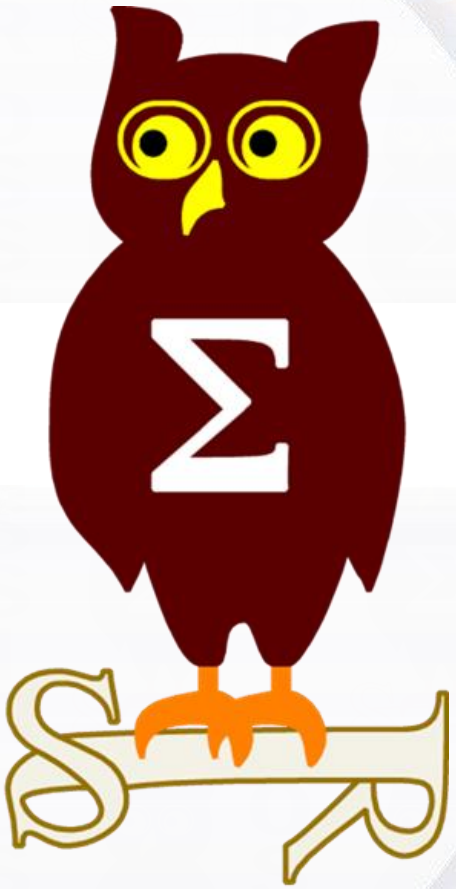


Revue d'actualité

14/04/2015

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Avis Février 2015

MS15-009 Vulnérabilités dans Internet Explorer (39 CVE)  [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplace MS14-080
- Exploit:
  - 35 x Corruptions de mémoire aboutissant à une exécution de code
    - Dont correctif CVE-2014-8967, publié en décembre 2014 par ZDI après le dépassement des 120 jours de grâce http://zerodayinitiative.com/advisories/ZDI-14-403/
  - 1 x Contournement ASLR
  - 2 x Elévations de privilèges
  - 1 x Contournement du filtrage anti XSS
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-0041)
  - Adlab de Venustech (CVE-2015-0017)
  - Aniway.Anyway@gmail.com par ZDI (CVE-2015-0017, CVE-2015-0031)
  - Anonymous par ZDI (CVE-2015-0025, CVE-2015-0036, CVE-2015-0038)
  - Bo Qu de Palo Alto Networks (CVE-2015-0018, CVE-2015-0019, CVE-2015-0045, CVE-2015-0068)
  - Chen Zhang (demi6od) de NSFOCUS Security Team (CVE-2015-0026, CVE-2015-0030)
  - Clement Lecigne de Google Inc. (CVE-2015-0071)
  - Edward Torkington de NCC Group (CVE-2015-0066)
  - Jack Tang de Trend Micro (CVE-2015-0069)
  - James Forshaw de Google Project Zero (CVE-2015-0054, CVE-2015-0055)
  - Jason Kratzer par ZDI (CVE-2015-0027)
  - Jihui Lu de KeenTeam (@K33nTeam) (CVE-2015-0039, CVE-2015-0066)
  - José A. Vázquez de VeriSign iDefense Labs (CVE-2015-0023)
  - Qihoo 360
    - Liu Long (CVE-2015-0020, CVE-2015-0021)
    - Yujie Wen (CVE-2015-0022, CVE-2015-0028, CVE-2015-0029)
  - Omair working par ZDI (CVE-2015-0042, CVE-2015-0043)
  - Pawel Wylecial par ZDI (CVE-2015-0035)
  - Peter Vreugdenhil de exodusintel.com (CVE-2015-0067)
  - Sky par ZDI (CVE-2015-0035)
  - SkyLined (CVE-2015-0048, CVE-2015-0049, CVE-2015-0050, CVE-2015-0051, CVE-2015-0052, CVE-2015-0040, CVE-2015-0053)
  - Stephen Fewer de Harmony Security par ZDI (CVE-2015-0046)
  - The Labs Team de iSIGHT Partners (CVE-2015-0071)
  - ca0nguyen par ZDI (CVE-2015-0044, CVE-2015-0045)
  - sweetchip@GRAYHASH par ZDI (CVE-2015-0037)

Failles / Bulletins / Advisories

Microsoft - Avis Février 2015

MS15-010 Vulnérabilité dans le Kernel (6 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - 3 x élévations de privilèges, dont :
    - Double free sur des Curseurs de la souris (CVE-2015-0058) http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Just-another-day-at-the-office-A-ZDI-analyst-s-perspective-on/ba-p/6710637
    - Single bit des barres de défilement (CVE-2015-0057) http://breakingmalware.com/vulnerabilities/one-bit-rule-bypassing-windows-10-protections-using-single-bit/
  - 1 x exécution de code à l'affichage (donc traitement) d'une police de caractères TrueType spécialement formatée (CVE-2015-0059)
  - 1 x déni de service
- Crédits:
  - Marcin Wiazowski par ZDI (CVE-2015-0003)
  - James Forshaw de Google Project Zero (CVE-2015-0010)
  - Udi Yavo, CTO de enSilo (CVE-2015-0057)
  - n3phos par ZDI (CVE-2015-0058)
  - Cris Neckar de Divergent Security (CVE-2015-0059)
  - Cris Neckar de Divergent Security (CVE-2015-0060)

Failles / Bulletins / Advisories

Microsoft - Avis Février 2015

Deux failles liées et vieilles de 15 ans

MS15-011 Vulnérabilité dans Group Policy (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées), pas de correctif pour Windows 2003
- Exploit:
  - Sur un réseau, usurpation d'un domaine et exécution de code si la cible exécute un .bat sur le réseau (*\Share\login.bat)
    http://blogs.technet.com/b/srd/archive/2015/02/10/ms15-011-amp-ms15-014-hardening-group-policy.aspx
    Plus de détails : https://labs.mwrinfosecurity.com/blog/2015/04/02/how-to-own-any-windows-network-with-group-policy-hijacking-attacks/
- Crédits:
  - Jeff Schmidt de JAS Global Advisors (CVE-2015-0008)
  - Dr. Arnoldo Muller-Molina de simMachines (CVE-2015-0008)
  - ICANN (CVE-2015-0008)

MS15-014 Vulnérabilité dans Group Policy (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées), pas de correctif pour Windows 2003
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Désactivation de la signature SMB dans les Group Policy
    http://blogs.technet.com/b/srd/archive/2015/02/10/ms15-011-amp-ms15-014-hardening-group-policy.aspx
- Crédits:
  - Luke Jennings (CVE-2015-0009)

Failles / Bulletins / Advisories

Microsoft - Avis Février 2015

MS15-012 Vulnérabilité dans Office (3 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007, 2010 et Compatibility Pack SP3
  - SharePoint Server 2010
  - Office Web Apps 2010
  - Word & Excel Viewers
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier spécialement formaté
- Crédits:
  - Fermin J. Serna de Google Security Team (CVE-2015-0063)
  - Ben Hawkes of Google Project Zero (CVE-2015-0064, CVE-2015-0065)

MS15-013 Vulnérabilité dans Office (1 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007, 2010 et 2013
- Exploit:
  - Contournement d'ASLR
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Février 2015

MS15-015 Elévation de privilèges (12 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS15-001
- Exploit:
  - Élévation de privilèges à la création d'un processus (!SeAssignPrimaryTokenPrivilege)
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2015-0062)

MS15-016 Vulnérabilité dans Microsoft Graphics (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Contournement d'ASLR par la récupération d'information sur la pile lors du traitement d'une image TIFF spécialement formaté
- Crédits:
  - Michal Zalewski de Google Inc. (CVE-2015-0061)

MS15-017 Élévation de privilèges dans Microsoft System Center Virtual Machine Manager (1 CVE) [Exploitabilité ?]

