OSSIR
Groupe Paris

Réunion du 14 mai 2013

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Avril 2013**

  - **MS13-028 Correctif cumulatif pour IE (x2) [2]**
    - **Affecte: IE (toutes versions supportées)**
    - **Exploit: "*use after free*"**
    - **Crédits:**
      - **Ivan Fratric & Ben Hawkes / Google Security Team (x2)**
      - **Anonymous**

  - **MS13-029 Faille dans le contrôle ActiveX "RDP" (x1) [1]**
    - **Affecte: client RDP (toutes versions supportées)**
    - **Exploit: "*use after free*"**
    - **Crédits:**
      - **c1d2d9acc746ae45eeb477b97fa74688 + ZDI**

Avis Microsoft

- **MS13-030 Faille SharePoint (x1) [3]**
  - **Affecte: SharePoint Server 2013**
  - **Exploit: accès non autorisé possible aux listes SharePoint**
  - **Crédits: N/D**

- **MS13-031 Failles noyau (x2) [2]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: "race condition"**
    - **Elévation de privilèges**
    - **Accès en lecture à la mémoire noyau**
  - **Crédits:**
    - **Gynvael Coldwind & Mateusz "j00ru" Jurczyk / Google Inc (x2)**

Avis Microsoft

- MS13-032 Faille Active Directory (x1) [3]
  - Affecte: Windows
    - Toutes versions supportées, sauf:
      - RT, 2008/Itanium et 2008R2/Itanium
    - AD / ADAM / AD LDS
  - Exploit: déni de service (via consommation mémoire excessive)
  - Crédits: N/D

- MS13-033 Faille dans CSRSS (x1) [3]
  - Affecte: Windows
    - Toutes versions supportées, sauf:
      - Windows 7, 2008R2, 8, 2012, RT
  - Exploit: élévation de privilèges locale
  - Crédits:
    - George Georgiev Valkov

Avis Microsoft

- **MS13-034 Faille dans Microsoft Anti Malware Client (x3) [1]**
  - **Affecte: Windows Defender (Windows 8 et RT)**
  - **Exploit: élévation de privilèges locale**
  - **Crédits:**
    - **Bruce Monroe / Intel**
    - **Shai Sarfaty**
    - **Tony Robotham / Centrica**
  - **Notes: contient également des mises à jour fonctionnelles**

- **MS13-035 Faille dans le filtre anti-XSS (x1) [3]**
  - **Affecte:**
    - **InfoPath 2010SP1**
    - **SharePoint Server 2010SP1**
    - **Groove Server 2010SP1**
    - **SharePoint Foundation 2010SP1**
    - **Office Web Apps 2010SP1**
  - **Exploit: défaut dans le filtre anti-XSS**
  - **Crédits:**
    - **Drew Hintz & Andrew Lyons / Google Security Team**

Avis Microsoft

- MS13-036 Failles noyau (x4) [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit:
    - "Race condition" dans WIN32K.SYS (x2)
    - Faille dans le traitement des polices par WIN32K.SYS
    - Pointeur NULL lors de l'accès à un système NTFS malformé
  - Crédits:
    - Gynvael Coldwind & Mateusz "j00ru" Jurczyk / Google Inc (x3)
    - Wang Yu / Qihoo 360 Security Center

Avis Microsoft

- Advisories
  - Q2847140 Faille IE exploitée en "0day"
    - Utilisée pour attaquer le nucléaire américain
      - http://thehackernews.com/2013/05/internet-explorer-zero-day-exploit.html
    - V1.0: publication du bulletin
    - V1.1: ajout d'un "fix it"
- Prévisions pour Mai 2013
  - 10 bulletins
    - Affecte: IE, Office, Windows
    - Corrige: le 0day IE et la faille PWN2OWN
- Failles à venir
- Retour sur des failles antérieures

