

Phishing, repérez les faux mails et déjouez les pièges des pirates



Phishing,
repérez
les faux
mails et
déjouez
les
pièges
des
pirates

Le phishing, ou hameçonnage, a pour but de vous dérober vos données personnelles en douceur, au moyen d'un simple courriel ou d'un faux site Web, depuis un ordinateur ou un mobile. Voici quelques conseils et outils pour mieux vous protéger.

Faites appel à votre bon sens et restez sur vos gardes

Lorsque vous recevez un mail censé provenir d'un portail gouvernemental ou bancaire, demandez-vous pourquoi vous le recevez et scrutez attentivement cette correspondance avant de cliquer sur le moindre lien ! Examinez l'intitulé et surtout l'adresse de l'expéditeur. Impensable que le centre des impôts vous écrive avec une adresse @free.fr ! L'inspection des éventuelles fautes d'orthographe et l'exactitude de vos infos personnelles doivent également susciter la méfiance.

En cas de doute sur l'authenticité du message reçu de votre banque ou d'un organisme officiel, prenez le temps de le contacter par téléphone. Sachez en outre que les grandes entreprises disposent de plus en plus souvent de services dédiés à la protection des données de leurs clients. Certaines proposent même depuis leur site Internet de transmettre le mail suspect ou frauduleux, c'est le cas chez EDF notamment...[lire la suite]

Denis JACOPINI : Face au développement incoercible de la cybercriminalité, suivez **nos formations** pour anticiper les prochains piratages et prochaines arnaques dont vous risquez bien de vous retrouver la cible. Nous partons du principe que le meilleur moyen de se protéger des pirates, c'est non seulement de connaître leur mode opératoire mais de **savoir reconnaître les symptômes**.

Découvrez nos nouvelles formations : les 30 plus dangereuses arnaques sur Internet

NOTRE MÉTIER :

- FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
- EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
- AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
- MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



Contactez-nous

Réagissez à cet article

Source : *Phishing, repérez les faux mails et déjouez les pièges des pirates – SFR News*

Cybersécurité : les 10 chiffres qui font peur – Silicon

x	Cybersécurité : les 10 chiffres qui font peur
---	--

L'explosion du trafic Internet et des activités numériques est un progrès incontestable. Mais il fait aussi courir des risques grandissants en matière de sécurité. La preuve avec ces dix exemples, qui doivent alerter sur les mesures à prendre.

3 minutes pour pirater un nouvel objet connecté

Caméras de surveillance, imprimantes, thermostats intelligents... Les milliards d'objets reliés au web sont extrêmement mal sécurisés. Les utilisateurs omettent la plupart du temps de changer le mot de passe par défaut et, d'autre part, les fabricants n'intègrent pas de réel système de sécurité dans leurs dispositifs. Résultat : moins de 3 minutes sont nécessaires à un hacker pour prendre le contrôle d'un objet connecté, selon l'éditeur de sécurité ForeScout, partenaire de Malwarebytes.

1,1 million de victimes de fraude à la carte bancaire par an

Le nombre de ménages victimes d'une fraude à la carte bancaire a plus que doublé en 5 ans, passant de 500.000 en 2011 à 1,1 million en 2015,...[lire la suite]

+83 % de smartphones infectés au 2e semestre 2016

65 vols de données par seconde

41 % : le taux de succès d'un ransomware

201 jours pour découvrir une cyberattaque

1,7 milliard de publicités fraudueuses en 2016

140 attaques de phishing par heure

Les particuliers deux fois plus infectés que les professionnels

Une entreprise subit 29 cyberattaques par an

[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Cybersécurité : les 10 chiffres qui font peur* –

Faire face aux cyberattaques

	Faire face aux cyberattaques
---	-------------------------------------

Notre niveau de défense informatique doit se hisser au niveau d'expertise des attaquants. Il faut veiller à la sensibilisation des salariés et des citoyens.

