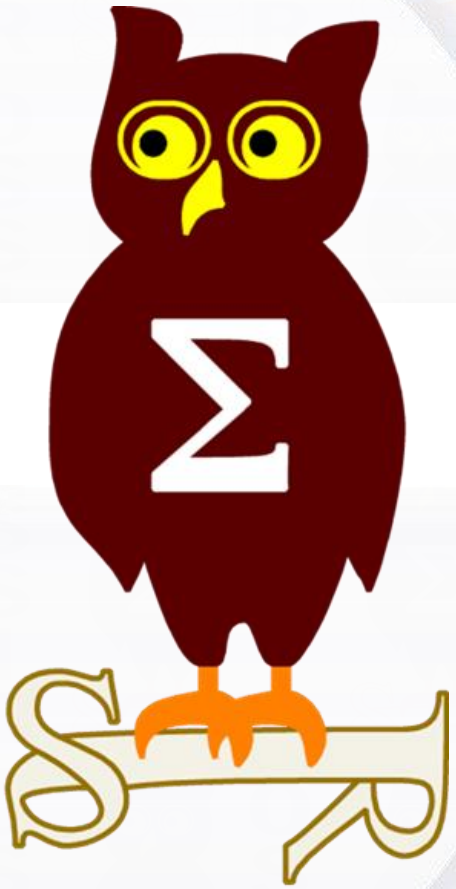


Revue d'actualité

10/02/2015

Préparée par

*Ary **K**OKOS*
*Arnaud **S**OULLIE @arnaudsoullie*
*Vladimir **K**OLLA @mynameisv_*

Failles / Bulletins / Advisories

Microsoft - Avis Janvier 2015

MS15-001 Vulnérabilité dans "Windows Application Compatibility" (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS13-031, MS13-046, MS13-048 et MS13-063
- Exploit:
  - Élévation de privilèges depuis AppCompat grâce à une impersonification de l'appelant
  - Publiquement publié avant correction par Google
    https://code.google.com/p/google-security-research/issues/detail?id=128
- Crédits:
  - Non crédité sur le site de Microsoft (CVE-2015-0002)

MS15-002 Exécution de code à distance par Telnet (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Buffer overflow sur le service Telnet aboutissant à une exécution de code
  - Code en Python pour tester la présence de la vulnérabilité : http://pastebin.com/aTxca42w
  - Quelques détails (en Chinois) : http://drops.wooyun.org/papers/4621
- Crédits:
  - Daiyuu Nobori et Christopher Hiroshi Higuchi SMITH de l'Université de Tsukuba (CVE-2015-0014)

Failles / Bulletins / Advisories

Microsoft - Avis Janvier 2015

MS15-003 Vulnérabilité dans Windows User Profile Service (ProfSvc) (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Élévation de privilèges en chargeant un profil depuis le service User Profile Service, uniquement pour un utilisateur déjà authentifié
  - Publiquement publié avant correction par Google https://code.google.com/p/google-security-research/issues/detail?id=123
- Crédits:
  - Non crédité sur le site de Microsoft (CVE-2015-0004)

MS15-004 Élévation de privilèges dans Terminal Service WebProxy (1 CVE) [Exploitabilité 0]

- Affecte:
  - Windows (toutes versions supportées) sauf 2003
- Exploit:
  - Évasion de la sandbox IE grace à un appel à StartRemoteDesktop par lequel l'attaquant peut contrôler l'application à exécuter http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2015-0016-escaping-the-internet-explorer-sandbox/
  - Crédits:
  - Equipe Threat Intel de Symantec (CVE-2015-0016)

Failles / Bulletins / Advisories

Microsoft - Avis Janvier 2015

MS15-005 Contournement de Network Location Awareness (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Contournement de Network Location Awareness (et donc du firewall windows) par un attaquant répondant aux requêtes DNS et LDAP d'un utilisateur sur le même réseau
- Crédits:
  - Jonas Vestberg de Sentor (CVE-2015-0006)

MS15-006 Vulnérabilité dans Windows Error Reporting (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 8.x, 2012 R2/Core, RT
  - Remplace MS14-071
- Exploit:
  - Accès à la mémoire protégée de processus par un administrateur
- Crédits:
  - Alex Ionescu (CVE-2015-0001)

Failles / Bulletins / Advisories

Microsoft - Avis Janvier 2015

MS15-007 Déni de service dans Network Policy Server (NPS) (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows server 2003, 2008, 2008 R2, 2012, 2012 R2
- Exploit:
  - Déni de service par l'envoie d'un nom d'utilisateur spécialement formaté à Internet Authentication Service (IAS) ou Network Policy Server (NPS)
- Crédits:
  - ?

MS15-008 Vulnérabilité dans le Kernel (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Élévation de privilèges par l'interception d'une requête WebDAV (mrxdav.sys) et redirection vers un autre fichier
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2015-0011)

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

Contournement de la Same Origin Policy sous Internet Explorer

- Un site malveillant peut exécuter du code dans un autre domaine
- Utilisation habile de 2 iframes et de timers
- Affecte Internet Explorer 10 et 11 sous Windows 7 et 8.1

POC : http://www.deusen.co.uk/items/insider3show.3362009741042107/
http://seclists.org/fulldisclosure/2015/Feb/0
http://innerht.ml/blog/ie-uxss.html

```
<iframe src="redirect.php"></iframe>
<iframe src="https://www.google.com/images/srpr/logo11w.png"></iframe>
<script>
    top[0].eval('_=top[1];with(new
XMLHttpRequest)open("get","sleep.php",false),send();_.location="javascript:alert(document.domain)"');
</script>
```

Encore des 0 days publiées par Google

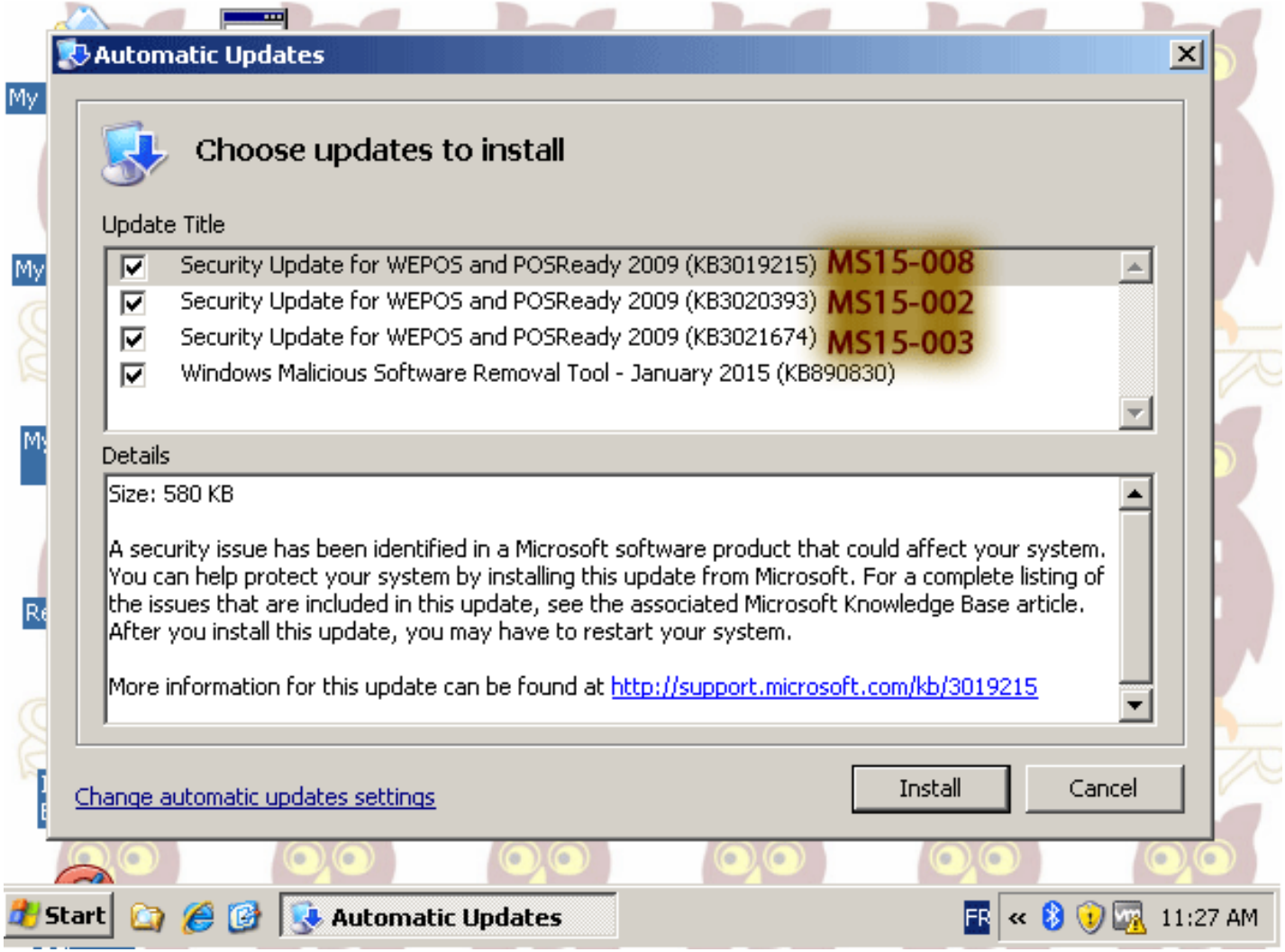
- Un serveur SMB peut forcer un client à ouvrir un fichier
  https://code.google.com/p/google-security-research/issues/detail?id=138
- Exécution de code à l'ouverture d'un fichier RTF dans Office 2007
  https://code.google.com/p/google-security-research/issues/detail?id=132

Failles / Bulletins / Advisories

Microsoft - Avis Janvier 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Autre

Windows 7

- Fin du support standard (au 13 janvier 2015)
- Mises à jours de sécurité jusqu'au 14 janvier 2020
  http://windows.microsoft.com/en-us/windows/lifecycle

Windows 10

- Spartan, le nouveau navigateur et son moteur EdgeHTML
  http://www.clubic.com/windows-os/windows-10/actualite-751355-windows-10-testez-spartan-sein-derniere-build.html
- Protection des traitements des polices (Usermode Font Driver Host)
  https://twitter.com/crypt0ad/status/558798426989535232

Outlook pour mobile

- Même sur un terminal managé, il est possible d'utiliser des documents personnels, par OneDrive ou Dropbox
- Envoie d'informations sensibles (mot de passe...) dans le Cloud Microsoft
  https://blog.winkelmeyer.com/2015/01/warning-microsofts-outlook-app-for-ios-breaks-your-company-security/

Failles / Bulletins / Advisories

Système (principales failles)

Adobe Flash

- Use-after-free aboutissant à une exécution de code (CVE-2015-0311)
  http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-cve-2015-0311-flash-zero-day-vulnerability/
- Code d'exploitation (remis en cause)
  http://kernelmode.info/forum/viewtopic.php?f=16&t=3697&p=25065#p25065
- Exploité dans la nature par le malware Angler
  http://blogs.cisco.com/security/talos/angler-variants
- Et par beaucoup d'autres
  http://malware.dontneedcoffee.com/2015/01/cve-2015-0311-flash-up-to-1600287.html

Adobe Flash encore...

