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

24.000 bitcoins saisis par la police vendus aux enchères

24.000 bitcoins saisis par la police vendus aux enchères

La police Australienne va mettre aux enchères, le 20 juin 2016, 24.000 bitcoins saisis dans des affaires criminelles. Montant du lot, plus de 15.000 euros.

15 882 euros de bitcoins saisis par la justice (24,500 BTC) vont être mis aux enchères, le 20 juin, par la police australienne. De l'argent « dématérialisé » qui sera mis en vente le 20 juin 2016. Pour les autorités, cet argent « virtuel » doit être converti en monnaie sonnante et trébuchante afin de le reverser à l'autorité fiscale locale. Ces bitcoins ont été saisis dans des affaires criminelles et la police a décidé de passer par le mode enchères publique pour s'en débarrasser. C'est la société Ernst & Young qui va se charger de la vente. Ca sera la deuxième vente mondiale de ce type de « produit ».

24.000 Bitcoins saisis

Je vous révélais, en 2014, comment la police fédérale américaine des US Marshall avait revendu pour treize millions de dollars de Bitcoins (144.000 BTC), soit l'équivalent de 8.431.689 euros, dans une vente aux enchères qui commercialisait les BTC du propriétaire de Silk Road, Ross Ulbricht, une boutique du blackmarket spécialisée dans la commercialisation de drogue.
Les bitcoins australiens, ils sont au nombre de 24.518, ont été confisqués en décembre 2013 dans une affaire de drogue, à Melbourne. Son propriétaire, Richard Pollard, 32 ans, a été condamné en octobre 2015, à 11 ans de prison pour trafic de drogue… sur le site Silk Road. Les bitcoins seront vendus par lots d'environ 2.000 BTC… [Lire la suite]
Article original de Damien Bancal

Réagissez à cet article

Source : *ZATAZ Vente aux enchères de 24.000 bitcoins saisis par la police – ZATAZ*

Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

---

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.
Nous connaissions la Fraude au Président, l'arnaque aux faux virements via des informations bancaires soutirées à des entreprises par ruse. Un piège qui fonctionne, malheureusement aussi, sur les locataires de logements sociaux. Les escrocs se font passer pour le bailleur afin de faire modifier les données concernant les virements des loyers.
Aujourd'hui, je viens d'apprendre une nouvelle ruse. Des escrocs se font passer pour les stars de la radio (Manu de NRJ, Camille Combal de Virgin Radio…) en téléphonant et en promettant de l'argent à leurs interlocuteurs. « Un homme dans un soi-disant bureau d'antenne de radio vous dit que vous venez de gagner 2000€ et de doubler vôtre salaire, souligne l'un des témoins de ZATAZ.COM. Il y a beaucoup de bruit derrière. Comme dans un studio de radio ».

Ils visent vos informations bancaires

Une fois l'interlocuteur appâté, l'appel est transféré à une standardiste « On vous demande un numéro de compte bancaire, souligne un autre lecteur de ZATAZ. Ce qui m'a mis la puce à l'oreille est que le soi-disant animateur fusionne plusieurs jeux du 6/9 de NJR et de Virgin Radio. Pour mettre la personne en confiance, on vous ovationne et félicite pour votre prix. »
La question est de savoir maintenant comment les escrocs peuvent avoir le numéro de téléphone portable et l'identité complète (Nom, prénom) des personnes appelées.
Bref, prudence ! Si vous ne vous inscrivez pas à un jeu officiel, il n'y a pas de raison que ce dernier vous téléphone !… [Lire la suite]

Merci à Damien Bancal auteur de cet article

M

Réagissez à cet article

Source : *ZATAZ Informations bancaires : des pirates se font passer pour Manu, Camille Combal – ZATAZ*

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

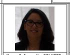
Bruno Nabagné KONE,
Ministre de l'Economie numérique et de la Poste – Côte d'Ivoire

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*

La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

	La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

Les attaques visant les systèmes bancaires connectés au réseau Swift soulèvent de vastes inquiétudes au point que les autorités européennes pourraient être appelées à conduire un stress-test visant à éprouver leur cybersécurité.

