Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable

	Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable par les anti-virus

Les attaques ransomwares ne baissent pas. Après avoir usurpé des avocats, des comptables, des PME, des mairies, FREE, voici le courriel piégé aux couleurs d'Orange. Ne cliquez surtout pas sur la pièce jointe.

Le courriel s'invite dans votre boites à mails avec comme objet : « ***Votre demande d'assistance*** » ; « ***Votre assistance Orange*** » ; « ***Votre assistance Orance Business***« . La missive pirate indique qu'une anomalie lors d'un prélèvement oblige le lecteur internaute à lire le fichier joint, un PDF piégé baptisé « ***Montant du mois*** » ou encore « ***Montant de la facture***« . Un piège qui, heureusement, est plutôt mal réalisé pour les internautes avertis. Il peut, cependant, piéger les plus curieux. La cible étant clairement les entreprises, une secrétaire, un comptable ou un responsable n'ayant pas vraiment le temps de lire autrement qu'en « Z » sera tenté de cliquer.

Au moment de l'analyse des fichiers, aucun antivirus n'avait la signature de la bestiole en mémoire. **A noter qu'un antivirus, face à ce genre d'attaque ne peut pas grand chose. Chaque mail et fichier joint portent en eux une signature (identification) unique et différente…** [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Attaques ransomwares aux couleurs d'Orange – ZATAZ*

Discuter avec des robots, les chatbots, simple mode ou avenir certain ?

	**Discuter avec des robots, les chatbots, simple mode ou avenir certain ?**

À terme, les robots conversationnels vont remplacer les applications et exécuter tout type de services au sein des messageries instantanées.

À l'origine, il y a un concept, **le test de Turing**, formulé par l'informaticien et mathématicien Alan Turing au début des années 1950. Conçu pour mesurer la capacité d'une machine informatique à penser, celui-ci consiste à tromper au moins un tiers de juges humains en cinq minutes d'échanges conversationnels. Un programme l'a passé avec brio pour la première fois en 2014. Le logiciel « Eugene Goostman » a conversé si naturellement avec des humains que ses interlocuteurs ont cru qu'il était l'un des leurs.

Ces dernières années, les programmes informatiques intelligents capables de soutenir une discussion avec des humains ont fait d'immenses progrès grâce aux avancées de l'intelligence artificielle. Si bien qu'**après plus de 60 ans de travaux, les « chatbots » sont en passe de révolutionner le dialogue entre les services en ligne et les utilisateurs**. Contraction de « chat », pour « converser » en anglais, et de « bots », pour « robots », les chatbots sont désormais en mesure de passer en revue d'énormes bases de données pour trouver des éléments de réponse en quelques instants. Ce brassage massif de données leur permet d'adopter les mécanismes de langage des humains pour converser avec eux tout en améliorant leurs connaissances au fil des discussions.

Dans le sillage du chinois WeChat, les chatbots sont déjà utilisés par plusieurs applications de messagerie sécurisées comme Kik et Telegram et l'outil de communication en entreprises Slack pour réaliser des tâches simples à partir d'une conversation. **Dans le futur, chaque entreprise disposera de son chatbot à qui les clients pourront demander des services.** Il sera ainsi possible de commander une pizza ou de réserver un billet d'avion tout en discutant avec ses amis au sein d'une même interface conversationnelle. À terme, ils rendront les applications archaïques. Pour les grands groupes technologiques, tout l'enjeu est de réussir à attirer le plus de bots afin de proposer la plateforme la plus complète possible.

Les assistants intelligents, passerelles entre utilisateurs et services

Pour Microsoft, les bots sont tout simplement « les nouvelles applications ». Malgré les dérapages de son chatbot Tay, qui a publié des messages racistes, antisémites et d'insultes sur Twitter sous la pression des internautes, l'éditeur de logiciel veut faire des robots conversationnels le pivot de sa nouvelle stratégie. « Commander un taxi, acheter un billet d'avion ou une pizza, tout ce que vous faites aujourd'hui en surfant sur le web ou en utilisant une application, vous pourrez le faire demain en discutant avec un bot », a prédit le PDG de Microsoft Satya Nadella en ouverture de la conférence Build fin mars. À terme, il suffira de parler à son assistant vocal Cortana, sur smartphones, tablettes, montres connectée ou PC, pour entrer en contact avec n'importe quel service.

