Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

	Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.
Nous connaissions la Fraude au Président, l'arnaque aux faux virements via des informations bancaires soutirées à des entreprises par ruse. Un piège qui fonctionne, malheureusement aussi, sur les locataires de logements sociaux. Les escrocs se font passer pour le bailleur afin de faire modifier les données concernant les virements des loyers.
Aujourd'hui, je viens d'apprendre une nouvelle ruse. Des escrocs se font passer pour les stars de la radio (Manu de NRJ, Camille Combal de Virgin Radio…) en téléphonant et en promettant de l'argent à leurs interlocuteurs. « Un homme dans un soi-disant bureau d'antenne de radio vous dit que vous venez de gagner 2000€ et de doubler vôtre salaire, souligne l'un des témoins de ZATAZ.COM. Il y a beaucoup de bruit derrière. Comme dans un studio de radio ».

Ils visent vos informations bancaires

Une fois l'interlocuteur appâté, l'appel est transféré à une standardiste « On vous demande un numéro de compte bancaire, souligne un autre lecteur de ZATAZ. Ce qui m'a mis la puce à l'oreille est que le soi-disant animateur fusionne plusieurs jeux du 6/9 de NJR et de Virgin Radio. Pour mettre la personne en confiance, on vous ovationne et félicite pour votre prix. »
La question est de savoir maintenant comment les escrocs peuvent avoir le numéro de téléphone portable et l'identité complète (Nom, prénom) des personnes appelées.
Bref, prudence ! Si vous ne vous inscrivez pas à un jeu officiel, il n'y a pas de raison que ce dernier vous téléphone !… [Lire la suite]

Merci à Damien Bancal auteur de cet article

M

Réagissez à cet article

Source : *ZATAZ Informations bancaires : des pirates se font passer pour Manu, Camille Combal – ZATAZ*

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir

---

Un fichier comportant des informations sur plusieurs centaines de millions de comptes MySpace, dont 427 millions de mots de passe, a été mis en vente sur un site spécialisé, a révélé le site LeakedSource. Selon des tests effectués par Motherboard, les mots de passe figurant dans les documents correspondent bien à des comptes existant ou ayant existé.

Selon LeakedSource, les mots de passe de la base de données étaient chiffrés, mais protégés par une technologie aisément contournable avec du temps et de la puissance de calcul. L'intégralité de la base de donnée a été mise en vente pour environ 2 500 euros sur un site spécialisé dans le recel de données volées.

Un milliard d'inscrits

MySpace, considéré il y a dix ans comme le site le plus populaire pour les adolescents et les étudiants, n'est aujourd'hui plus que l'ombre de ce qu'il était. Le service, qui permet de créer sa page personnelle, avait notamment construit sa popularité en attirant de nombreux groupes de musique populaires. Le service existe toujours, et annonçait à la fin de 2015 avoir dépassé le seuil symbolique du milliard d'inscrits au cours de son existence. Les données contenues dans les fichiers volés restent cependant sensibles – de nombreux internautes réutilisent le même mot de passe pour plusieurs applications ou services. Il est conseillé aux utilisateurs ayant détenu ou détenant un compte MySpace de changer leur mot de passe s'ils l'ont réutilisé sur d'autres services… [Lire la suite]

