Alerte : Faille Wifi du WPA2. Risques et solutions pour s’en protéger

	Alerte : Faille Wifi du WPA2. Risques et solutions pour s’en protéger

Dévoilée au public lundi 16 octobre 2017, Krack Attacks est une faille qui permet aux pirates d'espionner votre connexion wifi. Que doit-on craindre ? Comment se protéger ? Denis JACOPINI nous apporte des éléments de réponse.

Que doit-on craindre de cette faille découverte dans le WPA2 ?

Mathy Vanhoef, chercheur à l'université KU Leuven, a découvert une faille permettant d'intercepter des données transmises sur un réseau Wi-Fi, même lorsqu'il est protégé par le protocole WPA2. Pire, il est également possible d'injecter des données, et donc des malwares, en utilisant la technique découverte. Les réseaux domestiques aussi bien que les réseaux d'entreprises sont concernés, c'est donc une découverte majeure dans le domaine de la sécurité informatique.

La technique décrite par Mathy Vanhoef est appelée Key Reinstallation AttaCK, ce qui donne KRACK.

Comment se protéger de cette faille ?

Il n'y a pas de meilleur protocole que le WPA2. Il ne faut surtout pas revenir au protocole WEP. Changer de mot de passe ne sert à rien non plus. Le seul moyen de se protéger de cette faille est de mettre à jour votre système d'exploitation et les appareils concernés. Les acteurs du marché, fabricants ou éditeurs, ont été notifiés de cette faille le 14 juillet 2017. Certains l'ont comblée par avance comme Windows.

Il faut combler la faille à la fois sur les points d'accès et sur les clients, c'est-à-dire que patcher vos ordinateurs et smartphones ne vous dispense pas de mettre à jour votre routeur ou votre box Wi-Fi.

Même si, en tant qu'utilisateur, vous n'avez pas grand chose à faire de plus que de mettre à jour votre système d'exploitation et le firmware de votre point d'accès pour vous protéger contre la faille Krack Attacks, nous vous énumérons une liste de préconisations qui mises bout à bout, rendront plus difficile aux pirates les plus répandus l'intrusion dans votre Wifi.

Les Conseils de Denis JACOPINI pour avoir un Wifi le plus protégé possible :

1. Mettez à jour les systèmes d'exploitation de vos ordinateurs, smartphones, tablettes et objets.
2. Mettez à jour votre point d'accès Wifi (le firmware de votre Box, routeur…)
3. Modifier le SSID ;
4. Modifier le mot de passe par défaut ;
5. Filtrage des adresses MAC (facultatif car peu efficace);
6. Désactiver DHCP ;
7. Désactiver le MultiCast (pour les appareils qui disposent de cette fonction) ;
8. Désactiver le broadcast SSID (pour les appareils qui disposent de cette fonction) ;
9. Désactiver le WPS (pour les appareils qui disposent de cette fonction) ;
10. Utilisez un VPN ou un accès http**s** pour envoyer ou recevoir des informations confidentielles
11. Choisissez un cryptage fort de votre Clé WIFI :

- Technologie WPA 2 (également connu sous le nom IEEE 802.11i-2004) ;
- **Protocole de chiffrement AES** (ou CCMP) : **Important !**

Des personnes peuvent accéder librement à votre Wifi ?

Condition exigée depuis plusieurs années par les touristes et les nomades, il y a de fortes chances que les clients de votre hôtel, de vos chambres d'hôtes, de vos gîtes ou tout simplement des amis vous demandent absolument de disposer du Wifi.

Je tiens à vous rappeler que selon l'article L335-12 du Code de la Propriété Intellectuelle, l'abonné Internet reste le seul responsable des usages de sa connexion.

