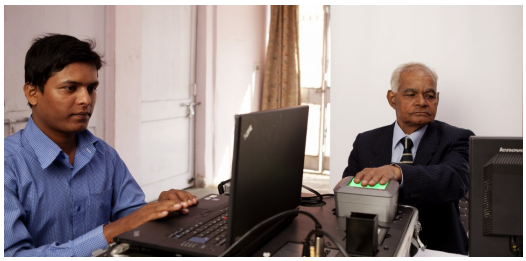
Morpho, le français qui fiche un milliard d’Indiens – Challenges.fr



Morpho, le français qui fiché un milliard d’Indiens

La filiale de Safran est en train de fournir une identité numérique à 1,2 milliard d'Indiens. Une base de données biométrique unique au monde, qui effraie certains.

Une base de données biométrique rassemblant 1,3 milliard d'individus, soit 18% de la population mondiale… C'est le défi incroyable que le français Morpho, filiale de Safran, est en train de relever en Inde.
Concrètement, le programme, baptisé Aadhaar (socle, en hindi), consiste à offrir un numéro d'identification unique à 12 chiffres à chaque citoyen. Cette identité numérique est sécurisée par la prise des données biométriques de son propriétaire: les 10 empreintes digitales, les 2 iris, et une photo du visage. Quatre ans après le début de l'opération, la base de données vient d'atteindre la barre symbolique du milliard d'individus fichés. « Chaque jour, jusqu'à 1 million de personnes peuvent être « enrôlées » dans le système », souligne Jessica Westerouen van Meeteren, directrice de la division Government Identity chez Morpho.
Pourquoi cette base de données géante? L'idée de départ du programme, lancé en 2009 par New Delhi, était d'offrir une existence officielle à des centaines de millions d'Indiens qui, faute de carte d'identité, restaient invisibles à l'administration, et donc exclus des programmes d'aide sociale. Dans un pays à l'administration pléthorique où la corruption reste importante, l'argent atterrissait souvent dans les mauvaises poches. Le numéro d'identification doit permettre de corriger le problème des fraudes à l'identité, mais aussi d'ouvrir un compte en banque simplifié ou d'obtenir un passeport plus facilement.

La complexité d'un programme spatial

Pour mener à bien ce projet colossal, le gouvernement indien a créé une agence d'Etat, la Unique Identification Authority of India (UIDAI).
Morpho est l'un des fournisseurs retenus par l'agence, avec le japonais NEC et l'américain L1 (autre filiale de Safran). Le groupe français fournit les scanners biométriques destinés à l'enregistrement des données, mais aussi la technologie de « dédoublonnement » qui permet de vérifier qu'un individu n'est pas déjà enregistré sous un autre numéro. Le système est capable de répondre à un million de requêtes par jour. « C'est un programme d'une complexité inédite dans le secteur, qu'on peut comparer à celle d'un programme spatial », assure Jean-Pierre Pellestor, directeur de programme chez Morpho.
Si le projet est en train d'arriver à bon port, c'est en grande partie grâce à l'action d'un homme: Nandan Nikelani, le cofondateur du géant de l'informatique indien Infosys. Le puissant homme d'affaires, qui fut le premier président de l'UIDAI, a pesé de tout son poids pour passer outre les légendaires pesanteurs de l'administration indienne. Au point que la loi avalisant le programme n'a été votée à la Lok Sabha, la chambre basse du parlement indien, que le 16 mars dernier… soit six ans après le début des opérations d'enregistrement. Nikelani avait même réussi à convaincre le premier ministre Narendra Modi, très critique contre Aadhaar durant la campagne électorale de 2014, de poursuivre le projet. « Modi l'a finalement accéléré », se félicite-t-on chez Morpho.

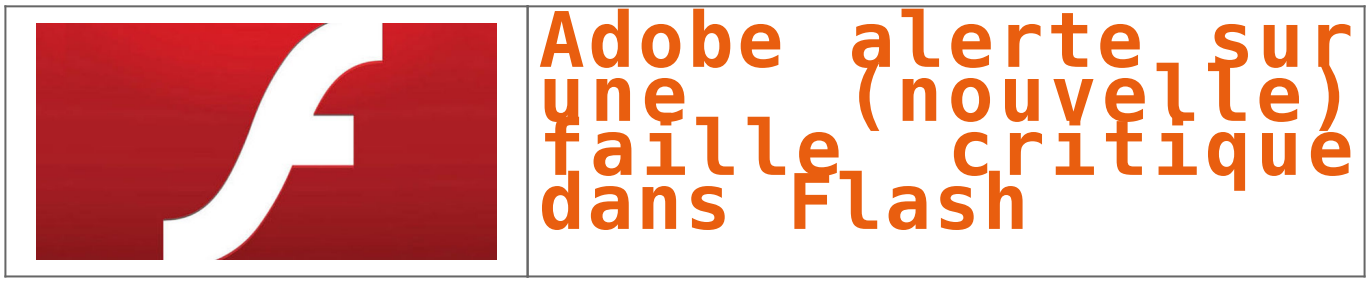
Risque de Big Brother?

