# Les autorités US invitent les hackers à pirater le Pentagone

Les autorités US invitent les hackers à pirater le Pentagone

**Les autorités militaires américaines proposent aux meilleurs hackers du pays d'essayer de pirater le Pentagone. Les gagnants de ce « concours » se partageront 150.000 dollars**

Les autorités militaires américaines ont procédé à l'enregistrement des participants au projet Hack the Pentagone (Piratez le Pentagone), a annoncé le porte-parole du Pentagone Peter Cook.

Anonymous déclare la guerre à Donald Trump

Les projets de ce type ont fait leurs preuves dans nombreuses compagnies privées des Etats-Unis et ont pour but de révéler les failles dans leur système de sécurité. En analysant les cyberattaques, les experts peuvent détecter les brèches dans la défense informatique, en vue de les colmater avant que les malfaiteurs ne causent des dégâts.

« Dans le cadre du programme, les participants auront à travailler avec certains sites du département américain de la Défense, ceux-ci étant désignés à la veille du concours », indique le site du Pentagone.

cyberguerre

© PHOTO. PIXABAY

Pourquoi n'a-t-on pas encore coupé la connexion Internet de Daech?

Le projet se déroulera du 18 avril au 12 mai. En cas de succès, les gagnants se partageront une cagnotte de 150.000 dollars. Tous les participants, qui doivent être des citoyens américains, seront soumis à un contrôle de leurs données personnelles.

Le 1er mars, le secrétaire américain à la Défense a présenté le projet à San Francisco, dans le cadre du « Commonwealth Club ». C'est la première fois que l'administration américaine se tourne vers des pirates pour tester sa sécurité.

… [Lire la suite]

---

Réagissez à cet article

Source : *Les autorités US invitent les hackers à pirater le Pentagone*

---

# Et si vous vendiez les données personnelles de votre enfant pour financer ses études ?

Et si vous vendiez les données personnelles de votre enfant pour financer ses études ?

---

**Ce service permettrait de réduire l'inégalité de chances en permettant aux enfants de familles modestes d'accéder à des études supérieures.**

Certes, nous adorons nos chers bambins. Mais au regard de ce que coûte l'entretien d'un enfant au quotidien puis du véritable gouffre financier qu'entraînent ses études, on en aurait presque des sueurs froides.
La société australienne DataChild l'a bien compris, et propose depuis janvier dernier un service inédit : collecter (avec l'accord des parents, bien entendu) les données personnelles des enfants, de leur naissance jusqu'à leur 18ème anniversaire, en l'échange de 50 000 dollars destinés à financer leurs études, le moment venu.

**Comment ça marche ?**
Souscrire à ce service demande rigueur et organisation. Les familles inscrites se voient remettre un petit ordinateur avant la naissance de leur bébé depuis lequel elles enverront quotidiennement les données sur l'enfant à DataChild.
Et celles-ci sont nombreuses : chaque soir, les parents devront remplir et transmettre à la firme australienne un formulaire détaillé sur la journée de l'enfant. Cela va du nombre de couches utilisées, aux durées des siestes qu'il a réalisées, en passant pas la quantité précise de chaque aliment ingurgité et même par le détail des mictions et des selles (avec couleur et consistance) produites.

**Nos enfants, gros producteurs de données**
Et cela ne s'arrête pas là ! Chaque semaine, il est demandé aux parents d'envoyer un rapport sur la santé de l'enfant contenant ses poids et taille (avec tour de tête, de poignet et de cheville), listant ses pathologies, mais aussi les éléments de croissance marquants observés (apparition ou chute d'une dent, acquisition de la marche, de la parole, évolution de la pilosité, etc.) ainsi que ses résultats scolaires (notes, commentaires de professeurs, etc). Et ce de sa naissance jusqu'au jour de ses 18 ans.
A partir de ses 4 ans, des questionnaires ponctuels seront également soumis à l'enfant afin que celui-ci s'exprime sur des sujets précis (par exemple, son sentiment vis à vis d'une marque ou d'un produit).

**Réduire l'inégalité des chances**
En l'échange de toutes ces informations, et dès la signature du contrat, un compte bancaire au nom de l'enfant est créé par DataChild et garni de la coquette somme de 50 000 dollars. Le contenu de ce compte restera bloqué jusqu'à ses 18 ans et ne pourra être utilisé qu'à des fins scolaires. DataChild souhaite ainsi réduire l'inégalité des chances en permettant aux enfants de familles modestes d'accéder à des études supérieures sans se soucier du financement.
Certes, DataChild peut sembler bien gourmande en données. Et c'est normal : imaginez la variété de sociétés potentiellement intéressées pour les racheter ! L'éventail de data collectées par la firme australienne se doit donc d'être aussi vaste que possible afin de satisfaire à la fois les besoins des industriels de l'agro-alimentaire, des soins ou de la santé, que ceux des assurances ou des banques.

**Une femme refuse d'accoucher pour signer son contrat**
Plusieurs centaines de futurs parents ont d'ores et déjà signé un contrat avec DataChild et des centaines d'autres, sur liste d'attente, trépignent en craignant que leur enfant ne naisse avant d'avoir pu souscrire au service (il est en effet impératif que la collecte des données démarre le jour de la naissance du bébé). Certaines maternités ont d'ailleurs signalé avoir été submergées d'appels émanant de femmes enceinte demandant à être hospitalisées et alitées de peur d'une naissance trop précoces de leur bébé.
Des incidents ont même été relevés : une résidente de Melbourne, suivie pour sa grossesse à l'Hôpital Saint Vincent, aurait par exemple refusé le déclenchement de son accouchement préconisé par l'équipe médicale bien que son bébé ait dépassé le terme depuis 17 jours. Elle ne voulait pas manquer le rendez-vous prévu trois jours plus tard avec l'équipe de DataChild, lors duquel elle devait signer son contrat… [Lire la suite]

---

Réagissez à cet article

Source : *Vendre les données personnelles de son enfant pour financer ses études est désormais possible ! | Archimag*

---

# Et si la publicité cachait des Malwares ?

Et si la publicité cachait des Malwares ?

---

**Alors que plusieurs sites d'information ont récemment mené une action pour dénoncer l'utilisation des bloqueurs publicitaires rappelant que la publicité était le principal revenu pour les sites web, il est également bon de savoir qu'elle tend à devenir un véritable vecteur d'attaque pour les pirates informatiques.**

## Des ransomwares cachés dans les publicités en ligne

Depuis plusieurs jours maintenant, de nombreux internautes se retrouvent piégés par des rançongiciels sans réellement comprendre comment ces derniers ont pu infecter leur ordinateur.

En effet, alors que beaucoup ont bien compris qu'ils devaient accorder la plus grande attention aux pièces jointes adressées par mail ainsi qu'aux fichiers qu'ils téléchargent sur la Toile, ils sont également nombreux à ne pas savoir que les publicités en ligne peuvent être à l'origine de l'infection.

Eh oui, de plus en plus de pirates informatiques parviennent à compromettre des réseaux d'annonces publicitaires en se faisant passer pour des personnes fiables. Ils adressent alors à la régie des bannières à faire afficher par des sites web, certaines intégrant un malware qui pourra infecter les ordinateurs des milliers d'internautes qui verront la publicité.

Cette forme de piratage est d'autant plus « sournoise » que le malware utilisé et baptisé Angler détecte l'existence de logiciel de sécurité et n'est réellement actif que si l'ordinateur ne dispose pas de sécurité. Autant qu'il est très complexe à détecter.

## Les bloqueurs de publicité, finalement utiles pour sécuriser un ordinateur ?

Quelques heures seulement après que plusieurs sites d'informations français aient dénoncé le recours de plus en plus fréquent des internautes aux bloqueurs publicitaires, ces derniers viennent d'avoir un joli coup de publicité.

En effet, les bloqueurs de publicité peuvent être une solution pour sécuriser un ordinateur et tout du moins se protéger contre le malvertising.

Le développement de ce phénomène devrait en tout cas complexifier un peu plus encore la tâche des webmasters puisque l'image de la publicité, déjà jugée intrusive et gênante, devrait être davantage écornée en devenant une menace en matière de sécurité… [Lire la suite]

---

Réagissez à cet article

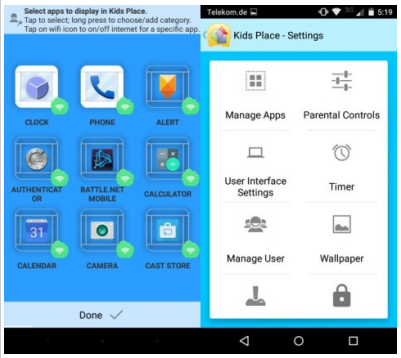
Source : *Quand la publicité devient un vecteur d'attaque*

# Le contrôle parental sur mobile et tablette Android avec Kids Place

| | |
|---|---|
|  | **Comment mettre en place un contrôle parental sur son mobile ou sa tablette Android ?** |

**Confier son smartphone à ses enfants n'est pas sans risque. Un smartphone avec accès à Internet c'est comme une porte ouverte sur le monde entre les mains d'un enfant. Il est important de les protéger.**

Et la meilleure sécurité, c'est bien sûr nous-mêmes ! En apprenant à notre enfant les règles de la sécurité et en surveillant son utilisation. Cependant, en fonction des âges de nos enfants, difficile d'être toujours derrière leurs dos.
Grâce à l'application de contrôle parental Kid's Place, protégez vos enfants des dangers d'internet, lorsqu'ils se connectent depuis d'un smartphone ou tablette Android.
Kid's Place est l'une des meilleures applications permettant de limiter l'accès à certaines applications ou fonctions de votre smartphone ou tablette Android. Elle crée une zone sécurité pour vos enfants sur votre appareil mobile.




Après l'installation de l'application, la première chose que vous devrez faire sera de créer un mot de passe. Ce mot de passe vous sera nécessaire pour de nombreuses fonctions de l'application, ne l'oubliez donc pas.

Ensuite, l'application vous propose deux actions : **bloquer le bouton d'accueil, ou sélectionner les applications pour Kids Place**. En cliquant sur cette dernière action, vous retrouvez toutes les applications présentes sur votre smartphone ou tablette, et vous pouvez simplement sélectionner celles que vous souhaitez voir apparaître pour votre enfant.

