Alerte : Arnaque par téléphone d'un agent Microsoft

Alerte : Arnaque par téléphone d'un agent Microsoft

Depuis quelques temps, une arnaque au cours de laquelle un agent vous appelle afin de résoudre avec vous vos soucis d'informatique prend de l'ampleur à la Police.

Le principe?
De nombreuses personnes témoignent à présent du même mode opératoire : vous êtes appelé par un opérateur à l'accent anglophone, se faisant passer pour un employé de « Microsoft », ou bien de son service client « Customer Care Center ».
Selon cet opérateur, des messages d'erreur leur seraient parvenus via votre ordinateur, et pour y remédier, il vous suffit d'accéder, avec un code, à une page web « infosis.net » ou bien « logme120.com ». Ces noms changent régulièrement, c'est pourquoi c'est essentiellement le mode opératoire qui doit vous alerter.
L'agent vous demande alors d'installer un logiciel pour voir votre écran et commencer un tutoriel afin que vous puissiez résoudre ensemble votre problème informatique. Vous l'avez compris: ce programme n'est autre qu'un espion informatique chargé de s'introduire dans des relations bancaires ou des données de cartes de crédit.
Que faire?
Important :La société Microsoft a déjà réagi dans de nombreux pays, en précisant qu'elle ne contacte jamais les usagers, sans que ceux-ci ne l'aient préalablement sollicitée. De plus, l'aide de spécialistes de dépannage Microsoft ne vous est jamais facturée ainsi en ligne !
Afin de protéger un ordinateur contre diverses formes d'escroquerie, il est conseillé d'utiliser un outil de suppression de logiciels espions fiables.
Si vous n'avez pas reçu un faux appel de téléphone mais cela ne signifie pas que vous êtes protégé contre d'autres types d'escroquerie, c'est pourquoi il est conseillé d'utiliser un programme de prévention de spyware.
Dans le doute, passez en revue tous les programmes de votre ordinateur en vérifiant la fonctionnalité de chacun d'entre eux, de détecter les éventuels programmes « espions » afin de les supprimer.
Vous pouvez également signaler ces messages à la police judiciaire via Pharos : www.internet-signalement.gouv.fr
N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile)
! SOYEZ VIGILANT !

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

Références :
http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Arnaque-via-un-appel-d-un-agent-Microsoft

Alerte Ebola : Les arnaques sur Internet sur l’aide humanitaire ont déjà commencé

Alerte Ebola : Les arnaques sur Internet sur l’aide humanitaire ont déjà commencé

Les cybers-escrocs ne laissent aucune opportunité leur passer sous le nez. Pendant que le virus Ebola sévit en Afrique, ils tentent de profiter de la psychose pour vendre un remède miracle.D'après le site d'information burkinabé fasozine.com, un des messages envoyés par ces malfrats d'une nouvelle ère dirait ceci :
"Bonjour cher internaute, Sous le haut parrainage du Ministre de la santé canadienne Rona Ambrose Dans le cadre de la difficulté dans laquelle l'Afrique de l'ouest précisément a été confronté par le virus EBOLA et nous avons constaté que ce virus se développer et très bientôt".

Si vous ne l'avez pas encore dans votre boite mail, sachez que c'est avec ce français douteux que beaucoup d'internautes ont été abordés par ces "brouteurs" ces derniers jours.
(brouteurs = jeunes férus d'internet basés principalement en afrique qui ont trouvé le moyen de gagner de l'argent facilement grâce à des arnaques en escroquant des Occidentaux naïfs)
"Toute l'Afrique sera bientôt atteinte par ce virus", annoncent les oiseaux de mauvais augures. Pour tenter de vous soutirer une somme, ces voleurs proposent aux internautes une porte de sortie : **"Un laboratoire canadien vient justement de trouver deux remèdes miracles : l'un pour guérir et l'autre pour la prévenir". Toutefois, les doses seraient limitées selon leur propos. Pour avoir gratuitement ces doses, ces arnaqueurs vont suggérer de verser une somme de 180 dollars qui, toujours selon eux, "représente l'argent du service courrier DHL". Une somme variable " selon la distance aérienne de votre pays par rapport au republique du bénin"**.
Nous rappelons tout simplement que les médicaments qui existent aujourd'hui sont à un stade expérimental. Les conseils que l'on formule pour lutter contre ce virus sont entre autres d'éviter de toucher un animal trouvé mort en forêt, éviter de toucher sans protection les vomissures, le sang, la selle d'un malade, ni rester sans protection près de lui, ne pas toucher ou laver les vêtements et autres objets souillés ou d'un cadavre…

