Alerte : 1 million de comptes Google dérobés. Outil gratuit pour vérivier votre compte

	Alerte : 1 million de comptes Google dérobés. Outil gratuit pour vérivier votre compte

Un logiciel malveillant, ou malware, nommé Gooligan, a infecté plus d'un million de téléphones fonctionnant sur Android et permis à des pirates de dérober les données d'autant de comptes Gmail, a révélé aujourd'hui la compagnie israélienne spécialisée en solutions de sécurité, Check Point.
«Grâce à ces informations, les agresseurs peuvent accéder aux données confidentielles des utilisateurs dans Gmail, Google Photos, Google Docs, Google Play, Google Drive et G Suite», précise la compagnie dans un communiqué.

13 000 appareils infectés chaque jour

Gooligan infecterait 13 000 appareils par jour, en ciblant les appareils sur Android 4 (Jelly Bean, KitKat) et 5 (Lollipop), soit 74% des appareils Android aujourd'hui en usage. C'est la première fois qu'une cyberattaque de ce genre parvient à toucher plus d'un million d'appareils.
Selon Check Point, environ 57% de ces appareils infectés sont situés en Asie et environ 9% en Europe.

Comment fonctionne ce malware ?
L'infection se produit lorsqu'un utilisateur télécharge puis installe une application infectée par *Gooligan* sur un appareil Android vulnérable, ou s'il clique sur des liens malveillants dans des messages de *phishing*. «Une fois que les agresseurs parviennent à prendre le contrôle d'un appareil, ils gênèrent des revenus frauduleux en installant des applications à partir de Google Play et en les évaluant au nom de la victime», explique Check Point.

Vérifier l'état de son compte en ligne

Prévenu par la société israélienne, Google aurait contacté les utilisateurs concernés pour «désinfecter» les appareils touchés et ajouter de nouvelles protections à sa technologie Verify Apps.

Check Point propose un outil en ligne gratuit permettant aux utilisateurs d'Android de vérifier si leur compte n'a pas été infecté par *Gooligan*.
[Lien vers l'outil gratuit en ligne]

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : les données d’un million de comptes Google dérobées par Gooligan – Le Parisien

---

Le décret du fichier biométrique TES attaqué en justice

Le décret du fichier biométrique TES attaqué en justice

Le collectif des Exégètes Amateurs annonce son intention d'attaquer devant le Conseil d'État le décret donnant naissance au controversé fichier TES.

L'offensive judiciaire est lancée. Mardi, le collectif des Exégètes Amateurs a annoncé sa décision d'engager un recours au Conseil d'État – la plus haute des instances administratives en France – contre le décret du fichier TES (Titres Électroniques Sécurisés), qui a été publié discrètement au Journal officiel le 30 octobre 2016, en plein week-end de la Toussaint.
Découvert à ce moment-là, le fichier TES inquiète. Il s'agit d'une base de données qui réunira les données personnelles et biométriques de la quasi totalité des Français. En effet, il est destiné aux passeports et aux cartes d'identité. Néanmoins, il inquiète par l'ampleur et la nature des informations qu'il est amené à recevoir. Surtout, il pourrait servir tôt ou tard à d'autres fins que celles actuellement prévues.

La stratégie exacte des Exégètes Amateurs – qui rassemble La Quadrature du Net, la fédération de FAI associatifs FFDN et l'opérateur French Data Network (FDN) – contre le décret n'a pas été précisée. La coordinatrice des campagnes de La Quadrature du Net, Adrienne Charmet, a simplement indiqué sur Twitter que les détails seront communiqués ultérieurement.
Parmi les angles d'attaque éventuels, l'avocat des nouvelles technologies Rubin Sfadj suggère sur son blog une incompatibilité du décret avec l'article 34 de la Constitution. Celui-ci expose que c'est au législateur que revient le pouvoir de fixer les règles applicables en matière de libertés publiques et de procédure pénale. Dit autrement, c'est au parlement de décider par à l'exécutif.
Les Exégètes Amateurs – une expression de l'ex-député socialiste Jean-Jacques Urvoas, désignant, de manière dédaigneuse, ceux qui s'opposent par des arguments de droit à la loi sur le renseignement dont il était le rapporteur – regroupent des juristes et bénévoles qui ont pris l'habitude de multiplier les recours en justice contre des textes législatifs et réglementaires qu'ils jugent dangereux…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l’article mis en page : Le décret du fichier biométrique TES attaqué en justice – Politique – Numerama

---

Les données biométriques de tous les Français dans un fichier commun. Utile ou risqué ?

