Faille de sécurité dans des caméras de vidéosurveillance FLIR

	Faille de sécurité dans des caméras de vidéosurveillance FLIR

Un chercheur en sécurité informatique découvre comment accéder aux images de caméras de vidéosurveillance thermiques FLIR.

Infiltration possible dans des caméras de vidéosurveillance ! Étonnante révélation, fin septembre, par un internaute du nom de LiquidWorm. Ce chercheur en sécurité informatique a diffusé un code qui permet de découvrir que les caméras thermiques de vidéo surveillance de marque FLIR pouvaient être espionnées. FLIR Systems a des identifiants de connexion SSH codés en dur dans sa version distribuée sous Linux.

Bref, un accès aux images, via cet accès caché qui ne peut être modifié !

Cette backdoor est dénoncée quelques jours avant le salon Milipol qui se déroulera en novembre à Paris. Flir Systems y sera présent pour présenter son matériel.

Selon l'information diffusée par « Zero science« , les modèles de caméras incriminées sont les 10.0.2.43 (logiciel F/FC/PT/D) et les versions du micrologiciel 8.0.0.64: □□1.4.1, 1.4, 1.3.4 GA, 1.3.3 GA et 1.3.2 sont concernés par cette porte cachée…[lire la suite]

Réagissez à cet article

Source : *ZATAZ Une porte cachée dans des caméras de vidéosurveillance FLIR – ZATAZ*

Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

	Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

Sounds really scary! Isn't it? But this scenario is not only possible but is hell easy to accomplish.A UX design flaw in the Google's Chrome browser could allow malicious websites to record audio or video without alerting the user or giving any visual indication that the user is being spied on.

AOL developer Ran Bar-Zik reported the vulnerability to Google on April 10, 2017, but the tech giant declined to consider this vulnerability a valid security issue, which means that there is no official patch on the way.

How Browsers Works With Camera & Microphone

Before jumping onto vulnerability details, you first need to know that web browser based audio-video communication relies on WebRTC (Web Real-Time Communications) protocol – a collection of communications protocols that is being supported by most modern web browsers to enable real-time communication over peer-to-peer connections without the use of plugins.

However, to protect unauthorised streaming of audio and video without user's permission, the web browser first request users to explicitly allow websites to use WebRTC and access device camera/microphone.

Once granted, the website will have access to your camera and microphone forever until you manually revoke WebRTC permissions.

In order to prevent 'authorised' websites from secretly recording your audio or video stream, web browsers indicate their users when any audio or video is being recorded.

« Activating this API will alert the user that the audio or video from one of the devices is being captured, » Bar-Zik wrote on a Medium blog post. « This record indication is the last and the most important line of defense. »

In the case of Google Chrome, a red dot icon appears on the tab, alerting users that the audio or video streaming is live.

How Websites Can Secretly Spy On You

The researcher discovered that if any authorised website pop-ups a headless window using a JavaScript code, it can start recording audio and video secretly, without the red dot icon, giving no indications in the browser that the streaming is happening…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication*

Des centaines de caméras de vidéo surveillance françaises piratées par… Hitler !

Des centaines de caméras de vidéo surveillance françaises piratées par… Hitler !

Piratage : Plus de 1500 caméras de vidéo surveillance d'entreprises Françaises infiltrées par un pirate informatique. Il a signé son forfait « Heil Hitler » sur les écrans de contrôle.
Je vous contais, il y a peu, de la vente d'accès à des caméras de vidéo surveillance. Un grand classique, malheureusement ! Les pirates profitent de la feignantise de certains utilisateurs à lire le mode d'emploi de leur appareil. Des utilisateurs qui ne changent pas le mot de passe usine, ou ne pensent même pas à l'activer. Bilan, l'accès aux images et à la webcam se font en deux clics de souris…[lire la suite sur ZATAZ]

Réagissez à cet article

Source : *ZATAZ Vidéo surveillance : des centaines de caméras françaises piratées par… Hitler ! – ZATAZ*

Un hacker réussit à formater 2 millions d’objets connectés au hasard

	Un hacker réussit à formater 2 millions d’objets connectés au hasard

Après les ordinateurs et les smartphones, c'est au tour des objets connectés de se faire hacker (ou pirater). Il semblerait qu'il soit facile de prendre leur contrôle. Ainsi il y a toujours un risque que votre drone prenne la fuite, que vos radiateurs connectés grimpent à 40 degrés. Pire encore : que vos alarmes connectées deviennent inefficaces !

