

# République Tunisienne

Ministère des Technologies de la Communication



الوكالة الوطنية للأمناء للمعلوماتية  
Agence Nationale de la Sécurité Informatique



## RECAPITULATIF

Public Cible	Date de Publication	Date de Révision	Version
Simple Utilisateur	Mai 2008	Mai 2009	02

## Qu'est ce qu'un virus?

Un virus est un petit programme nocif qui s'insère automatiquement dans le corps d'un autre programme légitime. Lorsqu'on exécute notre programme légitime, le virus se chargera en même temps en mémoire et exécutera les instructions que son auteur a programmées. La définition simple d'un virus pourrait être la suivante : "tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire."

## Qu'est ce qu'un ver?

Un ver est un programme parasite. Il n'est pas forcément autopropageable. Son but est de grignoter des ressources système : CPU, mémoire, espace disque, bande passante... La définition d'un ver s'arrête à la manière dont il se propage de machine en machine, mais le véritable but de tels programmes peut aller au delà du simple fait de se reproduire : espionner, offrir un point d'accès caché (porte dérobée), détruire des données, faire des dégâts, envoi de multiples requêtes vers un site Internet dans le but de le saturer, etc. Il se propage, comme toutes données binaires, par disquettes, CD ROM, réseaux (LAN ou WAN).

Pour détruire des données sur une machine infectée, les vers peuvent parfois utiliser les virus, et ce afin de remplir des fonctions de porte dérobée ou de cheval de Troie.

### Comment s'en protéger (virus + ver) ?

- Utilisation d'un firewall pour filtrer ce qui vient d'extranet.
- Utilisation d'au moins un antivirus, remis à jour très régulièrement et exécuté régulièrement.

## Qu'est-ce qu'un antivirus ?

Un antivirus est un logiciel qui protège un ordinateur contre les virus, et de plus en plus contre d'autres malwares : «trojans», scripts malicieux dans les pages web, etc. Il est souvent composé de différents modules.

## Qu'est-ce qu'un firewall ?

Un pare-feu est un système permettant de protéger un ordinateur des intrusions provenant du réseau. Il permet de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante. Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et les "réseaux extérieurs".

### **Quelques Firewalls PC gratuits pour usage Domestique (non professionnels) :**

- Comodo <http://www.comodo.com/products/free-products.php>
- Sunbelt Personal Firewall [www.sunbeltsoftware.com/](http://www.sunbeltsoftware.com/)
- ZoneAlarm : [www.zonealarm.com/](http://www.zonealarm.com/)

## Qu'est ce qu'un Hoax?

Un hoax (en français canular) est un e-mail propageant une fausse information, poussant le destinataire à réaliser (de lui-même) des actions nocives pour l'intégrité ou la sécurité de son ordinateur et à faire suivre cette information à toutes ses connaissances, ou à une adresse de courrier électronique bien précise, sans vérifier la véracité des propos qui y sont contenus.

Voici ci-dessous quelques bonnes adresses pour ne plus se laisser piéger, en s'informant sur tous les hoax en circulation:

<http://www.hoaxbuster.com>

<http://www.inoculer.com/hoax.php3>

<http://www.secuser.com/hoax>

<http://www.f-secure.com/news/hoax.htm>

## Qu'est-ce qu'un cheval de Troie ?

Un "Cheval de Troie" (plus brièvement baptisé " Troyen Horse" et en anglais trojan horse) est un programme malicieux, permettant à un attaquant d'effectuer à distance et à votre total insu, tous types d'opérations malicieuses sur votre PC.

## Qu'est ce qu'un spyware (et leurs engins d'infection : les outils dits "adware") ?

Les spywares (ou espiogiciels en français) sont des logiciels parasites indétectables. Ils n'ont pas une action destructive (comme les virus), mais servent à espionner vos habitudes et vos "besoins", pour des buts "commerciaux malsains".

### Outils Anti –spyware :

Le moyen le plus efficace, consiste à utiliser plusieurs outils anti-spyware combinés : Il existe deux excellents outils gratuits pour usage domestique, qui reconnaissent et peuvent supprimer la plupart des spywares (ET qui ne contiennent pas eux-même de spywares", du moins pour les versions actuelles préconisées) :

- Ad-Aware, Pour le télécharger : <http://abcdelasecurite.free.fr>

- Spybot : Search and Destroy ( Spybot SD), qui permet de supprimer les fichiers contenant des informations d'utilisation comme les fichier .log (enregistrant des informations de configuration), les traces de surf, d' historique et d'autres fonctions toutes aussi utiles.