Le programme ne fait pourtant toujours pas l'unanimité en Inde. Si plus d'un milliard de personnes ont accepté de s'enregistrer dans la base de données, d'aucuns y voient un Big Brother potentiel, qui pourrait être détourné au détriment de la vie privée des citoyens. « Le gouvernement peut-il nous assurer que Aadhaar et les données collectées ne vont pas être détournées comme ce qui a été fait par la NSA aux Etats-Unis? »,s'interrogeait auprès de Reuters Tathagata Satpathy, une avocate basé dans l'Odisha (est de l'Inde). L'accès au fichier pour un usage lié à la « sécurité nationale » fait notamment débat. « Le projet apporte une protection de la vie privée d'une grande robustesse, au-delà de tout ce qu'ont apporté les autres lois en Inde« , répondait mi-mars Nandan Nikelani à l'Indian Express.
En tout cas, Morpho espère bien surfer sur le contrat indien pour vendre d'autres systèmes similaires. « Nous avons des campagnes commerciales en cours dans d'autres pays sur des programmes comparables, mais la taille du projet indien restera probablement unique », détaille Jessica Westerouen van Meeteren. Mais la bonne santé de Morpho (1,9 milliard d'euros de chiffre d'affaires en 2015, en croissance organique de 11%) n'empêche pas le directeur général de Safran Philippe Petitcolin de réfléchir à son avenir, la division n'ayant pas vraiment de synergie avec le reste du groupe, ni le poids suffisant pour équilibrer les activités aéronautiques. Après avoir mis en vente l'activité de détection d'explosifs (Morpho Detection), le groupe pourrait annoncer la cession de toute la division dans le courant de l'année 2016… [Lire la suite]

Réagissez à cet article

Source : *Morpho, le français qui fiche un milliard d'Indiens – Challenges.fr*

Adobe alerte sur une (nouvelle) faille critique dans Flash



Adobe publie une notification de sécurité signalant la présence d'une vulnérabilité dans le format Flash. Une solution provisoire est proposée pour réduire les risques, en attendant la publication du patch.

Les raisons de détester Flash ne manquent pas. Depuis des années, le format conçu par Adobe fait l'objet de vives critiques tout à fait justifiées : de la lourdeur du logiciel à l'intégration médiocre avec le web, en passant par les soucis d'interopérabilité et le fait qu'il s'agisse d'une technologie propriétaire, Flash traîne une vilaine réputation. Pas étonnant que de nombreux acteurs souhaitent le voir disparaître.

Un format massivement utilisé mais bourré de défauts.

À cette liste déjà gratinée, il faut aussi inclure les problèmes de sécurité récurrents. Cela s'est encore vérifié récemment avec la découverte d'une vulnérabilité critique qui affecte toutes les versions du format, y compris la dernière disponible sur le site d'Adobe (numérotée 21.0.0.197). Et le pire, c'est que la brèche en question, identifiée sous le code CVE-2016-1019 est déjà exploitée.

« *Une vulnérabilité critique (CVE-2016-1019) existe dans Adobe Flash Player 21.0.0.197 et les versions précédentes dans Windows, Macintosh, Linux et Chrome OS. Une exploitation réussie pourrait provoquer un crash et permettre en théorie à un assaillant de prendre le contrôle du système affecté* », commente Adobe, qui confirme que la brèche est d'ores et déjà en cours d'utilisation.

Un correctif est attendu le 7 avril

« *Adobe est au courant des informations indiquant que CVE-2016-1019 est en train d'être activement exploité sur les systèmes utilisant Windows 7 et Windows XP avec Flash Player en version 20.0.0.306 et inférieur* ». Adobe explique qu'une solution permettant d'atténuer le problème est disponible avec la branche 21.0.0.182, de façon à empêcher l'exploitation de cette faille.

Les utilisateurs sont invités à mettre à jour sans tarder le logiciel Flash, même s'il n'existe pas encore de patch colmatant une bonne fois pour toutes cette brèche. En effet, l'usage d'une version réduisant l'exposition à un piratage à distance constitue déjà une protection supplémentaire. Adobe prévoit de publier dès demain, jeudi 7 avril, une mise à jour de sécurité qui réglera le problème … [Lire la suite]

Source : *Adobe alerte sur une faille critique dans Flash – Tech – Numerama*

Les terminaux de paiement cibles des pirates chasseurs de failles

	**Les terminaux de paiement cibles des pirates chasseurs de failles**

Avant le passage à des cartes à puce plus sécurisées, les cybercriminels sont à l'affût de failles dans les anciens systèmes de paiement aux États-Unis, pour continuer à voler des identifiants et des mots de passe. Vu les revenus qu'ils peuvent encore en tirer, l'enjeu reste assurément très attractif.

Selon FireEye, les cybercriminels redoublent d'efforts pour voler les informations des cartes de paiement sur les terminaux des détaillants américains avant la mise en place de nouveaux systèmes de défense.

L'an dernier, plus d'une douzaine de logiciels malveillants différents ciblant les TPV utilisés par de nombreux détaillants pour le traitement des paiements électroniques ont été découverts. Ces dernières années, les pirates ont réussi à pénétrer plusieurs fois dans ces systèmes, ciblant faiblesses ou vulnérabilités des logiciels afin d'extraire les informations qu'ils peuvent revendre sur le marché noir.

Depuis le mois d'octobre dernier, les détaillants endossent la responsabilité des transactions frauduleuses quand les paiements ne sont pas réalisés avec des cartes EMV. Celles-ci ont été dotées d'une puce électronique et bénéficient de meilleures sécurités pour protéger les données inscrites sur la puce. D'importants revendeurs qui ont été victimes de ces usurpations ces dernières années, comme le distributeur américain Target, ont amélioré leurs systèmes. Mais le coût et les retards de livraison des nouveaux systèmes certifiés ont ralenti la transition, laissant encore une marge d'action pour les cybercriminels. Au City Target sur Bush Street à San Francisco la semaine dernière, un achat de moins de 10$ effectué avec une carte à puce française n'a donné lieu à aucune vérification : ni code, ni signature et encore moins d'ID.

