Les six choses à faire pour éviter 95% des attaques informatiques

Les six choses à faire pour éviter 95% des attaques informatiques

La cybersécurité est essentielle, d'accord, mais par où commencer ? Pour vous aider à faire le premier pas, nous avons identifier 6 principes clés qui, lorsqu'ils sont suivis, peuvent éviter la grande majorité des attaques.

1/ FAIRE DE LA SÉCURITÉ UN PROCESS (CE N'EST PAS UN PRODUIT)

« Je dois protéger mon entreprise ? Certes. Quel produit faut-il que j'achète ? » La réflexion peut sembler naturelle. Après tout, autant faire appel à des professionnels. Le problème, c'est qu'on ne sécurise pas son entreprise en signant un chèque. La cybersécurité est avant tout une façon de penser, et passe par une organisation, par la mise en place de règles et méthodes. Elle implique de connaître son système d'information sur le bout des doigts pour en cartographier la surface d'attaque, de savoir tout ce qui est connecté (et ce qui ne doit pas l'être). Elle implique aussi de déterminer quels sont les services et les données qui sont réellement cruciaux au fonctionnement de la structure pour s'assurer que l'on concentre ses forces là où elles doivent l'être, sans s'évertuer à défendre plus que nécessaire des ressources non critiques. *« La sécurité est une composante au service du coeur de métier,* explique Eric Filiol, directeur du laboratoire de virologie et de #cryptologie opérationnelles de l'école d'ingénieurs ESIEA. *Il faut comprendre son métier et ce qui est critique. »* La stratégie doit être sensée pour que les ressources engagées (financières, humaines, temporelles) soient utilisées au mieux.

2/ PATCHER, PATCHER, PATCHER

Les révélations sur les méthodes de la NSA ou les gros titres sur les attaques contre des opérateurs d'importance vitale qui s'étalent sur des mois voire des années peuvent laisser penser que les hackers exploitent systématiquement des failles complexes et jamais référencées (appelées « zero days ») pour s'infiltrer dans un SI. Rien n'est moins vrai. Ces zero days ne sont utilisés qu'extrêmement rarement et seulement pour les cibles les plus importantes. La très grande majorité des attaques ciblent au contraire des failles bien connues et pour lesquelles existent déjà des correctifs de sécurité, souvent depuis des années. C'est pourquoi il est capital de faire systématiquement ces mises à jour (aussi bien pour le système d'exploitation que les frameworks ou les applications), et de concevoir son SI autour de cette nécessité. *« Il faut savoir que les criminels font du reserve engineering sur les patchs dès leur sortie pour exploiter les failles qu'ils corrigent. Auparavant cela leur prenait des mois, aujourd'hui ce ne sont plus que des heures,* détaille Thomas Tschersich, director of IT security chez Deutsche Telekom.*Et ils automatisent ensuite le processus pour toucher de très nombreuses cibles. »* Et ce besoin reste le même dans le cas d'un environnement de production industriel qui se doit d'être opérationnel 365 jours par an. La perception selon laquelle les environnements industriels sont fondamentalement différents des environnements de bureau est fausse et contribue à renforcer leur vulnérabilité.

3/ NE PAS SE CROIRE NON CONCERNÉ

Si les réseaux industriels sont de plus en plus visés par des attaques informatiques, c'est parce qu'ils y sont particulièrement vulnérables. La faute à l'évolution dramatique de la connectivité à Internet au cours des 20 dernières années. Lors de leur conception, il était assumé que ces systèmes ne couraient pas de risques car ils n'étaient pas visibles. Quand bien même ce fut jamais vrai, ce n'est définitivement plus le cas. Des services gratuits comme shodan.io permettent depuis des années de chercher parmi des centaines de milliers de systèmes ouverts, connectés à Internet sans aucune protection. Cela va de simples caméras de surveillance (résidentielles ou industrielles) jusqu'aux ICS qui supervisent le parc machine, que les opérateurs laissent sans protection car ils veulent pouvoir en prendre facilement le contrôle à distance. *« Il y a beaucoup de négligence et de mauvaises pratiques,* assène Frédéric Planchon, PDG de FPC Ingénierie. *Cela laisse des portes ouvertes à des malwares qui ne sont normalement pas si nocifs. »* Peu importe la taille de votre installation ou la nature de votre activité, si vous êtes vulnérables, vous serez tôt ou tard attaqué. Et ce même lorsqu'il n'y a rien à en obtenir, car de nombreux hackers agissent simplement « pour le sport ».