- Affecte:
  - Microsoft System Center 2012 R2 Virtual Machine Manager
- Exploit:
  - Erreur de vérification des rôles d'un utilisateur authentifié et possibilité de prise de contrôle de toutes les VM
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Mars 2015

MS15-018 Vulnérabilités dans Internet Explorer (12 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - 9 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Corruptions de mémoire dans un script VBSCript aboutissant à une exécution de code
  - 2 x élévations de privilèges
    - dont 1 XSS divulgué en février et exploité dans la nature (CVE-2015-0072)
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-0056, CVE-2015-1623)
  - Anonymous par Beyond Security's SecuriTeam Secure Disclosure team (CVE-2015-1634)
  - Arthur Gerkis par ZDI (CVE-2015-1624)
  - Ashutosh Mehra (CVE-2015-1627)
  - Bo Qu de Palo Alto Networks (CVE-2015-0032)
  - Ca0nguyen par ZDI (CVE-2015-0100, CVE-2015-1626)
  - SkyLined par ZDI (CVE-2015-0099, CVE-2015-1622)
  - Modification du bulletin
  - Michal Zalewski de Google Project Zero
  - Noriaki Iwasaki
  - Zhang Yunha

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

MS15-019 Vulnérabilités dans VBScript (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 2003, Vista, 2008
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code depuis VBScript, exploitable depuis IE
- Crédits:
  - Bo Qu de Palo Alto Networks (CVE-2015-0032)

MS15-020 Vulnérabilités dans Windows (2 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Exécutions de code lors du traitement d'une page web spécialement formaté
  - Exécutions de code lors de l'affichage dans l'explorateur d'un répertoire contenant un fichier .LNK (et son icône .CPL)
    - Vulnérabilité utilisée par Stuxnet et partiellement corrigé par MS10-046

    http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/CVE-2015-0096-issue-patched-today-involves-failed-Stuxnet-fix/ba-p/6718402#.VP9GQFV4o50
- Crédits:
  - Garage4Hackers par ZDI (CVE-2015-0081)
  - Francis Provencher de Protek Research Lab's (CVE-2015-0081)
  - Michael Heerklotz par ZDI (CVE-2015-0096)

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

MS15-021 Vulnérabilités dans Adobe Font Driver (8 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Vulnérabilité sur "Adobe Type Manager" (atmfd.dll) d'Adobe, exploitable depuis une page web
    - 5 x Exécutions de code en ring 0 lors du traitement de police de caractère
    - 2 x fuites d'information permettant le contournement d'ASLR (KASLR)
    - 1 x déni de service lors du traitement de police de caractère
- Crédits:
  - Mateusz Jurczyk de Google Project Zero (CVE-2015-0074,CVE-2015-0087 à 93)

MS15-022 Vulnérabilité dans Office (5 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007, 2010 et 2013, visionneuse Word et Excel
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier Office spécialement formaté
- Crédits:
  - 3S Labs par ZDI (CVE-2015-0085)
  - Ben Hawkes de Google Project Zero (CVE-2015-0086)
  - Noam Rathaus par Beyond Security's SecuriTeam Secure Disclosure team (CVE-2015-0097)
  - Adi Ivascu (CVE-2015-1633, CVE-2015-1636)

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

MS15-023 Vulnérabilités noyau (4 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Fuites d'information permettant le contournement d'ASLR
  - Elévation de privilèges
- Crédits:
  - WanderingGlitch par ZDI (CVE-2015-0077)
  - James Forshaw de Google Project Zero (CVE-2015-0078)
  - Ashutosh Mehra de Adobe Systems Inc. (CVE-2015-0078)
  - WanderingGlitch par ZDI (CVE-2015-0094)
  - KK (CVE-2015-0095)

MS15-024 Vulnérabilité PNG (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Fuites d'information permettant le contournement d'ASLR lors du traitement d'une image PNG
- Crédits:
  - Michal Zalewski de Google Inc. (CVE-2015-0080)

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

MS15-025 Vulnérabilités noyau (2 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Reboot et plantage sur Windows 7 et 2008 R2
    http://krebsonsecurity.com/2015/03/ms-update-3033929-causing-reboot-loop/
- Exploit:
  - Élévations de privilèges
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2015-0073)

MS15-026 Vulnérabilités dans Microsoft Exchange serveur (5 CVE) [Exploitabilité 2]

- Affecte:
  - Exchange Serveur 2013 SP1 et 2013 Cumulative Update 7
- Exploit:
  - 4 x élévations de privilèges(XSS) dans OWA
  - 1 x usurpation d'identité sur les réunions, permettant d'en modifier le contenu
- Crédits:
  - Adi Ivascu (CVE-2015-1629, CVE-2015-1630)
  - Darius Petrescu (CVE-2015-1632)
  - Francisco Correa (CVE-2015-1628)
  - Nicolai Grodum (CVE-2015-1631)

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

MS15-027 Vulnérabilité dans Netlogon (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Serveur toutes version supportées (2003, 2008, 2008 R2, 2012, 2012 R2)
- Exploit:
  - Usurpation d'identité d'une machine d'un réseau, nécessitant d'être authentifié sur ce réseau
- Crédits:
  - Alberto Solino et Joaquín Rodríguez Varela de Core Advisories Team (CVE-2015-0005)

MS15-028 Vulnérabilité dans le planificateur de taches (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 7, 8, 2008, 2008 R2, 2012, 2012 R2
- Exploit:
  - Élévation de privilèges locale depuis le planificateur de taches
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2015-0084)

MS15-029 Vulnérabilité PG XR (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista, 7, 8, 2008, 2008 R2, 2012, 2012 R2
- Exploit:
  - Fuite d'information permettant le contournement d'ASLR lors du traitement d'une image Windows Media Photo (JPG XR)
- Crédits:
  - Michal Zalewski de Google Inc. (CVE-2015-0076)

Failles / Bulletins / Advisories

Microsoft - Autre vulnérabilités

MS15-030 Déni de service dans RDP (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 7, 8, 8.1, 2012, 2012 R2
- Exploit:
  - Déni de service dans RDP
- Crédits:
  - ?

MS15-031 Vulnérabilité FREAKS dans SChannel (1 CVE) [Exploitabilité 1]

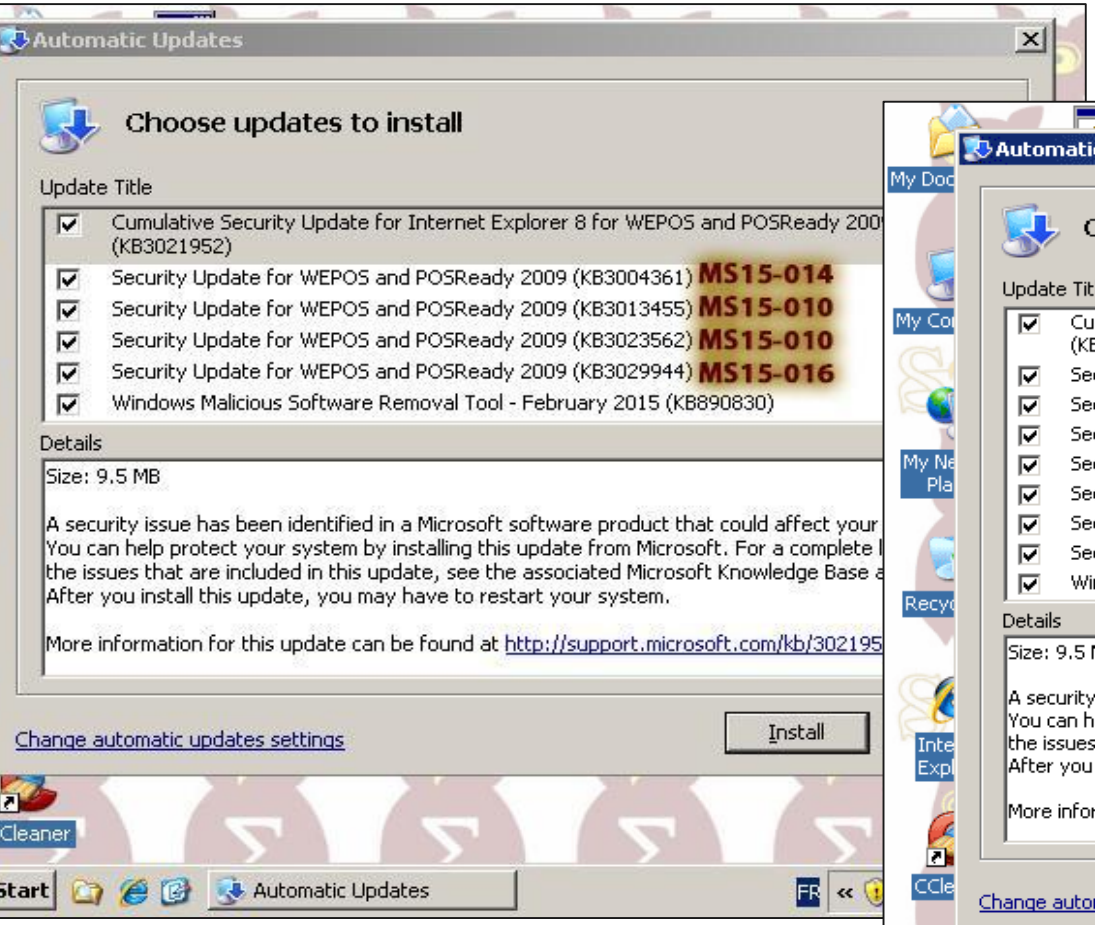
- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Déchiffrement des flux chiffrés par l'attaque FREAK (Factoring RSA Export Keys)
  - Concerne toutes les suites “RSA_EXPORT”
- Crédits:
  - Cf. ci-après 

