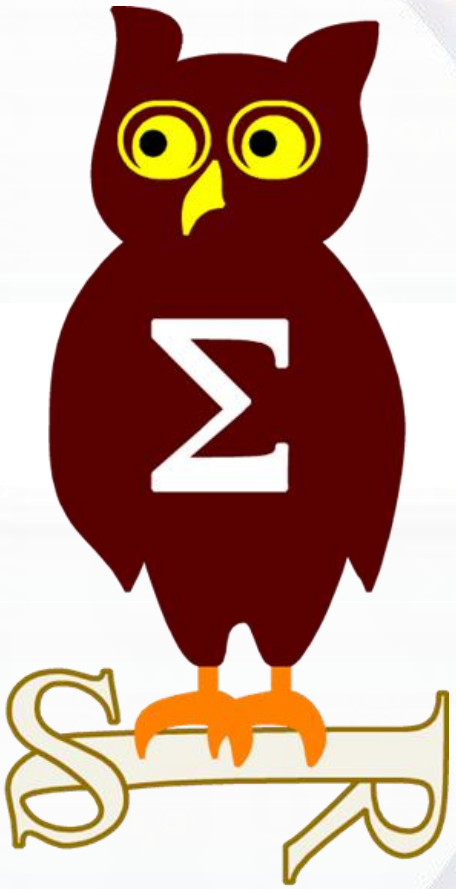


Revue d'actualité

08/07/2014

Préparée par

Jean-Philippe GAULIER
Ary KOKOS
Vladimir KOLLA
Arnaud SOULLIE

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2014

MS14-030 Vulnérabilité dans Remote Desktop Protocol (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 7, 8, 8.1 et 2012
- Exploit:
  - Fuite d'information lors d'une connexion RDP au moment de la vérification de la MAC générée.
- Crédit:
  - Andrew Swoboda and Tyler Reguly / Tripwire (CVE-2014-0296)

MS14-031 Déni de service TCP (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées sauf Windows 2003, car la fonctionnalité n'y est pas présente)
- Exploit:
  - Déni de service avec des paquets TCP aux options malformées
- Crédit: ?

MS14-32 Vulnérabilité dans Microsoft Lync (1 CVE) [Exploitabilité ?]

- Affecte:
  - Microsoft Lync Server 2010 et 2013
- Exploit:
  - Fuite d'information qui pourrait permettre à un attaquant d'envoyer une URL de réunion Lync avec un ID valide et d'exécuter un script dans le navigateur pour voler les informations de session
- Crédit: ?

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2014

MS14-33 Vulnérabilité dans Microsoft XML Core Services (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif pour Windows XP Embedded POSReady, kb2939576 (cf. screenshot après)
- Exploit:
  - Divulgation d'information de l'utilisateur, lors du traitement d'un XML par MSXML. Cas de l'hébergement du XML sur un site "malfaisant" (Dédicace à Hervé ^_^)
- Crédit:
  - Christian Kulenkampff (CVE-2014-1816)

MS14-034 Vulnérabilité dans Word (1 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007 Service Pack 3
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier Word (doc et docx) spécialement formaté
- Crédit:
  - s3tm3m par VeriSign iDefense Labs (CVE-2014-2778)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2014

MS14-035 Vulnérabilité dans Internet Explorer (**59** CVE) [Exploitabilité 1]

- Affecte:
  - Internet Explorer (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady, kb2957689 (cf. screenshot après)
- Exploit:
  - use-after-free, élévations de privilèges, fuite d'information lors d'une renégociation TLS...
  - 2 publiées publiquement (CVE-2014-1770 par ZDI car Microsoft a dépassé le délai de 180 jours)
  - Corrige la fameuse "CMarkup Use-After-Free RCE" pour Windows 8 (CVE-2014-1770)
    - http://www.youtube.com/watch?v=pHonj1nUZu0
  - Corrige également la faille utilisée par ZDI à CanSecWest 2014 / Pwn2own
    - http://www.zerodayinitiative.com/advisories/ZDI-14-186/
- Crédits : *liste trop longue, donc voici un extrait 100% Subjectif*
  - VUPEN par ZDI (CVE-2014-1764)
  - VUPEN par ZDI (CVE-2014-2777)
  - The Prosecco team de l'INRIA (CVE-2014-1771) (TLS Server Certificate Renegotiation)
  - **23** CVE remontées par la société chinoise Qihoo

