Comment bien se protéger contre les Cyberattaques ?

Comment bien se protéger contre les Cyberattaques ?

On l'a encore vu récemment, aucun système informatique n'est à l'abri d'une faille…

Et en matière de cybercriminalité, les exemples nous montrent que l'attaque semble toujours avoir un coup d'avance sur la défense. L'enjeu, pour les institutions et les entreprises, est d'anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d'informations, cyber-espionnage économique ou industriel…, en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n'est malheureusement pas à l'amélioration et l'actualité récente regorge d'exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l'on connait, l'attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale…, les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes :

1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;
2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu'humaines ;
3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
4. Assurer une surveillance des mesures de sécurité et s'assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.

• Vous souhaitez faire un point sur l'exposition de votre entreprise aux risques cyber ?
• Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu'il ne soit trop tard ?
• Vous rechercher une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Cyberattaque, comment faire pour limiter les risques*

?

Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?

Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?

Les rançongiciels (ransomware en anglais) sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des internautes et réclament le paiement d'une rançon pour en obtenir à nouveau l'accès.
Depuis 2013, une variante est apparue avec des virus chiffrants ou crypto-virus (cryptolocker, cryptoDefense, cryptorBit et plus récemment locky, petya ou WannaCry). Cette forme de rançongiciels chiffre les documents se trouvant sur l'ordinateur cible, voire sur des serveurs qui hébergent les données. Les cybercriminels communiquent parfois la clé de déchiffrement une fois le paiement de la rançon effectué, mais ce n'est jamais une garantie.
Cliquez ci-dessous pour en savoir plus:


CYBERMALVEILLANCE.GOUV.FR
VOUS ÊTES VICTIME D'UN RANÇONGICIEL ?

Victime d'un rançongiciels / ransomwares / cryptovirus ou d'une demandes de rançon informatiques ? Contactez-nous

---

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Les rançongiciels ou ransomware – ANSSI – Plateforme Cyber Malveillance*

Un outil gratuit pour analyser et nettoyer votre ordinateur

Un outil gratuit pour analyser et nettoyer votre ordinateur

Avec plus de 40.000 visiteurs uniques par an, ESET Online Scanner apparaît comme l'un des outils gratuits les plus plébiscités par les internautes soucieux de leur sécurité. Fort de ce constat, ESET améliore son scanner basé sur le moteur d'analyse ThreatSense® permettant d'analyser et nettoyer son ordinateur sans contrainte d'installation logicielle.

Conçue pour être conviviale, cette dernière version devient complètement indépendante des navigateurs Internet. De plus, l'installation est désormais possible sans les droits d'administrateur, ce qui rend l'analyse et le nettoyage des ordinateurs contenant des logiciels malveillants encore plus simples.
ESET Online Scanner améliore l'élimination des logiciels malveillants, par l'ajout de ces nouvelles fonctions :
• **Analyse des emplacements de démarrage automatique** et du secteur d'amorçage pour les menaces cachées – choix de cette option dans setup / cibles d'analyse avancées
• **Nettoyage du registre système** – Supprime les traces des logiciels malveillants du registre système
• **Nettoyage après analyse lors du redémarrage** – Si nécessaire, ESET Online Scanner est capable de repérer les malwares les plus persistants afin de les nettoyer après redémarrage
Pour plus d'informations sur l'outil gratuit ESET Online Scanner, contactez-nous ou rendez-vous sur http://www.eset.com/fr/home/products/online-scanner/

