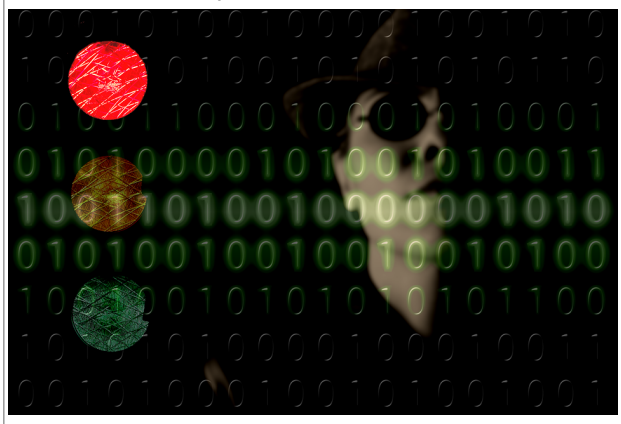
Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

	Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

D'après les informations de FireEye, le malware Irongate, qui vise les systèmes de contrôle des procédés industriels ressemble en certains points au terrible ver Stuxnet. Cette découverte est une nouvelle source d'inquiétude pour les membres de la communauté de la sécurité de l'information et elle vient confirmer la nécessité du perfectionnement des systèmes de détection des malwares qui attaquent les infrastructures critiques.



Les chercheurs ont également signalé qu'Irongate ne constituait pas une menace sérieuse pour l'instant car il fonctionne uniquement dans des environnements simulés. Ceci étant dit, FireEye indique que ce malware est passé inaperçu pendant des années alors qu'il figurait pendant tout ce temps dans la base VirusTotal. « La compétence du secteur dans le domaine de l'identification et de la détection des menaces s'améliore, mais elle n'a pas encore atteint un niveau satisfaisant comme le montrent ces exemples » constate Rob Caldwell, directeur du groupe d'analyse FireEye Labs Advanced Reverse Engineering (FLARE). Il poursuit en expliquant qu'il faut absolument mieux comprendre ce que représentent les menaces pour les systèmes de contrôle des procédés industriels, comment les détecter et comment améliorer la protection contre celles-ci. »

D'après FireEye, le malware qu'elle a identifié se distingue par sa capacité à mener une attaque de type homme du milieu contre l'entrée et la sortie des procédés et à attaquer l'application qui exécute des opérations sur les processus dans les environnements simulés. Un système compromis par Irongate permet aux attaquants de substituer les contrôles industriels à l'insu de l'opérateur du système. Des techniques semblables ont déjà été utilisées par le passé pour mettre hors service des infrastructures critiques diverses, depuis des réseaux de distribution d'électricité jusqu'aux contrôleurs logiques de centrifugeuses dans le secteur nucléaire.

Les chercheurs ont découvert une exemplaire d'Irongate vers la fin de l'année 2015 sur VirusTotal alors qu'ils recherchaient des droppers compilés à l'aide PyInstaller. L'échantillon trouvé ressemblait très fort aux malwares qui visaient les systèmes d'automatisation industrielle et autres systèmes de contrôle des procédés industriels. Il se fait que ce modèle avait été chargé pour analyse en 2012, mais aucun logiciel antivirus ne l'avait reconnu.

L'analyse a démontré que le malware utilise une technique de l'homme du milieu qui permet de réaliser des attaques contre une application personnalisée de l'utilisateur qui fonctionne dans un milieu de modélisation des contrôleurs logiques programmables Step 7 de Simens Les experts ont découvert également une bibliothèque dynamique capable de masquer le comportement malveillant du code exécutable. Cette DLL est capable d'enregistrer cinq secondes du trafic « normal » provenant du contrôleur logique programmable modélisé ; l'attaquant peut reproduire ce fragment afin de masquer le transfert des données codées en dur vers l'équipement d'imitation.

Les chercheurs ont été surpris de voir que pour rendre l'analyse plus difficile, ce malware spécialisé se comporte comme un malware traditionnel : lorsqu'il est exécuté sur une machine virtuelle ou dans un bac à sable (Cuckoo), il passe en mode de veille et refuse de s'exécuter.

