OSSIR
Groupe Paris

Réunion du 11 décembre 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Novembre 2012**

  - **MS12-071 Failles IE 9 (x3) [1,1,1]**
    - **Affecte: IE 9**
    - **Exploit:**
    - **Crédit:**
      - **Jose A. Vazquez / spa-s3c.blogspot.com + iDefense (x2)**
      - **Cheng-da Tsai, Sung-ting Tsai, Ming-chieh Pan / Trend Micro**

  - **MS12-072 Failles dans Windows Shell (x2) [1,1]**
    - **Affecte: Windows (toutes versions supportées sauf Core, RT et Itanium)**
    - **Exploit: integer overflow / underflow dans le support des fichiers briefcase**
    - **Crédit: Tal Zeltzer / VeriSign**

Avis Microsoft

- MS12-073 Fuite d'information dans IIS (x2) [?,?]
  - Affecte: serveur FTP (IIS 7.0 et 7.5)
  - Exploit:
    - Permissions incorrectes sur les fichiers journaux
    - Injection de commandes FTP avant le démarrage de la session SSL/TLS
  - Crédit: Justin Royce / ProDX

- MS12-074 Failles .NET Framework (x5) [1,3,1,1,1]
  - Affecte: .NET Framework (toutes versions supportées)
  - Exploit:
    - Abus de la réflexion
    - Fuite d'information depuis un code "partially trusted"
    - DLL Preloading
    - Faille dans le support WPAD
    - Abus de la réflexion (WPF)
  - Crédit:
    - James Forshaw / Context IS (x4)

Avis Microsoft

- MS12-075 Failles noyau (x3) [1,1,2]
  - Affecte: Windows (toutes versions supportées, y compris 8 / RT)
  - Exploit:
    - Use after free dans Win32k.sys (x2)
    - Faille dans le traitement des polices TTF
  - Crédit:
    - Matthew Jurczyk / Google Inc
    - Eetu Luodemaa, Joni Vähämäki / Documill + Chromium Security Rewards Program
  - Détails concernant CVE-2012-2897
    - http://dl.dropbox.com/u/22903093/CVE-2012-2897_info.png
    - http://pastebin.com/nWjbEGg7
    - Bloqué dans Chrome (avant le correctif Microsoft)
      - https://code.google.com/p/chromium/issues/detail?id=146254
      - http://git.chromium.org/gitweb/?p=external/ots.git;a=commitdiff;h=54380c8e93060a771a2b4bf608e6d7160b3a71e4;hp=92ae1613a125071690336a57cedd4dd9e298cf20

Avis Microsoft

- MS12-076 Failles Excel (x4) [1,1,1,1]
  - Affecte: Excel 2003 / 2007 / 2008 / 2010 / 2011 /Viewer / Compatibility Pack
  - Exploit:
    - Heap overflow
    - Memory corruption
    - Use after free
    - Stack overflow
      - … à l'ouverture d'un fichier Excel malformé
  - Crédit:
    - Sean Larsson + iDefense
    - Anonymous + iDefense (x2)
    - Anonymous + ZDI

Avis Microsoft

- Advisories
  - Q2269637 DLL Preloading
    - V18.0: ajout du bulletin MS12-074
  - Q2749655 Problème de signature sur les correctifs
    - V1.2: ajout du bulletin MS12-046
  - Q2755801 Flash Player vulnérable dans IE 10
    - V4.0: ajout du KB2770041

Avis Microsoft

- **Prévisions pour Décembre 2012**
  - **7 bulletins (5 critiques, 2 importants)**
  - **Windows, IE, Office affectés**
    - **… et ça va envoyer du lourd**
      - **http://www.theregister.co.uk/2012/12/07/patch_tuesday_dec_2012_pre_alert/**

- **Failles antérieures**
  - **MS12-027 / CVE-2012-0158**
    - **http://blog.accuvantlabs.com/blog/emiles/analyzing-cve-2012-0158**

Avis Microsoft

- **Failles à venir**
  - **Faille dans le support NTFS**
    - **Exploitable depuis une clé USB**
      - **http://www.livehacking.com/2012/11/13/windows-7-ntfs-bug-allows-any-user-to-get-admin-privileges/**
  - **Comment exploiter le noyau Windows 8 ?**
    - **En chargeant un driver Windows 7 bogué et signé par Microsoft**
      - **http://code.google.com/p/bypass-x64-dse/**
  - **Windows 8**
    - **http://pastebin.com/4sdXqS0B**
    - **http://wj32.wordpress.com/2012/11/30/obquerytypeinfo-and-ntqueryobject-buffer-overrun-in-windows-8/**
  - **IE 10**
    - **http://krash.in/crash-dump-IE-10-1.txt**

Avis Microsoft

- Révisions
  - MS12-046
    - V2.0: republication du bulletin (suite à un problème de signature)
  - MS12-058
    - V2.2: correction documentaire
  - MS12-062
    - V1.2: republication du bulletin dans SCCM 2007
  - MS12-072
    - V1.1: le correctif n'est installé sur 2008 et 2008R2 que si la feature "Desktop Experience" est activée
  - MS12-073
    - V2.0: republication du bulletin pour Vista et 2008
    - V2.1: correction documentaire
  - MS12-074
    - V1.1: correction documentaire
  - MS12-075
    - V1.1: correction documentaire

Infos Microsoft

- **Sorties logicielles**
  - **Windows "Blue" arrive rapidement**

Infos Microsoft

- **Autre**
  - **Skype #epic #fail**
    - **http://www.reddit.com/r/netsec/comments/13664q/skype_vulnerability_allowing_hijacking_of_any/**
    - **http://heartbeat.skype.com/2012/11/security_issue.html**
  - **25 millions de comptes actifs sur Outlook.com**
    - **http://www.linformaticien.com/actualites/id/27216/deja-25-millions-d-utilisateurs-pour-outlook-com.aspx**
  - **Il y aura un Office sur iOS et Android**
    - **http://www.linformaticien.com/actualites/id/26969/microsoft-office-sur-ios-et-android.aspx**

