PODCAST FRENCH TO GO
Saison 6 - Episode 232

Et si votre frigo était piraté ?

Cette semaine, je voudrais vous parler de mon imprimante. Oui, je sais, ça n'a pas l'air vraiment intéressant. Mais attendez, vous allez voir… Il y a une bonne raison à cela. Depuis quelque temps, je pense que mon imprimante a une vie personnelle. Elle s'allume toute seule, elle s'éteint toute seule et, parfois, elle se met soudainement à imprimer. Enfin… "imprimer', c'est un bien grand mot : disons plutôt qu'elle crache deux ou trois pages complètement blanches. Comme ça. Sans raison.
Au début, je pensais que c'était un simple problème technique. Maintenant, je commence à me demander si elle n'a pas développé une personnalité. Peut-être qu'elle s'ennuie. Peut-être qu'elle cherche à attirer mon attention. Peut-être qu'un jour elle va décider elle-même de modifier la police de caractères de mes documents. Ou peut-être qu'elle va imprimer mes cours en caractères minuscules simplement pour économiser de l'encre. Après tout, vu le prix des cartouches, elle aura peut-être raison.
Mais une autre possibilité m'est venue à l'esprit : et si mon imprimante avait été piratée ? Alors, ne vous dites pas immédiatement : "Elle est complètement folle, cette Delphine." Enfin, vous pouvez le penser, mais pas uniquement à cause de cette histoire d'imprimante. Parce que, techniquement, ce n'est pas complètement impossible. Mon imprimante est connectée à mon ordinateur et à mon téléphone. Je peux lui envoyer un document sans utiliser de câble, grâce au Bluetooth ou au réseau Wi-Fi. Et aujourd'hui, malheureusement, pratiquement tout appareil connecté peut présenter un problème de sécurité. Alors, ça ne veut pas dire qu'un pirate informatique s'intéresse personnellement à mes documents de grammaire française. Je pense sincèrement qu'il existe des activités criminelles bien plus passionnantes. Mais, en théorie, une personne pourrait profiter d'une faille, c'est-à-dire d'un défaut dans la sécurité du système, pour prendre le contrôle d'un appareil. Et donc, dans notre cas, le contrôle de mon imprimante.
Jusqu'à récemment, les histoires de piratage informatique me semblaient assez faciles à comprendre. Attention, je ne dis pas que je trouvais cela normal ou acceptable. Je veux simplement dire qu'on pouvait généralement identifier l'objectif des pirates. Souvent, ils cherchent à gagner de l'argent. Ils entrent dans le système informatique d'une banque, d'une compagnie d'assurance, d'un opérateur téléphonique ou d'un service administratif pour voler des informations personnelles : des noms, des adresses, des numéros de téléphone, des coordonnées bancaires ou des mots de passe. Ils peuvent ensuite utiliser ces informations ou les revendre.
Parfois, les pirates bloquent complètement le système informatique d'une entreprise, d'une mairie ou même d'un hôpital. Les employés ne peuvent plus accéder aux dossiers, aux logiciels ou aux machines. Les pirates réclament alors une rançon. Une rançon, c'est une somme d'argent demandée pour libérer une personne ou, dans ce cas, pour rendre l'accès aux données et aux ordinateurs. Le principe est simple : "Donnez-nous de l'argent et nous débloquerons, peut-être, votre système." Je dis "peut-être", parce qu'on ne peut évidemment pas faire entièrement confiance à une personne qui vient de pirater votre entreprise.
Il existe également des attaques pour espionner un gouvernement ou une grande entreprise, pour perturber un service public, pour défendre une cause politique ou simplement pour se venger. Dans tous ces cas, le principe est inquiétant, mais l'objectif paraît relativement clair : voler de l'argent, obtenir des informations, faire pression sur quelqu'un, créer du désordre ou montrer sa puissance.

