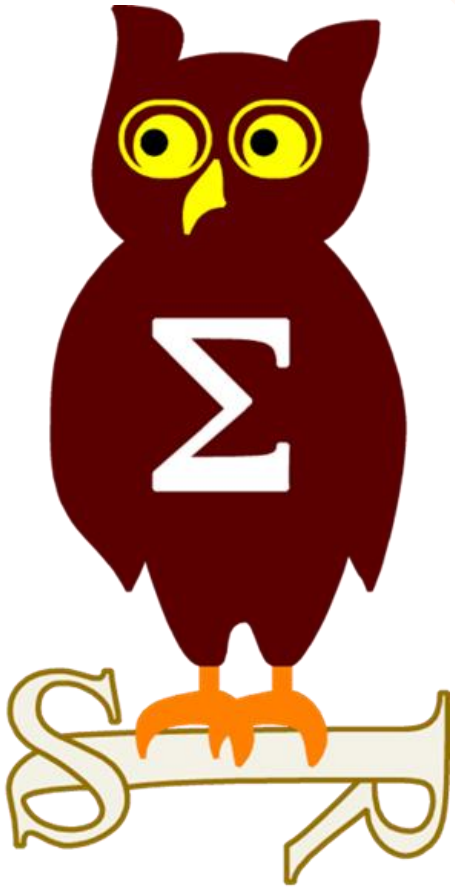
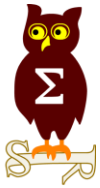


Revue d'actualité

08/12/2015

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

MS15-112 Vulnérabilités dans Internet Explorer (26 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées dont Windows XP Embedded POSReady)
  - Remplaces MS15-106
- Exploit:
  - **23** x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Fuites d'informations
  - 1 x Contournement ASLR
- Crédits:
  - 0011 par ZDI (CVE-2015-6075)
  - 0016EECD9D7159A949DAD3BC17E0A939 par ZDI (CVE-2015-6077)
  - Anonymous par ZDI (CVE-2015-6076)
  - Ashfaq Ansari par ZDI (CVE-2015-6086)
  - B6BEB4D5E828CF0CCB47BB24AAC22515 par ZDI (CVE-2015-6081)
  - Bo Qu de Palo Alto Networks (CVE-2015-6066, CVE-2015-6069, CVE-2015-6070, CVE-2015-6071, CVE-2015-6078, CVE-2015-6087)
  - Jason Kratzer par VeriSign iDefense Labs (CVE-2015-6065, CVE-2015-6085)
  - Kai Kang de Tencent's Xuanwu LAB (CVE-2015-6072, CVE-2015-6073)
  - Simon Zuckerbraun par ZDI (CVE-2015-6064)
  - Yuki Chen de Qihoo 360Vulcan Team (CVE-2015-6089, CVE-2015-6079, CVE-2015-6080, CVE-2015-6082, CVE-2015-6068, CVE-2015-6084)

MS15-113 Vulnérabilités dans Edge (4 CVE) [Exploitabilité 1,1,1,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS15-107
- Exploit:
  - 3 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement ASLR
- Crédits:
  - Bo Qu de Palo Alto Networks (CVE-2015-6078)
  - JaeHun Jeong (CVE-2015-6088)
  - Kai Kang de Tencent's Xuanwu LAB (CVE-2015-6073)
  - Simon Zuckerbraun par ZDI (CVE-2015-6064)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

MS15-114 Vulnérabilités dans le Journal Windows (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows Vista, 7, 2008, 2008 R2
  - Remplaces MS15-098
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier .JNT spécialement formaté
- Crédits:
  - Jason Kratzer par VeriSign iDefense Labs (CVE-2015-6097)

MS15-115 Vulnérabilités noyau Win32k.sys (7 CVE) [Exploitabilité 1-2]

- Affecte:
  - Windows (toutes versions supportées dont Windows XP Embedded POSReady)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplaces MS15-097 MS15-111 MS15-073
- Exploit:
  - 2 x Élévations de privilèges
  - 2 x Fuite d'informations
  - 2 x Exécutions de code lors du traitement d'une police de caractères
  - 1 x Contournement de Kernel ASLR
- Crédits:
  - Google Project Zero
  - James Forshaw (CVE-2015-6113)
  - Mateusz Jurczyk (CVE-2015-6103,CVE-2015-6104)
  - Nils Sommer de bytegeist (CVE-2015-6100, CVE-2015-6101, CVE-2015-6102)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

MS15-116 Vulnérabilités dans Office (7 CVE) [Exploitabilité 1,1,1,2,1,1,3]

- Affecte:
  - Microsoft Office toutes versions supportées (Windows et Mac)
  - Microsoft SharePoint 2007, 2010, 2013
  - Skype 2016, Lync 2013
  - Remplaces MS15-046 MS15-110 MS12-066 MS14-048 MS14-020 MS13-035 MS15-081 MS15-022
- Exploit:
  - Elévation de privilèges et possibilité de sortie de la sandbox d'internet explorer
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
- Crédits:
  - Mark Robbins Rebelmail (CVE-2015-6123)
  - SignalSEC Research par ZDI (CVE-2015-6093)
  - Steven Seeley de Source Incite par ZDI (CVE-2015-6038, CVE-2015-6094)
  - Steven Vittitoe de Google Project Zero (CVE-2015-6091, CVE-2015-6092)

MS15-117 Vulnérabilité NDIS (1 CVE) [Exploitabilité 2-4]

- Affecte:
  - Windows (toutes versions supportes)
- Exploit:
  - Élévation de privilèges locale avec le pilote réseau

  https://code.google.com/p/google-security-research/issues/detail?id=516
- Crédits:
  - Nils Sommer de bytegeist par Google Project Zero (CVE-2015-6098)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

MS15-118 Vulnérabilités dans .NET (3 CVE) [Exploitabilité 1,2,2]

- Affecte:
  - .NET 2.0 SP2, 4, 4.5, 4.6,
  - Remplaces MS14-057 MS11-100 MS14-009
- Exploit:
  - Élévation de privilèges
  - Contournement d'ASLR
  - Fuite d'informations
- Crédits:
  - John Page aka hyp3rlinx (CVE-2015-6099)

MS15-119 Vulnérabilité Winsock (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplaces MS14-040
- Exploit:
  - Élévation de privilèges
- Crédits:
  - Alex Ionescu de Winsider Seminars & Solutions Inc. (CVE-2015-2478)
  - Thomas Faber, de CrowdStrike Inc. (CVE-2015-2478)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

MS15-120 Vulnérabilité IPSec (1 CVE) [Exploitabilité 2-4]

- Affecte:
  - Windows 8, 8.1, 2012, 2012 R2,
- Exploit:
  - Déni de service sur IPSec (nécessite une authentification)
- Crédits:
  - ?

