Une faille dans Windows 10 utilisée pour vous espionner !

Une faille dans Windows 10 utilisée pour vous espionner !

Selon un rapport publié sur le blog de la firme de sécurité informatique FireEye, les pirates procédaient comme suit : un fichier Word ouvert innocemment par l'utilisateur activait la faille 0-Day -CVE-2017-8759- et permettait au maliciel d'installer à son insu un programme informatique destiné à vous espionner. L'ordinateur visé par la manoeuvre était alors contraint d'installer FinSpy – le spyware en question.

Ce malware est développé par une entreprise anglaise particulièrement controversée qui commercialise ses produits à des gouvernements partout dans le monde : **Gamma Group**. Selon le rapport de FireEye, **FinSpy a déjà été vendu à de multiples acheteurs,** il est donc plus que probable que ceux-ci s'en servent activement pour tenter d'infiltrer de nombreuses cibles.

Selon les experts en cybersécurité de Microsoft, les hackers en question font **partie du groupe NEODYMIUM**, déjà connu pour des pratiques de hacking similaires. Microsoft reste donc très vigilant par rapport à ces failles de sécurité : n'hésitez donc pas à télécharger les patchs proposés dès que possible !

On ne le répétera jamais assez, si vous recevez un fichier Word suspect sur votre boîte mail ne l'ouvrez pas, même s'il vous promet de vous révéler la suite de Game Of Thrones !…[lire la suite]

NOTRE MÉTIER :

• FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO
• EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES
• AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT
• MISE EN CONFORMITE RGPD / FORMATION DPO

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons 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 ;

AUDITS RGPD / 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 nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons 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-nous

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 : *Windows 10 : une faille de sécurité permet aux pirates d'y installer un dangereux malware !*