Microsoft mise sur l'intégration de bots dans Skype et sa base de plus de 300 millions d'utilisateurs pour s'implanter sur le plus grand nombre d'appareils. Le groupe informatique entend également devenir l'intermédiaire privilégié entre les entreprises et les développeurs dans la conception de chatbots et va lancer prochainement une plateforme pour mettre à disposition des professionnels ses compétences en matière d'intelligence artificielle. La firme de Redmond, qui a raté le virage du mobile, y voit l'occasion de **porter un coup au modèle d'Apple et Google qui tirent une part significative de leurs revenus de leurs magasins d'applications**. Mais avec Siri et Google Now, ces derniers planchent également sur leurs propres solutions depuis plusieurs années.

Les avancées de Facebook officialisées mardi ?

Les bots vont aussi envahir Facebook. Mark Zuckerberg estiment qu'ils vont révolutionner les relations entre les entreprises et leurs clients en permettant aux premières de toucher une audience plus large et plus personnalisée. Le réseau social compte sur « M », un assistant intelligent mêlant intelligence artificielle et expertise humaine, pour monétiser pour de bon son service de messagerie Messenger et faire fructifier sa communauté de plus de 800 millions d'utilisateurs. Chaque marque ou entreprise pourra utiliser les bots pour répondre et interagir aux demandes des membres au sein même de Messenger et fournir ensuite des publicités de plus en plus ciblées en fonction de leurs comportements.

Selon des documents révélés par *TechCrunch,* Facebook veut rapidement mettre les professionnels en relation avec des développeurs et des services pour qu'ils conçoivent leur propre chatbot. Deux nouvelles interfaces de programmation, Chatbots et Live Chat seraient déjà sur les rails. La première combinant intelligence artificielle et assistance humaine fournira des réponses automatiques et des messages structurés via Messenger tandis que la seconde facilitera l'implémentation de boutons « contacts » renvoyant vers Messenger sur les sites web des entreprises. Ces avancées devraient être officialisées lors de sa conférence annuelle dédiée aux développeurs, le Facebook F8 qui se tient mardi et mercredi à San Francisco… [Lire la suite]

Réagissez à cet article

Source : *Facebook, Microsoft… Pourquoi les géants de l'informatique misent sur les chatbots*

Les établissements scolaires également victimes de ransomwares

	Les établissements scolaires également victimes de ransomwares

---

Après les hôpitaux, les ransomwares s'attaquent de plus en plus aux établissements scolaires. Retour sur plusieurs cas aux Etats-Unis.

Les ransomwares sont devenus la plaie des responsables sécurité des entreprises ou des administrations. On peut se remémorer le témoignage du RSSI de l'AFP qui en a fait l'expérience. Le secteur hospitalier a été particulièrement touché avec différents exemples. Le plus symptomatique est le Hollywood Presbyterian Medical Center de Los Angeles qui a été obligé de payer 17 000 dollars en bitcoin pour retrouver l'usage de son réseau.

Certains payent la rançon

Après les hôpitaux, les ransomwares s'intéressent à une autre cible : les écoles. Plusieurs cas ont été recensés aux Etats-Unis. En février dernier, plusieurs écoles primaires du Horry County en Caroline du Sud ont été victimes d'un rançongiciel qui a bloqué 25 serveurs. Immédiatement après avoir été alertée par les enseignants, l'équipe IT a débranché les serveurs affectant ainsi les services en lignes des écoles. Après enquête, la porte d'entrée du malware était un vieux serveur non mis à jour. Toujours est-il que les responsables de l'école ont se sont vus réclamer 0,8 bitcoin par ordinateur soit un total de 20 bitcoins (environ 7600 euros). Malgré l'aide du FBI, le conseil d'administration du campus a décidé de payer la rançon demandée.

