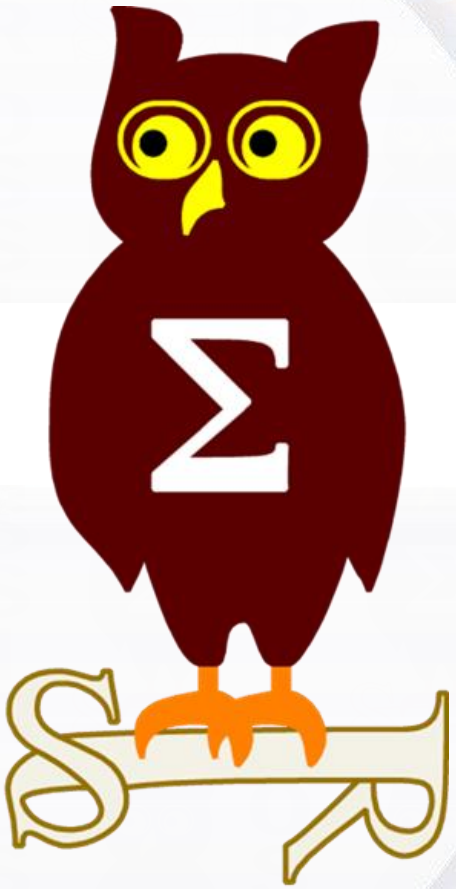


Revue d'actualité

12/05/2015

Préparée par

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

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

MS15-032 Vulnérabilités dans Internet Explorer (10 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportées)
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
  - Replace MS15-018
- Exploit:
  - 9 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement ASLR
- Crédits:
  - par ZDI
    - Omair (CVE-2015-1668)
    - ca0nguyen (CVE-2015-1667)
    - b0nd@garage4hackers@ (CVE-2015-1666)
    - AMol NAik & Garage4Hackers (CVE-2015-1665)
    - AbdulAziz Hariri (CVE-2015-1661)
    - Arthur Gerkis (CVE-2015-1660)
    - Jason Kratzer (CVE-2015-1659)
    - 0016EECD9D7159A949DAD3BC17E0A939 (CVE-2015-1652)
  - Jihui Lu of KeenTeam (@K33nTeam) (CVE-2015-1657)

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

MS15-033 Vulnérabilité dans Office (5 CVE) [Exploitabilité 1]

- Affecte:
  - Microsoft Office 2007, 2010 2013
  - Office pour Mac, Word Viewer et Compatibility Pack SP3
  - SharePoint Server 2010 et 2013
  - Replace MS14-081 et MS15-022
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier spécialement formaté
  - Utilisé dans la nature et ciblant Word 2010
- Crédits:
  - Ben Hawkes de Google Project Zero (CVE-2015-1651)
  - Chris Parmer de Plotly
  - 3S Labs par ZDI (CVE-2015-1650)
  - Jack Tang de Trend Micro (CVE-2015-1649)
  - The Labs Team de iSIGHT Partners (CVE-2015-1641)
  - Rakesh Dharmavaram (CVE-2015-1639)

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

MS15-034 Vulnérabilité dans IIS (1 CVE) [Exploitabilité 1]

- Affecte:
  - IIS toutes versions supportées
- Exploit:
  - 2 x Integer overflow aboutissant à une exécution de code dans IIS
    - Range: bytes=0-18446744073709551615 (0xff...ff)-> Overflow lors du calcul de la longueur de l'intervalle "lenght=end - start + 1"
    - Range: bytes=284-18446744073709551615 (0xff...ff)-> Overflow lors du calcul de la fin de l'intervalle "end = start + length"
  - Article du SANS : https://isc.sans.edu/forums/diary/MS15034+HTTPsys+IIS+DoS+And+Possible+Remote+Code+Execution+PATCH+NOW/19583/
  - Détails supplémentaires : http://blog.trendmicro.com/trendlabs-security-intelligence/iis-at-risk-an-in-depth-look-into-cve-2015-1635/
  - Et en français : http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-018/index.html
- Crédits:
  - Citrix Security Response Team (CVE-2015-1635)

MS15-035 Vulnérabilité dans le moteur graphique Windows (gdi.dll) (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 7, Vista, Server 2003 and 2008.
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Exécutions de code à l'ouverture d'un fichier "Enhanced Metafile" (EMF) spécialement formaté
- Crédits:
  - Hossein Lotfi de Secunia Research (CVE-2015-1645)

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

MS15-036 Vulnérabilité dans Sharepoint (2 CVE) [Exploitabilité 2]

- Affecte:
  - SharePoint et Office WebApp tous deux en 2010 et 2013
- Exploit:
  - Élévation de privilèges (XSS) dans Sharepoint
- Crédits:
  - Renato Ettisberger de IOprotect GmbH (CVE-2015-0098)

MS15-037 Vulnérabilité dans le planificateur de tâches (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 7 et 2008 R2
  - Correctif... sans correctif ;-)
    - Le correctif cherche des taches planifiées invalides et les supprime
- Exploit:
  - Élévation de privilèges par la modification de taches planifiées invalide pour exécuter son propre code en tant que SYSTEM
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

MS15-038 Vulnérabilité Noyau (2 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportées)
- Exploit:
  - Elévation de privilège par la création de lien symbolique dans DosDevices et \??\LOG
  - Codes :
    - https://code.google.com/p/google-security-research/issues/detail?id=245
    - https://code.google.com/p/google-security-research/issues/detail?id=240
  - Le correctif désactive l'impersonification avec un nouvel attribut d'objet (0x800)
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2015-1644 et CVE-2015-1643)

MS15-039 Vulnérabilité dans MSXML (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista et 7, Windows 2003, 2008 et 2008 R2
  - Déjà corrigé sur Windows 8.x et 2012 
  - Correctif également pour Windows XP Embedded POSReady (cf. screenshot après)
- Exploit:
  - Contournement des "same origin policy" permettant d'accéder aux fichiers du disque dur
- Crédits:
  - Hormazd Billimoria, Xiaoran Wang, Sergey Gorbaty, Anton Rager et Jonathan Brossard de Salesforce.com (CVE-2015-1646)

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

MS15-040 Vulnérabilité ADFS (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows 2012 R2 et Core
- Exploit:
  - Usurpation d'identité lors de l'utilisation d'ADFS (Active Directory Federation Services, pour du SSO). Si l'utilisateur ne ferme pas son navigation à la clôture de session, un autre peut la reprendre avec les mêmes permissions.
- Crédits:
  - ?

MS15-041 Vulnérabilité dans .NET (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows Vista, 7 et 8.x
  - Windows 2003, 2008, 2008 R2, 2012 et 2012 R2
- Exploit:
  - Fuite d'information par la récupération d'une partie de la configuration du serveur ASP.NET (web.config) en cas d'activation des messages d'erreurs personnalisés
- Crédits:
  - ?

