

**Mettez à jour de toute
urgence votre Windows**

	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 dénicher 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>



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.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Microsoft corrige encore Windows Defender en toute discrétion*

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 dénicher 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>



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.

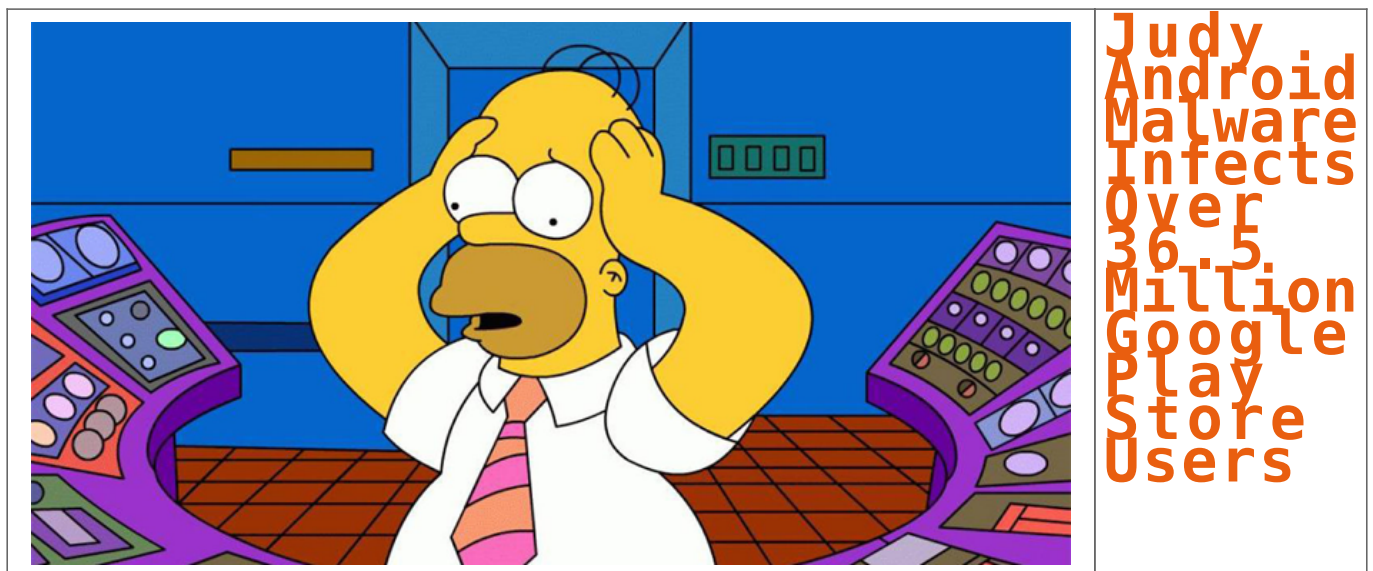


[Contactez-nous](#)

Réagissez à cet article

Source : *Microsoft corrige encore Windows Defender en toute discrétion*

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]

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.



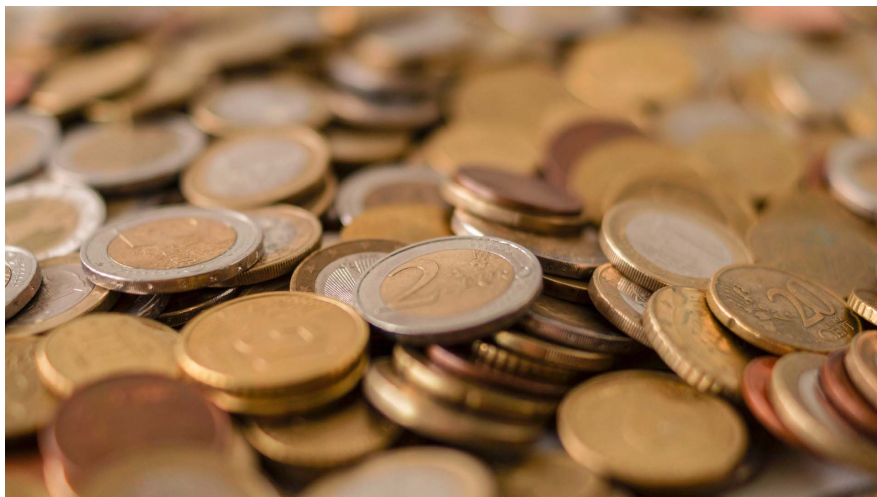
[Contactez-nous](#)



