Le portable de Manuel Valls a-t-il été piraté par Israël ?

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Lors de son déplacement en Israël, une délégation de Matignon a laissé ses portables sans surveillance pendant une réception officielle. Et a relevé des anomalies de fonctionnement sur certains terminaux ensuite, assure l'Express.

Manuel Valls s'est-il fait pirater son smartphone lors de son déplacement en Israël, fin mai dernier ? C'est la question que posent nos confrères de l'Express. Lors de son déplacement qui avait pour ambition de relancer le processus de paix avec la Palestine, le Premier ministre, qui se présente volontiers comme « l'ami d'Israël » et la délégation l'accompagnant ont été priés de laisser leurs téléphones portables à l'accueil avant d'être reçu en haut lieu. Demande à laquelle ils auraient accédé, laissant leurs terminaux sans surveillance pendant l'entretien.
Problème : quand ils ont récupéré leurs terminaux pourtant sécurisés, certains présentaient des « anomalies », selon l'Express. Des dysfonctionnements qui peuvent laisser suspecter une tentative d'intrusion de la part des services secrets israéliens. L'Express ne précise pas le ou les modèles des terminaux concernés par ces tentatives d'espionnage supposées.

Pas d'espionnage entre alliés. Sans blague ?
Depuis, les téléphones en question ont été remis à l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui mène l'enquête. Interrogée par nos confrères, celle-ci s'est toutefois refusée à tout commentaire. De son côté, Matignon reconnaît qu'un terminal est bien tombé en panne durant la visite du Premier ministre en Israël. Et indique à nos confrères qu'un allié n'espionne jamais ses amis. Défense de rire.
Rappelons que, pour les échanges les plus sensibles, les officiels français disposent de terminaux Teorem, fournis par Thales et habilités confidentiel-défense. Ceux-ci se révèlent toutefois peu pratiques d'usage, si bien que les ministres utilisent souvent des smartphones du commerce, durcis avec des technologies de sécurité complémentaires. Récemment, l'Elysée s'est ainsi équipé de smartphones Hoox, conçus par Bull. Ces machines, des smartphones Android bénéficiant d'une surcouche logicielle de sécurisation, sont vouées aux échanges de type « diffusion restreinte », un niveau de classification de l'information moins exigeant que le confidentiel-défense.
Article original de Reynald Fleychaux

Réagissez à cet article

Original de l’article mis en page : Le portable de Manuel Valls a-t-il été piraté par Israël ?

Un nouveau malware s’attaque aux Mac

Un nouveau malware s’attaque aux Mac

BitDefender a découvert Backdoor.MAC.Eleanor, un malware qui permet aux attaquants de prendre le contrôle des machines Apple sous Mac OS et de les piloter à travers le réseau d'anonymisation Tor.

Selon l'éditeur de sécurité, Eleanor est distribué sous forme d'un logiciel que l'on peut télécharger depuis des sites web légitimes dédiés à l'univers Apple. Une fois installé, l'agent malveillant affiche une interface de conversion de fichiers par drag&drop, service supposément légitime qui, en toute opacité, installe des composants sur le système. A partir de là, l'attaquant peut prendre le contrôle complet de la machine, y compris capturer des images depuis la webcam du portable. Comme Eleanor n'est pas certifiée Apple, les utilisateurs sous El Capitan, la dernière version d'OS X verront s'afficher un message d'alerte de sécurité lors de l'installation de l'application infectieuse. Une barrière qui permettra d'éviter le pire.
Article original de Silicon

Réagissez à cet article

Original de l’article mis en page : Télégrammes :Darktrace; Google; e-Privacy; backdoor Mac

---

Ce qui changera après l’adoption du règlement général sur la protection des données

Ce qui changera après l’adoption du règlement général sur la protection des données

---

La Cnil a mis en ligne, le 15 juin dernier, une de ses synthèse qui facilitent, même pour les juristes, lappréhension intellectuelle dune nouvelle législation, en loccurrence le désormais célèbre « Règlement général sur la protection des données », puisque tel est le nom raccourci officiel du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à légard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (notre actualité du 4 mai 2016).

