De nouveaux malwares super furtifs se cachent dans la mémoire des serveurs

De nouveaux malwares super furtifs se cachent dans la mémoire des serveurs

Kaspersky met en évidence une souche malveillante qui se cache dans la mémoire des systèmes et exploite des applications de confiance pour dérober des données. 10 organisations au moins en ont été victimes en France.

Une nouvelle espèce de logiciels malveillants, mise en évidence par Kaspersky Lab, ressemble bien à un cauchemar pour administrateurs système et responsables informatiques. Il s'agit d'une forme de malware utilisant des logiciels légitimes (comme l'outil de tests de pénétration Meterpreter) pour infecter un système, avant de détourner des services Windows couramment utilisés pour assurer son implémentation et son fonctionnement. Une fois le malware en cours d'exécution à l'intérieur de Windows, il efface toute trace de son existence et réside dans la mémoire du serveur. Le temps d'exfiltrer des informations qu'il convoite avant de s'effacer de lui-même.
Parce que ces nouveaux malwares, que Kaspersky a baptisés MEM: Trojan.win32.cometer et MEM: Trojan.win32.metasploit, résident en mémoire, ils ne peuvent pas être détectés par des antivirus standards, qui analysent le disque dur d'un ordinateur. En outre, le malware se cache en réalité à l'intérieur d'autres applications, ce qui le rend pratiquement invisible également des outils utilisant des techniques de listes blanches, comme c'est le cas de nombreux pare-feu.

Le redémarrage efface toute trace

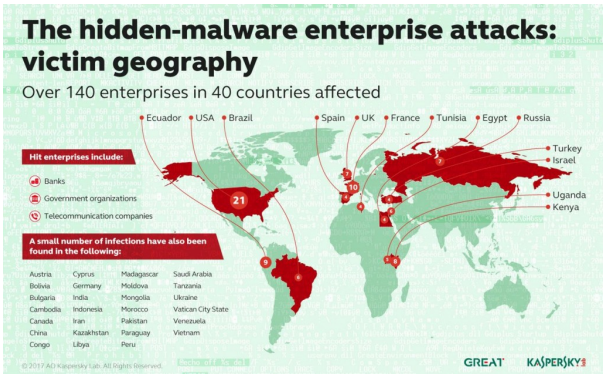
Selon un billet de Kaspersky sur le blog Securelist, le processus fonctionne en plaçant temporairement un utilitaire d'installation sur le disque dur de l'ordinateur. C'est ce petit outil qui loge le logiciel malveillant directement en mémoire en utilisant un fichier MSI standard de Windows avant d'effacer l'utilitaire. Une fois que le malware commence à collecter les données ciblées, il emploie une adresse de port inhabituelle (:4444) comme voie d'exfiltration.
L'ensemble de ces caractéristiques rendent ces malwares très furtifs. Car ils n'existent que dans la mémoire d'un ordinateur, ce qui signifie qu'un logiciel anti-malware n'a une chance d'identifier l'infection que lors d'une analyse de ladite mémoire, et uniquement pendant que le malware est toujours actif. Le redémarrage de l'ordinateur effacera toute trace, rendant inutile toute analyse 'forensic'.

PowerShell détourné

Kurt Baumgartner, chercheur au sein des Kaspersky Lab, explique que ses équipes de recherche ont d'abord trouvé ce logiciel malveillant dans une banque en Russie. L'équipe a pu accéder au serveur, dans ce cas un contrôleur de domaine, avant que le système ne redémarre, ce qui leur a permis d'isoler la souche infectieuse. L'équipe de Kaspersky a alors constaté que les attaquants utilisaient un script PowerShell pour installer un service malveillant dans la base de registre de l'ordinateur.
Selon le chercheur, si ce malware furtif échappera aux antivirus qui cherchent des signatures sur le disque dur d'un ordinateur, il peut toujours être découvert via des logiciels de protection qui traqueront ses activités suspectes : création de tunnels de communication chiffrée pour exfiltrer les données, démarrage de services ou lancement de l'activité PowerShell. Kurt Baumgartner assure que ses équipes suivent l'évolution du malware – qui devrait muter pour échapper aux défenses qui vont être mises en œuvre suite à la publication de Kaspersky – et qu'il convient notamment de surveiller la diffusion de données à partir de lieux différents sur le réseau utilisant le tunnel de communication caractéristique de la souche.

