Microsoft corrige encore Windows Defender en toute discrétion

	Mettez à jour de toute urgence votre Windows

Une vulnérabilité critique découverte par Google et touchant Windows a vite été corrigée par Microsoft. Au bénéfice de ceux qui laissent Windows Update activé.

La semaine dernière, le 24 mai, Microsoft a discrètement corrigé une vulnérabilité critique du composant MsMpEng de Windows. Plus précisément, MsMpEng est un processus de base de Windows Defender, le logiciel anti-malware livré en standard sur Windows 10 et 8.1, et installable sur Windows 7. Découverte le 12 mai dernier par Tavis Ormandy, chercheur en sécurité du Google Zero Project, cette faille autorise l'exécution de programmes non certifiés et donc potentiellement malveillants.
« *MsMpEng comprend un émulateur système x86 complet qui est utilisé pour exécuter des fichiers non fiables qui ressemblent à des programmes exécutables. L'émulateur s'exécute sous la forme NT AUTHORITY\SYSTEM et ne réside pas dans un bac à sable* », explique l'expert sur la page signalant le bug. Et sur laquelle il revient avec moult détails techniques sur le mode d'exploitation de la vulnérabilité.
Cette nouvelle brèche qui touche l'anti-malware de Microsoft est la deuxième que Tavis Ormandy déniche à quelques jours d'intervalle. Le 9 mai dernier, une faille de MsMpEng risquait d'infecter les utilisateurs… qui lançaient une inspection de leur machine à l'aide de l'outil de sécurité. Paradoxalement, les utilisateurs qui avaient désactivé le scan automatique en étaient donc protégés…[lire la suite]

Denis JACOPINI :
Vous avez aussi la possibilité (et nous vous recommandons fortement) d'installer un logiciel de sécurité géré par ceux pour qui la cybersécurité est le métier. Nous vous recommandons depuis 1996 les produits ESET et en particulier celui-ci (cliquez).

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 : *Microsoft corrige encore Windows Defender en toute discrétion*

Un simple lien permet de faire planter les PC Windows 7 et 8.1

Un simple lien permet de faire planter les PC Windows 7 et 8.1

Un bug du NTFS exploitable depuis le web met à genoux les PC Windows. Windows 10 est épargné, mais Windows 7 et 8.1 devront être corrigés.
À l'époque de Windows 95 et Windows 98, un bug permettait de faire planter un PC via un simple document au nom non supporté par le système de fichiers. Il suffisait pour cela d'accéder à certains périphériques, représentés par un nom de fichier virtuel.
Aussi incroyable que cela paraisse, un bug similaire existe dans **Windows 7 et Windows 8.1**, dévoile *Ars Technica*. Tenter d'accéder au fichier « **c:\$MFT\123** » bloque complètement le système de fichiers NTFS. La MFT n'est pas en principe accessible directement, mais en la traitant comme un dossier, son accès est totalement bloqué. Tout le système se trouve alors figé, ne pouvant plus accéder aux données de la partition NTFS concernée. Seule solution : redémarrer la machine…[lire la suite]

Réagissez à cet article

Source : *Un simple lien permet de faire planter les PC Windows 7 et 8.1*

Des centaines de caméras de vidéo surveillance françaises piratées par… Hitler !

Des centaines de caméras de vidéo surveillance françaises piratées par… Hitler !

Piratage : Plus de 1500 caméras de vidéo surveillance d'entreprises Françaises infiltrées par un pirate informatique. Il a signé son forfait « Heil Hitler » sur les écrans de contrôle.
Je vous contais, il y a peu, de la vente d'accès à des caméras de vidéo surveillance. Un grand classique, malheureusement ! Les pirates profitent de la feignantise de certains utilisateurs à lire le mode d'emploi de leur appareil. Des utilisateurs qui ne changent pas le mot de passe usine, ou ne pensent même pas à l'activer. Bilan, l'accès aux images et à la webcam se font en deux clics de souris…[lire la suite sur ZATAZ]

Réagissez à cet article

Source : *ZATAZ Vidéo surveillance : des centaines de caméras françaises piratées par… Hitler ! – ZATAZ*

10 règles à respecter pour utiliser un drone en toute sécurité

	10 règles à respecter pour utiliser un drone en toute sécurité

1. Ne pas survoler les personnes
2. Respecter les hauteurs maximales de vol
3. Ne pas perdre de vue son drone, ne pas l'utiliser de nuit
4. Ne pas utiliser son drone au-dessus de l'espace public en agglomération
5. Ne pas utiliser son drone à proximité d'un aérodrome
6. Ne pas survoler de sites sensibles ou protégés
7. Respecter la vie privée des autres
8. Ne pas diffuser les prises de vue sans l'accord des personnes concernées et ne pas en faire une utilisation commerciale
9. Vérifier les conditions d'assurance
10. Se renseigner en cas de doute

