SECURIMAG

LE MAGAZINE ANNUEL DU PREMIER CLUB DE SÉCURITÉ INFORMATIQUE EN TUNISIE

EDITO

La vie nous a toujours été généreuse. Elle nous a donné l'occasion de vivre des moments inédits et des expériences extraordinaires. L'évènement particulier de l'année serait le 10eme anniversaire du club dans le cadre de la bonne ambiance de la famille SecuriNets.

10 ans, 10 staffs, 7 Securiday dont 4 sont qualifiés de « journée nationale de la sécurité informatique », sans oublier les centaines de réunions organisées de façon hebdomadaire mais toujours constructives et innovatrices.

Chaque année, un nombre notable de membres anime les réunions de SecuriNets, travaille et présente différents projets et participe aux différentes actions du club.

Ce sont des chiffres énormes qui montrent bien l'ampleur de SecuriNets sur le plan universitaire comme sur le plan national. On se permet donc de se poser la question :

« Quel serait le secret derrière le succès de SecuriNets ? ».

Aujourd'hui, à l'occasion de nos 10 ans, on vous révèle ce secret. Notre recette magique combine passion et esprit de groupe.

Généralement, lorsqu'on possède un don pour une chose bien particulière, on finit souvent par la maîtriser. Et SecuriNets n'échappe pas à cette règle. Ici, on trouve d'innombrables personnes qui ont découvert leur penchant ou encore plus leur passion pour la sécurité informatique. Ils se sont mis à creuser, à apprendre, à se poser des questions et à chercher encore et encore. Et c'est ainsi que commence leurs histoires avec la sécurité informatique.

Néanmoins, on découvre rapidement que la route est rude et difficile à parcourir seul. Et c'est ici qu'intervient l'esprit de groupe.

A SecuriNets, on s'encourage, on partage le savoir et les connaissances et on s'entraide. Ici, on rencontre des gens qui marquent nos chemins, on tisse des liens d'amitiés et on forme une équipe solidaire et enthousiaste.

Toutes ces raisons nous comblent de joie et de fierté essentiellement le jour du Securiday, lorsqu'on goutte enfin au fruit de notre dur labeur. Le travail dur mais fructueux, d'une équipe de jeune motivés et déterminés.

Securinets est plus qu'un club, c'est toute une famille solidaire où règne le sérieux et la bonne ambiance. Il y a de quoi être fier d'y appartenir.

Alors, je vous invite tous à nous rejoindre pour découvrir de près l'admirable ambiance du club et le grand enthousiasme de l'équipe qui font que chaque SecuriHebdo soit une réussite. Venez gouter à notre bonne humeur et profiter de notre savoir-faire.

Soyez les bienvenus dans la famille de Securinets.

Joyeux anniversaire SecuriNets

Mohamed Nadhir Salem
Rédacteur en Chef

SOMMAIRE

4 SecuriCalendar

6 Actu mobile
Hoax
Galaxy Gear

8 Actu web
Black Market
Dark web
Yahoo tourne SSL
TOP 10 des anti-virus

10 Actu sécurité
NFC
Poubelle Wifi
Sophos
USB
Voxx
VariantMaster

12 Dossier

15 Interview

18 SecuriTool

20 Loisirs
La vie des geekettes
Astuce Sécurité
Quelle type de virus êtes-vous ?
Watch dogs
What others think you do ?

HOOX M2

LE SMARTPHONE PROFESSIONNEL SÉCURISÉ DE BULL

En Octobre dernier, L'entreprise française Bull a dévoilé le nouveau Smartphone sécurisé pour les entreprises baptisé Hoox m2.
Ce Smartphone est à base d'Android 4.1 mais son noyau a été durci par les équipes de cyber sécurité de Bull : Il est équipé d'un moteur de sécurité intégré et certifié. En plus d'une protection contre les malwares et les intrusions, il propose des communications et données stockées qui sont chiffrées en AES 256 bits. Mais le hic c'est que le chiffrement des communications ne fonctionne que si les deux personnes qui communiquent ensemble ont ce terminal à savoir le Smartphone Hoox. Ce téléphone est aussi doté d'un capteur biométrique, comme sur iPhone 5s ce qui permet de reconnaître les empreintes digitales de l'utilisateur.
Il dispose d'un processeur Quadri core Cortex A5 à 1,2 GHz, un écran QHD 4,68", 1 Go de RAM, mémoire Flash 8 Go, GPS, accéléromètre, deux caméras (5.0 Mpx auto-focus ; 0,3 Mpx) et les concepteurs ont choisi de ne pas le doter de carte MicroSD pour plus de sécurité.
Hoox est commercialisé depuis le 1er janvier 2014 au prix de 2000 euros et il n'est destiné qu'aux professionnels.

