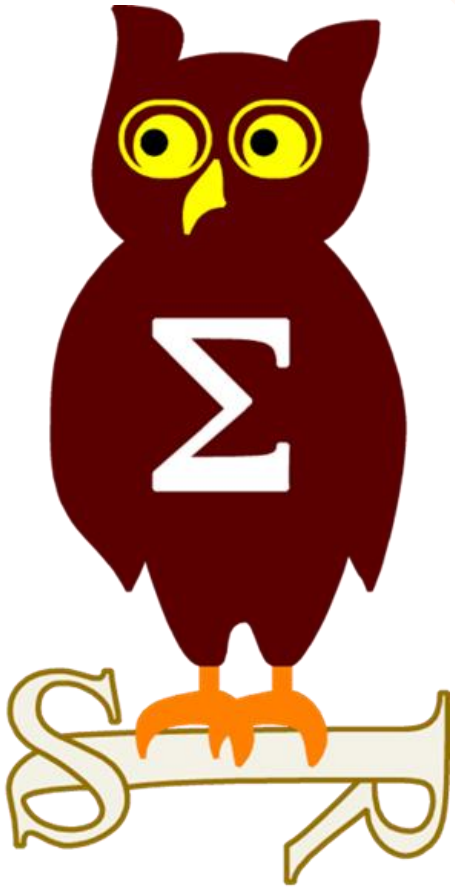
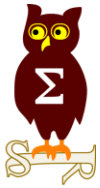


Revue d'actualité

12/01/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-124 Vulnérabilités dans Internet Explorer (30 CVE) [Exploitabilité 1-4]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 23 x Corruptions de mémoire aboutissant à une exécution de code
    - Code d'exploitation d'un Use-After-Free (2015-6152)
      https://www.exploit-db.com/exploits/38972/
  - 3 x Contournements des filtres anti-XSS
  - 2 x Fuites d'informations
  - 1 x Contournement ASLR
  - 1 x Élévation de privilèges
- Crédits:
  - A3F2160DCA1BDE70DA1D99ED267D5DC1EC336192 par ZDI (CVE-2015-6148)
  - Anonymous contributor par VeriSign iDefense Labs (CVE-2015-6156)
  - B6BEB4D5E828CF0CCB47BB24AAC22515 par ZDI (CVE-2015-6083, CVE-2015-6141, CVE-2015-6147, CVE-2015-6149, CVE-2015-6150)
  - Bo Qu de Palo Alto Networks (CVE-2015-6140, CVE-2015-6146)
  - ChenDong Li et YunZe Ni de Tencent (CVE-2015-6154)
  - Cong Zhang et Yi Jiang par Beijing VRV Software Co., LTD. (CVE-2015-6145)
  - Garage4Hackers par ZDI (CVE-2015-6160)
  - Hui Gao de Palo Alto Networks (CVE-2015-6083)
  - Jason Kratzer par ZDI (CVE-2015-6159)
  - Li Kemeng de Baidu Security Team(x-Team) par ZDI (CVE-2015-6151)
  - Masato Kinugawa (CVE-2015-6144)
  - Michal Bentkowski (CVE-2015-6139)
  - Moritz Jodeit de Blue Frost Security (CVE-2015-6152)
  - Rh0 (CVE-2015-6161)
  - Shi Ji (@Puzzor) (CVE-2015-6153)
  - Simon Zuckerbraun par ZDI (CVE-2015-6135, CVE-2015-6136, CVE-2015-6142)
  - SkyLined par ZDI (CVE-2015-6134)
  - Wenxiang Qian de TencentQQBrowser (CVE-2015-6162)
  - Zheng Huang de Baidu Scloud XTeam (CVE-2015-6159, CVE-2015-6155, CVE-2015-6157, CVE-2015-6158)

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-125 Vulnérabilités dans Edge (15 CVE) [Exploitabilité 1-4]

- Affecte:
  - Windows 10
  - Remplaces MS15-112
- Exploit:
  - 10 x Corruptions de mémoire aboutissant à une exécution de code
  - 2 x Élévations de privilèges
  - 1 x Contournement ASLR
  - 1 x Contournement des filtres anti-XSS
  - 1 x usurpation de site web par redirection
- Crédits:
  - A3F2160DCA1BDE70DA1D99ED267D5DC1EC336192 par ZDI (CVE-2015-6148)
  - Bo Qu de Palo Alto Networks (CVE-2015-6140)
  - ChenDong Li et YunZe Ni de Tencent (CVE-2015-6154)
  - Jason Kratzer par ZDI (CVE-2015-6159)
  - Li Kemeng de Baidu Security Team(x-Team) par ZDI (CVE-2015-6151)
  - Mario Heiderich de Cure53 (CVE-2015-6170)
  - Masato Kinugawa (CVE-2015-6176)
  - Michal Bentkowski (CVE-2015-6139)
  - Rh0 (CVE-2015-6161)
  - Shi Ji (@Puzzor) (CVE-2015-6153)
  - Simon Zuckerbraun par ZDI (CVE-2015-6142)
  - SkyLined par ZDI (CVE-2015-6168)
  - Zheng Huang de Baidu Scloud XTeam (CVE-2015-6159, CVE-2015-6155, CVE-2015-6158)

Failles / Bulletins / Advisories

Microsoft - Avis

Vulnérabilités communes entre Internet Explorer et Edge

- **2** en Octobre
  - CVE-2015-2485
  - CVE-2015-2486
- **3** en Juillet
  - CVE-2015-2446
  - CVE-2015-2449
  - CVE-2015-2341
- **3** en Novembre
  - CVE-2015-6078
  - CVE-2015-6073
  - CVE-2015-6064
- **11** en Décembre
  - CVE-2015-6139 Élévation de privilèges
  - CVE-2015-6140 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6142 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6148 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6151 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6153 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6154 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6155 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6158 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6159 Corruptions de mémoire aboutissant à une exécution de code
  - CVE-2015-6161 Contournement ASLR

Vulnérabilités en 2015

- **251** CVE sur Internet Explorer *(CVEDetails en compte 231, on vous laisse recompter* 😜 *)*
- **27** CVE sur Edge *(en 4 mois…)*

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-126 Vulnérabilités dans VBScript (3 CVE) [Exploitabilité 2,1]

- Affecte:
  - JScript 5.7 et 5.8 (Windows Vista, 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:
  - Anonyme par ZDI (CVE-2015-6136)
  - Anonyme par VeriSign iDefense Labs (CVE-2015-6137)
  - Simon Zuckerbraun par ZDI (CVE-2015-6135), CVE-2015-6136)
  - Yuki Chen de Qihoo 360Vulcan Team (CVE-2015-6136)

MS15-127 Microsoft DNS Serveur (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 2008, 2008 R2, 2012, 2012 R2
  - Remplaces MS12-017
- Exploit:
  - Exécution de code lors du traitement d'une requête
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-128 Vulnérabilités dans .NET (3 CVE) [Exploitabilité 1,1,1]

- Affecte:
  - Windows (toutes versions supportées)
  - En particulier .NET, Office, Skype for Business, Lync et Silverlight
  - Remplaces MS15-115
- Exploit:
  - 3 x Corruptions de mémoire du composant graphique aboutissant à une exécution de code

Crédits:

- Steven Vittitoe de Google Project Zero (CVE-2015-6106, CVE-2015-6107)