Des terminaux toujours très vulnérables aux Etats-Unis

Hier, un chercheur senior de FireEye spécialisé dans l'intelligence et les menaces, Nat Villeneuve, a écrit que plus d'une douzaine de logiciels malveillants de familles différentes ciblant les systèmes TP avaient été découverts l'an dernier. « Aux États-Unis, les criminels sont très actifs et cherchent par tous les moyens à infecter rapidement les systèmes de paiement avant que les détaillants américains n'achèvent la transition vers des systèmes plus sécurisés », a prévenu le chercheur. En réponse, les émetteurs de cartes et les banques ont amélioré leur capacité à identifier et à bloquer les transactions potentiellement frauduleuses. Mais la fraude reste suffisamment lucrative pour inciter les criminels à y consacrer encore beaucoup de ressources.

Nat Villeneuve parle d'un nouveau type de malware appelé POS Treasurehunt, qui vole les données des cartes de paiement à partir de la mémoire d'un ordinateur. « Le mode opératoire classique consiste à implanter Treasurehunt sur un système de TP, soit en utilisant des identifiants déjà volés, soit par force brute, c'est-à-dire en testant des séries de mots de passe courants pour accéder à des systèmes de paiement mal sécurisés », a-t-il écrit. Jusqu'ici, le champ d'action de Treasurehunt a été limité, signe que ses auteurs l'ont déployé sélectivement. Une chaîne de code du malware indique qu'il a été développé par un groupe dénommé Bears Inc. « Bears Inc. est très actif sur un forum dédié à la cybercriminalité souterraine liée à la fraude aux cartes de crédit », écrit le chercheur. « Sur ce forum, Bears Inc. a mis en vente des informations de carte de paiement volées ». Une autre chaîne de code comporte le message suivant : « Bonjour à Xylitol and Co ». Xylitol est le surnom d'un chercheur en malware bien connu, basé en France, qui anime un blog technique très suivi.

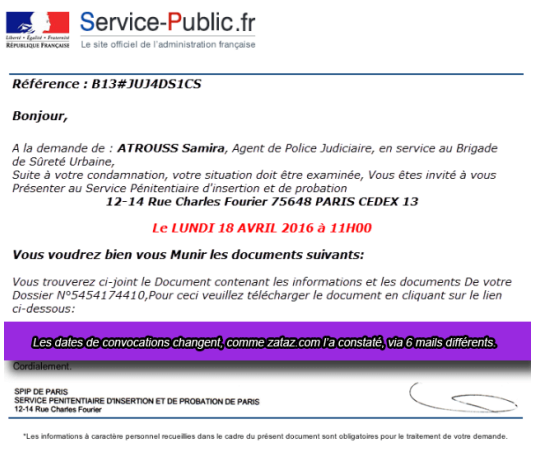
Une activité très rentable

Le piratage des TPV est toujours rentable pour les cybercriminels. On trouve facilement des forums de « carding » sur lesquels il est possible d'acheter des identifiants de carte de paiement. Le tarif de ces informations varie en fonction de la date limite d'utilisation de la carte et de la date où les données ont été volées. Les revenus tirés par les cybercriminels semblent tellement intéressants que les prix de ces informations ont même baissé.

Réagissez à cet article

Source : *Les pirates cherchent activement des failles dans les terminaux de paiement – Le Monde Informatique*

Alerte – Arnaque à la fausse convocation de la Police



Service-Public.fr
Le site officiel de l'administration française

Référence : B13#JUJ4DS1CS

Bonjour,

*A la demande de : **ATROUSS Samira**, Agent de Police Judiciaire, en service au Brigade de Sûreté Urbaine,*
Suite à votre condamnation, votre situation doit être examinée, Vous êtes invité à vous Présenter au Service Pénitentiaire d'insertion et de probation
12-14 Rue Charles Fourier 75648 PARIS CEDEX 13

Le LUNDI 18 AVRIL 2016 à 11H00

Vous voudrez bien vous Munir les documents suivants:

Vous trouverez ci-joint le Document contenant les informations et les documents De votre Dossier N°5454174410,Pour ceci veuillez télécharger le document en cliquant sur le lien ci-dessous:

Les dates de convocations changent, comme zataz.com l'a constaté, via 6 mails différents.

Cordialement.

SPIP DE PARIS
SERVICE PENITENTIAIRE D'INSERTION ET DE PROBATION DE PARIS
12-14 Rue Charles Fourier

*Les informations à caractère personnel recueillies dans le cadre du présent document sont obligatoires pour le traitement de votre demande.

Alerte – Arnaque à la fausse convocation de la Police

C'est derrière un document présumé aux couleurs de la Police Judiciaire que des centaines de Français sont piégés, depuis quelques jours, par un courriel malveillant aux couleurs du Service Pénitentiaire d'insertion et de probation de Paris.