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2014

MS14-036 Vulnérabilité dans GDI+ (2 CVE) [Exploitabilité 1]

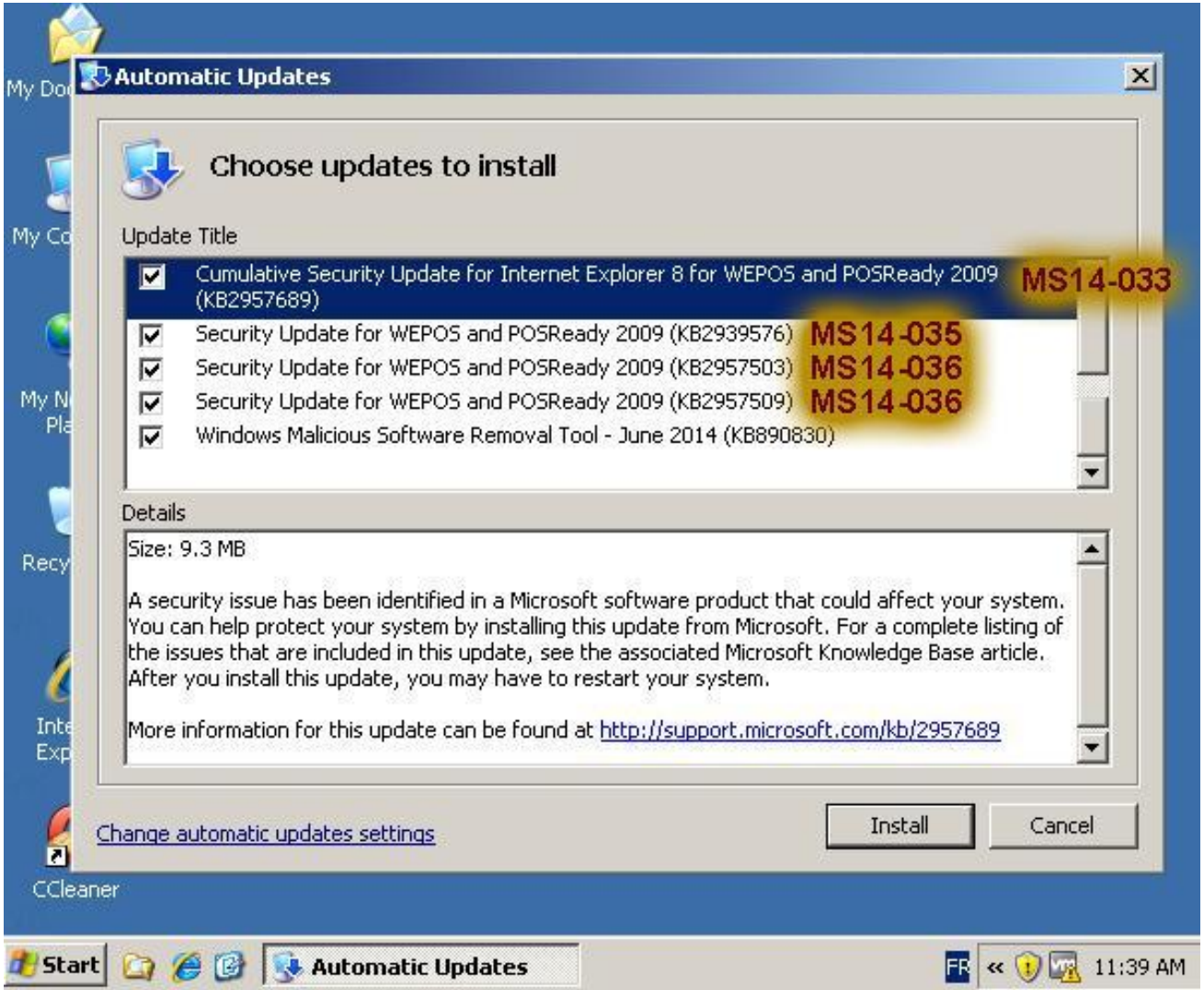
- Affecte:
  - Windows (toutes versions supportées)
  - Microsoft Office pour Windows 2007 et 2010
  - Microsoft Lync Server 2010 et 2013
  - Correctif pour Windows XP Embedded POSReady, kb2957503 (cf. screenshot après)
  - Correctif pour Windows XP Embedded POSReady, kb2957509 (cf. screenshot après)
    - Un “diff” permet d’obtenir une 0-day pour Windows XP “normal”
- Exploit:
  - Exécution de code à l'affichage (donc traitement) de polices unicodes spécialement formatée (CVE-2014-1817)
  - Exécution de code à l'affichage (donc traitement) d'image spécialement formatée au niveau de ses métadonnées (CVE-2014-1818)
- Crédits :
  - Scott Bell de Security-Assessment.com (CVE-2014-1817)
  - Mateusz "j00ru" Jurczyk de Google (CVE-2014-1818)