Un hacker qui a bonne conscience

Sous son nom de code « Janit0r », le hacker annonce avoir **détruit deux millions d'objets connectés** en l'espace de quelques mois. **Pour la bonne cause**.
Car il n'a en vérité volé aucune donnée, ni utilisé l'internet des objets pour répandre des spams comme le faisait le logiciel « Mirai ». En revanche, ce Malware-là **efface la mémoire de tout objet connecté** auquel il accède. L'objet devient alors inutilisable, et doit retourner à l'usine pour être reprogrammé.
Sa revendication semble honorable : **il dénonce le laxisme des entreprises en matière de sécurité des technologies connectées.**

Le chercheur Pascal Geenens a étudié ce ver d'un peu plus près. **Seraient le plus touchées les caméras connectées**. Et la méthode est simple… **Le virus utilise le mot de passe par défaut des systèmes d'exploitation** dédiés aux objets connectés, basés sur Linux OS…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Un hacker réussit à formater 2 millions d'objets connectés au hasard*

Des fabricants d’objets connectés poursuivis en raison de failles de sécurité

Des fabricants d’objets connectés poursuivis en raison de failles de sécurité

La Federal Trade commission (FTC) américaine poursuit un troisième fabricant, l'accusant de mettre en danger la sécurité des consommateurs et la confidentialité de leurs données, en raison de la sécurité inadéquate de son routeur et de ses webcams. Derrière cette troisième plainte, c'est tout un plan d'action qui se dévoile en vue de contraindre les fabricants à augmenter le niveau de conception des objets connectés, même ceux d'entrée de gamme.

Et de trois ! La plainte déposée en janvier 2017 contre D-Link fait partie du plan de campagne de la FTC visant à renforcer la confidentialité et la sécurité des consommateurs par rapport à ce que l'on appelle l'Internet des objets (IoT). La FTC avait déjà dégainé deux fois, contre ASUS (un fabricant de matériel informatique) et TRENDnet (un distributeur de caméras vidéo).

IoT ?

Internet se transforme progressivement en un réseau étendu, appelé « Internet des objets », reliant tous les objets devenus connectables. Cette évolution soulève de nombreuses questions concernant la croissance économique et les mutations sociales, mais aussi les libertés individuelles et la souveraineté nationale, auxquelles les décideurs publics devront au plus tôt répondre. (http://www.strategie.gouv.fr).

Selon certaines études, c'est pas moins de 80 milliards d'objets connectés qui interagiront d'ici 2020. De la montre intelligente au téléphone, en passant par le frigo connecté, la webcam, le système d'alarme, la domotique, les outils de Smartcities (parcmètres, etc.), … la liste est quasiment infinie.

À côté des enjeux sociétaux, il y en a un autre dont on parle de plus en plus souvent : la sécurité.

La sécurité, enjeu technique mais aussi juridique

Les objets connectés ont, pour certains, mauvaise réputation. Surtout lorsqu'il s'agit objets connectés ayant une petite valeur économique. On songe par exemple aux webcams connectées à l'Internet. On peut en acheter pour quelques dizaines d'euros. Le problème vient du fait qu'étant connectés à l'Internet, ces objets représentent un point de faiblesse s'ils ne sont pas bien conçus et protégés. Une personne malintentionnée peut utiliser cet appareil connecté pour pénétrer le réseau, et ensuite s'y balader.

Exemples : si le système d'alarme connecté à l'Internet est mal protégé au niveau du routeur, on pourrait le désactiver à distance et entrer dans la maison. Si la webcam est mal protégée, on pourrait observer à distance une personne, voire enregistrer ses conversations, et la faire chanter ensuite.

La Federal Trade Commission a déposé une plainte contre le fabricant de matériel de réseau informatique Taiwanais D-Link Corporation et sa filiale américaine, alléguant que les mesures de sécurité inadéquates prises par la société ont laissé ses routeurs sans fil et caméras Internet vulnérables aux attaques de pirates, mettant en danger la sécurité et la vie privée des consommateurs américains.

Dans une plainte déposée dans le district nord de la Californie, la FTC a accusé D-Link de ne pas prendre de mesures raisonnables pour sécuriser ses routeurs et ses caméras (de surveillance) connectées, créant un risque important pouvant aller jusqu'à l'interception des flux audio et vidéo. En clair : on vous observe en vidéo ou on vous écoute, sans que vous le sachiez !