À très grands traits, selon la Cnil :

« La réforme de la protection des données poursuit trois objectifs :
• Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
• Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
• Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées. »
Source : « Règlement européen sur la protection des données : ce qui change pour les professionnels », Cnil, 15 juin 2016.
S'ensuit une série de chapitres présentant les diverses facettes des quelque 173 considérants et 99 articles du règlement ainsi décrypté :
• Un cadre juridique unifié pour l'ensemble de l'UE
• Un renforcement des droits des personnes
• Une conformité basée sur la transparence et la responsabilisation
• Des responsabilités partagées et précisées
• Le cadre des transferts hors de l'Union mis à jour
• Des sanctions encadrées, graduées et renforcées
• Comment les autorités de protection se préparent-elles ?

Peu de changements en vérité…

Signalons, pour ceux qui s'imagineraient que tout change puisque le nouveau règlement abroge toutes les lois de protection des données des États membres de l'Union, que les changements sont en fait fort peu nombreux et que le cadre de protection, surtout tel que nous le connaissions depuis la réforme de notre loi du 6 janvier 1978 sous l'influence de l'ancienne directive 95/46 CE, en date du 1er août 2004. Ce sont les mêmes fondements qui ont présidé à l'élaboration de ces règles communes, automatiquement insérés dans le droit national des États membres.

…Mais des changements piégeant à la marge

Mais cependant, il faut s'attendre à des changements, d'autant plus subreptices qu'ils interviennent dans un océan de stabilité.
On pourrait distinguer deux ordres de dispositions modificatrices :
• Les dispositions qui sont réellement nouvelles, comme par exemple, en France, la disparition des déclarations préalables à la Cnil et quelques autres dispositions vraiment nouvelles ;
• Les dispositions qui existaient déjà dans l'ancienne directive mais qui n'avaient pas été transposées dans la loi d'un pays membre. C'est par exemple le cas du droit à l'oubli dans la loi allemande.

Une marge de manœuvre résiduelle

Cependant, il reste dans le règlement, une certaine latitude d'action de la part des États membres. On peut le comprendre techniquement en comparant un règlement européen à une loi nationale, ce qu'il est effectivement. Il faut donc prendre en compte le fait que chaque pays pourra selon sa sensibilité prendre les mesures d'application de ce règlement – sous forme de décrets en France – ce qui aura de nouveau pour effet d'introduire des divergences de régime d'un pays à l'autre.

Article original de Didier Frochot

Réagissez à cet article

Original de l'article mis en page : Le règlement général sur la protection des données : ce qui change en Europe

---

Peut-on communiquer les données personnelles du

défunt à ses ayants droit ?

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Toute personne physique justifiant de son identité a le droit dobtenir la communication des données personnelles qui la concernent. En revanche, est exclue la communication de ces données aux ayants droit qui ne sauraient être regardés comme des « personnes concernées ».

Mme et MM. D., ayants droit de Mme E. D., décédée le 2 août 2012, ont demandé à la Banque de France, dernier employeur de la défunte, la communication du relevé des derniers appels téléphonique qu'elle avait passé avec le corps médical avant son décès.
Après le refus de la Banque de France, ils ont déposé une plainte le 1er février 2013 auprès de la Cnil.
La Cnil ayant confirmé le refus de la Banque de France dans une décision du 29 mai 2013, ils saisissent le tribunal administratif de Paris qui, par un jugement du 9 décembre 2014, a directement transmis cette requête au Conseil d'Etat.

