Note de sécurité Avril 2021

LES VIRUS INFORMATIQUES

Sôter Conseil
Ingénierie de sécurité globale

Industrie | Formation | Events | Conseil

Sôter Conseil – SAS au capital de 6000€ - 3 cours Charlemagne – 69 217 LYON Cedex 2597
contact@soter-conseil.fr – www.soter-conseil.fr

Les virus informatiques – Définition et solutions

De quoi s'agit-il ?

Un virus informatique, c'est un petit programme qui, en s'exécutant, provoque des dégâts sur l'ordinateur qui l'héberge. Il a été ainsi nommé par analogie avec les virus biologiques. L'analogie peut se poursuivre assez loin, puisque le virus peut se reproduire et se transmettre d'un ordinateur à l'autre. Ces « virus » prennent de très nombreuses formes et sont souvent très élaborés. Ils peuvent activer des CryptoLockers, des chevaux de Troie, ou même de petits serveurs qui permettront de voler des informations. Ils prennent parfois la forme de fausses mises à jour, peuvent se cacher dans des logiciels téléchargés sur le web et se propagent par tous les vecteurs imaginables (clés USB, téléphones portables, mails, sites web et même objets connectés).

Quels sont les enjeux ?

Ces virus sont évidemment destinés à nuire, parfois pour le simple « plaisir » de leur auteur, mais le plus souvent ils servent des objectifs mercantiles. Les informations personnelles volées sont revendues à des groupes de criminels qui les exploitent pour toute sorte d'extorsions, des rançons peuvent être demandées pour « libérer » les données chiffrées par les CryptoLockers (ou ransomware) et parfois même, ces virus permettent d'organiser des opérations d'espionnage économique.

Tout ceci participe d'un marché criminel qui génère tous les ans des milliards de dollars. On peut même trouver des « cyber mercenaires », qui vendent leurs compétences informatiques et fabriquent sur commande des virus « sur mesure », notamment afin de déjouer la surveillance des logiciels antivirus. L'exemple ci-dessous est une copie d'écran extraite du dark web qui montre une telle offre de services.

Comment s'en prémunir ?

Comme souvent, les solutions sont simples et font appel au bon sens et à beaucoup de vigilance : ne jamais télécharger un fichier d'origine non certifiée (œuvres ou logiciels piratés), éviter les sites web « sulfureux », ne pas accepter de clés USB d'un inconnu et non vérifiées, se protéger avec un antivirus à jour, sont des bonnes pratiques qui réduiront la probabilité d'une infection. On voit que l'analogie avec le biologique peut là aussi être reprise. […]

Sôter Conseil – SAS au capital de 6000€ - 3 cours Charlemagne – 69 217 LYON Cedex 2597
contact@soter-conseil.fr – www.soter-conseil.fr