- Pour le télécharger : <http://www.spybot.info/en/mirrors/index.html>

Pour une protection totale et efficace, Il est conseillé d'utiliser ensemble ces deux programmes complémentaires.

## Qu'est-ce qu'un spamming (dit communément "Spam") ?

Le spamming consiste à envoyer massivement des e-mails de type généralement publicitaire (dit aussi "junk mail"), à un grand nombre de personnes n'ayant pas sollicité ce type d'envoi publicitaires, engorgeant ainsi les serveurs de messagerie et vos boites à lettres de messages publicitaires inutiles, non sollicités et généralement mensongers.

## Qu'est-ce qu'un rootkit ?

Un rootkit est un code malicieux permettant à un attaquant de maintenir en temps réel un accès frauduleux à un système informatique, se greffant dans le noyau du système d'exploitation. A la différence d'un virus ou d'un ver, un rootkit ne se réplique pas.

Un rootkit agit sur une machine déjà compromise. Il est utilisé dans une étape après intrusion et l'installation d'une porte dérobée pour cacher tous les changements effectués lors de l'intrusion afin de préserver l'accès à la machine. Ces portes dérobées utilisables à distance permettent au pirate de s'introduire à nouveau au cœur de la machine sans essayer d'exploiter une nouvelle fois la faille initiale utilisée pour obtenir l'accès, qui serait tôt ou tard corrigée.

### Quelques Outils Anti-RootKit

- RootkitRevealer (windows)
- RootKit Unhooker (windows)
- chkrootkit (Linux, BSD)
- Rootkit Hunter (Linux,BSD)

## Qu'est-ce qu'un keylogger ?

Un KeyLogger est un enregistreur de touches et par extension un enregistreur d'activités informatiques permettant d'enregistrer les touches utilisées par un utilisateur sur son clavier et tous les événements déclenchés. Il se présente généralement sous forme logicielle et travaille en arrière plan, en toute discrétion. Selon l'utilisation, le procédé peut s'avérer illégal (espionnage, etc.) ou utile (parents très inquiets de leurs enfants, etc.).

Même s'il existe une multitude de KeyLoggers différents, leur mode opératoire est identique. Ils sont installés directement par le pirate sur la machine visée, si l'ordinateur

n'a pas de connexion Internet permettant une installation à distance via un cheval de Troie.

### **Quelques Outils Anti-KeyLoggers**

- Logiciels
- Anti-keylogger
- SpyCop
- Matériels

Une mémoire peut stocker jusqu'à 256 Ko de données. Cette petite prise est indétectable par logiciel, elle est transparente du système d'exploitation pour l'enregistrement.

La seule manière de repérer les KeyLoggers matériels est de se familiariser avec ces dispositifs et de faire une vérification visuelle complète de la machine de façon régulière.

### **Qu'est-ce qu'un cookie ?**

Un «cookie», est un petit fichier de type texte (.txt), aussi appelé témoin, qui est créé dans votre disque dur destiné à mémoriser les coordonnées des pages Web que vous avez ouvertes, de façon à les ouvrir plus rapidement lorsque vous retournez dessus. Ce cookie est temporaire et est effacé chaque fois que vous videz votre cache. Un cookie contient en général des informations comme l'identifiant et/ou le mot de passe d'un utilisateur, ses configurations préférées. Pour les sites commerciaux, il peut contenir des informations sur des éléments relatifs au "panier d'achat" de l'internaute (ce que vous avez acheté sur les pages).

### **Qu'est-ce qu'un IDS ?**

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

## Qu'est-ce qu'un IPS ?

L'IPS (Intrusion Prevention System) est un Système de Prévention/Protection contre les intrusions et non plus seulement de reconnaissance et de signalisation des intrusions comme la plupart des IDS le sont. La principale différence entre un IDS (réseau) et un IPS (réseau) tient principalement en 2 caractéristiques :

→ Le positionnement en coupure sur le réseau de l'IPS et non plus seulement en écoute sur le réseau pour l'IDS (traditionnellement positionné comme un sniffer sur le réseau).

→ La possibilité de bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce, ce qui induit que l'IPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocages (drop connection, drop offending packets, block intruder, Etc.).

## Qu'est-ce qu'un Proxy ?

Un serveur proxy (serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et internet.

La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP.

Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, Etc.).