Failles / Bulletins / Advisories

Microsoft - Avis Juin 2014

Mise à jour pour Windows XP Embedded POSReady

- Toujours sans le documenter dans ses bulletins...



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Juin 2014

2755801 Mise à jour de Flash Player

- V25.0 nouvelle mise à jour de Flash Player

2862973 les certificats racine ne peuvent plus utiliser MD5

- V3.0 Mise à jour pour Windows 8 et Windows Server 2012.

2962824 Mise à jour des révocations de modules UEFI

- V1.1 Changement dans le mode de détection

2974294 Vulnérabilité(déni de service) dans le moteur anti-malware Microsoft

- V1.0 version initiale

2960358 Désactivation de RC4 pour .NET (TLS)

- V1.1 Ajout d'un lien vers l'article 2978675

Failles / Bulletins / Advisories

Réseau (principales failles)

Juniper

- Firewall NetScreen (en fin de vie...)
  - Déni de service lors du traitement de paquets spécialement formatée (CVE-2014-3813 et CVE-2014-3814)

VMWare Tools

- Drivers et outils installés sur les serveurs ou postes virtuels
- Elévation de privilèges par à un déréférencement du pointeur "NULL"

Failles / Bulletins / Advisories

Crypto

OpenSSL

- Faille DTLS CVE-2014-0195
  - Ecriture jusqu'à 16Mo dans la mémoire du processus
  - Déni de service voir plus...
  - Vulnérabilité introduite par Robin Seggelmann, déjà à l'origine de HeatBleed
    http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/ZDI-14-173-CVE-2014-0195-OpenSSL-DTLS-Fragment-Out-of-Bounds/ba-p/6501002

- ChangeCipherSpec (CCS) CVE-2014-0224
  http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html

Failles / Bulletins / Advisories

Divers

PHP

- Buffer overflow et exécution de code depuis la fonction dns_get_record() sur les enregistrements "TXT" (utilisés pour du SPF / anti-spam)
  https://github.com/php/php-src/commit/b34d7849ed90ced9345f8ea1c59bc8d101c18468
- Vulnérabilité dans phpinfo()
  https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.htm

Apache

- Déni de service lors du traitement d'un cookie (mod_log_config / CVE-2014-0098)
- Déni de service lors du traitement de données CDATA… contenant un espace (mod_dav / CVE-2013-6438)
  http://www.apache.org/dist/httpd/CHANGES_2.4.9

Samba

- Déni de service sur nmbd, avec un paquet UDP (CVE-2014-0244)
- Déni de service sur smbd, pour un utilisateur authentifié (CVE-2014-3493)

Android

- Contournement de la whitelist ADB dans Android 4.4.2

https://labs.mwrinfosecurity.com/advisories/2014/07/03/android-4-4-2-secure-usb-debugging-bypass/