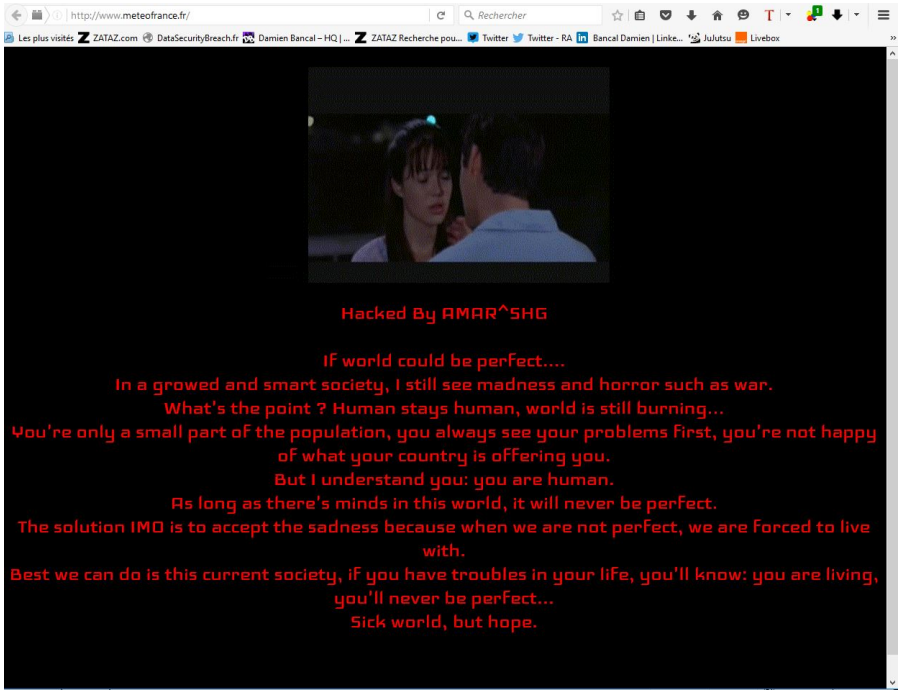
Réagissez à cet article

Source : *Les informations de millions de comptes MySpace en vente en ligne*

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*

Furtim, le malware qui détruit les solutions de sécurité.

	**Furtim, le malware qui détruit les solutions de sécurité**

Alors que de nouveaux malwares sont découverts quasiment chaque jour, voilà que l'un d'entre eux fait beaucoup parler. Il s'agit de Furtim, un #logiciel malveillant qui se caractérise par sa faculté à détruire les solutions de sécurité présentes sur le PC infecté.

Si l'on en croit nos confrères de Silicon, un nouveau malware a été découvert par les équipes d'EnSilo. Comme son nom l'indique, Furtim est capable de passer inaperçu sur les machines qu'il a réussi à infecter.

Probablement crée par des hackers d'Europe de l'Est, ce malware se compose d'un driver qui scanne le PC infecté, d'un module downloader, d'un gestionnaire d'alimentation, d'un voleur de mots de passe et d'un module de communication serveur.

Toutefois, avec une telle composition, impossible de comprendre comment fonctionne réellement ce malware. Pour l'heure, Furtim apparait seulement comme un logiciel malveillant très sophistiqué et capable d'analyser son environnement avant de s'exécuter. Pour cela, il va scanner la machine infectée pour détecter les solutions de sécurité et les outils de filtrage DNS.

Preuve que les pirates ont pensé à tout, Furtim bloque l'accès à de nombreuses sites spécialisés dans la sécurité informatique et à des forums d'aide à la désinfection et désactive les notifications Windows, le gestionnaire des tâches et diverses autres fonctionnalités.

Furtim, un éclaireur en vue de futures attaques

Selon les premières recherches menées par les équipes d'EnSilo, Furtim n'aurait probablement pas vocation à agir seul puisqu'il pourrait bien uniquement jouer un rôle d'éclaireur.

En effet, puisqu'il est capable de déjouer les outils de sécurité, il pourrait être utilisé pour introduire des menaces sur des PC sans que cela ne soit décelable… [Lire la suite]

Réagissez à cet article

Source : *Furtim, le malware qui détruit les solutions de*

sécurité

Auteur : Fabrice Dupuis

L’eau d’une station d’épuration manipulée par des hackers – Sciencesetavenir.fr

L’eau d’une station d’épuration manipulée par des hackers

L'opérateur de télécommunications américain Verizon révèle dans un rapport une cyberattaque ayant touché à la composition et à la distribution d'eau potable d'une station. Le système informatique était perclus de failles.

