Les sites Internet de la Gendarmerie et de la Police attaqués par des Anonymous pour dénoncer les bavures

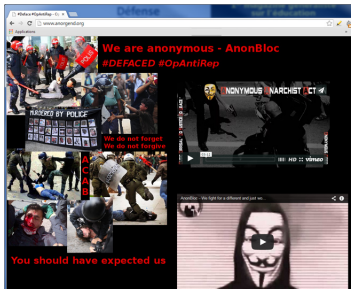
	Les sites Internet de la Gendarmerie et de la Police attaqués par des Anonymous pour dénoncer les bavures

Aux manifestations organisées partout en France samedi dernier contre les violences policières se sont jointes des opérations menées en ligne par un collectif affilié à Anonymous. Des bases de données sur des Gendarmes ont été publiées, et des sites ont été piratés.

Les manifestations en hommage à Rémi Fraisse et contre les violences policières qui se sont déroulées samedi dernier dans une vingtaine de villes françaises ont également connu un relais immatériel. Dans le cadre d'une action mondiale « contre les répressions policières » baptisée #OpAntiRep, un collectif de hackers anonymes utilisant la bannière Anonymous a réalisé samedi une série d'actions, en particulier contre les policiers et gendarmes italiens, mais également en France.

Outre d'habituelles attaques DDOS qui ont provoqué l'indisponibilité d'une vingtaine de sites internet, dont celui du syndicat de policiers Alliance http://anorgend.org, le collectif a surtout piraté le forum d'un site internet dédié aux réservistes de la Gendarmerie http://www.reserve-gendarmerie.org, destiné à « faire connaître la réserve et à mettre en relation les réservistes et candidats ». Ils affirment avoir réussi à pirater les noms, adresse e-mail, adresse IP et mot de passe (pour certains déchiffrés) de quelques 2 000 membres inscrits sur ce forum, et fournissent une capture d'écran de la base de données en guise de preuve :

Ce lundi, le site non officiel de la réserve de la Gendarmerie française était toujours fermé, un message expliquant aux visiteurs qu'il était « en maintenance ». Le forum est toutefois accessible, et affiche 1544 membres inscrits à l'heure où ces lignes ont été publiées sur le site source.
D'autres actions ont été menées, notamment contre le site de l'Association nationale des officiers de réserve de la Gendarmerie nationale (Anorgend), qui a été piraté pour en modifier la page d'accueil, désormais toute à la gloire d'Anonymous. Là aussi, une base de données de membres avec des mots de passe chiffrés a été diffusée :

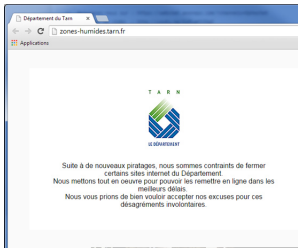


Dans un communiqué diffusé dans trois langues, le collectif #OpAntiRep explique que la journée du 22 novembre avait « pour origine des collectifs – occupants de différentes ZAD (Zones à défendre) – suite au décès par grenade offensive d'un étudiant en écologie lors d'un rassemblement », et affirme que « partout dans le monde, de nombreux camarades ont été tués ou blessés par leurs armes dans des manifestations contre l'oppression de ces gouvernements,sous la pression du monde capitaliste qui veut imposer ses projets de société ». L'appel à manifester partout dans le monde avait été relayé sur un site anarchiste.

« Nous devons informer le peuple par toutes les tactiques possibles », ajoutait le collectif Anonymous pour expliquer le sens de sa mobilisation en ligne. « Nous ne pouvons pas tolérer plus longtemps que le peuple soit mis à genoux par des robots sans âmes. Qui « servent et protègent » des machines, des institutions capitalistes et l'injustice. Nous protégeons le peuple. Nous ripostons ! ».
L'appel d'Anonymous France à agir en ligne le 22 novembre avait été lancé le 11 novembre dernier par une vidéo sur YouTube, vue près de 7000 fois :

D'autres documents ont été obtenus par les pirates, dont le plus sensible est le calendrier prévisionnel de positionnement et de relève des unités de CRS en France, dans le cadre des missions permanentes, jusqu'à la fin de l'année 2014. Le reste est plus anecdotique, avec la grille de rémunérations des CRS en fonction des grades, le règlement intérieur des compagnies, ou encore un manuel détaillé des véhicules de reconnaissance utilisés par les CRS.