La France, second pays ciblé

Et de conseiller aux équipes de sécurité de scruter les journaux système et de surveiller le trafic sortant du réseau. Tout en précisant qu'il vaut mieux stocker ces données hors ligne de sorte que le logiciel malveillant ne puisse pas trouver et effacer ces preuves. Autre astuce pour contrarier les assaillants : désactiver PowerShell. Une solution radicale mais parfois difficile à mettre en œuvre, de nombreux administrateurs ayant recours à cet utilitaire…[lire la suite]



Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Anatomie du malware super furtif, caché dans la mémoire des serveurs

---

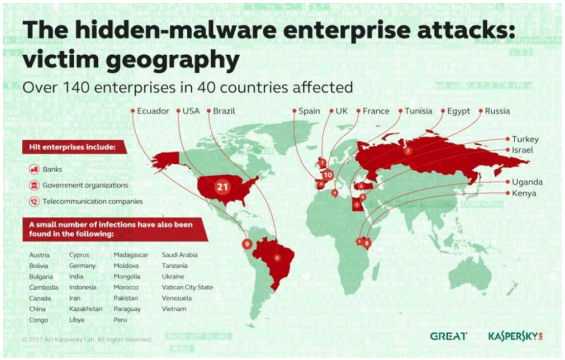
Une nouvelle menace plane sur les distributeurs automatiques de billets

Une nouvelle menace plane sur les distributeurs automatiques de billets

---

Des chercheurs en sécurité informatique ont découvert une faiblesse des DAB, difficilement détectable à ce jour.

Les distributeurs automatiques de billets restent une cible appréciée des pirates informatiques. Selon une étude publiée par Kaspersky , une entreprise spécialisée en cybersécurité, et relayée par 01Net , les « DAB » seraient vulnérables à une attaque informatique perfectionnée et surtout, discrète. Cette attaque a été détectée 10 fois en France, rapporte Kaspersky. C'est le deuxième pays à être autant ciblé après les Etats-Unis.
La méthode est assez ingénieuse. « Alors que les virus que l'on connaît aujourd'hui écrivent des fichiers sur le disque dur du DAB, cette nouvelle génération d'attaques va s'en prendre à la mémoire vive, ce qui ne laisse aucune trace », décrit Daniel Fages, directeur technique de Stormshield, une entreprise française spécialisée, aux « Echos ». Une fois introduit dans le système, qui est peu ou prou un ordinateur, l'attaquant va pouvoir prendre le contrôle de la machine à distance, à n'importe quel moment. L'attaque a un nom : « fileless malware », ou malware « sans fichier », en bon français.



Les Etats-Unis sont particulièrement touchés par le phénomène – Kaspersky

A partir de là, tout est possible. « L'attaquant peut faire sortir des billets comme il l'entend, ou bien capturer les données des utilisateurs qui retirent des billets dans le DAB infecté », décrit Daniel Fages.

Les DAB, pas réellement protégés

Cette vulnérabilité est d'autant plus importante que les distributeurs ne sont que très rarement mis à jour aujourd'hui. Si certaines banques disposent de protection contre les virus « classiques », très souvent, elles s'en contentent. « Tant que ça marche, on ne touche pas », résume Daniel Fages.
Difficulté supplémentaire : les DAB sont produits sur un mode industriel. Une faille telle que celle-ci peut donc fonctionner sur de très nombreux appareils.

Une attaque difficile à réaliser

Néanmoins, une telle attaque n'est pas facile à réaliser. Pour infiltrer la mémoire vive du distributeur, il faut d'abord avoir infecté le réseau qui relie les DAB d'une même banque entre eux. Ce réseau, souvent interne, n'est pas directement exposé à Internet et donc à une attaque.
« Les attaquants capables d'une telle manoeuvre ont des moyens et de très bonnes connaissances techniques », estime Daniel Fages.

Une sécurité : protéger son code PIN

Qui plus est, si les attaquants décident de s'en prendre aux données des …[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Une nouvelle menace plane sur les distributeurs automatiques de billets, Banque – Assurances

Précautions à prendre avant de se débarrasser du vieux matériel informatique

Précautions à prendre avant de se débarrasser du vieux matériel informatique

Lors de la mise au rebut ou de la revente, il est nécessaire de se préoccuper de l'effacement préalable des informations stockées sur tout dispositif comportant un support de stockage (ordinateur, serveur, téléphone, imprimante, clé USB, appareil photo numérique, récepteur GPS).Il est tout aussi important d'appliquer ces règles d'hygiène lors de la réception d'un matériel d'occasion avant sa réutilisation.La méthode choisie pour effacer les informations existantes sur le support informatique obsolète dépend de son niveau de sensibilité et du risque associé (voir Guide technique de l'ANSSI n° 972-1/SGDN/DCSSI). Dans le cas particulier de données ou de matériels protégés par l'instruction générale interministérielle 1300, une procédure stricte doit être appliquée par des personnels habilités. Dans le cas de l'exportation de matériel hors de l'environnement sécurisé de l'entreprise, ou lors d'un transfert interne entre entités ayant des besoins de confidentialité distincts, la mesure la plus sûre reste l'extraction et la destruction physique des supports de stockage, puis leur remplacement lors de la remise en service.Si cette destruction n'est pas envisageable, il existe, pour des composants type PC (comme les disques durs), des logiciels spécialisés destinés à effacer l'intégralité des données stockées. On peut citer le logiciel Blancco, dont la version 4.8 bénéficie d'une Certification de Sécurité de Premier Niveau délivrée par l'ANSSI.

Les imprimantes et photocopieurs multifonctions

Les imprimantes et photocopieurs multifonctions se comportent comme un ordinateur en intégrant souvent un navigateur web, une messagerie électronique, une connectivité Wifi et Ethernet, un accès USB et un disque dur. Le fonctionnement standard de ce type de matériel implique de stocker sur le disque dur les documents à imprimer ou à scanner. Selon vos activités ou votre mission, ce disque dur pourrait stocker des données confidentielles de votre entreprise. Un point d'attention particulier doit être porté sur les contrats de maintenance qui intègrent parfois un accès distant non contrôlé à l'équipement depuis Internet.

L'imprimante ou le photocopieur propose souvent des fonctionnalités de sécurité permettant l'effacement du disque dur ou la suppression des données liées aux impressions, copies, télécopies et numérisations pouvant être enregistrées sur le disque dur. Ce processus d'effacement peut parfois être activé automatiquement après chaque utilisation, ou programmé pour s'exécuter à intervalles spécifiés. Ces fonctionnalités ne garantissent pas toujours un effacement sécurisé des données considérées, et les périphériques de stockages internes et externes devront faire l'objet d'une procédure similaire aux autres équipements informatiques avant le décommissionnement de l'appareil. Attention toutefois, ces composants restent généralement la propriété de la société louant les appareils.

Lors de la réception d'un matériel de ce type, il conviendra de désactiver les fonctionnalités de stockage «dans le cloud» lors du paramétrage initial de l'appareil si celles-ci sont disponibles, et de s'assurer du niveau de mise à jour de l'appareil. Il faudra bien sûr maintenir ce niveau régulièrement afin de limiter l'exposition de son système d'information à des failles éventuellement apportées par cet équipement.

Les autres matériels informatiques

La plupart des matériels modernes intègrent des fonctions de restauration des paramètres d'usine. Il convient a minima de réinitialiser ainsi tout équipement entrant ou sortant de l'entreprise afin de supprimer par exemple certains mots de passes ou autres paramètres de configuration sensibles qui pourraient être stockés sur ces appareils.

Une réinitialisation permet également de se prémunir d'un éventuel piégeage logiciel simple de l'appareil par son précédent propriétaire.

Documentation

• Guide technique n° 972-1/SGDN/DCSSI : Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter.
http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf
• Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale :
http://www.sgdsn.gouv.fr/IMG/pdf/IGI_1300.pdf
• CSPN du logiciel Blancco :
http://www.ssi.gouv.fr/entreprise/qualification/blancco-data-cleaner-version-4-8/

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Bulletin d'actualité CERTFR-2017-ACT-007

---

6 bonnes pratiques pour se

protéger du piratage informatique

	6 bonnes pratiques pour se protéger du piratage informatique

Par manque de temps ou de ressources, les PME négligent le risque de piratage informatique. Quelques règles de bon sens suffisent pourtant à écarter en partie les menaces.

Perdre ses données suite à une attaque informatique peut avoir de lourdes conséquences pour une start-up ou une PME. L'entreprise peut même ne jamais s'en relever. Piratage de site Internet, clé USB piégée, vol de mot de passe, programme espion caché dans des pièces jointes… Les cyber menaces sont de plus en plus fréquentes. Quelles sont les règles simples pour s'en protéger ? Le point avec Stéphane Dahan, président de Securiview, entreprise spécialisée dans le management de la sécurité informatique.

