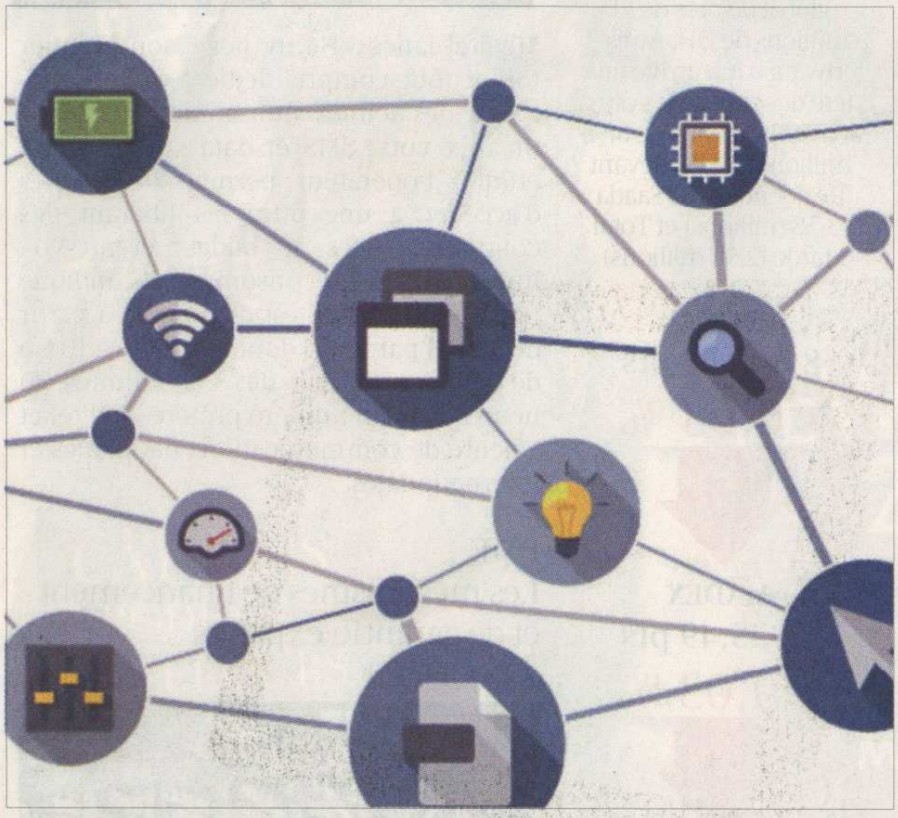
Cybercriminalité

Les objets connectés rattrapés par les hackers



Dans la plupart des cas, c'est l'administrateur des systèmes d'information de l'entreprise qui est visé.

En 2016, les menaces sur la mobilité et l'internet des objets vont s'accentuer. En effet, les hackers, qui ont longtemps ciblé les serveurs des grandes entreprises, se tournent aujourd'hui vers des maillons faibles, mal sécurisés : Smartphones, tablettes et objets connectés. Les explications de Frédéric Goux, analyste chez le cabinet français de conseil Solucom.

Usurper des identités, récupérer des données personnelles ou bancaires, bloquer la diffusion d'informations, procéder à des transferts d'argent, prendre le contrôle de systèmes de trading. Ce sont là les priorités des cybercriminels. Le phénomène connaîtra vraisemblablement, cette année, une recrudescence, avec une évolution du type de menaces. Les hackers, qui ont longtemps ciblé les serveurs des grandes entreprises, se tournent aujourd'hui vers des maillons faibles, mal sécurisés : Smartphones, tablettes et objets connectés. En clair, pour arriver à leurs fins, les cybercriminels passent en premier par l'utilisateur, maillon faible de la sécurité des entreprises. «Le plus simple c'est le Spearfishing, un fishing donc plus ciblé. Dans la plupart des cas, c'est l'administrateur des systèmes d'information (SI) de l'entreprise qui est visé en premier. Les hackers vont chercher ses informations personnelles, son cercle d'amis et toute autre information sur lui», décrypte Frédéric Goux, analyste chez le Cabinet Solucom. Selon le spécialiste, il faut en moyenne 205 jours pour détecter une attaque. «C'est à la fois une mauvaise et une bonne nouvelle. Il y a quelques années, la moyenne était de 400 jours. Mais pour reconstituer le système, les experts pensent qu'il faut compter une moyenne de 90 jours. En somme, il faut être capable de détecter et de réagir», insiste l'analyste lors d'une rencontre organisée à la Chambre française de commerce et d'industrie du Maroc à Casablanca, le 22 janvier.

> Il faut en moyenne 205 jours pour détecter une attaque et 90 jours pour reconstituer le système.

L'expert rappelle qu'en 2015, TV5 avait été bloquée pendant 20 heures (attaque signée Cybercaliphate) et était dans l'incapacité de diffuser. La France n'est pas la seule touchée. Les cybercriminels n'ont pas de frontières et opèrent au gré des opportunités avançant masqués et protégés par leur virtualité. Autre exemple, Ryanair a annoncé le 29 avril dernier qu'un virement de 4,5 millions d'euros vers un compte chinois avait été réalisé à son insu. «Le secteur bancaire, l'agroalimentaire et l'industrie sont les plus touchés par les pirates. Les données bancaires des clients et les données confidentielles sont prisées vu les gains qu'elles génèrent», précise Goux.

Selon l'éditeur des solutions de sécurité McAfee, 91% des failles sont d'origine humaine et cette première règle viendra compléter l'arsenal sécuritaire : procédures de sécurité, vigilance, éducation, formation... Enfin, «pour anticiper la fraude, la sécurité doit être intégrée dès le développement des services et des produits», conseille Goux. ■

Ilham Lamrani Amine