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

---

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

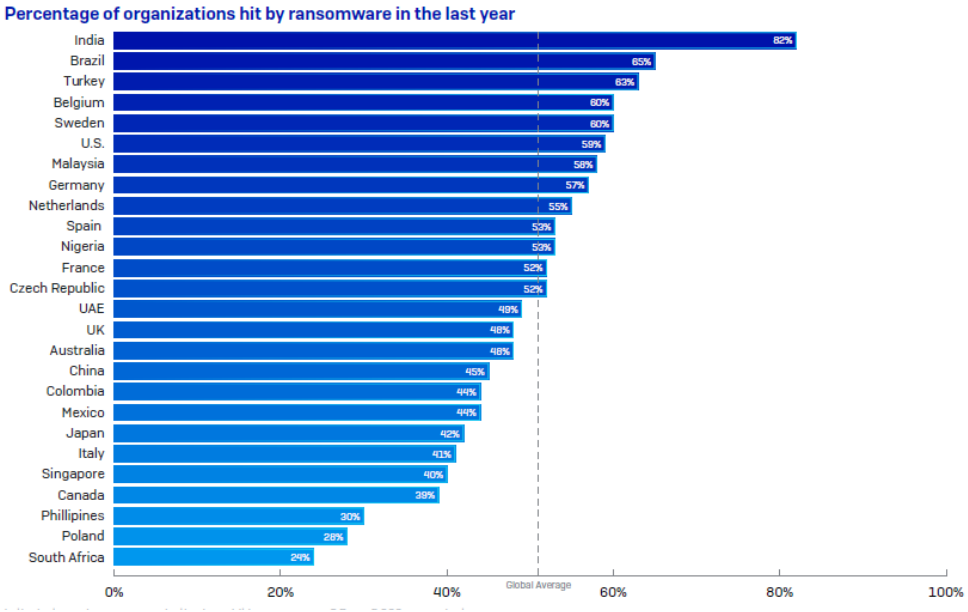
Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

Original de l’article mis en page : Conseils aux usagers | Gouvernement.fr

---

52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois

En France, 52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois. Elles étaient 48 % en 2019. Le coût moyen d'une attaque par rançongiciel est de 420 000 euros en dehors de la rançon exigée. Ce montant prend en compte les temps d'arrêt, la perte de chiffre d'affaires et les coûts opérationnels. En cas de paiement de la rançon, cette somme double.



LA CLÉ DE CHIFFREMENT N'EST PAS UNE SOLUTION MIRACLE

« *Les entreprises se sentent parfois sous pression pour payer la rançon afin d'éviter les temps d'arrêt préjudiciables. À première vue, effectuer le paiement de la rançon semble être une manière efficace de restaurer les données, mais ce n'est qu'illusoire (…) En effet, une simple clé de chiffrement n'est pas un remède miracle et il faut souvent bien plus pour restaurer les données*« , a expliqué Chester Wisniewski, Principal Research Scientist chez Sophos.

En France, plus de la moitié (61%) des responsables IT interrogés déclarent avoir pu restaurer leurs données à partir de sauvegardes sans payer la rançon. Dans 2 % de cas, le paiement de la rançon n'a pas permis de restaurer les données. À l'échelle mondiale, ce chiffre s'élève à 5 % pour les organisations du secteur public.

…[lire la suite]

Commentaire de notre Expert : Denis JACOPINI

La demande de rançon est la résultante dans la quasi totalité des cas de l'ouverture d'une pièce jointe à e-mail piégé ou le clic sur un lien aboutissant sur un site Internet piégé.

Les conséquences

Il n'est plus a rappeler qu'être victime d'un ransomware entraînent un arrêt de l'outil informatique, une perte de productivité et une dégradation de la réputation auprès des clients et partenaires.

Les solutions

Nous le répéterons jamais assez, les seuls moyens d'empêcher ce type de situation sont l'utilisations d'outils de filtrage et la sensibilisation. N'hésitez pas à nous contacter pour l'organisation de sessions de sensibilisation auprès de vos équipes pour leur apprendre à détecter e-mails et sites Internet malvéillants, en quasi totalité à l'origine des rançongiciels dans les systèmes informatiques.

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Etude : Payer la rançon multiplie par deux le coût total d'un ransomware*

Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus

Des pirates informatiques profitent du coronavirus pour vous piéger et vous infecter avec un virus

Les courriels – qui circulent principalement en Asie pour le moment – prétendent contenir de l'information légitime au sujet du coronavirus.
Le destinataire est invité à cliquer sur une pièce jointe pour obtenir plus d'information. Ceux qui tombent dans le piège permettent involontairement aux pirates d'avoir accès à leurs documents personnels.
IBM dit qu'on s'attend à «voir circuler davantage de courriels malveillants inspirés par le coronavirus dans le futur, alors que l'infection se propagera. Cela se produira probablement aussi dans d'autres langues».
Les pirates informatiques exploitent régulièrement l'actualité et les craintes de la population pour sévir. «Une telle stratégie permet de berner plus de victimes pour qu'elles cliquent des liens malveillants ou ouvrent des fichiers malveillants, accroissant ultimement l'efficacité de la campagne malveillante», peut-on lire dans le rapport…[lire la suite]

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes

pratiques ?
Victime d’usurpation d’identité sur facebook, tweeter ? Portez plainte mais d’après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Des pirates informatiques profitent du coronavirus pour répandre un logiciel malveillant | HuffPost Québec*

Envoyé spécial sur les Cyberattaques : les braqueurs de l’ombre – 14 décembre 2017 (France 2)

Envoyé spécial sur les Cyberattaques : les braqueurs de l’ombre – 14 décembre 2017 (France 2)

Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.