MS15-121 Vulnérabilités Schannel (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Remplaces MS15-055 MS15-076
- Exploit:
  - Usurpation d'identité en cas de MitM durant le hand-shake TLS
    - Lié à l'implémentation de la RFC 7627
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

MS15-122 Vulnérabilité Authentification / Kerberos (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplaces MS14-068 MS15-076 MS15-052
- Exploit:
  - Contournement de BitLocker (même si puce TPM) à chaud
    - Présenté à la Blackhat Amsterdam
- Crédits:
  - Ian Haken de Synopsys Inc. (CVE-2015-6095)

MS15-123 Vulnérabilité Skype/Lync (1 CVE) [Exploitabilité 2]

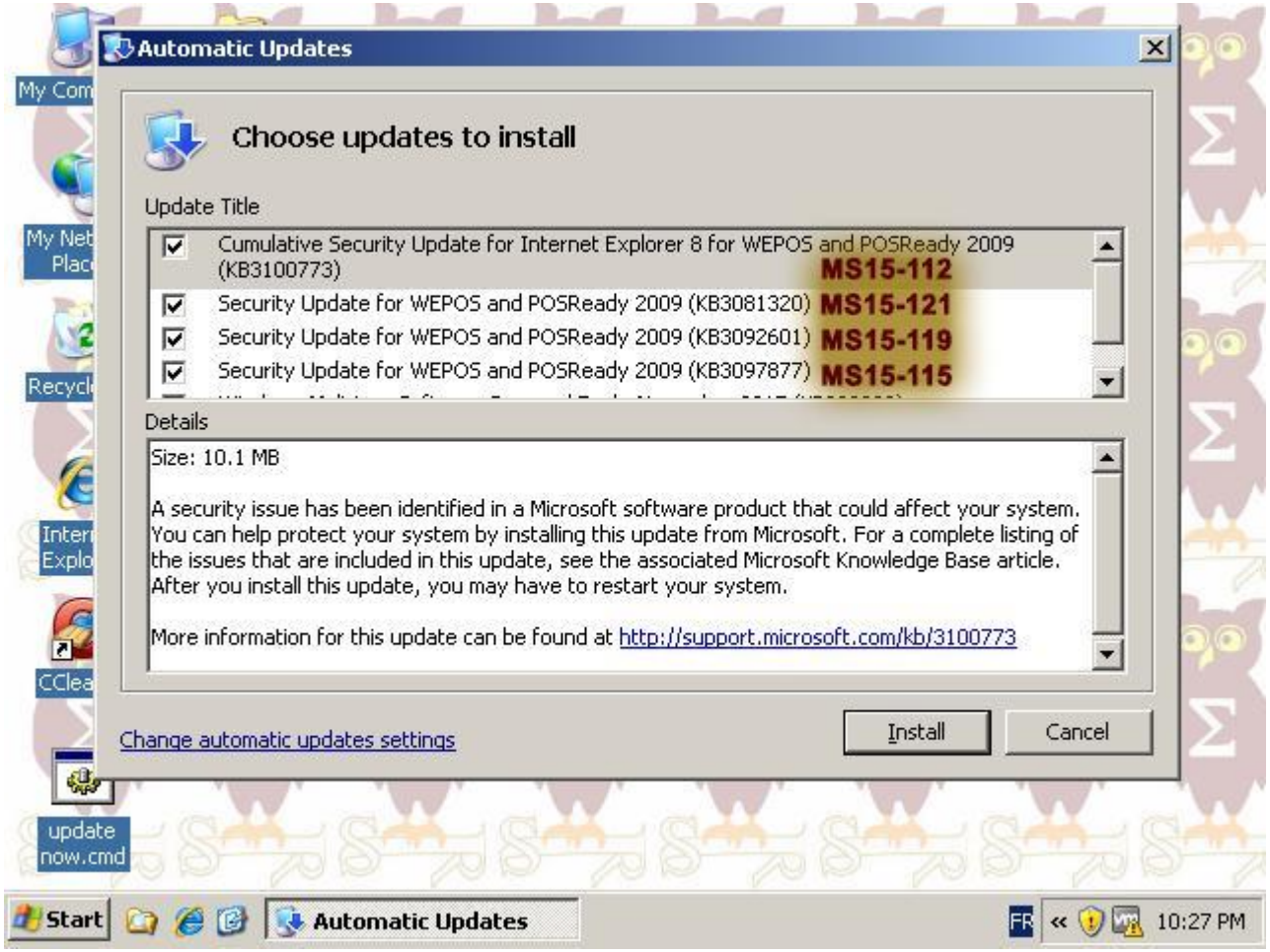
- Affecte:
  - Skype 2016, Lync 2010, Lync 2013
  - Remplaces MS15-097
- Exploit:
  - Injection de code Html et Javascript
- Crédits:
  - Fatih Ozavci - Sense de Security (CVE-2015-6061)

Failles / Bulletins / Advisories

Microsoft - Avis Novembre 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Novembre 2015

2755801 Mise à jour de Flash Player

- V47.0 Nouvelle mise à jour de Flash Player

3108638 DoS Hyper-V

- V1.0 Correction d'une faille de certains chipsets à l'origine d'un DoS sur Hyper-V

