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 avril 2011
N° CERTA-2011-ACT-013

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-13

Gestion du document

Référence	CERTA-2011-ACT-013
Titre	Bulletin d'actualité 2011-13
Date de la première version	01 avril 2011
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-2011-ACT-013.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-2011-ACT-013/

1 Incidents de la semaine

Faux antivirus

Si cette journée, le premier avril, est propice aux plaisanteries, les faux antivirus dépassent le cadre de la blague et sévissent toute l'année.

Cette semaine le CERTA a reçu plusieurs signalements dont le point commun est l'infection de postes de travail par de faux antivirus. La terminologie anglo-saxonne fréquente est *fake* AV ou *rogue* AV.

Les modes de propagation sont divers, mais reposent souvent sur la crédulité de l'internaute :

– sites proposant gratuitement une analyse antivirale du poste ou des antivirus ;
– invitation de réseaux sociaux piégées ;
– courriels alarmistes sur l'état du poste et proposant un lien miracle ou une pièce jointe salvatrice...

Pour mieux tromper la victime potentielle, les noms présentés par ces programmes malveillants se rapprochent de ceux d'outils légitimes. Ainsi un *MS Removal Tool* tente de créer la confusion avec l'outil Microsoft *Malicious Software Removal Tool*.

La première étape du schéma consiste à inhiber les défenses présentes sur le poste (antivirus réel), à simuler une analyse du poste et à prétendre avoir trouvé des infections. En général, le blocage de l'ordinateur accompagne cette information toujours inquiétante.

La deuxième étape consiste à indiquer que la version gratuite ne permet pas l'éradication et à demander des informations bancaires pour permettre le téléchargement d'une version payante, prétendument capable d'éradiquer les virus présents. La captation des informations bancaires est quasi certaine tandis que la remise en état du poste reste très hypothétique.

Le CERTA recommande donc la plus grande méfiance à l'égard :

- des sites qui proposent des analyses antivirales de l'ordinateur ;
- des messages alarmistes sur l'état d'infection du poste, simples canulars (*hoax*) ou bien courriels avec pièce jointe ou lien malveillants ;
- des fenêtres surgissantes indiquant une infection, en particulier si l'icône ou la présentation est différente (même légèrement) de celle du produit antiviral présent sur le poste. Parfois la ressemblance est forte. L'utilisateur pourra être systématiquement méfiant.

Pour l'utilisateur, le plus sage face à une alerte de cette nature est d'en référer sans délai à son support informatique ou à son RSSI. L'incident sera traité selon les procédures en vigueur.

Pour le gestionnaire d'un parc, il est primordial, lorsque la gestion de l'antivirus est centralisée, de regarder quotidiennement les journaux, voire en temps quasi-réel pour détecter les arrêts imprévus de l'antivirus installé sur le poste, signes d'une infection possible, et les alertes réelles, de manière à avertir l'utilisateur par un moyen que ce dernier peut reconnaitre comme fiable, un agent de support de proximité par exemple. L'utilisateur saura mieux être circonspect quand une fenêtre surgissante d'alerte virale apparaît et qu'il n'est pas informé par le canal fiable.

Par ailleurs, le téléchargement d'un produit de sécurité comme un antivirus doit se faire depuis le site de l'éditeur ou depuis un miroir officiel, c'est-à-dire mentionné par l'éditeur, et non depuis un site sans rapport avec l'éditeur, voire avec des noms de domaine aux extensions exotiques (`.cc`, `.vu`...).

2 Attaque via le User-Agent

La lecture des journaux peut parfois révéler des attaques étranges, basées sur des commandes UNIX stockées dans le champ *User-Agent*. Pour l'attaquant, la technique est simple : il lui suffit de modifier son propre *User-Agent* en le remplaçant par des commandes UNIX. Il navigue ensuite sur des sites Web, en limitant son activité au minimum (en général, une seule requête GET suffit). Ces actions sont donc théoriquement enregistrées dans les journaux d'accès du site Web, ce qui revient à réaliser une injection de code indirecte persistante.

Si un administrateur lit ses journaux avec un logiciel vulnérable, sa machine peut exécuter le code stocké dans le champ *User-Agent*.

Quelques mesures peuvent être mises en place pour se préserver de telles attaques :

- mettre à jour les logiciels de lecture des journaux ;
- consulter les journaux depuis des consoles soumises à du filtrage en sortie (pas le droit de se connecter sur l'Internet par exemple) ;
- utiliser un compte non privilégié.

L'enregistrement du *User-Agent* reste pertinent car cette information peut être importante, notamment dans le cadre du traitement d'un incident.

3 Campagne d'hameçonnage contre le Ministère du Travail, de l'Emploi et de la Santé

Cette semaine, il a été signalé au CERTA qu'une campagne d'hameçonnage à l'encontre du site www.sante.gouv.fr était en cours. Le Ministère du Travail, de l'Emploi et de la Santé a d'ailleurs réagit rapidement en publiant sur son site un message d'alerte avertissant les visiteurs de l'existence de site usurpant l'original : `http://www.sante.gouv.fr/carte-vitale-et-hameconnage-ou-phishing.html`.