4/ PROTÉGER SES DONNÉES

La meilleure façon de garantir la sécurité de ses données, que ce soit contre le vol ou contre des attaques de type ransomwares, c'est de prendre les mesures adéquates en amont. Cela passe par deux axes clés : le chiffrement et la sauvegarde. Le chiffrement garantit que seuls les individus autorisés peuvent accéder aux données, même si le canal de communication ou le support de stockage est compromis. Ainsi, même en cas de vol, les dégâts restent minimaux. De son côté, la sauvegarde évite la perte de données, qu'elle soit dûe à un accident ou à un acte de malveillance. Une politique de sauvegarde rigoureuse et régulière peut faire la différence entre « plus de peur que de mal » et « la clé sous la porte ».

5/ FORMER SES TROUPES

Une vaste majorité d'attaques ont un point commun : l'erreur humaine. Un collaborateur qui ouvre le mauvais email ou clique sur le mauvais lien. Un autre qui perd son appareil ou sa clé USB. Un troisième qui laisse traîner ses identifiants de connexion (ex. post-it sur l'écran) ou les communique par erreur/inattention… La sécurité n'est pas innée, elle s'enseigne. Il est impératif de former les équipes aux bonnes pratiques à adopter et de les sensibiliser aux conséquences que la négligence peut avoir. Les rendre personnellement responsables de la protection de leurs données et appareils au travers de mesures simples peut suffire à largement diminuer les accidents.

6/ SÉCURISER AUSSI LES ACCÈS PHYSIQUES

Une #attaque informatique n'est pas forcément menée depuis l'autre bout du monde. Il faut donc s'assurer en premier lieu que le périmètre de l'entreprise est sécurisé pour limiter les accès non autorisés en interne. Car le « social engineering », qui consiste à obtenir accès à un système en trompant son interlocuteur, est au coeur de nombreuses attaques. Il suffit parfois de mettre un uniforme de réparateur, de prendre une boîte à outils et de demander poliment l'accès à un local technique pour qu'on vous ouvre. Ou de mettre un costume et de se tenir devant une porte les bras chargés de documents. *« Nous appelons ça les attaques 'femme de ménage', et cela permet de prendre le contrôle d'un serveur en 5 secondes, »* explique Eric Filiol. Autre exemple, lorsque le réseau Wi-Fi interne d'une usine, non protégé car l'accès au bâtiment est restreint, peut aussi être capté depuis le parking… Les cas de figure sont nombreux et leur exploitation bien documentée. Ces éléments doivent donc systématiquement être pris en compte.

Article de Julien BERGOUNHOUX

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 : *Cybersécurité : Les six choses à faire pour éviter 95% des attaques*

La France adopte son arsenal anti-hackers

La France adopte son arsenal anti-hackers

La loi de programmation militaire a placé le secteur financier en première ligne des 12 opérateurs d'importance vitale, soumis à de nouvelles règles de sécurité.

