Nouvelle forme d’attaque informatique, les crypto-vers

Nouvelle forme d’#attaque informatique, les crypto-vers

Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints d'inventer une nouvelle façon d'installer leur rançongiciel (#ransomware). Leur solution: le ver.

Le spécialiste de la sécurité Kaspersky lance donc une mise en garde. Le 'crypto-ver' est « une forme mixte dangereuse de maliciel (malware) et de rançongiciel qui se répand d'elle-même ». Elle peut se propager d'ordinateur à ordinateur, sans spam (pourriel) ou autre infection. Le malware se duplique simplement dans les appareils interconnectés.
Le premier ver, baptisé SamSam, s'est manifesté en avril. Et au cours des dernières semaines, des experts en sécurité ont découvert le ver ZCryptor. Ce dernier se présente sous la forme d'une simple mise à jour d'un programme largement utilisé tel Flash. Une fois en place, le ver commence à se propager, puis il crypte des dizaines d'extensions. Les victimes voient ensuite apparaître leur écran habituel, qui les informe que leurs fichiers ont été pris en otage et qu'ils doivent verser une rançon pour pouvoir y accéder de nouveau.
Les spécialistes des la sécurité n'ont pas encore trouvé une parade contre ZCryptor. Voilà pourquoi Kaspersky prodigue le conseil suivant: soyez sur vos gardes, veillez à disposer d'une bonne protection et effectuez régulièrement des sauvegardes (backups).

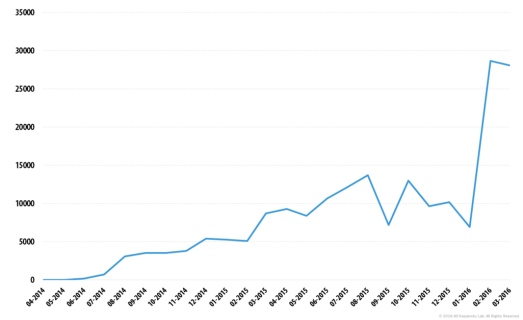
Réagissez à cet article

Original de l'article mis en page : Nouveau: le ver ravisseur – ICT actualité – Data News.be

Evolution des Ransomwares pour appareils mobiles en 2014-2016

Evolution des Ransomwares pour appareils mobiles en 2014-2016

L'activité des ransomwares pour appareils mobiles, qui ne bénéficie pas de la même couverture médiatique que les ransomwares pour PC, a également explosé au cours de la période couverte par le rapport. Et plus particulièrement au cours de la deuxième moitié de celle-ci.



Nombre d'utilisateurs confrontés à des ransomwares pour appareils mobiles au moins une fois au cours de la période comprise entre avril 2014 et mars 2016

D'avril 2014 à mars 2015, les solutions de Kaspersky Lab pour Android ont protégé 35 413 utilisateurs contre des ransomwares pour appareils mobiles. Un an plus tard, ce nombre avait presque quadruplé et atteignait 136 532 utilisateurs. La part des utilisateurs attaqués par des ransomware par rapport aux utilisateurs attaqués par n'importe quel autre type de malware a également augmenté : de 2,04 % pour la période 2014-2015, elle est passée à 4,63 % pour la période 2015-2016. La courbe de croissance est peut-être plus modeste que celle observée pour les ransomwares pour PC, mais son ampleur suffit à confirmer une tendance inquiétante.

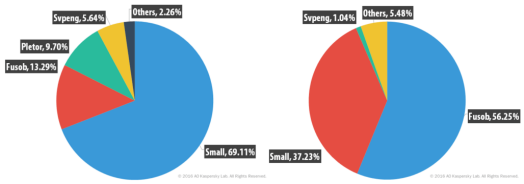
Principaux acteurs dans le milieu des ransomwares pour appareils mobiles

Sur l'ensemble de la période couverte par le rapport, les chercheurs de Kaspersky Lab ont été en mesure d'identifier les quelques familles de ransomwares pour appareils mobiles auxquelles les utilisateurs de nos produits étaient les plus souvent confrontés. En 2014-2015, il s'agissait de : Pletor, Fusob, Svpeng et Small. En 2015-2016, l'activité de Svpeng a enregistré une dégringolade et n'a concerné qu'une part modeste des utilisateurs attaqués.

A un moment donné en 2014-2015, Svpeng, connu à l'origine comme un malware bancaire, a été modifié par ses créateurs afin de pouvoir verrouiller un appareil infecté. Depuis lors, nous avons suivi les deux versions de Svpeng : le malware bancaire et le ransomware. La version ransomware est devenue populaire en 2014-2015 lorsqu'elle a touché 5,64 % des utilisateurs attaqués par un malware quelconque.

La situation a toutefois changé au cours de la deuxième période lorsque le ransomware a chuté vers le bas du Top 30 des menaces. Toutefois, la version malware bancaire de Svpeng a repris du service, ce qui signifie probablement que les créateurs du malware ont simplement perdu leur intérêt dans le développement d'un ransomware et ont décidé de se concentrer sur le malware bancaire.

Pletor, le malware considéré comme le premier exemple de ransomware et prétendument créé par les auteurs du tristement célèbre trojan bancaire Acecard, a connu une situation similaire. Au cours de la période 2014-2015, il a touché une part considérable des utilisateurs mobiles attaqués par des ransomwares mais en 2015-2016, il ne figurait plus dans le haut du classement et laissait le « marché » à seulement trois grandes familles de ransomwares.



