Les métadonnées téléphoniques très bavardes sur notre vie privée

Les métadonnées téléphoniques très bavardes sur notre vie privée

Les métadonnées téléphoniques révèlent des informations très privées

Une équipe de chercheurs de l'université de Stanford a publié une vaste étude montrant l'étendue des informations personnelles qui peuvent être déduites des seules métadonnées de ses appels et SMS sur la vie privée d'une personne. A savoir toutes les informations qui « entourent » un message : durée d'un appel, numéro appelé, heure de l'envoi d'un SMS… En bref, tout ce qui concerne un message, à l'exception de son contenu.
En 2013, le lanceur d'alerte Edward Snowden avait révélé que la NSA, les services secrets américains, et leurs partenaires procédaient à une surveillance de masse de ces métadonnées, enregistrant quotidiennement les informations autour de millions de messages. La NSA affirme depuis 2013 que ces informations ne revêtent pas un caractère privé, mais qu'elles sont indispensables à l'efficacité de ses actions, notamment en matière de lutte contre le terrorisme.
Les conclusions de l'étude menée par les chercheurs de Stanford montrent tout le contraire. Pendant plusieurs mois, ils ont enregistré, avec l'accord des 823 participants à l'étude, les métadonnées de 251 788 appels et de 1 234 231 SMS. Ils ont ensuite analysé de manière automatique les tendances récurrentes dans les métadonnées. Des appels réguliers à des commerces dans une zone géographique précise peuvent par exemple indiquer que la personne habite dans ce quartier. Les chercheurs ont ensuite procédé à des analyses « manuelles » pour identifier des numéros appelés et tenter d'en déduire des informations sur la vie privée des participants.

GROSSESSE, PROBLÈME CARDIAQUE, ARMES À FEU…

Ils sont ainsi parvenus à déterminer que l'un des participants venait de se voir diagnostiquer un problème cardiaque : après un long appel à un centre de cardiologie, l'homme avait appelé un laboratoire médical, puis reçu plusieurs coups de fil d'une pharmacie, avant d'appeler le service consommateur d'une entreprise qui commercialise des outils permettant de surveiller son rythme cardiaque. Dans d'autres cas, la seule analyse des métadonnées a permis de montrer l'existence de grossesses, ou le fait qu'une personne avait acheté une arme à feu.
Les analyses automatiques des données se sont révélées moins précises : la technique n'a permis d'identifier la ville où résident les participants à l'expérience que dans 57 % des cas – mais dans 90 % des cas, l'analyse a permis de déterminer la localisation des personnes à moins de 80 km de leur domicile réel.
Interrogé par le Guardian, l'un des coauteurs de l'étude, Patrick Mutchler, affirme que ces résultats sont bien en deçà de ce dont sont capables les agences de renseignement, qui disposent de moyens considérables. « Gardez à l'esprit que [ces résultats] ne sont que le reflet de ce que peuvent faire deux doctorants disposant de ressources limitées. »… [Lire la suite]

Réagissez à cet article

Source : *Les métadonnées téléphoniques révèlent des informations très privées*

Et si la reconnaissance faciale de Facebook était excessive ?

Et si la reconnaissance faciale de Facebook était excessive ?

Depuis 2010, Facebook propose à ses utilisateurs un système de reconnaissance faciale qui permet de gagner du temps dans le « taguage » des personnes qui sont sur les photos. Sous couvert d'une nouvelle fonctionnalité, c'est un véritable dispositif biométrique qui a été mis en œuvre car il permet d'identification d'un individu à partir d'une simple photographie de son visage.

En Californie, trois utilisateurs ont reproché au réseau social n°1 d'avoir « secrètement et sans leur consentement » collecté des « données biométriques dérivées de leur visage ». Ces plaintes ont été jugées recevables par le juge James Donato qui « accepte comme vraies les allégations des plaignants » et juge « plausible » leur demande.

Au sein de l'Union européenne, le danger a rapidement été perçu s'agissant du système de reconnaissance faciale de Facebook qui l'a suspendu en 2012. Mais aux Etats-Unis, bien moins vigilants, cette fonctionnalité a perduré et il apparait bienvenu que la Justice y réagisse enfin. Facebook a constitué des profils qui répertorient les caractéristiques du visage de ses utilisateurs, leur cercle d'amis, leurs goûts, leurs sorties, etc. Avec plus de 3 milliards d'internautes dans le monde, cela revient à ce qu'environ 28% de la population ait un double virtuel rien que sur Facebook.