MS15-042 Déni de service sur Hyper-V (1 CVE) [Exploitabilité 2]

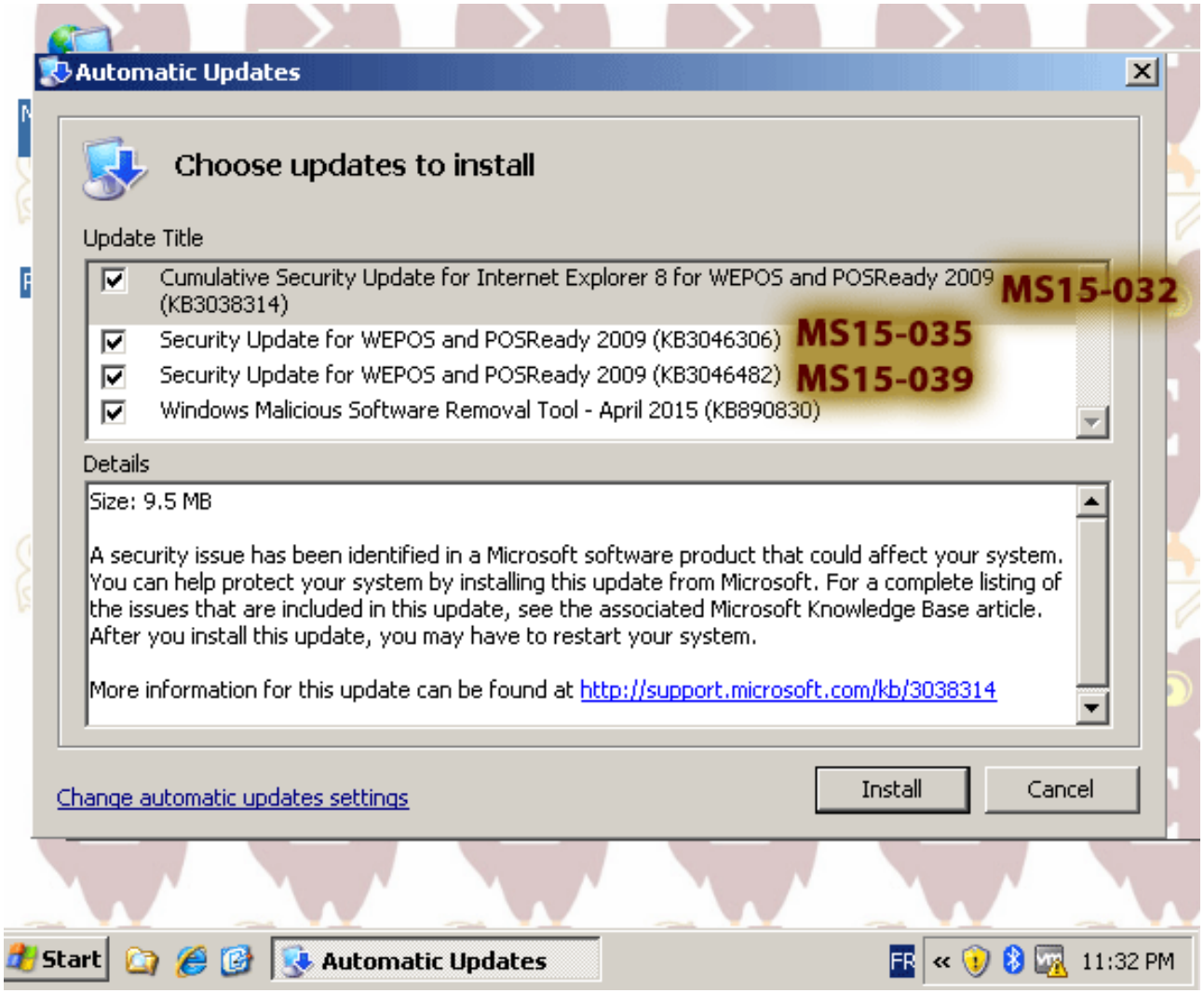
- Affecte:
  - Windows 8.1, 2012 R2 et Core
- Exploit:
  - Déni de service de l'hyperviseur depuis une machine virtuelle
- Crédits:
  - Dmitry Alikov de Veeam Software AG (CVE-2015-167)

Failles / Bulletins / Advisories

Microsoft - Avis Avril 2015

Mise à jour pour Windows XP Embedded POSReady

- Encore et toujours sans documenter dans les bulletins…



Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Avril 2015

3045755 Amélioration de l'authentification PKU2U

- V1.0 Plus d'authentification sur Live ID après un premier échec

3009008 Désactivation de SSLv3

- V3.0 Désactivation de SSLv3 dans IE11

2755801 Mise à jour de Flash Player

- V39.0 Nouvelle mise à jour de Flash Player

3062591 Local Administrator Password Solution (LAPS)

- V1.0 Gestion centralisé des comptes "administrateur local"
  - Mot de passe stocké dans un objet protégé de l'AD et associé au serveur
  - L'admin de domaine peut en donner l'accès à la demande, puis le changer
  - Mais nous y reviendrons...

0-Day de Google Zero

- Sortie de Sandbox sur Windows 8.1
  http://googleprojectzero.blogspot.fr/2015/05/in-console-able.html

Failles / Bulletins / Advisories

Microsoft - Autre

Windows 10

- Fin des fameux "patch tuesday" pour les entreprises
- Remplacé par Windows Update for Business (WUB)
  http://www.databreachtoday.com/windows-10-no-more-monthly-patches-a-8202

Support de SHA-1

- Microsoft fait machine arrière et les certificats émis avant le 01/01/2016 seront valide jusqu'au 14/01/2020
  https://technet.microsoft.com/en-us/library/security/3033929.aspx
- Le tableau qui résume tout :
  https://www.globalsign.com/en/blog/microsoft-announces-updates-sha-1-code-signing-policy/

Le “Bug Bounty” de Spartan est ouvert !

- Prix publics entre $500 et $15 000 pour une exécution de code
  - Est-ce suffisant ?
  - https://technet.microsoft.com/en-us/security/dn972323

Failles / Bulletins / Advisories

Système (principales failles)

OpenOffice

- Exécution de code à l'ouverture d'un fichier
  http://www.openoffice.org/security/cves/CVE-2015-1774.html

WordPress

- XSS (CVE-2015-1774)
  https://wordpress.org/news/2015/04/wordpress-4-2-1/
- Ayons peur : des millions de blogs vulnérables
  http://www.01net.com/editorial/653515/une-faille-dans-wordpress-rend-des-millions-de-blogs-vulnerables/

Claws, le client email de Tails, divulgue les emails en clair aux serveurs IMAP

- Les brouillons sont envoyés en clair au serveur….puis chiffrés avec OpenPGP lorsque l'email est envoyé ...
- !! Même problème avec Outlook + S/MIME si vous ne chiffrez pas par défaut !!
  https://tails.boum.org/security/claws_mail_leaks_plaintext_to_imap/

Vulnérabilité dans Pydio

- Pas de détail pour le moment, à priori une élévation de privilèges sur le système hôte pour un admin
  https://github.com/pydio/pydio-core/commit/2049254e7a215491019d2646a274a8fb1cf29e3b

Failles / Bulletins / Advisories

Système (principales failles)

XXE dans le module “services” de Drupal

- Contournement des restrictions
- Timeline intéressante
  http://www.synacktiv.fr/ressources/synacktiv_drupal_xxe_services.pdf

Attention au groupe “docker”

- Donne des privilèges root aux utilisateurs faisant partie de ce groupe
  https://fosterelli.co/privilege-escalation-via-docker.html