Dès la fin octobre, Anonymous avait réagi à la mort de Rémi Fraisse en affirmant qu'il « ne restera pas les bras croisés », et en annonçant une « Opération Testet » (#OpTestet) pour s'opposer au barrage de Sivens sur la zone humide du Testet. S'en était suivie une série d'actions menées notamment contre le site officiel de la Région du Tarn ou celui de la FNSEA locale :



Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.numerama.com/magazine/31367-opantirep-anonymous-s-attaque-a-la-gendarmerie-francaise.html

---

Virus Regin : Conséquences informatiques ou clash diplomatique ?

Virus Regin : Conséquences informatiques ou clash diplomatique ?

REGIN – Il est déjà considéré comme l'un des malwares les plus sophistiqués de l'histoire de l'informatique. « Regin », le mystérieux logiciel malveillant dont le spécialiste de sécurité Symantec (éditeur de l'antivirus Norton) a révélé l'existence dimanche soir, pourrait bien continuer à faire parler de lui.

Selon le site américain The Intercept, les services de renseignement américains et britanniques se cacheraient derrière. Pour mémoire, The Intercept a été créé par Glenn Greenwald, l'enquêteur ayant publié les révélations d'Edward Snowden sur les programmes de surveillance la NSA.
Citant des sources du secteur et une analyse technique du logiciel, The Intercept affirme que « Regin » est référencé dans des documents fournis par Edward Snowden lui-même, alors qu'il était encore consultant de l'agence américaine de renseignement. Interrogée sur ces informations, une porte-parole de la NSA a répondu par un lapidaire: « Nous n'allons pas commenter des rumeurs ».

L'affaire est néanmoins prise très au sérieux car « Regin » avait des objectifs très ambitieux
le malware aurait été utilisé contre des réseaux informatiques de gouvernements européens et Belgacom, le réseau public de télécommunications belge.
Dans le détail, « Regin » serait capable d'apporter une grande flexibilité aux attaquants. En effet, ces derniers seraient en mesure de charger des fonctions personnalisées adaptées à des objectifs individuels en cas de besoin. Le virus serait notamment capable de réaliser des captures d'écran, de prendre le contrôle d'une souris et de son curseur, de voler des mots de passe, de surveiller le trafic d'un réseau, et de récupérer des fichiers effacés.

Après l'abandon du dossier des « écoutes Merkel »
Si la nature des assaillants parvient à être authentifiée, les vieux démons pourraient se réveiller des deux côtés de l'Atlantique. L'affaire des écoutes de la NSA venait pourtant de refroidir avec l'abandon samedi de l'enquête concernant la mise sur écoute présumée d'un téléphone d'Angela Merkel. Selon le magazine allemand Focus, aucune preuve n'aurait été trouvée sur la responsabilité de la NSA. « Regin » pourrait donc raviver les tensions.
Interrogé par The Intercept, l'expert en sécurité qui a aidé à supprimer le logiciel espion des réseaux de Belgacom est formel. « Après avoir analysé ce malware et regardé les documents Snowden, je suis convaincu que Regin est utilisé par les services de renseignement américain et britannique », a affirmé Ronald Prins. C'est lui qui permet à l'équipe de Glenn Greenwald d'être si confiante dans ses affirmations.
D'autres sources abondent dans ce sens. « Nous sommes convaincus que ce produit est l'oeuvre des Etats-Unis ou de la Grande-Bretagne », a assuré à SC Magazine Erik de Jong, un expert en cyber-sécurité de la firme Fox-IT. « Nous avons examiné les documents de Snowden, les pièces s'imbriquent ». La société finlandaise F-Secure assure sur son blog que le virus, « pour une fois », ne vient pas de Russie ou Chine.

« Considéré comme révolutionnaire »
Symantec se dispense de donner des noms, mais plutôt des indices sur le niveau de sophistication. « Dans le monde des virus informatiques, rares sont les exemples qui peuvent être réellement considérés comme révolutionnaires. Ce que nous avons là en fait partie ». C'est par cette phrase que débute le rapport de la société publié dimanche.
La complexité de « Regin » implique une phase de conception ayant duré plusieurs mois, voire plusieurs années, et qui a nécessité un investissement financier important. « Le temps et les ressources employés indiquent qu'une nation est responsable », assure Candid Wueest, un chercheur travaillant pour le spécialiste américain de la sécurité informatique.

