


# A quelles attaques informatiques doit-on s'attendre dans les mois qui viennent ? | Le Net Expert Informatique

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p><b>vous informe...</b></p>	<p>A quelles attaques informatiques doit-on s'attendre dans les mois qui viennent ?</p>
---	---

**Brèches de sécurité et atteintes à la vie privée font régulièrement la une des journaux. Comment la course à l'armement entre les auteurs de cyberattaques et les spécialistes de la défense se développe-t-elle ? Nous analysons dans cet article les prévisions des experts.**

La sécurité des informations et le respect de la vie privée ont toujours été des sujets brûlants, mais cette année la température semble encore monter d'un cran. Ces derniers mois ont été marqués par des cyberattaques très médiatisées qui ont concentré l'attention du monde entier sur la protection des données, le cryptage, le respect de la vie privée et la surveillance, comme jamais auparavant. Ces événements ô combien médiatiques se déroulent sur fond de multiplication des fuites de données au niveau des gouvernements, des entreprises et autres organisations, familles et individus.

Nous avons examiné les articles prospectifs de 17 entreprises et attribué les 130 prévisions résultantes à un certain nombre de catégories émergentes pour produire le graphique ci-dessous.

Prévisions de sécurité de Blue Coat, Damballa, FireEye, Fortinet, Forrester, Gartner, IDC, ImmuniWeb, Kaspersky Lab, Lancope, McAfee, Neohapsis, Sophos, Symantec, Trend Micro, Varonis Systems et Websense.  
Image : Charles McLellan/ZDNet

En tête de liste, figurent les « nouveaux vecteurs et plates-formes d'attaque » et « l'évolution des solutions de cybersécurité existantes », deux catégories qui illustrent la réalité de la course à l'armement en matière de cybersécurité.

Dans la première catégorie, plusieurs commentateurs ont souligné les « nouveaux bugs dans du code ancien largement utilisé » (Kaspersky Lab), tels que Heartbleed/OpenSSL et Shellshock/Bash. Sophos a noté des failles exploitables dans le protocole IPv6, ainsi que des capacités de robot et de rootkit dans l'environnement d'amorçage enrichi UEFI qui peuvent générer de nouveaux vecteurs d'attaque. Apple était la principale nouvelle plate-forme signalée, par exemple par FireEye, qui note que « étant donné qu'Apple est de plus en plus présent dans les entreprises, les concepteurs de programmes malveillants vont ajuster leur jeu d'outils ». Les récents chiffres de ventes record ne feront que creuser davantage l'appétit des pirates informatiques pour les produits d'Apple.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.zdnet.fr/actualites/cybersecurite-a-quoi-s-attendre-dans-les-mois-qui-viennent-39822112.htm>

Par Charles McLellan