Magento

- Mise à 0 des prix des paniers sur 88 000 boutiques eBay (CVE-2015-1397, CVE-2015-1398, CVE-2015-1399)
  http://blog.checkpoint.com/2015/04/20/analyzing-magento-vulnerability/

Paypal

- Exécution de code à distance en exploitant Java Debug Wire Protocol... accessible sur le port 8000
  http://securityaffairs.co/wordpress/36394/hacking/paypal-remote-code-execution.html
  http://blog.ioactive.com/2014/04/hacking-java-debug-wire-protocol-or-how.html

Failles / Bulletins / Advisories

Système (principales failles)

HostAP daemon et wpa_supplicant

- Dénis de service
  - http://w1.fi/security/2015-2/wps-upnp-http-chunked-transfer-encoding.txt
  - http://w1.fi/security/2015-3/integer-underflow-in-ap-mode-wmm-action-frame.txt
  - http://w1.fi/security/2015-4/eap-pwd-missing-payload-length-validation.txt
  - Par Kostya Kortchinsky de Google Security Team
- Exécution de code
  - http://security.alibaba.com/blog/blog.htm?spm=0.0.0.0.p1ECc3&id=19
  - Par l'équipe sécurité d'Alibaba

Linux, élévation de privilège depuis chown()

- 0-day lors de la publication
  http://seclists.org/oss-sec/2015/q2/216

Failles / Bulletins / Advisories

Matériel

JavaCard YubiKey NEO

- Cartes NFC et USB, utilisées pour l'accès au bâtiment, SSH, PGP, Gmail, Facebook...
  https://www.yubico.com/2015/03/employees-day-showcases-yubikeys-flexibility/
- Réalisation d'opérations crypto sans entrer le PIN
- Possible extraction des clefs en cas d'utilisation d'OpenPGP 1.0.9 (CVE-2015-3298)
  https://developers.yubico.com/ykneo-openpgp/SecurityAdvisory%202015-04-14.html

Enceintes Wifi Bang & Olufsen A9

- Mot de passe stocké non chiffré… et accessible depuis une page sans authentification
- Récupérable avec un JavaScript malveillant utilisant WebRTC
  https://miki.it/blog/2015/4/20/the-power-of-dns-rebinding-stealing-wifi-passwords-with-a-website/

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco UCS / Unified Central Software

- Exécution de code à distance avant authentification (CVE-2015-0701)
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150506-ucsc

Juniper JunOS

- Exécution**s** de code à distance, dénis de service à distance...
  http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10672 à 680

Citrix Netscaler

- Déni de service à distance (CVE-2015-2829)
  http://support.citrix.com/article/CTX200861

BlueCoat ProxySG

- Récupération des Hash NTLM des autres utilisateurs par une simple requête HTTP 407
  http://www.securitytracker.com/id/1032149

Routeurs SOHO D-Link et Trendnet

- Exécution de code à distance
- Ne sera jamais corrigé
  http://arstechnica.com/security/2015/04/no-patch-for-remote-code-execution-bug-in-d-link-and-trendnet-routers/

Failles / Bulletins / Advisories

Apple

No iOS zone

- Hotspot Wifi exploitant une vulnérabilité SSL plantant les applications, voire le kernel
  https://www.rsaconference.com/writable/presentations/file_upload/mbs-t09--mobile-vulnerabilities-from-data-breach-to-complete-shutdown.pdf

Mac OS X

- Vulnérabilité Rootpipe, permettant de devenir root au redémarrage
- Apple semble ne pas réussir à corriger…
- Pas de correctif pour les versions < Yosemite
  http://www.computerworld.com/article/2912619/mac-os-x/apples-os-x-rootpipe-patch-flops-fails-to-fix-flaw.html

Failles / Bulletins / Advisories

Google

Google Password Alert

- Pour vous protéger des attaques par phishing
  http://googleblog.blogspot.com.es/2015/04/protect-your-google-account-with.html
- Possible à contourner en modifiant le DOM
  https://www.youtube.com/watch?v=HwEGYwCgqtk

Et Google tua l'URL

- http://wikipedia.org/wiki/Google => Wikipedia > Wiki > Google
  http://googlewebmastercentral.blogspot.fr/2015/04/better-presentation-of-urls-in-search.html

Failles / Bulletins / Advisories

Divers

Suricata 2.0.8

- Exploit:
  - Déni de service lors du décodage de SSL/TLS (Heap overflow)
    https://github.com/inliniac/suricata/commit/5f26824a4b3a4dbfe158db218067bed4aa4741b5
- Auteur:
  - Kostya Kortchinsky de the Google Security Team (CVE-2015-0971) 

Cross-Site WebSocket Hijacking

- Les websockets ne respectent pas la *Same-Origin Policy*
- Le serveur devrait vérifier l'en-tête "Origin"
  http://www.christian-schneider.net/CrossSiteWebSocketHijacking.html

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

L’hôtel Hard Rock Café de Vegas infecté par un POS

http://www.hotforsecurity.com/blog/hard-rocks-las-vegas-hotel-casino-hit-by-hackers-11768.html

Les hackeurs Russes ont pu lire les mails non classifiés d’Obama

www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html

- Mais comment son BlackBerry est-il sécurisé ?
  http://electrospaces.blogspot.fr/2013/04/how-obamas-blackberry-got-secured.html

Hacking de Firmware de Disque Dur

http://www.malwaretech.com/2015/04/hard-disk-firmware-hacking-part-1.html
http://www.malwaretech.com/2015/04/hard-disk-firmware-hacking-part-2.html
http://www.malwaretech.com/2015/04/hard-disk-firmware-hacking-part-3.html
http://www.malwaretech.com/2015/05/hard-disk-firmware-hacking-part-4.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Collision MD5 sur un binaire

- Intéressant mais peu utilise face à des IOC mixant MD5/Sha1/SSDeep…
  https://twitter.com/subTee/status/596751152051453953/photo/1
- Le code pour réaliser la collision
  http://natmchugh.blogspot.co.uk/2015/05/how-to-make-two-binaries-with-same-md5.html

Macro is back !

http://www.welivesecurity.com/2015/04/29/macro-malware-attacks-rise-says-microsoft/

- Bonne analyse de la chose : http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-017/index.html

Après le rootkit d'OS, celui des firmware de disques durs, voici celui des GPU

- Code fonctionnel en "user land"
- Peut rester persistant au reboot mais pas à l'arrêt complet
  https://github.com/x0r1/jellyfish
  http://arstechnica.com/security/2015/05/gpu-based-rootkit-and-keylogger-offer-superior-stealth-and-computing-power/

Analyse de Kraken, le malware utilisé contre les Etats Arabes Unis

https://blog.gdatasoftware.com/blog/article/dissecting-the-kraken.html

Piratages, Malwares, spam, fraudes et DDoS

Malwares

Rançongiciel : déchiffrer les fichiers chiffrés par TeslaCrypt

- Grâce à la clef de chiffrement laissée parfois sur le PC infecté
  http://blogs.cisco.com/security/talos/teslacrypt

Deux mois d'observation d'un HoneyPot ElasticSearch

http://jordan-wright.github.io/blog/2015/05/11/60-days-of-watching-hackers-attack-elasticsearch/

Analyse d'un exploit-pack pour Microsoft Word

http://blog.0x3a.com/post/117760824504/analysis-of-a-microsoft-word-intruder-sample

Un malware qui efface toute le disque s'il détecte une machine virtuelle

http://arstechnica.com/security/2015/05/super-secretive-malware-wipes-hard-drive-to-prevent-analysis/

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Les hôpitaux US vont sécuriser les appareils médicaux par analyse side-channel de la consommation électrique

- Faut-il rire ou pleurer ?
- Solution nommée (on ne rigole pas) “Wattsupdoc”
- “Même efficacité que les antivirus” ⇒ on est sauvés \o/
  http://securityaffairs.co/wordpress/36339/hacking/ac-power-malware-medical-devices.html

Nombreuses vulnérabilités dans les prises intelligentes G-Homa

http://seclists.org/fulldisclosure/2015/May/45

Piratages, Malwares, spam, fraudes et DDoS

Espionnage

Les routeurs de la NSA

- Les reliant à leurs partenaires ?
  http://electrospaces.blogspot.fr/2015/04/some-equipment-that-connects-nsa-with.html

Un outil pour détecter QUANTUM INSERT

- Basé sur les numéros de séquence TCP dupliqués
  http://blog.fox-it.com/2015/04/20/deep-dive-into-quantum-insert/

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Thales piraté

- Attaqué avec succès par les Russes
  http://www.lemondeinformatique.fr/actualites/lire-thales-pirate-comme-les-autres-60848.html

Hellsing vs Naikon, quand 2 groupes s'affrontent

- Pour le contrôle de bots/zombies
- Parfois, ils installent des antivirus pour tenter de supprimer le virus de l'autre
  http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/quand-les-hackers-attaquent-les-hackers-16-04-2015-1921751_506.php

RyanAir, vol de $5 millions durant un transfert avec la Chine

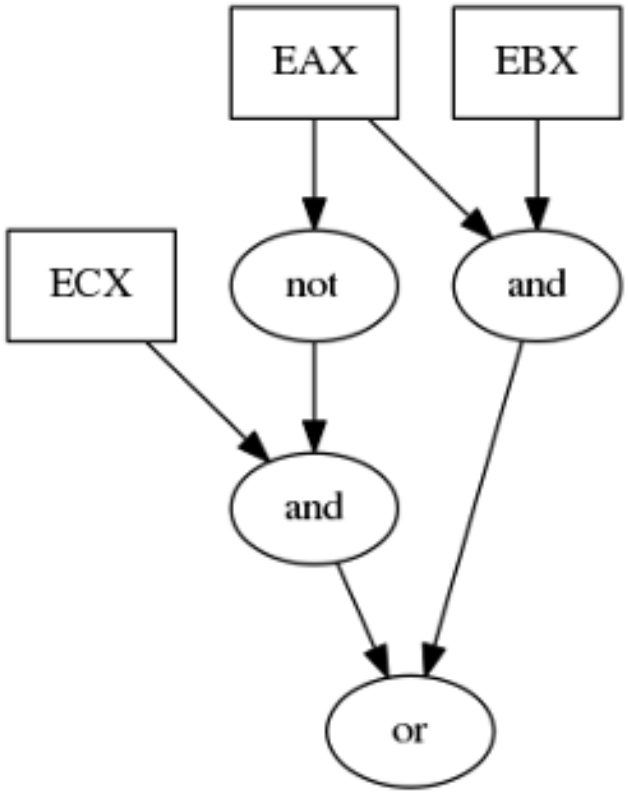
http://www.theguardian.com/business/2015/apr/29/ryanair-confirms-hackers-stole-almost-5m-via-chinese-bank-electronic-transfer

La panne majeure de courant en Turquie en mars, serait due à un piratage

- Coupure d'une douzaines de villes
  http://seclists.org/dailydave/2015/q2/22

Ingénierie à reculons automatisée d'algorithmes cryptographiques
Basée sur des "signatures" DFG (Data Flow Graph)
http://blog.amossys.fr/Automated%20Reverse%20Engineering%20of%20Cryptographic%20Algorithms.html

```
1   and     ebx,eax
2   not     eax
3   and     eax,ecx
4   or      eax,ebx
```



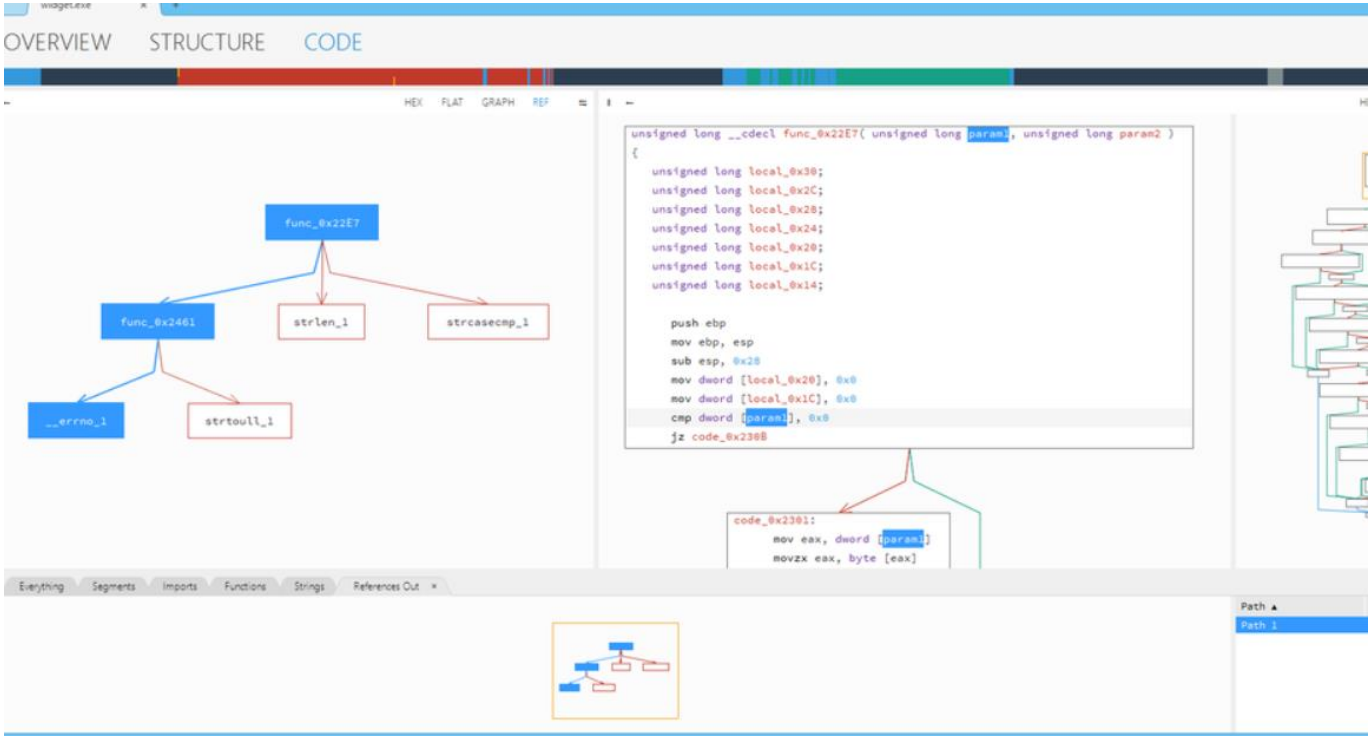
Pentest
Techniques & outils

Powershell, source de code malveillants et d'outils "post exploitation"

- Sera encore plus intéressant avec Windows Nano
  https://www.lemagit.fr/article/PowerShell-derriere-loutil-la-menace

Relyze

- Visualiser et analyse du code sous forme d'arbre
  https://www.relyze.com/



Faraday, le premier IPE (Integrated Penetration-test Environment) ?

- Permet la collaboration entre plusieurs pentesteurs et s'interface avec plus de 40 outils
  https://www.faradaysec.com/

Analyse et reverse engineering de communications sans fil

https://bytebucket.org/rootbsd/433mhz-ask-signal-analysis/raw/5f4937e4efb2198abcc375b8aefee41421941fca/pdf/433MHz_ASK_sginal_analysis-Wireless_door_bell_adventure-1.0.pdf

Détection de reverse shell Meterpreter

http://blog.didierstevens.com/2015/05/11/detecting-network-traffic-from-metasploits-meterpreter-reverse-http-module/

- N'oubliez pas de créer vos propres meterpreters…
  - /usr/share/metasploit-framework/lib/msf/core/payload/windows

```
#
def generate
  # Generate the simple version of this stager if we don't have enough space
  if self.available_space.nil? || required_space > self.available_space
    return generate_reverse_http(
      ssl:  false,
      host: datastore['LHOST'],
      port: datastore['LPORT'],
      url:  generate_small_uri,
      retry_count: datastore['StagerRetryCount'])
  end
```

Florilège de techniques de persistance sur un système

http://jumpespjump.blogspot.ca/2015/05/many-ways-of-malware-persistence-that.html

Détection de tickets Kerberos forgés

- Repose uniquement sur le fait que les outils actuels (Mimikatz et PyKEK notamment) sont repérables sur certains attributs lors de la création de tickets.
- Heureusement, le code source est disponible et on peut corriger cela :
  `kekeo/modules/kuhl_m_kerberos_pac.c`
  http://adsecurity.org/?p=1515

```
BOOL status = FALSE;
KERB_VALIDATION_INFO validationInfo = {0};
STRING user;
kull_m_kerberos_asn1_helper_util_UTCKerberosTimeToFileTime(AuthTime, &validationInfo.LogonTime);
KIWI_NEVERTIME(&validationInfo.LogoffTime);
KIWI_NEVERTIME(&validationInfo.KickOffTime);
KIWI_NEVERTIME(&validationInfo.PasswordLastSet);
KIWI_NEVERTIME(&validationInfo.PasswordCanChange);
KIWI_NEVERTIME(&validationInfo.PasswordMustChange);
RtlInitUnicodeString(&validationInfo.LogonDomainName, L"eo.oe.kiwi :)");
```

Utilisation de Radare2

- Pour résoudre un challenge de PlaidCTF
  http://dustri.org/b/exploiting-ezhp-pwn200-from-plaidct

Un plugin Burp pour collaborer en pentest

- Utilisation de git pour stocker les données
- Peu mature pour le moment, mais le concept est intéressant pour les “grosses” applications
  https://github.com/jfoote/burp-git-bridge

Pentest

Techniques & outils

Mode d'emploi pour hacker les cartes MiFare classic

https://www.firefart.at/how-to-crack-mifare-classic-cards/

Copie de cartes HID Prox

- Très répandues pour les accès physiques en entreprise

http://www.tad0.org/BlackLoop/AVRFID-Prez_BlackLoop_042015-par_tAd.pdf

Décompresser le firmware d'une caméra de surveillance

http://itsjack.cc/blog/2015/04/unpacking-cctv-firmware/

Exécuter des scripts PS avec "imports" depuis un meterpreter

http://carnal0wnage.attackresearch.com/2015/02/running-powershell-scripts-that-require.html

Shell PowerShell interactif avec Metasploit

https://www.nettitude.co.uk/interactive-powershell-session-via-metasploit/

IDAPython, le guide pour les débutants
http://hooked-on-mnemonics.blogspot.ru/2015/04/the-beginners-guide-to-idapython.html

IDA passe de PySide à PyQT
http://www.hexblog.com/?p=906

SMBMap

- Outil Python pour accéder aux shares Windows
- Supporte Pass-the-Hash
- Recherche de contenu distribuée

https://github.com/ShawnDEvans/smbmap

WPSploit - Exploiting Wordpress With Metasploit.
https://github.com/espreto/wpsploit

Gentil Kiwi publie des règles Yara pour détecter Mimikatz et kékéo
https://github.com/gentilkiwi/mimikatz/blob/master/kiwi_passwords.yar

Dumper les mots de passe en clair sous Windows 8.1

- Il suffit de modifier la clé de registre, il fallait y penser…
- Pentesters, pensez à remettre la valeur d'origine après !
  https://www.trustedsec.com/april-2015/dumping-wdigest-creds-with-meterpreter-mimikatzkiwi-in-windows-8-1/

Kali Linux, d'HTTP directement en RAM

- Boot en PXE du Kernel, puis du reste en HTTP (avec Squashfs)
  https://www.offensive-security.com/kali-linux/boot-kali-live-over-http/

Tutoriel pour faire du "Stack Smashing" en 64 bits sous Linux

http://blog.techorganic.com/2015/04/10/64-bit-linux-stack-smashing-tutorial-part-1/

Attaquer WPA2 sans le point d'accès

- Reste une attaque par dictionnaire ou brute force
  http://www.brunovalentin.com/sans-categorie/wpa2-halfhandshake-crack-craquer-le-wpa2-meme-sans-point-dacces/
  https://github.com/dxa4481/WPA2-HalfHandshake-Crack

Scada
Divers

Les Américains s'inquiètent pour leurs SCADA

- L'ancien directeur de la NSA parle de risque d'apocalypse numérique
  http://www.zdnet.fr/actualites/les-tats-unis-s-inquietent-aussi-pour-leurs-systemes-scada-39818720.htm

