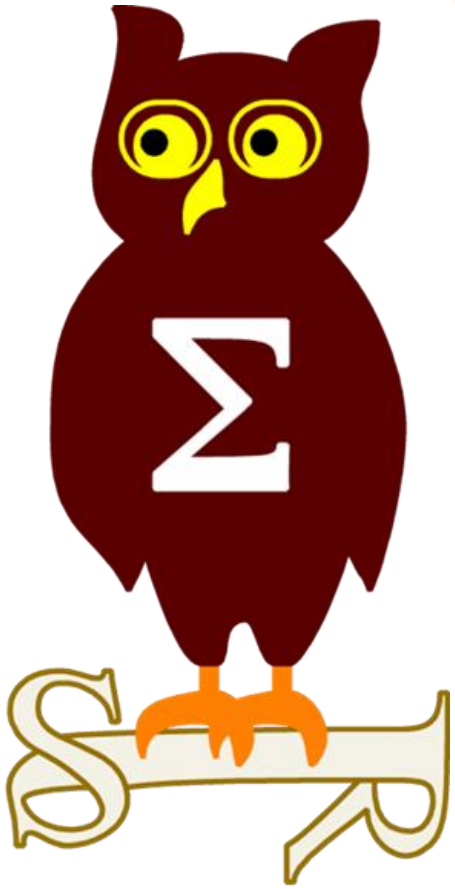
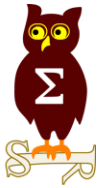


Revue d'actualité

08/11/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-118 Vulnérabilités dans Internet Explorer (11 CVE) [Exploitabilité 1,1,1,1,1,1,1,1,1,1,3]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 6 x Corruptions de mémoire aboutissant à une exécution de code
  - 3 x Contournements ASLR (fuite d'information)
  - 2 x Élévations de privilèges, dont codes d'exploitation publics disponible
    CVE-2016-3388 https://www.exploit-db.com/exploits/40606/
    CVE-2016-3387 https://www.exploit-db.com/exploits/40607/
- Crédits:
  - 0011 par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3383)
  - 62600BCA031B9EB5CB4A74ADDDD6771E par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3384)
  - Anonymous par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3382)
  - Jaehun Jeong (n3sk), de WINS, WSEC Analysis Team par VERISIGN iDefense (CVE-2016-3385)
  - James Forshaw de Google Project Zero (CVE-2016-3387, CVE-2016-3388)
  - Stefaan Truijen par NVISOAdrian Toma par NVISO (internship) Daan Raman par NVISOArne Swinnen par NVISO (CVE-2016-3391)
  - Wenxiang Qian de Tencent QQBrowser (CVE-2016-3267)
  - Will Metcalf et Kafeine de Proofpoint (CVE-2016-3298)
  - Zheng Huang de Baidu Security Lab (CVE-2016-3331)

MS16-119 Vulnérabilités dans Edge (13 CVE) [Exploitabilité 1,1,1,1,1,1,1,1,3,3,2,1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - 8 x Corruptions de mémoire aboutissant à une exécution de code
    https://bugs.chromium.org/p/project-zero/issues/detail?id=923
    https://bugs.chromium.org/p/project-zero/issues/detail?id=920
  - 2 x Contournements ASLR (fuite d'information)
  - 2 x Élévations de privilèges
  - 1 x Contournement du filtre anti-XSS
- Crédits:
  - Anonymous par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3382)
  - James Forshaw de Google Project Zero (CVE-2016-3387, CVE-2016-3388)
  - Microsoft ChakraCore Team (CVE-2016-3389, CVE-2016-3390)
  - Natalie Silvanovich de Google Project Zero (CVE-2016-3386, CVE-2016-7189, CVE-2016-7190, CVE-2016-7194)
  - Richard Zhu (fluorescence) par Trend Micro's Zero Day Initiative (ZDI) (CVE-2016-3386)
  - Stefaan Truijen par NVISOAdrian Toma par NVISO (internship)Daan Raman par NVISOArne Swinnen par NVISO (CVE-2016-3391)
  - Wenxiang Qian de Tencent QQBrowser (CVE-2016-3267)
  - Xiaoyin Liu (CVE-2016-3392)
  - Zheng Huang de Baidu Security Lab (CVE-2016-3331)

Dont 6 communes avec IE:

- CVE-2016-3267
- CVE-2016-3331
- CVE-2016-3382
- CVE-2016-3387
- CVE-2016-3390
- CVE-2016-3391

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-120 Vulnérabilités dans GDI+ (7 CVE) [Exploitabilité 2,2,4,1,1,1,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Office 2007, 2010, Skype 2016, Lync 2010 et 2013
- Exploit:
    - 2 x Élévations de privilèges, dont une utilisée lors d'une attaque ciblée "FruityArmor" CVE-2016-3393 https://securelist.com/blog/research/76396/windows-zero-day-exploit-used-in-targeted-attacks-by-fruityarmor-apt/
  - 3 x Contournements ASLR (fuite d'information)
  - 2 x Corruptions de mémoire aboutissant à une exécution de code
    - Code d'exploitation public disponible CVE-2016-7182 https://www.exploit-db.com/exploits/40599/
- Crédits:
  - Anton Ivanov de Kaspersky Lab (CVE-2016-3393)
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-7182)
  - pgboy, zhong_sf de Qihoo 360 Vulcan Team (CVE-2016-3270)

MS16-121 Vulnérabilités dans Office (1 CVE) [Exploitabilité 1]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier RTF
    - Exploitée dans la nature
- Crédits:
  - Austrian MilCERT (CVE-2016-7193)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-122 Vulnérabilité dans le contrôleur vidéo (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-104, MS16-111, KB3175024, KB3185319, KB3185611, KB3185614, KB3189866
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à l'ouverture depuis un document ou une page web
- Crédits:
  - ?

MS16-123 Vulnérabilités noyau Win32k (6 CVE) [Exploitabilité 1,1,2,2,2,1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-016, MS16-098, MS16-104, MS16-111, KB3124280, KB3175024, KB3177725, KB3185319, KB3185611, KB3185614, KB3189866
- Exploit:
  - 6 x Élévations de privilèges
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-7185)
  - Mateusz Jurczyk de Google Project ZeroJames Forshaw de Google Project Zero (CVE-2016-3376)
  - Peter Hlavaty (@zer0mem), KeenLab, Tencent (CVE-2016-3341)
  - fanxiaocao (@TinySec), et pjf de IceSword Lab, Qihoo 360 (CVE-2016-7211)
  - pgboy, zhong_sf de Qihoo 360 Vulcan Team (CVE-2016-3266)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-124 Vulnérabilités dans la base de registre (4 CVE) [Exploitabilité 2,2,2,2]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-098, MS16-104, MS16-104, MS16-111, MS16-111, KB3175024, KB3175024, KB3177725, KB3185319, KB3185319, KB3185611, KB3185614, KB3189866
- Exploit:
  - 4 x Élévations de privilèges en chargeant des clefs de base de registre
    - Avec des valeurs négatives CVE-2016-0070 https://www.exploit-db.com/exploits/40600/
    - En lecture, basculant en écriture CVE-2016-0079 https://www.exploit-db.com/exploits/40608/
    - Par impersonification CVE-2016-0073 https://www.exploit-db.com/exploits/40574/
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-0073, CVE-2016-0075, CVE-2016-0079, CVE-2016-0070)

