Les clients de 12 banques suisses attaqués par des cybercriminels

Les clients de 12 banques suisses attaqués par des cybercriminels

Des pirates informatiques se sont lancés, depuis peu, dans une attaque d'envergure contre les comptes e-banking de douze banques suisses. Leurs méthodes sont perfides et laissent peu de traces, avertit Switch.

Le virus, de type cheval de Troie, a été nommé Retefe, a indiqué mardi Serge Droz, expert en sécurité auprès de l'organisme qui administre les noms de domaines en Suisse. Il confirmait une information parue sur le site Internet de la Handelszeitung. C'est l'entreprise de sécurité informatique Trend Mikro qui a rendu publique l'information sur l'attaque.

Le client de banque ouvre un spam – un courrier électronique indésirable – qui libère le virus. Le programme malicieux s'efface, une fois que l'infection a réussi. Aussitôt que le client ouvre une session e-banking, il est redirigé sur un mauvais serveur, sur lequel apparaît une copie de page Internet de sa banque. Le client entre alors ses informations de sécurité, qui sont désormais en main des malfaiteurs.

Lire la suite…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lematin.ch/economie/hackers-s-attaquent-clients-12-banques-suisses/story/16520131

Une manière de nous espionner sur Internet sans laisser de traces !

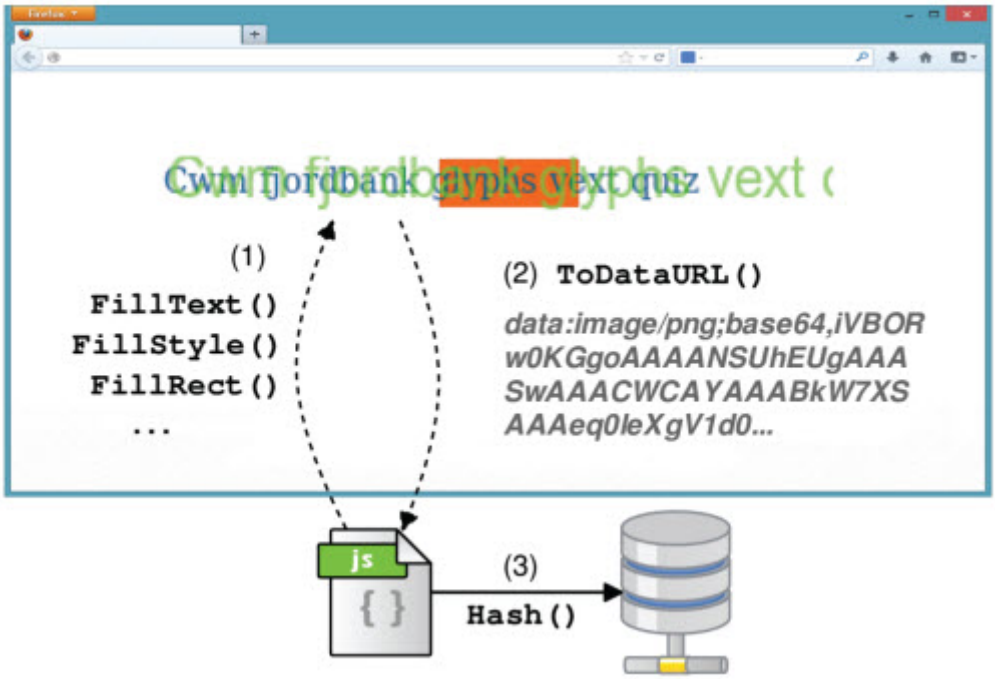
Depuis plusieurs années, le mécanisme de suivi des internautes qui récupère votre « empreinte numérique » est utilisé par la société AddThis. Il serait installé sur plus de 5000 sites Web parmi les plus consultés, et surtout difficilement contournable.

Atlantico, MetroNews, Letudiant, PAP, Telerama, Sports, Elle, LeGorafi… Ce sont autant de sites qui utilisent le fameux mécanisme d'empreinte numérique (la liste entière est consultable ici). Ce ne sont que quelques exemples français. Aux Etats-Unis, le site de la Maison-Blanche l'utilise également. S'il n'est pas tout à fait nouveau, il a été découvert assez récemment par des chercheurs des universités de Ku Leuven en Belgique, et de Princeton outre-Atlantique.