Les données biométriques de tous les Français dans un fichier commun. Utile ou risqué ?

Un fichier unique, baptisé « Titres électroniques sécurisés » (TES). Ce fichier a un rôle-clé : rassembler dans une même base de données les données personnelles et biométriques des Français pour la gestion des cartes nationales d'identité et des passeports. Mais il suscite de vives inquiétudes.

À la toute fin du mois d'octobre, le gouvernement a fait publier un décret qui donne le coup d'envoi à la création d'un fichier qui rassemblera les données personnelles et biométriques de la quasi totalité des Français. Destiné aux passeports et aux cartes nationales d'identité, il inquiète par son ampleur et la nature des informations qu'il est amené à recevoir. Nous vous expliquons de quoi il en retourne en quelques questions.

À QUOI ÇA SERT ?

Le fichier en question, dénommé « Titres Électroniques Sécurisés » (TES), a vocation à être une base de données centrale rassemblant des informations personnelles et biométriques relatives aux détenteurs d'un passeport et / ou d'une carte nationale d'identité. Il remplace deux fichiers précédents, l'un pour le passeport l'autre pour la carte nationale d'identité.

QUELLES SONT LES ALTERNATIVES ?

Était-il possible de faire autrement ? Pour la commission nationale de l'informatique et des libertés (CNIL), sans aucun doute. Dans sa délibération, elle évoque un « *composant électronique sécurisé dans la carte nationale d'identité* » qui « *serait de nature à faciliter la lutte contre la fraude documentaire, tout en présentant moins de risques de détournement et d'atteintes au droit au respect de la vie privée* »

Elle ajoute que cette solution, qui n'a pas été censurée par le Conseil constitutionnel quand un précédent texte du même acabit a été présenté sous une autre majorité, « *permettrait de conserver les données biométriques sur un support individuel exclusivement détenu par la personne concernée, qui conserverait donc la maîtrise de ses données, réduisant les risques d'une utilisation à son insu* ».

SUIS-JE DÉJÀ FICHÉ ?

En pratique, oui. Il existe déjà deux fichiers, l'un pour le passeport, l'autre pour la carte nationale d'identité. La nouvelle base de données n'est que le prolongement de ce qui existait déjà. À moins de n'avoir jamais possédé ces titres (ils ne sont pas obligatoires), vous figurez déjà certainement dans ces fichiers. Seuls les enfants en bas âge peuvent y échapper, si aucune demande de titre d'identité n'a été faite.

EST-CE ACTÉ ?

Le système TES existe déjà pour le passeport et, pour les demandes de passeport, le dispositif n'est pas modifié par le décret ; TES est donc actif. Quant aux demandes de cartes, la CNIL nous précise que le nouveau dispositif entrera progressivement en vigueur, selon les arrêtés mentionnés dans le décret ; les empreintes seront prises à partir des dates de ces arrêtés ; le tout doit être finalisé avant le 31 décembre 2018.

POURQUOI C'EST DANGEREUX ?

« *Ce que la technique a fait, la technique peut le défaire* » prévient le sénateur PS Gaëtan Gorce, commissaire de la CNIL, dans une interview à Libération. Aujourd'hui, l'exécutif a pris des dispositions pour éviter certaines dérives (croisement ou remontée de données) et assurer un bon niveau de sécurité, ce que la CNIL reconnaît dans sa délibération. Mais demain ?

Comme nous l'indiquions dans notre sujet, maintenant que la base existe il pourrait bien y avoir un jour la tentation de l'utiliser pour faire de la reconnaissance automatisée des visages avec des caméras de surveillance. Un futur gouvernement, moins scrupuleux sur les questions de libertés publiques, pourrait vouloir l'employer autrement. Après tout, ne sommes-nous pas en guerre contre le terrorisme ?