Réagissez à cet article

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

Des banques autorisées par la Cnil à tester la reconnaissance vocale



Des banques
autorisées par
la Cnil à
tester la
reconnaissance
vocale

La Cnil indique avoir autorisé neuf établissements bancaires à expérimenter la reconnaissance vocale pour s'authentifier lors d'une connexion à un compte ou pour effectuer certaines transactions.

Lorsque vous vous connectez à votre compte bancaire, vous entrez certainement le numéro de votre compte, un mot de passe et éventuellement d'autres informations, comme votre code postal, pour être redirigé sur votre caisse régionale. Quand vous effectuez un virement bancaire ou un paiement quelconque, peut-être validez-vous la transaction en tapant un code. Ces méthodes d'authentification mises en place pour s'assurer que c'est bien vous qui cherchez à accéder au compte ou qui donnez certains ordres ne sont pas la panacée en matière de sécurité informatique mais elles ont le mérite d'être familières pour le grand public et facilement renouvelables en cas de besoin. Or aujourd'hui, elles sont concurrencées par la biométrie...[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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Neuf banques autorisées par la Cnil à tester la reconnaissance vocale – Business – Numerama*

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

     <div><div>Démonstrations Conférences</div><div>JOURNÉE DE LA BIOMETRIE SAVE THE DATE</div><div>Public académique industriel</div></div> <div></div> <div><div>Le 7 juillet 2017 9h30-17h</div><div>ENSICAEN, 6 boulevard Maréchal Juin 14000 Caen</div><div></div></div>	<p>Journée de la Biométrie 2ème édition le 7 juillet 2017 à l'ENSICAEN</p>
--	--

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>



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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Journée de la Biométrie – AD Normandie*

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]

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.



[Contactez-nous](#)

Réagissez à cet article

Mieux protéger les TPE/PME du cyber-risque



Mieux
protéger les
TPE/PME du
cyber-risque

Les cyberattaques concernent tous les acteurs de la société: particuliers, entreprises ou administrations. Mais force est de constater que les principaux impactés sont généralement les entreprises de petite ou de moyenne taille.

Une étude IFOP montre que, en France, près de 77% des cyberattaques toucheraient les TPE/PME. Par ailleurs, les dommages de ces attaques numériques peuvent se révéler d'une importance telle qu'elle pourrait compromettre l'avenir même de l'entité touchée. Outre la **baisse ou l'interruption des activités** pendant une certaine durée, une cyberattaque peut également **impacter la réputation ainsi que les relations contractuelles** de l'entreprise touchée, notamment celles avec ses partenaires et/ou sa clientèle.

Pourtant, seulement un tiers des entreprises de petite ou moyenne taille se dit consciente des dangers d'une cyberattaque et prend les précautions de prévention nécessaires. Pour les autres, elles disposeraient de systèmes vulnérables et facilement accessibles aux hackers.

Les assureurs : nouveaux acteurs de la cybersécurité

Si la plupart des assureurs proposent désormais aux professionnels des **assurances cyber-risques** et **e-reputation**, un assureur a décidé d'aller plus loin. Generali s'associe à ENGIE Ineo et Europ Assistance pour lancer une **offre d'assurance spécifique pour les TPE/PME**. Cette dernière vise la réparation et l'indemnisation de ces entreprises en cas de cyberattaque. Le partenariat entre les trois sociétés a pour but d'optimiser au maximum la prise en charge de l'entreprise touchée. Elle sera axée sur trois points :

- **Europ Assistance assurera une prise en charge immédiate :**

Europ Assistance dispose d'un **service d'assistance informatique disponible à tout moment**. Elle prendra en charge l'entreprise victime d'une cyberattaque dans les plus brefs délais. Les chargés d'assistance travailleront en collaboration avec les experts informatiques d'Engie Ineo. Ils mettent également en place un accompagnement humain de l'entreprise afin de s'assurer qu'elle comprenne les différentes étapes du processus de restauration.