MS16-125 Vulnérabilité dans le service de collecte d'événements (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 10
  - Remplace KB3185611, KB3185614, KB3189866
- Exploit:
  - Élévation de privilège locale à partir de "Diagnostics Hub Standard Collector Service" (collecte en temps réel des évènements "Event Tracing" et traitement)
    - Code d'exploitation https://www.exploit-db.com/exploits/40562/
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-7188)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-126 Vulnérabilité dans l'API Microsoft Internet Messaging (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-111, KB3175024
- Exploit:
  - Contournement d'ASLR (fuite d'information)
- Crédits:
  - Will Metcalf et Kafeine de Proofpoint (CVE-2016-3298)

MS16-127 Vulnérabilités dans Adobe Flash Player (12 CVE) [Exploitabilité 1,1,1,1,1,1,1,1,1,1,1,1]

- Affecte:
  - Windows (toutes versions supportées)
  - Remplace MS16-117, KB3188128
- Exploit:
  - Exécutions de code
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

- Publication Hors-bande -

MS16-128 Vulnérabilité dans Adobe Flash Player (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Exécutions de code à l'ouverture d'une page web contenant un Flash

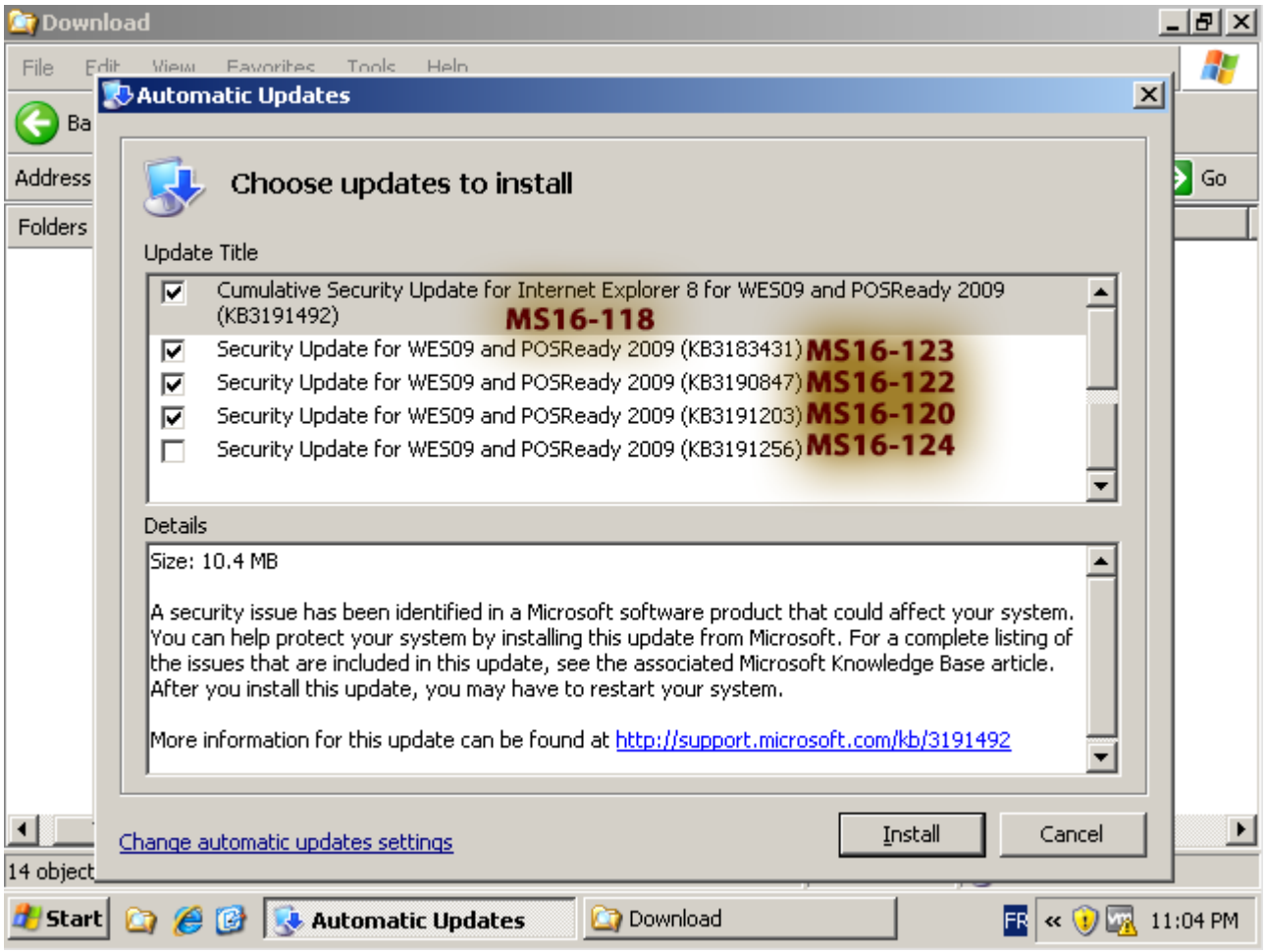
    https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html
- Crédits:
  - Non crédité, situation tendue entre Google et Microsoft, cf. ci-après (CVE-2016-7855)

Failles / Bulletins / Advisories

Microsoft - Avis

Mise à jour pour Windows XP Embedded POSReady

- Windows XP Embedded Service Pack 3 (SP3) fin de support en **janvier 2016**
- Windows Embedded POSReady 2009 fin de support en **avril 2019**



