Caméras IP installées par des incompétents ? Une aubaine pour les pirates

	Caméras IP installées par des incompétents ? Une aubaine pour les pirates

Le piratage des caméras de vidéo surveillance, un jeu d'enfant pour les plus dégourdis du web. Sauf que ces pirates n'ont rien de génie, ils profitent uniquement de la fainéantise des utilisateurs.

Le piratage des caméras de vidéo surveillance n'est pas nouveau. Je vous parlais déjà de ces infiltrations de webcams en 2000. En novembre 2015, par exemple, je revenais sur un fichier contenant des centaines de webcams non sécurisées vendues dans le blackmarket ou encore de ce bébé réveillé par des hurlements d'un idiot du village ayant pris la main sur le baby phone de la famille.

En 2014, je vous révélais la création d'un site Internet Russe qui référencent plusieurs dizaines de milliers de webcams. Bref, un business juteux pour les commerçants du voyeurisme et autres vendeurs de données sensibles (La boutique est-elle vide ? Le hangar stocke en ce moment des téléphones portables ; la banque vient d'être livrée en billets frais…).

Je te soupçonne de taper dans la caisse ! (Boutique de la Ville de Rai)

La sécurité des caméras sur IP est souvent mise à la mal comme j'ai pu le montrer dans ZATAZWeb.tv de mars 2014. Il ne devrait pas être si facile, normalement, de regarder dans la chambre d'un étranger, et encore moins dans des centaines de chambres filmées par ces caméras de vidéo surveillance. Pourtant, cela reste possible comme je vais vous l'expliquer plus bas.

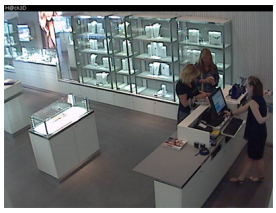
Montrez moi votre contrat, que je vous renseigne. (Boutique du 92)

Failles et mots de passe facilitent le piratage des caméras de vidéo de surveillance

Pour accéder à une caméra de vidéo surveillance rien de plus facile. D'abord avoir l'IP de la cible. Un détail pour les adeptes du social engineering. Autant dire que cette adresse n'est à communiquer à personne. Lisez le mode d'emploi de votre caméra. Chercher les options de sécurité proposées. Soyons honnête, plus votre webcam IP aura d'option, plus elle sera coûteuse. Mais la réflexion vaut, je pense, la sécurité de ce que vous souhaitez protéger. Ensuite, le malveillant va rechercher la marque de votre matériel. Pour cela, rien de plus simple une fois encore. La page d'accès à l'administration de votre matériel parle.

Mais tu vas le changer ce password… c'est marqué en GRAS ! (Hôtel du 77)

Un conseil, faites de manière à ce qu'elle ne soit pas lisible : un Htaccess par exemple, ou modifier le logo et toutes marques de reconnaissance pour le malveillant. Ensuite, le mot de passe. Trop de webcam IP, de caméras de vidéo surveillance gardent le mot de passe usine. Je vous laisse imaginer la facilité déconcertante que de retrouver ce sésame dans les notices et listes disponibles sur la toile. Un *admin:admin ; root:root et autre admin:0000* sont légions. Des clés qui se changent. Vous le faites bien quand vous perdez les clés de votre maison, faites le sur Internet. Enfin, les failles. Assurez-vous que votre cerbère ne soit pas référencé comme étant un outil « *open bar*« . Pour cela, un petit coup de Google ou ne soyez pas timide, posez la question !



La bijouterie est vide ! Le matériel, la caisse, le coffre sont repérés. Autant d'informations qui faciliteront l'action d'un malveillant. Vous aurez remarqué le petit « H@ck3D » en haut à gauche qui ne semble perturber personne !

Branleurs, voleurs, mateurs… même combat

Dans mon exemple, le pirate possède donc dorénavant l'IP, l'accès à la page d'administration de votre webcam IP, sa marque, vous n'avez pas changé le mot de passe usine et si c'est le cas, il vient de rechercher sur la toile les failles et accès « *pasvraimentprévudanslemodedemploi*« . Dernier exemple en date que ZATAZ a pu constater, l'alerte au sujet de la société AXIS. Un logiciel pirate, baptisé « *Hack AXIS* » permettait (permet toujours pour les caméras non mises à jour, NDR) d'accéder à la racine des périphériques sans avoir besoin de connaitre le mot de passe ; changer le mot de passe du matériel ; contrôler la caméra et, dans ce cas, lancer des attaques via la caméra transformée en Zombie/botnet. La caméra prise en main de la sorte par un pirate au fait de la faille, même mise à jour ensuite, restait dans le sac à malveillance de l'intrus. Une attaque d'autant plus gênante que l'exploit a été diffusé, en juillet 2016.

Bref, voilà donc le pirate avec une nouvelle source d'information à votre sujet. Imaginez, le serveur et l'IP l'oriente sur votre situation numérique ; la caméra, et les informations qu'elle peut transporter, fournissent au malveillant les yeux qu'il n'avait pas. En France, c'est une liste de plusieurs milliers de webcams accessibles qui trainent sur la toile, que ce soit dans le blackmarket ou sur des sites offrant de regarder à travers ces « yeux » non sécurisés.

Auteur : Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : ZATAZ Vidéo surveillance : Vous n’en avez pas marre d’être des idiots du 2.0 – ZATAZ