MS15-129 Vulnérabilités dans Silverlight (3 CVE) [Exploitabilité 2,2,1]

- Affecte:
  - Microsoft Silverlight 5
  - Remplaces MS15-080
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code
  - 2 x Fuites d'informations
- Crédits:
  - Marcin 'Icewall' Noga de Cisco Talos (CVE-2015-6165)

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-130 Vulnérabilité dans l'API Uniscribe (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows 7 et 2008 R2
  - Remplaces MS14-036
- Exploit:
  - Exécutions de code lors du traitement d'une police de caractères
- Crédits:
  - Hossein Lotfi, Secunia Research (now part de Flexera Software) (CVE-2015-6130)

MS15-131 Vulnérabilités dans Office (6 CVE) [Exploitabilité 1,1,1,1,1,1]

- Affecte:
  - Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, 2016, 2013 RT, pour Mac 2011
  - Remplaces MS15-116
- Exploit:
  - 3 x Exécutions de code à l'ouverture d'un fichier Excel spécialement formaté
  - 3 x Exécutions de code à l'ouverture d'un fichier Office spécialement formaté
    - "BadWinmail", exploité dans la nature avant l'avis de sécurité
      http://eromang.zataz.com/2015/12/28/cve-2015-6172-badwinmail-found-exploited-in-the-wild/
    - Les outils de Didier Stevens peuvent être utilisés..
      https://twitter.com/DidierStevens/status/588053259283210240/photo/1
- Crédits:
  - Haifei Li (CVE-2015-6172)
  - Kai Lu de Fortinet's FortiGuard Labs (CVE-2015-6118, CVE-2015-6177)
  - Steven Vittitoe de Google Project Zero (CVE-2015-6040, CVE-2015-6122)

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-132 Vulnérabilité dans LoadLibrary (3 CVE) [Exploitabilité 2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplaces MS15-122 MS15-115
- Exploit:
  - 3 x Erreurs de validation des entrées utilisateurs lors du chargement d'une librairie et exécution de code
    - Cumulable avec l'auto-download de Chrome et Edge

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/january/remote-exploitation-of-microsoft-office-dll-hijacking-ms15-132-via-browsers/

- Crédits:
  - Steven Vittitoe de Google Project Zero (CVE-2015-6132)
  - Yorick Koster de Securify B.V. (CVE-2015-6132)

MS15-133 Vulnérabilité dans le gestionnaire de message (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées) et Microsoft’s Message Queuing Service / MSMQ
- Exploit:
  - Élévation de privilèges locale par l'envoie d'une requête PGM (Pragmatic General Multicast) spécialement formaté
  - A noter que le Service MSMQ n’est pas activé par défaut mais souvent utilisé par des applications web
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS15-134 Vulnérabilité dans Media Center (2 CVE) [Exploitabilité 2,2]

- Affecte:
  - Windows Vista, 7, 8 et 8.1
  - Remplaces MS15-100
- Exploit:
  - 1 x Corruption de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier .mcl
    https://www.exploit-db.com/exploits/38918/
  - 1 x Fuite d'informations et téléchargement de fichier
    http://www.coresecurity.com/advisories/microsoft-windows-media-center-link-file-incorrectly-resolved-reference
- Crédits:
  - Francisco Falcon de Core Security (CVE-2015-6127)
  - Parvez Anwar (CVE-2015-6128)
  - Steven Vittitoe de Google Project Zero (CVE-2015-6128)
  - Zhang YunHai de NSFOCUS Security Team (CVE-2015-6131)

MS15-135 Vulnérabilité noyau (4 CVE) [Exploitabilité 1,1,1,4]

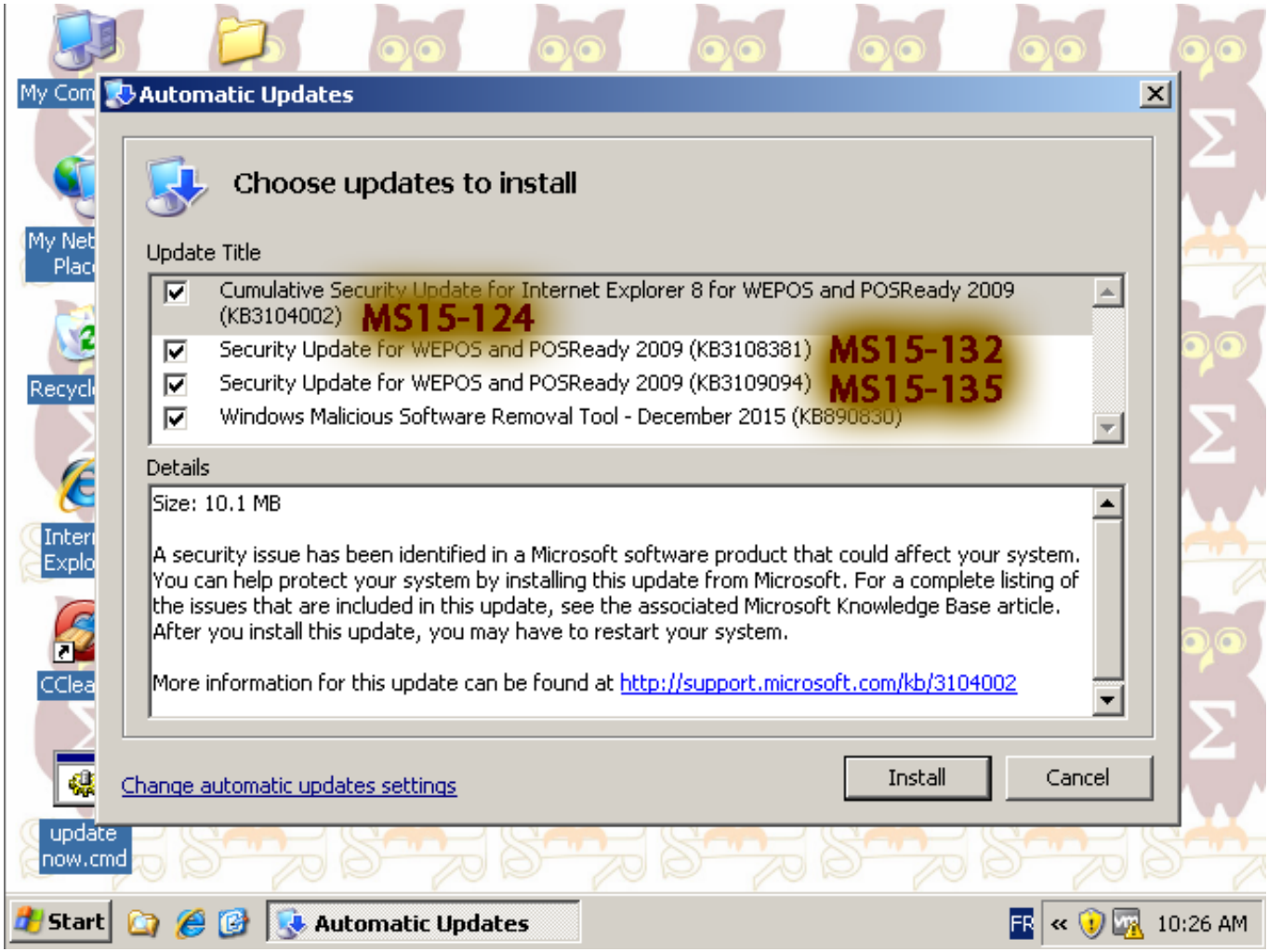
- Affecte:
  - Windows (toutes versions supportées)
  - Remplaces MS15-122 MS15-115
- Exploit:
  - 4 x Élévations de privilèges
- Crédits:
  - ChenDong Li de Tencent (CVE-2015-6175)
  - Nils Sommer de bytegeist par Google Project Zero (CVE-2015-6171, CVE-2015-6173, CVE-2015-6174)

Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions

3057154 Durcissement des configurations utilisant encore DES

- V1.1 Autorisation de DES pour de la rétrocompatibilité

3123040 Révocation de certificat

- V1.0 Révocation du certificat signant *.xboxlive.com https://crt.sh/?caid=1469
    - Suite à une fuite de la clef privée

Failles / Bulletins / Advisories

Microsoft - Autre

Un script pour détecter les services sans double quote

- Utilisés pour des élévations de privilèges locales
  https://gallery.technet.microsoft.com/scriptcenter/Windows-Unquoted-Service-190f0341

Internet Explorer 8, 9, 10 et 11, c'est la fin (aujourd'hui)

- Raccourcis rapide, dans les fait c'est plus compliqué et lié au système d'exploitation
  https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support
- Versions encore supportées :

Windows Desktop Operating Systems	**Internet Explorer Version**
Windows Vista SP2	Internet Explorer 9
Windows 7 SP1	Internet Explorer 11
Windows 8.1 Update	Internet Explorer 11
Windows Server Operating Systems	**Internet Explorer Version**
Windows Server 2008 SP2	Internet Explorer 9
Windows Server 2008 IA64 (Itanium)	Internet Explorer 9
Windows Server 2008 R2 SP1	Internet Explorer 11
Windows Server 2008 R2 IA64 (Itanium)	Internet Explorer 11
Windows Server 2012	Internet Explorer 10
Windows Server 2012 R2	Internet Explorer 11
Windows Embedded Operating Systems	**Internet Explorer Version**
Windows Embedded for Point of Service (WEPOS)	Internet Explorer 7
Windows Embedded Standard 2009 (WES09)	Internet Explorer 8
Windows Embedded POSReady 2009	Internet Explorer 8
Windows Embedded Standard 7	Internet Explorer 11
Windows Embedded POSReady 7	Internet Explorer 11
Windows Thin PC	Internet Explorer 8
Windows Embedded 8 Standard	Internet Explorer 10
Windows 8.1 Industry Update	Internet Explorer 11

Failles / Bulletins / Advisories

Microsoft - Autre

PAW : Privileged Access Workstations

- Recommandations Microsoft sur l'utilisation de postes dédiés à l'administration
- Rien de révolutionnaire dans l'approche, en ligne avec les recommandations de l'ANSSI
- Très opérationnel, un guide pas-à-pas

  https://technet.microsoft.com/en-US/library/mt634654.aspx

Analyse de la protection contre l'injection de DLL d'Edge

- Contournable... en signant sa DLL avec une AC reconnue 

  http://www.sekoia.fr/blog/microsoft-edge-binary-injection-mitigation-overview/ 

Failles / Bulletins / Advisories

Microsoft - Autre

DLL Hijacking, c'est sans fin

1. Auto-Download sur les navigateurs Edge et Chrome par défaut
2. Installation d'une application téléchargée et dont l'installer est une vieille version de NSIS
3. Chargement de la DLL précédemment téléchargées

http://textslashplain.com/2015/12/18/dll-hijacking-just-wont-die/

http://blog.opensecurityresearch.com/2014/01/unsafe-dll-loading-vulnerabilities.html

- Des « installer » vulnérables
  - EMSISoft -> UXTheme.dll

    http://seclists.org/fulldisclosure/2016/Jan/24
  - ZoneAlarm -> UXTheme.dll, WindowsCodecs.dll et ProfAPI.dll

    http://seclists.org/fulldisclosure/2016/Jan/21
  - TrueCrypt -> USP10.dll, RichEd20.dll, NTMarta.dll et SRClient.dll

    http://seclists.org/fulldisclosure/2016/Jan/22
  - Outils gratuits de Kaspersky -> UXTheme.dll, HNetCfg.dll, RichEd20.dll...

    http://seclists.org/fulldisclosure/2016/Jan/1

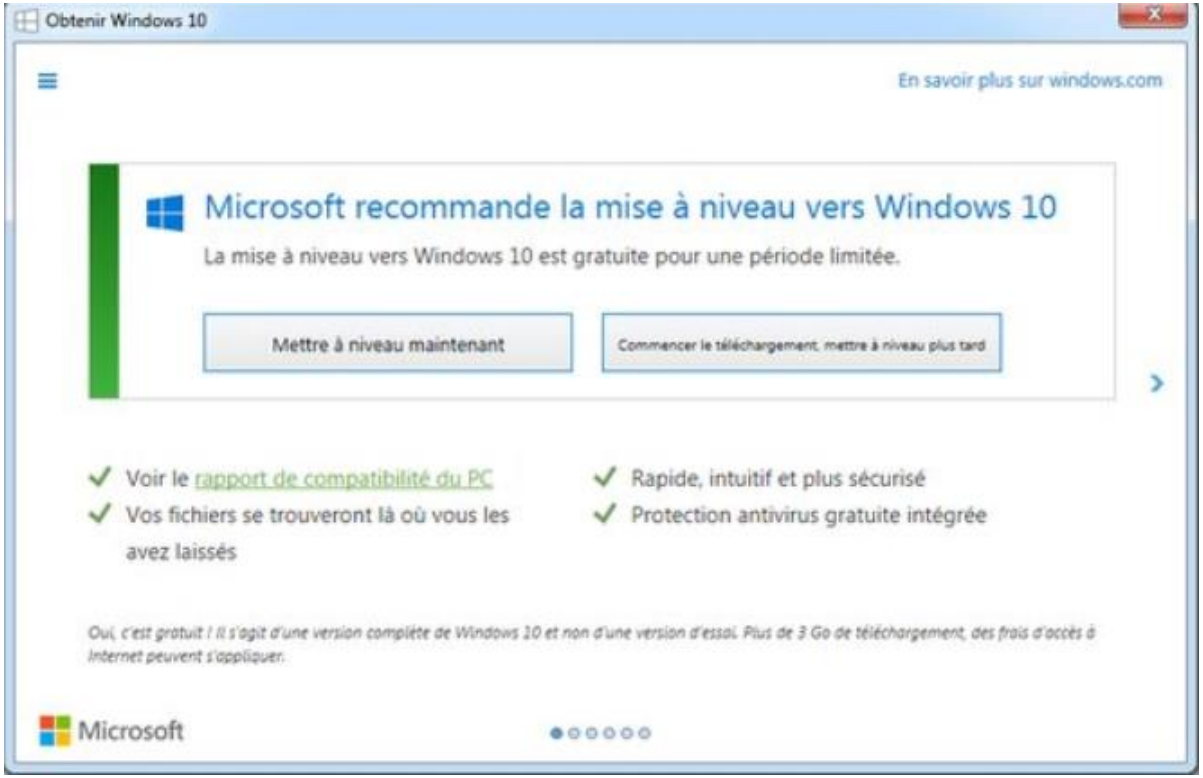
Contournement d'AppLocker grâce à c:\windows\tracing

https://twitter.com/subTee/status/681604454051778561

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10 : Passage en force !!!