Service-Public.fr
Le site officiel de l'administration française

Référence : B13#JUJ4DS1CS

Bonjour,

*A la demande de : **ATROUSS Samira**, Agent de Police Judiciaire, en service au Brigade de Sûreté Urbaine,*
Suite à votre condamnation, votre situation doit être examinée, Vous êtes invité à vous Présenter au Service Pénitentiaire d'insertion et de probation
12-14 Rue Charles Fourier 75648 PARIS CEDEX 13

Le LUNDI 18 AVRIL 2016 à 11H00

Vous voudrez bien vous Munir les documents suivants:

Vous trouverez ci-joint le Document contenant les informations et les documents De votre Dossier N°5454174410,Pour ceci veuillez télécharger le document en cliquant sur le lien ci-dessous:

Les dates de convocations changent, comme zataz.com l'a constaté, via 6 mails différents.

Cordialement.

SPIP DE PARIS
SERVICE PENITENTIAIRE D'INSERTION ET DE PROBATION DE PARIS
12-14 Rue Charles Fourier

*Les informations à caractère personnel recueillies dans le cadre du présent document sont obligatoires pour le traitement de votre demande.

Êtes-vous un dangereux criminel ? Normalement, non ! Avez-vous oublié de payer une année de contraventions ? Si tout va bien, non ! Avez-vous oublié votre séjour en prison ? Bref, le courriel communiqué ce week-end au nom d'un « ***Agent de police Judiciaire, en service en Brigade de Sureté Urbaine*** » vous n'avez rien à craindre de cette missive.
Depuis quelques jours, un étonnant mail aux couleurs de l'administration judiciaire Française s'invite dans les boites mails de nombreux, très nombreux lecteurs de ZATAZ.COM. La missive indique, en objet, être une « ***Convocation par Officier de Police Judiciaire (C.O.P.J)***« . Un titre suffisamment inquiétant, mais le pirate a rajouté en bonus « ***Obligation*** » histoire de renforce son social engineering.

Bonjour,

*A la demande de : **ATROUSS Samira**, Agent de Police Judiciaire, en service au Brigade de Sûreté Urbaine,*
Suite à votre condamnation, votre situation doit être examinée, Vous êtes invité à vous Présenter au Service Pénitentiaire d'insertion et de probation
12-14 Rue Charles Fourier 75648 PARIS CEDEX 13

Le LUNDI 18 AVRIL 2016 à 11H00

Vous voudrez bien vous Munir les documents suivants:

Vous trouverez ci-joint le Document contenant les informations et les documents De votre Dossier N°5454174410,Pour ceci veuillez télécharger le document en cliquant sur le lien ci-dessous:

Le courriel informe le lecteur qu' »***à la demande de*** [identité d'une personne], ***Agent de police Judiciaire, en service en Brigade de Sureté Urbaine.*** » vous êtes convoqués à la suite de votre condamnation et que « ***votre situation doit être examinée***« . La missive se termine par une date et une adresse postale. Une adresse officielle du *Service Pénitentiaire d'insertion et de probation de Paris (SPIP)*.
Le bot pirate [robot informatique], derrière cette diffusion malveillante, propose des rendez-vous, les lundis (11, 18 avril…). Comme vous l'aurez compris, une pièce jointe est proposée dans cette arnaque. Un PDF qui cache surtout une malveillance informatique. Attention, ne mettez pas en automatique, dans les options de votre logiciel de correspondance, la confirmation de lecture. L'attaque pirate demande, justement, que soit confirmé la lecture du courrier. Évitez de confirmer à l'escroc votre existence.
Bien entendu, ne cliquez surtout pas sur ce genre de fichier (ici, il ne s'agit pas d'un ransomware), surtout si vous n'êtes pas attirés par le chiffrement de vos données et l'obligation de payer une « rançon » pour récupérer vos documents privés, ou vous retrouver avec un logiciel espion dans votre machine. Ne rappelez pas, non plus, les numéros de téléphones qui peuvent être fournis.

Réagissez à cet article

Source : *ZATAZ Piège informatique à partir d'une fausse convocation de la Police – ZATAZ*

Les autorités US invitent les hackers à pirater le Pentagone

Les autorités US invitent les hackers à pirater le Pentagone

Les autorités militaires américaines proposent aux meilleurs hackers du pays d'essayer de pirater le Pentagone. Les gagnants de ce « concours » se partageront 150.000 dollars

Les autorités militaires américaines ont procédé à l'enregistrement des participants au projet Hack the Pentagone (Piratez le Pentagone), a annoncé le porte-parole du Pentagone Peter Cook.

Anonymous déclare la guerre à Donald Trump

Les projets de ce type ont fait leurs preuves dans nombreuses compagnies privées des Etats-Unis et ont pour but de révéler les failles dans leur système de sécurité. En analysant les cyberattaques, les experts peuvent détecter les brèches dans la défense informatique, en vue de les colmater avant que les malfaiteurs ne causent des dégâts.

« Dans le cadre du programme, les participants auront à travailler avec certains sites du département américain de la Défense, ceux-ci étant désignés à la veille du concours », indique le site du Pentagone.

cyberguerre

© PHOTO. PIXABAY

Pourquoi n'a-t-on pas encore coupé la connexion Internet de Daech?

Le projet se déroulera du 18 avril au 12 mai. En cas de succès, les gagnants se partageront une cagnotte de 150.000 dollars. Tous les participants, qui doivent être des citoyens américains, seront soumis à un contrôle de leurs données personnelles.

Le 1er mars, le secrétaire américain à la Défense a présenté le projet à San Francisco, dans le cadre du « Commonwealth Club ». C'est la première fois que l'administration américaine se tourne vers des pirates pour tester sa sécurité.