Vulnérabilités dans les pompes à insuline

https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01

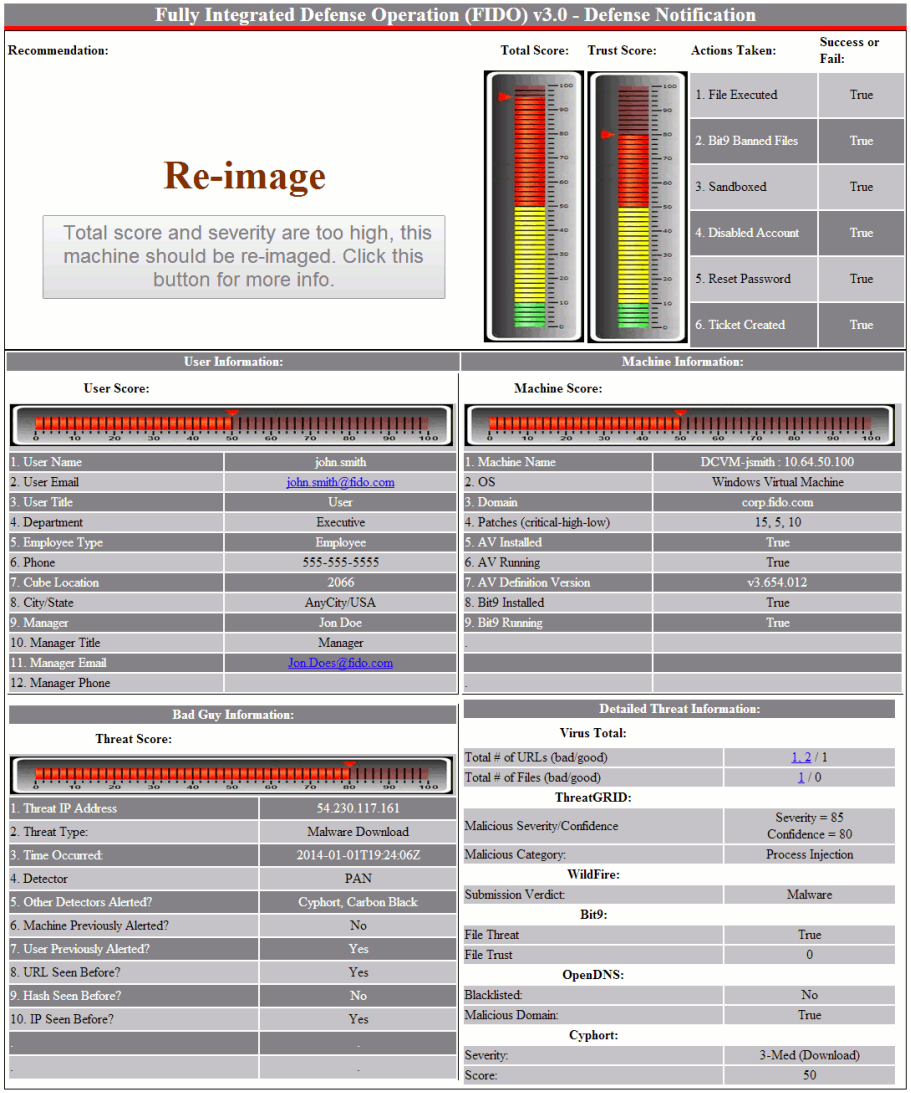
Peu de publication de bulletins sur l'ICS-CERT ….

Nouveautés (logiciel, langage, protocole...)

Open Source

Netflix publie FIDO, son outil d'automatisation de la réponse à incidents

https://github.com/Netflix/Fido



Fully Integrated Defense Operation (FIDO) v3.0 - Defense Notification

Recommendation:

Re-image

Total score and severity are too high, this machine should be re-imaged. Click this button for more info.

Total Score: **Trust Score:**

Actions Taken:	Success or Fail:
1. File Executed	True
2. Bit9 Banned Files	True
3. Sandboxed	True
4. Disabled Account	True
5. Reset Password	True
6. Ticket Created	True

User Information:

User Score:

1. User Name	john smith
2. User Email	john.smith@fido.com
3. User Title	User
4. Department	Executive
5. Employee Type	Employee
6. Phone	555-555-5555
7. Cube Location	2066
8. City/State	AnyCity/USA
9. Manager	Jon Doe
10. Manager Title	Manager
11. Manager Email	Jon.Does@fido.com
12. Manager Phone	

Machine Information:

Machine Score:

1. Machine Name	DCVM-jsmith : 10.64.50.100
2. OS	Windows Virtual Machine
3. Domain	corp.fido.com
4. Patches (critical-high-low)	15, 5, 10
5. AV Installed	True
6. AV Running	True
7. AV Definition Version	v3.654.012
8. Bit9 Installed	True
9. Bit9 Running	True

Bad Guy Information:

Threat Score:

1. Threat IP Address	54.230.117.161
2. Threat Type:	Malware Download
3. Time Occurred:	2014-01-01T19:24:06Z
4. Detector	PAN
5. Other Detectors Alerted?	Cyphort, Carbon Black
6. Machine Previously Alerted?	No
7. User Previously Alerted?	Yes
8. URL Seen Before?	Yes
9. Hash Seen Before?	No
10. IP Seen Before?	Yes

Detailed Threat Information:

Virus Total:	
Total # of URLs (bad/good)	1, 2 / 1
Total # of Files (bad/good)	1 / 0
ThreatGRID:	
Malicious Severity/Confidence	Severity = 85 Confidence = 80
Malicious Category:	Process Injection
WildFire:	
Submission Verdict:	Malware
Bit9:	
File Threat	True
File Trust	0
OpenDNS:	
Blacklisted:	No
Malicious Domain:	True
Cyphort:	
Severity:	3-Med (Download)
Score:	50

Nouveautés (logiciel, langage, protocole...)

Microsoft

Grosse actualité sécu pour Microsoft dans cette revue d'actu !

LAPS : Local Administrator Password Solution

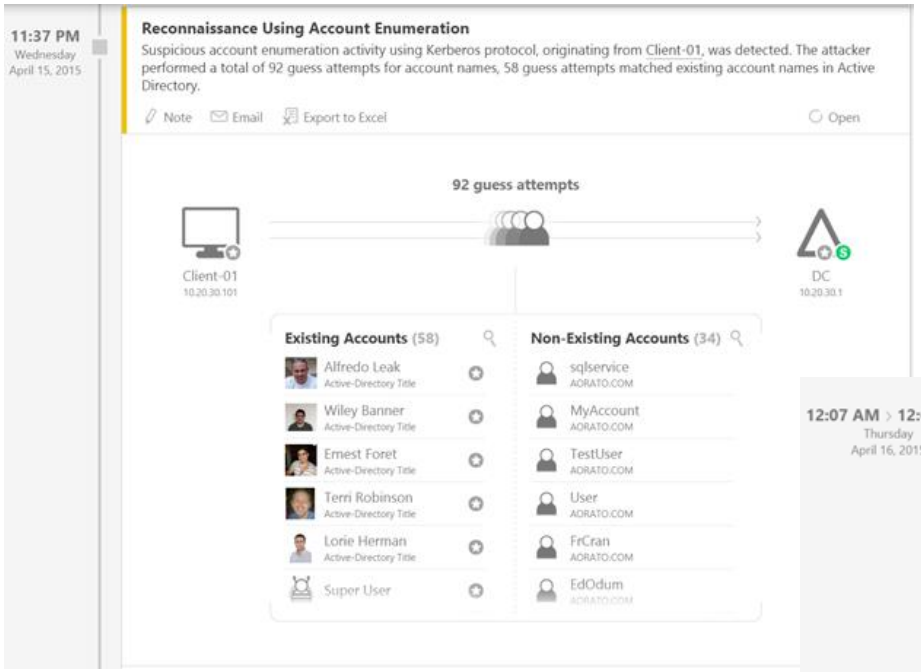
- Automatisation du changement de mot de passe Administrateur local sur les machines Windows
- Version officiel d'un script existant depuis -au moins- octobre 2014
- Stocke EN CLAIR les mots de passe admin local dans un attribut caché de l'Active Directory
  https://technet.microsoft.com/en-us/library/security/3062591
- Pour vérifier si les ACLs sont bien positionnés, un script PowerShell (utile en pentest)
  https://blog.netspi.com/running-laps-around-cleartext-passwords/

Nouveautés (logiciel, langage, protocole...)

Microsoft

ATA : Advanced Threat Analysis

- Rebranding des produits vendus par Aorato, racheté en Novembre par Microsoft
- Console de gestion + sondes qui analysent une copie des flux vers les contrôleurs de domaine
- Version d'évaluation gratuite valide 90j
  http://blogs.technet.com/b/ad/archive/2015/05/04/microsoft-advanced-threat-analytics-public-preview-release-is-now-available.aspx

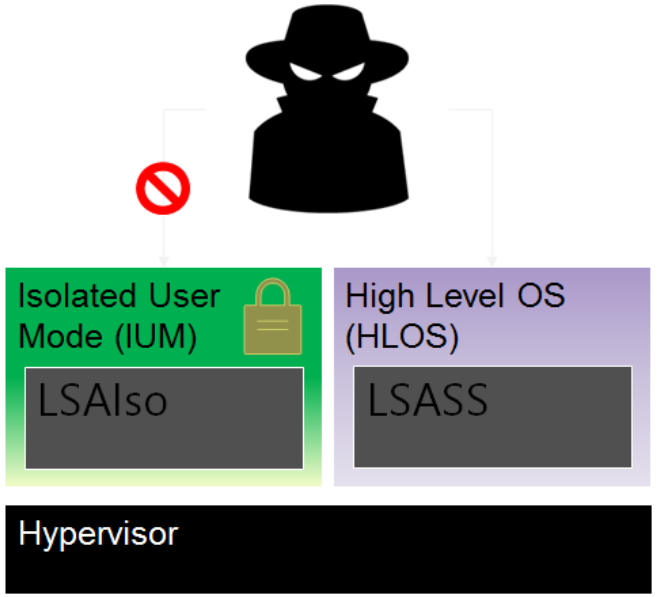


Nouveautés (logiciel, langage, protocole...)

Microsoft

IUS (Isolated User Mode) / VSM (Virtual Secure Mode)

- Objectif : empêcher la récupération en mémoire et le rejeu de mots de passe, hashes ou tickets Kerberos
- Utilisation d'Hyper-V pour stocker la mémoire du processus LSASS dans un "conteneur" inaccessible depuis l'espace utilisateur ou le kernel !
- Utilisation de Microsoft Passport : crypto asymétrique, utilisation de TPM v2
- Kerberos avec crypto asymétrique !!!
- Pour NTLM, création d'un "token" NTLM dans le VSM, utilisation restreinte à la machine sur laquelle il a été créé.
- Tout cela nécessitera un niveau fonctionnel 2016.
  http://channel9.msdn.com/Events/Ignite/2015/BRK2334
  http://adsecurity.org/?p=1535



Nouveautés (logiciel, langage, protocole...)

Open Source

Une documentation sur les SSD pour les gouverner toutes

http://codecapsule.com/2014/02/12/coding-for-ssds-part-1-introduction-and-table-of-contents/

Nouveautés (logiciel, langage, protocole...)

Divers

Firefox entame l'après HTTP (sans TLS)

https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/

Microsoft Edge remplacera IE

- Améliorations de sécurité au programme
- Arrêt du support d'ActiveX / VBScript / BHO / Toolbars / etc
- Utilisation de Microsoft Passport pour l'authentification
- Certificate Reputation
- SmartScreen
- Enhanced Protected Mode (EPM, sandboxing)
  http://blogs.windows.com/msedgedev/2015/05/11/microsoft-edge-building-a-safer-browser/

Exécuter Google Chrome dans un conteneur docker

https://github.com/jlund/docker-chrome-pulseaudio

Business
International

Le marché gris des 0-days

https://hackerone.com/news/the-wolves-of-vuln-street

Mozilla révoque une AC Turque “e-Guven Elektronik Bilgi Guvenligi A.S.”

- Quelques mois après la révocation d’une AC Chinoise
- L’AC ne respecte pas certaines parties de la politique de Mozilla
  https://blog.mozilla.org/security/2015/04/27/removing-e-guven-ca-certificate/

Droit / Politique

France

Ingénierie à reculons de Skype

- L'auteur condamné à 6 mois avec sursis en appel
  http://www.nextinpact.com/news/93727-un-informaticien-condamne-pour-avoir-contrefait-skype-et-revele-ses-fragilites.htm
- A noter qu'il est actuellement condamné à 15 ans de prison en Australie pour viol sur mineure**s**
  http://m.20minutes.fr/marseille/1558251-aix-provence-vingt-ans-prison-requis-contre-adepte-hare-krishna

Loi sur le renseignement adoptée par l'assemblée

http://www2.assemblee-nationale.fr/scrutins/detail/%28legislature%29/14/%28num%29/1109

- Aux USA, une cours fédérale juge illégale l'espionnage massif de la NSA
  http://www.nationaljournal.com/tech/federal-appeals-court-rules-nsa-spying-illegal-20150507

Loi sur le renseignement : France-IX ne coopèrera pas

- <<France-IX ne coopère avec aucun service de l'état quel qu'il soit pour fournir des renseignements sur la nature des flux et sur les flux eux-mêmes qui passent via nos infrastructures>>
  https://twitter.com/ixpfranceix/status/591606336305127424

Loi sur le renseignement : Mozilla s'y oppose

https://blog.mozilla.org/press-fr/2015/04/22/loi-renseignement-mozilla-sexprime/

Droit / Politique

France

Espionnage FR par les Allemands

- Espionnage de 690 000 n° de téléphone et 7,8 millions d'IP entre 2012 et 2013
- Les USA les ont forcés !!?
  http://go.theregister.com/feed/www.theregister.co.uk/2015/04/24/bnd_nsa_spying_collaboration/
- Mais cet espionnage aurait eu lieu pour rechercher des trafics d'armes
  http://www.sueddeutsche.de/politik/geheimdienst-affaere-bnd-half-nsa-beim-ausspaehen-von-frankreich-und-eu-kommission-1.2458574
- Mais surtout pour de l'espionnage industriel
  http://www.sueddeutsche.de/politik/geheimdienst-affaere-bnd-half-nsa-beim-ausspaehen-von-frankreich-und-eu-kommission-1.2458574

Droit / Politique

France

krach.in

TODO ASO

Droit / Politique
International

Une jeune femme pirate des PC et les webcams des domiciles

- Elle parle aux victimes depuis les PC compromis, leur montre des vidéos porno…
- … et fini en prison
- Alors qu'elle dirigeait un forum de 35 000 hackeurs (n00bs?)
  http://www.cbc.ca/news/canada/montreal/val%C3%A9rie-gignac-accused-of-spying-via-webcams-harassing-children-1.3053722

Présentation de TOR aux polices belges et hollandaises

- Avec des réactions intéressantes
  - Même si la police sait que l'IP est un noeud TOR, ils perquisitionnent pour dissuader
  - La police hollandaise ont leur propre réseau d'anonymisation
  - ...

  https://blog.torproject.org/blog/trip-report-tor-trainings-dutch-and-belgian-police

La "Cyber" stratégie du DoD

- Plus d'ouverture ? Avec la sécurité intérieur voire avec celles d'autres pays ?
- Recrutement de 6 200 personnes
  https://publicintelligence.net/dod-cyber-strategy/

Terrorisme
International

La police américaine utiliserait des bombes EMP pour désarmer les bombes.

http://www.infowars.com/report-emp-device-used-to-disable-possible-explosives-following-garland-attack/

Conférences

Passées

- Insomni'hack - 20 mars 2015 à Genève

Texte en gris = déjà traité précédemment

A venir

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

  http://www.youtube.com/watch?v=Ulbx4IFTG7E
- SSTIC 2015 - 3, 4 et 5 juin 2015 à Rennes
  - Challenge résolu http://communaute.sstic.org/ChallengeSSTIC2015
  - Qui a eu sa place ?

Divers / Trolls velus

La DGSE utilise encore Windows XP !!?

- Et le logiciel open source Audacity
  https://twitter.com/newsoft/status/592608913834516480/photo/1

Mettez à jour qu'ils disaient…

- Selon une étude de Sécunia
- 65% des lecteur de PDF ne sont pas à jour
- 77% des JRE non plus
- …
  http://www.net-security.org/secworld.php?id=18329

Facepwn, une faille 0-day pour lire les messages privés de Facebook

https://phl4nk.wordpress.com/2015/04/27/facepwn-a-facebook-0day-for-reading-private-messages/

- Ou une farce du 1er avril pour tracer indiscrets avec une carte
  https://phl4nk.wordpress.com/2015/05/10/facepwn-part-2-the-results/

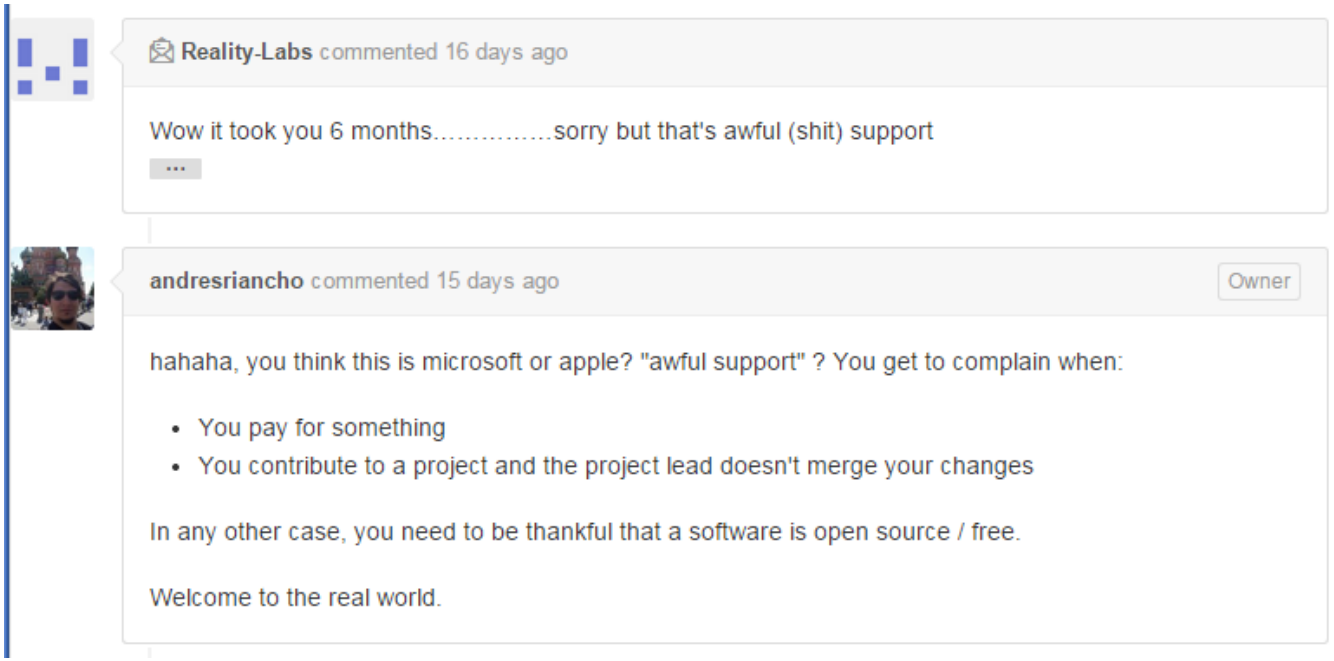
Divers / Trolls velus

Les antivirus abaissent votre niveau de sécurité

- Interception TLS vulnérable à FREAK
- Désactivation du Key Pinning
- …
  https://blog.hboeck.de/archives/869-How-Kaspersky-makes-you-vulnerable-to-the-FREAK-attack-and-other-ways-Antivirus-software-lowers-your-HTTPS-security.html

L'Open-Source…

https://github.com/andresriancho/w3af/issues/5593



Reality-Labs commented 16 days ago

Wow it took you 6 months.....sorry but that's awful (shit) support

...

andresriancho commented 15 days ago — Owner

hahaha, you think this is microsoft or apple? "awful support" ? You get to complain when:

- You pay for something
- You contribute to a project and the project lead doesn't merge your changes

In any other case, you need to be thankful that a software is open source / free.

Welcome to the real world.

Divers / Trolls velus

Panne d'iPad == Avion au sol

- chez American Airlines, car les plans de vols sont sur une application iPad
  http://www.lefigaro.fr/secteur/high-tech/2015/04/29/01007-20150429ARTFIG00068-les-avions-d-american-airlines-cloues-au-sol-apres-un-bug-d-ipad.php

Chirurgie robotisée… et les hackeurs dans tout ca ?

http://www.sciencesetavenir.fr/sante/20150427.OBS8001/chirurgie-robotique-les-patients-a-la-merci-des-hackers.html

Les objets connectés…

http://weputachipinit.tumblr.com/

Les panneaux connectés…

- Accessible depuis internet, en HTTP, parfois dans login/pass
  http://cybergibbons.com/security-2/shodan-searches/interesting-shodan-searches-yesco-electronic-billboards/

Mots de passe à la télé : il n'y a pas que TV5 Monde..

- Mot de passe du C&C de trains sur la BBC
  https://grahamcluley.com/2015/05/train-control-centre-passwords-revealed/

Divers / Trolls velus

Méfiez-vous des taxi

- Escroquerie par des chauffeurs de taxi disposant de terminaux de paiement compromis
  http://www.cbanque.com/actu/51833/une-escroquerie-inedite-a-la-carte-bancaire-demantelee-en-france

Les criminels numériques ne sont pas tous intelligents

- Envoie de photos d'eux-mêmes
- Divulgation d'informations personnelles sur les forums
- ...
  http://www.zdnet.fr/actualites/les-bras-casses-de-la-cybercriminalite-39818696.htm

Les bornes d'arcade Capcom CPS1 enfin complètement reversé

http://arcadehacker.blogspot.fr/2015/04/capcom-cps1-part-1.html

CrowdStrike suffisamment fort pour décourager des attaquants ?

http://blog.crowdstrike.com/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/

Prochaines réunions

Prochaines réunions

- Mardi 9 Juin 2015

After Work

- A définir

Questions ?