Nouvelle alerte: la plus dangereuse arme d’internet a maintenant un rival

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Nouvelle alerte: la plus dangereuse arme d’internet a maintenant un rival				

Un nouveau logiciel malveillant, aussi dangereux que Mirai, connu pour avoir coupé l’accès à internet à plusieurs pays en 2016, est apparu sur le Net.

Un expert bulgare en cybersecurité, connu sur le Web sous le pseudonyme VessOnSecurity, a annoncé l’apparition d’un nouveau virus. Selon lui, celui-ci est même plus agressif que le virus Mirai, qui avait réussi en 2016 à bloquer l’accès à internet à plusieurs pays.

«Toujours aucune idée de ce que c’est, mais il se propage TRÈS agressivement. Le schéma d’attaque ressemble vaguement à Mirai mais ce n’est PAS Mirai. Le fichier exécutable est compressé et les commandes sont assez polymorphes», a écrit VessOnSecurity sur Twitter…[Lire la suite]

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique 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).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par*

des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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

Le ransomware GlobeImposter frappe la France

Le ransomware GlobeImposter frappe la France

Vade Secure alerte sur les premières vagues d'un nouveau ransomware GlobeImposter détectée en France.…[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.

Réagissez à cet article

Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed

Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed

Check Point Software Technologies Ltd révèle que 28 % des entreprises dans le monde ont été affectées par la campagne de publicités malveillantes RoughTed en juin, selon son tout dernier indice des menaces.

Check Point Software Technologies Ltd révèle que 28% des entreprises dans le monde ont été affectées de près ou de loin par la campagne de publicités malveillantes RoughTed en juin, selon son tout dernier indice des menaces.

RoughTed est une campagne de publicités malveillantes à grande échelle utilisée pour diffuser des sites web malveillants et des charges embarquées malveillantes telles que des escroqueries, des logiciels publicitaires, des kits d'exploitation de vulnérabilités et des logiciels rançonneurs. Elle a connu une forte poussée fin mai, puis a continué de se répandre en juin, touchant des entreprises dans 150 pays.

Large éventail

Les entreprises les plus touchées par RoughTed font partie des secteurs de la communication, de l'éducation, de la vente au détail et du commerce de gros… Les taux d'infection liés aux publicités malveillantes ont augmenté au cours des derniers mois, car il suffit aux pirates d'infecter une seule plate-forme de publicités en ligne pour atteindre un large éventail de victimes sans trop d'efforts, et il n'est pas nécessaire de se doter d'une infrastructure de diffusion lourde pour le logiciel…

En seconde place, Fireball, qui a touché 20% des entreprises en mai, a fortement reculé et n'a affecté que 5% des entreprises en juin. Le ver Slammer est la troisième variante la plus courante, touchant 4 % des entreprises…[lire la suite]

Réagissez à cet article

Source : *Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed*

LeakerLocker : du rançonnage nouvelle génération sur Google Play

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.

Réagissez à cet article

Le logiciel malveillant CopyCat infecte 14 millions d'appareils Android

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.

Réagissez à cet article

Beware! New Android Malware Infected 2 Million Google Play Store Users

Beware! New Android Malware Infected 2 Million Google Play Store Users

Initially thought to be 600,000 users, the number of Android users who have mistakenly downloaded and installed malware on their devices straight from Google Play Store has reached 2 Million.…[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.

Réagissez à cet article

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]

Réagissez à cet article

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

---

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

---

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

---

Nasty Android Malware that Infected Millions Returns to Google Play Store

HummingBad – an Android-based malware that infected over 10 million Android devices around the world last year and made its gang an estimated US$300,000 per month at its peak – has made a comeback.…[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.

Réagissez à cet article

Fake Apps Take Advantage of Mario Run Release

Fake Apps Take Advantage of Mario Run Release

Earlier this year, we talked about how cybercriminals took advantage of the popularity of Pokemon Go to launch their own malicious apps. As 2016 comes to a close, we observe the same thing happening to another of Nintendo's game properties: Super Mario.…[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.

Réagissez à cet article