Encore difficile d'identifier formellement le(s) responsable(s)
Pas question néanmoins d'accuser formellement un Etat. « On ne fait pas d'attribution tant que l'on n'a pas de faits concrets, de preuves irréfutables », se justifie-t-il, « mais il est certain qu'on peut tirer des conclusions ». Chez Kaspersky Lab, le principal concurrent de Symantec en matière de sécurité informatique, on se refuse également à pointer du doigt un pays en particulier. La compagnie russe explique néanmoins que ce virus ne peut avoir été développé qu'avec le financement et les moyens techniques d'une agence nationale de renseignement.
Les experts détaillent ensuite le processus. « Les équipes de Symantec ont détecté des brèches de sécurité avérées dans 10 pays, en premier lieu la Russie puis l'Arabie saoudite, qui concentrent chacune environ un quart des infections », a indiqué Candid Wueest. Les autres pays touchés par ordre d'importance sont le Mexique et l'Irlande suivis par l'Inde, l'Afghanistan, l'Iran, la Belgique, l'Autriche et le Pakistan. Un travail d'orfèvre pour les spécialistes du genre.
Lire la suite….

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.huffingtonpost.fr/2014/11/25/regin-virus-snowden-nsa-gchq-belgique-greenwald_n_6217356.html
Par Grégory Raymond

Les ordinateurs de Sony Pictures piratés, et paralysés

Les ordinateurs de Sony Pictures piratés, et paralysés

Décidement, Sony Pictures est une cible de prédilection pour les pirates. En 2011, c'est le site du studio qui avait été compromis et des données personnelles dérobées. A présent, c'est le réseau informatique qui a fait l'objet d'une intrusion.

Comme le rapporte The Verge, les salariés des différents bureaux de Sony Pictures ont ainsi découvert une image inattendue sur l'écran de leur ordinateur au moment de se connecter à leur session.

Une entreprise paralysée

Une image représentant un squelette écarlate les informait qu'ils avaient été hacké par #GOP. Le message précise que des données sensibles de l'entreprise et ont été dérobées. Les pirates menacent d'ailleurs de les dévoiler sur Internet si leur demande n'est pas satisfaite – une ou des exigences qui ne sont pas précisées.

Les salariés de Sony Pictures étaient hier encore dans l'incapacité d'utiliser les outils informatiques, d'envoyer par exemple un mail ou même de répondre au téléphone – vraisemblablement de la ToIP.
Outre le blocage des ordinateurs de Sony Pictures, ce sont des douzaines de comptes Twitter de Sony qui ont été provisoirement piratés afin de tweeter le même message sur le réseau social. L'entreprise a depuis repris le contrôle de ces comptes Twitter.
Une affaire de plus à suivre…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/les-ordinateurs-de-sony-pictures-pirates-et-paralyses-39810107.htm

Un virus informatique prend pour cible la Russie et l’Arabie Saoudite

Un virus informatique prend pour cible la Russie et l’Arabie Saoudite

Un virus informatique très sophistiqué a lancé une attaque contre des opérateurs télécoms russes et saoudiens, a révélé la compagnie de cyber-sécurité Symantec.

Ce virus, baptisé « Regin », serait au moins aussi redoutable que « Stuxnet », qui avait causé de gros dégâts en 2010 dans le programme nucléaire iranien, retardant sans doute de plusieurs années les travaux des ingénieurs iraniens soupçonnés de mettre au point des armements nucléaires…
Stuxnet avait été développé par les services secrets américains et israéliens, selon des sources concordantes.

Un voleur qui fait disparaître ses traces…
Selon le ‘Financial Times’, qui cite lundi des sources au sein de Symantec, Regin pourrait lui aussi avoir été mis au point par des services secrets occidentaux, et serait d’une sophistication sans précédent… On ignore encore de quelle manière le virus infecte les systèmes informatiques, mais il s’est jusqu’à présent attaqué à des fournisseurs d’accès à internet en Russie, Arabie Saoudite, au Mexique en Irlande et en Iran.
Son objectif serait de dérober des données confidentielles, et il aurait la capacité de s’adapter à tous types de réseaux. Il serait aussi capable, dans certains cas, de faire disparaître toute trace de son passage une fois son forfait accompli… Regin aurait notamment ciblé les serveurs de messageries gérées par Microsoft, ainsi que les conversations de téléphones mobiles circulant sur de grands réseaux mondiaux.