Répartition de la part d'utilisateurs attaqués entre les familles de ransomwares pour appareils mobiles les plus actives en 2014-2015 (gauche) comparée à celle de 2015-2016 (droite).

Parmi les autres phénomènes importants observés au cours des 24 mois couverts par le rapport, on ne peut ignorer la concurrence entre deux grandes familles de ransomwares : Small et Fusob. En 2014-2015, c'est la famille Small qui dominait, du moins en termes de parts d'utilisateurs attaqués. Elle était signalée par 69,11 % de l'ensemble des utilisateurs qui avaient été confrontés au moins une fois à des ransomwares pour appareils mobiles. Mais un an plus tard, c'est la famille Fusob qui prenait la tête avec 56,25 % des utilisateurs. Toutefois, la famille Small se maintenait en 2e position avec 37,23 % des utilisateurs attaqués. Il est probable que les malwares Svpeng, Pletor, Small et Fusob seront vendus par leurs auteurs à d'autres cybercriminels ou qu'ils seront propagés via des réseaux d'affiliés. Les quatre familles ont subi de nombreuses modifications. Cependant, Small et Fusob semblent avoir été les plus modifiés, comme on peut le voir clairement dans les statistiques.

A la différence du phénomène des ransomwares pour PC qui est déjà largement couvert par les chercheurs de différentes sociétés, dont Kaspersky Lab, les ransomwares pour appareils mobiles n'ont pas encore fait l'objet d'une analyse en profondeur. Afin de remédier à cette situation, nous proposons une brève description des ransomwares les plus répandus et les plus dangereux à compter d'avril 2016

Pour en savoir plus sur l'évolution de la menace des ransomwares, lisez le rapport complet accessible via.

Article original de Kaspersky Lab

Réagissez à cet article

Original de l’article mis en page : Rapport KSN : ransomwares pour appareils mobiles en 2014-2016 – Securelist

---

Le nombre de cyberattaques contre des cibles françaises double chaque année

	Le nombre de cyberattaques contre des cibles françaises double chaque année

---

Le salon international Eurosatory de défense et de sécurité s'ouvre lundi près de Paris alors que les cyberattaques contre des cibles françaises se multiplient.

Le salon international Eurosatory de défense et de sécurité s'installe comme tous les deux ans à partir de lundi à Villepinte, près de Paris. Cette manifestation qui rassemble les stratèges et les industriels du monde entier met de plus en plus l'accent sur deux concepts devenus incontournables : l'utilisation des drones et les outils de la cyberguerre. Une demi-douzaine de conférences se tiendront cette semaine sur la cybermenace et sur les moyens de la contrer ou de la mettre en œuvre. En France, depuis l'adoption du livre blanc 2013 et la loi de programmation militaire 2014-2019, la dimension « cyber » de nos armées « a changé de braquet », comme le confie au *JDD* l'un des meilleurs experts gouvernementaux de ce dossier.

Selon lui, le nombre de cyberattaques contre des cibles françaises double chaque année et le niveau de sophistication des agressions également. « Un individu aujourd'hui peut nous faire autant de mal qu'un État », précise notre source. Chaque jour en France, les unités informatiques liées aux institutions ou aux entreprises du secteur de la défense sont agressées par des milliers d'attaques. Des raids visant à saturer des adresses liées au ministère de la Défense se multiplient et il peut arriver que le compte personnel du ministre soit visé avec intention de nuire. Au point qu'aujourd'hui pas une seule clé USB ne peut entrer dans une installation de défense française sans être passée par une « station blanche » de décontamination.

Détruire sans avoir à bombarder

Mais le plus grand risque serait évidemment que nos unités militaires engagées sur un théâtre d'opérations soient attaquées en pleine action. Le pacte défense cyber lancé début 2014, et renforcé après les attentats de 2015, a prévu un investissement de plus d'un milliard d'euros et le triplement des effectifs militaires et civils concernés. « Aujourd'hui, plus un seul déploiement d'une unité sur le terrain ne se conçoit sans un accompagnement cyber », indique notre source.

Un officier général « cyber » est affecté en permanence auprès de l'état-major au Centre de planification et de conduite des opérations (CPCO). Il ne s'agit pas seulement de se protéger lors d'une attaque mais aussi de se défendre lorsqu'elle est en cours ou même d'attaquer en cas de besoin. Tout comme le fait depuis longtemps Israël contre ses adversaires au Moyen-Orient, l'État hébreu étant avec les États-Unis, la Chine et la Russie l'un des quatre pays les plus avancés dans ce domaine avec des moyens dix à vingt fois plus importants que ceux de la France. Mais on réfléchit à Paris à l'idée de créer une cyberarmée à l'image de l'US Cyber Command américain. Pour se préparer à ces guerres invisibles où l'on peut détruire une installation ennemie sans avoir à la bombarder ou à brouiller ses radars depuis un ordinateur pour mieux déclencher des raids plus… conventionnels.

Article original de François Clemenceau – Le Journal du Dimanche

---

Réagissez à cet article

Original de l’article mis en page : Faut-il investir dans la guerre invisible? – leJDD.fr

---

Inquiétantes intrusions dans les réseaux d’entreprises

Inquiétantes intrusions dans les réseaux d’entreprises

Les intrusions dans les réseaux informatiques des entreprises se sont multipliées en France ces derniers mois et labsence de vols de données laisse craindre des tentatives de sabotages ou dattaques terroristes, a déclaré lundi le directeur général de lAgence nationale de la sécurité des systèmes dinformation (Anssi).

