Une victime des pirates informatique guidée en ligne pour payer la rançon

Une victime des pirates informatique guidée en ligne pour payer la rançon

Témoignage d'un client :
L'informaticien Robert Hyppolite a dû payer une rançon aux pirates de SynoLocker… qui lui ont offert une assistance en ligne.

«Imaginez une entreprise de conseil juridique qui perd tous ses documents: mémoires, pièces, scans.
C'est un énorme coup dur. Sans les pièces, il y a de quoi perdre un procès!» Robert Hyppolite travaille depuis trente ans dans l'informatique à Genève. Il a notamment fondé l'entreprise Infologo, rachetée par VTX. Depuis 2007, il propose à ses clients le produit Synology, un système d'exploitation pour les serveurs de stockage en réseau. Des pirates ont élaboré un virus baptisé «SynoLocker TM» (sic) qui exploite la faille de sécurité de certaines anciennes versions du système. La police genevoise prend connaissance de cinq à dix nouveaux cas chaque semaine. Sur les trente clients de Robert Hyppolite équipés de Synology, deux ont été infectés et leurs sauvegardes ont également été atteintes. L'informaticien a dû payer une rançon en urgence dans la nuit de mardi à mercredi: l'un des deux clients touchés demandait une solution immédiate.

«La première difficulté était qu'il fallait payer en bitcoins, explique-il. On ne peut pas en acheter du jour au lendemain: il faut ouvrir un compte, donner son identité, faire un virement… Pour gagner du temps, je suis allé au distributeur de bitcoins des Pâquis (lire: Le bitcoin gagne l'économie réelle à Genève). La somme exigée par les pirates est de 0,6 bitcoin, ce qui correspondait à 650 francs, mais le cours est très fluctuant et dépend des pays et des plates-formes. »

Contre paiement de la rançon, un code permet normalement de décrypter les données et de retrouver ses fichiers. Sauf que l'aventure ne s'est pas arrêtée là. «Le virus chiffre les fichiers avec une clé réputée inviolable (2048 bits), ce qui les rend inutilisable. Ils restent normalement visibles avec leur nom correct. Mais le système de cette entreprise n'a pas réagi comme les autres et a été entièrement corrompu.» Conséquence: il a fallu réinstaller le système d'exploitation Synology, puis… réinstaller le virus, pour pouvoir permettre le décryptage des fichiers au moyen du code.

Les pirates répondent en ligne
Comment installer soi-même un virus? L'informaticien fait une curieuse découverte: «Sur le site Internet des ravisseurs, on trouve un onglet «support»… avec un chat en direct. Ils m'ont répondu très poliment: «Cher Monsieur, nous avons pris note de votre problème…» J'avais l'impression de parler à l'assistance en ligne d'une compagnie officielle! Une heure après, ils m'envoyaient une marche à suivre: il fallait entrer manuellement des instructions en ligne de commande. Tout a fonctionné sauf la dernière opération. A nouveau, le support informatique des pirates m'a répondu: leur dernière instruction contenait une erreur. J'ai ensuite pu entrer le code et tout est revenu à la normale.»
Une sauvegarde sur un serveur ou un disque dur séparé aurait permis de récupérer les données sans être rançonné. «Je préconise toujours cette mesure, mais dès qu'il faut s'équiper, il n'y a plus personne, regrette l'informaticien. Les clients pensent qu'on veut leur vendre des produits ou services inutiles, sauf ceux qui ont déjà vécu un sinistre…»
L'entreprise Synology souffrira-t-elle du virus SynoLocker? «Oui, mais ce sera vite oublié, estime Robert Hyppolite. J'ai vécu la mise à jour de l'antivirus Avast qui rendait les machines inutilisables… Pendant une année, leurs ventes ont baissé. Depuis, ils se sont rattrapés.» L'informaticien devra encore résoudre le problème du second client pris en otage. L'occasion, peut-être, d'une nouvelle discussion avec des ravisseurs informatiques très organisés et qui semblent prendre soin de leurs «clients».
Note: en cas d'infection avec SynoLocker, la police recommande de ne pas s'acquitter de la rançon et de réinitialiser les disques durs. Dans une note publiée ce jeudi, la Confédération émet des recommandations contre SynoLocker et conseille un outil de décryptage gratuit contre un virus au fonctionnement semblable, Cryptolocker.
Lire la suite…
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.tdg.ch/high-tech/hard-software/Des-pirates-informatiques-guident-leurs-victimes-en-ligne/story/19256356