3119884 Révocation du certificat de Dell

- V1.0 Révocation du certificat eDellRoot de Dell

Failles / Bulletins / Advisories

Microsoft - Autre

Internet Explorer 8, 9 et 10 , c'est bientôt la fin

- Prévu pour janvier 2016

https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support

UXSS dans Internet Explorer, tous les détails

https://blog.innerht.ml/ie-uxss/

Windows = 100% Backdoor

https://www.gnu.org/philosophy/malware-microsoft.html

Microsoft Edge empêche l'injection de code

- Seules les DLL signées sont acceptées

https://blogs.windows.com/msedgedev/2015/11/17/microsoft-edge-module-code-integrity/

Le moteur JavaScript d'Edge devient OpenSource

https://blogs.windows.com/msedgedev/2015/12/05/open-source-chakra-core/

https://github.com/Microsoft/node/tree/chnext/deps/chakrashim

Windows 10 prêt pour les IoT

http://www.theregister.co.uk/2015/12/04/new_version_of_windows_10_turns_security_nightmares_into_reality/

Failles / Bulletins / Advisories

Système (principales failles)

NVidia

- Élévation de privilèges locale à partir d'un Pipe nommé écrivant ce qui lui est envoyé dans une clef RUN du registre
- Corruption de mémoire

  https://code.google.com/p/google-security-research/issues/detail?id=515

Linkedin, XSS persistant

- <<a>body onload = alert('XSS') > devient <body onload = alert('XSS') >

  http://seclists.org/fulldisclosure/2015/Nov/82

eBay Magento

- XSS assez simple http://seclists.org/fulldisclosure/2015/Nov/73
  - <td width="10%">"><img src="c" onerror="alert(1)"><script>alert(1)</script> "><img src="c" onerror="alert(1)"><script>alert(1)</script></td>
- CSRF http://seclists.org/fulldisclosure/2015/Nov/74

Jenkins, exécution de code à distance sans authentification

- Pardon, non, en fait c'est une fonctionnalité activée par défaut ! 

  https://highon.coffee/blog/jenkins-api-unauthenticated-rce-exploit/

Failles / Bulletins / Advisories

Système (principales failles)

Dell et la récupération du service Tag

- Récupération en JavaScript en appelant Dell Foundation Services
  - sur le port 7779

http://lizardhq.rum.supply/2015/11/25/dell-foundation-services.html

Dell et son certificat racine

- Autorité racine eDellRoot installée par défaut… avec la clef privée

http://joenord.blogspot.in/2015/11/new-dell-computer-comes-with-edellroot.html

Dell et son second certificat racine

- Autre autorité racine DSDTestProvider avec la clef privée

http://www.silicon.fr/apres-edellroot-dell-de-nouveau-frappe-par-dsdtestprovider-132497.html

Lenovo ThinkVantage System Update

- Service en écoute sur 0.0.0.0:20050… accessible s'il n'y a pas de firewall
- Possibilité d'envoyer des objets .Net Remoting permettant de télécharger et installer des choses

http://en.wooyun.io/2015/11/13/30.html

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco FireSIGHT Manager des sondes IPS SourceFire

- "**curl -k**" et non vérification du certificat du site des mises à jour de signatures
  - Télécharge un .sh, exécuté en tant que root
  - Prise de contrôle du manager

http://wadofstuff.blogspot.com.au/2015/11/cve-2015-6357-firepwner-exploit-for.html

FireEye MPS, exécution de code à distance

https://twitter.com/taviso/status/672935668385890304

http://www.securityweek.com/fireeye-patches-critical-flaw-found-google-researchers

Routeur ADSL Arris, une backdoor dans la backdoor

- Une backdoor connue depuis 2009
  - Management web caché, accessible avec un mot de passe "journalier" généré à partir d'une graine
    - Rarement changée…
  - Activation du Telnet ou SSH
    - Shell retreint
- Accès SSH complet en utilisant les derniers nombres du numéro de série du routeur

  http://w00tsec.blogspot.fr/2015/11/arris-cable-modem-has-backdoor-in.html
- 600 000 routeurs seraient vulnérables au Brésil

  http://www.theregister.co.uk/2015/11/20/arris_modem_backdoor/

Failles / Bulletins / Advisories

Réseau (principales failles)

D-Link routeur WiFi, quand y'en a plus, y'en a encore !

- Buffer Overflow non authentifié sur l'administration https://packetstormsecurity.com/files/134363/D-Link-DGL5500-HNAP-Buffer-Overflow.html
- Buffer Overflow authentifié https://packetstormsecurity.com/files/134366/D-Link-DIR-615-Buffer-Overflow.html
- Buffer Overflow depuis UPnP https://packetstormsecurity.com/files/134367/D-Link-DIR-645-UPNP-Buffer-Overflow.html
- Buffer Overflow https://packetstormsecurity.com/files/134372/D-Link-DIR-866L-Buffer-Overflow.html
- Buffer Overflow https://packetstormsecurity.com/files/134373/D-Link-DIR-890L-R-Buffer-Overflow.html
- Directory Traversal https://packetstormsecurity.com/files/134371/D-Link-DIR-825-Buffer-Overflow-Directory-Traversal.html
- Injection de commande, encore le Ping https://packetstormsecurity.com/files/134365/D-Link-DIR-601-Command-Injection.html
- Injection de commande https://packetstormsecurity.com/files/134368/D-Link-DIR-815-Buffer-Overflow-Command-Injection.html
- Injection de commande par SSDP non authentifié https://packetstormsecurity.com/files/134374/D-Link-SSDP-Command-Injection.html

```
M-SEARCH * HTTP/1.1\r\nHOST:1.2.3.4:1900\r\n ST:urn:schemas-upnp-
  org:service:WANIPConnection:1;telnetd -p 9094;ls\r\n
  MX:2\r\nMAN:"ssdp:discover"\r\n\r\n'
```

Belkin n'est pas en reste

- Plusieurs vulnérabilités identifiées sur le routeur N150
- Aucune réponse de la part de l'équipe sécurité

https://0x62626262.wordpress.com/2015/11/30/belkin-n150-router-multiple-vulnerabilities/

Multiples vulnérabilités sur les routeurs WiMax Huawei

https://pierrekim.github.io/blog/2015-12-01-Huawei-Wimax-routers-vulnerable-to-multiple-threats.html