Arij Elmajed

Galaxy Gear

Septembre 2013, lors de l'IFA à Berlin, Samsung lance sa première montre connectée : Galaxy Gear. Le constructeur coréen souhaitait sans doute doubler Apple, mais il s'est finalement retrouvé trop en avance avec un produit pas vraiment intéressant.

Pourtant, Samsung a su commercialiser une montre alléchante sur le papier :
« Comme toute montre, elle donne l'heure mais, vous l'aurez compris, la Galaxy Gear vous propose bien plus. Pour profiter pleinement de l'intégralité des applications de cette montre, il vous suffit d'installer Gear Manager sur votre smartphone et de vous laisser guider. Ainsi, vous pouvez, entre autres, prendre et passer des appels téléphoniques, lire vos SMS et e-mails, et contrôler la lecture de vos fichiers audios (volume, pistes audio,t vidéo, etc.). À chaque nouvelle notification (réception de SMS, d'e-mail, d'appel, etc.), l'écran s'allume pour vous en informer.

En plus de vous permettre de prendre des clichés et des vidéos grâce à la caméra de 1,9 mégapixels, vous bénéficiez d'une reconnaissance de texte pour traduire en temps réel ce que vous avez sous les yeux. Pratique ! Côté applications, la Galaxy Gear est fournie avec un podomètre synchronisable avec l'application S Health de Samsung. Vous retrouverez aussi Runkeeper, Path et Evernote. Des applications supplémentaires peuvent également être téléchargées.

Les fonctions comprises incluent un minuteur, un chronomètre, un calendrier, un Memo Vocal, le journal d'appel et une application météo. Vous pouvez également utiliser la fonction commande vocale via S-Voice avec laquelle vous pouvez notamment demander la consultation de votre agenda et envoyer des messages. »

La Galaxy Gear écarte ses concurrentes sur le papier. Néanmoins, cela ne suffit pas : son autonomie réduite, sa compatibilité limitée à sa sortie à 2 appareils Samsung, et son logiciel encore rudimentaire peinent à la détacher de son statut de gadget.

Depuis, Samsung a corrigé certains défauts, notamment les notifications d'applications tierces, et a étendu la compatibilité de la montre aux Galaxy S3 et S4 via une mise à jour vers Android 4.3.
On imagine qu'une Galaxy Gear 2 est déjà en projet : elle aura sans doute du chemin à faire pour prouver son intérêt !

Black Market

Trend Micro vient de rendre public son rapport de sécurité annuel 2013, intitulé « Cashing in on Digital Information ». Dans un rapport de 34 pages, l'entreprise y révèle qu'il est quasiment impossible de garantir la parfaite confidentialité des données personnelles et des informations bancaires, que ce soit à cause des menaces de sécurité, des actes malveillants menés par les cybercriminels ou des attaques sophistiquées.

Définissons tout d'abord ce que c'est le « black Market ».
Le « black market » ou marché noir prend sa définition du secteur économique. En économie, ce terme définit tout marché clandestin pouvant porter sur des biens autorisés, qui sont par ailleurs traités dans le marché public. Il est apparenté à la contrebande où les restrictions réglementaires et fiscales du pouvoir en place sont contournées, et les marchandises illégales y trouvent leur place comme les armes, la drogue et le trafic d'organes. Ce type de marché favorise la corruption, et de manière plus générale la criminalité. Par analogie, le marché noir des données définit une plateforme où on vend des données confidentielles et généralement des données bancaires. Ces éléments proviennent dans la plupart des cas des opérations de violation de données.

Les attaques à grande échelle, précisément celles qui mettent en péril confidentialité et sécurité, sont détaillées dans ce rapport qui couvre notamment le piratage bancaire, les menaces mobiles, ainsi que les attaques sur les infrastructures. L'entreprise souligne que les cyber-menaces et les attaques ont gagné en complexité et en précision.

Ce rapport annuel se penche sur les vulnérabilités des technologies actuelles, toujours plus interconnectées et sophistiquées. Malheureusement, ces dernières sont également de nouveaux vecteurs pour les cybercriminels, qui font évoluer leurs cyber-attaques et mettent en danger les entreprises, notamment les banques, les acteurs du e-commerce, ainsi que les particuliers toujours plus nombreux à utiliser les technologies mobiles.
A titre d'exemple, Xylitol, un internaute francophone connu pour son talent d'investigation, annonce sur son blog avoir détenu tous les secrets d'un forum BlackMarket connu au niveau mondial appelé Darkode. Parmi les multiples captures d'écran publiées, on y trouve des preuves montrant comment certains pirates se font beaucoup d'argent en commercialisant des accès à des Botnets (y compris SpyEye).

