# Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

**Android est à nouveau visé par un malware vendredi 13 octobre : DoubleLocker, un redoutable ransomware, chiffre les fichiers sur le smartphone et change son mot de passe, même s'il n'est pas rooté. Des chercheurs de ESET à l'origine de la découverte expliquent que ce ransomware se cache dans un APK d'Adobe Flash Player ce qui peut augmenter le risque d'une propagation rapide. La seule façon de s'en débarrasser c'est de réinitialiser le smartphone. Ce serait le pire ransomware détecté à ce jour.**

Les chercheurs de ESET viennent de découvrir le premier **ransomware Android** capable de prendre le contrôle total de votre smartphone. Il parvient à obtenir des droits administrateur même sur des smartphone non-rootés, ce qui le rend extrêmement dangereux. Android/DoubleLocker.A est basé sur un trojan bancaire modifié pour changer le code PIN du smartphone sur lequel il est installé et chiffrer ses données. Les chercheurs précisent qu'un tel mode d'action était jusqu'ici du jamais vu.

# Android : le pire ransomware jamais détecté, DoubleLocker, bloque et chiffre les smartphones

Le chercheur Lukáš Štefanko à l'origine de la découverte de DoubleLocker ajoute : « *à cause du fait qu'il trouve son origine dans un malware bancaire, DoubleLocker pourrait très bien être modifié pour devenir ce que l'on pourrait appeler un malware bancaire-rançon. Un malware à deux étages, qui essaie d'abord de voler vos données bancaires et/ou vider votre compte ou compte PayPal, puis bloque votre appareil et ses données pour exiger une rançon… spéculation de côté, on a détecté la version test d'un tel malware dans la nature pratiquement en même temps, en mai 2017*« .

On trouve DoubleLocker dans des APK de Flash Player sur de sites compromis méthode déjà utilisée par d'autres malwares. Une fois lancée, l'application lance un service d'accessibilité baptisé Google Play Service. Le malware obtient ensuite tout seul les permissions d'accessibilité, puis les utilise pour activer les droits administrateurs et se définir comme *Launcher* par défaut. Dès que l'utilisateur appuie sur le bouton Home, le malware est activé. Le PIN est alors changé et les fichiers du répertoire principal chiffrés. Le ransomware demande alors de payer 0.013 BTC dans les 24 heures, soit environ 62 euros au moment où nous écrivons ces lignes. Les chercheurs relèvent que les fichiers chiffrés, qui prennent l'extension .cryeye, ne sont pas supprimés à l'issue de ce délai…[lire la suite]

---



Réagissez à cet article

Source : *Android : le pire ransomware jamais détecté fait ses premières victimes*

---

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


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

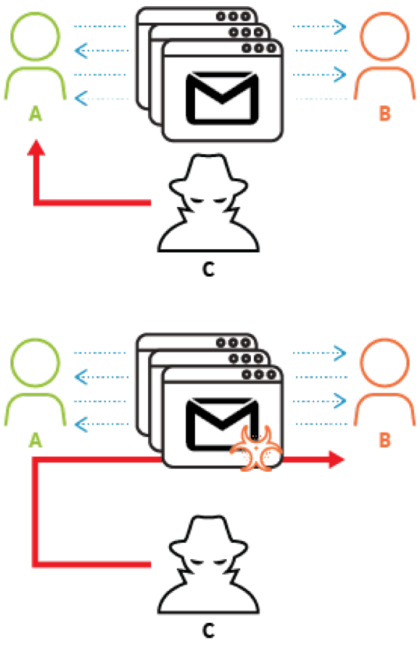
---

**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*

---

# Vérifiez d'urgence que vos enfants n'utilisent pas l'application Sarahah

Vérifiez d'urgence que vos enfants n'utilisent pas l'application Sarahah

---

**« Sarahah » est la nouvelle application à la mode chez les adolescents mais qui inquiète les adultes. Basé sur le principe des messages anonymes, le réseau social apparaît comme une porte ouverte au cyber-harcèlement.**

Sarahah n'avait pas vocation à se retrouver dans les mains des adolescents. Conçue par Zain al-Abidin Tawfiq, l'application permet à ses utilisateurs d'envoyer des messages en gardant l'anonymat. Une méthode que l'homme imagine pour des entreprises afin que les employés puissent proposer des améliorations à leur patron sans s'exposer.

Oui mais voilà, comme toute application celle-ci a vite été appropriée par les jeunes qui en ont détourné le but premier : exit les messages pour améliorer les entreprises, bonjour le harcèlement anonyme.