La nouveauté : il permet de traquer les internautes sans qu'ils s'en rendent compte et sans pouvoir y échapper. Car aucun mécanisme, une application tierce par exemple, ne permet de la contourner : le Graal pour les annonceurs, un fléau pour la vie privée ! Il existe toutefois des moyens d'y échapper, en bloquant le chargement des JavaScript sur votre navigateur, en utilisant NoScript par exemple, en choisissant Tor ou l'extension (expérimentale) Chameleon.

Le mécanisme de fonctionnement de l'empreinte numérique.
Cette technique d'empreinte numérique, décrite par des chercheurs californiens en 2012 (consultez le PDF du détail de la technique), est notamment proposée dans les outils de la société AddThis, qui fournit entre autres des boutons de partage vers les réseaux sociaux.

Le système est très simple en théorie. Lorsqu'un internaute se connecte sur un site Web, une requête est envoyée demandant au navigateur de « dessiner » une image invisible qui est ensuite transmise à AddThis par exemple. Il utilise la fonction Canvas de HTML5 (« canvas fingerprinting »). Et c'est grâce à cette image unique qu'il est possible de pister discrètement et individuellement chaque internaute.



Dans cet article, on peut y voir AddThis reconnaître avoir commencé à tester ce système depuis le début de l'année cherchant « une alternative aux cookies traditionnels ». Depuis la publication de l'article, certains sites ont fait marche arrière, à l'instar de YouPorn notamment.

Le PDG de l'entreprise estime que le mécanisme est tout à fait légal, même si les premiers résultats ne seraient pas satisfaisants, selon lui. AddThis se défend sur son blog, expliquant que le mécanisme est utilisé uniquement dans un but de R&D. Il nous tarde de connaître la réaction de la CNIL : un mécanisme divulgué à tous et incontournable semble difficile à imposer en toute légalité…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.linformaticien.com/actualites/id/33713/tous-traques

-addthis-nous-suit-a-la-trace-sans-laisser-de-traces.aspx

Les entreprises sous-estiment le risque juridique du Big Data

Les entreprises sous-estiment le risque juridique du Big Data

Pour le Boston Consulting Group (BCG) et le cabinet d'avocats DLA Piper dans leur étude sur « Le Big Data face au défi de la confiance » publiée le 18 juillet 2014, l'exploitation de très nombreuses données peut exposer l'entreprise à des risques juridiques et économiques méconnus.

De fait, ils constatent que la surveillance exercée à grande échelle par la NSA sur les communications électroniques et téléphoniques, la navigation sur Internet et les réseaux privés ou encore les services de Cloud américains et étrangers, a heurté un public déjà très sensibilisé aux problématiques de protection des données. Ils rappellent que «

certains acteurs clés d’Internet comme Google et Facebook ont été violemment critiqués après avoir modifié leurs règles de confidentialité ».

De plus, ils relèvent que la nouvelle réglementation européenne en cours d’élaboration aura « des incidences certaines sur les entreprises utilisant le Big Data (…). Le poids et le coût administratif du traitement de données pourraient augmenter. Cet ensemble de règles nouvelles pourrait aussi constituer une menace pour les stratégies de monétisation de données, diminuer l’innovation et réduire les opportunités futures ».

« Le Big Data face au défi de la confiance », 18 juill. 2014 ; Site de BCG

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/124969/Default.aspx

La CNIL autorise la collecte de prévention de la délinquance pour les Collectivités locales

La CNIL autorise la collecte de prévention de la délinquance pour les Collectivités locales

La CNIL a adopté une nouvelle autorisation unique n° AU-038 par une délibération du 26 juin 2014 « portant autorisation unique concernant les traitements de données relatifs aux personnes faisant l'objet d'un suivi par le maire dans le cadre de ses missions de prévention de la délinquance ».

Cette autorisation unique encadre uniquement les traitements mis en œuvre dans le cadre du fonctionnement des groupes relevant directement des pouvoirs du maire en la matière comme les conseils locaux de sécurité et de prévention de la délinquance (CLSPD) et les conseils pour les droits et devoirs des familles (CDDF).

Pour les traitements concernés, la délibération de la CNIL précise les finalités exactes qui peuvent être poursuivies et les utilisations qui doivent être exclues, notamment l'alimentation d'autres traitements locaux ou de fichiers nationaux.

Elle établit une liste limitative des données qui peuvent être collectées dans le cadre de ces fichiers et prévoit des conditions supplémentaires pour le traitement de certaines données sensibles du point de vue de la protection des données personnelles.