Le Secrétariat général de la défense et la sécurité nationale (SGDSN) et l'Anssi, deux services rattachés à Matignon, ont présenté lundi les trois premiers arrêtés liés à la protection des opérateurs d'importance vitale dans la santé, la gestion de l'eau et l'alimentation, qui entreront en vigueur le 1er juillet.
« Il y a de plus en plus d'attaquants, ce sont des agents dormants qui préparent les choses », a expliqué Guillaume Poupard à des journalistes. « Il y a eu beaucoup de cas à traiter ces derniers mois ».
Ces intrusions, par exemple par le biais d'emails piégés envoyés dans les entreprises, permettent aux attaquants de cartographier un réseau en toute discrétion et, en passant d'un réseau à l'autre, de pénétrer dans des zones inattendues.
« Ils prennent pied progressivement (..) et on les retrouve très profond au sein des réseaux d'entreprises, à des endroits où il n'y a même plus d'informations secrètes à voler, par exemple sur les systèmes de production de contrôle qualité », a ajouté Guillaume Poupard.
Ce nouveau type d'intrusion est d'autant plus inquiétant qu'il est presque plus facile d'entrer dans un réseau pour en modifier le fonctionnement ou en prendre le contrôle que pour voler des données, a-t-il souligné.
Au contraire de la banque, de l'aérospatiale et de l'automobile, habitués à surveiller de près leurs réseaux, l'industrie est encore mal préparée, étant moins sujette aux vols de données, a noté Guillaume Poupard.
« L'idée que des gens qui depuis l'autre bout du monde puissent chercher à détruire leur système de production c'est un nouveau scénario qui n'a pas vraiment d'équivalent dans le monde réel », a-t-il souligné.
Pour mieux défendre les PME, « un des maillons faibles », cible rêvée d'un attaquant, il prône le recours aux solutions de « cloud computing » des spécialistes de la sécurité numérique et à l'intégration de systèmes de protection dans les machines outils et les automates industriels dès leur conception. (Cyril Altmeyer, édité par Jean-Michel Bélot)

Réagissez à cet article

Original de l’article mis en page : SAFRAN : France : Inquiétantes intrusions dans les réseaux dentreprises

Des caméras de surveillance piratées pour mener des attaques DDoS

Des caméras de surveillance piratées pour mener des attaques DDoS

Tous ceux qui refusent d'admettre que l'Internet des Objets pourrait être à l'origine de nombreuses menaces dans la sphère informatique de demain vont probablement avoir du mal à tenir leur position après l'affaire présentée ici. En effet, des hackers ont utilisé un réseau de 25 000 caméras de surveillance piratées pour conduire des attaques DDoS.

Des caméras de surveillance piratées pour former un botnet

Il y a quelques heures, l'entreprise Sucuri, spécialisée dans la sécurité informatique, a découvert que des hackers avaient réussi à prendre le contrôle de quelques 25 000 caméras de surveillance présentes au quatre coins de la planète.

Mais l'objectif des pirates n'était pas que de récupérer des images ou d'espionner des individus puisqu'ils ont utilisé les caméras de surveillance pour créer un botnet, autrement dit un réseau de machines contrôlées à distance par un seul et même individu.

Capables d'agir ensemble, les 25 000 caméras ont ainsi pu être à l'origine d'attaques DDoS contre plusieurs sites Internet. En effet, les hackers se sont servis du réseau de caméras de surveillance pour envoyer des requêtes simultanées sur des sites causant ainsi leur paralysie pendant de longues minutes.

Une preuve supplémentaire de la menace que laissent planer les objets connectés

Si l'utilisation d'objets connectés par les pirates pour mener des attaques DDoS est tout sauf une nouveauté, c'est l'ampleur de l'attaque qui surprend. En effet, même les spécialistes sont restés « coi » devant la capacité d'un réseau de 25 000 caméras de surveillance à générer autant de requêtes simultanément.

L'autre surprise tient au fait que les caméras piratées sont dispatchées aux quatre coins de la planète. 2% seraient d'ailleurs basées en France alors que c'est aux Etats-Unis, en Indonésie et à Taïwan que la majorité d'entre elles se situerait.

Sucuri a d'ailleurs cherché à comprendre ce que pouvait avoir en commun l'ensemble de ces appareils et la piste la plus sérieuse mène à BustyBox, un système qui serait intégré à tous. Or, une importante faille avait été découverte au printemps dans celui-ci ce qui aurait pu permettre à des pirates de l'exploiter pour commettre leurs actions.

Affaire à suivre…

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l’article mis en page : Des caméras de surveillance piratées pour mener des attaques DDoS

L’Etat français (ANSSI) va certifier les Cloud de confiance

L’Etat français (ANSSI) va certifier les Cloud de confiance

L'Agence nationale pour la sécurité des systèmes d'information (Anssi) s'apprête à certifier les Cloud de quelques prestataires. Deux niveaux de labellisation sont attendus.