QU'EN PENSE LA CNIL ?

La CNIL, garante du respect des libertés et de l'équilibre des traitements automatisés de données, fait part de « *plusieurs réserves* » dans sa délibération. Le contournement du législateur est regretté, au regard de « *l'ampleur inégalée de ce traitement et du caractère particulièrement sensible des données qu'il réunira* ». La commission demande une « *évaluation complémentaire du dispositif* ».

QUELS SONT LES RECOURS ?

Le gouvernement ayant fait le choix de passer par un décret, il n'a pas été possible de discuter de la création de ce fichier au cours de son parcours parlementaire s'il avait été présenté sous la forme d'un projet de loi. Interrogé à ce sujet par Libération, le sénateur PS Gaëtan Gorce, commissaire de la CNIL, explique qu'il doit être possible d'attaquer le décret par un recours devant le Conseil d'État

[Article de Numerama]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l’article mis en page : Le fichage biométrique des Français en 7 questions – Politique – Numerama

60 millions de Français fichés dans une base de données commune des titres d’identité

60 millions de Français fichés dans une base de données commune des titres d’identité

Un décret publié pendant le pont de la Toussaint officialise la création d'un gigantesque fichier national.
Soixante millions de Français glissés, à l'occasion d'un week-end de pont de la Toussaint, dans une même base de données : un décret paru au Journal officiel dimanche 30 octobre, et repéré par le site NextInpact, officialise la création d'un « traitement de données à caractère personnel commun aux passeports et aux cartes nationales d'identité ». En clair, les données personnelles et biométriques de tous les détenteurs d'une carte d'identité ou d'un passeport seront désormais compilées dans un fichier unique, baptisé « Titres électroniques sécurisés » (TES). Cette base de données remplacera à terme le précédent TES (dédié aux passeports) et le Fichier national de gestion (dédié aux cartes d'identité), combinés dans ce nouveau fichier.

La base de données rassemblera ainsi des informations comme la photo numérisée du visage, les empreintes digitales, la couleur des yeux, les adresses physiques et numériques… Au total, la quasi-totalité des Français y figurera, puisqu'il suffit de détenir ou d'avoir détenu une carte d'identité ou un passeport pour en faire partie – les données sont conservées quinze (pour les passeports) à vingt ans (pour les cartes d'identité)…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : 60 millions de Français fichés dans une base de données commune des titres d'identité

Cash investigation ne comprend rien à la cybersécurité

Cash investigation ne comprend rien à la cybersécurité

La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que Cash Investigation a tenté de montrer.

La cybersécurité est un sujet suffisamment sensible pour qu'il mérite d'être traité par les journalistes avec rigueur et sérieux. En la matière, l'approximation et la sous-estimation de sa complexité conduisent inévitablement à des contre-vérités médiatiques et à des biais de représentation.
C'est précisément ce que l'émission de France 2 Cash Investigation Marchés publics : le grand dérapage nous a fourni le mardi 18 octobre à 20h55, tant les approximations et les contre-vérités se succédaient à grande vitesse tout au long du reportage sur le système d'exploitation des ordinateurs du Ministère de la Défense.
Je dois avouer qu'il en faut en général beaucoup pour me choquer mais que ce beaucoup a été très vite atteint par l'équipe de Cash Investigation ! Jamais réalité n'avait été à ce point tordue et déformée dans l'unique but d'entrer par le goulot étroit du format préfabriqué de la désinformation. En clair, on a voulu se payer les balourds du Ministère de la Défense et les militaires qui ont choisi le système d'exploitation Windows (Microsoft) pour équiper leurs machines…

Un piratage en trois clics ?

