La réalité virtuelle utilisée pour décrypter les scènes de crime

	La réalité virtuelle utilisée pour décrypter les scènes de crime

La gendarmerie a développé une technique permettant de naviguer dans une scène de crime numérisée à l'aide d'un scanner laser.

Après le jeu vidéo, la réalité virtuelle va-t-elle bousculer la Justice ? En mai dernier, l'université de Staffordshire au Royaume-Uni a commencé à utiliser des casques de réalité virtuelle pour plonger les jurés sur des scènes de crimes recréées en trois dimensions. Enfiler le casque permet de se projeter dans une scène et de s'y déplacer.

« **Nous voulons trouver la meilleure solution pour aider le système de justice pénale en aidant les jurés à mieux comprendre ces crimes », explique le médecin légiste Caroline Sturdy Colls, à la BBC.**

L'expérimentation a donné des idées à l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN), qui vient de développer la même technique de déplacement dans des scènes de crimes numérisées en réalité virtuelle. Disposant déjà d'outils de numérisation, l'institut est désormais capable de l'exporter pour le visionner en réalité virtuelle sur un casque embarquant un smartphone.

1h30 pour reproduire une scène de crime

Depuis un peu plus de dix ans, l'IRCGN utilise un scanner laser capable de modéliser n'importe quelle scène en trois dimensions. La technique a été utilisée pour la première fois en décembre 2006, sur les lieux d'un carambolage monstre en Vendée qui avait impliqué une quarantaine de véhicules. Depuis, il revient de plus en plus sur des scènes d'accidents mais aussi de crimes.

Le scanner laser – le Focus 3D de la marque allemande Faro – permet de numériser une scène d'un premier point de vue en 2 à 5 minutes, en fonction de s'il capte (ou non) les couleurs. Pour reproduire l'intégralité d'un lieu et des éléments présents, les spécialistes de la gendarmerie doivent effectuer entre 10 et 90 scans.

« Il nous faut environ une heure et demi pour reproduire une scène », explique le chef d'escadron Christophe Lambert. « C'est beaucoup plus rapide que de réaliser des croquis, et cela permet ensuite de retrouver tous les détails, avec une précision de 3 mm à 25 m. »

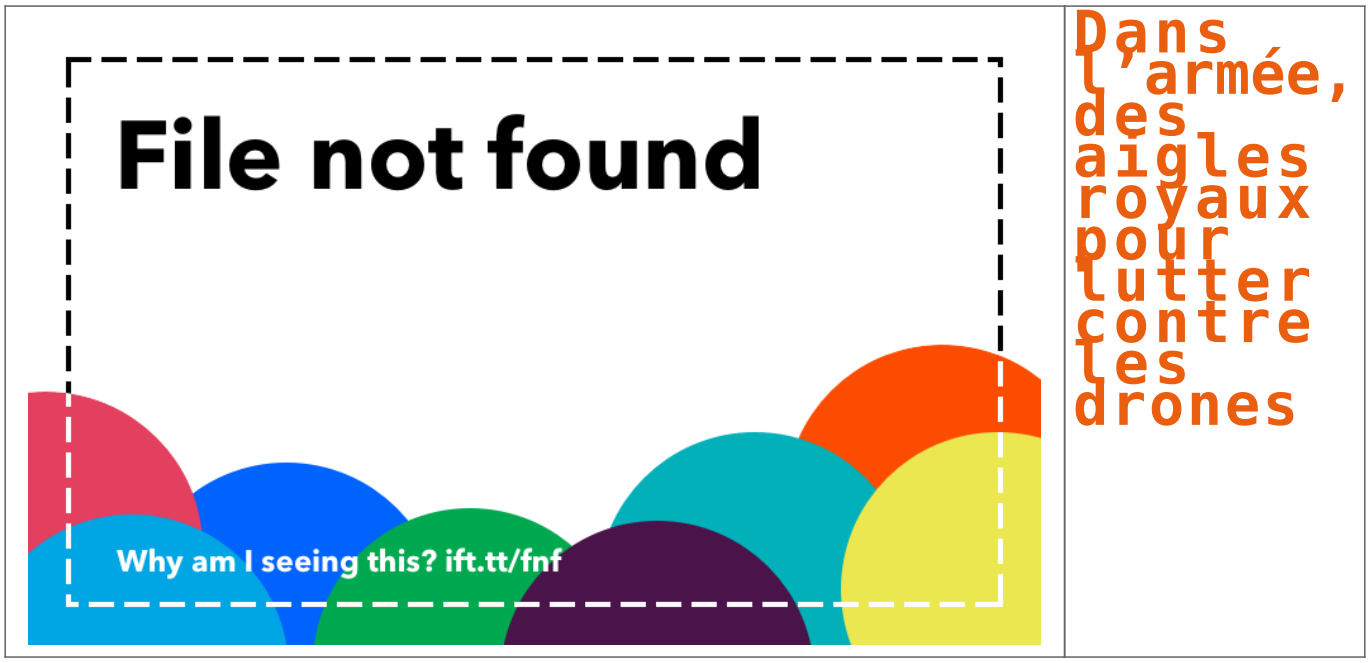
Sur son ordinateur, le gendarme montre le rendu d'une scène de crime dans un garage, scène qu'il est possible de visionner sous n'importe quel angle, où l'on peut se déplacer numériquement mais aussi de zoomer sur des détails (un tournevis qui traîne, un étui négligé au sol, etc.)…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : La réalité virtuelle, nouvel outil pour décrypter les scènes de crime