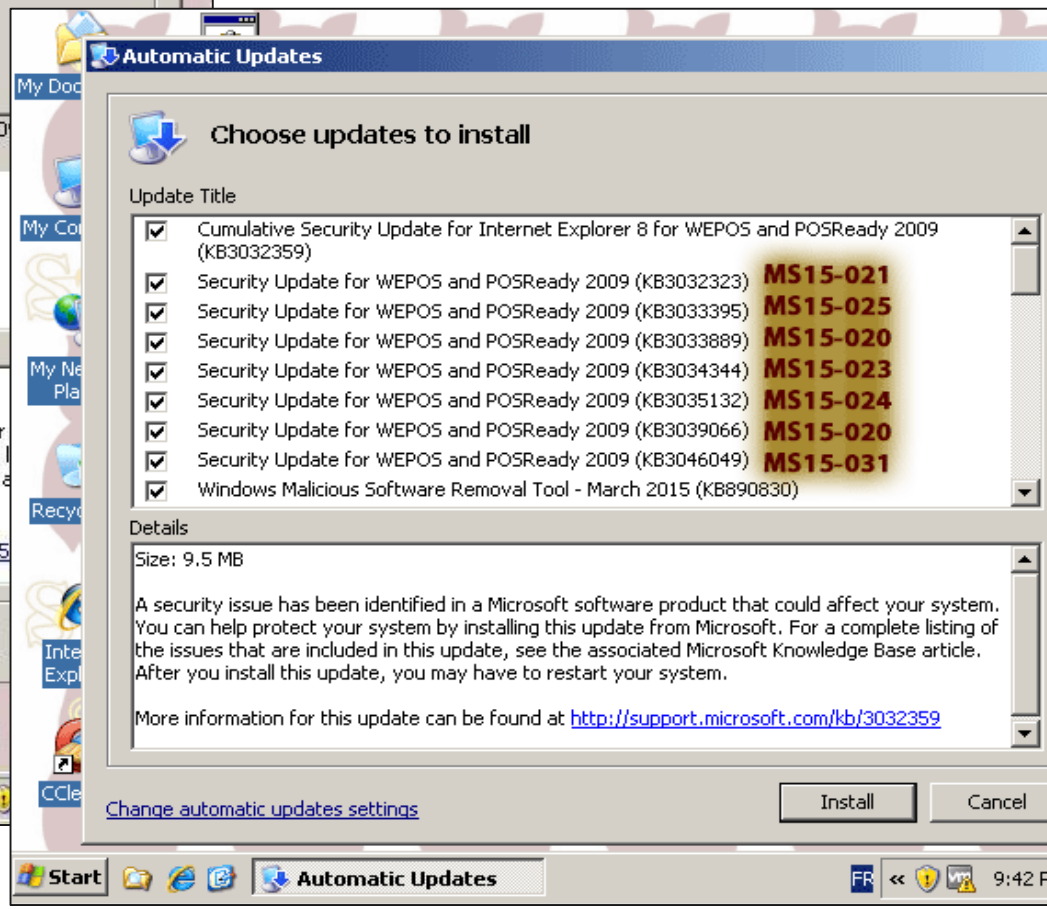
Failles / Bulletins / Advisories

Microsoft - Avis Février & Mars 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…





Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Février & Mars 2015

Publication de 0day par Google

- Élévation de privilège locale par une réflexion NTLM sur WebDav
  http://seclists.org/fulldisclosure/2015/Mar/149

3004375 Audit de processus

- V1.0 Ajout de la ligne de commande dans les possibilités d'audit des processus (Audit Process Creation policy)

3009008 Désactivation de SSLv3

- V2.2 Désactivation par défaut dans IE11
- V2.3 Réactivation et annonce d'une date de désactivation dans IE11 : 14 avril 2015

2755801 Mise à jour de Flash Player

- V38.0 Nouvelle mise à jour de Flash Player

3033929 Ajout du support de SHA2 dans Windows 7 et 2008 R2

- V1.0 Ajout pour les CAB, PE (exe, dll...), Cert...

3046015 FREAK

- Prépublication avant MS15-031

3046310 Révocation du certificat de live.fi et www.live.fi

- V1.0 Publication
  http://arstechnica.com/security/2015/03/bogus-ssl-certificate-for-windows-live-could-allow-man-in-the-middle-hacks/
- V2.0 Ajout du support de Windows 2003

Failles / Bulletins / Advisories

Microsoft - Autre

Nouveaux leviers de croissance chez Microsoft ?

- Prix du support étendu de Windows XP **x 2** à $400/licence/an
  http://www.computerworld.com/article/2885759/microsoft-to-double-price-of-xps-post-retirement-support.html
- Support étendu de Windows 2003 (fin prévue pour le 14 juillet 2015) à $600/licence/an
  http://www.theregister.co.uk/2015/02/16/windows_server_2003_600_dollars/

Reconstruction d'un domaine Active Directory

- Un outil pour simplifier :
  - Réinitialise le mot de passe du **krbtgt**
  - Vérifier la réplication des clefs sur les DC (clefs dérivées du mot de passe)

  https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51
- Publication d'un document pour aller plus loin
  - Dont les évènements de sécurité à surveiller
    http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10 disponible à partir de l'été 2015

- Mise à jour gratuite, même pour les versions Warez
  http://www.theverge.com/2015/3/18/8241023/windows-10-free-for-software-pirates

Microsoft souhaite de débarrasser du nom "Internet Explorer"

- Qui joui d'une trop mauvaise image
  http://www.theverge.com/2015/3/17/8230631/microsoft-is-killing-off-the-internet-explorer-brand

Publication du code source d'un framework pour drivers

http://blogs.msdn.com/b/windows_hardware_and_driver_developer_blog/archive/2015/03/18/windows-driver-frameworks-source-on-github.aspx
https://github.com/Microsoft/Windows-driver-frameworks

Failles / Bulletins / Advisories

Système (principales failles)

Oracle

- Oracle Database Server, Java, MySQL, virtualbox...
- 169 vulnérabilités dont 93 exploitables à distance
  http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html

Fedora

- Élévation de privilège locale
  https://github.com/stealth/troubleshooter/blob/master/troubleshooter

OpenSSH

- Désactivation de SSHFP chez le client par un serveur (CVE-2014-2653)
- Usurpation d'identité pour un utilisateur déjà authentifié, avec les autorisations d'exécution de commande Kerberos, similaire à sudo (CVE-2014-9278)
  http://www.redhat.com/archives/enterprise-watch-list/2015-March/msg00012.html

XSS persistant dans WordPress à cause du plugin WP-Super-Cache

- Plus d'un million de sites potentiellement vulnérables
  https://blog.sucuri.net/2015/04/security-advisory-persistent-xss-in-wp-super-cache.html

Failles / Bulletins / Advisories

Système (principales failles)

NTP

- CVE-2015-1798
  - MitM dans les réponses NTP en cas d'utilisation d'une clef symétrique
    https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2015-1798
- CVE-2015-1799
  - Possibilité d'usurper une réponse NTP
    https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2015-1799

Adobe Flash

- Exécution de code CVE-2015-0311, exploité dans la nature par le kit d'exploitation HanJuan
  https://blog.coresecurity.com/2015/03/25/exploiting-cve-2015-0311-part-ii-bypassing-control-flow-guard-on-windows-8-1-update-3/
  https://nakedsecurity.sophos.com/2015/02/03/news-flash-3rd-time-newunlucky-0-day-hits-adobes-browser-plug-in/
- Exploit pour Metasploit
  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/browser/adobe_flash_uncompress_zlib_uaf.rb
- CVE-2015-0318
  https://code.google.com/p/google-security-research/issues/detail?id=199#c7
- Faux lecteur de vidéos porno -> 110 000 membres de Facebook infectés
  http://www.01net.com/editorial/643905/facebook-un-malware-cache-dans-une-video-porno-infecte-plus-de-110000-personnes/

Failles / Bulletins / Advisories

Système (principales failles)

Samba

- Exécution de code à distance sur **smbd** avant authentification (CVE-2015-0240)
  https://securityblog.redhat.com/2015/02/23/samba-vulnerability-cve-2015-0240/

