Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI
• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI
Notre dossier : Données personnelles, un gisement sous haute protection

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

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)

Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*

Popcorn Time, un rançongiciel bien vicieux

Popcorn Time, un rançongiciel bien vicieux

Depuis peu, les rançongiciels (ou ransomware) constituent de véritables fléaux dans l'univers de l'informatique et du web. Ils touchent les données personnelles de millions de gens de par le monde. Les experts en sécurité se sont même mis à taxer 2016 comme étant « l'année des rançongiciels ».

Payez ou infectez vos amis

Sur cette année, il se peut que Popcorn Time soit le rançongiciel qui vienne clore la propagation de ces logiciels de chantage. Ce nouveau ransomware pose un gros dilemme à sa victime en lui imposant de payer une rançon ou d'infecter ses amis.

Pour commencer, il emprunte le nom d'une application de streaming vidéo ayant défrayé la chronique en 2015, ce qui incite au téléchargement de celle-ci. Ensuite, il infecte l'ordinateur de la victime par le biais d'un courriel piégé ou d'un lien malveillant, puis crypte ses données personnelles en usant d'un algorithme de chiffrement AES 256 bits.

Après que les données ont été cryptées, il impose à la victime de donner la valeur de 1 bitcoin (soit environ 700 €) ou de le transmettre sur l'ordinateur d'un ami. C'est une méthode toute nouvelle avec en plus une limite du nombre d'introductions de clé de déchiffrement. Entrer quatre fois la mauvaise clé ferait perdre définitivement ses données.

Les dossiers Windows sont les premières cibles

D'après la conclusion des enquêtes réalisées par le site Bleeping Computer sur ce rançongiciel, il ciblerait en premier les fichiers présents dans les dossiers Windows : Mes Documents, Images, Musiques et toutes les données sur le Bureau.

Afin de faire face à ce logiciel de rançon, la meilleure façon pour un utilisateur lambda est de prendre des précautions préventives basées sur les mesures de sécurité les plus basiques :

• faire des copies de ses données personnelles vers un support externe qui se débranche de l'ordinateur après chaque usage de ce dernier et sur les Clouds comme Dropbox, OneDrive, Google Drive, Mediafire, Mega, pCloud, Flipdrive… ;

• éviter d'ouvrir les mails aux destinateurs inconnus et contenant des liens ou des pièces jointes. Il est aussi possible que Popcorn Time provienne d'une personne de votre liste de contact. Prenez les mêmes réserves tant que le contenu n'a pas été formellement reconnu ;

• mettre à jour son système d'exploitation et son antimalware.

…[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 Certifié ISO 27005 Risk Manager, 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 : Popcorn Time : le plus vicieux rançongiciel de cette année – @Sekurigi

---

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

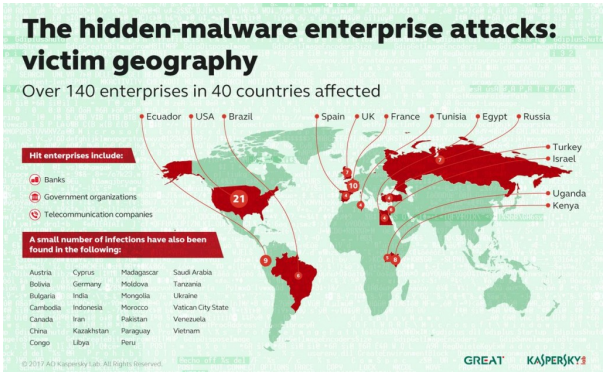
Selon un billet de Kaspersky sur le blog Securelist, le processus fonctionne en plaçant temporairement un utilitaire d'installation sur le disque dur de l'ordinateur. C'est ce petit outil qui loge le logiciel malveillant directement en mémoire en utilisant un fichier MSI standard de Windows avant d'effacer 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

---

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

	Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Cette étude analyse les risques de cyberattaques sur des infrastructures énergétiques européennes, ainsi que leurs potentielles conséquences, notamment sur les réseaux électriques. Elle offre également une approche comparative des mesures prises par différents pays d'Europe afin de protéger leur industrie et collaborer à l'échelle de l'Union européenne.

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité sur toute la chaîne de valeur énergétique, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné cette industrie : les cyberattaques.

Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique.

La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

LIRE L'ETUDE (PDF)

Original de l'article mis en page : Cyberattaques et systèmes énergétiques: faire face au risque | IFRI – Institut français des relations internationales

---

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

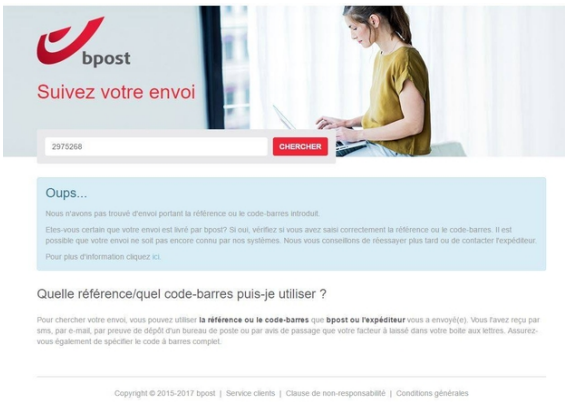
Réagissez à cet article

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.

Réagissez à cet article

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

Protéger son identité contre le vol sur Internet devrait être une priorité

Protéger son identité contre le vol sur Internet devrait être une priorité

Selon une étude concernant le vol d'identité et menée aux États-Unis par l'entreprise spécialisée dans la cybersécurité mobile Lookout auprès de 2000 clients, les délits concernant les données personnelles sont en pleine expansion. Ils constituent l'un des principaux soucis des usagers d'Internet et de la téléphonie mobile, qu'ils soient particuliers ou entreprises. Actuellement, le vol… Lire la suite

Actuellement, le vol d'identité est considéré comme un phénomène inéluctable d'après les enquêtes réalisées par Lookout. Les résultats démontrent que près de 35 % des sondées ont été victimes de vol d'identité. 41 % affirment que leurs données personnelles ne peuvent plus être sécurisées et, à un moment donné, elles seront inévitablement volées. D'ailleurs, aux États-Unis, le pourcentage d'infraction sur les identités des personnes a augmenté de près de 20 % depuis octobre 2015.

Internet : principal moyen de vol

Lookout affirme que le vol de données personnelles ne se passe plus par les méthodes classiques telles que la fouille des ordures dans les rues ou encore le vol de courrier dans les boîtes aux lettres ou il est très facile d'y trouver des informations permettant d'accéder aux numéros de carte de crédit ou de comptes divers. De nos jours, les criminels sont plus malins et bien plus discrets en usant de moyens sophistiqués et d'Internet comme les techniques de « phishing ».

Cette méthode profite de la faille humaine et non de l'informatique. Les voleurs se font passer pour une banque, un opérateur téléphonique ou une entreprise pour pousser la victime à se connecter sur leur site à travers un faux lien hypertexte. De cette manière, ils peuvent récolter des informations personnelles (des coordonnées bancaires surtout) qu'ils vont utiliser pour réaliser des achats ou des transferts d'argent vers leur compte.

En effet, l'étude menée par Lookout démontre que 60 % des Américains ont effectué à leur insu, des achats à de grandes entreprises de vente en ligne ou des transactions bancaires à cause d'une cyberattaque via de courriels frauduleux d'hameçonnage (phishing).

Les chiffres démontrés par l'étude de Lookout

D'autres chiffres révèlent aussi que les personnes ne se sentent pas en sécurité : 77 % craignent de perdre leur numéro de sécurité sociale, 74 % leurs données bancaires, 71 % leur code et carte de crédit et 56 % leurs données personnelles.

Par ailleurs, la plus grande peur des gens concerne le fait qu'ils ne soient pas immédiatement au courant du vol de leur identité au moment des actes de fraudes commises par les criminels. Selon l'enquête faite par Lookout, une personne victime d'un vol d'identité ne le découvrira que par une lettre postale (33 %), une information télévisée ou radio (31 %) ou un mail inattendu (31 %). Cela résulte du fait que les factures sur les crimes commis lui sont toujours renvoyées plus tard par mail ou par la poste.

Toujours d'après l'étude, 65 % des personnes ayant subi un vol ou une usurpation de leur identité via un site sur lequel elles se sont inscrites n'en seront averties qu'un mois après la cyberattaque. De même, 75 % des usurpés ne connaissent pas les actions à entreprendre dans de telles situations.

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 vol d’identité en nette progression : les données personnelles ne sont plus sécurisées

---

Des pirates informatiques demandes une rançon pour débloquer les serrures électroniques d’un hôtel de luxe

Des pirates informatiques demandes une rançon pour débloquer les serrures électroniques d’un hôtel de luxe

---

Des pirates informatiques ont utilisé un ransomware pour désactiver le système électronique d'un hôtel autrichien et demander une rançon de 1 500 euros. Il s'agit de la troisième attaque informatique qui cible l'établissement.

Des pirates informatiques ont transformé les vacances de plusieurs clients d'un hôtel autrichien en un véritable cauchemar. En effet, ils ont utilisé un ransomware qui a ciblé le système de sécurité et a désactivé les clés électroniques de l'établissement, en coinçant les touristes à l'extérieur de leurs chambres. La caisse, les ordinateurs et le système de réservation ont été également bloqués par l'attaque. L'affaire s'est déroulée au début de la dernière saison hivernale dans le Romantik Seehotel Jaegerwirt, situé près d'un lac idyllique au milieu des Alpes autrichiennes.

À vrai dire, les responsables de l'établissement affirment qu'il s'agit de la troisième attaque informatique menée par ces pirates informatiques, qui demandent chaque fois des rançons de plusieurs milliers d'euros. Cette fois, les propriétaires ont dû payer 1 500 euros en bitcoin pour pouvoir rétablir le système et réactiver les clés magnétiques.

L'ÉTABLISSEMENT AVAIT 180 CLIENTS, IL N'Y AVAIT PAS D'AUTRE CHOIX

Le directeur général de l'hôtel, Christoph Brandstaetter, explique : « L'établissement avait 180 clients, nous n'avions pas d'autre choix. Ni la police, ni l'assurance vous aide dans ce cas-là. » Payer la rançon était la solution la plus rapide et la plus efficace d'après le directeur.

Cependant, Brandstaetter ajoute avec frustration manifeste : « La réactivation de notre système, après la première attaque de cet été, nous a coûté plusieurs milliers d'euros. Nous n'avons reçu aucun remboursement de la part de l'assurance, parce que les coupables n'ont pas été trouvés. » Ainsi, l'hôtel devient malheureusement une double victime des nouvelles technologies et d'un système bureaucratique sans pitié.

Mais Brandstaetter avoue que son hôtel n'est pas un cas isolé : « Nous savons que d'autres collègues ont subi ces attaques, qui se sont déroulées de la même façon. »

Finalement, pour contraster efficacement les prochains attaques informatiques, l'équipe de l'hôtel a décidé de s'appuyer sur un système efficace. Après avoir remplacé les ordinateurs, l'établissement utilisera à nouveau des clés traditionnelles et des serrures. Et Brandstaetter de conclure : « Nous sommes en train de planifier la rénovation des chambres pour installer des serrures avec de véritables clés. Comme c'était au temps de nos arrière-grand-pères il y a 111 ans »…

***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

ESET intègre un bouclier anti-ransomware et rejoint « No More Ransom »

ESET intègre un bouclier anti-ransomware et rejoint « No More Ransom »

En prenant part au projet « No More Ransom », ESET fournit un outil qui permet d'analyser les impacts d'une attaque par des ransomwares. Les utilisateurs n'en mesurent la gravité qu'une fois qu'ils ont été infectés. Grâce à cet outil, ESET espère les sensibiliser en amont, afin de limiter les infections de ce type.

De plus, ESET renforce la sécurité de ses utilisateurs en ajoutant une couche de sécurité supplémentaire capable de bloquer les ransomwares. La fonctionnalité est disponible gratuitement et sans intervention de l'utilisateur dès maintenant pour les solutions de sécurité Windows destinées aux particuliers.

Le bouclier anti-ransomware d'ESET contrôle et évalue toutes les applications exécutées en utilisant l'heuristique comportementale. Il bloque activement tous les comportements qui s'apparentent à une attaque par ransomware et peut également forcer l'arrêt des modifications apportées aux fichiers existants (c'est-à-dire leur chiffrement).

Activé par défaut, le bouclier anti-ransomware ne demande l'intervention de l'utilisateur qu'une fois la menace détectée en lui demandant d'approuver ou non son blocage.

Pour plus d'informations à propos de notre bouclier anti-ransomware et de l'implication d'ESET au sein de l'organisation « No More Ransom », n'hésitez pas à nous contacter.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister 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

GRIZZLY STEPPE – Russian Malicious Cyber Activity

GRIZZLY STEPPE – Russian Malicious Cyber Activity

On October 7, 2016, the Department Of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI) issued a joint statement on election security compromises.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister 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 sur cette page.

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

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

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

Contactez-nous

Réagissez à cet article