Ainsi, je ne peux que vous conseiller d'être prudent concernant l'usage de votre connexion Wifi par des tiers et de vous munir de moyens technologiques permettant de conserver une trace de chaque personne se connectant sur votre Wifi afin que si votre responsabilité en tant qu'abonné à Internet était recherchée, vous pourriez non seulement vous disculper mais également fournir tous les éléments permettant l'identification de l'individu fraudeur.

Les personnes intéressées par les détails techniques, et pointus, concernant la découverte de la faille WPA2 peuvent se rendre sur le site du chercheur dédié à ce sujet.

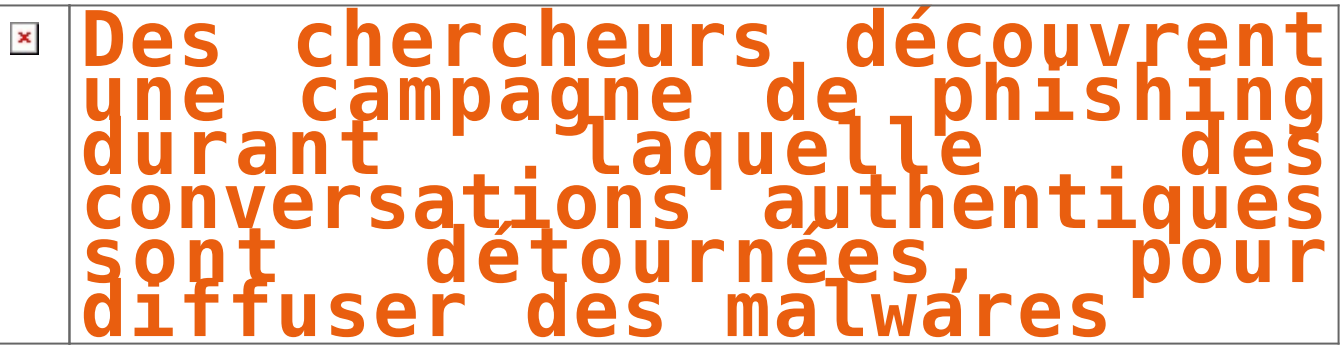
Bulletin d'alerte du CERT-FR

Va-t-on aller vers un WPA 3 ?

Réagissez à cet article

Source : *KRACK Attacks: Breaking WPA2 / KRACK : faille du Wi-Fi WPA2, quels appareils sont touchés ? Comment se protéger ?*

Des chercheurs découvrent une campagne de phishing durant laquelle des conversations authentiques sont détournées, pour diffuser des malwares

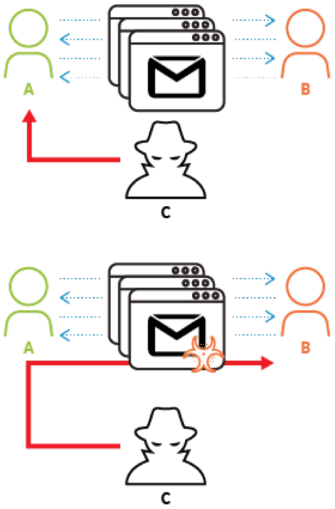


En mai 2017, l'unité 42 de Palo Alto Networks a identifié une campagne d'hameçonnage limitée baptisée FreeMilk qui a visé différents individus et entités à travers le monde. L'acteur de la menace a exploité la vulnérabilité d'exécution de code à distance CTP-2017-0199 Microsoft Word Office / WordPad avec un contenu soigneusement conçu pour chaque destinataire cible.

Les chercheurs de Palto Alto ont expliqué que leur analyse a révélé que les courriels utilisés pendant la campagne portaient sur de multiples comptes de messagerie compromis liés à un domaine légitime en Asie du Nord-Est. « Nous croyons que l'acteur de la menace a détourné une conversation en cours existante et légitime et s'est posé par la suite comme l'expéditeur légitime afin d'envoyer des courriels malveillants de phishing aux destinataires. »

En clair, les chercheurs ont fait valoir que des hackers ont été en mesure d'intercepter des conversations légitimes par courrier électronique entre les individus et les ont détournées. L'objectif était de diffuser des logiciels malveillants vers les réseaux d'entreprise en utilisant des messages de phishing hautement personnalisés conçus pour ressembler à des communications avec l'interlocuteur d'origine.