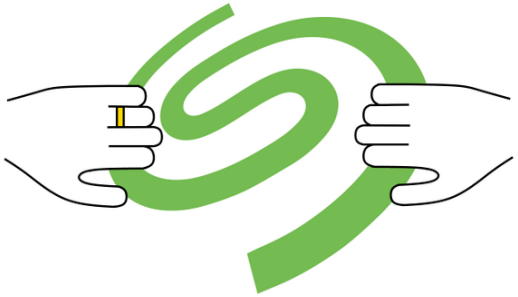
SuperFish, la backdoor de Lenovo

- Ce n'est pas une vraie vulnérabilité
  - Un site (celui de Komodia, l'éditeur) ✔
  - Un nom (Superfish) ✔
  - Pas de logo officiel ✘
- MitM SSL dans les navigateurs pour injecter de la publicité
  - Une AC ajouté au magasin de certificats
  - Un service permettant l'injection et signant les faux certificats
  - Le service contient la clef privée
    - Protégé par le mot "komodia"
    - et écrite à l'envers !!?
  - Le service ne vérifie pas les certificats remplacés
    - Auto-signé, périmé ou révoqué : Superfish les considère comme valide !
  - Chrome ne protège pas, le « certificate pining » ne vérifie pas les autorités locales
- Des exploitations dans la nature
  http://arstechnica.com/security/2015/02/researchers-unearth-evidence-of-superfish-style-attacks-in-the-wild/

Failles / Bulletins / Advisories

Matériel

Business Storage 2-Bay NAS de Seagate : Seagape



- Une vraie vulnérabilité :
  - Un site ✔
  - Un nom ✔
  - Un logo ✔
- Exécution de code à distance avant authentification
  - Injection de code PHP
  - Exécution par manipulation de la variable “language”
  - Status d’authentification laissé à la main du client
    - “Chiffré” par une clef XOR commune à tous les NAS

  https://beyondbinary.io/advisory/seagate-nas-rce/
- Exploit :

  http://www.exploit-db.com/exploits/36202/
- Plus de 2500 NAS référencés dans Shodan…
- Timeline de la publication particulièrement intéressante

Failles / Bulletins / Advisories

Réseau (principales failles)

BufferOverflow sur le SSO des firewalls Fortinet

- 20 lignes pour le POC…

```
message = "\x80\x01\x42\x42"
buff = "A"*248
buff += "B" * (0xfffff - len(buff))
payload = struct.pack(">I", 0x000fffff) + message + buff
```

http://www.coresecurity.com/advisories/fortinet-single-sign-on-stack-overflow

Netgear WNDR3700v4 et WNR2500 : Prise de contrôle à distance

- Le système du routeur peut recevoir des requêtes SOAP mais filtre les accès non authentifiés
- Sauf si... la requête débute par un champ SOAP vide
  http://seclists.org/fulldisclosure/2015/Feb/56

Ingénierie à reculons de l'algorithme WPS de Belkin

http://www.devttys0.com/2015/04/reversing-belkins-wps-pin-algorithm/

Failles / Bulletins / Advisories

Virtualisation

Xen

- Accès à la console graphique depuis une VM (XSA-119 / CVE-2015-2152)
- Déni de service, accès à des zones mémoire de l'hyperviseur, élévation de privilèges…

Xen : Analyses de deux vulnérabilités de 2014Q3

http://www.insinuator.net/2015/02/the-dangers-of-x86-emulation-xen-xsa-110-and-105/

Contournement de SMEP et SMAP (Registre de contrôle CR4)

- SMEP empêche l'exécution et SMAP empêche l’écriture/lecture de zones mémoire
  https://www.nccgroup.trust/en/blog/2015/04/xen-smep-and-smap-bypass/

Failles / Bulletins / Advisories

Apple

Apple supprimes les antivirus d'AppleStore

- Antivirus = présence de Virus
- Supprimer les antivirus = plus de virus, logique !

http://www.clubic.com/application-mobile/actualite-759671-apple-retirerait-antivirus-app-store-degrader-image.html

iOS 8.3 et Mac OS X 10.10.3 ne suivront plus les redirections ICMP

https://support.apple.com/en-us/HT204661
https://support.apple.com/en-us/HT204659

iTunes embarque (volontairement?) **des failles**

- libeay32.dll et ssleay32.dll 0.9.8za datant de juin 2014, contenant plus de 21 failles
- libcurl.dll 7.16.2 datant de 2007, contenant 22 failles

http://seclists.org/fulldisclosure/2015/Feb/5

Paingu, tous les détails du jailbreak d'iOS 8

http://blog.pangu.io/wp-content/uploads/2015/03/CanSecWest2015_Final.pdf

Failles / Bulletins / Advisories

Apple

Authentification à double facteur pour FaceTime et iMessage

http://arstechnica.com/apple/2015/02/apple-extends-two-factor-authentication-to-facetime-and-imessage/

Premières fraudes sur Apple Pay

- Trop de laxisme sur les vérifications des CB et utilisation de cartes volées
  http://www.wsj.com/articles/apple-pay-stung-bylow-techfraudsters-1425603036

Accès illégitime aux cookies dans Safari

- versions iOS/OSX/Windows vulnérables
- Désormais corrigé
  http://seclists.org/fulldisclosure/2015/Apr/30

Failles / Bulletins / Advisories

Google

Android 4.4(?)

- Exécution de code par l'appel à java.io.ObjectInputStream (CVE-2014-7911)
  - Article : http://seclists.org/fulldisclosure/2014/Nov/51
  - Code d'exploitation : https://github.com/retme7/CVE-2014-7911_poc
  - Explications : http://researchcenter.paloaltonetworks.com/2015/01/cve-2014-7911-deep-dive-analysis-android-system-service-vulnerability-exploitation/
- Élévation de privilèges, system -> root CVE-2014-4322)
  - https://www.codeaurora.org/projects/security-advisories/memory-corruption-qseecom-driver-cve-2014-4322
  - Code d'exploitation : https://github.com/retme7/CVE-2014-4322_poc

Youtube, effacer n'importe quelle vidéo

- Prime de $5,000 pour le chercheur Kamil Hismatullin

```
POST /live_events_edit_status_ajax?action_delete_live_event=1 HTTP/1.1
Host : www.youtube.com
...
event_id=<video id>&session_token=<any token>
```

https://nakedsecurity.sophos.com/2015/04/02/how-one-man-could-have-deleted-every-video-on-youtube/

Failles / Bulletins / Advisories

Google

Project Zero ajoute 14 jours à sa période de grâce de publication des 0-days

- Passant de 90 à 104 jours : monseigneur est trop généreux

  http://googleprojectzero.blogspot.fr/2015/02/feedback-and-data-driven-updates-to.html

Google ne supportera plus SHA1 (160 bits) **après Déc. 2015**

- Déjà implémenté dans Chrome 41 puis 42
  - Un certificat expirant après 2016 lève une **alerte**
  - Un certificat expirant après 2017 lève une **erreur**

  https://blog.filippo.io/the-unofficial-chrome-sha1-faq/

Vulnérabilité dans SANTA

- Outil de black/whitelisting de binaires pour OSX

  https://reverse.put.as/2015/04/13/how-to-bypass-googles-santa-lockdown-mode/

Failles / Bulletins / Advisories

Crypto

FREAK

- Affecte:
  - OpenSSL, SChannel (Microsoft) et Apple SecureTransport
- Exploit:
  - Fonctionnalité antédiluvienne toujours supportée : Activation du chiffrement faible avec une clef RSA de 512bits max imposée par le gouvernement US
  - Exploitable lors d'un MitM actif puis factorisation de la clef
- Crédit:
  - Karthik Bhargavan, Antoine Delignat-Lavaud, Benjamin Beurdouche et Jean Karim Zinzindohoué de l'INRIA  et Microsoft

OpenSSL , 13 CVE

- Déni**s** de service
- Contournement de signature de PKCS#7
- Aléa faible
- ...
  http://www.openssl.org/news/vulnerabilities.html

Failles / Bulletins / Advisories

Divers

Rowhammer, une faille matérielle.