Facebook is watching you : Reconnaissance faciale, intelligence artificielle et atteinte aux libertés

Eu égard à leur grand potentiel discriminatoire, les données biométriques sont strictement encadrées par la loi du 6 janvier 1978 puisque d'après son article 25, une autorisation préalable de la Commission nationale de l'informatique et des libertés est indispensable pour mettre en œuvre des « traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ». Cela regroupe l'ensemble des techniques informatiques qui permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les conditions générales d'utilisation de Facebook ne sont pas donc pas conformes à la législation française sur les données personnelles, notamment s'agissant de la condition de consentement préalable, spécifique et informé au traitement des multiples données à caractère personnel collectées. Mais le géant de l'internet ne répond qu'à l'autorégulation. Par opposition à la règlementation étatique, la régulation n'entend prendre en compte que la norme sociale, c'est-à-dire l'état des comportements à un moment donné. Si la norme sociale évolue, alors les pratiques de Facebook s'adapteront.

Vers une remise en cause mondialisée des abus de Facebook ?

L'affaire pendante devant les Tribunaux met en lumière le manque de réactivité des américains face aux agissements de Facebook. C'est seulement au bout de 5 années que la Justice s'empare de la question des données biométriques à l'initiative de simples utilisateurs, alors même qu'une action de groupe à l'américaine d'envergure aurait pu être engagée pour mettre sur le devant de la scène les abus de Facebook.

Néanmoins, « mieux vaut tard que jamais » et l'avenir d'une décision répressive ouvre la porte vers de nouveaux horizons pour l'ensemble des utilisateurs. En effet, Facebook prend comme modèle pour toutes ses conditions générales d'utilisation à travers le monde la version américaine de « licencing ». Plus Facebook se verra obligé dans son pays natal à évoluer pour respecter les libertés individuelles des personnes inscrites, plus on s'éloignera du système tentaculaire imaginé par Mark Zuckerberg qui n'est pas sans rappeler celui imaginé par Georges Orwell dans son roman 1984.

Par Antoine CHERON, avocat associé, est docteur en droit de la propriété intellectuelle, avocat au barreau de PARIS et au barreau de BRUXELLES et chargé d'enseignement en Master de droit à l'Université de Assas (Paris II). Il est le fondateur du cabinet d'avocats ACBM… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Facebook is watching you : système biométrique efficace – Data Security BreachData Security Breach*

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

---

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*

Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Oui, selon les sénateurs, qui ont réservé cette publication aux particuliers sur des sites strictement non commerciaux pour protéger les droits des créateurs.

Avez-vous le droit de photographier la pyramide du Louvre, et d'en publier l'image sur les réseaux sociaux ? Avez-vous le droit de vous prendre en photo devant la tour Eiffel illuminée en arrière-plan, et de diffuser le cliché ? C'était tout l'enjeu de la « liberté de panorama » qui était soumise à la discussion parlementaire dans le cadre du vote de la loi numérique. Et comme les députés avant eux, les sénateurs ont répondu non. Sauf à demander son avis à l'ayant-droit de l'oeuvre, il sera possible de diffuser des photos de bâtiments ou de sculptures protégées par le droit d'auteur, mais en les réservant aux seuls particuliers et à l'exclusion de tout usage à caractère directement ou indirectement commercial. Excluant de ce champ les associations, les sénateurs ont plongé Wikimedia (l'association qui a pour objet la diffusion de connaissance, via Wikipedia entre autres) dans un cauchemar sans fin : le site internet ne pourra désormais plus illustrer ses articles avec des photos des œuvres dont il parle.

Protéger la démarche artistique

L'objectif de cet amendement est d'empêcher un quidam de tirer un bénéfice financier de l'utilisation d'une photo d'une œuvre (même si c'est lui qui l'a prise) sans en avoir demandé l'autorisation aux ayants-droit de leur créateur, de manière à protéger la création. L'amendement concerne « les reproductions et représentations d'oeuvres architecturales et de sculptures, placées en permanence sur la voie publique », comme par exemple les illuminations de la tour Eiffel ou encore la pyramide du Louvre.