Infos Microsoft

- Surface se vend mal
  - Probablement à cause du modèle de commercialisation
    - http://www.linformaticien.com/actualites/id/27317/microsoft-surface-le-bide-de-trop.aspx
- 40 millions de Windows 8 vendus
    - http://www.linformaticien.com/actualites/id/27215/40-millions-de-windows-8-vendus.aspx
- Les applications Windows 8 déjà piratées
    - http://geekslop.com/2012/wsservice_crk-sideload-apps-windows-8-crack-trial-apps-into-full-versions
- Un patch pour Microsoft Money sur Windows 8 ☺
    - http://blogs.msdn.com/b/oldnewthing/archive/2012/11/13/10367904.aspx

Infos Microsoft

- Campagne de pub IE 10
  - http://browseryoulovedtohate.com/
  - http://www.youtube.com/watch?v=lD9FAOPBiDk&feature=youtu.be
- VLC lance un projet KickStarter pour financer la version Windows 8
  - http://www.kickstarter.com/projects/1061646928/vlc-for-the-new-windows-8-user-experience-metro
- Surface Pro disponible en Janvier 2013
  - $899

Infos Microsoft

- C'est confirmé: OpenOffice est inutilisable ☺
  - http://www.arnnet.com.au/article/442330/german_city_says_openoffice_shortcomings_forcing_it_back_microsoft/
- Moins de 500 jours avant la fin de support Windows XP
  - http://www.lemondeinformatique.fr/actualites/lire-le-compte-a-rebours-de-xp-est-passe-sous-les-500-jours-51422.html
- Le site Microsoft contient le plus de "traqueurs" au monde
  - http://www.theregister.co.uk/2012/11/29/web_tracking/
- Nouveau brevet Microsoft
  - Détecter le nombre de gens qui regarde un DVD grâce à Kinect
  - … et faire payer en conséquence
    - http://falkvinge.net/2012/11/10/copyright-industry-reality-takes-six-years-to-catch-up-with-the-worst-satire-of-it/
- Deux femmes pour remplacer Steven Sinofsky
  - http://www.infodsi.com/articles/136701/windows-windows-live-femmes-prennent-pouvoir-chez-microsoft.html

Infos Microsoft

- **Microsoft autorisé à opérer le botnet Zeus pendant 2 ans**
  - **http://www.techweekeurope.co.uk/news/court-order-allows-microsoft-to-retain-control-of-zeus-botnets-100741**
- **Un bootloader alternatif pour UEFI**
  - **Signé par Microsoft**
    - **http://mjg59.dreamwidth.org/20303.html**

Infos Réseau

- (Principales) faille(s)
  - RoTLD a bien été piraté
    - http://rotld.ro/portal/news/ro/38/index.html
  - Routeurs WiFi Belkin
    - Clé WPA par défaut == adresse MAC (grosso modo)
      - http://www.jakoblell.com/blog/2012/11/19/cve-2012-4366-insecure-default-wpa2-passphrase-in-multiple-belkin-wireless-routers/
  - Huwaei réinvente le mot de passe "Cisco Type 7"
    - http://www.securityfocus.com/archive/1/524701/30/0/threaded
  - WebSense
    - Contournement du filtrage
      - http://seclists.org/fulldisclosure/2012/Nov/171

Infos Réseau

- Bind < 9.9.2-P1
  - https://kb.isc.org/article/AA-00829
- Lighttpd 1.4.31
  - Déni de service
    - http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2012_01.txt
- cPanel 11.32.5.11
  - CSRF
    - http://www.1337day.com/exploit/19609

Infos Réseau

- **Autres infos**
  - **SPDY (draft IETF)**
    - **http://tools.ietf.org/html/draft-ietf-httpbis-http2-00**
  - **HSTS (RFC 6797)**
    - **http://tools.ietf.org/html/rfc6797**
  - **Cisco**
    - **… va publier un outil pour détecter le matériel contrefait**
      - **http://www.nextgov.com/cio-briefing/2012/11/cisco-takes-rogue-suppliers-device-id-counterfeit-parts/59782/**
    - **… rachète Cloupia**
  - **Le "Copyright Alert System" entre en application aux USA**
    - **Partenariat FAI / Center for Copyright Information / MarkMonitor pour couper l'accès Internet**
      - **http://www.copyrightinformation.org/node/709**
  - **L'ITU travaille sur le DPI**
    - **http://www.theregister.co.uk/2012/12/06/dpi_standard_leaked/**

Infos Réseau

- IPv6 est une nécessité … à moyen terme
  - http://www.numerama.com/magazine/24429-le-passage-a-ipv6-est-une-necessite-a-moyen-terme-selon-fleur-pellerin.html
  - http://questions.assemblee-nationale.fr/q14/14-2375QE.htm
  - http://questions.assemblee-nationale.fr/q14/14-2374QE.htm
- Conférence ITU à Dubai
  - Faut-il réguler Internet ?
    - http://www.linformaticien.com/actualites/id/27265/l-avenir-de-l-internet-se-joue-dans-les-prochains-jours.aspx
    - http://www.linformaticien.com/actualites/id/27349/tensions-a-dubai-autour-de-la-regulation-d-internet.aspx
- Va-t-il y avoir un Internet différencié chez Orange ?
  - http://www.rue89.com/2012/10/11/fin-de-linternet-illimite-ca-se-precise-chez-orange-236102
- En tout cas le peering n'est pas suffisant
  - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202428574474-l-ufc-que-choisir-epingle-les-fournisseurs-d-acces-a-internet-517252.php
- Le réseau Free Mobile existe ☺
  - http://mobile.free.fr/couverture/

Infos Unix

- (Principales) faille(s)
  - PERL
    - L'opérateur 'x' peut provoquer un heap overflow (!)
      - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-5195
  - Retrouver le seed à partir d'un PHPSESSID
    - http://www.openwall.com/lists/john-users/2012/09/20/2

Infos Unix

- **Autre**
  - **RHEL 6.4 plus intégré avec Windows**
    - **Support Hyper-V, Exchange …**
      - **http://news.efytimes.com/e1/96029/Beta-Of-Red-Hat-Enterprise-Linux--Released**