Failles / Bulletins / Advisories

Réseau (principales failles)

Divulgation d'adresses IP réelles derrière un VPN qui autorise la redirection de port

- Possibilité pour d'autres utilisateurs du même service de VPN d'accéder aux IPs réelles des utilisateurs
  - Nécessite que le service de VPN permette la redirection de port
  - Nécessite de se connecter au même serveur VPN (même adresse IP)
- Affecte toutes les technologies de VPN, et tous les systèmes d'exploitation
- Description détaillée (extraite du site source)

1. *Victim is connected to VPN server 1.2.3.4*
2. *Victim's routing table will look something like this:*
3. *0.0.0.0/0 -> 10.0.0.1 (internal vpn gateway ip)*
4. *1.2.3.4/32 -> 192.168.0.1 (old default gateway)*
5. *Attacker connects to same server 1.2.3.4 (knows victim's exit through IRC or other means)*
6. *Attacker activates Port Forwarding on server 1.2.3.4, example port 12345*
7. *Attacker gets the victim to visit 1.2.3.4:12345 (for example via embedding <img src="http://1.2.3.4:12345/x.jpg"> on a website)*
8. *This connection will reveal the victim's real IP to the attacker because of the "1.2.3.4/32 -> 192.168.0.1" vpn route.*

https://www.perfect-privacy.com/blog/2015/11/26/ip-leak-vulnerability-affecting-vpn-providers-with-port-forwarding/

Failles / Bulletins / Advisories

Google

Google collecte des données sur les étudiants

- Grâce à la synchronisation de Chrome dans le cloud activée par défaut sur Chromebook
  http://www.wired.com/2015/12/google-collected-data-on-schoolchildren-without-permission/
- Google nie, c'est uniquement pour améliorer l'expérience utilisateur ;-)
  http://www.bbc.com/news/technology-34994207

XSS sur Google Translate

- A base de "multipart/form-data"
  http://seclists.org/fulldisclosure/2015/Nov/104

Injection XSS dans l'application email AOSP

- *<meta http-equiv="refresh" content="0;URL='http://www.maliciousurl.com'" />*
- Toutes versions jusqu'à 7 vulnérables
- https://labs.integrity.pt/advisories/google-aosp-email-app-html-injection/

Failles / Bulletins / Advisories

Crypto

Le projet “Let’s encrypt” en béta publique

- Il est désormais possible de demander et obtenir des certificats

  https://letsencrypt.org/2015/12/03/entering-public-beta.html

Nouvelles vulnérabilités dans OpenSSL

- Rien de “critique”
- DoS sur la vérification de certificat, fuite mémoire lors du traitement de PKCS#7

  https://openssl.org/news/secadv/20151203.txt

Failles / Bulletins / Advisories

Divers

Contournement de l'authentification sur les SIEM McAfee

- Injection LDAP : NGCP|NGCP|NGCP; et n'importe quel mot de passe

  https://kc.mcafee.com/corporate/index?page=content&id=SB10137

Analyse statique de code PHP sur ~1000 plugins

- 103 vulnérabilités identifiées (XSS, SQLi, ..)

  http://blog.cinu.pl/2015/11/php-static-code-analysis-vs-top-1000-wordpress-plugins.html?m=1

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Derniers numéros d'une nouvelle CB American Express prédictibles

- A partir des numéros de la carte précédente

  http://www.wired.com/2015/11/samy-kamkar-10-dollar-tool-can-guess-and-steal-your-next-credit-card-number/

Point d'accès WiFi avec compromission automatique des binaires téléchargés

- Metasploit + BDFProxy

  http://decidedlygray.com/2015/11/19/evil-access-point-with-auto-backdooring-ftw/

Désanonymisation de TOR pour le compte du FBI

- Des universitaires auraient été payés $1 million pour attaquer (avec succès) TOR
- Lié aux arrestations de 2014 et à la présentation annulée de la Blackhat 2014

  https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users

  http://motherboard.vice.com/read/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects

Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS sur 3 banques Grecques

http://www.welivesecurity.com/2015/12/01/armada-collective-launches-ddos-attacks-greek-banks/

DDoS sur les serveurs DNS racine

xxxxxxxxxxxxxxxxxxxxxxxxxx

45% des Botnets servant aux DDoS seraient sous Linux

http://www.generation-nt.com/ddos-botnet-linux-kaspersky-xor-actualite-1921447.html

- Dont le principal serait XOR DDoS et son virus ELF polymorphe
  http://blog.malwaremustdie.org/2015/09/mmd-0042-2015-polymorphic-in-elf.html

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

Des milliers (millions?) d'objets partageant les mêmes clefs SSH et/ou TLS

http://thehackernews.com/2015/11/iot-device-crypto-keys.html

http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html

Raspbery Raspbian : PRNG prédictible

- Non utilisation de l'aléa matériel par défaut

  https://www.raspberrypi.org/forums/viewtopic.php?f=66&t=126892

Hello Barbie

- Une barbie version "Siri" qui envoie tout ce qu'elle entend à Mattel (ToyTalk)
- Début de la rétro ingénierie, la suite dans quelques semaines

  http://www.somersetrecon.com/blog/2015/11/20/hello-barbie-security-part-1-teardown

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Le Venezuela aurait espionné ses citoyens

- Avec FinFisher, le virus des allemands de Gamma Group

  http://www.el-nacional.com/tecnologia/Venezuela-usa-FinFisher-espiar-ciudadanos_0_725927530.html

Le Venezuela aurait été espionné par la NSA

- Retour d'un analyste de la NSA
  - Ou comment il a ciblé une compagnie pétrolière vénézuélienne

  http://electrospaces.blogspot.fr/2015/12/how-nsa-targeted-venezuelan-oil-company.html

ThinThread, le programme de collecte fermé par la NSA

- Collecte et croisement des métadonnées, peu cher et
- Remplacé par TrailBlazer, bien plus cher et collectant trop d'informations

  http://www.01net.com/actualites/thinthread-le-programme-ferme-par-la-nsa-qui-aurait-pu-eviter-les-attentats-du-11-septembre-932074.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