… [Lire la suite]

Réagissez à cet article

Source : *Les autorités US invitent les hackers à pirater le Pentagone*

Et si la publicité cachait des Malwares ?

Et si la publicité cachait des Malwares ?

Alors que plusieurs sites d'information ont récemment mené une action pour dénoncer l'utilisation des bloqueurs publicitaires rappelant que la publicité était le principal revenu pour les sites web, il est également bon de savoir qu'elle tend à devenir un véritable vecteur d'attaque pour les pirates informatiques.

Des ransomwares cachés dans les publicités en ligne

Depuis plusieurs jours maintenant, de nombreux internautes se retrouvent piégés par des rançongiciels sans réellement comprendre comment ces derniers ont pu infecter leur ordinateur.

En effet, alors que beaucoup ont bien compris qu'ils devaient accorder la plus grande attention aux pièces jointes adressées par mail ainsi qu'aux fichiers qu'ils téléchargent sur la Toile, ils sont également nombreux à ne pas savoir que les publicités en ligne peuvent être à l'origine de l'infection.

Eh oui, de plus en plus de pirates informatiques parviennent à compromettre des réseaux d'annonces publicitaires en se faisant passer pour des personnes fiables. Ils adressent alors à la régie des bannières à faire afficher par des sites web, certaines intégrant un malware qui pourra infecter les ordinateurs des milliers d'internautes qui verront la publicité.

Cette forme de piratage est d'autant plus « sournoise » que le malware utilisé et baptisé Angler détecte l'existence de logiciel de sécurité et n'est réellement actif que si l'ordinateur ne dispose pas de sécurité. Autant qu'il est très complexe à détecter.

Les bloqueurs de publicité, finalement utiles pour sécuriser un ordinateur ?

Quelques heures seulement après que plusieurs sites d'informations français aient dénoncé le recours de plus en plus fréquent des internautes aux bloqueurs publicitaires, ces derniers viennent d'avoir un joli coup de publicité.

En effet, les bloqueurs de publicité peuvent être une solution pour sécuriser un ordinateur et tout du moins se protéger contre le malvertising.

Le développement de ce phénomène devrait en tout cas complexifier un peu plus encore la tâche des webmasters puisque l'image de la publicité, déjà jugée intrusive et gênante, devrait être davantage écornée en devenant une menace en matière de sécurité… [Lire la suite]

Réagissez à cet article

Source : *Quand la publicité devient un vecteur d'attaque*

Des Box pourraient être piratées pour mener des attaques DDOS ?

Des Box pourraient être piratées pour mener des attaques DDOS ?

Eset a signalé l'activité d'un ver exploitant une faiblesse du protocole de gestion réseau distant Telnet implémenté dans les routeurs domestiques sous Linux. Des pirates peuvent s'en servir pour construire un botnet et lancer des attaques DDoS.

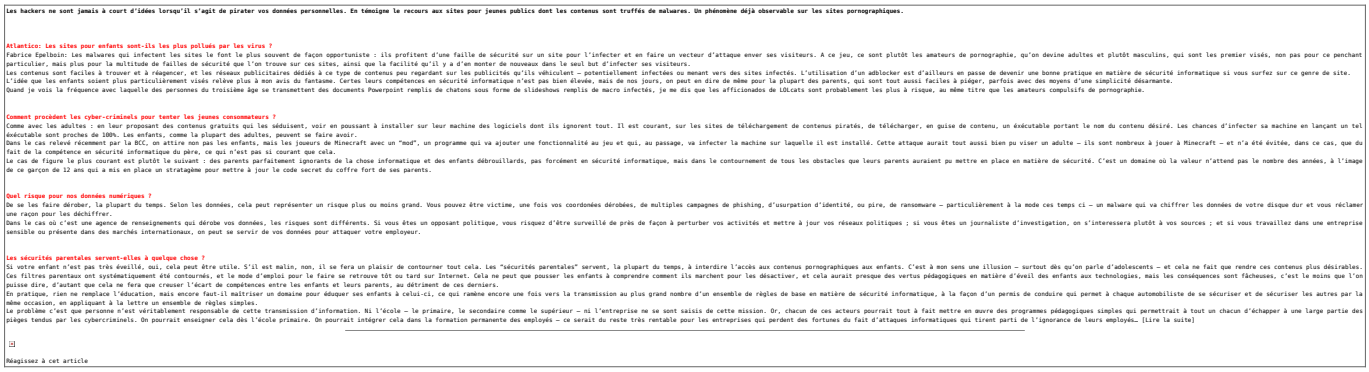
Construire des botnets à partir de routeurs, modems, points d'accès sans fil et autres terminaux réseaux ne nécessite pas d'exploits très sophistiqués. C'est le cas par exemple de Remaiten, un nouveau ver exploitant les routeurs domestiques sous Linux en tirant partie d'une faiblesse liée aux mots de passe du service de gestion réseau distant Telnet. Remaiten n'est autre que la dernière incarnation de bots Linux distribués spécialement conçus pour lancer des attaques par déni de service (DDoS). Lorsqu'il scanne des points d'entrée, Remaiten tente de se connecter à des adresses IP aléatoires sur le port 23 (Telnet) et, en cas de connexion fructueuse, il tente de s'authentifier en utilisant une combinaison de nom d'utilisateur et mot de passe en provenance d'une liste d'authentifiants communs, ont indiqué dans un billet de blog les chercheurs de l'éditeur en solutions de sécurité Eset. Ce n'est pas la première fois que les routeurs domestiques sont exposés à du piratage. On se souvient que l'année dernière 700 000 avaient été exposés à cause d'une faille NetUSB et plus récemment, des failles avaient été trouvées dans de nombreux routeurs WiFi Netgear et D-Link.
Scan de ports et fermeture du service Telnet pour se protéger
En cas de succès, le bot exécute plusieurs commandes pour déterminer l'architecture système avant de transférer un petit programme compilé pour permettre de télécharger l'ensemble des commandes de contrôle du botnet. Le ver dispose de versions pour jeux d'instructions mips, mipsel, armeabi et armebeabi. Une fois installé, il se connecte à un canal IRC et attend les commandes d'un pirate distant. Ce bot supporte une variété de commandes pour lancer différentes attaques DDoS et peut même scanner d'autres bots DDoS afin de les désinstaller.
Il est surprenant que de nombreux terminaux réseau utilisent encore Telnet pour la gestion réseau à distance plutôt que le protocole plus sécurisé SSH. Il est encore plus malheureux que de nombreux terminaux soient livrés avec le service Telnet ouvert par défaut. Afin de se protéger, il est recommandé d'utiliser un outil de scan de port en ligne et, dans le cas où le port 23 est ouvert, de fermer le service Telnet depuis la console d'administration web. Une possibilité qui n'est malheureusement pas offerte par tous les fournisseurs d'accès à leurs clients… [Lire la suite]