Failles

- **Principales applications (liste non exhaustive …)**
  - **FireFox < 17.0.1**
  - **Opera 12.11**
    - **http://seclists.org/fulldisclosure/2012/Dec/54**
  - **Call of Duty: Modern Warfare 3**
    - **DoS**
      - **http://revuln.com/files/ReVuln_CoDMW3_null_pointer_dereference.pdf**

Failles

- Communauté SNMP "en dur" dans les imprimantes Samsung
  - "s!a@m#n$p%c"
    - http://www.kb.cert.org/vuls/id/281284
    - http://l8security.com/post/36715280176/vu-281284-samsung-printer-snmp-backdoor
  - Le matériel est certifié Critères Communs
    - http://www.samsung.com/us/it_solutions/healthcare/_pdf/1_Common%20Criteria%20Rev0A.pdf
- SmartCard Oberthur ID-One COSMO 64
  - "Weak certificates"
    - http://www.kb.cert.org/vuls/id/659615
- Une faille dans Java 7 vendue $100,000
  - … et actuellement non corrigée
    - http://krebsonsecurity.com/2012/11/java-zero-day-exploit-on-sale-for-five-digits/

Failles

- Symantec Messaging Gateway
  - Login: support, password: symantec
    - http://www.securityfocus.com/archive/1/524876

- King Cope joue le Père Noël
  - Failles multiples dans MySQL
  - Faille dans FreeSSHd
  - Faille dans ssh.com (Tectia)
  - … publiées en 0day

Failles 2.0

- La librairie OWASP PHP CSRF Guard est vulnérable
  - http://blog.kotowicz.net/2012/12/on-handling-your-pets-and-csrf.html
- Instagram sur iOS n'utilise pas SSL
  - http://secunia.com/advisories/51270/
- Un ver se répand à la vitesse de l'éclair sur Tumblr
  - http://nakedsecurity.sophos.com/2012/12/03/how-tumblr-worm-worked/

Failles 2.0

- GOOD For Enterprise < 2.0.2
  - … ne vérifie pas les certificats ?
    - http://seclists.org/fulldisclosure/2012/Nov/72
- Fingerprinting IP + TCP + HTTP
    - http://noc.to/
- Le problème des mots de passe sur les post-its
  - C'est qu'on peut les lire sur les photos ☺
    - http://www.lepoint.fr/monde/couac-autour-de-photos-du-prince-william-sur-sa-base-militaire-20-11-2012-1531448_24.php

Failles 2.0

- Paypal est-il honnête dans son "bug bounty" ?
  - http://thehackernews.com/2012/11/paypal-bug-bounty-program-playing-fair.html
- 2013: no more free bugs
  - http://www.darkreading.com/vulnerability-management/167901026/security/news/240142947/how-the-sale-of-vulnerabilities-will-change-in-2013.html
- ReVuln ne communiquera pas ses failles SCADA aux éditeurs
  - Note: il s'agit de Luigi Auriemma
    - http://www.computerworld.com/s/article/9233916/Security_firm_finds_SCADA_software_flaws_won_t_report_them_to_vendors
- Ne pas énerver les hackers chinois
  - Jamais
    - http://www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html

Sites piratés

- **Les sites piratés du mois**
  - **FreeBSD.org**
    - **http://www.freebsd.org/news/2012-compromise.html**
  - **LogMeIn (non confirmé)**
    - **http://community.logmeinrescue.com/t5/Miscellaneous-Offtopic/LogMeIn-leaked-my-email-address/td-p/88548/highlight/false**
  - **eBay**
    - **Injection SQL**
      - **http://blog.majorsecurity.net//2012/11/18/exploitable-sqli-on-ebay-dot-com-analysis/**

Sites piratés

- Société Générale
  - Injection SQL (sur le site de recrutement)
    - https://twitter.com/FawziiColdFire/status/275676690376704000/photo/1/large
- UGC.fr
  - #fail uniquement
    - http://twitpic.com/bfr593
- Piwik.org
    - http://piwik.org/blog/2012/11/security-report-piwik-org-webserver-hacked-for-a-few-hours-on-2012-nov-26th/

Sites piratés

- Nationwide Insurance (1,000,000 utilisateurs)
  - http://www.insurance.ca.gov/0400-news/0100-press-releases/2012/release162-12.cfm
- Adobe "Connectusers.com" (150,000 utilisateurs)
  - http://blogs.adobe.com/adobeconnect/2012/11/connectusers-com-forum-outage-following-database-compromise.html
- Acer India (20,000 utilisateurs)
  - http://thehackernews.com/2012/12/acer-domains-defaced-and-20k.html
- Plusieurs sites de presse français (via une régie publicitaire)
  - Arte, Les Echos, SPQN …
    - http://www.zataz.com/news/22519/iframe--injection--site-piege.html
    - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202416987628-le-site-du-spqn-vraisemblablement-pirate-515328.php

Sites piratés

- ESA
  - http://slixme.me/dumps/ESAInt.txt
- Japan Aerospace Exploration Agency
  - http://thehackernews.com/2012/12/malware-swipes-rocket-data-from.html
- International Atomic Energy Agency
  - http://thehackernews.com/2012/11/hackers-break-into-international-atomic.html
  - http://cryptome.org/2012/11/parastoo-hacks-iaea.htm

Sites piratés

- Tentative de chantage à la clinique de Champagne
  - http://www.ticsante.com/show.php?id=1280&page=story
- Un employé Orange se fait pirater des données à la maison
  - … incluant le réseau Europol
    - http://vrritti.com/2012/12/06/it-employee-of-telco-orange-caused-data-breach-at-europol-orange-tried-to-block-dutch-news-broadcast/
    - https://www.europol.europa.eu/content/news/no-sensitive-europol-information-compromised-orange-data-breach-1871
- Un SysAdmin des services secrets Suisse part avec toutes les données …
  - http://www.lepoint.fr/monde/les-services-secrets-suisses-se-font-voler-des-millions-de-donnees-30-09-2012-1511764_24.php

Malwares, spam et fraudes

- W32/Narilam s'attaque aux bases de données
  - Essentiellement prévalent en Iran
    - http://www.computerworld.com/s/article/9233940/Symantec_spots_odd_malware_designed_to_corrupt_databases
- W32/Shylock ne se lance pas si RDP est utilisé
    - http://www.mag-securs.com/News/tabid/62/id/29566/Shylock-malware-de-nouvelle-generation.aspx
- APT contre la Syrie
    - https://www.securelist.com/en/blog/774/A_Targeted_Attack_Against_The_Syrian_Ministry_of_Foreign_Affairs
- APT contre Coca-Cola
    - http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/

Malwares, spam et fraudes

- La saga John McAfee
  - http://www.whoismcafee.com/
- 80% des malwares arrivent par des sites "légitimes"
  - http://news.techworld.com/security/3415156/80-of-malware-attacks-in-2012-were-redirects-from-legitimate-sites/
- Android plus souvent attaqué par des malwares que les PC sous Windows
  - http://www.infoworld.com/d/security/android-devices-in-us-face-more-malware-attacks-pcs-208462

Malwares, spam et fraudes

- Le botnet TDSS complètement retourné
  - Une saine lecture technique !
    - http://nobunkum.ru/analytics/en-tdss-botnet
- MoneyGram condamné à $100m d'amende pour fraude
    - http://krebsonsecurity.com/2012/11/moneygram-fined-100-million-for-wire-fraud/
- Une banque américaine condamné à rembourser un client
  - Le "login / mot de passe" n'a pas été jugé comme une mesure de sécurité suffisante
    - http://www.wired.com/threatlevel/2012/11/bank-to-pay-hacking-victim/all/
- Un rootkit Linux qui injecte des IFRAME malveillantes
    - http://seclists.org/fulldisclosure/2012/Nov/94
- Sophos trolle les chercheurs en sécurité
    - http://nakedsecurity.sophos.com/2012/12/05/web-exploit-kits-whitehat/
- Imperva trolle les antivirus
    - http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf

Actualité (francophone)

- "Comment les américains ont piraté l'Elysée"
  - http://lexpansion.lexpress.fr/high-tech/cyberguerre-comment-les-americains-ont-pirate-l-elysee_361225.html
  - … ou pas
    - http://reflets.info/lexpress-a-vu-le-chasseur-qui-a-vu-lours-qui-a-vu-les-americains/
    - http://www.zdnet.fr/actualites/securite-la-cyberattaque-sur-l-elysee-en-cinq-questions-39784833.htm
    - http://photos.state.gov/libraries/france/5/pa/L_ExpressDroitdeReponse.pdf
- Les 10 pépites de la cybersécurité française
  - … ou pas
    - http://www.usinenouvelle.com/article/cybersecurite-dix-pepites-a-suivre.N187060
- L'industrie française de la cybersécurité se porte bien
  - … ou pas
    - http://www.usinenouvelle.com/article/la-cybersecurite-francaise-passe-a-l-attaque.N186926

Actualité (francophone)

- La "réserve citoyenne cyber"
  - http://www.defense.gouv.fr/actualites/economie-et-technologie/des-reservistes-specialises-en-cyberdefense
- Un nouveau patron pour l'Open Data
  - http://www.linformaticien.com/actualites/id/27334/henri-verdier-a-la-tete-de-l-open-data-en-france.aspx
- La Bretagne choisit le Cloud … d'Amazon
  - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202430446845-a-peine-cree-le-cloud-a-la-francaise-est-deja-sous-pression-517347.php

Actualité (francophone)

- Python au Bac l'année prochaine
  - http://cache.media.enseignementsup-recherche.gouv.fr/file/CPGE/90/4/Informatique-TSI-MP-PC-PT-TPC-PSI-22-11-2012_233904.pdf
- Guerre autour de la taxe sur la copie privée
  - http://www.linformaticien.com/actualites/id/27104/copie-privee-il-n-y-aura-pas-de-reforme.aspx
- L'UMP victime du Cloud
  - Son fichier d'adhérents bloqué chez Oracle
    - http://www.lefigaro.fr/politique/2012/11/30/01002-20121130ARTFIG00613-le-fichier-de-l-ump-bloque.php

Actualité (francophone)

- Sénateur Bockel vs. Cybercriminalité
  - http://www.channelbp.com/content/apr%C3%A8s-les-routeurs-chinois-le-s%C3%A9nateur-bockel-s%E2%80%99attaque-%C3%A0-la-cybercriminalit%C3%A9
- Le vote électronique
  - Ca ne marche pas ☺
    - http://lafactory-npa.fr/sma/votez/
- Le fisc français réclame $200m à Amazon
    - http://fr.reuters.com/article/technologyNews/idFRPAE8AB06F20121112
  - … et ça n'est que le début
    - http://www.linformaticien.com/actualites/id/27110/le-gouvernement-impatient-de-s-attaquer-a-la-fiscalite-du-numerique.aspx

Actualité (francophone)

- L'état français achète un "0day" pour 160,000€
  - Info ou intox ?
    - http://lexpansion.lexpress.fr/high-tech/la-nouvelle-force-de-frappe-du-contre-espionnage-francais-sur-internet_361502.html
- Simulation d'attaque contre la place financière de Paris
    - http://www.lesechos.fr/entreprises-secteurs/finance-marches/actu/0202420389089-la-place-financiere-de-paris-cible-d-une-cyber-attaque-fictive-515802.php
- L'ANSSI peut inspecter les opérateurs télécom à sa guise
    - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026638421&dateTexte=&categorieLien=id

Actualité (francophone)

- **ANSSI: publications récentes**
  - **"Nos entreprises ne sont pas assez protégées"**
    - **http://www.usinenouvelle.com/article/nos-entreprises-ne-sont-pas-assez-protegees-contre-les-cyberattaques.N186981**
  - **"On the Use of Shamir's Secret Sharing Against Side-Channel Analysis"**
    - **http://www.ssi.gouv.fr/IMG/pdf/aesshamir_Coron_Prouff_Roche.pdf**
  - **"Politique de certification concernant les autorités de certification racines gouvernementales"**
    - **http://www.ssi.gouv.fr/IMG/pdf/igca-pc-v2.pdf**
  - **"Sécurité des technologies sans contact pour le contrôle des accès physiques"**
    - **http://www.ssi.gouv.fr/IMG/pdf/Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf**

