

Plus de 2 millions d'internautes victimes de phishing en 2015 | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p>vous informe...</p>	<p>Plus de 2 millions d'internautes victimes de phishing en 2015</p>
--	--

Pour renforcer la lutte contre le phishing, le Ministère de l'Intérieur a signé le 5 novembre, une convention de partenariat avec l'association Phishing Initiative, soutenue par Lexsi et Microsoft France. Cet accord vise à mutualiser les informations entre sa propre plateforme, PHAROS, et celle de Phishing Initiative qui a identifié de son côté plus de 150 000 adresses uniques de sites frauduleux visant la France depuis sa création en 2011.

Une convention commune pour renforcer la lutte contre le Phishing

En signant la convention de lutte anti-phishing, Catherine Chambon, sous-directeur de la lutte contre la cybercriminalité et Jérôme Robert, président de Phishing Initiative souhaitent renforcer la sensibilisation des internautes aux risques liés à cette malveillance majeure. « La complémentarité de nos actions rend évidente la nécessité d'un rapprochement et d'une coordination entre nos deux organisations », explique Jérôme Robert. « PHAROS et Phishing Initiative opèrent en effet tous deux des plateformes de signalement à destination du grand public. Il est par conséquent possible d'instaurer des conditions de partage de l'information de manière à optimiser d'une part, la recherche de données et d'autre part, la protection de l'internaute. »

Suite à la signature de cette convention et à l'engagement des parties prenantes, le Ministère de l'Intérieur et Phishing Initiative travailleront également à la rédaction d'un rapport commun et à l'élaboration d'un suivi des tendances au service de la protection des internautes.

Phishing Initiative et PHAROS : l'union des expertises

Elaborée et construite sous l'impulsion de Madame Catherine Chambon, Madame Valérie Maldonado, chef de l'OCLCTIC, Messieurs Jérôme Robert, Directeur Marketing, Vincent Hinderer, Expert Cybersécurité chez Lexsi, et Bernard Ourghanlian, directeur technique et sécurité de Microsoft, la convention a pour objectif d'augmenter le nombre d'URLs traitées et analysées. Avec respectivement 60 000 et 30 000 URLs traitées depuis début 2015, Phishing Initiative et PHAROS unissent leurs forces pour protéger les internautes et rendre le web plus sûr. « L'association de nos dispositifs de lutte contre la fraude sur Internet représente une avancée majeure dans la protection des particuliers comme des entreprises » précise Bernard Ourghanlian de Microsoft France. « Face à la malveillance et à la fraude organisée, chaque citoyen et chaque entreprise est acteur d'un Internet plus sûr au bénéfice de tous. » La Sous-Direction de la Lutte contre la Cybercriminalité (SDLC) a développé deux dispositifs destinés aux particuliers : la Plateforme d'Harmonisation d'Analyse et de Recoupement et d'Orientation des Signalements (PHAROS), lancée en janvier 2009, et Info-Escroqueries, une hotline téléphonique dédiée aux arnaques. PHAROS a notamment pour mission de recueillir et traiter les signalements de contenus et de comportements illicites détectés sur Internet.

Phishing Initiative, un programme de lutte européen

Cofinancé par le Programme de Prévention et de Lutte contre le Crime de l'Union Européenne, Phishing Initiative offre à tout internaute la possibilité de lutter contre les attaques d'hameçonnage en signalant de manière simple les liens lui paraissant suspects en un clic sur www.phishing-initiative.fr.

Chaque signalement fait l'objet d'une analyse par les experts Lexsi qui, s'il se révèle frauduleux, est transmis aux partenaires de Phishing Initiative, notamment Microsoft. Ces derniers enrichissent alors leurs listes noires, de sorte que le lien frauduleux est bloqué par les principaux navigateurs Web (Edge, Internet Explorer, Chrome, Firefox et Safari).

Phishing Initiative en chiffres

A ce jour, plus de 400 000 adresses suspectes ont été signalées dans le cadre de la Phishing Initiative, dont plus de 300 000 uniques. Depuis le début de l'année 2015, 110 000 signalements ont déjà été transmis, représentant plus de 60 000 nouvelles adresses uniques. Parmi elles, plus de 35 000 URLs uniques ont été confirmées comme faisant partie d'une campagne de phishing, soit près de 120 adresses distinctes par jour. A noter que le temps médian nécessaire aux analystes pour catégoriser un nouveau cas signalé est de moins de 20 minutes. Microsoft rafraîchit sa liste noire toutes les 20 minutes au sein d'Internet Explorer et Edge, ce qui protège en moyenne les internautes en moins de 40 minutes suite à un signalement sur www.phishing-initiative.fr.