Pensez donc, Madame, en trois clics et deux failles de sécurité, Élise Lucet nous démontrait qu'elle pouvait prendre le contrôle des ordinateurs du Ministère de la Défense pour déclencher dans la foulée la troisième guerre mondiale…. Il est vrai qu'elle venait de pirater sans pression l'ordinateur de l'un de ses collègues, avec l'aide de deux experts en cybersécurité de l'ESIEA. Et comme chacun le sait, si l'opération fonctionne avec la machine Windows de madame Michu, ça marchera tout pareil avec les machines de la Grande Muette.
Dans le cadre d'un renouvellement de contrat, Microsoft a remporté en 2013 le marché public du Ministère de la Défense concernant l'équipement en systèmes d'exploitations du parc informatique des Armées. Windows est donc installé sur 200 000 ordinateurs de l'armée française.
Partant de cette réalité, Élise Lucet et son équipe en ont déduit que cela constituait un choix risqué en matière de cybersécurité & cyberdéfense tant ce système d'exploitation est truffé de vulnérabilités et de Back Doors (portes dérobées) installées par les méchants espions américains de la NSA.

Le « piège » de Microsoft

En conclusion, toujours selon Élise Lucet, les militaires français sont tombés dans le piège tendu par Microsoft qui dispose désormais de toutes les entrées possibles pour la prise de contrôle à distance des ordinateurs sensibles du Ministère et de leurs secrets Défense. La théorie du complot n'est pas très éloignée dans tout cela, surtout lorsque l'hypothèse d'Élise Lucet se trouve plus ou moins confirmée par les déclarations de l'expert cryptologue Éric Filiol, retraité des services de renseignement et actuellement directeur du centre de recherche en cybersécurité de l'ESIEA.
Ce que dit Éric Filiol durant ses courtes interventions n'est pas contestable : il effectue une démonstration de prise de contrôle à distance d'un ordinateur équipé du système Windows 7 à la suite d'un clic de l'utilisateur (la cible) sur un lien malveillant transmis par mail. La démonstration qu'il donne d'une prise de contrôle n'appelle aucune critique puisqu'elle est un classique du genre, connue de tous les étudiants préparant un Master en cybersécurité.

Quelle preuve des failles de sécurité ?

C'est l'usage qui en est fait qui devient très contestable : puisque la manipulation fonctionne sur l'ordinateur doté de Windows de mon collègue journaliste (qui, au demeurant, a le clic facile et l'antivirus laxiste), c'est qu'elle fonctionne également avec l'ensemble du parc informatique relevant du Ministère de la Défense (cqfd). Preuve est donc faite de l'incompétence des services de l'État, de services chargés de la cybersécurité des infrastructures militaires et de l'ensemble des experts, ingénieurs et chercheurs qui œuvrent chaque jour en France pour sécuriser les systèmes…
Le reportage pousse encore un peu plus loin sa courageuse investigation en allant interroger très brièvement l'Officier Général Cyberdéfense, le vice Amiral Coustillière. Ce dernier est interrogé entre deux portes sur le choix improbable d'installer Windows sur des machines qui font la guerre.

White Hat au grand cœur

N'écoutant que leur sagacité et leur expertise autoproclamée, nos journalistes hackers « White Hat » au grand cœur (donc toujours du bon côté de la Force) donnent pour finir une leçon de cyberstratégie à l'Amiral responsable de la sécurité des infrastructures numériques militaires, tout en le faisant passer pour un amateur déconnecté des réalités informatiques… C'est à ce point que l'on touche au paroxysme de la désinformation du spectateur que l'on considère comme un consommateur compulsif de dysfonctionnements et malversations étatiques…
Et bien non, Madame Lucet, non, le choix de Windows n'est pas plus ou moins défendable que celui d'un système open source. Linux et ses dérivés souffrent également de vulnérabilités, subissent des attaques et des correctifs. C'est le triste destin de tout système complexe que d'avoir été créé imparfait, ouvert aux agressions extérieures exploitées par des individus mal intentionnés ou en quête d'information.