- Des lectures répétées de certains espaces de la mémoire DRAM introduise le changement de certains bits
- Problème connu depuis au moins 2014 mais pas identifié comme vulnérabilité
- Il est ainsi possible d'élever ses privilèges sur le système
- Comment on patche le matériel ?
  - En achetant de la RAM ECC ?

http://googleprojectzero.blogspot.fr/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

Vulnérabilités dans les lecteurs Blu-ray

https://www.nccgroup.trust/en/blog/2015/02/abusing-blu-ray-players-pt-1-sandbox-escapes/

Multiple vulnérabilités dans Jenkins

https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2015-02-27

Backdoor dans plusieurs routeurs

- Digicom, Alpha Network, Pro-Link, Planet Networks, TrendNet, Realtek, Bless, SmartGate, Blue Link
- Ils partagent le même firmware
  - avec le même compte super/super

http://blog.ensolnepal.com/router_backdoor/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

JP Morgan, vol de 76 millions de données de foyers et 7 millions de petite entreprises

- MitM suite au vol du certificat + Spearfishing
  http://www.itnews.com.au/News/397445,jpmorgan-found-breach-through-corporate-challenge-site.aspx

Des milliers de compte Uber vendus sur le marché noir du net pour 5$

http://www.theregister.co.uk/2015/03/30/unlimited_uber_accounts_flogged_for_5/
http://arstechnica.com/tech-policy/2015/03/dark-web-vendors-offer-up-thousands-of-uber-logins-starting-at-1-each/
http://thehill.com/policy/cybersecurity/237336-uber-denies-hack-after-discovery-of-user-info-for-sale

+50% de Phishing en France entre 2013 et 2014

www.silicon.fr/50-de-phishing-en-france-en-2014-112923.html

Piratages de milliers de sites WordPress a cause du plugin RevSlider

- Faille corrigée en février 2014 (CVE-2014-5460)
  - Possibilité d'uploader un webshell PHP considéré comme un thème par RevSlider
- Exploitée massivement à partir de septembre 2014 par le vers SoakSoak
  http://blog.sucuri.net/2014/12/revslider-vulnerability-leads-to-massive-wordpress-soaksoak-compromise.html

Désarmer les freins d'une voiture (FUD inside)

- Par un chercheur de la DARPA
  http://www.01net.com/editorial/644940/video-il-a-pirate-une-voiture-a-distance-et-desactive-les-freins/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Anthem, assureur américain, vol de 40 et 78 millions de données (suivant les sources)

- Dont le numéro de sécurité sociale

  http://www.zdnet.fr/actualites/piratage-d-ampleur-chez-un-assureur-americain-39814244.htm

Un casino piraté (par les Iraniens il paraît)

- 1 To d'infos exfiltrées

  http://news.softpedia.com/news/Las-Vegas-Casino-Hacked-By-Iranians-in-2014-Bloomberg-474440.shtml

Un détenu relâché par erreur suite à un phishing

- Il avait acheté un nom de domaine très semblable à celui de l'administration pénitentiaire

  http://www.bbc.com/news/uk-england-london-32095189

Piratage de la maison blanche par la Russie

- A base de phishing

  http://www.01net.com/editorial/651491/comment-des-hackers-russes-ont-pirate-la-maison-blanche-a-coup-de-phishing/

Nouveau canal auxiliaire : la chaleur

http://www.silicon.fr/hacker-un-ordinateur-par-la-chaleur-des-composants-112391.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Gazon, le virus Android qui s'envoie par SMS

https://nakedsecurity.sophos.com/2015/03/06/gazon-android-virus-smses-everyone/

Les dangers des JavaScript externes (tracking, publicité)

- Un script de tracking d'une banque finlandaise permettait de retrouver les numéros de comptes des utilisateurs

  http://oona.windytan.com/pankki.html

Un malware Android qui fausse l'arrêt du téléphone

http://betanews.com/2015/02/18/your-android-device-may-be-spying-on-you-even-when-its-off/

Campagne visant les sociétés du domaine de l'énergie : Trojan.Laziok

http://arstechnica.com/security/2015/03/energy-companies-around-the-world-infected-by-newly-discovered-malware/

http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

LogPOS, un nouveau malware s'attaquant aux terminaux de paiement

http://morphick.com/blog/2015/2/27/mailslot-pos

Malware avec Mutex dynamique

- Il va falloir penser à changer ses IOC !

  http://www.hexacorn.com/blog/2014/12/23/santas-bag-full-of-mutants/

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Nouveau mécanisme de persistance pour Gootkit

- Malware bancaire classique
- Exploite la technologie “Fix it” de Microsoft pour la persistance
  http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html

Un hébergeur qui loue des VPS compromis

http://morris.guru/huthos-the-totally-100-legit-vps-provider/

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

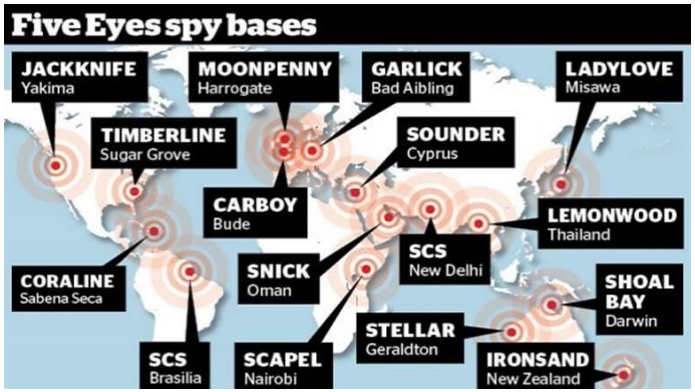
Vulnérabilités des dispositifs d'auto-administration de calmants

- Modification des limites autorisées, voir des valeurs...
- ...via une interface web
  http://www.wired.com/2015/04/drug-pumps-security-flaw-lets-hackers-raise-dose-limits/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Espionnage des communications en Polynésie par le GCSB

- Depuis sur la base militaire de Waihopai
  http://www.stuff.co.nz/national/67082905/snowden-files-inside-waihopais-domes



Equation Group de la NSA (L33t inside)

- Travaillent dans le domaine depuis les années 90
- A l'origine des codes offensifs les plus évolués
  - Stuxnet, Regin… ne serait que les miettes laissées aux autres équipes moins compétentes
- Backdoor de disque dur, partition fantôme, résistance à une mise à jour du firmware, fonctionnalités d'autodestruction…
- Plusieurs niveaux de compromission suivant les besoins

  << The malware platform is so complex that Kaspersky researchers still understand only a fraction of its capabilities and inner workings.>>

  https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Espions privés, barbouzes 2.0

- Reportage de Spécial Investigation mais rien de bien nouveau :
  - lockpicking et intrusion physique, spearphishing, IMSI Catcher, dépoussiérage, EDF vs Greenpeace… et quelques mots sur la sous-division K pour relever le niveau

http://www.canalplus.fr/c-infos-documentaires/pid3357-c-special-investigation.html?vid=1225013

Implant français : Après Babar et Evilbunny voici Casper 

- Adapte son comportement suivant la présence d'un antivirus
- Configuration interne en XML 
- Exploite une faille Flash
- Cible supposée : la Syrie

http://www.cyphort.com/babars-little-brother-meet-casper-friendly-ghost/

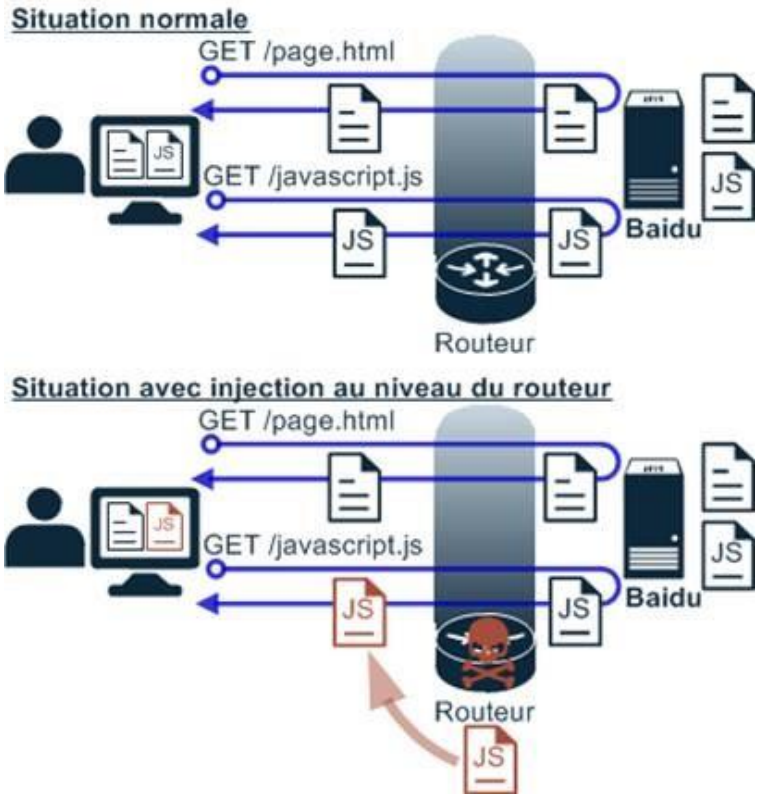
http://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/

Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS massif sur GitHub

- Modification à la volée de scripts de tracking Baidu pour insérer des requêtes vers Github
- Uniquement sur les requêtes HTTP (non chiffrées)
  http://taosecurity.blogspot.fr/2015/03/the-attack-on-github-must-stop.html
  http://insight-labs.org/?p=1682
  http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html



Les USA ont bien DDoSé la Corée du Nord en décembre 2014

- Mais aucun impact réel
  http://www.techworm.net/2015/03/we-did-north-korea-united-states-says-north-korea-web-outage-was-revenge-for-sony-hack.html