Le bilan dressé par l'opérateur américain Verizon publié en mars 2016 et consacré aux fuites de données a de quoi faire frémir. Il recense pas moins de cinq cents incidents de cybersécurité dans quarante pays en 2015 (le rapport en anglais ici**).** Parmi eux, l'un attire tout particulièrement l'attention : il concerne la Kemuri Water Company (KWC), une station d'épuration bien réelle mais dont le nom a été changé et le pays d'implantation non divulgué pour éviter de la compromettre. Et pour cause ! Verizon relate la façon dont des hackers ont réussi, très facilement, à manipuler la composition chimique de l'eau qui est redistribuée aux habitants après traitement ! Le tout, sans même en avoir eu l'intention au départ…
L'affaire a été révélée lorsque la société a décidé de faire appel aux équipes chargées du cyber-risque de Verizon pour renforcer son système d'information afin d'anticiper tout problème éventuel. Or, une fois sur place, les experts ont constaté avec stupeur que la station d'épuration était déjà la proie de pirates informatique depuis deux mois ! Et que ses responsables s'en doutaient… Des mouvements suspects de valves et de tuyauteries avaient été remarqués. Beaucoup plus grave ! Les gestionnaires avaient constaté des modifications inexpliquées de dosage dans les produits injectés dans l'eau pour la rendre portable. Sans conséquence désastreuse heureusement…

« Pour tout dire, KWC était un candidat tout trouvé pour une fuite de données. Son interface Internet présentait plusieurs failles à haut risque dont on sait qu'elles sont souvent exploitées» mentionne le rapport de Verizon. Et son système opérationnel, qui commande les applications industrielles (traitement des eaux, gestion du débit), reposait quant à lui sur une infrastructure informatique vieille de plusieurs dizaines d'années.
En outre, de nombreuses fonctions de ce système cohabitaient avec des applications « business » de l'entreprise sur un même et unique serveur, un AS/400 d'IBM, ordinateur commercialisé en… juin 1988. En clair, si des hackers pénétraient le système, ils pouvaient sans peine passer du contrôle du traitement des eaux aux informations financières et aux données de facturation de la compagnie. Et c'est exactement ce qui s'est passé.

L'opérateur liste une série de failles assez confondantes

Au cours de son enquête, Verizon s'est rendu compte que des adresses IP de hackers déjà rencontrées dans trois autres affaires s'étaient connectées au système de paiement en ligne de la KWC, cette interface permettant aux clients d'accéder à leur compte à distance (depuis un ordinateur, un mobile) ; c'est a priori par cette voie que les hackers sont passés, comme d'autres l'ont fait lors du piratage en octobre 2015 de l'hydrolienne Sabella.

2,5 MILLIONS. L'opérateur liste ensuite une série de failles confondantes : l'accès aux données clients n'était protégé que par un login/mot de passe, sans double authentification ; une « *connexion directe par câble* » existait entre l'application de paiement en ligne et l'AS/400, ce dernier ayant un accès ouvert à Internet, avec une adresse IP et des données d'identification administrative disponibles sur le serveur web de paiement, écrites en clair dans un fichier ! Au final, les pirates ont pu sortir du système 2,5 millions de dossiers clients avec leurs données de paiement. Pour l'heure, il semble qu'ils n'en aient pas fait usage.

ALERTE. Mais le plus grave restait à venir. Une fois à l'intérieur du réseau, les pirates se sont en effet rendus compte qu'ils pouvaient accéder aux fonctions opérationnelles.
En se servant des données d'identification administrative, ils ont ainsi pu intervenir sur des fonctions clés : le débit de l'eau potable, son traitement chimique et le temps de remplissage des réserves. A priori – et c'est une chance – les hackers ne semblent pas avoir eu l'intention de nuire et ne poursuivaient pas un but précis, mais les autorités frémissent à l'idée des conséquences dramatiques qu'une telle ingérence aurait pu occasionner. « *Si les attaquants avaient eu un peu plus de temps et avaient été un peu plus familiers du système de contrôle industriel, la KWC et les populations locales auraient pu subir de sérieux dommages* » conclut le rapport… [Lire la suite]

Réagissez à cet article

Source : *L'eau d'une station d'épuration manipulée par des hackers – Sciencesetavenir.fr*

Attaque informatique auprès de plusieurs grands sites de presse suédois

Attaque informatique auprès de plusieurs grands sites de presse suédois

Au moins 7 sites de grands journaux suédois ont été paralysés simultanément samedi 19 mars en raison d'une attaque par déni de service.

« *Il s'agit sans doute de la plus grande attaque jamais commise contre des sites de médias suédois* », estime le *Dagens Nyheter*, l'un des journaux ciblés, pour qui il était « *encore difficile de publier des articles* » quelques heures après le pic de l'attaque.