Recommander les autorités locales des pays membres de l'Union européenne à soumettre les systèmes de sécurité informatique des institutions financières à des stress-tests. C'est l'idée qu'a avancé Andrea Enria, président de l'Autorité Bancaire Européenne, l'autorité indépendante chargée de garantir un niveau de surveillance prudentiel efficace et cohérent à l'échelle de l'Union, à l'occasion d'un échange avec nos confrères de Reuters.
Dans ce cadre, il estime que les banques pourraient avoir à provisionner des réserves supplémentaires afin de se protéger, financièrement, du risque associé à des attaques informatiques. Le risque informatique doit d'ailleurs être explicitement pris en compte dans le cadre des règles Pilier 2. Celles-ci font partie des accords Bâle II et portent justement sur la surveillance prudentielle ainsi que la gestion des risques.
Et la prise en compte des risques associés aux attaques informatiques apparaît particulièrement importante qu'ils sont appelés à être de plus en plus considérés dans les analyses de solvabilité des agences de notation. Moody's et Standard & Poor l'ont ainsi ouvertement indiqué à l'automne dernier.
Fin 2013, les banques britanniques ont été soumises à un stress-test IT, après un premier en 2011. Mais l'opération n'avait pas manqué de soulever plusieurs critiques, certains experts estimant notamment qu'elle devrait survenir plus régulièrement. D'autres s'interrogeaient sur la manière dont étaient définies les attaques imaginées pour l'exercice.
Très récemment, la patronne du gendarme des marché boursiers américains a de son côté estimé que le risque d'attaque informatique constitue la principale menace pour le système financier mondial, notamment après les opérations qui ont visé dernièrement les systèmes plusieurs banques connectés au réseau Swift… [Lire la suite]

Merci à Valery Marchive pour son 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 : *Vers un stress-test de la cybersécurité des banques*

européennes ?

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.

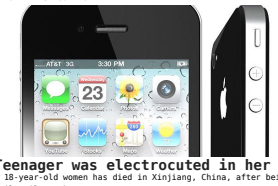
Follow

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.

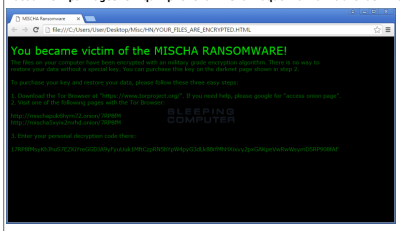
Article de Alexey Komarov

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.*

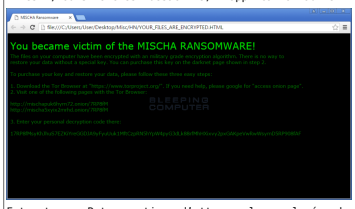
Mischa, le ransomware successeur de Petya

Mischa, le ransomware successeur de Petya

Apparu au mois de mars, le ransomware Petya a ouvert une nouvelle voie dans le développement des ransomwares. Il s'agissait du premier cas d'un malware qui allait au-delà du chiffrement des fichiers sur les disques locaux et partagés et qui préférait s'attaquer à la table de fichiers principale



Ceci étant dit, Petya n'était pas infaillible et les chercheurs ont été rapidement en mesure de créer un outil de restauration de certains des fichiers chiffrés par ce malware. Les individus malintentionnés n'ont pas perdu leur temps et ils ont trouvé le moyen de contourner une autre lacune de Petya : sa dépendance vis-à-vis de la volonté de la victime qui doit octroyer au malware les autorisations d'administrateur pour accéder à la table de fichiers principale (MFT).
Un nouveau programme d'installation de Petya a été détecté la semaine dernière. Celui-ci utilise un scénario de réserve. Si le malware n'obtient pas les autorisations d'administrateur au lancement, c'est un autre ransomware qui sera installé sur la machine infectée, en l'occurrence Mischa.
D'après les explications de Lawrence Abrams, de chez Bleeping Computer, les autorisations d'administrateur indispensables au fonctionnement de Petya figurent dans le manifeste de la version originale. Dans les commentaires envoyés à Threatpost, Lawrence Abrams explique « qu'avant l'exécution du code, Windows affiche la boîte de dialogue UAC qui sollicite ces autorisations. Si le service UAC est désactivé, l'application est exécutée automatiquement avec [les autorisations d'administrateur]. Si l'utilisateur clique sur « No » dans la fenêtre UAC, l'application n'est pas exécutée et, par conséquent, l'installation de Petya n'a pas lieu ».
Pour les exploitants de Petya, ces échecs représentent un gaspillage de ressources d'après Lawrence Abrams. Pour rectifier le tir, ils ont empaqueté un autre ransomware avec le programme d'installation. Il s'agit de Mischa qui sera exécuté si l'option « Petya » n'a pas pu être mise en œuvre.
Le manifeste de la nouvelle version indique que le fonctionnement requiert les données du compte utilisateur. Dans ce cas, Windows autorise le lancement de l'application sans afficher d'avertissement UAC. Comme l'explique Lawrence Abrams, « au lancement du programme d'installation, il sollicite les autorisations d'administrateur conformément à ses paramètres. La boîte de dialogue UAC s'affiche et si l'utilisateur choisit « Yes », ou si UAC est désactivé, l'application obtient les autorisations d'administrateur et installe Petya. Dans le cas contraire, c'est Mischa qui sera installé. Cette méthode est très intelligente ».