D'autres non

D'autres ont décidé de ne pas payer la rançon comme dans le cadre du Oxford School District dans le Mississipi. En février dernier aussi, ce réseau de 8 campus a été infecté par un rançongiciel réclamant environ 9000 dollars pour un retour à la normal. Le superintendant de l'établissement, Brian Harvey, a préféré ne pas payer et s'est concentré sur la récupération des données. Dans un entretien accordé à HottyDotty, il précise que « nous avons restauré à partir d'une sauvegarde ». Mais les dégâts étaient importants. « Je ne sais pas combien de données nous avons perdu. Je peux dire que nous avons perdu la plupart des serveurs Windows. La chose la plus importante a été de tout effacer et de tout réinstaller depuis la sauvegarde. » L'attaque a privé les établissements d'Internet pendant plus d'une journée. Les 4 premiers jours après l'attaque ont été focalisés sur la récupération du système des carnets de notes des élèves. D'autres applications ont souffert comme les reporting ou le recrutement des agents. Au final, deux semaines ont été nécessaires pour tout remettre à peu près d'aplomb : les sites web, la gestion de la cafeteria, ainsi que des plateformes pour l'éduction comme PowerSchool et Schoology.

Les parents d'élève s'inquiètent

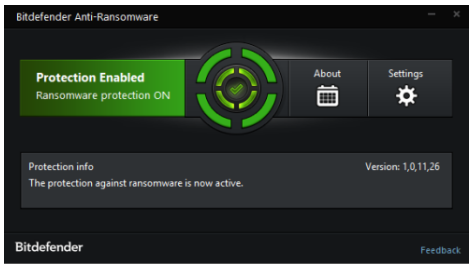
Autre affaire, le Texas School District qui gère une vingtaine d'établissements. Un ransomware a infecté le réseau, provoquant le blocage de plusieurs fichiers. La direction du district s'est voulue rassurante en expliquant que seule une petite partie des informations est concernée par le blocage. Ce dernier porte néanmoins sur un volume de 2,5 To de données. Les responsables ont choisi de ne pas payer la rançon demandée par les cybercriminels. « Nous avons réussi à effacer les fichiers chiffrés et à réinstaller données à partir d'une sauvegarde », précise un porte-parole du district. Un cas similaire à celui du Mississipi qui inquiète les parents d'élèves. « Ils [NDLR les établissements] détiennent des actes de naissance, des numéros de sécurité sociale ou des données médicales comme les vaccins », souligne une des parents d'élèves.

En France, aucun cas n'a été relevé ou publié sur des expositions à des ransomwares. Les écoles, universités et autres établissements scolaires font partie de cibles privilégiés par les cybercriminels. Obsolescence des parcs informatiques, système IT peu mis à jour, les pirates se ont trouvé un terrain de jeu grandeur nature pour tester et peaufiner leurs attaques. Les sommes demandées restent modestes, un signe selon les spécialistes pour reconnaître le degré de résistance des victimes à payer la rançon. En tout cas, les exemples américains doivent alerter les établissements bancaires européens et français sur les risques des ransomwares… [Lire la suite]

Réagissez à cet article

Source : *Les ransomwares prennent le chemin des écoliers*

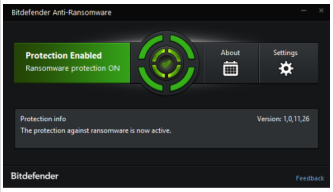
Bitdender met à disposition un outil gratuit de protection contre les Ransomwares



Bitdender met à disposition un outil gratuit de protection contre les Ransomwares

---

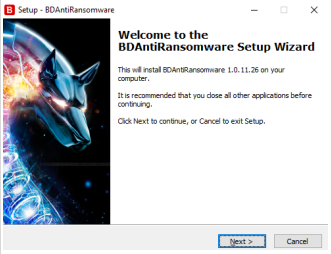
Bitdefender has just released a free tool that can protect against ransomeware viruses. Here is how to install it.



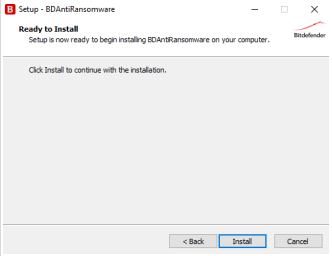
Hackers have been hitting everything from hospitals to police stations with Ransomeware viruses. Bitdefender has released a tool that could help fight it:
“Bitdefender anti-malware researchers have released a new vaccine tool which can protect against known and possible future versions of the CTB-Locker, Locky and TeslaCrypt crypto ransomware families.
“The new tool is an outgrowth of the Cryptowall vaccine program, in a way.” Chief Security Strategist Catalin Cosoi explained. “We had been looking at ways to prevent this ransomware from encrypting files even on computers that were not protected by Bitdefender antivirus and we realized we could extend the idea.”

