Sensibilisation au Phishing

Sensibilisation au Phishing

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

Campagne Paypal France 2016

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

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

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

Contactez-nous

Réagissez à cet article

Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

Les dirigeants sont premiers responsables cas cyberattaques subies entreprise

Près d'un tiers (29 %) des responsables informatiques et près d'un cinquième (21 %) des employés en France considèrent donc que leur dirigeant devrait être tenu responsable en cas d'importante fuite de données. Pourtant, un quart (25%) des responsables informatiques admet ne pas informer son dirigeant en cas d'incident de ce type. Ce manque de transparence prive donc les dirigeants, considérés comme principaux responsables, d'une visibilité réelle sur les risques que représentent les fuites de données pour leur entreprise.

L'ampleur de ce constat est encore plus frappante dans une autre enquête menée par l'Economist Intelligence Unit pour le compte de VMware en début d'année. Celle-ci révélait en effet que seuls 8 % des dirigeants d'entreprises dans la région EMEA (11% en France) considéraient la cybersécurité comme une priorité. Alors que les cyberattaques s'intensifient et deviennent de plus en plus préjudiciables pour les entreprises – avec à la clé le risque de perte de propriété intellectuelle, de positionnement concurrentiel, et de données clients – l'impact sur la performance et l'image de marque peut être considérable.

Une nouvelle approche de la sécurité s'impose

Les entreprises sont de plus en plus menacées par de graves cyberattaques : plus d'un tiers (37 %) des répondants dans la région EMEA (seulement 28 % en France) s'attendent à en être victimes dans les 3 prochains mois. Malheureusement, les approches de sécurité actuelles ne sont pas adaptées à un monde toujours plus tourné vers les technologies numériques. Ainsi, plus d'un responsable informatique français sur trois (35 %) estime que l'un des principaux risques pour son organisation réside dans le fait que les menaces évoluent plus vite que les systèmes de défense mis en place.

« Le fossé entre dirigeants et responsables informatiques est symptomatique. Il symbolise le défi que doivent relever les entreprises cherchant à repousser leurs limites, à se transformer, à se différencier et à se protéger de menaces en constante évolution », déclare Sylvain Cazard, directeur général de VMware France. *« Aujourd'hui, les organisations les plus performantes sont celles qui sont capables de réagir rapidement et de préserver aussi bien leur image de marque que la confiance de leurs clients. Les applications et données des utilisateurs étant présentes sur un nombre d'appareils sans précédent, ces entreprises ont abandonné les approches traditionnelles de sécurité informatique incapables de protéger les entreprises numériques d'aujourd'hui. »*

Les employés et les processus aussi problématiques que les technologies

L'un des principaux risques pour la sécurité d'une entreprise provient de l'intérieur. Ainsi, pour 45 % des responsables informatiques de la région EMEA (et 37 % en France), la négligence ou le manque de formation des employés en matière de cybersécurité représente le principal défi pour leur entreprise. L'enquête montre également jusqu'où les salariés sont prêts à aller pour accroître leur productivité : 15 % d'entre eux (contre 21% au niveau EMEA) utilisent leurs appareils personnels pour accéder à des données professionnelles, tandis que 14 % (17% en EMEA) sont prêts à enfreindre la politique de sécurité de leur entreprise afin de travailler plus efficacement.

« La sécurité n'est pas qu'une question de technologie. Comme le montrent les résultats de notre enquête, les décisions et les comportements des employés ont également un impact sur l'intégrité d'une entreprise » remarque Sylvain Cazard. *« Malgré tout, la solution n'est pas non plus de tout verrouiller et d'instaurer une culture de la peur. Les organisations qui adoptent des approches intelligentes proposent plus de moyens et non de restrictions à leurs employés, leur permettant de s'épanouir, d'adapter les process et de transformer leur activité pour réussir.»*

« Les entreprises tournées vers l'avenir sont conscientes du fait que les stratégies de sécurité réactives d'aujourd'hui ne sont plus efficaces pour protéger leurs applications et données. Adopter une approche software-defined garantissant l'omniprésence de la sécurité leur offre la flexibilité nécessaire pour réussir en tant qu'entreprises numériques », conclut Sylvain Cazard.

Réagissez à cet article

Original de l’article mis en page : Les dirigeants sont les premiers responsables en cas de cyberattaques subies par leur entreprise

---

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

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

---

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

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

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

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

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

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

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

Réagissez à cet article

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

---

Code de la communication – La loi contre la

cybercriminalité à réviser

	Code de la communication – La loi contre la cybercriminalité à révise

Les internautes et les utilisateurs des réseaux sociaux espèrent que le projet de code de la communication a abrogé l'article 20 de la loi sur la lutte contre la cybercriminalité. Le gouvernement tiendra-t-il une promesse faite en 2014 ?

