L’investigation pour recouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

	L’investigation pour recouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.

L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.

L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel.
Article original de Balázs Scheidler

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse

---

Cloud souverain : les collectivités locales ne

pourront pas y couper

Cloud souverain : les collectivités locales ne pourront pas y couper

Dans une circulaire publiée au Journal Officiel, le Ministère de la Culture indique que les collectivités locales françaises devront passer par des prestataires hébergés en France pour traiter les données relatives aux citoyens français.

Mieux vaut tard que jamais : une circulaire parue au Journal officiel et signée par la direction générale des collectivités locales et le service interministériel des Archives de France vient clarifier les dispositions relatives au « cloud souverain ». Le texte, repérée par NextInpact, explique que les collectivités françaises devront impérativement passer par des prestataires situés sur le territoire français pour stocker et traiter les données dans le cloud.

Le texte se veut une clarification des directives données dans le cadre du « Guide sur le cloud computing et les datacenters à l'attention des collectivités locales. » La circulaire précise notamment le statut des données produites par les collectivités territoriales. Celles-ci « relèvent du régime politique des archives publiques dès leur création. ».

Point de salut

Outre cet aspect, la circulaire précise quelques lignes plus loin que « toutes les archives publiques sont par ailleurs des trésors nationaux en raison en raison de l'intérêt historique qu'elles présentent ou sont susceptibles de présenter. » Un régime qui s'applique autant aux documents physiques qu'à leurs équivalents numériques et qui implique une nécessaire localisation des données sur le territoire national. Celle-ci ne peut être contournée qu'à titre temporaire sur une demande adressée directement au ministère de la Culture.

Hors des fournisseurs de cloud souverain, point de salut pour les collectivités qui souhaitent avoir recours à ce type de service. La circulaire donne également une définition de ce que l'administration entend par cloud « souverain » : un « cloud dont les données sont entièrement stockées et traitées sur le territoire français. » La circulaire précise également que l'Anssi travaille sur la production d'une offre de labellisation des offres qui répondent à ces critères, label baptisé « Secure Cloud ».

Initié en 2014, le label n'est pas encore entièrement opérationnel et est encore en « phase d'expérimentation » jusqu'à la moitié de l'année 2016 selon le site de l'Afnor. Celui-ci devrait donc sous peu être en mesure de proposer une liste de fournisseurs qualifiés pour répondre aux besoins des collectivités locales en matière de services cloud.

Article original de ZDNet

Réagissez à cet article

Original de l’article mis en page : Cloud souverain : les collectivités locales ne pourront pas y couper – ZDNet

---

WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

---

Si les messageries mobiles se renforcent grâce à un dispositif de chiffrement, un hackeur a trouvé le moyen de récupérer l'intégralité des messages en clair.

Avec un chiffrement de bout-en-bout, les messages sont normalement sécurisés. Cela permet d'éviter les attaques de type man-in-the-middle, et par ailleurs, même le prestataire de service n'est pas en mesure de prendre connaissance du contenu de ces échanges. Pourtant, il existe un moyen de contourner ces dispositifs. La société Ability a partagé ses exploits en vidéo avec le magazine Forbes.
Concrètement, la faille se trouve au sein du système de signalisation n° 7 (SS7), un ensemble de protocoles de signalisation téléphonique. C'est le réseau principal permettant de connecter les réseaux téléphoniques entre eux. C'est également lui qui établit des relations entre le téléphone d'un utilisateur et le réseau, par exemple les tonalités d'appel après une numérotation ou de mise en attente ou encore le renvoi vers la messagerie.

Téléchargez WhatsApp Le hackeur fait ainsi croire au SS7 qu'il dispose du même numéro de téléphone que celui de la victime. Il est ensuite en mesure d'installer l'application WhatsApp ou Telegram puis de recevoir le code secret permettant d'authentifier son smartphone.
sécurité security banner gb
Dès lors, le hackeur peut récupérer l'historique des conversations synchronisées et se faire passer pour la victime. De son côté, cette dernière recevra un message l'avertissant que son compte est utilisé autre part. L'application sera donc déconnectée et l'identité de la victime… usurpée.
Puisque le SS7 est un réseau global utilisé par les opérateurs téléphoniques à travers le monde, celui-ci n'appartient vraiment à personne. Cela signifie que la vulnérabilité n'a pas été corrigée et le processus semble pour l'heure compliqué. Autant dire qu'il s'agit d'une porte ouverte pour les agences de renseignement.

