Forum: Aide - Recherche de logiciels

Topic: pour ne plus avoir de pb avoir mon PC

Subject: Re: pour ne plus avoir de pb avec mon PC.

Publié par: skorpix38

Contribution le : 27/01/2008 06:57:35

Citation :

noucha a écrit:
Bonjour à tous, hier j'ai fais un scan avec Avast et il a détecté un Cheval de Troie que heureusement qu'il a été supprimé avec succès. Je vous demande si toutefois vous savez biensur, de quoi peut-il s'agir?
Nom du Fichier: C:SystemVolumeInformation-restore{8AE7BAOD-584F-4E2F-9B}
Nom du logiciel malveillant : win32:Agent-QLC[Tri]
Type de logiciel malveillant : Cheval de Troie
Version VPS : 080123-2, 23/01/2008
Si quelqu'un sait ce que çà veut dire, je le remercie par avance. A+. Noucha.
Noucha,

Pour faire un peu le tri dans tout ça, et garder l'esprit clair :
- si Avast t'a détecté une "infection virale", il n'y a pas lieu d'accuser cet AV d'être une passoire, ce n'est pas logique, puisqu'il a vu l'intrus ! (comme l'écrivent Malekal et qq autres, Avast est qqfois moins rapide à réagir aux "nouveautés" virales. Mais ceci est surtout préjudiciable aux cow-boys solitaires qui cliquent plus vite que leur ombre)
- ton "malveillant" semble se trouver dans la partie Restauration : est-il réellement suprrimé ? Sinon, attention à la ré-infection lors d' éventuels "Restore" que tu pourrais être amenée à faire...
- Win32.Agent.QLC est une des nombreuses incarnations d'une longue série de Win32.Agent.Qxx, généralement des infections de type Troyen, mais il y aurait aussi des RootKits (des bestioles plus furtives...)
- La description sur le lien de Malekal est excellente dans le sens général, mais pas à jour. Il y a eu des douzaines de variantes depuis 6 mois... Toujours bien regarder la date des documents !
- Tu dois absolument réfréner ton instinct de téléchargement : avant tout "download", deux questions primordiales, en ai-je besoin, et ça vient d'où ? (cf Malekal...) D'ailleurs, même des *add-ons* "propres" peuvent embêter ton système, voire le planter...
- pour ne plus avoir de pb (sujet de ce post...), il serait sage d'éviter MSN et MS OutlookExpress, deux vecteurs d'Infection expresse. Et bannir le *peer-to-peer*, que je préfère écrire, de nos jours, **pire-to-pire**...
- les noms de code pour désigner les infections varient d'un fournisseur d'AV à l'autre, ça ne facilite pas nos recherches.
- cette variante"QLC" est apparemment toute "jeune" : une interro rapide de Google ne fournit que qq misérables réponses, dont une en turc et une en japonais, langues que je capte pas...
- comme tous les AV basés sur des signatures, Avast peut aussi se tromper, et pointer du doigt un fichier innocent dont une séquence de l'"empreinte génétique" ressemble à celle d'un virus réel. Ce n'est pas si rare !
- ce que tu as recopié en tant que Nom du Fichier n'est apparemment que le chemin ("path") pointant vers le fichier incriminé par Avast...

Impossible d'en dire plus : ne suis malheureusement pas voyant extra-lucide.
Mais je m'efforce de rester lucide !

@+ et bon courage

Edit - PS: Merci à Léa d'apporter sa contribution sous un angle "féminin". Malgré leur bonne volonté, les "mecs" ont un langage masculin...