Avis Microsoft

Révisions

- MS12-043
  - V4.2: correction documentaire sur les bulletins remplacés
- MS13-028
  - V1.1: ajout d'un CVE, ce bulletin remplace MS13-010
- MS13-029
  - V1.1: correction documentaire sur la version du client RDP
- MS13-031
  - V1.1: correction documentaire
- MS13-034
  - V1.1: changement dans la logique de détection
- MS13-036
  - V2.0: suppression du correctif (trop de problèmes connus)
  - V2.1: assistance aux utilisateurs qui n'arrivent plus à rebooter
  - V3.0: re-publication du correctif
  - V3.1: correction documentaire

Infos Microsoft

- **Sorties logicielles**
  - **Windows Embedded 8**
  - **EMET 4.0**
    - **http://blogs.technet.com/b/srd/archive/2013/04/18/introducing-emet-v4-beta.aspx**
  - **Office pour Android et iOS**
    - **Pas avant 2014**
      - **http://www.ubergizmo.com/2013/04/office-for-android-and-ios-allegedly-delayed-till-october-2014/**
  - **Security Intelligence Report (SIR) 14**
    - **http://blogs.technet.com/b/security/archive/2013/04/17/volume-14-of-the-microsoft-security-intelligence-report-released-hundreds-of-pages-of-new-security-intelligence-now-available.aspx**
  - **Authentification à 2 facteurs pour les services Microsoft**
    - **http://www.theverge.com/2013/4/17/4234890/microsoft-accounts-two-factor-authentication**

Infos Microsoft

- **Autre**
  - **Microsoft gagne plus d'argent que prévu**
    - **http://www.lemonde.fr/technologies/article/2013/04/19/microsoft-devoile-des-resultats-superieurs-aux-attentes_3162872_651865.html**
  - **Le CFO de Microsoft s'en va**
    - **http://news.slashdot.org/story/13/04/22/0342233/microsoft-cfo-quits**
  - **Windows 8.1 aura un bouton "démarrer"**
    - **http://www.slashgear.com/microsoft-reportedly-bringing-back-start-button-in-windows-8-1-22278728/**
  - **Windows 8.1 a leaké**
    - **http://thepiratebay.sx/torrent/8393079/Windows_8.1_Pro_Preview_Build_9374_X86(32bit)**
  - **Microsoft pourrait acheter Nook Media**
    - **http://www.ubergizmo.com/2013/05/microsoft-could-purchase-nook-media-for-1-billion/**
  - **Windows, MinDef, APRIL**
    - **La saga continue**
      - **http://www.april.org/lotan-impose-microsoft-et-les-backdoors-de-la-nsa-au-ministere-de-la-defense**
      - **http://levinvinteur.com/larmee-accro-a-microsoft/**

Infos Réseau

- **(Principales) faille(s)**
  - **Failles Cisco**
    - **Cisco NAC SQL Injection**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130417-nac**
    - **Cisco TP DoS**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130417-tpi**
    - **Cisco IKE Group Enumeration**
      - **https://www.trustwave.com/spiderlabs/advisories/TWSL2013-004.txt**
    - **Cisco Device Manager Command Execution**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-fmdm**
    - **...**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-ucsmulti**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-nxosmulti**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130508-cvp**
      - **http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121031-dcnm**
  - **La sécurité des routeurs domestiques**
    - **Nulle**
      - **http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp**

Infos Réseau

- **Autres infos**
  - **OVH + rand() = #fail**
    - **http://forum.ovh.com/showthread.php?t=88277**
  - **Sortie de l'offre OVH VPN**
    - **http://www.ovh.fr/vpn/**

Infos Unix

- **(Principales) faille(s)**
  - **PostgreSQL**
    - **Génération d'aléa incorrecte dans les fonctions cryptographiques**
      - **https://bugzilla.redhat.com/show_bug.cgi?id=929255**
  - **MongoDB**
    - **char version[32] FTW**
      - **https://github.com/mongodb/mongo/blob/master/src/mongo/util/net/httpclient.cpp #L128**
  - **Exim + Dovecot = #fail**
    - **http://seclists.org/fulldisclosure/2013/May/7**
  - **Linux <= 2.6.37**
    - **http://digitalsec.net/semtex.c**
  - **Linux 3.8**
    - **file_ns_capable() local root**
      - **http://packetstormsecurity.com/files/121561/userns_root_sploit.c**