Le gouvernement tiendra-t-il les promesses faites par ses anciens membres ? La révision, voire l'abrogation de l'article 20 de la loi sur la lutte contre la cybercriminalité, fait partie des dispositions les plus attendues du projet de code de la communication. Adopté jeudi en conseil des ministres, et attendu incessamment devant les bureaux du Parlement, le projet reste, pour l'instant, inaccessible. Le sort de l'article 20 de la loi contre la cybercriminalité qui avait été abrogé dans l'avant-projet de texte soumis au gouvernement demeure encore inconnu.

Le président de la République ayant déjà affiché sa volonté de supprimer les peines de prison pour sanctionner certains délits de presse comme les injures ou la diffamation, on voit mal comment le Conseil des ministres aurait pu enlever du projet la disposition finale qui a indiqué, entre autres, l'abrogation du fameux article 20. Sanctionnant de peine de prison pouvant aller jusqu'à cinq ans, et d'amende pouvant s'élever jusqu'à 100 millions d'Ariary, toute personne coupable d'injures, de diffamation ou d'atteinte à la dignité d'une personne, par le biais de tout type de support, écrit, audio-visuel ou électronique, le fameux article 20 a soulevé un tollé aussi bien dans le milieu de la presse que parmi les utilisateurs des réseaux sociaux.

La ministre de la Justice et celui de la Communication de l'époque, pour calmer les esprits, avaient alors promis que des ajustements pourraient être apportés au texte s'il devait se trouver en contradiction avec le code de la Communication qui était alors en cours d'élaboration.

Or, en instituant les peines de prison et les amendes exorbitantes pour toute diffamation ou injure faite par voie électronique, la loi, sur la lutte contre la cybercriminalité est entrée en contradiction avec l'esprit qui avait guidé l'élaboration du Code de la communication.

Risque de maintien

De l'eau a, pourtant, coulé sous le pont depuis la validation du texte par le monde médiatique. Vu les relations de la présidence avec les internautes, notamment les utilisateurs du réseau social Facebook, il n'est pas impossible que les autorités aient préféré laisser tel quel l'article 20 de la loi sur la lutte contre la cybercriminalité. L'objectif étant que, comme l'aiment le dire les responsables de la communication des autorités, « limiter le confort de l'internaute qui se trouve devant son clavier et qui se croit intouchable ».

Certaines sources laissent par ailleurs entendre que durant ce long intervalle de temps entre la validation de l'avant-projet et son adoption en conseil des ministres, l'Exécutif a trouvé le temps de réintégrer les dispositions qui avaient été jugées liberticides par les professionnels des médias, et de retirer les articles plus « libéraux », tel que celui qui a abrogé l'article 20 de la loi contre la cybercriminalité. Il semblerait même que le texte, dans une de ses versions manipulées par le Gouvernement, fasse référence à cet article 20 en indiquant que certaines peines seront appliquées sans préjudice de celles prévues par la loi sur la lutte contre la cybercriminalité.

Attendue depuis sa promulgation en 2014, la révision de la loi sur la lutte contre la cybercriminalité, notamment en ce qui concerne l'abrogation de son article 20, pourrait finalement être une réalité maintenant que le code de la communication est en passe d'être adopté. Tout comme la fameuse loi peut encore rester telle une épée de Damoclès suspendue au-dessus de la tête des professionnels des médias, mais aussi des internautes et des utilisateurs des réseaux sociaux.

Réagissez à cet article

Original de l’article mis en page : Code de la communication – La loi contre la cybercriminalité à réviser | LExpress de Madagascar – Actualités en direct sur Madagascar

---

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

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

---

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

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

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

Voici la procédure en vidéo :

Article original de Guillaume Belfiore

Réagissez à cet article

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

---

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Adepte du malware Lurk, un réseau de cybercrimels vient dêtre démantelé en Russie. Il est responsable du vol de plus de 22 millions deuros à des banques.

Une cinquantaine d'interpellations en Russie ont abouti au démantèlement d'un réseau de cybercriminels surnommé Lurk. Un nom qui découle de l'emploi d'un cheval de Troie identifié en 2012.
À l'époque, Kaspersky Lab avait évoqué le cas de Lurk dans des attaques drive-by. Conçu pour voler des données sensibles d'utilisateurs afin d'obtenir un accès à des services de banques en ligne russes, le malware n'était pas téléchargé sur le disque dur et opérait uniquement dans la mémoire RAM.
Threatpost (Kaspersky Lab) écrit que Lurk a commencé à attaquer des banques il y a un an et demi, et a rapatrié divers malwares de serveurs de commande et contrôle. Les attaquants ont utilisé un VPN compromis afin de rendre leur campagne plus difficile à détecter.
Grâce à Lurk, les cybercriminels ont dérobé plus de 1,7 milliard de roubles (près de 22 millions d'euros) à des comptes d'institutions financiers russes, a indiqué le FSB (l'ancien KGB) à l'agence de presse russe TASS.
Article original de Jérôme GARAY