Elle liste également les seules personnes habilitées à connaître des informations collectées dans le cadre de la prévention de la délinquance, en distinguant les personnels pouvant disposer d'un accès direct aux traitements mis en œuvre, des personnes à qui ces informations peuvent être communiquées, pour certaines de manière ponctuelle uniquement.

L'autorisation unique n° AU-38 prévoit enfin une durée de conservation limitée, des modalités particulières d'information des personnes concernées ainsi que des mesures de sécurité adaptées à la sensibilité des traitements mis en œuvre.

Délib. CNIL n° 2014-262, 26 juin 2014, JO 22 juill. ; Site de la CNIL

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/124981/Default.aspx

Les objets connectés à notre e-santé dévoilent nos données personnelles

Les objets connectés à notre e-santé dévoilent nos données personnelles

Alors que la présence du wearable (ensemble des vêtements et accessoires comportant des éléments informatiques et électroniques avancés) croît rapidement et avec elle, la collecte d'informations de santé, la Commission fédérale du commerce américain s'inquiète de ce que peuvent devenir ces données très personnelles.

Samsung a SAMI, Apple a Healthkit Google a Google Fit.

Trois grands noms des smartphones et trois approches de l'e-santé qui ont pour point commun de recueillir, formaliser et stocker vos données de santé sur votre téléphone ou sur des serveurs.

Quoi de plus personnel que votre état de santé et ses indicateurs ? Quoi de plus précieux et éventuellement de plus

valorisés pour fournir des services complémentaires ?

Julie Brill, commissaire au sein de la Commission fédérale du commerce (FTC) s'inquiétait en tout cas de l'accélération de cette tendance qui va prendre encore plus d'importance avec la multiplication des montres et bracelets connectés. Pour elle, la façon dont les données sont « siphonnées » par ces applications est préoccupante. « Nous ne savons pas où ces informations vont en définitive », indiquait-t-elle devant un groupe de discussion organisé par le site politique The Hill. « Cela met les consommateurs dans une situation inconfortable », continuait-elle. La Commissaire a souligné devant le Congrès l'importance de voter une loi pour interdire la collecte d'informations personnelles sous de faux prétextes.

Le besoin de régulation ?

En mai dernier, la FTC rendait un rapport dans lequel elle indiquait qu'une bonne part des développeurs d'applications d'e-santé donnait accès aux données de santé collectées à des sociétés extérieures. Ainsi, l'étude menée sur douze applications de fitness et e-santé démontrait que ces informations électriques étaient partagées avec 76 entreprises différentes, y compris pour du marketing.

Face à un paysage si inquiétant et totalement dépourvu de cadre légal, la commissaire de la FTC s'inquiète que « personne ne parle de nouvelle réglementation ».

L'ACT, Association for Competitive Technology, lobby qui défend les intérêts des développeurs d'applications, craint

évidemment qu'une quelconque réglementation nuise à l'innovation. Morgan Reed, directeur exécutif de l'ACT, déclarait ainsi à l'occasion de ce groupe de discussion : « L'industrie de la santé mobile a besoin d'éduquer la FTC sur les apports positifs que peut avoir la collecte d'informations sur la santé. […] Si nous échouons dans ce rôle, la commission pourrait prendre des décisions qui pourraient dévaster les développeurs d'applications ».

Ci-dessous à la 34ème minute, Julie Brill, commissaire au sein de la Commission fédérale du commerce.

http://www.ustream.tv/recorded/50427445

Si les bénéfices de la surveillance régulière de notre santé sont indéniables, il va une fois encore faire attention à ne pas devenir un produit dans la stratégie marketing d'acteurs peu soucieux de nos vies privées. Pour éviter ces pièges, Julie Brill préconise qu'un gros effort pédagogique soit fourni, d'une part et d'autre part que les utilisateurs soient toujours informés des informations recueillies et partagées. Un effort de transparence pour les plus personnelles de nos données…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.01net.com/editorial/624302/e-sante-debut-de-la-bataille-pour-nos-donnees-entre-la-ftc-et-les-lobbies/#?xtor=EPR-1-NL-01net-Actus-20140724

Cybercriminalité : La Tunisie dispose de compétences hautement qualifiées pour lutter contre le terrorisme

La Tunisie dispose de compétences hautement qualifiées dans le domaine des technologies de l'information et de la communication (TIC) capables de protéger l'espace cybernétique de la Tunisie et de lutter contre la cybercriminalité et contre le terrorisme et la violence ». C'est en tout cas ce que vient de déclarer à l'agence TAP, le ministre de l'Enseignement supérieur, de la Recherche scientifique et des TIC, Taoufik Jelassi, en marge de la conférence participative sur la réforme de l'enseignement supérieur et l'employabilité, organisée dans la soirée du dimanche 20 juillet à Monastir.