Actualité (anglo-saxonne)

- La DARPA veut lancer un programme de détection automatique des backdoors
  - http://www.homelandsecuritynewswire.com/dr20121203-darpa-s-program-to-reveal-backdoors-hidden-malicious-functionality-in-commercial-it-devices
- Condamnation d'Andrew Auernheimer
  - Une "anti affaire Tati"
    - http://erratasec.blogspot.de/2012/11/you-are-committing-crime-right-now.html
- La vérification d'intégrité sur les binaires fait l'objet d'un brevet
  - … déposé en 2007
    - http://www.equities.com/news/headline-story?dt=2012-11-14&val=705467&cat=tech

Actualité (anglo-saxonne)

- Le Pentagone construit "cybercity"
  - Pour s'entrainer à la "cyberguerre"
    - http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/five/index.html
- UK: programme de cyber sécurité ambitieux
  - Incluant des "cyber réservistes"
    - http://www.lemagit.fr/projets/secteur-activite/secteur-public/2012/12/04/le-royaume-uni-va-se-doter-de-cyber-reservistes/
- Raytheon recrute …
    - http://blogs.csoonline.com/security-careerstaffing/2462/defcon-black-badges-decorate-our-offices-our-nerf-collection-dwarfs-most-toy-stores

Actualité (européenne)

- Le projet de protection des données à caractère personnel s'appliquera sans transposition
  - http://www.globalsecuritymag.fr/Protection-des-donnees-a-caractere,20121115,33756.html
- ZTE & Huawei vs. Commission Européenne
  - http://www.linformaticien.com/actualites/id/27344/dumping-fiscal-la-ce-pourrait-lancer-une-procedure-contre-zte-et-huawei.aspx
- "Horizon 2020 – The Challenge Of Providing Cybersecurity"
  - http://cordis.europa.eu/fp7/ict/security/home_en.html

Actualité (Google)

- AdBlock Plus disponible pour Android
- Google Knowledge Graph disponible pour la France
- Un plugin officiel pour faire de la prise en main à distance via Google Chrome
  - https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhmhahfdphkhkmpfmihenigjmpp
- Flash est désormais sandboxé dans Chrome/Mac OS X
  - http://chrome.blogspot.fr/2012/11/securing-flash-player-for-our-mac-users.html
- Chrome/Linux supporte seccomp-bpf
  - http://blog.chromium.org/2012/11/a-safer-playground-for-your-linux-and.html
- Faille dans la gestion des permissions avec Google Webmaster Tools
  - http://www.davidnaylor.co.uk/webmastertools-in-dangerous-security-flaw.html
- Le "Google Private Play Channel" apparait dans Android
  - http://googleenterprise.blogspot.fr/2012/12/a-new-way-to-distribute-your-internal.html

Actualité (Google)

- N'insistez pas …
  - Il ne sera pas possible de déplacer les onglets Chrome ailleurs qu'en haut
    - https://code.google.com/p/chromium/issues/detail?id=44106#c187
- Google devient FAI aux USA
  - Offre gratuite
  - … ou accès 1Gb/s pour $70/mois
- "Green Google"
  - Google construit des éoliennes

Actualité (Apple)

- Safari sur iOS 6 met en cache les requêtes POST
  - http://www.mnot.net/blog/2012/09/24/caching_POST
- Google Maps revient sur iOS
  - http://www.linformaticien.com/actualites/id/27106/une-appli-google-maps-prochainement-sur-ios.aspx
- Apple Plans … tue
  - http://www.linformaticien.com/actualites/id/27348/bugs-d-apple-plans-la-police-australienne-ne-rit-plus.aspx
- Les virus pour Mac OS X
  - … ne vont pas s'arrêter de si tôt
    - http://www.f-secure.com/weblog/archives/00002466.html
- Sortie de iTunes 11
- Grosse réorganisation de l'exécutif

Actualité (crypto)

- Attaque "générique" contre tous les block ciphers
  - http://eprint.iacr.org/2012/677.pdf
- La faille est toujours dans le générateur d'aléa
  - https://spideroak.com/blog/20121205114003-exploit-information-leaks-in-random-numbers-from-python-ruby-and-php

Actualité

- Conférences passées
  - LeWeb'12
  - PacSec 2012
    - Contournement de la sandbox OS X
      - http://www.macg.co/news/voir/257811/securite-grosse-faille-dans-le-bac-a-sable-d-os-x
  - ZeroNights 2012
      - http://fr.slideshare.net/DefconRussia/tag/zeronights-2012
  - HitCon 2012
    - Sécurité du noyau Windows 8
      - http://hitcon.org/2012/download/0720A5_360.MJ0011_Reversing%20Windows8-Interesting%20Features%20of%20Kernel%20Security.pdf
  - Passwords^12
    - Optimisation de 20% sur les attaques contre SHA-1
      - http://arstechnica.com/security/2012/12/oh-great-new-attack-makes-some-password-cracking-faster-easier-than-ever/
      - https://hashcat.net/p12/
  - MalCon 2012
      - http://www.malcon.org/

Actualité

- **Conférences à venir**

  - **Conférences francophones avec CFP ouverts**
    - **JSSI de l'OSSIR**
      - **http://www.ossir.org/jssi/index/jssi-2013-appel-a-communications.shtml**
    - **SSTIC 2013**
    - **GS Days 2013**

    - **BotConfs 2013**
      - **Décembre 2013 à Nantes**
      - **https://www.botconf.eu/**

Actualité

- **Sorties logicielles**
  - **Metasploit 4.5**
  - **Androguard 1.9**
    - **+ plugin SublimeText**
  - **Netzob 0.4.0**
  - **F-Secure Software Updater**
    - **http://www.f-secure.com/en/web/business_global/software-updater**

Actualité

- La capitalisation boursière de Qualcomm dépasse celle d'Intel
  - http://www.linformaticien.com/actualites/id/27043/qualcomm-surpasse-intel-en-capitalisation-boursiere.aspx
- Les prochains processeurs Intel seront soudés à la carte mère
  - http://www.linformaticien.com/actualites/id/27232/intel-pourrait-mettre-fin-aux-processeurs-amovibles.aspx
- Texas Instruments arrête les processeurs OMAP
  - http://www.linformaticien.com/actualites/id/27091/ti-abandonne-les-processeurs-mobiles-et-supprime-1700-postes.aspx
  - Pas d'inquiétude: tout le monde est parti chez Apple
    - http://www.linformaticien.com/actualites/id/27287/apple-se-renforce-dans-les-processeurs.aspx
- Nokia Here arrive sur iOS et Android
  - http://www.linformaticien.com/actualites/id/27075/here-nokia-etend-ses-services-de-cartographie-a-d-autres-plates-formes.aspx

Actualité

- Le Patriot Act s'applique aux sociétés américaines
  - … sans contrainte de territorialité des données
    - http://www.linformaticien.com/actualites/id/27313/cloud-computing-le-patriot-act-s-applique-aussi-en-europe.aspx

- Tenable USM (incluant Nessus) certifié EAL2+
    - http://blog.tenablesecurity.com/2012/11/tenable-awarded-common-criteria-certification-eal2.html

- BitCoin Central devient une banque à part entière
  - … grâce au Crédit Mutuel
    - http://arstechnica.com/tech-policy/2012/12/bitcoin-going-mainstream-exchange-approved-to-operate-as-a-bank/

Actualité

- Guido van Rossum recruté chez Dropbox
  - https://tech.dropbox.com/2012/12/welcome-guido/
- BlackBerry Messenger propose la téléphonie en WiFi
  - http://www.linformaticien.com/actualites/id/27079/blackberry-le-nouveau-bbm-integre-la-voix-par-wi-fi.aspx
- La carte d'identité biométrique requise pour accéder à Internet en Iran
  - http://zataz.com/news/22536/Nationale-Smart-Card--iran--Mohammad-Ebrahim.html
- Itanium n'est pas mort !
  - http://www.linformaticien.com/actualites/id/27010/hp-et-intel-offrent-une-seconde-vie-a-l-itanium.aspx

Divers

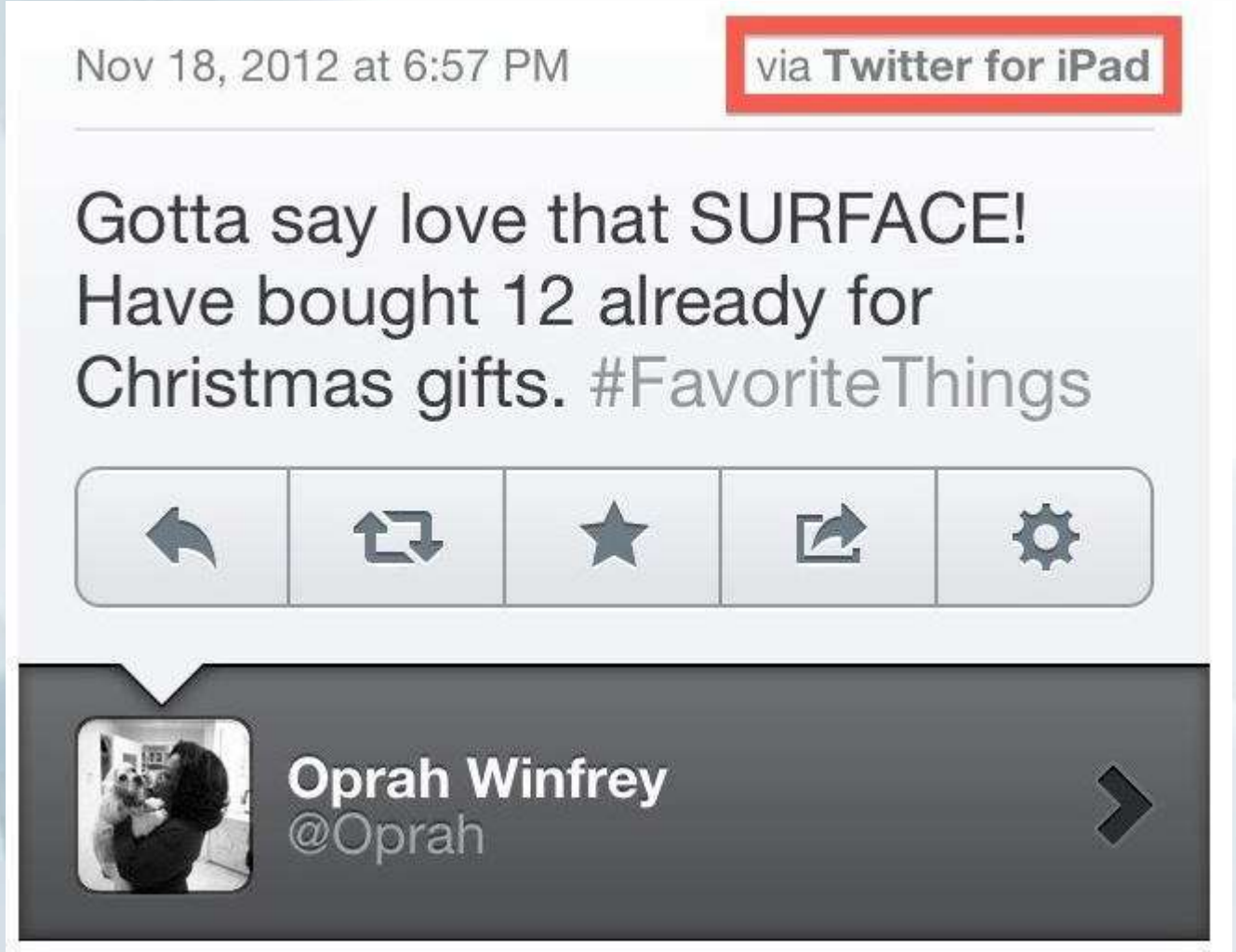
- Il y a 8,311,000 développeurs Java dans le monde
  - http://www.javacodegeeks.com/2012/11/how-many-java-developers-are-there-in-the-world.html
- Sam Sung
  - … travaille chez Apple
    - http://www.theregister.co.uk/2012/11/21/sam_sung_the_apple_store_employee/
- RubyCon annulé
  - … il n'y avait que des blancs (?!)
    - http://www.newstatesman.com/sci-tech/2012/11/tech-has-gender-problem-and-it-doesnt-get-better-not-talking-about-it
- Un émulateur de PC XT en JavaScript
  - http://jsmachines.net/
- Duck Duck Go FTW
  - https://duckduckgo.com/tty/