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions

Aucune publication ce mois-ci

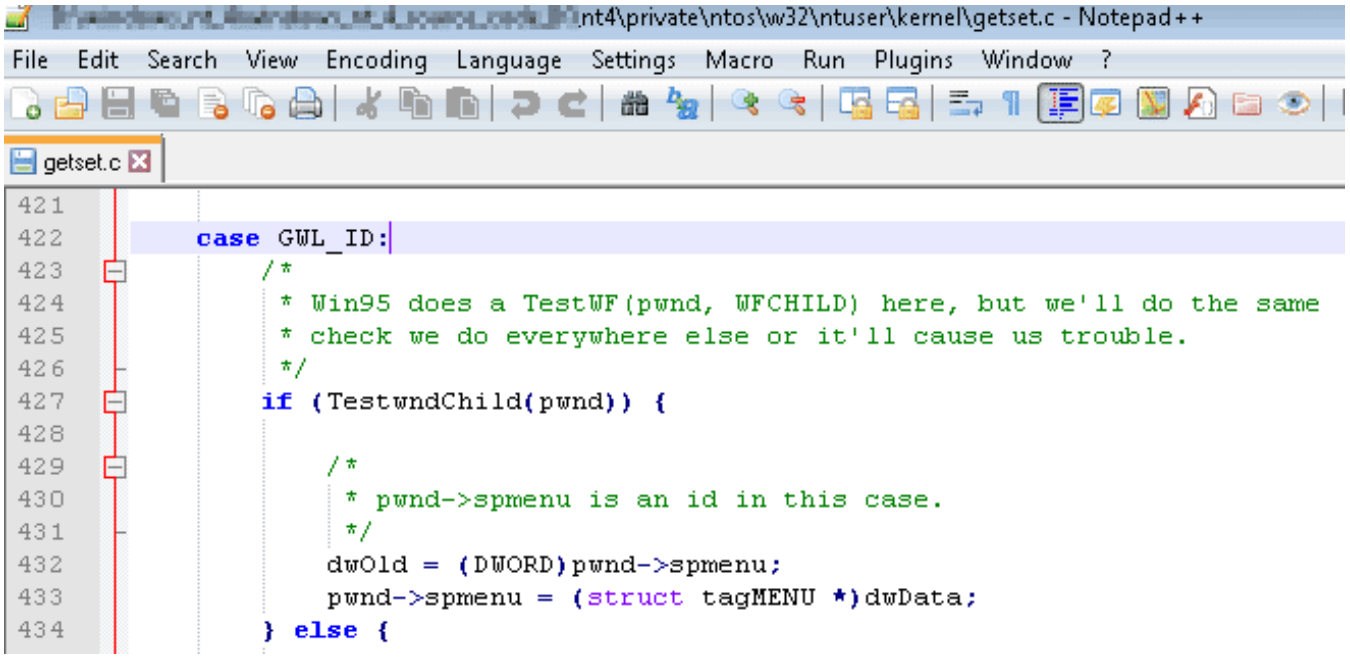
- Vx.x

Failles / Bulletins / Advisories

Microsoft - Autre

Vulnérabilité publiée par Google Project Zero et activement exploitée (CVE-2016-7855)

- Elévation de Privilège locale et évasion de la Sandbox du navigateur
  - Exploité en combinaison avec une vulnérabilité Flash
- Critique + pas de correction de Microsoft en 7 jours + bloqué dans Chrome = Google publie
  - C'est rude !
- Résultat : la vulnérabilité est massivement exploitée dans la nature
  https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html
- La vulnérabilité date de Windows NT4 et semble liée à la publication du code source
  https://twitter.com/aionescu/status/793663980191358981
- Variable nommée "pwnd" 😱



Failles / Bulletins / Advisories

Microsoft - Autre

Atom bombing, nouvelle technique d'injection de code

- Il ne s'agit pas en soi d'une vulnérabilité, mais de l'exploitation d'une fonctionnalité
- Permet de dissimuler du code malveillant au sein d'un programme légitime
- Exploitation des tables "atom" ainsi que APC : *Async Procedure Calls*
- Pas de correctif prévu

http://blog.ensilo.com/atombombing-a-code-injection-that-bypasses-current-security-solutions
https://breakingmalware.com/injection-techniques/atombombing-brand-new-code-injection-for-windows/

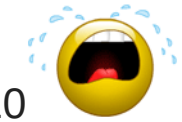
Sécuriser ses postes de travail Windows & contrôleurs de domaine

- Conseils de base

https://adsecurity.org/?p=3299 / https://adsecurity.org/?p=3377

La fin d'EMET

- Fin de vie du projet le 31/07/2018
- Solution ? Migrer vers Windows 10



https://blogs.technet.microsoft.com/srd/2016/11/03/beyond-emet/

Nouvelles mitigations anti-exploits dans Windows 10

https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf

Failles / Bulletins / Advisories

Système (principales failles)

NVidia

- Déni de service et exécution potentielle de code
- La carte graphique, un bon vecteur d'attaque pour contourner Credential Guard

  https://www.exploit-db.com/exploits/40661/ à 40668

Joomla

- Création d'un utilisateur sans authentification (CVE-2016-8870) et élévation de privilège (CVE-2016-8869)
- Vulnérabilités activement exploitées dans la nature

  https://blog.sucuri.net/2016/10/joomla-mass-exploits-privilege-vulnerability.html

DirtyCow : la vache qui broot Linux et Android

- Elévation de privilège sous Linux datant de 2007

  https://dirtycow.ninja/
- Activement exploité dans la nature du fait de la publication de codes sources

  https://github.com/rapid7/metasploit-framework/pull/7478/files

  https://github.com/dirtycow/dirtycow.github.io/blob/master/dirtyc0w.c

  https://nakedsecurity.sophos.com/2016/10/25/dirtycow-linux-hole-works-on-android-too-root-at-will/

  https://gist.github.com/Arinerron/0e99d69d70a778ca13a0087fa6fdfd80

Failles / Bulletins / Advisories

Système (principales failles)

Exécution de code sur la solution de SSO Atlassian Crowd

- Exécution de code en insérant un objet Java dans un champ d'une requête LDAP

  https://confluence.atlassian.com/crowd/crowd-security-advisory-2016-10-19-856697283.html

MySQL / MariaDB / PerconaDB : Élévations de privilèges locales

- Race condition lors de la réparation d'une table
- Race condition lors du redémarrage du service MySQL

  http://legalhackers.com/advisories/MySQL-Maria-Percona-PrivEscRace-CVE-2016-6663-5616-Exploit.html

  https://legalhackers.com/advisories/MySQL-Maria-Percona-RootPrivEsc-CVE-2016-6664-5617-Exploit.html

Arrêtez de regarder des images

- LibTIFF, exécution de code lors du traitement d'une image **TIFF**

  http://blogs.cisco.com/security/talos/libtiff-code-execution

- CoreGraphics Apple iOS / Mac OSX, exécution de code lors du traitement d'une image **Jpeg**

  https://nakedsecurity.sophos.com/2016/10/25/apple-ios-users-taste-android-anxiety-with-nasty-coregraphics-image-flaw/amp/

Failles / Bulletins / Advisories

Système (principales failles)

