OSSIR
Groupe Paris

Réunion du 10 septembre 2013

Revue des dernières vulnérabilités

Nicolas RUFF
EADS-IW
nicolas.ruff (à) eads.net

Avis Microsoft

- **Juillet 2013**
  - **MS13-052 Failles .NET (x7) [1]**
    - **Affecte: .NET Framework (toutes versions supportées), Silverlight 5**
    - **Exploit: évasion de la *sandbox***
      - **http://weblog.ikvm.net/PermaLink.aspx?guid=50d94ff6-f418-42b4-8cc5-33996d0c7cf3**
    - **Crédits:**
      - **Ling Chuan Lee & Lee Yee Chan / F-13 Laboratory**
      - **Alon Fliess**
      - **James Forshaw / Context Information Security (x3)**
      - **Vitaliy Toropov**

Avis Microsoft

- MS13-053 Failles WIN32K.SYS (x8) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges locale
    - Corrige la "fameuse" faille découverte par Tavis Ormandy et exploitée dans la nature
    - http://blog.cmpxchg8b.com/2013/05/introduction-to-windows-kernel-security.html
  - Crédits:
    - Jon Butler & Nils / MWR Labs + ZDI
    - Alexander Chizhov / Dr.Web
    - Anonymous + ZDI
    - Ling Chuan Lee & Lee Yee Chan / F13 Laboratory
    - Yinliang / Tencent PC Manager
    - Mateusz "j00ru" Jurczyk / Google Inc
    - Wen Yujie & Guo Pengfei / Qihoo 360 Security Center

- MS13-054 Faille dans le rendu des polices TrueType (x1) [1]
  - Affecte: librairie GDI+ installée avec de nombreux produits
    - Windows (toutes versions supportées), Office < 2013, Lync 2010 et 2013, Visual Studio 2003, …
  - Exploit: élévation de privilèges lors du rendu d'une police TrueType
  - Crédits: Ling Chuan Lee & Lee Yee Chan / F13 Laboratory

Avis Microsoft

- MS13-055 Correctif cumulatif pour IE (x17) [1]
  - Affecte: IE 6 – IE 10
  - Exploit: exécution de code à l'ouverture d'une page Web malformée
    - http://blogs.technet.com/b/srd/archive/2013/07/10/running-in-the-wild-not-for-so-long.aspx
  - Crédits:
    - Ivan Fratric & Ben Hawkes / Google Security Team (x3)
    - SkyLined + ZDI
    - Simon Zuckerbraun + ZDI
    - Toan Pham Van + ZDI (x3)
    - Aniway.Anyway@gmail.com + ZDI
    - Bluesea + ZDI (x2)
    - Omair + ZDI
    - Anonymous + ZDI
    - e6af8de8b1d4b2b6d5ba2610cbf9cd38 + ZDI
    - Jose Antonio Vazquez Gonzalez + iDefense
    - Scott Bell / Security-Assessment.com
    - Masato Kinugawa
    - Mark Yason / IBM X-Force
    - Amol Naik + ZDI

Avis Microsoft

- MS13-056 Faille dans le support GIF par DirectShow (x1) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code à l'ouverture d'un fichier GIF malformé
    - http://kuronosec.blogspot.de/2013/07/directshow-arbitrary-memory-overwrite.html
  - Crédits: Andrés Gómez Ramírez

- MS13-057 Faille dans la support WMV (x1) [2]
  - Affecte: Windows Media Player
  - Exploit: exécution de code à l'ouverture d'une vidéo WMV malformée
  - Crédits: anonymous + ZDI

- MS13-058 Faille dans Windows Defender
  - Affecte: Windows 7 et 2008 R2
  - Exploit: élévation de privilèges locale
    - Guillemets manquants autour d'un chemin …
  - Crédits: Alton Blom / Reserve Bank of Australia

Avis Microsoft

Août 2013

- MS13-059 Correctif cumulatif pour IE (x11) [1]
  - Affecte: IE 6 – IE 10
  - Exploit: exécution de code à l'ouverture d'une page Web malformée
  - Crédits:
    - Peter 'corelanc0d3r' Van Eeckhoutte / Corelan + ZDI
    - Fermin J. Serna / Google Security Team
    - Arthur Gerkis + ZDI (x2)
    - Scott Bell / Security-Assessment.com (x2)
    - Ivan Fratric & Ben Hawkes / Google Security Team (x2)
    - Alex Inführ
    - Jose Antonio Vazquez Gonzalez + ZDI
    - Anonymous + ZDI
    - VUPEN + ZDI (exploitée à pwn2own)
      - http://seclists.org/bugtraq/2013/Aug/203

Avis Microsoft

- MS13-060 Faille dans le support des scripts Unicode (x1) [2]
  - Affecte: Windows XP et 2003
  - Exploit: élévation de privilèges
    - … si la police Bengali est installée
  - Crédits: Bob Clary / Mozilla

- MS13-061 Faille OWA (x3) [2]
  - Affecte: Exchange 2007, 2010 et 2013
  - Exploit: exécution de code lors de la prévisualisation de pièces jointes
    - … liée à la technologie "Oracle Outside"
    - Failles publiées par Oracle il y a plusieurs mois
  - Crédits: n/a

Avis Microsoft

- **MS13-062 Faille RPC (x1) [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges**
    - **"Race condition" exploitable pour "voler" une session RPC locale**
  - **Crédits: n/d**

- **MS13-063 Failles noyau (x4) [1]**
  - **Affecte: Windows (toutes versions supportées sauf Windows 8 x64, Windows 2012 et Windows RT)**
  - **Exploit:**
    - **Elévation de privilèges locale**
    - **Fuite d'information permettant de contourner ASLR**
  - **Crédits:**
    - **VUPEN Security + ZDI (exploitée à pwn2own)**
      - **http://seclists.org/bugtraq/2013/Aug/202**
    - **Yang Yu / Nsfocus Security Team**
    - **Mateusz "j00ru" Jurczyk / Google Inc (x2)**