L'utilisation d'une caméra

Les prises de vue (photos ou vidéos) sont possibles en aéromodélisme dès lors que ces **prises de vue sont réalisées sans usage commercial ou professionnel.**

Le droit à la vie privée des autres personnes doit être respecté. **Les personnes présentes doivent être informées** si l'aéromodèle est équipé d'une caméra ou de tout autre capteur susceptible d'enregistrer des données les concernant.

Par ailleurs, **toute diffusion d'image permettant de reconnaître ou identifier les personnes (visages, plaques d'immatriculation …) doit faire l'objet d'une autorisation** des personnes concernées ou du propriétaire dans le cas d'un espace privé (maison, jardin etc.) et doit respecter la législation en vigueur (notamment la **loi du 6 janvier 1978 modifiée dite « Informatique et Libertés »**).

La violation de la vie privée est passible d'un an d'emprisonnement et 45 000 euros d'amende…[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

---

Réagissez à cet article

Source : *Quelle réglementation pour les drones en 2017 ?*

Journée de la Biométrie – 2ème édition le 7 juillet 2017 à l'ENSICAEN

Journée de la Biométrie – 2ème édition le 7 juillet 2017 à l'ENSICAEN

Suite au succès de The Biometrics Day In Normandy de novembre 2014, le Laboratoire GREYC en partenariat avec l'ENSICAEN, le Pôle TES, l'AD Normandie, Orange et Normandie Université organise la seconde édition le 7 juillet prochain.
La journée dédiée aux acteurs de la Biométrie, enseignants-chercheurs et partenaires industriels, sera ponctuée de conférences, de démonstrations et de temps d'échanges. L'occasion de faire connaître les activités de recherche dans ce domaine, mettre à l'honneur les innovations et la vision de demain de la Biométrie.
L'inscription est gratuite mais obligatoire : inscription
Journée de la Biométrie – vendredi 7 juillet 2017, de 9h30 à 17h
ENSICAEN – 6 Boulevard Maréchal Juin – Caen

Téléchargez l'affiche

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 : *Journée de la Biométrie – AD Normandie*

EternalRocks, le successeur de WannaCry encore plus inquiétant ?

	EternalRocks, le successeur de WannaCry encore plus inquiétant ?

Après l’attaque du ransomware WannaCry, les chercheurs ont identifié le ver de réseau EternalRocks. Celui-ci utilise jusqu’à 7 outils de hacking ayant été volés à la NSA puis exposés par le groupe Shadow Brokers.

Selon Malwarebytes, WannaCry a recherché les ports SMB vulnérables avant d’utiliser EternalBlue pour rentrer sur le réseau et le backdoor DoublePulsar pour installer le ransomware. EternalRocks utilise aussi ces deux outils. (crédit : D.R.)

Une semaine après l’attaque perpétrée par le ransomware WannaCry au niveau mondial, un autre logiciel d’exploitation de failles fait parler de lui. Selon des chercheurs en sécurité, il y a au moins une personne qui utilise 7 des outils d’attaque volés à la NSA dans un ver de réseau dénommé EternalRocks par ceux qui l’ont identifié. Les chercheurs ont constaté que ce ver ciblait la même vulnérabilité du protocole SMB de Windows, en s’avérant plus menaçant et plus difficile à contrer. Comme WannaCry, EternalRocks utilise EternalBlue, l’un des outils de la NSA.

Malwarebytes pense que WannaCry n’a pas été diffusé par une campagne de spams malveillant mais par une opération de scanning qui a d’abord recherché les ports SMB accessibles publiquement et vulnérables avant d’utiliser EternalBlue pour rentrer sur le réseau et d’utiliser la porte dérobée DoublePulsar pour installer le ransomware…[lire la suite]

Réagissez à cet article

Autonomie des laptops : les

mensonges des industriels démontrés par une étude

Autonomie des laptops : les mensonges des industriels démontrés par une étude

A l'instar des volumes de consommation d'essence et d'émanation de CO2 des voitures, l'autonomie des laptop atteint rarement les belles promesses affichées par le constructeur.…[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

Autonomie des laptops : les mensonges des industriels démontrés par une étude

A l'instar des volumes de consommation d'essence et d'émanation de CO2 des voitures, l'autonomie des laptop atteint rarement les belles promesses affichées par le constructeur.…[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

Surprise : HP enregistre tout ce que vous tapez grâce à un keylogger !

Surprise : HP enregistre tout ce que vous tapez grâce à un keylogger !

La société ModZero a découvert un keylogger caché dans les pilotes de nombreux ordinateurs portables HP. Ils stockent toutes les touches appuyées sur son clavier dans un fichier texte non-chiffré (C:\Users\Public\MicTray.log). Même si le fichier est écrasé à chaque redémarrage, il représente une faille critique, car il permet à n'importe qui de découvrir les mots de passe tapés par l'utilisateur. C'est d'autant plus grave si un système de backup à de multiples copies de ce fichier.

Manque de réactivité

Les pilotes ont été développés par Conexant. Malheureusement, ni HP, ni les programmeurs n'ont donné suite à ModZero, qui s'est retrouvé dans l'obligation de divulguer publiquement le problème avant la sortie du correctif. Les équipes américaines de Laptop Mag ont pu confirmer la faille, et elles ont découvert que chaque touche appuyée était stockée sous la forme d'un code hexadécimal. Sur la capture ci-dessus, « Mic target 0x1 scancode 0x1e flags 0x0 extra 0x0 vk 0x41 » représente « a ».

Un correctif, finalement

HP a finalement annoncé, en fin de semaine dernière, qu'une mise à jour corrigeant le problème était disponible sur le site HP.com ou Windows Update. La firme a expliqué que le keylogger n'était pas censé être livré avec les ordinateurs vendus au grand public.

Liste des ordinateurs portables concernés :

• HP EliteBook 820 G3
• HP EliteBook 828 G3
• HP EliteBook 840 G3
• HP EliteBook 848 G3
• HP EliteBook 850 G3
• HP ProBook 640 G2
• HP ProBook 650 G2
• HP ProBook 645 G2
• HP ProBook 655 G2
• HP ProBook 450 G3
• HP ProBook 430 G3
• HP ProBook 440 G3
• HP ProBook 446 G3
• HP ProBook 470 G3
• HP ProBook 455 G3
• HP EliteBook 725 G3
• HP EliteBook 745 G3
• HP EliteBook 755 G3
• HP EliteBook 1030 G1
• HP ZBook 15u G3 Mobile Workstation
• HP Elite x2 1012 G1 Tablet
• HP Elite x2 1012 G1 with Travel Keyboard
• HP Elite x2 1012 G1 Advanced Keyboard
• HP EliteBook Folio 1040 G3
• HP ZBook 17 G3 Mobile Workstation
• HP ZBook 15 G3 Mobile Workstation
• HP ZBook Studio G3 Mobile Workstation
• HP EliteBook Folio G1
•

…[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

---

Réagissez à cet article

Source : *Surprise : HP enregistre tout ce que vous tapez grâce à un keylogger ! – PC Astuces*

WannaCry : seulement trois antivirus protègent de l’exploit EternalBlue

WannaCry : seulement trois antivirus protègent de l’exploit EternalBlue

---

Prompts à clamer qu'ils bloquent WannaCry, les éditeurs d'antivirus oublient de mentionner qu'ils ne détectent pas, à trois exceptions près, l'exploit EternalBlue. Or, c'est celui-ci qui risque d'être réutilisé par de nouvelles menaces.

Depuis la crise WannaCry, qui s'est déclenchée le 12 mai 2017 et s'est traduite par l'infection de centaines de milliers de systèmes, les éditeurs d'antivirus n'hésitent pas à clamer que leurs outils arrêtent tous la menace. Un test monté par MRG Effitas, une entreprise anglaise spécialisée dans la recherche en sécurité informatique (MRG signifiant Malware Research Group), montre que la réalité est un peu plus contrastée.

En testant la capacité des logiciels de protection grand public (avec leurs paramétrages par défaut) à détecter l'exploit EternalBlue, mis à profit par WannaCry pour se diffuser, MRG Effitas établit que seuls trois produits stoppent le code de la NSA récupéré par les auteurs du ransomware : Eset Smart Security, F-Secure Safe et Kaspersky Internet Security. « *Deux de ces produits utilisent le filtrage réseau pour détecter cet exploit et le bloquer avant son exécution au niveau du noyau* », écrit MRG Effitas, qui précise que ce mode de détection pourrait être contourné en masquant la signature de l'exploit.
..[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

---

Réagissez à cet article

Source : *WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue*