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 su

: 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.



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 rybersécurité

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.



Contactez-nous

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.

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

 $: \ https://www.lenetexpert.fr/formations-cybercriminal ite-protection-des-donnees-personnelles$



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.



Contactez-nous

Réagissez à cet article

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

Le réseau informatique des drones militaires américains piraté ?



Le réseau informatique des drones militaires américains piraté?

Le 9 septembre dernier, le réseau informatique de la base Creech de l'US Air Force, dans le Nevada, est tombé en panne, peut-être en raison d'un acte de piratage. C'est de là que sont conduites les opérations de surveillance et de bombardement par drones. Le réseau n'est toujours pas rétabli complètement.

L'armée américaine s'est-t-elle fait pirater le réseau de communication qu'elle utilise pour piloter à distance sa flotte de drones tueurs, qui bombardent quotidiennement dans de multiples pays du monde dont l'Afghanistan, la Syrie, le Pakistan, la Somalie, ou l'Irak ? La question se pose alors que BuzzFeed dévoile que l'US Air Force a reconnu que le réseau informatique de sa base Creech Air Force, dans le Nevada, était tombé en panne le 9 septembre dernier, et qu'il n'avait toujours pas pu être rétabli complètement depuis.

La base Creech Air Force est celle qui abrite les militaires qui, joystick à la main et yeux rivés sur un écran, déclenchent les frappes aériennes à des milliers de kilomètres de distance — parfois en utilisant uniquement des collectes de métadonnées pour présumer de l'identité des cibles, l'armée ayant développé des algorithmes pour les détecter. Les drones sont pilotés à travers des liaisons satellite qui permettent de relayer les ordres du Nevada jusqu'aux théâtres de guerre, avec un minimum de temps de latence et en toute sécurité.

Mais le système repose au moins partiellement sur le réseau SIRPnet (Secret Internet Protocol Router Network), une sorte de réseau Internet privé de l'armée américaine, utilisé pour véhiculer des informations confidentielles en toute sécurité. Or selon un appel d'offres étonnamment détaillé publié par l'armée, « le système SIRPNet actuellement en opération à Creech AFB a échoué et des services essentiels ont été touchés ». Elle précise que « les systèmes ont été quelque peu restaurés avec l'utilisation de plusieurs appareils moins puissants », et que « cette solution temporaire a stabilisé les services, mais ne sera pas capable de satisfaire la demande encore très longtemps ». Or, « si cette solution échoue, il n'y actuellement aucun système de sauvegarde »…[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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Un système essentiel pour les drones tueurs américains est tombé en panne — Politique — Numerama

Drone piégé utilisé par l'EI contre deux militaires français



Selon des informations du Monde, deux militaires français qui étaient en opération auprès des Kurdes en Irak ont été rapatriés en France après avoir été grièvement blessé par un drone piégé de l'État

C'est un mode d'action que les forces de l'ordre redoutent sur le territoire national, et qui semble désormais déployé sur le terrain de l'adversaire. Le Monde affirme ce mardi que deux militaires français ont été gravement blessés par un drone qui avait été piégé par des militants de l'État islamique, en Irak. L'un des deux serait entre la vie et la mort.

« Les deux commandos ont été touchés par un drone volant piégé, envoyé par un groupe lié à l'EI, dans des circonstances qui restent à préciser. Les militaires auraient intercepté le drone, avant que celui-ci explose à terre. Ce mode d'action contre des forces françaises est en tout état de cause inédit », rapporte le quotidien, qui précise que ses informations sont confirmées par d'autres médias. Ce piège aurait été tendu aux commandos parachutistes qui intervenaient auprès des forces kurdes à Erbil, dans le nord de l'Irak, entre Mossoul et Kirkouk. La ville est la capitale de la région

Le Monde indique que le ministère de la Défense ne souhaite pas confirmer cette attaque d'un nouveau genre et le rapatriement des deux soldats à l'hôpital militaire de Percy-Clamart, non seulement par souci de protéger les familles, mais aussi peut-être en raison des « moyens employés pour cette attaque » (on peut ajouter que de manière plus générale s'agissant des propagandes de guerre, les armées n'aiment jamais communiquer sur leurs propres pertes, préférant mettre en avant leurs réussites pour conserver le moral des troupes et le soutien des populations).

