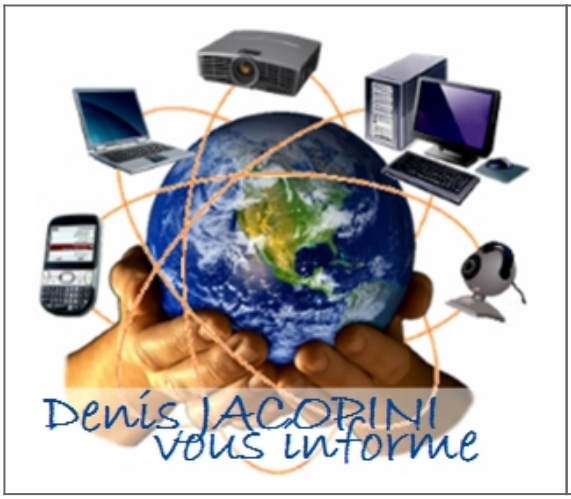
Les offres d’essai Cloud pour avoir un superordinateur gratuit ! Une idée qui va faire des eMules…



Les offres d’essai Cloud pour avoir un superordinateur gratuit ! Une idée qui va faire des eMules…

Un botnet gratuit ? C’est l’expérimentation menée par deux chercheurs américains, Rob Ragan et Oscar Salazar. Plutôt que de se fatiguer à infecter des centaines d’ordinateurs appartenant à des utilisateurs peu soucieux de leur sécurité, ils ont décidé de se tourner vers les services Cloud qui proposent généralement tous un service gratuit à l’essai.

À l’aide d’un script, ils ont donc généré des comptes d’essai sur plus de 150 services Cloud tels que Amazon Web Service, puis en utilisant Python Fabric, une librairie permettant de gérer de multiples scripts pythons, ils se sont amusés à utiliser la puissance de calcul ainsi accumulée pour plusieurs expériences.

Un déficit de sécurité

Ils ont ainsi commencé par miner du Litecoin, une cryptomonnaie reposant sur un principe similaire à celui du Bitcoin. Après un test de plusieurs heures, les chercheurs sont parvenus à dégager une rapide estimation de ce que leur

botnet Cloud pourrait leur rapporter : environ 1750 dollars par semaine. « On a construit un superordinateur sans lâcher un centime » explique Rob Ragan dans les colonnes de Wired « Et en s'épargnant même la facture d'électricité ! » précise-t-il.

Pour tester les capacités de ces fournisseurs de service, les deux chercheurs expliquent avoir laissé une partie de leurs scripts dédiés au minage de Litecoin tourner pendant deux semaines, sans qu'ils ne soient inquiétés. Autre utilisation également envisagée : le DDos, qui selon leurs estimations équivaudrait à une attaque provenant lancée depuis un botnet de 20.000 ordinateurs

Une dérive inquiétante

Un botnet basé sur le Cloud, cela n'est pas réellement nouveau : des cas similaires avaient émergés, notamment autour de l'utilisation du malware Zeus. Mais le but de l'expérience est ailleurs : d'une part, les deux chercheurs veulent avant tout alerter les entreprises qui proposent ce type de service sur les risques auxquels ils s'exposent en proposant ainsi des offres gratuites et ne nécessitant pas d'authentification forte.

Mais surtout, cela pose la question de la légalité de ce type de botnet : certes, les chercheurs sont passés outre quelques termes des CGV de ces différents services, mais le risque encouru est nettement moindre qu'un botnet reposant sur des ordinateurs infectés.

Lors d'une conférence à l'événement Black Hat qui aura lieu début aout, les chercheurs détailleront avec plus de précisions les outils et méthodes utilisées pour construire ce superordinateur à peu de frais.

Cet article vous à plu ? Laissez-nous un commentaire (Source

de progrès)

Références :
http://www.zdnet.fr/actualites/un-superordinateur-base-sur-des-offres-d-essai-cloud-39804301.htm

---

Vol de données et racket auprès de la BCE (Banque centrale européenne)

Vol de données et racket auprès de la BCE (Banque centrale européenne)

Par le biais d'un email anonyme, un pirate a tenté d'extorquer de l'argent à la BCE en échange de données dérobées dans une base de données liée au site Web de la Banque centrale. Les données de marché sensibles n'ont pas été compromises.