Pour la FTC, *« les pirates informatiques ciblent de plus en plus les routeurs et les caméras IP – et les conséquences pour les consommateurs peuvent inclure non seulement un problème de défectuosité du matériel, mais aussi un enjeu en termes de sécurité de l'individu et de sa vie privée. Lorsque les fabricants disent aux consommateurs que leur équipement est sécurisé, il est essentiel qu'ils prennent les mesures nécessaires pour s'assurer que ce soit vrai ».*

La sécurité est-elle défaillante ?

La FTC relève notamment :

• Défaut de sécurité lié aux identifiants de connexion intégrés en usine. Si tous les appareils d'un même modèle sortent de l'usine avec un paramétrage par défaut comprenant une identification et un mot de passe identiques, le risque est important que ces réglages d'usine ne soient pas modifiés par l'utilisateur, créant une voie d'entrée royale pour les pirates ;

• Sécurité insuffisante par rapport aux attaques par injection de commande. Ces attaques permettent d'utiliser une page d'erreur pour poser une série de questions de type True/False afin de prendre le contrôle total de la base de données ou d'exécuter des commandes sur un système. On en a beaucoup parlé avec les consoles de jeu en 2016.

• Mauvaise gestion d'un code d'accès privé utilisé pour se connecter au logiciel D-Link, ouvert sur un site public pendant six mois ;

• Absence de sécurisation des informations d'identification des utilisateurs pour l'application mobile (texte clair et lisible sur les appareils mobiles) alors qu'il existe des logiciels disponibles pour sécuriser ces informations.

Selon la plainte, les pirates pourraient exploiter ces vulnérabilités en utilisant plusieurs méthodes relativement simples.

Par exemple, en utilisant un routeur compromis, un pirate pourrait obtenir les déclarations de revenus des consommateurs ou d'autres fichiers stockés sur le périphérique de stockage attaché du routeur. Ils pourraient rediriger un consommateur vers un site Web frauduleux ou utiliser le routeur pour attaquer d'autres périphériques sur le réseau local, tels que des ordinateurs, des smartphones, des caméras IP ou d'autres appareils connectés.

Autre exemple : la FTC allègue qu'en utilisant une caméra compromise, un pirate pourrait surveiller le lieu où se trouve le consommateur afin de les cibler en cas de vol ou d'autres crimes, ou de regarder et d'enregistrer leurs activités personnelles et leurs conversations.

Original de l'article mis en page : Internet des objets : des fabricants poursuivis en raison des failles de sécurité des objets connectés – Droit & Technologies

---

Réagissez à cet article

Original de l'article mis en page : Internet des objets : des fabricants poursuivis en raison des failles de sécurité des objets connectés – Droit & Technologies

---

Salariés et vidéo surveillance, comment faire

bon ménage ?

	Salariés et vidéo surveillance, comment faire bon ménage ?

Dans le cadre de son pouvoir de direction, l'employeur a le droit de surveiller et de contrôler l'activité de ses salariés durant leur temps de travail. Les dispositifs de contrôle mis en place à cet effet doivent néanmoins respecter le principe énoncé à l'article L1121-1 du Code du travail aux termes duquel « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Certaines règles doivent donc être respectées par l'employeur afin de rendre licite l'utilisation de ces dispositifs de contrôles.

1) Les conditions de mise en place d'un système de vidéo surveillance dans l'entreprise

Le législateur a subordonné la validité du système de vidéosurveillance à 3 conditions cumulatives :

• Le système de vidéo-surveillance doit avoir pour but de préserver un intérêt légitime de l'entreprise pouvant être caractérisé par un risque particulier de vol ou par la surveillance d'un poste de travail dangereux (fondement : article L1121-1/ Atteinte aux libertés des salariés) ;

• Préalablement à sa mise en place, l'employeur doit consulter le Comité d'Entreprise et le CHSCT (article L2323-32 et L4612-9 du Code du travail) ;

• Les salariés doivent être individuellement informés : (article L1222-4 Code du travail et Cass.Soc.20 novembre 1991). Le signalement du dispositif par de simples affichettes ne suffit pas : Cass.Soc.7 juin 2006 ;

• Lorsque les informations à caractère personnel collectées au moyen du dispositif de vidéosurveillance font l'objet d'un traitement informatisé ou d'un fichier structuré, une déclaration préalable à la CNIL s'impose.

Le non-respect de ces obligations entraîne l'irrecevabilité des éléments recueillis par de tels dispositifs visant à prouver le comportement fautif des salariés.

2) L'exception au respect des conditions de validité du système de vidéo surveillance

Il existe une exception à la condition relative à l'information préalable des salariés : l'information préalable des salariés ne s'impose pas lorsque le dispositif est uniquement destiné à surveiller des locaux où les salariés n'ont pas accès et non au contrôle de leur activité : Cass.Soc.31 janvier 2001 ; Cass.Soc.19 avril 2005.