Avis Microsoft

- **MS13-064 Faille dans le support NAT (x1) [3]**
  - **Affecte: Windows 2012**
  - **Exploit: déni de service via un paquet ICMP malformé**
  - **Crédits: n/d**

- **MS13-065 Faille dans le support ICMPv6 (x1) [3]**
  - **Affecte: Windows (toutes versions supportées sauf XP et 2003)**
  - **Exploit: déni de service distant**
  - **Crédits: Basil Gabriel / Symantec**

- **MS13-066 Faille dans AD FS (x1) [3]**
  - **Affecte: Windows (toutes versions "serveur" supportées)**
  - **Exploit: fuite d'information sur le compte de service utilisé**
    - **… permettant éventuellement de verrouiller ce compte**
  - **Crédits: n/d**

Avis Microsoft

- **Advisories**
  - **Q2755801**
    - **V14.0: mise à jour du lecteur Flash embarqué dans IE10+**
  - **Q2854544: renforcement de la gestion des certificats dans Windows**
    - **V1.1: ajout de nouveaux correctifs**
    - **V1.2: le correctif est disponible dans "Microsoft Update Catalog"**
  - **Q2861855: renforcement de l'authentification NLA avec RDP**
    - **V1.0: version initiale**
  - **Q2862973: les certificats racine ne peuvent plus utiliser MD5**
    - **V1.0: version initiale**
    - **V1.1: le correctif est disponible dans "Microsoft Update Catalog"**
  - **Q2876146: fuite d'information lorsque MS-CHAPv2 / PEAP est utilisé pour authentifier un Windows Phone sur un point d'accès WiFi malveillant**
    - **V1.0: version initiale**

Avis Microsoft

- **Prévisions pour Septembre 2013**
  - **14 failles (4 critiques, 10 importants)**
- **Failles à venir**
- **Retour sur des failles antérieures**
  - **Exploitation des "race conditions" difficiles**
    - **Ex. MS13-016**
      - **http://gynvael.coldwind.pl/?id=509**
      - **http://j00ru.vexillium.org/?p=1880**

Avis Microsoft

- **Révisions**
  - **MS11-007**
    - **V2.1: changement dans la logique de détection**
  - **MS11-043**
    - **V2.2: changement dans la logique de détection**
  - **MS11-076**
    - **V1.1: changement dans la logique de détection**
  - **MS12-006**
    - **V1.2: changement dans la logique de détection**
  - **MS12-036**
    - **V1.3: changement dans la logique de détection**
  - **MS12-048**
    - **V1.1: changement dans la logique de détection**
  - **MS12-049**
    - **V1.1: changement dans la logique de détection**
  - **MS12-054**
    - **V2.2: changement dans la logique de détection**
  - **MS12-056**
    - **V1.1: changement dans la logique de détection**
  - **MS12-082**
    - **V1.2: changement dans la logique de détection**
  - **MS13-006**
    - **V1.2: changement dans la logique de détection**
  - **MS13-027**
    - **V1.2: changement dans la logique de détection**

Avis Microsoft

- MS13-052
  - V2.0: re-publication de la mise à jour
- MS13-054
  - V1.1: changement dans la logique de détection
  - V1.2: changement dans la logique de détection
- MS13-055
  - V1.1: existence d'attaques ciblées contre IE8
  - V1.2: correction documentaire
- MS13-057
  - V2.0: re-publication de la mise à jour
  - V3.0: re-publication de la mise à jour
- MS13-061
  - V2.0: re-publication de la mise à jour
  - V3.0: re-publication de la mise à jour
- MS13-063
  - V1.1: ajout d'un problème connu
- MS13-066
  - V2.0: suppression du correctif pour cause de problème majeur
  - V2.1: corrections documentaires
  - V3.0: re-publication de la mise à jour

Infos Microsoft

- **Sorties logicielles**
  - **Office 2010 SP2**
  - **Windows 8.1 RTM**
    - **Disponibilité officielle: 18 octobre**
  - **IE 11**
    - **Disponible avec Windows 8.1 et backporté sur Windows 7**
  - **Windows 2012 R2, System Center 2012 R2, …**
    - **Disponibilité officielle: 18 octobre**
  - **Office Mobile sur Android**
    - **Désormais disponible en France**
    - **Réservé aux clients Office 365**

Infos Microsoft

- **Autre**
  - **Microsoft rachète entièrement Nokia**
  - **Steve Ballmer ne sera plus là dans 1 an**
    - **En cause: l'échec commercial de Surface ?**
      - **http://www.nextmicrosoftceo.com/**
  - **Windows Phone ne synchronise plus les comptes Google**
      - **http://www.engadget.com/2013/07/31/psa-windows-phone-google-sync/**
  - **Surface RT est mort, vive Surface 2**
      - **http://www.linformaticien.com/actualites/id/30185/la-surface-2-remplacera-la-surface-rt.aspx**
  - **Windows 8.1 n'est disponible pour personne (y compris les abonnés MSDN)**
      - **http://www.theverge.com/2013/8/27/4663074/microsoft-announces-windows-8-1-rtm**
    - **… sauf en Torrent**
      - **http://forums.mydigitallife.info/threads/47388-LEAK-Windows-8-1-Enterprise-X64-zh-CN**

Infos Microsoft

- Microsoft fournit à la NSA tout le contenu disponible sur Hotmail, Outlook.com, SkyDrive et Skype
  - http://yro.slashdot.org/story/13/07/11/2041244/ms-handed-nsa-access-to-encrypted-chat-email
- Le programme MAPP étendu
  - Nouveau: "Responder" et "Scanner"
    - http://blogs.technet.com/b/msrc/archive/2013/07/29/announcing-the-2013-msrc-progress-report-featuring-mapp-expansions.aspx
- Les applications mobiles vulnérables non corrigées seront retirées des Marketplaces après 180 jours
  - http://www.scmagazine.com/microsoft-invokes-six-month-deadline-to-replace-vulnerable-mobile-apps/article/302321/
- BlueHat Challenge
  - Pour gagner un T-Shirt virtuel
    - … ou un job chez MS ☺
      - http://blogs.technet.com/b/srd/archive/2013/07/31/the-bluehat-challenge.aspx