Voici la procédure en vidéo :

Article original de Guillaume Belfiore

Réagissez à cet article

Original de l’article mis en page : WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

---

Sensibilisation aux Arnaques à la Loterie

	**Sensibilisation aux Arnaques à la Loterie**

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Euro 2016 et sécurité

informatique, quelques conseils face à quelques risques…

	**Euro . 2016 et sécurité . informatique, quelques conseils face à quelques risques…**

Euro 2016 – Les événements sportifs mondiaux ont toujours constitué un terrain de chasse idéal pour les cybercriminels. L'Euro 2016, qui débute le 10 juin prochain, ne devrait pas déroger à la règle.

Euro 2016 – Voici quelques éléments clés à retenir, amateur de football, de l'Euros 2016 ou non. Se méfier du spam et autre fausses « bonnes affaires » (places pour assister aux matchs à des prix défiant toute concurrence, par exemple). Ces mails peuvent contenir une pièce jointe infectée contenant un malware accédant au PC et interceptant les données bancaires des internautes lorsqu'ils font des achats en ligne. Ils peuvent également contenir un ransomware, qui verrouille et chiffre les données contenues dans le PC et invite les victimes à verser une rançon pour les récupérer.
Détecter les tentatives de phishing (vente de tickets à prix cassés voire gratuits, offres attractives de goodies en lien avec l'évènement,…) en vérifiant l'URL des pages auxquelles le mail propose de se connecter et en ne communiquant aucune information confidentielle (logins/mots de passe, identifiants bancaires, etc.) sans avoir préalablement vérifié l'identité de l'expéditeur.
Être prudent vis à vis du Wi-Fi public pour éviter tout risque de fuite de données, par exemple en désactivant l'option de connexion automatique aux réseaux Wi-Fi. Les données stockées sur les smartphones circulent en effet librement sur le routeur ou le point d'accès sans fil (et vice-versa), et sont ainsi facilement accessibles.
Redoubler de vigilance vis-à-vis des mails invitant à télécharger un fichier permettant d'accéder à la retransmission des matchs en temps réel. Il s'agit en réalité de logiciels malveillants qui, une fois exécutés, permettent d'accéder aux données personnelles stockées dans le PC (mots de passe, numéro de CB, etc.) ou utilisent ce dernier pour lancer des procédures automatiques comme l'envoi de mails massifs. (TrendMicro).
Auteur : Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Football : Euro 2016 et sécurité informatique – Data Security BreachData Security Breach

---

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

La rencontre qui devrait être clôturée vendredi dernier vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité.

(CIO Mag) – Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

Le directeur général de l'agence tunisienne de sécurité informatique, lui, indique que Tunis a pris très tôt des initiatives pour lutter contre la cybercriminalité. Mohamed Naoufel Frikha, repris par nos confrères, rappelle qu'un travail important a été réalisé depuis 1999 avec la création du premier centre en Afrique, le troisième dans le monde arabe.

Le rendez-vous de Tunis entend amener les pays arabes à créer des centres de cyber-alerte. Leur nombre est très insuffisant dans l'espace arabophone puisque seuls dix pays en disposent. Des représentants de treize Etats prennent part aux échanges.

Article de Ousmane Gueye

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité: les pays

arabes mutualisent leurs forces pour faire face au phénomène | CIO MAG

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016

	**Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016**

Denis JACOPIN sera présent à l'IT Forum 2016 les 7 et 8 juin prochains, invité auprès des plus grands Experts en Cybersécurité. La 8ème édition de ce Forum aura pour thème Protection des Données, Gestion de l'identité numérique, Protection des transactions à l'ère du numérique : Risques, Enjeux et Stratégies de mise en oeuvre.