1,2 milliard d’identifiants volés par des pirates russes – Vol d’identifiants au dessus d’un nid de coucou

1,2 milliard d’identifiants volés par des pirates russes – Vol d’identifiants au dessus d’un nid de coucou

Le vol d'identifiants est passé à l'échelle supérieure avec la découverte que des cybercriminels russes avaient détourné 1,2 milliard de noms et mots de passe. A ce niveau, cela touche tout le monde, estime la firme de sécurité Hold Security qui a découvert ce groupe de pirates qu'il désigne sous le nom de CyberVor.
En Russie, des criminels ont constitué une énorme base constituée de 1,2 milliard de noms d'utilisateurs et de mots de passe volés, auxquels s'ajoutent 500 millions d'adresses e-mail, selon Hold Security, une société américaine spécialisée sur la sécurité Internet. Il s'agit probablement de la plus grosse base d'identifiants dérobés, récupérés d'attaques conduites dans tous les coins du web et qui ont touché environ 420 000 sites. « Jusqu'à présent, nous étions stupéfaits lorsque 10 000 mots de passe avaient été compromis, maintenant nous en sommes au stade du vol massif », a confié Alex Holden, fondateur de Hold Security, à nos confrères d'IDG News Service. Sa société n'a pas communiqué le nom des sites qui avaient été attaqués, invoquant des accords de confidentialité avec ses clients, mais elle a indiqué que cela incluait des familles et de petits sites web.

Le New York Times, qui fut le premier à rapporter ce vol, s'est adressé à un expert en sécurité indépendant pour vérifier que les données volées étaient authentiques. L'ampleur de la base constituée semble éclipser les précédentes découvertes de données compromises. Par comparaison, le vol subi par Target (révélé en janvier dernier) a affecté 40 millions de cartes de débit et 70 millions d'informations personnelles. C'est, en matière de détournement d'identifiants, l'un des faits de cybercriminalité les plus importants constatés jusqu'à présent et qui porte ce type de délit à un niveau supérieur. « Ces gens n'ont rien fait de nouveau ni d'innovant », constate Alex Holden. « Ils l'ont juste fait mieux et à un niveau de masse ce qui touche absolument tout le monde ».

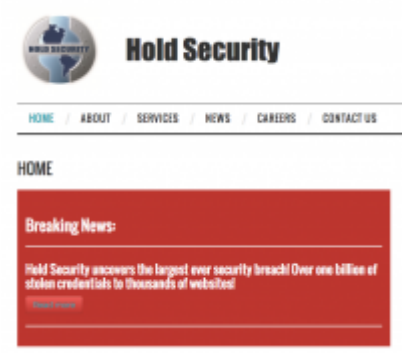
Le gang CyberVor est constitué d'une douzaine de jeunes gens
Le groupe derrière l'attaque semble être basé dans le centre-sud de la Russie, a indiqué Alex Holden au New York Times. Selon les informations qu'il a communiquées au quotidien américain, il s'agit d'une douzaine de personnes d'une vingtaine d'années qui ne semblent pas avoir de liens avec le gouvernement. Avec des serveurs basés en Russie, le groupe a étendu ses activités cette année, probablement après avoir été en contact avec une organisation plus importante. Hold Security a dénommé le gang CyberVor d'après le mot russe « vor » (voleur). La société a indiqué qu'elle fournirait un service pour permettre aux utilisateurs de vérifier si leurs identifiants figurent parmi ceux qui ont été volés. L'information sera disponible dans deux mois environ. Le pré-enregistrement pour y accéder est possible dès maintenant.
Ce détournement massif de noms d'utilisateurs et de mots de passe met une fois de plus en lumière le peu de sécurité apportée par ces méthodes d'authentification, en particulier si les personnes se servent des mêmes noms et passwords pour plusieurs sites. Le recours à une méthode d'authentification à deux niveaux (avec envoi d'un code par SMS) renforce la sécurité mais ne constitue pas une garantie comme un utilisateur de PayPal vient tout juste de le démontrer. Après avoir, sans succès, alerté PayPal sur cette faille, il a expliqué comment cette fonction pouvait, en l'occurrence, être détournée via une connexion eBay.
Article de Martyn Williams / IDG News Service (adapté par Maryse Gros)