« Bien que Stuxnet soit plus complexe sur le plan technique, Irongate possède quelques traits similaires » a déclaré Sean McBride, analyste antivirus principal chez FireEye. Pour être plus précis, il a noté que ces deux malwares sont destinés à attaquer un système particulier de gestion et ils utilisent des outils de protection contre la détection : Stuxnet est capable de détecter la présence d'un logiciel antivirus et Irongate, celle d'une machine virtuelle. Toutefois, à la différence de ses rares confrères commeBlackEnergy, Havex, et même Stuxnet, Irongate n'est pas très répandu dans la pratique : il fonctionne seulement dans les environnements simulés orientés sur les systèmes Siemens.

Qui est donc à l'origine de ce malware et quel est son objectif ? FireEye avance trois hypothèses en réponse. Tout d'abord, les experts supposent que son auteur peut avoir nourri l'espoir que quelqu'un transfèrerait ce code depuis l'environnement simulé et commencerait à l'utiliser dans son environnement de travail. Il est également possible qu'Irongate soit un modèle expérimental et que son créateur a décidé de vérifier à quel point il était facile de le détecter via les services VirusTotal. La troisième hypothèse est celle considérée comme la plus probable par FireEye : un expert en sécurité de l'information a oublié qu'il avait soumis ce code à une vérification il y a un certain temps.

« Il convient de fournir de plus gros efforts dans le secteur pour détecter les menaces qui visent les systèmes de contrôle des procédés industriels » conclut Dan Scali, conseiller principal de la division conseil de FireEye sur les questions de sécurité des systèmes d'automatisation industrielle. « Globalement, il n'y a pas eu de gros progrès dans la résolution des problèmes posés par Irongate depuis Stuxnet. Dans la mesure où l'accès à de tels attaques se démocratise, le thème de l'adéquation des mesures de protection est source de préoccupation.

Réagissez à cet article

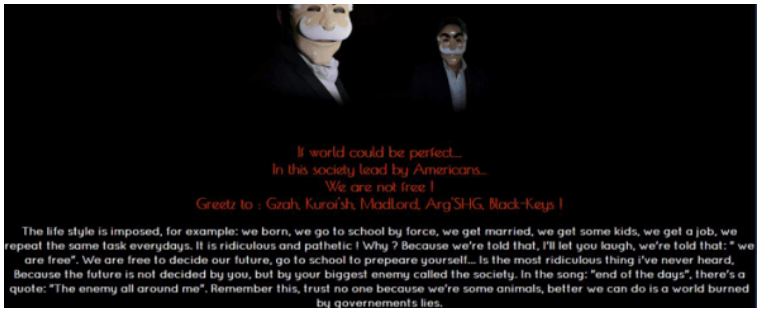
Original de l’article mis en page : Un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet – Securelist

---

Déffaçage (piratage) du site Internet des espaces de la CAF

Déffaçage (piratage) du site Internet des espaces de la CAF

Barbouillage de sites – Plusieurs pirates informatiques se sont amusés à modifier des espaces Internet appartenant à la CAF.



Barbouillage de sites – Samedi 11 juin, vers 16 heures, plusieurs sites Internet appartenant à la Caisse des Allocations Familiales Françaises se sont retrouvées modifiés, du barbouillage de sites, par trois pirates informatiques « différents » : Mad Lord, ArG'Sh et Sneaky. Les sites impactés (ils étaient tous sur le même serveur) : lacafrecrute.org, lacafrecrute.com, fraude-caf.fr et lacaf.com.Les adolescents ont taggué les espaces ainsi infiltrés.

Barbouillage de sites

*Dans le premier cas, celui de lacaf.com, le pirate indique que « **Si le monde pouvait être parfait … sans corruption, duperie … Ensemble, nous pouvons agir pour créer** !« . Dans le site dédié à la lutte contre la Frauce, ArG'SH affiche une jeune fille tirée d'un manga et une tirade sur la corruption des gouvernements. Même son de cloche pour lacafrecrute.com, espace dédia aux offres d'emplois à la CAF [le site lacafrecrute.fr fonctionne, NDR] , modifié par Sneaky. Les adresses Internet des sites impactés sont redirigées vers l'url officiel de la Caisse des Allocations Familiales : caf.fr. D'après mes constations, les données privées et sensibles appartenant aux allocataires n'ont pas été impactées.*
Article original de Damien BANCAL

Réagissez à cet article

Original de l'article mis en page : Barbouillage de sites ! Des espaces de la CAF piratés – ZATAZ

Pourquoi l’inventeur du Web rêve d’un autre Internet ?