L’industrie, nouvelle cible des « hackers », selon Kaspersky
Au même moment, Eugene Kaspersky, le directeur général d’une autre firme de sécurité informatique, Kaspersky Labs, a mis en garde contre la multiplication des cyberattaques contre les systèmes de groupes industriels, notamment dans le secteur énergétique (centrales électriques…). Selon lui, l’industrie est devenue la cible privilégiée du crime organisé, avec des attaques qui vont plus loin que les récents vols de données personnelles dont ont été victimes les clients de JP Morgan, Home Depot ou Target aux Etats-Unis. Les hackers ont notamment réussi à éviter que des chargements soient contrôlés dans des ports, ou à voler des stocks de céréales dans une usine ukrainienne en falsifiant les jauges pour qu’elles affichent des poids inférieurs à la réalité, a indiqué M. Kaspersky au ‘FT’…

L’an dernier, l’office de police criminelle intergouvernemental Europol avait rendu public le démantèlement d’un réseau de trafiquants de drogue, qui avaient « hacké » les ordinateurs du port belge d’Anvers… Les trafiquants étaient parvenus à déplacer les conteneurs contenant de la drogue pour leur éviter de subir des contrôles douaniers.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.boursier.com/actualites/economie/un-virus-informatique-prend-pour-cible-la-russie-et-l-arabie-saoudite-26186.html

Un livre consacré à la cybercriminalité souligne la nécessité d’un cadre juridique approprié

Un livre consacré à la cybercriminalité souligne la nécessité d’un cadre juridique approprié

Le magistrat sénégalais Pape Assane Touré a présenté, samedi à Dakar, son ouvrage consacré à la cybercriminalité, dans lequel il souligne la nécessité d’un cadre juridique approprié permettant de trouver «des solutions originales» à ce phénomène.

Intitulé «Le traitement de la cybercriminalité devant le juge : l’exemple du Sénégal», cet ouvrage édité par les éditions L’Harmattan (France), tente, selon son auteur, d’apporter des éléments de réponse au plan juridique à la lutte contre la cybercriminalité.

«Il s’agit d’apporter des éléments de réponse au plan juridique dans la lutte contre la cybercriminalité», a-t-il expliqué lors de la cérémonie de dédicace, en présence de magistrats, d’avocats et d’un public composé notamment de membres de sa famille.
«Il n’est pas possible d’apporter des réponses techniques ou économiques mais l’ouvrage a tenté d’apporter des réponses juridiques à la cybercriminalité mais une fois devant le juge», a dit l’auteur.
«On pensait que la cybercriminalité est un mythe pas une réalité mais à la réflexion, on se rend compte que c’est un phénomène réel. Ce sont les études rendues par les juridictions qui ont permis de se rendre compte de l’existence du phénomène», a-t-il souligné.
«Nous avons insisté sur la nécessité d’avoir un cadre juridique approprié. Le Sénégal l’a déjà, mais il est important d’avoir un juge qui ose aller au-delà des faits pour trouver des solutions originales au phénomène de la cybercriminalité», a indiqué Pape Assane Touré.

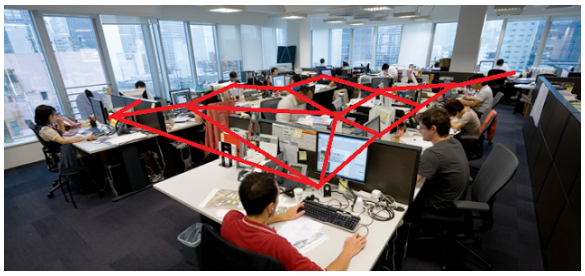
Selon le magistrat, conseiller technique au ministère de la Justice, le législateur seul ne peut apporter des réponses concernant par exemple le piratage dans le domaine informatique.

«Les instances juridiques, les intermédiaires de l’Internet, les conditions d’accès, d’hébergement voire tous les acteurs doivent aller ensemble pour trouver une réponse globale et définitive à la cybercriminalité», a-t-il déclaré.
Intervenant lors de cette cérémonie de dédicace, le garde des Sceaux, ministre de la Justice, Sidiki Kaba, a soutenu que cette publication offre «une bonne base» pour aller de l’avant, comprendre les instruments et les outils pour une répression adéquate de la délinquance.
«La cybercriminalité est une des formes modernes de la délinquance que nous avons pu voir avec l’avènement de la société numérique. Et on ne peut pas utiliser des instruments classiques contre ces personnes qui commettent ces crimes», a-t-il dit, estimant que l’ouvrage ouvre notamment une perspective sur la prévention.
Le ministre de la Justice n’a pas tari d’éloges à l’endroit de l’auteur, le qualifiant de praticien et théoricien du droit tout à la fois. »Et cela est difficile à avoir, parce que c’est deux domaines différents», a-t-il commenté.
Selon Me Sidiki Kaba, le magistrat Pape Assane Touré participe à la pratique du droit, à la construction de la jurisprudence, soulignant que la cybercriminalité est l’avenir du droit.
APS

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.senenews.com/2014/11/23/un-livre-consacre-a-la-cybercriminalite-souligne-la-necessite-dun-cadre-juridique-approprie_96296.html

A quand le premier virus informatique acoustique ? ~ Sweet Random Science

	A quand le premier virus informatique acoustique ?