Google Maps utilisé pour du DDoS

- En cas d'utilisation d'un plugin de Joomla
  http://www.net-security.org/secworld.php?id=18002

Les plus gros DDoS en 2014 faisaient entre 300 et 400Gbps

http://www.techworld.com/news/security/worlds-largest-ddos-attack-reached-400gbps-says-arbor-networks-3595715/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Vol de plus de 2 millions de données médicales en 2014 aux USA

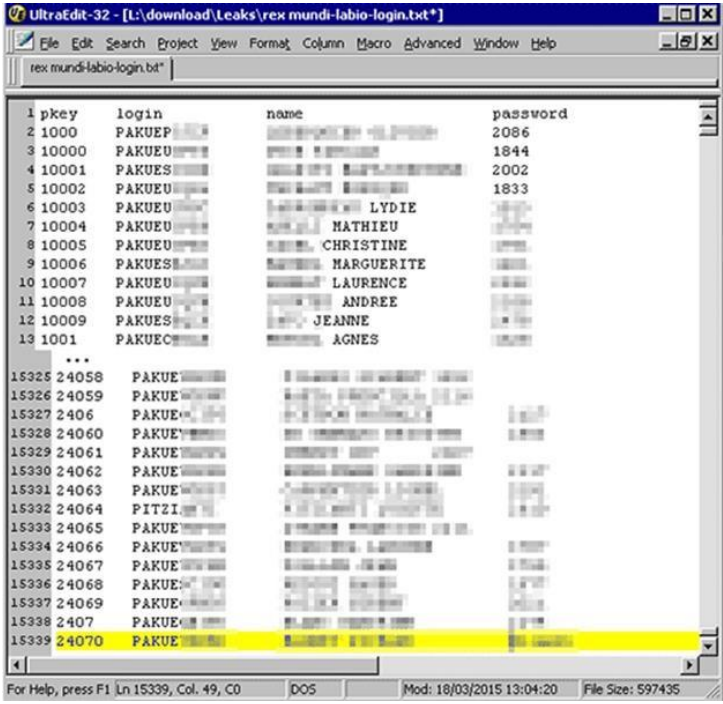
- +22% par rapport à 2013
- Dans 3% des cas, cela à conduit à des licenciements

http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/

Publication de données médicales (sur TOR)

- Par les criminels de Rex Mundi
- Vol et chantage (20ke) sur le laboratoire d'analyse Labio
  - Après Accord, Numéricable, Domino's Pizza…

http://www.01net.com/editorial/649252/rex-mundi-les-mysterieux-pirates-qui-extorquent-des-entreprises-francaises/



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Le site de rencontre Russe Topface paye son maître chanteur

- Le criminel Mastermind qui avait volé près de 20 millions de données personnelles (~20% des utilisateurs)
  - Et placé celles-ci sur un forum pour les revendre

http://www.techworld.com/news/security/mastermind-hacker-steals-20-million-credentials-from-dating-website-3595593/

Piratage du site de Forbes et injection d'un kit d'exploitation

- Abode Flash CVE-2014-9163 et Microsoft IE CVE-2015-0071

http://arstechnica.com/security/2015/02/pwned-in-7-seconds-hackers-use-flash-and-ie-to-target-forbes-visitors/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage de TV5 Monde

- Concours du journaliste relatant le plus d'inepties sur la sécurité
  http://www.lesechos.fr/tech-medias/medias/0204290083596-comment-le-directeur-informatique-de-tv5-monde-a-vecu-lattaque-de-linterieur-1109778.php
- Un bon article technique sur le sujet
  http://www.fixsing.com/tv5monde-a-tentative-technical-analysis/
- L'ANSSI est sur le coup (13 personnes?)

Piratage de Gemalto

- Par la NSA ou ses alliés ?
- Vol supposé des clefs secrètes de cartes SIM
- Discours officiel : "*pas d'inquiétude*". Mais en fait, si.
  http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx

Crypto
Divers

Audit du code crypto de TrueCrypt 7.1a (suite de l'audit de 2013)

- 4 vulnérabilités ou faiblesses
  - Faiblesse d'un générateur d'aléa **mais** dans de rares cas d'utilisation non standard de TrueCrypt
  - Canal auxiliaire sur AES **mais** si exécution de code sur l'ordinateur
  - Faiblesse du fichier contenant la clef de chiffrement
  - Fuite d'informations par l'entête des volumes Truecrypt **mais** sans idées de l'impact réels
- Pas de backdoor, tout du moins pas "évidente"
  https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf

L'IETF interdit RC4

- La RFC
  https://datatracker.ietf.org/doc/rfc7465/
- La traduction par Bortz
  http://www.bortzmeyer.org/7465.html

Pentest
Techniques & outils

SQL Inception

- Nouvelle technique d'injection SQL permettant de retrouver les requêtes SQL et donc faciliter l'exploitation
  http://www.contextis.com/resources/blog/sql-inception-how-select-yourself/

Forensics : Surveiller la délégation d'identité

http://digital-forensics.sans.org/blog/2015/03/30/monitoring-for-delegation-token-theft

Contournement de l'UAC

https://github.com/hfiref0x/UACME

Metasploit propose des meterpreter stageless

- Bypasser l'AV Sophos en ajoutant un "nop"
  https://www.youtube.com/watch?v=4xEzqISAmKI&feature=youtu.be

Pentest

Techniques & outils

Pentesting, you're doing it wrong

http://www.pentesticles.com/2015/03/penetration-testing-youre-doing-it.html

Utiliser des sessions ssh pour faire du port forwarding

http://0xthem.blogspot.fr/2015/03/hijacking-ssh-to-inject-port-forwards.html

Bruteforce de PIN d'iPhone assisté matériellement

- Coupe le courant avant l'incrément du compteur d'essais infructueux

http://blog.mdsec.co.uk/2015/03/bruteforcing-ios-screenlock.html

Identifier les relations de confiance dans un domaine Windows

http://www.harmj0y.net/blog/redteaming/domain-trusts-why-you-should-care/

Utiliser l'économiseur d'écran comme backdoor

http://www.labofapenetrationtester.com/2015/02/using-windows-screensaver-as-backdoor.html

Exporter les certificats en Powershell

http://carnal0wnage.attackresearch.com/2015/02/powershell-dumping-all-certs-in-cert.html

Combinaisons de touches pour s'échapper des modes "kiosque"

https://www.trustedsec.com/april-2015/kioskpos-breakout-keys-in-windows/

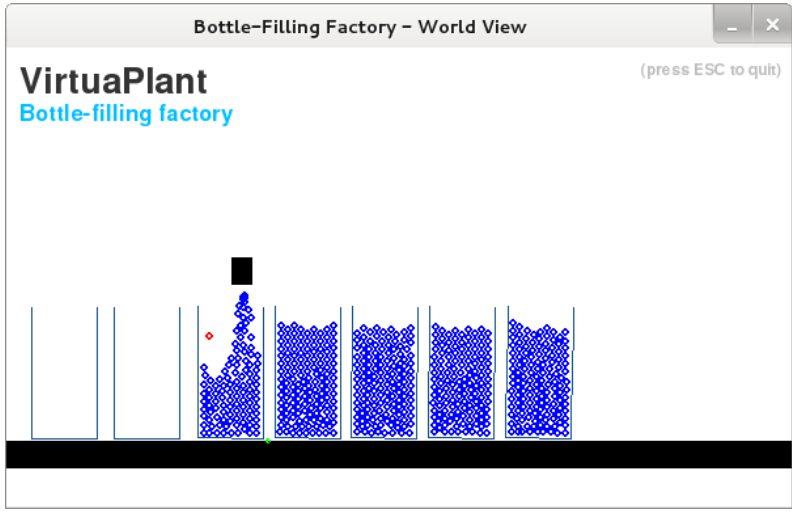
Scada
Divers

Modéliser le protocole s7 pour détecter les attaques

http://www.research.ibm.com/haifa/Workshops/security2014/present/Avishai_Wool_AccurateModelingoftheSiemensS7SCADAProtocol-v5.pdf

Un SI industriel virtuel : Virtuaplant

http://wroot.org/posts/introducing-virtuaplant-0-1/



Patcher des machines non-connectées

http://www.darkoperator.com/blog/2015/3/11/patching-with-wsus-offline

Dumb crypto in smartgrids

http://cryptomaths.com/data/talks/2015-03-10-osgp-fse.pdf

Vulnérabilités dans les IHM Siemens

Quarklsab et PositiveTechnologies

https://ics-cert.us-cert.gov/advisories/ICSA-15-099-01

Vulnérabilités dans les équipements Metasys

- Plus d'un an pour publier un bulletin d'alerte...

https://ics-cert.us-cert.gov/advisories/ICSA-14-350-02

http://xs-sniper.com/blog/2015/03/23/johnson-controls-metasys-vulnerabilities-part-i/

Nouveautés (logiciel, langage, protocole...)
Open Source

unmask_jemalloc

- Visualisation des structures (chunks, arenas...) de "Jason Evans" JEMalloc (utilisé dans Firefox)
  https://github.com/argp/unmask_jemalloc

HTTP Public Key Pinning

- RFC en cours de rédaction et de validation auprès de l'IETF
- Mais tout comme HSTS, reste basé sur du trust-on-first-use
  http://www.ietf.org/id/draft-ietf-websec-key-pinning-21.txt

Filtrage réseau directement avec les NIC

http://www.reddit.com/r/netsec/comments/30oomf/traffic_filtration_using_nic_capabilities_on_wire/

Logiciel de prise ne main à distance open source

https://github.com/maxogden/screencat

Sortie du noyau Linux 4.0

- Application de correctifs sans reboot,
  http://www.omgubuntu.co.uk/2015/04/linux-kernel-4-0-new-features

Nouveautés (logiciel, langage, protocole...)

Open Source

RDPY : Microsoft RDP en Python !!!

https://github.com/citronneur/rdpy

Pydgin : Emulateur de CPU en Python

https://github.com/cornell-brg/pydgin

Nouveautés (logiciel, langage, protocole...)

Divers

Scripts Nmap pour exploiter la verbosité des authentification NTML

http://blog.gdssecurity.com/labs/2014/2/12/http-ntlm-information-disclosure.html

L'ANSSI très prolifique en cette fin d'hiver 

- Recommandations de déploiement des navigateurs Firefox et Chrome
- Guide de sécurisation de l'administration de SI
- Les profils de protection pour les systèmes industriels (firewall, vpn…)
- Guide sur la sécurisation des SI industriels
- Guide sur le DDoS
- ...

http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/

EMET 5.2

http://blogs.technet.com/b/srd/archive/2015/03/12/emet-5-2-is-available.aspx

Microsoft va proposer des "nano" serveurs

To achieve these benefits, we removed the GUI stack, 32 bit support (WOW64), MSI and a number of default Server Core components. There is no local logon or Remote Desktop support. All management is performed remotely via WMI and PowerShell. We are also adding Windows Server Roles and Features using Features on Demand and DISM.

http://blogs.technet.com/b/windowsserver/archive/2015/04/08/microsoft-announces-nano-server-for-modern-apps-and-cloud.aspx

Nouveautés (logiciel, langage, protocole...)

Divers

WinDBG

- Une GUI DbgKit

  http://www.andreybazhan.com/dbgkit/

- Une extension pour visualiser la mémoire du kernel

  http://scrammed.blogspot.fr/2015/02/a-windbg-extension-to-print-kernel.html

Business
France

Docker chez Viadeo

- Pour déployer facilement et rapidement sur les postes des développeurs
- Mais pas encore en prod
  https://speakerdeck.com/viadeoteam/docker-at-viadeo

Business
International

Le Myanmar (ex-Birmanie) s'ouvre aux GSM

http://www.economist.com/news/business/21640355-one-last-great-unphoned-territories-opens-up-mobile-mania

Cyanogen lève $80 millions

- Quelques mois après l'échec de rachat par Google

  http://techcrunch.com/2015/03/23/cyanogen-grabs-another-80-million-in-funding/

Droit / Politique

France

Google ne fait pas appel de l'amende de la CNIL

- Le conseil d'état a confirmé l'amende

  http://www.zdnet.fr/actualites/face-a-la-cnil-google-se-couche-39814080.htm

La CNIL place un juge au centre du blocage administratif

http://www.linformaticien.com/actualites/id/35731/blocage-administratif-des-sites-la-cnil-designe-un-ancien-magistrat-alexandre-linden-pour-valider-les-filtrages.aspx

La CNIL rappelle les bonnes pratiques du BYOD

http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/byod-quelles-sont-les-bonnes-pratiques/

Cyberattaques : mais que fait-on pour nous protéger ?

- Source infinie de mèmes 

  http://www.capital.fr/enquetes/revelations/cyberattaques-mais-que-fait-on-pour-nous-proteger-1029212

Pourquoi les perquisitions de nuit sont-elles interdites ?

- Pas vraiment de raisons claire, si ce n'est une loi de la révolution (Article 76 de la Constitution de l'An VIII, c'est-à-dire 1799)

  http://ledroitderaler.blogspot.fr/2015/02/pourquoi-les-perquisitions-de-nuit-sont.html

Droit / Politique

France

Les députés reçoivent BlueCoat

http://www.zdnet.fr/actualites/les-francais-bientot-espionnes-par-les-memes-systemes-americains-que-les-syriens-ou-les-birmans-39816912.htm

Hadopi vs la haine sur internet

http://www.numerama.com/magazine/32722-la-hadopi-prete-a-riposter-contre-la-haine-sur-internet.html

Le code civil sur GitHub

- Visualisez facilement tous les changements 

https://github.com/steeve/france.code-civil

Les hébergeurs français vs la loi de renseignement

- Lettre ouverte signée par AFHADS (Asso des hébergeurs de données de santé), Gandi, IDS, Ikoula, Lomaco, Online (Illiad) et OVH
- Risques d'exil et de suppression d'emplois

http://www.ovh.com/fr/news/articles/a1743.le-gouvernement-veut-il-contraindre-les-hebergeurs-internet-a-l-exil

Procès de Gilbert Chikli

- Le pionnier des arnaques au prédisent

http://www.france24.com/fr/20150330-gilbert-chikli-proces-pere-arnaques-president-faux-virement-banque-poste-israel-france/

Droit / Politique

International

Le pentagone va embaucher 3 000 professionnels de la sécurité

- Entre $42k et $132k / an
  http://www.net-security.org/secworld.php?id=18061

La maison blanche entre en guerre contre les hackers

- Executive Order under the authority of the International Emergency Economic Powers Act, Grosso modo : interdiction de commercer avec ces entités, d'entrer sur le territoire US voir gel des assets financiers aux US
  http://blog.crowdstrike.com/cyber-sanctions/

La chine veut accéder au code source des applications bancaires

- Pour vendre en chine, il faut livrer ses secrets
  http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html

Les chinois auraient 100 000 hackeurs visant les USA

- Selon l'ancien directeur de la NSA Mike McConnell
  http://www.bizjournals.com/cincinnati/morning_call/2015/03/former-nsa-leader-china-has-hacked-every-major-u-s.html

Droit / Politique

International

Chrome : Suppression de l'AC Chinoise CNNIC (China Internet Network Information Center)

- Suite à un MitM visant GMail
  http://arstechnica.com/security/2015/04/google-chrome-will-banish-chinese-certificate-authority-for-breach-of-trust/
  http://www.securityweek.com/google-revoke-trust-cnnic-certificates
  http://arstechnica.com/security/2015/04/google-chrome-will-banish-chinese-certificate-authority-for-breach-of-trust/
  http://it.slashdot.org/story/15/03/24/1730232/chinese-ca-issues-certificates-to-impersonate-google
  http://googleonlinesecurity.blogspot.fr/2015/03/maintaining-digital-certificate-security.html

GnuPG sauvé par les dons

- $137 000 dont $60 000 de la Linux Fondation
- Facebook et Stripe donneront $50 000 /an
  http://www.01net.com/editorial/644468/le-chiffrement-open-source-gnupg-sauve-in-extremis-par-les-dons-des-internautes/

Droit / Politique
International

Affaire SilkRoad

- 2 agents auraient volé $1 million en Bitcoins (DEA et services secrets)
- Revente d'informations sur l'enquête au principal accusé
  - Un des agents a donné accidentellement son vrai nom à l'accusé lors d'échanges
- Vol de bitcoins d'un compte gelé

https://s3.amazonaws.com/s3.documentcloud.org/documents/1697973/charges-against-former-federal-agents-in-silk.pdf

Dénoncez l'auteur de Zeus et empochez $3 millions

- Evgeniy MIKHAILOVICH BOGACHEV

http://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

Démantèlement du botnet Ramnit de 3,2 millions de zombies

http://www.01net.com/editorial/646882/ramnit-reseau-de-3-2-millions-de-pc-zombies-a-ete-demantele-par-europol/

Publication des pseudos des agents ayant espionné Anonymous

- Dont "angryhippo" 

https://pdf.yt/d/dGwko0Hb6fyHY8bS

Conférences

Passées

Texte en gris = déjà traité précédemment

- JSSI 2015 - 10 mars 2015 à Paris
  - Les slides : http://www.ossir.org/jssi/index/jssi-2015.shtml
- GS Days - 24 mars 2015 à Paris
- Insomni'hack - 20 mars 2015 à Genève