L'Agence nationale pour la sécurité des systèmes d'information (Anssi), dépendant du Premier ministre, est engagée dans un processus qui aboutira à la qualification des fournisseurs de Cloud. Les prestataires présentant le niveau de sécurité requis recevront donc un label de l'Agence, qui permettra aux entreprises et administrations de recourir à leurs services en se basant sur les garanties fournies par l'Etat français. « *Huit prestataires se sont lancés dans ce processus de qualification* », assure Guillaume Poupard, le directeur général de l'Anssi, qui a appelé les grands acteurs du Cloud américains à rejoindre le mouvement. « *La qualification n'est pas un outil de protectionnisme* », reprend Guillaume Poupart. Selon lui, les AWS et autre Microsoft (pour Azure) sont en train d'étudier une éventuelle qualification. Façon de dire aussi qu'il n'est pas acquis qu'ils se soumettent un jour aux exigences de l'Anssi.
Notons que, sur ce dossier, l'Anssi travaille en coordination avec ses homologues allemands du BSI (l'Office fédéral de la sécurité des technologies de l'information) : un prestataire homologué outre-Rhin recevra automatiquement son label dans l'Hexagone et vice-versa.

Deux niveaux : Cloud Secure et Cloud Secure +

Ce label étatique fait suite à une démarche entamée dès la mi-2014. A cette époque, l'Anssi avait publié un premier référentiel et appelé les entreprises à le commenter. Un grand nombre de commentaires, parfois critiques, avaient été remontés à l'Agence. Depuis, cette dernière a réuni un comité restreint pour travailler à une seconde version du référentiel, largement inspiré de la norme ISO 27 001.

Guillaume Poupard, directeur général de l'Anssi.

En réalité, la démarche doit accoucher de deux niveaux de qualification : Cloud Secure et Cloud Secure +. Dans la première, selon des déclarations publiques d'un membre de l'Anssi en octobre dernier, on retrouve des bonnes pratiques assez classiques : contrôles d'accès physiques, authentification forte avec mots de passe hachés et salés, chiffrement logiciel et hébergement des données en Europe. Le niveau le plus élevé ira plus loin, imposant une authentification multi-facteurs, un chiffrement matériel (via HSM) ou encore un hébergement en France. Parmi les acteurs figurant dans la liste des premiers prestataires certifiés, on devrait retrouver Thales, Orange ou Oodrive, qui se présentait en octobre dernier comme l'acteur pilote de la qualification Secure Cloud +. Notons qu'à l'époque, l'Anssi indiquait que les OIV – les quelque 250 organisations identifiées comme essentielles au fonctionnement de la nation – pourraient se voir imposer le recours à des prestataires certifiés Secure Cloud +. Les premiers arrêtés encadrant les politiques de sécurité des OIV n'y font toutefois pas référence à ce jour.

Cloud Secure + : les Américains out ?

« *Nous nous sommes engagés à nous conformer à cette norme auprès de certains clients* », explique Laurent Seror, le président d'Outscale, le fournisseur de Iaas né sous l'impulsion de Dassault Systèmes. « *Etant donné que nous sommes déjà certifiés ISO 27 001, je considère que nous sommes prêts. Ne pas être certifié juste au moment de la sortie du référentiel ne sera pas pénalisant compte tenu de la longueur des cycles de décision* », ajoute Laurent Seror. Ce dernier relève toutefois que, par construction, le niveau Cloud Secure + restera difficile à atteindre pour les grands prestataires américains. D'abord parce qu'ils ne possèdent pas, à ce jour, de datacenter en France (à l'exception de Salesforce). Mais, au-delà de ce seul élément, d'autres questions se posent. Selon lui, chez AWS, un administrateur américain, donc soumis au Patriot Act, peut accéder à toutes les machines virtuelles, quelle que soit la zone où ces dernières sont hébergées. « *On en est sûr à 99% en raison de la nature d'une fonction qu'ils proposent pour la migration entre deux régions géographiques. Celle-ci suppose l'existence d'un réseau à plat entre toutes les plates-formes.* »
La question de la localisation des données reste un élément central de la politique de certains pays européens souhaitant reconquérir leur souveraineté dans le Cloud. Lors du débat au Sénat sur le projet de loi pour une République numérique (porté par Axelle Lemaire), un amendement, déposé par les sénateurs du groupe communiste et prévoyant d'obliger les entreprises à stocker les données personnelles des citoyens français sur le territoire européen, a été voté. « *Cet amendement n'était pas téléguidé*, assure aujourd'hui Guillaume Poupard. *Je l'ai découvert au moment des débats.* » Le 29 juin, une commission mixte paritaire doit harmoniser les versions de ce projet de loi sorties respectivement des débats à l'Assemblée et au Sénat. Rien ne permet d'affirmer que ledit amendement, absent de la version votée par le Palais Bourbon, soit présent dans la mouture finale du texte de loi.
Article original de Reynald Fléchaux

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 du 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 : L'Etat français va certifier les Cloud de confiance

---

Cybercriminalité : « Il faut qu'on voie que la Côte d'Ivoire réagit » | CIO MAG

Cybercriminalité : « Il faut qu'on voie que la Côte d'Ivoire réagit »

« L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici », assure Denis Jacopini, expert informatique assermenté spécialiste en cybercriminalité et protection des données personnelles. Membre de la Compagnie nationale française des experts de Justice en Informatique et techniques associées (CNEJITA), il a participé du 7 au 8 juin 2016 à Abidjan, à la 8ème édition de l'IT Forum Côte d'Ivoire sur la « Transformation numérique face à la protection des utilisateurs ». Loin des clichés et des idées reçues, le professionnel du crime en ligne a confié à CIO Mag l'image que la Côte d'Ivoire donne de l'extérieur et fait des propositions allant dans le sens de l'amélioration de la lutte contre la cybercriminalité. Sensibilisation des décideurs, opérations coup de poing, médiatisation des arrestations… la Côte d'Ivoire est, selon lui, en bonne voie pour renforcer la confiance dans son environnement numérique.

