisateurs et les aider à configurer leurs postes vers ce choix quand cela est possible.

4.4 Documentation associée

- Site "Wireless Vulnerabilities and Exploits, WVE-2008-0013, en référence à l'intervention de M. Beck, E. Tews, « Practical attacks against WEP and WPA », PACSEC 2008 :
<http://www.wirelessve.org/entries/show/WVE-2008-0013>
- Bloc-Notes de C. Blancher, « Des fameuses faiblesses de TKIP... » :
<http://sid.rstack.org/blog/index.php/305-des-fameuses-faiblesses-de-tpip>
- Présentation de J. Wright, « Understanding the WPA/WPA2 Break », 2008 :
http://www.willhackforsushi.com/presentations/TKIP_Attack_Webcast_2008-11-17.pdf
- Réponse de Cisco, « Cisco Response to TKIP Encryption Weakness », 21 novembre 2008 :
<http://www.cisco.com/warp/public/707/cisco-sr-20081121-wpa.shtml>
- Aruba Networks, « TKIP Vulnerabilities », 10 novembre 2008 :
<https://edge.arubanetworks.com/article/tpip-vulnerabilities>

5 Les URI Data:

5.1 Présentation

Les *URI (Uniform Resource Identifier)* de type *Data:* permettent l'insertion de données dans tout fichier acceptant ce format d'adresse. Les *URI Data:* sont définies dans la RFC 2397 et la syntaxe est la suivante :

```
data:[<mediatype>][ ;encodage ] , <data>
```

La RFC fait état de fichier média mais il est cependant possible d'envoyer des fichiers de différents types : texte, images, données à passer en paramètre à une application, vidéo, ...

Cette fonctionnalité pourrait être détournée à des fins malveillantes en envoyant des données malformées. De plus, l'encodage des données à leur émission permet une obfuscation des données transmises.

Ces *URI* ne sont pas encore supportées par tous les navigateurs, Safari, Firefox, Opera et Chrome sont capables des les traiter, Internet Explorer ne les prendra en compte que dans sa version 8 selon le format des données envoyées.

Le CERTA recommande cependant de prêter attention à cette fonctionnalité qui pourrait être de plus en plus utilisée dans les années à venir et recommande une analyse, voir un filtrage des données transmises par l'intermédiaire de ces *URI* afin de limiter les risques de compromission.

Documentation

- RFC 2397, « The "data" URL scheme », août 1998 :
<http://www.ietf.org/rfc/rfc2397.txt>

5.2 OpenSSH : une vulnérabilité pas si triviale à exploiter

Vendredi dernier, le 14 novembre 2008, le CPNI (*Centre for the Protection of National Infrastructure*) a publié un bulletin de sécurité à propos d'OpenSSH. La vulnérabilité permettrait de décrypter n'importe quelle partie de 32 bits d'un bloc chiffré, sous certaines conditions.

Si l'on se penche sur les explications, la vulnérabilité n'est pas si évidente à exploiter dans un contexte opérationnel.

5.2.1 Explication de la vulnérabilité

En cryptographie, on appelle *mode opératoire de chiffrement* la manière dont seront traitées les données à chiffrer. En effet, lorsque l'on doit appliquer certains algorithmes de chiffrement à un gros ensemble de données, ces données sont découpées en blocs et le chiffrement est appliqué à ces blocs suivant un traitement particulier : le mode opératoire.

La vulnérabilité décrite pour OpenSSH est due au choix du mode opératoire de chiffrement CBC (*Chipher Block Chaining* ou *Enchaînement de blocs*) comme mode opératoire par défaut (cf RFC. 4251). Ce mode opératoire est initialisé par un vecteur d'initialisation, et chaque bloc chiffré sert dans le processus de chiffrement du bloc suivant (cf. figure 1).