Mais, au mois d'octobre 2026, il s'est passé quelque chose de beaucoup plus étrange en France. Des pirates informatiques ont pris le contrôle des systèmes de réfrigération d'environ 700 supermarchés de plusieurs grandes enseignes, c'est-à-dire de plusieurs grandes chaînes comme Intermarché, Carrefour ou Leclerc.
Et là, vous vous posez peut-être la même question que moi : comment peut-on pirater les frigos d'un supermarché ? En fait, ces appareils sont connectés pour permettre aux responsables et aux techniciens de contrôler leur température à distance et de recevoir une alerte en cas de problème.
Les pirates ont réussi à entrer dans le système et, dans certains magasins, ils ont fait monter la température jusqu'à 50 degrés pendant plusieurs heures. Évidemment, les aliments frais et surgelés ne pouvaient plus être vendus. La chaîne du froid avait été rompue, c'est-à-dire que les produits n'étaient pas restés à la bonne température et pouvaient donc devenir dangereux pour la santé.
Les magasins ont dû jeter une grande partie de leur marchandise, fermer certains rayons, réparer les installations et commander de nouveaux produits. Les pertes se comptent probablement en millions d'euros.
Mais, personnellement, ce qui me rend surtout triste, c'est toute cette nourriture jetée. Bien sûr, les supermarchés ne pouvaient pas la donner à des associations puisqu'elle pouvait présenter un risque. Mais quand on sait que tant de personnes ne mangent pas à leur faim, voir autant de marchandises partir à la poubelle est franchement révoltant.

Et c'est à ce moment-là que je me suis posé la question : pourquoi quelqu'un ferait-il cela ?
Au moment où j'enregistre cet épisode, l'attaque n'a apparemment pas été revendiquée. "Revendiquer une attaque", ça veut dire annoncer publiquement qu'on en est responsable et, généralement, expliquer pourquoi on l'a faite. Pour l'instant, on ne connaît ni l'identité des pirates ni leur motivation. Alors, évidemment, mon imagination a commencé à travailler.
Peut-être que le pirate a simplement fait cela pour s'amuser ou pour montrer ce qu'il était capable de faire. Une sorte de défi personnel (c'est un peu plus impressionnant que de faire sortir trois pages blanches de mon imprimante, je dois le reconnaître).
Peut-être qu'il s'agissait d'une vengeance. On peut imaginer un ancien employé de l'entreprise qui produit le logiciel de contrôle des réfrigérateurs. Il a été licencié, il est furieux et il connaît parfaitement les faiblesses du système. Alors il décide de se venger en transformant les chambres froides de plusieurs centaines de supermarchés en saunas.
Ou alors, le pirate a lui-même été victime d'une intoxication alimentaire après avoir mangé un produit surgelé mal conservé. Il est resté malade pendant trois jours et il a décidé de se venger de tous les congélateurs de France.
Peut-être aussi que cette attaque n'était qu'un test. Les pirates voulaient vérifier jusqu'où ils pouvaient aller avant de préparer une opération beaucoup plus importante. C'est cette possibilité qui est la plus inquiétante. Parce que si on peut prendre le contrôle à distance de centaines de chambres froides, qu'est-ce qu'on pourrait contrôler d'autre ?

En fait, de plus en plus d'objets de notre quotidien sont connectés à Internet. Notre téléphone, notre télévision, notre montre, notre voiture, notre système de chauffage, nos caméras de surveillance, notre porte de garage et parfois même notre cafetière. Cela rend la vie plus pratique. Mais cela signifie aussi que chacun de ces objets peut devenir une porte d'entrée pour un pirate.
Commençons par quelque chose d'assez amusant : la machine à café connectée. Imaginez qu'un pirate décide de modifier son fonctionnement. Vous demandez un café court et très fort, elle vous prépare un immense café presque transparent. Vous demandez un cappuccino, elle vous donne uniquement de la mousse de lait. Et le matin où vous avez une réunion importante, elle refuse complètement de fonctionner et affiche simplement : "Vous