Mais les partisans d'une liberté totale de panorama pointent les restrictions considérables qu'apporte cet amendement. En effet, de tels clichés devenant interdits pour « tout usage à caractère directement ou indirectement commercial », ils seront désormais interdits de séjour sur les réseaux sociaux comme Facebook, Twitter ou Instagram. Il ne restera plus qu'à patienter jusqu'à ce que les œuvres tombent dans le domaine public (70 ans après la mort de l'artiste) pour partager entre amis un selfie touristique, ou bien créer un site internet personnel ne laissant aucune place à la publicité. Le nain de jardin d'Amélie Poulain, photographié devant les monuments du monde entier pour les besoins d'un film – commercial –, ne connaîtrait plus aujourd'hui le même fabuleux destin…. [Lire la suite]

Réagissez à cet article

Source : *Liberté de panorama : publier un selfie devant la pyramide du Louvre, est-ce du vol ?*

Comment fonctionnent les Kits

d’exploitation ?

Comment fonctionnent les Kits d’exploitation ?

Ces dernières années, nous avons observé une augmentation massive de l'utilisation des kits d'exploitation de vulnérabilités. Aucun site web n'est de taille face à la puissance d'un grand nombre de ces kits, à l'image de celui d'un célèbre quotidien britannique, notoirement victime d'une campagne de publicité malveillante exposant des millions de lecteurs au ransomware CryptoWall.

Les Exploit kits, des boites à outils faciles à utiliser

Cependant, l'aspect peut-être le plus préoccupant des kits d'exploitation tient à leur facilité d'utilisation. Ces « boîtes à outils à louer » ont principalement pour but de réduire les compétences techniques nécessaires au lancement de campagnes de malware, afin qu'un assaillant n'ait pas besoin de créer ou implanter le code malveillant lui-même. De fait, de nombreux kits s'accompagnent même désormais d'une interface ergonomique, permettant aux malfaiteurs de gérer et de surveiller leur malware tout au long d'une campagne.

La charge malveillante des kits d'exploitation se présentait jusque-là sous la forme de différentes sortes de malwares, qu'il s'agisse de fraude au clic publicitaire, de malware bancaire ou de ransomware, la nature de ces attaques variant selon le profil de l'utilisateur. Compte tenu de la facilité de personnalisation d'une attaque et de l'ergonomie des kits, il n'est guère surprenant que ceux-ci soient devenus l'arme de prédilection d'un grand nombre de cybercriminels, moins compétents sur le plan technique.

De quoi sont-ils faits ?

En règle générale, l'infrastructure d'un kit d'exploitation comprend trois composants :

- le « back-end », qui contient le tableau de commande et les charges malveillantes ;
- la couche intermédiaire, qui héberge le code malveillant et crée un tunnel dans le serveur back-end ;
- la couche proxy, qui transmet le malware directement à la victime.

La chaîne d'infection/exploitation demeure en outre largement similaire pour les différents kits :

- La victime se rend sur le site web, entièrement ou partiellement contrôlé par l'assaillant ;
- Elle est ensuite redirigée à travers de nombreux serveurs intermédiaires ;
- À son insu, elle aboutit sur le serveur hébergeant le kit d'exploitation ;
- Le kit tente alors de s'installer en exploitant une vulnérabilité logicielle sur le serveur cible ;

En cas d'installation réussie, la charge malveillante est alors activée.

La différence marquante entre les kits réside dans les types de vulnérabilités exploitées pour infecter les visiteurs et les diverses astuces employées pour échapper aux antivirus.

Vers la multiplication des cibles mobiles

Alors que les kits d'exploitation avaient traditionnellement tendance à cibler principalement les ordinateurs, les appareils mobiles sont de plus en plus visés en raison du grand nombre d'utilisateurs qui s'en servent pour surfer sur le Web, échanger des e-mails, consulter les réseaux sociaux et même pour effectuer des opérations bancaires. La plupart de ces utilisateurs n'étant pas au fait des meilleures pratiques pour sécuriser correctement leur mobile, ils offrent par essence une cible bien plus facile.

Il faut donc s'attendre à ce que les auteurs des attaques s'orientent progressivement vers la diffusion de malware mobile via des pages web sur un navigateur mobile, c'est-à-dire essentiellement le même mode d'infection que dans la plupart des cas sur les ordinateurs.

Dès lors que le virus réussit à s'implanter sur un ordinateur ou un mobile, il peut opérer derrière les firewalls d'une entreprise ou d'un particulier. Le malware se propage ainsi à d'autres équipements et se connecte au serveur de commande et de contrôle (C&C) via Internet, ce qui lui permet ensuite d'exfiltrer des données ou de télécharger d'autres logiciels malveillants. Cette communication entre le serveur C&C et la machine infectée passe souvent par le serveur de noms de domaines (DNS) de la cible.

