Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?

	Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?

Suite à une nouvelle panne de courant, la compagnie nationale d'électricité de l'Ukraine enquête pour savoir si une attaque de cyberpirates est à l'origine du problème.
Des experts en sécurité cherchent à savoir si la panne de courant qui a affecté ce week-end certains quartiers de la capitale ukrainienne, Kiev, et la région environnante provient d'une cyberattaque. Si ce dernier point venait à être confirmé, il s'agirait du deuxième black-out causé par des pirates informatiques en Ukraine, après celle qui s'est produite en décembre 2015.

L'incident a affecté les systèmes de commande d'automatisation d'un relais de puissance près de Novi Petrivtsi, un village situé au nord de Kiev, entre samedi minuit et dimanche. Cela a entraîné une perte de puissance complète pour la partie nord de Kiev sur la rive droite du Dniepr et la région environnante…

75 minutes pour rétablir le courant

Les ingénieurs d'Ukrenergo, la compagnie d'électricité ukrainienne, ont commuté l'équipement de commande en mode manuel et commencé à rétablir la puissance par palier de 30 minutes, a dit Vsevolod Kovalchuk, directeur d'Ukrenergo, dans un billet posté sur Facebook. Il a fallu 75 minutes pour restaurer toute la puissance électrique dans les zones touchées de la région, où les températures descendent jusqu'à -9 en ce moment. Une des causes suspectées est « une interférence externe à travers le réseau de données » a déclaré sans plus de précision Vsevolod Kovalchuk. Les experts en cybersécurité de la société étudient la question et publieront très bientôt un rapport.
Parmi les causes possibles de l'accident figurent le piratage et un équipement défectueux, a déclaré Ukrenergo dans un communiqué. Les autorités ukrainiennes ont été alertées et mènent une enquête approfondie. En attendant, les premières conclusions, tous les systèmes de commande ont été basculés du mode automatique au manuel, a indiqué la compagnie.

Un Etat derrière les attaques sophistiquées

Si un piratage venait à être confirmé, ce serait la seconde cyberattaque en un an contre le réseau électrique ukrainien. En décembre dernier, juste avant Noël, des pirates informatiques avaient lancé une attaque coordonnée contre trois compagnies d'électricité régionales ukrainiennes. Ils avaient réussi à couper l'alimentation de plusieurs sous-stations, provoquant des pannes d'électricité qui ont duré entre trois et six heures et touché les résidents de plusieurs régions.
A l'époque, les services de sécurité ukrainiens, le SBU, avaient attribué l'attaque à la Russie. Bien qu'il n'y ait aucune preuve définitive liant ces attaques au gouvernement russe, les cyberattaquants avaient utilisé un morceau de malware d'origine russe appelé BlackEnergy, et la complexité de l'attaque suggère l'implication d'un État. La semaine dernière, des chercheurs du fournisseur de sécurité ESET ont alerté la communauté au sujet d'attaques récentes contre le secteur financier ukrainien menées par un groupe qui partage de nombreuses similitudes avec le groupe BlackEnergy…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une cyberattaque suspectée de causer un black-out en Ukraine – Le Monde Informatique

---

Que nous réserve la CyberSécurité en 2017 ?

Que nous réserve la CyberSécurité en 2017 ?

La fin de l'année c'est aussi et surtout la période des bilans. Dans cet article, nous mettrons en évidence les cinq tendances les plus importantes tendances à venir. Qu'elles se maintiennent ou évoluent durant l'année 2017, une chose est sûre, elles risquent de donner du fil à retordre aux professionnels de la cybersécurité.