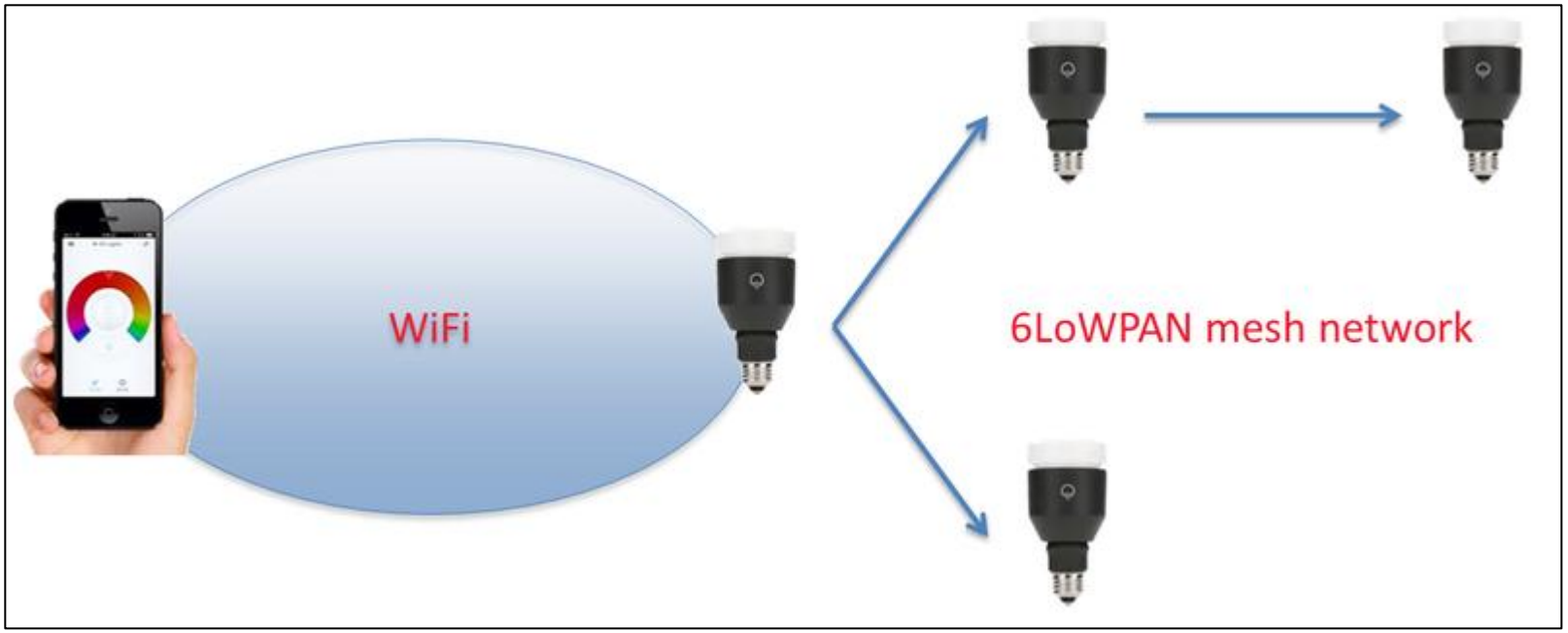
Failles / Bulletins / Advisories

Internet of (insecure) things

Hacking des ampoules connectées

Utilisation de credentials hardcodés

http://www.contextis.co.uk/blog/hacking-internet-connected-light-bulbs/



Hack de robots par SpiderLabs

Après récupération des credentials dans une base de données MySQL sans mot de passe …

http://blog.spiderlabs.com/2014/06/weak-passwords-better-call-the-doctor.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Des données de clients AT&T dévoilées

http://www.11alive.com/story/news/nation/2014/06/15/att-data-breach/10555039/

Des vulnérabilités dans le plugin WordPress "All in One SEO Pack" met de millions de sites en danger

http://thehackernews.com/2014/05/vulnerabilities-in-all-in-one-seo-pack.html

Des fraudeurs installent physiquement des malwares sur des DABs

http://thehackernews.com/2014/05/fraudsters-physically-deploy-malicious.html

Le malware BKDR_VAWTRAK utilise une fonctionnalité de sécurité de Windows pour bloquer les antivirus plus de 53 logiciels concernés

http://www.developpez.com/actu/72206/Le-malware-BKDR-VAWTRAK-utilise-une-fonctionnalite-de-securite-de-Windows-pour-bloquer-les-antivirus-plus-de-53-logiciels-concernes/

Les shell C99 sont backdorés : une backdoor dans la backdoor

http://thehackerblog.com/every-c99-php-shell-is-backdoored-aka-free-shells/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Selon IBM, la faille serait toujours la même…

http://www.scmagazine.com/human-error-contributes-to-nearly-all-cyber-incidents-study-finds/article/356015/

- C'est Dave !