Infos Unix

- **Autres infos**
  - **Linux/Cdorked.A**
    - **Pour servir du BlackHole**
      - **http://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/**
  - **Debian 7.0**
    - **http://lists.debian.org/debian-devel-announce/2013/04/msg00006.html**

Failles

- **Principales applications**

  - **Oracle Quaterly Patch**
    - **Java < 1.7.21, < 1.6.45**
      - **http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html**
    - **PoC**
      - **http://weblog.ikvm.net/PermaLink.aspx?guid=acd2dd6d-1028-4996-95df-efa42ac237f0**
    - **"Oracle fixes 42 holes in Java to revive security confidence" (SRSLY)**
      - **http://mobile.reuters.com/article/idUSBRE93F1AK20130416?irpc=932**
    - **Mais … il y a encore des failles dans Java ☺**
      - **http://seclists.org/fulldisclosure/2013/Apr/194**
    - **Note: Java 1.8 retardé … pour le rendre plus sûr ☺**
      - **http://mreinhold.org/blog/secure-the-train**

Failles

- Adobe
  - ColdFusion
    - http://www.adobe.com/support/security/bulletins/apsb13-10.html
  - Flash Player < 11.7
    - http://www.adobe.com/support/security/bulletins/apsb13-11.html
  - ShockWave Player
    - http://www.adobe.com/support/security/bulletins/apsb13-12.html
- Chrome

Failles 2.0

- Un faux Tweet sur Associated Press provoque un "Flash Crash"
  - Plus de $150Md évaporés …
    - http://www.atlantico.fr/decryptage/piratage-twitter-ap-hackers-ont-pouvoir-faire-plonger-economie-charles-bwele-708008.html
- "Bug" chez SABRE
  - Conséquence: tous les vols American Airlines annulés
    - http://www.dallasnews.com/business/20130416-faa-grounds-all-american-airlines-flights-due-to-computer-crash.ece
- La Corée du Sud déconnecte "préventivement" ses réacteurs nucléaires d'Internet
    - http://french.yonhapnews.co.kr/national/2013/04/14/0300000000AFR20130414000700884.HTML

Failles 2.0

- **Brute-force massif sur les mots de passe Wordpress (et d'autres)**
  - **http://nakedsecurity.sophos.com/2013/04/13/wordpress-blogs-and-more-under-global-attack-check-your-passwords-now/**
- **Un sysadmin chez HostGator backdoore 2,700 serveurs**
  - **http://arstechnica.com/security/2013/04/former-employee-arrested-charged-with-rooting-2700-hostgator-servers/**
- **Diablo III ruiné … par un integer overflow**
  - **http://pastebin.com/YYPM4uQK**
- **Faille dans Brainlab Exac Trac 5.5**
  - **http://ansm.sante.fr/S-informer/Informations-de-securite-Autres-mesures-de-securite/Systeme-de-positionnement-du-patient-Exac-Trac-5.x-Brainlab-Information-de-securite2**

Failles 2.0

- **Apple déchiffre votre iPhone pour le FBI**
  - **Délai: entre 7 semaines et 4 mois**
    - **http://arstechnica.com/apple/2013/05/apple-will-reportedly-unlock-your-iphone-for-police-but-theres-a-wait-list/**
  - **Note: Google offre le même service**

- ***What could possibly go wrong?***
  - **JSON Pointer**
    - **http://www.rfc-editor.org/rfc/rfc6901.txt**
  - **JSON Patch**
    - **http://www.rfc-editor.org/rfc/rfc6902.txt**