Dans un communiqué, la BCE, la Banque centrale européenne, responsable de la monnaie unique au sein de l'UE, alerte sur le vol d'une base de données de contacts. Selon La Tribune, ce sont potentiellement 20.000 personnes dont les données pourraient être ainsi exposées.

La BCE précise que seules des informations de contacts, dont des adresses email, des noms et coordonnées, ont été dérobées dans cette base de données isolée de son système interne. « Aucune donnée sensible de marché n'a été compromise » assure ainsi la Banque centrale.

Des données partiellement chiffrées

Cette base de données est attachée au site Web de la BCE et contient l'identité des personnes inscrites à des évènements organisés par la Banque, dont ses conférences. Celle-ci précise que seule une partie des données volées sont chiffrées – la nature de ce chiffrement n'est pas mentionnée.

La BCE contacte actuellement l'ensemble des personnes dont les données pourraient ainsi avoir été compromises et a, par précaution, réinitialisé l'ensemble des mots de passe. Une vulnérabilité, non spécifiée mais corrigée selon la BCE, serait à l'origine du vol.

Et comment la Banque centrale a-t-il pris connaissance de cette intrusion informatique ? Grâce à un email anonyme, n'émanant toutefois pas d'un bienfaiteur. Au contraire, l'auteur du message a exigé de l'argent en échange des données subtilisées. La justice allemande – le siège de la BCE est à Francfort – a été saisie et une enquête de police a été ouverte.

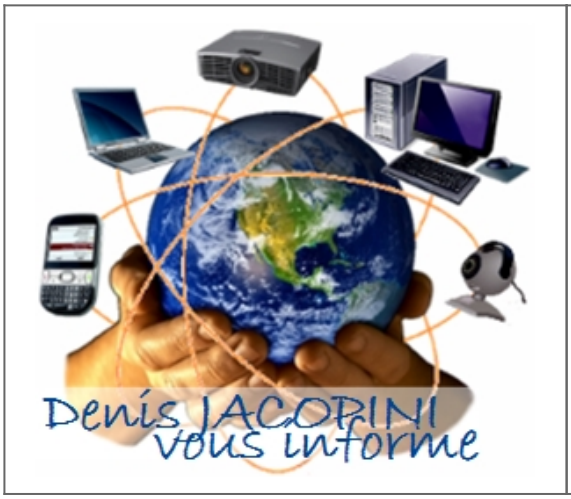
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.zdnet.fr/actualites/vol-de-donnees-et-racket-aupres

-de-la-banque-centrale-europeenne-39804225.htm

Les clients de 12 banques suisses attaqués par des cybercriminels



Les clients de 12 banques suisses attaqués par des cybercriminels

Des pirates informatiques se sont lancés, depuis peu, dans une attaque d'envergure contre les comptes e-banking de douze banques suisses. Leurs méthodes sont perfides et laissent peu de traces, avertit Switch.

Le virus, de type cheval de Troie, a été nommé Retefe, a indiqué mardi Serge Droz, expert en sécurité auprès de l'organisme qui administre les noms de domaines en Suisse. Il confirmait une information parue sur le site Internet de la Handelszeitung. C'est l'entreprise de sécurité informatique Trend Mikro qui a rendu publique l'information sur l'attaque.

Le client de banque ouvre un spam – un courrier électronique indésirable – qui libère le virus. Le programme malicieux

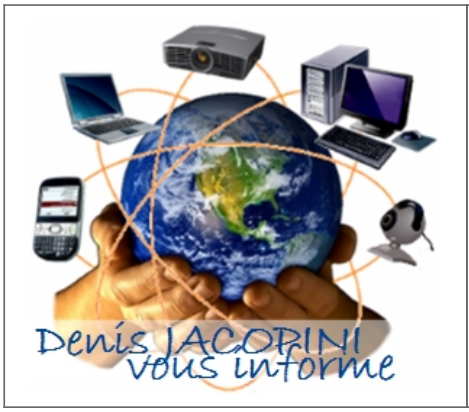
s’efface, une fois que l’infection a réussi. Aussitôt que le client ouvre une session e-banking, il est redirigé sur un mauvais serveur, sur lequel apparaît une copie de page Internet de sa banque. Le client entre alors ses informations de sécurité, qui sont désormais en main des malfaiteurs.