Infos Microsoft

- Des failles découvertes dans IE11 suite au Bug Bounty
  - … par un employé Google
    - http://www.zdnet.fr/actualites/vulnerabilite-microsoft-recompense-financierement-un-salarie-de-google-39792441.htm
- Les serveurs Teredo vont s'éteindre
    - https://isc.sans.edu/diary/Microsoft+Teredo+Server+%22Sunset%22/16153
- SkyDrive Pro passe à 25 Go
    - http://www.engadget.com/2013/08/27/microsoft-boosts-base-skydrive-pro-storage-to-25gb/
- Le procès du vol du code source de Skype … jugé au tribunal de Caen
    - http://www.pcinpact.com/news/82083-le-proces-diffusion-sources-skype-souvre-en-france.htm
- Bing vous prévient si vous faites une recherche pédophile
    - http://searchenginewatch.com/article/2285542/Bing-Adds-Pop-Up-Child-Abuse-Warnings-to-UK-Searchers

Infos Réseau

- **(Principales) faille(s)**
  - **Cisco …**
    - **CUCM: injection(s) SQL pre-auth**
      - **Présentée à SSTIC 2013**
        - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130717-cucm**
        - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130821-cucm**
    - **ACS: injection de commandes dans l'identité EAP-FAST (!)**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130828-acs**
    - **… et plein d'autres**
  - **Améliorations techniques pour l'empoisonnement DNS**
    - **http://www.bortzmeyer.org/dns-attaques-shulman.html**

Infos Réseau

- **Autres infos**
  - **Cisco rachète SourceFire ($2,7 milliards)**
    - http://news.slashdot.org/story/13/07/23/1331244/cisco-to-acquire-sourcefire-for-27-billion
  - **.GOV temporairement indisponible**
    - **… à cause d'un problème DNSSEC**
      - https://isc.sans.edu/diary/.GOV+zones+may+not+resolve+due+to+DNSSEC+problems./16367
  - **ICANN refuse le .amazon**
    - **Sous la pression de l'Amérique du Sud**
      - http://pro.clubic.com/it-business/nom-de-domaine/actualite-573204-gtld-icann-refuse-extension-domaine-amazon.html
  - **OVH offre une protection totale contre les DDoS**
    - **Hmm …**
      - http://www.pcinpact.com/news/81703-ovh-protection-ddos-capable-d-encaisser-nimporte-quelle-attaque.htm
  - **Perquisition chez Orange, Deutsche Telekom et Telefonica**
    - **La commission européenne cherche les accords de peering**
      - http://www.journaldunet.com/ebusiness/telecoms-fai/perquisition-orange-peering-0713.shtml

Infos Unix

- (Principales) faille(s)
  - Elévation de privilèges locale sur Debian/Ubuntu
    - Fonctionne avec vmware_mount (mais potentiellement d'autres binaires setuid)
      - http://blog.cmpxchg8b.com/2013/08/security-debianisms.html
      - http://www.vmware.com/security/advisories/VMSA-2013-0010.html
  - Faille Struts 2.0.0 – 2.3.15
    - http://struts.apache.org/release/2.3.x/docs/s2-016.html
  - Kernel panic … à l'insertion d'un clavier
    - Trouvé avec un Facedancer
      - http://marc.info/?l=linux-input&m=1377721805146 08&w=1

Infos Unix

- **Autres infos**

  - **GCC transforme les boucles for() en appel à memcpy()**
    - **Quand applicable**
      - **http://gcc.gnu.org/bugzilla//show_bug.cgi?id=56888**

  - **Apache supporte DH 2048+**
    - **Requis pour l'évaluation EAL4+**
      - **https://issues.apache.org/bugzilla/show_bug.cgi?id=49559**

Failles

- **Principales applications**
  - **Firefox < 23.0.1**
  - **Putty < 0.63**
    - **http://www.chiark.greenend.org.uk/~sgtatham/putty/**
  - **Java < 1.7.25**
    - **http://packetstormsecurity.com/files/122777/**
    - **http://packetstormsecurity.com/files/122806/**
    - **http://packetstormsecurity.com/files/122865/**
    - **http://packetstormsecurity.com/files/122980/**

Failles

- Faille dans le microcode Intel (Core i3/i5/i7et Xeon)
  - Probablement exploitables …
    - https://launchpad.net/debian/+source/intel-microcode/1.20130808.2

- L'OTAN publie quelques 0day

- McAfee ePO
  - http://www.securityfocus.com/archive/1/527228/30/0/threaded

- BMC Service Desk
  - http://www.securityfocus.com/archive/1/527229/30/0/threaded

Failles

- Autres
  - VLC vs. Secunia
    - http://www.jbkempf.com/blog/post/2013/More-lies-from-Secunia
  - Le prix des failles d'envole sous la pression des gouvernements
    - http://www.lemagit.fr/actualites/2240201609/Failles-un-marche-noir-dope-par-limplication-des-gouvernements
  - La faille McAfee ePO activement exploitée dans la nature
    - https://www.us-cert.gov/ncas/alerts/TA13-193A
  - Intel MPX (Memory Protection Extensions)
    - Détecte les buffer overflow
      - http://software.intel.com/en-us/articles/introduction-to-intel-memory-protection-extensions

Failles 2.0

- Yahoo! va "libérer" les comptes inactifs depuis plus d'un an
  - http://blog.zoller.lu/2013/07/an-prime-example-at-bad-thread-modeling.html
- Comment prouver que Facebook est vulnérable ?
  - En piratant le compte de Mark Zuckerberg
    - http://khalil-sh.blogspot.ru/p/facebook_16.html
    - http://www.gofundme.com/3znhjs
- Le "Bug Bounty" Facebook a déjà coûté … $1m
  - http://www.engadget.com/2013/08/03/facebook-bug-bounty/
- La plupart des portefeuilles Bitcoin sur Android vulnérables
  - En cause: le nombre aléatoire utilisé pour la signature ECDSA des transactions
    - java.security.SecureRandom peut générer deux fois la même valeur
      - http://bitcoinmagazine.com/6251/critical-vulnerability-found-in-android-wallets/
- FBI: "Anonymous est neutralisé"
  - http://www.mag-securs.com/News/tabid/62/id/33185/Le-FBI-declare-avoir-reussi-a-neutraliser-le-groupe-Anonymous.aspx