Sites piratés

- **Les sites piratés du mois (liste partielle)**
  - **$45m volés dans des DAB en quelques heures**
    - **http://www.leparisien.fr/international/une-mafia-informatique-detourne-45-m-en-quelques-heures-09-05-2013-2791303.php**
  - **Le cerveau de l'opération abattu chez lui en jouant aux dominos**
    - **http://www.wired.com/threatlevel/2013/05/bank-cashing-suspect-killed/**
  - **QinetiQ**
    - **Complètement pillé depuis des années**
      - **http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html**
  - **Opérations en cours**
    - **"Black Summer"**
    - **#OpIsraël**
    - **#OpUSA**
    - **Pays-Bas**
      - **http://www.lemonde.fr/europe/article/2013/05/08/pays-bas-les-sites-du-gouvernement-victimes-d-une-cyberattaque_3173559_3214.html**

Sites piratés

- CBS
  - Par "Syrian Electronic Army"
    - http://venturebeat.com/2013/04/21/sea-cbs/
- Washington State (160,000 SSN, 1M permis de conduire)
    - http://www.scmagazine.com/hackers-raid-washington-state-court-system-to-steal-160000-ssns-1m-drivers-license-numbers/article/292730/
- Mediapart
  - Vol des RIB abonnés
    - http://blogs.mediapart.fr/blog/la-redaction-de-mediapart/100413/nos-abonnes
- Name.com (registrar)
    - http://threatpost.com/name-com-breached-users-asked-to-reset-passwords/

Sites piratés

- Living Social (50M comptes)
  - https://www.livingsocial.com/createpassword
- Yahoo! Japon (1,27M comptes)
- Schnuck Markets
  - 2,4M de CB volées dans 79 magasins
    - http://www.schnucks.com/pressreleases/pressrelease.asp?id=219
- Goo (100K comptes)

- Verizon publie le DBIR 2013
  - http://www.verizonenterprise.com/DBIR/2013/

Malwares, spam et fraudes

- Vrai ou faux ?

Malwares, spam et fraudes

- Vrai ☺
  - http://www.winzip.com/win/en/prodpagemp.htm
- "Magic"
  - Une APT qui utilise Twitter comme C&C
    - http://www.crn.com.au/News/340215,mysterious-new-trojan-uses-magic-code.aspx
- "FinSpy"
  - Encore plus répandu que prévu
    - https://citizenlab.org/2013/04/for-their-eyes-only-2/

Malwares, spam et fraudes

- L'auteur du botnet Carberp arrêté en Ukraine
  - http://www.zdnet.com/suspected-hackers-behind-carberp-botnet-eurograbber-arrested-7000013580/
- L'auteur du DDoS contre SpamHaus arrêté en Espagne
  - Dans un camping car
    - http://www.bbc.co.uk/news/technology-22314938
- Le leader de LulzSec arrêté en Australie
  - http://www.itnews.com.au/News/340983,it-security-firm-names-sydneys-lulzsec-hacker.aspx
  - http://www.tenable.com/blog/our-company-our-mission-bringing-cybercriminals-to-justice
- L'auteur de SpyEye arrêté en Thaïlande
  - http://www.scmagazineuk.com/spyeye-trojan-developer-and-marketer-extradited-to-us/article/292418/

Malwares, spam et fraudes

- vSkimmer
  - Un malware qui collecte les CB … sur les terminaux de paiement Windows
    - https://blogs.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals
- La fraude à la CB passe désormais … par les achats alimentaires en ligne
  - Moins surveillés
    - http://www.lefigaro.fr/conso/2013/04/11/05007-20130411ARTFIG00662-la-fraude-a-la-carte-bancaire-s-industrialise.php
- TDOS: déni de service contre les services d'urgence aux USA
    - http://krebsonsecurity.com/wp-content/uploads/2013/04/DHSEM-16-SAU-01-LEO.pdf

Actualité (francophone)