Connaître son ennemi

Même si tous les kits d'exploitation ne sont pas identiques, il est important d'en identifier deux principaux.

Le baromètre Infoblox des menaces DNS observées au 4ème trimestre 2015 révèle que le kit Angler a représenté 56 % des nouvelles activités de ce type, et le kit RIG 20 %. En quoi consistent ces kits et leurs activités ?

Le kit d'exploitation Angler est l'un des plus élaborés actuellement utilisé par les cybercriminels. Notoirement connu pour avoir inauguré la technique du « masquage de domaine », Angler peut ainsi contrer les stratégies de blocage sur la base de la réputation et infiltrer des URL malveillantes dans des réseaux publicitaires légitimes. Il redirige ensuite les visiteurs du site web qui cliquent sur les liens publicitaires infectés vers d'autres sites qui implantent à leur tour un malware. Ces kits tendent à être actualisés avec les dernières failles « zero day » découvertes dans des logiciels répandus, tels que Apache Flash ou WordPress. Si l'on y ajoute l'utilisation de techniques complexes de dissimulation, cela rend Angler particulièrement difficile à détecter pour les solutions antivirus classiques.

Face à cette évolution constante, les entreprises doivent investir dans des technologies de protection qui non seulement bloquent un composant du kit Angler mais sont aussi capables d'identifier et d'interrompre l'activité malveillante sur l'ensemble de la chaîne d'infection.

Bien que de conception plus ancienne, le kit d'exploitation RIG a récemment fait son retour. Cela montre que les menaces passées peuvent réapparaître sous une nouvelle forme à mesure que les kits sont mis à jour. L'analyse par Infoblox de l'activité de RIG en 2015 révèle que celui-ci a commencé à utiliser des techniques de masquage de domaine similaires à celles employées par Angler.

Même si RIG est souvent déployé dans le cadre de campagnes de publicité malveillante, Heimdal Security a récemment découvert qu'il sert également pour la pollution de référencement Google, consistant à détourner les tactiques d'optimisation du moteur de recherche pour faire la promotion de sites web malveillants.

Avec leurs différentes déclinaisons et techniques, les kits d'exploitation offrent aux malfaiteurs dépourvus de compétences techniques l'opportunité de tirer profit du monde de la cybercriminalité. Pour se protéger contre cette menace sans cesse croissante, les entreprises doivent faire appel à une source fiable de veille des menaces et s'appuyer sur ces informations pour interrompre les communications des malwares passant par des protocoles au sein de leur propre infrastructure, notamment le DNS… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Suivez-nous sur

Réagissez à cet article

Source : *Comment fonctionnent les Kits d'exploitation ? – Global Security Mag Online*

Des hackers proches de Daech menacent les New-Yorkais

Des hackers proches de Daech menacent les New-Yorkais

Un groupe de hackers liés à Daech a dévoilé sur Internet une liste contenant les données personnelles de milliers de new-yorkais et a exhorté les adeptes du groupe à les cibler.

Les hackers ont mis en ligne non seulement les noms des New-Yorkais, mais aussi les lieux de résidence et leurs adresses électroniques, rapporte le Reuters, qui précise qu'une grande partie des données sont désuètes. En outre, la liste inclut les données personnelles d'un grand nombre de fonctionnaires du département d'Etat américain ainsi que de citoyens sans relations avec les services publics.
Des agents fédéraux et des policiers de New York ont contacté les personnes figurant sur la liste pour les informer, mais les forces de l'ordre ne considèrent pas cette menace comme crédible, indique la source.
« Bien que notre pratique courante consiste à refuser de commenter les questions opérationnelles et les enquêtes spécifiques, le FBI avertit régulièrement les individus et les organisations sur l'information recueillie au cours d'une enquête qui peut être perçue comme une menace potentielle », stipule la déclaration du FBI.
Précédemment, le groupe de pirates informatiques de Daech connu comme « Cyber-califat uni » a annoncé qu'il avait obtenu les informations personnelles de 50 employés du département d'Etat américain, y compris leurs noms et numéros de téléphones. Pour le prouver, les pirates ont publié des captures d'écran et ont menacé d' »écraser » les Etats-Unis, de tuer ces employés et de détruire le système de sécurité nationale. De son côté, le département d'Etat américain n'a fourni aucun commentaire.