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

Références :
http://www.lemondeinformatique.fr/actualites/lire-des-pirates-russes-ont-amasse-1-2-milliard-d-identifiants-58272.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Un milliards de mots de passe volés par un gang de pirates…



Un milliards de mots de passe volés par un gang de pirates…

Un petit groupe de cybercriminels a employé un botnet pour infiltrer des dizaines des milliers de sites web et récupérer une quantité gigantesque de données sensibles. Mais la firme qui a fait cette découverte en profite pour faire un formidable coup de com' et vendre un service derrière. Bizarre.La page d'accueil alarmiste de Hold Security, entreprise qui a révélé le piratage… Et qui propose une solution payante pour tenter d'y remédier.
Que vous soyez un expert en informatique ou un technophobe, à partir du moment où vous avez des données quelque part sur le web, vous pouvez être affecté par cette brèche. On ne vous a pas nécessairement volé directement. Vos données ont peut être été subtilisées à des services ou des fournisseurs auxquels vous avez confié des informations personnelles, à votre employeur, même à vos amis ou votre famille ». Voilà le discours flippant de Hold Security pour décrire la gigantesque collection de données personnelles volées que cette entreprise de sécurité a mis au jour.
Les chiffres présentés donnent en effet le tournis : d'après Hold Security, un gang d'une douzaine de hackers russes baptisé CyberVor aurait donc récupéré pas moins de 4,5 milliards de combinaisons de mots de passe et de noms d'utilisateurs. En omettant les doublons, CyberVor aurait accès à plus d'un milliard de comptes sur des milliers de sites différents, qui seraient rattachés à 500 millions d'adresses e-mail. Le hack du siècle, en somme.
Pour voler autant d'informations sensibles, CyberVor aurait usé de multiples sources et techniques, mais aurait surtout profité des services d'un botnet (un réseau de PC infectés par un logiciel malveillant) « qui a profité des ordinateurs des victimes pour identifier des vulnérabilités SQL sur les sites qu'ils visitaient. » Les membres de CyberVor auraient de cette manière identifié plus de 400 000 sites web vulnérables, qu'ils ont ensuite attaqué pour voler leur bases de données d'utilisateurs.

Des détails qui clochent
Sauf qu'il y a quelques petits détails qui clochent dans cette histoire. A commencer par le fait que Hold Security profite de cette annonce hallucinante pour tenter de s'enrichir immédiatement, en misant sur la peur du hacker qu'il a généré. En gros, la firme propose aux entreprises et aux particuliers de se préinscrire à un service –payant même s'il y a un essai gratuit- qui leur permettra notamment de savoir si oui ou non ils sont concernés par cette fuite de données. Et ce n'est pas donné : comptez 120 dollars par mois si vous êtes une entreprise.
D'autre part, Hold Security se refuse à donner le moindre nom de site dont la base a été piratée. Ce peut être compréhensible : son patron Alex Holden l'explique dans le New York Times, il ne souhaite pas révéler le nom des victimes pour des raisons de confidentialité. Il y aurait pourtant des entreprises du Fortune 500 selon lui dans le lot.
Mais comme le fait remarquer Forbes, il semble pour le moins étonnant (mais pas totalement impossible) que de si grandes entreprises se soient fait berner par une injection SQL, une technique très connue des hackers… et des experts en sécurité qui protègent les sites importants de telles attaques.

Des infos de piètre qualité ?
Il y a aussi de nombreuses informations qui manquent, dans la description de Hold Security. Quels botnets ont été utilisés ? Comment le malware a-t-il été inoculé dans la machine des victimes ? Et surtout pourquoi, comme l'indique le New York Times, le gang se contente-t-il d'utiliser pour l'instant leur fabuleuse base de données pour… envoyer du spam sur les réseaux sociaux, alors qu'ils pourraient à priori faire bien plus de mal ?
En réalité, il se peut que les milliards de mots de passe collectés par CyberVor étaient déjà disponibles sur le web underground depuis bien longtemps. Hold Security l'avoue sur son site : « Au départ, le gang a acquis des bases de données d'identifiants sur le marché noir ». Une pratique fort courante chez les cybercriminels, mais qui ne repose pas sur le moindre hack : il suffit de payer. Il est fort possible que ces « collectionneurs » aient au fil du temps accumulé un nombre de données incroyable, mais pas forcément « fraîches » et donc de piètre qualité. Il se peut aussi que la technique de l'audit d'un site par un botnet ait été fructueuse… Sur des sites de moindre envergure, voire des sites perso, mal sécurisés, qui n'ont pas fourni à Cybervor de quoi faire autre chose que du spam sur Twitter.
Quoiqu'il en soit, l'annonce de Hold Security vous donne une excellente excuse pour changer dès aujourd'hui vos mots de passe, ça ne fait jamais de mal !