- Nouvelle 0-day exploitée dans la nature (pas encore de CVE)
  http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/
- Heureusement, Youtube passe à HTML5. Flash ne sert plus à rien 
  http://youtube-eng.blogspot.jp/2015/01/youtube-now-defaults-to-html5_27.html

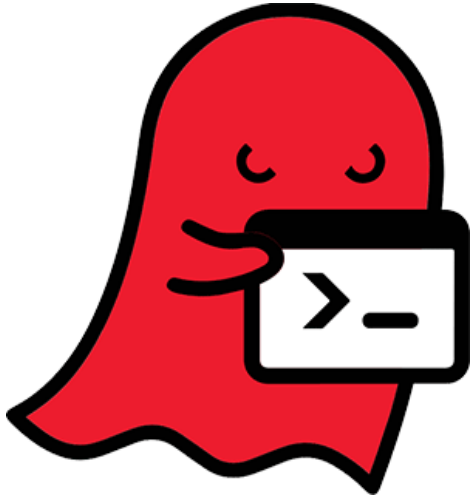
VLC

- Exécutions de code (CVE-2014-9597 et CVE-2014-9598)
- A l'ouverture de fichiers FLV et M2V
  http://seclists.org/fulldisclosure/2015/Jan/72

Failles / Bulletins / Advisories

Système (principales failles)

Ghost par Qualys



- Exécution de code à distance par glibc (CVE-2015-0235)
  http://www.frsag.org/pipermail/frsag/2015-January/005722.html
- Explication détaillée
  http://www.openwall.com/lists/oss-security/2015/01/27/9
- Liste non exhaustive des périmètres “potentiellement” vulnérables
  - Debian et Ubuntu
  - RedHat et CentOS
  - Slackware
  - Exim mais pas Postfix, avec un exemple :
    http://packetstormsecurity.com/files/130171/Exim-ESMTP-GHOST-Denial-Of-Service.html
- Mais les risques étaient finalement limités, peu d’applications réellement exploitables
  http://seclists.org/oss-sec/2015/q1/283

Failles / Bulletins / Advisories

Système (principales failles)

La Backdoor de Lotus Notes

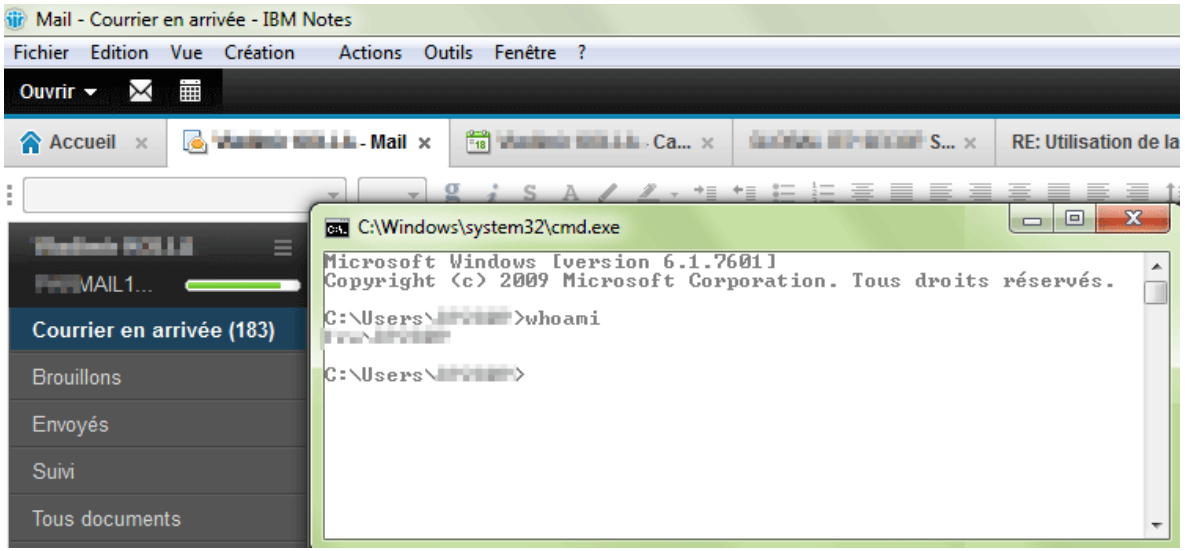
- Service tournant en tâche de fond avec les droits SYSTEM
- Possibilité de lui passer des commandes
  - et d'exécuter un processus avec les droits SYSTEM
- Découvert par des auditeurs de Cogiceo 

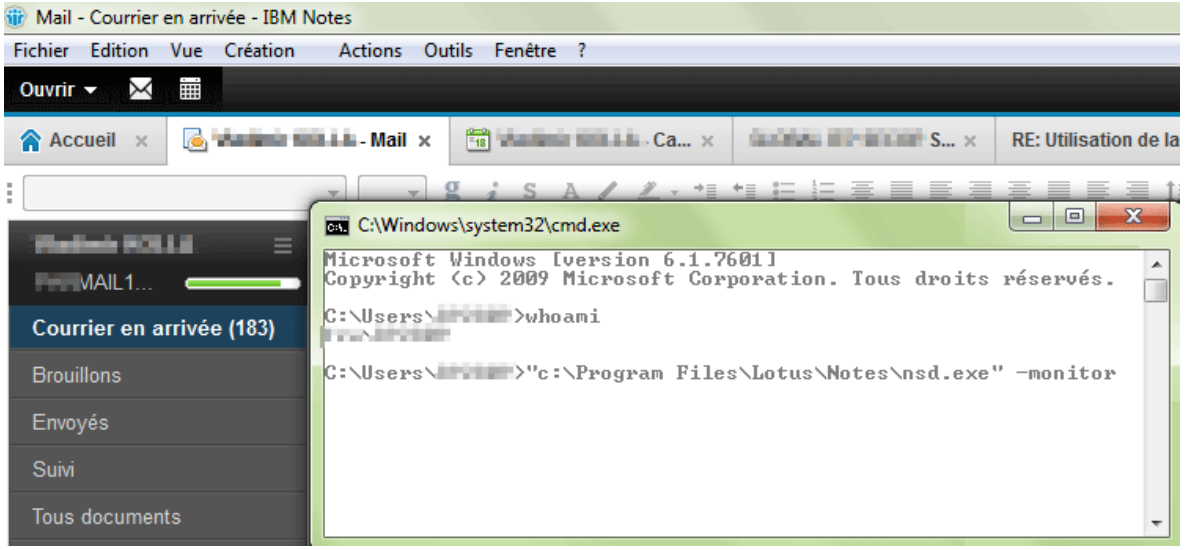
http://reniknet.blogspot.fr/2015/01/la-cas-de-la-backdoor-incluse-dans.html

Failles / Bulletins / Advisories

Système (principales failles)