Je sais qu'ils sont payés pour cela, mais quand même : où diable vont-ils pêcher toutes ces idées ? Après la démonstration du Stanford Security Laboratory sur la façon dont les capteurs peuvent servir à espionner, voire détourner nos téléphones portables, des experts en informatique de l'institut Fraunhofer FKIE ont mis au point un protocole de transmission acoustique : des ordinateurs, pourvus qu'ils soient assez proches les uns des autres, peuvent communiquer via leurs haut-parleurs et microphones, à des fréquences inaudibles pour l'Homme, sans que cette activité ne soit détectée par les moyens de protection classiques.

Une idée qui semble relever de la science-fiction, même si la possibilité de la transmission acoustique avait déjà été proposée pour expliquer la mystérieuse persistance du malware polémique BadBIOS.

Dans leur article, publié le mois dernier dans Journal of Communications, Michael Hanspach et Michael Goetz exposent la méthode qui leur a permis de réaliser cette prouesse : en adaptant un système qui avait été imaginé pour établir des communications sous l'eau, ils sont parvenus à transmettre des informations sur des distances d'une vingtaine de mètres. Les signaux sont modulés en ondes sonores à une fréquence proche de celles des ultrasons, et sont donc inaudibles pour l'oreille humaine. Les chercheurs démontrent que cette méthode peut être utilisée pour établir un véritable réseau par lequel peuvent transiter des informations comme des mots de passe ou des identifiants de connexions, notamment lorsqu'ils sont saisis sur le clavier.

La vitesse de transmission, de l'ordre de 20 bits par seconde, ne permet évidemment pas de transmettre directement un document mais elle pourrait être suffisante pour placer une commande simple : désactiver une protection et envoyer un document par mail par exemple. De quoi rendre complètement inutiles les mesures de précaution d'isolement physique de certains site sensibles, comme les bases miliaires, les centres de services secrets ou les centrales nucléaires.

Dans une des expériences, Hanspach et Goetz établissent un réseau dans les propres locaux du Fraunhofer Institute for Communication, Information Processing and Ergonomics. Un espace de travail ouvert peut donc devenir un réseau d'échange à l'insu des utilisateurs et des logiciels anti-virus. Ce réseau serait accessible via n'importe quel terminal en mesure d'émettre et de capter des sons : un téléphone portable par exemple.

Utilisé de façon malveillante, ce système permettrait d'infiltrer un réseau, récupérer des mots de passe et les transmettre à des tiers, sans provoquer la moindre réaction des dispositifs de protection. Les anti-virus se concentrent en effet sur les modes de communication plus classiques et seraient totalement impuissants face à une attaque de ce genre.

Une faille qui sera sans doute corrigée rapidement, avec l'ajout d'un système anti-intrusion basé sur l'analyse des signaux audio émis et reçus. En attendant, on peut tout simplement désactiver les composants audio ou brider les haut-parleurs en supprimant la transmission des hautes fréquences.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://sweetrandomscience.blogspot.fr/2013/12/a-quand-le-premier-virus-informatique.html

Paiement par mobiles : Trop peu de sécurité face au piratage

Paiement par mobiles : Trop peu de sécurité face au piratage

Dans ses prédictions de sécurité pour les années à venir, Trend Micro fait un point sur la multiplication des nouveaux moyens de paiement et leur impact potentiel en termes de cybercriminalité.

Le paiement mobile et sans contact
Le lancement d'Apple Pay ou de Google Wallet sont la preuve de l'évolution des usages des consommateurs, désormais prêts à payer directement depuis leur mobile. Cependant, les terminaux mobiles sont toujours peu sécurisés.
Les solutions existantes sont encore trop rarement utilisées par les mobinautes qui n'ont pas pleinement conscience des risques, bien que les cybercriminels ne cessent de perfectionner leurs techniques pour tirer profit de ces nouveaux outils. A titre d'illustration, CurrentC, projet d'un consortium de distributeurs américains pour concurrencer Apple Pay, a récemment été piraté et ce, avant même d'avoir été lancé.

La technologie NFC, largement utilisée dans les solutions de paiement mobile, va ainsi continuer d'être l'objet d'une attention toute particulière des pirates. Les utilisateurs de Google Wallet l'ont déjà appris à leurs dépens lorsqu'une application malveillante, à laquelle des privilèges NFC avaient été accordés, s'est montrée capable de dérober les informations de leur compte utilisateur et leur argent.