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

Références :
http://www.01net.com/editorial/624854/comment-un-gang-de-pirates-a-t-il-pu-voler-plus-d-un-milliard-de-mots-de-passe/#?xtor=EPR-1-NL-01net-Actus-20140806

Un logiciel d'extorsion (ransomware) utilise un simple fichier batch

Un logiciel d'extorsion (ransomware) utilise un simple fichier batch
Informatique

Des chercheurs de Symantec ont récemment identifié une menace d'extorsion qui fonctionne avec un script et une ligne de commande en utilisant le programme de chiffrement Open Source

GnuPG.

Pour extorquer de l'argent aux utilisateurs, des pirates ont mis au point un nouveau programme capable de chiffrer les fichiers sur l'ordinateur cible. Ce nouveau type de malware indique que les attaquants n'ont plus besoin de compétences pointues en programmation pour créer de dangereux programmes d'extorsion (ransomware) très efficaces, surtout quand les technologies de chiffrement avancé sont accessibles gratuitement. Des chercheurs du fournisseur d'antivirus Symantec sont récemment tombés sur un logiciel malveillant de ce type, d'origine russe, dont le composant principal se limite à un simple fichier batch, c'est à dire un script avec une ligne de commande. Cette stratégie de développement permet à l'attaquant de contrôler et de mettre facilement à jour le malware, explique dans un billet le chercheur Kazumasa Itabashi.

Le fichier batch télécharge une clef publique RSA en 1024 bits depuis un serveur et l'importe dans GnuPG, un programme de chiffrement gratuit qui fonctionne également par ligne de commande. GnuPG est une implémentation Open Source de la norme de chiffrement OpenPGP. Il est utilisé pour chiffrer les fichiers de la victime avec la clé téléchargée. « Si l'utilisateur veut déchiffrer les fichiers concernés, ils a besoin de récupérer la clé privée de l'auteur du malware », indique le chercheur.

Une rançon de 150 € pour déchiffrer ses propres données

Dans le chiffrement à clé publique sur lequel est basé OpenPGP, les utilisateurs génèrent une paire de clés associées, l'une rendue publique et l'autre qui reste privée. Le contenu chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. La nouvelle menace représentée par le ransomware que Symantec appelle Trojan.Ransomcrypt.L chiffre les fichiers avec les extensions

suivantes: .xls, .xlsx, .doc, .docx, .pdf, .jpg, .cd, .jpeg, .1cd, .rar, .mdb et .zip. Les victimes sont invitées à payer une rançon de 150 € pour récupérer la clef privée.

Ce qui distingue le Trojan.Ransomcrypt.L des autres malwares ne tient pas à l'usage du chiffrement à clé publique – d'autres menaces adoptent la même technique – mais à sa simplicité et au fait que l'auteur a choisi d'utiliser un programme de chiffrement légal et Open Source, au lieu de créer sa propre mise en oeuvre, ce que font souvent les auteurs de malwares.

Les chercheurs prévoient une augmentation des menaces

Il existe certains programmes d'extorsion complexes avec des fonctionnalités avancées, développés essentiellement pour être vendus à d'autres cybercriminels qui n'ont pas les compétences nécessaires. Mais Trojan.Ransomcrypt.L montre qu'il est devenu possible de développer ce type de logiciels malveillants à peu de frais et sans connaissance de programmation avancée. Si bien que les chercheurs de Symantec s'attendent à une augmentation du nombre de menaces de ce type dans l'avenir.

Article de Jean Elyan avec IDG News Service

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

Références :

http://www.lemondeinformatique.fr/actualites/lire-un-logiciel-d-extorsion-utilise-un-simple-fichier-batch-58248.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

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

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