Ce sont en tout 4 477 captures écrans et autres fichiers qui ont été récupérés lors de l'infiltration. L'archive diffusée fait quand à elle 763 Mo et contient des captures d'écran de chacun des principaux espaces privés du forum (à part les niveaux très restreint, dont Xylitol fait omission et réserve pour les forces de l'ordre pour des raisons de sécurité et de confidentialité). A noter que ce forum est réputé et beaucoup de piliers du monde Black Hat (des pirates talentueux, dangereux et recherchés) y sont inscrits et actifs. L'espace peut être assimilé à une organisation mafieuse dont les rouages sont bien huilés.

Mohamed Nadhir Salem

DARK WEB

(WEB PROFOND)

Vous pensez tout connaitre du web ... Mais saviez- vous qu'une grande partie est réellement cachée et que l'internet qu'on côtoie ne représente en vérité qu'environ 20% d'Internet ?

A cette base on parle du web profond ou le Dark Web .C'est une face du web non référencé par les moteurs de recherche classiques (Google, Explorer, Yahoo, etc...).
Mais pour quelles raisons ces pages sont-elles cachées ?

De quoi s'agit-il ?

Certains documents sont trop complexes et d'autres sont trop volumineux pour qu'ils soient indexés par les browsers. Et parfois c'est exprès ! Certains hackers et développeurs en souhaitant garder une certaine privatisation de l'information et choisissent de ne pas référencer leurs sites. Donc, pour accéder à ces pages, il faut forcement connaitre l'adresse ou l'URL. Les développeurs du site pourront alors transmettre leurs données à quelques personnes et le reste ne pourront pas y accéder. Malheureusement, ce milieu est favorable pour la circulation d'informations illégales...

A quoi sert le web profond ?

Derrière le web profond se cache une multitude de sites illégaux non atteignables au grand public sous peine de poursuites pénales ou de prison (Marché noir, Arme, Drogue ...). Il est possible d'acheter n'importe quel type de drogue sur un site, trouver des offres pour embaucher un tueur à gage, faire fabriquer de faux papiers ou acheter des armes.

Peut-on y accéder ?

Oui, on peut y accéder mais avant tout il faut bien mesurer les risques. Personne ne peut nous poursuivre pour avoir simplement navigué sur le web profond. En revanche, les sanctions pour toute sorte de transaction illégale sont souvent dures. Il est également dangereux de télécharger n'importe quel document à partir de ces sites.

Comment y accéder ?

Puisque le Dark Web assure à ses internautes une haute sécurisation de la navigation par le cryptage de ces pages, il faut donc utiliser des applications qui peuvent atteindre des adresses URL cryptées et qui garantissent plus ou moins l'anonymat de la connexion, en modifiant, par exemple, l'adresse IP. Ceci se fait grâce au réseau TOR (The Onion Router).
Mais avant de vous connecter à ces adresses, il est recommandé de prendre quelques précautions : vérifiez que votre antivirus est mis à jour et que votre ordinateur est protégé au maximum !

Khouloud Gattoussi

YAHOO!

Renforce la sécurité de sa messagerie avec l'activation par défaut de la connexion SSL pour l'ensemble des utilisateurs.

Après une refonte graphique importante, le service Mail de Yahoo! s'offre une nouvelle fonctionnalité demandée par les utilisateurs depuis des années déjà : le chiffrement des données.

Le mécanisme est loin d'être nouveau puisque Google l'appliquait à Gmail en 2008 avant de l'activer par défaut deux ans plus tard. En novembre 2010, Microsoft chiffrait également l'intégralité des sessions de Hotmail.

Yahoo Mail utiliserait prochainement le chiffrement SSL par défaut pour l'ensemble de son service webmail. La mise en place de la sécurisation SSL devrait intervenir à partir du 8 janvier 2014.
Auparavant, seule la connexion au compte Yahoo! était effectuée via HTTPS, c'est-à-dire en apposant un chiffrement SSL sur le protocole HTTP. La société introduisait une nouvelle option permettant de sécuriser cette connexion durant tout le temps de la session, c'est-à-dire même en consultant ses messages.
Ce chiffrement protège les messages envoyés entre le PC de l'utilisateur et les serveurs de Yahoo et le changement chez Yahoo s'explique en partie par les différentes affaires liées aux écoutes de la NSA et la collecte de millions de carnets d'adresses. De récents rapports indiquent que l'agence de sécurité aurait ainsi collecté deux fois plus de mails Yahoo que d'autres services au cours des dernières années.

Pour activer tout de suite le chiffrement SSL, rendez-vous dans
options > sécurité

Pour la société, l'enjeu est d'ajouter cette nouvelle couche de chiffrement sans pour autant affecter les performances de l'application Web. Il faut dire que plusieurs vulnérabilités ont été repérées au sein du webmail ces derniers temps.

Faten Mkacher

TOP 10

DES ANTI-VIRUS

« QUEL EST SELON VOUS LE MEILLEUR ANTIVIRUS ? »
UNE QUESTION QUI NOUS TRACASSE SANS CESSE !!!
ON S'EST DONC PERMIS DE VOUS PROPOSER UN CLASSEMENT DES DIX ANTI-VIRUS LES PLUS PERFORMANTS ET LES PLUS EFFICACES DE L'ANNÉE 2014

1. AVAST!

Haute protection anti-spyware et antimalware. Avast! Free Antivirus fournit une meilleure détection que les produits concurrents payants, assure une mise à jour automatique pendant un an et offre une version d'essai de 1 mois.

2. AVIRA ANTIVIR

C'est un antivirus utilisé par des millions d'utilisateurs, protège efficacement et gratuitement votre ordinateur contre la plupart des programmes malveillants .Mais son point faible consiste à donner des faux positifs c à d prendre des programmes sains pour des programmes malveillants.

3. KASPERSKY

C'est un anti-virus qui protège en temps réel contre les virus et les spywares sur net et assure une protection efficace contre les menaces web comme le vol d'identité, et ceci sans ralentir votre pc.

4. AVG INTERNET SECURITY 2014

Semblable à kaspersky, il assure une protection complète et en temps réel des dangers sur Internet et détecte également les problèmes de performance potentiels.

5. BITDEFENDER

Anti-virus qui se présente en plusieurs versions, les plus connus BitDefender Internet Security, BitDefender Total Security... Assure une protection de la vie privée mais malheureusement il ralentit le démarrage du pc.

6. ESET NOD32 ANTIVIRUS 6

La dernière version est la plus performante vu que le temps du scan a été réduit par deux. Connu par une faible utilisation des ressources système, une rapidité et surtout une détection des virus, vers, chevaux de Troie.

7. MCAFEE

Il est Caractérisé par une simple utilisation et adapté pour tout usage .Mais les dernières versions sont très chères.

8. F-SECURE

Antivirus très récent mais qui s'est attribué des récompenses. Assure une protection en ligne et des contenus dans le cloud pour les particuliers et les entreprises.

9. MICROSOFT SECURITY ESSENTIALS

N'est pas très connu et pourtant il mérite plus de reconnaissance car il assure une véritable protection contre toute menace.

10. NORTON ANTIVIRUS

Très ancien, assure lentement le scan des fichiers .Il est très récalcitrant lors de la désinstallation. Il reste souvent des fichiers qui peuvent ne pas permettre l'installation d'un autre antivirus. Ceci peut menacer le système (crash).

Vous pouvez maintenant choisir votre antivirus!!

Gattoussi Khouloud

NFC

NEAR FIELD COMMUNICATION SOLUTION OU PROBLÈME ?

Le NFC est une technologie de communication de données révolutionnaire qui a fait le Buzz depuis son apparition au grand public grâce aux tablettes et aux Smartphones. Mais question sécurité, peut-on vraiment s'y mettre sans crainte ?

Le NFC a connu le jour durant les années 2000 par les sociétés Sony et Philips, mais n'a été connu chez le grand public que récemment grâce aux terminaux Android, BlackBerry et Windows Phone et plus particulièrement les appareils hauts de gamme. Cette technologie sans fil à courte portée permet l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm et avec un débit maximum de 424 Kbits/s.

Qu'elle est son utilité ?

Comme la technologie Bluetooth, le NFC est intégré récemment aux nouveaux Smartphones et est géré nativement par Android grâce à une fonction appelée Android Beam depuis Ice Cream Sandwich. Le principe d'Android Beam consiste à échanger des fichiers (son, vidéo, lien vers une application, image...) juste par un simple contact entre Smartphones (tablettes). D'autre part, le NFC ajouté aux Smartphones permet d'effectuer des transactions bancaires et réaliser des achats en magasins (achat d'un produit vendu en distributeur en approchant son téléphone portable de la vitre, par exemple...). L'échange de données n'est pas son unique application, le NFC est présent aussi dans quelques modèles de téléviseurs de LG, ainsi que les nouvelles cartes bancaires.

Mais la véritable force de cette technologie réside dans la possibilité de l'utiliser dans le domaine de la domotique c'est pour cela plusieurs entreprises tel que Sadeghi, qui a développé un système appelé ShareKey qui tente carrément de remplacer les clés de la maison par les Smartphones, en dotant les portes de lecteurs NFC. De même pour l'entreprise Hyundai, qui vise à remplacer les clés des véhicules par les Smartphones.

Ce n'est pas tout, aujourd'hui dans quelques villes en Europe, les monuments et les transports sont dotés de tags NFC et de plus en plus des commerçants acceptent ce nouveau mode de payement sans contact.