La Backdoor Lotus Notes

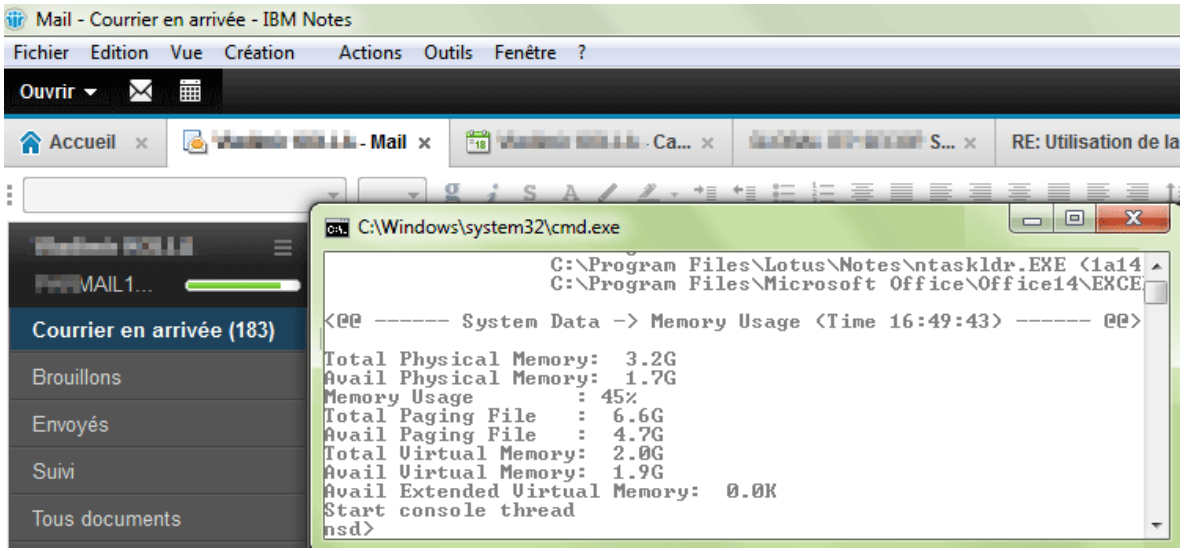


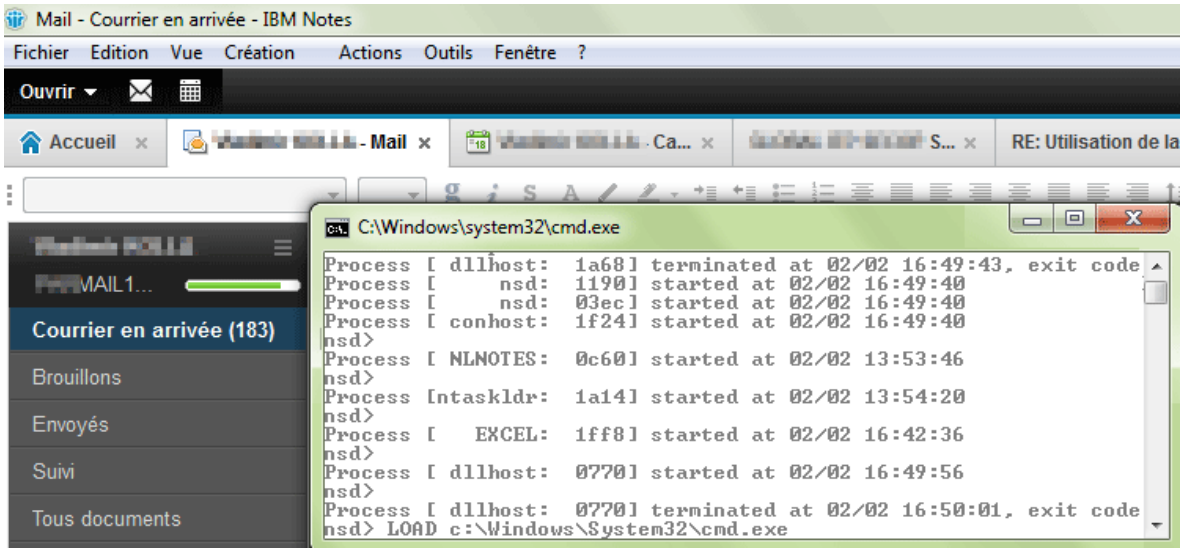


Failles / Bulletins / Advisories

Système (principales failles)

La Backdoor Lotus Notes

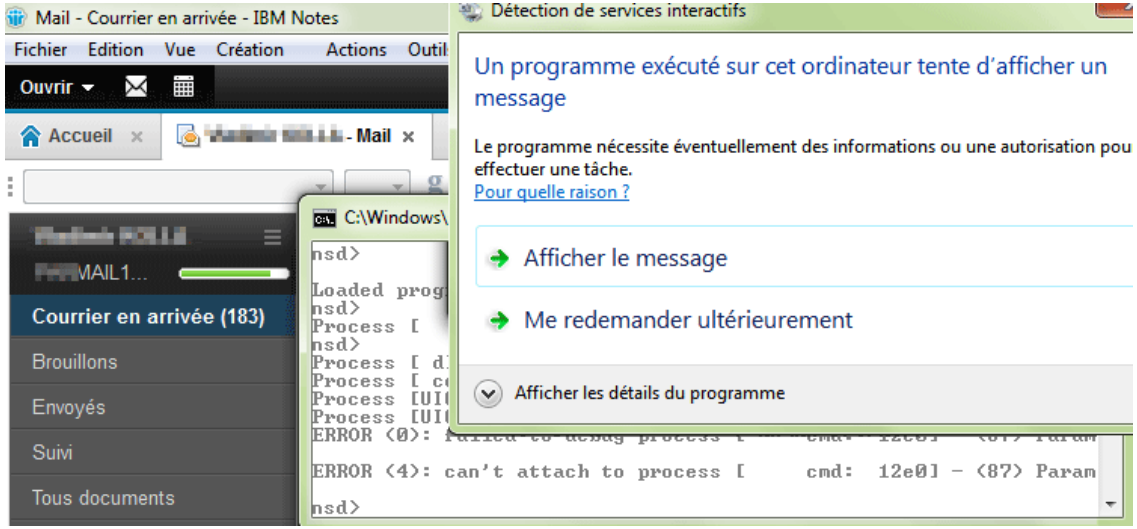


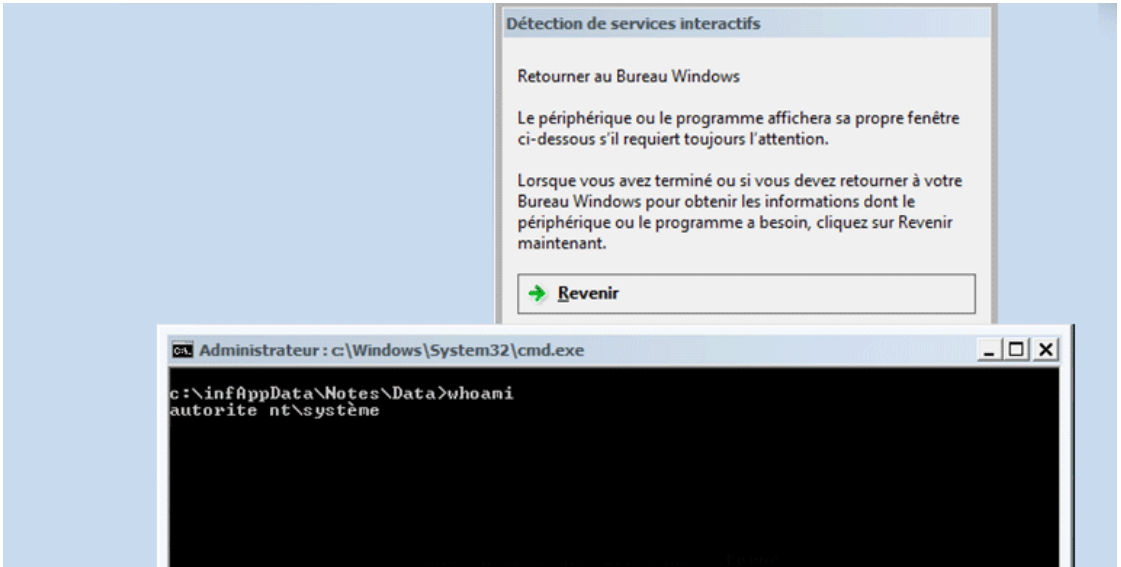


Failles / Bulletins / Advisories

Système (principales failles)

La Backdoor Lotus Notes

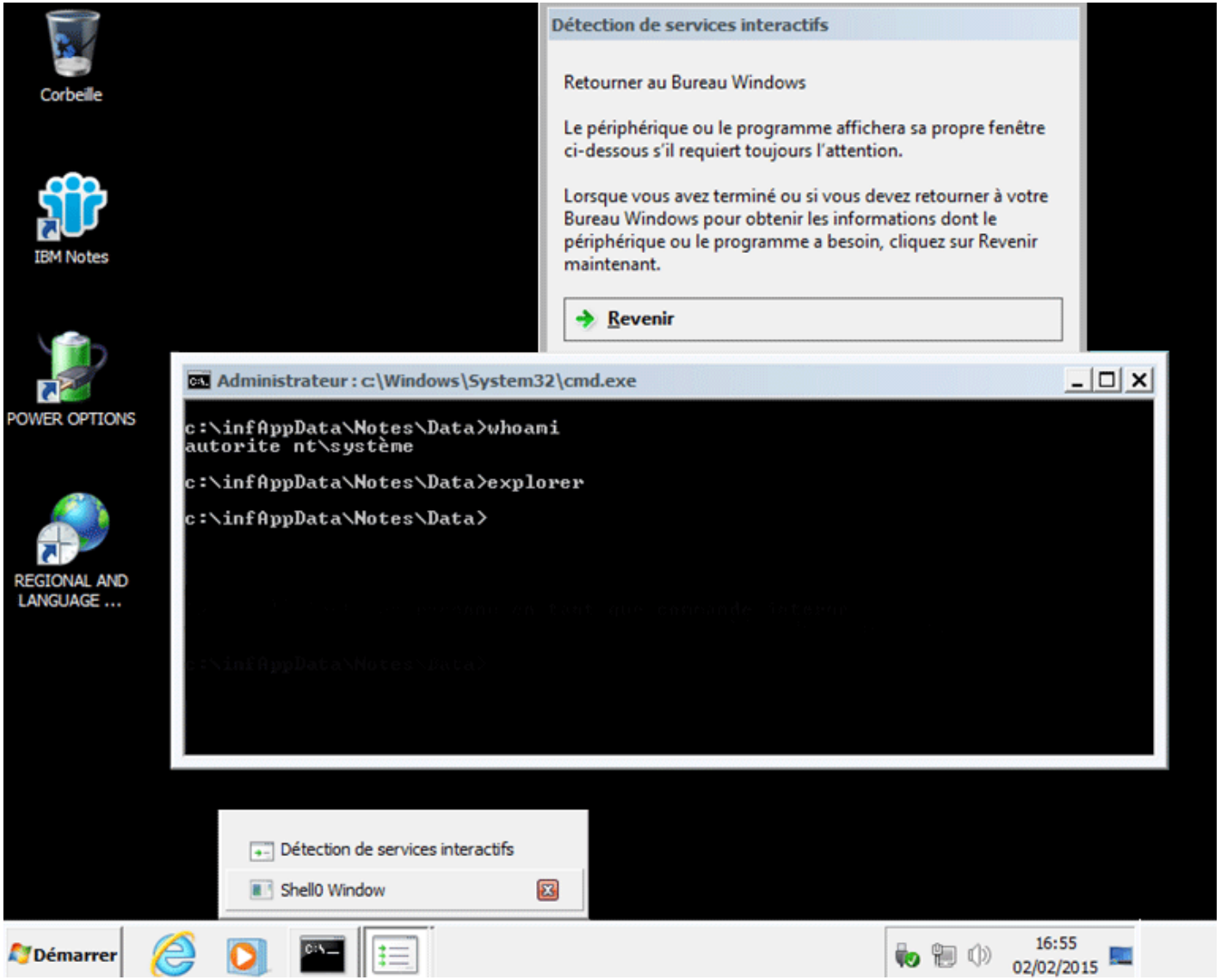




Failles / Bulletins / Advisories

Système (principales failles)