On ne clique pas tous sur les malware

Non, Madame Lucet, ce n'est pas parce qu'un de vos collègues journalistes clique facilement sur un lien malveillant que tout le monde le fait. Ce n'est pas parce que son antivirus ne détecte pas un malware qu'aucun autre antivirus ne le détectera. Ce n'est pas parce que Windows possède des vulnérabilités que les autres systèmes d'exploitation n'en possèdent pas.
Ce n'est pas parce que Microsoft a pu transmettre ou vendre certaines données aux services gouvernementaux américains que cette firme cherche obsessionnellement à piéger l'armée française. Enfin, non chère Élise, l'armée française ne découvre pas les problématiques de sécurité numérique avec votre reportage et ne sous-estime pas les risques de vol de données sensibles. C'est quelque part faire injure aux spécialistes civils et militaires qui œuvrent quotidiennement à la défense des intérêts numériques de la nation.
La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que ce triste reportage a tenté de montrer.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l’article mis en page : Cash investigation ne comprend rien à la cybersécurité | Contrepoints

---

Sednit : dissection d’un groupe de cyber-espions

	**Sednit : dissection d’un groupe de cyber-espions**

Les chercheurs ESET annoncent la publication d'un vaste document de recherche en 3 parties « En route with Sednit ». L'observation de l'utilisation simultanée d'un bootkit et d'un rootkit par les cybercriminels a permis d'analyser leurs cibles et méthodes.

Ce groupe aussi connu sous le nom d'APT28, Fancy Bear ou Sofacy, agit depuis 2004. Son principal objectif **est le vol d'informations confidentielles de cibles spécifiques :**

• Partie 1 : « En route with Sednit : Approaching the Target » se concentre sur la cible des campagnes de phishing, les méthodes d'attaque utilisées ainsi que la première phase de l'attaque utilisant le malware SEDUPLOADER, composé d'un compte à rebours et d'une charge utile associée.

• Partie 2 : « En route with Sednit : Observing the comings and goings » couvre les activités de Sednit depuis 2014 et détaille la boîte à outils d'espionnage utilisée pour la surveillance à long terme des ordinateurs compromis. Cela est rendu possible grâce à deux backdoor SEDRECO et XAGENT, ainsi qu'à l'outil réseau XTUNNEL.

• Partie 3 : « En route with Sednit : a mysterious downloader » décrit le logiciel permettant la première phase de l'attaque DOWNDHELPH qui selon nos données de télémétrie n'aurait servi que 7 fois. A noter que certains de ces déploiements ont requis des méthodes de « persistances avancées » : Windows bootkit et Windows rootkit.

« L'intérêt d'ESET pour ces activités malveillantes est née de la détection d'un nombre impressionnant de logiciels personnalisés déployés par le groupe Sednit au cours des deux dernières années », déclare Alexis Dorais-Joncas, Security Intelligence team lead chez ESET et dédié à l'exploration des activités du groupe Sednit. « L'arsenal de Sednit est en constante évolution. Le groupe déploie régulièrement des logiciels et techniques de pointe, tandis que leur malware phare a également évolué de manière significative au cours des dernières années ».

Selon les chercheurs ESET, les données collectées à partir des campagnes de phishing menées par Sednit montrent que plus de **1.000 profils d'individus hauts-placés impliqués dans la politique d'Europe de l'EST ont été attaqués.** « Contrairement aux autres groupes d'espionnage, le groupe Sednit a développé son propre « exploit kit » et utilisé un nombre étonnamment important d'exploits 0-day», conclut Alexis Dorais-Joncas.

Les activités du groupe cybercriminel de ces dernières années envers les personnalités hauts-placées, ont suscité l'intérêt de nombreux chercheurs. **Le document réalisé par les experts ESET fournit une description technique accessible et contenant les indicateurs de compromission (IOCs), à destination des chercheurs et des entreprises afin de vérifier qu'ils n'ont pas été compromis par le groupe Sednit**.

La première partie de cette recherche est disponible sur WeLiveSecurity, l'intégralité l'étant sur le Github ESET.

Réagissez à cet article

Original de l’article mis en page : Boîte de réception (2) – denis.jacopini@gmail.com – Gmail

Pourquoi les vols de données sont en forte hausse ?

Pourquoi les vols de données sont en forte hausse ?

Une étude du Ponemon Institute pour Varonis révèle que la plupart des collaborateurs disposent d'accès trop importants, ce qui multiplie les dommages lorsque leurs comptes sont compromis

Trois entreprises sur quatre ont été victimes de la perte ou du vol de données importantes au cours des deux dernières années. Selon une nouvelle enquête menée auprès de plus de 3 000 collaborateurs et informaticiens aux États-Unis et en Europe, cela représente une très forte augmentation depuis 2014. Le rapport publié aujourd'hui a été rédigé par le Ponemon Institute et sponsorisé par Varonis Systems, Inc., principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques.
Selon l'enquête, l'augmentation de la perte et du vol des données est en grande partie due aux compromissions de comptes internes. Celles-ci sont aggravées par des accès aux informations critiques bien plus permissifs que nécessaire par les collaborateurs et les tiers. Sans oublier le constant défaut de supervision des accès et de l'activité dans les systèmes de messagerie et les systèmes de fichiers, là où se trouvent les données les plus sensibles et les plus confidentielles.
Parmi les principales conclusions :
• 76 % des informaticiens indiquent que leur entreprise a fait l'expérience de la perte ou du vol de ses données au cours des deux dernières années. Ce chiffre représente une augmentation importante par rapport aux 67 % d'informaticiens interrogés ayant donné la même réponse lors de l'étude de 2014 réalisée par Ponemon pour le compte de Varonis.
• Les informaticiens indiquent que la négligence des collaborateurs a deux fois plus de chances d'entraîner la compromission des comptes internes que tout autre facteur, y compris les attaquants externes ainsi que les collaborateurs ou les prestataires malveillants.
• 78 % des informaticiens déclarent être très préoccupés par les ransomware, un type de logiciels malveillants qui bloque l'accès aux fichiers jusqu'au paiement d'une somme d'argent. 15 % des entreprises ont déjà fait l'expérience des ransomware et seule une petite moitié d'entre elles a détecté l'attaque au cours des 24 premières heures.
• 88 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations propriétaires telles que des données relatives aux clients, des listes de contacts, des renseignements sur les collaborateurs, des rapports financiers, des documents commerciaux confidentiels ou d'autres actifs informationnels critiques. C'est nettement plus que les 76 % enregistrés dans l'étude de 2014.
• **62 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter**.
• Seuls 29 % des informaticiens interrogés indiquent que leur entreprise applique un modèle strict de moindre privilège pour s'assurer que les collaborateurs ont accès aux données de l'entreprise en fonction de leur besoin de les connaître.
• Seulement 25 % des entreprises supervisent toute l'activité relative à la messagerie et aux fichiers, alors que 38 % ne supervisent aucune activité.
• 35 % des entreprises ne disposent d'aucun enregistrement interrogeable de l'activité du système de fichiers, ce qui les rend incapables de déterminer les fichiers chiffrés par ransomware (entre autres choses).
Le rapport d'étude intitulé « *Closing Security Gaps to Protect Corporate Data: A Study of U.S. and European Organizations* » se fonde sur des entretiens menés en avril et mai 2016 auprès de 3 027 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne. L'ensemble des personnes interrogées comprend 1 371 utilisateurs finaux ainsi que 1 656 informaticiens et professionnels de la sécurité informatique issus d'entreprises de tailles variant de quelques douzaines à plusieurs dizaines de milliers d'employés. Ils proviennent de divers secteurs, dont les services financiers, le secteur public, le secteur des soins de santé et des sciences de la vie, la vente au détail, le secteur industriel, le secteur technologique et l'industrie du logiciel…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : Vols de données en forte hausse, cause principale: les menaces internes | Docaufutur

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

	Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo a accepté sans combattre d'installer un logiciel sur ses serveurs, qui regarde le contenu des e-mails qui arrivent et transmet aux services de renseignement américains ceux qui peuvent les intéresser. Il est plus que temps de fermer son compte Yahoo.

L'agence Reuters a révélé mardi que les ingénieurs en charge du service des e-mails de Yahoo ont développé et mis en place en 2015 un logiciel qui scanne le contenu de tous les messages envoyés vers les centaines de millions de comptes Yahoo, pour copier et mettre à la disposition des autorités américaines ceux qui contiennent certaines chaînes de caractères intéressant les services de renseignement. L'ordre confidentiel, qui émanerait de la NSA ou du FBI et a été confirmé par quatre sources dont trois anciens employés de Yahoo, a été suivi sans que la direction de Yahoo le conteste.
C'est la découverte du bout de code qui aurait conduit le chef de la sécurité de Yahoo, Alex Stamos, à démissionner et partir chez Facebook en juin 2015. Ses équipes n'avaient pas été informées et il jugeait que le code mettait en danger la sécurité des utilisateurs…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI – Tech – Numerama

Un sous-traitant de la NSA accusé de vol de données secrètes

Un sous-traitant de la NSA accusé de vol de données secrètes

’affaire est embarrassante pour la National Security Agency (NSA). Le ministère américain de la justice a annoncé, mercredi 5 octobre, l’arrestation d’un homme soupçonné d’avoir volé des données classées « top secret » alors qu’il travaillait pour une agence fédérale, identifiée comme la NSA par le New York Times.

L’homme arrêté, Harold Thomas Martin III, travaillait comme sous-traitant à l’agence de renseignement américaine, spécialisée dans l’espionnage des communications mondiales. Il était employé par Booz Allen Hamilton, un grand groupe privé américain qui fournit de nombreux sous-traitants aux agences du renseignement des Etats-Unis.
« Lorsque nous avons appris l’arrestation de notre employé, nous avons immédiatement joint les autorités fédérales pour proposer notre totale coopération, et nous avons licencié » le sous-traitant, a confirmé, mercredi, dans un communiqué Craig Veith, le vice-président de Booz Allen Hamilton.

Embarrassant pour la NSA

Pour la deuxième fois en trois ans, la NSA voit l’un de ses sous-traitants dérober des informations ultrasecrètes. Edward Snowden, qui a révélé au grand public l’ampleur des programmes de surveillance de la NSA, était également un sous-traitant de Booz Allen Hamilton. La NSA n’a pas répondu aux sollicitations de l’Agence France-Presse.
Selon le *New York Times*, M. Martin est *« soupçonné d’avoir pris les codes source très secrets développés par la NSA pour s’introduire dans les systèmes informatiques d’adversaires comme la Russie, la Chine, l’Iran et la Corée du Nord »*.
L’acte d’accusation se borne à mentionner que M. Martin a emporté chez lui du matériel informatique et des documents confidentiels qui n’auraient jamais dû sortir du bureau où il travaillait. Il encourt respectivement un an et dix ans de prison pour ces faits, selon la même source.
[Source : Le Monde]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l’étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d’un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l’article mis en page : Etats-Unis : un sous-traitant de la NSA accusé de vol de données secrètes

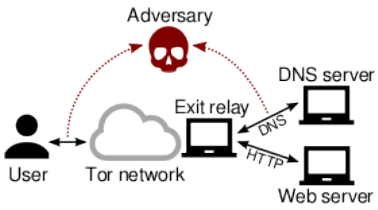
---

Désanonymiser Tor. Possible ?

Désanonymiser Tor. Possible ?

Des chercheurs ont étudié la variante d'une attaque par corrélation permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. « DefecTor » est centrée sur les requêtes DNS.

Des chercheurs de Princeton, aux État-Unis, et des universités Karlstad et KTH, en Suède, ont étudié la faisabilité d'une méthode permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. Leurs travaux orientés sur le DNS sont en ligne (*« The Effect of DNS on Tor's Anonymity »*).
L'attaque nommée DefecTor est une variante d'une attaque par corrélation centrée sur les requêtes DNS (Domain Name System). Elle est possible car Tor Browser, le navigateur qui permet aux internautes d'accéder au réseau Tor, regroupe et chiffre le trafic HTTP et le trafic DNS. Ensuite la requête DNS est traitée au niveau du noeud de sortie, et le trafic HTTP est envoyé vers sa destination…[lire la suite]



Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : DefecTor : s'appuyer sur

le DNS pour désanonymiser Tor