M. Jelassi a soutenu que la sécurité informatique et cybernétique est une priorité nationale, notamment au cours de cette étape, ajoutant qu'il a été convenu, au terme d'une réunion, la semaine dernière avec des responsables de la sécurité de l'espace cybernétique, de soutenir davantage l'Agence technique des télécommunications (ATT). « L'agence assurera l'appui technique des investigations judiciaires dans le domaine de la cybercriminalité et appuiera les efforts des autorités judiciaires et sécuritaires dans la protection du pays », a-t-il dit.

Le ministre des TIC a par ailleurs indiqué que l'Agence technique des télécommunications veille sur la protection des citoyens et des intérêts supérieurs du pays 24h/24 et 7jours/7, conformément à la loi et sous contrôle judiciaire.

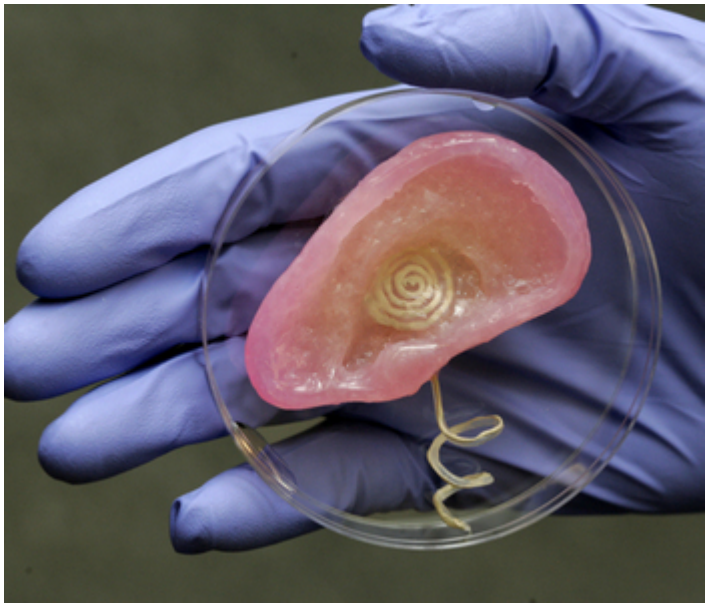
A noter que l'agence technique des télécommunications a été créée en vertu du décret 4506 en date du 6 novembre 2013..

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.webmanagercenter.com/actualite/technologie/2014/07/21/152736/terrorisme-la-tunisie-dispose-de-competences-hautement-qualifiees-pour-lutter-contre-le-terrorisme

Une oreille bionique fabriquée avec une imprimante 3D



Une oreille bionique fabriquée avec une imprimante 3D

Une équipe de chercheurs de l'université de Princeton a imprimé une oreille bionique mi-électronique mi-cartilage. © Frank Wojciechowski

En combinant l'impression 3D de matériaux électroniques, de plastique et de cartilage, des chercheurs de l'université de Princeton ont réussi à créer une « oreille » bionique. Cette oreille est capable de percevoir des fréquences inaudibles par un humain normal et ouvre donc la voie à des organes « augmentés », se réjouissent les chercheurs auteurs de cet exploit.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.journaldunet.com/economie/magazine/creations-en-3d/oreille-bionique.shtml

---

Le «Wall Street Journal» victime d’une cyberattaque – News High-Tech: Web – 24heures.ch

Le «Wall Street Journal» victime d’une cyberattaque

Le «Wall Street Journal» a annoncé dans la nuit de mardi avoir été victime d'une cyberattaque par un hacker qui proposait de vendre des codes d'accès au serveur du journal économique américain.

Dans son édition en ligne, le quotidien des affaires Wall Street Journal, indique que son service infographie a été «piraté par des tierces parties» tout en affirmant qu'aucun «dommage» n'a pour l'heure été constaté.

«A ce stade, nous ne voyons aucune preuve d'un quelconque impact sur les clients de Dow Jones ou sur les informations personnelles des clients», a assuré une porte-parole du journal, citée dans l'article.

