De l'expérience – La détection des virus

Auteurs : ***Olga Tcaci, Olga Severin, Daniela Istrati***

Qu'est-ce qu'un virus informatique ?

D'après le chercheur Fred Cohen un virus informatique c'est un programme qui peut contaminer un autre programme en le modifiant pour inclure une copie de lui-même. Tous ces virus se reproduisent d'eux-mêmes.

Nous, on a dépisté qu'un virus informatique partage bien des traits communs avec son homologue biologique. Comme lui, il ne peut survivre lui-même : il doit s'associer intimement avec un objet du système afin d'en faire son vecteur, et le détourner pour assurer sa reproduction, donc sa survie. Sur un ordinateur Windows, ces « objets » infectables sont divers et ils déterminent la famille à laquelle appartient un virus donné.

Quelques définitions

Les médias utilisent le mot « virus » pour nommer tous les programmes parasites, mais en fait, il existe des sous classes.

- Virus
- Ver ou *worm*
- Cheval de Troie ou *Trojan (horse)*
- Microvirus ou macro

Quels sont les risques ?

Si les virus sont parfois destructeurs, ils peuvent aussi servir à espionner de l'intérieur un ordinateur. En gros, ils peuvent tout faire, selon le désir de son créateur, du plus bénin au plus grave :

- Afficher simplement un message narquois ;
- Surcharger jusqu'à l'engorgement le disque dur ;
- Affecter la mémoire et ralentir l'ordinateur ;
- Supprimer certains types de fichiers, graphiques par exemple ;

Effacer des fichiers plus fondamentaux comme les fichiers du système d'exploitation, empêchant alors la machine de redémarrer ;

Ralentir le Web, c'est le cas des vers que l'on appelle « masse mailer » ou @mm.

Carrément reformater le disque dur, ce qui occasionnera la perte de toutes les données (les sauvegardes ont du bon).

Certains *Trojan*, appelés *Backdoor*, peuvent aussi donner le contrôle de l'ordinateur à un tiers, ce qui lui permet de lire tous les fichiers, confidentiels ou non (comme les codes secrets ou numéros de comptes bancaires) ;

De faire exécuter à l'ordinateur toutes les tâches que l'utilisateur lui-même pourrait faire.

Pourquoi crée-t-on les virus ?

Les virus sont souvent écrits par de jeunes adolescents boutonneux en mal d'aventures (appelé Script Kiddy's) ; cela relève du jeu et du défi.

D'autres personnes créent des virus dans le but de démontrer leur savoir faire ou pour expérimenter, juste pour savoir si c'est possible d'en créer un (éducatif). Certains en font pour mettre en évidence les failles de sécurité de certains logiciels, surtout Windows et Outlook.

Il y a aussi des virus plus sérieux, préparés par des groupes de pirates informatiques : ceux-ci attaquent plutôt les grandes organisations et compagnies (C.I.A., Microsoft, gouvernement américain, N.A.S.A., O.T.A.N…)

Quelques réflexes de base à acquérir

Que faire devant toutes les menaces des virus? Idéalement, se munir d'un bon Antivirus et le mettre à jour régulièrement : la majeure partie des éditeurs offre en principe des mises à jour (gratuites) plusieurs fois par semaine ! Il est préférable d'utiliser un Antivirus connu, car ces compagnies d'Antivirus font un sérieux effort pour mettre à notre disponibilité les dernières définitions de virus. En passant, les « définitions de virus » sont des données sur les caractéristiques ou *signatures* de tous les virus connus. Donc, avec les mises à jour régulières, on sera protégés de nouveaux virus.

Mais avant de parler d'antivirus, il y a des réflexes de bon sens à acquérir, car on est la première ligne de défense :

- Toujours se méfier d'un nom de fichier attaché ou d'un objet de courriel trop attractif. Rien que ça devrait mettre la puce à l'oreille.
- Ne jamais ouvrir un fichier joint dont le nom se termine par .EXE, .COM, .BAT, .VBS, .PIF, .OVL ou .SCR, sauf à être complètement sûr de son contenu (en principe, personne n'a de raison d'envoyer ce genre de fichiers, outre : direction corbeille, sans lire).
- Sauvegarder régulièrement ses fichiers importants, car même avec la plus extrême vigilance, le pire peut arriver.
- Installer un antivirus (la plus récente version).
- Analyser tout ce que vous recevez : il s'agit d'un des points fondamentaux de la prévention. Vérifier tous les programmes ou fichiers avant de les exécuter ou de les ouvrir. Détecter les éventuels virus avant qu'ils n'aient le temps d'infecter aucun de vos fichiers.
- Mettre à jour vos définitions de virus.

Comment fonctionne un Antivirus ?

Il y a deux fonctions essentielles dans un antivirus. Premièrement la fonction de balayage (communément appelée « *scan »)*, permettant sur demande à l'utilisateur, de vérifier son disque dur ou fichier à la recherche d'un virus qui pourrait déjà y être présent. Idéalement, ce « *scan »* doit être effectué une fois par semaine.

Et puis une action *résidente* ou permanente, c'est-à-dire qui fonctionne dès le lancement de l'ordinateur jusqu'à son extinction. Cette fonction opère en *arrière plan*, ou en *tâche de fond*, c'est-à-dire de façon transparente. Sans rentrer dans les détails, elle surveille toute l'activité du PC: elle analyse de façon dynamique les fichiers entrant et sortant de l'ordinateur, soit par disquette, courriel ou téléchargement. Elle inspecte aussi tous les applications à leur lancement, afin d'être sûre qu'ils ne déclenchent pas un virus dont ils seraient porteurs.

Enfin, si un virus est détecté, l'antivirus propose en principe de le «nettoyer» ou de le mettre en quarantaine.

Un bon antivirus doit posséder ces deux fonctionnalités.

Comment se débarrasser d'un virus informatique ?

Le monde informatique n'est pas aussi aseptique que l'on aimerait qu'il soit. Il y aura toujours un nouveau virus qui réussira à déjouer notre vigilance et qui utilisera un des nombreux trous de sécurité de Windows pour infecter notre ordinateur.

Si on doute d'avoir attrapé un virus informatique, on recommande de s'assurer que le logiciel d'antivirus est à jour pour reconnaître les derniers virus (vers ou cheval de Troie). Et ensuite balayer (scan) tous les disques durs de l'ordinateur...

Il faudra prendre une grande respiration et surtout pas de panique... Il existe une façon d'éliminer ce virus.

Le premier reflex de 80 % des gens, est de formater leur disque dur... Mais en fait, la seule chose que cela fait est d'effacer toutes les données précieuses. Il ne faut jamais formater le disque dur, à moins d'avoir tout fait pour l'éliminer.

Conclusion

Nous pensons qu'il n'y a pas de formule magique pour se débarrasser d'un virus informatique. C'est plus sage de dire que chaque virus a son remède ou antidote particulier, selon les dommages causés par le virus en question. D'après la croyance populaire, les logiciels d'antivirus détectent et se débarrassent automatiquement des virus informatiques. Cela est en partie vrai. Si le logiciel est mis à jour et balaye les courriels entrants, et qu'il perçoit la présence d'un virus, normalement il nous avertit par un message d'alerte et met le fichier contenant le virus en quarantaine pour le rendre inactif.

Si notre ordinateur est déjà infecté, le logiciel d'antivirus va percevoir la présence d'un virus et il nous avertit par un message d'alerte (incluant le nom du virus), mais il n'élimine pas automatiquement le virus. C'est pour cette raison qu'il est important de prendre en note le nom du virus... On a besoin du nom du virus de faire une recherche pour trouver un outil de suppression.

Bibliographie

1. Ludwig Mark Allen, Naissance d'un virus, Addison-Wesley France
2. Ludwig Mark Allen, Mutation d'un virus, Addison-Wesley France
3. Ludwig Mark Allen, Du virus à l'antivirus, guide d'analyse Dunod
4. Filiol Eric, Les virus informatiques : théorie, pratique et applications, Collection Iris.
5. www.symantec.com
6. www.branchez-vous.com