



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 septembre 2011
N° CERTA-2011-ACT-037

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-37

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-037>

Gestion du document

Référence	CERTA-2011-ACT-037
Titre	Bulletin d'actualité 2011-37
Date de la première version	16 septembre 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-037.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-037/>

1 Mises à jour Microsoft de la semaine

Cette semaine *Microsoft* a émis cinq bulletins de sécurité concernant *Microsoft Windows*, *Microsoft Office* ainsi que des logiciels serveurs *Microsoft*. Les vulnérabilités qui y sont décrites sont jugées comme étant importantes par l'éditeur.

Le CERTA recommande d'appliquer rapidement les correctifs de sécurité associés.

Documentation

- Synthèse des bulletins de sécurité Microsoft de Septembre 2011 :
<http://technet.microsoft.com/fr-fr/security/bulletin/ms11-sep>
- Avis du CERTA concernant la vulnérabilité MS11-070 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-510/index.html>
- Avis du CERTA concernant la vulnérabilité MS11-071 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-511/index.html>
- Avis du CERTA concernant la vulnérabilité MS11-072 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-512/index.html>

- Avis du CERTA concernant la vulnérabilité MS11-073 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-513/index.html>
- Avis du CERTA concernant la vulnérabilité MS11-074 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-514/index.html>

2 Mises à jour Adobe de la semaine

Cette semaine, *Adobe* a émis plusieurs mises à jour de sécurité concernant différents produits, notamment *Adobe Acrobat* et *Adobe Reader*.

Le CERTA recommande d'appliquer ces mises à jour rapidement.

Documentation

- Bulletin de sécurité Adobe pour le mois de septembre 2011 :
<http://www.adobe.com/support/security/bulletins/apsb11-24.html>
- Avis du CERTA concernant le bulletin de sécurité Adobe du 14 septembre 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-508/index.html>

3 Filtrage et tunnels chiffrés

3.1 Introduction

Contrôler efficacement des flux chiffrés à l'aide d'équipements actifs se révèle bien souvent problématique. En effet, par leur nature, ces flux ne peuvent être inspectés. Ainsi, la plupart du temps ils sont soit autorisés par défaut, soit totalement interdits. Bien entendu, de telles configurations posent des problèmes évidents de sécurité dans le premier cas et d'accessibilité dans le second. Il est effectivement difficile aujourd'hui de bannir totalement un protocole comme SSL mais il est cependant nécessaire de s'assurer que le trafic est légitime. Dans la suite de cet article, nous allons nous concentrer sur SSL et son fonctionnement et fournir quelques pistes de réflexion concernant le filtrage de flux chiffrés.

3.2 SSL et la méthode CONNECT

La gestion de SSL au niveau des équipements actifs fait appel à un mécanisme bien particulier décrit dans la RFC 2616, concernant HTTP/1.1. Il est possible de signifier dynamiquement à un équipement que l'on désire utiliser un tunnel chiffré grâce à la méthode HTTP CONNECT. L'équipement concerné va alors passer en mode tunnel : il va agir comme un simple relais et ne plus exercer son rôle de filtrage sur le flux.

L'utilisation de cette méthode rend donc possible le contournement des équipements de types pare-feux et serveurs mandataires.

Notons que la RFC 2817 complète la RFC 2616 et propose notamment des considérations de sécurité sur la méthode CONNECT.

3.3 Exemple de communication SSL

Lorsqu'un client, situé derrière un serveur mandataire (ou *proxy*), souhaite établir un tunnel chiffré vers un serveur distant, il s'adresse à son *proxy* en précisant l'adresse et le port de destination. Ce dernier se charge alors d'établir la connexion avec le serveur distant, si cette dernière est autorisée. Une fois cette connexion établie (réception d'une réponse de type 200), il ne sert plus que de relais entre le client et le serveur distant et n'intervient pas sur les données chiffrées.