Failles 2.0

- BlackBerry envoie les logins/mots de passe POP/IMAP à RIM
  - http://yro.slashdot.org/story/13/07/18/1249236/blackberry-10-sends-full-email-account-credentials-to-rim
  - Note: c'est logique pour bénéficier du PUSH
    - http://forums.crackberry.com/native-blackberry-os-apps-f152/how-does-bis-email-work-152955/
- Les autorités indiennes ont accès au trafic BlackBerry
  - http://www.theregister.co.uk/2013/07/11/blackberry_gives_indian_spooks_access/
- Backdoor dans "US Emergency Alert System"
  - Clé "SSH" en dur
  - Résultat: une attaque de zombies annoncée dans le Montana
    - http://www.ioactive.com/pdfs/IOActive_DASDEC_vulnerabilities.pdf
- L'ampoule Philips HUE piratée
  - http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html
- Les laptops HP EliteBook 8460p retransmettent les bruits ambiants sur un porteuse à 24 MHz
  - http://www.reddit.com/r/RTLSDR/comments/1le3if/so_i_discovered_that_my_hp_laptop_leakstransmits/

Sites piratés

- Les pannes informatiques (liste partielle)
  - Explication de la panne Chorus
    - http://www.lemagit.fr/technologie/datacenter-technologie/architectures-datacenters/2013/06/27/arret-de-chorus-les-raisons-de-la-panne-du-datacenter-de-bull/
  - La banque postale
    - http://www.leparisien.fr/economie/votre-argent/la-banque-postale-perturbee-par-un-probleme-informatique-30-07-2013-3018517.php
  - Hôpital Robert Boulin
    - http://www.sudouest.fr/2013/07/18/panne-informatique-a-l-hopital-robert-boulin-1118085-2966.php
  - Amazon en panne
    - 2 fois dans la semaine
      - http://www.01net.com/editorial/601760/deuxieme-panne-en-une-semaine-pour-amazon/

- Les sites piratés du mois (liste partielle)
  - Apple Dev Center
    - http://techcrunch.com/2013/07/21/apple-confirms-that-the-dev-center-has-potentially-been-breached-by-hackers/
    - Notez le "*potentially*"
      - http://www.youtube.com/watch?v=q000_EOWy80&feature=youtu.be
  - OVH
    - http://travaux.ovh.net/?do=details&id=8998

Sites piratés

- Ubuntuforums.org (1,8M comptes)
  - Excellente lecture
    - http://blog.canonical.com/2013/07/30/ubuntu-forums-are-back-up-and-a-post-mortem/
- Forum de discussion du NASDAQ
    - http://magazine.qualys.fr/menaces-alertes/communaute-nasdaq-compromis/
- Site Web de Toyota
    - http://blogs.wsj.com/japanrealtime/2013/06/19/hackers-break-into-toyota-server/
- Déni de service contre Network Solutions (DNS)
    - http://www.journaldunet.com/solutions/dsi/network-solutions-tombe-0713.shtml
- Le sysadmin vendait des backdoors dans ses propres réseaux
    - http://arstechnica.com/security/2013/08/hacker-pleads-guilty-to-charges-he-sold-magic-passwords-to-sensitive-networks/

- Syrian Electronic Army (SEA)
  - Les domaines New York Times, Twitter, Huffington Post
    - http://thehackernews.com/2013/08/Syrian-Electronic-Army-New-York-Times-hacked.html
  - Tango (1,5 To)
    - Via une faille WordPress
      - http://www.theregister.co.uk/2013/07/23/tango_chat_smackdown/
  - TrueCaller (450 Go)
    - http://thehackernews.com/2013/07/Truecaller-hacked-database-leaked.html

Malwares, spam et fraudes

- L'EDA ne rigole pas avec les APT
  - $170,000 de matériel détruit au pilon après une intrusion
  - … incluant claviers, souris …
    - http://it.slashdot.org/story/13/07/09/1330201/got-malware-get-a-hammer
- Un botnet met son C&C dans Tor
    - http://threatpost.com/huge-botnet-found-using-tor-network-for-communications/102179
- Observatoire de la Sécurité des Cartes de Paiement
  - Le nombre de terminaux de paiement compromis a plus que doublé en 2012
    - http://www.banque-france.fr/observatoire/rap_act_fr_12.htm
- 160m de numéros de cartes volés
  - Chez Nasdaq, Carrefour, Dexia, …
  - 5 personnes arrêtées
    - http://www.journaldemontreal.com/2013/07/25/cinq-personnes-inculpees-pour-avoir-pirate-160-millions-de-carte-de-credit
- Le Bitcoin illégal en Thaïlande
    - http://www.zdnet.fr/actualites/le-bitcoin-illegal-en-tha-lande-39792836.htm
- Perfect Money remplace Liberty Reserve

Actualité (francophone)

- La loi de programmation militaire va obliger les entreprises "sensibles" à se protéger
  - Déclaration des incidents
  - Sonde de l'ANSSI
  - Etc.
    - http://lexpansion.lexpress.fr/high-tech/exclusif-cybersecurite-une-loi-pour-contraindre-les-entreprises-a-mieux-se-proteger_394903.html

- CNIL
  - Télédéclaration des pertes de données personnelles
    - http://www.cnil.fr/nc/linstitution/actualite/article/article/notifications-de-violation-de-donnees-personnelles-une-nouvelle-teleprocedure/
  - Conclusion sur les cartes bleues sans contact
    - http://www.cnil.fr/linstitution/actualite/article/article/securite-des-cartes-bancaires-sans-contact-quelles-sont-les-avancees-et-les-ameliorations-pos/

- Info / escroqueries en lignes
  - Préfecture du Cher
    - http://www.slideshare.net/slideshow/embed_code/24294488