WannaCry et Pethia prouvent que nous entrons dans l'ère de la cyberguerre marquée par la volonté des pirates de nuire pour nuire sans forcément chercher à extorquer des rançons. Le scénario actuel avait été anticipé par l'Etat français. La création de l'Agence nationale de la sécurité des systèmes d'information, dès 2009, démontre qu'en France, nous étions pionniers. Nous savions que plus la technologie progressait, plus l'entrée en cyberguerre était inévitable.

Certains minimisaient les risques. Ils se plaisaient à rappeler que le «bug de l'an 2000» n'avait été qu'une grande peur médiatique. Aujourd'hui, ils constatent que nous avons face à nous des prédateurs déterminés. Les assauts digitaux ne touchent pas seulement les PME réputées plus fragiles. Lorsque l'on veut nuire, le plus efficace n'est-il pas de s'attaquer à des grandes entreprises qui rendent des services essentiels aux citoyens ?

Aucune entreprise n'est épargnée...[lire la suite]

NOTRE MÉTIER :

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
 - **MISE EN CONFORMITE RGPD / FORMATION DPO**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS


: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Faire face aux cyberattaques*

**FIC 2018 les 23 et 24 janvier
à Lille : à l'ère de
l'hyperconnexion, comment
s'organise la cyber-
résilience ?**

	FIC 2018 les 23 et 24 janvier à Lille : à l'ère de l'hyperconnexion, comment s'organise la cyber-résilience ?
---	--

Organisé conjointement par la Gendarmerie Nationale, CEIS et EuraTechnologies, et co-financé par la Région Hauts-de-France, la 10^è édition du Forum International de la Cybersécurité entre dans l'ère de l'hyperconnexion.

« Les individus et les machines sont connectés en permanence et communiquent sans discontinuer entre eux et les uns avec les autres. Cette imbrication de réseaux expose le système aux effets dominos sur l'une de ses composantes et pose d'abord la question de la résilience, c'est à dire la capacité du système à faire face aux conséquences d'une attaque ou d'une défaillance sur l'un des maillons de la chaîne, et à récupérer ses aptitudes à opérer normalement. Cette nouvelle configuration bouleverse aussi les modes de fonctionnement et d'organisation de nos sociétés, et nécessitera d'adapter nos comportements, pratiques, technologies de sécurité et corpus législatifs et règlementaires. A l'ère de l'hyperconnexion, la cyber-résilience suppose donc une approche systémique de la sécurité impliquant à la fois les individus, les processus et les techniques » explique le Général Marc Watin-Augouard, fondateur du Forum International de la Cybersécurité...[lire la suite]

Denis JACOPINI :

C'est sur ce thème que le FIC 2018 ouvrira. Conférences, démonstrations, ateliers seront au rendez-vous. Le FIC 2018 est aussi le point de rencontre international des principaux acteurs de la cybersécurité. Donnons-nous donc rendez-vous les 23 et 24 janvier à Lille Grand Palais. Consultez le Pré Programme du FIC 2018 au 02/09/2017.

NOTRE MÉTIER :

FORMATIONS EN CYBERCRIMINALITE / RECHERCHE DE PREUVES / EXPERTISES INFORMATIQUES / AUDITS RGPD / MISE EN CONFORMITE RGPD / FORMATION DPO

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : 23 et 24 janvier Lille – FIC 2018 : à l'ère de l'hyperconnexion, comment s'organise la cyber-résilience ? – Global Security Mag Online

Swidget : Les prises électriques du futur ?

✕	Swidget : Les prises électriques du futur ?
---	---

Et si tout se passait dans la prise électrique ? Telle est la proposition de Swidget, un système de prises modulaires conçu pour la maison connectée. L'opération se termine bientôt sur Kickstarter.

Amazon Echo, Google Home et bientôt Swidget ? Sans être autant ambitieux que les principaux assistants du marché, le système Swidget pourrait représenter une alternative intéressante, **notamment pour ceux qui ont l'âme d'un bricoleur**. On vous explique en détail.