La NFC n'est-elle pas un nouveau terrain de jeu pour les pirates?

Contrairement au Bluetooth, les données échangées via NFC ne sont pas chiffrées, elles sont en claires. Ce qui pose, selon le rapport des experts de Sophos, un réel problème. D'ailleurs, lors de la Defcon, une conférence autour de la sécurité à Las Vegas, un pirate a pu démontrer qu'il est facile de bidouiller des "antennes" permettant de capter et d'enregistrer les données venant de téléphones utilisant la NFC. Donc le piratage est possible, mais il nécessite des "moyens sophistiqués". Tout le monde n'est pas un hacker confirmé

D'autres part, les sociétés comme Sadeghi affirment que la solution NFC est plus convenable que celle de Bluetooth ou wifi vu que la portée de NFC est limitée à quelques centimètres, elle est donc plus difficile à intercepter.

Bref, voici quelques solutions de prévention. Si

vous utilisez une carte NFC, rangez-là dans un étui métallique, ça coupera le signal. Dans le cas d'un Smartphone, rendez-vous dans les paramètres avancées, là où l'on peut déjà désactiver le Wi-Fi, et décochez la case NFC. Sauf si vous possédez un iPhone, vu que même les nouveaux iPhone 5s et 5c n'intègrent toujours pas le NFC.

Alyssa Berriche

Une poubelle publique, un truc qui échappe a votre attention la plupart du temps, eh ben vous feriez mieux de bien ouvrir les yeux la prochaine fois car même les poubelles ont évoluées ! En effet la ville de Londres a récemment équipé ses rues d'un nouveau type de poubelles publiques assez particulières. Ces dernières sont en effet équipées d'antennes Wi-Fi capables de reconnaître les téléphones portables des passants afin de revendre ces données aux annonceurs et autres publicitaires.

À vocation de stations de recyclage, les poubelles intelligentes de la société Renew ont commencé à être déployées à Londres à l'occasion des Jeux Olympiques de 2012 pour leur capacité à résister à l'explosion d'une bombe. Avec leur conception en acier, elles peuvent réduire l'onde de choc, empêcher le dégagement de chaleur et les éclats produits par une explosion. Ces poubelles WiFi sont également dotées de panneaux numériques pour afficher des messages d'urgence mais aussi de l'information locale en temps réel et pour vendre de la publicité. Depuis début juin, Renew a commencé à tester une technologie Renew ORB avec une douzaine de ses poubelles à Londres sur une centaine disséminées. Un test qui vient de s'arrêter brutalement.

Suite à la parution d'un article de Quartz et la polémique suscitée, les autorités ont mis le holà. Le bêta-test consistait à détecter les smartphones à proximité dont le WiFi était activé.

Via la collecte de l'adresse MAC, les poubelles recueillaient des données sur l'itinéraire du passant, son temps et sa vitesse de déplacement, et sur le fabricant de l'appareil.

La technologie employée est présentée comme un cookie pour le monde réel par analogie avec le cookie du monde informatique, et ainsi un objectif sous-jacent de publicité ciblée.

Pour les autorités de la Cité de Londres qui a alerté la Cnil britannique, " tout ce qui se passe dans les rues doit être fait avec précaution, avec le soutien d'un public informé ". Le test " a été précipité et doit clairement être débattu - dans le même temps, la collecte de données, même anonymisées, doit cesser".

Le PDG de Renew a confirmé que le test a été stoppé " À ce stade, nous étions simplement en cours d'exécution d'un programme pilote extrêmement limité, chiffré, avec des données recueillies anonymisées ".

Hadhemi Samali

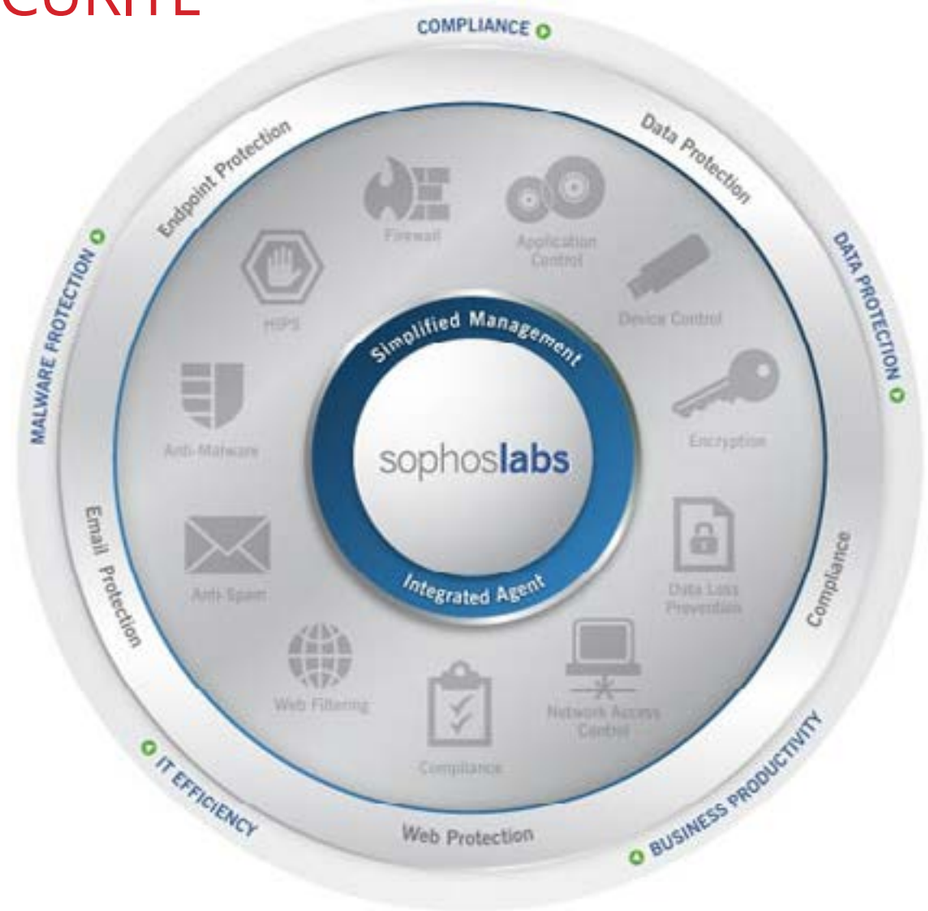
SOPHOS

Sophos, une société de logiciels et d'appliances de sécurité fondée en 1985 basée à Abingdon en Angleterre, a dévoilé son dernier Rapport sur les menaces de la sécurité informatique sur le niveau mondial.

Le rapport met en lumière des changements significatifs dans le comportement des cybercriminels au cours de l'année écoulée et prévoient leurs méthodes favorites d'attaque en 2014. L'an dernier, les cybercriminels ont poursuivi la professionnalisation croissante de leur « industrie », proposant des services toujours plus simples à acheter et à mettre en œuvre, qui ont porté le cyber-crime à des niveaux encore jamais atteints.

« Alors que de nombreux experts en sécurité sont conscients de cette tendance, peu d'entre eux reconnaissent pleinement sa signification », a déclaré James Lyne, chef de l'unité de recherche en sécurité de Sophos. « Si l'année 2013 a une chose à nous enseigner, c'est que les contrôles de sécurité traditionnels sont sous pression. Ces nouveaux comportements forcent notre industrie à s'adapter et changer, ainsi qu'à reconsidérer les bonnes pratiques de sécurité les plus établies. »

Le rapport a souligné l'émergence de nouveaux sujets de préoccupation, allant d'outils permettant une dissimulation dynamique des menaces pour donner un accès persistant et prolongé aux données des utilisateurs, à la prolifération de périphériques connectés, qui représentent des cibles nouvelles et souvent mal protégées. Il y'a de plus en plus d'objets connectés qui font irruption dans notre domicile et au sein de l'infrastructure qu'on utilise tous les jours, offrant aux cybercriminels la possibilité de nous atteindre dans notre vie quotidienne, plutôt que de se limiter simplement au vol d'informations financières.



« Ces tendances vont continuer en 2014, alors que les menaces deviennent de plus en plus intelligentes, dangereuses et discrètes » poursuit James Lyne.

En 2014, Sophos prédit que les cybercriminels monteront des attaques de phishing et d'ingénierie sociale encore plus sophistiquées et convaincantes, pour compenser la diffusion de systèmes d'exploitation plus difficiles à exploiter, tels que Windows 8.1. Des systèmes embarqués (systèmes de point de vente, médicaux ou d'infrastructure intelligents) rouvriront d'anciennes blessures, en répétant par négligence des erreurs d'implémentation éliminées des environnements PC modernes. Les attaques sur les données d'entreprises ou personnelles dans le Cloud continueront à augmenter, poussant les fournisseurs de services à affiner leur stratégie de sécurité pour ce nouvel environnement. Et les malwares pour les mobiles finiront par devenir aussi sophistiqués que sur les PC.

« En 2014, il ne faudra pas juste se contenter de surveiller l'évolution d'attaques existantes, mais se préparer à l'émergence de nouvelles menaces que nous n'avons pas encore observées. », déclare Gerhard Eschelbeck, directeur de Technologie de Sophos. « Notre industrie s'adapte pour étendre les mécanismes de protection afin de couvrir de nouveaux périphériques et combattre de nouvelles menaces. C'est un sujet qui concerne de plus en plus chaque individu et pas seulement les gouvernements et les entreprises. »

Une copie complète du Rapport sur les menaces à la sécurité 2014, avec plus d'informations et de statistiques sur les cyber-menaces en 2013, ainsi que des conseils et prédictions sur les tendances émergentes, est téléchargeable sur le site de Sophos.

Mohamed Nadhir Salem

VOXX

Oublier son mot de passe c'est le pire cauchemar qu'on puisse avoir!

De nos jours ce risque ne cesse d'augmenter vu le nombre croissant de machines informatiques qu'on possède : PC, téléphones portables, tablettes ,etc... sans oublier la crainte d'être piraté qui nous pousse à utiliser des mots de passe un peu longs et compliqués et donc faciles à oublier !!

Comme solution : Voxx International vient de dévoiler "Myris", un procédé substituant la reconnaissance oculaire au mot de passe pour réduire le niveau de risque de piratage à "un sur 2.000 milliards".

La société américaine (ex-Audiovox) a présenté en marge du Consumer Electronics Show à Las Vegas un gadget pas plus grand qu'un palet de hockey permettant par un simple regard le déverrouillage de toute machine informatique qui jusqu'à présent nécessitait un mot de passe.

"A l'exception du test ADN, la reconnaissance oculaire est le procédé d'identification le plus fiable", a expliqué devant la presse Tom Malone, président de Voxx Electronics.

Myris, que l'on peut charger sur une clé USB pour ouvrir son compte sur tout support informatique (PC, tablette, smartphone etc..), est doté d'une technologie capable de scanner l'iris de l'utilisateur et de crypter ses données d'identification personnelles.

Ce nouvel outil mis au point en collaboration avec la société spécialisée dans la biométrie Eye-Lock offre un risque d'erreur infime estimé à "un sur plus de 2.000 milliards", selon M. Malone.

"C'est tout simplement la fin du mot de passe", a-t-il ajouté.

Voxx présente Myris comme la première version destinée au grand public, de cette technologie de pointe qui n'est utilisée, jusqu'à présent, que par les administrations et les entreprises à cause de sa complexité et son coût très élevé.

Tom Malone n'a pas révélé le prix de cet outil innovant, mais il a assuré que Myris serait abordable et accessible à tous les utilisateurs.

La question qui nous vienne à l'esprit : Serait-elle l'approche suivante qu'adoptera Apple pour améliorer la reconnaissance biométrique de l'IPhone 5S ??

Salah Khemiri

UNE CLÉ
MAIS PAS COMME LES AUTRES !

Une clé USB est connue comme étant un support de stockage ; mais on peut faire bien plus que ça avec un tel objet !
Lors du « March Patch Tuesday de 2013 » Microsoft a publié sept bulletins de sécurité dont le plus important était le « MS13-027 » vu que cette attaque nécessitait un accès physique à la machine victime.
Cette faille permet à quiconque disposant d'une clé USB qui comporte un payload de franchir la barrière de sécurité d'une machine vulnérable et d'accéder au système tout entier même si l'Autorun est désactivé et l'écran est verrouillé.
On doit donc tenir compte des risques majeurs auxquels notre PC windows sera confronté suite à une attaque pareille. Prenons l'exemple de Stuxnet, un ver qui a été injecté dans le programme du système nucléaire Iranien par l'intermédiaire d'un lecteur de clé USB et qui a causé des dommages énormes.
Pour exploiter cette vulnérabilité, le pirate commence par insérer un périphérique USB malicieusement formaté. Ensuite, lorsque les pilotes de l'équipement USB énumèrent le dispositif, le pirate amène le système à exécuter un code malveillant dans le contexte du noyau Windows.
Parce que la vulnérabilité est déclenchée lors de l'énumération de l'appareil, aucune intervention de l'utilisateur n'est requise. L'attaque pourrait donc être déclenchée bien que le poste de travail est verrouillé ou qu'aucun utilisateur n'est connecté et c'est grâce à cette non-authentification qu'on privilégie les pirates ayant un accès occasionnel à la machine.
Le piratage par le biais d'une clé USB a laissé libre cours à l'imagination des hackers et c'est de cette manière-là qu'un distributeur de billets a été récemment piraté.
Il est devenu possible d'exécuter tout et n'importe quoi via une clé USB particulière : injection de code malveillant, interception de connexion wifi, récupération de données à partir d'un disque dur...
Ce genre d'outil n'est pas encore pris au sérieux, et pourtant la banque postale a eu recours à deux informaticiens allemands pour tester la sécurité de ses distributeurs après avoir constaté que les guichets automatiques de billets avaient été ponctionnés sans que la société financière ne comprenne vraiment comment.
En effet, un petit trou dans le distributeur de billets, juste en face du PC sous windows XP, a permis aux pirates d'y insérer une clé USB. Le support de stockage comportait un script qui automatisait l'installation de code malveillant ayant autorisé les hackers de se servir en monnaie sonnante et trébuchante.
Ingénieux ces pirates, Ils semblent avoir utilisé des « mules » pour retirer de l'argent. Et en plus de ça, le cheval de Troie sauvegardé via la clé USB possédait un code supplémentaire qui empêchait les retraits non autorisés par le pirate en chef.
En conclusion, ceci nous amène à penser qu'il serait plus pertinent d'assurer la sécurité physique du système avant de penser au contrôle logistique et l'administration.