Le Conseil d'Etat se prononce dans un arrêt du 8 juin 2016.
Il rappelle qu'aux termes du dernier alinéa de l'article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ».
En outre, aux termes de l'article 39 de cette même loi, « toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir (…) la communication, sous une forme accessible, des données à caractère personnel qui la concernent (…) ».
Ainsi, il résulte de ces dispositions qu'elles ne prévoient la communication des données à caractère personnel qu'à la personne concernée par ces données. C'est donc à bon droit que la présidente de la Cnil a pris la décision attaquée à l'égard de Mme et MM. D., qui ne pouvaient, en leur seule qualité d'ayants droit, être regardés comme des « personnes concernées ».
Article original de Céline Solomides

Réagissez à cet article

Original de l'article mis en page : Impossibilité de communiquer les données personnelles du défunt à ses ayants droit

Les géants d’internet contrôlent de plus en plus l’information

Les géants d’internet contrôlent de plus en plus l’information

Entre les médias et les lecteurs, l'information passe aujourd'hui le plus souvent par les algorithmes des géants d'internet, qui contrôlent de fait ce flux et une bonne partie des revenus qu'il génère. Au point de susciter des inquiétudes.

« Ces 18 derniers mois, (ces géants d'internet) qui avaient jusqu'ici une relation distante avec le journalisme sont devenus des acteurs dominants de l'écosystème de l'information », résume le Tow Center for Digital Journalism de l'Université américaine de Columbia, dans une étude publiée en juin 2016. Beaucoup proposent aux éditeurs de presse de publier directement leur contenu sur leurs plateformes, à l'instar des canaux Instant Articles de Facebook ou Discover de Snapchat, et sont*« désormais directement impliqués dans tous les aspects du journalisme »*, fait valoir l'étude. La plupart des médias nouent des partenariats avec ces nouveaux acteurs de l'information pour maintenir ou développer leur exposition sur les moteurs de recherche et les réseaux sociaux, mais les perspectives financières restent incertaines.
« Il y a des gens qui font de l'argent sur internet, mais pas les médias, qu'ils soient tous supports ou uniquement en ligne », affirme une autre étude, du centre indépendant Pew Research Center, publiée mi-juin. Elle souligne ainsi qu'en 2015, 65% des revenus publicitaires en ligne étaient concentrés par cinq places fortes du web, Google, Facebook, Microsoft, Yahoo et Twitter, une proportion en hausse par rapport à 2014 (61%). Tout comme le modèle économique, c'est aussi le contenu et sa hiérarchie qui leur échappent, soumis au filtre des algorithmes. *« L'impact que ces sociétés technologiques ont sur le secteur du journalisme va bien au-delà de l'aspect financier, jusqu'à ses composantes les plus essentielles »*, considère l'institut Pew.
Désormais, les géants d'internet *« supplantent les choix et les objectifs des sites d'information et leurs substituent (les leurs) »*, affirme l'étude. Si certains y voient l'occasion d'une démocratisation de l'information, d'autres s'inquiètent d'une altération de sa qualité. *« Vous n'avez aucune idée de ce que les gens vont voir et il se peut tout à fait que (ce soit) quelque chose d'assez léger plutôt que des informations majeures »*, prévient Dan Kennedy, professeur de journalisme à l'Université Northeastern.

