Un virus utilise votre téléphone pour fabriquer des bitcoins

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Un virus utilise votre téléphone pour fabriquer des bitcoins

« Cryptojacking ». Ce nom ne vous dit certainement rien, mais il s'agit pourtant d'une cyberattaque à prendre très au sérieux. Celle-ci fait fabriquer des bitcoins à votre téléphone sans que vous puissiez vous en rendre compte.

Pour attirer les utilisateurs, les pirates informatiques mettent souvent en ligne des reproductions factices d'applications populaires, se révélant être des applications de minage dissimulées. « ***Les utilisateurs n'en ont généralement pas conscience***« de l'attaque, avec pour seuls indices « *l'autonomie et les performances des appareils (qui) diminuent brusquement sans raison apparente* » et l'appareil qui peut se mettre à « *dangereusement surchauffer*« , explique David Emm.
Une version du populaire jeu « *Bug Smasher*« , installée plus d'un million de fois à partir du magasin d'applications Google Play, a été détectée en mars par le groupe de sécurité informatique ESET basé aux États-Unis. Il a averti sur son site que « *l'application sert en réalité secrètement au minage de la cryptomonnaie monero*« .
L'iPhone est moins visé par les pirates, car Apple contrôle davantage les applications pouvant y être installées.
Partager surTwitter
Autre exemple, un logiciel malveillant du nom de « *Coin.Miner* » a été découvert par le spécialiste de cybersécurité TrendLabs en décembre. « ***Le +malware+ est lancé dans une fenêtre de navigateur cachée****, ce qui empêche l'utilisateur de s'en rendre compte*« , détaille la société sur son blog.
Le cryptojacking touche surtout les appareils sous Android, le système d'exploitation mobile de Google. L'iPhone est moins visé par les pirates, car Apple contrôle davantage les applications pouvant y être installées, selon les experts en sécurité informatique.
Google a d'ailleurs décidé récemment de faire le ménage dans sa boutique d'applications mobiles, Google Play, en informant fin juillet les développeurs qu'il n'accepterait plus les applications de minage de cryptomonnaies sur sa plateforme…[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Quand votre téléphone fabrique des bitcoins à votre insu*

Le Nist déconseille le SMS pour l'authentification à double-facteur

LE NET EXPERT VOUS INFORME

Le Nist déconseille le SMS pour l'authentification à double-facteur

L'envoi de codes à usage unique pour assurer une authentification en ligne à facteurs multiples est largement répandu. Google le propose ainsi pour ses services en ligne. Techniquement, de nombreuses banques ne font pas autre chose lorsqu'il s'agit de valider certains ordres de virement.…[Lire la suite sur la source]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Google lance Titan Security Key, une clé USB pour la sécurité de vos comptes

Google lance la Titan Security Key, une clé USB pour protéger ses services en ligne et assurer la sécurité de vos comptes. Google s'apprête à commercialiser une clé USB spécialement conçue pour protéger votre accès à ses services en ligne.

Google s'apprête à commercialiser une clé USB spécialement conçue pour protéger votre accès à ses services en ligne.

Convaincu de l'importance d'une bonne sécurité informatique et après avoir longuement testé toutes les solutions sur le marché, Google est sur le point de commercialiser un modèle de clé USB assez particulier.

Not your typical USB Drive
Baptisée Titan Security Key, la prochaine clé USB « made in Google » est faite pour la sécurité informatique. Conçue pour protéger votre accès aux services Google, la Titan Security Key dispose d'un firmware pour s'assurer de l'intégrité de vos comptes et en assurer la sécurité…[Lire la suite sur la source]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Les systèmes de fichiers sont bien plus en danger qu'on ne le pense

Les systèmes de fichiers sont bien plus en danger qu'on ne le pense

Dans une entreprise, un dossier sur cinq est lisible par n'importe lequel des collaborateurs. Et dans presque la moitié des entreprises, ce sont jusqu'à 1 000 documents sensibles qui se trouvent en accès libre pour tous les salariés !…[Lire la suite sur la source]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

20 failles de sécurité repérées dans la plateforme IoT SmartThings Hub de Samsung

Un chercheur en sécurité de Cisco Talos a identifié 20 vulnérabilités dans la plateforme SmartThings Hub de Samsung permettant de contrôler et de gérer des objets connectés.

Pratiques, utiles et dans l'ère du temps, les objets connectés n'en demeurent pas moins de véritables nids à vulnérabilités. Un chercheur en sécurité de Cisco Talos, Claudio Bozzato, le prouve une fois de plus en venant récemment de démontrer l'existence de plusieurs vulnérabilités présentes dans le firmware du Samsung SmartThings Hub. Cette plateforme permet de surveiller et de gérer divers dispositifs IoT tels que des prises, ampoules, thermostats, des caméras et d'autres déployés dans les maisons connectées. Le SmartThings Hub fonctionne comme un contrôleur centralisé pour ces périphériques et permet aux utilisateurs de se connecter à distance et de gérer ces périphériques à l'aide d'un smartphone….[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *20 failles de sécurité repérées dans la plateforme IoT SmartThings Hub de Samsung – Le Monde Informatique*

Une faille de sécurité Bluetooth intercepte nos données et affecte nos smartphones

Une faille de sécurité Bluetooth intercepte nos données et affecte nos smartphones