- **Livre Blanc de la Défense 2013**
  - La cyberdéfense à l'honneur
    - http://www.gouvernement.fr/gouvernement/livre-blanc-2013-de-la-defense-et-de-la-securite-nationale
  - Respect de l'hygiène informatique
  - IDS pour tous
  - Notification de tous les incidents de sécurité
  - Inspections par l'ANSSI
    - http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/la-cybersecurite-au-coeur-du-nouveau-livre-blanc-sur-la-defense-et-la-securite.html
  - … et lutte informatique offensive
    - http://www.opex360.com/2013/04/30/la-france-devra-pouvoir-passer-a-loffensive-dans-le-cyberespace/
  - Voir aussi:
    - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202695560931-cybersecurite-electrochoc-en-vue-pour-les-entreprises-556936.php
    - https://www.cdse.fr/l-obligation-de-declaration-d.html?&id_mot=69

Actualité (francophone)

- ANSSI
  - Sécuriser son site Web
    - http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf
  - Avoir Java sur son poste de travail
    - http://www.ssi.gouv.fr/IMG/pdf/NP_Securiser_JRE_NoteTech.pdf
  - Utiliser OpenSSH correctement
    - http://www.ssi.gouv.fr/IMG/pdf/NP_OpenSSH_NoteTech.pdf
  - A comparer avec:
    - http://www.scmagazineuk.com/ssh-inventor-proposes-best-practice-guidance-in-face-of-poor-deployment-and-management-of-keys/article/289186/
  - Le TJM de l'ANSSI: 1000€/jour
    - http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027385171

- La DGCCRF jouera les clients mystère sur Internet
  - http://www.pcinpact.com/news/79589-les-agents-dgccrf-bientot-cyber-clients-mysteres.htm

Actualité (francophone)

- **CNIL**
  - **Résultat de l'étude Mobilitics sur iPhone**
    - **http://www.cnil.fr/linstitution/actualite/article/article/voyage-au-coeur-des-smartphones-et-des-applications-mobiles-avec-la-cnil-et-inria/**
  - **La CNIL inspecte 250 sites Web français**
    - **http://www.cnil.fr/linstitution/actualite/article/article/journee-daudit-en-ligne-a-la-cnil-les-250-principaux-sites-informent-ils-suffisamment-les-inte/**
  - **Le G29 des CNIL vs. Tablettes et SmartPhones**
    - **http://www.cnil.fr/linstitution/actualite/article/article/les-recommandations-du-g29-sur-les-applications-mobiles-pour-smartphones-ou-tablettes/**

- **ARJEL**
  - **Premier retrait d'agrément**
    - **http://www.arjel.fr/Decision-de-la-Commission-des,929.html**

Actualité (francophone)

- **Organisation de la DGSIC**
  - http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000027385669&dateTexte=&oldAction=rechJO&categorieLien=id
- **Le français, langue officielle de la République**
  - http://circulaires.legifrance.gouv.fr/pdf/2013/05/cir_36918.pdf
- **La Cyber Réserve Citoyenne**
  - … vue d'ailleurs
    - http://www.zdnet.com/france-gets-crack-team-of-civilian-cyberdefenders-who-wont-get-to-do-much-7000013596/
- **Cap Digital**
  - Plan stratégique 2018
    - http://www.capdigital.com/retour-sur-restitution-plan-strategique-cap-2018/
- **Il y a trop "d'agences" en France ☺**
  - http://circulaires.legifrance.gouv.fr/pdf/2013/04/cir_36773.pdf

Actualité (francophone)

- Pas de taxe sur les données personnelles …
  - … mais sur la bande passante (?!)
    - http://www.numerama.com/magazine/25757-bercy-veut-taxer-la-bande-passante-les-fai-seraient-d-accord.html
  - Le CNN travaille dessus également
    - http://www.itespresso.fr/cnn-ouvre-concertation-fiscalite-numerique-63774.html

- Le rapport Lescure
  - Suppression de HADOPI
  - Taxe sur les tablettes (?!)
  - Révision du statut d'hébergeur
    - http://www.culture-acte2.fr/