Aucune altération sur des infographies (chartes, tableaux…) n'a par ailleurs été relevée mais le système est encore «en cours d'examen», assure le journal, précisant que plusieurs ordinateurs ont été mis hors ligne afin d'«isoler» les attaques.

Le Wall Street Journal (WSJ) dit avoir révélé cette intrusion informatique après sa «revendication» sur Twitter par un hacker qui offrait, moyennant finances, des informations de clients mais également des données permettant d'accéder au serveur du journal.

Selon Andrew Komarov, l'expert en cybersécurité qui a alerté le quotidien, un tel accès permettrait de «modifier des articles, d »ajouter des nouveaux contenus (…) et de supprimer des comptes d'utilisateurs».

Selon le WSJ, Andrew Komarov, patron de la firme californienne IntelCrawler, est sur les traces de ce pirate informatique qui s'est successivement fait connaître sous le pseudonyme de Rev0lver et de Worm et qui a fondé un marché noir des «failles informatiques» baptisé Worm.in.

Les Etats-Unis ont à plusieurs reprises alerté sur les dangers de la cybercriminalité et de son impact économique. Mi-juillet, le secrétaire au Trésor américain Jacob Lew avait ainsi affirmé qu'une cyberattaque «réussie» pourrait menacer la stabilité financière du pays.

Lire

L'évolution de l'homme passera t-elle par le Web ? Web 1.0 au Web 6.0

	L'évolution de l'homme passera t-elle par le Web ? Retour sur 20 ans d'évolution du Web et tendances à venir avec cet outil de communication extraordinaire mais aussi siège de nouveaux risques…

Le web est sans nul doute une technologie majeure du 21ème siècle. Et si sa nature, sa structure et son utilisation ont évolué au cours du temps, force est de constater que cette évolution a également profondément modifié nos pratiques commerciales et sociales.

Pour mieux comprendre les enjeux et les différentes phases de cette évolution, je me suis livrée pour vous à un exercice de synthèse, qui ne se veut en aucun cas exhaustif, mais qui devrait vous fournir quelques clés de compréhension.

Evolution du Web vs Evolution de l'homme ?

Retour sur 20 ans d'évolution et d'utilisation du Web, cet outil de communication extraordinaire mais aussi siège de nouveaux risques…

Au fil de mes lectures, discussions, émissions, conférences ou tables rondes, de plus en plus de personnes me parlent de web 3.0, voire même 4.0!

Et si tout le monde s'accorde à dire que les Web 3.0 et 4.0 sont les prochaines phases de l'évolution du Web que nous connaissons, les avis sont loin de converger quant à la chronologie ou aux concepts et technologies propres à chaque étape.

Mais une chose est sûre : l'accélération remarquable de cette évolution est d'autant plus vertigineuse que je constate, dans la pratique, que bien des PME peinent à intégrer la seule notion de web 2.0 !

Il m'a donc semblé utile de revenir sur l'évolution d'Internet vous aider à mieux comprendre les enjeux et l'importance de

cette transformation, ainsi que son impact sur la manière de gérer préparer l’avenir.

Le Web 1.0 des années 90 (Le Web Passif ou Web traditionnel)

Souvenez-vous ! Le Web 1.0, celui des années 90, a un fonctionnement très linéaire : un contenu proposé par un producteur est affiché sur un site Internet consulté par des internautes. C’est un web statique et passif : les sites internet sont centrés sur la distribution d’information consommée passivement par l’internaute comme on peut le faire dans un bibliothèque par exemple
Le Web à ce stade se caractérise par des sites orientés produits, qui sollicitent peu l’intervention des utilisateurs. Les premiers sites d’e-commerce datent de cette époque. Le coût des programmes et logiciels propriétaires est énorme et l’explosion de la bulle internet en 2000 remet en question cette approche de la toile.

Le Web 2.0 des années 2000 à 2009 (Le Web collaboratif)

Au début des années 2000 apparaît l’avènement du web 2.0. Le rêve de Tim Berners-Lee (principal inventeur du World Wide Web (WWW) au tournant des années 1990) devient réalité : les internautes ne sont plus seulement consommateurs passifs, mais contribuent activement d’une part à la création de contenus, mais aussi à la validation de leur valeur.

Les blogs apparaissent (Blogger en 1999 – racheté par Google en 2003, Skyblog en 2002), les forums se développent (phpBB, 2000), ainsi les wiki (Wikipédia, 2001), et sans oublier les réseaux sociaux (MySpace en 2003, Facebook en 2004)…

Complément :
On attribue communément à Wikipédia le statut de premier site collaboratif d'envergure, marquant la date effective de naissance du web 2.0.