Il est aussi possible pour SSL d'utiliser une connexion de type SOCKS. Dans ce cas, le tunnel est pré-établi et le *proxy* n'a pas à effectuer la négociation avec le serveur distant. En terme de filtrage, il n'a alors que deux options, bloquer ou autoriser le flux.

En pratique, la mise en place de filtrage des flux à destination du port SSL (443/TCP) n'est pas courante : les flux sont autorisés par défaut.

3.4 Impact sur la sécurité

Le relatif laxisme envers les flux à destination du port 443/TCP permet notamment de contourner un serveur mandataire ou bien encore d'échapper aux règles des pare-feux. En effet, il est possible, au moyen d'outils spécifiques, de créer un tunnel HTTP vers ce port, grâce à la méthode CONNECT, et d'y faire transiter toutes sortes de flux normalement filtrés (Skype, SSH encapsulé dans du HTTP...). Ces flux, légitimes ou non, ne seront pas bloqués par les équipements de filtrage puisque ces derniers agissent uniquement comme des relais.

De plus, en cas de mauvaise configuration, cela peut également être un point d'entrée dans un réseau : l'attaquant se connecte au relais, et envoie une requête à un serveur interne en utilisant la méthode CONNECT. Ici encore, les équipements de filtrage laisseront passer le flux, pensant qu'il s'agit d'une connexion chiffrée.

L'utilisation de ce type de mécanisme afin de cacher du trafic illégitime a d'ailleurs été observée récemment par le centre de détection de l'ANSSI. Il s'agissait d'une fausse connexion SSL dans laquelle étaient encapsulés des flux de type RTMP, afin de faire passer des données en *streaming* à travers les équipements de contrôle. Ces flux ne sont pas nécessairement malveillants mais peuvent être illégitimes ou bien encore alourdir le trafic.

Le CERTA a également publié une note d'information sur ce type de problématiques le 29 août 2001, actualisée le 21 mars 2011.

3.5 Quelles réponses?

Il est important d'observer la nature réelle des flux transitants afin d'en valider la légitimité. Il est par exemple possible de créer une alerte quand un tunnel chiffré à destination du port 443/TCP transporte autre chose que du HTTPS. Il est également envisageable de contrôler par une liste blanche les destinataires légitimes de flux chiffrés. D'autres solutions sont proposées dans la note d'information rédigée par le CERTA.

Des solutions techniques d'inspection directe des flux chiffrés existent mais peuvent entrer en conflit avec le secret de la correspondance et/ou nécessiter une déclaration spécifique à la CNIL.

Documentation

- RFC 2616 :
www.ietf.org/rfc/rfc2616.txt
- RFC 2817 :
www.ietf.org/rfc/rfc2817.txt
- Article de Wikipedia concernant les tunnels HTTP :
http://en.wikipedia.org/wiki/HTTP_tunnel
- Note d'information CERTA-2001-INF-003, *Tunnels et pare-feux* :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/index.html>

4 Typosquatting et vol de courriels

Deux chercheurs ont mené une étude sur une technique de « typosquatting » nommée le « doppleganger domain ».

Le « typosquatting » de nom de domaine consiste à acheter des noms de domaine dont la graphie ou la phonétique est proche de celle du site d'une marque ou d'une entreprise connue.

Les « doppleganger domain » sont des noms approchant du domaine légitime, mais qui diffèrent légèrement par l'absence de séparation entre le sous-domaine et le domaine principal, par exemple : seibm.com à l'instar de se.ibm.com.

Les chercheurs ont enregistré 30 « doppleganger domain », visant des entreprises du Fortune 500, et ont récupéré tous les courriels envoyés par erreur à ces adresses. Sur une période de 6 mois, 120 000 courriels représentant un volume de 20 giga-octets de données ont été collectés. Sachant que d'après l'étude publiée, sur les 500 sociétés, 151 sont vulnérables à une telle attaque, soit près de 30%.