Des milliers d'internautes contribuent anonymement à ce projet chaque année et plusieurs centaines d'individus ont créé depuis la rentrée un compte personnel sur le site Phishing Initiative. Il leur permet désormais de signaler des URLs suspectes plus simplement et d'accéder à des informations, statistiques et services additionnels, relatifs notamment aux signalements effectués par leurs soins. Ces internautes peuvent, par exemple, suivre l'état du site en temps réel et demander à être prévenus du caractère frauduleux ou non d'une adresse ainsi soumise, mais surtout participer à la lutte anti-phishing et empêcher que d'autres internautes soient victimes de ce fléau.

A propos de Phishing Initiative

Créé sous l'impulsion conjointe du cabinet Lexsi, de Microsoft et de PayPal Europe en 2011, Phishing Initiative, association à but non lucratif, offre à tout internaute la possibilité de vérifier un site suspect et lutter contre les attaques de phishing. En signalant l'adresse d'un site suspecté d'héberger un cas de phishing francophone, vous contribuez à diminuer l'impact de cette cybercriminalité en évitant que d'autres internautes soient piégés par ces attaques. Chaque adresse différente fera en effet l'objet d'une vérification humaine et si confirmée comme frauduleuse d'un envoi pour blocage dans les listes noires des principaux navigateurs Plus d'informations sur : <https://phishing-initiative.fr>

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet.. ;
 - **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
 - **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
- Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : <http://www.globalsecuritymag.fr/Plus-de-2-millions-d-internautes,20151105,57293.html>

Une vulnérabilité dans les Cartes bancaires connue et exploitée discrètement | Le Net Expert Informatique



Des chercheurs viennent de publier un rapport d'étude sur l'exploitation concrète mais discrète d'une vulnérabilité affectant les cartes EMV et connue depuis plus de 5 ans.

Combien de cas réellement constatés ? Combien de cas non constatés ? C'est la question que soulève l'étude que viennent de publier Houda Ferrradi, Rémi Géraud, David Naccache et Assia tria, de l'Ecole normale supérieure et du CEA-TEC Paca.

Dans celle-ci, les quatre chercheurs se penchent des cartes bancaires EMV modifiées pour permettre leur utilisation sans en connaître le code PIN, en toute discrétion, grâce à deux puces câbles l'une sur l'autre, sur la puce d'origine : « la première puce est clipsée sur une carte authentique volée. La seconde puce joue le rôle d'intermédiaire et communique directement avec le terminal de point de vente. L'ensemble est intégré au corps en plastique d'une autre carte également volée ».

Le concept est connu depuis début 2010. C'est le chercheur Steven J. Murdoch, de l'université de Cambridge qui avait levé le voile sur une vulnérabilité potentiellement grave des cartes bancaires à puces dites EMV.

Une faille qui « permet à un fraudeur d'utiliser une carte de paiement à puce volée pour régler un achat, via un terminal de paiement électronique non modifié, sans connaître le code PIN du porteur légitime de la carte bancaire ». Ainsi, un dispositif électronique intercepte et modifie les communications entre la carte à puce et le terminal de paiement électronique. Lorsque celui-ci demande à la carte de vérifier le code PIN saisi par l'utilisateur, le dispositif du pirate intercepte la requête et se charge, à la place de la carte, de répondre au TPE que le code a été vérifié et confirmé. Voilà ce que décrivait alors, par le menu, le chercheur britannique dans un rapport d'étude préliminaire.

Lors d'un entretien téléphonique avec LeMagIT, Steven J. Murdoch évoquait alors l'ampleur de la menace : « le reçu indique que la transaction a été autorisée par code PIN », du moins était-ce le cas lors de ses tests au Royaume-Uni, pour des transactions de type offline comme online – à savoir, avec ou sans connexion aux serveurs de contrôle des transactions. Un détail lourd de conséquences : même armé d'une déclaration de perte ou de vol, comment le porteur légitime de la carte pourra-t-il dégager sa responsabilité face à un banquier qui ne manquera pas de lui rappeler qu'il est responsable de la confidentialité de son code PIN ?