La crainte est sans doute que le mode opératoire, relativement peu coûteux et surtout peu risqué pour les attaquants, ne donne des idées sur le front irakien ou syrien, mais aussi en occident. L'hypothèse qu'une petite bombe puisse être transportée par un drone sans savoir d'où il a décollé et d'où il est contrôlé est soulevée depuis longtemps par les experts de la sécurité aérienne. Elle ent été évoquée en France lors du survol des centrales nucléaires par des drones

Depuis, le législateur s'est emparé du sujet en élaborant une proposition de régulation des drones en cours d'examen, qui prévoit notamment l'obligation d'identifier les drones à distance ou de brider leur utilisation dans certaines zones réglementées. Mais par définition les lois n'ont aucune influence contre ceux qui veulent les violer, et il paraît bien difficile d'empêcher totalement le transport de bombes par drone, sauf à utiliser des moyens technologiques encore balbutiants et impossibles à déployer sur tout le territoire comme des brouilleurs, des lasers, des perturbateurs de signaux GPS, des filets, ou même des aigles.

Le fait que les troupes de l'EI utilisent des bombes montées sur des drones n'est aussi, hélas, qu'une réponse attendue à l'utilisation croissante des drones et autres engins militaires conduits à distance par les troupes alliées. En août dernier, l'armée irakienne était fière de présenter un fusil mitrailleur monté sur un véhicule conduit à 1 km de distance, qui permettait d'aller tuer sans risquer de se faire tuer, ce qui est aussi l'objectif des avions de combat semi-autonomes, des navires de guerre ou des nouveaux chars d'assaut. L'utilisation de drones piégés n'est à cet égard qu'une

Il faut ajouter qu'en droit international, l'utilisation de telles armes n'est pas interdite dès lors qu'elles visent à tuer des militaires combattants, et non des civils. La question de la réqulation des « robots tueurs » a déjà fait l'objet de débats dans la communauté internationale, dans le cadre de révisions des conventions de Genève, mais les perspectives d'un accord sont excessivement lointaines. La seule piste évoquée, encore très incertaine, est l'obligation qui pourrait être faite qu'un humain reste en permanence aux commandes des engins robotisés, pour ne pas parvenir à des guerres menées par IA interposées. [Article source]

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





Original de l'article mis en page : L'État islamique aurait piégé un drone et blessé grièvement deux militaires français -Politique - Numerama

Même le FBI vous recommande très fortement de faire cela sur votre ordinateur Suivez leurs conseils !



Même le FBI vous recommande très fortement de faire cela sur votre ordinateur ! Suivez leurs conseils !

C'est lors d'une conférence organisée à Washington que le directeur du Bureau fédéral d'enquête (FBI), James Comey, a évoqué la question de la cybersécurité.

C'était le 14 Septembre dernier. Et il a donné un conseil très précieux que nous devrions tous appliquer : « Si vous allez dans n'importe quel bureau du gouvernement, vous verrez ces petites caméras au-dessus des écrans. Toutes ont un petit cache placé dessus. On fait ça pour éviter que des gens qui n'y sont pas autorisés ne nous regardent. [...] Je pense que c'est une bonne chose. »

Effectivement, même si vous êtes un simple particulier, vous n'êtes pas à l'abri qu'un hacker prenne la main sur votre ordinateur et accède à votre webcam et votre micro. Etre écouté et observé dans son intimité ? Non merci sans façon ! Alors on vous conseille d'aller vite mettre un petit bout d'adhésif sur votre ordi...Question de précaution !

Beaucoup de gens le font déjà, rappelez vous au mois de Juin, nous vous avions parlé de cette photo de Mark Zuckerberg où l'on peut voir son ordinateur avec la cam et le micro protégés …

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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?



Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «non coopératifs» à «retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre « judiciaire ». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté « Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges ». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

...[lire la suite]

Denis Jacopini anime des **conférences et des formations** 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-en-cybercriminalite-et-en-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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Une initiative francoallemande contre le chiffrement numérique

Révélations sur de petits piratages informatiques entre alliés...