A venir

- 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
  - Challenge du 1er avril http://static.sstic.org/challenge2015/chlg-2015
  - Vrai challenge http://communaute.sstic.org/ChallengeSSTIC2015
    - Déjà résolu

challenge-2015-fish@sstic.org

Divers / Trolls velus

Zstd bon ratio compression/vitesse par l'auteur de LZ4

http://fastcompression.blogspot.fr/2015/01/zstd-stronger-compression-algorithm.html

- Vive l'open-data : La liste des communes française disposant d'un site web pas à jour
  https://www.data.gouv.fr/fr/datasets/securite-des-sites-informatiques-des-communes-francaises/

250 000 équipements avec la même clef SSH sur Shodan

- Avec l'empreinte est : dc:14:de:8e:d7:c1:15:43:23:82:25:81:d2:59:e8:c0
  https://www.shodan.io/search?query=dc%3A14%3Ade%3A8e%3Ad7%3Ac1%3A15%3A43%3A23%3A82%3A25%3A81%3Ad2%3A59%3Ae8%3Ac0
- Le TOP 1000 des clefs SSH les plus utilisées à travers le monde
  https://gist.github.com/achillean/07f7f1e6b0e6e113a33c

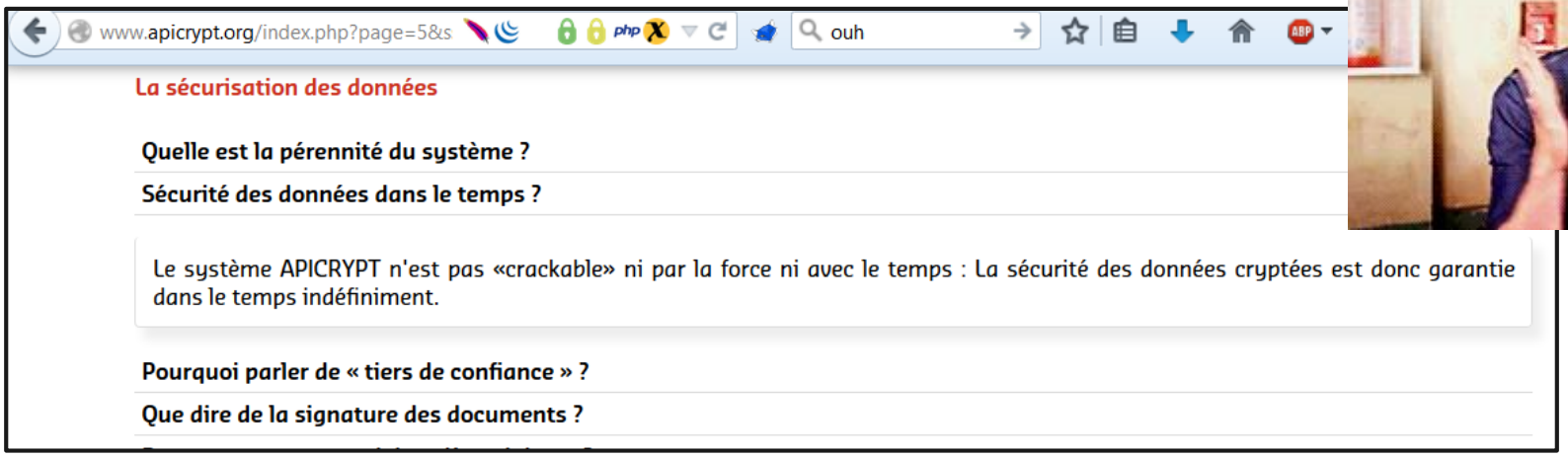
Pwn2Own

- Tout à été piraté
- Un coréen seul repart avec $225,000 de lot
  http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Pwn2Own-2015-Day-Two-results/ba-p/6722884#.VRFQqx4udX_

Divers / Trolls velus

APICRYPT

- Le ~~cryptage~~ chiffrement ultime !
  http://www.apicrypt.org/index.php?page=5&sspage=75#question15



- One-Time Pad / Masque Jetable
  - Double XOR avec 2 clefs
  - Clef de 20Mb (ne pas chiffrer de fichier plus gros )
  - Clef utilisée pendant 365 jours
  - Algo propriétaire et secret
    - Enfin plus maintenant https://github.com/schlecky/apicrypt
- Solution assez douteuse
  http://renaud.schleck.free.fr/apicrypt.php

Divers / Trolls velus

Le chiffrement sur Android par NQ Vault

- L'application de chiffrement la plus téléchargée (>30 millions)
- Utilise un algorithme extrêmement avancé : XOR
- Chiffre… les 128 premiers bits des fichiers

  https://ninjadoge24.github.io/#

Le cambrioleur de demain sera un hackeur

http://www.postaccess.fr/

La DARPA développe un moteur de recherche pour TOR !!?

- Nommé "Memex"

  www.darpa.mil/newsevents/releases/2014/02/09.aspx

Publication d'une liste de 10 millions de mots de passe

- Rapidement analysés

  http://wpengine.com/unmasked/

  http://web.archive.org/web/20150316185559/https://xato.net/passwords/ten-million-passwords/ (fichier texte de 190Mo)

Divers / Trolls velus

L'ANSSI chiffre ses offres d'emplois

- Uniquement sur IE
- A noter que le site a fait peau neuve

Et le Service d'Information du Gouvernement les poste sur Google Drive

https://drive.google.com/file/d/0B6K7htLtvvUsX1cyNXNyejVpYkJOb1lVLVo2aldBYnB6VmVv/view

Divers / Trolls velus

La journée de la femme digitale

- <<... Et parce qu'il est indispensable de mieux comprendre comment le **digital** transforme nos sociétés, notre manière de vivre ensemble, de travailler, de consommer, pour trouver sa place dans le monde de demain>>
  http://lajourneedelafemmedigitale.evolero.com/journeedelafemmedigitale/

Les soucis de la maison intelligente

- DoS réseau depuis sa lampe qui demandait qu'on change son ampoule
- Réveil en pleine nuit par les robots de nettoyage
  http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/

Oups, nous avons oublié de renouveler nos certificats expirés

- Pour régler le problème, changer la date de votre ordi
  https://manjaro.github.io/expired_SSL_certificate/

“Killer USB” La Clef USB à ne pas mettre dans tous les ordi

http://thehackernews.com/2015/03/killer-usb-explode-computer.html

Divers / Trolls velus

Pourquoi les nazis ont gagné la guerre de 1940 ?

- La réponse est dans les rapport TICOM (Target Intelligence Committee)
  - Programme d'espionnage du savoir-faire cryptographique des nazis
- La crypto française a été cassée (Machines suédoises Hagelin B-211 et BC38)
- <<Après 1940, tous les systèmes de Vichy étaient automatiquement compromis dès lors qu'ils étaient pris en compte par la Commission d'Armistice de Wiesbaden...>>
- Les détails :
  https://www.bakchich.info/france/2015/02/24/la-debacle-de-juin-1940-expliquee-par-la-nsa-63915
  http://en.wikipedia.org/wiki/Cipher_Department_of_the_High_Command_of_the_Wehrmacht

Après la pelleteuse et la grand-mère Géorgienne, voici le scooter brûlé qui coupe les fibres

http://bigbrowser.blog.lemonde.fr/2015/02/17/ariege-lincendie-dun-scooter-provoque-une-gigantesque-coupure-dinternet/

Divers / Trolls velus

Flash in PDF: 'The ideal solution'

- Existe-t-il une pire combinaison ???
  https://acrobatusers.com/tutorials/embedding-flash-brings-interactive-pdf-product-tour-life

Oui : Adobe qui fait du code pour Microsoft

http://blogs.msdn.com/b/ie/archive/2015/03/23/partnering-with-adobe-on-new-contributions-to-our-web-platform.aspx

Les excuses Cyber Sécurité

- “Il faut utiliser des mots de passe simples à retenir, ils sont partagés entre tant d'équipes !”
- “Désolé, je suis administrateur système, je ne sais pas corriger les problèmes de sécurité.”
- “Je ne sais pas ce que vous entendez par chiffrer, moi je vous dis que c'est crypté. Il n'y a que notre programme qui y a accès.”
  http://cyber.excusesecu.fr/

Pour rendre du code encore plus illisible

- Utilisez unicode
  https://twitter.com/kaepora/status/581437283200581632

Prochaines réunions

- Mardi 12 Mai 2015

After Work

- ~~Mardi~~ Mercredi 29 Avril 2015 à 19h30

  Bar "La Kolok"
  20 rue du croissant
  75002 Paris

  Présentation de "**FastResponder**" par Sébastien LARINIER de Sekoia

Questions ?