La Backdoor Lotus Notes



Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco ASA et ACE (Application Control Engine Appliances)

- Vulnérables à Poodle
  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-8730

Failles / Bulletins / Advisories

Virtualisation

VMWare

- Déni de service sur OpenSSL et Poodle (CVE-2014-3513, CVE-2014-3567, CVE-2014-3566, CVE-2014-3568)
- Dénis de service
  - Lors du traitement de fichier XML (CVE-2014-3660)
  - Localement, sur vmware-authd (CVE-2015-1044)
  - Localement, avec le système de fichier Host Guest File System (HGFS) (CVE-2015-1043)
- Élévation de privilèges localement (CVE-2014-8370)
  http://www.vmware.com/security/advisories/VMSA-2015-0001.html

Failles / Bulletins / Advisories

Apple

3 0-days plubliées par Google

- Évasion de sandbox grâce au service networkd
  https://code.google.com/p/google-security-research/issues/detail?id=130&q=label%3AVendor-Apple
- I/O Kit, déréférencement de pointeur NULL
  https://code.google.com/p/google-security-research/issues/detail?id=135&q=label%3AVendor-Apple
- I/O Kit bluetooth, exécution de code
  https://code.google.com/p/google-security-research/issues/detail?id=136&q=label%3AVendor-Apple

http://arstechnica.com/security/2015/01/google-drops-three-os-x-0days-on-apple/

Le script d'infection d'un OS X présenté à ShmooCon

https://gist.github.com/secretsquirrel/2ba497786027472f98dd

Failles / Bulletins / Advisories

Google

Google publie des vulnérabilités des autres...

- Mais ne corrige pas les siennes exposant 60% de ses clients (Android 4.3 Jelly Bean)
  https://plus.google.com/+AdrianLudwig/posts/1md7ruEwBLF
  https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior
- Un workarround est proposé mais pas exhaustif
  http://www.cnet.com/news/google-leaves-most-android-users-exposed-to-hackers/
- cf. parabole biblique de la paille et de la poutre

Contournement de la Sandbox Google App Engine

- Principalement du fait de Java JRE
  http://www.net-security.org/secworld.php?id=17765
  http://www.security-explorations.com/en/SE-2014-02-faq.html

Failles / Bulletins / Advisories

Crypto

Collisions sur des identifiants de clef GPG de 32 bits

- 4 s. avec un bon GPU
  http://www.theregister.co.uk/2014/12/01/evil_researchers_dupe_every_32bit_gpg_print/
  https://evil32.com/

Failles / Bulletins / Advisories

Divers

BlackPhone

- Exécution de code dans le client de messages instantanés Silent Text
- Lors de la désérialisation des messages encodés en JSON
  http://blog.azimuthsecurity.com/2015/01/blackpwn-blackphone-silenttext-type.html

Vulnérabilité sur les téléphones LG

- Une vulnérabilité a été découverte dans la fonctionnalité « *On Screen Phone* », qui permet de piloter son téléphone à distance, depuis un PC (via USB, Bluetooth ou WiFi).
  - Activée par défaut, et ne peut pas être désactivée.
- En théorie, l'utilisateur doit valider cet accès distant en cliquant sur une fenêtre de son écran. Malheureusement, cette étape n'est pas obligatoire et un PoC est disponible sur Internet pour prendre le contrôle total de l'appareil, sans interaction de la part de l'utilisateur. L'attaquant dispose alors d'un accès complet au téléphone.
  https://github.com/irsl/lgosp-poc/

Jabberbleed ?

- Mauvais traitement de l'encodage UTF-8
  https://github.com/jabberd2/jabberd2/issues/85

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Les nouveautés dans les pack d'exploitation

- Recherche de plugins de navigateur vulnérables
- Détection de certains antivirus
- De l'Obfuscation
- Conclusion : beaucoup de travail mais exploitant majoritairement des vulnérabilités disposant de correctif
  http://blog.trendmicro.com/trendlabs-security-intelligence/whats-new-in-exploit-kits-in-2014/

Hack 0.2 avec l'utilisation d'outils vieux de 12 ans

- Pour des attaques ciblées
  http://blog.trendmicro.com/trendlabs-security-intelligence/over-a-decade-and-still-running-targeted-attack-tool-hides-windows-tasks/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Le virus REGIN serait bien Américano-Anglais (cf. Revue d'actu du 2014-12-09)

http://www.cio.com/article/2876114/link-between-nsa-and-regin-cyberespionage-malware-becomes-clearer.html

- Le module KeyLogger QWERTY… en base64 dans un PDF, très similaire à REGIN
  http://www.spiegel.de/media/media-35668.pdf

Le reportage Citizen Four disponible sur Cryptome

http://cryptome.org/2013/11/snowden-tally.htm

Programmes d'espionnage du Canada

- BADASS
  - Collecte de toutes les informations non chiffrées sortant des Smartphones
  - Pour obtenir des empreintes et suivre l'utilisateur
- LEVITATION
  - Collecte d'information sur 10 à 15 millions de fichiers quotidiennement uploadés sur internet

http://www.net-security.org/secworld.php?id=17892

Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS de sites français ?

- 20 minutes, l'Express, Marianne, Le Parisien, Mediapart, France Info…
- Ah non… juste une boucle niveau 2 sur le réseau d'administration out-of-band d'Oxalide :-)
  - http://www.linformaticien.com/actualites/id/35519/oxalide-explique-les-causes-de-sa-panne.aspx

DDoS sur l'AFNIC

- Enregistrement des noms de domaines .fr coupé durant 2h
  http://www.zdnet.fr/actualites/ddos-le-site-de-l-afnic-vise-par-une-attaque-39813445.htm

L'attaque du Poivre du Sichuan - Stéphane BORTZMEYER

- Illustration avec l'attaque sur le serveur de la Quadrature du Net
  https://benjamin.sonntag.fr/DDOS-on-La-Quadrature-du-Net-analysis

Rapport sur le DDoS selon Kaspersky

- Le coût d'une attaque pourrait osciller entre $52k et $444k
  https://press.kaspersky.com/files/2014/11/B2B-International-2014-Survey-DDoS-Summary-Report.pdf
- Et l'infographie qui va bien
  http://www.kaspersky.com/about/news/business/2015/A-single-DDoS-attack-can-cost-a-company-more-than-400000-dollar

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Lizard Squad (suite, cf. Revue d'actu du 2015-01-13)

- Fausse attribution de la panne de Facebook et Instagram

  https://twitter.com/LizardMafia/status/559963134006292481

  https://developers.facebook.com/status/issues/393998364112264/

- De nombreux membres arrêtés

  http://www.dailymail.co.uk/news/article-2893549/Spokesman-Lizard-Squad-hacking-group-allegedly-attacks-Microsoft-Sony-arrested-PayPal-thefts.html

  http://www.dailymail.co.uk/news/article-2913619/British-teenager-18-arrested-connection-Christmas-cyber-attacks-Playstation-Xbox-networks-joint-FBI-British-investigation.html

  https://www.youtube.com/watch?v=fPX8yCBdIZ8

- La base de données de leur service de DDoS volée et publiée

  http://krebsonsecurity.com/2015/01/another-lizard-arrested-lizard-lair-hacked/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Sony (suite de 2014)

- La NSA espionnait la Corée du Nord depuis 2010 et aurait des preuves du piratage de Sony
  http://www.spiegel.de/media/media-35679.pdf
- Publication des résultats décalés
  http://www.sony.net/SonyInfo/IR/news/20150123_E.pdf
- Enquête + dédommagements + réparations des infra = $15m
  - $20m supplémentaire provisionnés

Sony à nouveau

- Un second piratage par des Russes ?
  http://www.networkworld.com/article/2880073/russian-hackers-have-a-foothold-in-sony-pictures-network-security-firm-says.html

Attaques anti-Charlie

- Près de 20 000 sites piratés ou plutôt “défacés”
- Surtout à l’opportunisme
  http://www.01net.com/editorial/641277/plus-de-20-000-sites-francais-pirates-par-des-hackers-anti-charlie-hebdo/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Skeleton Key

- Backdoor dédiée aux domaines Microsoft
  - Extraction des mots de passe en mémoire
  - Patch des DC en mémoire pour autorisé tout utilisateur avec un mot de passe choisir par la backdoor
  - S'efface après patch et doit réinfecter un DC après reboot
    http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/
- Selon Symantec, lié une ancienne backdoor Backdoor.Winnti
  http://www.symantec.com/connect/blogs/backdoorwinnti-attackers-have-skeleton-their-closet
- Patch implémenté dans Mimikatz 2003-2012r2
  https://github.com/gentilkiwi/mimikatz/releases/tag/2.0.0-alpha-20150122

Anthem piraté

- 2ème assureur santé américain
- 70 à 80 millions de donnes utilisateur (nom, adresse, numéro de sécurité sociale, salaires, …)
- A priori pas de données médicales
- Campagne de phishing en cours
  http://www.anthemfacts.com/faq
  http://www.theregister.co.uk/2015/02/05/anthem_hacked/
  http://threatpost.com/anthem-data-breach-could-affect-millions-of-consumers/110867

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Le fabricant français de smartphones Archos victime d'une attaque par injection SQL, 100.000 utilisateurs impactés

http://www.scmagazineuk.com/up-to-100k-archos-customers-compromised-by-sql-injection-attack/article/395642/

Verizon patche une vulnérabilité permettant de lire les emails de ses clients

- A priori une vulnérabilité dans l'une des APIs de l'application My FIOS
- Classique problème de contrôle d'accès

```
getEmail?format=json&uid[his user name]
```

http://www.cnet.com/news/verizon-races-out-fix-for-email-security-flaw/
http://securityaffairs.co/wordpress/32428/hacking/verizon-fios-app-flaw.html

Le monde :Comment notre compte Twitter a été piraté

- Belle démarche de transparence
  http://www.lemonde.fr/pixels/article/2015/01/24/comment-notre-compte-twitter-a-ete-pirate_4562506_4408996.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Découverte d'une nouvelle variante de CTBLocker

- Encore un cryptolocker
- A priori une campagne d'ampleur
- Des IOCs dans le bulletin d'alerte du CERT-FR
- Analyse détaillée : http://christophe.rieunier.name/securite/CTB-Locker/CTB-Locker_analysis.php

Confirmation de commande: No.H3623686070577VQ

Inbox x Pub x

Roger Domino <resealed@apcs.asso.fr> 9:29 AM (6 hours ago)

to

Chère Client(e),

Merci de votre commande!