« Le NFC s'impose de plus en plus or aujourd'hui, si l'on parle de sécurité, ni les utilisateurs, ni les fabricants d'équipements mobiles ne semblent vraiment prêts », commente Loïc Guézo, de chez Trend Micro. « Les utilisateurs doivent prendre conscience que les attaquants vont se donner les moyens d'intercepter les tags NFC en transit, et se montrer prudents. De leur côté, il est essentiel que les fabricants prennent des mesures et envisagent la sécurité des produits dès leur conception. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lafibreoptique.com/focus/20112014,cybercriminalite-des-terminaux-mobiles-peu-securises,1920.html

---

Une ville victime de Cyberattaques. Ottawa ciblée, Toronto menacée

Une ville victime de Cyberattaques. Ottawa ciblée,

«Anonymous» attaque le site de la Ville d'Ottawa
Un pirate informatique qui dit faire partie du groupe Anonymous a menacé dimanche de cibler les sites web appartenant à la Ville et à la police de Toronto.

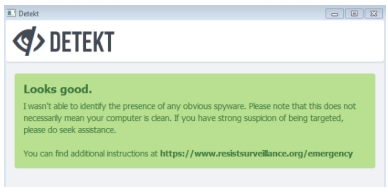
Cette menace en ligne provient d'un présumé pirate appelé Aerith. Il s'agit du même internaute qui aurait paralysé le site internet de la Ville d'Ottawa, vendredi soir. La page en question affichait alors une image d'une banane dansante et un message menaçant envers un policier d'Ottawa.

Aerith a également revendiqué les problèmes informatiques ayant paralysé ce week-end le site web de la police d'Ottawa. De samedi soir jusqu'à tôt dimanche matin, le site ottawapolice.ca était complètement hors service.
«Notre équipe d'enquête travaille aux côtés de nos experts en technologie de l'information afin d'identifier la source des problèmes techniques qui ont eu lieu la nuit dernière, a indiqué dimanche le chef de la police d'Ottawa, Charles Bordeleau. Notre réseau reste sécurisé», a-t-il assuré.
Le porte-parole de la Ville de Toronto Jackie DeSouza a indiqué que la Ville était au courant de ce qui était arrivé à Ottawa. Les fonctionnaires «demeurent très vigilants» et surveillent toute activité suspecte sur le site toronto.ca, a-t-il assuré.
Le compte Twitter de Aerith – qui indiquait, probablement à tort, avoir été fondé en Turquie – a été suspendu depuis les possibles cyberattaques.
Le groupe Anonymous s'en prendrait ainsi à la Ville d'Ottawa pour défendre la cause d'un adolescent de Barrhaven, en banlieue de la capitale nationale. Ce dernier fait face à 60 chefs d'accusation pour avoir fait de faux appels rapportant des menaces à la bombe, des prises d'otages ou des fusillades, tout en imitant la voix d'une autre personne, généralement un rival de la communauté de jeu en ligne.
Les attaques informatiques revendiquées par «Anonymous» seraient en lien avec une nouvelle preuve qui n'aurait pas été retenue par les enquêteurs et qui démontrerait que l'adolescent de Barrhaven n'est pas responsable des méfaits, mais qu'il s'agit plutôt d'un homme du New Jersey. La police de Toronto aurait déposé quelques-unes des 60 accusations.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://fr.canoe.ca/techno/nouvelles/archives/2014/11/20141123-175629.html

Déception : on a testé Detekt, il ne s’est rien passé



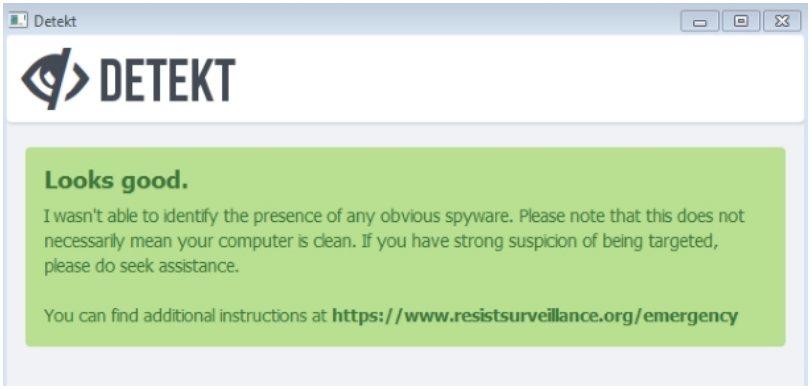
Déception : on a testé Detekt, il ne s’est rien passé

La promesse était belle : Detekt scanne votre ordinateur à la recherche des logiciels espions qui ciblent les activistes de tout poil, les minorités religieuses, et les journalistes. Nous avons essayé. Ça semble marcher, mais on est un peu amer.

