

SECURITE AVEC INTERNET – Jacques Delattre

Cet article répond à plusieurs demandes pour essayer de comprendre les intrusions dans nos PCs et résumer les possibilités de protection sachant que nos problèmes et nos compétences ne sont pas ceux des entreprises. S'il ne peut être question d'une étude d'ensemble dans un domaine riche en nouveautés quotidiennes, on peut regrouper quelques informations et règles permettant d'évaluer les risques et de mettre en place des défenses en fonction de la situation et des besoins de chacun.

- Qui peut en vouloir à nos petites machines, et pourquoi ?
- Quels outils ces gens-là utilisent-ils ?
- Quels outils et moyens avons-nous pour les contrer ?

Sans être paranoïaques, nous protégeons nos biens par des portes, des volets, des armoires, des clés, des coffres-forts, des alarmes, nous examinons et surveillons les gens qui rentrent chez nous et que nous ne connaissons pas. Pourquoi laisser ouverts à tous les vents nos ordinateurs qui contiennent nos informations financières, courriers, photos, documents d'études et de recherches ?



QUI PEUT EN VOULOIR A NOS MACHINES ?

Des anarchistes géniaux, encore appelés « hackers ». Dotés de très solides connaissances techniques, ils ne supportent pas les insuffisances des logiciels, ceux de Microsoft en particulier, et les font remarquer en attaquant les sites des éditeurs mais également nos propres machines équipées de ces produits. Ils ne nous connaissent pas, ne nous veulent aucun mal mais dénaturent nos fichiers, empêchent nos connexions ou les interrompent etc ...

Des anarchistes terroristes. Cherchent à prendre le contrôle de nos machines pour les lancer à l'attaque de sites qui ne leurs plaisent pas ou pour dissimuler chez nous des informations qu'ils préfèrent ne pas garder chez eux.

- Les attaques contre les sites directeurs internet (une douzaine) mettent en jeu des milliers, voire des dizaines de milliers de machines infiltrées de programmes déclenchant des flots de messages au jour et à l'heure prévue qui saturent et font disjoncter les machines visées.
- La dissimulation de documents est une sécurité très efficace pour le pirate mais vous êtes responsable des documents stockés chez vous, même à votre insu. Détectables seulement si vous connaissez bien le contenu de vos disques ce qui devient difficile avec des machines de plus de 100Goctets.

Des anarchistes imbéciles. Du genre qui raie les carrosseries de voitures et casse les pare-brise, ni vu ni connu. Ils ne cherchent qu'à détruire, le plus possible. Leurs compétences sont limitées ou nulles mais on trouve sur Internet tout l'outillage pour s'amuser. Ils étaient autrefois (il y a deux ou trois ans !) les plus nombreux mais sont maintenant débordés par les autres catégories.

Des amis qui nous veulent du bien. Tellement de bien qu'ils brûlent de connaître tout de nous, nos courriers, nos promenades sur internet, nos finances ... certainement pour partager nos joies et nos soucis.

Des amis qui ne nous veulent pas du bien. Les mêmes, avec détournements et/ou chantage à la clé. Ceux-ci sont le plus souvent, et heureusement, le fait de parfaits inconnus qui partent en promenade sur Internet et découvrent des opportunités !

Des gens faisant des études de marché ou de comportement. Une autre forme d'amis, ces études étant évidemment menées pour nous fournir des produits et des services parfaitement adaptés à nos goûts. Il n'y aurait rien à redire si nous donnions notre accord mais il s'agit plus souvent de véritables opérations d'espionnage menées par des entreprises spécialisées agissant sur contrat mais pouvant revendre à tout va les trouvailles inattendues, ce dont elles se défendent évidemment dans leurs publicités.

Des entreprises faisant la publicité de leurs produits. Ce sont les fameux spams ou pop-ups, courriers non sollicités ou placards venant s'incruster sur nos écrans. Plus agaçante que dangereuse (sauf si des programmes d'espionnage y sont associés), cette publicité constitue, semble-t-il, plus de la moitié du trafic internet, au point de pousser les Etats à préparer des législations pour tenter de régulariser le flot.

ETC. L'industrie est maintenant entrée dans des actions de piratage ciblées qui risquent de s'étendre. Les dégâts matériels liés à cette activité sont limités mais nous payons le trafic engendré et il devient difficile de maintenir le secret de nos affaires

○ ○ ○

DE QUELS MOYENS CES GENS DISPOSENT-ILS ?

Des programmes et des fichiers comme ceux que nous utilisons et les moyens pour les introduire dans nos machines.

Programmes. Ils ont été baptisés au fur et à mesure de leur apparition : virus, cheval de Troie, espion, pop-up (mettre en relief) etc. en relation avec leurs capacités.

- Virus : petit et reproductible dans la machine pour être disséminé. Caractéristiques nécessaires d'une part pour les rendre difficilement détectables dans les machines des années 1970 et, d'autre part, pour paralyser rapidement les réseaux attaqués au plus fort de la guerre froide.
- Cheval de Troie : se met en sommeil pour s'activer à une date ou à un signal donné.
- Espion. Envoie à son commanditaire les informations pour lesquelles il a été programmé : sites internet visités, banque, numéro de compte, composition de la machine etc ...
- Cookie : forme particulière d'espion créée par Microsoft. Il ne s'agit pas d'un programme mais d'un fichier (un millier d'octets) mis à la disposition d'un programme introduit de façon licite dans votre machine. Créé par ce programme s'il n'existe pas, consulté s'il existe, enrichi des informations intéressantes qui peuvent paramétrer le programme, le contenu peut être envoyé au propriétaire du programme. Utilisé à l'origine pour compter des occurrences ou des avancements de tâches mais largement dévié depuis.
- Pop-up : incruste dans l'écran des textes ou bannières publicitaires que vous ne sollicitez pas.

Le tout est maintenant mélangé : un pop-up peut être conçu comme un virus ou jouer à l'espion ou contenir un virus, on parle maintenant plus souvent de « peste » (pest: parasite).

Inoculation. Le réseau téléphonique est le moyen le plus classique, avec mention spéciale pour les pièces jointes au courriel et pour les ActivX mais il ne faut pas négliger les disquettes, CDs et clés USB.

- Réseau téléphonique. Quand vous activez Internet Explorer (ou Mozilla ...) vous commencez par établir un lien physique avec votre FAI (Fournisseur d'Accès Internet) en format RTC (Réseau Téléphonique Commuté) ou ADSL, puis vous lancez sur ce lien une communication au protocole internet par lequel messages et pestes peu-

vent passer. Quand vous fermez Internet Explorer (ou Mozilla ...) le lien physique reste généralement ouvert et tous les parasites imaginables peuvent continuer à y circuler et à frapper votre machine. Le protocole IE sera ignoré mais d'autres protocoles peuvent être utilisés en fonction de l'équipement de votre machine, licites (voix téléphonique, Minitel etc.) ou illicites (drivers introduits sous forme de peste). La liaison téléphonique est donc une entrée permanente, que IE (ou Mozilla ...) soit activé ou non, sauf si elle est coupée. Ceux qui ont installé ZoneAlarm peuvent arrêter IE en gardant la ligne ouverte, afficher le centre de contrôle de ZA et voir les parasites continuer d'être refoulés.