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Puce 3G dans les Core i5 et i7 (~o~ Rumeur ~o~)

- Suite à présentation de Laurent Bloch de juin dernier ;-)
  http://www.infowars.com/91497/print/

Android 4.4.3

- Local root par Airbus Defense and Space (ex-Cassidian)
  http://blog.cassidiancybersecurity.com/post/2014/06/Android-4.4.3%2C-or-fixing-an-old-local-root

Faille XSS en chaine chez TweetDeck

- TweetDeck fait de la récupération automatique de tweets… sans les filtrer
- XSS Chained : re-tweet automatique du XSS à tous les followers, qui re-tweet...

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Feedly

- Plusieurs “grosses” attaques le 11 et le 13 juin (sans détail)
- Rançon de $300 et $800, c’est peu :-)
- Géré avec leur “opérateur” (sans détail)
  - Un traceroute permet de trouver Telefonica comme opérateur et CloudFlare comme hébergeur

  http://blog.feedly.com/2014/06/11/denial-of-service-attack/

Société de Jeux Vidéo

- Entre 100 et 120 Gbps de réflexion + amplification DNS, mi juin
- Traité par l’acteur du DDoS Incapsula (Qui fait sa publicité grâce à cela)

  http://thehackernews.com/2014/06/dns-flood-ddos-attack-hit-video-gaming.html

Deezer

- Attaque le 7 juin (sans détail)
- Indisponibilité totale pendant plusieurs heures

  http://nl-international.deezer.com/E10062014125337.cfm?WL=56170&WS=47588701_2717594&WA=46160

Evernote

- Attaque le 7 juin (sans détail)
- Indisponibilité totale pendant plusieurs heures

  http://www.zdnet.com/evernote-struck-down-by-ddos-attack-for-several-hours-7000030417/

Protonmail, un webmail chiffré pas si sécurisé

- Exécution de persistent xss directement dans le code

  http://vimeo.com/99599725

Piratages, Malwares, spam, fraudes et DDoS

Sites piratés

Piratage du site de Domino's Pizza

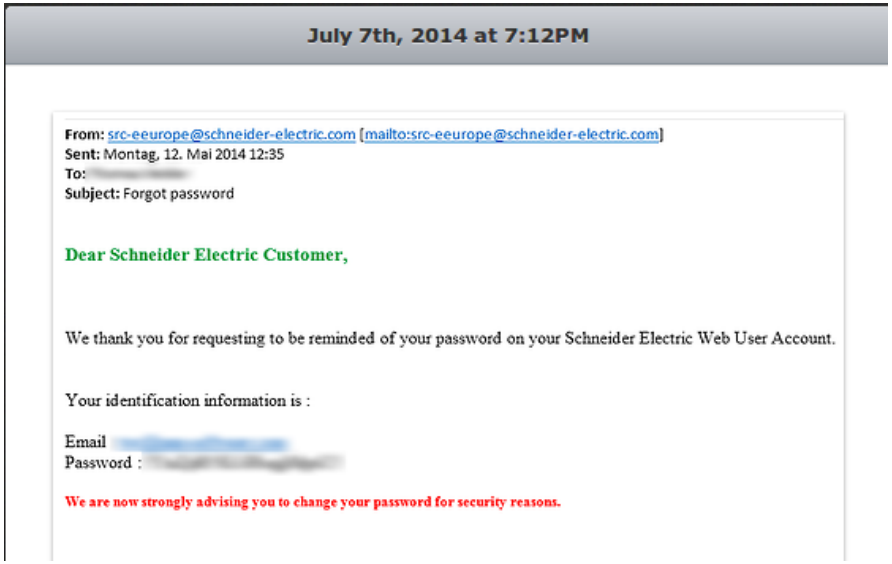
- Les hackeurs demandent 30k€ pour ne pas publier les données de 650 000 clients
  http://www.clubic.com/antivirus-securite-informatique/actualite-709779-domino-pizza-hackeurs-demandent-rancon.html

Aviva compromis via l'exploitation d'une faille sur l'infrastructure de MDM (Mobile Iron)

- On parlerait de HeartBleed …http://www.theregister.co.uk/2014/06/23/aviva_heartbleed_hack/

Un site qui répertorie les sites web qui stockent votre mot de passe en clair

http://plaintextoffenders.com/



Crypto
Divers

TrueCrypt, déjà oublié ?