Croyant attaquer Google, les hackers de Daech manquent leur cible
Auparavant, les Etats-Unis avaient ouvert une nouvelle ligne de combat contre l'Etat islamique, comprenant des attaques contre des réseaux informatiques de Daech. Des cyberattaques seront réalisées contre l'Etat islamique parallèlement à l'usage des armes traditionnelles.
Depuis 2013, les autorités américaines ont arrêté plus de 70 personnes pour collaboration avec l'Etat islamique… [Lire la suite]

Réagissez à cet article

Source : *Des hackers proches de Daech menacent les New-Yorkais*

Peut-on s’attendre à la fin de la loi Hadopi ?

Peut-on s’attendre à la fin de la loi Hadopi ?

Les députés ont adopté un amendement qui supprimera l'institution Hadopi en 2022, mais même s'il est promulgué en l'état, le texte ne fait pas disparaître la riposte graduée, qui pourra être reprise par une autre administration.

Il ne faut pas confondre l'Hadopi et la loi Hadopi

Victimes d'un excès d'optimisme, certains imaginent que la riposte graduée elle-même disparaîtra en 2022. Mais il n'en est rien. Si les quatre députés qui ont fait majorité ont bien voté une mise à mort de l'institution Hadopi, il n'en va pas de même pour la riposte graduée.

Plusieurs raisons invitent donc à ne pas sauter trop vite aux conclusions :

Sur l'ensemble des quatre sous-sections du code de la propriété intellectuelle dédiées à la riposte graduée, seule la première intitulée « Compétences, composition et organisation » sera supprimée le 4 février 2022. Les autres, notamment la troisième relative à la riposte graduée, est conservée.

Il sera donc facile pour le législateur de pérenniser la riposte graduée en confiant simplement la riposte graduée à une autre autorité administrative. Comme nous l'expliquions hier, c'est ce qui est proposé dans le rapport Warsmann qui accompagne la proposition de loi examiné par les députés, sur les autorités publiques ou administratives indépendantes : « les compétences (de l'Hadopi) pourraient être transférées soit au CSA, soit à l'ARCEP, soit à une nouvelle AAI ayant une compétence élargie en ces matières ».

Avant cela, le Sénat pourra faire sauter la disposition lorsqu'il examinera lui-même la proposition de loi. Lui qui et traditionnellement attaché à la protection des droits d'auteur devrait y être sensible, même s'il ne sera sans doute pas fâché de se débarrasser d'une patate chaude à quelques mois de la campagne présidentielle.

Enfin, quand bien même le texte serait-il adopté et promulgué, il restera cinq ans à la prochaine majorité, pour glisser dans un projet de loi un amendement qui supprimera l'article qui supprime l'Hadopi. Une seule ligne suffira.

Pour toutes ces raisons, aucun cri d'orfraie n'a été entendu ce vendredi du côté des ayants droit, d'habitude très prompts à publier des communiqués rageurs dès que leurs intérêts sont bousculés. Ils savent que l'affaire est plus anecdotique qu'autre chose, et que le bug législatif sera vite réparé. Voire, que l'amendement adopté leur rend service, puisqu'il précipitera un éventuel transfert des compétences de l'Hadopi vers le CSA, qu'ils appellent de leurs vœux depuis plusieurs années… [Lire la suite]

Réagissez à cet article

Source : *Non, la loi Hadopi ne va pas mourir – Tech – Numerama*

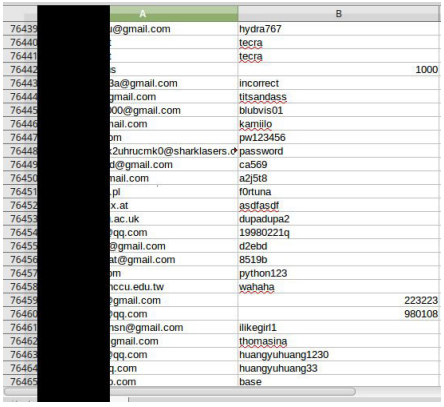
Un site Internet pour adultes piraté. Les comptes d'accès bradés sur le BlackMarket

Un site Internet pour adultes piraté. Les comptes d'accès bradés sur le BlackMarket

---

Un internaute a tenté de revendre les données de 270 000 amateurs de sites pornographiques dans le blackmarket. Le business du Porn Account pour les nuls !