Les courriels récupérés grâce à cette technique contenaient des informations sensibles qui pourraient être utilisées de façon malveillante. On peut citer entre autres : les noms de connexions et mots de passe des employés, des informations sur les configurations et les architectures des intranets des entreprises, des accès VPN mais aussi des informations personnelles.

Toutes ces informations peuvent être obtenues de manière passive en mettant en place un « doppleganger domain » et un serveur de courriel. Cependant, l'attaquant peut aussi répondre aux courriels afin d'obtenir plus d'informations.

De plus, durant cette étude, les chercheurs se sont aperçus qu'un certain nombre de grandes entreprises américaines sont victimes de cette pratique.

Afin de se prémunir au mieux de ce type d'attaque il convient :

- d'utiliser un logiciel de chiffrement afin de protéger les échanges d'informations sensibles ;
- d'avoir une veille sur les possibles noms de domaines pouvant être « typosquattés » susceptibles d'avoir un impact ;
- de lancer des procédures de recouvrement de noms de domaines « typosquattés » par des tiers, au moyen d'une procédure UDRP.

Documentation

- Article sur le site wired :
<http://www.wired.com/threatlevel/2011/09/doppelganger-domains/>
- Rapport des deux chercheurs :
http://www.wired.com/images_blogs/threatlevel/2011/09/Doppelganger.Domains.pdf
- Procédure UDRP :
<http://www.icann.org/en/udrp/>

5 Diffusion d'un faux client BitTorrent malveillant

Cette semaine, le site <http://www.bittorrent.com> a averti ses utilisateurs d'un incident de sécurité survenu sur l'un de ses serveurs hébergeant le client pour réseau pair à pair, uTorrent. En effet, le 13 septembre 2011 entre 11h20 et 13h10 GMT, le site <http://www.uTorrent.com> a diffusé un code malveillant en lieu et place du client légitime suite à une compromission du serveur. Le code malveillant affichait une fausse alerte antivirale demandant le paiement d'une certaine somme afin de se débarrasser du logiciel indésirable.

Le site <http://www.bittorrent.com> a publié une procédure de désinfection sur l'Internet (cf. section documentation). Le CERTA recommande à toute personne ayant téléchargé le client uTorrent pendant la plage horaire indiquée précédemment à suivre les instructions afin de supprimer au plus vite ce code malveillant.

Documentation

- Incident de sécurité sur le site <http://www.uTorrent.com> :
<http://blog.bittorrent.com/2011/09/13/security-incident/>

6 Rappel des avis émis

Dans la période du 09 au 15 septembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-501 : Vulnérabilités dans IBM Open Administration Tool
- CERTA-2011-AVI-502 : Vulnérabilité dans libsvg
- CERTA-2011-AVI-503 : Multiples vulnérabilités dans Wireshark
- CERTA-2011-AVI-504 : Vulnérabilités dans Spring Framework
- CERTA-2011-AVI-505 : Vulnérabilité dans Cyrus IMAPd
- CERTA-2011-AVI-506 : Vulnérabilités dans MantisBT
- CERTA-2011-AVI-507 : Vulnérabilités dans FFmpeg
- CERTA-2011-AVI-508 : Multiples vulnérabilités dans Adobe Reader et Adobe Acrobat
- CERTA-2011-AVI-509 : Vulnérabilité dans EMC Avamar
- CERTA-2011-AVI-510 : Vulnérabilité dans Microsoft WINS
- CERTA-2011-AVI-511 : Vulnérabilité dans des composants Windows
- CERTA-2011-AVI-512 : Vulnérabilités dans Microsoft Excel
- CERTA-2011-AVI-513 : Vulnérabilités dans Microsoft Office
- CERTA-2011-AVI-514 : Vulnérabilités dans Microsoft SharePoint
- CERTA-2011-AVI-515 : Vulnérabilités dans IBM WebSphere
- CERTA-2011-AVI-516 : Vulnérabilité dans Apache