IT Forum Côte d'Ivoire — Club DSI Côte d'Ivoire

2 jours de networking organisés par CIO Mag et le Club DSI de côte d'Ivoire sous le parrainage de

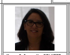
Bruno Nabagné KONE,
Ministre de l'Economie numérique et de la Poste – Côte d'Ivoire

Venez discuter, échanger et dialoguer avec des donneurs d'ordre, rencontrez-les en rendez-vous :

Freddy TCHALA, CEO MTN CI

Euloge SORO-KIPEYA, CEO ANSUT

Nongolougo SORO, CEO SNDI



Mme. Saloua K. BELKZIZ, Présidente de la Fédération APEBI – Maroc

Jean Kacou DIAGOU, Président du CGECI – Côte d'Ivoire

Une vingtaine d'experts partageant leurs retours d'expériences et les meilleures pratiques

Cdt Guelpétchin Ouattara, Directeur de l'Informatique et des Traces Technologiques – Côte d'Ivoire

Yann PILPRE, Expert Sécurité, CEO YPSI

Denis JACOPINI, Expert en Cybercriminalité et Protection des données personnelles

Ange DIAGOU, CEO NSIA Technologies

Frédéric MASSE, Vice-Président SAP

Alain DOLIUM, Expert Transformation numérique PDG SMS Group

vous souhaitez y participer ?
Entrée gratuite mais inscription obligatoire : Cliquez ici

PROGRAMME

Heures	Activités	Intervenants
Journée du Mardi 07 juin 2016		
08h00 – 09h00	Accueil et installation des invités	*Comité d'organisation*
09h00 – 09h05	Mot de Bienvenue	· **M. Mamadou NAON**, Président CDSI
09h05 – 09h15	Mot du Sponsor Officiel	· **M. Freddy TCHALA**, DG MTN
09h15 – 09h25	Mots des sponsors Leaders	· **M. Nongologou SORO**, DG SNDI · **M. Ange DIAGOU**, DG NSIA TECHNOLOGIES
09h25 – 09h35	Présentation du contenu de l'IT FORUM 2016	· **M. Mohamadou DIALLO**, Directeur de Publication CIO MAG
09h35 – 09h40	Mot du Pays Invité (Maroc)	· **Mme Saloua K. BELKZIZ**, Présidente de la Fédération APEBI
09h40 – 09h50	Mot du Président de l'IT FORUM 2016	· **M. Jean Kacou DIAGOU**, Président CGECI
09h50 – 10h05	Discours d'ouverture des travaux	· **M. Bruno KONE**, Ministre de la Poste et de l'Economie Numérique
10h05 – 10h20	REMISE DE TROPHEES	
10h20 – 10h45	Coupure de ruban – Visite des stands – Cocktail	
10h45 – 10h50	**TIRAGE TOMBOLA**	
10h50 – 11h05	Les principales tendances IT en Afrique occidentale et centrale	· **M. Mohamed ZIZI**, Directeur régional pour l'Afrique Francophone IDC
11h05 – 12h00	Plénière/Panel 01 **La protection des données, une nécessité pour le respect des libertés fondamentales**	· **Cdt Guelpétchin Ouattara**, Directeur de l'Informatique et des Traces Technologiques (DITT Côte d'Ivoire) · ***Ibrahima DIAGNE***, *Administrateur Délégué Gaindé 2000* ***Modérateur : Dr GUIBESSONGUI N'Datien Sévérin***, *ICT CONSULTING* ***Rapporteur : M. Auger SEOULOU***, *DSI Ministère de la Justice – Côte d'Ivoire*
12h00 – 12h05	**TIRAGE TOMBOLA**	
12h05 – 12H35	Atelier 01 **Optimisation des coûts en relation avec votre business model**	· **M. Christophe Thénégal**, Associé PWC
12h35 – 12h40	**TIRAGE TOMBOLA**	
12h40 – 14h20	Pause déjeuner	
14h30 – 14h35	**TIRAGE TOMBOLA**	
14h35 – 15h20	Plénière/Panel 02 **Fluidité des transactions : Comment mieux réglementer le secteur en vue de développer l'adoption de la monnaie électronique**	· ***M. Frédéric MASSE***, *Vice-Président SAP* · ***M. Francis Dufay***, *Directeur Général de JUMIA Côte d'Ivoire* · ***Représentant MTN MFS*** ***Modérateur : M. Lacina KONE***, *Conseiller NTIC –Président de la République* ***Rapporteur : M. Eric YAO***, *DSI CNCE*
15h20 – 15h30	**FIGHT 1 : Logiciel open source VS Logiciel Propriétaire (compétions des solutions IT)**	
15h30 – 15h35	**TIRAGE TOMBOLA**	
15h35 – 15h50	Atelier 01	· *SAP*
15h50 – 15h55	**TIRAGE TOMBOLA**	
15h55 – 16h10	Plénière **Méthode, technique et outils des transactions électroniques et leur sécurité**	· **M. Yann PILPRE**, Expert Sécurité, DG de YPSI
16h10 – 16h20	**FIGHT 2 : Approche de sécurisation de données à caractère personnel et des transactions électroniques : méthode et outils (compétition des approches IT)**	
16h20 – 17h05	Panel 03 **Données dans le Cloud public/privé: Comment et avec qui assurer la sécurité ?**	· ***M. Nongolougo SORO***, *DG de la SNDI* · ***M. Euloge SORO***, *DG de l'ANSUT* · ***AUSIM*** *(Maroc)* · ***M. Brice DEMONGE***, *Directeur de développement secteur public – GFI Informatique* · ***Camille AMEYAO / MTN Business*** · ***Denis JACOPINI***, *Expert Informatique assermenté spécialisé en Cybercriminalité et en Protection des données personnelles* · ***Modérateur : Conrad GBAGUIDI***, *DG MGT Conseils* ***Rapporteur : M. Aboadjé KOUADIO***, *DSI SNDI*
17h05– 17h10	**TIRAGE TOMBOLA**	
Fin de la première journée		