MyFreeCams

- Authentification non sensible à la casse et supprimant les caractères spéciaux
- D'anciens développeurs ont laissé une backdoor et vendent des tokens sur TOR avec une promotion de 90%

  http://motherboard.vice.com/read/a-dark-web-vendor-is-selling-millions-of-hacked-cam-girl-site-tokens

Pearson Vue

- Gestionnaire centralisé des candidats aux examens de certification (Cisco, IBM, F5…)
- Vol d'identifiants et adresses mails

  http://www.theregister.co.uk/2015/11/23/pearson_vue_data_breach_pcm/

  http://home.pearsonvue.com/About-Pearson-VUE/Press-Room/2015/Public-Statement-Regarding-Pearson-Credential-Mana.aspx

Amazon

- Possible compromission avec vol des mots de passe
- L'e-marchand demande à ses clients de changer leur mot de passe

  http://www.zdnet.com/article/amazon-is-resetting-account-passwords-for-some-accounts/

Piratage des Hôtels Hilton, Marriott, Holiday Inn, Renaissance, Sheraton et Radisson

- Vol des noms, numéros de CB et CVV2

  http://www.zdnet.fr/actualites/vaste-piratage-des-hotels-hilton-39828734.htm

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Des hackers Russes volent $3.8 Million dans des ATM

- Avec une technique originale :
  a. Dépôt de liquide
  b. Retrait immédiat de la somme
  c. Annulation du retrait grâce à un complice ayant le contrôle de l'ATM

http://thehackernews.com/2015/11/atm-hacker.html

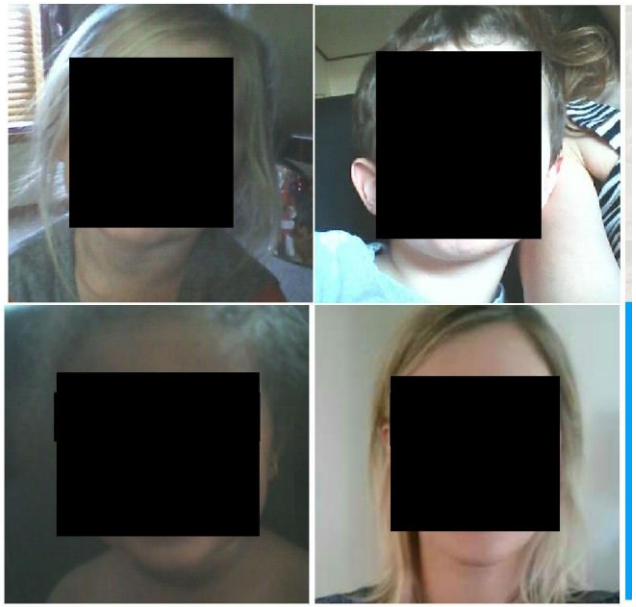
VTECH piraté

- La base de données contenant les informations de 5 millions de parents et 200 000 enfants a été piratée
  - Via une injection SQL sur un de leur sites
- Mots de passe stockés en MD5
- Des photos et discutions entre enfants et parents diffusées

https://www.vtech.com/en/press_release/2015/statement/

http://www.troyhunt.com/2015/11/when-children-are-breached-inside.html

http://motherboard.vice.com/en_uk/read/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech

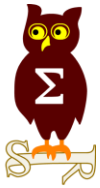


Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage d’une banque aux Emirats Arabes Unis (Invest Bank?)

- Demande d’une rançon en bitcoin d’environ 3 000 000 $
- Refus de payer => publication sur Twitter des comptes d’officiels du pays



Nouveautés, outils et techniques

L'Institut Fraunhofer analyse TrueCrypt en 75 pages, pour le compte du BSI

- Malgré les vulnérabilités récentes, les conteneurs sont solides
- Mais une faiblesse a été trouvée dans le PRNG

  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Truecrypt/Truecrypt.pdf;jsessionid=C46A2F3B7C535BDB330D47BCD470621E.2_cid286

Pentest

Techniques & outils

PSPunch, encore un outil d'intrusion en PowerShell

http://seclist.us/pspunch-an-offensive-powershell-console.html

MPC / MsfVenom Payload Creator

- Un Wrapper pour MsfVenom (le générateur de payloads de metasploit)

http://seclist.us/msfvenom-payload-creator-mpc-v-1-4-released.html

3 attaques sur le Tacacs Cisco

http://agrrrdog.blogspot.ca/2015/11/3-attacks-on-cisco-tacacs-bypassing.html

Z-Attack, pour tester la sécurité des réseaux Z-Wave

https://www.advens.fr/ressources/blog/z-attack-un-outil-pour-tester-la-securite-des-reseaux-z-wave

WebGun, constructeur d'XSS en ligne

http://brutelogic.com.br/webgun/

PemCracker, pour attaquer les certificats (et clef privées) protégés par mot de passe

https://github.com/bwall/pemcracker

Pentest
Techniques & outils

Booster AirCrack

- En couplant tous les outils déjà existant

  http://www.rootsh3ll.com/2015/11/aircrack-boost-script/

Acquisition de la mémoire sous Linux

http://www.kitploit.com/2015/11/lime-linux-memory-extractor.html

Persistance via Outlook

http://silentbreaksecurity.com/malicious-outlook-rules/

Interface web pour massscan

- Permet notamment de filtrer et chercher dans les résultats

  https://www.offensive-security.com/offsec/masscan-web-interface/

Récupérer les mots de passe en clair des admins de domaine

- En modifiant la politique de mot de passe

  https://adsecurity.org/?p=2053

Scada
Divers

3 nouveaux scripts pour le projet RedPoint de DigitalBond

https://github.com/digitalbond/Redpoint

Contournement de McAfee Application Whitelisting for Critical Infrastructure Systems

- Chargement de Shellcode avec PowerShell
- Formats de fichiers non vérifiés : HTA, JS,
- Utilisation d'un logiciel de compression ZIP de 1999, vulnérable ⇒ Exécution de code

https://bsidesvienna.at/slides/2015/a_case_study_on_the_security_of_application_whitelisting.pdf