Développé pendant deux ans par Claudio Guarnieri (un informaticien basé à Berlin) en partenariat avec Amnesty International et l'EFF entre autres, Detekt est un logiciel gratuit dont la promesse est d'informer l'utilisateur sur les spyware qui se seraient potentiellement glissés dans sa machine.

« Les défenseurs des droits de l'homme, les journalistes, les ONG, les opposants politiques, les minorités religieuses ou ethniques » sont particulièrement ciblés par les agences de renseignement qui utilisent des outils numériques d'espionnage, avertit l'auteur du logiciel.

La rédaction s'est donc prêtée au jeu du test. Après tout, savoir être espionné par la NSA, la DGSE ou Kim Jong-un, ça crédibilise notre travail.



(Personne ne nous espionne)

Après un scan offline de la machine, le verdict tombe. Rien de suspect sur l'ordinateur utilisé pour rédiger cet article. D'où deux propositions qui nous chagrinent : nous n'entrons dans aucune des catégories espionnées sus-nommées, ou bien nous sommes totalement inoffensifs pour les dites agences de renseignement. Préférons dire que nous avons beaucoup de chance.

En cas de détection d'un danger, l'auteur de Detekt mentionne que le nettoyage reste à faire soi-même. Detekt avertit, mais ne soigne pas. Par ailleurs, s'il ne trouve rien, cela ne signifie pas nécessairement que l'ordinateur ne soit pas la cible d'un service espion, mentionne le site de Detekt (ndlr. ouf !).

Programmé en Python, Detekt recherche des chevaux de Troie de certaines familles, comme DarkComet RAT, XtremeRAT, BlackShades RAT, njRAT, FinFisher FinSpy, HackingTeam RCS, ShadowTech RAT et Gh0st RAT. L'acronyme RAT signifie ici Remote Access Trojans. Le fichier readme.md donne d'autres informations techniques.

Au delà de cette annonce, qui est assurons-le une initiative salutaire, se pose la question de la pérennité de ce type de solution. Tout comme les antivirus, les anti spyware ne sont efficaces que s'ils sont régulièrement mis à jour, pour intégrer les nouvelles menaces, et celles déjà recensées, mais qui évoluent.

Et vous ? Vous en pensez quoi ?

Cliquez et laissez-nous votre avis…

Source : http://www.zdnet.fr/actualites/deception-on-a-teste-detekt-il-ne-s-est-rien-passe-39809965.htm

Quand chaque minute compte

	**Quand chaque minute compte..**

McAfee, filiale d'Intel Security, publie aujourd'hui un nouveau rapport, « Prévention des menaces : chaque minute compte ! », qui évalue la capacité des entreprises à détecter et à détourner les attaques ciblées.