Sur le site contrefait, de façon très classique, l'aspect général du site légitime a été repris mais on y trouve en plus la présence d'un formulaire invitant les victimes à donner leurs coordonnées bancaires, leur numéro de carte vitale ainsi que leur numéro de carte d'identité.

Le CERTA rappelle donc que d'autres entités que les banques peuvent être la cible de campagnes de *phishing*. En particulier, les sites de télépaiement de l'administration peuvent être usurpés mais également les sites comme celui de la Caisse des Affaires Familiales ou bien encore celui du Ministère de la Santé.

4 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=1937
- 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/

5 Rappel des avis émis

Dans la période du 25 au 31 mars 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-170 : Vulnérabilité dans SPIP
- CERTA-2011-AVI-171 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-172 : Vulnérabilité dans Zend Server
- CERTA-2011-AVI-173 : Vulnérabilité dans IBM Rational
- CERTA-2011-AVI-174 : Vulnérabilité dans Xerox WorkCentre (SMB)
- CERTA-2011-AVI-175 : Vulnérabilité dans Xerox WorkCentre (Web)
- CERTA-2011-AVI-176 : Vulnérabilité dans rsync
- CERTA-2011-AVI-177 : Vulnérabilité dans Pure-FTPd
- CERTA-2011-AVI-178 : Vulnérabilité dans VMWare
- CERTA-2011-AVI-179 : Vulnérabilité dans EMC Data Protection Advisor Collector
- CERTA-2011-AVI-180 : Vulnérabilité dans Cisco Secure ACS
- CERTA-2011-AVI-181 : Vulnérabilité dans Cisco NAC Guest Server

6 Actions suggérées

6.1 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 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

7 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.

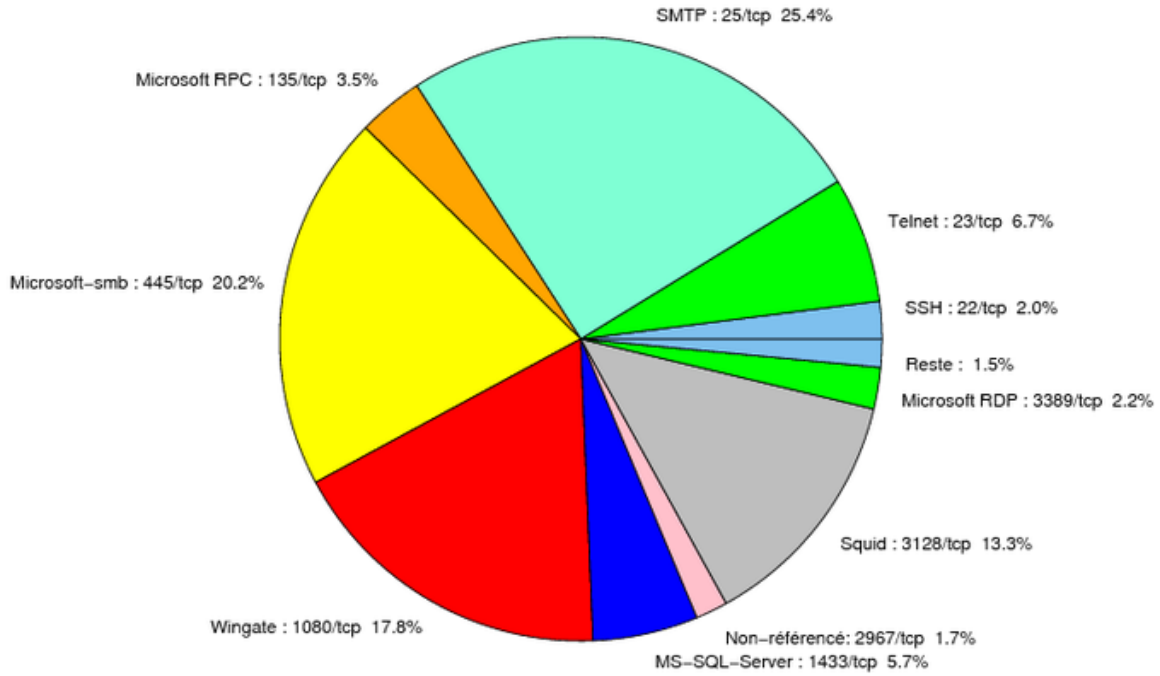

FIG. 1: Répartition relative des ports pour la semaine du 25 au 31 mars 2011

port	pourcentage
25/tcp	25.42
445/tcp	20.27
1080/tcp	17.76
3128/tcp	13.25
23/tcp	6.73
1433/tcp	5.65
135/tcp	3.58
3389/tcp	2.22
80/tcp	2
2967/tcp	1.71
21/tcp	0.85
3306/tcp	0.42
4899/tcp	0.21

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

01 avril 2011 version initiale.