Par ailleurs, l'employeur ne peut être autorisé à utiliser comme mode de preuve les enregistrements d'un système de vidéo-surveillance installé sur le site d'une société cliente permettant le contrôle de leur activité dont les intéressés n'ont pas été préalablement informés de l'existence : Cass.Soc.10 janvier 2012.

Autre exemple : Cass.Soc.26 juin 2013, n° 12-16.564.

La Cour de cassation a récemment eu l'occasion de se pencher sur l'articulation des règles relatives à la vidéosurveillance dans un arrêt du 26 juin 2013 (Cass. Soc, 26 juin 2013, n° 12-16.564). En l'espèce, un magasin de grande distribution équipé d'un système de vidéosurveillance visant à se prémunir contre le risque de vols de la part de la clientèle s'était servi des enregistrements de ces caméras pour établir la faute grave d'un salarié. Les caméras avaient révélé le vol du téléphone qu'une cliente avait oublié au magasin par un salarié à la fin de sa journée de travail. Plus précisément, le salarié qui était employé au rayon boucherie du magasin avait été filmé se rendant au rayon billetterie du magasin qui se situait dans la galerie marchande, sur place il y avait dérobé le téléphone d'une cliente. Par ailleurs, les faits filmés s'étaient déroulés en dehors des heures de travail de l'intéressé.

Selon le salarié, les enregistrements ne pouvaient être produits par la société à l'appui du licenciement dont il avait fait l'objet dans la mesure où l'employeur n'avait pas respecté son obligation d'information préalable à l'égard des salariés et des représentants du personnel. La Haute cour, validant la cour d'appel, a rejeté son argumentation en rappelant que :

« Le système de vidéosurveillance avait été installé pour assurer la sécurité du magasin et n'avait pas été utilisé pour contrôler le salarié dans l'exercice de ses fonctions » ; dès lors, la cour d'appel *« a exactement retenu que le salarié ne pouvait invoquer les dispositions du code du travail relatives aux conditions de mise en œuvre, dans une entreprise, des moyens et techniques de contrôle de l'activité des salariés »*…[lire la suite]

Amandine Sarfati, Avocat.

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 : La vidéo surveillance dans l'entreprise. Par Amandine Sarfati, Avocat.

Les tendances de la vidéo surveillance en 2017

Les tendances de la vidéo surveillance en 2017

LE CABINET AMÉRICAIN IHS TECHNOLOGY, SPÉCIALISÉ DANS LES ÉTUDES DE MARCHÉ AU NIVEAU MONDIAL VIENT D'ÉDITER UNE ANALYSE DES TENDANCES 2017 DU MARCHÉ DE LA VIDÉO SURVEILLANCE.

Il en ressort les grandes lignes ci-dessous :

2017, UNE ANNÉE OÙ LES TENDANCES SE CONFIRMENT

2017 a toutes les chances de ressembler fortement à 2016. Nous devrions assister à la continuité et à la confirmation des grandes tendances déjà relevées en 2016. Ces tendances relèvent bien entendu l'abandon des équipements analogiques au profit des systèmes de vidéo surveillance haute définition et IP, une concurrence qui s'intensifie entre les constructeurs et l'accroissement de la part de marché des fabricants Chinois.

iHS prévoit une progression du marché de la vidéosurveillance identique à celle de 2016, c'est à dire dans la zone des 7%. L'étude relève que ce marché est constitué de très nombreux produits très différents les uns des autres, qu'il faut également constater les disparités entre utilisateurs finaux et régions du monde.Concernant les équipements, le marché des caméras de surveillance haute définition et des enregistreurs DVR connaitra encore cette année une hausse marquée du côté des entreprises et du marché résidentiel. Du côté institutionnel et administratif, les investissements se dirigent vers la surveillance des villes et des lieux publics dans la cadre de la lutte contre le terrorisme qui a fortement marqué ces 2 dernières années.

Si l'Europe n'est pas ou que peu sujette aux mouvements des monnaies, l'étude souligne que ces facteurs peuvent encore peser cette année sur les grandes régions que sont l'Amérique du Sud et la Russie.