1 : intensification de la guerre de l'information
S'il y a bien une chose que la cybersécurité nous a apprise en 2016, c'est que désormais, les fuites de données peuvent être motivées aussi bien par la recherche d'un gain financier ou l'obtention d'un avantage concurrentiel que pour simplement causer des dommages dus à la divulgation d'informations privées. À titre d'exemples, le piratage du système de messagerie électronique du Comité National Démocrate (DNC) américain qui a conduit à la démission de Debbie Wassermann Schultz de son poste de présidente ; ou encore, la sécurité des serveurs de messagerie qui a miné la campagne présidentielle américaine de la candidate Hillary Clinton dans sa dernière ligne droite. Il est également inexcusable d'oublier que Sigmundur Davíð Gunnlaugsson, le Premier ministre islandais, a été contraint de démissionner en raison du scandale des Panama Papers.
Les évènements de ce type, qui rendent publiques de grandes quantités de données dans le cadre d'une campagne de dénonciation ou pour porter publiquement atteinte à un opposant quelconque d'un gouvernement ou d'une entreprise, seront de plus en plus fréquents. Ils continueront de perturber grandement le fonctionnement de nos institutions et ceux qui détiennent actuellement le pouvoir.

2 : l'ingérence de l'État-nation
Nous avons assisté cette année à une augmentation des accusations de violations de données orchestrées par des États-nations. À l'été 2015, l'administration Obama a décidé d'user de représailles contre la Chine pour le vol d'informations personnelles relatives à plus de 20 millions d'Américains lors du piratage des bases de données de l'Office of Personnel Management. Cette année, le sénateur américain Marco Rubio (républicain, État de Floride) a mis en garde la Russie contre les conséquences inévitables d'une ingérence de sa part dans les élections présidentielles.
Il s'agit là d'une autre tendance qui se maintiendra.
Les entreprises doivent donc comprendre que si elles exercent ou sont liées de par leur activité à des secteurs dont les infrastructures sont critiques (santé, finance, énergie, industrie, etc.), elles risquent d'être prises dans les tirs croisés de ces conflits.

3 : la fraude est morte, longue vie à la fraude au crédit !
Avec l'adoption des cartes à puces – notamment EMV (Europay Mastercard Visa) – qui a tendance à se généraliser, et les portefeuilles numériques tels que l'Apple Pay ou le Google Wallet qui sont de plus en plus utilisés, les fraudes directes dans les points de vente ont chuté, et cette tendance devrait se poursuivre. En revanche, si la fraude liée à des paiements à distance sans carte ne représentait que de 9 milliards d'euros en 2014, elle devrait dépasser les 18 milliards d'ici 2018.
Selon l'article New Trends in Credit Card Fraud publié en 2015, les usurpateurs d'identité ont délaissé le clonage de fausses cartes de crédit associées à des comptes existants, pour se consacrer à la création de nouveaux comptes frauduleux par l'usurpation d'identité. Cette tendance devrait se poursuivre, et la fraude en ligne augmenter.
Le cybercrime ne disparaît jamais, il se déplace simplement vers les voies qui lui opposent le moins de résistance. Cela signifie, et que les fraudeurs s'attaqueront directement aux systèmes de paiement des sites Web.

4 : l'Internet des objets (IdO)
Cela fait maintenant deux ans que les experts prédisent l'émergence d'un ensemble de risques inhérents à l'Internet des objets. Les prédictions sur la cybersécurité de l'IdO ont déjà commencé à se réaliser en 2016. Cela est en grande partie dû à l'adoption massive des appareils connectés d'une part par les consommateurs, mais aussi par les entreprises. En effet, d'après l'enquête internationale portant sur les décideurs et l'IdO conduite par IDC, environ 31 % des entreprises ont lancé une initiative relative à l'IdO, et 43 % d'entre elles prévoient le déploiement d'appareils connectés dans les douze prochains mois. La plupart des entreprises ne considèrent pas ces initiatives comme des essais, mais bien comme faisant partie d'un déploiement stratégique à part entière.
Cette situation va considérablement empirer. L'un des principaux défis de l'IdO n'est pas lié à la sécurisation de ces appareils par les entreprises, mais plutôt au fait que les fabricants livrent des appareils intrinsèquement vulnérables : soit ils sont trop souvent livrés avec des mots de passe par défaut qui n'ont pas besoin d'être modifiés par les utilisateurs, soit la communication avec les appareils ne requiert pas une authentification de niveau suffisant ; ou encore, les mises à jour des firmwares s'exécutent sans vérification adéquate des signatures. Et la liste des défauts de ces appareils n'en finit pas de s'allonger.
Les entreprises continueront d'être touchées par des attaques directement imputables aux vulnérabilités de l'IdO, que ce soit par des attaques par déni de service distribué (attaques DDoS), ou par le biais d'intrusions sur leurs réseaux, rendues possibles par les « faiblesses » inhérentes de l'IdO.