Mise à jour de Windows 10 : les espions sont juste renommés !

http://www.networkworld.com/article/3010268/microsoft-subnet/microsoft-windows-10-update-privacy-spying.html

Failles / Bulletins / Advisories

Système (principales failles)

Grub 2, contournement de l'authentification

- [Back][Back][Back] ... x28 ... -> grub rescue
  - Mais qui utilise l'authentification Grub ? 

http://hmarco.org/bugs/CVE-2015-8370-Grub2-authentication-bypass.html

Joomla

- Exécution de code par desérialisation grâce à l'user-agent, non-contrôlé
  - A distance et sans authentification
  - Activement exploité

https://blog.patrolserver.com/2015/12/17/in-depth-analyses-of-the-joomla-0-day-user-agent-exploit/

http://arstechnica.com/security/2015/12/hackers-actively-exploit-critical-vulnerability-in-sites-running-joomla/

glibc:strncat(), integer overflow... inexploitable

https://sourceware.org/bugzilla/show_bug.cgi?id=19390

Wireshark, des dizaines de vulnérabilités

https://code.google.com/p/google-security-research/issues/detail?id=641 jusqu'à 663

Xen, explication des failles de type "double fetch"

- Liées à la paravirtualisation

https://www.insinuator.net/2015/12/xen-xsa-155-double-fetches-in-paravirtualized-devices/

Failles / Bulletins / Advisories

Système (principales failles)

Les anvitirus en 2016 ?

- McAfee, contournement des listes blanches d'applications exécutables

  http://en.wooyun.io/2015/12/15/Bypass-McAfee-Application-Control.html

- MacKeeper (AV pour Mac), piraté et vol des données de 13 millions de clients
  - 21Go de données dont les mots de passe (condensats en MD5)
  - Leur base de données était ouverture sur internet

  http://thehackernews.com/2015/12/mackeeper-antivirus-hacked_14.html

- Antivirus AVG, ajout d'une extension bourrée de failles à Chrome

  https://code.google.com/p/google-security-research/issues/detail?id=675

- TrendMicro, à l'installation, ajout d'un gestionnaire de mots de passes basé sur node.js et…
  - Ecoute en web sur le port **49155** avec possibilité d'envoyer des commandes
  - Donc depuis n'importe quel site web :

```
x = new XMLHttpRequest()
x.open("GET",
"https://localhost:49155/api/openUrlInDefaultBrowser?url=c:/windows/
system32/calc.exe true");
try { x.send(); } catch (e) {};
```

  - Mieux, on peut y mettre un stager ou launcher en PowerShell 

  https://code.google.com/p/google-security-research/issues/detail?id=693

Failles / Bulletins / Advisories

Réseau (principales failles)

FireEye, exécuter du code à distance sur une appliance

- Avant traitement d'un mail/document/navigation dans une machine virtuelle :
  - Vérification des adresses IP dans des blacklists
  - Vérifications des noms de domaines dans des blacklists
  - Passage dans des règles de détection d'intrusion (Snort)
  - Désobfuscation des fichiers
  - Analyse par un antivirus et par des règles Yara
- En cas de fichier Java -> désobfuscation en… exécutant certaines méthodes !!?

  https://code.google.com/p/google-security-research/issues/detail?id=666

Web Application Firewall F5 ASM, contournement des règles de filtrage

- En jouant avec la version déclarée du protocole HTTP (HTTP/x.x)

  http://seclists.org/fulldisclosure/2016/Jan/2

Failles / Bulletins / Advisories

Réseau (principales failles)

Firewalls Juniper, gamme Netscreen, deux portes dérobées avérées

- Revue de code et découverte de portions de code “non autorisées”

  https://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554

  https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST

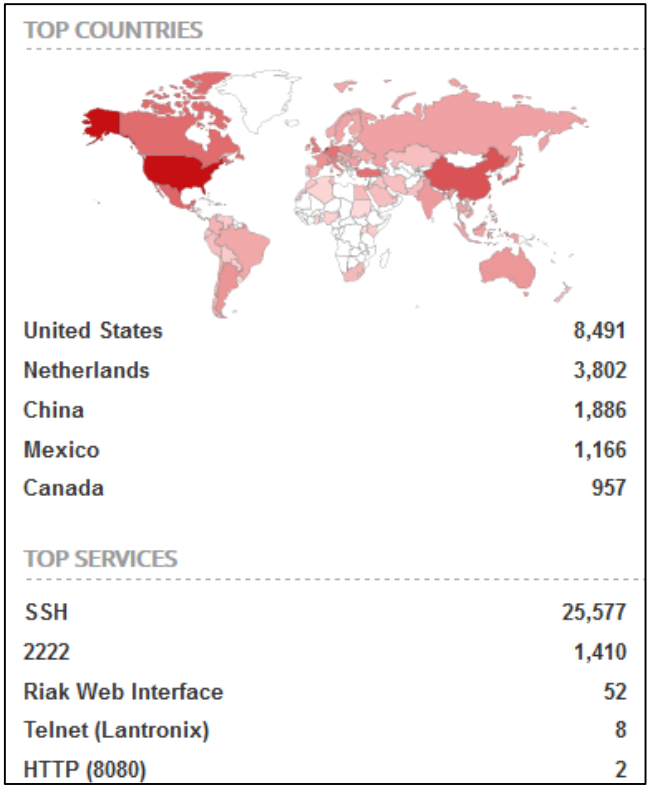
  - CVE-2015-7755, mot de passe d’admin universel
    - <<< %s(un='%s') = %u -> Sun Tzu ?
  - CVE-2015-7756, déchiffrement des tunnels VPN
    - Une backdoor de la backdoor Dual EC BRBG

    http://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/

- 26 000 Firewalls NetScreen accessible en SSH sur internet

  https://www.shodan.io/search?query=netscreen+product%3A%22NetScreen+sshd%22

  - Sans compter ceux connectés à Swift, CoreNet… face aux USA



Et FortigateOS ?

http://seclists.org/fulldisclosure/2016/Jan/26

Firewalls Juniper, suite (2/3)

- Lié à la NSA et son programme FEEDTROUGH ?
  - Aucune preuve formelle
  - Edward Snowden n'y croit pas

