Des noms de domaines détournés pour mieux vous infecter

Des noms de domaines détournés pour mieux vous infecter

Efficacité et transparence chez le registar Gandi. L'entreprise, via un partenaire, a du faire face au détournement de 751 noms de domaines. Mission de ce hijacking, diffuser des codes malveillants par l'intermédiaire des noms de domaine ainsi pris en main par le pirate.

Vendredi 7 juillet, un incident de type hijacking est survenu chez un partenaire technique du fournisseur de noms de domaine Gandi. Un partenaire qui gère 31 extensions. Suite à une connexion non autorisée chez ce partenaire, l'attaquant a utilisé des identifiants Gandi pour se connecter à cette interface. Le pirate informatique a pu détourner 751 noms de domaines et renvoyé les visiteurs sur un espace numérique, basé au Gabon, ayant pour mission de lancer des tentatives d'infiltration dans les ordinateurs des visiteurs. Le but étant de lancer des exploits via des navigateurs web (IE, Chrome, Firefox, …) non mis à jour. Le pirate a utilisé Rig Exploit Kit et Neutrino Bot lors de son opération….[lire la suite]

Commentaire de Denis JACOPINI :
Mélange probablement de phishing (pour obtenir les identifiants du prestataire), d'attaque en point d'eau (qui consiste à prendre le contrôle et de piéger un espace de confiance à fort trafic) et d'attaque par exploitation de faille (le code malveillant permettra d'infiltrer les navigateurs qui n'ont pas été mis à jour). Malheureusement un grand classique très répandu dans les structures où le personnel n'est pas sensibilisé.
Suivez nos formation https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles/

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec le RGPD (réglement Européen relatif 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 : *ZATAZ Hijacking : 751 noms de domaines détournés chez Gandi – ZATAZ*

Les avions, vraiment insensibles aux cyber-attaques ?

Les avions, vraiment insensibles aux cyber-attaques ?

Après le piratage des voitures connectées et la profusion des attaques cybernétiques à travers le monde, une question se pose : les appareils volants peuvent-ils être eux aussi victimes de ce genre d'incident ? Car force est de constater que les avions de nouvelle génération embarquent bon nombre de systèmes connectés. Sachez cependant que « c'est impossible » selon les experts. Si des tentatives de hacking sont bel et bien enregistrées, la conception de l'appareil permet d'y faire face.

Ces campagnes de hackings n'aboutissent jamais affirment les experts

Une cyber-attaque contre un avion et sa multitude de systèmes connectés est un formidable défi pour les hackers. Toutefois, aucune n'a eu d'effet, le risque étant pris en compte dès la conception des appareils, selon les experts.

En témoigne la déclaration de Pascal Andréï, qui affirme que les tentatives, même, si elles sont nombreuses, n'ont pas abouti jusqu'à maintenant. De plus, ce directeur de la sécurité aérienne du groupe Airbus rajoute que la plupart des hackers veulent juste faire le buzz en faisant savoir qu'ils peuvent contrôler un avion à distance. M. Andréï a annoncé ces propos durant le « Paris Air Forum « qui rassemble chaque année plusieurs experts du domaine de l'aéronautique.

Une équipe d'élite spécialement choisie pour venir à bout des hackers

Pour faire face à ses nombreuses menaces, les constructeurs ont mis en place leurs propres armées de pirates informatiques. Thales, l'un des leaders européens de la cybersécurité et le leader mondial de la protection des données en déploient notamment plusieurs centaines pour contrôler la vulnérabilité de ses clients. Selon Marc Damon,directeur général délégué de Thales responsable des activités système d'information et de communication sécurisés, 4 plans de défense doivent être mis en place pour faire face aux attaques. Pour commencer,il y a « les règles fondamentales ». Celles-ci comprennent l'actualisation des serveurs, des logiciels, le changement permanent des mots de passe, la surveillance des téléchargements…Vient ensuite « l'intégration des systèmes de cyber-sécurité dès la conception », puis la « supervision des systèmes » et pour finir le « chiffrement des données »…[lire la suite]

Réagissez à cet article

Source : *Les avions, insensibles aux cyber-attaques –*

@Sekurigi

LeakerLocker : du rançonnage nouvelle génération sur Google Play

LeakerLocker, des applications pour Android qui cachent un système de ransomware nouvelle génération. Il menace de diffuser les données volées dans le smartphone infiltré. LeakerLocker, un logiciel malveillant de type ransomware nouvelle génération a été découvert par Mcafee.…[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

Le logiciel malveillant CopyCat infecte 14 millions d’appareils Android

C’est ce que révèle un rapport du bureau d’enquête Check Point. Le logiciel malveillant pour Android a déjà attaqué 14 millions de smartphones et tablettes.…[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.