Réagissez à cet article

Original de l’article mis en page : Piratage de banques : un gang russe démantelé

Skimer, la nouvelle menace pour distributeurs de billets

Skimer, la nouvelle menace pour distributeurs de billets

Skimer, un groupe russophone, force les distributeurs automatiques de billets (DAB) à l'aider à dérober de l'argent. Découvert en 2009, Skimer a été le premier programme malicieux à prendre pour cible les DAB. Sept ans plus tard, les cybercriminels ré-utilisent ce malware. Mais le programme, ainsi que les escrocs, ont évolué ; ils représentent une menace encore plus importante pour les banques et leurs clients partout dans le monde.

Imaginons qu'une banque découvre avoir été victime d'une attaque. Étrangement, aucune somme d'argent n'a été dérobée et rien n'a été modifié dans son système. Les criminels sont partis comme ils sont venus. Serait-ce possible ? Je vous parlais de ce type d'attaque l'année dernière. L'éditeur Gdata m'avait invité en Allemagne pour découvrir l'outil malveillant qui permettait de pirater un distributeur de billets. Aujourd'hui, l'équipe d'experts de Kaspersky Lab a mis au jour le scenario imaginé par les cybercriminels et découvert des traces d'une version améliorée du malware Skimer sur l'un des DAB d'une banque. Il avait été posé là et n'avait pas été activé jusqu'à ce que les criminels lui envoient un contrôle : une façon ingénieuse de couvrir leurs traces.
Le groupe Skimer commence ses opérations en accédant au système du DAB, soit physiquement, soit via le réseau interne de la banque visée. Ensuite, après été installé avec succès dans le système, l'outil Backdoor.Win32.Skimer, infecte le cœur de l'ATM, c'est-à-dire le fichier exécutable en charge des interactions entre la machine et l'infrastructure de la banque, de la gestion des espèces et des cartes bancaires.
Ainsi, les criminels contrôlent complètement les DAB infectés. Mais ils restent prudents et leurs actions témoignent d'une grande habileté. Au lieu d'installer un skimmer (un lecteur de carte frauduleux qui se superpose à celui du DAB) pour siphonner les données des cartes, les criminels transforment le DAB lui-même en skimmer. En infectant les DAB avec Backdoor.Win32.Skimer, ils peuvent retirer tout l'argent disponible dans le distributeur ou récupérer les données des cartes des utilisateurs qui viennent retirer de l'argent, y compris le numéro de compte et le code de carte bancaire des clients de la banque.
Il est impossible pour un individu lambda d'identifier un DAB infecté car aucun signe de le distingue d'un système sain, contrairement à un DAB sur lequel a été posé un skimmer traditionnel qui peut être repéré par un utilisateur averti.

Un zombie dormant
Les retraits directs depuis un DAB ne peuvent pas passer inaperçu alors qu'un malware peut tranquillement siphonner des données pendant une longue période. C'est pourquoi le groupe Skimer n'agit pas immédiatement et couvre ses traces avec beaucoup de prudence. Leur malware peut opérer pendant plusieurs mois sans entreprendre la moindre action.
Pour le réveiller, les criminels doivent insérer une carte spécifique, qui contient certaines entrées sur sa bande magnétique. Après lecture de ces entrées, Skimer peut exécuter la commande codée en dur ou requérir des commandes via le menu spécial activé par la carte. L'interface graphique de Skimer n'apparaît sur l'écran qu'une fois la carte éjectée et si les criminels ont composé la bonne clé de session, de la bonne façon, sur le pavé numérique en moins de 60 secondes.
À l'aide du menu, les criminels peuvent activer 21 commandes différentes, comme distribuer de l'argent (40 billets d'une cassette spécifique), collecter les données des cartes insérées, activer l'auto-suppression, effectuer une mise à jour (depuis le code du malware mis à jour embarqué sur la puce de la carte), etc. D'autre part, lors de la collecte des données de cartes bancaires, Skimer peut sauvegarder les fichiers dumps et les codes PIN sur la puce de la même carte, ou il peut imprimer les données de cartes collectées sur des tickets générés par le DAB.
Dans la plupart des cas, les criminels choisissent d'attendre pour collecter les données volées afin de créer des copies de ces cartes ultérieurement. Ils utilisent ces copies dans des DAB non infectés pour retirer de l'argent sur les comptes clients sans être inquiétés. De cette manière, ils s'assurent que les DAB infectés ne seront pas découverts. Et ils récupèrent de l'argent simplement.