7 juin 2016. Denis Jacopini à la 8ème édition de l'IT Forum Côte d'Ivoire qui s'est déroulée du 7 au 8 juin dernier à la Maison de l'Entreprise, à Abidjan, sur le thème : « Transformation numérique face à la protection des utilisateurs ».

CIO Mag : Quelle image la Côte d'Ivoire donne-t-elle de l'extérieur dans le domaine de la cybercriminalité ?
Denis Jacopini : Depuis quelques années, la Côte d'Ivoire est connue en Europe comme le pays d'Afrique où se passent la très grande majorité des arnaques sur internet, à un point où lorsque quelqu'un reçoit un email qui vient de Côte d'Ivoire, il pense automatiquement à une arnaque, au mieux se méfie, au pire supprime le message sans même lui accorder la moindre attention. Ainsi, associer la Côte d'Ivoire à des arnaqueurs, n'est pas bon pour l'image du pays. Ceci dit, ma présence ici m'a réconforté.
En lisant la presse spécialisée, dont CIO Mag, je savais déjà que la Côte d'Ivoire réagissait face à ce phénomène, qu'elle mettait en place des méthodes et qu'elle engageait des actions pour permettre à la fois aux directeurs de systèmes d'information – DSI – et aux utilisateurs d'augmenter en compétence et de se soucier de ce problème de sécurité. Et, en venant ici, ça m'a réconforté. Je m'en suis surtout rendu compte au travers du discours du ministre de l'Economie numérique et de la Poste (à l'ouverture de la 8ème édition de l'IT Forum Côte d'Ivoire, NDLR). Il a fait une présentation de la manière dont il voit l'évolution de la Côte d'Ivoire dans le domaine du numérique. Son discours a été rassurant en indiquant que le pays avait à la fois une démarche active dans la cybersécurité et accordait une attention particulière aux moyens permettant d'associer confiance et développement numérique.
On a facilement pu remarquer que le ministre maîtrise le sujet et qu'il sait de quoi il parle. Il est prêt à emmener avec lui le pays dans cette transformation numérique. Quasiment toutes les entreprises vont devoir assurer cette métamorphose. Le pays doit pouvoir les accompagner dans cette transformation numérique. L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici.

C.M : Selon vous quels sont les actions sur lesquelles la Côte d'Ivoire doit miser pour véritablement restaurer son image et créer un environnement numérique de confiance ?
D.J : A mon avis, ça devrait passer par une médiatisation des arrestations. Il y a des milliers de délinquants ayant organisé et mené des arnaques en tous genres à partir de cybercafés. On apprend de temps en temps sur la presse francophone spécialisée que se sont produites des arrestations mais ça reste sur les journaux peux lus. Il faut vraiment s'intéresser à la Côte d'Ivoire et consulter la presse locale pour le savoir. A mon avis, les actions qui sont faites dans le pays mais aussi tous les accords et toutes les coopérations qui sont établis avec les autres pays doivent internationalement être connues et notamment par le grand public qui a besoin d'être rassuré car régulièrement victime d'actes originaires d'ici.
Lorsqu'il y a une coopération qui est mise en place avec l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information, NDLR) en France, avec l'OCLCTIC, l'Office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication, en termes de formation et de sensibilisation en Côte d'Ivoire, il faut que cela se sache. Il faut qu'on voie que la Côte d'Ivoire réagit que les autorités se forment, sont en train de monter en compétence. Maintenant, ce qui manque, ce sont les preuves. Mais les preuves, ce sont effectivement les statistiques pouvant faire mention de l'évolution du nombre d'arrestations que j'espère suivies d'une chute considérable des arnaques qui pourraient venir rassurer les pays victimes. Il y aura toujours des arnaques, mais celles venant de Côte d'Ivoire doivent être combattues sans cesse pour finir par les rendre anecdotiques.

C.M : Hormis les arrestations, une forte sensibilisation de la jeunesse ivoirienne ne peut-elle pas également contribuer à réduire le nombre d'arnaques venant de la Côte d'Ivoire ?
D.J : D'après ce que j'ai compris, les adolescents ou les jeunes qui sont concernés sont des personnes qui, dans la société, sont déjà en marge des règles. Ils essaient de se débrouiller par leurs propres moyens sans passer par la case Travail, la case Honnêteté. C'est tout aussi grave que de se rapprocher de la drogue. Que fait le pays contre la drogue ? Ce qu'elle fait contre ce fléau, elle doit aussi le faire pour combattre la cybercriminalité. Comme dans d'autres régions du monde, s'attaquer à ce phénomène doit se faire en s'appuyant sur des entraides internationales.
« CE QUI MANQUE MAINTENANT CE SONT LES MOYENS POUR LES POUVOIRS PUBLICS DE MENER DES OPÉRATIONS COUP DE POING. GRÂCE À CELA, IL EST PROBABLE QUE LES JEUNES POUVANT ENCORE CHANGER DE VOIE, LE FERONT PAR PEUR.»
L'analyse des flux financiers au travers de réseaux et des trains de vie incohérents avec les revenus connus sont de bonnes pistes à suivre pour comprendre le phénomène de la cybercriminalité. Ce qui manque maintenant ce sont les moyens pour les pouvoirs publics de mener des opérations coup de poing. Grâce à cela, il est probable que les jeunes pouvant encore changer de voie, le feront par peur. Ensuite, pour ceux qui, influencés, n'auront pas envie de rentrer dans le droit chemin, je pense en effet qu'une une forte sensibilisation pourra évidemment contribuer à réduire le nombre d'arnaques venant de Côte d'Ivoire.