Révélations sur de petits piratages informatiques entre alliés… C'est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l'ancien directeur technique de la DGSE, le service de renseignement extérieur français, s'est livré en juin dernier à une longue confession devant les élèves de l'école d'ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l'explique Le Monde.

Cet ex-cadre de l'espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l'attaque informatique de l'Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l'Elysée. Jusqu'à présent, les soupçons se portaient bien vers la NSA mais ils n'avaient jamais été confirmés. « Le responsable de la sécurité informatique de l'Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l'aide. On a vu qu'il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J'en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s'entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c'était eux. A la fin de la réunion, Keith Alexander (l'ex-directeur de la NSA), n'était pas content. Alors que nous étions dans le bus, il me dit qu'il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : 'Vous êtes quand même bons.' Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. » Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l'implication de la France dans une vaste opération d'espionnage informatique commencée en 2009 qui avait touché notamment l'Espagne, la Grèce ou l'Algérie. Le Canada, lui aussi visé, avait à l'époque soupçonné Paris, mais rien n'avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu'ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu'il était français. Et effectivement, c'était un Français. »

Article original de Thomas Liabot



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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les Etats-Unis étaient bien à l'origine du piratage informatique de l'Elysée en 2012 — leJDD.fr

Découvez à quoi ressemble une plateforme de cyberespionnage avancée

Découvez à guoi ressemble une plateforme de cyberespionnage avancée Kaspersky détaille le fonctionnement d'une plateforme avancée de cyberespionnage, baptisée Projet Sauron. Un outil remarquablement sophistiqué et probablement aux mains d'un Etat.

Kaspersky détaille le fonctionnement d'une plateforme avancée de cyberespionnage, baptisée Projet Sauron. Un outil remarquablement sophistiqué et probablement aux mains d'un Etat.

Symantec et Kaspersky mettent au jour ce qu'ils présentent comme un nouvel acteur du cyberespionnage, probablement soutenu par un État étant donné le niveau de sophistication atteint et les investissements requis (plusieurs millions de dollars, selon les chercheurs de l'éditeur russe). Kaspersky explique que la découverte de ce qu'il a baptisé le Projet Sauron, un nom que les assaillants emploient dans leurs fichiers de configuration, remonte à septembre 2015, suite à la détection de trafic réseau anormal au sein d'une organisation gouvernementale, via un de ses produits. Selon le Russe, la menace, qui cible les environnements Windows, est active depuis au moins juin 2011. Symantec, de son côté, a baptisé la nouvelle menace du nom de Strider. Chez l'éditeur américain également, la détection provient d'anomalies remontées par un de ses produits, travaillant par analyse comportementale.

×

Suite à leur première découverte, les équipes de Kaspersky racontent avoir isolé un étrange exécutable chargé en mémoire sur le serveur du contrôleur de domaine d'une organisation infectée. Une librairie enregistrée comme un filtre de mots de passe Windows, fonction utilisée par les administrateurs pour obliger les utilisateurs à respecter les règles de sécurité; et surtout un module ayant accès à des informations sensibles, comme les mots de passe desdits administrateurs. « La backdoor passive de Projet Sauron démarre chaque fois qu'un domaine, un utilisateur local ou un administrateur se connecte ou change son mot de passe, et elle récupère alors rapidement les mots de passe en clair », écrit Kaspersky.

Cibler les communications chiffrées

Au fil de son enquête, l'éditeur russe a pu mieux cerner les contours de cette menace jusqu'alors inconnue. Pour le spécialiste de la sécurité informatique, Projet Sauron masque une organisation à la pointe en matière de cyber-espionnage, une organisation à la tête d'une plate-forme modulaire de piratage, « conçue pour orchestrer des campagnes de long terme via des mécanismes de persistance furtifs couplés à de multiples méthodes d'exfiltration d'information ». Certaines d'entre elles étant peu communes. La plate-forme recourt notamment au protocole DNS pour exfiltrer des données. Tous les modules ou protocoles réseau de Sauron emploient par ailleurs des algorithmes de cryptage forts, comme RC4, RC5, RC6 ou AES.

D'autres éléments témoignent de la sophistication de cette menace et de son intérêt pour des informations hautement confidentielles. Comme l'utilisation de codes fonctionnant uniquement en mémoire, ce qui rend leur détection plus complexe. Une technique déjà exploitée par Duqu, une menace déjà mise au jour par Kaspersky et à l'œuvre… sur ses propres systèmes ! Le Russe explique encore que Projet Sauron s'intéresse tout particulièrement aux logiciels de chiffrement de ses cibles, tentant de dérober des clefs, des fichiers de configuration et les adresses IP des serveurs gérant les clefs. Autre détail révélateur de la volonté de Sauron de pénétrer les organisations les mieux protégées : la capacité, sur des réseaux isolés d'Internet (employés dans les domaines les plus sensibles), à exfiltrer des données sur des supports de stockage USB spécialement reconfigurés pour abriter une zone invisible du système d'exploitation hôte, zone dans laquelle vont être stockées des données à exfiltrer.

Si Kaspersky admet ne pas connaître le vecteur d'infection qu'utilisent les assaillants pour compromettre un premier système, il explique que Sauron détourne les scripts des administrateurs système de sa cible pour déployer ses malwares sur le réseau de sa victime. Des scripts normalement dédiés au déploiement de logiciels légitimes... De quoi faciliter les déplacements latéraux des assaillants une fois un premier système compromis.

Disparition des indicateurs de compromission

Pour Kaspersky, Projet Sauron a par ailleurs appris des erreurs d'autres acteurs similaires (comme Duqu, Flame, Equation ou Regin), évitant par exemple d'utiliser les mêmes artefacts d'une cible à l'autre. « Ce qui réduit leur valeur comme indicateurs de compromission pour les futures victimes », relève l'éditeur. Kaspersky estime que plus de 50 types différents de plug-ins peuvent venir se connecter sur la plate-forme de cyber-espionnage de Projet Sauron. « Presque tous les implants cœur de Projet Sauron sont uniques, possèdent des tailles et des noms de fichiers différents et sont bâtis individuellement pour chaque cible », écrit Kaspersky. Bref, pour l'éditeur, les assaillants ont intégré les méthodes des chercheurs en sécurité, qui traquent des schémas ou comportements identiques d'une cible à l'autre afin d'identifier de nouvelles menaces. « Sans ces schémas, l'opération sera plus difficile à mettre au jour », résume la société russe.

Cette dernière dit avoir identifié 30 organisations attaquées. « Mais nous sommes sûrs qu'il ne s'agit là que du minuscule sommet de l'iceberg. » Les organisations attaquées sont situées en Russie, en Iran et au Rwanda. Et opèrent dans des secteurs sensibles : gouvernement, recherche scientifique, armée, opérateurs télécoms, finance. S'y ajouteraient des cibles situées dans les pays italophones, selon Kaspersky, qui relève que la plate-forme de Sauron a été configurée pour cibler des organisations utilisant cette langue. De son côté, Symantec explique avoir identifié la menace chez 4 organisations ou individus en Russie, au sein d'une compagnie aérienne chinoise, dans une organisation suédoise et dans les murs d'une ambassade située en Belgique.

Difficile évidemment de déterminer d'où émane l'attaque. Kaspersky estime qu'il s'agit même là d'un problème « insoluble », étant donné la capacité des assaillants à multiplier les écrans de fumée afin de brouiller les pistes. L'éditeur russe relève toutefois un détail intéressant : l'emploi de termes renvoyant aux manuels Unix et notamment de 'Cruft' (désignant un élément superflu du logiciel), utilisé par les spécialistes de BSD. Pour Kaspersky, cette bizarrerie pourrait indiquer la présence, dans les équipes du Projet Sauron, de développeurs 'old school' ayant effectué leurs premières armes au sein de ces environnements. A moins qu'il ne s'agisse là que d'un écran de fumée de plus.

Article original de Reynald Fléchaux



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.



Contactez-nous

Original de l'article mis en page : Projet Sauron : anatomie d'une plateforme de cyberespionnage avancée

Quel cadre pour l'État d'urgence et la copie des données informatiques ?



Oyel cadre pour l'État d'urgence et la copie des données informatiques ?



Original de l'article mis en page : État d'urgence et copie des données informatiques : le cadre prévu par le gouvernement — Politique — Numerama