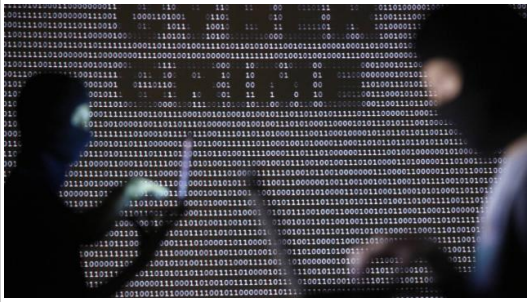
Crainte d’attentats pilotés à partir d’Internet en 2016

Crainte d’attentats pilotés à partir d’Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*