Pour Steven J. Murdoch, le risque était notamment que « d'autres aient découvert la faille avant nous ». La lecture du rapport des quatre chercheurs français nous apprend qu'environ 40 modifications frauduleuses de cartes, exploitant la vulnérabilité dévoilée par Murdoch, ont été découvertes en 2011 : « en mai 2011, le GIE Cartes Bancaires a relevé qu'une dizaine de cartes EMC, volées en France quelques mois plus tôt, étaient utilisées en Belgique. Une enquête de police a été ouverte ». Le montant de la fraude liée à cette opération : un peu moins de 600 000 € sur plus de 7 000 transactions.

Début 2010, sans surprise, le GIE Cartes Bancaires minimisait toutefois la menace, estimant qu'elle « nécessitait des équipements qui ne sont pas très discrets ». Certes, la carte frauduleuse présente une puce d'apparence plus épaisse que la normale. Mais au moins dans le cas de cette fraude ayant fait l'objet d'une enquête, cela n'a pas éveillé de soupçons.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lemagit.fr/actualites/4500256061/Cartes-bancaires-une-vulnerabilite-con nue-exploitee-discretement>
par Valéry Marchive

Une famille valaisanne a volé en éclats après que le père a été victime d'un arnaqueur | Le Net Expert Informatique



Une famille valaisanne a volé en éclats après que le père a été victime d'un arnaqueur.

«C'est quarante ans de mariage et de vie de famille mis à la poubelle.» La voix de Suzanne est emplie de larmes. En six mois, sa famille a volé en éclats. La faute à une arnaque sur le Web.

«Début 2015, j'ai entendu mon père passer un coup de fil pour faire verser une grosse somme d'argent au Mali via Western Union», raconte la Valaisanne. Intriguée, Suzanne prévient son frère, puis sa mère.

Ensemble, ils vont découvrir que le père de famille est en réalité victime d'une escroquerie via Internet. «Il croit discuter avec une Française partie vivre au Mali. Il l'a rencontrée sur un jeu en ligne», explique la Valaisanne. La prétendue expatriée, mère de famille et veuve, jure avoir hérité de près d'un million de francs. Seul problème, pour débloquer la somme, elle a besoin d'un petit investissement de départ. «Papa a déjà versé plusieurs dizaines de milliers de francs. Heureusement, on a réussi à faire bloquer les comptes pendant un temps», détaille la Valaisanne. Elle a bien essayé de discuter avec son père, mais le résultat a été catastrophique. «Il s'est énervé et il a quitté la maison. Il est persuadé que tout est vrai», soupire-t-elle. Le père n'a donc plus aucun contact avec le reste de la famille, surtout que les parents de Suzanne se sont officiellement séparés en juin dernier.

La juge, tout comme la police avant elle, a bien essayé de raisonner le sexagénaire, mais rien n'y fait. «Pourtant, il est loin d'être bête, mais là c'est gros comme un camion et il ne voit rien», assure Suzanne. Au point qu'elle se demande s'il se rendra compte un jour qu'il s'agit d'une arnaque. «Il a tellement peur qu'elle l'abandonne qu'il continue de verser encore et encore», précise la Valaisanne. Mais le plus dur pour elle, c'est le côté humain. «On est désemparés et on ne comprend pas. Il a toujours été plutôt radin, et là, il dépense des fortunes pour une femme qu'il ne connaît pas. Il rêve même de faire baisser la pension alimentaire de ma mère parce qu'il n'a plus un rond à lui envoyer», souligne-t-elle.

Aujourd'hui, Suzanne ne sait plus quoi faire. Elle regrette le manque de structures de soutien en Suisse. «Il n'y a rien ni personne pour nous aider. Je suis fatiguée par cette histoire. Cela me rend malade.»

Une détresse que comprend André Frachebourg, responsable sécurité d'un établissement bancaire et connaissance de la famille. «Les enfants ont un sentiment d'impuissance. Leur père ne croit plus ce que ses proches disent, il n'écoute plus personne», témoigne-t-il. Lui-même a essayé de raisonner le sexagénaire. En vain. «Il est dans ce qu'on appelle un effet «tunnel», analyse-t-il.