- La mode est passée, plus personne n'en parle...
  - Ou presque
    http://www.darkreading.com/endpoint/privacy/data-security-decisions-in-a-world-without-truecrypt/a/d-id/1278624
  - Selon un des développeurs, il serait impossible de “forker”
    http://www.net-security.org/secworld.php?id=17031

VeraCrypt, d'Idrix

- Une alternative Française
  http://www.lemondeinformatique.fr/actualites/lire-veracrypt-une-alternative-francaise-a-truecrypt-57737.html

BoringSSL

- Après avoir utilisé et forké WebKit, Google réitère avec OpenSSL
  - Les correctifs OpenSSL seraient trop complexes à maintenir
  - Les exigences de stabilité d'OpenSSL ne seraient pas en ligne avec Google
    https://boringssl.googlesource.com/
- Alors qu'en Avril, les grands du web annonçaient faire des dons à OpenSSL
  - Facebook, Microsoft, Intel, Rackspace, Amazon... mais également Google

Le NIST supprime Dual EC DRBG NSA

- De son guide des bonnes pratiques
  www.nist.gov/itl/csd/sp800-90-042114.cfm

SCADA
Divers

HAVEX, un virus qui cibles les systèmes SCADA

- Un RAT assez classique, mais qui se distingue par le fait qu'il cible le protocole OPC, très souvent utilisé pour l'échange de données dans les SI industriels.
- Il aurait été distribué par des attaques de type "watering hole" sur les sites de vendeurs de composants industriels.
- Symantec parle d'une campagne d'attaque sur les companies énergétiques, "*DragonFly*"
  http://www.net-security.org/malware_news.php?id=2791
  http://www.digitalbond.com/blog/2014/07/02/havex-hype-unhelpful-mystery/
  http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat?inid=us_ghp_hero2_dragonfly
  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

Nouveautés (logiciel, langage, protocole...)

Matériel

Smartphone Hoox m2 de Bull

- Agréé "Diffusion Restreinte" par l'ANSSI
  http://www.globalsecuritymag.fr/Le-smartphone-securise-Hoox-m2,20140624,45876.html
- Pour rappel :
  - Basé sur Android
  - 2000 euros pièces

EviKey : Clef USB sécurisée

- Par la startup française Freemindtronic
- “Déverrouillable” à l’aide d’un appareil sans contact (NFC)
- Un challenge pour tester la robustesse du produit :
  http://www.undernews.fr/reseau-securite/evikey-la-cle-usb-la-plus-securisee-est-francaise.html

Nouveautés (logiciel, langage, protocole...)

Divers

Chrome en 64bits

http://blog.chromium.org/2014/06/try-out-new-64-bit-windows-canary-and.html

PHP Script Decoder 0.1

- “Désobfuscateur” PHP
  http://www.kahusecurity.com/2014/deobfuscating-php-scripts/

RpcView 0.1

- Naviguer dans les RPC Microsoft
  http://rpcview.org/index.html

Script IDA

- Pour reverse .NET contenant du code natif
  https://github.com/shuffle2/IDA-ClrNative

Netflix publie son outil de monitoring pour Amazon AWS

http://www.lemagit.fr/actualites/2240223970/Netflix-rend-public-son-outil-de-monitoring-de-la-securite-AWS

Business
France

La CNIL se fâche

- Contre Cetelem (BNP Paribas Personal Finance)
  - Plainte d'une personne fichée par erreur au FICP, n'arrivant pas à s'en faire enlever
    http://www.cnil.fr/linstitution/actualite/article/article/fichage-illegal-au-ficp-mise-en-demeure-de-bnp-paribas-personal-finance/
- Contre DHL
  - 700.000 données de clients en libre accès
    http://www.zdnet.fr/actualites/dhl-700000-donnees-clients-en-libre-acces-la-cnil-se-fache-39802741.htm#null

Business
International

Cisco invente le "fog computing"

http://www.cisco.com/web/about/ac50/ac207/crc_new/university/RFP/rfp13078.html

Combien a couté la Cyber Criminalité en 2013 ?