---

Dans l'armée, des aigles royaux pour lutter contre les drones



Des soldats d'un nouveau genre… A l'occasion de ses vœux aux Armées, vendredi, François Hollande a pu se glisser dans la peau d'un dresseur d'aigles. Depuis le mois de septembre, ces rapaces sont en effet utilisés par l'Armée de l'Air pour lutter contre les 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

Parapluie, pommeau de douche et diffuseur d'odeurs… Ces objets connectés pour faciliter le quotidien

Parapluie, pommeau de douche et diffuseur d'odeurs… Ces objets connectés pour faciliter le quotidien

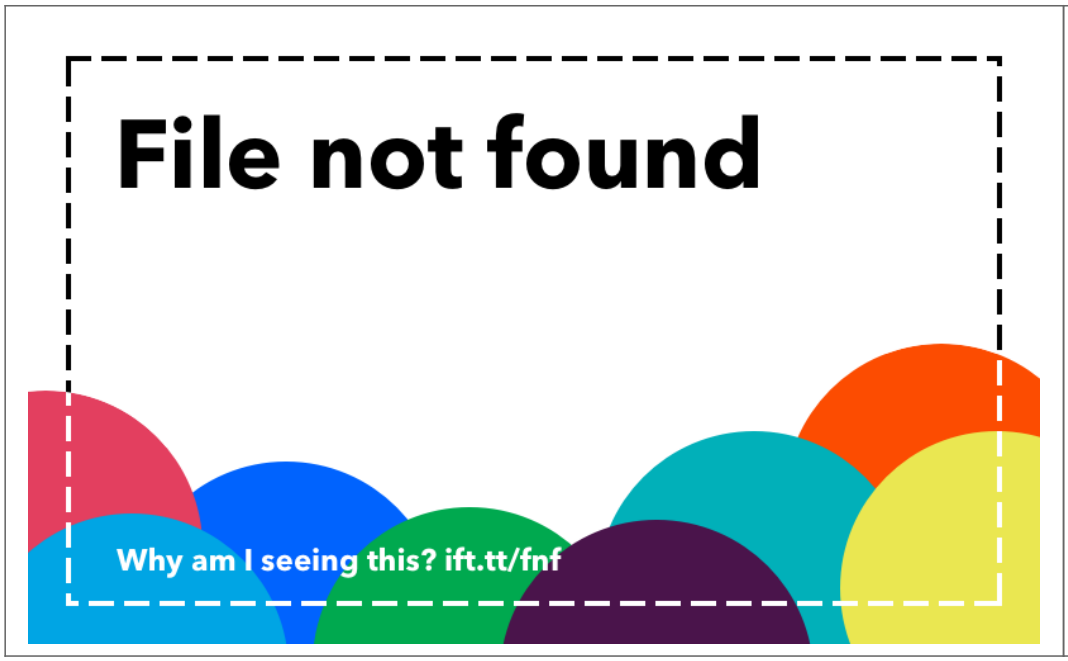
Des odeurs pour nous aider à mieux dormir, un parapluie connecté ou encore un pommeau de douche pensé pour responsabiliser son utilisateurs sur sa consommation