Actualité (francophone)

- CIGREF
  - "Indice de l'innovation par les TIC"
    - http://images.cigref.fr/Publication/2013-Innovation-entreprise-numerique-Indice-Innovation-TIC-CEFRIO-CIGREF.pdf

- Le FreePlayer ne lit pas les fichiers contenant "S*xx*E*yy*"
  - Bug ou feature ?
    - http://www.freenews.fr/spip.php?article13336

Actualité (francophone)

- Yahoo! ne rachètera pas DailyMotion
  - http://www.lefigaro.fr/societes/2013/05/01/20005-20130501ARTFIG00069-sous-la-pression-de-montebourg-yahoo-aurait-renonce-a-dailymotion.php
- HSC en redressement judiciaire
  - http://www.societe.com/societe/herve-schauer-consultants-444475891.html
- Cassidian rachète Arkoon
  - http://www.cassidian.com/fr_FR/web/guest/latest-news/-/asset_publisher/T6Gp/content/id/164075
- "Secure Identity Alliance"
  - 3M + Gemalto + Morpho + Oberthur
    - http://secureidentityalliance.org/

Actualité (francophone)

- "Delta Search"
  - Le faux moteur de recherche qui cartonne en France
    - http://fjb.blogs.com/weblog/2013/04/delta-search.html
- L'espionnage industriel devient "*mainstream*"
    - http://www.leparisien.fr/seine-et-marne-77/chefs-d-entreprise-gare-aux-espions-10-05-2013-2792517.php
- Ne dites plus SSII
  - … mais ESN
    - http://www.syntec-numerique.fr/content/les-ssii-changent-de-nom-et-se-renomment-esn

Actualité (anglo-saxonne)

- Les USA accusent officiellement la Chine d'espionnage informatique
  - http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf
- CISPA officiellement voté
  - http://www.lemonde.fr/technologies/article/2013/04/19/le-cispa-vote-par-la-chambre-des-representants-americaine_3163177_651865.html
- La FTC enquête sur la (non) mise à jour des téléphones Android par les opérateurs
  - Sur requête de l'ACLU
    - http://arstechnica.com/security/2013/04/wireless-carriers-deceptive-and-unfair/
- Rechercher sur le Web … comme la NSA
  - http://www.nsa.gov/public_info/_files/Untangling_the_Web.pdf

Actualité (européenne)

- Il faut renforcer la sécurité au niveau européen
  - http://www.senat.fr/rap/l12-491/l12-491.html
- Une nouvelle agence européenne: "eu-LISA"
  - Gestion du système d'information Schengen
    - http://www.europarl.europa.eu/news/fr/headlines/content/20130426STO07652/html/Une-nouvelle-agence-europ%C3%A9enne-pour-les-syst%C3%A8mes-d%27information-%C3%A0-grande-%C3%A9chelle
- Publications de l'ENISA
  - L'Internet peut-il mourir ?
    - http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability/at_download/fullReport
- Cyber-exercice de l'OTAN
  - 24 avril 2013
    - http://www.ccdcoe.org/412.html

Actualité (Google)

- Google rejoint la Fast Identity Online Alliance (FIDO)
- Des services payants sur YouTube
  - http://youtube-global.blogspot.fr/2013/05/yt-pc-2013.html
- Google Death
  - http://googlepublicpolicy.blogspot.fr/2013/04/plan-your-digital-afterlife-with.html
- Il est interdit de revendre ses Google Glasses
  - http://www.wired.com/gadgetlab/2013/04/google-glass-resales/
- Migration de GMail vers Yahoo! pour les clients BSkyB
  - Détail: ils ont retrouvé tous leurs emails effacés depuis la création du compte
    - http://www.theregister.co.uk/2013/04/05/bskyb_migration_to_yahoo_from_gmail_proves_big_headache_for_subscribers/print.html

Actualité (Apple)