5 : bouleversements de la réglementation…[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 : Les grandes tendances 2017 de la cybersécurité, Le Cercle

---

La Poste livrera ses colis par drones dans le Var

Dans le Var, après deux ans d'essais, La Poste a obtenu de Direction Générale de l'Aviation Civile (DGAC) le droit d'ouvrir une ligne commerciale régulière de 15 km pour la distribution de colis par drones. Elle se situera entre Saint-Maximin-La-Sainte-Baume et Pourrières.…[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 sur cette page.

Réagissez à cet article

La Poste livrera ses colis par drones dans le Var

Dans le Var, après deux ans d'essais, La Poste a obtenu de

Direction Générale de l'Aviation Civile (DGAC) le droit d'ouvrir une ligne commerciale régulière de 15 km pour la distribution de colis par drones. Elle se situera entre Saint-Maximin-La-Sainte-Baume et Pourrières.…[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 sur cette page.

Réagissez à cet article

Android Things , le nouvel OS

pour objets connectés de Google

	Android Things , le nouvel OS pour objets connectés de Google

En 2015, lors de sa conférence annuelle Google I/O, le géant de Mountain View dévoilait Brillo, un système d'exploitation destiné aux objets connectés.

Faute d'une adoption de grande ampleur par la communauté des développeurs, le groupe Internet revient à l'assaut avec un nouvel OS léger baptisé Android Things qui n'est autre qu'une mouture améliorée de Brilllo. En rassemblant leurs compétences, **Google** et de Qualcomm souhaitent offrir aux développeurs des environnements de connectivité familiers: réseaux cellulaires, Wi-Fi, Bluetooth, prise en charge d'un large éventail de capteurs, caméras, cartes graphiques, sécurité matérielle, services **Google**, intégration du Cloud, etc. Jeffery Torrance, vice-président du développement des affaires de Qualcomm Technologies, a déclaré que « depuis le lancement du premier téléphone Android, Qualcomm et **Google** ont collaboré étroitement pour créer de nouvelles opportunités intéressantes pour les développeurs de mobiles, de portables et d'IoT ». Aujourd'hui le projet est beaucoup plus abouti et **Android Things** est accompagné d'Android Studio, des services **Google** Play, de la **Google** Cloud Platform et du SDK Android. **Google** fait remarquer qu'il existe déjà du hardware pour cela: **Android Things** est compatible avec Intel Edison, NXP Pico et Raspberry Pi 3.

Weave, bientôt sur Android et. iOS!

Il s'agit également d'un système d'exploitation temps réel (RTOS), domaine où la concurrence est rude avec une myriade d'alternatives: Contiki (disponible gratuitement sous licence BSD) et TinyOS.La firme annonce avoir aussi mis à jour sa plateforme Weave permettant aux objets connectés déjà sur le marché de profiter de ses services, à l'instar de **Google** Assistant.
Pour rappel, Weave fournit l'infrastructure cloud qui permet de relier les objets connectés entre eux et à Internet.
Dans un effort d'harmonisation des approches de standardisation, l'Open Interconnect Consortium et l'AllSeen Alliance regroupent des myriades de sociétés IT accompagner l'essor de l'IoT. Le kit de développement (SDK) Weave Device vient d'être introduit.

Réagissez à cet article

Original de l'article mis en page : Google présente son nouvel OS pour objets connectés – Android Things

JT 20H – La Poste se lance dans la livraison par drones

JT 20H – La Poste se lance dans la livraison par drones

JT 20H – Après près de deux ans de tests, La Poste a décidé de faire un grand pas vers l'avant dans son mode de livraison en adoptant la livraison par drones.…[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 sur cette page.