LES PRINCIPALES PROGRESSIONS EN 2017

*** L'émergence confirmée de la vidéo surveillance 4K**
*** La croissance toujours forte des caméras et DVR Haute Définition HDVCVI, HDTVI et AHD**
*** Des capacités accrues pour le stockage des images**
*** La faillite des solutions d'analyse des images 100% serveur réseau**
*** Des marchés émergents pour les caméras portées sur le corps**
*** Des considérations encore plus grandes en matière de sécurité du public**
*** La vidéo surveillance 2.0 avec le phénomène lié au drones**
*** La progression des objets connectés (IoT) liés à la vidéo surveillance**

Réagissez à cet article

Original de l'article mis en page : 2017 : les tendances de la vidéo surveillance

---

Quels changements en Cybersecurité pour 2017 ?

Quels changements en Cybersecurité pour 2017 ?

Yahoo, Twitter, Spotify, Amazon, eBay, CNN… lannée 2016 aura été fructueuse en attaques informatiques majeures. Si, les conséquences sont limitées, elles prouvent que les hackers sont tenaces et créatifs. Faut-il sattendre à un nouveau type dattaque en 2017 ?

Historiquement, les cyber-pirates ont focalisé leur attention sur les grandes entreprises. Ces sociétés ont donc été les premières à adopter les nouvelles technologies, via des solutions souvent à peine testées. Résultat : elles peuvent plus facilement être compromises, via certaines failles qui n'ont pas encore été repérées par les fabricants. En conséquence, ce sont les grandes sociétés qui attirent les hackers en quête de nouveaux défis et subissent les attaques de grande ampleur.

En parallèle, par effet pyramidal, ces mêmes technologies sont progressivement adoptées par les moyennes entreprises puis, en bas de pyramide, par les PME. Lorsque le deuxième échelon de la pyramide est atteint, les technologies sont plus sécurisées grâce au retour d'expérience. Les hackers les délaissent donc bien souvent pour se concentrer sur des technologies plus récentes.

Mais 2017 devrait marquer un tournant : en effet, ce sont aujourd'hui ces entreprises de taille moyenne qui – dans un souci d'accélérer leur transformation numérique – adoptent en premier les nouvelles technologies. Elles s'équipent donc plus rapidement que les grands groupes – qui ont un process plus lourd et laisse moins de place à la flexibilité. En adoptant, par exemple, l'IoT et les technologies de l'industrie 4.0, ces sociétés "mid market" sont en train de devenir la cible privilégiée des hackers.

Type d'attaque : Des ransomwares liés à l'IoT

Après des années d'observation, on assiste enfin au déploiement à grande échelle de l'IoT. Chambres froides, kiosques, usines, voitures, et même machines de nettoyage industriel, tout cela sera bientôt connecté dans un souci de performance et de monitoring. Espérons qu'ils soient également sécurisés.

Le déploiement de ces dispositifs connectés n'est pas sans risque : leur intégrité peut être compromise si la sécurité n'est pas pensée d'une nouvelle manière. Certaines rumeurs prétendent même que des hackers se sont déjà servis de l'IoT pour attaquer une entreprise et lui demander une rançon. Nous risquons donc de voir une augmentation de ce type d'attaques dans un avenir proche. Par conséquent, l'année 2017 sera certainement la première où une entreprise admettra de façon publique qu'elle a été confrontée à ces cyber-attaques par rançon….[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 : Cybersécurité : quels changements pour 2017 ?

Rakos, un nouveau botnet qui vise aussi les Objets connectés

Rakos, un nouveau botnet qui vise aussi les Objets connectés

Après Mirai, voici venir Rakos, un malware infectant des serveurs et des réseaux d'objets connectés, tournant sous Linux, afin de créer des botnets. ET, demain, lancer des attaques DDoS.

Comme le tristement célèbre malware Mirai, Rakos prend pour cible l'Internet des objets (IoT). Ces deux logiciels malveillants compromettent en effet des serveurs sous Linux et des réseaux d'appareils connectés. La capacité de nuisance de ces botnets contrôlés à distance est bien réelle. Si Mirai se propage essentiellement via les ports logiciels Telnet, Rakos vise lui les ports SSH. Les périphériques embarqués et les serveurs ayant un port SSH ouvert ou un mot de passe très faible sont les plus exposés. Rakos a été découvert cet été par les chercheurs de ESET.

À ce jour, Rakos est utilisé pour mener des attaques par force brute, indique l'entreprise dans un billet de blog. Et ce, afin d'ajouter d'autres appareils compromis à son réseau de machines zombies. Mais le programme pourrait également servir à mener des campagnes de spam ou des attaques par déni de service distribué (DDoS) d'ampleur, comme l'a fait Mirai…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Rakos, un nouveau botnet IoT en constitution