Mais l'application ne s'arrête pas là : de nombreuses paramètres vous permettent d'avoir une utilisation plus optimisée de l'application. **Vous pourrez par exemple autoriser ou non les appels, la connexion à Internet ou encore le Wi-Fi et le Bluetooth. Vous pourrez également créer plusieurs profils** (un pour chacun de vos enfants)/ Pour cela, Il vous suffit d'appuyer sur la touche **Options** pour y accéder.
Enfin, vous pouvez **établir une durée d'utilisation**. Vous pouvez laissé affiché le temps restant pour que votre enfant en ait conscience, ou ne pas le laisser visible. Dans tous les cas, à la fin du temps déterminé, Kids Place bloque votre mobile en demandant votre mot de passe, et vous permet de décider de fermer l'application, ou de continuer à l'utiliser… [Lire la suite]

---

Réagissez à cet article

# Source : *Le contrôle parental sur mobile et tablette Android avec Kids Place*

# Des Box pourraient être piratées pour mener des attaques DDOS ?


Des Box pourraient être piratées pour mener des attaques DDOS ?

**Eset a signalé l'activité d'un ver exploitant une faiblesse du protocole de gestion réseau distant Telnet implémenté dans les routeurs domestiques sous Linux. Des pirates peuvent s'en servir pour construire un botnet et lancer des attaques DDoS.**

Construire des botnets à partir de routeurs, modems, points d'accès sans fil et autres terminaux réseaux ne nécessite pas d'exploits très sophistiqués. C'est le cas par exemple de Remaiten, un nouveau ver exploitant les routeurs domestiques sous Linux en tirant partie d'une faiblesse liée aux mots de passe du service de gestion réseau distant Telnet.
Remaiten n'est autre que la dernière incarnation de bots Linux distribués spécialement conçus pour lancer des attaques par déni de service (DDoS). Lorsqu'il scanne des points d'entrée, Remaiten tente de se connecter à des adresses IP aléatoires sur le port 23 (Telnet) et, en cas de connexion fructueuse, il tente de s'authentifier en utilisant une combinaison de nom d'utilisateur et mot de passe en provenance d'une liste d'authentifiants communs, ont indiqué dans un billet de blog les chercheurs de l'éditeur en solutions de sécurité Eset. Ce n'est pas la première fois que les routeurs domestiques sont exposés à du piratage. On se souvient que l'année dernière 700 000 avaient été exposés à cause d'une faille NetUSB et plus récemment, des failles avaient été trouvées dans de nombreux routeurs WiFi Netgear et D-Link.
Scan de ports et fermeture du service Telnet pour se protéger
En cas de succès, le bot exécute plusieurs commandes pour déterminer l'architecture système avant de transférer un petit programme compilé pour permettre de télécharger l'ensemble des commandes de contrôle du botnet. Le ver dispose de versions pour jeux d'instructions mips, mipsel, armeabi et armebeabi. Une fois installé, il se connecte à un canal IRC et attend les commandes d'un pirate distant. Ce bot supporte une variété de commandes pour lancer différentes attaques DDoS et peut même scanner d'autres bots DDoS afin de les désinstaller.
Il est surprenant que de nombreux terminaux réseau utilisent encore Telnet pour la gestion réseau à distance plutôt que le protocole plus sécurisé SSH. Il est encore plus malheureux que de nombreux terminaux soient livrés avec le service Telnet ouvert par défaut. Afin de se protéger, il est recommandé d'utiliser un outil de scan de port en ligne et, dans le cas où le port 23 est ouvert, de fermer le service Telnet depuis la console d'administration web. Une possibilité qui n'est malheureusement pas offerte par tous les fournisseurs d'accès à leurs clients… [Lire la suite]

---

Réagissez à cet article

---

# Utilisateurs de Tor identifiés – Le FBI reste muet


# Utilisateurs de Tor identifiés – Le FBI reste muet

**Le FBI soppose à une demande de la justice qui exige de la police américaine quelle présente sa méthode lui ayant permis didentifier des utilisateurs d'un site pédopornographique, en les piratant.**

Le FBI n'a absolument aucune envie de dévoiler la méthode secrète qu'il a employé pour pirater plus d'un millier de membres d'un site pédopornographique. Et cela, même si c'est la justice américaine qui lui demande.
C'est en effet ce qu'est en train de révéler le procès visant une personne accusée d'avoir fréquenté cet espace, dont l'accès ne pouvait se faire qu'à travers le réseau d'anonymisation TOR.
Dans cette affaire, les avocats du prévenu souhaitent connaître la technique utilisée par la police fédérale pour infecter les ordinateurs de ceux qui visitaient Playpen – le nom de ce site pédopornographique – lorsqu'il était encore en ligne.
Pour la défense, il s'agit de tenter de démontrer que le FBI a outrepassé ses prérogatives au cours de l'enquête, en débordant du cadre de son mandat.