Journée du Mercredi 08 juin 2015		
08h30 – 09h15	Accueil et installation des invités	Comité d'organisation
09h15 – 09h30	Rappel des travaux de la journée du 07 juin	Club DSI
09h30 – 09h35	**TIRAGE TOMBOLA**	
09h35– 10h20	Panel 04 **Les entreprises et administrations ivoiriennes face à la cybersécurité** –	· **M. Freddy TCHALA**, DG MTN Côte d'Ivoire · ***M. Nongolougo SORO***, *DG de la SNDI* · ***M.Ange DIAGOU***, *DG NSIA Tech* · ***M. Bilé DIEMELEOU***, *DG ARTCI* ***Modérateur : Patrick M'BENGUE, Président GOTIC***
10h20 – 10h25	**TIRAGE TOMBOLA**	
10h25 –10h40		
10h40 – 10h45	**TIRAGE TOMBOLA**	
10h45– 11h00	Atelier 04 **Les services managés: garants d'une transformation numérique efficace, rentable et sécurisée**	*NSIA TECHNOLOGIES*
11h00 – 11h15	Atelier 05	*FEITAN France*
11h15 – 11h20	**Cloud privé VS Cloud Public (Compétition des technologies Cloud)**	
11h20 – 12h15	**Comment sécuriser ses infrastructures et plateformes de services pour la transformation numérique?**	· ***Représentant de l'ARTCI*** · ***Denis JACOPINI***, *Expert Informatique assermenté spécialisé en Cybercriminalité et en Protection des données personnelles* · ***Jean-François TESSERAUD***, *Chief Information Security Officer – Systemis* · ***Yves MIEZAN EZO, Conseil***, *Stratégie & Formation Open Source* · ***Modérateur : Ludovic MORINIERE***, *International Development BearinPoint*
12h15 – 12h20	**TIRAGE TOMBOLA**	
12h30 – 14h20	Pause déjeuner	
14h30 – 14h35	**TIRAGE TOMBOLA**	
14h35 – 14h50	Atelier 06	VEONE
14h50 – 15h00	**FIGHT 04**	
15h00 – 15h15	Atelier 07 **Pourquoi et Comment protéger efficacement vos données dans la transformation numérique ?**	· ***Marcial MONTHE***, *Ingénieur Avant-Vente, Responsable de la Business Unit Veritas –* ***SOCITECH***
15h15 – 15h20	**TIRAGE TOMBOLA**	
15h20 – 15h35		
15h35 – 16h40	**TIRAGE TOMBOLA**	
15h40 – 15h55	Récompense des Sponsors et Partenaires	***Club DSI***
15h55– 16h20	Restitution des travaux	
Fin de la 2ème journée		
Soirée de Gala		

Merci à l'auteur de cet article

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Jour J-16*

ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ

	**Fuites de données de Santé en France**

Santé et fuite de données – Plus de 200 millions de dossiers médicaux de ressortissants américains ont disparu depuis 2015. Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Le Parlement européen a adopté le jeudi 14 avril 2016 le règlement européen sur la protection des données. Le règlement qui sera applicable à partir du 25 mai 2018 dans l'ensemble des pays membres de l'Union européenne. Avec cette jolie annonce que l'on attend depuis des années, je me suis penché sur un cas concret de fuites de données : les dossiers médicaux. A la fin de ma compilation et analyses des datas collectées, ma question est la suivante : Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Santé et fuite de données : Plus de 200 millions de dossiers médicaux perdus en 1 an