Installation could not be easier

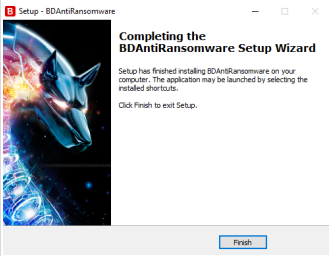
1. Download the file:
https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/
2. Run it:



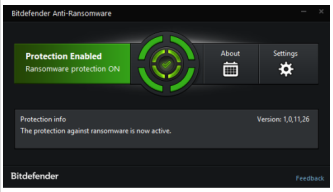
3. Click Next, and then install:



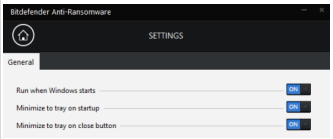
4. And then Finish



And that is it!



How easy was that?
If you want you can change the settings for the program. You may want to set it to “minimize on startup” and “minimize to tray on close”:



But it is pretty much an install and forget about it type app, no fuss, no muss.
Bitdefender has always been one of my favorite anti-virus programs, and this is a handy tool to have.
Check it out!

Réagissez à cet article

Source : *How to install Bitdender’s free Ransomware Protection Tool | CYBER ARMS – Computer Security*

Caméras-piétons : la CNIL réclame des garanties

	**Caméras-piétons : la CNIL réclame des garanties**

Dans son rapport de l'année 2015 publié vendredi 8 avril, la Commission nationale pour l'Informatique et les Libertés (CNIL) insiste sur la nécessité d'encadrer juridiquement l'utilisation des dispositifs de vidéosurveillance mobile et embarqués. Une injonction visant à mieux protéger la vie privée, qui prend tout son sens à l'heure où le ministère de l'Intérieur entend généraliser les caméras dites boutonnières, et alors que plusieurs polices municipales en sont d'ores et déjà équipées.

Le projet de loi renforçant la lutte contre le crime organisé permettra-t-elle la généralisation des caméras-piétons à toutes les patrouilles de police ? Pour que ce souhait formulé par le ministre de l'Intérieur, Bernard Cazeneuve, le 9 avril dernier, puisse se concrétiser, la Commission nationale pour l'Informatique et les Libertés (CNIL) rappelle l'importance de prévoir un encadrement « de nature légale, spécifique et adapté à de tels dispositifs. »
A travers un chapitre de quatre pages, la publication de son rapport annuel 2015 a été une nouvelle fois l'occasion de sensibiliser le ministère de l'Intérieur et les collectivités territoriales à cette problématique. Une détermination qui pourrait bien finir par payer. Alors que l'utilisation de telles technologies ne reposait jusqu'ici sur aucune base légale pour les forces de l'ordre, nationales comme municipales, l'article 32 de ce nouveau texte législatif – qui plusieurs dispositions spécifiques – devrait en toute logique y… [Lire la suite]

Réagissez à cet article

Source : *Caméras-piétons : la CNIL réclame des garanties – Club Prevention Securite – Lagazette.fr*

Que deviendront nos données personnelles après notre mort ?

Que deviendront nos données personnelles après notre mort ?

Après la disparition d’un proche, peut-on récupérer les fichiers, les achats réalisés par celui-ci ?

3 milliards d’êtres humains sont aujourd’hui connectés à Internet, échangeant de nombreuses données. Mais que deviennent celles-ci après la mort ? En France, plus de 85% de la population sont ainsi connectés. Réseaux sociaux, messagerie, photos… D’innombrables données personnelles numériques sont échangées.

Bientôt une loi sur les données numériques

Les personnes interrogées ne savent pas ce qu’elles deviennent. Depuis 40 ans, un texte interdit à quiconque de consulter ou de porter atteinte aux informations personnelles. C’est la protection des données qui, de facto, s’est étendue au numérique. « La protection des données personnelles stipule qu’un tiers n’a pas le droit d’accéder aux données sauf en cas de force majeure ou sous mandat d’un juge », explique Gilbert Kallenborn, du site zero1net.com.