Swidget vous aide à contrôler votre maison intelligente

L'un des principaux défis sur le chemin de la maison connectée, c'est le prix. **Transformer votre domicile en un espace domotique fonctionnel peut se révéler coûteux. Très coûteux.** C'est pour cela que des appareils commencent à apparaître qui permettent de rendre intelligent un espace existant comme les lampes Phillips Hue. Un nouveau venu apparaît dans cette gamme, les prises connectées Swidget.

Visuellement, cela ressemble à une prise classique. Mais, elle a deux avantages. Tout d'abord, elle est connectée, vous pourrez donc y accéder depuis votre smartphone et surveiller par exemple la consommation de vos accessoires un peu trop gourmands. Mais surtout, elle est modulaire. L'espace du milieu peut être adapté selon vos besoins avec **un module Wi-Fi, Z-Wave ou encore détecteur de présence**.

La liste proposée par le fabricant semble très longue. Ceux-ci peuvent ensuite se connecter à des systèmes comme Smartthings, Nest, Google Home, Alexa... Il vous suffit de changer de module pour adapter l'appareil à vos nouveaux besoins.

Un véritable succès sur Kickstarter

L'opération de financement participatif sur Kickstarter est bientôt terminée. Il ne vous reste plus que jusqu'au 1er septembre pour profiter de cette offre lancée le 24 juillet...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Swidget cache votre maison intelligente dans les prises électriques*

Alerte : Facebook Messenger pourrait propager un virus



Alerte : Facebook Messenger pourrait propager un virus

Les applications de messageries instantanées sont souvent la cible de virus informatiques. Facebook Messenger n'a pas échappé à cette règle: selon Le Monde Informatique, un logiciel malveillant (« malware », ndlr) se propage actuellement sur le réseau social. C'est le chercheur David Jacoby, de la société informatique spécialisée dans la sécurité des systèmes d'information, qui a pu détecter ce virus. Le principe est classique: un de vos contacts envoie une vidéo nommée « David Video ». David Jacoby précise au *Monde Informatique*: « Lorsque la victime clique sur la fausse vidéo, le malware redirige vers un éventail de sites énumérant leur navigateur, système d'exploitation et d'autres informations vitales. Selon leur OS, ils sont redirigés vers d'autres sites web ». Ce virus, qui ne menace pas l'appareil en lui-même, peut installer des logiciels malveillants à l'insu de l'utilisateur. En outre, il peut également récupérer les données personnelles...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à votre disposition une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Un virus informatique détecté sur Facebook Messenger*

Plus de 100 000 smartphones Android infectés par un botnet DDoS

	Plus de 100 000 smartphones Android infectés par un botnet DDoS
---	--

Les victimes étaient infectées par des centaines d'applications en apparence inoffensives, diffusées par le Google Play Store.

On ne cesse de le répéter : attention aux applications que vous téléchargez, y compris sur le Google Play Store. Des chercheurs en sécurité viennent de démanteler WireX, un botnet spécialisé en attaques par déni de service distribuées (DDoS) et qui regroupait jusqu'à 120.000 smartphones zombies répartis dans plus de 100 pays. Ce n'est pas la première fois qu'un tel botnet est détecté. En septembre 2016, les chercheurs d'Imperva avait déjà mis le doigt sur un réseau de smartphones Android zombies destiné au DDoS et composé de plus de 26.000 nœuds...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à votre disposition une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Plus de 100 000 smartphones Android esclaves d'un botnet DDoS*

Des hackers utilisent des

spoilers de «Game of Thrones» pour propager un logiciel malveillant

✕	Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant
---	--

En règle générale mieux vaut éviter les spoilers. Surtout, quand ceux-ci proviennent d'un email suspect. D'après un article Proofpoint, une entreprise américaine de cybersécurité, une «campagne d'emails ciblées» qui utilise des spoilers des prochains épisodes de «Game of Thrones» comme appât est actuellement en cours. À la clef, pour les internautes malchanceux qui cliqueraient sur la pièce jointe, un logiciel malveillant.