Vous avez peut-être entendu à la radio et lu dans la presse généraliste ce piratage de données ayant visé 270 000 amateurs de sites pornographiques. Un piratage qui a débuté via l'attaque par injection SQL de plusieurs sites pour adultes appartenant au groupe Paper Street Media.
Le pirate a expliqué avoir contacté l'entreprise pour « discuter ». Soyons clair, il a tenté de leur soutirer de l'argent en proposant la faille qui lui a permis d'extraire les informations des clients (IP, mail, mots de passe…).
Paper Street Media n'a pas répondu dans le sens de l'internaute. Bilan, l'adolescent a mis en vente, dans le blackmarket, la base de données volée pour 360 euros. Pourquoi revendre les données dans le BM ? Toutsimplement pour que les professionnels du porn account puissent sauter sur l'occasion.
Dans cette même boutique qui aurait servi au pirate à revendre cette base de données [je n'ai pas retrouvé le vendeur], d'autres « commerçants » proposent des accès « piratés » aux sites interdit au – de 18 ans de Paper StreetMedia pour 9 $. Je vous laisse faire l'addition. Nous sommes très très loin des 360 euros réclamés ! « **Je peux me faire entre 300 et 500 dollars par semaine** » m'indique un de ces vendeurs de Porn Account croisé dans une boutique spécialisée.



	A	B
76439	[redacted]@gmail.com	hydra767
76440	[redacted]	tecra
76441	[redacted]	tecra
76442	[redacted]s	1000
76443	[redacted]3a@gmail.com	incorrect
76444	[redacted]gmail.com	titsandass
76445	[redacted]00@gmail.com	blubvis01
76446	[redacted]ail.com	kamiilo
76447	[redacted]m	pw123456
76448	[redacted]2uhrucmk0@sharklasers.c	password
76449	[redacted]d@gmail.com	ca569
76450	[redacted]ail.com	a2j5t8
76451	[redacted].pl	f0rtuna
76452	[redacted]x.at	asdfasdf
76453	[redacted].ac.uk	dupadupa2
76454	[redacted]qq.com	19980221q
76455	[redacted]@gmail.com	d2ebd
76456	[redacted]at@gmail.com	8519b
76457	[redacted]m	python123
76458	[redacted]ccu.edu.tw	wahaha
76459	[redacted]gmail.com	223223
76460	[redacted]qq.com	980108
76461	[redacted]nsn@gmail.com	ilikegirl1
76462	[redacted]gmail.com	thomasina
76463	[redacted]qq.com	huangyuhuang1230
76464	[redacted]q.com	huangyuhuang33
76465	[redacted]o.com	base

Un pirate russe revend des milliers de comptes du site Naughty America.
A noter que j'ai pu consulter [ci-dessus] un document diffusé par un autre pirate informatique. Ce dernier, il est russe, a mis la main sur 150 000 comptes clients du site pornographique Naughty America. Un injection SQL, une backdoor (shell) dans le serveur et les comptes clients ont fini dans les mains du pirate.

Pendant ce temps…
… le groupe hôtelier Trump est de nouveau piraté. Des logiciels d'espionnage ont été retrouvés dans les ordinateurs des hôtels Trump situés à New York, Toronto et Honolulu. Même type d'attaque vécue en juillet 2015. Cela donne une idée de la gestion de la sécurité informatique de ce groupe. Les pirates visaient les identités et les données bancaires.
En ce qui concerne les numéros de CB, pas besoin d'être intelligent pour comprendre l'intérêt. Achats de produits dématérialisés qui seront revendus moitié prix [blanchir l'argent détourné]… En ce qui concerne les informations dédiées aux identités : fraude bancaire [ouverture de compte], usurpation d'identité, … [Lire la suite]

Réagissez à cet article

Source : *Porn Account : 270000 amateurs de pornos piratés – Data Security BreachData Security Breach*

Mieux connaître le

consommateur avec ses données

	**Mieux connaître le consommateur avec l'analyse prédictive et le Big Data**

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients.

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients. Habitudes d'achat, fréquence et lieux des visites, horaires… Toutes ces informations forment une base de données gigantesque et sans cesse en mouvement. C'est ce que l'on nomme « Big Data » et il s'agit d'une véritable mine d'or pour les professionnels du marketing. Fini les suppositions logiques et autres préjugés, l'analyse prédictive permet maintenant de dégager des statistiques et schémas de consommation concrets.

D'où viennent les informations qui composent le Big Data ?