Pourquoi l’inventeur du Web rêve d’un autre Internet ?

Inventeur du Web il y a plus de 25 ans, Tim Berners-Lee regrette le pouvoir quont pris sur lui les états et les grandes entreprises comme Google ou Facebook. Il souhaite pousser vers un Web plus déconcentré et plus sûr pour ses utilisateurs.

Mais qu'a-t-on fait d'Internet ? C'est la question que se posent régulièrement des pionniers du Web, qui rêvaient de changer le monde et qui l'ont effectivement fait, sans toujours bien savoir si c'est pour le meilleur ou pour le pire. Internet a apporté son lot incontestable d'améliorations dans la vie sociale, en permettant aux citoyens de s'informer davantage, de partager des connaissances et d'entrer plus facilement en contact les uns avec les autres. Mais il est aussi devenu un moyen inédit de surveillance de la population, et une machine libérale qui favorise les plus gros dans une économie plus que jamais mondialisée.
Parmi ceux qui semblent avoir quelques regrets figure l'inventeur du World Wide Web, Tim Berners-Lee. L'homme, qui a créé la première page Web il y a plus d'un quart de siècle, s'est désolé dans le New York Times de ce qu'était devenu en partie Internet. « Il contrôle ce que les gens voient, crée des mécanismes sur la manière dont les gens interagissent. Ce fut génial, mais l'espionnage, le blocage de sites, le détournement du contenu des gens, vous faire aller sur les mauvais sites web… tout ça mine complètement l'esprit d'aider les gens à créer », condamne-t-il.

NOUS N'AVONS PAS UN PROBLÈME TECHNOLOGIQUE, NOUS AVONS UN PROBLÈME SOCIAL

Berners-Lee voit un problème majeur dans le développement du Web qu'il a créé ; la possibilité pour les états ou de grandes entreprises de prendre le contrôle et d'imposer leur puissance. Pour les états, il s'agit par exemple de la possibilité qu'ils ont de bloquer l'accès à des sites internet (comme c'est désormais fréquent en France), ou de traquer les communications pour identifier ou géolocaliser des dissidents. Concernant les entreprises, le souci est davantage dans le pouvoir immense que des Facebook ou Google ont sur les populations du monde entier, en étant les principaux vecteurs d'informations, et en glanant des informations de plus en plus précises sur les habitudes et les pensées de chacun.

Pour défendre l'idée de repenser Internet, l'ingénieur a donc participé cette semaine à la conférence Decentralized Web Summit de San Francisco, organisée notamment par la fondation Internet Archive, et des acteurs impliqués dans le bitcoin et la blockchain. Mais il prévient que la solution ne sera pas seulement technique. « Le Web est déjà décentralisé », rappelle-t-il. « Le problème c'est la domination d'un moteur de recherche, d'un grand réseau social, d'un Twitter pour le microblogging. Nous n'avons pas un problème technologique, nous avons un problème social ».
« Nous sommes au bord de découvrir qu'une entreprise peut en arriver au point où en réalité elle contrôlera tout ce que chacun d'entre nous voit », s'était déjà inquiété Berners Lee dans une interview à GeekWire. « Elle décidera des posts de ses amis et des articles de journaux qu'une personne voit, et nous réalisons que nous parlons d'une seule grande multinationale qui a soudainement le contrôle complet sur la perception qu'a quelqu'un de la planète sur laquelle il habite. C'est une bataille constante et nous en sommes très proches tout le temps ».

