Alerte : CCleaner compromis par une backdoor

Alerte : L'utilitaire CCleaner compromis par une backdoor

Piriform avertit que son logiciel CCleaner a été compromis. Avec des risques de fuites de données persos de 130 millions d'utilisateurs.

Piriform, l'éditeur de l'utilitaire CCleaner de nettoyage et d'optimisation de Windows, vient de reconnaître qu'il a fait l'objet d'une attaque.

Les versions 5.33.6162 sur poste fixe et 1.07.3191 en mode Cloud de sa solution ont été compromises.

« Une activité suspecte a été identifiée le 12 septembre 2017, où nous avons vu une adresse IP inconnue recevant des données du logiciel trouvé dans CCleaner et CCleaner Cloud sur les systèmes Windows 32 bits », alerte Paul Yung, Vice-Président Produit de Piriform.

Selon l'éditeur, le logiciel a été illégalement modifié avant sa livraison publique. Le pirate a réussi à installer une backdoor à deux niveaux afin d'exécuter du code envoyé à partir d'une adresse IP sur les systèmes affectés…[lire la suite]

Réagissez à cet article

Source : *L'utilitaire CCleaner compromis par une backdoor*

Alerte : Facebook Messenger

pourrait propager un virus

	Alerte : Facebook Messenger pourrait propager un virus

Les applications de messageries instantanées sont souvent la cible de virus informatiques. Facebook Messenger n'a pas échappé à cette règle: selon Le Monde Informatique, un logiciel malveillant (« malware », ndlr) se propage actuellement sur le réseau social.

C'est le chercheur David Jacoby, de la société informatique spécialisée dans la sécurité des systèmes d'information, qui a pu détecter ce virus. Le principe est classique: un de vos contacts envoie une vidéo nommée « David Video ». David Jacoby précise au *Monde Informatique*: « Lorsque la victime clique sur la fausse vidéo, le malware redirige vers un éventail de sites énumérant leur navigateur, système d'exploitation et d'autres informations vitales. Selon leur OS, ils sont redirigés vers d'autres sites web ».

Ce virus, qui ne menace pas l'appareil en lui-même, peut installer des logiciels malveillants à l'insu de l'utilisateur. En outre, il peut également récupérer les données personnelles…[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

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

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons 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 : *Un virus informatique détecté sur Facebook Messenger*

Plus de 100 000 smartphones Android infectés par un botnet DDoS

	**Plus de 100 000 smartphones Android infectés par un botnet DDoS**

Les victimes étaient infectées par des centaines d'applications en apparence inoffensives, diffusées par le Google Play Store.

On ne cesse de le répéter : attention aux applications que vous téléchargez, y compris sur le Google Play Store. Des chercheurs en sécurité viennent de démanteler WireX, un botnet spécialisé en attaques par déni de service distribuées (DDoS) et qui regroupait jusqu'à 120.000 smartphones zombies répartis dans plus de 100 pays. Ce n'est pas la première fois qu'un tel botnet est détecté. En septembre 2016, les chercheurs d'Imperva avait déjà mis le doigt sur un réseau de smartphones Android zombies destiné au DDoS et composé de plus de 26.000 nœuds…[lire la suite]

Réagissez à cet article

Source : *Plus de 100 000 smartphones Android esclaves d'un botnet DDoS*

Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant

Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant

En règle générale mieux vaut éviter les spoilers. Surtout, quand ceux-ci proviennent d'un email suspect. D'après un article Proofpoint, une entreprise américaine de cybersécurité, une «campagne d'emails ciblées» qui utilise des spoilers des prochains épisode de «Game of Thrones» comme appât est actuellement en cours. À la clef, pour les internautes malchanceux qui cliqueraient sur la pièce jointe, un logiciel malveillant.