Des voleurs expérimentés
Skimer a été largement répandu entre 2010 et 2013. À son arrivée correspond une augmentation drastique du nombre d'attaques sur des distributeurs automatiques de billets, avec jusqu'à neuf différentes familles de malwares identifiées par Kaspersky Lab. Cela inclut la famille Tyupkin, découverte en mars 2014, qui est devenue la plus populaire et la plus répandue. Cependant, il semblerait maintenant que Backdoor.Win32.Skimer soit de retour. Kaspersky Lab identifie 49 modifications de ce malware, dont 37 ciblent les DAB émanant de l'un des plus importants fabricants. La version la plus récente a été découverte en mai 2016.
En observant les échantillons partagés avec VirusTotal, on note que les DAB infectés sont répartis sur une large zone géographique. Les 20 derniers échantillons de la famille Skimer ont été téléchargés depuis plus de 10 régions à travers le monde : Émirats Arabes Unis, France, États-Unis, Russie, Macao, Chine, Philippines, Espagne, Allemagne, Géorgie, Pologne, Brésil, République Tchèque… [Lire la suite]
Remarquable 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 : *Skimer, la nouvelle menace pour distributeurs de billets – Data Security BreachData Security Breach*

Un caïd du ransomware gagne 90 000 dollars par an

Un caïd du ransomware gagne 90 000 dollars par an

Spécialiste du Dark web, Flashpoint a étudié les dessous d'une campagne russe de « ransomware-as-a-service » (RaaS). Son pilote aurait gagné 7 500 dollars par mois en moyenne.

Fournisseur d'analyses des Deep et Dark web, Flashpoint a étudié les dessous d'une campagne de « ransomware-as-a-service » (RaaS) pilotée, selon lui, par des escrocs russes. Le RaaS consiste pour l'auteur du rançongiciel à proposer à d'autres de diffuser des versions personnalisées de son programme pour chiffrer les données et verrouiller les terminaux d'utilisateurs. Les cibles sont appelées à payer en cryptomonnaie pour reprendre le contrôle de leurs données. La rançon est perçue par l'auteur du ransomware qui la partagera ensuite avec les diffuseurs.
C'est ainsi qu'une pointure des ransomwares en Russie aurait mené la campagne RaaS étudiée ces cinq derniers mois par Flashpoint. L'auteur de la campagne, qui ciblait des entreprises occidentales et des particuliers depuis au moins 2012, selon Flashpoint, aurait recruté des diffuseurs du programme ayant pour mission de trouver et infecter des cibles en échange d'un pourcentage sur les profits générés. Les novices étaient également invités à se lancer, sans frais d'entrée, le programme malveillant à diffuser étant accompagné d'instructions détaillées qu'un « écolier » pourrait suivre.

L'appât du gain

Le « patron » russe aurait ainsi recruté 10 à 15 « affiliés » chargés de diffuser le code de son ransomware. Soit en achetant un accès à des ordinateurs infectés, soit en passant par des serveurs insécurisés, ou du spam, ou encore en leurrant des utilisateurs de sites de rencontre et réseaux sociaux. Une fois que le code est installé et s'exécute, son auteur se charge des communications avec les victimes pour obtenir une rançon d'un montant moyen de 300 dollars par clé de déchiffrement et par victime, mais une somme additionnelle peut être exigée avant l'envoi de la clé.
Pour le paiement, la cryptomonnaie Bitcoin a été utilisée. 40 % des fonds ainsi détournés auraient été partagés entre les affiliés et 60 % seraient revenus au pilote de la campagne. Le « boss du ransomware » aurait ainsi empoché 7 500 dollars par mois en moyenne (90 000 dollars par an) et ses affiliés près de 600 dollars par mois chacun. Cela représente près de 30 paiements de rançon par mois.
« Nos résultats contestent la perception commune de cybercriminels hors du commun, éclairés, aisés, inaccessibles, inexposables et inarrêtables », soulignent les auteurs de l'étude. Et « Les montants des revenus du ransomware ne sont pas aussi séduisants et juteux » que l'on pourrait le croire. Il n'empêche, ces montants sont bien supérieurs au salaire moyen russe passé, selon une analyse de la Sberbank citée par RFI, de 1058 dollars par mois en 2012 à 433 dollars par mois en 2016.

crédit photo © frank_peters / Shutterstock.com
Article original de Ariane Beky

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 : Un caïd du ransomware gagne 90 000 dollars par an

---

Sensibilisation aux Arnaques

à la Loterie

Sensibilisation aux Arnaques à la Loterie

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

Campagne Paypal France 2016

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

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

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

Contactez-nous

Réagissez à cet article

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

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

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

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

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

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

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

Contactez-nous

Réagissez à cet article

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