UN PAIEMENT PLUS FLUIDE POUR UN INTERNET PLUS SAIN

Pour aider à réinventer le Web, Tim Berners-Lee rêve notamment d'un réseau social respectueux de la vie privée des utilisateurs et de leur liberté d'expression. Il est membre du conseil d'administration de MeWe, qui se rêve en Facebook éthique. D'autres technologies décentralisées peuvent aussi aider, comme Tor bien sûr, mais aussi des initiatives comme ZeroNet, qui prétend héberger un Web non censurable en utilisant BitTorrent et du chiffrement, ou MaidSafe, qui utilise aussi une architecture P2P et un système d'échange monétaire baptisé SafeCoin.
À cet égard, Tim Berners-Lee espère aussi voir prospérer un Web où le paiement électronique serait beaucoup plus aisé, et sans intermédiaires à qui verser des commissions (ce qui était à l'origine l'idée du bitcoin, même s'il manque de fluidité dans la validation des transactions). « Imaginez un monde où le fait de payer pour des choses serait facile des deux côtés », demande-t-il, en faisant remarquer que « le modèle publicitaire est le seul modèle pour trop de gens sur le web actuellement ».
Les journaux, par exemple, devraient pouvoir proposer de faire payer quelques centimes pour lire un article, ce qui rapporterait davantage que la publicité, offrirait davantage d'espace d'affichage pour l'information, et éviterait de tracer l'internaute. Or aujourd'hui, le jeu des commissionnements et des empilements d'intermédiaires fait qu'il est pratiquement impossible d'avoir sur internet la fluidité de paiement offerte par l'argent liquide.
Crédit photo de la une : CC Kristina D.C. Hoeppner
Article original de Guillaume Champeau

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

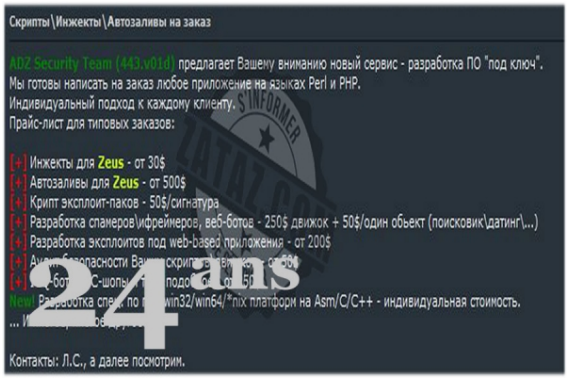
Original de l'article mis en page : Pourquoi linventeur du Web rêve dun autre Internet — Politique — Numerama

---

Prison ferme pour les auteurs de SpyEye botnet

Prison ferme pour les auteurs de SpyEye botnet

Le code malveillant SpyEye botnet a fait de gros dégâts en son temps. Les deux auteurs, Russe et Algérien, de ce kit informatique dédié à l'espionnage viennent d'écoper de 24 ans de prison ferme.



Les deux pirates Russe et Algérien cachés derrière le code malveillant SpyEye ont été reconnus coupables par la justice américaine d'avoir fabriqué et vendu ce kit malveillant dont le but premier était d'infiltré les ordinateurs pour espionner et voler les données des machines infiltrées.

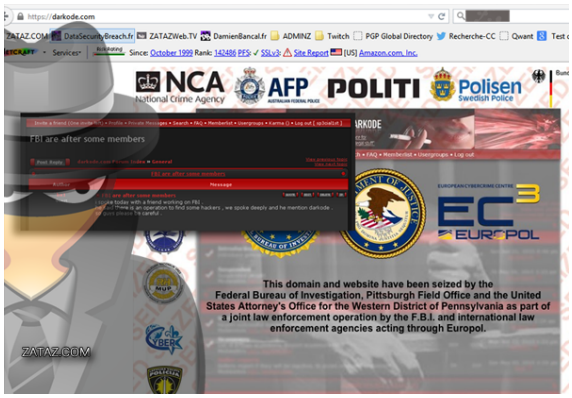
Le prix de SpyEye botnet

Les deux pirates ont été condamnés à 24 ans de prison ferme (les deux peines cumulées). Une condamnation forte pour un outil, aussi baptisé Zeus, qui a permis d'infecter des centaines de milliers d'ordinateurs de par le monde. Une peine de neuf ans et six mois pour Aleksandr Andreevich Panin (27 ans), connu sur la toile sous le pseudonyme de « Gribodemon » et « Harderman ». Le FBI avait lancé un « Wanted » sur la tête de Panin de 3 millions de dollars. En juin 2015, l'ensemble des interactions de Zeus / SpyEye avait été stoppé par le FBI, Europe et Eurojust. Plusieurs dizaines de personnes ont été arrêtés, de l'utilisateur de SpyEye aux blanchisseurs d'argent volé.

