Mise en garde sur l'installation de logiciel piraté

Document envoyé le 23 mai 2013 par le RSSI adjoint du CNRS à tous les CSSI d'Unité :

Installation de logiciel pirate Il a été détecté par un CERT européen qu'une des machines d'une unité du CNRS hébergeait le cheval de Troie Zeus. Ce code malfaisant est très élaboré et permet de récupérer toutes sortes d'informations sur une machine dont les différents identifiants et mots de passe utilisés pour se connecter sur les sites bancaires en particulier.

Dans le cas présent, l'origine de l'infection a pu être identifiée. Il s'agit de chargement d'une version piratée (crack) d'un logiciel payant pour ne pas avoir à payer la licence.

Il est rappelé que ceci est totalement contraire à la charte du CNRS

```
[L'utilisateur] doit suivre les règles en vigueur au sein de l'entité
pour toute installation de logiciel et ne pas télécharger ou
utiliser de logiciels ou progiciels sur le matériel de l'entité sans
autorisation explicite. Notamment, il ne doit pas installer de
logiciels à caractère ludique, ni contourner les restrictions
d'utilisation d'un logiciel. Les logiciels doivent être utilisés
dans les conditions des licences souscrites. (3.2 Règles d'utilisation)
```

```
L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser,
modifier ou utiliser les logiciels, bases de données, pages web,
images, photographies ou autres créations protégées par le droit
d'auteur ou un droit privatif, sans avoir obtenu préalablement
l'autorisation des titulaires de ces droits. (5. Respect de la
propriété intellectuelle)
```

```
L'utilisateur s'engage à ne pas apporter volontairement
des perturbations au bon fonctionnement des ressources informatiques
et des réseaux que ce soit par des manipulations anormales du
matériel, ou par l'introduction de logiciels parasites connus
sous le nom générique de virus, chevaux de Troie, bombes logiques...
(6. Préservation de l'intégrité des ressources informatiques)
```

De même dans les Règles élémentaires de sécurité sur le poste de travail il est précisé :

```
Il est prudent d'éviter de télécharger des logiciels dont l'innocuité
n'est pas garantie (pérennité du logiciel, nature de l'éditeur,
mode de téléchargement, etc.).
```

Dans la PSSI du CNRS il est précisé :

```
Protection juridique : la mise en oeuvre des systèmes d'information
s'inscrit dans un cadre législatif et réglementaire destiné en particulier
à protéger les droits de propriété intellectuelle et industrielle et ceux
de la vie privée (fichiers nominatifs, cybersurveillance…).
Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie
et des administrateurs systèmes et réseaux peut être recherchée.
```

Voici pour information le message qui a été envoyé par la direction de l'unité concernée :

```
Bonjour,

Un virus a récemment été découvert sur un des ordinateurs de l'unité.
L'origine de l'infection est établie. Un logiciel scientifique "cracké"
(licence piratée) a été installé volontairement sur un ordinateur de l'unité
par un collègue qui souhaitait disposer des mêmes outils sur son PC fixe
professionnel que sur son portable personnel. A cause de ce logiciel
infecté,
le pirate a pu ajouter à distance toutes sortes d'outils facilitant
ses attaques depuis l'étranger.

Ce virus a pu dérober des identifiants et mots de passe.
La détection rapide du virus par les structures spécialisées
au niveau national (CERT RENATER, CERTA) nous a permis d'agir immédiatement,
limitant ainsi la propagation du virus et l'exfiltration d'autres
types de données professionnelles ou personnelles.

Si le coût des licences pour nos logiciels métiers est important voire
prohibitif,
il est inadmissible de tolérer ces agissements sur des ordinateurs
professionnels.
Il en va de la responsabilité juridique de chacun et de la sécurité des
informations
que nous partageons ou protégeons au quotidien.

Pour rappel, lorsqu'un nouveau logiciel doit être installé,
il doit être validé par un correspondant informatique ou par les équipes
de proximité et d'assistance de nos tutelles. Si besoin, l'ensemble des
personnels peut solliciter leur aide pour déterminer si un logiciel
est fiable ou non.

A noter également : un antivirus à jour ne détecte pas tous les virus
et ne doit pas dispenser l'utilisateur d'être vigilant voire méfiant.
Plus généralement, un programme d'origine non fiable ou inconnue
est réputé dangereux et ne doit jamais être exécuté !

Bien cordialement
```

From:
https://docinfo.ias.u-psud.fr/ - **Informations, recommandations et conseils du service informatique de l'IAS**

Permanent link:
https://docinfo.ias.u-psud.fr/doku.php/ssi:logiciels_pirates?rev=1395050267

Last update: **2014/03/17 10:57**