Le schéma ci-dessous résume assez bien la situation.



Source : Palto Alto
Conversation détournée pour diffuser des logiciels malveillants

Des attaques utilisant cette technique ont permis d'infiltrer plusieurs réseaux, y compris ceux d'une banque du Moyen-Orient, des entreprises européennes de services relatifs à la propriété intellectuelle, une organisation sportive internationale et des « individus ayant des liens indirects avec un pays de l'Asie du Nord-Est. »

Les chercheurs de Palto Alto ont expliqué qu'en cas de succès, le document malveillant télécharge deux charges utiles malveillantes : PoohMilk et Freenki…[lire la suite]

Réagissez à cet article

Source : *Des chercheurs découvrent une campagne de phishing durant laquelle des conversations authentiques sont détournées, pour diffuser des malwares*

Quels risques pour ne pas

avoir fait faire d’expertise indépendante avant ses élections par voie électronique ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Quels risques pour ne pas avoir fait faire d’expertise indépendante avant ses élections par voie électronique ?				

La fiabilité et les modalités de mise en œuvre du vote électronique sont soumises quasiment chaque année à l'examen du juge. Plus d'un a pu se dire surpris de la contradiction apparente entre la jurisprudence du Conseil d'État et celle de la Cour de cassation relativement à l'obligation de réaliser une expertise indépendante préalablement à chaque scrutin recourant au vote électronique.

Le Conseil d'État, dans son arrêt 368748 du 11 mars 2015, a jugé nécessaire la réalisation d'une telle expertise avant chaque scrutin, afin de garantir de manière certaine « la sincérité des opérations électorales ».

La Cour de cassation, dans son arrêt du 21 septembre 2016, indique « qu'il résultait de l'expertise indépendante conduite entre juillet et octobre 2012 que le système de vote électronique utilisé pour le scrutin ne présentait aucune modification substantielle depuis celle qui avait été diligentée en 2005 lors de sa mise en place, le tribunal a exactement décidé qu'il avait été satisfait aux prescriptions des articles R. 2314-12 et R. 2324-8 du code du travail ; » On voit ici le problème qui se pose à l'organisateur d'un scrutin désireux de satisfaire à ses obligations mais aussi désireux de gérer au mieux les coûts occasionnés par l'organisation du vote électronique. Faut-il ou non diligenter une expertise indépendante, alors que la solution de vote a été expertisée auparavant ? Une circonstance est de nature à jeter un trouble encore plus grand lorsque l'on sait que le même système de vote a été utilisé dans les deux cas, objet de ces jurisprudences apparemment contradictoires, mais pour des élections différentes. Le problème n'est qu'apparent et la contradiction peu fondée….[lire la suite]

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *Vote électronique : l'expertise préalable comme principe fondamental du droit électoral – Global Security Mag Online*

Les nouvelles techniques des pirates pour piller les distributeurs de billets

Les nouvelles techniques des pirates pour piller les distributeurs de billets

---

Phishing, hacking, infections « fileless », prise de contrôle à distance… Les braqueurs de banque utilisent des méthodes de plus en plus sophistiquées, presque invisibles, pour mettre la main sur le pactole des banques.

Quand on pense à des braqueurs de banque, on s'imagine la plupart du temps une bande de malfrats cagoulés et armés jusqu'aux dents, fonçant sur les agences en voiture-bélier. Mais la réalité est bien différente de nos jours. C'est souvent à coup d'ordinateurs et de codes malveillants que les braqueurs du XXIe siècle mettent la main sur le liquide des distributeurs, et cela avec un degré de technicité de plus en plus impressionnant.