L'Algérien Hamza Bendelladj, alias Bx1 a écopé de 15 ans. Ce dernier, âgé de 27 ans, était le partenaire d'affaires de Panin. Ce ressortissant algérien avait plaidé coupable en Juin 2015. Il avait modifié SpyEye pour réaliser son propre outil malveillant qui lui a permis de voler 200.000 numéros de carte de crédit. Bendelladj, baptisé « Le pirate souriant » avait été arrêté à Bangkok, en janvier 2013. Extradé aux USA en mai 2013. Il vient de perdre définitivement son grand sourire !
Dans les outils proposés par les pirates, des ransomwares, comme Locker, qui se faisait passer pour le FBI.

Dans les outils proposés par les pirates, des ransomwares, comme Locker

Dans les outils proposés par les pirates, des ransomwares, comme Locker, qui se faisait passer pour le FBI.



SpyEye, comme j'avais pu vous le montrer à l'époque [1e capture écran de cet article], était commercialisé dans le black market, dans une boutique baptisée à l'époque DarkCode.
Article original

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 : Prison ferme pour les auteurs de SpyEye botnet

---

32 millions de mots de passe Twitter dérobés

	32 millions de mots de passe Twitter dérobés

---

Après LinkedIn, MySpace et Tumblr, Twitter a lui aussi été victime d'un piratage massif. 32,8 millions de comptes seraient affectés.

Une nouvelle fuite de données pour un réseau social. Un hacker russe affirme avoir dérobé 379 millions d'adresses email et de mots de passe non chiffrés associés à des comptes Twitter. Identifié sous le pseudonyme Tessa88, il aurait mis en vente la base de données en question sur VK, le Facebook russe. LeakedSource, qui a révélé l'information, estime que 32,8 millions de comptes seraient effectivement compromis, une fois les doublons éliminés.

«Nous sommes convaincus que ces noms d'utilisateurs et les identifiants n'ont pas été obtenus par une violation des données Twitter. Nos systèmes n'ont pas été hackés», a déclaré un porte-parole de Twitter. La base de données serait donc le fruit d'une campagne de malware ciblant les particuliers pour récupérer leurs mots de passe.

Sollicité par Techcrunch, Troy Hunt, le fondateur de site haveibeenpwned.com qui permet de voir si une adresse mail fait partie d'une base de données piratée, émet des doutes par rapport à l'authenticité des données piratées: «Les piratages de comptes que nous avons vus jusqu'à présent sont très probablement le résultat de la réutilisation de données issues d'autres piratages», indique-t-il.

Une incitation de plus à modifier son mot de passe

Si Leakedsource propose de vérifier si vos identifiants et mots de passe sont dans leur base et de les retirer gratuitement, le plus simple reste encore de modifier son mot de passe.

Twitter a suggéré au passage de le complexifier, en suivant ses recommandations.

7 Juin

Twitter Support
@Support
To help keep people safe and accounts protected, we've been checking our data against what's been shared from recent password leaks.
Suivre

Twitter Support
@Support
Any time is a good time to make sure your account is secure, starting w[illegible] an updated password. More tipshttps://support.twitter.com/articles/76036
00:36 – 7 Juin 2016

Safe Tweeting: the basics
Keeping your account secure We want Twitter to be a safe and open community. This help page provides some information and tips to help you practice safe Tweeting and keep your acco
support.twitter.com
•
•
128128 Retweets
•
170170 j'aime

Selon la liste des données divulguées, bien trop de ***mots de passe*** *restent basiques et facilement trouvables. 123455 prend la première place du podium, suivi de 123456789, qwerty et du classique password.*
Ce piratage suit celui de MySpace, de Tumblr et de LinkedIn. ***100 millions de mots de passe*** *du réseau professionnel récupérés en 2012 ont été mis en vente mi-mai. Ce piratage avait valu à Mark Zuckerberg, adepte du mot de passe unique «dadada», de* ***voir ses comptes Twitter et Pinterest piratés****.*
Article original

Réagissez à cet article

Original de l’article mis en page : Un hacker russe prétend avoir dérobé des millions de mots de passe Twitter

---

La France dans le Top 10 du piratage informatique

La France dans le Top 10 du piratage informatique

NATIC Magazine vous fait une synthèse de l'actualité tournant autour des problématiques de cybersociété: Hacking, Sécurité, Codes malveillants, Piratage, Vie privée numérique, Protocole d'alerte, Alerte propagande, Web Tv, etc.