En tant que responsable sécurité, il a régulièrement affaire à ce genre de cas: «Il y a des victimes de tout âge. Nous, on essaie de faire des mises en garde quand on voit qu'il y a des sommes inhabituelles qui sortent», explique-t-il.

André Frachebourg regrette que le phénomène soit encore aussi tabou en Suisse: «Souvent, les victimes n'osent pas en parler. Elles ont honte d'avoir été grugées. Il devrait y avoir un soutien plus fort pour elles», conclut-il.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : <http://www.lematin.ch/suisse/On-est-desempares-on-ne-comprend-pas/story/12808386>

L'arnaque de 1,6 million d'euros menace de couler BRM | Le Net Expert Informatique



L'arnaque de 1,6 million d'euros menace de couler BRM

Le cauchemar que vivent les 44 salariés de BRM (Bressuire) semble irréal. Victime d'une arnaque au président que l'on croit habituellement réservée aux grosses entreprises et aux magazines à sensation, ils sont pourtant menacés de chômage suite à la disparition de près de 1,6 millions d'euros des caisses de l'entreprise de fabrication de meubles.

L'escroquerie a été découverte le 1er septembre dernier par la direction. A quelques heures d'un comité d'entreprise de rentrée habituel, Jean Brossier, son PDG, a découvert que les comptes avaient été vidés de leur contenu dans l'été. « Lors de ce comité d'entreprise, la direction ne savait pas encore ce qui s'était passé », racontent les représentants du personnel. « Ils nous ont demandé de leur laisser le temps de déterminer ce qui s'était passé. Mais la situation a été officialisée deux jours plus tard, le 3 septembre, lors d'un comité d'entreprise extraordinaire. »

Une arnaque à 1,6 millions d'euros

Le scénario reconstitué par la direction est classique. Entre le 21 juillet et le 14 août, un escroc a usurpé le compte mail de Jean Brossier puis contacté par téléphone l'entreprise sous le sceau de la confidentialité. Il prétendait être le représentant d'un cabinet d'expertise comptable et d'un avocat et agir dans le cadre d'une stratégie de rachat d'une entreprise par BRM. Il a ainsi obtenu plusieurs versements d'un montant total de près de 1,6 million d'euros. « Nous pensons qu'on espionnait nos comptes mails parce que cette escroquerie est survenue au moment où nous avions reçu les règlements de plusieurs grosses commandes », supposent les représentants du personnel.

« Nous demandons à ce que la chaîne des responsabilités soit clairement établie par l'enquête. Nous sommes convaincus qu'il y a plusieurs responsables et que cette situation résulte d'un défaut de contrôle ou de procédure. Nous ne voulons pas faire porter le chapeau à une seule personne. »

La direction leur a annoncé le 3 septembre dernier avoir déposé plainte auprès du procureur de la République de Niort et, lors d'un comité d'entreprise extraordinaire hier, elle a annoncé son intention de déposer le bilan au tribunal de commerce de Niort. Jean Brossier, qui s'est rendu au tribunal de commerce, était d'ailleurs injoignable ce matin. Les représentants du personnel envisagent aussi de se joindre à la plainte pour escroquerie.

C'est un gâchis.

Pour l'heure, le choc et la consternation sont énormes pour les 44 salariés de l'entreprise de la zone Saint-Porchaire à Bressuire (durement touchée récemment). « Nous vivions depuis plusieurs années mais 2015 était plutôt meilleure. Nous avons des marchés et des projets », racontent les représentants du personnel. « Mais Mecaseat (maison mère belge) nous a déjà annoncé ne plus vouloir injecter de nouveaux fonds dans BRM. Il reste deux hypothèses : soit nous trouvons un repreneur soit nous sommes liquidés. On ne peut plus payer les fournisseurs. »

Certains veulent toutefois être optimistes. « Nous sommes en contact avec les élus et les représentants de l'Etat pour la suite qui doit suivre deux étapes : la nomination rapide d'un administrateur pour que l'activité puisse redémarrer puis la recherche d'une solution de reprise. » Mais ils ne se font guère d'illusions. « Nous avons un sentiment d'amertume. Nous avons tellement porté cette entreprise. C'est un gâchis. »

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.


Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lanouvellerepublique.fr/Deux-Sevres/Actualite/Faits-divers-justice/n/Contenus/Articles/2015/09/08/L-arnaque-de-1-6-million-d-euros-menace-de-couler-BRM-2456884>
Par Dominique Guinefoleau

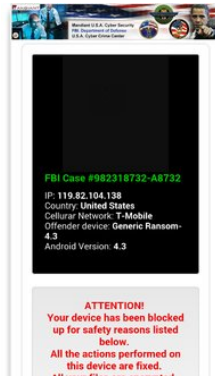
Insolite : Une application porno fait du racket – Un Racketware ? | Le Net Expert Informatique

 <p>Insolite : Une application porno fait du racket – Un Racketware ?</p>	
---	--

Adult Player, une prétendue application mobile de pornographie, dérobe des clichés de ses utilisateurs avant de les obliger à payer 500 dollars pour débloquent leur smartphone.

On le sait, smartphone et pornographie font bon ménage. Récemment, d'après une étude du cabinet Juniper Research, plus de 136 milliards de vidéos X devraient être consultées depuis des terminaux mobiles en 2015, soit 348 vidéos par utilisateur. Ce chiffre devrait s'élever à 193 milliards en 2020. Une application malveillante a choisi de surfer sur cette tendance.

Le spécialiste de la sécurité Zscaler explique sur son site avoir découvert l'application Adult Player, ciblant les smartphones Android. Il s'agit plus précisément d'un ransomware, c'est-à-dire que ses concepteurs effectuent une forme de racket auprès des victimes.



Adult Player se fait passer pour un lecteur de vidéos pornographiques mais effectue des clichés de ses victimes à leur insu en exploitant la caméra frontale de l'appareil. Par la suite, l'application bloque le smartphone et présente la photo sur l'écran de verrouillage tout en demandant une rançon de 500 dollars. Pour désinstaller cette application malveillante, il faudra redémarrer le smartphone en safe mode, c'est-à-dire sans exécuter les applications tierces. Rendez-vous ensuite dans les Paramètres > Sécurité > Administrateur pour désactiver les droits alloués à Adult Player. Ensuite, toujours dans les paramètres, rendez-vous dans Applications > Désinstaller.



Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : <http://www.clubic.com/insolite/actualite-778656-insolite-application-porno-racket.html#pid=22889469>
Par Guillaume Belfiore

Top 5 des arnaques du moment en Côte d'Ivoire | Le Net Expert Informatique



Top 5 des arnaques du moment en Côte d'Ivoire

A mi-parcours de son activité 2015, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) dans un souci de prévention, vous présente à travers cet article, les arnaques auxquels vous pourriez être confronté, parce que prisées par les cyberdélinquants. Voici le top 5 des arnaques du semestre écoulé, en nombre de dossiers traités, sur les 491 dossiers reçus par la PLCC, et leurs préjudices enregistrés, sur les 1 milliard 199 millions 319 milles 880 Fcfa de dommage subit par les victimes des 6 premiers mois de l'année 2015.

1- L'ACCÈS FRAUDULEUX À UN SYSTÈME D'INFORMATION

Cette arnaque concerne les détournements de transfert d'argent. C'est une escroquerie qui consiste pour le cyberdélinquant à faire à votre insu le retrait d'une somme d'argent qui vous est destinée via une institution de transfert d'argent. Elle occupe la première place de notre classement, avec 91 dossiers traités par la PLCC, pour un préjudice estimé à 68 millions 903 milles 772 F CFA. Ce sont les populations ivoiriennes qui sont surtout touchées par cette infraction »nouvelle «.

2- FRAUDE SUR LE PORTEFEUILLE ÉLECTRONIQUE

Elle s'est développée avec l'avènement des services Mobile Money proposés par les compagnies de téléphonie mobile dans nos pays africains. Les cyberdélinquants s'attaquent au portefeuille électronique des utilisateurs en vidant leur compte. Avec 86 dossiers et un préjudice estimé à 37 millions 906 milles 300 F CFA, cette arnaque occupe la seconde marche du podium. Toujours avec les populations ivoiriennes qui prennent la place de victime numéro un des cyberdélinquants depuis un certain temps (voir article CYBERCRIMINALITÉ EN CÔTE D'IVOIRE: LESIVOIRIENS, PLUS TOUCHÉS PAR LES ARNAQUES).

