

Affaire suivie par :
CERTA

RECOMMANDATION DU CERTA

Objet : Usage de la messagerie instantanée ou de l'IRC

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-2002-REC-001>

Gestion du document

Référence	CERTA-2002-REC-001
Titre	Usage de la messagerie instantanée ou de l'IRC
Date de la première version	28 mars 2002
Date de la dernière version	-
Source(s)	Note d'incident du CERT/CC IN-2002-03 Avis de sécurité du CERTA CERTA-2002-AVI-012
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Divulgence d'informations ;
- exécution de code arbitraire ;
- participation à des attaques en déni de service distribuées (DDoS).

2 Résumé

Les logiciels de messagerie instantanée et de discussion en ligne (IRC, *Chat* ou « causerie ») sont de plus en plus répandus. Ces logiciels comportent certains risques qu'il faut connaître :

- ils exposent l'utilisateur à une divulgation rapide de son identité ou éventuellement d'autres informations le concernant ou concernant son système ;
- l'utilisateur peut être tenté de télécharger toute sorte d'outils contenant des chevaux de Troie et permettant à un utilisateur mal intentionné d'exploiter les machines de ses victimes ;
- ces logiciels, souvent installés par défaut sur les systèmes Windows ou avec un navigateur web, présentent un certain nombre de vulnérabilités connues.

Il faut donc rester aussi vigilant pour les logiciels de messagerie instantanée et pour l'IRC que pour le mél.

3 Introduction

Le m el est un moyen simple et rapide de communication, avec tous les risques qu'il comporte (fichiers attach es, courrier compos e en HTML et renfermant des scripts ou autres contenus actifs, liens cach es, etc.). Il existe d'autres outils de communication plus simples et plus ludiques :

- la messagerie instantan ee : ICQ (*I Seek You*), AIM (*AOL Instant Messenger*), MSN Messenger (*the MicroSoft Network Messenger*), Yahoo Messenger, etc.
- l'IRC (*Internet Relay Chat*) aussi appel e *chat*.

3.0.1 Qu'est-ce que la messagerie instantan ee ?

La messagerie instantan ee est un moyen de communiquer en priv e avec d'autres personnes de son choix. Le client se connecte   un serveur qui contient les informations sur tous les utilisateurs inscrits, connect es ou non. Chaque personne poss ede un pseudonyme qui n'est pas forc ement unique, et un identifiant unique dans la base de donn ees du serveur. Cet identifiant peut  tre un num ero, une adresse m el, etc. Si l'on d esire parler   une personne, on la recherche dans cette base. On peut cr eer une liste d'interlocuteurs pr ef er es. Deux personnes peuvent communiquer en direct si elles sont simultan ement connect ees au serveur. Sinon, elles peuvent consulter leurs messages dans leur bo te aux lettres au moment o  elles se connectent.

3.0.2 Qu'est-ce que l'IRC ?

L'IRC est un moyen de communiquer en direct avec des groupes de personnes via l'Internet. Les clients se connectent   des serveurs qui sont eux-m emes reli es entre eux, formant un r eseau IRC. Tous les clients sont donc susceptibles de communiquer entre eux en temps r eel   travers le r eseau.

4 Les dangers

4.1 Divulgarion d'informations « sensibles »

Sur IRC ou par messagerie instantan ee, certains de vos interlocuteurs chercheront   obtenir des informations sur vous, votre employeur ou sur le syst eme que vous utilisez :

- il faut savoir que sur IRC et sur la plupart des logiciels de messagerie instantan ee, votre adresse IP est visible de fa on imm ediate ;
- vos messages transitent par des serveurs bien d efinis :
 - certains syst emes de messagerie instantan ee sont des logiciels propri etaires se connectant   des serveurs administr es par des soci etes de droit priv e souvent situ es   l' tranger ;
 - Sur IRC, les op erateurs IRC et les administrateurs des serveurs ont la possibilit e de suivre les conversations tenues sur un canal ou suivre les connexions d'une adresse IP donn ee. De plus, l'administrateur de serveur IRC peut avoir une visibilit e compl ete de tous les  changes r ealis es au travers de son serveur.
- Comme par t el ephone, vous prenez part   une discussion, vous n' crivez pas une lettre que vous pourrez relire. Une phrase envoy ee est lue instantan ement par vos correspondants. Il n'est plus possible de la corriger ...
Faites attention   ce que vous dites. Parler en direct fait parfois dire beaucoup (trop) de choses ...
- Sur les logiciels de messagerie instantan ee, il est possible de remplir un formulaire d'informations vous concernant. Ce que vous mettrez dans ce formulaire sera visible par n'importe quelle personne utilisant le m eme logiciel. Dans certains cas, ces informations sont aussi visibles sur un site web d edi e   ce logiciel. Sur IRC, il est possible de donner des informations suppl ementaires dans les param etres de votre client (nom d'utilisateur, nom r eel, etc.). Ne laissez pas ces param etres tels qu'ils sont d efinis par d efaut, il peuvent  tre r ev elateurs pour un curieux. Ne mettez pas de vraies informations si celles-ci sont sensibles.