Le Web 3.0 de 2010 à ? (Le Web sémantique ou « smart » Web)

La bataille est rude entre les experts pour se mettre d'accord sur ce que sera le futur du web. Ce qui est certain, c'est que ce web sera technologique : les machines et les individus sont de plus en plus connectés entre eux. Nous avons déjà les smartphones, les tablettes, et on voit arriver doucement mais sûrement la connexion à Internet de nos outils de tous les jours : les réfrigérateurs, les voitures, les chaussures aussi…

Ce futur Web vise à organiser la masse d'informations disponibles en fonction du contexte et des besoins de chaque utilisateur, en tenant compte de sa localisation, de ses préférences, etc. C'est un web qui tente de donner sens aux données. C'est aussi un web plus portable et qui fait de plus en plus le lien entre monde réel et monde virtuel. Il répond aux besoins d'utilisateurs mobiles, toujours connectés à travers une multitude de supports et d'applications malines ou ludiques, l'ensemble créant et échangeant automatiquement des données (géolocalisation, goût, reconnaissance faciale…).

Les sites Internet deviennent des applications en ligne qui

savent analyser automatiquement les contenus écrits et picturaux, qui savent les interpréter, les comprendre, les classer et les rediffuser vers un nouveau public internaute. L'ensemble des données devenant par le fait des outils, on parle donc de web sémantique.

Le Web 4.0 ou HyperWeb ? de 2020 ? à ?

Le web 4.0, évoqué par certains comme le web intelligent, effraie autant qu'il fascine, puisqu'il vise à immerger l'individu dans un environnement (web) de plus en plus prégnant. Il pousse à son paroxisme la voie de la personnalisation ouverte par le web 3.0 mais il pose par la même occasion de nombreuses questions quant à la protection de la vie privée, au contrôle des données, etc. C'est un terrain d'expérimentation où tous ne sont pas (encore) prêts à s'aventurer!

Et l'évolution de l'homme dans tout ça me direz-vous ?

Je vous laisse ouvrir les yeux et imaginer…

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Références :

http://www.univ-bpclermont.fr/Ressources_Num/Les_reseaux_sociaux_web_web/co/1-2_Web2.html
http://fr.wikipedia.org/wiki/Tim_Berners-Lee
http://c-marketing.eu/du-web-1-0-au-web-4-0/

Piratage informatique d'une banque : 500 000 euros dérobés aux clients d'une banque européenne

	Piratage informatique d'une banque : 500 000 euros dérobés aux clients d'une banque européenne *Une banque européenne s'est fait dérober 500 000 euros en l'espace d'une semaine suite à une fraude réalisée à l'aide d'un cheval de Troie.*

Piratage informatique d'une banque : 500 000 euros dérobés aux

clients d’une banque européenne

Une banque européenne s’est fait dérober 500 000 euros en l’espace d’une semaine suite à une fraude réalisée à l’aide d’un cheval de Troie.

500 000 euros en 7 jours, tel est le butin que des cybercriminels ont réussi à subtiliser à une grande banque européenne dont l’identité n’est pas connue. C’est l’éditeur Kaspersky qui a découvert la fraude qui aurait eu cours entre le 13 et le 20 janvier.

Un cheval de Troie, surnommé Luuuk, a servi à collecter les données bancaires de quelque 190 clients basés en Italie et en Turquie. Le trojan a semble-t-il été injecté via une attaque de type « man-in-the-browser » afin de pouvoir déclencher des transactions en arrière-plan à l’insu des victimes. Les sommes étaient envoyées sur des comptes fictifs créés à cet effet puis l’argent était ensuite retiré en espèces à des distributeurs.

Deux jours après avoir découvert un serveur de commande et de contrôle, Kaspersky a averti la banque concernée. Mais les cybercriminels avaient eu le temps d’effacer toute trace pouvant permettre de remonter jusqu’à eux, ce qui laisse penser que cette fraude est peut-être toujours en cours. (Eureka Presse)

Cet article vous à plu ? Laissez-nous un commentaire
(notre source d’encouragements et de progrès)

Références :

http://www.zdnet.fr/actualites/cyberfraude-500-000-euros-derobes-aux-clients-d-une-banque-europeenne-39803001.htm