- **La réparation des données par Engie Ineo**

Pour l'assureur Generali, la société Engie Ineo sera chargée de **restaurer les données informatiques**. A cet effet, son équipe technique devra effectuer une enquête pour établir un diagnostic et déceler les preuves de l'attaque. Ils doivent ensuite reconstituer et restaurer les différentes données volées ou cryptées par les hackers. Le contrat d'assurance prévoit une **garantie « temps d'intervention » d'une heure**. Enfin, les services informatiques de l'entreprise devront étroitement collaborer avec la société Engie Ineo.

- **Generali indemniser les dommages**

Pour l'assureur Generali, sa mission tiendra à l'**indemnisation des dommages matériels mais aussi des pertes financières** découlant de l'attaque. Elle prendra donc en charge les frais d'expertise et de restauration des données, les pertes d'exploitation ainsi que la responsabilité civile et autres frais générés par la cyberattaque. Pour couvrir exactement chaque entreprise assurée, Generali prévoit de mettre en place un questionnaire spécifique afin d'évaluer le niveau d'exposition de l'entreprise au risque d'attaque numérique et d'adapter la protection selon sa taille.

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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

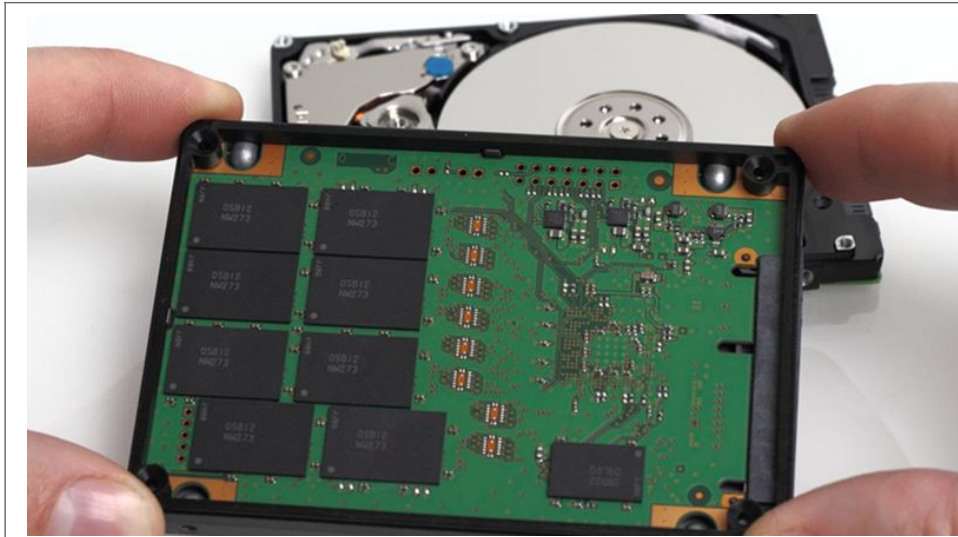


[Contactez-nous](#)

Réagissez à cet article

Source : *Cyberattaques: l'assurance se développe*

SSD : une faille de sécurité les rend vulnérables aux attaques de hackers !



SSD : une faille de sécurité les rend vulnérables aux attaques de hackers !

Les SSD sont vulnérables aux attaques de hackers en raison d'une faille de sécurité affectant la mémoire flash NAND MLC, rapporte une étude....[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.



[Contactez-nous](#)

Réagissez à cet article

La cyberattaque ‘ ‘WannaCry’ ’ aurait déjà coûté... 1 Milliard de dollars



La
cyberattaque
WannaCry
aurait déjà
côuté...
Milliard de
dollars

La cyberattaque globale WannaCry a causé des dégâts s'élevant à 1 milliard de dollars, relate le cabinet spécialisé 'McClatchyDC'. Ces dommages ont été causés par l'immobilisation de la production de grandes entreprises dans le monde entier.

Une situation liée à la perte de données, à la réduction de la productivité, à des perturbations du travail, au préjudice porté à la réputation, ainsi qu'à plusieurs autres facteurs.

La cyberattaque utilisant le virus WannaCry est considérée comme le plus grand piratage à rançon de l'histoire.