En effet, comme le rapport le Tribunal du net, certains ados s'en serviraient déjà en France pour harceler leurs camarades. Sous couvert d'anonymat, l'insulte est plus facile. D'autant que les personnes attaquées ne peuvent se défendre puisqu'ils ne peuvent pas répondre aux messages… L'inquiétude grandit donc dans les écoles, d'autant que Sarahah aurait déjà plus de succès que Snapchat ou Instagram…[lire la suite]

---



Réagissez à cet article

Source : *La nouvelle application qui inquiète les parents et les professeurs: la nouvelle porte ouverte au cyber-harcèlement? – www.sudinfo.be*

---

# 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 !

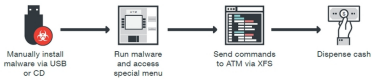



Figure 4. How a typical physical ATM malware attack is carried out

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

---



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

---

# Une extension qui fait discrètement bosser votre

# ordi pour faire gagner de la cryptomonnaie à d’autres

| | |
|---|---|
|  | Une extension qui fait discrètement bosser votre ordi pour faire gagner de la cryptomonnaie à d’autres |

**Alors que les cryptomonnaies, Bitcoin et Ethereum en tête, sont de plus en plus appréciées et commencent à prendre de l'ampleur (une rumeur qui n'a pas été confirmée prêterait à Amazon la volonté d'accepter des Bitcoins pour les paiements), il semblerait qu'une de leurs consœurs soit cryptée à l'insu des internautes par des sites plus ou moins sûrs.**

Cette cryptomonnaie s'appelle Monero et elle a la particularité de ne pas être minée sur le processeur graphique (le GPU) mais sur le processeur central (le CPU).

## Des extensions et du code source pour miner Monero

La particularité de Monero, le fait qu'elle soit minée par le CPU, semble avoir donné des idées à plusieurs sites et entreprises : pourquoi ne pas faire travailler les ordinateurs des internautes ? Ainsi, par exemple, l'extension Chrome SafeBrowse, téléchargée plus de 140.000 fois, utiliserait le CPU des ordinateurs l'ayant installée pour miner de la cryptomonnaie Monero pour le compte de ses créateurs.

Cette utilisation n'a pas manqué d'être vivement critiquée mais elle aurait été reproduite à de nombreuses reprises : sur le site de torrent The Pirate Bay, une phase de test a été menée mi-septembre selon les administrateurs. L'idée serait de remplacer les bannières publicitaires par un script permettant de miner du Monero….[lire la suite]

---



Source : *Monero : la cryptomonnaie que vous minez sans le savoir*

# 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]

---

# 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, suivez nos formations ;

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

**COLLECTE & RECHERCHE DE PREUVES** : Nous mettrons 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 nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Réglement 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 protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

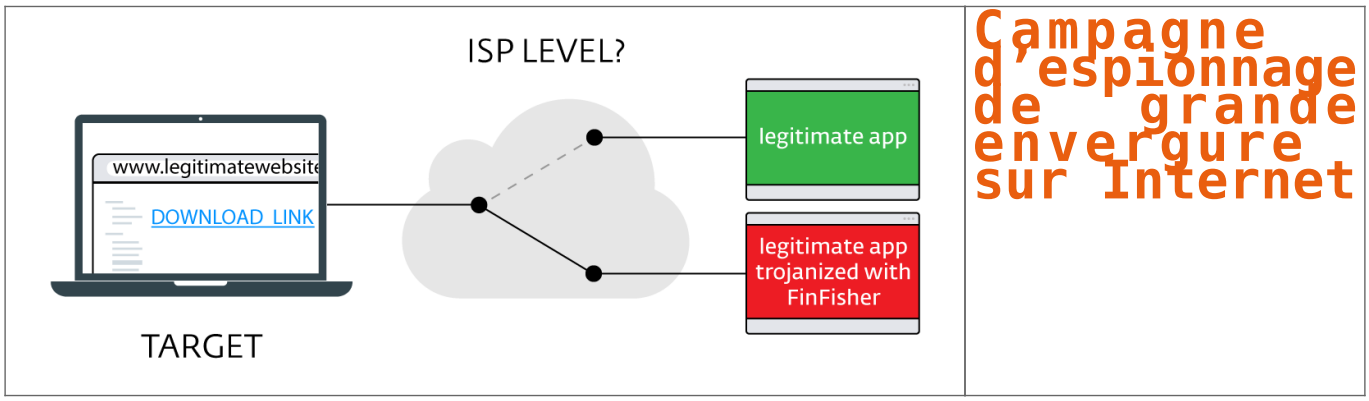
Contactez-nous

Réagissez à cet article

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

---

# Campagne d'espionnage de grande envergure sur Internet




---

**Les chercheurs ESET® ont détecté des campagnes d'espionnage liées à FinFisher, le célèbre spyware également connu sous le nom de FinSpy. Sept pays sont infectés.**

**FinFisher** est un spyware (logiciel espion) **commercialisé en tant qu'outil de surveillance et d'intrusion informatique.**Il est **vendu à une vingtaine d'organismes gouvernementaux** à travers le monde. ESET pense qu'il a également été utilisé par des régimes autoritaires.

