Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2011
N° CERTA-2011-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-23

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-2011-ACT-023`

Gestion du document

Référence	CERTA-2011-ACT-023
Titre	Bulletin d'actualité 2011-23
Date de la première version	10 juin 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-023.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-023/

1 Cycbot : description et contre-mesures

1.1 Description

Des fichiers exécutables codés et embarqués dans des images téléchargées sur l'Internet ont révélé la présence d'un cheval de Troie. Ce programme, dénommé *Cycbot*, envoie des données binaires à un serveur et pourrait recevoir des commandes de celui-ci fournissant ainsi un contrôle total de la machine.

Au moins une trentaine de noms de domaine différents sont contactés par les postes infectés. Un certain nombre de points communs dans les requêtes HTTP envoyées au serveur de contrôle et de commande sont caractéristiques de ce logiciel malveillant. Toutes les URL contiennent le paramètre `tq` dont la valeur est un flux binaire codé en base64. Une partie des requêtes utilisent également le paramètre `vNUM1=NUM2` où `NUM1` et `NUM2` sont des nombres composés de 1 à 3 chiffres décimaux. Certaines requêtes utilisent aussi le *User-Agent* `mozilla/2.0`. Habituellement, cet en-tête HTTP comprend aussi la version du navigateur et du système d'exploitation, par exemple :
`Mozilla/5.0 (X11; Linux x86_64; rv:2.0.1) Gecko/20100101 Firefox/4.0.1`.

L'URI envoyée dans la requête HTTP correspond parfois au chemin d'une image, par exemple `/images/im134.jpg`. Enfin, des requêtes utilisant la méthode HTTP POST comportant aussi le paramètre `tq` sont envoyées vers `zonedg.com/index.html`.

1.2 Mesures de protection envisageables

La détection et l'identification des machines compromises par ce cheval de Troie peuvent être réalisées par une analyse des journaux HTTP de la passerelle Web. Le *User-Agent* `mozilla/2.0` et les requêtes `POST` envoyées vers le domaine `zonedg.com` identifient en effet de manière quasi-certaine des machines infectées par le virus *Cycbot*. La recherche des requêtes HTTP contenant un paramètre dans l'URL nommé `tq`, notamment grâce à l'expression rationnelle `[&?]tq=[%[:alnum:]]+` permettra d'obtenir une liste plus complète des postes compromis. Toutefois, il est possible que cette recherche fasse apparaître quelques requêtes légitimes.

Il est plus hasardeux de considérer la machine comme infectée si elle effectue des requêtes vers une URL correspondant au chemin d'une image. En effet, la recherche de ce type de requêtes fournira de nombreux faux positifs car elles sont très courantes.

De manière générale, les bonnes pratiques suivantes permettent de prévenir l'infection d'une machine ou d'en limiter l'impact :

- contrôler les *User-Agents* au niveau du serveur Web mandataire grâce à une liste blanche adaptée ;
- interdire le téléchargement d'exécutables au niveau des serveurs Web mandataires, sauf exceptions paramétrables, par exemple, sous la forme d'une liste blanche ;
- tenir à jour les logiciels et restreindre les droits des comptes des utilisateurs au strict minimum afin d'éviter toute installation non légitime ;
- éduquer les utilisateurs pour limiter les conduites à risques.

Documentation

- Microsoft Malware Protection Center : Win32/Cycbot.B
  http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FCycbot.B
- Symantec Threats and Risks : Backdoor.Cycbot
  http://www.symantec.com/security_response/writeup.jsp?docid=2010-103008-0555-99

2 Reconnaissance faciale sur *Facebook*

Depuis quelque temps déjà, le réseau social *Facebook* a mis en place une nouvelle fonctionalité : la reconnaissance faciale.

Lors du téléchargement sur le site de photos par un utilisateur, un logiciel de reconnaissance faciale est utilisé. Il compare les photos nouvellement ajoutées aux photos où l'utilisateur est déjà marqué afin de trouver d'éventuelles correspondances entre les visages des personnes présentes. Si des visages connus sont trouvés, alors le site propose automatiquement à l'utilisateur de marquer ces personnes.

Cette fonctionnalité pose des problèmes évidents de contrôle d'image sur l'Internet en favorisant le marquage des photos. D'autant plus qu'elle est activée par défaut. Il est cependant possible de la désactiver dans les options de configuration d'un compte : paramètres de confidentialité -> personnaliser les paramètres -> "Ce que d'autres partagent" -> "Suggérer à mes amis les photos où j'apparais" -> modifier les paramètres -> désactiver. Attention, ce paramètrage n'empêche pas le marquage manuel des photos.

Documentation

- Blog Facebook :
  http://blog.facebook.com/blog.php?post=467145887130

3 Incident de la semaine

Cette semaine, un correspondant du CERTA lui a confié l'analyse d'un serveur au comportement suspect.

Les exploitants analysant les journaux de connexion sur le mandataire (*proxy*) ont constaté des flux IRC anormaux pour ce serveur. L'analyse des journaux et du disque a permis de retracer la chronologie et de trouver la cause decette anomalie.

Des attaquants ont tenté diverses attaques contre le serveur, sur lequel un Apache, phpMyAdmin, Plone, Zope et un serveur pour le protocole de partage de données OPeNDAP s'exécutaient. Certaines attaques étaient des recherches de mots de passe par dictionnaire. Elles ont échoué.

Par contre, une attaque contre un script du serveur OPeNDAP a réussi et a donné aux agresseurs la possibilité d'exécuter des actions avec les droits de l'utilisateur www-data. Cela a suffi à installer un serveur IRC et, bien entendu, à l'utiliser.

Le succès de l'attaque a été permis par l'abscence de mise à jour des logiciels, et dans ce cas précis, de ce serveur OPeNDAP. Les attaquants ont probablement recherché des proies de manière méthodique. Le champ *referrer* dans la requête HTTP du début de l'attaque est une recherche Google sur le nom du script vulnérable.

La morale de l'incident est double ;

- maintenir les logiciels à jour est indispensable ;
- analyser les journaux sortants permet de déceler des intrusions et les entrants d'en comprendre la cause et de réagir en conséquence.

Ceci illustre un des concepts de la défense en profondeur :

- face à l'agresseur, il faut multiplier les obstacles et en varier la nature ;
- et, comme dans le cas présent, associer à chaque obstacle, qui ne doit être perçu que comme un retardateur, un système de détection du franchissement ou de l'imperfection de l'obstacle (ici par l'analyse des journaux) et une procédure de réaction appropriée (par exemple, l'isolement de l'ordinateur).

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 03 mai au 09 juin 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-324 : Multiples vulnérabilités dans Plone
- CERTA-2011-AVI-325 : Vulnérabilités dans Wireshark
- CERTA-2011-AVI-326 : Vulnérabilités dans plusieurs produits Symantec
- CERTA-2011-AVI-327 : Multiples vulnérabilités dans Apache Subversion
- CERTA-2011-AVI-328 : Vulnérabilités dans les postes téléphoniques Cisco Unified Phones 7900 Series
- CERTA-2011-AVI-329 : Vulnérabilités dans Cisco AnyConnect Secure Mobility Client

– CERTA-2011-AVI-330 : Multiples vulnérabilités dans les produits VMWare
– CERTA-2011-AVI-331 : Vulnérabilité dans Asterisk
– CERTA-2011-AVI-332 : Vulnérabilité dans Adobe Flash Player
– CERTA-2011-AVI-333 : Vulnérabilités dans Novell iPrint
– CERTA-2011-AVI-334 : Multiples vulnérabilités dans Google Chrome
– CERTA-2011-AVI-335 : Vulnérabilité dans VLC
– CERTA-2011-AVI-336 : Multiples vulnérabilités dans Oracle Java

Durant la même période, les publications suivantes ont été mises à jour :

– CERTA-2011-AVI-093-002 : Multiples vulnérabilités dans Oracle Java (ajout de la mise à jour de Java pour les systèmes HP-UX)

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.

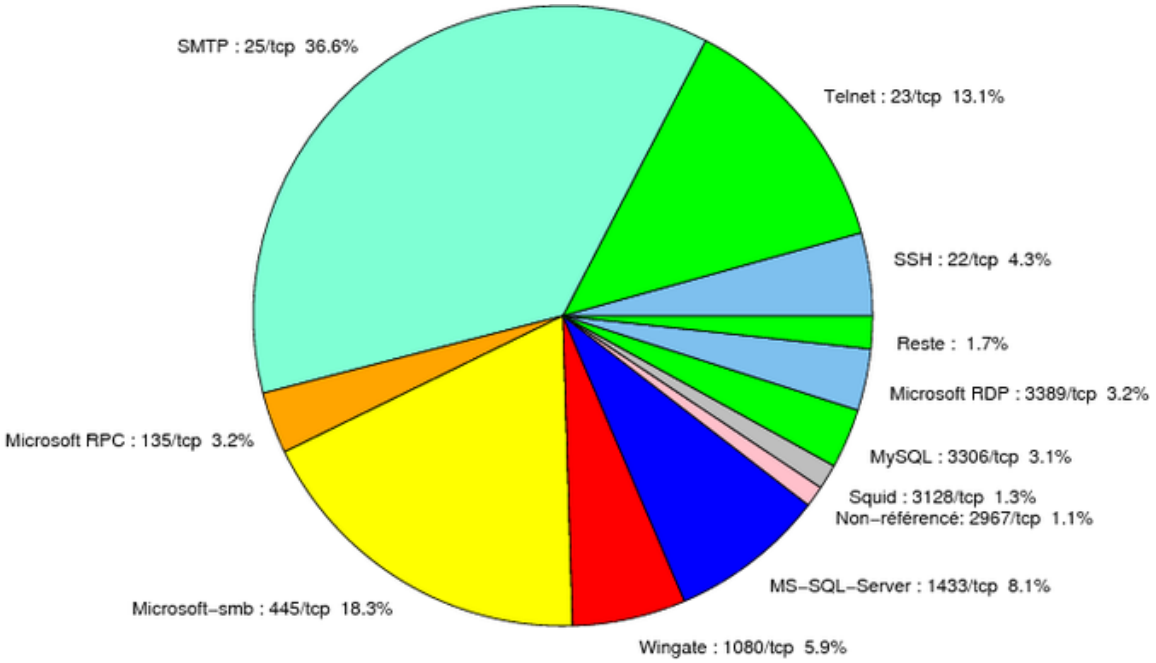

FIG. 1: Répartition relative des ports pour la semaine du 28 mai au 02 juin 2011

port	pourcentage
25/tcp	36.64
445/tcp	18.27
23/tcp	13.25
1433/tcp	8.13
1080/tcp	5.92
80/tcp	4.51
22/tcp	4.31
3389/tcp	3.21
3306/tcp	3.11
3128/tcp	1.3
2967/tcp	1.1
4899/tcp	0.9
21/tcp	0.4
10080/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Paquets rejetés 6

Gestion détaillée du document

10 juin 2011 version initiale.