Le secret des algorithmes

Une étude réalisée par Nic Newman du Reuters Institute a fait état de*« préoccupations liées à la personnalisation des informations et une sélection algorithmique qui pourraient passer à côté de nouvelles importantes et de points de vue différents »*, selon le blog de son auteur. Mais *« les jeunes préfèrent les algorithmes aux éditeurs »* qui organisent l'information, constate-t-il. Ce pouvoir croissant des incontournables d'internet a attiré l'attention début mai lorsque le site d'information Gizmodo a accusé, témoignages à l'appui, Facebook d'avoir manipulé son fil de tendances. Après enquête interne, le plus grand réseau social du monde a conclu qu'il n'y avait pas eu de démarche concertée ou de manipulation, mais s'est engagé à préserver la neutralité de sa plateforme.
« Nous sommes une entreprise technologique, pas un média », a expliqué récemment la directrice d'exploitation de Facebook, Sheryl Sandberg, lors d'une table ronde à Washington. *« Nous n'essayons pas de recruter des journalistes ou de rédiger des nouvelles »*, a-t-elle martelé. Pour autant, l'intervention humaine reste nécessaire, selon elle, *« parce que sans cela, tous les jours à midi, le déjeuner serait une tendance »*. Même si la hiérarchisation des informations est largement automatisée sur ces plateformes, les programmes qui régissent ce processus sont bien rédigés par des humains qui opèrent, pour ce faire, des choix. Cela pose, dès lors,*« des questions quant à la transparence »* de l'ensemble, souligne Nicholas Diakopoulos, professeur de journalisme à l'université du Maryland. *« Il pourrait être intéressant de savoir de quelles données se nourrit le logiciel ou quels sites il suit »*, estime l'universitaire, pour qui *« il faut réfléchir à des normes de transparence ».*
Une étude publiée l'an dernier a révélé que le trafic des principaux sites d'information en provenance de Facebook avait chuté de 32% après une modification des algorithmes du réseau social. *« Il est vrai que Facebook peut faire décoller ou tuer un site d'information selon la façon dont il calibre son algorithme »*, reconnaît Nikki Usher, professeure de nouveaux médias à l'Université George Washington. *« D'un autre côté, les médias n'ont jamais eu à rendre de compte sur les décisions qu'ils prenaient »* en matière éditoriale, fait-elle valoir.

Article original de Joël Ignasse

Réagissez à cet article

Original de l'article mis en page : Les géants d'internet contrôlent de plus en plus l'information – Sciencesetavenir.fr

Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

	Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

La Commission de l'Informatique et des Libertés (CIL) en partenariat avec les tribunaux du palais de justice de Ouagadougou, organise un séminaire de sensibilisation des magistrats et greffiers du palais de justice de Ouagadougou aux « enjeux de la protection des données personnelles et de la vie privée des citoyens à l'ère du numérique ». Ce séminaire se déroule à Ouagadougou ce mardi 28 juin 2016.

« Aucune personne n'est, de nos jours, à l'abri des actes cybercriminels, quel que soit son statut, son rang ou l'état de ses connaissances », a lancé Marguerite Ouédraogo/Bonané, présidente de la CIL. Si de nos jours la cybercriminalité avance à grand pas dans le monde entier, force est de constater que les initiatives pour l'affronter ne manquent pas. La lutte contre cette nouvelle forme de criminalité impose donc que de « nouvelles approches soient développées et que toutes ses dimensions soient maitrisées », a-t-elle reconnu. Dans l'optique de protéger les données des justiciables en justice, la CIL entend informer et sensibiliser les magistrats aux droits des personnes dont les données sont utilisées. « Notre mission aujourd'hui c'est de les informer et de les sensibiliser aux droits des personnes dont les données sont utilisées », a confié marguerite Ouédraogo/Bonané. A l'en croire, la protection des données couvre tout le territoire. Par conséquent, tous les Burkinabé sont concernés par cette protection. Elle révèle que ce séminaire ouvert aux magistrats permettra à ces derniers de protéger les données des justiciables comme le stipule « notre loi ».

Des communications qui seront faites dans ce séminaire

Plusieurs communications seront faites durant ce séminaire. En substance, une communication sera faite à l'intention des magistrats pour leur faire connaitre le cadre juridique et institutionnel des données personnelles au Burkina Faso. Une autre sera de leur faire connaitre la communication sur l'enquête judiciaire et la protection des données personnelles face à l'enquête judiciaire. Aussi, la formation sur l'utilisation de l'internet et des réseaux sociaux leur sera-t-elle donnée.

Vu l'importance de ce séminaire qui est focalisé sur les acteurs de la justice, Dieudonné Manly, Conseiller Technique du ministère de la justice, accorde un peu plus de crédit à l'ordre du jour quand il affirme qu' « aujourd'hui la cybercriminalité a pris de l'ampleur et il va falloir outiller les magistrats afin qu'ils puissent faire face à ce phénomène ». Aussi, pense-t-il que les thèmes choisis sont bien réfléchis et que ces thèmes vont, à son avis, « permettre aux magistrats de faire face à la cybercriminalité ».