L'entreprise de cyber-sécurité explique avoir repéré un de ces emails le 10 août dernier, à la suite du piratage de HBO par des hackers. Intitulé *«Vous voulez voir «Game of Thrones» en avance ?»*, le courrier contient quelques détails concernant les prochains épisodes de la série ainsi qu'une pièce jointe word contenant un maliciel. Une fois téléchargé, celui-ci tente d'installer un Remote Access Trojan (cheval de Troie à distance) qui est ensuite capable d'envoyer des informations et des données à un serveur.
D'après The Verge, ce genre d'attaque a été associée par le passé avec le gouvernement chinois et il serait possible *«que cette attaque provienne des mêmes acteurs»*. Cet email fait suite au hack massif de HBO. La chaîne américaine, qui diffuse «Game of Thrones», s'était fait voler 1,5 To de données en juillet dernier, dont des informations sur la saison de la série. Une demande de rançon avait rapidement suivi ce hack…[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;
PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;
SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;
AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;
MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons 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 : *Des hackers utilisent des spoilers de «Game of Thrones» pour propager un logiciel malveillant | Slate.fr*

Alerte : Un vidéo infecte votre ordinateur via Facebook Messenger

Sur Facebook Messenger, des messages incitant à regarder une vidéo sont envoyés. Ne cliquez surtout pas sur le lien : il s'agit d'un piège qui installera un malware sur votre ordinateur.

Des vidéos piégées sur Facebook Messenger

D'après la société spécialisée dans la sécurité informatique Kaspersky Lab, des messages piégés incitant à regarder une vidéo circulent sur Facebook Messenger. Il s'agirait d'une tactique dont le but serait d'infecter votre ordinateur avec un *malware*.

« *Le mécanisme initial de propagation semble être Facebook Messenger, mais nous ne savons toujours pas comment il se propage via Messenger. Il se pourrait que ce soit à partir d'identifiants volés, de navigateurs piratés ou en détournant des clics* », a indiqué Kaspersky Lab dans une note de blog.

© Fournis par Clubic Facebook Messenger

Un malware qui cible Windows et macOS

Les pirates informatiques à l'origine de cette attaque ciblent tout autant les ordinateurs tournant sous Windows que ceux tournant sous macOS…[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

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

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons 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 : *Facebook Messenger : attention à ce nouveau malware*

Un nouveau ransomware, Defray, cible l’éducation et la santé

Un nouveau ransomware, Defray, cible l’éducation et la santé

Les chercheurs Proofpoint ont récemment analysé un nouveau ransomware, nommé Defray. Durant le mois d'août, ils ont observé plusieurs attaques ciblées, visant notamment les secteurs de la santé, de l'éducation, de l'industrie et de l'informatique.

« Defray » a été choisi en rapport avec le nom d'hôte du serveur de commande et de contrôle (C&C) de la première attaque observée : defrayable-listings[.]000webhostapp[.]com Par coïncidence, le terme « defray » signifie fournir de l'argent pour payer une partie d'un coût, bien que ce dont les victimes doivent s'acquitter ne soit pas tout à fait clair.

La distribution de Defray présente plusieurs caractéristiques :

• Defray est diffusé via des documents Word dans des pièces jointes d'emails

• Les pièges sont conçus sur mesure pour attirer toutes les victimes potentielles

• Les destinataires sont des individus ou bien des groupes d'individus, par exemple, group@ ou websupport@

• Les pays les plus touchés sont le Royaume-Uni et les États-Unis

[Global Security Mag Online]

Réagissez à cet article

Source : *Defray, le nouveau ransomware qui cible l'éducation et la santé – Global Security Mag Online*

Attention à Faketoken, le malware Android qui vole les données bancaires en copiant des applis

Attention à Faketoken, le malware Android qui vole les données bancaires en copiant des applis

---

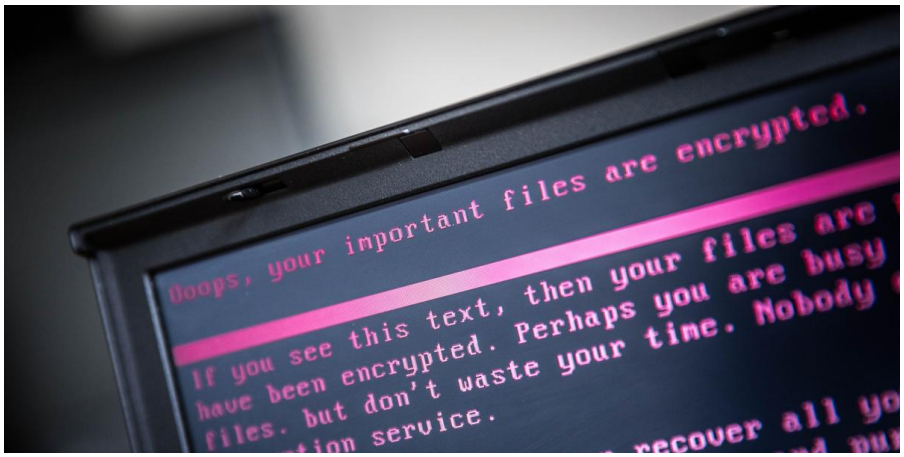
Une version améliorée d'un cheval de Troie bancaire vieux d'un an a été repérée par des chercheurs en sécurité en Russie.