J'ai analysé les établissements de santé américains. Il faut dire que cela est plus simple. La France n'a aucun moyen de contrôle au sujet des fuites d'informations dans le secteur Français de la santé. Et ce n'est pas faute d'avoir des personnes très compétentes au Ministère de la Santé et des Affaires Sociales. Mais en France, pour le moment, aucune obligation n'est faite pour que les patients soient alertés en cas de fuite, de piratage, de perte de leurs données (clé usb, portable…). Sur le sol de l'Oncle Sam, il en est tout autre. La loi ***Hitech Act*** *(section 13402) impose l'affichage public de toutes fuites d'informations concernant plus de 500 patients dans le même établissement.*

En 1 an, la plus grosse fuite de données médicales aux USA aura visé l'Anthem, Inc. Affiliated Covered Entity. Nous sommons alors en mars 2015. 78,8 millions de dossiers suite à un « ***Hacking/IT Incident Network Server*** *» comme le référence le Ministère américain de la Santé (****HHS****). Depuis le 1er janvier 2016, 103 établissements de santé (Hôpitaux, centres de soin…) ont été touchés par une perte, un vol, un piratage. Dernier cas en date, 2.213.597 de données de patients piratés au 21st Century Oncology de Floride. Ici aussi, le HHS (U.S. Department of Health and Human Services) parle de «* ***Hacking/IT Incident Network Server****« . L'attaque date du 4 avril 2016.*

Depuis le 1er janvier 2016, 3.605.511 dossiers de patients américains ont volés, piratés ou perdus. Et en France ?

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ*

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir

---

Un fichier comportant des informations sur plusieurs centaines de millions de comptes MySpace, dont 427 millions de mots de passe, a été mis en vente sur un site spécialisé, a révélé le site LeakedSource. Selon des tests effectués par Motherboard, les mots de passe figurant dans les documents correspondent bien à des comptes existant ou ayant existé.

Selon LeakedSource, les mots de passe de la base de données étaient chiffrés, mais protégés par une technologie aisément contournable avec du temps et de la puissance de calcul. L'intégralité de la base de donnée a été mise en vente pour environ 2 500 euros sur un site spécialisé dans le recel de données volées.

Un milliard d'inscrits

MySpace, considéré il y a dix ans comme le site le plus populaire pour les adolescents et les étudiants, n'est aujourd'hui plus que l'ombre de ce qu'il était. Le service, qui permet de créer sa page personnelle, avait notamment construit sa popularité en attirant de nombreux groupes de musique populaires. Le service existe toujours, et annonçait à la fin de 2015 avoir dépassé le seuil symbolique du milliard d'inscrits au cours de son existence. Les données contenues dans les fichiers volés restent cependant sensibles – de nombreux internautes réutilisent le même mot de passe pour plusieurs applications ou services. Il est conseillé aux utilisateurs ayant détenu ou détenant un compte MySpace de changer leur mot de passe s'ils l'ont réutilisé sur d'autres services… [Lire la suite]

Réagissez à cet article

Source : *Les informations de millions de comptes MySpace en vente en ligne*

Et si charger la batterie de son smartphone via un port USB était dangereux ?

Et si charger la batterie de son smartphone via un port USB était dangereux ?

On s'est tous probablement retrouvés un jour ou l'autre dans une situation où il nous restait peu de batterie sur notre téléphone et que nous n'avions pas de chargeur à portée de main. Le pire, c'est ce que ça nous est arrivé au moment même où on en avait le plus besoin, comme attendre un appel important, un message ou un e-mail, etc.

Il parait donc tout à fait normal de chercher une source d'électricité à proximité lors d'une telle situation, par exemple utiliser un port USB. Mais est-ce bien sûr ? Non, en réalité cela peut s'avérer dangereux. Via une connexion USB, n'importe qui peut s'emparer de vos fichiers, infecter votre smartphone d'un virus ou même le rendre inutilisable.

Chevaucher la foudre

Avant d'aborder le problème des hackers, il est important de préciser que toute les sources d'électricité ne sont pas forcément bonnes pour votre téléphone. Il existe beaucoup de plaintes sur Internet, principalement d'utilisateurs tentant de charger leur téléphone dernier cri en les connectant à des adaptateurs ou des chargeurs d'occasion (ou non originaux). Dans certains cas, les téléphones ont été rendus inutilisables. Dans certains cas encore plus étranges, des personnes prenant leur téléphone alors qu'ils étaient en charge ont été sérieusement blessées ou même tuées.