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

Références :
http://www.afriqueitnews.com/2014/08/20/les-brouteurs-sautent-sur-lopportunite-offerte-par-ebola/

4,5 millions de données médicales dérobées aux Etats-Unis – Un vol de données de plus…

Community Health Systems, un spécialiste américain de la gestion des hôpitaux, a reconnu avoir été victime d'une attaque informatique entre avril et juin 2014. Résultats : 4,5 millions de données personnelles ont été dérobées. Un vol de données de plus…

Attaque informatique contre les fournisseurs d'énergie – Dragonfly lance la cyberguerre froide…

Attaque informatique contre les fournisseurs d'énergie – Dragonfly lance la cyberguerre froide…
Le scénario du pire. Ou presque. Un groupe de hackers, baptisé Dragonfly, est parvenu à corrompre certains systèmes de contrôle des opérateurs d'énergie. Notamment en France. Les pirates avaient alors la possibilité de saboter la distribution d'énergie de certains pays.

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 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

Les Objets connectés et leurs failles de sécurité ont de quoi nous inquiéter

Les Objets connectés et leurs failles de sécurité ont de quoi nous inquiéter
Dans une étude, HP s'est penché sur les failles de sécurité au sein de 10 objets connectés parmi les plus populaires. L'entreprise relève que ces nouveaux objets présentent de nombreuses vulnérabilités et incite les constructeurs à en tenir compte.

Cybercriminalité : « la situation française, en terme de ressources humaines, est proche de l'artisanal »

Un rapport sur la cybercriminalité a été dévoilé le 30 juin

2014, visant à renforcer l'arsenal pénal contre les infractions commises sur internet. Par ailleurs, de prochaines lois pourraient s'en inspirer, comme le projet de loi sur le terrorisme, qui en affiche un certain nombre de traits.

Le rapport de Marc Robert, « protéger les internautes », avait été remis dès le mois de février. L'objectif de cet épais volume : renforcer la lutte contre la cybercriminalité, dont les statistiques croissantes démontrent l'urgente nécessité pour la France de se doter d'un arsenal adapté.

Très rapidement, le rapport dresse un constat cruel : « comparé à ce dont disposent les États étrangers voisins, la situation française, en terme de ressources humaines, est proche de l'artisanal ». Il fait 54 propositions pour pallier ces lacunes.

Certaines d'entre elles tracent des axes de réflexions, mais beaucoup ont de concrètes implications. Pour preuve : le projet de loi relatif à la lutte contre le terrorisme, présenté le 9 juillet dernier à l'Assemblée nationale, s'en est directement inspiré. L'exposé des motifs de son article 12 reprend en substance la proposition n° 15, qui préconise une augmentation du quantum de la peine pour les atteintes aux systèmes de traitement automatisés de données (STAD) et la création d'une circonstance aggravante de commission en bande organisée. Globalement, l'ensemble des dispositions de la loi concernant le cyber-terrorisme, notamment les articles 10 à 16, découlent de ce rapport.

Comme base de toute action, le rapport recommande que des statistiques précises soient établies chaque année, sous l'égide de l'office national de la délinquance et des réponses pénales (ONDRP). En 2012, 84 774 infractions ont été recensées par la Police et la Gendarmerie sur internet en 2012, l'immense majorité (84 %) sont des escroqueries, des abus de

confiance et des fraudes à la carte bancaire. Mais comme le relève le rapport, « les infractions constatées par les services de Police et de Gendarmerie n'épuisent pas la réalité de la cybercriminalité ». Il faut donc appréhender la cybercriminalité à travers l'action des services de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), l'action des douanes ou encore de la commission nationale de l'informatique et des libertés (CNIL).