Réagissez à cet article

Cybercriminalité en région : une victime raconte son « traumatisme »

Cybercriminalité en région : une victime raconte son « traumatisme »

La lutte contre la cybercriminalité se joue aussi en région. Parmi les victimes de ces nouvelles pratiques de fraude numérique, des particuliers mais aussi des entreprises. Bruno a récemment vécu une attaque informatique dans son agence immobilière à Lunel. Il raconte.

C'était il y a un mois, au retour d'un week-end. Bruno rouvre son agence immobilière et se retrouve sans téléphone. La société qui gère son système de téléphonie déportée le prévient alors : « Nous vous avons coupé parce que nous nous sommes rendu compte qu'il y avait un problème. » Les lignes de l'entreprise ont en fait été victimes durant le week-end d'un hacker. Lequel a pu se brancher sur ses lignes et les a dirigées vers un service surtaxé au lieu du bas prix initial choisi par le chef d'entreprise et son opérateur.

« Et s'ils avaient pris nos fichiers ? »

Repérée très rapidement, la fraude n'aura eu que peu d'incidence financière : « 300 à 400 euros de téléphone volé, précise Bruno. Mais c'est un véritable traumatisme ! Quand j'ai appris ça, il y a eu dix minutes de flottement, où je me suis posé beaucoup de questions ! Ce n'est pas tant ce qu'ils m'ont volé, mais ce qu'ils auraient pu faire. Ils ont pu rentrer. Et s'ils avaient pris nos fichiers ? Quasiment toutes nos données sont informatisées… Ils peuvent foutre en l'air une entreprise ! » Cinq cents dossiers de propriétaires et leur historique, toute la comptabilité de l'agence…

Bruno a immédiatement porté plainte à la gendarmerie de Lunel. « Ils ont un super-service. Ils ont été à l'écoute, ont pris le problème au sérieux et très rapidement, ils sont remontés jusqu'à la source, dans un pays lointain. Vers Israël, je crois. Ils ont retrouvé le hacker, même s'il est impossible d'aller le chercher. Vous vous rendez compte de ce que ces gens sont capables de faire ! » Et de saluer le travail d'investigations des militaires.

« Les gens paient. Ils n'ont pas d'autre choix. »

Ces derniers rencontrent d'ailleurs souvent ce type de piratage des autocom ces derniers temps, avec des montants qui peuvent s'envoler à plusieurs dizaines de milliers d'euros si la fraude n'est pas détectée assez tôt. Bruno, lui, a finalement été remboursé par son opérateur. Il a renforcé son système de façon simple.

Ce qui n'empêche pas l'inquiétude de se retrouver un jour avec ses données prises en otage ou chiffrées… « J'ai plusieurs collègues qui ont répondu à des e-mails et qui se sont retrouvés victimes d'un chantage. Les gens paient. Ils n'ont pas d'autre choix » explique-t-il…[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 : Cybercriminalité en région : une victime raconte son « traumatisme »

Prévisions cybercriminalité pour 2017

Prévisions cybercriminalité pour 2017

Nous sommes tombés sur cet article sur le site Internet « Informaticien.be » et n'avons pas pu nous empêcher de le partager avec vous tant il est en accord avec les prévisions ressorties de nos analyses. Aux portes de 2017, les entreprises, administrations et association non seulement vont devoir s'adapter à une réglementation Européenne risquant s'impacter lourdement la réputation des établissements qui devront signaler à la CNIL qu'elle viennent d'être victime de piratage, mais également, l'évolution des techniques de piratage vont augmenter les risques qu'auront les organismes à se faire pirater leurs systèmes informatiques. N'hésitez pas à consulter notre page consacrée aux bons conseils que nous prodiguons depuis de nombreuses années sur https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles.
Denis JACOPINI

Trend Micro présente son rapport annuel des prévisions en matière de sécurité: 'The Next Tier – 8 Security Predictions for 2017'. L'année prochaine sera marquée par des attaques de plus grande envergure à tous les niveaux. Les cybercriminels adopteront des tactiques différentes pour tirer parti de l'évolution du paysage technologique.
« Nous pensons que la General Data Protection Regulation (GDPR) va non seulement changer fondamentalement la manière dont les entreprises gèrent leurs données, mais aussi induire de nouvelles méthodes d'attaque. La tactique du ransomware va également s'étendre pour toucher plus d'appareils, tandis que la cyberpropagande influencera de plus en plus l'opinion publique", déclare Raimund Genes, CTO de Trend Micro.
En 2016, l'on a assisté à une formidable augmentation des vulnérabilités d'Apple avec pas moins de 50 fuites. A cela s'ajoutent 135 bugs Adobe et 76 bugs Microsoft. Alors que Microsoft continue d'améliorer ses facteurs limitatifs et qu'Apple est de plus en plus considéré comme le système d'exploitation prépondérant, ce déplacement apparent des 'exploits' des logiciels vulnérables va encore s'accentuer en 2017.
L'IoT et l'IIoT – dans la ligne de mire des attaques ciblées
L'Internet of Things (IoT – internet des objets) et l'Industrial Internet of Things (IioT – internet industriel des objets) seront de plus en plus dans la ligne de mire des attaques ciblées en 2017. Ces attaques tirent parti de l'engouement croissant suscité par les appareils connectés en exploitant les failles et les systèmes non protégés et en perturbant des processus d'entreprise. L'usage croissant d'appareils mobiles pour surveiller les systèmes de production dans les usines et les milieux industriels, combiné au nombre important de vulnérabilités dans ces systèmes constitue une réelle menace pour les organisations.
Explosion de l'extorsion professionnelle
Le Business E-mail Compromise (BEC) et le Business Process Compromise (BPC) représentent de plus en plus une forme relativement simple et économiquement rentable d'extorsion professionnelle. En incitant un employé innocent à verser de l'argent sur le compte bancaire d'un criminel, une attaque BEC peut rapporter 140.000 dollars. Bien que le piratage direct d'un système de transaction financière exige plus d'efforts, cela représente une manne de pas moins de 81 millions de dollars pouvant tomber aux mains des criminels.
Autres faits marquants du rapport
Le nombre de nouvelles familles de ransomware ne progresse que de 25 %. Mais le ransomware s'étend désormais aux appareils IoT et aux terminaux informatiques autres que les desktops (par exemple les systèmes POS ou les distributeurs automatiques).
Les fournisseurs ne parviendront pas à protéger à temps les appareils IoT et IIoT pour éviter des attaques DoS (refus de service) ou d'autres types d'attaques.
Le nombre de failles découvertes dans les technologies Apple et Adobe augmente, ce qui vient s'ajouter aux « exploit-kits ».
46 pour cent de la population mondiale est aujourd'hui reliée à l'internet : la cyberpropagande ne va cesser d'augmenter, à présent que les nouveaux dirigeants des grands pays sont en place. L'opinion publique risque donc d'être influencée par de fausses informations.
Comme ce fut le cas lors de l'attaque de la Banque du Bangladesh plus tôt cette année, les cybercriminels parviennent à modifier des processus d'entreprise via des attaques BPC, et à en tirer largement profit. Les attaques BEC restent d'actualité pour extorquer des fonds à des employés qui ne se doutent de rien.
Le GDPR produira des changements de politique et administratifs qui auront un lourd impact sur les coûts. Cela exigera aussi des examens complexes des processus de données pour assurer la conformité réglementaire.
De nouvelles méthodes d'attaques ciblées déjoueront les techniques de détection modernes, permettant aux criminels de s'attaquer à différentes organisations.
Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

---

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 : Le ransomware s’étend aux appareils connectés et à l’internet des objets – Press Releases – Informaticien.be

---

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 centaine 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]

Réagissez à cet article

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

Ballons, satellites, drones… Comment les milliardaires du web vont connecter le monde

Ballons, satellites, drones… Comment les milliardaires du web vont connecter le monde

Des connexions à très haut débit qui tomberaient du ciel, c'est presque un conte de fées pour quiconque habite dans un secteur où la 3G passe à peine et où l'ADSL arrive en bout de course.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.

Réagissez à cet article