Réagissez à cet article

Les sites pour enfants se

transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?



Les hackers ne sont jamais à court d'idées lorsqu'il s'agit de pirater vos données personnelles. En témoigne le recours aux sites pour jeunes publics dont les contenus sont truffés de malwares. Un phénomène déjà observable sur les sites pornographiques.

Atlantico: Les sites pour enfants sont-ils les plus pollués par les virus ?

Fabrice Epelboin: Les malwares qui infectent les sites le font le plus souvent de façon opportuniste : ils profitent d'une faille de sécurité sur un site pour l'infecter et en faire un vecteur d'attaque enver ses visiteurs. A ce jeu, ce sont plutôt les amateurs de pornographie, qu'on devine adultes et plutôt masculins, qui sont les premier visés, non pas pour ce penchant particulier, mais plus pour la multitude de failles de sécurité que l'on trouve sur ces sites, ainsi que la facilité qu'il y a d'en monter de nouveaux dans le seul but d'infecter ses visiteurs.
Les contenus sont faciles à trouver et à réagencer, et les réseaux publicitaires dédiés à ce type de contenus peu regardant sur les publicités qu'ils véhiculent – potentiellement infectées ou menant vers des sites infectés. L'utilisation d'un adblocker est d'ailleurs en passe de devenir une bonne pratique en matière de sécurité informatique si vous surfez sur ce genre de site.
L'idée que les enfants soient plus particulièrement visés relève plus à mon avis du fantasme. Certes leurs compétences en sécurité informatique n'est pas bien élevée, mais de nos jours, on peut en dire de même pour la plupart des parents, qui sont tout aussi faciles à piéger, parfois avec des moyens d'une simplicité désarmante.
Quand je vois la fréquence avec laquelle des personnes du troisième âge se transmettent des documents Powerpoint remplis de chatons sous forme de slideshows remplis de macro infectés, je me dis que les afficionados de LOLcats sont probablement les plus à risque, au même titre que les amateurs compulsifs de pornographie.

Comment procèdent les cyber-criminels pour tenter les jeunes consommateurs ?

Comme avec les adultes : en leur proposant des contenus gratuits qui les séduisent, voir en poussant à installer sur leur machine des logiciels dont ils ignorent tout. Il est courant, sur les sites de téléchargement de contenus piratés, de télécharger, en guise de contenu, un éxécutable portant le nom du contenu désiré. Les chances d'infecter sa machine en lançant un tel éxécutable sont proches de 100%. Les enfants, comme la plupart des adultes, peuvent se faire avoir.
Dans le cas relevé récemment par la BCC, on attire non pas les enfants, mais les joueurs de Minecraft avec un "mod", un programme qui va ajouter une fonctionnalité au jeu et qui, au passage, va infecter la machine sur laquelle il est installé. Cette attaque aurait tout aussi bien pu viser un adulte – ils sont nombreux à jouer à Minecraft – et n'a été évitée, dans ce cas, que du fait de la compétence en sécurité informatique du père, ce qui n'est pas si courant que cela.
Le cas de figure le plus courant est plutôt le suivant : des parents parfaitement ignorants de la chose informatique et des enfants débrouillards, pas forcément en sécurité informatique, mais dans le contournement de tous les obstacles que leurs parents auraient pu mettre en place en matière de sécurité. C'est un domaine où la valeur n'attend pas le nombre des années, à l'image de ce garçon de 12 ans qui a mis en place un stratagème pour mettre à jour le code secret du coffre fort de ses parents.

Quel risque pour nos données numériques ?