**Sceau FBI**

L'approche du FBI dans l'affaire PlayPen fait polémique outre-Atlantique.
En février, le magistrat a donné suite à cette demande et exigé du FBI qu'il communique à la partie adverse tous les détails de sa méthode de piratage. Mais comme le pointe la BBC, le service de police est particulièrement hostile à cette demande. Un courrier a été adressé cette semaine au juge afin de l'inviter à reconsidérer sa position, estimant que la défense dispose déjà de suffisamment de pièces pour travailler.
En réalité, l'opposition du FBI vise avant tout à préserver l'intérêt de sa technique. En effet, il se pourrait qu'une communication des détails à la partie adverse affaiblisse l'efficacité de cette méthode. Si celle-ci devient publiquement connue, les failles qu'elle exploite seraient tôt ou tard colmatées par TOR, les navigateurs et les serveurs hébergeant des sites web. De même, les utilisateurs se montreraient aussi plus prudents.

**LE FBI VEUT PRÉSERVER L'EFFICACITÉ DE SA MÉTHODE EN LA GARDANT SECRÈTE**

C'est sans doute ce scénario que le FBI veut éviter, afin de pouvoir l'appliquer de nouveau à l'avenir si le besoin s'en fait sentir. Et si la position de la police fédérale se défend, celle de la défense, qui agit dans l'intérêt de son client, est tout aussi audible : le FBI a-t-il enfreint son mandat au nom de la loi ? Et la méthode employée est-elle vraiment fiable ? Une erreur au niveau de l'identification de l'internaute est toujours possible.
L'affaire Playpen remonte au tout début de l'année 2015, lorsque le FBI réussit à prendre le contrôle des serveurs du site pédopornographique. Plutôt que de le fermer immédiatement, ce qui a aussi provoqué son lot de critiques lorsque l'information a été révélée publiquement, la police opte pour une autre approche, celle du honeypot : le site est demeuré actif pendant près de deux semaines, en utilisant ses propres serveurs, de façon à voir qui se connecte sur Playpen.

Le principe du réseau TOR rappelle celui des couches de l'oignon qui masquent le cœur de la plante.
C'est à ce moment-là que le FBI a utilisé sa fameuse technique pour contaminer le poste informatique des visiteurs, afin, notamment, de récupérer leur véritable adresse IP, qui est habituellement cachée avec le réseau d'anonymisation TOR, puisque la connexion passe par une succession de relais afin de camoufler la géolocalisation du PC d'origine.
Une fois l'adresse IP en main, il a suffit de contacter les fournisseurs d'accès à Internet – en tout cas ceux aux USA – pour avoir l'identité des internautes. Au total, la technique du FBI a permis de collecter pas moins de 1 300 adresses IP… [Lire la suite]

---

Réagissez à cet article

Source : *Le FBI refuse de dire comment il identifie des utilisateurs de Tor – Politique – Numerama*

---

# Futur Règlement européen sur la protection des données, qui est concerné ?

Futur Règlement européen sur la protection des données, qui est concerné ?

---

**Le 25 février dernier, Arendt & Medernach organisait une conférence sur le futur Règlement européen sur la protection des données (ci-après « le Règlement »[1]afin de permettre aux entreprises de mieux comprendre les nouvelles obligations auxquelles elles seront prochainement soumises et leur procurer l'essentiel de ce qu'il faut retenir de ce nouveau texte.**

**Contexte**

Après deux années riches en actualités en matière de données personnelles (droit à l'oubli consacré par la Cour de Justice de l'Union européenne (CJUE)[2], et invalidation du Safe Harbor[3] notamment), le nouveau Règlement arrive à point nommé pour remplacer le cadre juridique actuel adopté il y a plus de 20 ans[4].

4 ans de discussions et 4000 amendements ont été nécessaires pour parvenir à un accord autour de ce nouveau texte qui sera adopté en mai/juin prochain. Il sera applicable dans deux ans à compter de sa date d'entrée en vigueur, soit pour l'été 2018.
Si l'échéance semble lointaine, il est toutefois nécessaire d'envisager dès à présent les changements apportés par ce nouveau texte.

De nouvelles obligations pour les entreprises
Il résulte de ce Règlement diverses obligations pour les entreprises et notamment :
• De mettre en œuvre les principes de « privacy by design / privacy by default» afin d'assurer une protection des données dès leur conception et par défaut ;
• De tenir des registres des traitements de données personnelles sauf cas exceptionnels ;
• De notifier toute violation de données dans les 72h auprès de l'autorité de contrôle voire de la personne concernée le cas échéant ;
• De détailler/préciser l'information des personnes concernées ;
• D'adapter leurs contrats de sous-traitances ;
• D'assurer la portabilité des données ;
• De nommer un Délégué à la Protection des Données le cas échéant.
• Les entreprises doivent envisager ces obligations avec le plus grand sérieux puisque de nouvelles sanctions financières pourront désormais être prononcées par les autorités nationales de protection des données. En effet, selon le manquement, ces sanctions pourront atteindre de 2 à 4% du chiffre d'affaires mondial d'une entreprise ou de 10 à 20 millions d'euros, le montant le plus important devant être retenu.

**Qu'est-ce qu'une donnée personnelle ?**

"Les données à caractère personnel sont définies par le futur Règlement comme « toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement , notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale ».
Cette définition est identique à celle prévue actuellement dans la loi luxembourgeoise[7] mais elle ajoute quelques exemples. Il est notamment précisé qu'un identifiant en ligne, tel qu'une adresse IP, peut être qualifié de données à caractère personnel," explique Héloïse Bock, Partner Arendt & Medernach.