- iMessage … est trop sécurisé !
  - D'après la DEA
    - http://news.cnet.com/8301-13578_3-57577887-38/apples-imessage-encryption-trips-up-feds-surveillance/

Actualité (crypto)

- Comment l'Arabie Saoudite monte une autorité de certification *délibérément malveillante*
  - http://www.thoughtcrime.org/blog/saudi-surveillance/
- IBM publie une librairie de chiffrement homomorphique
  - HELib
    - http://nakedsecurity.sophos.com/2013/05/05/ibm-takes-big-new-step-in-cryptography/

Actualité

- Conférences passées
  - HES 2013
  - HITB Amsterdam 2013
    - https://conference.hitb.org/hitbsecconf2013ams/materials/
    - Prendre le contrôle d'un avion … avec un téléphone ?
      - Hmm …
    - Les caméras sur IP sont trouées
      - http://sourceforge.net/projects/foscam-util/
      - http://www.openipcam.com/

Actualité

Conférences à venir

- NoSuchCon 2013
- HIP / NDH 2013
- GreHack 2013

- OHM 2013
  - https://ohm2013.org/site/

Actualité

- **Sorties logicielles**
  - **BinWalk 1.2**

Actualité

- L'OCDE attend vos contributions
  - … sur la cybersécurité
    - http://www.oecd.org/sti/ieconomy/OECD-Security-Guidelines-Review-flyer-13-04.pdf
- Le Samsung Galaxy S4 certifié par les militaires américains
  - Avec le module Knox
    - http://french.yonhapnews.co.kr/techscience/2013/05/03/0700000000AFR20130503001000884.HTML
- McAfee rachète StoneSoft
- Twitter #Music
  - … mais pas en France (pour le moment)
- O'Reilly Open Books Project
    - http://oreilly.com/openbook/

Divers

- ISS migre de Windows XP à Debian 6
  - http://news.techworld.com/security/3446685/linux-replaces-windows-xp-on-international-space-station-laptops/
- Slashdot interviewe John McAfee
  - http://features.slashdot.org/story/13/05/07/2017203/interview-john-mcafee-answers-your-questions
- Ajouter un logo de chien
  - … a doublé les ventes
    - http://www.webpop.com/blog/2013/04/16/can-a-puppy-sell-a-cms
- Chuck Norris s'est rasé
  - http://now.msn.com/chuck-norris-has-shaved-his-beard
- BudWeiser crée des verres RFID
  - … pour se connecter sur Facebook en trinquant
    - http://leblog.wcie.fr/2013/04/25/budweiser-cree-un-verre-avec-puce-reliee-a-facebook-trinquez-gagnez-un-ami/
- Des HLM … dans le Cloud
  - http://www.leparisien.fr/montrouge-92120/et-si-on-se-chauffait-avec-des-ordinateurs-18-03-2013-2649039.php

Divers

- "Black Annex": un jeu Steam …
  - … entièrement développé en QBasic
    - http://www.pcworld.com/article/2033318/black-annex-is-the-best-qbasic-game-youve-ever-seen.html

Divers

- **Source: http://www.bcgreen.com/comments/2005/scojob.html**

Job opportunity

Troll Herder

There's a new exciting opportunity at SCO that is as unique as SCO's business plan.