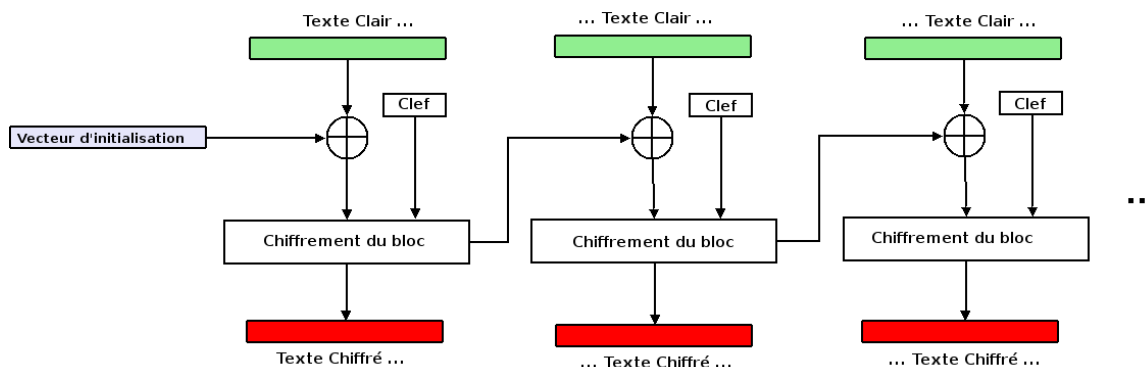


FIG. 1: Mode opératoire CBE

D'après le CPNI, l'utilisation de ce mode opératoire affaiblit le chiffrement des messages échangés via un tunnel SSH. Ainsi, en procédant par injection de fautes, il est a priori possible de décrypter un bloc de 32 bits avec une probabilité de 2^{-18} .

5.2.2 Et d'un point de vue pratique ?

Pour conduire cette attaque, une personne malintentionnée doit tout d'abord être capable d'analyser en temps réel la connexion SSH dans son intégralité, afin d'analyser le résultat des injections d'erreurs.

Elle doit de plus injecter de nombreuses erreurs, ce qui a généralement pour conséquence de couper la connexion.

L'attaque est donc loin d'être triviale et réalisable dans un cas concret.

5.2.3 Comment me protéger ?

La solution la plus évidente consiste à changer le mode opératoire, et d'utiliser le mode CTR (*CounTeR*, c'est à dire basé sur un compteur) au lieu du mode CBC (cf. RFC 4344). De même, le mode de chiffrement *Arcfour* ne semble pas être vulnérable.

Pour utiliser un de ces modes, il convient de n'utiliser que les modes suivants dans les fichiers *sshd_config* and *ssh_config* :

```
Ciphers aes128-ctr , aes256-ctr , arcfour256 , arcfour , aes128-cbc , aes256-cbc
```

5.2.4 Documentation

- Avis de sécurité OpenSSH :
<http://www.openssh.com/txt/cbs.adv>

- Bulletin de sécurité du CPNI :
http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt
- RFC 4251, « The Secure Shell (SSH) Protocol Architecture », janvier 2006 :
<http://www.ietf.org/rfc/rfc4251.txt>
- RFC 4344, « The Secure Shell (SSH) Transport Layer Encryption Modes », janvier 2006 :
<http://www.ietf.org/rfc/rfc4344.txt>

6 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 13 et le 20 novembre 2008.

7 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

8 Rappel des avis émis

Dans la période du 14 au 21 novembre 2008, le CERTA a émis l'alerte et les avis suivants :

- CERTA-2008-ALE-014 : Vulnérabilité dans Opera
- CERTA-2008-AVI-556 : Vulnérabilité dans GnuTLS
- CERTA-2008-AVI-557 : Vulnérabilités de Safari
- CERTA-2008-AVI-558 : Vulnérabilités dans Mozilla Thunderbird
- CERTA-2008-AVI-559 : Multiples vulnérabilités dans Symantec Backup Exec
- CERTA-2008-AVI-560 : Multiples vulnérabilités dans Adobe AIR
- CERTA-2008-AVI-561 : Multiples vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2008-AVI-562 : Vulnérabilités de Libxml2
- CERTA-2008-AVI-563 : Multiples vulnérabilités dans Citrix XenServer

Durant la même période, l'avis suivant a été mis à jour :

- CERTA-2008-AVI-302-002 : Vulnérabilité dans Net-SNMP
(ajout de la référence debian)

9 Actions suggérées

9.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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 réglementaire, 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.