3- L'ARNAQUE AUX FAUX SENTIMENTS

Considérée comme la »mère « des arnaques sur internet, l'arnaque aux faux sentiments, bien qu'elle soit la plus connue, continue de faire des victimes. C'est une escroquerie qui consiste pour le cyberdélinquant à utiliser les sentiments amoureux de leur proie pour leur soutirer de l'argent.

Si en nombre de dossier la baisse est significative par rapport aux semestres des années antérieures (59 dossiers reçus), elle continue d'affoler les compteurs en terme de préjudice avec 448 millions 431 milles 586 F CFA seulement pour le premier semestre 2015 soit 37,39 % du préjudice totale, toute catégorie confondue, du premier semestre 2015, estimé à 1 milliard 199 millions 319 milles 880 Fcfa.

4- LE CHANTAGE À LA VIDÉO

Classé 4ième, le chantage à la vidéo peut être vue comme une résultante de l'arnaque aux faux sentiments. Le cyberdélinquant menace de divulguer des photos ou vidéo à caractère sexuelle de vous, prise dans l'intimité d'une relation.

Avec 54 dossiers, pour un préjudice de 66 millions 832 milles 324 F CFA, cette arnaque touche de plus en plus les Ivoiriens.

5- L'ARNAQUE AUX FAUX HÉRITAGES

La dernière place de ce top 5 revient à l'arnaque aux faux l'héritage. L'une des plus vieilles ruses utilisée par les cyberdélinquants. Et pourtant, elle continue de faire des victimes. C'est une escroquerie ou tentative d'escroquerie, à la fois très ancienne et très commune encore aujourd'hui. Les escrocs vous envoient un mail vous informant que vous avez été choisi pour toucher un fabuleux héritage providentiel. Ce sont 37 dossiers qui ont été introduit à la PLCC, pour un préjudice qui s'élève à 407 millions 920 milles 762 F CFA. Le nombre d'affaires et le montant des préjudices liés à ces infractions indiquent que le travail de sensibilisation contre la cybercriminalité doit se poursuivre. Car bien que la majorité de ces arnaques soit connue et expliquée à travers la toile, elles sont encore nombreuses ces personnes qui se laissent duper par les cyberdélinquants. Une fois de plus la PLCC vous invite à la prudence !!!

lu sur <http://cybercrime.interieur.gouv.ci/>

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous


Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :

http://www.imatin.net/article/societe/broutages-cybercriminalite-en-cote-d-rsquo-ivoire-voici-le-top-5-des-arnaques-du-moment_30029_1440509278.html

Fausses police et gendarmerie

aident à rembourser l'argent perdu des victimes d'arnaque de Côte d'Ivoire et Bénin | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Fausses police et gendarmerie, aident à rembourser l'argent perdu des victimes d'arnaque de Côte d'Ivoire et Bénin</p>
--	---

Kaspersky trompe ses client avec de faux virus ? | Le Net Expert Informatique



Kaspersky trompe ses client avec de faux virus ?

Deux ex-employés de l'éditeur accusent Kaspersky d'avoir inondé ses concurrents de fichiers spécialement conçus pour tromper leur algorithme de détection de malwares. Et créer de faux positifs chez les utilisateurs.

Selon Reuters, Kaspersky a tenté de faire passer des fichiers bénins pour malicieux afin de tromper les capacités de détection de ses concurrents sur le marché des antivirus. Ces affirmations, très graves pour l'éditeur russe, se basent sur les déclarations à nos confrères de deux ex-employés de la société basée à Moscou, aujourd'hui parmi les leaders mondiaux des logiciels de sécurité.

Cette duperie, qui aurait démarré il y a plus de dix ans – avec un pic entre 2009 et 2013 -, ciblait notamment les antivirus de Microsoft, AVG ou Avast et visait à les inciter à effacer des fichiers importants sur les PC de leurs utilisateurs. Les deux sources de nos confrères, qui demeurent anonymes, affirment que des chercheurs ont été affectés à ces sabotages pendant des semaines ou des mois, avec pour tâche principale la rétro-ingénierie des technologies de détection des concurrents ciblés. Une étape indispensable à la mise au point de faux positifs.

