MarcoServices initiation & dépannage informatique (pc) à domicile

Voici les menaces les plus connues :

Afin de savoir ce qui peut menacer vos données, il serait utile de savoir quels programmes malveillants (**Malware**) existent et comment ils fonctionnent. Tous les **Malwares** peuvent être subdivisés en types suivants :

Virus : les programmes qui infectent d'autres programmes en leur ajoutant un code de virus afin d'accéder au démarrage du fichier infecté. Cette définition simple découvre l'action principale d'un virus - l'infection. La vitesse de propagation du virus est inférieur à celle des vers.

Vers : ce type de Malware utilise les ressources du réseau pour se propager. Cette classe a été appelée **vers** en raison de sa particularité de «glissement» d'un ordinateur à l'autre via le réseau, mail et autres canaux d'information. Grâce à cela, sa vitesse de propagation est très élevée.

Les **vers** pénètrent l'ordinateur, calculent les adresses réseau des autres ordinateurs et envoient ses copies à ces adresses. Outre les adresses de réseau, les données de carnets d'adresses des messageries sont également utilisées. Les représentants de ce type de **Malware** créent parfois des fichiers fonctionnels sur les disques système, mais ils ne peuvent pas déployer des ressources informatiques (sauf la mémoire vive).

Trojans : les programmes qui exécutent sur les ordinateurs infectés les actions non-autorisées par l'utilisateur. Par exemple, selon des conditions, supprimer des données sur les disques, provoquer un échec du système, voler des informations personnelles, etc. Ce type de **Malware** n'est pas un virus dans le traditionnel sens de terme (il ne s'agit pas d'infection d'autres programmes ou de données) : les chevaux de Troie ne peuvent pas pénétrer un ordinateur par eux-mêmes et ils sont répartis par les personnes malveillants comme les logiciels «utiles» et nécessaires. L'endommagement causé par un cheval de Troie est supérieur à l'attaque de virus traditionnelle.

Spywares : des logiciels qui permettent de recueillir des informations sur un utilisateur ou une entreprise, sans qu'ils le sachent. Vous ne pouvez même pas deviner d'avoir un logiciel espion sur votre ordinateur. En général, le but de spywares est de :

• espionner l'activité des utilisateurs sur les ordinateurs ;
• collecter les informations sur le contenu du disque dur ; souvent cela signifie une analyse des dossiers et de la base de registre afin de créer la liste des applications installées ;
• collecter les informations sur la qualité de la connexion, moyen de la connexion, vitesse de modem, etc.

La collecte d'informations n'est pas la fonction principale de ces programmes, ils menacent également la sécurité. Minimum deux programmes connus -

Gator et **eZula** - permettent à la personne malveillante de non seulement recueillir des informations mais aussi de contrôler l'ordinateur. Un autre exemple de logiciels espions sont des programmes qui s'intègrent dans le navigateur de l'ordinateur et re-transfèrent le trafic. Vous avez certainement rencontré de tels programmes lorsque vous avez demandé une adresse d'un site web, un autre site web a été ouvert. L'un des logiciels espions est le **mailing-phishing**.

Phishing : une expédition du courrier dont l'objectif est d'obtenir des informations financières confidentielles de l'utilisateur. Le phishing est une forme de l'ingénierie sociale caractérisée par des tentatives d'acquérir frauduleusement des informations sensibles, telles que mots de passe et numéros de cartes bancaires, en se faisant passer par une personne de confiance ou d'affaires dans une communication électronique, soit disant officiel, comme un e mail ou un message instantané. Les messages contiennent un lien vers un site frauduleux où l'utilisateur est suggéré de saisir le numéro de sa carte bancaire et autres informations confidentielles.

Adwares : un code intégré dans un logiciel sans que l'utilisateur en soit conscient dont le but est d'afficher la publicité. En général, les adwares sont intégrés dans les logiciels distribués gratuitement. La publicité s'affiche dans l'interface du logiciel. Souvent, les **adwares** collectent les renseignements personnels de l'utilisateur et les transfèrent à leur distributeur.

Riskwares : ce logiciel n'est pas un virus, mais il contient une menace potentielle. A certaines conditions, la présence de tels riskwares sur votre ordinateur met vos données à risque. Parmi les logiciels de risque on peut nommer les services de l'administration à distance, les programmes payants qui utilisent Dial Up connexion pour la connexion à des sites Internet.

Jokes : un logiciel qui ne nuit pas à votre ordinateur, mais qui affiche des messages qu'un endommagement a déjà été causé ou va être causé sur certaines conditions. Souvent, ce logiciel met l'utilisateur en garde sur un danger qui n'existe pas, par exemple, il affiche des messages sur un formatage du disque (tandis qu'aucun formatage ne se passe réellement), il détecte les virus dans les fichiers qui en réalité ne sont pas infectés etc.

Rootkits : ce sont des outils utilisés pour dissimuler une activité malveillante. Ils cachent la présence d'un malware afin d'éviter sa détection par un logiciel antivirus. Les rootkits peuvent également modifier le système d'exploitation de l'ordinateur et remplacer ses principales fonctions afin de dissimuler sa présence et les actions effectués par la personne malveillante sur l'ordinateur infecté.

Autres malwares : de différents programmes qui ont été développés pour créer d'autres logiciels malveillants, pour organiser des attaques DoS sur les serveurs à distance, pour l'effraction d'autres ordinateurs etc. Parmi ce type de menace on peut nommer les outils d'hacker (Hack Tools), les utilitaires pour la création de virus etc.

Spam : un courriel indésirable anonyme. Par exemple, les message de la propagande politique, les mails qui demandent d'aider quelqu'un. Une autre catégorie de spam sont des messages suggérant de verser une grande somme d'argent ou les invitations aux pyramides financières, les mails qui volent les mots de passe et les numéro de cartes bancaires, les messages suggérant le transfert à vos amis (messages de bonheur) etc. Le spam augmente la charge sur les serveurs de messagerie et augmente le risque de la perte des informations importantes pour l'utilisateur.

C'est pourquoi, qu'il est conseillé de faire des contrôles de votre ordinateur au moins une fois par mois.

Je me déplace à votre domicile pour faire l'entretien de l'ordinateur à votre domicile ou en enlevant votre ordinateur. **Contactez-moi**