d’eau……[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

Dans l’armée, des aigles royaux pour lutter contre les drones



Dans l'armée, des aigles royaux pour lutter contre les drones

Des soldats d'un nouveau genre… A l'occasion de ses vœux aux Armées, vendredi, François Hollande a pu se glisser dans la peau d'un dresseur d'aigles. Depuis le mois de septembre, ces rapaces sont en effet utilisés par l'Armée de l'Air pour lutter contre les 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

Ça y est, les ransomwares qui désactivent les téléviseurs connectés arrivent !

Ça y est, les ransomwares qui désactivent les téléviseurs connectés arrivent !

L’infection d’un téléviseur LG par un malware, racontée sur Twitter par un ingénieur informatique, rappelle la vulnérabilité des téléviseurs connectés face à ces logiciels malveillants. Et la difficulté de s’en débarrasser.

Les réserves des experts en sécurité informatique au sujet des téléviseurs connectés fonctionnant avec Android, qui seraient vulnérables aux mêmes malwares que ceux diffusés sur les smartphones, remontent à loin. L’incident raconté par Darren Cauthon prouve que ces craintes étaient justifiées.

À Noël, cet ingénieur informatique a découvert que le téléviseur connecté LG de l’un de ses proches était victime d’un ransomware que l’on trouve plus communément sur smartphone. Ce dernier est connu sous le nom de Cyber.Police, FLocker, Frantic Locker ou encore Dogspectus.

Le téléviseur aurait été infecté par une application de streaming. À la moitié du film, l’appareil s’est arrêté pour finalement rester bloqué sur la page d’accueil du ransomware. L’ingénieur ne sait néanmoins pas si l’application venait du PlayStore ou d’un tiers. Ce qui pourrait, dans le cas d’une application de piratage, expliquer que le ransomware se soit introduit si facilement sur le téléviseur.

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 : Un ransomware désactive un téléviseur connecté LG — Tech — Numerama

---

100 000 emplois en Tunisie grâce aux smart-cities et

objets connectés

100 000 emplois en Tunisie grâce aux smart-cities et objets connectés

La Tunisie se met au numérique pour son développement économique. Avec la régression de l'une des principales sources de revenu qu'est le tourisme, la Tunisie ambitionne d'optimiser son économie avec le projet « Tunisie Numérique 2020 ».
Le numérique, dans l'économie de la Tunisie, représente déjà 11% de taux de croissance annuelle et 7% du PIB, devant le secteur du tourisme. Avec les initiatives privées, le gouvernement travail à faire progresser ce chiffre.
« C'est la première fois que le secteur public se dit : « Je ne vais pas tout faire tout seul et il y a des secteurs que je connais mal », « De notre côté, nous sommes conscients qu'après la révolution, le rôle de la société civile devient plus important et c'est pourquoi nous mettons notre savoir-faire au service de la Tunisie », a expliqué l'entrepreneur, éditeur du logiciel Badredine Ouali, qui préside également le partenariat public-privé Smile Tunisia.
D'ici 2020, le gouvernement tunisien vise créer 100 000 emplois en misant sur les smart-cities ou les objets connectés.