Pour la firme de sécurité Kaspersky les malwares bancaires sont l'une des plus grandes menaces qui pèsent sur les smartphones Android. L'un d'eux, Faketoken, connu depuis un an environ, est de retour sous une nouvelle forme plus dangereuse, prévient-elle.
Au départ, ce cheval de Troie interceptait des SMS pour y récupérer des données bancaires que des utilisateurs imprudents auraient pu y indiquer. Désormais, il se greffe directement sur des applis bancaires ou sur des applis de réservations de taxis, de VTC ou d'hôtels afin de faire la même opération et écoute vos appels.
Comment parvient-il à infecter un smartphone ? Grâce à l'envoi en masse de SMS proposant de télécharger des photos. Dès lors qu'un utilisateur clique sur le lien, le malware s'installe discrètement sur l'appareil…[lire la suite]

Réagissez à cet article

Source : *Faketoken, le malware qui vole les données bancaires en copiant des applis*

Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?



Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?

Il s'est répandu à très grande vitesse, et est plus évolué que son prédécesseur, WannaCry.

Après WannaCry, Petya. Pour la deuxième fois en quelques semaines, un « rançongiciel » (*ransomware*, en anglais) s'est largement propagé sur Internet, rendant inutilisable de nombreux ordinateurs et perturbant lourdement le fonctionnement de plusieurs grandes entreprises.
Le code de ce rançongiciel a été disséqué par de nombreux experts et entreprises de sécurité informatique ces dernières heures, permettant de mieux comprendre la manière dont il fonctionne.

Que fait-il exactement ?

Petya est un rançongiciel visant les systèmes Windows : il rend indisponibles les données d'un ordinateur, qui ne peuvent être déverrouillées qu'en versant une rançon. Il s'agit d'une variation très modifiée d'une souche apparue au printemps 2016.
A la différence de WannaCry, Petya commence par s'attaquer à la toute petite partie du disque dur – qui recense tous les fichiers présents dans la mémoire d'un ordinateur – et la chiffre, les rendant inutilisables. Ensuite, il s'en prend à la partie du disque dur qui permet de lancer le système d'exploitation, le logiciel qui fait fonctionner l'ordinateur. Cette partie est modifiée de manière à ce que l'ordinateur ne puisse plus démarrer en utilisant le système d'exploitation prévu. Lorsqu'on allume l'ordinateur, c'est Petya qui se lance, et le rançongiciel fait son travail. Un message s'affiche alors, réclamant que soient envoyés 300 dollars en bitcoin, la monnaie électronique, pour obtenir la clé de déchiffrement.
Il est extrêmement déconseillé de verser la rançon : outre le fait que payer entretient les réseaux mafieux qui se cachent souvent derrière les rançongiciels, l'adresse e-mail qui servait aux auteurs de Petya à rentrer en contact avec les victimes a été désactivée par le fournisseur de messagerie, rendant tout versement parfaitement inutile.

Comment se propage-t-il ?

Les développeurs de ce logiciel ont mis beaucoup de soin aux fonctionnalités d'infection de Petya, qui utilise plusieurs méthodes de propagation dites « *latérales* », vers les ordinateurs appartenant au même réseau que la machine infectée.
Une fois installé sur un ordinateur, Petya va chercher à y obtenir les plein pouvoirs et repérer les autres appareils branchés sur le même réseau. Le rançongiciel va ensuite fouiller dans l'ordinateur qu'il a infecté pour récupérer des identifiants et des mots de passe qu'il va pouvoir ensuite réutiliser dans le réseau pour prendre le contrôle de davantage d'appareils et démultiplier sa propagation. Ensuite, à l'aide de fonctionnalités classiques de Windows utilisées pour gérer les réseaux, il va se transférer vers d'autres machines.
Outre cette fonctionnalité, il utilise aussi deux outils – EternalBlue et EternalRomance – volés à la NSA, la puissante agence de renseignement américaine, qui, en exploitant une faille dans un protocole permettant aux ordinateurs de se « parler » au sein d'un même réseau, permettent sa propagation de machine en machine. EternalBlue était d'ailleurs déjà utilisé par WannaCry.
L'utilisation de plusieurs méthodes d'infection expliquerait pourquoi certaines machines pourtant immunisées contre EternalBlue et EternalRomance, car ayant installé les mises à jour de sécurité correspondantes de Microsoft, soient quand même infectées par Petya.
Son mécanisme de propagation à l'intérieur d'un réseau d'une entreprise fait que les postes de travail classiques ne sont pas les seuls à succomber à Petya. Des ordinateurs plus centraux, plus sensibles, sont aussi atteints, comme les serveurs sur lesquels fonctionnent les sites Web. C'est pour cette raison que plusieurs sites du groupe Saint-Gobain étaient inaccessibles mercredi 28 juin au matin, selon une source interne…[lire la suite]

Réagissez à cet article

Source : *Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?*

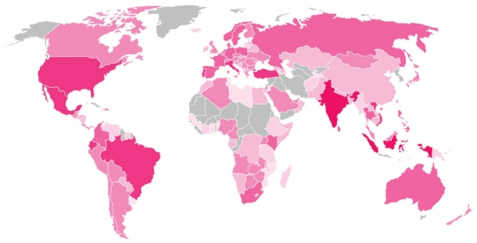
250 millions de PC infectés par un nouveau malware

250 millions de PC infectés par un nouveau malware

Après Wannacry, c'est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l'argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.

Les internautes n'ont pas fini de s'arracher les cheveux à cause des virus informatiques. Après Wannacry qui bloquait les ordinateurs pour demander des rançons, voici le malware Fireball. Ce logiciel asiatique qui infecte les ordinateurs a été détecté par les experts de **Check Point**.
Il prend discrètement le contrôle d'un PC pour détourner les recherches et récupérer les données. Il aurait déjà infecté plus de 250 millions de machines dans le monde. Les zones géographiques les plus touchées sont l'Inde, le Brésil et l'Amérique, mais l'Europe et la France ne sont pas épargnées.

Ce logiciel n'est pourtant pas le fruit d'un gang de hackers. C'est officiellement un adware -nom donné aux logiciels publicitaires- qui a été développé en toute légalité par **Rafotech**, une agence de marketing digitale chinoise qui a pignon sur rue. Et pour le répandre, l'entreprise l'a inséré discrètement dans des suites logicielles téléchargeables gratuitement, tels que « FVP Imageviewer », « Deal Wifi » ou « SoSo Desktop ». Mais il ne se contente pas de diffuser de la pub.



Check Point – Diffusion mondiale de Fireball
Une fois installé, Fireball change la page d'accueil du navigateur pour afficher un faux moteur de recherche (« Trotux ») qui redirige les recherches vers des moteurs que l'utilisateur n'aura pas forcément choisis. Il va également installer un système de traçage pour collecter des données de navigation, mais aussi, selon Check Point, les mots de passe ou les numéros de cartes bancaires.
Fireball pourrait également prendre le contrôle d'une machine pour installer et d'exécuter à distance des logiciels espions. Il crée aussi une porte dérobée pour espionner ses victimes. Les experts en sécurité conseillent aux victimes de le supprimer au plus vite. Si la page d'accueil de votre PC a été modifiée sans votre intervention, il y a de grande chance qu'il ait été contaminé.
[Source : BFM Business]

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

---

Réagissez à cet article

Source : *Après Wannacry, c'est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l'argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.*

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

Security researchers have claimed to have discovered possibly the largest malware campaign on Google Play Store that has already infected around 36.5 million Android devices with malicious ad-click software.

The security firm Checkpoint on Thursday published a blog post revealing more than 41 Android applications from a Korean company on Google Play Store that make money for its creators by creating fake advertisement clicks from the infected devices.

All the malicious apps, developed by Korea-based Kiniwini and published under the moniker ENISTUDIO Corp, contained an adware program, dubbed Judy, that is being used to generate fraudulent clicks to generate revenue from advertisements.

Moreover, the researchers also uncovered a few more apps, published by other developers on Play Store, inexplicably containing the same the malware in them…[lire la suite]

Réagissez à cet article

Source : *Judy Android Malware Infects Over 36.5 Million Google Play Store Users*