- Ports de communication. On connaît les ports (prises) installés au dos de la machine : parallèle (imprimante, 1 ou 2), série (communication, 1 à 3), USB (tout et n'importe quoi, 2 à 4 en général mais démultipliables), chacun ayant son adresse dans le BIOS ... qui peut en reconnaître 65000 environ correspondant à autant de ports logiques, donc de points d'entrée et de possibilités de sortie. En l'état actuel des choses, il n'y a aucun obstacle physique ni logique au transit dans ces ports et la machine peut donc être considérée comme ouverte à tous les vents.
- Courriel et pièces jointes. Le courriel ne constitue pas une peste par lui-même (au moins aujourd'hui !) tout au plus peut-on rencontrer des liens (adresse en clair ou « cliquer ici ») qui, si vous les actionnez, avertissent l'émetteur du message qu'il y a quelqu'un au bout du fil. Par contre les pièces jointes peuvent être des programmes, pestiférés ou non, du genre .exe .com .doc etc. qui démarrent dès que vous en commandez l'ouverture. S'il contient une peste, l'infection est instantanée.
- ActivX. Un document informatique est soit un fichier passif, collection d'informations que l'on consulte (textes et multimédia), soit un programme, fichier exécutable qui déroule ses instructions quand on l'ouvre. ActivX est une technique Microsoft (Windows) qui introduit un programme rendu passif dans un fichier passif, l'en extrait et reconstitue le programme qui vient se planter dans la machine sous forme de « plug-in » exécutable. On peut en trouver dans des pièces jointes de courriel mais plus généralement dans des pages diffusées par les sites internet. Les pages animées, en particulier, sont souvent diffusées sous cette forme mais c'est évidemment un moyen facile pour inoculer des pestes. ActivX est une réponse au langage Java de Sun qui proposait les mêmes possibilités, que Microsoft n'a jamais apprécié mais qui est maintenant considéré comme sécurisé vis-à-vis des pestes.
- Disquettes (en voie d'extinction), clés USB (en phase explosive), disques amovibles et CDs. Rarement utilisés de manière systématique sauf par des anarchistes imbéciles et à petite échelle. Mais ils peuvent ramasser des incongruités présentes dans une machine quand vous faites des copies et vous les passer incognito. Les musiques en MP3 obtenues à partir de réseaux du genre Kazaa et les compilations en résultant sont quasi systématiquement infectées.

○ ○ ○

QUELS MOYENS POUR NOUS DEFENDRE ?

Les moyens de défense ne manquent pas, vous en trouverez plus loin présentés sans ordre particulier car c'est probablement ainsi que vous serez amenés à les utiliser, qu'il s'agisse de méthodes, de possibilités de Windows ou de logiciels spécifiques. Mais c'est d'abord une affaire de comportement.

Comportement. Nous protégeons nos biens, appartements ou maisons en apportant les moyens et l'attention voulus sans pour autant devenir paranoïaques. Les risques d'intrusion dans nos machines sont assez récents, ne font pas encore partie de la culture générale et nécessitent des outils nouveaux mais avec le même genre d'attention et de sang-froid. Met-

tez en place les outils et méthodes que vous aurez sélectionnés, tenez-les à jour, vérifiez qu'ils sont fonctionnels, passez régulièrement votre machine aux détecteurs de pestes, nettoyez-la des résidus d'Internet, moyennant quoi les risques se trouvent aussi limités que lorsque vous montez en voiture.

Les possibilités d'Internet Explorer. Ce navigateur n'est pas vraiment réputé pour sa sécurité. Il comporte cependant des possibilités qui peuvent être intéressantes, toutes sont actionnées depuis la séquence Outils/Options Internet.

- Onglet Général: faites **démarrer** sur une page vierge, cela vous évitera de passer systématiquement par le portail de votre FAI mais aussi de démarrer contre toute défense sur un site indésirable qui aura glissé son adresse en « Page par défaut ».
- Onglet Sécurité. Internet Explorer peut vous informer chaque fois qu'une intervention **ActivX** est demandée que vous acceptez ou refusez selon la confiance que vous accordez au site. Parfois crispant (mais on peut désactiver momentanément), évitez pas mal de « plug-in » douteux. Ce même onglet permet aussi de régler le niveau de sécurité de Java, prenez le plus élevé.
- Onglet Confidentialité. Permet de régler le niveau de confidentialité des **cookies**, depuis la libre utilisation jusqu'au refus total.
- Onglet Contenu: filtre les accès aux **sites**, aux **forums** ou aux **comptes** de courriel par listes d'autorisation et d'interdiction. Vous pouvez par exemple recevoir du courriel de tous les comptes sauf de ceux que vous signalez ou, au contraire, seulement de ceux que vous listez. Contient également une protection parentale par paramétrage et par appel à des sites d'organisations spécialisées.