- Selon Steria et Pierre Audoin Consultant : 110 Milliards d'euros
  http://www.lemondeinformatique.fr/actualites/lire-la-cyber-criminalite-a-coute-110-mdeteuro-en-2013-56489.html
- Selon McAfee : $445 milliards
  - $160 milliards de perte en propriété intellectuelle
  - $200 milliards pour USA + la Chine + le Japon + l'Allemagne
  - $150 milliards en vols de données personnelles

  http://gadgets.ndtv.com/internet/news/cybercrime-costs-global-economy-445-billion-a-year-report-538632
- Le PIB "monde" étant de $75 000 milliards, cela ne ferait que 0,6%

Nokia cible d'un chantage

- vers 2007, vol des clefs de chiffrement, permettant de signer les applications.
- La suite ressemble une scène d'un film d'Audiar :
  - Rançon en liquide dans une mallette ;
  - Rendez-vous dans le parking d'un parc d'attraction finnois, le Särkänniemi ;
  - Perte de la trace des hackeurs par la police

  http://www.mtv.fi/uutiset/rikos/artikkeli/nokia-paid-millions-of-euros-in-ransom/3448918

Business
International

Bug Bounty chez Mozilla

- $10,000 par faille critique sur la nouvelle librairie de vérification des certificats
- Valable jusqu'à fin juin 2014
  http://blog.mozilla.org/security/2014/04/24/10000-security-bug-bounty-for-certificate-verification/

Droit / Politique

France

RGS 2.0 Publié !

http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000029122964

Droit / Politique

France

Lenovo

- La cession de l'activité serveur d'IBM au Chinois Lenovo inquiète les militaires Français
  http://www.01net.com/editorial/621632/securite-larmee-francaise-sinquieterait-pour-ses-serveurs-ibm/

Droit / Politique
International

Classement NPR 2014

- Après le classement de l'EFF de ceux qui protègent le mieux les données personnelles
- voici le classement de NPR, une radio américaine indépendante
  - Avec des critères plus techniques (SSL, HSTS, PFS…)
- Les meilleurs élèves sont Google, Facebook et Twitter ;-)
  http://www.npr.org/blogs/alltechconsidered/2014/06/12/320997037/how-well-do-tech-companies-protect-your-data-from-snooping

No-IP vs Microsoft

- Tentative d'entente (sans succès) entre Microsoft et No-IP, depuis des années contre les domaines dynamiques frauduleux
- Microsoft a obtenu une ordonnance d'une Cour fédérale et a saisi 22 domaines de No-IP
- Coupure de service pour de nombreux utilisateurs du service gratuit
  http://www.noip.com/blog/2014/06/30/ips-formal-statement-microsoft-takedown/

Agent double USA-Allemagne

- se faisant détecter en tentant de vendre des secrets aux Russes et canaux chiffrés dans l'application météo... un vrai scénario de film
  http://www.theregister.co.uk/2014/07/07/federal_intel_agency_staffer_allegedly_spied_on_nsa_inquiry_report/

Conférences

Passées

- Hack in Paris - 23 au 27 juin 2014 chez Mickey

A venir

- SSTIC 2014 - du 7 au 11 juillet 2014
  - **S**ummer **S**chool on **T**rends **i**n **C**omputing
    http://grammars.grlmc.com/sstic2014/

- HACK.LU - 21 au 24 octobre 2014
  - CFP ouvert jusqu'au 15 juillet
- ASFWS - 4 au 6 novembre 2014 en Suisse
  - **A**pplication **S**ecurity **F**orum **W**estern **S**witzerland
  - Une conférence co-organisée par Nicolas Ruff
    http://www.appsec-forum.ch/