Actualité (francophone)

- **Les plans de la DGSE sur le Web**
  - **http://bugbrother.blog.lemonde.fr/2013/08/21/le-systeme-anti-intrusion-de-la-dgse-etait-sur-le-web/**
- **RENATER passe sous Zimbra**
  - **http://pro.01net.com/editorial/597805/lachat-patriotique-il-y-a-ceux-qui-en-parlent-et-il-y-a-ceux-qui-le-sapent/**
- **Zythom n'a pas été recruté par l'ANSSI**
  - **http://zythom.blogspot.fr/2013/08/lanssi-et-le-test-google.html**

Actualité (anglo-saxonne)

- iGuardian
  - Un site du FBI pour signaler (et partager) les intrusions informatiques
    - http://www.csoonline.com/article/737669/fbi-s-new-iguardian-portal-aims-to-ease-cyber-crime-reporting
- BugCrowd lève $1,6m
  - Pour acheter des failles
    - http://www.forbes.com/sites/andygreenberg/2013/09/04/startup-bugcrowd-raises-1-6-million-to-pay-hacker-hordes-to-hunt-clients-bugs/
- L'administration américaine priée de ne plus acheter Lenovo
  - … pour cause de "backdoors"
    - http://www.theregister.co.uk/2013/07/29/lenovo_accused_backdoors_intel_ban/

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (1/4)**
  - **Crypto: la NSA …**
    - **http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1&**
  - **… installe des *backdoors* logicielles et matérielles**
    - **Avec ou sans la coopération des entreprises**
  - **… influence les standards**
    - **Ex. choix des courbes elliptiques du NIST**
  - **… demande les clés privées aux fournisseurs**
    - **http://news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys/**
  - **… a réalisé des "progrès cryptographiques majeurs"**
    - **http://www.wired.com/threatlevel/2013/08/black-budget/**
  - **… par exemple en "cassant" RC4 (?)**
    - **http://www.theregister.co.uk/2013/09/06/nsa_cryptobreaking_bullrun_analysis/**

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (2/4)**
  - La NSA …
    - … surveille tout Internet
      - Programme Xkeyscore
        - http://www.zdnet.com/prism-heres-how-the-nsa-wiretapped-the-internet-7000016565/
    - … a piraté la visioconférence de l'ONU
        - http://www.numerama.com/magazine/26820-la-nsa-a-pirate-la-visioconference-interne-de-l-onu.html
      - Après les chinois (!)
        - http://rt.com/news/nsa-us-un-germany-snowden-964/
    - … a piraté le réseau des ambassades françaises
        - http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf
    - … ainsi que des représentations européennes
        - http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html
    - … contrôle 85,000 machines après 231 opérations d'infiltration (en 2011)
        - http://mobile.lemonde.fr/technologies/article/2013/08/31/les-renseignements-americains-auraient-lance-231-cyberattaques-en-2011_3469431_651865.html
    - … préfère pirater les équipements de routage que les *endpoints*
        - http://www.wired.com/threatlevel/2013/09/nsa-router-hacking/
    - … dépense $25m/an pour acheter des failles
        - http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/
    - … joue la transparence … ou pas
        - http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (3/4)**
  - **Les autres agences américaines sont jalouses de la NSA**
    - **http://www.lemonde.fr/technologies/article/2013/08/04/surveillance-les-autres-agences-americaines-jalouses-de-la-nsa_3457284_651865.html**
  - **Il existe encore plus secret que la NSA**
    - **http://www.washingtonpost.com/world/national-security/black-budget-leaked-by-edward-snowden-gives-details-of-agencies-beyond-cia-nsa/2013/08/29/a7f20890-10f0-11e3-bdf6-e4fc677d94a1_story.html**
  - **Le compagnon d'un journaliste du Guardian arrêté pour "atteinte à la sécurité nationale du Royaume Uni"**
    - **http://www.lemonde.fr/technologies/article/2013/08/30/nsa-le-compagnon-de-greenwald-detenait-58-000-documents-secrets-lors-de-son-arrestation_3469229_651865.html**
  - **Le DLP selon la NSA**
    - **La NSA va remplacer 90% de ses informaticiens par des machines**
      - **http://www.01net.com/editorial/601057/affaire-snowden-la-nsa-va-remplacer-90pour-cent-de-ses-informaticiens-par-des-robots/**

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin … (4/4)**
  - **Lavabit et Silent Circle ferment du jour au lendemain**
    - **http://www.groklaw.net/article.php?story=20130818120421175**
  - **Le gouvernement indien interdit l'utilisation de services américains**
    - **http://www.zdnet.fr/actualites/prism-les-fonctionnaires-indiens-pries-de-renoncer-aux-services-mails-us-39793552.htm**
  - **La FIDH et la Ligue des Droits de l'Homme portent plainte contre X**
    - **http://lexpansion.lexpress.fr/high-tech/affaire-prism-plainte-en-france-contre-google-apple-facebook-et-microsoft_394002.html**
  - **Des parodies …**
    - **http://getprsm.com/**
  - **… et du ransomware**
    - **https://twitter.com/kafeine/status/371716133323153408**

Actualité (anglo-saxonne)

- Source
  - https://twitter.com/stefLP/status/355404484614168576

Actualité (Google)

- Google en panne pendant 11 minutes
  - Le nombre de pages Web vues chute de 40%
    - https://engineering.gosquared.com/googles-downtime-40-drop-in-traffic
- Google n'obtient pas le TLD "." auprès de l'ICANN ☺
  - http://tech.slashdot.org/story/13/08/31/045225/dotless-domain-names-prohibited-icann-tells-google
- La signature de code sur Android contournée
  - A cause d'un "integer overflow"
    - http://blog.sina.com.cn/s/blog_be6dacae0101bksm.html
- La résistance s'organise contre les Google Glasses
  - http://stopthecyborgs.org/
- De la passion, du drame sur le campus de Google
  - http://www.linformaticien.com/actualites/id/30094/sergey-amanda-et-hugo-google-se-lance-dans-le-vaudeville.aspx
- Android 4.4 a pour nom de code … "Kit Kat"
  - http://www.bbc.co.uk/news/technology-23926938