  https://twitter.com/snowden/status/680057235825901572?refsrc=email&s=11

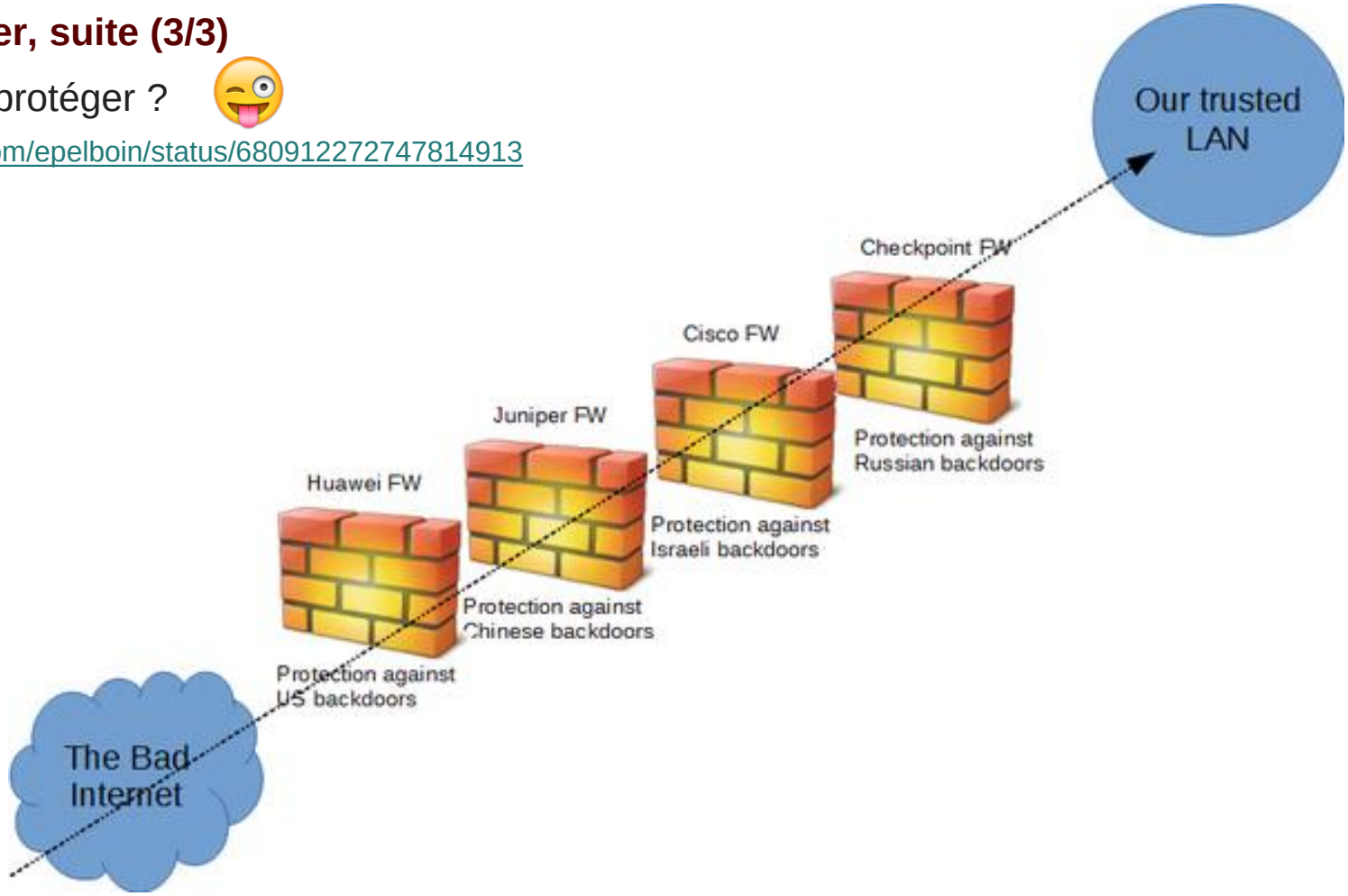
- "Fun fact" : La NSA réalise des mini-études type Gartner pour le compte du GCHQ dont celle sur Juniper

  <<Currently exploit capability :
  * Juniper NetScreen Firewalls models NS5gt, N25, NS50, NS500, NS204, NS208, NS5200,
  * NS5000, SSG5, SSG20, SSG140, ISG 1000, ISG 2000. Some reverse engineering may be required [...]>>
  https://theintercept.com/2015/12/23/juniper-firewalls-successfully-targeted-by-nsa-and-gchq/

Firewalls Juniper, suite (3/3)

- Comment se protéger ? 😜

  https://twitter.com/epelboin/status/680912272747814913



- Déjà en 2009, on parlait d'installer des portes dérobées dans ScreenOS

  http://phrack.org/issues/66/5.html#article

Failles / Bulletins / Advisories

Matériel

Trezor, porte monnaie physique de bitcoins

- Extraction de la clé privée

  https://jochen-hoenicke.de/trezor-power-analysis/

Porte dérobée dans une caméra IP sous BusyBox

- Il audit sa caméra et y découvre un service telnet accessible avec le compte root:123456

  http://jumpespjump.blogspot.fr/2015/09/how-i-hacked-my-ip-camera-and-found.html

BlackPhone, prise de contrôle du smartphone

- En cause, un service NVidia en écoute par défaut

  https://www.sentinelone.com/blog/vulnerability-in-blackphone-puts-devices-at-risk-for-takeover/

Failles / Bulletins / Advisories

Apple

Apple, pire que Microsoft ou Adobe en 2015 ?

- iOS : **375**
- Mac OS X : **384**
- Adobe Flash : **314**

https://www.cvedetails.com/top-50-products.php?year=2015

Failles / Bulletins / Advisories

Crypto

Vulnérabilité dans le client Jabber de CISCO : downgrade STARTTLS

- Exploitable sur Windows, iOS et Android

  http://synacktiv.ninja/ressources/cisco_jabber_starttls_downgrade.pdf

Failles / Bulletins / Advisories

Divers

Etude du niveau de sécurité des outils de monitoring

- Dans le scope : Cacti, Observium, Ganglia
- Utilisation d'analyse statique et dynamique

  http://www.eurecom.fr/fr/publication/4652/download/rs-publi-4652.pdf

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Écrasement de la pile sur z/OS

https://www.reddit.com/r/mainframe/comments/400ogh/smashing_the_zos_le_daisy_chain_for_fun_and_cease/

GPU Nvidia

- Non-effacement du tampon d'affichage de l'écran lors du passage à une autre application

https://charliehorse55.wordpress.com/2016/01/09/how-nvidia-breaks-chrome-incognito/

Cambrioler une maison 2.0, sécurisée par Comcast

- En brouillant les échanges ou en dé-authentifiant les capteurs utilisant ZigBee

http://arstechnica.com/security/2016/01/comcast-security-flaw-could-help-burglars-break-into-homes-undetected/

Microsoft IIS, énumérer les fichiers grâce aux noms courts 8.3

- Et avec les noms raccourcis contenant un tilde "~"

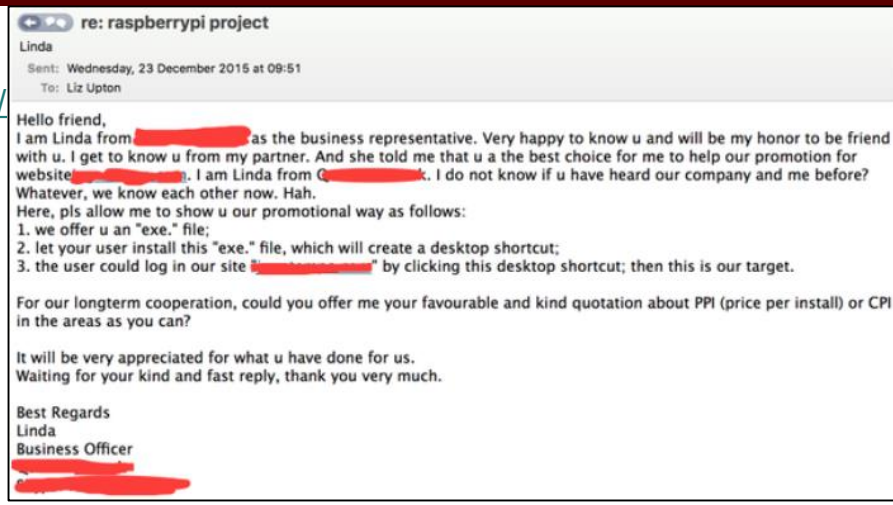
https://webbreacher.wordpress.com/category/tilde_enum/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Raspberry Pi, un malware contre de l'argent