Entre temps, Petya continue d'attaquer les employées des services des ressources humaines allemands à l'aide de messages non sollicités qui contiennent des liens vers un fichier malveillant dans le cloud. Au début, les individus malintentionnés utilisaient Dropbox, mais depuis le blocage des liens Dropbox malveillants, ils se sont rabattus sur le service allemand TelekomCloud. Le fichier exécutable se dissimule sous les traits d'un fichier PDF qui serait un prétendu CV d'un candidat à un poste libre. Il contient même une photo.
« Lorsque l'utilisateur télécharge le fichier exécutable, l'icône PDF s'affiche, ce qui laisse penser qu'il s'agit bien d'un CV au format PDF » explique Lawrence Abrams. Toutefois, lorsque ce fichier est ouvert, il tente d'installer Petya. Et si cela ne marche pas, il installe le ransomware Mischa.
Le comportement de Mischa est identique à celui des autres ransomwares standard. Il analyse le disque local à la recherche de fichiers portant certaines extensions. Il chiffre les fichiers à l'aide d'une clé AES et ajoute à leur nom une extension de 4 caractères, par exemple 7GP3. Lawrence Abrams explique que « lorsque Mischa chiffre le fichier, il conserve la clé de chiffrement à la fin du fichier obtenu. Il convient de noter qu'il ne chiffre pas uniquement les fichiers traditionnels dans ce genre d'attaque (PNG, JPG, DOCX, etc.), mais également les fichiers EXE. »
Une fois qu'il a chiffré les fichiers, Mischa exige le versement d'une rançon de 1,93 bitcoins (environ 875 dollars américains) pour le déchiffrement. La somme doit être payée via le site Tor. Il n'existe pas encore d'outil de déchiffrement pour ce ransomware. « Nous conseillons aux victimes de vérifier avant tout la conservation des clichés instantanés à l'aide de Shadow Explorer. Ils pourraient être utile pour restaurer une ancienne version des fichiers chiffrés » conclut Lawrence Abrams.

Article du Kaspersky Lab

Réagissez à cet article

Source : *Petya possède un suppléant : Mischa – Securelist*

Forte hausse des applications Android malveillantes

Forte hausse des applications Android malveillantes

Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publie son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à » usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernièresannées selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)… [Lire la suite]

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

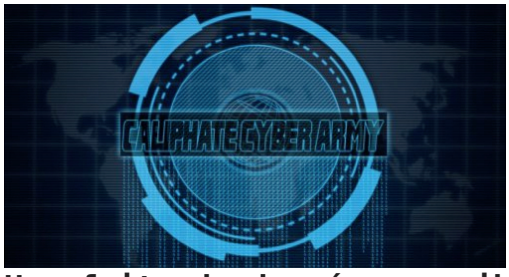
Réagissez à cet article

Source : *Forte hausse des applications Android malveillantes – Data Security BreachData Security Breach*

La France visée par une nouvelle cyberattaque de l’EI

La France visée par une nouvelle cyberattaque de l’EI

Les équipes CybelAngel ont repéré lundi 16 mai une base de coordonnées de citoyens français et américains publiée sur le site justepaste.it. L'utilisateur à l'origine de la publication se revendique de la Caliphate Cyber Army (#CCA).



Une fuite de données sensibles mais accessibles depuis 6 mois

Le message commence par une représentation de la basmala, un verset leitmotiv du Coran à la gloire de Dieu. Des mots-dièse "CCA #CyberCaliphate #UCC" et un logo de la Caliphate Cyber Army viennent compléter la revendication introductive.

Vient ensuite une liste de 77 emails, mots de passe, numéros de téléphone, adresses, comptes Paypal et soldes de compte Paypal. La liste concerne 38 adresses françaises, 31 américaines, 6 australiennes, 1 philippine et 1 néerlandaise. Les coordonnées semblent être uniquement personnelles et non professionnelles.

Après analyse, il semblerait que les données exposées ici étaient déjà présentes sur le Dark Web avant cette publication. En effet, un message publié le 12 janvier dernier sur le site pastebin.com reprenait 35 paires d'emails/mots de passe correspondant exactement à ceux publiés le 16 mai par la Cyber Caliphate Army. A l'aune de cette troublante similarité entre le 12 janvier et le 16 mai, la CCA reprendrait à son compte des adresses en libre accès sur le Dark Web ; ce qui ne serait pas la première fois.