C.M : Parlant de moyens, n'est-il pas opportun de renforcer la coopération avec la France et des pays comme le Canada pour muscler les opérations terrain, ce d'autant plus que les populations de ces pays sont bien souvent ciblées par les arnaques venant de Côte d'Ivoire ?
D.J : Jusqu'à maintenant, la coopération n'y était pas. Elle était surtout en Europe. En dehors de l'Europe, c'était très difficile d'établir une coopération. Moi, il y a une question que je me pose : pourquoi d'ici ils vont essayer d'arnaquer la France ou le Canada ? Déjà parce qu'il n'y a pas de barrière au niveau de la langue. Puis, ce sont des pays qui ont des moyens. Qui sont prêts à payer pour rencontrer l'amour. On ne va pas essayer d'arnaquer un pays pauvre. Donc, on s'oriente vers ces pays-là.
Depuis maintenant quelques années, au-delà de l'évolution de la législation, la coopération internationale entre pays intérieurs et extérieurs de l'Europe s'est accentuée. Sans que ces pays n'aient forcément ratifié la Convention de Budapest, seul contrat officiel existant et contenant des protocoles d'entraides entre les autorités compétentes des différents pays impliqués, une entraide entre les organes judiciaires s'est naturellement créée. Aujourd'hui, l'entraide internationale est légion. C'est une forme de coopération qui n'a pas besoin de convention et qui, avec certains pays fonctionne très bien. En partie grâce à cela, la Côte d'Ivoire a commencé ces dernières années à s'attaquer au délinquants du numérique, réaliser des arrestations et amplifier ses actions…

C.M : Vous avez participé à l'IT Forum Côte d'Ivoire 2016 sur la sécurité des utilisateurs des services numériques. Partant de tout ce qui a été dit, comment entrevoyez-vous l'avenir de la Côte d'Ivoire dans 5 à 10 ans ?
D.J : La Côte d'Ivoire est en bonne voie pour sortir la tête de la cybercriminalité. Elle est en bonne voie parce que le combat commence obligatoirement par la sensibilisation des décideurs. Et ce forum a réuni des DSI, des directeurs de la sécurité numérique, des chefs d'entreprises, des officiels, donc des personnes qui décident de l'économie du pays. Si, nous formateurs, consultants, professionnels de la cybersécurité, on a bien fait notre travail pendant ces deux jours, il est clair que les visiteurs sont repartis d'ici avec de nouvelles armes. Maintenant, ceux qui auront été convaincus aujourd'hui ne seront pas forcément ceux qui seront les cibles de demain, des prochaines failles ou des prochaines attaques. Les prochaines victimes continueront à être les utilisateurs imprudents, ignorants et des proies potentielles qui n'ont pas pu être présentes à l'IT Forum. À force de sensibiliser les chefs d'entreprises, les DSI, et de faire en sorte que la sensibilisation à la cybersécurité et aux comportements prudents commence dès l'école, nous auront bientôt une nouvelle génération d'utilisateurs mieux formés et mieux armés.
Un autre phénomène qui tend à être inversé est celui de la faible importance accordée à la sécurité informatique. Quel que soit l'endroit dans le monde, la cybercriminalité est quelque chose d'inévitable et la sécurité informatique, en raison d'une course effrénée à la commercialisation à outrance, a trop longtemps été négligée par les constructeurs et les éditeurs de logiciels. Ils devront sans doute se conformer au concept « Security by design ».
Avant de miser sur sa R&D (Recherche et Développement) pour créer ou répondre à des besoins et commercialiser à tout prix pour rapidement la rentabiliser et ne chercher que les profits financiers, il deviendra bientôt obligatoire de penser sécurité avant de penser rentabilité. Avec l'évolution incoercible du numérique dans notre quotidien (objets connecté, santé connectée, vie connectée), il est indispensable que la sécurité des utilisateurs soit aussi le problème des inventeurs de nos vies numériques et pas seulement de ceux dont le métier est de réparer les bêtises des autres. La Côte d'Ivoire fait désormais partie des pays impliqués par ce combat et je n'ai aucun doute, ce pays se dirige droit vers une explosion de l'usage du numérique et une amélioration de sa lutte contre la cybercriminalité.