Lire la suite…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lematin.ch/economie/hackers-s-attaquent-clients-12-banques-suisses/story/16520131

Cybercriminalité : La Tunisie dispose de compétences hautement qualifiées pour lutter contre le terrorisme



Cybercriminalité : La Tunisie dispose de compétences hautement qualifiées pour lutter contre le terrorisme

La Tunisie dispose de compétences hautement qualifiées dans le domaine des technologies de l'information et de la communication (TIC) capables de protéger l'espace cybernétique de la Tunisie et de lutter contre la cybercriminalité et contre le terrorisme et la violence ». C'est en tout cas ce que vient de déclarer à l'agence TAP, le ministre de l'Enseignement supérieur, de la Recherche scientifique et des TIC, Taoufik Jelassi, en marge de la conférence participative sur la réforme de l'enseignement supérieur et l'employabilité, organisée dans la soirée du dimanche 20 juillet à Monastir.

M. Jelassi a soutenu que la sécurité informatique et cybernétique est une priorité nationale, notamment au cours de cette étape, ajoutant qu'il a été convenu, au terme d'une réunion, la semaine dernière avec des responsables de la sécurité de l'espace cybernétique, de soutenir davantage l'Agence technique des télécommunications (ATT). « L'agence assurera l'appui technique des investigations judiciaires dans le domaine de la cybercriminalité et appuiera les efforts des autorités judiciaires et sécuritaires dans la protection du pays », a-t-il dit.

Le ministre des TIC a par ailleurs indiqué que l'Agence technique des télécommunications veille sur la protection des citoyens et des intérêts supérieurs du pays 24h/24 et 7jours/7, conformément à la loi et sous contrôle judiciaire.

A noter que l'agence technique des télécommunications a été créée en vertu du décret 4506 en date du 6 novembre 2013..

Cet article vous à plu ? Laissez-nous un commentaire (Source

de progrès)

Références :
http://www.webmanagercenter.com/actualite/technologie/2014/07/21/152736/terrorisme-la-tunisie-dispose-de-competences-hautement-qualifiees-pour-lutter-contre-le-terrorisme

---

Le «Wall Street Journal» victime d'une cyberattaque – News High-Tech: Web – 24heures.ch

Le «Wall Street Journal» victime d'une cyberattaque

Le «Wall Street Journal» a annoncé dans la nuit de mardi avoir été victime d'une cyberattaque par un hacker qui proposait de vendre des codes d'accès au serveur du journal économique américain.

Dans son édition en ligne, le quotidien des affaires Wall Street Journal, indique que son service infographie a été «piraté par des tierces parties» tout en affirmant qu'aucun «dommage» n'a pour l'heure été constaté.

«A ce stade, nous ne voyons aucune preuve d'un quelconque impact sur les clients de Dow Jones ou sur les informations personnelles des clients», a assuré une porte-parole du journal, citée dans l'article.

Aucune altération sur des infographies (chartes, tableaux…) n'a par ailleurs été relevée mais le système est encore «en cours d'examen», assure le journal, précisant que plusieurs ordinateurs ont été mis hors ligne afin d'«isoler» les attaques.

Le Wall Street Journal (WSJ) dit avoir révélé cette intrusion informatique après sa «revendication» sur Twitter par un hacker qui offrait, moyennant finances, des informations de clients mais également des données permettant d'accéder au serveur du journal.

Selon Andrew Komarov, l'expert en cybersécurité qui a alerté le quotidien, un tel accès permettrait de «modifier des articles, d »ajouter des nouveaux contenus (…) et de supprimer des comptes d'utilisateurs».

Selon le WSJ, Andrew Komarov, patron de la firme californienne IntelCrawler, est sur les traces de ce pirate informatique qui s'est successivement fait connaître sous le pseudonyme de Rev0lver et de Worm et qui a fondé un marché noir des «failles informatiques» baptisé Worm.in.