Présence de clé SSH "en dur" sur les passerelles Modbus/IP d'Advantech

- Un correctif a été publié, regardé en détail : ShellShock, Heartbleed, Buffer overflow sur DHCP...

https://ics-cert.us-cert.gov/advisories/ICSA-15-309-01

https://community.rapid7.com/community/infosec/blog/2015/12/01/r7-2015-25-advantech-eki-multiple-known-vulnerabilities

Vulnérabilités sur les détecteurs de gaz Honeywell

- Modification de la configuration sans authentification

https://ics-cert.us-cert.gov/advisories/ICSA-15-309-02

Scada
Divers

Mot de passe codé en dur dans les contrôleurs Saia Burges

https://ics-cert.us-cert.gov/advisories/ICSA-15-335-01

Exécution de code à distance sur Schneider ProClimate

https://ics-cert.us-cert.gov/advisories/ICSA-15-335-02

Contournement de l'authentification sur les modules de communication pour automate Siemens

- Via le port TCP 102 (protocole S7)

https://ics-cert.us-cert.gov/advisories/ICSA-15-335-03

Contournement de l'authentification sur Moxa OnCell Central Manager

- Outil de gestion / paramétrage d'équipements distants
- Contournement de l'authentification
- Mot de passe codé en dur et donnant les privilèges "root"

https://ics-cert.us-cert.gov/advisories/ICSA-15-328-01

Nouveautés (logiciel, langage, protocole...)

Open Source

7-Zip, première nouvelle version stable depuis 2010 !!!

- Notable, bien que ce ne soit pas de la sécurité 

  http://www.7-zip.org/

Nmap 7.0.0

https://nmap.org/7/

Nmap sur Mainframe

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

OclHashcat enfin OpenSource

- Version de HashCat optimisée pour les GPU

  https://github.com/hashcat/

  https://hashcat.net/forum/thread-4880.html

Firefox 64bits est enfin là

- Et est donc éligible à EMET (Car contournable en 32bits)

  https://ftp.mozilla.org/pub/firefox/releases/42.0/win64/fr/

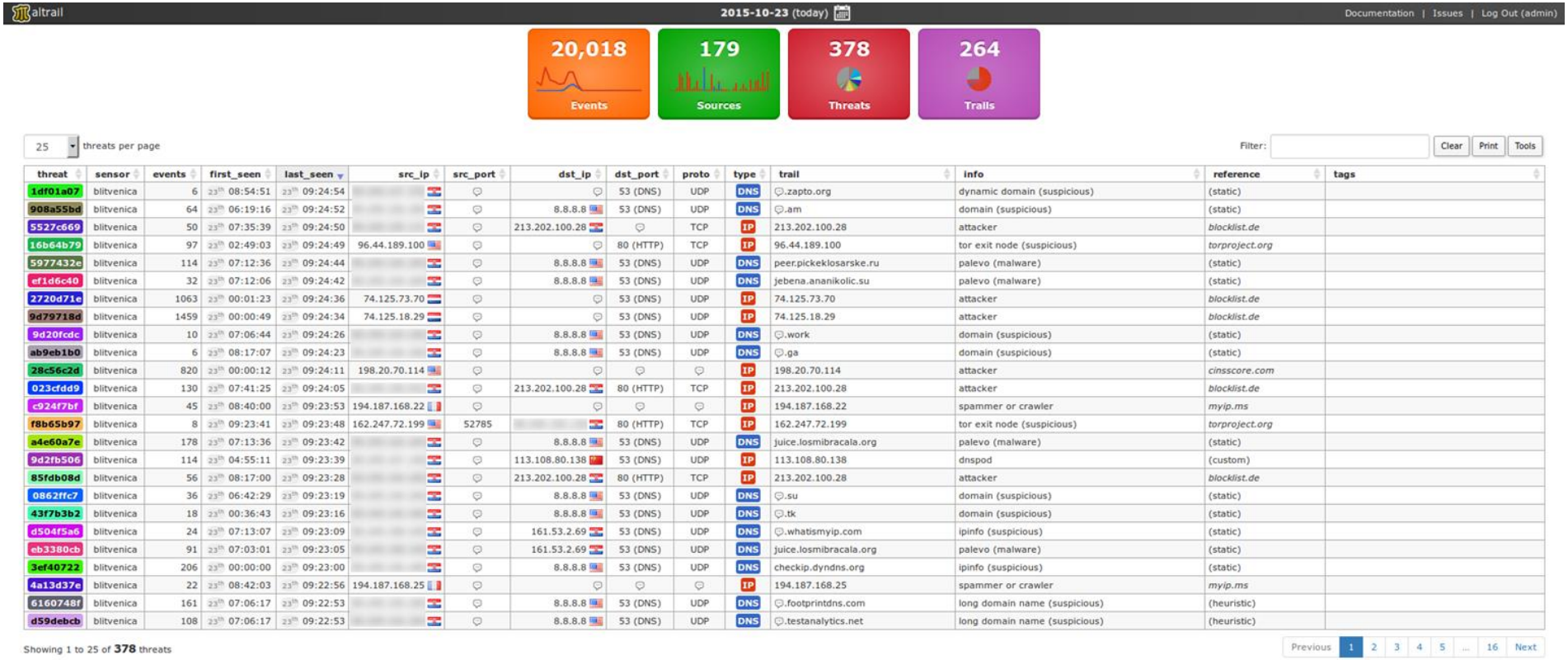
Nouveautés (logiciel, langage, protocole...)

Open Source

MalTrail

- Outil d'analyse réseau pour identifier des IPs/URL blacklistées

  https://github.com/stamparm/maltrail



Utilisation d'unikernels avec Qubes

https://danny.mantor.org/qubes-rumprun/

Nouveautés (logiciel, langage, protocole...)