La police a ouvert une enquête pour tenter d'identifier le ou les auteurs de cette attaque, qualifiée « *de grande ampleur* » par Anders Ahlqvist, spécialiste de la criminalité en ligne au sein du département des opérations nationales suédois, l'organisme consacré au crime organisé.
« *Nous coopérons avec plusieurs partenaires, à la fois en Suède et à l'étranger* », a-t-il précisé dans les colonnes d'*Aftonbladet*, un des titres visés. Anders Ahlqvist laisse entendre que cette attaque aurait transité par la Russie, tout en soulignant que cela ne signifie pas automatiquement qu'elle est issue de ce pays.

Tweets menaçants

Une piste est notamment suivie, celle de l'auteur de deux tweets menaçants relatifs à cette attaque, dont le premier a été publié quelques minutes avant le début de l'offensive. « *C'est ce qui arrive quand on diffuse de la propagande mensongère* », indiquait ce message en anglais, accompagné du mot-clé #offline et de l'adresse du site d'*Aftonbladet*.

Moins d'une heure plus tard, un autre tweet, issu du même compte, renouvelait la menace pour les jours à venir : « *dans les prochains jours, le gouvernement suédois et les médias diffusant de la propagande mensongère seront visés par des attaques* ».

L'auteur de ces tweets, qui utilise un pseudonyme, est inconnu. « *Nous ne savons pas encore qui est derrière les attaques, mais ce qui est arrivé est une menace pour la démocratie* », a déclaré la responsable de l'Association suédoise des éditeurs de presse, Jeanette Gustafsdotter, au *Dagens Nyheter*… [Lire la suite]

Réagissez à cet article

Source : *Plusieurs grands sites de presse suédois victimes d'une attaque informatique*

Cyberprotect | Nouvelles

vagues de rançongiciels : comportement, conseil, solution

Nouvelles vagues de rançongiciels : comportement, conseil, solution

Les actes de cybercriminalités se comptent en nombre et de façon récurrente. Beaucoup d'entreprises, d'administrations ou de commerces sont victimes de cyberattaques. Parmi ces attaques nous trouvons des logiciels malveillants comme les rançongiciels. Pour citer l'ANSSI, « c'est une technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de p

Ces rançongiciel sont de plus en plus présents en ce moment et se renouvellent. Actuellement les alertes portent sur le rançongiciel Locky qui se propage via un e-mail de relance qui contient une facture sous le format Word. Ce serait ce même logiciel qui aurait attaqué il y a quelques jours un centre hospitalier américain, perturbant et endommageant considérablement ses activités.
http://www.lefigaro.fr/secteur/high-tech/2016/02/16/32001-20160216ARTFIG00205-un-hopital-americain-paralyse-par-des-pirates-informatiques.php
http://www.lemonde.fr/pixels/article/2016/02/18/un-hopital-americain-paye-une-rancon-a-des-pirates-informatiques_4867296_4408996.html

Malheureusement ce type de logiciel malveillant n'est pas nouveau et s'inspire même de maliciels déjà connus comme le trojan bancaire Dridex. Plusieurs campagnes de prévention avaient été déployées suite à l'identification de ce maliciel par l'ANSSI notamment, mais également par Cyberprotect, service de contrôle et de prévention en continu de la cybersécurité en entreprise :
https://www.cyberprotect.fr/bulletin-dalerte-Cyberprotect-campagne-courriel-malveillant-trojan-bancaire-dridex/

La principale raison d'être et/ou motivation de ces cyberattaques est d'extorquer de l'argent à leur victime, comme ce fut le cas pour cet hôpital américain cité plus haut qui a dû s'acquitter de 17 000 dollars de rançon pour pouvoir rétablir son activité. Et ce n'est qu'une victime parmi d'autres. La propriété intellectuelle de l'entreprise est également visée par ce type d'attaque.

Se pose maintenant la question : comment se prémunir contre ces cyberattaques ?
Une première chose est de ne pas cliquer sur un lien ou d'ouvrir une pièce jointe dont on ne connait pas la provenance. Maintenir le système d'exploitation ainsi que les antivirus à jour est également une bonne pratique. Toutefois, avec le volume de données échangées, il est devenu plus difficile d'éviter ces attaques dont les techniques d'infection se font toujours plus subtiles et discrètes… [Lire la suite]

Réagissez à cet article

Source : *Cyberprotect | Nouvelles vagues de rançongiciels : comportement, conseil, solution*

Comment une cyberattaque a mis des centrales ukrainiennes hors service

Comment une cyberattaque a mis des centrales ukrainiennes hors service ?