https://twitter.com/Raspberry_Pi/status/679640660044058624/



re: raspberrypi project

Linda

Sent: Wednesday, 23 December 2015 at 09:51

To: Liz Upton

Hello friend,
I am Linda from [redacted] as the business representative. Very happy to know u and will be my honor to be friend with u. I get to know u from my partner. And she told me that u a the best choice for me to help our promotion for website [redacted]. I am Linda from [redacted]. I do not know if u have heard our company and me before?
Whatever, we know each other now. Hah.
Here, pls allow me to show u our promotional way as follows:
1. we offer u an "exe." file;
2. let your user install this "exe." file, which will create a desktop shortcut;
3. the user could log in our site [redacted]" by clicking this desktop shortcut; then this is our target.

For our longterm cooperation, could you offer me your favourable and kind quotation about PPI (price per install) or CPI in the areas as you can?

It will be very appreciated for what u have done for us.
Waiting for your kind and fast reply, thank you very much.

Best Regards
Linda
Business Officer
[redacted]

Ransom32 : un rançongiciel en JavaScript (Le premier?)

- Basé sur Node-Webkit, lui-même basé sur NodeJS
- Pour packager du Javascript dans Chromium et en faire une application exécutable.

http://blog.emsisoft.com/2016/01/01/meet-ransom32-the-first-javascript-ransomware/

BlackEnergy, attaque de centrale électrique Ukrainienne

- Coupure du courant pour 700 000 maison
- L'origine serait un groupe de criminels Russes, liés à l'état

http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Piratages, Malwares, spam, fraudes et DDoS

DDoS

Linode, DDoS et exfiltration de données

http://www.zdnet.fr/actualites/linode-sous-le-feu-des-ddos-l-hebergeur-reinitialise-les-mots-de-passe-de-ses-clients-39830700.htm

http://status.linode.com/incidents/mmdbljlglnfd

BBC victime d'un DDoS revendiqué par des opposants à Daesh

- Juste pour un test !!?
- Utilisation d'Amazon AWS
- Bande passante estimée à plusieurs centaines de Gbps

http://www.zdnet.fr/actualites/la-bbc-visee-par-une-attaque-ddos-revendiquee-par-des-opposants-a-daesh-39830528.htm

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Hack d’une montre Tom-tom runner

- Parties 2 et 3

  http://grangeia.io/2015/11/16/hacking-tomtom-runner-pt2/

  http://grangeia.io/2015/11/30/hacking-tomtom-runner-pt3/

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Quelle attaque correspond à quel groupe ?

- Référencement des groupes étatiques et criminels

  https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratage d'une compagnie aérienne

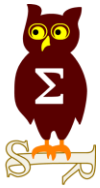
- Vol de 1,6 millions de données via un site B2B
- Les pirates annulaient les vols et proposaient un rebooking avec des frais supplémentaires

http://www.cyberexperts.co.in/?p=837

Vol du code source de Yandex, le moteur de recherche Russe

- Le voleur, un ancien employé a été appréhendé
- Il tentait de vendre le code $25 000

http://www.linformaticien.com/actualites/id/38982/combien-pour-le-code-source-du-moteur-de-recherche-russe-yandex.aspx



Nouveautés, outils et techniques

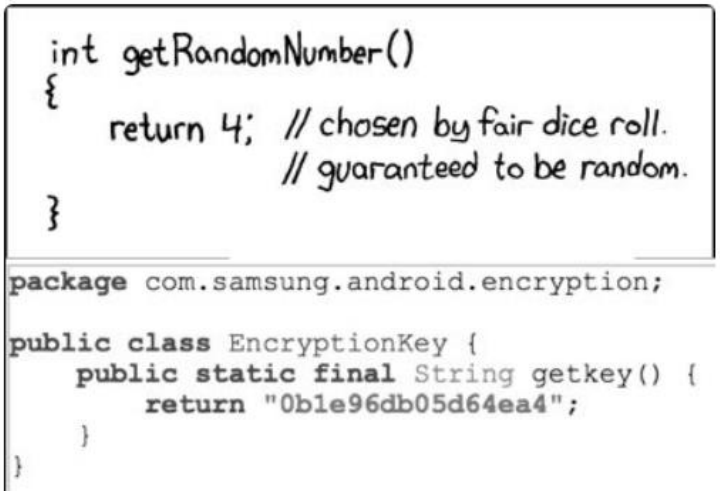
Crypto
Divers

Vuvuzela, la nouvelle messagerie chiffrant aussi les métadonnées

http://korben.info/vuvuzela-la-messagerie-qui-chiffre-aussi-les-metadonnees.html

A peine croyable !!! (si véridique)

https://twitter.com/marcograss/status/684547023354335232/photo/1



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

```
package com.samsung.android.encryption;

public class EncryptionKey {
    public static final String getkey() {
        return "0b1e96db05d64ea4";
    }
}
```

Quelques règles à respecter sur Tor

- Règles “de base”

  https://www.whonix.org/wiki/DoNot

CypherShed (ex- TrueCryptNext) sort en version RC1

- version 0.7.4

  https://github.com/CipherShed/CipherShedBuilds

Pentest
Techniques & outils

Kali NetHunter3

https://www.offensive-security.com/kali-nethunter/nethunter-3-0-released/

Mimikatz

- Fiabilisation des nom de domaine dans les tickets kerberos générés (MS14-068)

  https://adsecurity.org/?p=2495

```
588   601         KIWI_NEVERTIME(&validationInfo.PasswordMustChange);
589         -     RtlInitUnicodeString(&validationInfo.LogonDomainName, L"<3 eo.oe ~ ANSSI E>");
      602   +     RtlInitUnicodeString(&validationInfo.LogonDomainName, LogonDomainName);
```

- Fonctionnement sous Windows 10

  https://twitter.com/gentilkiwi/status/685228576350859264/photo/1

Burp paramalyzer

- Plugin détectant certaines informations sur les paramètres (XML, hashs, SSN…)

  https://github.com/JGillam/burp-paramalyzer

Florilège de techniques d'attaque de domaine Windows

https://adsecurity.org/?p=2362

Dnscat beta 5

- Tunneling DNS

  https://github.com/iagox86/dnscat2/releases/tag/v0.05

DSInternals : module AD en PowerShell

- Manipulation sur les identifiants et la base de données ntds.dit
- Récupération du mot de passe GMSA (Group Managed Service Accounts)

  https://github.com/MichaelGrafnetter/DSInternals

Exploiter un serveur JBOSS depuis un agent Empire

http://www.rvrsh3ll.net/blog/offensive/exploiting-jboss-with-powershell-and-empire/

Phishing via les applications de type Facebook, WhatsApp, etc..