avez déjà bu suffisamment de café cette semaine.”
On peut aussi imaginer une télévision qui s’allume et s’éteint toute seule en pleine nuit. Ou qui change de chaîne dès qu’un programme devient intéressant. Vous regardez les cinq dernières minutes d’un film policier, le détective est sur le point de révéler l’identité du meurtrier et, tout à coup, la télévision passe sur un documentaire consacré à la reproduction des escargots.
Un réfrigérateur connecté pourrait commander automatiquement des produits dont vous n’avez absolument pas besoin. Vous rentrez chez vous et vous découvrez qu’il a commandé 40 yaourts, douze litres de lait et trois kilos de fromage. Vous n’aviez rien demandé, mais votre réfrigérateur a analysé vos habitudes et il estime que vous ne mangez pas suffisamment de produits laitiers. C’est pour votre bien, évidemment.
Tout cela est embêtant, mais pas vraiment grave. Malheureusement, d’autres scénarios peuvent être beaucoup plus tristes. Imaginez un aquarium dont la température et la qualité de l’eau sont contrôlées à distance. Si quelqu’un modifie les réglages, les poissons peuvent mourir.
On peut ensuite passer à quelque chose de franchement effrayant. Certains aspirateurs robots possèdent une caméra pour se déplacer dans la maison et éviter les obstacles. Imaginez qu’un pirate puisse accéder à cette caméra. Il pourrait observer l’intérieur du logement, enregistrer des images privées ou repérer les objets de valeur : l’ordinateur, la télévision, les bijoux ou les œuvres d’art. Il pourrait même savoir à quels moments les habitants sont absents et transmettre ces informations à des voleurs. À ce stade, l’aspirateur qui devait simplement nettoyer le salon devient un petit espion qui se promène librement dans toute la maison.
Un pirate pourrait aussi ouvrir une porte de garage, désactiver une alarme ou bloquer une serrure connectée. Vous pourriez vous retrouver enfermé à l’extérieur de votre propre maison, pendant que votre téléphone vous informe très calmement que la porte est parfaitement sécurisée.
Et puis, il y a les situations réellement dangereuses. Pensons à une voiture connectée. Si quelqu’un modifie le GPS, les conséquences peuvent être graves. Pensons aussi aux réfrigérateurs des pharmacies et des hôpitaux, qui conservent des vaccins, des médicaments ou des échantillons biologiques. Une modification de quelques degrés peut détruire des produits indispensables.
Enfin, on arrive au scénario mortel : les feux de signalisation. Imaginez qu’une personne pirate le système qui contrôle les feux d’un grand carrefour et mette tous les feux au vert en même temps. Les automobilistes pensent qu’ils peuvent passer, les piétons aussi, et personne ne comprend ce qui se produit avant qu’il soit trop tard. Là, on ne parle plus d’un problème informatique, de quelques pages blanches ou de produits à jeter. On parle directement de vies humaines.
Alors, est-ce qu’il faut avoir peur de tous les objets connectés et revenir immédiatement aux téléphones fixes, aux cartes routières en papier et aux cafetières italiennes ? Non, je ne pense pas. Les appareils connectés sont utiles. Le problème n’est pas nécessairement la connexion elle-même. Le problème, c’est la manière dont elle est sécurisée.
Quant à mon imprimante, je vais continuer à la surveiller. Pour le moment, elle se contente de cracher quelques pages blanches. Mais si, un matin, elle imprime un message disant : “Versez 500 euros si vous voulez revoir vos documents”, je saurai qu’il est temps de m’inquiéter sérieusement.
Et vous, quels appareils connectés avez-vous chez vous ? Lequel serait le plus amusant s’il était piraté ? Lequel serait le plus inquiétant ?

frenchcarte@gmail.com - Sound : http://www.freesound.org/people/klankbeeld/

Creative Commons Attribution – NonCommercial NoDerivatives 4.0 International License