Merci à Clément Le Goff et Guillaume Beaufils pour ce beau travail d'enquête. Tout est vrai, et encore, tout n'est pas dit. Quelles conséquences avec les objets connectés, bientôt principaux cadeaux de noël, les voitures connectées, et tous les outils informatiques ou algorithmiques dont leurs usages peuvent être détournés à des fins malveillantes.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik…) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter le plus possible ces attaques en leur apprenant à se protéger des pirates informatiques.
Avec un tel reportage, j'espère que le plus grand nombre de personnes sera sensibilisé de manière à enrayer ce phénomène incoercible.

Seul petit bémol dans ce reportage. Beaucoup auront entendu et retenu les recommandations de la police qui sont qu'il ne faut pas payer la rançon lorsqu'un pirate prend vos données en otage. Je compléterais par le fait qu'il ne faut pas payer si vous avez la possibilité d'utiliser des sauvegardes ou si les conséquences sont minimes. Par contre, si la vie d'une entreprise est en jeu et la seule chance restante (même infime) pour sauver l'entreprise est de payer la rançon, ne pas la payer risquerait bien de vous être reproché… à moins que ça soit, comme dans le reportage un coup de grâce accepté par désespoir.
Corriger le message afin de ne pas induire les entreprises en erreur me paraît indispensable.

Réagissez à cet article

Les hold-up 2.0 par des « rançongiciels », logiciels de rançon, se multiplient : en France, une entreprise sur deux aurait déjà été piratée de cette façon. Enquête du magazine « Envoyé spécial » sur un fléau invisible en pleine explosion.

Depuis plusieurs années, Denis JACOPINI essaie par le biais de conférences ou en participant à des émissions de radio ou de TV (D8, LCI, NRJ12, Sud Radio, Sputnik) de sensibiliser la population à ces risques afin de les aider à anticiper et éviter ces attaques.
Merci à *Clément Le Goff et Guillaume Beaufils*
Avec un tel reportage, j'espère que

LE NET EXPERT
• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)
- ANALYSE DE VOTRE ACTIVITÉ
- CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
- IDENTIFICATION DES RISQUES
- ANALYSE DE RISQUE (PIA / DPIA)
- MISE EN CONFORMITÉ RGPD de vos traitements
- SUIVI de l'évolution de vos traitements
• FORMATIONS / SENSIBILISATION :
- CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
- AU **RGPD**
- À LA **FONCTION DE DPO**
• RECHERCHE DE PREUVES (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• EXPERTISES & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- SÉCURITÉ INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous
Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Réagissez à cet article

Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes

Android est à nouveau visé par un malware vendredi 13 octobre : DoubleLocker, un redoutable ransomware, chiffre les fichiers sur le smartphone et change son mot de passe, même s'il n'est pas rooté. Des chercheurs de ESET à l'origine de la découverte expliquent que ce ransomware se cache dans un APK d'Adobe Flash Player ce qui peut augmenter le risque d'une propagation rapide. La seule façon de s'en débarrasser c'est de réinitialiser le smartphone. Ce serait le pire ransomware détecté à ce jour.

Les chercheurs de ESET viennent de découvrir le premier **ransomware Android** capable de prendre le contrôle total de votre smartphone. Il parvient à obtenir des droits administrateur même sur des smartphone non-rootés, ce qui le rend extrêmement dangereux. Android/DoubleLocker.A est basé sur un trojan bancaire modifié pour changer le code PIN du smartphone sur lequel il est installé et chiffrer ses données. Les chercheurs précisent qu'un tel mode d'action était jusqu'ici du jamais vu.

Android : le pire ransomware jamais détecté, DoubleLocker, bloque et chiffre les smartphones

Le chercheur Lukáš Štefanko à l'origine de la découverte de DoubleLocker ajoute : « *à cause du fait qu'il trouve son origine dans un malware bancaire, DoubleLocker pourrait très bien être modifié pour devenir ce que l'on pourrait appeler un malware bancaire-rançon. Un malware à deux étages, qui essaie d'abord de voler vos données bancaires et/ou vider votre compte ou compte PayPal, puis bloque votre appareil et ses données pour exiger une rançon… spéculation de côté, on a détecté la version test d'un tel malware dans la nature pratiquement en même temps, en mai 2017*« .

On trouve DoubleLocker dans des APK de Flash Player sur de sites compromis méthode déjà utilisée par d'autres malwares. Une fois lancée, l'application lance un service d'accessibilité baptisé Google Play Service. Le malware obtient ensuite tout seul les permissions d'accessibilité, puis les utilise pour activer les droits administrateurs et se définir comme *Launcher* par défaut. Dès que l'utilisateur appuie sur le bouton Home, le malware est activé. Le PIN est alors changé et les fichiers du répertoire principal chiffrés. Le ransomware demande alors de payer 0.013 BTC dans les 24 heures, soit environ 62 euros au moment où nous écrivons ces lignes. Les chercheurs relèvent que les fichiers chiffrés, qui prennent l'extension .cryeye, ne sont pas supprimés à l'issue de ce délai…[lire la suite]

Réagissez à cet article

Source : *Android : le pire ransomware jamais détecté fait ses premières victimes*

Alerte ! LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android

Alerte ! LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android

---

Android doit faire face à un nouveau ransomware qui menace de dévoiler des informations compromettantes sur l'utilisateur du smartphone.

Android est le système d'exploitation le plus utilisé. Il est donc la cible de nombreux logiciels malveillants, c'est le cas de LeakerLocker. **Ce dernier est un ransomware, autrement dit un logiciel de rançon qui récupère des informations personnelles, menaçant de dévoiler leurs contenus si une certaine somme d'argent ne lui est pas versée.** LeakerLocker, quant à lui est un logiciel de rançon qui promet de vous humilier. **Pour cela, il utilise les données de votre historique de recherches et menace de l'envoyer à vos contacts**. Le montant de la rançon s'élève à 50 euros. Un logiciel de rançon d'un nouveau genre fait son apparition sur Android.

Un logiciel de rançon apparu en premier lieu sur Android

McAfee, le logiciel antivirus stipule que ce logiciel malveillant est né sur le système d'exploitation Android. **Il se propage avec l'installation de deux applications disponible sur Google Play : Booster & CCleaner Pro ainsi que Wallpapers Blur HD**. Il réussit à dérober des informations qui pourraient vous nuire, au sein de votre smartphone afin de les utiliser contre vous…[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

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

Source : *LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android*

Les points faibles du Ransomware Petya/NotPetya

Les points faibles du Ransomware Petya/NotPetya

Alors que le mystère s'épaissit sur les intentions réelles des auteurs du malware parti d'Ukraine fin juin, des chercheurs d'une société de sécurité informatique britannique sont parvenus à décrypter des fichiers endommagés sur une machine infectée.
Jusqu'à présent, toutes les actions entreprises pour récupérer les données attaquées par NotPetya sont vouées à l'échec.

Erreur de programmation de l'algorithme de cryptage

Un maigre espoir pour les victimes du malware Petya/NotPetya : sur leur blog les chercheurs en cybersécurité de la société britannique Positive Technologies expliquent avoir réussi à décrypter des fichiers endommagés sur un ordinateur infecté. Très ardue, la procédure de récupération ne serait possible que sur certaines machines, celles dont le virus a encrypté les droits d'administrateur. Une découverte fort intéressante, alors que jusqu'à présent, personne, y compris les victimes ayant payé la rançon exigée par les attaquants, n'a pu récupérer ses données…
Positive Technologies a découvert plusieurs erreurs commises par les pirates dans la conception du malware, en particulier dans la programmation de l'algorithme de cryptage Salsa20. Au lieu d'utiliser une clé de chiffrement de 256 bits, ils se sont apparemment contentés d'une clé moins puissante de 128 bits, que Positive Technologies est parvenu à contourner pour récupérer certains fichiers….[lire la suite]

Réagissez à cet article

Source : *Petya/NotPetya : des chercheurs ont découvert des points faibles*