D'après un rapport que vient de publier l'agence Europol, les premiers malwares qui ont permis de vider des guichets automatiques datent de 2009. Ils s'appellent Skimer, Ploutus ou Padkin-Tyupkin, et nécessitent d'accéder physiquement à l'intérieur de ces machines. Pour cela, les pirates s'appuient soit sur un complice de la banque, soit sur un jeu de clés. En effet, il arrive que les distributeurs ne soient protégés qu'avec de simples verrous de type boîte aux lettres !

A l'intérieur du distributeur se trouve généralement un PC sous Windows XP que les pirates infectent avec une porte dérobée. Celle-ci est installée directement depuis un CD ou une clé USB au niveau de XFS (Extension for Financial Services), un *middleware* qui permet de gérer l'interaction entre les différents éléments logiciels et matériels du distributeur: clavier, lecteur de carte, cassettes d'argent, processeur de chiffrement, etc.

Des mules pour récupérer le magot

L'infection nécessite habituellement un démarrage sous Linux. Puis les pirates repassent la machine sous Windows XP et referment les ouvertures physiques. Toute cette opération prend moins de 10 minutes. En apparence, tout fonctionne de nouveau comme avant. En réalité, la porte dérobée permet à des mules d'entrer des commandes secrètes par le clavier numérique et d'éjecter l'argent. Voici une démonstration réalisée en 2014 par les chercheurs de GData…[lire la suite]

http://www.youtube.com/embed/rZ8_tbTnNUE

Réagissez à cet article

Source : *Les nouvelles techniques des pirates pour piller les distributeurs de billets*

Télétravail : gare aux failles de sécurité

Télétravail : gare aux failles de sécurité

Le télétravail fait entrer dans les systèmes d'information de l'entreprise des appareils dont le niveau de sécurité peut s'avérer à risque.

Les directeurs des systèmes d'information (DSI) s'arrachent déjà les cheveux. Si nombre de métiers, comme ceux des commerciaux ou des consultants, sont déjà équipés pour travailler à distance en toute sécurité, le télétravail pousse hors des murs de l'entreprise des salariés souvent peu sensibilisés aux risques de cybersécurité.

D'une part, travailler de chez soi pose la question de la sécurité du matériel. La connexion Internet est-elle sécurisée ? Le chiffrement du disque dur en cas de perte est-il actif ? L'identification par SMS ou par token est-elle en vigueur ? « *Autant de questions auxquelles les DSI doivent répondre pour sécuriser le travail à distance. Les mesures sont simples et souvent déjà déployées pour certains salariés mais il faut désormais les généraliser* »…[lire la suite]

Réagissez à cet article

Source : *Télétravail : gare aux failles de sécurité, Cybersécurité – Les Echos Business*

20% des ordinateurs de la Police de Manchester son sous Windows XP

	20% des ordinateurs de la Police de Manchester son sous Windows XP

GREATER MANCHESTER POLICE are still using defunct operating system Windows XP on one-in-five machines in active use on the force.

The second biggest police force in the UK joins the Metropolitan Police on the list of shame, according to new findings from a Freedom of Information Act request made by*the BBC.*

« The remaining XP machines are still in place due to complex technical requirements from a small number of externally provided highly specialised applications, » a spokeswoman told Auntie Beeb.

« Work is well advanced to mitigate each of these special requirements within this calendar year, typically through the replacement or removal of the software applications in question. »

Most forces refused to cooperate with the FOI request, citing security reasons. This includes the Met Police who back in June admitted they had 18,000 machines that still run XP (including offline ones) and that only eight machines were running Windows 10…[lire la suite]

Réagissez à cet article

Source : *Manchester Police are using Windows XP on one in five computers*

Télétravail et protection des données personnelles

	Télétravail et protection des données personnelles

Le télétravail pose certaines questions concernant d'abord le droit du salarié à la déconnexion mais aussi sur la protection des données. La barrière de plus en plus floue entre outils personnels et outils professionnels avec la collecte d'informations impose de revoir le régime juridique de la protection des données. Explications par François Alambret, Counsel chez Bryan Cave Paris.