Actualité (Apple)

- Pages, Numbers et Keynote en version beta sur iCloud
- Open Source Jailbreak Framework
  - https://openjailbreak.org/
- *Pear is like Apple*
  - Mais c'est un Linux ☺
    - http://pearlinux.fr/
- Elévation de privilèges sous Mac OS X
  - sudo -k;systemsetup -setusingnetworktime Off -settimezone GMT -setdate 01:01:1970 -settime 00:00;sudo su
    - https://twitter.com/superevr/status/372896646503202816
- Une séquence de caractères qui "plante" toutes les applications Apple
  - Fonctionne aussi en SSID
    - \xD8\xAE \xCC\xB7\xCC\xB4\xCC\x90\xD8\xAE

Actualité (Apple)

- Source
  - https://twitter.com/iGrumZ/status/363224317573623808

Actualité (crypto)

- Tor vulnérable
  - Failles dans le plugin Firefox, localisation des services cachés …
    - https://blog.torproject.org/category/tags/freedom-hosting
    - https://blog.torproject.org/blog/tor-security-advisory-old-tor-browser-bundles-vulnerable
  - Et ça marche
    - http://www.reddit.com/r/onions/comments/1jmrta/founder_of_the_freedom_hosting_arrested_held/
- MEGA vulnérable
    - http://nzkoz.github.io/MegaPWN/
- Biclique vs. AES
  - AES-128 reste $2^{126.1}$
    - https://lirias.kuleuven.be/bitstream/123456789/314284/1/aesbc.pdf
- Une nouvelle technique d'obfuscation de code
  - Cryptographiquement sûre
    - http://newsroom.ucla.edu/portal/ucla/ucla-computer-scientists-develop-247527.aspx
- L'entropie de Shannon n'est pas une bonne mesure pour la sécurité d'un algorithme cryptographique
  - Il faut prendre en compte le pire cas
    - http://web.mit.edu/newsoffice/2013/encryption-is-less-secure-than-we-thought-0814.html
- H^2 (et donc HMAC) est moins sûr que H
    - http://eprint.iacr.org/2013/382

Actualité

- Conférences passées
  - BH US / DefCon 2013
    - Barnaby Jack retrouvé mort dans sa chambre d'hôtel
      - http://www.lemonde.fr/disparitions/article/2013/07/29/mort-du-hacker-barnaby-jack-detrousseur-de-distributeur_3454728_3382.html
    - Faille dans la signature des APK
    - Gestion des SIM OTA chiffrée avec DES
      - https://srlabs.de/rooting-sim-cards/
      - http://nakedsecurity.sophos.com/2013/07/22/rooting-sim-cards-blackhat-speaker-says-he-may-be-able-to-own-your-phone-with-a-text-message/
    - BB 10
      - http://threatpost.com/inside-the-security-model-of-blackberry-10/101542
    - BREACH vs. SSL
      - http://breachattack.com/
    - Pass the Hash et cartes à puce
      - https://www.blackhat.com/us-13/archives.html#Duckwall
    - "Pixel Perfect Timing Attacks"
      - https://media.blackhat.com/us-13/US-13-Stone-Pixel-Perfect-Timing-Attacks-with-HTML5-WP.pdf

Actualité

- Pwnie Awards
  - Best server-side bug: Ruby-on-Rails YAML
  - Best client-side bug: Adobe Reader sandbox escape
  - Best privilege escalation bug: iOS jailbreak
  - Most innovative research: identifying and exploiting Windows kernel race conditions
  - Best song: "all the things"
  - Epic fail: Hakin9 / D.I.C.K.S.
  - Epic 0wnage: Edward Snowden
  - Lifetime achievement: Barnaby Jack

Actualité

- Conférences passées
  - RMLL 2013
  - OHM 2013
    - Attaque sur les firmwares de disques durs
      - http://spritesmods.com/?art=hddhack
    - (évoquée à SSTIC 2013)
  - RECon 2013
      - http://recon.cx/2013/slides/

- Conférences à venir
  - Hack.Lu 2013
  - GreHack 2013
  - BotConf 2013
      - https://www.botconf.eu/index.php/programme-preliminary/
  - HITB 2014 Amsterdam
    - Tous les "keynote speakers" sont des femmes ☺
      - http://www.dailydot.com/news/hacking-conference-haxpo-female-keynote/

Actualité

- **Sorties logicielles**
  - **Hydra 7.5**
  - **Pac4Mac 0.1**
    - **Un cadriciel d'inforensique (déjà présenté à l'OSSIR)**
      - **http://sud0man.blogspot.fr/2013/09/pac4mac-forensics-framework-for-mac-os.html**
  - **ICQ pour Mac OS X (!)**
      - **http://www.pcinpact.com/breve/81066-icq-signe-retour-dans-mac-app-store-dos-x.htm**
  - **SMS Perseus**
    - **Parfait pour tester vos analyseurs statiques**
      - **https://code.google.com/p/libperseus/downloads/list**

Actualité

- *What could possibly go wrong?*
  - Paiement par reconnaissance faciale
    - http://www.numerama.com/magazine/26539-une-startup-teste-le-paiement-par-reconnaissance-faciale.html
- L'électrocardiogramme pour remplacer les mots de passe
    - http://threatpost.com/watch-like-heartbeat-monitor-seeks-to-replace-passwords/102192
- Nouvelle idée du marketing
  - La poubelle espionne
    - http://www.generation-nt.com/poubelle-wifi-londres-protection-donnees-smartphone-renew-actualite-1773322.html
- Comment disparaitre d'Internet ?
  - Pas facile/possible partout …
    - http://justdelete.me/
- La DRM arrive sur les imprimantes 3D
    - http://torrentfreak.com/3d-printing-drm-aims-to-stop-next-gen-pirates-130827/
- La Russie invite ses hackers à ne plus voyager à l'étranger
  - Surtout ceux qui sont recherchés par le FBI ☺
    - http://www.wired.com/threatlevel/2013/09/dont-leave-home/
- Un pentest qui démarre par Amazon Wish List
    - http://www.cbsnews.com/8301-205_162-57600158/amazon-wish-list-is-gateway-to-epic-social-engineering-hack/