Le rapport annuel de Symantec sur le piratage informatique est une fois encore percutant. Selon le géant mondial de la cybersécurité, la France fait partie des 10 pays les plus concernés par les attaques informatiques. En 9ème position mondiale, le pays subit plus de 10 millions de tentatives avérées par an, en forte hausse d'une année sur l'autre.
Selon la version 2016 du rapport, les brevets technologiques et les trésors de propriété intellectuelle des grands groupes français attirent les meilleurs pirates mondiaux. Lancées par des concurrents, des activistes ou même des états, ces attaques visent également des PME ou même des particuliers ce qui est plus étonnant. Ces derniers sont très vulnérables notamment lorsqu'ils utilisent les réseaux sociaux. On observe en particulier une percée remarquable de l'utilisation des ransomwares ou rançongiciels – en hausse de 260% en France en 2015. Le phénomène prend de l'ampleur.
Dans le rapport de Symantec version 2016, le Top 3 des pays victimes de piratage en 2015 est constitué de la Chine, des Etats-Unis et de l'Inde.
Article original

Réagissez à cet article

Original de l’article mis en page : La France dans le Top 10 du piratage

---

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

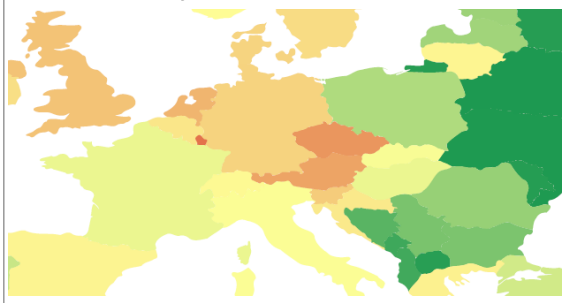
Contactez-nous

Réagissez à cet article

ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l’Europe

ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l’Europe

Les rapports de détection réalisés par ESET montrent une augmentation importante de la prolifération du malware JS/Danger.ScriptAttachement dans plusieurs pays européens. Les pays les plus touchés sont le Luxembourg (67 %), la République tchèque (60%), l'Autriche (57%), les Pays-Bas (54%) et le Royaume-Uni (51%).



ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l'Europe Les rapports de détection réalisés par ESET montrent une augmentation importante de la prolifération du malware JS/Danger.ScriptAttachement dans plusieurs pays européens. Les pays les plus touchés sont le Luxembourg (67 %), la République tchèque (60%), l'Autriche (57%), les Pays-Bas (54%) et le Royaume-Uni (51%).

ESET considère les ransomwares comme l'une des menaces informatiques les plus dangereuses à l'heure actuelle. Par conséquent, nous recommandons aux particuliers et aux entreprises de garder leurs ordinateurs et leurs logiciels à jour, d'utiliser un logiciel de sécurité fiable et de sauvegarder régulièrement leurs données importantes.

«Les utilisateurs d'ESET sont protégés contre cette menace. Nos solutions sont capables de bloquer le téléchargement et l'exécution en force par les différentes familles de ransomwares», commente Ondrej Kubovič, ESET IT Security Specialist.
En effet, lors du test réalisé par SE Labs qui compare 8 solutions de protection anti-malware, ESET Smart Security 9 remporte la première place avec 100% de réussite dans toutes les catégories.
«Chez ESET, nous nous engageons dans notre travail pour faire des produits qui protègent des millions d'utilisateurs à travers le monde. Nous apprécions de voir que les tests réalisés par SE Labs valident l'approche multicouches que nous construisons depuis plus de 20 ans.», a déclaré Palo Luka, Chief Technology Officer chez ESET.
ESET Smart Security 9 se distingue comme le seul produit ayant bloqué toutes les menaces. «ESET Smart Security contrôle parfaitement les attaques ciblées et les menaces Internet, ce qui est un excellent résultat. Il est rare d'obtenir 100% de réussite dans les tests de détection de menaces en temps réel, pour un produit sans compromis qui offre une protection complète et qui contrôle également des applications et des sites Web dits légitimes sans commettre une seule erreur», explique Simon Edwards, SE Labs' founder and Director.