4.2 Les sites web incitant à installer un outil

Comme indiqué dans l'alerte CERTA-2001-ALE-011 concernant la propagation d'un cheval de Troie au moyen d'un site web proposant de télécharger un faux anti-virus, méfiez-vous de la publicité reçue par mél, sur votre messagerie instantanée ou en arrivant dans un canal IRC, vous incitant à télécharger tel ou tel programme.

- N'installez que des logiciels téléchargés depuis le site web de leur éditeur (les autres pouvant contenir des portes dérobées par exemple) et préférez les CD-ROM originaux.
- Ne faites pas confiance aux pièces jointes d'un mél même s'il a l'air de provenir d'un éditeur de logiciel ou de personnes connues.
- Mettez à jour votre anti-virus et contrôlez avec celui-ci les fichiers téléchargés.
- Sous Linux il est possible d'aller vérifier les signatures MD5 sur le site web de la distribution concernée (commande `md5sum` dont le résultat est à comparer avec celui indiqué sur le site de l'éditeur).

Évitez d'installer des *scripts* IRC, ils peuvent contenir un cheval de Troie, changer les paramètres de votre client, voire y ajouter des composantes contrôlables à distance.

4.3 Téléchargement de fichiers

Avec les logiciels de messagerie instantanée, il est possible d'envoyer des fichiers en point à point. Vous pouvez envoyer une image, un document, ou un fichier exécutable à vos correspondants ; vous devenez alors serveur pendant le temps de cet envoi.

De même, deux clients IRC peuvent s'échanger d'autres éléments que des messages. Ils peuvent aussi échanger des fichiers. Pour cela il faut établir une connexion DCC (*Direct Client to Client*). Le récepteur doit accepter la requête (en faisant *DCC Get*), mais souvent les interfaces des clients IRC masquent cette étape. Encore une fois, certains clients sont paramétrés par défaut de façon à accepter automatiquement tout transfert de fichier par DCC.

Enfin, il est possible d'ajouter des scripts permettant aux clients IRC d'effectuer des tâches plus ou moins automatisées. Ces scripts sont un moyen de propagation supplémentaire pour les vers et les virus (cf. CERTA-2001-ALERTE-001 et CERTA-2001-ALE-009).

Comme pour le mél, prenez les précautions de base :

- n'exécutez pas ce qui provient d'un inconnu et vérifiez que vos interlocuteurs connus ne vous ont pas envoyé un fichier à leur insu. Vérifiez systématiquement le fichier avec un antivirus que vous avez mis à jour ;
- sachez qu'un éditeur d'antivirus ou de logiciel ne vous enverra jamais de correctif ou de mise à jour par le biais de la messagerie instantanée, de l'IRC ou du mél ;
- il est possible que votre logiciel soit paramétré par défaut pour accepter ces fichiers, assurez-vous que vous avez bien modifié ces configurations avant de vous connecter ;
- n'installez pas de scripts si vous n'en connaissez pas toutes les fonctionnalités (maîtriser le langage utilisé, et lire les sources). Surveillez les modifications des fichiers de scripts dans le répertoire courant du logiciel IRC ;
- ne suivez pas tous les liens hypertexte que vous lisez quelque soit leur moyen de diffusion.

4.4 Vulnérabilités des clients

Le logiciel en lui-même peut être vulnérable, et permettre l'exécution de code arbitraire par le biais d'un débordement de mémoire (cf. CERTA-2002-AVI-012).

Inversement, un logiciel de messagerie instantanée peut appeler d'autres composants Windows, tels que le navigateur web par défaut ou les éléments de Netmeeting par exemple. Il peut aussi exister des vulnérabilités dans ces composants (cf. CERTA-2000-AVI-063).

Ainsi il faut maintenir à jour des correctifs de tous les logiciels quels qu'ils soient. Un élément du système ou un module externe d'un logiciel doit être mis à jour s'il possède une vulnérabilité connue. Supprimez les outils non utilisés.

5 Documentation

- Les bulletins de sécurité du CERTA :
 - Débordement de mémoire dans ICQ : CERTA-2002-AVI-012

- Antivirus2001 est un cheval de Troie : CERTA-2001-ALE-011
 - Alerte de virus LOVE-LETTER-FOR-YOU (ILOVEYOU) : CERTA-2000-ALERTE-001
 - Retour d'expérience du ver ILOVEYOU : CERTA-2000-REC-001
 - Propagation du ver LifeStages : CERTA-2001-ALE-009
- Les bulletins de sécurité et notes d'incidents du CERT/CC sur le sujet :
- Attaques par ingénierie sociale via l'IRC et messagerie instantanée :
http://www.cert.org/incident_notes/IN-2002-03.html
 - Propagation du ver I Love You :
<http://www.cert.org/advisories/CA-2000-04.html>
 - Propagation du ver Goner.scr :
http://www.cert.org/incident_notes/IN-2001-15.html
 - Vulnérabilité du client ICQ :
<http://www.cert.org/advisories/CA-2002-02.html>

Gestion détaillée du document

28 mars 2002 version initiale.