C'est un test d'envergure pour les banques françaises. L'Etat a placé le secteur financier en première ligne des douze secteurs d'importance vitale qui devront adopter les nouvelles règles en matière de cybersécurité, arrêtées par la loi de programmation militaire de 2013.
Ce choix n'est pas dû à une recrudescence des cyber-risque dans le secteur, assure la puissance publique – en l'occurrence, c'est Bercy qui a fait l'objet de l'attaque la plus grave ayant jamais visé une administration en France en 2011. *« Le niveau de sécurité du secteur financier est jugé satisfaisant,* indique Yves Jussot, coordinateur sectoriel à l'Agence nationale de la sécurité des systèmes d'information (Anssi). *Cependant la menace évolue vite et de façon continue, en particulier avec le développement du numérique. »*
Considérées comme *« pionnières »* dans l'identification des menaces informatiques et de lutte contre les cyberfraudes, les banques fixeront la barre des nouvelles exigences en matière de protection, qui s'appliqueront aux autres secteurs vitaux comme l'énergie, aux transports, en passant par la santé. Définies par un arrêté d'ici au 1er juillet, celles-ci promettent d'être élevées. Des règles renforcées en matière d'administration des systèmes sont par exemple définies pour cantonner davantage les flux de données.
Surtout, l'Etat voit son pouvoir renforcé en matière de contrôle. L'Anssi, rattachée au secrétaire général de la Défense et de la sécurité nationale, pourra mener des audits réguliers, et des amendes pourront être délivrées pour infraction à la sécurité informatique ou non-application de la réglementation. Les incidents qui pouvaient jusqu'à présent ne pas être déclarés devront être notifiés et, en cas d'attaque majeure, l'Anssi pourra prendre la main sur les systèmes. L'Etat a pris soin de travailler de concert avec les banques, au travers du Forum des compétences, qui regroupe les experts informatiques des banques et des assurances. Restera la question des moyens. *« La course à la transformation digitale entre banques impose d'aller vite et d'y allouer des moyens. La mise à niveau des systèmes informatiques peut ne pas suivre et ne pas être prioritaire »*, note un expert en cybersécurité…[Suite de l'article original de Anne RIF et Véronique CHOCRON]

Réagissez à cet article

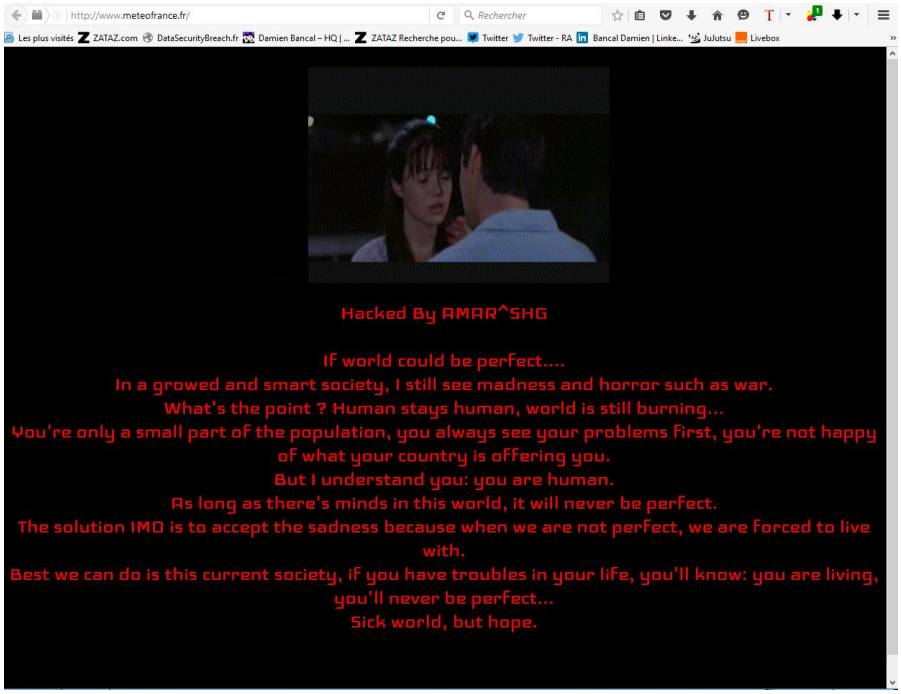
Source : *La France adopte son arsenal anti-hackers, Banque – Assurances*

Le site Internet de Météo

France piraté

	**Le site Internet de Météo France piraté**

Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.



Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

Détournement de DNS

*Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « **se plaignent pour leurs propres problèmes** ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « **Il faut vivre avec, avec espoir** »… [Lire la suite]*

Article de Damien BANCAL

Réagissez à cet article

Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

Google Chrome v51 corrige 42 failles de sécurité

Google Chrome v51 corrige 42 failles de sécurité

Google vient de publier une nouvelle mouture stable de son navigateur Chrome, en version 51.