Actualité

- **Georgia Weidman accuse Fernando Gont de tentative de viol**
  - **http://georgiaweidman.com/wordpress/guess-you-thought-i-was-someone-to-mess-with/**
- **Une "pierre espionne" en vente sur eBay**
  - **Prototype Lockheed Martin**
  - **Mise à prix: $10m …**
    - **http://www.ebay.com/itm/Prototype-Hardware-from-Lockheed-Martin-Surveillance-Project-/221272094476**
- **Xiaomi, le futur Apple chinois**
  - **http://techcrunch.com/2013/08/28/xiaomi-what-americans-need-to-know/**

Actualité

- **Le problème de la compression JPEG ?**
  - **Testé sur copieurs Xerox**
    - **http://www.dkriesel.com/en/blog/2013/0802_xerox-workcentres_are_switching_written_numbers_when_scanning**

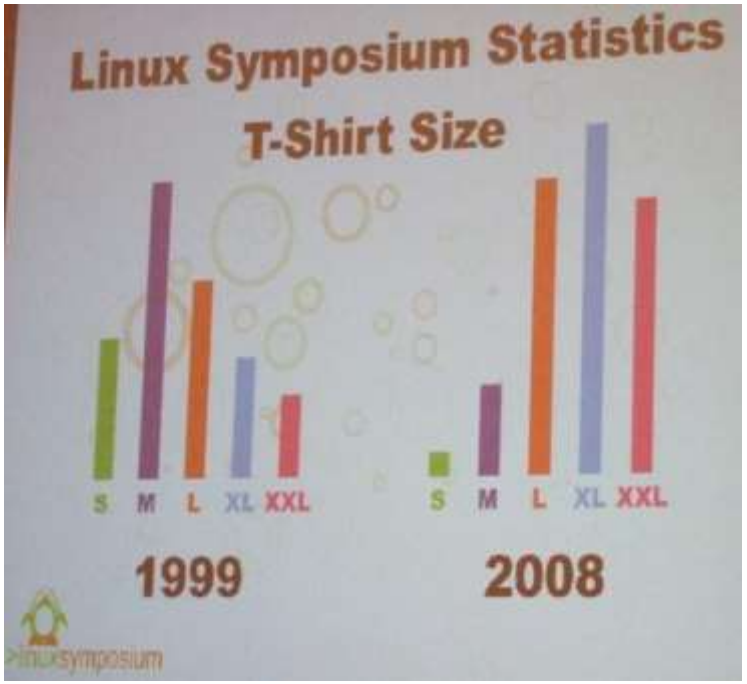
Before		After	
110.000	54,60	110.000	54,80
125.000	60,00	125.000	60,00
140.000	65,40	140.000	85,40
155.000	70,80	155.000	70,80
170.000	76,20	170.000	76,20

Divers

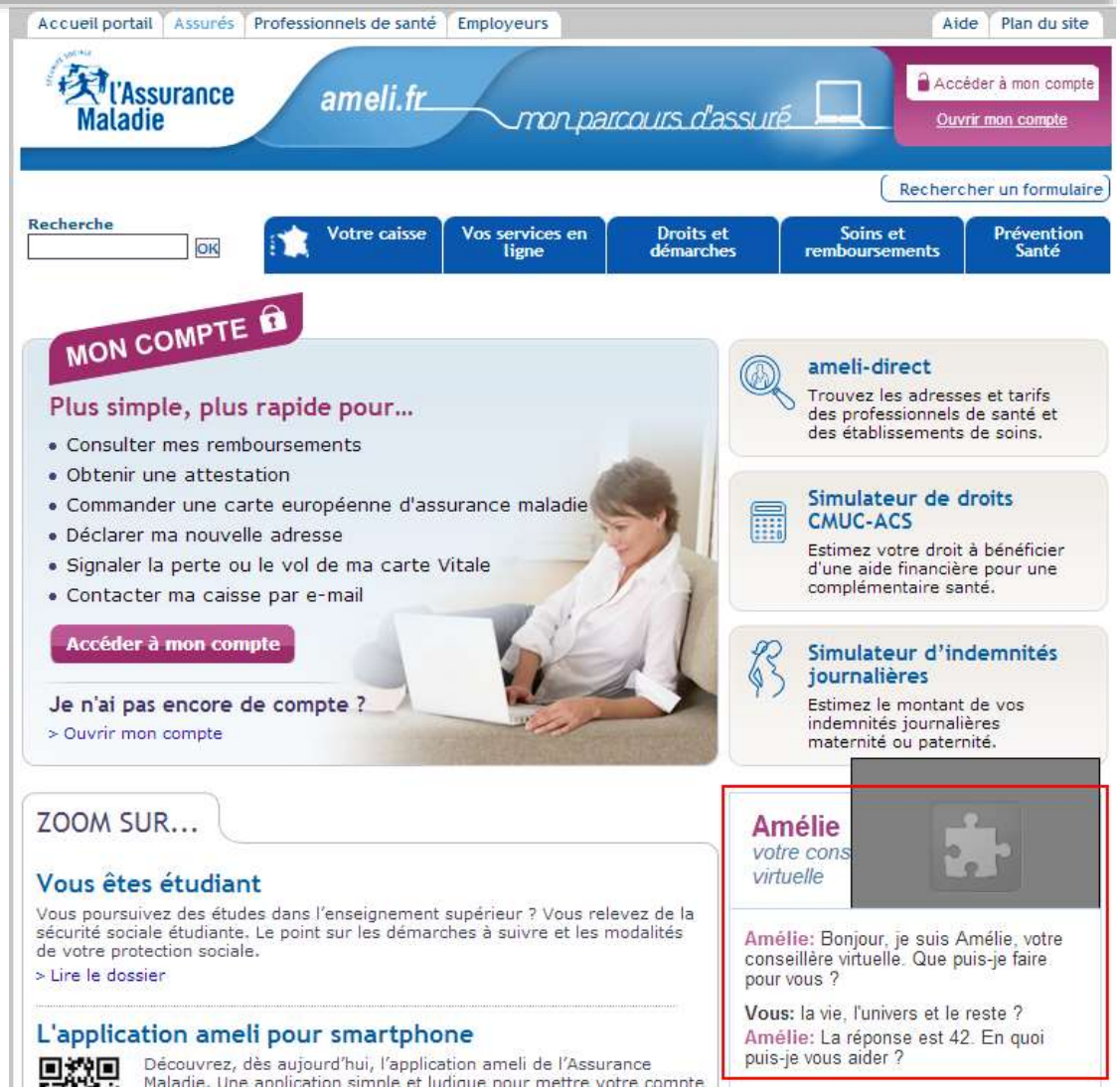
- **Un nouveau service en ligne**
  - **Dupliquer ses clés depuis une photo**
    - **http://keysduplicated.com/**
- **La seule chose qui ne devrait pas être vulnérable**
    - **https://www.trustwave.com/spiderlabs/advisories/TWSL2013-020.txt**
- **Goldman Sachs ne comprend pas bien la GPL**
    - **http://blog.garrytan.com/goldman-sachs-sent-a-brilliant-computer-scientist-to-jail-over-8mb-of-open-source-code-uploaded-to-an-svn-repo**
- **PHP reste un échec**
    - **http://www.reddit.com/r/PHP/comments/1l7baq/creating_a_user_from_the_web_problem/**
- **Amazon teste son réseau satellitaire**
    - **http://www.usine-digitale.fr/article/bientot-un-reseau-internet-par-satellite-dedie-pour-amazon.N203171**
- ***Better safe than sorry***
    - **http://www.gooze.eu/forums/support/security-announcement-for-gooze-oath-tokens**
    - **http://www.gooze.eu/forums/support/building-gooze-bunker-zero-faraday-cage**