Les opérateurs nucléaires américains ciblés par une cyberattaque

Les opérateurs nucléaires américains ciblés par une cyberattaque

Un groupe de hackers inconnu a attaqué plusieurs entreprises chargées de l'exploitation de centrales nucléaires américaines ces deux derniers mois. S'ils ont pu entrer sur certains réseaux bureautiques, ils n'ont toutefois pas pu accéder aux systèmes de contrôle des infrastructures.

Le nucléaire américain attise les convoitises de hackers. D'après le New York Time qui cite un rapport co-signé par le département de la sécurité national et le FBI, les réseaux informatiques d'entreprises chargées de l'exploitation des centrales nucléaires ont été la cible de hackers non identifiés ces deux derniers mois. La Wolf Creek Nuclear Operating Corporation, qui gère une infrastructure dans le Kansas, a été particulièrement visée. Des fournisseurs énergétiques et des fabricants de centrales ont également été ciblés sans être nommés.
D'après nos confrères de The Verge, la violence et l'objectif des attaques ne sont pas claires. Les hackers auraient pu aussi bien voler des secrets industriels que perturber la production d'électricité. Le rapport est également discret quand à ce qu'ont réussi à faire, ou non, les hackers, notamment sur le site de Wolf Creek. S'ils sont apparemment parvenus à accéder aux postes de travail de certains employés, rien ne dit qu'ils ont pu ensuite s'infiltrer sur les infrastructures de contrôle de la centrale…[lire la suite]

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec le RGPD (réglement Européen relatif 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 opérateurs nucléaires américains ciblés par une cyberattaque – Le Monde Informatique*

Cryptovirus Petya : La police ukrainienne saisit les PC de l’éditeur M.E.Doc

Cryptovirus Petya : La police ukrainienne saisit les PC de l’éditeur M.E.Doc

Les malwares Petya ont utilisé le mécanisme de mise à jour du logiciel de comptabilité et de fiscalité M.E.Doc, très répandu en Ukraine, pour se propager et bloquer les ordinateurs du pays et du monde entier.

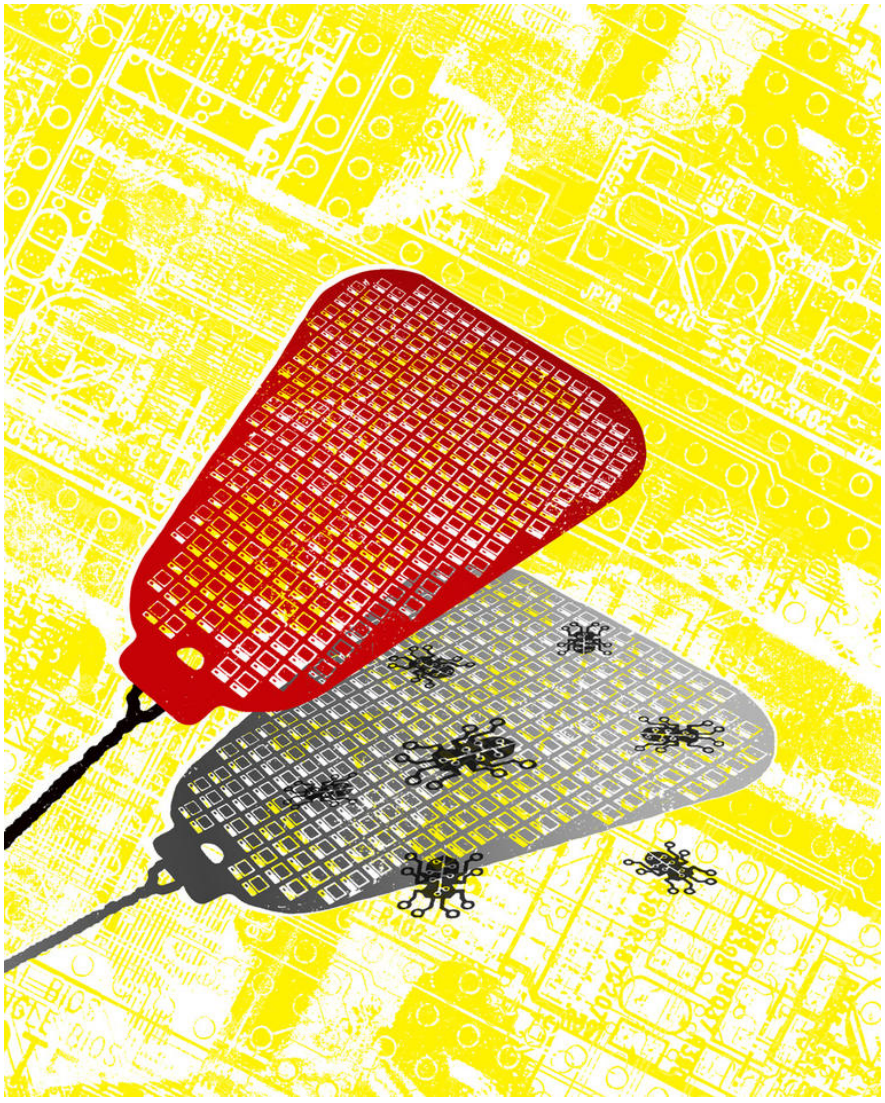
La cyberpolice ukrainienne est intervenue pour prévenir de nouvelles attaques à l'image de celle perpétrée en fin juin 2017. L'attaque NotPetya – également appelée Diskcoder.c, ExPetr, PetrWrap et Petya – avait été d'abord considérée par les chercheurs comme une attaque de ransomware. Si NotPetya a ciblé des entreprises partout dans le monde, l'Ukraine a été particulièrement touchée parce que, comme l'ont constaté les chercheurs en sécurité, pour diffuser le malware, les premières attaques ont détourné le système de mise à jour automatique du logiciel de comptabilité et de fiscalité M.E.Doc très utilisé dans le pays.