De se les faire dérober, la plupart du temps. Selon les données, cela peut représenter un risque plus ou moins grand. Vous pouvez être victime, une fois vos coordonnées dérobées, de multiples campagnes de phishing, d'usurpation d'identité, ou pire, de ransomware – particulièrement à la mode ces temps ci – un malware qui va chiffrer les données de votre disque dur et vous réclamer une rançon pour les déchiffrer.
Dans le cas où c'est une agence de renseignements qui dérobe vos données, les risques sont différents. Si vous êtes un opposant politique, vous risquez d'être surveillé de près de façon à perturber vos activités et mettre à jour vos réseaux politiques ; si vous êtes un journaliste d'investigation, on s'interessera plutôt à vos sources ; et si vous travaillez dans une entreprise sensible ou présente dans des marchés internationaux, on peut se servir de vos données pour attaquer votre employeur.

Les sécurités parentales servent-elles à quelque chose ?

Si votre enfant n'est pas très éveillé, oui, cela peut être utile. S'il est malin, non, il se fera un plaisir de contourner tout cela. Les "sécurités parentales" servent, la plupart du temps, à interdire l'accès aux contenus pornographiques aux enfants. C'est à mon sens une illusion – surtout dès qu'on parle d'adolescents – et cela ne fait que rendre ces contenus plus désirables. Ces filtres parentaux ont systématiquement été contournés, et le mode d'emploi pour le faire se retrouve tôt ou tard sur Internet. Cela ne peut que pousser les enfants à comprendre comment ils marchent pour les désactiver, et cela aurait presque des vertus pédagogiques en matière d'éveil des enfants aux technologies, mais les conséquences sont fâcheuses, c'est le moins que l'on puisse dire, d'autant que cela ne fera que creuser l'écart de compétences entre les enfants et leurs parents, au détriment de ces derniers.
En pratique, rien ne remplace l'éducation, mais encore faut-il maîtriser un domaine pour éduquer ses enfants à celui-ci, ce qui ramène encore une fois vers la transmission au plus grand nombre d'un ensemble de règles de base en matière de sécurité informatique, à la façon d'un permis de conduire qui permet à chaque automobiliste de se sécuriser et de sécuriser les autres par la même occasion, en appliquant à la lettre un ensemble de règles simples.
Le problème c'est que personne n'est véritablement responsable de cette transmission d'information. Ni l'école – le primaire, le secondaire comme le supérieur – ni l'entreprise ne se sont saisis de cette mission. Or, chacun de ces acteurs pourrait tout à fait mettre en œuvre des programmes pédagogiques simples qui permettrait à tout un chacun d'échapper à une large partie des pièges tendus par les cybercriminels. On pourrait enseigner cela dès l'école primaire. On pourrait intégrer cela dans la formation permanente des employés – ce serait du reste très rentable pour les entreprises qui perdent des fortunes du fait d'attaques informatiques qui tirent parti de l'ignorance de leurs employés… [Lire la suite]

Réagissez à cet article

Fabrice Epelboin est enseignant à Sciences Po et cofondateur de Yogosha, une startup à la croisée de la sécurité informatique et de l'économie collaborative.

Source : *Quand les sites pour enfants se transforment en pièges pour voler les données personnelles de leurs parents | Atlantico.fr*

2ème édition du Forum TAC, Technology Against Crime les 28 et 29 avril prochains à Lyon

INNOVER POUR UN MONDE PLUS SUR, Tel est le slogan de la 2ème édition du Forum TAC, Technology Against Crime qui réunit les acteurs mondiaux de la Sécurité à Lyon, les 28 et 29 avril prochains

Après le succès de la 1ère édition de 2013, le Forum international TAC, Technology Against Crime revient à Lyon en 2016, en présence du ministre de l'Intérieur, Bernard Cazeneuve, pour répondre à deux grands enjeux :
1/ Anticiper les menaces et répondre aux grands enjeux de sécurité
2/ Identifier et mettre en lumière les solutions de demain
Organisé autour de 3 menaces : cyber – crime organisé – terrorisme et de 3 solutions : l'innovation technologique – la coopération public/privé – la coordination internationale.
Le Forum TAC met en relation les besoins des donneurs d'ordres publics et privés et les solutions proposées par les entreprises et crée ainsi un dialogue de haut niveau axé sur la performance et l'innovation en matière de sécurité. Un événement au format unique qui associe des rendez-vous d'affaires, un Forum Innovation, des démonstrations, un espace networking, des cas pratiques et des interventions de haut niveau.

500 participants sont attendus :
• ministres, représentants d'Interpol et délégations officielles de plus de 190 pays
• forces de police et de sûreté internationales
• dirigeants et responsables de la sécurité de grands groupes industriels
• fournisseurs de solutions et services
• représentants institutionnels

Parmi les nombreux sujets traités :
• La protection des avions face aux cyber-attaques
• Le trafic d'êtres humains
• Le maintien de l'ordre et l'utilisation des media sociaux
• La protection des sites sensibles

En savoir plus : www.forum-tac.com

Réagissez à cet article

Source : Denis JACOPINI

Comment limiter simplement les risques de piratage informatique en entreprise ?

Comment limiter simplement les risques de piratage informatique en entreprise ?

La plupart du temps, les entreprises redoutent les cyberattaques provenant de l'extérieur. Pourtant, le personnel opérant dans les murs disposent souvent de droits d'accès excessifs par rapport à leurs rôles, et constituent le vecteur le plus probable de défaillances de sécurité, que ce soit en s'impliquant activement dans des activités malveillantes ou, plus souvent, en devenant inconsciemment les fournisseurs de comptes piratés et des droits associés. Entre 50% et 70 % des attaques réussies sont attribués à des utilisateurs internes. D'où la nécessité d'adopter un système IAM pour gérer dans les règles de l'art les identités des utilisateurs, et surveiller en permanence leurs droits d'accès aux ressources informatiques.