**Les capacités d'espionnage de FinFisher s'étendent à :**

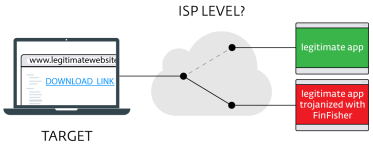
**• la surveillance via les webcams et les microphones (images retransmises en direct)**

**• l'enregistrement de frappe (keylogger)**

**• l'exfiltration des fichiers**

Ce logiciel espion a reçu un certain nombre de modifications via des correctifs dans sa dernière version. Elles améliorent ses fonctions pour se montrer plus intrusif. FinFisher peut ainsi rester sous le radar de détection des solutions de sécurité et empêcher une analyse approfondie de son comportement. L'innovation la plus importante reste la méthode pour pénétrer les machines ciblées.

Lorsqu'un utilisateur ciblé est sur le point de **télécharger une application populaire telle que WhatsApp®, Skype® ou VLC Player®,** il est **automatiquement redirigé vers le serveur de l'attaquant. La victime installe alors une version qui inclut un malware de type Trojan et se trouve ainsi directement infectée par FinFisher.**




*Mécanisme d'infection de la dernière variante de FinFisher*

« Sur deux des sept campagnes menées, les logiciels espions se sont propagés au moyen d'une attaque man-in-the-middle. Autrement dit, les communications sont interceptées à l'insu des parties concernées. Nous pensons que **les principaux fournisseurs d'accès à Internet de ces deux pays ont joué un rôle crucial dans cette infection** », explique Filip Kafka, Malware Analyst chez ESET et à l'origine de cette recherche. Ces campagnes sont les premières à révéler publiquement la probable implication (volontaire ou pas) d'un fournisseur d'accès à Internet dans la diffusion de malwares. « Les campagnes FinFisher sont des projets de surveillance perfectionnés et tenus secrets. Les méthodes utilisées associées à la portée de ces attaques en font une menace sans précédent », poursuit Filip Kafka.

Par le passé, ESET a publié un certain nombre d'articles sur les campagnes FinFisher. Vous pouvez les consulter ici. Les experts ESET ont également rédigé un article détaillé sur cette nouvelle campagne. Pour plus de détails, notre cybersecurity leader Benoit Grunemwald peut répondre à vos questions.

*Note pour les éditeurs:*

*FinFisher, le soi-disant malware du gouvernement et l'approche de l'industrie de la sécurité sont sous les feux de la rampe. Pour ESET, il n'existe pas de malware dans la mesure où ce programme a été acheté d'une part puis modifié et détourné d'autre part par des individus mal intentionnés.*

*Lire la réponse d'ESET à une lettre ouverte adressée à Bits of Freedom, un groupe de défense des droits numériques…*[lire la suite]

---



Source : ESET

---

# Votre appareil potentiellement piratable par Bluetooth


# 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]

---



Source : *Angoisse : des milliards d'appareils sont potentiellement piratables via Bluetooth*

---

# Une faille dans Windows 10 utilisée pour vous espionner

# !

## Une faille dans Windows 10 utilisée pour vous espionner !

**Selon un rapport publié sur le blog de la firme de sécurité informatique FireEye, les pirates procédaient comme suit : un fichier Word ouvert innocemment par l'utilisateur activait la faille 0-Day -CVE-2017-8759- et permettait au maliciel d'installer à son insu un programme informatique destiné à vous espionner. L'ordinateur visé par la manoeuvre était alors contraint d'installer FinSpy – le spyware en question.**

Ce malware est développé par une entreprise anglaise particulièrement controversée qui commercialise ses produits à des gouvernements partout dans le monde : **Gamma Group**. Selon le rapport de FireEye, **FinSpy a déjà été vendu à de multiples acheteurs,** il est donc plus que probable que ceux-ci s'en servent activement pour tenter d'infiltrer de nombreuses cibles.

Selon les experts en cybersécurité de Microsoft, les hackers en question font **partie du groupe NEODYMIUM**, déjà connu pour des pratiques de hacking similaires. Microsoft reste donc très vigilant par rapport à ces failles de sécurité : n'hésitez donc pas à télécharger les patchs proposés dès que possible !

On ne le répétera jamais assez, si vous recevez un fichier Word suspect sur votre boîte mail ne l'ouvrez pas, même s'il vous promet de vous révéler la suite de Game Of Thrones !…[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, suivez nos formations ;

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

**COLLECTE & RECHERCHE DE PREUVES** : Nous mettrons 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 nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Réglement 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 protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Windows 10 : une faille de sécurité permet aux pirates d'y installer un dangereux malware !*

# 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*