Vulnérabilités dans curl

- Découvertes lors d'un audit par Cure53

  https://curl.haxx.se/docs/security.html

Lynx : Vulnérabilité dans le traitement des URL

- `http://google.com?@hackdog.me/` renvoie vers `hackdog.me`

  http://seclists.org/oss-sec/2016/q4/328

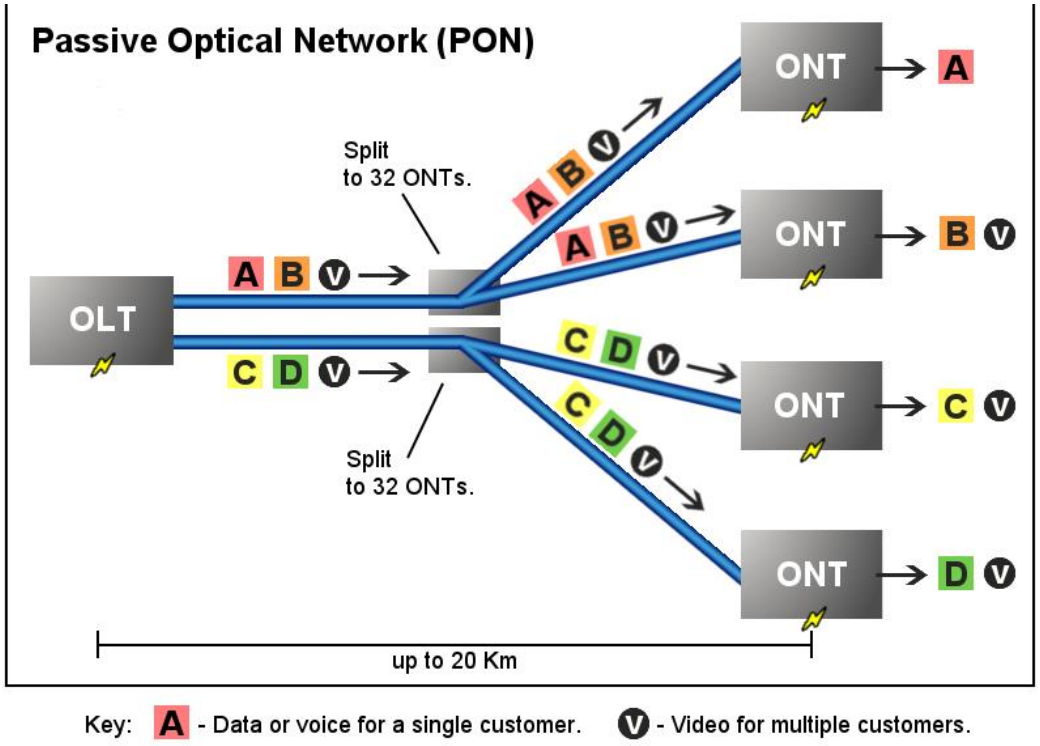
Failles / Bulletins / Advisories

Réseau (principales failles)

Vulnérabilités dans les réseaux FTTH GPON (Gigabit Passive Optical Network)

- Exécution de code à distance, comptes cachés dans les ONT (Optical Network Terminal)
  - Clef SSH commune à tous les boîtiers

https://pierrekim.github.io/blog/2016-11-01-gpon-ftth-networks-insecurity.html



Failles / Bulletins / Advisories

Réseau (principales failles)

Appliance de sécurité Mail SonicWall: Vulnérabilités sur le portail d'administration

- Contournement de l'accès à certaines parties de l'administration, dont les backups
- Téléchargement arbitraire de fichier si accès authentifié
- Exécution de code

https://www.digitaldefense.com/zero-day-alert-vulnerabilities-email-platform/

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Des défauts dans l'implémentation SSL permettent d'utiliser des appareils iOS dans une attaque DDoS

- Accès aux URLs OCSP lors d'une consultation HTTPS
- DDoS par réflexion en créant une liste d'URLs OCSP

http://www.scmagazineuk.com/ssl-handshake-weakness-leaves-macos-ios-devices-open-to-mitm-attacks/article/568353/

Exploitation de la fonction "Hover" d'Android pour du keylogging

https://arxiv.org/abs/1611.01477

Failles / Bulletins / Advisories

Divers

Plusieurs claviers/télécommandes sans fil vulnérables

http://seclists.org/fulldisclosure/2016/Oct/45

http://seclists.org/fulldisclosure/2016/Oct/41

http://seclists.org/fulldisclosure/2016/Oct/60

http://seclists.org/fulldisclosure/2016/Oct/61

Vulnérabilités dans les machines à voter électroniques aux Etats-Unis

- L'accès physique permet de flasher le firmware et de modifier les comptes

  https://blog.cylance.com/cylance-discloses-voting-machine-vulnerability

Casser le chiffrement A5/1 avec 3 cartes graphiques NVIDIA GeForce GTX690

- Cassé en temps réel
  - Et encore très utilisé

    http://gsmmap.org/assets/pdfs/gsmmap.org-country_report-France-2015-02.pdf

http://securityaffairs.co/wordpress/52666/hacking/gsm-crypto-hacking.html

2015	Networks		
	Bouygues	Orange	SFR
A5/0	1%	1%	0%
A5/1	**99%**	**99%**	**53%**
A5/3	0%	0%	47%

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Open Redirect, une faille à ne pas sous-estimer

- Exploitation de deux failles de ce type pour exploiter un XSS chez Google

  https://sites.google.com/site/bughunteruniversity/best-reports/openredirectsthatmatter

Déverrouiller et prendre le contrôle d'un iPhone 6 avec iOS 10

- Grâce à Whatsapp et la réinitialisation de compte par SMS

  http://securityaffairs.co/wordpress/52432/hacking/unlocked-stolen-iphone-6s.html

Contournement de l'authentification forte par double facteur

- **Office365**, car le service web "Exchange Web Services" peut être accédé avec un simple mot de passe

  http://www.blackhillsinfosec.com/?p=5396

- **Paypal**, la question de sécurité est en partie contrôlée localement

  https://henryhoggard.co.uk/blog/Paypal-2FA-Bypass

Contourner ASLR, grâce au prédiction de branchement

- Marche aussi pour Kernel-ASLR
- « Timing attack » sur des collisions entre les prédictions de branchement

  http://www.cs.ucr.edu/~nael/pubs/micro16.pdf

Contourner Kernel-ASLR sous Windows grâce au "paging" et "self-ref entry"

- Sorte de liste chaînée des pages mémoires

  https://blog.coresecurity.com/2016/06/21/getting-physical-extreme-abuse-of-intel-based-paging-systems-part-2-windows/

Auto-exécution de Macro Office avec “InkPicture1_Painted()”

- Change un peu des classiques AutoOpen(), WorkbookOpen() et AutoClose()
- Fonctionne également avec PowerPoint

  http://blog.joesecurity.org/2016/09/will-it-blend-this-is-question-new.html
- Supporté par OleTools 0.5

  https://www.decalage.info/python/oletools

RowHammer, encore et toujours

- Entre deux machines virtuelles

  https://www.blackhat.com/eu-16/briefings/schedule/#flip-feng-shui-rowhammering-the-vms-isolation-4878