L'entreprise de cyber-sécurité explique avoir repéré un de ces emails le 10 août dernier, à la suite du piratage de HBO par des hackers. Intitulé «*Vous voulez voir «Game of Thrones» en avance ?*», le courrier contient quelques détails concernant les prochains épisodes de la série ainsi qu'une pièce jointe word contenant un maliciel. Une fois téléchargé, celui-ci tente d'installer un Remote Access Trojan (cheval de Troie à distance) qui est ensuite capable d'envoyer des informations et des données à un serveur.

D'après The Verge, ce genre d'attaque a été associée par le passé avec le gouvernement chinois et il serait possible «*que cette attaque provienne des mêmes acteurs*». Cet email fait suite au hack massif de HBO. La chaîne américaine, qui diffuse «Game of Thrones», s'était fait voler 1,5 To de données en juillet dernier, dont des informations sur la saison de la série. Une demande de rançon avait rapidement suivi ce hack...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant | Slate.fr*

Alerte : Un vidéo infecte votre ordinateur via Facebook Messenger

✕	Alerte : Un vidéo infecte votre ordinateur via Facebook Messenger
---	---

Sur Facebook Messenger, des messages incitant à regarder une vidéo sont envoyés. Ne cliquez surtout pas sur le lien : il s'agit d'un piège qui installera un malware sur votre ordinateur.

Des vidéos piégées sur Facebook Messenger

D'après la société spécialisée dans la sécurité informatique Kaspersky Lab, des messages piégés incitant à regarder une vidéo circulent sur Facebook Messenger. Il s'agirait d'une tactique dont le but serait d'infecter votre ordinateur avec un *malware*.

« Le mécanisme initial de propagation semble être Facebook Messenger, mais nous ne savons toujours pas comment il se propage via Messenger. Il se pourrait que ce soit à partir d'identifiants volés, de navigateurs piratés ou en détournant des clics », a indiqué Kaspersky Lab dans une note de blog.



© Fournis par Clubic Facebook Messenger

Un malware qui cible Windows et macOS

Les pirates informatiques à l'origine de cette attaque ciblent tout autant les ordinateurs tournant sous Windows que ceux tournant sous macOS...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : Facebook Messenger : attention à ce nouveau malware

Intelligence artificielle: y a-t-il un pilote dans la maison ?

<input type="checkbox"/>	Intelligence artificielle: y a-t-il un pilote dans la maison ?
--------------------------	---

C'est un véritable chef d'orchestre qui vient d'arriver dans le secteur des nouvelles technologies. Les assistants personnels commandent les objets connectés, la domotique mais aussi répondent à vos questions. Dernier arrivé en France : Google Home qui allie la puissance de son moteur de recherche à un boîtier qui promet de modifier nos vies à la maison, voire nos habitudes futures avec les nouvelles technologies.

Mais de quoi s'agit-il exactement ? Les boîtiers truffés de micros (des micros ultrasensibles et un système de traitement du langage naturel perfectionné pour Google Home) et d'un haut-parleur sont connectés au Wifi de la maison. Ils vont pouvoir ainsi tirer tout leur potentiel dès que vous les déclenchez avec des mots magiques comme « OK Google » ou « Alexa ».

Vous dialoguez alors en direct avec une intelligence artificielle. Chacune a les caractéristiques de sa marque : Apple, Google, Amazon ou Microsoft. C'est cette dernière qui va s'efforcer de répondre à toutes vos questions ou vos demandes domotiques. Le marché des nouvelles technologies est depuis quelques années dopé par ces intelligences artificielles qui promettent désormais d'intervenir directement dans votre vie de tous les jours...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Intelligence artificielle: y a-t-il un pilote dans la maison?* – Hebdo – RFI