L'essor du télétravail a accru la nécessaire protection des données personnelles. Si ces deux sujets se complètent, ils ne doivent éclipser les autres aspects de la digitalisation des relations de travail.

Le développement du télétravail

Le télétravail n'a pas attendu l'émergence d'internet pour exister mais il s'est incontestablement développé par la conjonction de différents facteurs : les progrès des outils technologiques individuels, l'individualisation des relations du travail et l'accroissement des centres urbains et leur congestion concomitante.

Poussé d'abord par les revendications des salariés, le télétravail a été organisé par les entreprises par le biais d'accords collectifs ou de chartes (informatiques ou sur la qualité de vie au travail), puis reconnues par les organisations syndicales au niveau européen et national (accord cadre européen sur le télétravail du 16 juillet 2002 et accord national interprofessionnel du 19 juillet 2005). Enfin, encadré par le législateur par le biais des lois du 22 mars 2012, du 8 août 2016 (Loi travail dite loi « El-Khomri ») et les ordonnances Macron en cours de promulgation.

Cette dernière étape législative vise encore à simplifier le recours au télétravail, notamment par le biais d'un accord ou d'une charte d'entreprise en dispensant ensuite les parties d'un avenant au contrat de travail (voir article 24 de l'ordonnance n°3 du 31 aout 2017 modifiant les articles L.1222-9 et suivants du code du travail).

L'employeur n'est plus tenu, non plus, de supporter le coût de ce télétravail, ce qui autorise le salarié « de facto » à utiliser son propre matériel informatique (avec les conséquences afférentes en termes de confidentialité et de sécurité).

La protection des données personnelles

Dès son apparition, le télétravail s'est heurté aux problématiques de la protection des données informatiques. Cette contrainte a d'ailleurs été rappelée expressément par les partenaires sociaux dans leur premier accord européen (point 5 de l'accord cadre du 16 juillet 2002) et national (article 5 de l'accord national interprofessionnel du 19 juillet 2005).

Et de fait, le télétravail accroît les risques sur la protection des données de façon à la fois structurelle et technique. Structurellement, par le mode même d'organisation du travail (qui augmente les communications digitales au détriment de communications directes et orales dans l'entreprise) et techniquement car le salarié demeure à distance des services informatiques de l'entreprise et peut dorénavant utiliser ses propres matériels informatiques avec les risques qui en découlent.

Le règlement communautaire sur la protection des données en date du 27 avril 2016 (souvent dénommé GDPR « Global Data Protection Regulations ») prend acte de la digitalisation croissante de la société et de ses nouvelles formes de travail. Il renforce les mesures de protection à l'égard des personnes et donc vis-à- vis des salariés et des télétravailleurs.

L'imbrication des deux notions/ le rôle de l'entreprise

Ces deux sujets (télétravail et protection des données) s'accompagnent et s'encouragent mutuellement. Le renforcement de la protection des données offre des garanties nécessaires au développement du télétravail.

Toutefois, ce cadre législatif et réglementaire posé, c'est aux acteurs de l'entreprise de s'en saisir et de le façonner.

A eux de négocier et de rédiger un accord collectif ou une charte permettant une mise en œuvre fluide mais aussi sécurisée du télétravail, dans le respect du nouveau règlement communautaire du 27 avril 2016.

Mais traiter ces deux thèmes isolément méconnaît l'ampleur des bouleversements de la digitalisation de la société et des relations du travail…[lire la suite]

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Télétravail et protection des données personnelles – LE MONDE DU DROIT : le magazine des professions juridiques*

Votre appareil potentiellement piratable par Bluetooth

Des failles informatiques présentes sur des milliards d'objets disposant de la technologie Bluetooth viennent d'être dévoilées. Attention : danger.