L'attaque a fait, selon Europol, 300 000 victimes dans au moins 150 pays depuis le 12 mai.

Et parmi les organisations touchées par cette attaque, on retrouve notamment Vodafone, FedEx, Renault, le National Health Service britannique ou encore la Deutsche Bahn.

Rédaction Infomédiaire

Remarques de Denis JACOPINI

L'évolution de ce virus et les dégâts qu'il produit sont à la mesure du nombre d'ordinateurs interconnectés dans le monde.

Pour ma part, ce virus n'a à ce stade, rien d'exceptionnel en terme d'ampleur. Il suffit de se renseigner un peu et découvrir que le virus Conficker, un ver informatique exploitant une faille de Windows, apparu en 2008 a touché, d'après les estimations 15 millions de victimes alors qu'il y avait 2 milliards d'internautes en moins (57% en moins car aux alentours de 3.5 milliard aujourd'hui et seulement aux alentours de 1,5 milliard en 2018 <http://www.journaldunet.com/ebusiness/le-net/1071539-nombre-d-internautes-dans-le-monde>)

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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Economie mondiale : La cyberattaque ‘‘WannaCry’’ a coûté... 1 MM\$ | Infomédiaire*

http://www.liberation.fr/futurs/2017/05/15/guillaume-poupard-la-cybercriminalite-devient-une-question-de-securite-nationale_1569743

Les recommandations de Microsoft pour se protéger de Wannacry

A graphic with a red background titled "WannaCry Ransomware Attack" and "Patch for Unsupported Windows (Apply Now)". It shows a laptop displaying a ransomware screen with a padlock icon and text asking for payment. A hand on the left holds a fan of US dollar bills, and a hand on the right holds a key, symbolizing the ransom payment and the unlocking of files.

Les recommandations de Microsoft pour protéger se de Wannacry

Il fait le buzz à travers les systèmes d'exploitation de Microsoft, Windows, son nom c'est Wannacry.

VOICI LES ÉTAPES POUR SE PROTÉGER DE CETTE MENACE :

En mars dernier, nous avons publié une mise à jour de sécurité (MS17-010) qui corrige la vulnérabilité exploitée par ces attaques. Tous les clients ayant Windows Update activé sur les versions de Windows supportées, sont donc protégés contre cette attaque.

1.D éploier le bulletin de sécurité MS17-010 :

Nous conseillons d'ailleurs à toutes les organisations qui n'ont pas encore appliqué cette mise à jour de sécurité, de déployer immédiatement le Bulletin de sécurité Microsoft MS17-010.

Nous savons aussi que certains de nos clients entreprises et utilisateurs grand public exploitent encore des versions de Windows qui ne sont plus supportées. Ils n'ont donc pas reçu cette mise à jour de sécurité en mars. Compte-tenu de l'impact potentiel de cette attaque et afin d'en limiter la propagation, Microsoft a pris la décision de publier pour tous nos clients, même s'ils ne disposent pas d'un Custom Support Agreement, les mises à jour de sécurité permettant de corriger cette vulnérabilité pour Windows XP SP3, Windows 8 et Windows Server 2003 SP2.

2. Mettre à jour votre antivirus

Windows Defender, System Center Endpoint Protection, et Forefront Endpoint Protection détectent cette famille de virus sous le nom de Ransom:Win32/WannaCrypt.

En complément, l'outil Microsoft Safety Scanner <http://www.microsoft.com/security/scanner/> disponible gratuitement, a été mis à jour pour détecter aussi cette famille de virus.

En cas de menace avérée :

Si vous êtes victimes par cette attaque contacter le support Microsoft

3. Procédez à la restauration de votre machine

<https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/>

<https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>

Liens utiles :

- Microsoft Guidance for WannaCrypt
- Microsoft Malware Prevention Center Technical Details about the ransomware worm
- MS17-010 Update Catalogue

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 BA 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 (*Avies* techniques, Recherche de preuves téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (*Actualisation de la D38727 n°93-40 (2004) 84*)
- Formation de C.E.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Les recommandations de Microsoft pour se protéger de Wannacry – Socialnetlink-La référence technologique en Afrique*