- Sur Android (Drammer)
  - Fonctionne sur Nexus 4, 5, LG G4, Samsung Galaxy S4, S5… et permet de devenir Root

  http://arstechnica.com/security/2016/10/using-rowhammer-bitflips-to-root-android-phones-is-now-a-thing/

  https://www.vusec.net/projects/drammer/

Piratages, Malwares, spam, fraudes et DDoS
DDoS

Vers/Malware Mirai, la suite

- DDoS sur le service de DNS managé Dyn
  - Impactant Twitter, Spotify, Github, Paypal, Netflix, Playstation Network...
  - Conclusion (débile) : Internet est tombé
- Quelques informations de la part de Dyn

  http://hub.dyn.com/static/hub.dyn.com/dyn-blog/dyn-statement-on-10-21-2016-ddos-attack.html

  http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
- Mirai contient un dépassement de tampon de la pile, en cas d'attaque HTTP
  - Lors du traitement de l'entête "Location:" des réponses
  - Y'aura-t-il un code CVE ? 😆

    https://www.invincealabs.com/blog/2016/10/killing-mirai/
- Le constructeur Xiongmai rappelle ses caméras vulnérables

  https://www.theguardian.com/technology/2016/oct/24/chinese-webcam-maker-recalls-devices-cyberattack-ddos-internet-of-things-xiongmai
- 20 minutes tente un article et fait une erreur par ligne

  http://www.20minutes.fr/high-tech/1947575-20161022-comment-armee-objets-connectes-infectes-casse-internet

Le Libéria fortement touché par un DDoS Mirai

- Non, le pays n'a pas été coupé d'Internet
- Attaques ciblées sur les opérateurs de télécom locaux

  http://allafrica.com/stories/201510300843.html

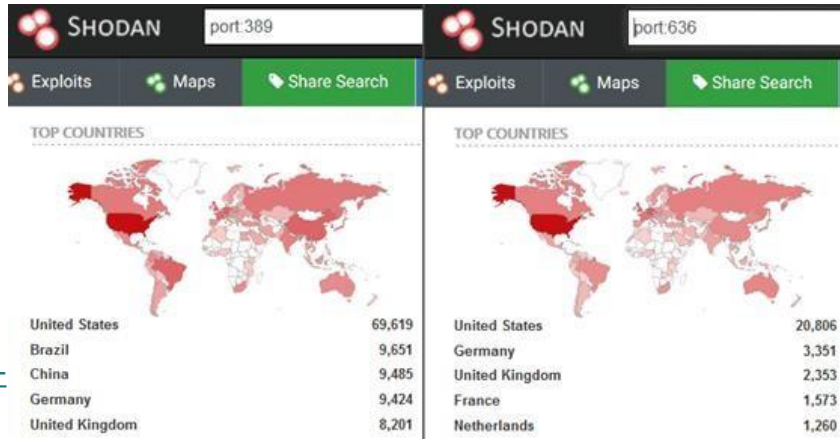
Piratages, Malwares, spam, fraudes et DDoS

DDoS

DDoS par réflexion Connectionless LDAP (CLDAP)

- En écoute sur les ports :
  - UDP 389 (clair)
  - UDP 636 (chiffré sur SSL/TLS)
- Effet de levier allant de x46 à x55

https://www.corero.com/company/newsroom/press-releases/corero-warns-of-powerful-new-ddos-attack-vector-with-potential-for-terabit-scale-ddos-events/



Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

La banque anglaise Tesco Bank suspend tous les paiements en ligne de ses clients

- 40 000 comptes piratés sur 136 000
- 20 000 se sont fait dérober de l'argent

http://securityaffairs.co/wordpress/53167/cyber-crime/tesco-bank-cyber-heist.html

La banque indienne SBI bloque 600 000 CB, sans prévenir

- A cause d'un malware sur les ATM/DAB de la Yes Bank
- Mais cela ne représente que 0,24% de ses cartes émises

http://news.softpedia.com/news/indian-bank-blocks-600-000-debit-cards-after-atm-malware-incident-509458.shtml

Magento, grosse campagne de piratages de sites d'e-commerce

- Vol des numéros de CB et CVV, enregistrés dans une image

http://gwillem.gitlab.io/2016/10/14/github-censored-research-data/

https://blog.sucuri.net/2016/10/magento-credit-card-swiper-exports-image.html

- Liste de 4 000 sites piratés
  - Dont des sites français

https://gitlab.com/gwillem/public-snippets/snippets/28813

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Cellebrite, outils d'extraction de données en libre téléchargement

- Société israélienne appartenant au groupe japonais Sun Corp
  - Spécialisée dans l'extraction de données de smartphone
- Téléchargement depuis le site d'un revendeur
  - Et en cache un peu partout…

http://motherboard.vice.com/read/the-phone-hackers-at-cellebrite-have-had-their-firmware-leaked-online

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Vendor	Model	Phonebook	Call Logs	Calendar	SMS	MMS	iMessages	Email	Browser	User	ESN/IMEI	Pictures	Videos	Ringtones	Audio/Music	Apps Data	Screen	Autodetect
305	Apple	iPhone 7 (A1660)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
306	Apple	iPhone 7 (A1778)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
307	Apple	iPhone 7 (A1779)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
308	Apple	iPhone 7 (A1780)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
309	Apple	iPhone 7 Plus (A1661)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
310	Apple	iPhone 7 Plus (A1784)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
311	Apple	iPhone 7 Plus (A1785)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y
312	Apple	iPhone 7 Plus (A1786)	Y	Y	Y	Y	Y	Y	Y-Only_Jailbroken	Y		Y	Y	Y	Y	Y	Y	Y	Y

NSA: Equation Group, suite des publications de Shadow Broker

- Quelques configuration d'outils non publiés et des IP de potentielles cibles compromises
- Mais datant de 9 ans

https://www.myhackerhouse.com/hacker-halloween-inside-shadow-brokers-leak/

Le pirate de Linkedin en 2012 arrêté

- C'est un jeune Russe de 29 ans dont l'arrestation a été filmée

http://thehackernews.com/2016/10/linkedin-russian-hacker-arrested.html

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Piratages de centrales électriques Russes par les américains

- La Russie attend des explications officielles

  https://www.rt.com/news/365423-russia-us-hacker-grid/

- Est-ce la contre-attaque annoncée par le vice-président américain ?

  http://hightech.bfmtv.com/securite/les-etats-unis-prepareraient-une-cyberattaque-sans-precedent-contre-la-russie-1048572.html

  - Attaque en représailles des piratages durant les élections US ?
  - Le groupe responsable des attaques (APT28) aurait utilisé 6 0-days au cours de l'année

    http://www.theregister.co.uk/2016/10/20/alleged_dnc_hackers_six_zerodays/

NSA, un ancien sous-traitant aurait volé 50 To de données en 20 ans

- Mais également des armes et de l'équipement

  https://amp.nextinpact.com/news/101854-nsa-ancien-sous-traitant-aurait-derobe-50-to-donnees-sensibles-sur-20-ans.htm

- La sécurité physique était catastrophique

  http://electrospaces.blogspot.fr/2016/10/with-nsa-contractor-martin-arrested.html

Celebgate, suite et fin

- Ryan COLLINS (36 ans) plaide coupable et prend 18 mois de prison ferme au lieu de 5 ans

  https://www.justice.gov/usao-mdpa/pr/lancaster-county-man-sentenced-18-months-federal-prison-hacking-apple-and-google-e-mail