Intoxiquer la concurrence

Reuters assure que, dans certains cas, la décision a été prise par Eugene Kaspersky en personne (en photo ci-dessus), le fondateur de l'éditeur russe souhaitant se venger de concurrents qui, selon lui, se contentaient d'imiter sa technologie. La société a démenti ces pratiques, assurant « n'avoir jamais mené de campagne secrète pour tromper des concurrents avec de faux positifs (des fichiers bénins identifiés comme malwares, NDLR) ».

En 2010, Kaspersky s'était plaint de l'exploitation que ses concurrents faisaient de ces travaux. A l'appui de sa démonstration, l'éditeur avait créé 10 fichiers sans risque et les avaient déclarés comme malicieux à VirusTotal, l'outil de partage d'informations sur les menaces de Google. Une semaine et demi plus tard, 14 fournisseurs d'outils de sécurité estimaient ces fichiers dangereux, suivant aveuglément les conclusions de la société russe, selon Kaspersky.

D'après les deux sources de Reuters, Kaspersky ne se serait pas arrêté à cette opération de communication. La société injectait ainsi du code malicieux dans des fichiers fréquemment rencontrés sur les PC puis les signalait anonymement à VirusTotal dans l'espoir de voir les antivirus concurrents assimiler ces fichiers essentiels au fonctionnement d'un PC à des malwares.

Pratiques connues

Reuters affirme par ailleurs que Microsoft, AVG et Avast lui ont confirmé que des tiers non identifiés avaient tenté d'introduire de faux positifs dans leur mécanisme de détection au cours des dernières années. Dennis Batchelder, qui dirige la recherche antimalware de Microsoft, a ainsi expliqué à Reuters avoir identifié, à partir de mars 2013, des fichiers altérés afin de paraître malicieux. Et d'affirmer que ses équipes ont isolé des centaines, voire des milliers de cas de la sorte. Sans toutefois faire un quelconque lien avec Kaspersky. Plus largement, aucun concurrent du Russe n'a émis de commentaire sur l'implication éventuelle de la société moscovite.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.silicon.fr/kaspersky-accuse-infecte-concurrents-faux-virus-124122.html#LJcrRvhoptort4dm.99>

Attention aux fausses mises à jour de Windows 10 dissimulant des Ransomware !

| Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p>vous informe...</p>	<p>Attention aux fausses mises à jour de Windows 10 dissimulant des Ransomware !</p>
---	---

Il n'a pas fallu longtemps pour voir apparaitre les premières tentatives d'escroquerie autour de la mise à jour vers Windows 10 proposée par Microsoft depuis le 29 juillet 2015. Une première campagne de Ransomware vient d'être détectée.

Cette campagne s'appuie sur l'actualité brûlante du moment, à savoir le lancement de la version finale de Windows 10 par Microsoft. L'objectif est de tromper les utilisateurs au sujet du téléchargement de la mise à jour gratuite. Il télécharge en réalité des fichiers malveillants sur leurs ordinateurs.

Définition d'un Ransomware selon Wikipédia:

Un Ransomware ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Windows 10, un contexte idéal pour les Ransomware

Disponible depuis quatre jours seulement, Windows 10 est désormais installé sur des dizaines de millions d'ordinateurs et Microsoft entrevoit une accélération de la demande. Windows 10 est l'actualité du moment et surtout un contexte idéal pour des campagnes de Ransomware. L'équipe Cisco Talos vient d'en détecter une.

Ses créateurs utilisent une adresse IP attribuée à la Thaïlande. Ils sont à l'origine d'un envoi massif d'emails soigneusement construits afin d'inviter leurs destinataires à installer Windows 10.

Ces e-mails s'accompagnent d'une pièce jointe, une archive ZIP, qui contient un exécutable qui lance CTB-Locker. Si l'antivirus présent sur la machine ne le détecte pas ou si l'archive en question n'a pas été vérifiée par un système web comme VirusTotal, le résultat est peu glorieux avec un verrouillage de données et l'apparition d'un message.

Celui-ci demande de payer une somme afin de rendre de nouveau accessible les données de l'ordinateur. Voici le message en question.