Une Cyber Armée aux attaques peu techniques mais à fort impact médiatique

La Cyber Caliphate Army est issue de la volonté de l'Etat Islamique de projeter son action dans l'espace virtuel en 2014. Elle est dans un premier temps dirigée, et probablement entièrement constituée par Junaid Hussain, un hacker anglais.

De son lancement pendant l'été 2014 jusqu'à l'assassinat de Hussain par un drône américain en août 2015, la CCA a revendiqué une série de cyberattaques peu sophistiquées mais très médiatiques : plusieurs défacements de comptes Twitter du Commandement Central des Armées américaines (CENTCOM), de Newsweek, de chaînes de télévisions américaines, l'arrêt des retransmissions des 11 chaînes de TV5 Monde (action dont la parenté est mise en doute par de nombreux experts).

Cette nouvelle fuite souligne les faiblesses de la Cyber Armée du Califat

Depuis la mort de Husain, la CCA a mené des actions nettement moins symboliques : des défacements indiscriminés de milliers de sites et des actions à la parenté douteuse dont des fermetures de systèmes informatiques revendiquées ex-post et des diffusions de données en réalité déjà en ligne, comme celle détectée ce 16 mai par CybelAngel.

Face à ce potentiel de nuisance visiblement réduit, 4 groupuscules d'hacktivistes islamistes dont la Cyber Caliphate Army ont proclamé leur union en un United Cyber Caliphate en avril ainsi que nous vous le rapportions la semaine dernière. Quelques semaines plus tard, le groupuscule Cyber Caliphate Army revendique pourtant en son nom propre une action et ne mentionne le United Cyber Caliphate qu'en un hashtag UCC. Il semblerait que l'intégration des différents groupes hacktivistes islamistes prenne plus de temps que prévu.

Article de CybelAngel Analyst Team

Réagissez à cet article

Source : *La France visée par une nouvelle cyberattaque de l'EI*

Un vague massive de spams JavaScript distribue le ransomware Locky

Un vague massive de spams JavaScript distribue le ransomware Locky

---

Les pays européens sont aujourd'hui victimes d'une vague de spams essayant d'exécuter un code JavaScript installant le redoutable ransomware Locky.

Au cours de la semaine écoulée, un grand nombre d'ordinateurs à travers l'Europe – et d'autres endroits dans le monde dont les Etats-Unis et le Canada – ont été touchés par une campagne massive de spams transportant des pièces jointes JavaScript malveillantes qui installent le ransomware Locky. Les pièces jointes sont généralement des fichiers d'archives .zip qui contiennent .js ou fichiers .jse intérieur. Ces fichiers s'exécutent directement sous Windows sans avoir besoin d'applications supplémentaires.

L'éditeur spécialisé dans la sécurité ESET a observé un pic dans les détections de JS / Danger.ScriptAttachment, un téléchargeur malware écrit en JavaScript qui a démarré le 22 mai et a atteint son sommet le 25 mai. JS / Danger.ScriptAttachment permet de télécharger divers programmes malveillants à l'insu des internautes, mais il a récemment été adapté pour distribuer Locky, un programme malveillant répandu qui utilise un chiffrement fort pour crypter les fichiers des utilisateurs. Cependant, il est très rare que des gens envoient des applications légitimes écrites en JavaScript par email. Les utilisateurs devraient éviter d'ouvrir ce type de fichiers.

La France touchée à 36%

De nombreux pays en Europe ont été touchés. Les taux de détection les plus élevés ont été observés au Luxembourg (67%), en République tchèque (60%), en Autriche (57%), aux Pays-Bas (54%), au Royaume Unie (51%) et en France 36%. Les données de télémétrie de l'éditeur ont également montré des taux de détection importants pour cette menace au Canada et aux États-Unis. Bien que Locky n'a pas de défauts connus qui permettraient aux utilisateurs de déchiffrer leurs fichiers gratuitement, les chercheurs en sécurité de Bitdefender ont développé un outil gratuit qui peut prévenir les infections Locky. L'outil trompe le ransomware en lui indiquant que l'ordinateur est déjà infecté.
L'utilisation de fichiers JavaScript pour distribuer Locky a commencé un peu plus tôt cette année, ce qui a incité Microsoft à publier une alerte à ce sujet en avril dernier.
Article de Lucas Mearian/ IDG NS (adaptation SL)

Réagissez à cet article

Source : *Un vague massive de spams JavaScript distribue le ransomware Locky – Le Monde Informatique*