**Est-ce qu'on peut dire que toutes les entreprises seront concernées par ce nouveau Règlement ?**

"Le champ d'application du règlement est élargi puisque celui-ci aura vocation à s'appliquer à toutes les entreprises traitant des données personnelles dès lors qu'elles sont établies sur le territoire de l'Union européenne ou, lorsqu'elles sont établies hors de l'Union européenne si ces traitements ciblent des citoyens européens.
Un grand nombre d'entreprises seront ainsi concernées en pratique," poursuit-elle.

**Des droits nouveaux et renforcés**

Pour les personnes concernées, ce nouveau Règlement introduit le célèbre droit à l'oubli ou droit à l'effacement, déjà consacré par la CJUE en 2014[5] mais également, le droit à la portabilité des données qui permet de transférer les données d'un prestataire vers un autre. Les droits d'accès, d'opposition et de rectification des données ainsi que le droit à l'information, existants dans le cadre juridique actuel, sont maintenus et renforcés.

**Les transferts de données hors de l'Union européenne**

Concernant les transferts de données en dehors de l'Union européenne, le Règlement ajoute de nouvelles bases de légitimité ponctuelles/limitées sur lesquelles un responsable de traitement pourra se fonder en cas de transfert vers un pays n'assurant pas un niveau de protection adéquat.
Le sort des transferts de données réalisés vers les Etats-Unis n'est pas réglé par le Règlement, toutefois, une nouvelle décision d'adéquation est attendue très prochainement[6]. La Commission européenne et les États-Unis se sont en effet accordés sur un nouveau cadre pour les transferts transatlantiques de données le mois derniers : le «bouclier vie privée UE-États-Unis» ou « EU-US Privacy Shield ».

**To do list avant 2018**

Pour conclure, les avocats d'Arendt & Medernach ont dressé une « to do list » générale reprenant les points suivants :
• Recenser les traitements de données réalisés en pratique et leurs finalités;
• Faire un audit pour évaluer le niveau de conformité actuel et identifier les lacunes;
• Réaliser un « mapping » de tous les transferts de données en considérant les catégories de données, les destinataires des transferts, les bases de légitimité etc.;
• Effectuer des études d'impact lorsqu'un traitement à risque est envisagé;
• Nommer un délégué à la protection des données si nécessaire;
• Mettre en place ou adapter la documentation existante (registres, policies, contrats de sous-traitance, etc.)

[1] Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (2012/0011 COD)
[2] CJUE, 13 mai 2014, affaire C-131/12
[3] CJUE, 6 octobre 2015, affaire C-362/14
[4] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[5] CJUE, 13 mai 2014, affaire C-131/12
[6] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[7] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
… [Lire la suite]

---

Réagissez à cet article

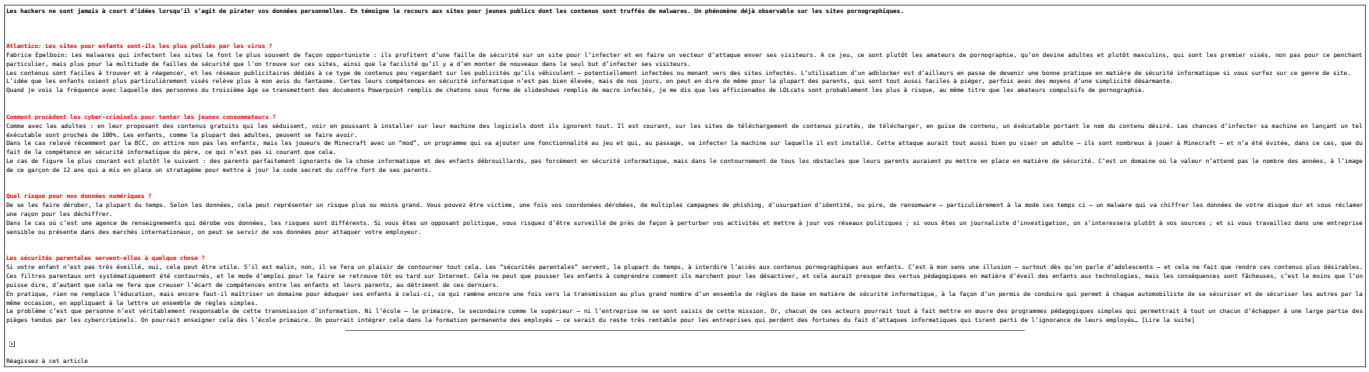
Source : *Futur Règlement européen sur la protection des données, qui est concerné ?*

---

# Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?


Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

---



**Les hackers ne sont jamais à court d'idées lorsqu'il s'agit de pirater vos données personnelles. En témoigne le recours aux sites pour jeunes publics dont les contenus sont truffés de malwares. Un phénomène déjà observable sur les sites pornographiques.**

**Atlantico: Les sites pour enfants sont-ils les plus pollués par les virus ?**

Fabrice Epelboin: Les malwares qui infectent les sites le font le plus souvent de façon opportuniste : ils profitent d'une faille de sécurité sur un site pour l'infecter et en faire un vecteur d'attaque enver ses visiteurs. A ce jeu, ce sont plutôt les amateurs de pornographie, qu'on devine adultes et plutôt masculins, qui sont les premier visés, non pas pour ce penchant particulier, mais plus pour la multitude de failles de sécurité que l'on trouve sur ces sites, ainsi que la facilité qu'il y a d'en monter de nouveaux dans le seul but d'infecter ses visiteurs.
Les contenus sont faciles à trouver et à réagencer, et les réseaux publicitaires dédiés à ce type de contenus peu regardant sur les publicités qu'ils véhiculent – potentiellement infectées ou menant vers des sites infectés. L'utilisation d'un adblocker est d'ailleurs en passe de devenir une bonne pratique en matière de sécurité informatique si vous surfez sur ce genre de site.
L'idée que les enfants soient plus particulièrement visés relève plus à mon avis du fantasme. Certes leurs compétences en sécurité informatique n'est pas bien élevée, mais de nos jours, on peut en dire de même pour la plupart des parents, qui sont tout aussi faciles à piéger, parfois avec des moyens d'une simplicité désarmante.
Quand je vois la fréquence avec laquelle des personnes du troisième âge se transmettent des documents Powerpoint remplis de chatons sous forme de slideshows remplis de macro infectés, je me dis que les afficionados de LOLcats sont probablement les plus à risque, au même titre que les amateurs compulsifs de pornographie.

**Comment procèdent les cyber-criminels pour tenter les jeunes consommateurs ?**

Comme avec les adultes : en leur proposant des contenus gratuits qui les séduisent, voir en poussant à installer sur leur machine des logiciels dont ils ignorent tout. Il est courant, sur les sites de téléchargement de contenus piratés, de télécharger, en guise de contenu, un éxécutable portant le nom du contenu désiré. Les chances d'infecter sa machine en lançant un tel éxécutable sont proches de 100%. Les enfants, comme la plupart des adultes, peuvent se faire avoir.
Dans le cas relevé récemment par la BCC, on attire non pas les enfants, mais les joueurs de Minecraft avec un "mod", un programme qui va ajouter une fonctionnalité au jeu et qui, au passage, va infecter la machine sur laquelle il est installé. Cette attaque aurait tout aussi bien pu viser un adulte – ils sont nombreux à jouer à Minecraft – et n'a été évitée, dans ce cas, que du fait de la compétence en sécurité informatique du père, ce qui n'est pas si courant que cela.
Le cas de figure le plus courant est plutôt le suivant : des parents parfaitement ignorants de la chose informatique et des enfants débrouillards, pas forcément en sécurité informatique, mais dans le contournement de tous les obstacles que leurs parents auraient pu mettre en place en matière de sécurité. C'est un domaine où la valeur n'attend pas le nombre des années, à l'image de ce garçon de 12 ans qui a mis en place un stratagème pour mettre à jour le code secret du coffre fort de ses parents.

**Quel risque pour nos données numériques ?**

De se les faire dérober, la plupart du temps. Selon les données, cela peut représenter un risque plus ou moins grand. Vous pouvez être victime, une fois vos coordonnées dérobées, de multiples campagnes de phishing, d'usurpation d'identité, ou pire, de ransomware – particulièrement à la mode ces temps ci – un malware qui va chiffrer les données de votre disque dur et vous réclamer une rançon pour les déchiffrer.
Dans le cas où c'est une agence de renseignements qui dérobe vos données, les risques sont différents. Si vous êtes un opposant politique, vous risquez d'être surveillé de près de façon à perturber vos activités et mettre à jour vos réseaux politiques ; si vous êtes un journaliste d'investigation, on s'interessera plutôt à vos sources ; et si vous travaillez dans une entreprise sensible ou présente dans des marchés internationaux, on peut se servir de vos données pour attaquer votre employeur.

**Les sécurités parentales servent-elles à quelque chose ?**

Si votre enfant n'est pas très éveillé, oui, cela peut être utile. S'il est malin, non, il se fera un plaisir de contourner tout cela. Les "sécurités parentales" servent, la plupart du temps, à interdire l'accès aux contenus pornographiques aux enfants. C'est à mon sens une illusion – surtout dès qu'on parle d'adolescents – et cela ne fait que rendre ces contenus plus désirables. Ces filtres parentaux ont systématiquement été contournés, et le mode d'emploi pour le faire se retrouve tôt ou tard sur Internet. Cela ne peut que pousser les enfants à comprendre comment ils marchent pour les désactiver, et cela aurait presque des vertus pédagogiques en matière d'éveil des enfants aux technologies, mais les conséquences sont fâcheuses, c'est le moins que l'on puisse dire, d'autant que cela ne fera que creuser l'écart de compétences entre les enfants et leurs parents, au détriment de ces derniers.
En pratique, rien ne remplace l'éducation, mais encore faut-il maîtriser un domaine pour éduquer ses enfants à celui-ci, ce qui ramène encore une fois vers la transmission au plus grand nombre d'un ensemble de règles de base en matière de sécurité informatique, à la façon d'un permis de conduire qui permet à chaque automobiliste de se sécuriser et de sécuriser les autres par la même occasion, en appliquant à la lettre un ensemble de règles simples.
Le problème c'est que personne n'est véritablement responsable de cette transmission d'information. Ni l'école – le primaire, le secondaire comme le supérieur – ni l'entreprise ne se sont saisis de cette mission. Or, chacun de ces acteurs pourrait tout à fait mettre en œuvre des programmes pédagogiques simples qui permettrait à tout un chacun d'échapper à une large partie des pièges tendus par les cybercriminels. On pourrait enseigner cela dès l'école primaire. On pourrait intégrer cela dans la formation permanente des employés – ce serait du reste très rentable pour les entreprises qui perdent des fortunes du fait d'attaques informatiques qui tirent parti de l'ignorance de leurs employés… [Lire la suite]

Réagissez à cet article

Fabrice Epelboin est enseignant à Sciences Po et cofondateur de Yogosha, une startup à la croisée de la sécurité informatique et de l'économie collaborative.