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

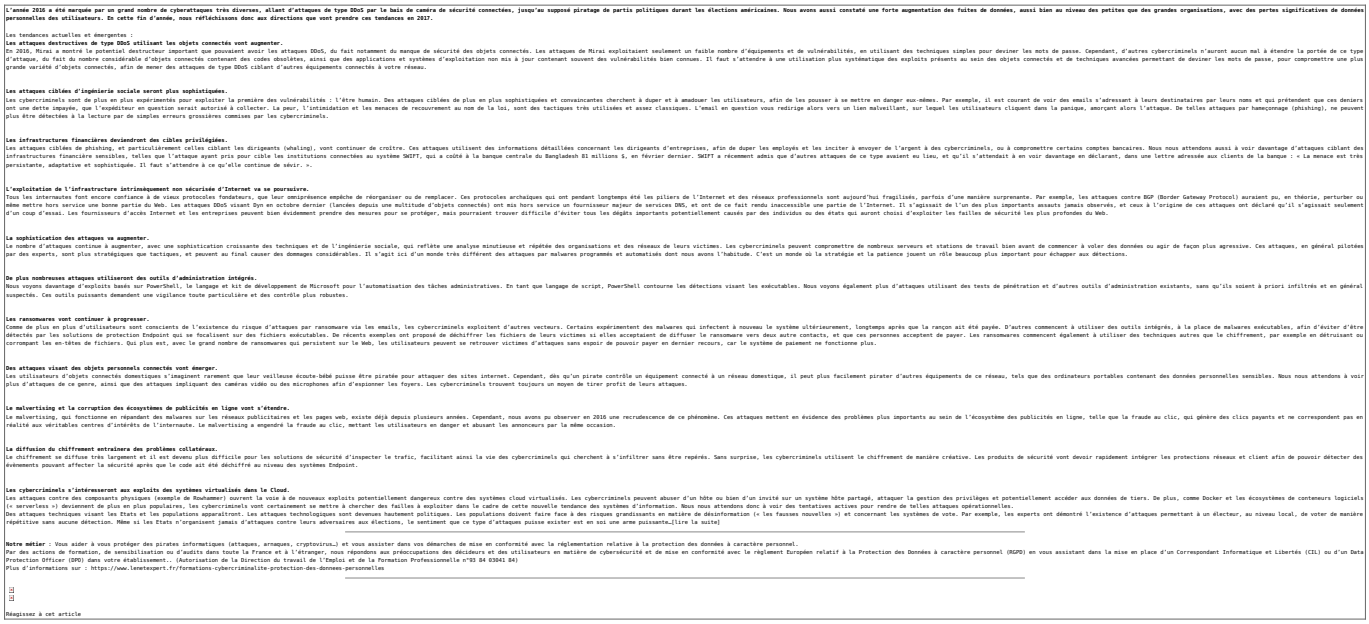
---

Réagissez à cet article

Original de l'article mis en page : Tunisie: 100 000 emplois grâce aux smart-cities et objets connectés | Africa Top Success

Tendances actuelles et émergentes pour la cybersécurité en 2017

	Tendances actuelles et émergentes pour la cybersécurité en 2017



L'année 2016 a été marquée par un grand nombre de cyberattaques très diverses, allant d'attaques de type DDoS par le bais de caméra de sécurité connectées, jusqu'au supposé piratage de partis politiques durant les élections américaines. Nous avons aussi constaté une forte augmentation des fuites de données, aussi bien au niveau des petites que des grandes organisations, avec des pertes significatives de données personnelles des utilisateurs. En cette fin d'année, nous réfléchissons donc aux directions que vont prendre ces tendances en 2017.

Les tendances actuelles et émergentes :

Les attaques destructives de type DDoS utilisant les objets connectés vont augmenter.

En 2016, Mirai a montré le potentiel destructeur important que pouvaient avoir les attaques DDoS, du fait notamment du manque de sécurité des objets connectés. Les attaques de Mirai exploitaient seulement un faible nombre d'équipements et de vulnérabilités, en utilisant des techniques simples pour deviner les mots de passe. Cependant, d'autres cybercriminels n'auront aucun mal à étendre la portée de ce type d'attaque, du fait du nombre considérable d'objets connectés contenant des codes obsolètes, ainsi que des applications et systèmes d'exploitation non mis à jour contenant souvent des vulnérabilités bien connues. Il faut s'attendre à une utilisation plus systématique des exploits présents au sein des objets connectés et de techniques avancées permettant de deviner les mots de passe, pour compromettre une plus grande variété d'objets connectés, afin de mener des attaques de type DDoS ciblant d'autres équipements connectés à votre réseau.

Les attaques ciblées d'ingénierie sociale seront plus sophistiquées.

Les cybercriminels sont de plus en plus expérimentés pour exploiter la première des vulnérabilités : l'être humain. Des attaques ciblées de plus en plus sophistiquées et convaincantes cherchent à duper et à amadouer les utilisateurs, afin de les pousser à se mettre en danger eux-mêmes. Par exemple, il est courant de voir des emails s'adressant à leurs destinataires par leurs noms et qui prétendent que ces derniers ont une dette impayée, que l'expéditeur en question serait autorisé à collecter. La peur, l'intimidation et les menaces de recouvrement au nom de la loi, sont des tactiques très utilisées et assez classiques. L'email en question vous redirige alors vers un lien malveillant, sur lequel les utilisateurs cliquent dans la panique, amorçant alors l'attaque. De telles attaques par hameçonnage (phishing), ne peuvent plus être détectées à la lecture par de simples erreurs grossières commises par les cybercriminels.

Les infrastructures financières deviendront des cibles privilégiées.

Les attaques ciblées de phishing, et particulièrement celles ciblant les dirigeants (whaling), vont continuer de croitre. Ces attaques utilisent des informations détaillées concernant les dirigeants d'entreprises, afin de duper les employés et les inciter à envoyer de l'argent à des cybercriminels, ou à compromettre certains comptes bancaires. Nous nous attendons aussi à voir davantage d'attaques ciblant des infrastructures financière sensibles, telles que l'attaque ayant pris pour cible les institutions connectées au système SWIFT, qui a coûté à la banque centrale du Bangladesh 81 millions $, en février dernier. SWIFT a récemment admis que d'autres attaques de ce type avaient eu lieu, et qu'il s'attendait à en voir davantage en déclarant, dans une lettre adressée aux clients de la banque : « La menace est très persistante, adaptative et sophistiquée. Il faut s'attendre à ce qu'elle continue de sévir. ».

L'exploitation de l'infrastructure intrinsèquement non sécurisée d'Internet va se poursuivre.

Tous les internautes font encore confiance à de vieux protocoles fondateurs, que leur omniprésence empêche de réorganiser ou de remplacer. Ces protocoles archaïques qui ont pendant longtemps été les piliers de l'Internet et des réseaux professionnels sont aujourd'hui fragilisés, parfois d'une manière surprenante. Par exemple, les attaques contre BGP (Border Gateway Protocol) auraient pu, en théorie, perturber ou même mettre hors service une bonne partie du Web. Les attaques DDoS visant Dyn en octobre dernier (lancées depuis une multitude d'objets connectés) ont mis hors service un fournisseur majeur de services DNS, et ont de ce fait rendu inaccessible une partie de l'Internet. Il s'agissait de l'un des plus importants assauts jamais observés, et ceux à l'origine de ces attaques ont déclaré qu'il s'agissait seulement d'un coup d'essai. Les fournisseurs d'accès Internet et les entreprises peuvent bien évidemment prendre des mesures pour se protéger, mais pourraient trouver difficile d'éviter tous les dégâts importants potentiellement causés par des individus ou des états qui auront choisi d'exploiter les failles de sécurité les plus profondes du Web.

La sophistication des attaques va augmenter.

Le nombre d'attaques continue à augmenter, avec une sophistication croissante des techniques et de l'ingénierie sociale, qui reflète une analyse minutieuse et répétée des organisations et des réseaux de leurs victimes. Les cybercriminels peuvent compromettre de nombreux serveurs et stations de travail bien avant de commencer à voler des données ou agir de façon plus agressive. Ces attaques, en général pilotées par des experts, sont plus stratégiques que tactiques, et peuvent au final causer des dommages considérables. Il s'agit ici d'un monde très différent des attaques par malwares programmés et automatisés dont nous avons l'habitude. C'est un monde où la stratégie et la patience jouent un rôle beaucoup plus important pour échapper aux détections.

De plus nombreuses attaques utiliseront des outils d'administration intégrés.

Nous voyons davantage d'exploits basés sur PowerShell, le langage et kit de développement de Microsoft pour l'automatisation des tâches administratives. En tant que langage de script, PowerShell contourne les détections visant les exécutables. Nous voyons également plus d'attaques utilisant des tests de pénétration et d'autres outils d'administration existants, sans qu'ils soient à priori infiltrés et en général suspectés. Ces outils puissants demandent une vigilance toute particulière et des contrôle plus robustes.

Les ransomwares vont continuer à progresser.

Comme de plus en plus d'utilisateurs sont conscients de l'existence du risque d'attaques par ransomware via les emails, les cybercriminels exploitent d'autres vecteurs. Certains expérimentent des malwares qui infectent à nouveau le système ultérieurement, longtemps après que la rançon ait été payée. D'autres commencent à utiliser des outils intégrés, à la place de malwares exécutables, afin d'éviter d'être détectés par les solutions de protection Endpoint qui se focalisent sur des fichiers exécutables. De récents exemples ont proposé de déchiffrer les fichiers de leurs victimes si elles acceptaient de diffuser le ransomware vers deux autre contacts, et que ces personnes acceptent de payer. Les ransomwares commencent également à utiliser des techniques autres que le chiffrement, par exemple en détruisant ou corrompant les en-têtes de fichiers. Qui plus est, avec le grand nombre de ransomwares qui persistent sur le Web, les utilisateurs peuvent se retrouver victimes d'attaques sans espoir de pouvoir payer en dernier recours, car le système de paiement ne fonctionne plus.

Des attaques visant des objets personnels connectés vont émerger.

Les utilisateurs d'objets connectés domestiques s'imaginent rarement que leur veilleuse écoute-bébé puisse être piratée pour attaquer des sites internet. Cependant, dès qu'un pirate contrôle un équipement connecté à un réseau domestique, il peut plus facilement pirater d'autres équipements de ce réseau, tels que des ordinateurs portables contenant des données personnelles sensibles. Nous nous attendons à voir plus d'attaques de ce genre, ainsi que des attaques impliquant des caméras vidéo ou des microphones afin d'espionner les foyers. Les cybercriminels trouvent toujours un moyen de tirer profit de leurs attaques.

Le malvertising et la corruption des écosystèmes de publicités en ligne vont s'étendre.

Le malvertising, qui fonctionne en répandant des malwares sur les réseaux publicitaires et les pages web, existe déjà depuis plusieurs années. Cependant, nous avons pu observer en 2016 une recrudescence de ce phénomène. Ces attaques mettent en évidence des problèmes plus importants au sein de l'écosystème des publicités en ligne, telle que la fraude au clic, qui génère des clics payants et ne correspondent pas en réalité aux véritables centres d'intérêts de l'internaute. Le malvertising a engendré la fraude au clic, mettant les utilisateurs en danger et abusant les annonceurs par la même occasion.

La diffusion du chiffrement entrainera des problèmes collatéraux.

Le chiffrement se diffuse très largement et il est devenu plus difficile pour les solutions de sécurité d'inspecter le trafic, facilitant ainsi la vie des cybercriminels qui cherchent à s'infiltrer sans être repérés. Sans surprise, les cybercriminels utilisent le chiffrement de manière créative. Les produits de sécurité vont devoir rapidement intégrer les protections réseaux et client afin de pouvoir détecter des évènements pouvant affecter la sécurité après que le code ait été déchiffré au niveau des systèmes Endpoint.

Les cybercriminels s'intéresseront aux exploits des systèmes virtualisés dans le Cloud.

Les attaques contre des composants physiques (exemple de Rowhammer) ouvrent la voie à de nouveaux exploits potentiellement dangereux contre des systèmes cloud virtualisés. Les cybercriminels peuvent abuser d'un hôte ou bien d'un invité sur un système hôte partagé, attaquer la gestion des privilèges et potentiellement accéder aux données de tiers. De plus, comme Docker et les écosystèmes de conteneurs logiciels (« serverless ») deviennent de plus en plus populaires, les cybercriminels vont certainement se mettre à chercher des failles à exploiter dans le cadre de cette nouvelle tendance des systèmes d'information. Nous nous attendons donc à voir des tentatives actives pour rendre de telles attaques opérationnelles.

Des attaques techniques visant les Etats et les populations apparaîtront. Les attaques technologiques sont devenues hautement politiques. Les populations doivent faire face à des risques grandissants en matière de désinformation (« les fausses nouvelles ») et concernant les systèmes de vote. Par exemple, les experts ont démontré l'existence d'attaques permettant à un électeur, au niveau local, de voter de manière répétitive sans aucune détection. Même si les Etats n'organisent jamais d'attaques contre leurs adversaires aux élections, le sentiment que ce type d'attaques puisse exister est en soi une arme puissante…[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 : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 — Global Security Mag Online

---

Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

La dernière étude dIFS sur les défis auxquels les DSI sont confrontés durant la période des fêtes de fin d'années révèle que 76% des sondés se sentent davantage préoccupés à l'approche de cette période et ce, pour plusieurs raisons : la disponibilité du personnel (41% des répondants), les risques de piratage liés à la sécurité IT (31%) ainsi que les besoins IT des collaborateurs travaillant à distance (31% également). Tout cela a un impact certain sur les processus et activités métier.

De tous, les plus inquiets quant à la disponibilité du personnel à la période des fêtes de fin d'année sont les français. 62% d'entre eux déclarent qu'il s'agit de l'une de leurs plus grandes préoccupations au cours de la saison des fêtes de fin d'année. Á l'opposé, près de la moitié des répondants américains (48%) citent le piratage informatique.

Du côté des « besoins », 42% des décideurs IT sont en demande d'un budget plus important. La migration vers le Cloud (18%) et le recrutement de personnel IT (16%) sont également cités dans le top 3 de leurs besoins. Par ailleurs, un quart des répondants américains et suédois (respectivement 26% et 25%) souhaitent, à court terme, une accélération de la migration vers le Cloud, alors qu'ils ne sont que 11% et 14% en Australie et Allemagne à privilégier cet enjeu.

« Ce qui ressort clairement de notre étude est que de nombreux décideurs IT ont des craintes légitimes pour la période des fêtes de fin d'année : disponibilité du personnel, risque de piratage informatique, commente Mark Boulton, CMO d'IFS. Il est essentiel que toutes les entreprises, quelle que soit leur taille, se préparent à affronter les problèmes qui pourraient survenir et soient en mesure d'accompagner, à distance, leurs collaborateurs ». L'IoT et la migration vers le Cloud faisant partie des solutions possibles.

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 : Pourquoi les DSI sont-ils inquiets à lapproche des Fêtes de fin dannée ?

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