# Cybersécurité : quand le « Shadow IoT » menace les entreprises

Le volume de trafic généré par l'Internet des objets (IoT) autorisés et non autorisés monte en flèche dans les entreprises, selon une analyse du trafic cloud menée par Zscaler.

C'est ce que souligne un rapport* publié par ThreatLabZ, l'entité de recherche du fournisseur de solutions de sécurité en mode cloud. Désormais, les clients de la société de cybersécurité génèrent un milliard de transactions IoT par mois. Ce chiffre a bondi de « 1500% » par rapport au volume annoncé en mai 2019 par la firme basée à San José (Californie).

En analysant près de 500 millions de transactions de plus de 2 000 organisations dans le monde sur une période de deux semaines cette année, Zscaler déclare avoir dénombré 553 appareils IoT différents provenant de 212 fabricants et appartenant à 21 catégories distinctes.

Des objets connectés souvent hors de contrôle des directions des systèmes d'information (DSI).

## Face au « Shadow IoT »

La hausse du trafic issu d'appareils IoT non autorisés inquiète. Parmi ces objets qu'utilisent des employés, des partenaires et des clients pour se connecter aux réseaux des entreprises figurent : des assistants domotiques, des décodeurs TV, des caméras IP, des montres et des téléviseurs intelligents, voire des systèmes multimédias de véhicules…

Or, les connexions issues des appareils IoT sont trop rarement sécurisées, rapporte le fournisseur dans son rapport. Ainsi, 83% des transactions IoT étudiées seraient réalisées via des canaux en texte brut. 17% seulement utilisant des canaux sécurisés (SSL).

Pourtant, lorsque l'on considère les transactions IoT dans leur ensemble, ce sont bien les appareils « métiers » qui dominent. La majorité du trafic IoT provenant de terminaux de collecte de données (56,8%), le plus souvent des lecteurs de codes-barres sans fil.

Viennent ensuite les imprimantes (16%), les lecteurs multimédias (7,7%) et les lecteurs d'affichage numérique dynamique (7,1%). Mais les connexions ne sont pas toujours sécurisées. Or, Zscaler déclare bloquer chaque mois 14 000 tentatives d'attaques de malwares et de botnets destructeurs, contre 2000 tentatives environ en mai 2019.

## Adopter le Zero Trust

Certes, le Shadow IoT (où l'Internet des objets qui échappent au contrôle des équipes IT) constitue une menace grandissante. Selon Zscaler, l'absence d'une approche Zero Trust (zéro confiance) de la sécurité informatique est plus néfaste encore pour les entreprises.

« La première chose à laquelle vous devez absolument vous attaquer est la visibilité. Vous ne pouvez pas protéger ce que vous ne connaissez pas », a déclaré à leur attention Deepen Desai, vice-

president de la recherche en securité chez Zscaler, dans un billet de blog.

« Une partie de la visibilité dans un monde mobile et axé sur le cloud implique une mentalité Zero Trust », selon lui. Il s'agit pour les RSSI de vérifier et d'authentifier tous les utilisateurs et les appareils qui tentent de se connecter au réseau et aux applications de l'entreprise.

*(source : Zscaler – « IoT Devices in the Enterprise 2020: Shadow IoT Threat Emerges »).

(crédit photo : fumi via VisualHunt / CC BY-NC-SA)