Divers

- De l'importance des polices de caractères …
  - "Georgia" est la meilleure
    - http://opinionator.blogs.nytimes.com/2012/08/08/hear-all-ye-people-hearken-o-earth/
- Les besoins spécifiques de la Wii U
    - http://www.p4rgaming.com/?p=481
- Un langage de programmation basé sur Dwarf Fortress
    - https://github.com/Frib/Armok

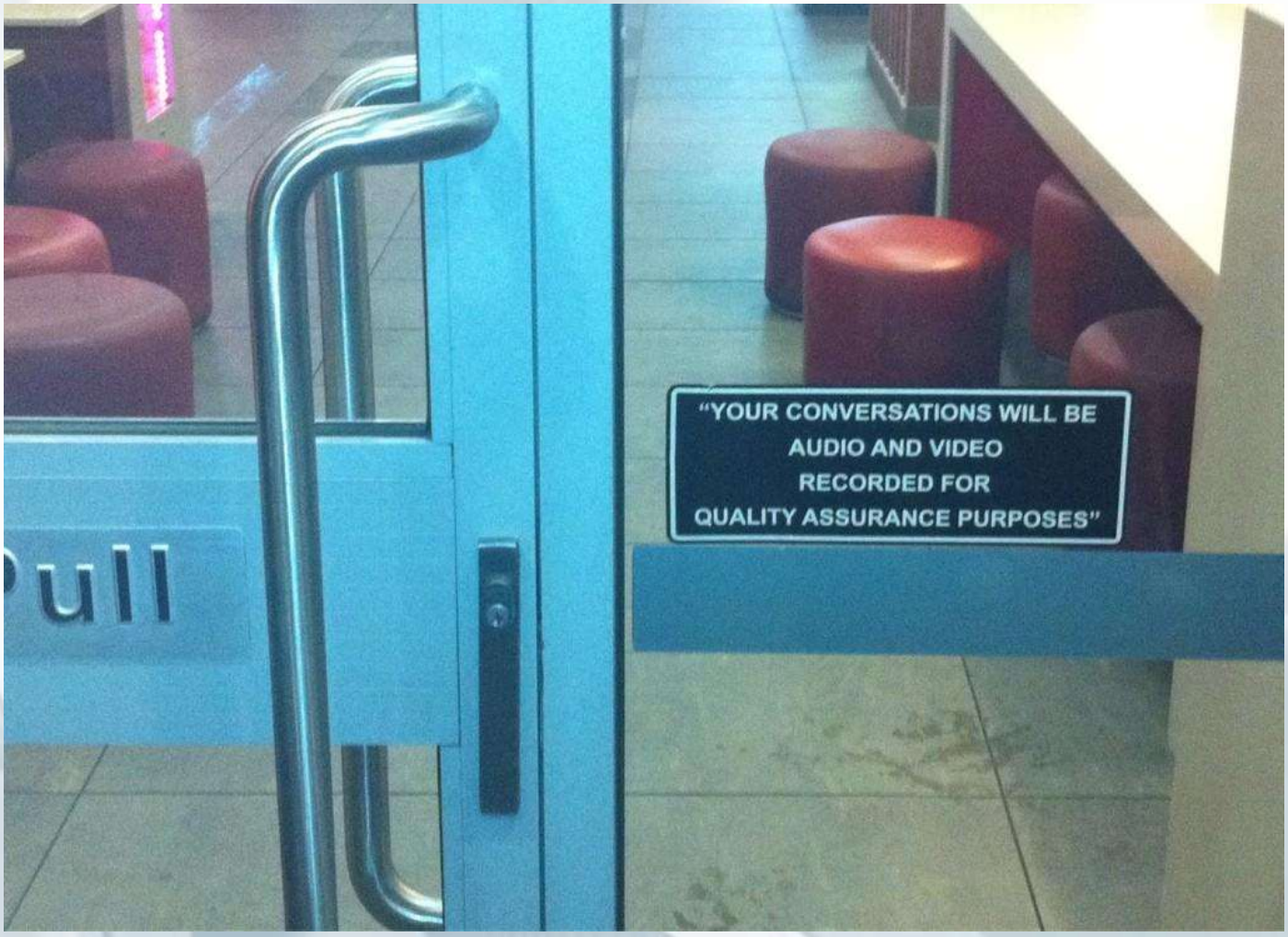
Divers

- **Source: https://twitter.com/BuzzFeedAndrew/status/270606674757316609/photo/1**