Article original de Armand Kinda

Réagissez à cet article

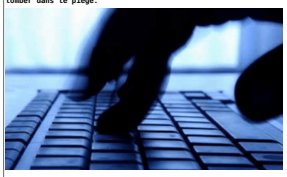
Original de l’article mis en page : Lutte contre la cybercriminalité : les magistrats du palais de justice de Ouagadougou outillés pour en faire face

---

Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

En Côte d'Ivoire, les préjudices financiers causés par les cybercriminels se chiffrent en milliards. Dans sa stratégie de sensibilisation, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) entreprend d'informer les populations sur les arnaques les plus récurrentes afin de leur permettre de ne pas tomber dans le piège.



Selon les chiffres communiqués par la PLCC, au cours de l'année 2015, le préjudice financier causé par la cybercriminalité a atteint 3 980 833 802 FCFA, contre **5 280 000 FCFA** en 2015. Ce sont **1 409** plaintes qui ont été enregistrées. Elles ont abouti à l'arrestation de **205** individus, dont **159** ont été déférés au parquet. Afin d'informer davantage les populations, la PLCC a sorti les 5 types arnaques qui ont été les plus récurrentes au cours du premier trimestre 2016.

1- La Sextorsion (Enregistrement illégal de communication privée, chantage à la vidéo)

Ce type d'arnaque a occasionné un préjudice de **119 millions de Franc CFA**. Cette technique consiste pour un cybercriminel à se procurer une vidéo intime de sa victime et d'exercer sur elle un harcèlement dont la condition de dénouement est le paiement d'une somme d'argent. Pour y arriver, le cybercriminel s'arrange à établir une relation amicale voire amoureuse avec sa future victime, de manière à gagner son entière confiance. Par la suite, il lui demandera de lui fournir ladite vidéo (en lui demandant d'activer sa caméra au cours d'un échange par exemple), qui deviendra finalement le moyen de pression du cybercriminel.

2 – L'accès frauduleux à un système informatique

Ce type d'arnaque est généralement orienté vers les entreprises. Au premier trimestre 2016, il a causé un préjudice financier de **42.271.426 F CFA**. Elle consiste pour le cybercriminel, à forcer l'accès d'un système informatique pour éventuellement voler des donner, ou causer des dégâts pour porter préjudice.

3 – L'usurpation d'identité (Utilisation frauduleuse d'élément d'identification de personne physique ou morale)

L'usurpation d'identité consiste pour un individu à se faire passer pour une autre. Avec des moyens détournés, le cybercriminel réussi à soutirer des informations sensibles qu'il utilise plus tard pour effectuer des paiements, effectuer des paiements etc. Il peut même aller plus loin en engageant la personne de sa victime, par une signature d'accord par exemple, sans son consentement préalable. Ce sont 37.851.973 Franc CFA de dommages qui ont été causés par ce type d'arnaque sur la même période.

Lire aussi : INTERNET : La sécurité des usagers, dernier soucis des fournisseurs d'accès en Côte d'Ivoire ?

4 – L'arnaque au faux sentiment

Ce type d'arnaque est en net recul, après avoir fait de nombreuses victimes à travers le monde. De plus en plus, les internautes sont plus prudents quoique des victimes continuent de se faire duper. 28.754.746 F CFA, c'est le préjudice causé par ce type d'arnaque au premier trimestre 2016.

5 – La fraude sur le porte-monnaie électronique

Avec l'expansion des services de porte-monnaie électronique via le mobile, ce type d'arnaque a pris de l'ampleur.