S'il reste encore des zones d'ombres, le doute n'est désormais plus permis : la panne électrique qui a touché l'Ukraine à Noël a bien été causée par une cyberattaque. C'est la première fois qu'un réseau électrique est mis hors service par une attaque informatique. Mais que les opérateurs d'importance critique soient prévenus : ce n'est sûrement pas la dernière.

Le rapport publié jeudi 3 mars par l'équipe de réponse d'urgence pour la sécurité informatique des systèmes de contrôle industriels (ICS-CERT) du département de la Sécurité intérieure des Etats-Unis (DHS) est sans appel : le blackout électrique qu'a connu une partie de l'Ukraine fin 2015 a bien été causé par des hackers. Il confirme ce faisant les conclusions avancées par le SANS ICS (un autre groupe d'experts en cybersécurité industrielle) début janvier, et entérine l'évènement comme étant la première attaque réussie sur un réseau électrique.

UNE SÉRIE D'ATTAQUES SOIGNEUSEMENT PLANIFIÉES

Les intrusions dans le réseau de trois opérateurs énergétiques ont impacté environ 225 000 clients. Bien que le service ait repris quelques jours plus tard, il reste encore limité, même à l'heure actuelle. D'après les témoins interrogés par l'ICS-CERT, les attaques auraient été coordonnées de telle manière qu'elles se sont produites à 30 minutes d'intervalle sur chaque réseau, touchant des installations centrales et régionales. L'opération a très probablement nécessité une longue reconnaissance et étude des victimes.

Lors de l'attaque, plusieurs individus ont pris l'accès des systèmes grâce à des outils de contrôle à distance, soit au niveau de l'OS, soit au niveau des systèmes ICS, le tout via des accès VPN (réseau privé virtuel) dont ils avaient précédemment obtenu les codes d'accès. Une fois l'attaque effectuée, le malware KillDisk a été utilisé pour effacer les fichiers compromis et corrompre les secteurs de démarrage des machines ou les firmwares des équipements pour les rendre inopérants. Les attaquants auraient également surchargé les centres d'appels des énergéticiens pour les empêcher de réagir immédiatement à l'évènement. De plus, trois autres organisations en charge d'infrastructures critiques ont aussi été pénétrées, mais sans impact direct sur leurs opérations.

DES ZONES D'OMBRES PERSISTENT

Malgré ces nouvelles informations, le rôle exact qu'a joué le malware BlackEnergy dans l'attaque n'est toujours pas connu. Ce malware, connu du milieu de la cybersécurité depuis 2007, a été retrouvé sur trois des systèmes impactés. Originellement présenté comme la potentielle arme du crime, il est possible qu'il n'ait en fait été utilisé que pour obtenir des codes d'accès. Il est aussi bon de noter que le rapport de l'ICS-CERT se base uniquement sur les témoignages du personnel IT de six organisations ukrainiennes qui ont été directement témoins des évènements, et pas sur une analyse technique du code ou du matériel impliqué dans l'incident.

Ces considérations mises à part, le fait que différents groupes d'experts soient d'accord sur l'origine cybercriminelle de la panne constitue une ultime (et sinistre) mise en garde à l'égard des opérateurs d'importance vitale (OIV). Car ces incidents ne font malheureusement que commencer. … [Lire la suite]

Réagissez à cet article

Source : *Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service*

Alerte vigilance – Ransomware Lockyx

Alerte vigilance – #Ransomware Lockyx

Bonjour, Une vague d'attaques du ransomware Locky touche actuellement de nombreuses entreprises dans le monde et depuis peu en France.Voici nos conseils pour se protéger contre cette nouvelle menace :

CONSEIL N°1 : VIGILANCE UTILISATEUR

Informez vos collaborateurs de l'importance de ne pas ouvrir la pièce jointe d'un email envoyé par un expéditeur inconnu. Soyez très vigilant notamment avec les pièces jointes .zip, .doc, .xls : sources de propagation de Locky.

Les sensibiliser à l'utilisation des macros et/ou les désactiver, source de propagation de Locky.