Voici les détails de votre commande:
Numéro de commande: H3623686070577VQ
Date de la commande: 03.01.2015 08:28:25
Option de livraison: Prioritaire

Ce message confirme que vous avez acheté les articles suivants :

---

1 x CHI MEI N154I3-L02 HM - LCD 15.4 WXGA, 1280x800, brillante, 30 Pin: EUR 97.41
4 x APC SMART-UPS 1000 LCD 1000VA IN LINE, 8 PRISES IEC, RS232/USB: 448.32*4 = EUR 1793.28
1 x ZYXEL - MODEM-ROUTEUR ADSL2+ P660H: EUR 90.5
2 x FANTEC ALUMOVIE - LECTEUR MULTIMEDIA USB2,HDMI,FULL HD-1080p: 62.43*2 = EUR 124.86
1 x MICROSOFT OFFICE 2010 PROFESSIONNEL BOITE COMPLETE: EUR 587.52
1 x BITDEFENDER INTERNET SECURITY 2013 2 ANS - 3 POSTES: EUR 53.72

Total HT: EUR 2747.29
TVA: EUR 521.99

Montant total pour cette commande : EUR 3269.28

Vous trouverez ci-joint une facture pro forma de même que les conditions de paiement et de livraison en annexe de ce courrier électronique.

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Des jauges de station service sur Internet

- Automated Tank Gauges (ATGs) accessibles sur le port TCP 10001
  https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges

Vulnérabilité des systèmes BMW Connected Drive

- Utilisation de clés de chiffrement identiques pour toutes les voitures
- Validation des commandes envoyées par une requête non-chiffrée aux serveurs BMW
  http://m.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

Un malware pour drones Parrot

- Sera présenté à NullCon à Goa
- Permet de prendre le contrôle à distance d'une Drone
- Passant par une faille de l'autopilotage de l'AR Drone 2.0 de Parrot
  http://www.linformaticien.com/actualites/id/35548/maldrone-une-faille-pour-hacker-un-drone-a-distance.aspx
  http://www.theregister.co.uk/2015/01/27/malware_backdoor_makes_parrot_ar_drones_squawk/
  http://www.01net.com/editorial/642968/une-faille-permet-de-pirater-les-drones-parrot-a-distance/

Rétro-ingénierie du protocole utilisé par le bracelet Nike+ Fuelband

http://www.evilsocket.net/2015/01/29/nike-fuelband-se-ble-protocol-reversed/

Rapports Annuels
Rapports et Prédictions

C'est la raison des rapports 2014

- Selon des éditeurs de solutions de sécurité hormis pour le Clusif et l'ENISA

- Akamai, The State of the Internet 2014Q3
  http://www.akamai.com/dl/akamai/akamai-soti-q314.pdf
- Arbor, rapport annuel sur le DDoS en 2014
  http://www.arbornetworks.com/resources/infrastructure-security-report
- Kaspersky, sur les malwares en 2014
  http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/

- Clusif, Panorama de la cybercriminalité en 2014 (Bientôt)
  https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2015-Panorama-Cybercriminalite-annee-2014.pdf
- Rapport ENISA
  http://www.enisa.europa.eu/media/press-releases/enisa-draws-the-cyber-threat-landscape-2014

La biométrie pour remplacer les mots de passe

- Comment révoquer un doigt ou une rétine !!!?
- Ces données sont-elles secrètes ou juste… restreintes ?
  http://www.zdnet.fr/actualites/securite-la-biometrie-pourra-t-elle-remplacer-les-mots-de-passe-39813573.htm
- Serait pertinent en second facteur d'authentification

Crypto
Divers

CipherShed : un développeur répond à vos questions (ex-TrueCryptNext)

- Jason Pyeron a lancé un fil de questions et réponses sur Reddit :
  https://www.reddit.com/r/netsec/comments/2tde4l/i_am_jason_pyeron_of_the_ciphershed_project_ama/

MegaChat : la messagerie chiffrée par Mega

http://www.nextinpact.com/news/92827-megachat-messagerie-chiffree-mega-est-disponible.htm

Les 12 premiers relais TOR deko Mozilla sont en ligne

http://www.nextinpact.com/news/92897-tor-12-premiers-relais-mozilla-sont-en-ligne.htm

Performance des FPGA pour la cryptographie

http://publications.jrc.ec.europa.eu/repository/bitstream/JRC91528/lbna26833enn.pdf

- La commission européenne sponsorise des FPGA à utiliser avec oclHashCat

Courbes elliptiques : les paramètres validés par l'ANSSI

- Avec ou sans backdoor ? Cf. Troll
  http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000024668816&dateTexte=&oldAction=rechJO&categorieLien=id

DIME, le protocole de mail chiffré

- Par Philippe Zimmerman (Auteur de PGP) et de Ladar Lavinson (Créateur de Lavabit)
- 2 principaux protocoles : DMTP (the Dark Mail Transfer Protocol) et DMAP (Dark Mail Access Protocol)
- Chiffrement de toutes les métadonnées
  https://darkmail.info/downloads/dark-internet-mail-environment-december-2014.pdf

Pentest

Techniques & outils

Un scanneur de port à haute vitesse

https://github.com/OffensivePython/Nscan/

Élévation de privilège Windows via Phishing avec Metasploit

- Module de post-exploitation qui affiche une popup d'authentification

https://forsec.nl/2015/02/windows-credentials-phishing-using-metasploit/

PCAPSIPDUMP : extraction d'appels SIP à partir d'un PCAP

http://n0where.net/pcapsipdump/

Scada
Divers

Les vulnérabilités DTM continuent à fleurir sur le site de l'ICS-CERT
https://ics-cert.us-cert.gov/advisories

GE Digital Energy (Division de General Electric)

- Clef SSL en dur dans des switchs MLxxxx
  http://threatpost.com/ge-ethernet-switches-have-hard-coded-ssl-key/110412

Usurpation d'identité sur les switchs Siemens SCALANCE X-200IRT Switch
https://ics-cert.us-cert.gov/advisories/ICSA-15-034-01

Contournement de l'authentification sur les Siemens Ruggedcom WIN (WiFi industriel)
https://ics-cert.us-cert.gov/advisories/ICSA-15-034-02

Déni de service sur les switch Siemens SCALANCE X-300/X408
https://ics-cert.us-cert.gov/advisories/ICSA-15-020-01

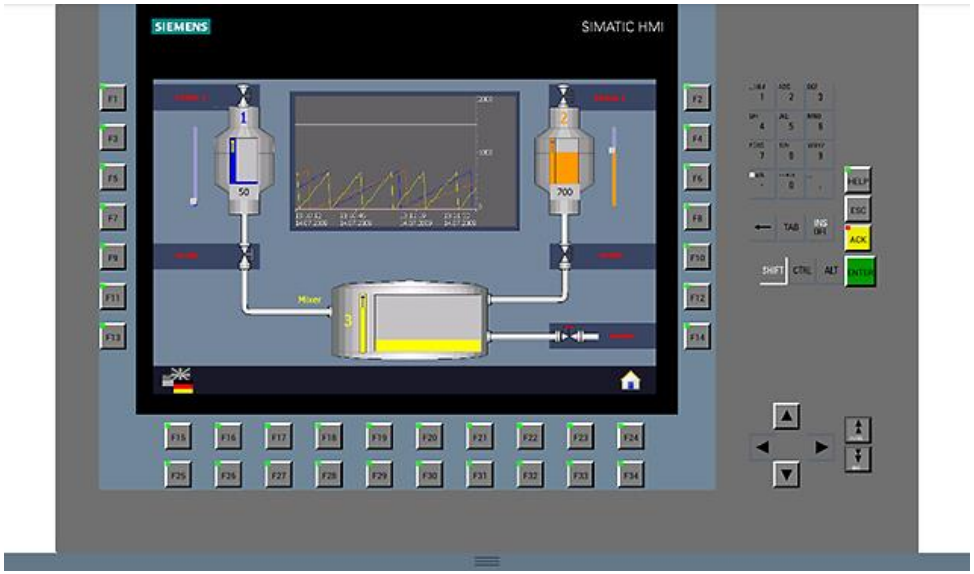
"Open redirect" dans le serveur web des automates Siemens S7-1200
https://ics-cert.us-cert.gov/advisories/ICSA-15-034-02

Vulnérabilités dans la gamme Schneider Electric ETG3000 FactoryCast HMI Gateway

- Même vulnérabilité que sur les automates de la gamme Modicon ?
- Récupération d'informations sensibles dans les fichiers jars, mot de passe FTP hardcodé...
  https://ics-cert.us-cert.gov/advisories/ICSA-15-020-02

Vulnérabiités dans SIMATIC WinCC Sm@rtClient iOS Application

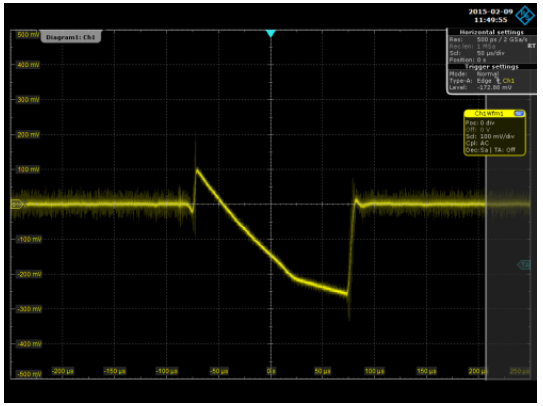
- Mauvaise protection des mots de passe, rien de très grave
- L'info intéressante est que, oui, il y a des application iOS pour accéder à son SI industriel …
- "The future of manufacturing" ...
  https://ics-cert.us-cert.gov/advisories/ICSA-15-013-01



Nouveautés (logiciel, langage, protocole...)