Bien ficelée, cette technique pousse la victime donner le contrôle absolu à un cybercriminel sur son compte, sans même le réaliser. Par un simple appel ou SMS, le cybercriminel invite son sa victime à saisir un code USSD, pour bénéficier d'un prétendu bonus. Une fois que la procédure est engagée, la carte SIM de la victime est désactivée, son compte transférée sur une nouvelle carte SIM. Le cybercriminel a alors le contrôle absolu.

Article original de Stéphane Agnini

CREDIT : DR

Original de l'article mis en page : Regionale.info CYBERCRIMINALITE : TOP 5 des arnaques les plus récurrentes au premier trimestre 2016 selon la PLCC > Regionale.info

---

Des complices de cyberescrocs arrêtés en Côte d'Ivoire

Des complices de cyberescrocs arrêtés en Côte d'Ivoire

Utilisation frauduleuse d'éléments d'identification de personne physique, tentative d'escroquerie et complicité d'escroquerie sur internet. Accusés de tous ces crimes, Traoré Issouf, 28 ans, et Kouadio Konan Daniel, 27 ans, tous deux caissiers dans une agence de transfert d'argent nouvellement ouverte, séjournent à la Maison d'arrêt et de correction d'Abidjan (Maca), dans l'attente d'un procès.

Comme l'explique la Plateforme de lutte contre la cybercriminalité (PLCC), ces deux individus ont été arrêtés le 20 juin 2016 par ses agents. Ils sont suspectés d'avoir effectué des transferts frauduleux au profit de quelques cyberescrocs, qui recourent bien souvent à des employés de maisons de transfert d'argent pour encaisser leur butin.
Pour chaque transfert effectué, Kouadio Konan Daniel a avoué avoir perçu une commission de 10%. Mais pouvaient-ils vraiment nier les faits? Après analyse des éléments en leur possession, le Laboratoire de criminalistique numérique (LCN) de la Direction de l'informatique et des traces technologiques (DITT) a pu extraire de nombreux codes de transfert d'argent envoyés par téléphone portable.
Article original de Anselme Akéko – CIO-Mag Abidjan

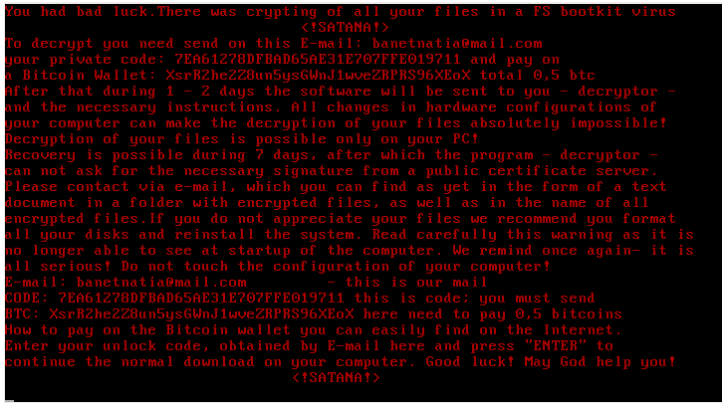
Réagissez à cet article

Original de l’article mis en page : Transfert d’argent : des complices de cyberescrocs arrêtés en Côte d’Ivoire | CIO MAG

Satana, un ransomware pire que Petya

Satana, un ransomware pire que Petya

Le nouveau rançomware Satana cumule chiffrement des fichiers et remplacement du secteur d'amorçage du disque.



Une nouvelle génération de ransomware est en train d'émerger. Satana, nom du nouveau malware, combine chiffrement des fichiers et écriture de code sur le secteur d'amorçage du disque, le MBR. Deux techniques inspirées de Petya et Mischa, note Malewarebytes qui constate la croissance du nouvel agent satanique ces dernières semaines.
« *Satana fonctionne en deux modes*, note la société de sécurité sur son blog. *Le premier se comporte comme Petya, un fichier exécutable (sous Windows, NDLR) [et] écrit au début du disque infecté un module de bas niveau, un bootloader avec un noyau personnalisé. Le deuxième mode se comporte comme un ransomware typique et chiffre les fichiers un par un (tout comme Mischa).* » Mais à la différence que les deux modes ne sont pas exploités alternativement mais bien appliqués ensemble, l'un après l'autre, pour s'attaquer à leurs victimes.

Payer ne garantit rien chez Satana

Malwarebytes ne le précise pas mais le mode de propagation de Satana reste probablement classique. A savoir par e-mail (et éventuellement d'un expéditeur en recherche de travail avec des liens vers les fichiers infectieux comme dans le cas de la première version de Petya). Une fois le MBR remplacé, le malware s'attaque au chiffrement des fichiers du disque (et des éventuels volumes reliés à l'ordinateur) et attend patiemment que le système soit redémarré. Quand c'est le cas, un message s'affiche sur l'écran expliquant la démarche à suivre pour récupérer l'accès à son PC, à savoir le paiement d'une rançon de 0,5 bitcoin (plus de 300 euros au cours du jour).
Si l'utilisateur parvient néanmoins à remplacer le MBR par un fichier d'amorçage sain (une manipulation manuelle qui est loin d'être à la portée de tout le monde), il se heurtera aux fichiers chiffrés sur le disque. Lesquels ont été renommés avec, en en-tête du nom, un e-mail aléatoirement choisi parmi ceux de l'équipe des développeurs de Satana, selon l'expert en sécurité (Gricakova@techmail.com, dans l'exemple présenté). Et les méthodes de chiffrement semblent suffisamment avancées pour rendre les fichiers piégés définitivement irrécupérables. D'autant que Malewarebytes pointe un bug pour le moins problématique pour la victime. De par le mécanisme de chiffrement/déchiffrement des fichiers, en cas de déconnexion au serveur de commandes et contrôle (C&C), la clé de décryptage (qui est la même que pour le cryptage) est perdue. Brisant tout espoir de la victime à pouvoir récupérer ses données (sauf à avoir fait préalablement des sauvegardes). « *Même les victimes qui paient peuvent ne pas récupérer leurs fichiers si elles (ou le C&C) sont hors ligne lorsque le chiffrement arrive* », prévient la société de sécurité.

Du code en cours de perfectionnement

Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. « *Habituellement les auteurs de logiciels malveillants ne veulent pas laisser le code de débogage dans leur produit final* », écrit le chercheur. Lequel conclut que Satana est probablement encore en cours de développement et contient des failles. « *Le code d'attaque de bas niveau semble inachevée – mais les auteurs montrent un intérêt dans le développement du produit dans ce sens et nous pouvons nous attendre que la prochaine version sera améliorée.* » Une nouvelle génération de rançongiciel est bien en marche.
Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Satana, un ransomware pire que Petya

---

Des cybercriminels s’attaquent à la ministre Raymonde Goudou

Des cybercriminels s’attaquent à la ministre Raymonde Goudou

La cybercriminalité prend de plus en plus de l'ampleur en Côte d'Ivoire. Malgré les moyens mis en place par le ministère de l'Intérieur à travers la plateforme de lutte contre la cybercriminalité (PLCC), certaines personnes s'évertuent à poursuivre cette infraction sans être inquiétés. La dernière en date est celle d'une personne qui se fait passer pour la Ministre de la Santé, Raymonde Goudou Coffie, pour arnaquer.

Nous ne savons pas si des individus ont piraté le compte Facebook de la ministre ivoirienne de la santé ou s'il s'agit d'une usurpation d'identité. Quoiqu'il en soit, des individus utilisent l'identité de la ministre Raymonde Goudou Coffie pour faire de l'aumône auprès des utilisateurs des réseaux sociaux.
A titre illustratif, nous vous publions la conversation que ces prémusés arnaqueurs (brouteurs dans le jargon ivoirien) ont eu avec l'une de leurs victimes.

K.O.
Article original de imatin

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité: Des « brouteurs » s’attaquent à la ministre Raymonde Goudou