Identification téléphonique (IP). Dans le cas d'une connexion RTC, l'identification sur le réseau internet (IP identification) est changée chaque fois que vous vous connectez. Contrairement à ce qui est souvent écrit, il en est généralement de même en connexion ADSL mais la publicité qui est faite sur la permanence de la liaison physique (pas de commutation) pousse à ne jamais déconnecter. La déconnexion physique est d'ailleurs rendue difficile par l'alimentation de l'adaptateur ADSL sur la prise USB qui suit le sort de l'unité centrale sauf en cas de hub alimenté. Mettez fin à la session quand vous terminez un travail, quitte à en ouvrir une nouvelle quelques minutes plus tard, vous éviterez d'être reconnu par un numéro IP fixe. Pour vérifier le numéro IP : connectez-vous, Démarrer/Exécuter, tapez WINIPCFG.

Identification personnelle. Malgré la présence d'espions en tous genres, vous avez probablement communiqué vous-même la plus grande partie des informations personnelles utilisées pour vous empester.

- Par principe, ne **communiquez pas vos noms, adresse, téléphone, IP, adresse de courriel et toutes choses de ce genre** à des inconnus (individus ou organisations), aussi aimables et serviables soient-ils. Examinez en quoi ce genre d'information est nécessaire à qui vous la demande et si le fait de la fournir peut vous être réellement utile. La réponse à cette question est généralement non. Exemple: vous pouvez fournir tout cela à Symantec qui vous enverra sa pub mais vous pourriez tout aussi bien consulter leur site quand vous en avez besoin. Ne fournissez pas non plus les coordonnées de vos correspondants sans leur accord ça pourrait fâcher (pour les courriels, utilisez la formule blank carbon !)
- Eventuellement, ouvrez un compte de courriel sur un site gratuit tel Hotmail que vous utiliserez pour les opérations pas sûres et que vous fermerez après quelque temps d'utilisation. Ou utilisez des éléments composés de toutes pièces et qui n'ont aucune chance d'arriver à une destination quelconque tel azertu.iop@nbvcx.sin

Etanchéité des machines. Une seule solution, un **PARE-FEU** (firewall) devenu aussi indispensable qu'un antivirus en protocole RTC ou ADSL. Un pare-feu ferme les ports non utilisés de la machine et contrôle le trafic téléphonique entrant. Un bon pare-feu (tel ZoneAlarm et à l'inverse de Microsoft) masque les ports inutilisés qui deviennent donc invisibles et contrôle les trafics entrant et sortant. Les tentatives d'effraction illicites sont bloquées, les applications licites doivent recevoir l'accord de l'opérateur au cas par cas avec une autorisation permanente pour les plus fréquentes. J'ai ainsi constaté que Norton AntiVirus appelait systématiquement le site Symantec et j'ai par ailleurs bloqué plusieurs programmes espions qui voulaient accéder à leurs sites. Les éditeurs de pare-feu sont en première ligne et améliorent leurs défenses, mettez-les régulièrement à jour.

Virus et programmes douteux : les antivirus. Ce sont des programmes surveillant toute la machine et tous les points d'entrée et de sortie pour détecter les virus repérés par leurs signatures (environ 65000 aujourd'hui) ou par la forme syntactique. Les éditeurs d'antivirus, une quinzaine, ont formé un groupe de recherche et de détection qui reçoit les informations en provenance des utilisateurs, traque les nouveautés en menant des surfs sur le réseau, analyse et décrit les nouveautés qui sont ensuite confiées aux différents éditeurs pour introduction dans leurs programmes de désinfection. La qualité d'un éditeur ne dépend plus de sa capacité de recherche mais de sa capacité à produire et à diffuser les contre-mesures appropriées.

Les mises à jour des fichiers de signatures sont au moins hebdomadaires, plus fréquentes et même quotidiennes en période de crise. N'omettez pas la mise à jour du moteur quand elle est proposée. Un antivirus insuffisamment mis à jour est nocif car vous vous pensez protégés.

Courrier électronique (courriel). Méfiance absolue, c'est le seul moment où on peut devenir un peu caractériel.