Source : *Quand les sites pour enfants se transforment en pièges pour voler les données personnelles de leurs parents | Atlantico.fr*

---

# L'évolution De La Carte SIM

## L'évolution De La Carte SIM

---

**Une carte SIM, ou Suscriber Identity Module en anglais (module d'identification de l'abonné), est un élément familier d'un téléphone portable. Elle peut facilement être échangée ou remplacée, mais elle n'est néanmoins pas née en même temps que le téléphone portable. Les premiers téléphones portables ne permettaient que des normes de communication « intégrées » : les paramètres de souscription étaient codés en dur dans la mémoire du terminal mobile.**

Les normes analogues les plus anciennes comme NMT-450 n'utilisaient aucune sécurité : les données d'abonnement pouvaient être copiées sur un autre appareil et clonées, ce qui permettait d'appeler et d'accepter des appels au nom du propriétaire légitime sans payer.

Le premier dispositif de sécurité, inventé un peu plus tard, fut le code SIS, Suscriber Identity Security en anglais (sécurité de l'identité de l'abonné) : il s'agissait d'un nombre à 18 chiffres unique à chaque appareil et codé en dur dans un processeur d'application. Les codes SIS étaient répartis entre les fournisseurs de manière à ce que deux appareils ne puissent pas partager le même code SIS. Le processeur comportait également un code RID de 7 chiffres qui était transmis à une station de base lorsqu'un abonné s'inscrivait dans un réseau mobile.

La station de base générait un nombre aléatoire que le processeur SIS utilisait couplé avec une réponse SIS unique pour produire la clé d'autorisation.

Les clés et les nombres étaient relativement courts, mais appropriés pour l'année 1994 ; de façon assez prévisible, le système a été décrypté plus tard, tout juste trois ans avant l'apparition de la norme GSM, Global System for Mobile en anglais (Communications – Système global pour les communications mobiles). Il était conçu de manière plus sûre étant donné qu'il utilisait un système d'autorisation similaire, mais au chiffrement plus résistant. Ainsi, la norme est devenue « détachée » .

Cela signifie que l'autorisation dans sa totalité avait lieu sur un processeur externe intégré dans une carte intelligente. La solution a été appelée SIM. Avec l'introduction des cartes SIM, l'abonnement ne dépendait plus l'appareil et l'utilisateur pouvait changer d'appareil aussi fréquemment qu'il le désirait tout en gardant son identité mobile.

Fondamentalement, une carte SIM est une carte intelligente selon la norme ISO 7816, qui ne présente pas de différence significative par rapport à d'autres cartes intelligentes de contact comme les cartes de crédit ou les cartes téléphoniques. Les premières cartes SIM faisaient même la taille d'une carte de crédit, mais la tendance globale de réduction des dimensions a mené à une nouvelle forme plus compacte.

Les cartes SIM traditionnelles 1FF (1st Form Factor) de taille complète ne rentraient plus dans les téléphones, et l'industrie a donc trouvé une solution de compatibilité simple : une carte SIM plus petite (mini-SIM, 2FF ou 2nd Form Factor) qui est commune pour les utilisateurs modernes, a été placée dans un support en plastique de taille 1FF afin que la nouvelle forme de carte comporte la puce et les contacts, mais avec une empreinte plus petite, et puisse facilement être sortie.

Bien que cette tendance à la réduction continue avec la micro-SIM (3FF) puis la nano-SIM (4FF) , la forme et les contacts ainsi que les fonctionnalités de ces puces intégrées n'ont pas changé depuis presque 25 ans. De nos jours, de grands supports en plastique sont produits pour répondre aux besoins des utilisateurs qui préfèrent encore des combinés à l'ancienne.

Ceci dit, de nombreux appareils obsolètes ne supporteraient pas les cartes SIM actuelles, même dans leur version complète. Cela vient du fait que la tension de fonctionnement était de 5 V dans les anciennes cartes SIM alors que les actuelles exigent 3 V. De nombreux fabricants de SIM préfèrent sacrifier la compatibilité pour réduire les coûts, et la majorité des cartes SIM modernes ne supporteraient donc pas deux tensions. C'est pour cela que dans un ancien téléphone uniquement compatible avec 5 V, les cartes SIM de seulement 3V ne fonctionneraient même pas à cause de la protection de la tension de leur processeur.