Une importante faille Bluetooth, qui a été révélée par des experts du Technion, l'Institut de technologie d'Israël, affecte notamment le protocole Bluetooth des smartphones et tablettes sous Android et Apple.
Il faut savoir que le protocole Bluetooth repose sur la méthode de chiffrement Diffie-Hellman (ECDH) permettant une connexion sécurisée entre deux appareils dont le principe repose sur l'échange de clés. Les chercheurs ont remarqué qu'une étape de validation n'était pas présente dans le processus. Les experts ont donc réussi à intercepter les données transférées pendant les communications sans fil Bluetooth.
Les chercheurs de Technion explique qu'un troisième appareil malveillant peut directement s'incruster dans la liaison dans un rayon de 30 mètres, et espionner la connexion entre les deux appareils afin de récupérer les données échangées. Ces experts sont d'ailleurs parvenus à développer une technologie permettant de trouver la clé de sécurité partagée entre deux appareils...[lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Une faille de sécurité Bluetooth intercepte nos données et affecte nos smartphones*

La méthode d'OVH pour démanteler les réseaux d'objets connectés zombies

Le premier hébergeur européen est une cible de choix pour les

attaques par déni de service, de plus en plus menées via des objets connectés. OVH a donc créé un système pour déconnecter automatiquement les serveurs présents sur son réseau, avec les risques que cela comporte. Entretien avec Sébastien Mériot, l'un des ingénieurs derrière cet outil.

La lutte contre les *botnets*, ces larges réseaux d'appareils zombies, nécessite de traiter toujours plus de données, toujours plus rapidement. En décembre, la Botconf 2017 était placée sous le signe de l'automatisation et de l'intelligence artificielle (voir notre compte-rendu). Des chercheurs y présentaient autant des outils d'apprentissage que des systèmes capables de désassembler à la chaine des logiciels, peu importe l'architecture sur laquelle ils reposent.

À cette occasion, Sébastien Mériot, ingénieur en sécurité chez OVH, a montré comment l'hébergeur automatise la suppression de serveurs de contrôle des *botnets* sur son réseau. « *La première menace pour un fournisseur d'accès est une attaque DDoS* [déni de service distribué, NDLR]*, pas un rançongiciel. Si le réseau tombe, notre activité meurt* » déclarait-il alors. C'est ce danger que portent les malwares destinés à l'Internet des objets.

L'Internet des objets, cobaye idéal

« *Nous avions choisi les malwares IoT, car c'est un domaine qui s'y prête très bien : la menace est en plein boom et les malwares sont généralement assez basiques* » nous déclare Mériot, dans un entretien écrit. S'ils existent depuis une dizaine d'années, ils ont gagné leurs lettres de noblesse fin 2016, avec des campagnes fondées sur Mirai, dont celle contre Dyn, qui a rendu un nombre important de sites inaccessibles….[Lire la suite sur la source]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Cyber sécurité : tous concernés

Les « rançongiciels » attaquent chaque année des milliers de sociétés de toutes tailles. N’attendez plus pour vous protéger.

Pour toutes les sociétés, 2018 sera l’année de la cyber sécurité. En 2017, le ransomwareWannaCry (ou annaCrypt), qui a paralysé des milliers d’entreprises dans le monde entier, a provoqué une réelle prise de conscience des dangers encourus par toutes les entreprises, y compris les plus petites.

Contrôle à distance d’une entreprise

Lors du voyage à Tel Aviv de la FF2i (Fédération française de l’Internet immobilier), on nous a montré des images spectaculaires de prise de contrôle à distance de voitures, de centrales électriques, de centres de traitements des eaux, d’usines. Et bien évidemment, les systèmes d’informations sont encore plus visés. À l’origine, il s’agissait principalement d’opérations militaires cherchant à déstabiliser un pays. L’opération la plus spectaculaire fut la paralysie des centrifugeuses nucléaires iraniennes par un virus, introduit sur une clé USB par la CIA.

Aujourd’hui, il s’agit de délinquance financière : paralysie d’un système, puis demande de rançon. Comme peu avaient anticipé le danger, la vulnérabilité des entreprises est très grande.Voici ce qui peut se passer demain dans votre agence immobilière : vous allumez vos ordinateurs et vous voyez un message demandant 50 000 euros pour rétablir vos

PC qui sont tous bloqués, écran noir total, l’entreprise est à l’arrêt !

Toutes les sociétés sont concernées

Les petites entreprises peuvent penser que les hackers s’intéressent uniquement aux grandes sociétés, plus riches donc capables de verser des rançons plus importantes. Hélas, ce n’est pas le cas ! Il existe à la fois des braqueurs de banques et des voleurs à la tire… Et aujourd’hui, sur Internet, pour attaquer une société, il n’est pas besoin d’être un hackeur expert, on peut louer les services de pirates du Net sans avoir de compétences techniques. Les spécialistes de la sécurité sur Internet rapportent que des milliers d’entreprises sont rançonnées, mais on ne le sait pas car elles préfèrent se taire plutôt que d’avouer s’être mal protégées…[Lire la suite sur le site source]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l’été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d’usurpation d’identité sur facebook, tweeter ? Portez plainte mais d’après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Des documents «très sensibles» de drones américains en vente sur le Dark Web

Des hackers ont tenté de vendre sur le Dark Web des informations volées concernant les drones des forces armées américaines MQ-9 Reaper, relate l'entreprise informatique internationale Recorded Future.…[Lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Piratage informatique : l'attaque de la pompe à essence

Des pirates informatiques auraient réussi à prendre le contrôle d'une pompe à essence en s'attaquant au logiciel de

qui permet de gérer les pompes de la station. Ils seraient parvenu à modifier le prix des carburants et à bloquer le système d'arrêt de la distribution du carburant.

C'est un piratage informatique hors norme non pas par sa technicité, ou encore son ampleur. Non, il est hors norme par son volume : à Marathon, près de Detroit (Etats-Unis), deux personnes auraient réussi à voler quelque 2.300 litres d'essence en piratant une pompe à essence (1.800 dollars en valeur). Une enquête est en cours. Le piratage a duré 90 minutes, et a permis à 10 voitures de faire le plein, gratuitement….[Lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]