- Choix d'un million de numéro de téléphones et récupération de toutes les infos possibles via les applis de messagerie, etc..

  http://arxiv.org/pdf/1512.07330v1.pdf

NPS : Not PowerShell

- Exécution de PowerShell sur des machines ne disposant pas de PowerShell

  https://github.com/Ben0xA/nps

Visionner l'écran d'une cible compromise via PowerShell

- Stream de l'écran accessible depuis un navigateur

  http://www.labofapenetrationtester.com/2015/12/stream-targets-desktop-using-mjpeg-and-powershell.html?m=1

Scada
Divers

The Great Train Cyber Robery

- Intervention de SCADA StrangeLove au 32C3

  http://fr.slideshare.net/AlexanderTimorin/the-great-train-cyber-robbery-scadastrangelove

  nouvelle liste de mots de passe par défaut : https://github.com/scadastrangelove/SCADAPASS

Panne électrique en Ukraine : une attaque informatique ?

- Peu d'informations techniques disponibles
- Semblerait qu'il s'agisse d'une attaque coordonnée sur plusieurs sous-stations électriques

  http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Vulnérabilité sur les API Schneider M340

- Stack-based buffer overflow sur le port 80

  https://ics-cert.us-cert.gov/advisories/ICSA-15-351-01

Nouveautés (logiciel, langage, protocole...)

Open Source

visUAL, un émulateur ARM graphique

http://salmanarif.bitbucket.org/visual/index.html

Expressions régulières faciles

https://github.com/VerbalExpressions/JSVerbalExpressions

```
// Create an example of how to test for correctly formed URL
var tester = VerEx()
    .startOfLine()
    .then('http')
    .maybe('s')
    .then('://')
    .maybe('www.')
    .anythingBut(' ')
    .endOfLine();
```

Mermaid : création de graphs à partir de texte

https://github.com/knsv/mermaid

Stateless computer par Joanna Rutkowska

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

WSUSpect Proxy

- Outil pour injecter de fausses mises à jour dans du trafic WSUS non chiffré

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

Business et Politique

Droit / Politique

France

Nouvelle version des exigences PASSI

- Uniquement des intervenants PASSI sur les missions
- Introduction des PASSI LPM (exigences spécifiques classifiées DR, à demander à l'ANSSI)
- Ajout d'une portée "SI industriels"

http://www.ssi.gouv.fr/uploads/2014/12/PASSI_referentiel-exigences_v2.1.pdf

Guide de l' ANSSI de recommandations de sécurité pour Linux

http://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

L'ANSSI déploiera des agents dans les 13 régions métropolitaines d'ici 2016

http://www.lagazettedescommunes.com/420754/securite-informatique-lanssi-deploiera-des-agents-dans-les-13-regions-metropolitaines-dici-2016/

L'OSSIR publie un livre blanc sur le PASSI

http://www.ossir.org/technico-juridique/index.shtml

Droit / Politique

France

Sécurité : l'inquiétante dérive vers la surveillance de masse

http://www.latribune.fr/technos-medias/internet/securite-l-inquietante-derive-vers-la-surveillance-de-masse-533211.html

UFC Que-Choisir dépose plainte contre VTech

- Faisant suite au piratage de novembre dernier

  http://www.linformaticien.com/actualites/id/38918/l-ufc-que-choisir-depose-une-plainte-contre-le-fabricant-de-jouets-vtech.aspx

Droit / Politique

International

Kim dot Com risque d'être extradé vers les USA

http://yro.slashdot.org/story/15/12/23/0259256/kim-dotcom-loses-extradition-case

Obama relance le débat sur le chiffrement et le terrorisme

http://www.numerama.com/politique/133859-obama-aide-firmes-tech-contre-terrorisme.html

L'Europe pourrait empêcher les adolescents d'aller sur Snapchat et Facebook sans accord parental

http://www.lefigaro.fr/secteur/high-tech/2015/12/15/32001-20151215ARTFIG00094-l-europe-pourrait-empecher-les-adolescents-d-aller-sur-snapchat-et-facebook-sans-accord-parental.php

Les Pays-Bas refusent les portes dérobées dans OpenSSL et y investissent 500 000 euros

http://www.silicon.fr/chiffrement-pays-bas-contre-backdoors-legales-134853.html

La chine dispose "officiellement" de capacité numériques offensives

http://sputniknews.com/asia/20160101/1032585585/china-cyberwarfare-military.html

Conférences

Conférences

Passées

- 32c3 - 27 au 30 décembre 2015 à Hambourg
  https://subtitles.media.ccc.de/event/32c3/

Texte en gris = déjà traité précédemment

A venir

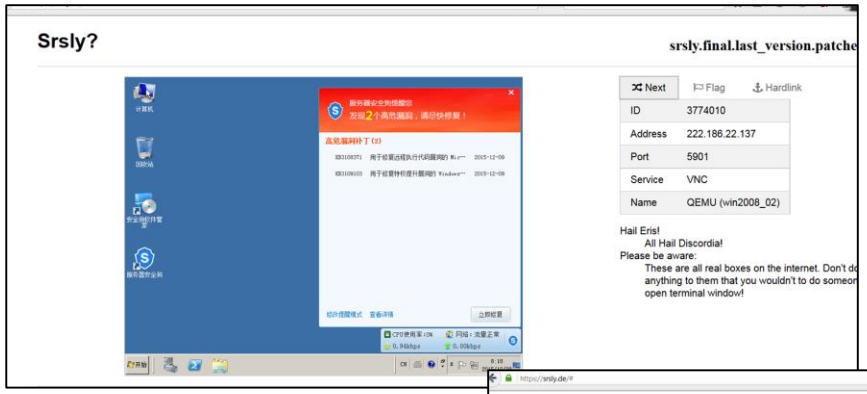
- FIC - 25 et 26 janvier 2016 à Lille
- CORI&IN - 27 janvier 2016 à Lille
- JSSI - 8 mars 2016 à Paris

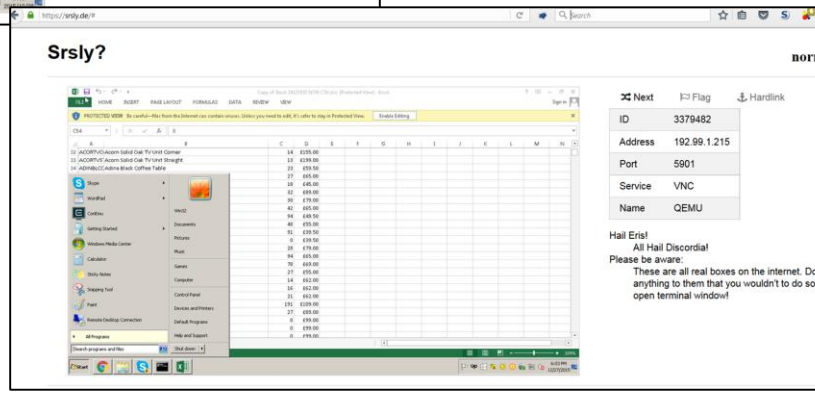
Divers / Trolls velus

Divers / Trolls velus

VNC Roulette 2, le retour

https://srsly.de/#





Déconnectez les caméras WiFi des locations

- Et conservez votre intimité

  https://julianoliver.com/output/log_2015-12-18_14-39

- Sinon, il y'a toujours ca : 

Audit de RedStar OS, le système nord-coréen

- Sert surtout à tracer les créations/modifications de fichier (Watermaking)

  https://lab.dsst.io/32c3-slides/slides/7174.pdf

  https://www.youtube.com/watch?v=8LGDM9exlZw

Divers / Trolls velus

Un russe découpe 29 billets pour en reconstituer 30 !!!