CONSEIL N°2 : SOLUTION DE PRA

Assurez-vous que vos machines sont correctement sauvegardées, et les images externalisées pour une restauration rapide en cas d'attaque.

Les équipes ESET sont mobilisées à l'heure actuelle pour vous apporter une solution rapide et continue contre ce ransomware et ses multiples variantes quotidiennes.

Note : si vos machines sont déjà infectées, isolez-les des autres, initiez leur restauration et lancez une analyse complète de vos systèmes.

Cordialement,

L'équipe ESET

… [Lire la suite]

Réagissez à cet article

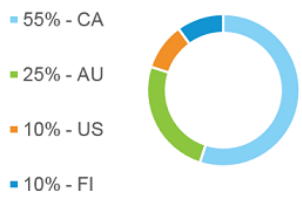
Source : *Alerte vigilance – Ransomware Lockyx*

Le cheval de Troie Ramnit refait surface

	Le cheval de Troie Ramnit refait surface

---

Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle Une première pour un botnet bancaire selon IBM



En février dernier, suite à une opération menée par plusieurs États ainsi que des acteurs privés (parmi lesquels Microsoft, Symantec et AnubisNetworks) qui a été coordonnée par le centre de lutte contre la cybercriminalité d'Europol, un réseau de serveurs de contrôle du botnet Ramnit a été démantelé. Trois cents domaines internet exploités par les pirates ont également été redirigés.
Détecté pour la première fois en 2010, le cheval de Troie Ramnit permettrait de gagner un accès distant aux ordinateurs Windows infectés et de subtiliser par la suite des données sensibles, comme des informations bancaires. Wil van Gemert, le directeur des opérations d'Europol, a salué le succès de l'opération : « cette opération réussie illustre l'importance pour les forces de l'ordre internationales de travailler de concert avec l'industrie privée afin de lutter contre la menace globale du cybercrime ».
Seulement, les chercheurs d'IBM ont mis la main sur une variante du cheval de Troie qui se base sur une infrastructure C&C différente de son prédécesseur et emploie un fichier de configuration plus court ainsi qu'un schéma d'injection web différent pour infecter les victimes. Plus de la moitié des infections a été observée au Canada. En seconde position sur la liste des pays les plus affectés viennent l'Australie qui compte à elle seule une infection sur quatre, puis les États-Unis.
Selon les chercheurs de la X-Force d'IBM, il semblerait que ce soit la première fois qu'un botnet de fraude bancaire refasse surface, ce qui a aiguisé leur curiosité puisque, jusqu'à présent, c'étaient plutôt les botnets de spams qui étaient souvent ramenés en circulation, les cybercriminels derrière les botnets de fraude bancaire préférant se contenter de l'argent déjà collecté et du fait qu'ils n'aient pas été arrêtés.
Les experts expliquent que « le cheval de Troie arborait un fichier de configuration lourd avec des déclencheurs d'URL qui lui indiquaient vers quelle banque, quelle transaction et quels sites de réseau social se tourner pour collecter des informations d'identification ». La configuration de Ramnit est orientée pour tenir les victimes éloignées d'une liste exhaustive d'outils de scans en ligne, de sites web d'antivirus, des sites d'information sur le cybercrime, mais également des blogs de sécurité. « Dans son ancienne configuration, la seule utilisation des mots « cybercriminalité » ou « police » de la part des victimes suffisait à déclencher un effet de redirection ».
Une autre trace laissée par les anciennes configurations est la liste relativement importante de sites de recrutements récoltant les informations d'identification, afin de viser ceux qui sont à la recherche d'un emploi et de les recruter. « Pour les victimes, cela pouvait être une lame à double tranchant étant donné que les opérateurs Ramnit pouvaient également obtenir toutes les informations qu'elles ont mises sur leur CV professionnel ».
La X-Force Threat Intelligence d'IBM n'a pas eu vent du fait que le code source de Ramnit ait été vendu ouvertement, partagé avec d'autres groupes de cybercriminels ou sur les forums dans le marché noir. Aussi, ils pensent qu'il y a de fortes chances qu'il s'agisse là du même groupe d'individus qui a remis cette nouvelle version en activité.

Réagissez à cet article

Source : *Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle, une première pour un botnet bancaire selon IBM*