Top 6 most surprising entry points for cyberattacks

Top 6 des points d'entrée de cyberattaques les plus inattendus

By Victor Poitevin – September 02, 2019.

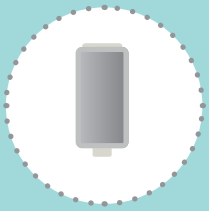
Whether at home or at work, hackers are becoming ever more ingenious when it comes to getting into IT networks. They exploit the vulnerabilities of susceptible smart devices to come up with cyberattacks which use very imaginative entry points. Synopsis of the most surprising entry points.

All the smart devices in your private and professional life represent a potential threat as long as manufacturers fail to incorporate security measures at the design stage. But, in addition to this "Security by design" approach, it is essential to maintain these devices in safe operating condition throughout their life cycle. And, therefore, users must be educated in a basic level of digital health. But that's another story.

Que ce soit au domicile ou sur le lieu de travail, les hackers redoublent d'ingéniosité pour infiltrer les réseaux informatiques. Exploitant les failles d'objets connectés souvent vulnérables, ils imaginent des cyberattaques aux points d'entrée pour le moins originaux. Tour d'horizon des plus inattendus.

Tous les objets connectés présents dans votre vie personnelle ou professionnelle représentent donc une menace potentielle tant que leurs constructeurs n'intégreront pas la sécurité dès la phase de conception. Mais en plus de cette approche « security-by-design », il est fondamental de maintenir ces objets dans des conditions opérationnelles de sécurité tout au long de leur cycle de vie. Et donc d'éduquer les utilisateurs à une certaine hygiène numérique. Mais ça, c'est une autre histoire…

AN ELECTRIC WATER HEATER

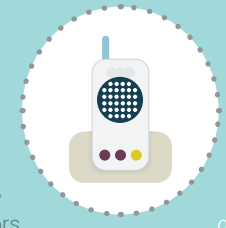


Researchers at Princeton University have simulated a scenario that could easily occur in the privacy of our own homes. In this sort of attack, hackers take control of power-hungry devices in order to disrupt the electricity network. According to this study, only 42,000 electric water heaters would be required to take down 86% of the Polish electrical grid. It's a chilling thought.

UN CHAUFFE-EAU ÉLECTRIQUE

Des chercheurs de l'Université de Princeton ont testé un scénario qui pourrait bien se dérouler dans l'intimité de nos propres maisons… Durant cette attaque, les hackers prennent le contrôle d'appareils énergivores afin de déstabiliser le réseau électrique. D'après cette étude, seuls 42 000 chauffe-eaux électriques suffiraient à couper 86% du réseau électrique polonais. De quoi en refroidir plus d'un.

A BABY MONITOR

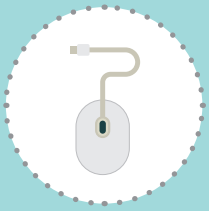


And, while on the subject of our homes, it was partly by hacking baby monitors that hackers orchestrated a distributed denial of service (DDoS) attack against Dyn in 2016. By overloading this service provider's servers, attackers managed to make some sites, including the very popular Twitter, Amazon and Airbnb, inaccessible for nearly 12 hours.

UN BABYPHONE

Toujours au cœur de nos habitations, c'est en partie en piratant des babyphones que des hackers ont dirigé une attaque par déni de service distribué (DDoS) contre la société Dyn en 2016. En saturant les serveurs de ce prestataire de service, les attaquants ont réussi à rendre certains sites inaccessibles dont les très populaires Twitter, Amazon ou encore Airbnb, et ce, pendant près de 12 heures.

A COMPUTER MOUSE

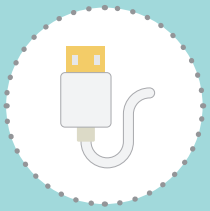


Whether it sits on your desk at work or at home, the mouse seems harmless. That's why Netragard, the IT security audit specialists, came up with the idea of hacking into one for the purpose of embedding spyware. It was sent as a promotional package to an employee and, once plugged in, it connected to a third-party server. Mission accomplished for Netragard, who were engaged by the company in question to investigate possible security vulnerabilities.

UNE SOURIS D'ORDINA-TEUR

Qu'elle trône sur votre bureau au travail ou à la maison, la souris paraît inoffensive. C'est pourquoi la société Netragard, spécialisée dans l'audit de sécurité informatique, a eu l'idée d'en pirater une pour y intégrer un logiciel espion. Envoyée sous forme de colis publicitaire à un employé, elle s'est connectée à un serveur tiers après branchement. Mission accomplie pour Netragard, missionné par l'entreprise en question pour rechercher d'éventuelles failles de sécurité…

A USB CABLE



We are often wary of USB sticks that we connect to our computer but did you know that USB cables can be compromised? So be extra careful the next time you go to use a USB device that you have received as a freebie at some event or that someone has loaned you.

UN CÂBLE USB

On se méfie souvent des clés USB que l'on connecte à son ordinateur mais saviez-vous que des câbles USB peuvent être corrompus ? Redoublez donc d'attention la prochaine fois que vous utiliserez un objet USB reçu en cadeau sur un événement ou prêté par quelqu'un.

AN AQUARIUM THERMOMETER

Hackers have used the smart thermometer from a North American casino aquarium to gain access to their data. Once again, this demonstrates that vulnerability can often be found in "gadgets" that aren't covered by the general security policy.

UN THERMOMÈTRE D'AQUARIUM

Des hackers ont utilisé le thermomètre connecté de l'aquarium d'un casino nord-américain pour accéder à ses données. La preuve encore une fois que la vulnérabilité réside souvent dans des « gadgets » non couverts par la politique de sécurité globale.

A FAX MACHINE

You thought the fax machine was obsolete? You were wrong! Nearly 17 billion faxes are still sent each year, especially in the health sector which processes a large volume of sensitive data. This information has not escaped the attention of the hackers who target these devices' vulnerabilities as a way of getting into an organisation's networks. You think you're protected because you've gone over completely to printers? Maybe you should check that your printer doesn't have a fax function!

UN TÉLÉCOPIEUR

Vous pensiez que le télécopieur était dépassé ? Détrompez-vous, près de 17 milliards de fax sont encore envoyés chaque année, notamment dans le secteur de la santé qui traite une grande quantité de données sensibles. Cette information n'a pas échappé aux hackers qui ciblent les vulnérabilités de ces appareils pour infiltrer les réseaux des entreprises. Vous vous pensez protégés car vous êtes passés au tout imprimante ? Vérifiez que votre machine n'intègre pas une fonction télécopie…