https://twitter.com/EnglishRussia1/status/681459459315642369/photo/1

Internet est massivement géo-réparti… en Virginie

- 70% du trafic mondial passerait par là, une grande partie vers AWS le Cloud Amazon

  http://www.nextgov.com/big-data/2016/01/70-percent-global-internet-traffic-goes-through-northern-virginia/124976/

Divers / Trolls velus

L’arme ultime de Poutine contre ISIS : des rats connectés :)

http://www.dailymail.co.uk/news/article-3383827/Vladimir-Putin-unleashes-new-secret-weapon-fight-against-ISIS-army-super-smelling-RATS-three-months-train-live-year.html

Divers / Trolls velus

Zerodium double temporairement la prime pour les vulnérabilités Flash

http://thehackernews.com/2016/01/flash-heap-isolation-exploit.html

https://twitter.com/cBekrar/status/685324527899824130

Le projet Tor ouvre son propre programme de prime à la vulnérabilité (Bug Bounty)

- Primes payées par l'Open Technology Fund et programme géré par HackerOne
- Pas encore d'information sur le montant des primes

https://hackerone.com/onion

http://motherboard.vice.com/read/the-tor-project-is-starting-a-bug-bounty-program

Si t'as pas scanné internet avant 40 ans, t'as raté ta vie

- Alors, fais le en 6 minutes avec Masscan (10 M paquets/s avec une carte 10Gb ethernet)

```
# masscan 0.0.0.0/0 -p0-65535
```

https://github.com/robertdavidgraham/masscan

Comprendre comment Volkswagen a triché

http://lwn.net/SubscriberLink/670488/4350e3873e2fa15c/

Divers / Trolls velus

S’initier aux rudiments de la sécurité informatique avec un jeu vidéo

http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__incendie/Zoom_article%2cI1602%2cZoom-98ef772f3230fc1241bc0756a9978b9c.htm

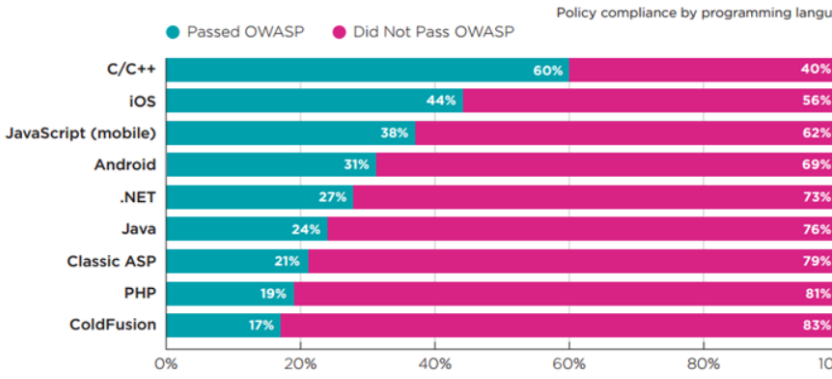
Encore une webcam filmant un token RSA…

- Accessible depuis un serveur web

https://twitter.com/davide_paltri/status/676696685456826368

Quel est le pire langage pour développer des appli web ?

http://thehackernews.com/2015/12/programming-language-security.html



Mail Tester

- Vérifiez si votre mail de phishing sera considéré comme du SPAM

http://www.mail-tester.com/

Divers / Trolls velus

Les Top arbitraire de l'année écoulée (1/2)

Les solutions de sécurité sont un *total* échec (©Nico)

- Les **Antivirus** sont bourrés de vulnérabilités (multiples parseurs + ajouts d'outils inutiles)
- Les **Firewalls** et routeurs sont backdoorés
  - Juniper (Backdoors dans le firmware)
  - Cisco (Backdoors "SYNful knock" dans certains routeurs)
- Les **appliances** de sécurité sont…
  - FireEye (Exécution de code à distance, contournement des analyses par collision MD5)
  - BlueCoat (https://ruxcon.org.au/assets/2015/slides/rucon-bluecoat-rigo.pdf)
  - SourceFire (Exécution de code à distance)
- Symantec signe des vrais faux certificats Google et se fait attraper

Les constructeurs d'ordinateurs ne sont pas fiables

- AC racine avec clef secrète pour Lenovo (Superfish) et Dell
- Samsung désactive Windows Update

Les routeurs SOHO sont… totalement troués

Divers / Trolls velus

Les Top arbitraire de l'année écoulée (2/2)

Piratages d'ampleurs : TV5 Monde, Gemalto, Thales, Hacking Team, Ashley Madison

Vulnérabilités

- Beaucoup d'évasions de machine virtuelle et exécution de code sur l'hyperviseur
- Freak sur SSL/TLS
- RowHammer
- MS15-034 (dump de la mémoire de IIS)
- Désanonymisation de TOR pour le compte du FBI
- Collision MD5

Retour en force des injections par des Macro Microsoft Office avec Dridex

Nous aussi nous avons nos codes offensifs : Dino, Babar, Casper et Bunny, rassurant !

Fin de :

- Flash
- Silverlight
- Internet Explorer 8, 9, 10 et 11 (en partie)
- SHA-1 160 bits (annoncé)

Prochains rendez-vous de l’OSSIR

Prochaines réunions

- Mardi 9 Février 2016

After Work

- Non planifié

JSSI 2016

- Mardi 8 mars 2016

Joyeux Anniversaire à l'OSSIR

JO/Association - Résultat

Page

Certains déclarants souhaitent qu'un lien hypertexte soit établi vers leur site propre. La Direction des Journaux Officiels décline toute responsabilité quant à la pertinence de ces liens et le contenu des informations ainsi mises à disposition

Autre recherche

1 réponse correspond à votre requête - Page 1 sur 1

Association: **OBSERVATOIRE DE LA SECURITE DES SYSTEMES D'INFORMATION ET DES RESEAUX (O.S.S.I.R.).** No/Identifiant:

Activité(s): **Communication/Technique et Recherche**

No de parution: **19960050** No d'annonce: **2263** Paru le: **11/12/96**

Département (Région): **75 - Paris (ILE-DE-FRANCE)**

Sous-préfecture: **Déclaration à la préfecture de police.**

Type d'annonce: **Création (déclaration d'association)**

Déclaration à la préfecture de police. **OBSERVATOIRE DE LA SECURITE DES SYSTEMES D'INFORMATION ET DES RESEAUX (O.S.S.I.R.).** *Objet :* développer et promouvoir l'utilisation sécurisée judicieuse des systèmes d'information et des réseaux électroniques de communication, faisant intervenir notamment les systèmes les plus avancés et l'Internet. Etude des performances, contraintes et avantages des divers systèmes de sécurité. Prise en compte des aspects juridiques. *Siège social :* 25, avenue Ledru-Rollin, 75012 Paris. *Date de la déclaration :* 21 novembre 1996.

Bonne année 2016

(et bon courage à tous…)

Pots de fleur connectés

Thermomètres connectés

https://twitter.com/ModusMundi/status/681275103435448320/photo/1

https://www.youtube.com/watch?v=Mm4r9DfKVn0

Parapluies connectés

Haltères connectées

Armes à feu connectées

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

- Contactez-nous

Des infos oubliées ? Des fautes ?

- Contactez-nous (vraiment, n’hésitez pas)