Le constat est sans appel : ces infractions augmentent de manière exponentielle. En 2012, Le montant moyen d'une transaction frauduleuse est de 125 €, celles-ci constituant 0,08 % du total des transactions, et touchant 2,3 % des ménages. Le taux de poursuite, la « réponse pénale » est très faible, et seules 2 222 condamnations ont été prononcées pour des crimes et délits spécifiquement visés par la loi comme faisant partie de la cybercriminalité. Un tiers d'entre eux sont des atteintes aux personnes (délinquance sexuelle, et surtout, en hausse, la pédopornographie) ; un autre tiers est constitué d'infractions à la loi de 1881 (presse). Les si nombreuses infractions aux instruments de paiement ne représentent que 15 % du taux de répression.

Pour mieux lutter contre la cybercriminalité, le rapport s'appuie évidemment sur un volet préventif. La meilleure information du public, l'éducation dès le plus jeune âge à la pratique d'internet, la mise en place de numéros d'urgence sont préconisés. Mais c'est l'appareil judiciaire qui est complètement remodelé : il s'agit, est-il affirmé, de « former les acteurs pénaux, eu égard à la spécificité de la cybercriminalité ». Cette formation interviendrait dès la formation initiale, mais aussi en continu, du fait de la nature fortement évolutive de cette matière. Des magistrats référents verraient ainsi le jour, spécialistes de la

cybercriminalité, pour traiter plus efficacement de ce contentieux. Le corpus pénal dont ils disposeraient ne doit pas être « gonflé de lois inutiles » estime le rapport, qui note que l'arsenal répressif est déjà assez complet, et qu'il est indispensable de n'adopter que des dispositions utiles.

L'idée générale est que l'action globale soit coordonnée par une délégation interministérielle de lutte contre la cybercriminalité, la nature protéiforme de ces infractions nécessitant une organisation transversale. Au sein de la justice, c'est une mission de lutte contre la cybercriminalité qui serait créée, rattachée au directeur des affaires criminelles.

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

Références :
http://www.dalloz-actualite.fr/flash/cybercriminalite-situation-francaise-en-terme-de-ressources-humaines-est-proche-de-l-artisanal

---

L'Union Européenne s'organise

enfin pour lutter contre la cybercriminalité

L'Union Européenne s'organise enfin pour lutter contre la cybercriminalité

L'Union Européenne prépare pour la rentrée la mise en place d'une force d'intervention commune dédiée à la cybersecurité. Cet organisme regroupera des experts venus de différents pays de l'UE et se penchera sur les cas dépassant la juridiction des enquêteurs nationaux.

Selon les informations du site britannique SCMagazine, cette force d'intervention commune répond au doux nom de Joint Cybercrime Action Taskforce et prendra ses fonctions en septembre 2014 pour une première période d'essai de 6 mois. Ce groupe aura pour objectif de lutter contre les réseaux de cybercriminalité étendus à l'international, à l'instar de certains botnets ou de plateforme de diffusion de malwares.

Ce groupe sera placé sous l'égide de l'European Cybercrime Task Force (EUCTF), un groupe constitué des différentes autorités nationales de lutte contre la cybercriminalité mis en place en 2010. L'EUCTF évaluera le travail de cette nouvelle force d'intervention. Cette dernière sera placée sous la direction d'Andy Archibald, le chef du département de lutte contre la cybercriminalité en Grande Bretagne.

Il aura sous ses ordres un ensemble d'expert en cybersecurité mandatés par différents pays mais SC magazine précise

également que des participants externes aux pays de l'UE seront amenés à collaborer ponctuellement avec la JCAT.

Agir efficacement à l'international

Pour l'instant, les premiers pays à participer à ce projet sont la France, l'Angleterre, l'Autriche, le Royaume Uni, la Hollande, l'Allemagne mais aussi les Etats-Unis, qui disposeront tous d'une place permanente et d'experts au sein de cette force d'intervention. Si les résultats de cette première période d'essai s'avèrent concluants, la JCAT pourrait s'ouvrir à l'ensemble des pays européens.

Sa mise en place fait écho aux grandes opérations de démantèlement de réseaux botnets qui ont eu lieu récemment, avec notamment l'offensive contre le malware Gameover Zeus étendu à plusieurs états dans le monde. L'objectif de cette force d'intervention sera de permettre une plus grande coopération entre les différentes autorités nationales de lutte contre la cybercriminalité.

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

Références :

http://www.zdnet.fr/actualites/une-force-d-intervention-cybersecurite-europeenne-sur-les-rails-39804343.htm