Open Source

Raspberry Pi 2



- Processeur ARM quad-core (Perf x6)
- Ram x2 (1 Go)
- Support de Windows 10 / Ubuntu snappy core
- Prix $35
  http://www.raspberrypi.org/raspberry-pi-2-on-sale/
- Rupture de stock un peu partout (il y en a encore sur The Pi Hut)
- Une mauvaise isolation d'un composant le rend vulnérable aux Flash Xénon
  http://www.raspberrypi.org/forums/viewtopic.php?f=28&t=99042
  http://www.raspberrypi.org/xenon-death-flash-a-free-physics-lesson/

coreCLR, le moteur d'exécution du framework ASP.NET 5 en opensource

http://github.com/Microsoft/dotnet

PolarSSL devient mbed TLS

- Racheté par ARM en novembre 2014
- Va par la même occasion passer sous licence Apache
  http://community.arm.com/groups/internet-of-things/blog/2015/02/09/polarssl-is-dead-long-live-mbed-tls

Processus de boot d'un noyau linux

https://github.com/0xAX/linux-insides/tree/master/Booting

Nouveautés (logiciel, langage, protocole...)

Divers

Hopper 3.7.3

- Debug de plusieurs éléments en même temps
  http://hopperapp.com/blog/?p=136

Samsung SSD

- Outils de désobfuscation des firmwares des disques SSD Samsung
  https://github.com/ddcc/samsung_ssd

Nouvelle version 7.0 du CMS Typo 3

- JPG ? Message recu ? ;-)
  http://typo3.org/news/article/embrace-and-innovate-typo3-cms-7/

XSS Payload

- Un framework de payload XSS par Renaud Bidou
  http://www.xss-payloads.com/

<autopromo> 

Extension Chrome : cyber-free disponible sur le Chromestore

- Enlève le préfixe “cyber” sur les pages web

</autompromo>

Nouveautés (logiciel, langage, protocole...)

Divers

Defensive Best Practices for Destructive Malware

- Les recommandations de la NSA anti-malware destructif
  - Ségrégation de ses réseaux
  - Limiter les droits d'admin
  - Limiter les communications P2P entre workstation
  - Firewall, WAF, Proxy, IDS/IPS…
  - Déployer EMET
  - ...

https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf

Guide de bonnes pratiques sur l'acquisition et l'exploitation des noms de domaine

- par l'ANSSI

http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/l-anssi-publie-un-guide-de-bonnes-pratiques-sur-l-acquisition-et-l-exploitation.html

Business
France

Cloudwatt passe sous le contrôle à 100% d'Orange

http://www.informatiquenews.fr/cloudwatt-passe-controle-100-dorange-28008

OVH certifié PCI-DSS

- Pour son système de paiement en ligne
  - OVH.com, So you Start, RunAbove, Kimsufi et hubiC

http://www.globalsecuritymag.fr/OVH-GROUP-est-certifie-PCI-DSS,20150122,50178.html

Second redressement fiscal pour Microsoft France

- 16,4 millions à ajouter aux 56 millions précédents

http://lexpansion.lexpress.fr/high-tech/microsoft-redresse-de-16-4-millions-d-euros-par-le-fisc-francais_1647114.html

Orange croit toujours à une consolidation des télécoms en France

http://www.lesechos.fr/tech-medias/hightech/0204078468801-orange-croit-toujours-a-une-consolidation-des-telecoms-en-france-1082853.php

Business
International

Huawei

- Forte croissance de 15% sur 2014

http://in.reuters.com/article/2015/01/03/huawei-tech-sales-idINKBN0KC0CI20150103

Baisse du chiffre d'affaire chez Google

http://www.forbes.com/sites/aarontilley/2015/01/29/google-continues-to-miss-revenue-estimates-in-fourth-quarter-earnings/

Rumeurs de licenciements chez IBM

- Qui pourrait monter à 112 000 personnes, soit 26% des effectifs
- Démenti par IBM

http://www.forbes.com/sites/robertcringely/2015/01/22/next-weeks-bloodbath-at-ibm-wont-fix-the-real-problem/

GitHub passe son Bug Bounty à $10 000

http://threatpost.com/github-doubles-down-on-maximum-bug-bounty-payouts/110730

Apple accepte les conditions d'auditabilité de la Chine

http://www.itworld.com/article/2874235/report-apple-agrees-to-chinese-security-audits-of-its-products.html

Microsoft inverti dans Cyanogen

http://www.wsj.com/articles/BL-DGB-40241

Business
International

TV vs Internet

- Il est venu le temps des larmes pour la télé

  http://meta-media.fr/2015/01/19/tv-fini-de-rigoler.html

$14 milliards pour la sécurité informatique Américaine

- Pour le budget 2016 (encore à l'état de proposition)

  http://www.washingtontimes.com/news/2015/feb/2/obama-budget-dedicates-14b-to-cybersecurity/

Droit / Politique

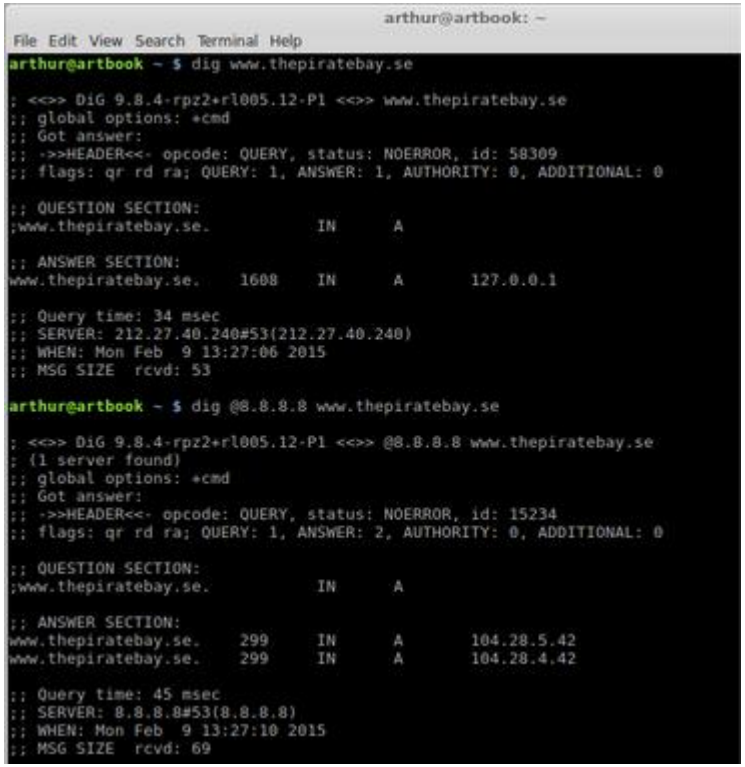
France

Blocage administratif de sites

C'est l' Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dresse la liste des sites visés

http://www.nextinpact.com/news/92852-la-france-veut-bien-etendre-blocage-sites-sans-juge.htm

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477&dateTexte=&categorieLien=id



Blocage de ThePirateBay

- Exemples chez Free et Orange

Droit / Politique

France

L'Agence du numérique est créée

http://www.numerama.com/magazine/32107-l-agence-du-numerique-est-officiellement-creee.html

Création et nomination d'un préfet chargé de la lutte contre les cybermenaces

- Avec un conseiller de grande qualité : Eric Freyssinet 

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029837986

http://www.nextinpact.com/news/87943-un-cyber-prefet-contre-cybermenaces-visant-pme-francaises.htm

Droit / Politique
International

Procès SilkRoad

- L'importance d'une emoticone
  http://www.nytimes.com/2015/01/29/nyregion/trial-silk-road-online-black-market-debating-emojis.html
- Discutions avec un possible Hell's Angel pour commanditer des assassinats
  http://www.wired.com/2015/02/read-transcript-silk-roads-boss-ordering-5-assassinations/
  - Les timestamp Bitcoins concordent avec les dates des discutions
    https://blockchain.info/address/1MwvS1idEevZ5gd428TjL3hB2kHaBH9WTL

Putin a bien tué Litvinenko en 2006

- Information obtenue par la NSA lors d'écoute
  http://www.telegraph.co.uk/news/uknews/law-and-order/11365730/Litvinenko-inquiry-the-proof-Russia-was-involved-in-dissidents-murder.html

L'Iran souhaite identifier tous ses internautes

http://www.haaretz.com/news/middle-east/.premium-1.630666

Open Data de la Maison Blanche

https://github.com/WhiteHouse/2016-budget-data

Droit / Politique
International

1ère condamnation de Google pour non-respect du droit à l'oubli

http://www.journaldugeek.com/2015/01/16/france-1ere-condamnation-google-non-respect-droit-a-loubli/

Loi Macron et le secret des affaires

- Proche d'un censure de la divulgation d'information… aux journalistes

  http://www.lemonde.fr/societe/article/2015/01/28/secret-des-affaires-informer-n-est-pas-un-delit_4564787_3224.html