Divers

- Les développeurs Open Source ?
  - Dépressifs
    - http://www.reddit.com/r/programming/comments/1kq06v/developers_and_depression_a_talk_from_steel_ruby/
  - … et gros
    - https://twitter.com/kapravel/status/375431377333653504/photo/1/large

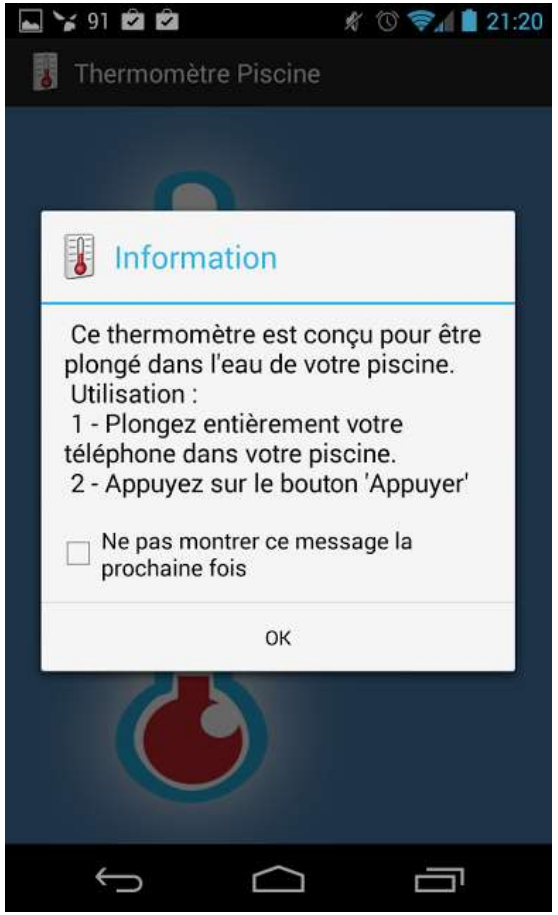


Divers


Accueil portail
Assurés
Professionnels de santé
Employeurs
Aide
Plan du site
l'Assurance Maladie
ameli.fr
mon parcours d'assuré
Accéder à mon compte
Ouvrir mon compte
Rechercher un formulaire
Recherche
OK
Votre caisse
Vos services en ligne
Droits et démarches
Soins et remboursements
Prévention Santé
MON COMPTE
Plus simple, plus rapide pour...
Consulter mes remboursements
Obtenir une attestation
Commander une carte européenne d'assurance maladie
Déclarer ma nouvelle adresse
Signaler la perte ou le vol de ma carte Vitale
Contacter ma caisse par e-mail
Accéder à mon compte
Je n'ai pas encore de compte ?
> Ouvrir mon compte
ameli-direct
Trouvez les adresses et tarifs des professionnels de santé et des établissements de soins.
Simulateur de droits CMUC-ACS
Estimez votre droit à bénéficier d'une aide financière pour une complémentaire santé.
Simulateur d'indemnités journalières
Estimez le montant de vos indemnités journalières maternité ou paternité.
ZOOM SUR...
Vous êtes étudiant
Vous poursuivez des études dans l'enseignement supérieur ? Vous relevez de la sécurité sociale étudiante. Le point sur les démarches à suivre et les modalités de votre protection sociale.
> Lire le dossier
L'application ameli pour smartphone
Découvrez, dès aujourd'hui, l'application ameli de l'Assurance
Amélie
votre cons
virtuelle
Amélie: Bonjour, je suis Amélie, votre conseillère virtuelle. Que puis-je faire pour vous ?
Vous: la vie, l'univers et le reste ?
Amélie: La réponse est 42. En quoi puis-je vous aider ?

Divers

- **Source**
  - **https://pbs.twimg.com/media/BSWkyesCIAApWTV.png:large**



Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 8 octobre 2013
- Prochain AfterWork
  - Mardi 22 octobre 2013
    - "Projet Ivy" (Fred Raynal / Quarkslab)
- Prochaine JSSI
  - Lundi 17 mars 2014
  - Profitez du combiné avec les GS-Days le mardi 18 mars
- N'hésitez pas à proposer des sujets et/ou des salles