- CERTA-2011-AVI-517 : Vulnérabilité dans Novell Cloud Manager
- CERTA-2011-AVI-518 : Vulnérabilité dans Cisco Unified Service Monitor et Cisco Unified Operations Manager
- CERTA-2011-AVI-519 : Multiples vulnérabilités dans Django
- CERTA-2011-AVI-520 : Vulnérabilités dans CiscoWorks LAN Management Solution

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

- CERTA-2011-AVI-490-001 : Vulnérabilité dans Apache httpd (ajout des références aux bulletins Cisco, Hitachi, HP, Mandriva, Novell (Suse), RedHat et Ubuntu)
- CERTA-2011-AVI-493-001 : Certificats SSL frauduleux (ajout de la référence au bulletin de sécurité Apple)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

8 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.

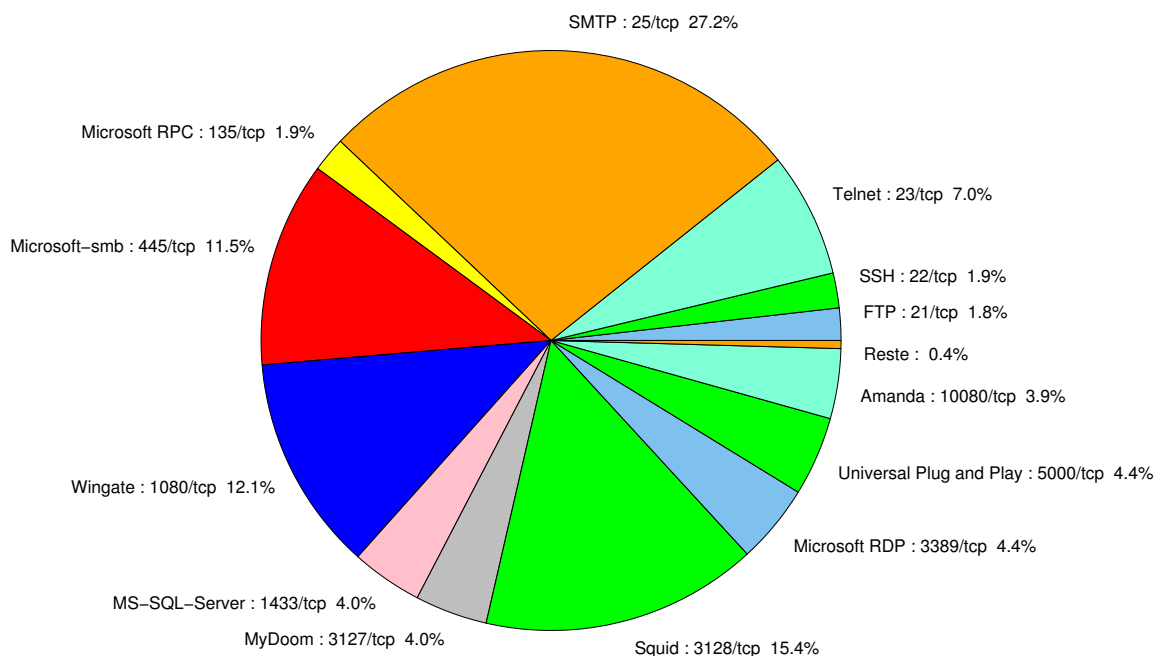


FIG. 1: Répartition relative des ports pour la semaine du 09 au 15 septembre 2011

port	pourcentage
25/tcp	27.24
3128/tcp	15.41
1080/tcp	12.05
445/tcp	11.45
80/tcp	7.78
23/tcp	7.03
5000/tcp	4.41
3127/tcp	4.04
1433/tcp	3.96
10080/tcp	3.89
135/tcp	1.94
21/tcp	1.79
4899/tcp	0.22

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	7

Gestion détaillée du document

16 septembre 2011 version initiale.