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Rançongiciel !XPTLOCK5.0

- Les clefs ont été publiées

  https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg

Piratages, Malwares, spam, fraudes et DDoS

SCADA

Une vulnérabilité critique dans les systèmes SCADA de Schneider

- Une vulnérabilité critique a été identifiée dans le logiciel Unity Pro, qui permet de programmer les automates (PLC) Schneider
- La fonction de « simulateur d'automate » est vulnérable et l'exploitation peut se faire depuis le réseau.

https://threatpost.com/major-vulnerability-found-in-schneider-electric-unity-pro/121550/

Déni de service sur les IHM Schneider

- Un super nom : #panelshock
- La vidéo : https://youtu.be/Ehzs0mlMtbc

http://www.critifence.com/blog/panel_shock/

https://ics-cert.us-cert.gov/advisories/ICSA-16-308-02

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Orange: Redirection des internautes vers une page du ministère de l'Intérieur

- Concernant les domaines Google.fr, Wikipedia.fr, Ovh

```
# dig A +short google.fr
90.85.16.52
```

Serveur Orange hébergeant la page https://www.shodan.io/host/90.85.16.52

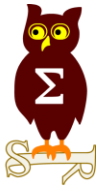
- Page dédiée aux visites de site terroriste
- "Erreur humaine" sur la liste noire des sites bloqués/censurés
- Qui ose encore parler de neutralité du net ?

http://www.nextinpact.com/news/101785-blocage-google-ovh-et-wikipedia-on-ne-cherche-pas-a-vous-cacher-verite-assure-orange.htm

Orange se prépare à l'espionnage/surveillance en masse (Deep Packet Inspection / DPI)

- Achat de cartes d'interception et d'analyse Medusa, du constructeur néo-zelandais : Endace
  - Ils auraient au moins pu acheter Français !
- Quelques autres clients : GCHQ, Israël, Inde, Maroc, USA, Australie, Espagne...

https://theintercept.com/2016/10/23/endace-mass-surveillance-gchq-governments/



Nouveautés, outils et techniques

Crypto
Divers

VeraCrypt, le rapport d'audit a été publié

- Rien de grave et la crypto tient bon :
  - **8** vulnérabilités **critiques,** surtout des élévations de privilège
  - **3** vulnérabilités **modérées**
  - **15** vulnérabilités **faibles**

https://ostif.org/the-veracrypt-audit-results/

Un IMSI catcher déguisé en imprimante HP

http://boingboing.net/2016/11/03/a-fake-hp-printer-thats-actu.html

MSSQL : exécution de commandes sans xp_cmdshell

https://www.optiv.com/blog/mssql-agent-jobs-for-command-execution

Backslash-powered scanner

- Nouvelle extension pour Burp
- Ne se contente pas d'envoyer une liste de payloads prédéfinies
- Analyse automatisée basée sur le comportement, tente de répliquer une démarche humaine

http://blog.portswigger.net/2016/11/backslash-powered-scanning-hunting.html

https://github.com/PortSwigger/backslash-powered-scanner

Pentest
Techniques & outils

Pour le fun : un sniffer réseau dans Excel

- Rien de magique, lancement d'un script Powershell

  http://pastebin.com/FvnwHzHf

Rappel des différences entre audit / test d'intrusion / red team …

- En anglais

  https://danielmiessler.com/study/security-assessment-types

Identifier l'antivirus d'un poste client, par sa navigation

- Du fait de l'injection de Javascript par les antivirus

  https://vah13.github.io/AVDetection/

Pentest
Défense

Un honeypot multiple

- Intègre plusieurs pots de miels, permettant d'émuler de nombreux services : SCADA, SSH, SIP, MySQL, etc..

  http://dtag-dev-sec.github.io/mediator/feature/2016/10/31/t-pot-16.10.html

Building a successful internal Adversarial Simulation Team

- Purple Team expliqué par deux pentesters

  https://www.youtube.com/watch?v=Q5Fu6AvXi_A&feature=share

Détecter les scripts PowerShell obfusqués à partir des répétitions de caractères

- Sorte d'entropie

  http://www.leeholmes.com/blog/2016/10/22/more-detecting-obfuscated-powershell/

PowerShell Empire “Security is Hard” 😉

- Très bonne démarche de faire un retour sur les vulnérabilité
  - Possibilité de prédire la crypto et faire qu’un agent s’arrête de lui même
  - Écraser n’importe quel fichier sur le serveur de contrôle en cas de téléchargement, cf. revue d'octobre
  - “Directory traversal” à partir de l’ID d’un agent

http://www.harmj0y.net/blog/empire/empire-fails/

Nouveautés (logiciel, langage, protocole...)

Open Source

Les dépôts open source du gouvernement américain

- NASA, OPM, Energy, …
- Vous n'y trouverez pas les outils de la division TAO ;)

https://code.gov/

Après PowerShell sur Linux

http://linkis.com/www.howtogeek.com/26/2GMrx

- Voici PowerShell sur MacOSX

http://theithollow.com/2016/08/22/install-powershell-mac/

Business et Politique

Droit / Politique

France

La CNIL épingle sévèrement CDiscount

- Un sous-traitant de la vente à distance conservait en base et en clair:
  - Des données bancaires dont le CVV
  - Des commentaires déplacés sur les clients

http://www.lepoint.fr/high-tech-internet/les-pratiques-douteuses-de-cdiscount-sanctionnees-par-la-cnil-19-10-2016-2077167_47.php

La CNIL épingle le parti socialiste

- Accès aux données personnelles des adhérents malgré plusieurs alertes
- Débat sur la confidentialité de ses opinions politiques :
  - Pour la CNIL c'est confidentiel
  - Pour le PS c'est un acte militant et donc public -> mode "mauvaise foi" engagé

http://www.lemonde.fr/pixels/article/2016/10/27/donnees-personnelles-le-parti-socialiste-sanctionne-pour-de-graves-defauts-de-securite_5021668_4408996.html

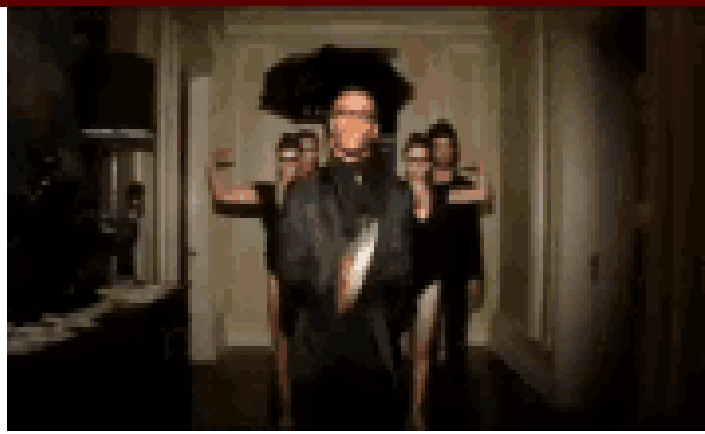
Droit / Politique

France

L'état utilisera le Cloud Orange pour 2 ans

- Ex-Cloudwatt, que l'état a financé à hauteur de 130M€

  http://www.orange-business.com/fr/presse/orange-remporte-le-contrat-de-la-premiere-plate-forme-cloud-public-de-l-etat-1



Il est possible de remonter des vulnérabilités à l'ANSSI

- La réponse reste très solennelle

  https://twitter.com/respssi/status/786648279241068545

Bonjour,

L'ANSSI vous remercie pour ces informations.