Selon la police qui a analysé l'un des ordinateurs du développeur du logiciel, une porte dérobée a probablement été introduite dans M.E.Doc dès le 15 mai. Mercredi, les autorités ont annoncé qu'elles avaient saisi des ordinateurs et des logiciels du développeur de M.E.Doc après avoir repéré de nouveaux signes d'activités malveillantes pour analyse. Les enquêteurs espèrent que la mise hors circuit de ces machines empêchera une nouvelle diffusion incontrôlée du malware NotPetya utilisé dans la précédente attaque…[lire la suite]

Réagissez à cet article

Source : *Petya : La police ukrainienne saisit les PC de l'éditeur M.E.Doc – Le Monde Informatique*

Cybersécurité. C’est à l’État de protéger les citoyens



Cybersécurité. C’est à l’État de protéger les citoyens

Demander aux particuliers de sécuriser leur ordinateur revient à leur demander d'installer un bouclier antimissiles dans leur jardin. Ce qu'il faudrait en revanche, c'est une "douane numérique", estime un spécialiste néerlandais en sécurité internationale.

Essayez de vous imaginer qu'un grand nombre de missiles russes ou nord-coréens soient pointés vers les Pays-Bas et que le gouvernement néerlandais reçoive une menace annonçant que ces missiles seront lancés dans trois jours, à moins que nous nous rendions sur-le-champ et que nous versions 100 milliards d'euros sur les comptes bancaires de Poutine et de Kim Jong-un. Et imaginez-vous que le gouvernement de Mark Rutte dise à l'ensemble des citoyens, des hôpitaux, des entreprises et des établissements scolaires néerlandais : vous allez devoir compter sur vos propres forces, débrouillez-vous pour installer un bouclier antimissiles dans votre jardin et ne leur versez pas un centime.

Pas une personne sensée ne serait prête à concevoir un tel scénario sans objecter aussitôt qu'une telle situation relève de la sécurité nationale, une mission fondamentale de l'État qui doit être centralisée. Quand un pays risque d'être mis en pièces par des crapules, que ce soit pour des raisons politiques ou simplement criminelles, il est difficilement justifiable de compter sur ses citoyens et ses institutions

Ko Colijn

Réagissez à cet article

Source : *Cybersécurité. C'est à l'État de protéger les citoyens | Courrier international*

ESET attribue la cyberattaque Petya au groupe TeleBots

	ESET attribue la cyberattaque Petya au groupe TeleBots

Selon les experts ESET®, la cyberattaque dite « Petya » pourrait être attribuée au groupe TeleBots. Il existe des similitudes entre les nombreuses campagnes menées contre l'Ukraine, l'amélioration des outils utilisés par le cyber-groupe entre décembre 2016 et mars 2017 et la menace Diskoder.C (Petya).

« La cyberattaque de 2016 menée contre les institutions financières ainsi que le développement d'une version Linux du malware KillDisk par TeleBots, ont attiré l'attention des chercheurs ESET. En parallèle, le nombre croissant d'attaques contre les systèmes informatiques que connaît l'Ukraine **nous ont fait pointer du doigt le groupe TeleBots,** » déclare Anton Cherepanov, Senior malware researcher chez ESET.

Le mode opératoire du groupe TeleBots est l'utilisation systématique du malware KillDisk qui réécrit les extensions de fichiers des victimes. L'obtention d'une rançon n'est donc pas leur objectif principal, car les fichiers cibles ne sont pas chiffrés, mais réécrit. Si l'évolution du malware contient de nouvelles fonctions, comme le chiffrement ou l'ajout de leurs coordonnées, l'objectif de KillDisk n'est toujours pas de récolter de l'argent.

Entre janvier et mars 2017, TeleBots a compromis une société d'édition de logiciels en Ukraine, utilisant alors des tunnels VPN pour accéder aux réseaux internes de plusieurs institutions financières. Au cours de cette campagne, l**es cybercriminels ont utilisé tout un arsenal d'outils en Python, SysInternals PsExec et des logins de session Windows volés pour déployer un nouveau ransomware.** Il fut détecté par ESET comme Win32/Filecoder.NKH et fut suivi par une version pour Linux, détecté comme Python/Filecoder.R.

TeleBots a ensuite lancé un nouveau malware le 18 mai 2017 : Win32/Filecoder.AESNI.C (également appelée XData). C**e ransomware s'est principalement diffusé en Ukraine via une mise à jour du logiciel financier M.E.Doc, largement utilisé en Ukraine.** Selon le LiveGrid® d'ESET, le malware se déploie juste après l'exécution du logiciel, **ce qui lui permet de se répandre automatiquement à l'intérieur d'un réseau compromis.** Bien qu'ESET ait mis à la disposition un outil de déchiffrement pour la plateforme Windows®, cette attaque ne fut pas très médiatisée.

Le 27 juin 2017, l'épidémie de ransomwares de type Petya (Diskoder.C) ayant compromis de nombreux systèmes notamment en Ukraine, a permis de montrer **la capacité du malware à remplacer le MBR par son propre code malveillant, code qui a été emprunté au ransomware Win32/Diskoder.Petya :** c'est pourquoi certains chercheurs ont nommé cette menace ExPetr, PetrWrap, Petya ou NotPetya.

Cependant, contrairement au ransomware original Petya, **les auteurs de Diskcoder.C ont modifié le code MBR de telle sorte que la récupération de fichiers ne soit pas possible, malgré l'affichage des instructions de paiement.** Une fois le malware exécuté, **il tente de se propager à l'aide de l'exploit Eternablue, en s'aidant de la backdoor DoublePulsar.** Il s'agit de la même méthode utilisée par le ransomware WannaCry.

Le malware est également capable de se diffuser de la même manière que le ransomware Win32/Filecoder.AESNI.C (XData), en utilisant Mimikatz, pour obtenir des mots de passe, puis en exécutant SysInternals PsExec. En outre, les attaquants ont mis en place une troisième méthode de diffusion à l'aide d'un mécanisme WMI.

Ces trois méthodes ont été utilisées pour diffuser les ransomwares, cependant et contrairement à WannaCry, l'exploit EternalBlue utilisé par le malware Diskoder.C cible uniquement des ordinateurs ayant un adressage interne.

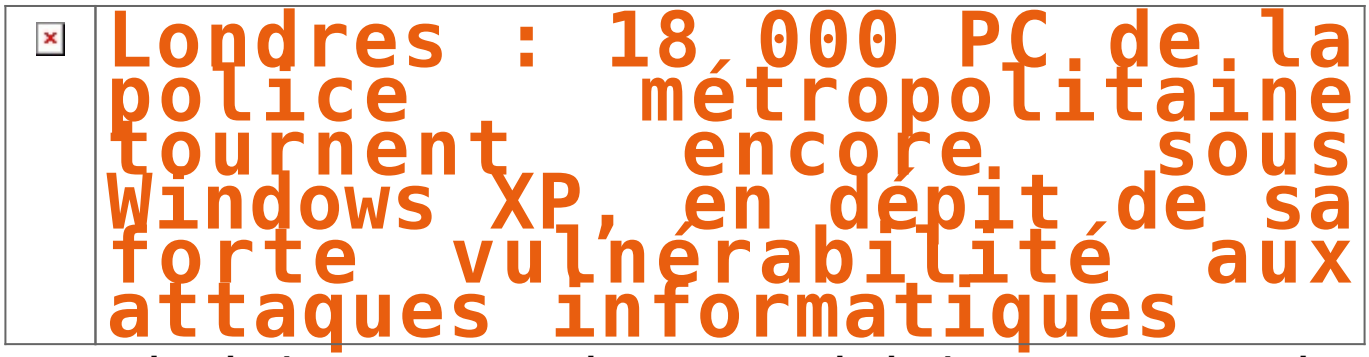
Lier TeleBots à cette activité permet de comprendre pourquoi les infections se sont étendues à d'autres pays que l'Ukraine. ESET a analysé les connexions VPN entre les employés, les clients et les partenaires mondiaux de l'éditeur ainsi que le système interne de messagerie et d'échange de documents. Tout cela a permis aux cybercriminels d'envoyer des messages aux victimes (spearphishing). Les pirates ayant eu accès au serveur légitime de mise à jour ont diffusé des mises à jour malveillantes automatiquement (aucune interaction avec l'utilisateur ne fut nécessaire).

« Avec une infiltration si poussée dans l'infrastructure de l'éditeur du logiciel M.E.Doc et de sa clientèle, les pirates disposaient des ressources nécessaires pour diffuser Diskoder.C. Bien qu'il y eut des dommages collatéraux, cette attaque a permis de démontrer la connaissance approfondie de leur cible par les pirates. D'autre part, **l'amélioration du kit d'exploit EternalBlue le rend encore plus sophistiqué, ce à quoi devront faire face les acteurs de la cybersécurité dans les prochaines années,** » conclut Anton Cherepanov.

Réagissez à cet article

Source : *ESET*

Londres : 18 000 PC de la police métropolitaine tournent encore sous Windows XP, en dépit de sa forte vulnérabilité aux attaques informatiques



La majorité des PC qui sont utilisés par la police métropolitaine de Londres tournent encore sous Windows XP, alors que ce système d'exploitation n'est plus pris en charge par Microsoft depuis 2014. Au total, on en dénombre environ 18 000, un chiffre aussi énorme qu'inquiétant.…[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

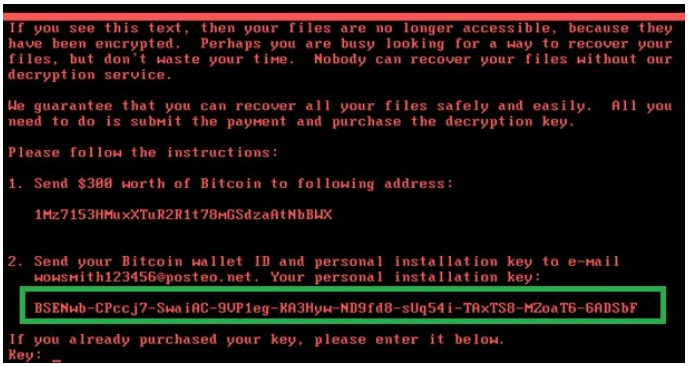
Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

Le déchiffrement des machines impactées est impossible. La demande de rançon n'était donc qu'un leurre pour camoufler un cybersabotage. La piste d'un acte politique, probablement réalisé par une agence gouvernementale, émerge.

Mauvaise nouvelle pour toutes les victimes de NotPetya. Les dernières analyses des chercheurs en sécurité montrent que ce malware est en réalité un logiciel de sabotage déguisé en ransomware. Les victimes ne pourront donc retrouver leurs données, à moins qu'un expert arrive à détecter une faille dans le processus de chiffrement.

Plusieurs indices prouvent que les auteurs de NotPetya n'ont jamais eu l'intention d'envoyer une quelconque clé de déchiffrement. Le premier concerne l'identifiant unique affiché dans le message de rançonnage et que la victime doit envoyer aux pirates après avoir effectué le paiement en bitcoins. En théorie, cet identifiant doit permettre aux auteurs de NotPetya d'identifier la victime. Il doit, par conséquent, contenir des informations sur les clés de chiffrement utilisées sur la machine en question. Mais selon les chercheurs de Kaspersky, il s'avère que cet identifiant est totalement aléatoire. *« Les attaquants ne peuvent extraire une quelconque information de déchiffrement d'une telle suite de caractères aléatoire »*, soulignent-t-ils dans une note de blog.



Kaspersky – L'identifiant unique affiché est totalement aléatoire

De son côté, le chercheur en sécurité Matt Suiche a découvert que les données de la zone d'amorçage ne sont sauvegardées nulle part, mais simplement remplacées par autre chose. Le système de fichier du disque serait donc de toute façon irrécupérable. *« La version actuelle de Petya a été réécrite pour être un wiper, et non un ransomware »*, souligne l'expert….[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 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 : *Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage*