



Cybercriminalité : les entreprises de plus en plus vulnérables

A l'ère du digital, il est possible d'infiltrer une centrale nucléaire iranienne, de faire tomber le site d'un conseil général, de pirater la carte bancaire du chef de l'Etat ou de pénétrer la forteresse informatique de Bercy. L'entreprise, de plus en plus dépendante du numérique, est aussi plus vulnérable. Florilège.

Le compte Twitter d'Obama piraté, des centaines d'euros prélevés sur le compte bancaire de Nicolas Sarkozy... Les chefs de l'Etat eux-mêmes ne sont pas à l'abri. Pas plus que les institutions. L'hiver dernier, une pièce jointe dans un e-mail a suffi pour infiltrer 150 ordinateurs de Bercy permettant à des pirates de se procurer des dossiers sur la présidence française du G20. Les antivirus n'avaient rien signalé. Attaqué, en mai 2011, le réseau PlayStation Network de Sony (qui permet d'acheter en ligne des films, des jeux et de la musique avec une console PS3) avait dû fermer quelques jours en avril au grand dam de ses 75 millions d'utilisateurs quotidiens. Sony n'excluant pas "que les données bancaires aient été dérobées". 93 000 comptes d'utilisateurs du géant japonais de l'électronique ont à nouveau été piratés début octobre. Les comptes ont été suspendus et leur utilisateurs légitimes invités à changer de mot de passe. Aux Etats-Unis en avril, Epsilon, entreprise de marketing en ligne, s'est fait voler quelque 100 millions de noms et d'adresses électroniques de clients de groupes bancaires et commerciaux. Un record historique ! Moralité : plus notre monde devient dépendant du digital, plus les menaces qui pèsent sur lui et sur les entreprises se multiplient. Et se démocratisent...

Graines de pirates

Plus besoin d'être un ingénieur en informatique comme il y a un quart de siècle pour s'installer hacker. La culture du contournement est devenue très populaire. Dès la cour de récréation, en réalité. "Vous savez ce qu'est une carte R4 ? Sa vente est licite - pour les consoles de jeu DS - mais certains de ses usages le sont moins, révèle Nicolas Arpagian, qui dirige le cycle "Sécurité numérique" à l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Les enfants s'en servent pour débrider des jeux vidéo ou en pirater."

L'an passé, un collégien d'Arras en classe de cinquième a réussi à s'introduire dans le serveur de son collègue pour modifier ses notes et ses appréciations. L'ex-champion cycliste Floyd Landis est soupçonné d'avoir, avec son entraîneur, réalisé une cyberattaque sur le laboratoire antidopage de Châtenay-Malabry afin de trafiquer les résultats de ses analyses.

Ce patron de PME s'étonne que le distributeur automatique de confiseries de sa boîte soit si souvent vide... Des salariés indécents avaient reprogrammé le système de la machine : tous les produits vendus l'étaient à zéro euro aux heures de bureau ! Le piratage informatique est devenu un sport populaire. Mais, pratiqué par des pros, il peut vite devenir très menaçant.

Attaques de zombies

Le phénomène des "botnets" a pris de l'ampleur en 2010, selon le Clusif (Club de la sécurité de l'information français). Pour quelques centaines d'euros, ces petits programmes installés sur des milliers d'ordinateurs peuvent les transformer en "zombies". Les objectifs d'une attaque par botnets sont vastes : relayer du spam pour du commerce illégal, infecter d'autres machines, paralyser le trafic, voler des données personnelles et bancaires...



Les attaques portent sur les tuyaux comme sur les contenus. Il s'agit d'abord de se brancher sur votre système d'information pour espionner votre contenu, sans vous déranger ni ralentir votre activité : une attaque informatique réussie est indolore ! Mais, même quand elle se sait attaquée, l'entreprise hésite à le faire savoir. "C'est un peu comme les maladies vénériennes, on a honte d'en parler !" observe Nicolas Arpagian. Quand Bercy a été attaqué, l'Agence nationale de la sécurité des systèmes d'information (Anssi, rattachée au Premier ministre) a pourtant préféré communiquer sur l'attaque plutôt que la garder secrète. "Pour inciter d'autres organisations et entreprises piratées à le faire savoir. Un but prophylactique en quelque sorte...", estime l'expert en sécurité numérique. Les réseaux de l'entreprise peuvent aussi être utilisés à leur insu. "Un peu comme un porteur sain peut diffuser une pathologie sans être affecté par elle", remarque Nicolas Arpagian. En 2010, de nombreux responsables de sécurité informatique (RSOI) ont ainsi vu passer un ver informatique, Stuxnet, dans leur système d'information : il était inoffensif tant qu'il n'avait pas trouvé sa cible... des installations nucléaires iraniennes !

Chantage aux données

Les opérations de chantage fonctionnent bien sur le Net. Chantage type : votre ordinateur est infecté et vous recevez un mystérieux coup de fil : "Si le 23 du mois vous ne payez pas, vos données seront inaccessibles." Vous payez ou non ? Le PDG de cette filiale industrielle d'un grand groupe coté a préféré payer 80 000 euros plutôt que risquer d'être victime d'une bombe numérique à retardement en cas de non-paiement. Il n'était pas sûr d'être bordé question cybersécurité... En février dernier, la filiale espagnole de Nintendo a été victime d'un tel chantage. Un pirate avait volé une base de données de l'entreprise contenant les informations personnelles de 4 000 clients et menacé de les publier sur un forum de discussion. Nintendo n'a pas cédé et le hacker a été arrêté...

Flotte automobile sous contrôle

Nos voitures sont désormais bourrées d'électronique. A Austin (Texas) l'an passé, plus de 100 véhicules ont été immobilisés : un individu a réussi à s'introduire dans le système web gérant l'immobilisation des véhicules en cas de défaut de paiement des mensualités ! Après une enquête, il s'agissait de la vengeance d'un ancien employé licencié par un loueur de voitures. Il s'était servi du logiciel de sécurité Emergency Start System (ESS) qui permet de contrôler à distance les automobiles, notamment leur démarrage!

Smartphones, nouvelles cibles

Les smartphones sont de petits ordinateurs à part entière. Ils sont une porte d'entrée supplémentaire dans le réseau de l'entreprise. Mais l'utilisateur ne se protège guère. "Il faut dire qu'Apple ou Microsoft font tout pour vous empêcher d'installer une sécurité sur votre téléphone", confie sous couvert d'anonymat un expert de la sécurité.

"Personne n'a de pare-feu, déplore aussi Pascal Lointier, président du Clusif. Or un site peut tout à fait installer un programme malveillant sur votre iPhone ou effacer vos données à distance. Et quand vous vous synchronisez avec votre PC ou votre Mac de bureau, si celui-ci est infecté, vous infectez votre smartphone..."

Les 525 millions de smartphones dans le monde (chiffres 2010) seraient-ils donc de vraies passoires ?

En 2011, Apple ou Google sont soupçonnés de géolocaliser les utilisateurs et de récupérer identifiants, comptes et mots de passe pour connaître leurs habitudes de consommation. Apple est poursuivi pour divulgation aux réseaux de publicité de données personnelles sans le consentement des détenteurs d'iPhone. Android, le système d'exploitation de Google pour smartphones et PDA, peut installer ou supprimer des applis à votre insu et prendre le contrôle de votre téléphone.

Par Étienne Gless