L'Inde bloque 32 sites web pour lutter contre le terrorisme

- Exemple de sites : DailyMotion, Vimeo, Internet Archive et GitHub

  http://www.developpez.com/actu/79838/l-Inde-bloque-32-sites-web-dont-DailyMotion-Vimeo-Internet-Archive-et-GitHub-la-lutte-contre-le-terrorisme-avance-comme-principal-justificatif/

Conférences

Texte en gris = déjà traité précédemment

Passées

- 31C3 - 28 au 30 décembre 2014
  - Les vidéos : http://media.ccc.de/browse/congress/2014/
- CoRIIN - 19 janvier 2015 à Lille
  http://www.cecyf.fr/activites/recherche-et-developpement/coriin/
- FIC 2015 - 20 et 21 janvier 2015 à Lille
- Shmoocon - 16 au 18 janvier 2015 à Washington
  - Les vidéos : https://archive.org/details/shmoocon-2015-videos-playlist

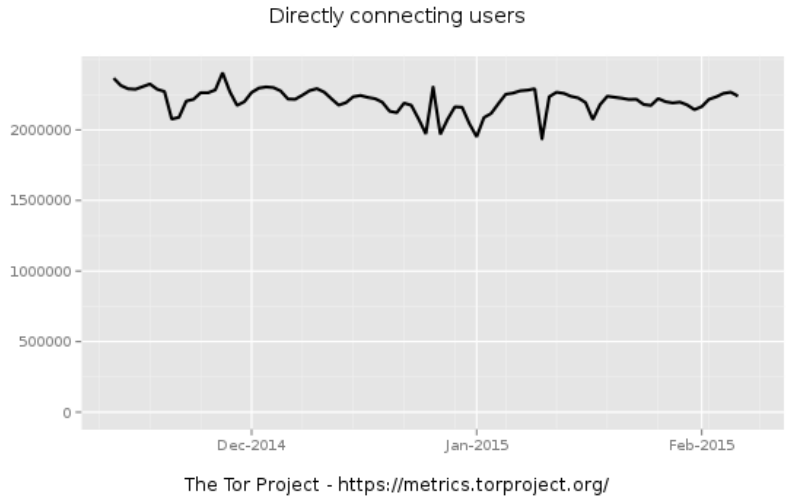
A venir

- JSSI 2015 - 10 mars 2015 à Paris
- GS Days - 24 mars 2015 à Paris
- Hack in Paris - 15 au 19 juin 2015 ~~chez Mickey~~ à l'Académie Fratellini
- Nuit du Hack - 20 au 21 juin 2015 ~~chez Mickey~~ à l'Académie Fratellini
  http://www.youtube.com/watch?v=Ulbx4IFTG7E
- SSTIC 2015 - 3, 4 et 5 juin 2015 à Rennes

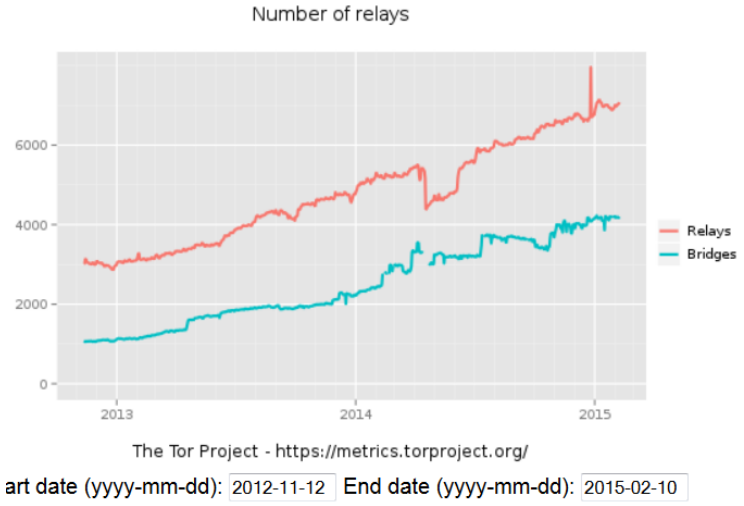
Divers / Trolls velus

Pour faire suite à la présentation « À TOR et à travers »

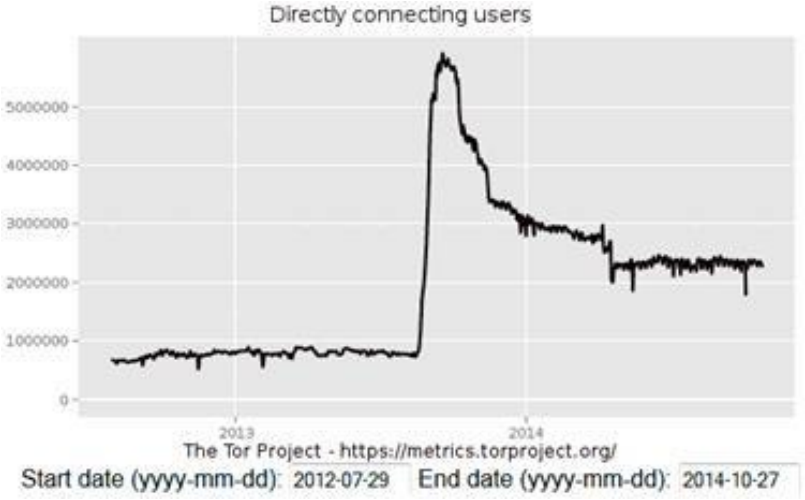
- Près de 2,2 millions d ‘utilisateurs



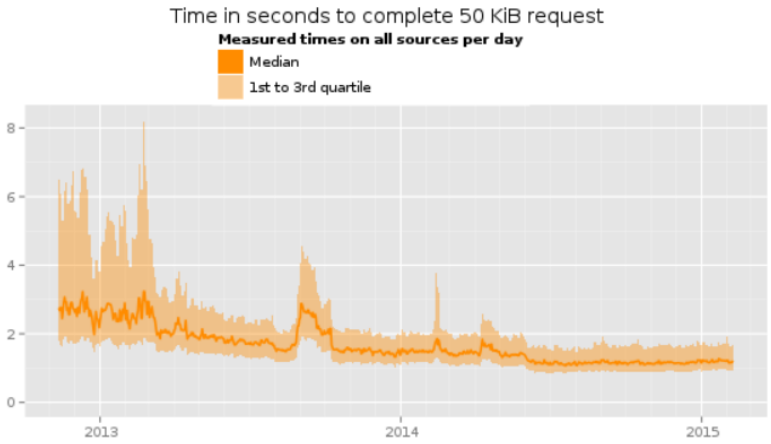
- Croissance du nombre de noeuds



- Un croissance suite à un évènement ?



- Un croissance suite à un évènement ?



Divers / Trolls velus

Kikilaperdu ?

https://twitter.com/balafon75/status/556006018078228480/photo/1

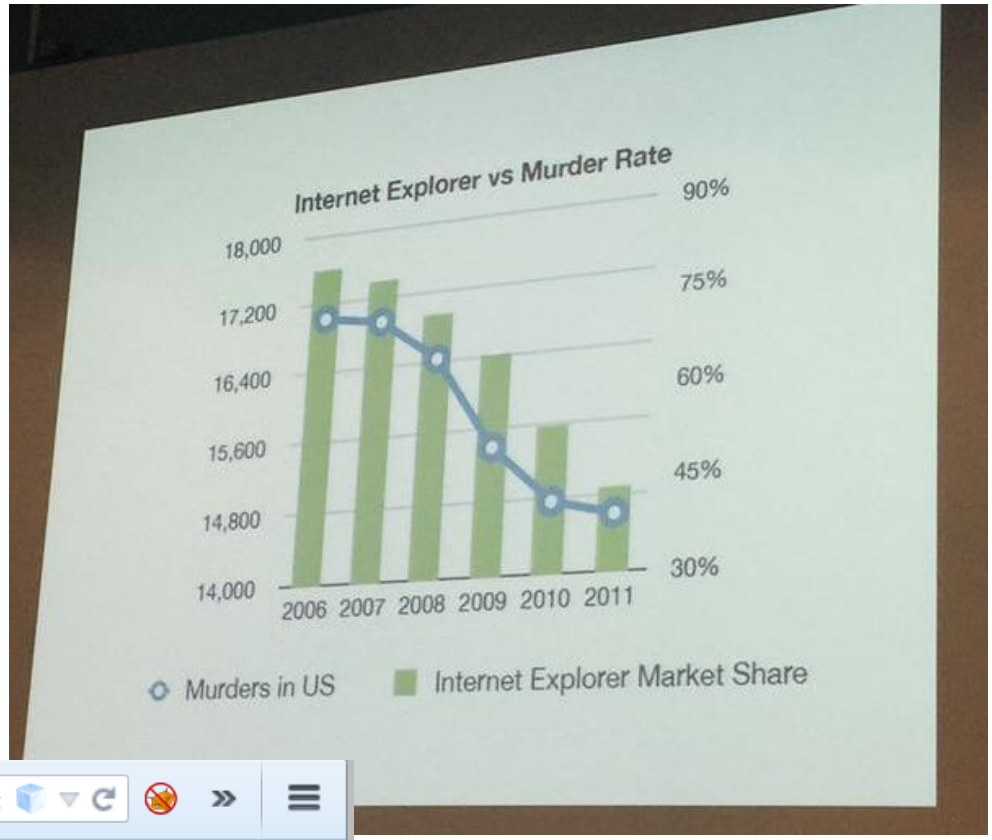
La sécurité des PLC / CPL d'Omron

- <<When a router is forwarding a TCP or UDP port to an Omron PLC, the traffic is being delivered to a non Windows based operating system. This makes the PLC impenetrable to standard hacking methods.>>
  http://echannel.omron247.com:8085/marcom/pdfcatal.nsf/0/7CC1E9D8D2A1C3BF862573760063920C/$file/InternetAccessToPLC_whitePaper_en_200910.pdf

Divers / Trolls velus

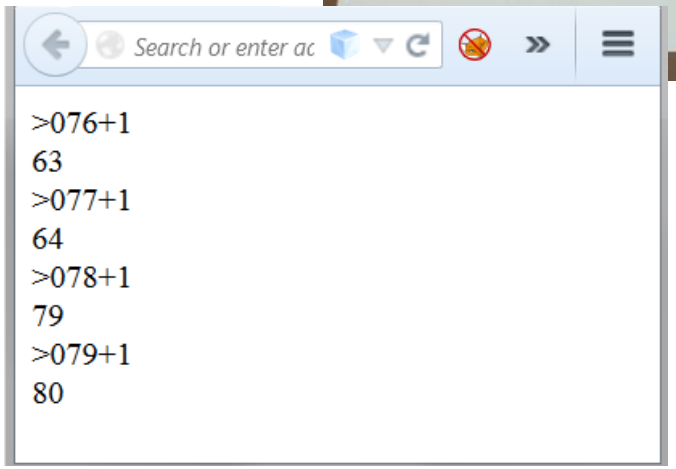
Internet Explorer vs **taux de meurtres**

- aux USA
  https://twitter.com/b_magnanti/status/555461494704709633/photo/1



Javascript…

- Octal puis décimal !!?