Rim Gheribi

Les Geekettes

Arij Elmajed

Il est vrai que les geekettes restent une minorité. En 2013, la communauté des hackers, reste masculine à 90% et les PDG de sexe féminin dans le domaine technologique se comptent sur les doigts de la main.

Ces geekettes ont certainement eu comme idole Ada Lovelace 1815-1852 qui est « le premier programmeur du monde ». En 1850, Elle a développé, avec l'aide de Charles Babbage, la fameuse «Machine Analytique» qui est tout simplement l'ancêtre de nos ordinateurs actuels. Elle a créé le logiciel de cette machine, et devenue ainsi la première femme de l'histoire de l'informatique.

On cite également Grace Murray Hopper qui a conçu le premier compilateur. Elle a conceptualisé l'idée des langages de programmation indépendants de la machine et elle a aussi inventé le mot « bug ».
En effet, le royaume des geeks, partout dans le monde, n'était pas très accueillant à l'égard du sexe féminin. Néanmoins, il existe des geekettes qui ont pu exceller et se distinguer de leurs concurrents masculins.

Parmi ces femmes on trouve Padmasree Guerrier, Chef de Technology & Strategy Officer (CTO) de Cisco Systems et ancien directeur technique de Motorola, Virginia « Ginni » M. Rometty, dirigeante chez IBM, Margaret C. Whitman, PDG du site de vente en ligne eBay et a pris la tête de Hewlett-Packard, Hilary Mason, occupe le poste de Data scientifique chez Accel , co -fondatrice d eHackNY , co-animateur de DataGotham et membre du NYCResistor .

Mais celles qui ont le plus de notoriété sont certainement Sheryl Sandberg, le bras droit de Mark Zuckerberg et Marissa Mayer qui, après treize ans passés chez Google, a été la première femme ingénieur de la firme de Mountain View et désormais elle prend les rênes de Yahoo !

Sheryl Sandberg, la geekette féministe

Diplômée de Harvard, souvent qualifiée de surdouée, Sheryl Sandberg est le bras droit de Mark Zuckerberg. A 43 ans, Elle est la directrice générale de Facebook, après avoir occupé un poste stratégique chez Google et avoir été économiste à la Banque mondiale. Elle veut lancer une nouvelle révolution féministe : Elle a exposé publiquement ses idées pour la première fois en 2010, dans un discours relayé par Ted, plate-forme vidéo d'échange de conférences. La vidéo a depuis été vue près de 2 millions de fois. Elle recommande notamment aux femmes de s'imposer au sein de leurs entreprises.

Marissa Mayer, la geekette glamour

Elle fut la première femme ingénieure à être embauchée par Google en 1999. Son diplôme de l'université de Stanford en poche, elle travaille de longues années à développer le moteur de recherche et participe également au lancement de Gmail et Images. Ensuite elle est devenue la directrice de Yahoo dans le but de donner un second souffle à ce dinosaure du Web. De plus, la multimillionnaire aime s'afficher dans les pages des magazines aux côtés de célébrités.

Joanna Rutkowska, la hackeuse

Elle est parmi les femmes hacker les plus connues. Elle se consacre rapidement au développement d'exploits pour les environnements Linux et Windows x86, avant de s'intéresser aux technologies furtives utilisées par les codes malveillants et les pirates. L'experte polonaise se dédie désormais à la détection de ces attaques, au développement et au test de nouvelles techniques offensives. Lors de la Black Hat Conference de 2006, elle a pu prouver son talent par une technique nommée Blue Pill, qui a permis de détecter des failles majeures au sein de Windows Vista permettant d'en prendre le contrôle total. En 2010, elle a créé le système d'exploitation Qubes avec son collègue Rafal Wojtczuk, un OS surpassant de loin Windows ou Linux en matière de sécurité. Qubes 1.0 est sorti officiellement le 3 Septembre 2012.

Le succès de ces femmes prouve que s'imposer et diriger une grande entreprise dans le domaine technologique est désormais plus que possible. Alors voilà le credo du jour :

« "Si elles l'ont fait et elles ont réussi , pourquoi pas moi ! »