



Communiqué de presse – libre à la publication immédiate

Discussion sur les logiciels malveillants dans le monde de la sécurité informatique : Existe t-il vraiment un sens de nettoyer des ordinateurs infectés ?

Emsi Software, proposeur de logiciels de sécurité comme a-squared Malware 4.0, reprend une actuelle discussion du monde de la sécurité informatique (IT-information technique) : Il y a-t-il vraiment un sens de nettoyer des ordinateurs infectés ? Est-ce que l'utilisateur peut encore faire confiance à ce système ? Premièrement pour pouvoir répondre à cette question, il faut tout d'abord éclaircir, si un nettoyage complet est techniquement possible.

À la plus petite perturbation de l'ordinateur, les utilisateurs pensent déjà à l'action d'un virus. L'imprimante ne fonctionne pas ? Certainement un virus ! La connexion Internet semble très lente ? Certes, un logiciel espion qui expédie maintenant les données personnelles de l'utilisateur dans un pays qui n'est pas à trouver sur l'Atlas européen !

La plupart des utilisateurs n'ont que très peu de connaissances sur la façon, dont un programme est **structuré**, de quelle manière ce logiciel fonctionne et les dommages qu'il peut faire sur l'ordinateur. Vous installez simplement un programme de protection et lui déléguez toutes les responsabilités à cet outil. La scène de sécurité informatique n'est pas du tout satisfaite avec ce genre de protection, et actuellement se montre très provocante : faut-il vraiment prendre la peine de nettoyer un ordinateur contaminé ?

En bonne traduction, cela ne signifie en aucun cas que, les logiciels malveillants sont aussi inoffensifs, que les utilisateurs d'ordinateur doivent la négliger en toute tranquillité. Au lieu de cela, la question reste dans le vague, s'il est effectivement possible pour les programmes de protection modernes, de nettoyer complètement un système déjà atteint, ou s'il n'était pas mieux de réinstaller complètement le système. Pour pouvoir en décider, il faudrait s'en s'occuper un peu plus et traiter cette matière plus en profondeur.

Connaissances de base : Quel est l'impact des virus, des chevaux de Troie et des outils de logiciels espions ?

Pour fonctionner correctement, un virus a besoin d'une application qui lui servira d'hôte. Un virus s'accroche à un programme "légitime" en insérant son propre code dans un fichier exécutable déjà existant. C'est seulement après que si le programme légitime est chargé, le virus peut devenir actif et infecter d'autres programmes.

Nettement plus importants, dans l'afflux quotidien des logiciels malveillants sur le disque dur, sont désormais **les chevaux de Troie**, les **portes dérobées** et pour terminer les **bots** et les **vers**. Les **chevaux de Troie** et **bots** sont des programmes autonomes, qui se nichent dans les profondeurs du système et ici n'éveillez surtout aucun soupçon. Ils sont là, tout d'abord pour ouvrir un port du PC pour que désormais le pirate informatique puisse prendre le plein contrôle du PC, pour le trafic d'envoi en masse de pourriels. Chevaux de Troie et les bots ne sont dangereux que lorsqu'ils ont été chargés dans la mémoire. Ils utilisent donc des fonctions de démarrage automatique, pour s'assurer qu'à chaque processus de démarrage ils soient de nouveau appelés.

Logiciels espions, Adware, faux logiciels de sécurité :



Communiqué de presse – libre à la publication immédiate

Les programmes-espions écoutent et notent en secret par exemple la connexion bancaire et les données d'accès de l'utilisateur, pour ensuite la communiquer alors discrètement à la mafia en ligne. Ces programmes d'espionnage sont de plus en plus sophistiqués dans leur programmation. Ainsi, de temps en temps ils démarrent plusieurs processus actifs, qui se surveillent mutuellement. Si un des processus est terminé, alors il peut tout de suite se relancer avec un autre processus. De faux programmes de sécurité vous font croire qu'ils vont à la chasse de routines malveillantes, mais eux-mêmes font partie de cette catégorie : quelques-uns d'entre eux s'injectent essentiellement dans les processus importants du système par exemple dans le fichier Winlogon.exe. En essayant de vouloir supprimer les programmes nuisibles, l'ordinateur se plante.

Les **Rootkits** sont les plus dangereux. Ces programmes nuisibles manipulent tellement le système d'exploitation qu'ils deviennent invisibles pour le système lui-même - ils ne seront plus affichés dans les fichiers ou dans le gestionnaire des tâches. Ainsi, les logiciels Antivirus ne peuvent plus dépister ces Rootkits. Ils arrivent même à créer des clés de registre, d'ouvrir des ports et de rendre des processus en cours invisibles.

Désinfection : Parfois nettoyage avec certains problèmes à la clé

Les programmes nuisibles une fois parvenus sur votre propre ordinateur, et qu'ils sont activés, il reste encore la question de savoir s'ils se laisseront également supprimer et ce entièrement et sans résidus indésirables.