Chaque fois que vous activez votre géolocalisation en consultant un site internet ou une application, cela laisse une trace. Les données du Big Data sont également composées par vos habitudes de navigation sur le net, les endroits où vous vous rendez, combien de temps vous restez, d'où vous venez, ce que vous regardez… Bien sûr toutes ces informations sont rendues anonymes, mais vos terminaux, dont votre smartphone, sont de véritables espions dans votre poche. Un data scientist, tels que sont nommés les experts du Big Data, s'intéressera aux patterns et croisera vos données avec celles de milliers d'autres personnes. Il s'agira par exemple de créer des algorithmes adaptés aux habitudes de navigation des utilisateurs d'un moteur de recherche. L'idée est d'aller chercher dans les données des tendances, et d'identifier des comportements. Analyser, comprendre… puis prédire les actions futures. Cela est désormais possible et relativement simple avec les outils dont disposent les analystes.

Le Big Data, un outil d'analyse prédictive qu'il faut savoir exploiter

Si le Big Data peut servir à améliorer l'expérience des utilisateurs d'un produit, il révèle surtout son potentiel dans le secteur du marketing. Grâce à l'analyse du flot des données, il est possible d'établir des segments toujours plus pertinents. Finie la publicité « à destination de la ménagère de 40 ans ». Vous êtes désormais en mesure de savoir qui est réellement susceptible d'utiliser vos produits, et avec quel argument mettre en avant votre offre. Bien sûr, cela demande un réel travail d'analyse et ce n'est pas un hasard si vous voyez fleurir les offres d'emploi de data scientist ou de data mining. Le marketing et l'analyse prédictive deviennent des travaux de statisticien. Cela demande également de disposer des bons outils. Il s'agit d'un investissement en plusieurs étapes :

1. Vous collectez les données transmises par toutes les sources pertinentes ;
2. Vous analysez les données et isolez les schémas de consommation qui vous intéressent. L'étude de leurs occurrences sera la base de vos analyses prédictives ;
3. Enfin, vous établissez une stratégie de marketing ciblée en fonction des résultats obtenus.

Pour une efficacité maximale, la majeure partie de ce processus sera automatisée. Pour gagner en efficacité mais aussi en efficience grâce à des outils de traitement des données en temps réel, il est possible de créer des processus semi-automatisés. L'intervention humaine n'est plus utile ? C'est le contraire. Elle est essentielle. L'œil humain est là pour aller chercher dans les données, fouiner et faire émerger des signaux faibles. La technologie libère le potentiel des données, mais il faut une intervention humaine pour bien utiliser ces outils, et en tirer des décisions actionnables.

Comment se servir de l'analyse prédictive pour optimiser son ROI ?

S'il peut être intéressant d'analyser le Big Data pour de multiples raisons, en matière de marketing l'objectif est avant tout d'améliorer votre ROI (Return On Investment). Pour cela, votre démarche analytique doit s'inscrire dans un plan d'action concret.
Que vous soyez spécialisé dans le e-commerce ou que vous réalisiez toutes vos ventes dans des magasins physiques, utilisez les données pour améliorer votre marketing digital.

Lancez des campagnes de marketing ciblées ;

Démarquez-vous du flot de publicité, et adaptez votre proposition aux envies réellement exprimées de vos clients.
Mais l'analyse prédictive ne sert pas qu'à générer des ventes. Elle trouve aussi son utilité dans le maintien de la relation client. Il est par exemple possible de déterminer quand un client est sur le point de résilier un abonnement, quand celui-ci est sur le point de basculer chez un concurrent… pour pouvoir le retenir ! A l'aide de ces informations contenues dans votre Big Data, vous pouvez améliorer votre taux de fidélité en adaptant vos offres au bon moment. Un exemple ? La chaîne d'hôtel Hyatt utilise désormais l'analyse prédictive pour donner à son personnel d'accueil des informations supplémentaires sur les clients. En analysant la recherche menée par ces derniers sur le site et les applications du groupe, Hyatt précise si un client peut être intéressé par une chambre avec vue (car il a regardé plusieurs fois la page) ou s'il désire peut-être une chambre avec des oreillers anallergiques, car il a tapé ce mot clé dans le moteur de recherche interne… Un bel exemple de personnalisation de la relation client, grâce aux données.M… [Lire la suite]

Suivez nous sur

Réagissez à cet article

Source : *Analyse prédictive et Big Data : mieux connaître le consommateur avec ses données*