Les Etats-Unis ont à plusieurs reprises alerté sur les dangers de la cybercriminalité et de son impact économique. Mi-juillet, le secrétaire au Trésor américain Jacob Lew avait ainsi affirmé qu'une cyberattaque «réussie» pourrait menacer la stabilité financière du pays.

Lire

Piratage informatique d'une banque : 500 000 euros dérobés aux clients d'une

banque européenne

	Piratage informatique d’une banque : 500 000 euros dérobés aux clients d’une banque européenne *Une banque européenne s’est fait dérober 500 000 euros en l’espace d’une semaine suite à une fraude réalisée à l’aide d’un cheval de Troie.*

Piratage informatique d’une banque : 500 000 euros dérobés aux clients d’une banque européenne

Une banque européenne s’est fait dérober 500 000 euros en l’espace d’une semaine suite à une fraude réalisée à l’aide d’un cheval de Troie.

500 000 euros en 7 jours, tel est le butin que des cybercriminels ont réussi à subtiliser à une grande banque européenne dont l’identité n’est pas connue. C’est l’éditeur Kaspersky qui a découvert la fraude qui aurait eu cours entre le 13 et le 20 janvier.

Un cheval de Troie, surnommé Luuuk, a servi à collecter les données bancaires de quelque 190 clients basés en Italie et en Turquie. Le trojan a semble-t-il été injecté via une attaque de type « man-in-the-browser » afin de pouvoir déclencher des transactions en arrière-plan à l’insu des victimes. Les sommes étaient envoyées sur des comptes fictifs créés à cet effet puis l’argent était ensuite retiré en espèces à des distributeurs.

Deux jours après avoir découvert un serveur de commande et de contrôle, Kaspersky a averti la banque concernée. Mais les cybercriminels avaient eu le temps d’effacer toute trace pouvant permettre de remonter jusqu’à eux, ce qui laisse penser que cette fraude est peut-être toujours en cours. (Eureka Presse)

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Références :

http://www.zdnet.fr/actualites/cyberfraude-500-000-euros-derobes-aux-clients-d-une-banque-europeenne-39803001.htm

---

Alerte vigilance Simplocker – L'ère des malwares 2.0 sur les mobiles a sonné : Simplocker un cryptolocker sur Android

Alerte vigilance – Simplocker un cryptolocker sur Android

Les experts savaient depuis un moment que les cybercriminels tenteraient de s'attaquer à la flotte mobile, une cible très en vogue dans un monde où le nombre d'utilisateurs frôle les 7 milliards en 2014

Alerte HeartBleed Acte II – Nom de code Cupid

Alerte HeartBleed Acte II – Nom de code Cupid
Cupid, nouvel exploit qui utilise la Heartbleed, ébranle les connexions Wi-Fi.

Pour l'instant, à l'état de preuve de concept, cette faille n'est sans doute que le premier écho du coup de tonnerre qui a fait trembler le Net en avril dernier.

Détection de virus en ligne, Antimalwares et Antivirus Online

Ce n'est pas parce que votre ordinateur fonctionne correctement qu'il n'est pas infecté.

En effet, que ça soit dans les ordinateurs, les téléphones portables, les smartphones et même les tablettes, de plus en plus de virus ou de logiciels espions fonctionnent dans l'ombre. Leur principale fonction est d'espionner ce que vous tapez au clavier ou ce que vos logiciels envoient sur le réseau interne, wifi ou internet.

Ces logiciels recherchent, mémorisent et peuvent envoyer à un serveur pour un usage ultérieur :

Mots de passe saisis au clavier, envoyés sur le réseau filaire ou Wifi
Numéros de carte bancaire saisis au clavier, envoyés sur le réseau filaire ou Wifi
Carnet d’adresse pour contaminer vos contacts en utilisant votre identification pour tromper la confiance des interlocuteurs
Besoin de détecter si votre ordinateur est infecté par un virus sans installer d’antivirus ou désinstaller votre antivirus actuel ?

Une victime du virus Windigo témoigne

Le 19 mars dernier, je vous informais au travers d’un article (http://www.lenetexpert.fr/alerte-virus-windigo) de la découverte du virus Windigo par une équipe de spécialistes en sécurité.

Quelques semaines après les premières attaques, le gérant d’une entreprise internationale touché par ce virus témoigne sur les dégâts qu’il a subit.