Ce dernier révèle également le Top 8 des indicateurs d'attaques les plus critiques et examine les meilleures pratiques proactives en matière de réponse aux incidents. Il illustre combien les entreprises sont plus efficaces lorsqu'elles effectuent des analyses des attaques subtiles en temps réel en prenant en compte plusieurs variables mais surtout dès lors qu'elles ont intégré et priorisé le temps de détection et les menaces intelligentes dans leur évaluation des risques.
Conjointement au rapport, une étude menée par Evalueserve, révèle que la majorité des entreprises interrogées manquent de confiance en leur capacité à détecter les attaques ciblées dans un temps opportun. Même les entreprises les mieux préparées à gérer les attaques ciblées passent beaucoup trop de temps à enquêter sur des événements, contribuant à un sentiment d'urgence, plutôt qu'à se concentrer pro-activement à la détection et à l'atténuation des menaces.
Le rapport met en évidence le fait qu'en France :
• Seulement 26 % des entreprises sont confiantes dans leur capacité à détecter une attaque en quelques minutes, et 29 % ont déclaré que cela pouvait leur prendre des jours, des semaines, voire des mois avant qu'elles ne remarquent un comportement suspect.
• 71 % des DSI interrogés ont indiqué que les attaques ciblées sont une préoccupation majeure pour leur entreprise.
• 54 % des entreprises ont enquêté sur plus de 10 attaques l'an dernier.
• 95 % de celles qui sont capables de détecter les attaques en quelques minutes possèdent une solution de gestion des évènements et des informations de sécurité (SIEM).
• Plus de la moitié des entreprises interrogées (61 %) ont indiqué qu'elles sont équipées des outils et des technologies nécessaires pour fournir une réponse rapide aux attaques. Cependant, les indicateurs critiques ne sont généralement pas isolés de la masse des alertes générées et provoquent une charge de travail supplémentaire aux équipes qui doivent passer au crible toutes les données des menaces.
« Pour garder la main sur les attaquants il faut relever le défi du temps dans la détection », déclare David Grout, Directeur Europe du Sud de McAfee, filiale d'Intel Security. « En simplifiant, grâce à une analyse intelligente et en temps réel, le travail frénétique de filtrage d'un large volume d'alertes et d'indicateurs d'attaques vous pourrez plus efficacement appréhender des événements pertinents et prendre des mesures pour contenir et détourner les attaques plus rapidement. »
Compte tenu de l'importance de l'identification des indicateurs critiques, le rapport de McAfee Intel Security a révélé le Top 8 des indicateurs d'attaque les plus courants.
Parmi ceux-ci, cinq reflètent le suivi des événements à travers le temps écoulé et montrent l'importance de la corrélation contextuelle :
1. Des hôtes internes communiquent vers des destinations inconnues ou mal connues ou vers un pays étranger où il n'y a pas d'affaire en cours.
2. Des hôtes internes communiquent vers des hôtes externes qui utilisent des ports non standards ou en inéquation avec le protocole/port, tels que l'envoi d'interpréteurs de commandes (SSH) plutôt que du trafic HTTP sur le port 80, qui est le port Web par défaut.
3. Des accès publiques ou en zone démilitarisée (DMZ) communiquant vers des hôtes internes. Cela permet de brûler les étapes de l'extérieur vers l'intérieur et en arrière-plan, permet l'exfiltration de données et l'accès à distance à des actifs. Il neutralise la valeur de la DMZ.
4. Détection de logiciels malveillants en heures Off. Ces alertes qui peuvent se produire en dehors des heures standards d'ouverture de l'entreprise (la nuit ou le week-end) et qui pourraient signaler un hôte compromis.
5. Scans de réseau par les hôtes internes communiquant avec plusieurs hôtes dans un court laps de temps, qui pourrait révéler une attaque se déplaçant latéralement au sein du réseau. Les défenses du périmètre réseau, tels que pare-feu et IPS, sont rarement configurées pour surveiller le trafic sur le réseau interne (mais pourrait l'être).
6. Plusieurs événements alarmants à partir d'un seul hôte ou à répétition sur une période de 24 heures sur plusieurs machines dans le même sous-réseau, tels que les échecs d'authentification.
7. Après avoir été nettoyé, un système est réinfecté par des logiciels malveillants dans les cinq minutes qui suivent – les réinfections répétées signalent la présence d'un rootkit ou d'une compromission persistante.
8. Un compte utilisateur tente de se connecter à de multiples ressources en quelques minutes à partir de ou vers différentes régions – signe que les informations d'identification de l'utilisateur ont été volées ou que l'utilisateur a des intentions suspectes.
« Un jour, nous avons remarqué qu'un poste de travail subissait des demandes d'authentification du contrôleur de domaine à deux heures du matin. Cela pouvait bien sur être tout à fait normal, mais il se pouvait aussi que cela soit un signe d'alerte malveillante », commente Lance Wright, directeur principal de l'information de sécurité et de conformité à Volusion, un fournisseur de solutions de commerce contributeur de l'élaboration du rapport. *« Suite à cet incident, nous avons créé une règle pour nous alerter si un poste de travail avait plus de cinq demandes d'authentification en dehors des heures ouvrables pour nous aider à identifier le début de l'attaque, avant que les données ne soient compromises. »*

« La veille en temps-réel, la bonne intelligence et les solutions de gestion des évènements et des informations de sécurité (SIEM), permettent de minimiser le temps de détection, d'éviter de manière proactive les violations fondées sur la contextualisation des indicateurs lors de l'analyse et d'apporter des réponses en matière d'action automatisés », précise David Grout *« Grâce aux solutions qui permettent d'accélérer la capacité de détection, de réaction et d'apprentissage sur les attaques, les entreprises peuvent grandement changer leur posture de sécurité et passer de 'traquées' à 'traqueuses'. »*

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

Source :
http://www.itrnews.com/articles/152073/chaque-minute-compte.html