Dossier d'étude:
les malware, première source d'insécurité

BTS SIO

Devenir Informaticien à Gap
c'est possible !

Sommaire

1. Les malwares. _____ p.2

2. Les protections. _____ p.3

2.1. Le fonctionnement des antivirus. _____ p.3

2.2. Le marché des antivirus. _____ p.4

2.3. Les autres protections. _____ p.5

1. Les malwares.

Un malware, ou logiciel malveillant, est un terme générique utilisé pour désigner une variété de logiciels hostiles ou intrusifs : virus informatiques, vers, cheval de Troie, etc. Il peut prendre la forme de code exécutable, de scripts, de contenu actif et d'autres logiciels. Les malwares sont définis par leur intention malveillante, agissant contre les exigences de l'utilisateur et de l'ordinateur.

Différents types de malwares :

- **Le virus** : Il a la particularité de s'auto-reproduire en infectant d'autres programmes ou machines. Il peut nuire d'une manière parfois radicale au bon fonctionnement d'un ordinateur ou d'un réseau.

  Les virus agissent en plusieurs temps:

  Tout d'abord, il se charge d'infecter tous les fichiers exécutables de l'ordinateur sur lequel il est, puis de se propager à travers le réseau.
  Très souvent, le virus possède un code hostile qui se déclenche suivant un événement donné.

- **Le Cheval de Troie** : Ce malware crée une porte d'entrée dans votre ordinateur afin de faire profiter à un tiers des ressources de votre ordinateur.

- **Le spyware** : Les logiciels espions ou « espiogiciels » collectent toute l'activité de l'utilisateur sur son ordinateur, ces informations sont collectées à son insu ou sans son consentement.

- **L'adware** : L'adware est un spyware qui consiste à espionner les données de navigation et modifier la page d'accueil du navigateur afin de rediriger l'utilisateur vers des annonces.

- **Le ransomware** : Ce malware est un cheval de troie qui chiffre toutes les données de l'ordinateur et réclame une rançon en échange de la clé de chiffrement.

- **Le ver informatique** : Il se reproduit sur plusieurs ordinateurs grâce à un réseau. Dès qu'il est en exécution, il se duplique très rapidement. Sa spécificité est de pouvoir se répandre sans jamais s'attacher à un autre programme exécutable.

- **Le keylogger** : Un keylogger est à l'origine un élément matériel placé entre le clavier et la machine permettant d'enregistrer tout ce qui est tapé au clavier (mot de passe, login, etc ...).
  Il existe une version logiciel sous forme de cheval de troie susceptible d'enregistrer les moindre actions de la machine.

- **Rootkit** : C' est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès administrateur à un ordinateur le plus furtivement possible. Il est souvent indétectable par l'utilisateur ou les anti-virus.

2. Les protections.

2.1. Le fonctionnement des antivirus.

Les **antivirus** sont des logiciels conçus pour **identifier**, **neutraliser** et **éliminer** des logiciels malveillants.

Identifier:
Un logiciel antivirus vérifie tous les fichiers , les courriers électroniques, mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.).
Pour cela il peut utiliser différentes méthodes :

- Ils se concentrent sur des fichiers et comparent alors la signature virale du virus aux codes à vérifier, ceci peut se faire de 2 manières.

  Par dictionnaires :
  Des informations sur les malwares étant préalablement identifiées et enregistrées, le logiciel antivirus peut ainsi détecter et localiser la présence d'un virus. On appelle ce dictionnaire la base de définition virale qui contient les signatures de virus.
  Il est donc nécessaire de mettre à jour l'antivirus afin de se protéger des malwares récents.

  Par liste blanche:
  Au lieu de rechercher les logiciels connus comme malveillants, on empêche l'exécution de tout logiciel à l'exception de ceux qui sont considérés comme fiables par l'administrateur système. Mais cette méthode est très restrictive.

- La méthode heuristique est la méthode la plus puissante, tendant à découvrir un code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Cette méthode permet d'identifier des virus très récents qui ne seraient pas encore connus dans le dictionnaire de l'antivirus.

Une fois le malware identifié, l'antivirus peut le **neutraliser** en le mettant en quarantaine pour éviter qu'il se propage et/ou l'**éliminer** en supprimant les fichiers malveillants et en tentant de réparer les fichiers infectés.

2.2. Le marché des antivirus.

Liste d'antivirus:

Logiciel	GNU/Linux	Windows	MacOS	Licence
ClamAV	Oui	Avec ClamWin	Avec ClamXav	GNU GPL
Avira AntiVir	Oui	Oui	Oui	Propriétaire, Version Pro Payante
Avast	Oui	Oui	Oui	Propriétaire, Version Pro Payante
AVG AntiVirus	Oui	Oui	Oui	Propriétaire, Version Pro Payante
Bitdefender	Oui	Oui	Oui	Propriétaire, Payant
McAfee VirusScan	Oui	Oui	Oui	Propriétaire, Payant
Kaspersky	Oui	Oui	Oui	Propriétaire, Payant

2.3. Les autres protections.

Les antivirus pourraient ne pas suffire à se protéger entièrement, pour combler cela il est important d'adopter de bons comportements face aux éventuelles menaces.

Un pare-feu : Un pare-feu actif et bien configuré, peut être un rempart contre les conséquence d'un malware, en empêchant celui-ci de communiquer des informations.

Les Mises à jour : En mettant régulièrement à jour les logiciels, le système d'exploitation, on prévient des risques de menaces dues aux failles de sécurité. Et évite ainsi une exploitation du système par des malwares.

Sources fiables : Télécharger et installer seulement des éléments provenant de sources fiables. Que ce soit un logiciel ou une pièce jointe à un mail, mais également de clés usb, disques durs, liens, etc...

Pour se prémunir des conséquences des malwares, il est nécessaire d'effectuer régulièrement des sauvegardes de ses données sur plusieurs supports différents (disques externes, serveur de stockage, cloud ...).