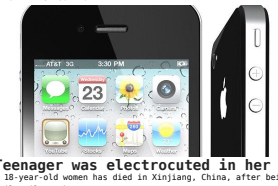
Follow

Daily Mail Online

@MailOnline

Teen dies after being electrocuted in her sleep while charging her iPhone http://dailym.ai/1o7Eia5

2:10 PM – 31 Jul 2014



Teenager was electrocuted in her sleep while charging her iPhone

A 18-year-old women has died in Xinjiang, China, after being electrocuted in her sleep while charging her iPhone 4s. It is not known if she was using an authentic Apple phone charger.

dailymail.co.uk

•

•

140140 Retweets

•

2424 likes

Malheureusement, il s'agit plus que de simples accidents. Par exemple, l'année dernière un appareil a été baptisé à juste titre : le tueur USB. Il contenait un impressionnant ensemble de condensateurs hébergés dans une carte mémoire flash USB, qui déchargeait 220 V dans le port USB auquel il était connecté. Une telle décharge pourrait dans le meilleur des cas détruire le port USB et dans le pire sans doute la carte mère de tout l'ordinateur. Nous doutons que vous souhaitiez tester la durabilité de votre téléphone de cette façon.

Montrez-moi vos fichiers

Deuxièmement, les ports USB n'ont pas été conçus uniquement pour la charge, mais aussi pour transférer des données. Les téléphones consommant le plus de données sont ceux conçus sur la plateforme Android 4 *x* et les versions antérieures, ils se connectent sur le mode MTP (Media Transfer Protocol) par défaut, exposant tous les fichiers de l'appareil.

En moyenne, il faut plus d'une centaine de kilo octets de données rien que pour le système hôte des fichiers et dossiers du téléphone. Pour vous donner une idée, il s'agit de la taille d'une copie de l'e-book d'*Alice au pays des merveilles*.

Bloquer votre téléphone vous éviterait de courir un tel risque mais honnêtement seriez-vous prêt à vous passer de votre téléphone pendant qu'il est en charge ? Et à toujours le débrancher du port USB lorsque vous recevez un message par exemple ?

A présent, jetons un coup d'œil de plus près aux données qui sont transmises du port USB même lorsque le mobile est en mode (bloqué) » charge seule « . La taille de ces données varie, dépendant de la plateforme du mobile et du système d'exploitation de l'hôte. Mais dans tous les cas, il s'agit plus que d'une » simple charge « . Comme nous l'avons découvert, ces données incluent le nom du mobile, le nom du fournisseur et le numéro de série.

Accès complet et au-delà

Vous devez sûrement penser que vous ne voyez pas où est le problème, seulement il y en a un, puisque nous avons trouvé en cherchant des informations accessibles au public qu'un fournisseur en particulier autorise beaucoup plus que ce qui est spécifié par le système.

Comment est-ce possible ?

Cela est rendu possible via un ancien système de commandes appelées commandes AT. Ces dernières ont été développées il y a quelques dizaines d'années afin de permettre les communications des modems et ordinateurs. Plus tard, elles ont été intégrées au standard du GSM et désormais sont toujours utilisées sur les smartphones.

Pour vous donner une idée de l'usage des commandes AT, laissez-moi vous donner quelques exemples que nous avons été en mesure de découvrir à la surface d'Internet : elles permettent à un hacker d'obtenir votre numéro de téléphone et de télécharger les contacts enregistrés dans la carte SIM. Ces commandes permettent d'établir un appel à n'importe quel numéro, et ce à vos frais, bien entendu. Et si vous êtes en roaming, de tels appels inattendus peuvent vite faire grimper la facture. Dépendant du vendeur, le mode du roaming peut faciliter l'accès à un hacker d'installer n'importe quel type d'applications, y compris malveillantes.

Tout ce qu'on vient de mentionner est possible, même si votre smartphone est bloqué !

En résumé, ne vous fiez pas aux apparences d'un port USB car il pourrait bien » cacher des choses « . Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchiez.

Article de Alexey Komarov

Source : *Les dangers de charger la batterie de son smartphone via un port USB – Kaspersky Daily – | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.*