Pour en savoir plus ces produits, rendez-vous sur http://www.eset.com/fr/
Article original de Benoit Grunemwald

Réagissez à cet article

Original de l'article mis en page : Locky se propage en Europe

---

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

---

Hardwear.io 2016 : Hardware Security Conference

Hardwear.io 2016 : Hardware Security Conference

Les 22 et 23 septembre 2016, à La Hague (Pays-bas) la seconde édition de la Hardwear.io se penchera sur la sécurité des objets connectés.

hardwear.io
Hardware Security Conference and Training

A l'ère de l'automatisation où la technologie joue un rôle clé dans l'amélioration de l'efficacité des dispositifs, la nécessité de traiter de manière proactive la sécurité matérielle est largement sous-estimée. Allant de simples gadgets connectés utilisés au quotidien, aux systèmes automobiles, aux appareils médicaux sans fil où au matériel de défense nationale ; tout fonctionne sur une technologie sophistiquée mais très vulnérable .
Hardwear.io propose à la fois une plate-forme et une communauté, une occasion d'échanger entre professionnels, et le plus important apporte des solutions aux problèmes critiques relatifs à la sécurité du hardware.
Des sessions de formation se tiendront pendant deux jours, avant la tenue de la conférence, les 20 et 21 septembre 2016 à la Hague, aux Pays-bas. Avec des intervenants de renom, pour échanger sur divers sujets comme les backdoors, l'exploitation des failles, la confiance, les assurances et les attaques sur l'équipement matériel, les firmware et protocoles connexes .
Hardwear.io est est menée par l'équipe de nullcon – Conférence internationale de sécurité basée en Inde, l'un des événements de la sécurité des systèmes d'information de premier plan en Asie depuis 2010. Hardwear.io est une conférence qui apporte à la fois une plate-forme et une communauté pour la sécurité du matériel informatique, où les chercheurs mettent en valeur leurs travaux et échangent leurs innovations liées aux attaques et à la défense hardware. L'objectif de la conférence tourne autour de quatre principales préoccupations : le firmware et les protocoles connexes à savoir backdoors, exploits, la confiance et les attaques.

L'APPEL A CONTRIBUTIONS EST OUVERT
Pour tous ceux qui souhaitent intervenir lors de la conférence Hardwear.io 2016, les sujets peuvent être soumis jusqu'au 5 juillet 2016 via hardwear.io. Hardwear.io privilégie les sujets ayant trait à la sécurité du matériel en profondeur, à la fois sous l'angle offensif et défensif.

Parmi les domaines proposés (sans s'y limiter) :
– Circuits intégrés
– Processeurs
– Internet des objets / Smart Devices
– Crypto Hardware
– Systems embarqués
– Systèlmes automatisés Automobile, Aerien, train et composants hardware
– Systèmes de controle industriels / SCADA
– Systèmes Satellites
– Objets médicaux connectés
– Smartphone firmware, hardware
– Firmware
– Test de pénétration Hardware
– Module plateforme de confiance
– Protocoles de communication Radio et hardware
– Confiance et assurance Hardware et algorithms
– Multimedia hardware, firmware, protocols
– Telecom Hardware et réseaux
– Serrures éléctroniques et physiques
Parmi les intervenants clés en 2015, Hardwear.io a accueilli : Jon Callas, Harald Welte, Javier Vidal, Jaya Baloo, Florian Grunow et d'autres experts de renom en sécurité qui ont tous renforcé l'équipe des organisateurs de la nécessité de poursuivre ces rencontres de la sécurité hardware dans le monde ultra connecté d'aujourd'hui. Pour plus d'information, et pré-ventes early bird: http://hardwear.io
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Hardwear.io 2016 : Hardware Security Conference – ZATAZ