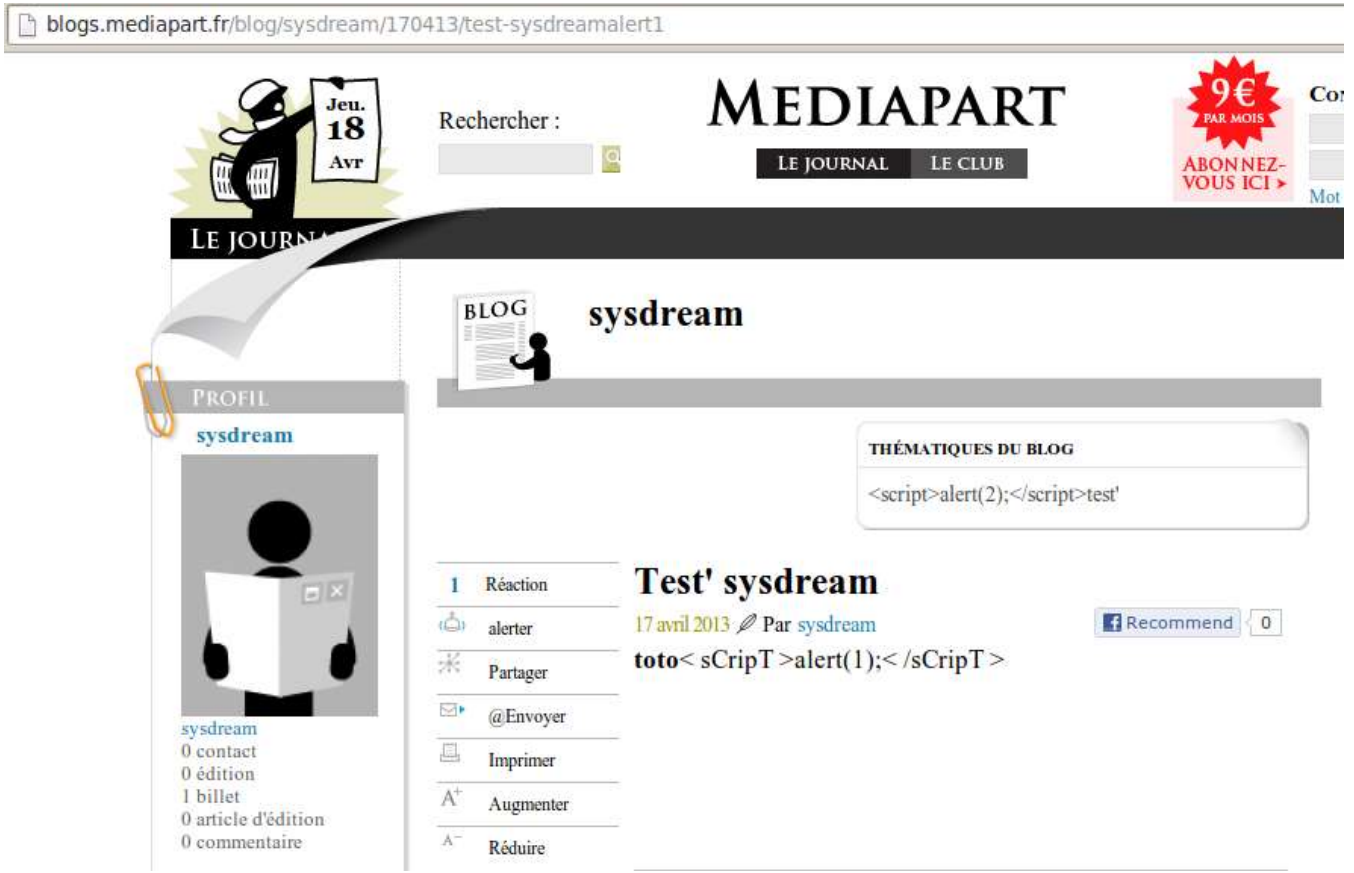
We're looking for a troll herder. We need someone good with open flames and with demonstrated experience at coordinating and controlling trolls. A good understanding of trollspeak is highly desirable, but an ability to communicate with worms may be acceptable. English is desirable but not necessery.

? We are also looking for someone who is good at working alone in large crowds, demonstrates unique logic and is able to carry an argument in the face of extreme adversity and evidence to the contrary.

The position is available immediately, as our last pro was eaten by a spider. To apply leave an apropriate message on this site.

Divers

- **Pentest #fail**
  - **Source: https://twitter.com/Xst3nZ/status/324924389860704256/photo/1**



Questions / réponses

- **Questions / réponses**

- **Prochaine réunion**
  - **Mardi 11 juin 2013**