Magnifique : En cas de simples logiciels malveillants, il est possible avec une sécurité relativement élevée d'éliminer complètement du système le logiciel nuisible. Pour les virus, c'est le plus facile, pour supprimer les fichiers infectés. De plus, il se peut que les programmes infectés à la fin ne puissent plus fonctionner. Pas de problème : ils se laissent facilement installer de nouveau. Avec les chevaux de Troie, il suffit de terminer les processus actifs, de se débarrasser des entrées de démarrage automatique et d'éliminer les fichiers exécutables du cheval de Troie pour le supprimer. Les programmes-espions classiques peuvent être désinstallés très facilement. De ce point de vue, il est également possible pour vous, après une découverte, de pouvoir rapidement remettre le système à son état d'origine.

En d'autres cas, cela est autrement avec les programmes-espions modernes ou les faux logiciels antivirus. Ceux-ci se terrent si profondément dans le système, que des outils spéciaux sont nécessaires, pour pouvoir supprimer ces fichiers avant le processus de démarrage. Ces infections sont très difficiles à cerner de manière définitive. Il en est de même pour les rootkits, qui possèdent les caractéristiques du camouflage presque parfait. Outre le fait que l'utilisateur ne peut dire exactement s'il peut vraiment dépister tous les rootkits sur son ordinateur : peut-il également vraiment être certain que le rootkit a été supprimé ? Les pirates informatiques trouvent toujours de nouvelles voies pour camoufler leurs logiciels malveillants.

Assez souvent, il est également possible qu'un logiciel malveillant malgré qu'il ait été supprimé fournisse par ces modifications apportées au système, mais subsiste malgré tout. Ainsi, il se peut que des ports aient été ouverts, qu'un pirate ait tout de même par son attaque de l'extérieur et puis se serait saisi du contrôle du système.

Une fois le PC infecté - Nouvelle installation !



Communiqué de presse – libre à la publication immédiate

Emsi Software en Autriche offre des logiciels de sécurité pour les ordinateurs fonctionnant avec Windows. Le gérant Monsieur Christian Mairoll nous confie : " D'après notre expérience récente, les rootkits et les faux logiciels antivirus ne se laissent pas supprimer des ordinateurs infectés avec les dernières protections de sécurité. Nous conseillons donc à nos clients dès la première installation du système d'exploitation sur l'ordinateur de faire une image de sauvegarde avec toutes les applications importantes de l'ensemble de toutes vos partitions. Cela peut alors en cas de sinistre être rejoué sur un disque dur fraîchement formaté."

Il est important, bien sûr, que, malgré toutes les inquiétudes d'un program de protection présent sur l'ordinateur, qu'il peut immédiatement afficher le malware, dès qu'il est détecté sur son propre ordinateur. Le logiciel Mamutu 1.7 d'Emsi-Software veille à la surveillance remarquable des actions comportementales sur votre propre PC et peut également détecter lui-même des logiciels nuisibles, même s'ils ne sont pas encore connus dans la scène des protections contre les logiciels malveillants.

Pour les utilisateurs privés, il existe **a-squared Free 4.0** complètement gratuit (en ce moment seulement en phase bêta). Cet outil numérise les ordinateurs et tout détecte déjà les infections, pour ensuite les éliminer immédiatement.

Le programme **a-squared Malware 4.0** fait partie de la classe royale. Il utilise deux scanneurs actifs en permanence en arrière-plan, afin de dépister toutes sortes de logiciels malveillants, avant qu'ils ne puissent se nicher dans les profondeurs du système. Une double protection en temps réel est composée d'une part par des analyses des signatures et d'autre part sur la surveillance comportementale des programmes (Malware-IDS). Plusieurs mises à jour journalières veillent à ce que cette arme reste tranchante. Un abonnement d'un an du logiciel coûte 29,95 euros.

Site Web : <http://www.emsisoft.fr/>

Téléchargements : <http://www.emsisoft.fr/fr/software/download/>

Sens et non-sens du nettoyage de logiciels malveillants (Base de connaissances) :
<http://www.emsisoft.fr/fr/kb/articles/tec081111/>

À PROPOS D'EMSI SOFTWARE

Emsi Software est une société privée ayant son siège en Autriche. Le bilan de l'entreprise croît positivement et rapidement depuis sa création en 2003, et sans capital emprunté. L'objectif d'Emsi Software est d'être l'un des principaux fournisseurs européens dans la technologie de l'analyse comportementale, pour étudier les logiciels, notamment les logiciels malveillants.

L'entreprise a été fondée en 2003 par Christian Mairoll, qui avec sa vision d'une société virtuelle et l'a mise en pratique : Les 15 collaborateurs de la société sont disséminés dans le monde entier, mais travaillent ensemble sur l'Internet, comme s'ils étaient assis côte à côte dans un bureau réel. Pour les visions techniques, Georg Wicherski s'en occupe, Georg, en tant que co-fondateur du "Nepenthes" du projet HoneyPot, ainsi que de la mwcollect Alliance (fusion de réseaux d'HoneyPot pour la capture automatique de logiciels nuisibles de l'Internet) il jouit d'une grande réputation dans le secteur de la sécurité.



Communiqué de presse – libre à la publication immédiate

Dans la gamme, des produits, d'Emsi Software, appartiennent les programmes de sécurité comme a-squared Anti-Malware, a-squared Free, a-squared HiJackFree, a-squared Anti-Dialer et depuis la fin de 2007 notre nouveau programme, Mamutu "Behavior Blocker".

Contact pour la presse

Thomas Günther
PR-Manager
Mail: tg@emsisoft.com
Fon: +43 664 344 60 68
Fax: +43 6235 200 53