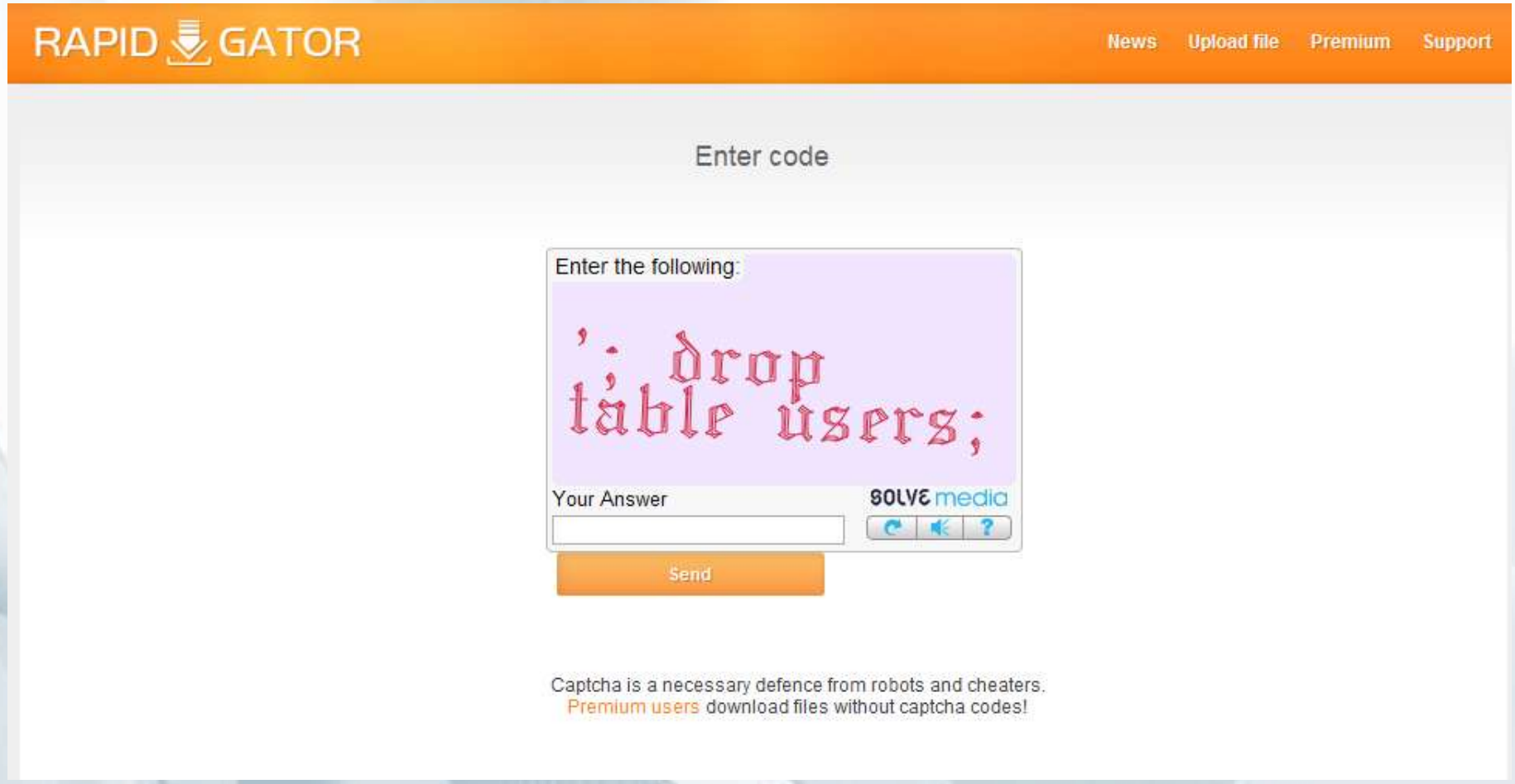
Divers

- Source: https://twitter.com/dlitchfield/status/267695613913726977/photo/1



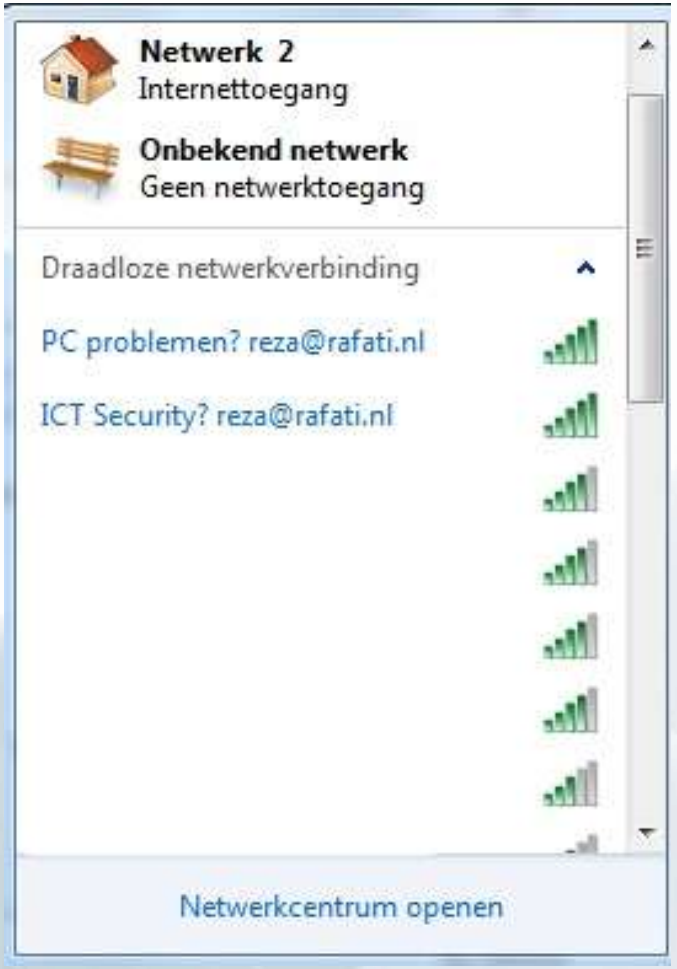
Divers

- Source: https://twitter.com/tchenapan/status/272826589815926784/photo/1



Divers

- Source: http://www.cyberwarzone.com/using-your-wifi-ssid-get-attention-or-potential-jobs



Divers

- Source: PHP

```
$ cat ternary.php
<?php
echo (TRUE ? "a" : TRUE ? "b" : "c")."\n";
```

Questions / réponses

- Questions / réponses
- Prochaine réunion et assemblée générale annuelle
  - Mardi 8 janvier 2013
- Conférence JSSI de l'OSSIR
  - Mardi 19 mars 2013
  - Le CFP est ouvert !
    - http://www.ossir.org/jssi/index/jssi-2013-appel-a-communications.shtml