Aujourd’hui, on stocke photos et messages tout au long de notre vie, des souvenirs auxquels les héritiers aimeraient avoir accès. Pour y arriver, les sénateurs préparent une nouvelle loi. Un internaute pourra indiquer des directives à suivre après sa mort : une personne de son choix pourra fermer les comptes et récupérer leurs données. A défaut, ses héritiers légaux s’en chargeront. Pour être vraiment sûr de l’avenir de ses données, ne reste qu’une garantie : le testament. La nouvelle loi sera débattue au parlement avant l’été… [Lire la suite]

Réagissez à cet article

Source : *Internet : que deviennent nos données personnelles après notre mort ?*

Apple a essayé d'aider le père de l'enfant mort à récupérer des données

	**Apple a essayé d'aider le père de l'enfant mort à récupérer des données**

Contrairement à ce que disent officiellement ses conditions d'utilisation, Apple accepte bien, au cas par cas, de donner à des vivants l'accès aux données iCloud d'un utilisateur mort.
Il y a ce qu'Apple écrit dans ses conditions d'utilisation, et il y a la pratique, plus humaine. À la suite de la lettre envoyée à Tim Cook par ce père endeuillé, qui souhaitait avoir accès aux données de l'iPhone de son enfant de 13 ans mort d'un cancer des os, CNN rapporte qu'Apple a bien essayé de venir en aide à l'architecte italien Leonardo Fabbretti.

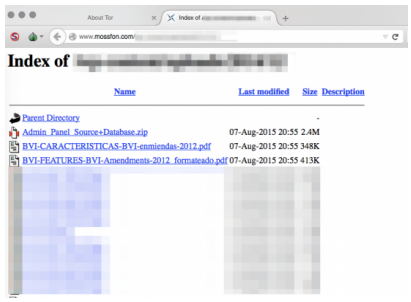
Fidèle à sa position de principe, Apple n'a pas accepté de tenter de casser la protection de l'iPhone 6 de l'enfant, qui aurait permis d'accéder aux données chiffrées contenues sur le téléphone, y compris aux photos et vidéos prises par l'enfant peu avant sa mort.
En revanche, au terme de quelques conversations, les équipes d'Apple ont bien accepté de regarder si des données n'avaient pas été synchronisées avec un cloud iCloud, ce qui aurait permis de les divulguer au père – il n'y avait toutefois aucune sauvegarde.

CE N'EST PAS LE PREMIER ÉCART QU'APPLE ACCEPTE DE RÉALISER, SANS JAMAIS ACCEPTER D'EN FAIRE UNE POLITIQUE GÉNÉRALE
Officiellement, Apple (qui a refusé de commenter) ne réalise pourtant pas ce type d'opération, y compris au bénéfice des parents ou des héritiers d'un défunt. « Dès réception d'une copie d'un certificat de décès, votre Compte pourra être résilié et l'intégralité du Contenu de votre Compte pourra être supprimée », dit simplement le contrat des conditions d'utilisation d'iCloud.
Il indique que le compte iCloud est « incessible et que tous les droits liés à votre identifiant Apple ou Contenu dans le cadre de votre Compte seront résiliés au moment de votre décès ».

Ce n'est pas le premier écart qu'Apple accepte de réaliser, sans jamais accepter d'en faire une politique générale, ni même de reconnaître officiellement des critères d'exceptions. Début 2016, au Canada, une veuve avait déjà obtenu d'Apple qu'il lui transmette les données de son défunt mari. Mais le transfert n'avait pu être obtenu qu'après médiatisation de l'affaire, et intervention d'une association.
L'article de CNN rapporte par ailleurs que Leonardo Fabbretti a pu rencontrer les équipes de l'entreprise israélienne Cellebrite qui propose de l'aider gratuitement à accéder aux données de l'iPhone 6.
Pour le moment, les hackers employés par le FBI pour débloquer l'iPhone 5C du tueur de San Bernardino auraient réussi à extraire le listing des données stockées, mais pas encore les données elles-mêmes. Ils se diraient toutefois « optimistes » sur leurs chances de succès. S'ils parvenaient à débloquer ainsi un iPhone 6, réputé plus sûr, l'annonce viendrait porter un nouveau coup à l'image de forteresse imprenable qu'Apple essaye de donner à l'iPhone… [Lire la suite]

Source : *iCloud : Apple a essayé d'aider le père de l'enfant mort à récupérer des données – Politique – Numerama*

#PanamaPapers : Les failles informatiques de Mossack Fonseca…

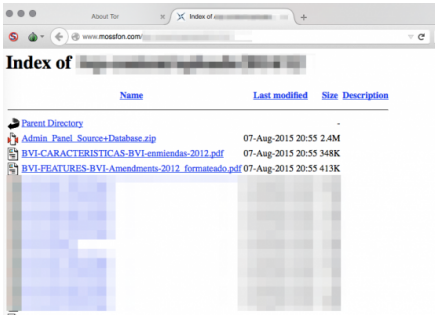


#PanamaPapers : Les failles informatiques de Mossack Fonseca…

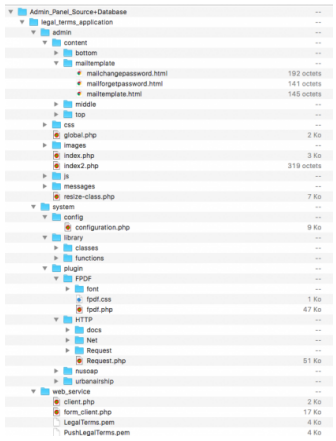
Un internaute vient de nous mettre sous le nez quelques éléments très, très … dur de trouver un qualificatif adapté. On se doutait bien en jetant un bref coup d'œil que le cabinet d'avocats panaméens avait une fâcheuse tendance à faire n'importe quoi, n'importe comment.
On peut également toujours spéculer sur l'origine de la fuite mais là n'est pas le problème, pour tout vous dire, l'origine de la fuite, on s'en fout, c'est la masse de données qui parle, et ce sont ces données qui sont importantes. Nous ne sommes évidemment toujours pas en mesure d'affirmer d'où vient la cette énorme fuite, mais comme nous le sentions, en collectionnant de si mauvaises pratiques, Mossack Fonseca s'assurait à plus ou moins long terme un drame.

Le WTF du jour

Aujourd'hui… la sauvegarde d'une application interne et d'un jeu de données, probablement sensibles, sauvegardés dans un répertoire public du site web vitrine de la société :

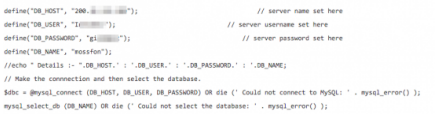


Et l'adresse IP internet du serveur de stockage des documents



La structure de l'application et son fichier de configuration
Et maintenant, admirez la complexité du password :

Rien de tel que de choisir le même mot de passe que le nom d'utilisateur et de base de données… et SURTOUT ne rien chiffrer, des fois qu'on oublierait un mot de passe si complexe.
… et évidemment



La base de données SQL est probablement un jeu de données tests qui est aussi sauvegardée au même endroit :

… oui tout ça accessible depuis un WordPress qui n'est pas à jour, installé sur un Apache mal configuré. …
… [Lire la suite]

Réagissez à cet article

Source : *PanamaPapers : Mossack Fonseca une incroyable bourde ? : Reflets*

Des attaques informatiques par Malwares de plus en plus perfectionnées…

Des attaques informatiques par Malwares de plus en plus perfectionnées…

Les chercheurs de Palo Alto Networks nous mettent en garde contre des diffusions de spam ciblées qui visent à introduire un malware sans fichier via des documents Word en pièce jointe contenant une macro malveillante. Jusqu'il y a peu, cette pratique était connue uniquement chez les trojans bancaires comme Dridex et Dyre, mais il semblerait que cette méthode ancienne, mais toujours efficace, est utilisée pour d'autres malwares comme le voleur d'informations Grabit, l'espion BlackEnergy, le bot Kasidet et le ransomware Locky.