Chrome 51 est disponible au téléchargement pour Windows, OS X et Linux. Cette mouture intègre les interfaces de programmation Credential Management. Avec ces dernières, les sites Internet peuvent directement communiquer avec le gestionnaire de mots de passe mais aussi avec Google Smartlock ou les autorisations liées à un compte Facebook. Le processus de connexion s'en trouve simplifié, notamment sur smartphones.

L'équipe a en outre procédé à des optimisations du chargement des pages, notamment en ne récupérant pas les éléments non visibles à l'écran. Il en résulterait une meilleure gestion de la batterie avec un navigateur 30% moins gourmand.

Coté sécurité, les ingénieurs ont comblé 42 failles de sécurité en reversant au total 65 000 dollars aux experts ayant partagé leurs recherches. Retrouvez davantage d'informations sur cette page.

- Téléchargez Google Chrome 51 pour Windows
- Téléchargez Google Chrome 51 pour OS X
- Téléchargez Google Chrome 51 pour Linux

Article de Guillaume Belfiore

Réagissez à cet article

Source : *Chrome 51 : Google corrige 42 failles de sécurité*

Augmentation de 30% des demande de rançon informatique en 3 mois

	**Augmentation de 30% des demande de rançon informatique en 3 mois**

Le #ransomware a dépassé les attaques de type APT (menaces persistantes avancées) pour devenir le principal sujet d'actualité du trimestre. 2900 nouvelles variantes de malwares au cours de ces 92 jours.

Selon le rapport de Kaspersky Lab sur les malwares au premier trimestre, les experts de la société ont détecté 2900 nouvelles variantes de malwares au cours de cette période, soit une augmentation de 14 % par rapport au trimestre précédent. 15 000 variantes de ransomware sont ainsi dorénavant recensés.

Un nombre qui va sans cesse croissant.
Pourquoi ? Comme j'ai pu vous en parler, plusieurs kits dédiés aux ransomwares sont commercialisés dans le blackmarket. Autant dire qu'il devient malheureusement très simple de fabriquer son arme de maître chanteur 2.0.
Au premier trimestre 2016, les solutions de sécurité de l'éditeur d'antivirus ont empêché 372 602 attaques de ransomware contre leurs utilisateurs, dont 17 % ciblant les entreprises. Le nombre d'utilisateurs attaqués a augmenté de 30 % par rapport au 4ème trimestre 2015. Un chiffre à prendre avec des pincettes, les ransomwares restant très difficiles à détecter dans leurs premiéres apparitions.

Locky , l'un des ransomwares les plus médiatisés et répandus au 1er trimestre
Le ransomware Locky est apparu, par exemple, dans 114 pays. Celui-ci était toujours actif début mai. Un autre ransomware nommé Petya est intéressant du point de vue technique en raison de sa capacité, non seulement à crypter les données stockées sur un ordinateur, mais aussi à écraser le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées.
Les trois familles de ransomware les plus détectées au 1er trimestre ont été Teslacrypt (58,4 %), CTB-Locker (23,5 %) et Cryptowall (3,4 %). Toutes les trois se propagent principalement par des spams comportant des pièces jointes malveillantes ou des liens vers des pages web infectées. « Une fois le ransomware infiltré dans le système de l'utilisateur, il est pratiquement impossible de s'en débarrasser sans perdre des données personnelles. » confirme Aleks Gostev, expert de sécurité en chef au sein de l'équipe GReAT (Global Research & Analysis Team) de KL.

Une autre raison explique la croissance des attaques de ransomware : les utilisateurs ne s'estiment pas en mesure de combattre cette menace. Les entreprises et les particuliers n'ont pas conscience des contre-mesures technologiques pouvant les aider à prévenir une infection et le verrouillage des fichiers ou des systèmes, et négligent les règles de sécurité informatique de base, une situation dont profitent les cybercriminels entre autres. Bref, trop d'entreprise se contente d'un ou deux logiciels de sécurité, se pensant sécurisées et non concernées. L'éducation du personnel devrait pourtant être la priorité des priorités… [Lire la suite]

Article de Damien BANCAL

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

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

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

Contactez-nous

Réagissez à cet article

Source : *Ransomware: +30% d'attaques en 3 mois – Data Security BreachData Security Breach*

Un gros botnet détourne des requêtes de recherche

Un gros botnet détourne des requêtes de recherche

Depuis septembre 2014, un botnet a pu compter près d'un million de zombies pour faire gonfler des revenus publicitaires de cybercriminels.

Actif depuis mi-septembre 2014, un botnet est parvenu à prendre le contrôle de près d'un million d'ordinateurs dans le monde. L'agent infectieux est un malware intégré dans un fichier d'installation modifié de type MSI pour Windows.
Botnet-Redirector.Paco-carte-BitdefenderCes fichiers corrompus sont associés à des programmes tels que WinRAR, YouTube Downloader, Connectify, Start8 et KMSPico. Après installation sur la machine prise pour cible, le nuisible dénommé Redirector.Paco s'appuie sur un fichier PAC (Proxy auto-config) pour rediriger des requêtes de recherches sur Google, Bing ou Yahoo.
Au gré de quelques modifications dans la base de registre, le trafic sera redirigé vers des publicités contextuelles permettant de générer des revenus ici frauduleux grâce au programme AdSense pour les recherches de Google.
Les opérateurs du botnet détournent les recherches vers un autre moteur de recherche personnalisé spécifiquement conçu qui affiche ses propres résultats, et détournent par la même occasion des revenus publicitaires… [Lire la suite]
Article de Jérôme GARAY

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 : *Un gros botnet détourne des requêtes de recherche*

Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX

Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX

Dans ses derniers correctifs pour MacOSX, Apple signale que plusieurs failles de corruption de mémoire ont été corrigées grâce à l'aide du CESG, l'équivalent britannique de l'Anssi rattaché au GCHQ.

Si les choses se passent plutôt mal entre le FBI et Apple, le constructeur semble entretenir des rapports bien plus cordiaux avec le GCHQ britannique. Celui-ci a en effet été crédité dans une note de patch pour avoir aisé à la correction de failles de sécurité au sein de MacOSX. Deux failles ont ainsi été corrigées à l'aide du CESG, l'une permettant une corruption de mémoire au niveau du kernel de Mac OSX et une autre au sein des technologies de gestion des ports Firewire. Celles-ci permettaient à un attaquant d'exécuter du code potentiellement malveillant sur la machine visée.

Ce n'est pas la première fois que le CESG est crédité pour avoir débusqué des failles au sein de logiciels et les avoir communiqué à l'éditeur. L'organisme est souvent présenté comme un équivalent britannique de l'Anssi, mais est de fait rattaché aux services du GCHQ, l'équivalent britannique de la NSA. Une position qui laisserait croire que celui-ci aurait plutôt tendance à garder les vulnérabilités découvertes par ses équipes pour ses activités d'espionnage informatique.

La collaboration entre les forces de l'ordre et les acteurs de l'IT est à géométrie variable. Si Apple semble travailler en bonne intelligence avec le CESG, ses rapports sont nettement moins apaisés avec le FBI. Aux États Unis, le FBI est d'ailleurs critiqué par les développeurs de Tor pour son refus de communiquer l'une des failles ayant été utilisées dans le démantèlement du réseau de pédopornographie Playpen. Le GCHQ tout comme le FBI ou la NSA ne donnent que peu d'information sur les raisons qui les poussent à dévoiler les failles qu'ils connaissent aux éditeurs des logiciels ou matériels affectés. Mais Apple ne crache pas dans la soupe et a profité du tuyau pour combler les deux failles signalées par le CESG… [Lire la suite]

Article de ZDNet

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 : *Le GCHQ aide Apple à corriger une faille de sécurité sur MacOSX – ZDNet*

