

Votre caméra IP peut-elle être piratée ?

Votre caméra IP peut-elle être piratée ?

Deux équipes de chercheurs ont découvert des failles de sécurité qui affectent des dizaines de modèles de caméras IP professionnelles et grand public.

Le malware Mirai n'a pas fini de lever des armées d'objets connectés corrompus pour lancer des attaques DDoS. Des chercheurs autrichiens de SEC Consult ont découvert que pas moins de 80 modèles de caméras IP Sony étaient accompagnées de backdoor d'origine exploitable par des pirates.

Les modèles IPELA Engine de Sony affectés

Les experts de SEC Consult ont précisément découvert deux comptes utilisateurs, et leurs mots de passe, non documentés, pour accéder aux caméras IPELA Engine du constructeur japonais. Des systèmes de vidéo surveillance principalement utilisés par les entreprises et les autorités. Ces comptes, baptisés « primana » et « debug » installés par défaut, pourraient être utilisés par des pirates pour prendre le contrôle du serveur Web intégré dans le périphérique depuis Internet (via Telnet/SSH, les services de commandes à distance des objets connectés) en plus d'un accès depuis le réseau local.

Ces « portes dérobées » sont généralement introduites par les développeurs du constructeur à des fins de maintenance ou de test à distance. Ou parfois par des organisations étatiques (comme dans le cas de la backdoor de la NSA sur des routeurs Juniper). Un accès distant qui se transforme en faille de sécurité quand il tombe entre de mauvaises mains (ce qui fut le cas pour Juniper, notamment).

Le correctif de Sony à appliquer en urgence

Pour SEC Consult, il ne fait aucun doute que ces accès backdoor « permettent à un attaquant d'exécuter du code arbitraire sur les caméras IP concernées [et les] utiliser pour pénétrer le réseau et lancer d'autres attaques, perturber la fonctionnalité de l'appareil, envoyer des images manipulées, ajouter des caméras dans un botnet type Mirai ou espionner les gens ». La référence à Mirai n'est pas neutre. Le malware s'était emparé de centaines de milliers d'objets connectés, essentiellement des caméras IP, pour lancer des attaques contre le fournisseur de services DNS Dyn, des clients d'OVH ou encore le site du journaliste spécialisé en sécurité Brian Krebs.

Sony a fourni une mise à jour du firmware. A installer avant que des individus malveillants ne se chargent de reconfigurer l'accès des caméras. Selon l'outil en ligne Censys.io, plus de 4 500 de ces caméras Sony vulnérables sont accessibles directement depuis Internet. Dont 1 510 aux Etats-Unis et 256 en France.

Des centaines de milliers de caméras résidentielles

Sony est loin d'être le seul acteur concerné par la sécurité de ses caméras IP. En parallèle, des chercheurs de la firme israélienne Cybereason déclarent avoir découvert au moins deux failles zero day dans une douzaine de familles de caméras IP vendues en marque blanche dans la grande distribution et notamment sur eBay ou Amazon. D'une part, ils ont identifié que le mot de passe du compte par défaut était le même pour tous les modèles de périphérique (« 888888 » en l'occurrence pour l'identifiant « admin »). Mot de passe qu'il est impossible de renforcer puisque le système refuse la combinaison de différents types de caractères (soit uniquement des chiffres, soit des caractères en minuscule ou en majuscule). Une fois identifié, l'utilisateur peut injecter des commandes dans la caméra à partir d'un serveur Web.

D'autre part, les experts ont trouvé un moyen d'accéder à l'objet même si celui-ci est protégé derrière un firewall, en passant par le serveur web du vendeur qui offre un service Cloud (pour visualiser les images à distance sur un PC ou smartphone). Les chercheurs ne détaillent pas la façon dont ils ont procédé. Mais, sur leur blog, ils assurent que « cet exploit affecte des centaines de milliers de caméras dans le monde entier et nous ne voulons pas que les personnes malintentionnés utilisent nos recherches pour attaquer des gens ou utiliser ces caméras dans de futures attaques botnet »...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Backdoor et Zero Days pour plusieurs milliers de caméras IP