Lors de la production, certaines informations sont écrites dans la mémoire d'une carte SIM : l'IMSI (International Mobile Suscriber Identity, Identité de l'abonné mobile international), en accord avec le porteur ayant commandé la carté, ainsi qu'une clé de 128 bits nommée Ki (Key Identification, identification de clé). Pour résumer simplement, on peut dire que l'IMSI et le Ki sont le l'identifiant et le mot de passe respectifs de l'abonné codés en dur dans la puce de la carte SIM.

La correspondance entre l'IMSI d'un abonné et son numéro de téléphone est stockée dans une base de données spéciale appelée HLR (Home Location Register). Ces données sont copiées sur une autre base de données, VLR (Visitor Location Register) dans chaque segment du réseau, sur la base de l'enregistrement temporaire de l'abonné en tant qu' « invité » sur une autre station de base.

Le processus d'autorisation est relativement simple. Lorsqu'un abonné est inscrit dans la base de données temporaire, VLR envoie un numéro de 128 bits aléatoire (RAND) au numéro de téléphone. Le processeur de la carte SIM utilise l'algorithme A3 pour créer une réponse de 32 bits (SRES) au VLR basé sur le numéro RAND et le Ki. Si VLR obtient une réponse qui correspond, l'abonné est inscrit dans le réseau.

La SIM crée également une autre clé temporaire appelée Kc. Sa valeur est calculée sur la base du RAND et du Ki mentionnés ci-dessus, à l'aide de l'algorithme A8. Cette clé est ensuite utilisée à son tour pour chiffrer des données transmises par l'algorithme A5.

Les noms de tous ces acronymes peuvent paraître un peu compliqués, mais l'idée de base est très simple : vous avez tout d'abord un identifiant et un mot de passe codés en dur dans la SIM, puis vous créez des clés de vérification et de chiffrement avec quelques trucs mathématiques et ça y est : vous êtes connecté !

Ce chiffrement est toujours activé par défaut, mais dans certaines circonstances (par exemple si un mandat est fourni), il peut être désactivé, ce qui permet qu'une agence de renseignement puisse intercepter les conversations par téléphone. Dans ce cas, les anciens dispositifs affichaient un cadenas ouvert, alors que les téléphones modernes (à part Blackberry) n'affichent aucune indication de ce type.

Il existe une attaque spécifiquement conçue pour intercepter les conversations téléphoniques ; pour la réaliser, l'adversaire a seulement besoin d'un appareil appelé IMSI Catcher qui imite une station de base et enregistre les téléphones qui se connectent avant d'envoyer tous les signaux vers une station de base réelle.

Dans ce cas, tout le processus d'autorisation se déroule de façon normale (il n'est pas nécessaire de décrypter les clés de chiffrement), mais la fausse station de base ordonne au dispositif de les transmettre sous forme de texte brut afin qu'un adversaire puisse intercepter les signaux sans que la compagnie ou l'abonné ne le sachent.

Cela peut paraître étrange, mais cette vulnérabilité n'en est pas vraiment une : en fait, cette fonctionnalité a été conçue pour faire partie du système depuis le début, afin que les services de renseignements puissent réaliser des attaques intermédiaires dans les cas appropriés… [Lire la suite]

Réagissez à cet article

Source : *L'évolution De La Carte SIM – Kaspersky Daily – | Nous Utilisons Les Mots Pour Sauver Le Monde | Le Blog Officiel De Kaspersky Lab En Français.*

---

# 2ème édition du Forum TAC, Technology Against Crime les 28 et 29 avril prochains à Lyon

# 2ème édition du Forum TAC, Technology Against Crime les 28 et 29 avril prochains à Lyon

**INNOVER POUR UN MONDE PLUS SUR, Tel est le slogan de la 2ème édition du Forum TAC, Technology Against Crime qui réunit les acteurs mondiaux de la Sécurité à Lyon, les 28 et 29 avril prochains**

Après le succès de la 1ère édition de 2013, le Forum international TAC, Technology Against Crime revient à Lyon en 2016, en présence du ministre de l'Intérieur, Bernard Cazeneuve, pour répondre à deux grands enjeux :
1/ Anticiper les menaces et répondre aux grands enjeux de sécurité
2/ Identifier et mettre en lumière les solutions de demain
Organisé autour de 3 menaces : cyber – crime organisé – terrorisme et de 3 solutions : l'innovation technologique – la coopération public/privé – la coordination internationale.
Le Forum TAC met en relation les besoins des donneurs d'ordres publics et privés et les solutions proposées par les entreprises et crée ainsi un dialogue de haut niveau axé sur la performance et l'innovation en matière de sécurité. Un événement au format unique qui associe des rendez-vous d'affaires, un Forum Innovation, des démonstrations, un espace networking, des cas pratiques et des interventions de haut niveau.

**500 participants sont attendus :**
• ministres, représentants d'Interpol et délégations officielles de plus de 190 pays
• forces de police et de sûreté internationales
• dirigeants et responsables de la sécurité de grands groupes industriels
• fournisseurs de solutions et services
• représentants institutionnels

**Parmi les nombreux sujets traités :**
• La protection des avions face aux cyber-attaques
• Le trafic d'êtres humains
• Le maintien de l'ordre et l'utilisation des media sociaux
• La protection des sites sensibles

En savoir plus : www.forum-tac.com

---

Réagissez à cet article

Source : Denis JACOPINI