- No Such Con - 19 au 21 novembre 2014 à Paris
- Bot Conf - 3 au 5 Décembre 2014 à ~~Nantes~~^w NANCY
- JSSI 2015 - 10 mars 2015 à Paris
  - Organisée par l'OSSIR

Divers / Trolls velus

Solution du challenge SSTIC 2014

http://communaute.sstic.org/ChallengeSSTIC2014

FireEye n’aime pas trop quand les problèmes sont chez eux

- @kmkz_security publie 8 failles sur un produit de fire eye sur exploit-db
- Fire eye les fait retirer et fait pression sur Sogeti pour renvoyer @kmkz_security…
- …et lance un challenge pour embaucher des hackers

http://pastebin.com/PWvU62tG
http://flare-on.com/

Divers / Trolls velus

Linkedin a encore du mal avec SSL

http://thehackernews.com/2014/06/millions-of-linkedin-users-at-risk-of.html
http://securityaffairs.co/wordpress/25892/hacking/linkedin-vulnerable-mitm.html

Savoir (bien?) gérer sa communication

- Selon "Le Point" : <<Lexsi, le premier cabinet de conseil en cybersécurité français>>
  http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/nsa-voici-l-arsenal-des-surveillants-et-quelques-pistes-pour-s-en-proteger-03-07-2014-1842879_506.php

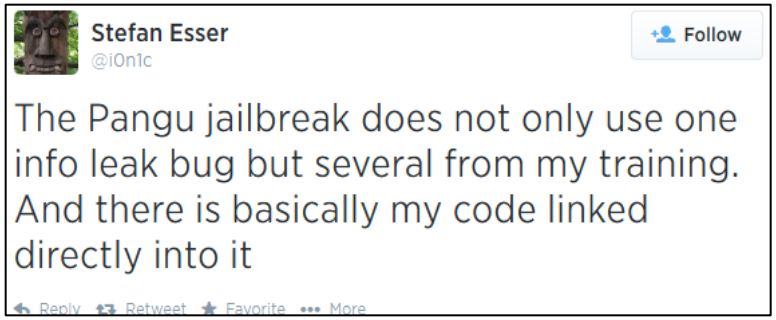
Portes ouvertes à l'ANSSI

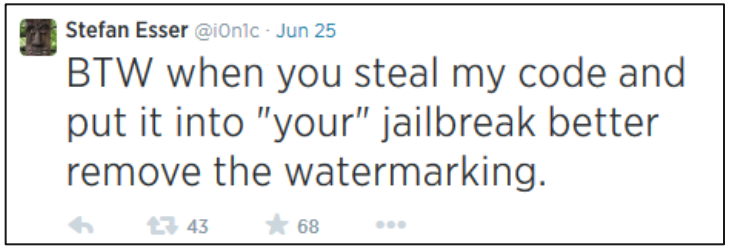
- C'était le 26 juin dernier
  http://www.aisg-univ-paris13.fr/uploaded/jpo-anssi-26-juin-2014.pdf

Divers / Trolls velus

Jailbreak iOS 7.1 : Chinois vs Stephen Esser

- *Esser* donne une formation à des chinois qui :
  - Lui piquent une 0-days iOS 7.1 et du code *(bugs inclus)*
  - Publient un jailbreak iOS 7.1 : Pangu
    - Accompagné d'un dépôt d'applications crackées (Installable "au choix")
- *Esser* s'énerve sur Twitter
  https://twitter.com/i0n1c/status/481923306371944450





- Réponse des Chinois :
  - Il n'y avait pas de NDA sur la formation

https://translate.google.fr/translate?hl=fr&sl=auto&tl=fr&u=http%3A%2F%2Fwww.zhihu.com%2Fquestion%2F24245064%2Fanswer%2F27190132

Divers / Trolls velus

Cherchez l'erreur...

Divers / Trolls velus

Google a de l'humour

- I'll be back

Prochaines réunions

Prochaines réunions

- Août
  - Congés, repos, soleil !

- Mardi 9 septembre 2014
  - Reprise

Afterwork

- Mardi 23 septembre
  - Réservé aux membres, ayant le droit d’inviter un non-membre

Questions ?