#1 : Identifier les données les plus sensibles

« *Faites preuve d'une saine paranoïa*, affirme Stéphane Dahan. *C'est-à-dire sachez définir précisément quelles sont les informations à protéger dans l'entreprise* ». Inutile donc de mettre des barrières partout sans discernement. Quelle que soit leur forme (mail, papier, fichier), posez vous donc la question : quelles sont les données les plus sensibles et quelle est la probabilité qu'on me les vole ? « *Ensuite, il faut les localiser. Messagerie, Dropbox, téléphone, autant de pistes de fuite possible pour des informations qui ont de la valeur.* »

#2 : Mettre à jour les systèmes et sauvegarder

« *Ne pas oubliez de mettre à jour régulièrement ses antivirus et ses systèmes d'information. On voit trop souvent des entreprises négliger cet aspect* », soutient Stéphane Dahan. N'oubliez pas non plus de **sauvegarder périodiquement vos dossiers stratégiques**. « *Idéalement, ils doivent être stockés à plusieurs endroits. Si un serveur brûle, que vous soyez capable de les retrouver ailleurs* ».

#3 : Assurer la confidentialité des données clés

A l'intérieur de l'entreprise, assurez-vous que seuls les salariés ayant besoin des informations sensibles puissent y accéder. Par exemple, que les mots de passe ou clés de chiffrement ne soient **attribués qu'aux personnes qui ont besoin de les connaître**.

#4 : Définir et faire appliquer la politique de mot de passe

Attention dans le choix des mots de passe ! C'est trop souvent le talon d'Achille des systèmes d'information. « *Eviter de choisir les plus bateau comme abc123 ou 12345, une mauvaise habitude plus courante qu'on ne le dit* », insiste Stéphane Dahan. Idéalement, fixez des règles de choix et de dimensionnement des mots de passe et **renouveler ces derniers régulièrement**.

#5 : Protéger les terminaux mobiles

Les postes mobiles sont des points d'accès potentiels pour des pirates informatiques. Selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ils doivent bénéficier au moins des mêmes mesures de sécurité que les postes fixes. Même si cela représente une contrainte supplémentaire, les conditions d'utilisation des terminaux nomades imposent même le renforcement de certaines fonctions de sécurité.

#6 : Sensibiliser l'équipe au risque de piratage

Périodiquement, rappelez à votre équipe quelques règles élémentaires : ne pas divulguer des mots de passe à un tiers, ne pas contourner les dispositifs de sécurité internes, éviter d'ouvrir la pièce jointe d'un message venant d'une adresse inconnue, etc. La sensibilisation doit également porter sur **l'utilisation des réseaux sociaux**. « *Les comptes Facebook ou Linkedin des collaborateurs sont des mines d'informations pour les pirates*, explique Stéphane Dahan. *Ils s'en servent pour adresser des messages très personnalisés qui vont leur permettre d'entrer dans le système d'information de l'entreprise.* »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : 6 bonnes pratiques pour se protéger du piratage informatique, Marketing et Vente – Les Echos Business

---

RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018

RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018

Le GDPR, règlement européen qui renforce le droit des utilisateurs en matière de données personnelles, entrera en vigueur en mai de l'an prochain. D'ici là, 4 actions doivent être menées.

2017 s'annonce chargé pour toutes les entreprises qui collectent et manipulent, de près ou de loin, de la data en provenance de leurs consommateurs. Pour cause, le nouveau règlement européen sur la protection des données personnelles (GDPR) entrera en application le 25 mai 2018. Son objectif est de renforcer les droits des personnes en la matière… et les obligations des entreprises. Voici comment éviter une amende qui sera salée pour les mauvais élèves : 2 à 4% du chiffre d'affaires ou 20 millions d'euros, le montant le plus élevé étant choisi.

Protéger les données personnelles en amont

Commençons par la bonne nouvelle. L'entreprise qui procède à un traitement de données personnelles n'aura plus à remplir de déclaration auprès de la Cnil pour l'en informer, comme elle y est pour l'instant tenue. Ce pilier de la loi « Informatique et liberté » saute.

« Les entreprises doivent 'en échange' se conformer au concept de « privacy by design » érigé par l'article 25 du règlement », explique Matthieu Berguig, avocat spécialisé en droit des nouvelles technologies. Ce concept leur impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. « Un fabricant d'objets connectés doit donc se poser des questions de base avant de mettre son produit sur le marché : où son stocké les données, par quel protocole de cryptage seront-elles protégées, sont-elles anonymisées… », illustre Matthieu Berguig. Délestée de ce travail de vérification, la Cnil s'évite beaucoup de paperasse… et gagne du temps pour auditer le marché. « On peut être sûrs que les contrôles seront plus nombreux », prévoit Matthieu Berguig.

Nommer un déléguer à la protection des données

La Cnil pourra travailler dans cette perspective main dans la main avec un collaborateur d'un nouveau genre, le délégué à la protection des données (DPD). L'article 37 impose sa nomination dans plusieurs cas de figure : lorsque « le traitement est effectué par une autorité publique ou un organisme public », lorsque le traitement impose « un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque le traitement à grande échelle concerne « les catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10« . Beaucoup d'entreprises sont donc concernées par l'obligation et toutes sont encouragées à en nommer un.

Chargé de faire respecter le règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, le DPD tient un peu du mouton à cinq pattes. Chez les entreprises déjà bien structurées, le « compliance officer », le collaborateur qui s'assure de la conformité de toute décision business à la législation, sera un candidat naturel à ce rôle de DPD. « Pour toutes les autres, il faut trouver la perle rare, un profil juridique capable également de comprendre les problématiques métiers », note Alan Walter, avocat associé chez Walter Billet Avocats.

Tenir un registre de traitement des données

« En 2017, beaucoup d'entreprises vont s'embarquer dans une totale remise à plat de leurs systèmes de traitement des données à caractère personnel », note Alan Walter. Pour cause, l'article 30 impose aux entreprises de plus de 250 salariés de tenir un registre des traitements effectués. Un registre qui comporte, entre autres, le nom et les coordonnées du responsable du traitement, les finalités du traitement, la catégorie de destinataires auxquels les données à caractère personnel ont été ou seront communiqués. « C'est ce registre qui sera consulté par la Cnil lorsqu'elle voudra entrer en action », précise Matthieu Berguig.

L'article 33 impose d'ailleurs à une entreprise qui a subi une violation de données à caractère personnel d'en notifier l'autorité de contrôle. « Seuls les opérateurs télécoms y étaient jusque-là tenus », note Matthieu Berguig.

Créer une base interopérable pour le droit à la portabilité

L'article 20 du règlement aboutit à la création d'un droit à la portabilité des données personnelles. Si un de vos clients vous quitte pour la concurrence, il a le droit de réclamer le transfert de l'intégralité des données le concernant. « Lorsque cela est techniquement possible », précise l'article. « En d'autres termes, lorsque vous passerez d'une boîte mail à une autre, vous aurez théoriquement le droit d'importer tout votre historique de mails », illustre Matthieu Berguig. Une obligation dont la mise en place pourrait être techniquement compliquée dans de nombreux cas.

Alan Walter souligne un autre écueil, juridique celui-ci, en prenant l'exemple de l'un de ses clients, courtier en assurance pour expatriés. « Les données qu'il recueille sont très sensibles car elles concernent le domaine médical. Elles ne peuvent être transmises à n'importe qui, du fait du secret médical. Donc comment doit-il faire ? », s'interroge-t-il. Dans ce cas, il faudrait s'assurer que le destinataire des données offre les garanties nécessaires pour qu'il ne soit pas porté atteinte aux droits des personnes concernées. Problématique d'autant plus épineuse avec des transferts de données qui sont susceptibles d'intervenir vers des opérateurs situés hors de l'Union européenne et donc soumis à des droits différents. Premiers éléments de réponse début mai 2018.

Original de l'article mis en page : Protection des données : voici comment être en règle pour 2018

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne.

Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement.

Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel.

Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation…), mais aussi les contrats passés avec les fournisseurs et clients sont impactés (voir encadré ci-dessous).

« Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le GRPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilité en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements.

Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs…

Le délégué à la protection des données

Le règlement européen consacre la fonction de Délégué à la Protection des Données (DPD ou en anglais DPO) dans les organismes.

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un DPO :

1. s'ils appartiennent au secteur public,
2. si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. si leur activité principale les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

Les responsables de traitement peuvent opter pour un DPO mutualisé ou externe.

Véritable « chef d'orchestre » de la conformité en matière de protection des données, le DPO est chargé :

1. d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
2. de contrôler le respect du règlement et du droit national en matière de protection des données ;
3. de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA ou EIVP) et d'en vérifier l'exécution ;
4. de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

QUI PEUT ÊTRE DPO ?

Le DPO est désigné sur la base de son expertise.

CONSEILS POUR LA MISE EN PLACE DU FUTUR DPO

Compte tenu que jusqu'au 25 mai 2018, ne non respect de la Loi Informatique et Libertés est passible de 5 ans de Prison et jusqu'à 300 000 euros d'amende, nous vous conseillons fortement d'entamer au plus vite les démarches suivantes déclarer un CIL avant le 25 mai 2018 ou désigner un DPO après. Puis :

1. Réaliser ou faire réaliser un indispensable état des lieux (appelé aussi audit) afin d'identifier l'ensemble des traitements de données personnelles et l'ensemble des lieux dans lesquels des données personnelles sont traitées ;
2. Identifier dans la Loi Informatique et Libertés ou dans le RGPD des particularités propres à votre métier qui vous autorise à certains traitements interdits à d'autres activités ou qui nécessiteraient une demande d'autorisation ;
3. Faire une analyse de risque autour des traitements et des données personnelles présentes dans votre établissement. Cette étape indispensable peut être assurée par notre Expert Denis JACOPINI, Certifié ISO 27005 Risk Manager ;
4. Porter au registre l'ensemble des traitements identifiés ;
5. Mettre en conformité les traitements qui ne respectent pas la loi ou le règlement.
6. Suivre régulièrement l'évolution des traitements au sein de l'organisme.

Articles du règlement associés

Article 13 | Article 14 | Article 30 | Article 33 | Article 35 | Article 36 | Article 37 | Article 38 | Article 39 | Article 47 | Article 57

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Datadock Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Nous animons des Formations sur le RGPD en individuel ou en groupes

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Original de l’article mis en page : Le règlement européen de protection des données et les contrats fournisseurs

Un collectif Anonymous pirate le site de l’Anssi

Un collectif Anonymous pirate le site de l’Anssi

Cible d'une attaque DDoS, le site Internet de l'Agence nationale de la sécurité des systèmes d'information (Anssi) a été bloqué à plusieurs reprises les 4 et 5 février.
Trois semaines après l'annonce d'une campagne de recrutement, l'Agence nationale de la sécurité des systèmes d'information (**Anssi**) fait les frais de sa popularité grandissante. Cible d'une attaque par déni de service distribué (DDoS), le site Internet de l'Anssi a été bloqué le 4 février au soir, rapporte Zataz, et a été à nouveau perturbé ce vendredi 5 février après-midi jusqu'à 15h30 environ.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Le site de l'Anssi piraté par un collectif Anonymous

---

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Souhaitant mettre rapidement sur le marché leurs produits, les fabricants d'objets connectés ont eu tendance à négliger l'aspect sécurité, contribuant ainsi à la vulnérabilité de leurs utilisateurs face à de possibles attaques.

Atlantico : En septembre et octobre 2016, deux attaques DDOS ont été particulièrement marquantes : la première sur l'entreprise OVH et la deuxième sur DYN. Dans les deux cas, ces attaques ont été rendues possibles par les objets connectés. Malgré l'ampleur de ces attaques, celles-ci sont à relativiser. Dans une récente étude réalisée pour le compte de l'entreprise HSB, on note que seulement 10% des utilisateurs ont été touchés par des problèmes de piratage. Quels sont les risques du piratage des objets connectés ?

Quel peut être le préjudice porté aux particuliers et aux entreprises ?

Yvon Moysan : Une attaque DDoS ou attaque par déni de service massive vise à **rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.** Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément et depuis de multiples endroits. L'intensité de ce « tir croisé » rend le service instable, voire indisponible. **Le risque d'être confronté à ce type d'attaque est important et surtout les tentatives sont nombreuses**. Dans le cas de la société américaine Dyn que vous évoquez, celle-ci a été victime d'une attaque de plus d'un Téra-octet par seconde, ce qui pourrait concerner environ 10 millions d'objets connectés piratés. Ce niveau d'intensité est toutefois très rare.

Le préjudice subi dépend du type d'objets connectés piratés et du caractère sensible des données des particuliers. Si la majorité des objets connectés contiennent rarement des informations aussi sensibles que celles qui sont stockées sur un ordinateur, **il en existe des sensibles comme les voitures connectées ou les fusils intelligents qui, piratés à distance, peuvent représenter un véritable danger, potentiellement mortel pour l'utilisateur.** Et **ce risque s'est d'ores et déjà avéré.** Des experts en sécurité informatique ont ainsi réussi à prendre le contrôle à distance d'une Jeep Cherokee. Ils ont pu agir sur la vitesse, freinant et accélérant à leur guise, envoyant même la voiture dans le fossé alors que pour le fusil intelligent, d'autres experts ont réussi a bloqué le déclenchement du tir.

Le risque existe également pour des objets plus communs comme les applications de smart home. Des hackers ont ainsi réussi à bloquer la température de thermostats connectés à une température polaire ou saharienne. Plus préjudiciable, des hackers ont pris le contrôle de caméras de surveillance, récupéré les vidéos enregistrées, et au final les ont diffusées sur le Web. Un baby phone a également été la cible d'un hacker terrorisant un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, celui-ci s'est mis à hurler des insanités sur le nourrisson. **Le risque peut surtout être généralisé si des hackers réussissent à prendre le contrôle des réseaux d'électricité ou de gaz sur un quartier par exemple.** Il devient en effet possible de plonger toute une zone dans le noir ou, en fonction des données récoltées sur la consommation, de savoir quelles habitations sont occupées ou pas, en vue d'éventuels cambriolages.

Cela peut ensuite être contraignant pour la société qui a fabriqué et vendu les objets piratés car cela révèle **la faiblesse du niveau de sécurité**. Dans le cas de l'attaque de la société Dyn, une partie des objets connectés étaient ceux de la société chinoise Xiongmai, qui a dû les rappeler en urgence pour leur appliquer un correctif de sécurité. Cela peut aussi être problématique pour les clients de la société victimes de l'attaque. Dans le cas de Dyn, cela a eu pour conséquence de rendre inaccessible pendant une dizaine d'heures des sites comme Twitter, Ebay, Netflix, GitHub ou encore PayPal.

On peut aussi s'interroger sur certaines pratiques des constructeurs. Le fait de mettre un mot de passe commun à tous les appareils avant une première connexion a déjà été pointé du doigt. Quels autres dysfonctionnements peut-on mettre en avant ? Face à l'augmentation du nombre d'objets connectés, comment s'adaptent précisément les constructeurs en termes de sécurité ?

Tout d'abord il est important de préciser que ce type d'attaques par déni de service n'a rien de nouveau : les cybercriminels utilisent depuis des années des armées d'ordinateurs piratés pour inonder de requêtes les sites ciblés et les rendre inaccessibles.

La nouveauté réside ici dans le nombre croissant des objets connectés qui accroit de manière exponentielle les possibilités d'attaques. Or **la puissance d'une attaque dépend essentiellement du nombre de périphériques piratés, d'où l'intérêt de passer par les objets connectés**. Il existe en effet **plusieurs milliards d'objets connectés dans le monde contre quelques centaines de millions d'ordinateurs.** Pour y faire face, il existe des solutions proposées par les hébergeurs pour protéger leurs serveurs des attaques. Ces solutions permettent, par exemple, d'analyser en temps réel et à haute vitesse tous les paquets, et si besoin d'aspirer le trafic entrant, voire de mitiger, c'est-à-dire repérer tous les paquets IP non légitimes, tout en laissant passer les paquets IP légitimes.

Du côté des constructeurs d'objets connectés, tous les thermostats, toutes les webcams ou les imprimantes ne présentent pas de faille de sécurité, mais il s'agit d'un point préoccupant car **pour la plupart des fabricants, la sécurité n'a pas été la priorité dès le départ**, **ayant souvent été donnée à la rapidité de la mise à disposition du produit sur le marché pour répondre à un nouveau besoin**. Il faudrait que des normes minimales de sécurité puissent être définies comme le cryptage des données échangées sur le réseau ou l'exigence de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance et l'interdiction de mots de passe comme « 123456 » particulièrement vulnérables. Dans cet esprit, la Online Trust Alliance, qui regroupe des éditeurs comme Microsoft, Symantec (Norton) et AVG, a rédigé un guide des bonnes pratiques pour minimiser les risques de piratage. Les constructeurs d'objets connectés peuvent, par ailleurs, faire évaluer leurs systèmes de cryptage par des sociétés spécialisées, pour identifier les éventuelles vulnérabilités.

Comment se prémunir du piratage d'objets connectés ? Quels sont les bons comportements à adopter ? Que faire en cas de doute ?

Du côté des particuliers, il apparait préférable de privilégier les produits de sociétés à la pointe des questions de sécurité informatique, comme Google ou Apple. Il faut également installer régulièrement **les mises à jour de sécurité et les mises à jour logicielles**, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut **changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle.** Pour finir, il faut **limiter l'accès d'un objet connecté aux autres objets connectés dans la maison.** Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau. Par exemple, il n'est pas vraiment nécessaire que l'imprimante soit connectée à la télévision.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Attention danger : apprenez à vous protéger contre le piratage de vos objets connectés du quotidien | Atlantico.fr

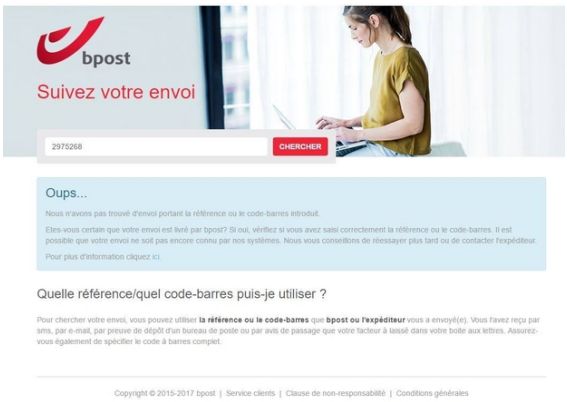
---

Attention à ce mail suspect. Ne cliquez pas !

Attention à ce mail suspect. Ne cliquez pas !

Il s'agit en réalité d'un ransomware, un logiciel malveillant qui vise à prendre vos données et fichiers personnels en otage et les bloquer !

Après la fausse facture de Free, c'est cette fois la marque et le logo bpost qui ont été détournés par des hackers avec l'ambition d'essayer de *pomper* vos données personnelles et de les prendre en otage afin de réclamer, par après, une « rançon » contre la libération de celles-ci ! Pour ce faire, les pirates utilisent ce qu'on appelle un *ransomware*.
Pour tenter d'arriver à leurs fins, les hackers ont donc emprunté les traits de bpost afin de vous demander de cliquer sur un lien permettant, soi-disant, de retrouver trace d'un colis qui n'a pas encore été livré. Le piège est en marche. Le principe est donc simple et diabolique puisque les utilisateurs qui reçoivent ce fameux mail ont, en théorie, toute confiance en l'institution.



En effet, s'il est trop tard et que vous avez déjà appuyé sur le bouton de votre souris, le mal est fait. Le logiciel ainsi installé aura tout le loisir de prendre connaissance de vos données et fichiers personnels, voire même prendre le contrôle de votre poste de travail, bloquant au passage l'accès à vos précieuses infos via une clé de cryptage… permettant aux malotrus de réclamer une rançon contre la libération de vos données ou de votre ordinateur ! Inutile de préciser que dans bien des cas, la spirale infernale est enclenchée !
L'excellente série de *Netflix Black Mirror* avait d'ailleurs centré un de ses épisodes sur cette problématique, les protagonistes perdant au fil de celui-ci, le contrôle total sur les événements.
Que faire en cas d'infection ?
Si vous avez installé ledit logiciel, il faudra de toute façon passer, au minimum, par la case du scan antivirus. Sans plus attendre également, il est fortement conseillé de débrancher immédiatement tous les disques durs externes et autres qui pourraient être plus facilement sauver, d'autant plus s'ils contiennent des sauvegardes de vos fichiers. Idem, pensez à déconnecter vos espaces de stockage virtuel (Dropbox, iCloud,…)
Dans certains cas, certains logiciels sont capables de combattre l'infection. Une petite recherche sur Google et différents forums s'impose donc.
Il est aussi très important de rappeler qu'il ne faut surtout pas rentrer dans « le jeu » et donc absolument éviter de payer la rançon demandée. Rien ne dit en effet que les pirates la joueront *fair play*… De plus, il est aussi très utile de prévenir les autorités compétentes…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Vous avez reçu un mail suspect de bpost ? Ne cliquez pas ! (PHOTOS) – DH.be

Les caméras de surveillance de Washington paralysées par le Ransomware again

Les caméras de surveillance de Washington paralysées par le Ransomware again

Selon le Washington Post, un ransomware aurait paralysé pendant plusieurs jours le réseau de cameras de surveillance municipale de Washington DC. Une réinitialisation générale a permis de se débarrasser du malware.

Quelques jours avant l'investiture de Donald Trump, la ville de Washington a fait face à une mauvaise surprise : selon le Washington Post, les cameras de la ville ont été victimes d'un malware de type ransomware qui les a rendus inutilisables, empêchant l'enregistrement d'image pendant plusieurs jours.

L'attaque a été détectée lorsque la police a réalisé que quatre caméras municipales ne fonctionnaient pas correctement et a contacté son prestataire informatique afin de résoudre le problème. La société a immédiatement détecté la présence de deux types de ransomware au sein des cameras, ce qui les a poussés à lancer une évaluation globale portant sur l'ensemble des appareils connectés au réseau de la ville. Au total, 123 caméras sur les 187 connectées au réseau présentaient des signes d'infection.
Les services municipaux n'ont néanmoins pas eu besoin de sortir leur porte-monnaie bitcoin pour remettre le système en route : une simple réinitialisation des cameras utilisées a permis de se débarrasser du malware et de relancer le fonctionnement. Le CTO de la ville a précisé qu'aucune rançon n'avait été payée par la ville et que le malware n'avait pas cherché à accéder au reste du réseau interne de la ville de Washington DC.
Washington s'en sort donc plutôt bien, contrairement à cet hôtel de luxe qui s'est vu contraint de payer les opérateurs d'un ransomware qui avaient bloqué l'ensemble du système de clef magnétique utilisé pour accéder aux chambres. Mais peu d'informations ont été diffusées par la ville sur la nature exacte de l'attaque, du ransomware ou même de la demande de rançon.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Ransomware again : les caméras de surveillance de Washington paralysées – ZDNet