« *On va peut-être atteindre un record d'attaques enregistrées ces dernières années.* » Le communiqué de la société américaine Armis, spécialisée dans la sécurité informatique, ne mâche pas ses mots. Pire encore : « *Nous craignons que la faille que nous avons découverte ne soit que la partie visible de l'iceberg.* » La raison de cette annonce gentiment alarmiste ? Potentiellement 5,3 milliards de terminaux dans le monde pourraient être attaqués. Leur point commun à tous ? Ils disposent du Bluetooth. Tous sont donc exposés aux attaques dites « BlueBorne ».

Freinons un tout petit peu le mouvement de panique : la faille BlueBorne ne fonctionne que si le Bluetooth est préalablement activé sur l'appareil, même si celui-ci est en mode invisible. Selon le terminal piraté, il est possible de prendre son contrôle ou de faire du « *man in the middle*« , autrement dit d'intercepter les communications entre plusieurs interlocuteurs sans se faire repérer. L'attaque n'est pas difficile à mener et peut, dans le meilleur des cas, aboutir en dix secondes. On peut bien sûr craindre la main mise sur des documents confidentiels. Mais on peut aussi redouter une opération « rançongiciel » d'envergure, à l'instar de WannaCry…[lire la suite]

Réagissez à cet article

Source : *Angoisse : des milliards d'appareils sont*

potentiellement piratables via Bluetooth

Pirate Bay contamine votre ordinateur pour fabriquer de la monnaie virtuelle

	Pirate Bay contamine votre ordinateur pour fabriquer de la monnaie virtuelle

---

Avec les années, il est devenu de plus en plus difficile pour les sites de torrent et de téléchargement pirates de survivre uniquement grâce aux revenus publicitaires. Mais ils ont su rebondir et trouver de nouvelles techniques pour parvenir à générer suffisamment de revenus, simplement en utilisant les processeurs des visiteurs pour miner des crypto-monnaies.

Le procédé a été découvert **dans un code JavaScript sur The Pirate Bay**, et si ce n'est pas systématique, c'est néanmoins assez fréquent pour devenir problématique, puisqu'il est très facile de se rendre compte **des pics soudains d'utilisation du CPU (jusqu'à 100%)** pour récupérer du **Monero**. Le site avance qu'il s'agit pour l'instant d'une phase de test, qui pourrait cependant mener à une utilisation plus mainstream du procédé qui lui permettrait de rester rentable….[lire la suite]

Réagissez à cet article

Source : *Pirate Bay emprunte les processeurs des visiteurs pour miner de la monnaie virtuelle | KultureGeek*

Comment pirater un téléphone sans le toucher ?

	Comment pirater un téléphone sans le toucher ?

L'exploitation de failles de sécurité se trouvant au niveau du protocole Bluetooth permet de pirater un appareil à distance. La démonstration est faite sur un smartphone Android, mais les vulnérabilités concernent potentiellement d'autres types d'appareils.

Armis, entreprise spécialiste des questions de sécurité informatique, a découvert huit exploits (ces éléments de programme visant à exploiter une faille informatique) réunis sous l'étiquette BlueBorne, et permettant de prendre à distance le contrôle de téléphones, d'objets connectés et même potentiellement d'ordinateurs. *« Nous nous attendons à découvrir beaucoup d'autres vulnérabilités de ce type sur diverses plateformes proposant une connexion Bluetooth. Ces failles sont actuellement ouvertes, et peuvent être exploitées par les hackers. Les attaques via BlueBorne peuvent être utilisées pour réaliser tout un arsenal de piratages différents, autorisant l'exécution de code malveillant à distance ou encore la prise de contrôle des appareils*« , explique Armis….[lire la suite]

Réagissez à cet article

Source : *BlueBorne : le hack qui permet de pirater un téléphone sans le toucher*