9.2 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 oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

9.3 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.

9.4 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.

9.5 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 CERTA peut vous aider dans ce travail d'analyse.

9.6 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 inexplicables 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.

9.7 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.ssi.gouv.fr/fr/formation/>

10 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.

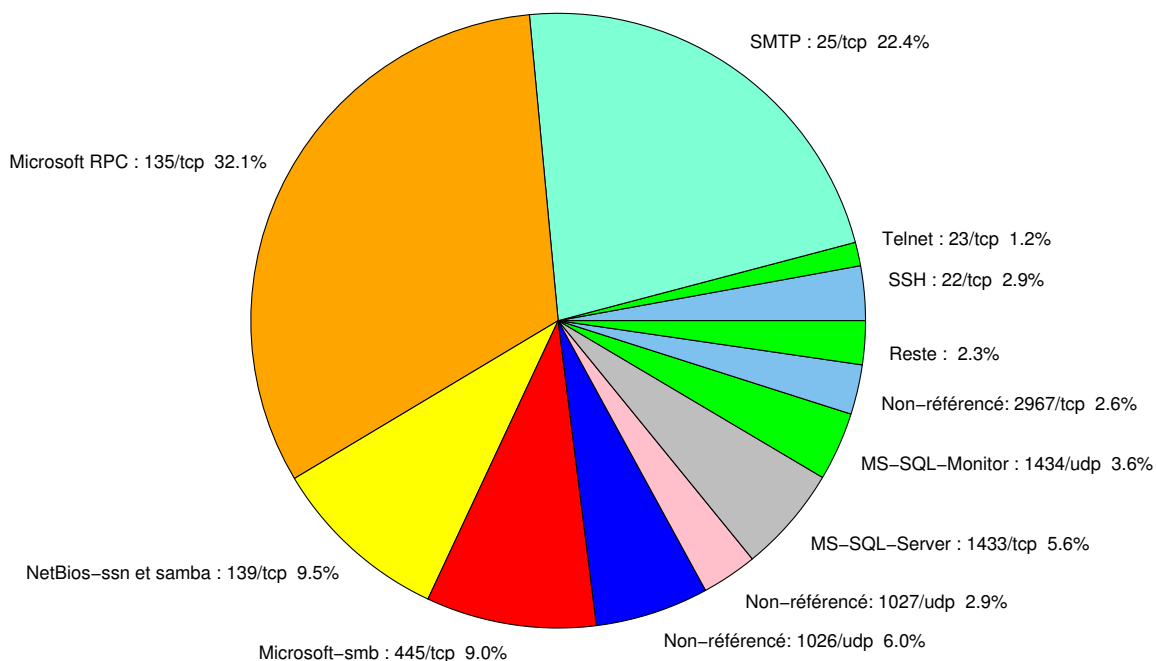


FIG. 2: Répartition relative des ports pour la semaine du 13.11.2008 au 21.11.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

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

port	pourcentage
135/tcp	32.08
25/tcp	22.38
139/tcp	9.45
445/tcp	8.95
1026/udp	5.97
1433/tcp	5.59
1434/udp	3.6
1027/udp	2.92
22/tcp	2.86
2967/tcp	2.61
23/tcp	1.3
4899/tcp	0.93
137/udp	0.62
3128/tcp	0.24
80/tcp	0.18
21/tcp	0.12
3389/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	10
3	Paquets rejetés	11

Gestion détaillée du document

21 novembre 2008 version initiale.