Divers / Trolls velus

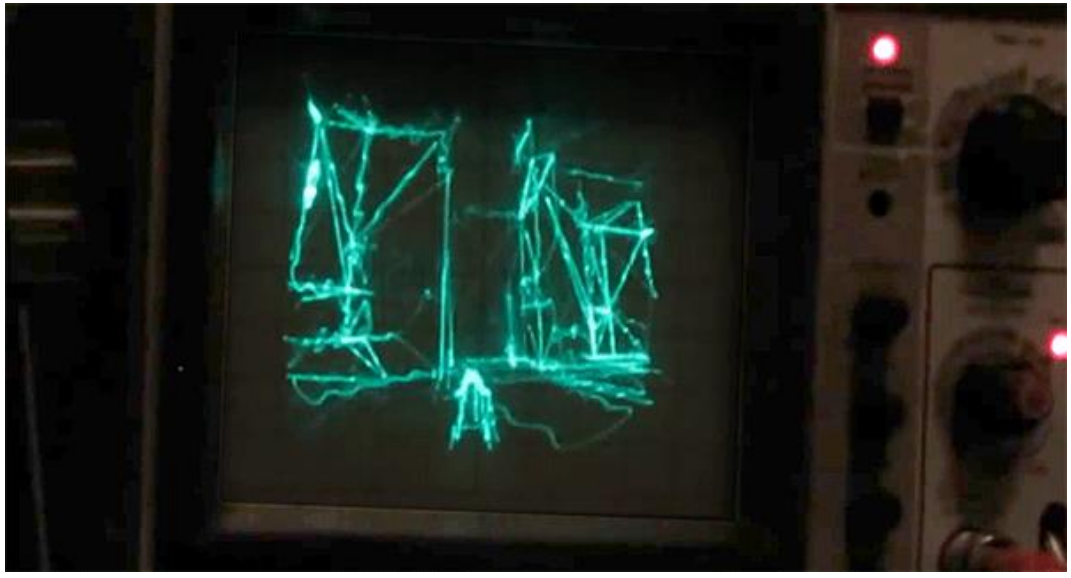
~# traceroute 216.81.59.173

- ...
- 9 10.26.26.22 (10.26.26.22) 179.158 ms 174.723 ms 187.900 ms
- 10 **Episode.IV** (206.214.251.1) 192.234 ms 183.206 ms 196.688 ms
- 11 **A.NEW.HOPE** (206.214.251.6) 205.395 ms 200.728 ms 207.279 ms
- 12 **It.is.a.period.of.civil.war** (206.214.251.9) 220.647 ms 216.199 ms 224.971 ms
- 13 **Rebel.spaceships** (206.214.251.14) 226.187 ms 230.289 ms 234.506 ms
- 14 **striking.from.a.hidden.base** (206.214.251.17) 223.962 ms 220.687 ms 235.099 ms
- 15 **have.won.their.first.victory** (206.214.251.22) 230.678 ms 236.231 ms 208.339 ms
- 16 **against.the.evil.Galactic.Empire** (206.214.251.25) 160.684 ms 169.533 ms 151.839 ms
- 17 **During.the.battle** (206.214.251.30) 156.424 ms 164.973 ms 173.811 ms
- 18 **Rebel.spies.managed** (206.214.251.33) 182.482 ms 178.059 ms 155.419 ms
- 19 **to.steal.secret.plans** (206.214.251.38) 177.184 ms 159.562 ms 168.366 ms
- 20 **to.the.Empires.ultimate.weapon** (206.214.251.41) 163.902 ms 172.704 ms 181.527 ms
- 21 **the.DEATH.STAR** (206.214.251.46) 185.901 ms 163.855 ms 172.403 ms
- 22 **an.armored.space.station** (206.214.251.49) 167.868 ms 181.101 ms 189.863 ms
- 23 **with.enough.power.to** (206.214.251.54) 185.421 ms 198.746 ms 194.053 ms
- 24 **destroy.an.entire.planet** (206.214.251.57) 173.997 ms 165.355 ms 191.534 ms
- 25 **Pursued.by.the.Empires** (206.214.251.62) 169.773 ms 160.417 ms 178.258 ms
- 26 **sinister.agents** (206.214.251.65) 187.034 ms 195.805 ms 160.127 ms
- 27 **Princess.Leia.races.home** (206.214.251.70) 164.471 ms 173.014 ms 182.030 ms
- 28 **aboard.her.starship** (206.214.251.73) 168.577 ms 178.169 ms 186.382 ms
- 29 **custodian.of.the.stolen.plans** (206.214.251.78) 190.786 ms 153.814 ms 157.929 ms
- 30 **that.can.save.her** (206.214.251.81) 149.352 ms 162.556 ms 177.822 ms

Divers / Trolls velus

Quake sur… un oscilloscope

http://www.lofibucket.com/articles/oscilloscope_quake.html



BFM…

https://twitter.com/mikko/status/560559455021326337

Divers / Trolls velus

Hacking de Sex toys

http://securityaffairs.co/wordpress/32950/hacking/hacking-sex-toys-dolls.html

Pour $150, un employé moyen donne son mot de passe

http://www.net-security.org/secworld.php?id=17872

Quel est votre mot de passe ?

- Des passants donnent leur mot de passe… innocemment
  https://www.youtube.com/watch?v=opRMrEfAIiI

Chine vs Outlook.com

- MitM sur SMTP et IMAP
  https://en.greatfire.org/blog/2015/jan/outlook-grim-chinese-authorities-attack-microsoft

La fiabilité des disques durs

- Selon BlackBlaze
  https://www.backblaze.com/blog/180tb-of-good-vibrations-storage-pod-3-0
- A mettre en regard avec le rapport de Google de 2007, bien plus complet
  http://research.google.com/archive/disk_failures.pdf

Un jihadiste se trahit sur Twitter grâce à la géolocalisation

http://www.bfmtv.com/international/un-jihadiste-repere-sur-twitter-grace-a-la-geolocalisation-855388.html

Divers / Trolls velus

Adobe a un CSIRT !!? (“**P**roduct” SIRT)

- Et ils communiquent
  http://blogs.adobe.com/psirt/

Amazon, Google et Microsoft auraient payé AdBlock Plus

http://www.theverge.com/2015/2/2/7963577/google-ads-get-through-adblock

DJI impose des "no-fly zones" à ses drones

- A quand le jailbreak de drone ?
  http://www.clubic.com/mag/transports/actualite-752475-no-fly-zones-drones-dji-maison-blanche-drogue.html

Brad Pitt et Angelina Jolie ont une “security team” pour protéger leurs enfants

http://www.people.com/article/angelina-jolie-brad-pitt-kids-monitor-internet

- info reprise par le Times http://time.com/3637164/angelina-jolie-brad-pitt-children-cyber-security/

Divers / Trolls velus

L’Anssi souhaite des backdoor cryptographiques

http://www.nextinpact.com/news/92857-anssi-recentes-attaques-par-defiguration-etaient-faible-niveau.htm

Alors que les britanniques souhaiteraient interdire le chiffrement

http://www.theguardian.com/commentisfree/2015/jan/13/banning-encryption-david-cameron-not-safer

Le logo de l’ANSSI décodé

- L’article est sous licence Creative Commons BY-NC-ND

http://blog.bienaime.info/2015/01/le-challenge-du-logo-anssi.html

Ne dites plus “Streaming” mais “Flux”

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030130862&dateTexte=&categorieLien=id

Divers / Trolls velus

Challenge Sogeti du FIC 2015

- Gros succès !
  - Site web hébergé sur un Windows 7 x64 SP1, faillible à des MS14-06x et plus
  - Aucun filtrage réseau
  - MySQL 4.1.22 (datant de 2006)
  - Exécution de code à distance (PHP CGI, overflow, phpmyadmin, mysql 4…)
  - Découverte d'un domaine SOGLU
  - ...
- Oups… il ne fallait analyser que l'image fournie par le site web ;-)
  http://news0ft.blogspot.fr/2015/01/fic-challenge-writeup.html

Challenge EPITA du FIC 2015

- Grosse préparation !
  - Recherche de la trace d'un virus dans un dump mémoire Windows
- Mais l'auteur du challenge :
  - A téléchargé le virus depuis son webmail
  - Dont des traces sont restées en mémoire (identifiant, mot de passe, intitulé des autres mails, contacts…)

  http://news0ft.blogspot.fr/2015/01/fic-challenge-writeup-epita-edition.html

Divers / Trolls velus

Skynet is coming

Une femme sud-coréenne attaquée par son robot aspirateur

- Sauvée par les pompiers
  http://www.dailydot.com/technology/robot-vacuum-attack/

Prochaines réunions

Prochaines réunions

- Pas de réunion en Mars du fait de la JSSI
- Mardi 14 Avril 2015

Questions ?