En collectant l'ensemble des informations liées à la structure d'autorisations, les solutions d'Identity and Access Intelligence offrent une vue d'ensemble des droits d'accès et des risques associés. Ces solutions disposent d'une ergonomie moderne et intuitive pour explorer, manipuler et restituer les données. S'appuyer sur des analyses approfondies et exhaustives facilite très largement le contrôle et l'audit des risques, la prise de décision et la gouvernance.
Ce guide pratique revient sur les principes de base de l'Identity and Access Intelligence. Il fournit un cadre simple pour aider votre entreprise à identifier les risques associés aux utilisateurs et liés à leurs droits d'accès.

1. Analyser les données de droits d'accès et évaluer les risques associés
Les solutions d'Identity and Access Intelligence s'appuient sur les technologies de business intelligence pour collecter les données d'identités et d'accès existantes, et les convertir en informations qualitatives facilitant la prise de décision. Elles fournissent à leurs utilisateurs une vue à 360° de toutes les informations liées aux droits d'accès (utilisateurs, rôles, groupes, ressources…) qui permet de naviguer de manière active au sein de ces données. Ils pourront les analyser depuis de multiples angles et axes à l'aide d'une interface graphique optimisée. Les systèmes les plus avancés proposent des analyses prêtes à l'emploi ainsi que des analyses ad-hoc pour construire ses propres requêtes.
Les solutions d'Identity and Access Intelligence permettent également d'identifier les risques potentiels associés aux utilisateurs et liés à leurs droits d'accès : utilisateurs à haut risque, comptes orphelins, failles de sécurité… Grâce à des indicateurs de risque et de conformité, l'entreprise peut se concentrer sur l'essentiel et dispose d'une aide précieuse au pilotage. Elle est alors en mesure de corriger plus rapidement des incohérences et des erreurs d'attribution de droits, et de mieux protéger ses ressources informatiques contre des interventions non autorisées et potentiellement dangereuses. En s'appuyant sur des faits démontrés, l'entreprise dispose des moyens nécessaires pour prouver l'efficacité des procédures de contrôle mises en place.

2. Adapter les informations à chaque type d'utilisateur
Le plus souvent, les solutions d'Identity and Access Intelligence intègrent des fonctionnalités d'exploration des données, comme l'analyse verticale et transversale, qui facilitent la recherche d'information et l'obtention de réponses pertinentes. La présentation graphique et intelligible des informations est adaptée à toutes les populations de l'entreprise : administrateurs informatiques, équipes métiers, auditeurs, direction générale…
Les RSSI et les auditeurs souhaitent visualiser les données de sécurité dans le moindre détail. Ils disposent d'un outil de surveillance dynamique à 360 degrés qui leur permet de déterminer le niveau de risque et le type de risque associés à un utilisateur. Ils peuvent aussi créer des rapports ad-hoc personnalisés pour croiser les informations comme bon leur semble et visualiser les données de sécurité qui les intéressent.
Les responsables métiers ont besoin de rapports standards prêts à l'emploi pour identifier rapidement les risques liés aux habilitations de leurs équipes et se concentrer sur les zones à haut risque. Pour aller à l'essentiel, la direction générale peut accéder à des tableaux de bord reprenant les principaux indicateurs de risque pondérés et hiérarchisés. Ils offrent un point de départ synthétique vers une analyse en profondeur si nécessaire. En pilotant l'évolution des indicateurs dans le temps, les décideurs déterminent les actions correctives à mener pour réduire le niveau de risque et améliorer la gouvernance à l'échelle de l'entreprise.

3. Réaliser un examen historique complet des droits d'accès
Les systèmes les plus avancés permettent de reconstituer tous les changements de droits ayant eu lieu au préalable, grâce à une historisation des modifications. Les changements de droits sont alors identifiés, tracés et consultables en toute simplicité.
Cette fonctionnalité est précieuse pour les auditeurs, car elle leur donne les moyens d'établir des pistes d'audit et de réaliser des investigations forensiques approfondies et exhaustives. En fonction de leurs besoins, ils passent en revue les droits d'accès d'un utilisateur à une date spécifique dans le passé, ou contrôlent ses changements successifs d'habilitations pendant une période donnée. Ainsi, l'historisation des droits d'accès est une fonctionnalité nécessaire pour détecter toute modification suspecte, identifier la source d'un problème, et réduire l'impact d'une fraude.

4. Identifier les utilisateurs à haut risque
Les solutions d'Identity and Access Intelligence offrent une visibilité à la demande sur les données de droits d'accès. Les informations relatives aux risques et aux habilitations sont mises à disposition dans un format compréhensible et intelligible, ce qui facilite très largement l'identification des groupes d'utilisateurs présentant le plus haut niveau de risque.
Une des recommandations de base de l'IAM est d'appliquer le principe du moindre privilège qui consiste à limiter les droits d'accès des utilisateurs au minimum requis pour leurs fonctions dans l'organisation. C'est pourquoi l'entreprise devra se concentrer sur la surveillance des utilisateurs à risque et évaluer régulièrement la pertinence de leurs droits d'accès spécifiques… [Lire la suite]

Réagissez à cet article

Source : *Bastien Meaux, Beta Systems : Le guide pratique de l'Identity and Access Intelligence – Global Security Mag Online*