L'équipe Cisco explique qu'il s'agit ici d'une méthode

« standard [...], en utilisant un cryptage asymétrique qui permet aux adversaires de crypter les fichiers de l'utilisateur sans avoir la clé de déchiffrement présente sur le système infecté. »

Les utilisateurs ont seulement quatre jours pour payer la «rançon». Les pirates se cachent au travers de « Tor » et de la monnaie « Bitcoin » afin d'être anonymes. Ils profitent ainsi de leur campagne de logiciel malveillant avec un risque minimal. L'équipe Cisco Talos recommande de créer des sauvegardes régulières de son PC et de stocker les archives en dehors de tous services en ligne.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.appy-geek.com/Web/ArticleWeb.aspx?regionid=2&articleid=45798024&source=hootsuite>

Par GINJFO

iPhone 6 à 1 euro – Une arnaque bien rodée | Le Net Expert Informatique



iPhone 6 à 1 euro – Une arnaque bien rodée

Diffusée partout, notamment sur les réseaux sociaux, cette arnaque qui débouche en fait sur des abonnements payants fait des dizaines de victimes, selon l'association de consommateurs.

Quand c'est trop beau, il faut se méfier... Allez dire ça aux victimes de Bernard Madhof qui promettait des placements assurant des rentabilité jamais vues ou à ceux qui ont cru à ces publicités proposant des iPhone 6 à 1 euro... Un iPhone à ce prix, personne ne devrait y croire, et pourtant...

Ils sont des dizaines à cliquer sur ces publicités qui pullulent actuellement sur la toile, notamment sur les sites de téléchargement ou via les réseaux sociaux. Au point que l'association de défense des consommateurs UFC Que Choisir s'en émeuve.

« Ces offres sentent le roussi à plein nez et pourtant, à en croire les messages qui arrivent sur différents forums Internet, leurs victimes se comptent par dizaines », souligne l'association qui a mené l'enquête.

Evidemment, en cliquant sur ces liens, point d'iPhone à l'horizon (ni de Galaxy S6 Edge, et encore moins d'Apple Watch) mais un abonnement surtaxé à un service quelconque.

Vrais-faux article de presse

« La page promotionnelle, au design et à la rhétorique soignés, invite l'internaute à saisir son adresse e-mail et à accepter les conditions générales. À l'étape suivante, il doit saisir ses coordonnées bancaires. Et, quelques jours plus tard, il constate qu'une somme rondelette, de 49 à 89 € selon les offres, a été débitée de son compte, en plus de l'euro prélevé initialement. Pire, ce prélèvement se répétera puisque l'internaute s'est en fait abonné à un site Internet de jeux en ligne, comme Rockyfroggy.com, un site de musique, comme Radioplanets.com, ou un club d'achat comme DealsOffToday.eu ou Wonkabonka.com », explique l'UFC.

Et ceux qui persistent à croire qu'ils recevront un jour leur précieux, peuvent attendre, longtemps. « En réalité, recevoir le produit promis n'est même pas garanti : il s'agit de lots que le nouvel inscrit peut potentiellement gagner, un gagnant étant le plus souvent « sélectionné » tous les 500 participants. L'euro payé par l'internaute lui ouvre en fait droit à une période d'essai de quelques jours aux services du site. Heureusement, d'après les témoignages lus sur les forums, ni la rétractation ni le désabonnement ne se semblent poser trop de problèmes ».

Le vrai problème, c'est la propagation massive et en augmentation de ces arnaques, sur Facebook, Twitter etc... « Il faut dire que Rockyfroggy, DealsOffToday et les autres usent de subterfuges variés et savent manifestement créer le « buzz ». Pour attirer les internautes à eux, ils arborent plusieurs « déguisements » dans lesquels ils glissent un lien vers leur page d'abonnement. Il peut s'agir d'une enquête de satisfaction émanant soi-disant de votre opérateur mobile, d'un jeu concours organisé par votre fournisseur d'accès à Internet, d'une note de blog imaginaire... »



Mieux, ces promos se glissent parfois dans des vrais-faux articles de presse. On a ainsi pu voir la charte graphique de La Tribune utilisée pour attirer le naïf... « Heureusement, les utilisateurs ne sont pas dupes », assure l'association, mais comme pour le spam, il suffit qu'un infime pourcentage clique pour faire le beurre de ces escrocs.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.zdnet.fr/actualites/iphone-6-a-1-euro-l-arnaque-fonctionne-plutot-bien-alerte-l-ufc-39819222.htm>