Voici les 12 pays africains qui espionnent les comptes sur Facebook | CIO-MAG

Voici les 12 pays africains qui espionnent les comptes sur Facebook

Egypte, Algérie, Tunisie, Soudan, Sénégal, Côte d'Ivoire, Nigéria, Kenya, Ouganda, Tanzanie, Botswana, Afrique du Sud. Voilà les douze Etats africains qui surveillent les comptes des utilisateurs du réseau social Facebook. Selon Les Dépêches de Brazzaville, ces Etats sont cités par Facebook dans son dernier rapport de transparence. Y figurent au total 92 pays qui envoient, à travers le monde, des requêtes en vue d'obtenir des informations sur l'identité des utilisateurs de certains comptes Facebook ou de ses autres services de messagerie électronique. Il s'agit notamment de Messenger, Instagram et Whatsapp.

Accepter ou refuser ? Les conditions de Facebook

De ce rapport, il ressort que Facebook peut donner une suite favorable à une requête quand celle-ci porte sur une affaire criminelle. C'est le cas par exemple des requêtes du Nigéria dans le cadre des enquêtes sur les attaques terroristes du mouvement Boko Haram. Lorsqu'une requête est jugée recevable par Facebook, il permet au pays intéressé d'accéder aux données personnelles (noms, adresse, ancienneté, adresse IP) ou à la messagerie privée d'un utilisateur. Par contre, une requête est jugée non recevable lorsque Facebook ne perçoit pas le « bien-fondé légal » et le « factuel » de la demande. C'est ainsi que des requêtes du Sénégal et de l'Algérie ont été rejetées. Au 31 décembre 2015, plus de la moitié des requêtes reçues par le réseau social américain visaient à résoudre des affaires de vol ou d'enlèvement. A ce jour, Facebook totalise 126 785 000 utilisateurs en Afrique.

Article de Anselme Akéko

Réagissez à cet article

Source : *Voici les 12 pays africains qui espionnent les comptes sur Facebook | CIO-MAG*

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

---

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*

Un hôpital paye la rançon mais n’obtient rien en échange.

Un hôpital paye la rançon mais n’obtient rien en échange

Certains groupes de pirates qui exploitent des ransomwares pour faire fortune sans effort n'ont ni morale ni parole, si l'on en croit la prise en otage de données d'un hôpital, qui a payé pour rien la rançon demandée.

Les maître-chanteurs sont aussi parfois de véritables escrocs, et ça n'est jamais une bonne idée de céder à leurs exigences. Après la messagerie chiffrée Protonmail qui avait payé une rançon et avait malgré tout continué à subir des attaques DDOS massives, c'est un hôpital américain qui l'apprend à ses dépens.

Ainsi Network World rapporte que le Kansas Heart Hospital à Wichita a accepté de payer une rançon après que des pirates ont réussi à infecter son système informatique avec un ransomware, qui chiffre les données stockées avec une clé que seul le ravisseur connaît. Ce n'est pas le premier hôpital à être visé et à céder ainsi à un chantage informatisé, mais c'est la première fois que les pirates ne respectent pas leur part du marché. Pire, ils en demandent plus.

PAYER ENCORE POUR DÉBLOQUER UN PEU PLUS

L'attaque avait eu lieu la semaine dernière, et avait rendu des fichiers de l'hôpital inaccessibles, sans possibilité de recourir à des archives. Pour les débloquer, il fallait payer de l'argent en utilisant un service anonymisé, sur Tor, avec un compte en bitcoins intraçable. Étant donnée l'importance des données, les administrateurs de l'établissement ont accepté de payer une somme indéterminée, relativement faible. Mais plutôt que de déchiffrer les données, les pirates n'en ont libéré qu'une petite partie, et exigé davantage d'argent pour déchiffrer le reste.

L'hôpital a alors refusé. « Ce n'était plus une manœuvre sage ou une stratégie », s'est justifiée la direction, qui a mis en place un plan B pour limiter les effets de l'attaque. Selon le Kansas Heart Hospital, aucun patient n'a eu à subir d'effets négatifs en raison de l'indisponibilité de certaines données… [Lire la suite]

Réagissez à cet article

Source : *Ransomware : un hôpital paye la rançon mais n'obtient rien en échange – Business – Numerama*

Auteur : Guillaume Champeau