- N'ouvrez jamais dans votre messagerie (généralement Outlook Express) un message d'apparence anormale ou de provenance totalement inconnue. Ouvrez-le éventuellement dans l'application messagerie sur le portail de votre FAI et supprimez-le s'il reste douteux.
- Ne répondez pas au message pour faire se découvrir l'émetteur. C'est en fait vous qui vous découvrez et qui validez votre adresse électronique, c'est le but de l'opération. Des messages contiennent parfois l'indication : cliquez ici pour me connaître. Une variante de l'opération avec le même résultat.
- Vérifiez que votre antivirus inspecte bien les pièces jointes.
- N'ouvrez jamais une pièce jointe exécutable et notamment avec une terminaison en .doc .com .bat .xls . Interrogez l'émetteur quand vous l'avez identifié sinon détruisez-la. De très nombreuses infections sont transmises par des correspondants qui vous transmettent un texte sans même l'avoir ouvert ou par des virus exploitant des fichiers d'adresses électroniques à l'insu du propriétaire.

Canular (hoax). Un message tout à fait sûr souvent transmis par un bon ami. Dans le meilleur des cas, un vrai canular sans danger. Dans de trop nombreux cas, souvent accompagnés d'une suggestion de re-routage, peut casser votre machine. Exemple vrai: vous êtes informé que le programme progr.exe est infecté, que vous devez l'effacer et charger une nouvelle version provenant du site microsuft sur lequel il suffit de cliquer. Le site est pirate et le programme est une peste. Renseignez-vous sur les sites Hoaxbuster.com ou Hoaxkiller.com ou Secuser.com qui ne sont pas des hoaxes !

Logiciels espions. Des programmes spécialisés souvent gratuits (Ad-aware, spybot) tiennent à jour des listes de ces programmes, les détectent et les effacent dans votre machine. A mettre à jour fréquemment. Les antivirus commencent à assurer cette fonction ce qui n'est pas trop difficile quand on gère déjà 65000 signatures.

Pop-up's. Des logiciels appropriés empêchent l'affichage des pop-up's , certains gratuits (barre d'affichage de Google par exemple).

Disquettes, clés USB et CDs. L'antivirus surveille normalement le trafic venant de ou allant vers ces périphériques. En cas de doute, faites une recherche spécifique de virus ou d'espion avant de commander l'ouverture. Concernant les CDs, **désactivez leur démarrage** automatique dans Windows (les démarrages en ce qui concerne XP), cela pourra vous éviter une infection foudroyante. Méfiez-vous particulièrement des disques publicitaires, des copies et compilations de musique ou de photos procurées par les petits-enfants ... et même par les enfants: une bonne moitié des machines amenées au cercle pour nettoyage a été empestée de cette manière.

Nettoyage. Les pestes sont une résultante non voulue des explorations sur l'Internet. Mais ces explorations laissent aussi des traces provenant de l'organisation même de Windows, fichiers bruts en provenance des sites (fichiers cache), historiques, traces d'activeX etc. qu'il est préférable d'effacer. Vous gagnerez de la place et vous éliminerez ces traces que des espions pourraient bien retrouver eux aussi.

- Analysez régulièrement tous les éléments de votre machine à la recherche des virus et, souvent maintenant, des programmes douteux qui ne sont pas des virus. Passez de la même manière le ou les programmes anti-espions : vous pouvez en utiliser plusieurs, ils sont partiellement complémentaires.
- Effacez régulièrement les traces de vos promenades sur le réseau. Plusieurs programmes le font, plus ou moins complètement, Internet Cleanup (Aladdin) efface en une seule commande les fichiers cache, cookies, historiques, composants ActivX générés, plugiciels (plug-in) messageries instantanées, liste des derniers fichiers utilisés et une sélection d'espions.



CONCLUSION. Les machines du cercle, et la mienne, sont équipées de :

- Norton Systems Works comportant Norton antivirus
- Pare-feu ZoneAlarm
- Anti-espions Ad-aware et, parfois, spybot
- Anti pop-up de Google
- Nettoyeur Internet Cleanup (Aladdin)

régulièrement mis à jour et utilisés. Internet Explorer est réglée pour une sécurité optima. Les courriers douteux sont éliminés. Et nous n'avons récolté ni virus ni, apparemment espions depuis longtemps.