Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les hackers ne sont jamais à court d'idées lorsqu'il s'agit de pirater vos données personnelles. En témoigne le recours aux sites pour jeunes publics dont les contenus sont truffés de malwares. Un phénomène déjà observable sur les sites pornographiques.

Atlantico: Les sites pour enfants sont-ils les plus pollués par les virus ?

Fabrice Epelboin: Les malwares qui infectent les sites le font le plus souvent de façon opportuniste : ils profitent d'une faille de sécurité sur un site pour l'infecter et en faire un vecteur d'attaque enver ses visiteurs. A ce jeu, ce sont plutôt les amateurs de pornographie, qu'on devine adultes et plutôt masculins, qui sont les premier visés, non pas pour ce penchant particulier, mais plus pour la multitude de failles de sécurité que l'on trouve sur ces sites, ainsi que la facilité qu'il y a d'en monter de nouveaux dans le seul but d'infecter ses visiteurs.
Les contenus sont faciles à trouver et à réagencer, et les réseaux publicitaires dédiés à ce type de contenus peu regardant sur les publicités qu'ils véhiculent – potentiellement infectées ou menant vers des sites infectés. L'utilisation d'un adblocker est d'ailleurs en passe de devenir une bonne pratique en matière de sécurité informatique si vous surfez sur ce genre de site.
L'idée que les enfants soient plus particulièrement visés relève plus à mon avis du fantasme. Certes leurs compétences en sécurité informatique n'est pas bien élevée, mais de nos jours, on peut en dire de même pour la plupart des parents, qui sont tout aussi faciles à piéger, parfois avec des moyens d'une simplicité désarmante.
Quand je vois la fréquence avec laquelle des personnes du troisième âge se transmettent des documents Powerpoint remplis de chatons sous forme de slideshows remplis de macro infectés, je me dis que les afficionados de LOLcats sont probablement les plus à risque, au même titre que les amateurs compulsifs de pornographie.

Comment procèdent les cyber-criminels pour tenter les jeunes consommateurs ?

Comme avec les adultes : en leur proposant des contenus gratuits qui les séduisent, voir en poussant à installer sur leur machine des logiciels dont ils ignorent tout. Il est courant, sur les sites de téléchargement de contenus piratés, de télécharger, en guise de contenu, un éxécutable portant le nom du contenu désiré. Les chances d'infecter sa machine en lançant un tel éxécutable sont proches de 100%. Les enfants, comme la plupart des adultes, peuvent se faire avoir.
Dans le cas relevé récemment par la BCC, on attire non pas les enfants, mais les joueurs de Minecraft avec un "mod", un programme qui va ajouter une fonctionnalité au jeu et qui, au passage, va infecter la machine sur laquelle il est installé. Cette attaque aurait tout aussi bien pu viser un adulte – ils sont nombreux à jouer à Minecraft – et n'a été évitée, dans ce cas, que du fait de la compétence en sécurité informatique du père, ce qui n'est pas si courant que cela.
Le cas de figure le plus courant est plutôt le suivant : des parents parfaitement ignorants de la chose informatique et des enfants débrouillards, pas forcément en sécurité informatique, mais dans le contournement de tous les obstacles que leurs parents auraient pu mettre en place en matière de sécurité. C'est un domaine où la valeur n'attend pas le nombre des années, à l'image de ce garçon de 12 ans qui a mis en place un stratagème pour mettre à jour le code secret du coffre fort de ses parents.

Quel risque pour nos données numériques ?

De se les faire dérober, la plupart du temps. Selon les données, cela peut représenter un risque plus ou moins grand. Vous pouvez être victime, une fois vos coordonnées dérobées, de multiples campagnes de phishing, d'usurpation d'identité, ou pire, de ransomware – particulièrement à la mode ces temps ci – un malware qui va chiffrer les données de votre disque dur et vous réclamer une rançon pour les déchiffrer.
Dans le cas où c'est une agence de renseignements qui dérobe vos données, les risques sont différents. Si vous êtes un opposant politique, vous risquez d'être surveillé de près de façon à perturber vos activités et mettre à jour vos réseaux politiques ; si vous êtes un journaliste d'investigation, on s'interessera plutôt à vos sources ; et si vous travaillez dans une entreprise sensible ou présente dans des marchés internationaux, on peut se servir de vos données pour attaquer votre employeur.

Les sécurités parentales servent-elles à quelque chose ?

Si votre enfant n'est pas très éveillé, oui, cela peut être utile. S'il est malin, non, il se fera un plaisir de contourner tout cela. Les "sécurités parentales" servent, la plupart du temps, à interdire l'accès aux contenus pornographiques aux enfants. C'est à mon sens une illusion – surtout dès qu'on parle d'adolescents – et cela ne fait que rendre ces contenus plus désirables.
Ces filtres parentaux ont systématiquement été contournés, et le mode d'emploi pour le faire se retrouve tôt ou tard sur Internet. Cela ne peut que pousser les enfants à comprendre comment ils marchent pour les désactiver, et cela aurait presque des vertus pédagogiques en matière d'éveil des enfants aux technologies, mais les conséquences sont fâcheuses, c'est le moins que l'on puisse dire, d'autant que cela ne fera que creuser l'écart de compétences entre les enfants et leurs parents, au détriment de ces derniers.
En pratique, rien ne remplace l'éducation, mais encore faut-il maîtriser un domaine pour éduquer ses enfants à celui-ci, ce qui ramène encore une fois vers la transmission au plus grand nombre d'un ensemble de règles de base en matière de sécurité informatique, à la façon d'un permis de conduire qui permet à chaque automobiliste de se sécuriser et de sécuriser les autres par la même occasion, en appliquant à la lettre un ensemble de règles simples.
Le problème c'est que personne n'est véritablement responsable de cette transmission d'information. Ni l'école – le primaire, le secondaire comme le supérieur – ni l'entreprise ne se sont saisis de cette mission. Or, chacun de ces acteurs pourrait tout à fait mettre en œuvre des programmes pédagogiques simples qui permettrait à tout un chacun d'échapper à une large partie des pièges tendus par les cybercriminels. On pourrait enseigner cela dès l'école primaire. On pourrait intégrer cela dans la formation permanente des employés – ce serait du reste très rentable pour les entreprises qui perdent des fortunes du fait d'attaques informatiques qui tirent parti de l'ignorance de leurs employés… [Lire la suite]

Réagissez à cet article

Fabrice Epelboin est enseignant à Sciences Po et cofondateur de Yogosha, une startup à la croisée de la sécurité informatique et de l'économie collaborative.

Source : *Quand les sites pour enfants se transforment en pièges pour voler les données personnelles de leurs parents | Atlantico.fr*