Dans le cas présent, Palo Alto rapporte que les messages malveillants sont diffusés en petites quantités vers des adresses professionnelles d'employés de sociétés américaines, canadiennes et européennes. Ces messages se présentent sous la forme de messages professionnels, contiennent le nom exact du destinataire ainsi que certaines informations sur la société pour laquelle il travaille. Ces petits détails, visiblement obtenus auprès de sources publiques, suffisent pour convaincre le destinataire d'accepter la demande de consulter le document en pièce jointe.
Si l'utilisateur ouvre le fichier malveillant et qu'il accepte l'activation des macros (les macros ne sont pas activées par défaut), il lance l'exécution du fichier powershell.exe masqué selon des arguments particuliers de la ligne de commande. La commande PowerShell exécutée dans ce cas, vise à identifier l'architecture Windows (32 ou 64 bits) et, en fonction du résultat, garantit le téléchargement d'un script PowerShell complémentaire avec code shell.
Cette charge utile permet de réaliser plusieurs vérification sur l'ordinateur infecté, de déterminer à quel point l'environnement d'exécution est hostile (machine virtuelle, bac à sable, débogueur) et de déterminer la valeur de la cible. Sur la base de listes noire et blanche, le malware recherche dans les paramètres réseau de la victime les lignes qui permettent d'identifier le profil de la machine attaquée, ainsi que les noms de quelques sites financiers et les noms Citrix, XenApp, dana-na (dossier partagé avec URL interne créee dans les VPN Juniper) dans les URL mises en cache.
« Il semblerait que ce malware tente dans la mesure du possible d'éviter les ordinateurs des médecins et des réprésentants du monde de l'enseignement. Il se concentre uniquement sur ceux qui réalisent des opérations financières » expliquent les chercheurs. « Au milieu de l'année 2015, des techniques similaires avaient été enregistrées dans la famille de malwares Ursnif. »
Le malware envoie les résultats des vérifications à son centre de commande. Si l'objet attaqué est intéressant pour les individus malintentionnés, le centre de commande envoie un fichier DLL crypté qui est enregistré temporairement sur le disque et qui est utilisé à l'aide de rundll32.exe.
Les chercheurs ont baptisé ce malware PowerSniff. Un des échantillons a même été analysé dans ISC SANS. D'après Palo Alto, l'ampleur de cette campagne malveillante n'est pas encore trop grande : à l'heure actuelle, seuls 1 500 messages de spam environ ont été référencés…. [Lire la suite]

Réagissez à cet article

Source : *Macros malveillantes dans des attaques ciblées – Securelist*

Chrome et Safari perdent face aux hackeurs

Chrome et Safari perdent face aux hackeurs

Comme tous les ans, lors de la conférence CanSecWest, les éditeurs de navigateurs soumettent leurs applications à une série de hackeurs tentant d'y orchestrer leurs attaques.

La communauté des *white hackeurs* joue un rôle fondamentale dans la sécurité des applications. Ces experts tentent effectivement de déceler des failles avant qu'elles ne soient exploitées par des personnes malveillantes. Pour inciter ces travaux, les éditeurs de navigateurs offrent des récompenses tout au long de l'année mais prennent également part à des concours. Le plus connu reste certainement Pwn2Own organisé chaque année.

Après une première journée Chrome, Safari et le lecteur Flash n'ont pas résisté aux *exploits* des hackeurs. Par la même occasion ces vulnérabilités ont permis de mettre à mal les dernières versions de Windows et OS X.

L'équipe 360Vulcan, de la société chinoise Qihoo 360, a réussi à exploiter une faille de Flash Player lui permettant d'exécuter du code à distance avec une autre affectant le kernel de Windows pour obtenir une élévation des droits du système. Ils ont obtenu 80 000 dollars (60 000 pour Flash Player et 20 000 pour Windows).

Cette même équipe a réussi à malmener le navigateur de Google sur le système Windows. Ils ont cette fois combiné 4 vulnérabilités : une au sein de Chrome, deux dans Flash Player et une dans le kernel de Windows. Cet exploit n'a en revanche été récompensé qu'à moitié puisque la faille de Chrome avait précédemment été partagée avec Google… quand bien même 360Vulcan n'était pas au courant. Ils ont toutefois obtenu 52 000 dollars.

De son côté le chercheur coréen JungHoon Lee a obtenir une élévation de droits sur OS X via un hack sur Safari. Il a obtenu 60 000 dollars. L'année dernière, l'homme s'était fait remarquer en obtenant au total 225 000 dollars. Il montrera la semaine prochaine deux autres attaques contre Chrome et Microsoft Edge sur Windows.

Le magazine Computerworld, qui rapporte l'information, ajoute que l'équipe de sécurité de Tencent a obtenu 40 000 dollars en faisant tomber Safari, et 50 000 dollars en présentant une attaque contre Flash Player…. [Lire la suite]

Source : *Pwn2Own : Chrome et Safari tombent face aux hackeurs*