C.M : Au niveau international, quelle est la nouvelle tendance en matière de cybercriminalité?
D.J : Au Forum international de la cybercriminalité (FIC 2016), j'ai assisté à une présentation faite par un chercher en cybersécurité autour de l'étude de l'évolution d'un RAT (Remote Access Tool). Des virus utilisant des failles existent déjà mais la présentation portait sur une nouvelle forme de logiciel malveillant encore plus perfectionné en matière d'impacts et de conséquences sur les postes informatiques des victimes. On connaissait des failles en Flash, en Visual Basic et dans d'autres types de langages mais la faille en Java est une faille qui aujourd'hui peut toucher tous les ordinateurs puisqu'énormément de systèmes et de web services sont conçus autour du langage Java.
J'ai trouvé la présentation très intéressante et j'ai trouvé l'effet dévastateur pour tous ceux qui attraperont ce « Méchangiciel ». A la fin de la présentation, j'ai approché l'intervenant et lui ai demandé quel était le moyen de propagation utilisé par ce virus ingénieux du futur ? Il m'a répondu qu'il se propage tout simplement par pièce jointe dans un e-mail. Ça reste aujourd'hui le principal vecteur de propagation de systèmes malveillants. Surtout, si c'est bien monté avec ce qu'on appelle des techniques d'ingénierie sociale, c'est-à-dire des actes qui permettent de manipuler la personne destinataire du piège, par exemple un CV piégé transmis à une agence d'emploi, rien de plus normal, même s'il est piégé ! C'est pourquoi l'autre vecteur sur lequel j'insiste, c'est le vecteur humain, la sensibilisation des utilisateurs afin d'augmenter le taux de prudence qu'ils doivent avoir lorsqu'ils reçoivent un email. Un email piégé a des caractéristiques que l'on peut assez facilement identifier et qui permettent de dire qu'il y a un risque, et mettre une procédure en cas de doute. Pour moi, même s'il existe des lunettes 3D, des hologrammes, des choses complétement folles au niveau technologique, j'ai l'impression que la propagation de la cybercriminalité va pouvoir se faire encore pendant pas mal de temps dans de vulgaires pièces jointes, et probablement encore dans les arnaques et le phishing.
Une fois que le pirate aura obtenu les clefs il pourra mener son attaque par « Menace Persistante Avancée (Advanced Persistent Threat) », autre grande tendance déjà depuis quelques années et encore pour longtemps !
Article original et propos recueillis par Anselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité : « Il faut qu’on voie que la Côte d’Ivoire réagit » | CIO MAG

Vidéo sur l’étude du marché de la cybersécurité par Xerfi

	**Vidéo sur l’étude du marché de la cybersécurité par Xerfi**

La cybersécurité est l'un des marchés les plus dynamiques de l'IT, d'après l'étude de Xerfi sur le sujet. Il faut dire que les soutiens à l'activité sont nombreux entre la recrudescence des menaces informatiques, la mise en place de nouvelles réglementations plus contraignantes et les nouvelles vulnérabilités liées aux évolutions des techniques et des pratiques […]

Article original de Alexandre Boulègue

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 : Alexandre Boulègue, Xerfi – Le marché de la cybersécurité – Secteurs & marchés – xerficanal-economie.com

---

Bulletin sécurité du 13 juin 2016 du CERTFR

Bulletin sécurité du 13 juin 2016 du CERTFR

La S . G . D . S . N (Agence nationale de la sécurité des systèmes d'information) met régulièrement à notre disposition ses avis et alertes sur de nouvelles vulnérabilités détectées.
Voici le dernier bulletin d'actualité : CERTFR-2016-ACT-024

1 – Sonde de détection d'intrusions réseau – Comment implémenter les points de mesure ?

Une sonde de détection d'intrusions réseau est un équipement passif, elle ne s'insère donc pas en coupure sur un flux de production. Il est donc nécessaire, pour implémenter les points de mesure définis, d'assurer une duplication en temps réel de l'activité réseau à analyser.
Deux techniques différentes existent pour dupliquer un trafic réseau : la première, généralement appelée « port miroir », est logicielle, et s'appuie sur les équipements réseau déjà en place ; la seconde, généralement appelée « tap », s'appuie sur des boîtiers matériels dédiés à cette fonction. Nous allons voir les avantages et les inconvénients de ces deux solutions.

Port miroir

La majorité des commutateurs du marché permettent de configurer une recopie logicielle de tout ou partie du trafic sur un ou plusieurs ports physiques dédiés. Le port miroir peut être un choix peu coûteux, si les équipements existants d'un réseau disposent déjà de cette fonctionnalité.
Toutefois, la recopie logicielle du trafic n'est pas sans risque. En effet, si l'équipement atteint sa limite de capacité sur ses fonctions « principales » (comme par exemple : la commutation de paquets, le routage, etc.), des fonctions annexes comme la recopie de paquets peuvent être dégradées, entraînant dans un tel cas des pertes sur l'activité à superviser.
La recopie logicielle peut également altérer le signal, car les couches basses réseau sont analysées et traitées par les commutateurs. Cette technique ne garantit donc pas la recopie de l'intégralité du trafic commuté sur le réseau de production. Étant donné qu'un seul paquet perdu sur un flux volumineux peut empêcher l'analyse par la sonde ou l'évader, il est primordial de considérer ce problème et de superviser la charge des commutateurs, si cette technique est mise en place.
La mise en place d'un port miroir sur un équipement du réseau augmente aussi la consommation de ressources : cela peut donc également dégrader le réseau de production. Une attention particulière doit être apportée au fond de panier, car le débit total commuté par l'équipement est décuplé.
D'autre part, il est important d'intégrer les ports miroirs dans les procédures d'exploitation : lors du remplacement d'un équipement ou d'un changement de configuration, il faut s'assurer que la recopie est toujours opérationnelle et qu'il n'y a pas de perte d'une partie des flux.
Une erreur de configuration peut également autoriser des communications depuis le réseau de duplication, voire même entre la sonde et le réseau de production.
Par contre, la mise en oeuvre d'un port miroir peut se faire sans interruption du réseau en production à superviser, à condition de disposer de suffisamment de ports physiques libres au niveau des commutateurs où les points de mesure sont effectués.