Divers

AD ACL Scanner

- Auditez vos permissions Active Directory

  https://adaclscan.codeplex.com/

VirusTotal permet de sandboxing des exécutables pour Mac OS

- Mais comment font-ils alors qu'Apple impose du matériel Apple ? 😜

  http://blog.virustotal.com/2015/11/virustotal-mac-os-x-execution.html

Business et Politique

Business
International

Twitter licencie 8% de son personnel

http://pro.clubic.com/blog-forum-reseaux-sociaux/twitter/actualite-782576-twitter-licencie.html

Games of Drones : Google prépare un service de livraisons pour 2017

http://www.begeek.fr/games-of-drones-google-prepare-un-service-de-livraisons-pour-2017-184095

Bruxelles insiste pour réformer le Safe Harbor

http://www.nextinpact.com/news/97058-il-y-a-urgence-a-reformer-safe-harbour-martele-bruxelles.htm

Droit / Politique

France

Hadopi contre le terrorisme ?

http://www.europe1.fr/politique/terrorisme-bertrand-sen-prend-a-limam-google-2623363

Données personnelles : Optical Center sanctionné par la Cnil

http://www.zdnet.fr/actualites/donnees-personnelles-optical-center-sanctionne-par-la-cnil-39828236.htm

France : l'assemblée nationale vote une loi permettant à l'État de fermer des sites

http://www.developpez.com/actu/93045/France-l-Assemblee-nationale-vote-une-loi-permettant-a-l-Etat-de-fermer-des-sites-sans-controle-judiciaire-ni-delai/

Blocage de TOR, interdiction des WiFi ouverts, récupération des clefs de chiffrement pour la VoIP

- Retour vers le futur : bienvenue en 1984 

http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html

Droit / Politique

International

Cisco Technology Verification Service

- Programme payant pour regarder la confiance des clients perdus à cause de la NSA
  - N'empêche pas de backdoorer lors du transport...

http://www.silicon.fr/cisco-veut-se-proteger-de-la-nsa-131918.html




Le “patent troll” du siècle : CryptoPeak Solutions poursuit… la terre entière

- Pour l’utilisation des courbes elliptiques dans TLS

http://arstechnica.com/tech-policy/2015/12/patent-troll-claims-https-websites-infringe-crypto-patent-sues-everybody/


La Chine bloque les applications de messagerie étrangères et les VPN

http://www.journaldugeek.com/2015/11/24/chine-bloque-applications-messagerie-etrangeres-vpn/

En Thaïlande, parler mal du roi = prison

- Individu retrouvé grâce à son IP, révélée par Microsoft et venant des métadonnées des mails

https://www.privacyinternational.org/node/674

Le Kazakhstan impose l’installation d’une AC racine gouvernementale

http://www.zdnet.com/article/kazakhstan-forces-its-citizens-into-installing-internet-backdoors/

Droit / Politique

International

Russie vs ECRH (European Cour of Human Rights)

- Le législateur a décidé que la Russie n'avait pas besoin de se conformer
- Et va continuer son programme de surveillance de masse

  http://www.theregister.co.uk/2015/12/07/russia_new_law_restrains_echr_judgments/

Conférences

Conférences

Passées

Texte en gris = déjà traité précédemment

- Botconf - 2 au 4 décembre 2015 à Paris

  https://blog.rootshell.be/2015/12/02/botconf-2015-wrap-up-day-1/

- Blackhat Amsterdam - 10 au 13 novembre 2015 à Amsterdam

A venir

- 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

Orly, plantage de Windows 3.1

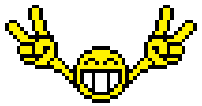
- L'application Decor (météo) tourne encore sous Windows 3.1 !!!
  http://www.clubic.com/insolite/actualite-785938-aeroport-orly-victime-panne-cause-windows-3-1.html

Sauvons la planète, utilisons les noms de domaine au lieu de Google

- 1 recherche = 7g de CO^2
  http://www.lemonde.fr/technologies/article/2009/01/12/une-recherche-google-a-un-cout-energetique_1140651_651865.html

Le CERT FR est en grande forme

- <<biscuit de pile>>, <<masque disjonctif>>
  http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-047/index.html



Divers / Trolls velus

Caches pour WebCam

- Pour les paranoïaques 

  http://soomz.io/

Savoir quelle application utilise la WebCam

https://phrozensoft.com/2015/11/who-stalks-my-cam-8

PS4, WoW, Call of Duty… autant de moyens de communication

- Impossible de tout surveiller

  http://www.numerama.com/politique/130839-non-rien-ne-dit-que-les-terroristes-de-paris-ont-utilise-des-ps4-pour-communiquer.html

Zerodium / iOS 9 : Les $1m auraient été remportés

http://www.pcworld.com/article/3000637/security/winner-claimed-in-1-million-ios-9-hacking-contest.html

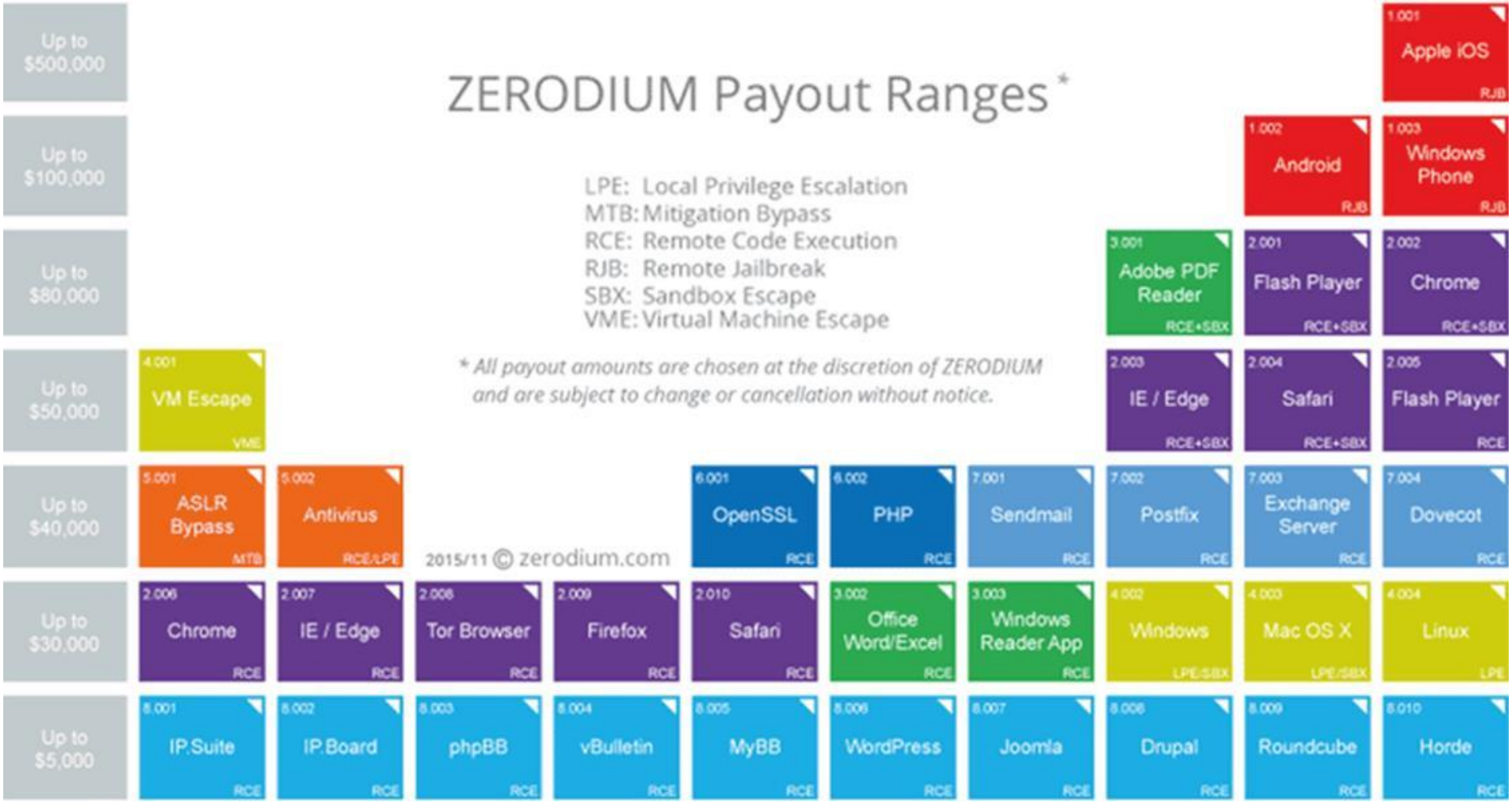
AT&T, un employé jugé pour avoir débloqué des milliers de smartphones de clients

- Moyennant finance (plusieurs dizaines de milliers de dollars)
- Il avait accès aux codes de déblocages en installant un malware sur les ordinateurs d'AT&T

  http://www.geekwire.com/2015/att-sues-former-employees-alleging-they-were-secretly-paid-to-unlock-hundreds-of-thousands-of-phones/

Divers / Trolls velus

Zerodium, les tarifs



Divers / Trolls velus

SQLi, 15 ans déjà

http://motherboard.vice.com/read/the-history-of-sql-injection-the-hack-that-will-never-go-away

Notepad++ et les élections

Divers / Trolls velus

La sécurité catastrophique d'un aéroport européen pointée du doigt par des hackers

http://www.01net.com/actualites/la-securite-catastrophique-d-un-aeroport-europeen-pointee-du-doigt-par-des-hackers-926508.html

HackingTeam, ils sont encore là!

Prochains rendez-vous de l’OSSIR

Prochaines réunions

- Mardi 12 Janvier 2016

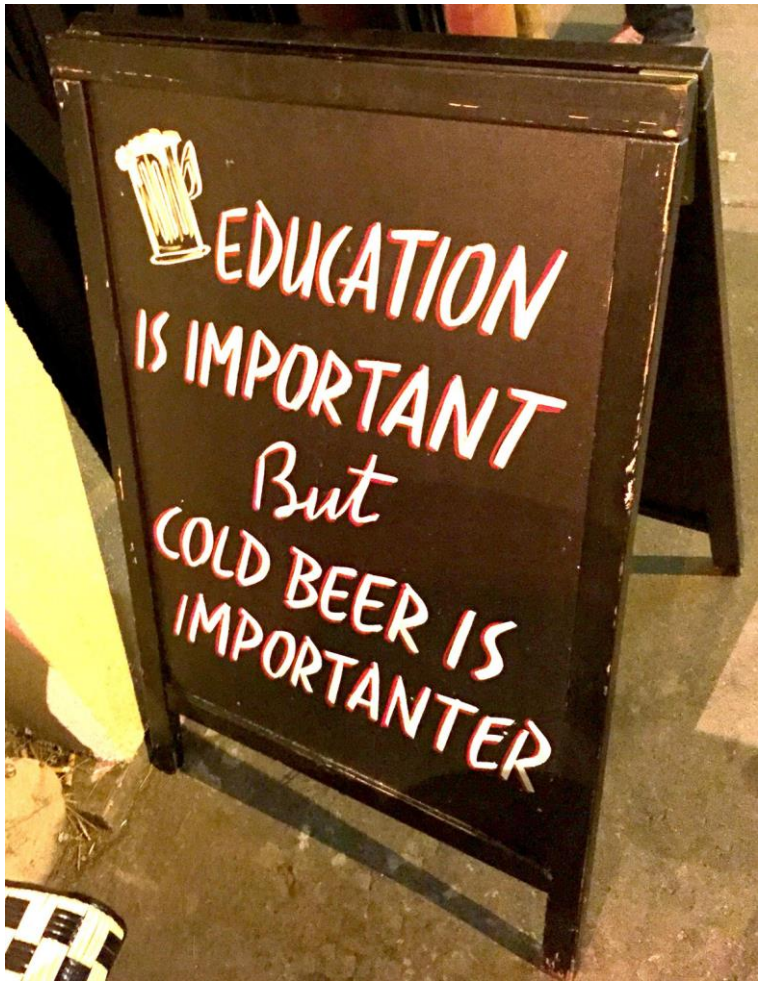
After Work

- 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