Nous allons procéder à des opérations techniques de vérification mais nous attirons votre attention sur les risques juridiques ou techniques qui peuvent être liés à la recherche de vulnérabilités.

- Le fait d'avoir découvert et signalé une vulnérabilité ne vous exonère pas complètement de votre responsabilité pénale. Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données (S.T.A.D.) demeure passible de sanctions pénales prévues aux articles 323-1 et suivants du Code pénal
- La recherche de vulnérabilités, même si elle n'est pas techniquement intrusive, peut potentiellement entraîner des effets secondaires et endommager un S.T.A.D.

[redacted]

Droit / Politique
International

L’europe pourrait revenir sur la localisation des données dans les pays

- Contrairement aux lois locales

https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/

La Chine légifère sur la sécurité informatique

- De loin, ça ressemble à notre LPM + CNIL : protection des infrastructures critiques, utilisation de matériel chinois, stockage en Chine des données personnelles

http://reuters.com/article/idUSKBN132049

Facebook, Google et Apple obligés de communiquer sur leurs intrusions

- Valable pour l'Irlande

http://www.thetimes.co.uk/article/facebook-ordered-to-report-cyberattacks-2rtch3nst

Yahoo dépose un brevet pour de la publicité ciblée, partout

https://iapp.org/news/a/eu-commission-aims-to-ban-forced-data-localization/

Profils techniques : comment attirer et conserver les talents ?

https://medium.com/center-for-strategic-and-international-studies/how-to-build-and-retain-a-talented-cybersecurity-team-378f7c920618#.eluzyodcw

Droit / Politique
International

Recherche sécurité aux États-Unis : le cadre législatif évolué

- La législation américaine évolue, notamment le Digital Millennium Copyright Act (“DMCA”). Il est désormais autorisé, à des fins de recherche sécurité, de contourner les mécanismes de protection de propriété intellectuelle. Cette exception s’applique uniquement aux équipements grand public (ordinateurs, objets connectés) ainsi que par exemple aux véhicules

  https://www.federalregister.gov/documents/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control

Les USA font pression sur l'Equateur pour couper la connexion internet de Julian Assange

- Ceci faisant suite à la publication des rémunérations d'Hillary Clinton pour 3 discours
- Accès coupé le dimanche 16 octobre

  http://www.nbcnews.com/news/us-news/u-s-urged-ecuador-act-against-assange-n669271

  http://www.telegraph.co.uk/news/2016/10/18/ecuador-cuts-julian-assanges-internet-access-after-hillary-clint/

USA, Angleterre : une réponse cyber-offensive aux cyber-attaques

http://www.reuters.com/article/us-usa-cyber-idUSKCN1061KT

http://securityaffairs.co/wordpress/52966/cyber-warfare-2/uk-active-defence.html

Droit / Politique
International

L'Angleterre espionne illégalement ses citoyens depuis 17 ans

- Jugement rendu par Investigatory Powers Tribunal

  http://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf

  http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf

Comment Google a caché ProtonMail dans les résultats de ses recherches

- Rendant le mail sécurisé invisible du quidam

  https://protonmail.com/blog/search-risk-google/

Reconnaissance faciale : 50% des américains “officiellement” fichés par la police

https://www.theguardian.com/world/2016/oct/18/police-facial-recognition-database-surveillance-profiling

- Les aéroports, Facebook, Dubaï, Palantir… le font également depuis longtemps

Conférences

Conférences

Passées

- Hack.lu : 18-20 octobre 2016
- BruCon : 27-28 octobre 2016
- 4SICS : 25-27 octobre à Stockholm
- BlackHat Europe : 1-4 novembre à Londres

A venir

- ZeroNights : 17-18 novembre à Moscou
- Botconf - 30 novembre au 2 décembre 2016 à Lyon
- 33C3 – 27-30 décembre 2016 à Hambourg
- FIC - 24-25 janvier 2017 à Lille

Divers / Trolls velus

Divers / Trolls velus

L’association Droit des lycéens demande le code source du portail Admission post-bac

- Et reçoit un PDF de 20 pages de procédures stockées PL/SQL en image
- Pas de structure de base, pas de doc…

http://rue89.nouvelobs.com/2016/10/18/voici-code-source-dapb-tenu-secret-jusqua-present-265443

Les français sont parmi les meilleurs développeurs au monde

- 1er: Chine, Russie, Pologne, Suisse, Hongrie, Japon, Taiwan, 8eme: France
- La France n°1 en C++
  - Mais pas les meilleurs en PL/SQL 

http://blog.hackerrank.com/which-country-would-win-in-the-programming-olympics/

Divers / Trolls velus

Contrefaçon de la JSSI de l'OSSIR ? 😉

- "JSSI / Journée Sécurité des Systèmes d'Informations" de l'INSA en novembre, depuis 2012
- Mais nous avons la précédence, notre JSSI datant de 2002 ✌🏾
  - Déposé à l'INPI
  - Et sans "s" à "information"

http://jssi.insa-rouen.fr/index.html

Analyse formelle de la cryptographie du protocole de Signal

- Conclusion : pas mal mais le générateur de nombres pseudo-aléatoires est prédictible

https://eprint.iacr.org/2016/1013.pdf

Des banques anglais font des réserves de Bitcoins pou😂yer les futurs rançongiciel

- Cela coûterait-il moins cher que de faire de la sécurité ?

http://www.01net.com/actualites/cyberattaques-les-banques-anglaises-font-des-reserves-de-bitcoin-1051247.html

Divers / Trolls velus

HSC by Deloitte, nouveau Logo ?

- Et nouveau secteur d'activité ?

  http://www.hossegor-surfclub.com/?lang=fr

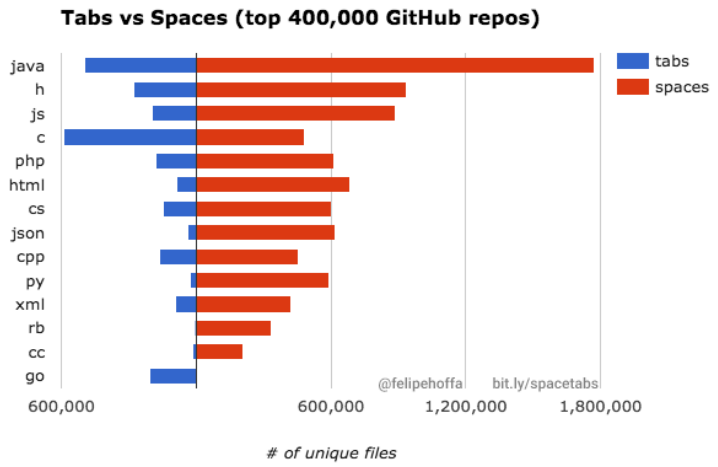
Espace, tabulations, points-virgules... Google a tranché !