TAP

Un TAP garantit la recopie stricte du signal reçu : aucune analyse des couches au-delà de celle physique n'est réalisée. Le signal est régénéré électriquement pour des TAP cuivre, et la lumière est divisée sur deux chemins pour les TAP fibre. La mise en oeuvre d'une duplication de trafic sur un réseau en production nécessite une brève interruption du lien à superviser : celle-ci correspond au temps nécessaire pour placer le boîtier TAP en « coupure », c'est-à-dire sur le chemin de câble.
Pour les TAP alimentés, un défaut d'alimentation arrête la duplication, mais le TAP reste passant pour le lien coupé, moyennant généralement une microcoupure de quelques millisecondes.
Pour les TAP fibre, une partie de la lumière incidente étant réfléchie et l'autre réfractée, le signal est affaibli en fonction de proportions précisées dans la documentation du TAP.
Contrairement au port miroir, le TAP garantit également l'isolation entre le réseau de production et le réseau de détection.
Le prix d'un boîtier de duplication de trafic (TAP) varie entre une centaine d'euros et un millier, en fonction du type de média à dupliquer.

Conclusion

En conclusion, bien que ces deux méthodes permettent la duplication du trafic, il est conseillé de privilégier l'utilisation d'équipement dédié afin de garantir la séparation entre le réseau de production et le réseau de détection, ainsi qu'une recopie à l'identique des flux réseau.

2 – Rappel des avis émis

Dans la période du 06 au 12 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-190 : Vulnérabilité dans VLC Media Player
- CERTFR-2016-AVI-191 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-192 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-193 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-194 : Multiples vulnérabilités dans les produits Symantec
- CERTFR-2016-AVI-195 : Multiples vulnérabilités dans PHP
- CERTFR-2016-AVI-196 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2016-AVI-197 : Vulnérabilité dans Citrix Xenserver
- CERTFR-2016-AVI-198 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-199 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

---

Réagissez à cet article

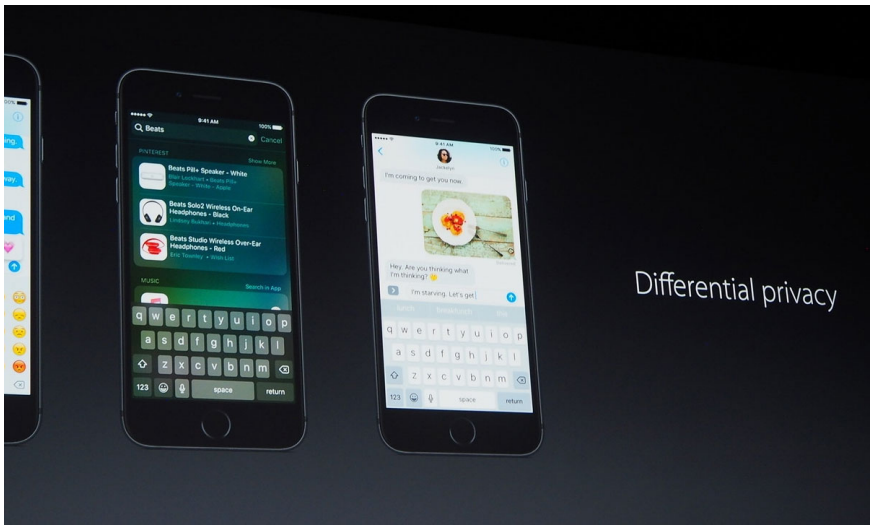
Original de l’article mis en page : Bulletin d’actualité CERTFR-2016-ACT-024

Finalement Apple collectera des données personnelles, avec votre accord

Finalement Apple collectera des données personnelles, avec votre accord

---

Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.



Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.
Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.
Cependant les nouvelles fonctionnalités de suggestion et d'identification d'iOS 10 ne peuvent se prétendre pertinentes sans avoir accès à un minimum de données !
Les techniques de « differential privacy » mises en oeuvre pour iOS 10 ne permettront pas une identification de l'utilisateur qui fournit ses données mais Apple, selon Recode, vous- demandera votre accord avant d'attaquer toute collecte d'information.
Dans un premier temps, le type de données collectées sera limité à quatre domaines :
– les nouveaux mots ajoutés au dictionnaire personnel d'iOS,
– les émoticônes utilisées,
– les liens profonds marqués comme public dans les applications,
– les suggestions de recherche dans les notes.
Pour ne pas rater le train de l'intelligence artificielle, Cupertino ne pouvait pas rester à l'écart d'une forme de collecte et d'exploitation de données. Cependant, ne souhaitant pas en faire directement commerce ni renier ses grands principes, Apple se doit de naviguer entre deux eaux et d'innover dans ce domaine.
On est encore loin de la façon de procéder de compagnies comme Google et Facebook !
Article original de bpepermans

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 : Finalement Apple collectera des données personnelles, avec votre accord | Slice42