- Tab vs Space

  https://twitter.com/thepracticaldev/status/737185546020126720

- Les espaces ont gagnés
  - Si on considère que la majorité a raison

  https://medium.com/@hoffa/400-000-github-repositories-1-billion-files-14-terabytes-of-code-spaces-or-tabs-7cfe0b5dd7fd#.8ahftovun



Une pile TCP/IP écrite en Go

https://github.com/google/netstack

Divers / Trolls velus

Quand IBM essaie de faire censurer la publication d'une vulnérabilité

- Exécution de code par désérialisation sur WebSphere

  http://seclists.org/fulldisclosure/2016/Oct/43

  https://twitter.com/SecLists/status/786611554573619201/photo/1

Hi,
Please remove section 2 and 5 which list the exploit details on
http://seclists.org/fulldisclosure/2016/Oct/43

IBM does not want to put customers at risk and so we do NOT like the
details of an exploit to come out since it puts all our customers at risk.

We would appreciate a quick response here...and removal of any type of
exploit details over the internet on this reported issue

Thanks

IBM Product Security Incident Response Team (PSIRT)
psirt@us.ibm.com | IBM PSIRT/Somers/IBM

Divers / Trolls velus

Tout savoir sur le JTAG

- Et pourquoi les constructeurs d'équipements connectés doivent y prêter attention

  http://blog.senr.io/blog/jtag-explained

Tout savoir sur WebRTC et sa sécurité

https://webrtc-security.github.io/

Etude des échanges entre Android et le Baseband

- Pour des exploitations OTA / Over-The-Air

  https://www.contextis.com/resources/blog/targeting-android-ota-exploitation/

Google Play sur Android, ce n'est plus de la géo-location mais du tracking acharné

https://www.grahamcluley.com/google-play-obsessed-tracking-android-users/

- Ce qui va dans le sens du livre "surveillance://"

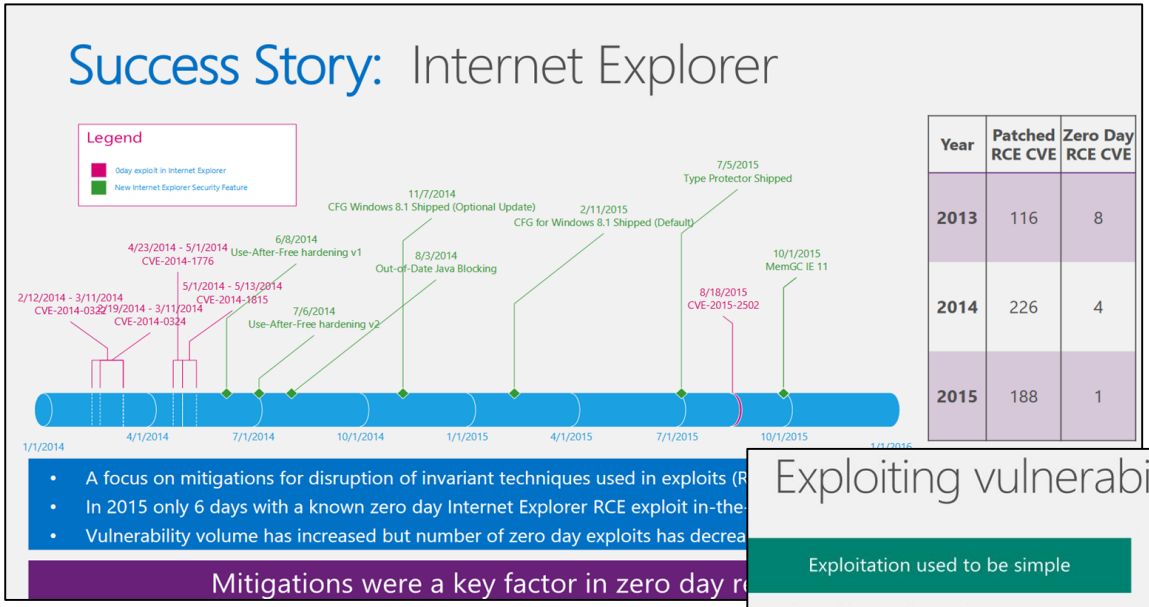
  http://www.bortzmeyer.org/surveillance.html

Divers / Trolls velus

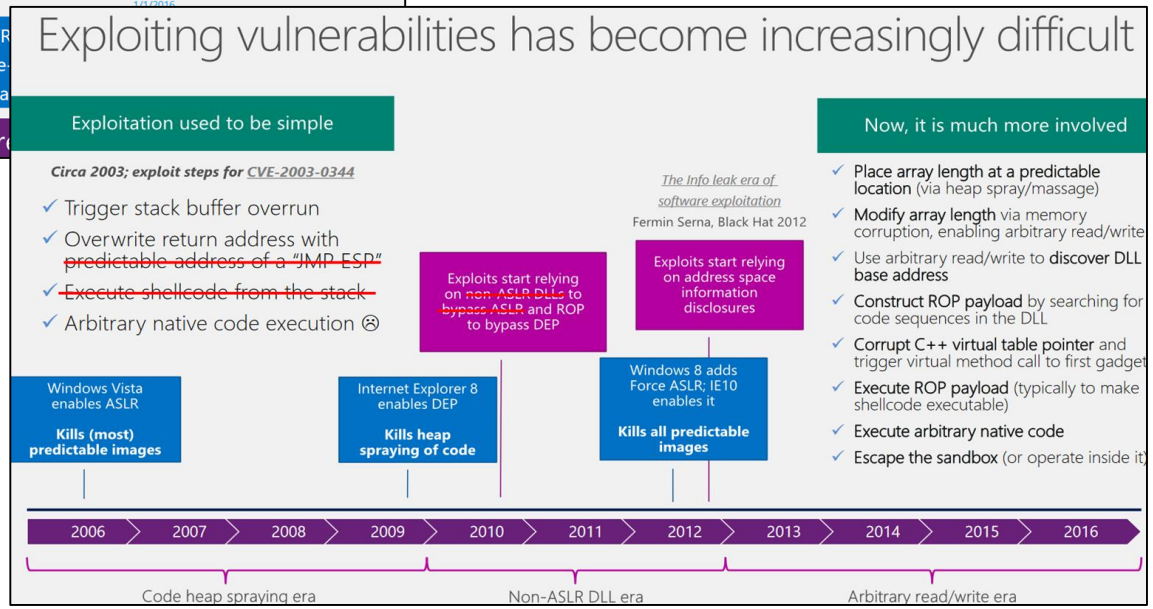
Présentation sur les sécurité de Windows 10 à la BlackHat

- Moitié trolls (sécurité IE = succès), moitié réelles avancées (2006 vs 2016)

https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf



Year	Patched RCE CVE	Zero Day RCE CVE
2013	116	8
2014	226	4
2015	188	1



Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 13 décembre 2016

After Work

- Mardi 31 janvier 2017

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous