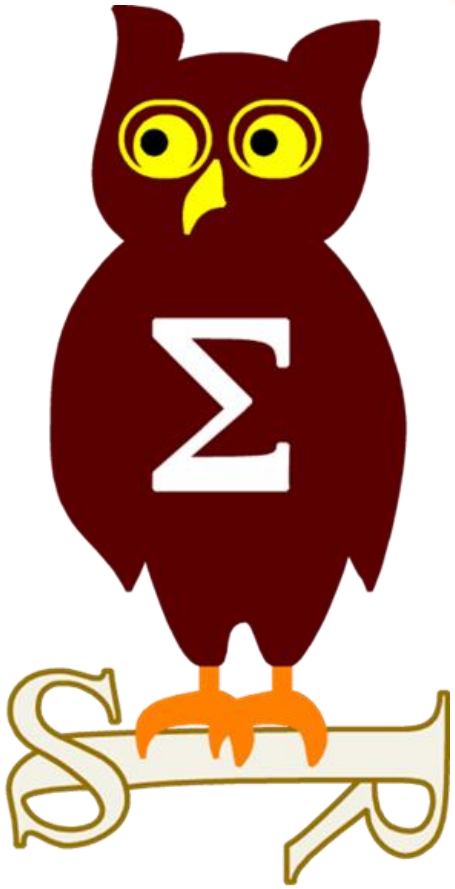
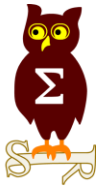


Revue d'actualité

12/07/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-063 Vulnérabilités dans Internet Explorer (10 CVE) [Exploitabilité 1,1,1,1,1,1,1,1,3,1]

- Affecte:
  - Windows (toutes versions supportes), remplace MS16-051, KB3156387, KB3156421
- Exploit:
  - 8 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement du filtrage anti XSS
  - 1 x usurpation du proxy / WAPD (BadTunnel)
    http://xlab.tencent.com/en/2016/06/17/BadTunnel-A-New-Hope/
- Crédits:
  - 62600BCA031B9EB5CB4A74ADDDD6771E par ZDI de Trend Micro (CVE-2016-0200)
  - Ashutosh Mehra par ZDI de Trend Micro (CVE-2016-3211)
  - Masato Kinugawa de Cure53 (CVE-2016-3212)
  - Moritz Jodeit de Blue Frost Security (CVE-2016-3210)
  - SkyLined par iDefense (CVE-2016-0199)
  - Tao Yan (@Ga1ois) de Palo Alto Networks (CVE-2016-3205, CVE-2016-3206, CVE-2016-3207)
  - Yu Yang (@tombkeeper) de Tencent's Xuanwu Lab (CVE-2016-3213)

MS16-068 Vulnérabilités dans Edge (8 CVE) [Exploitabilité 1,1,1,1,1,1,1,1]

- Affecte:
  - Windows 10, remplace KB3156387, KB3156421
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x Contournement du filtrage anti XSS
  - 1 x évasion du lecteur PDF
- Crédits:
  - Jaanus Kääp de Clarified Security (CVE-2016-3201)
  - Jordan Rabet de Microsoft Offensive Security Research Team (CVE-2016-3214)
  - Kai Song (exp-sky) de Tencent's Xuanwu Lab (CVE-2016-3222)
  - Ke Liu de Tencent's Xuanwu Lab (CVE-2016-3215)
  - Mario Heiderich de Cure53 (CVE-2016-3198)
  - Shi Ji (@Puzzor) de VARAS@IIE par ZDI de Trend Micro (CVE-2016-3222)
  - kdot par ZDI de Trend Micro (CVE-2016-3203, CVE-2016-3215)
  - lokihardt par ZDI de Trend Micro (CVE-2016-3199)

Dont 0 commune avec IE

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-069 Vulnérabilités dans JScript et VBScript (3 CVE) [Exploitabilité 1,1,1]

- Affecte:
  - VBScript 5.7 et 5.8 (Windows Vista, 2008), remplace MS16-053
- Exploit:
  - 3 x Corruptions de mémoire dans un script VBScript aboutissant à une exécution de code
- Crédits:
  - Tao Yan (@Ga1ois) de Palo Alto Networks (CVE-2016-3205, CVE-2016-3206, CVE-2016-3207)

MS16-070 Vulnérabilités dans Office (4 CVE) [Exploitabilité 1,1,2,2]

- Affecte:
  - Office 2007, 2010, 2013, 2013RT, 2016, Mac 2011 et 2016
  - Sharepoint 2010, 2013
  - Remplace MS16-004, MS16-042, MS16-054
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code à l'ouverture d'un fichier Office
- Crédits:
  - Danny Wei Wei de Tencent's Xuanwu Lab (----------)
  - David D. Rude II par iDefense (CVE-2016-3233)
  - Dhanesh Kizhakkinan de FireEye Inc (CVE-2016-3234)
  - LiYaDong de 360 QEX Team (CVE-2016-0025, (CVE-2016-0025)
  - Yorick Koster de Securify B.V. (CVE-2016-3235)

MS16-071 Vulnérabilité dans Microsoft DNS Serveur (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes), Remplace MS15-127
- Exploit:
  - Exécution de code à distance sans authentification
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-072 Security Update for Group Policy (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes), remplace KB3156387, KB3156421
- Exploit:
  - Usurpation d'un DC, ajout de Group Policies et exécution de code en tant que SYSTEM
    - Suite à MS16-014 (qui était une amélioration de MS15-122)
    - 8 mois pour corriger. La correction consiste à récupérer les Policies avec le compte machine

    http://www.slideshare.net/NabeelAhmed7/from-zero-to-system-on-full-disk-encrypted-windows-system

    https://blog.ahmednabeel.com/from-zero-to-system-on-full-disk-encrypted-windows-system-part-2/
- Crédits:
  - NabeelAhmed de Dimension Data (CVE-2016-3223)
  - Tom Gilis de Dimension Data (CVE-2016-3223)

MS16-073 Vulnérabilités noyau Win32k (3 CVE) [Exploitabilité 1,1,2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace MS16-062, KB3156387, KB3156387, KB3156421, KB3156421
- Exploit:
  - Élévations de privilège locale
- Crédits:
  - RanchoIce de Baidu Security Lab (CVE-2016-3221)
  - zhong_sf et pgboy de Qihoo 360Vulcan Team (CVE-2016-3218)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-074 Vulnérabilités dans GDI (3 CVE) [Exploitabilité 2,2,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace MS16-026, MS16-055, KB3156387, KB3156421
- Exploit:
  - 1 x Contournement ASLR (fuite d'information)
  - 2 x Élévations de privilège locale, dont Adobe Type Manager Font Driver (ATMFD.DLL)
    http://0day.today/exploit/25535
    https://bugs.chromium.org/p/project-zero/issues/detail?id=785
- Crédits:
  - James Forshaw de Google Project Zero (CVE-2016-3219)
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-3216, CVE-2016-3220)

MS16-075 Security Update for Windows SMB Server (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace MS15-052, MS15-122, MS16-007, KB3135173, KB3135174
- Exploit:
  - Élévation de privilège locale à partir de SMB
  - L'exploit pour Metasploit
    https://github.com/vvalien/win_exp/blob/master/one_day.rb
- Crédits:
  - ?

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-076 Vulnérabilité dans Netlogon (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows serveur 2008, 2008R2, 2012 et 2012R2
  - Remplace MS15-122, MS16-007
- Exploit:
  - Corruption de mémoire aboutissant à une exécution de code
    - Connexion à un DC en faisant une demande de synchro
- Crédits:
  - ?

MS16-077 BadTunnel / WPAD (2 CVE) [Exploitabilité 1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3156387, KB3156421
- Exploit:
  - Usurpation du WPAD (activé par défaut)
    - L'usurpation de requête NetBios est une fonctionnalité
  - Présentation à HITB 2016 d'une méthode liée permettant de contourner la sandbox d'IE11 (Enhanced Protected Mode / EPM)
    http://gsec.hitb.org/sg2016/sessions/look-mom-i-dont-use-shellcode-a-browser-exploitation-case-study-for-internet-explorer-11/
- Crédits:
  - Moritz Jodeit de Blue Frost Security GmbH (CVE-2016-3213)
  - Yu Yang (@tombkeeper) de Tencent's Xuanwu Lab (CVE-2016-3213)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-078 Security Update for Windows Diagnostic Hub (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows 10, remplace KB3156387, KB3156421
- Exploit:
  - Élévations de privilège locale à partir de "Diagnostics Hub Standard Collector Service" (collecte en temps réèl des évènements "Event Tracing" et traitement)
- Crédits:
  - Qihoo 360Vulcan Team (CVE-2016-3231)
  - lokihardt par ZDI de Trend Micro (CVE-2016-3231)

MS16-079 Vulnérabilité dans Microsoft Exchange (1 CVE) [Exploitabilité 3]

- Affecte:
  - Exchange 2007, 2010, 2013 et 2016
  - Remplace MS14-075, MS16-010
- Exploit:
  - Possibilité de récupérer du contenu web lors de la lecture d'un mail sur OWA
  - Correction de 3 vulnérabilités Oracle
- Crédits:
  - Louis-Paul Dareau de ProcessOut (CVE-2016-0028)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-080 Vulnérabilités dans la librairie PDF (3 CVE) [Exploitabilité 2,2,2]

- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
  - Remplace MS16-028, KB3156387, KB3156421
- Exploit:
  - 1 x Exécutions de code lors du traitement d'un fichier PDF spécialement formatée
  - 2 x Accès à des informations du contexte utilisateur
- Crédits:
  - Jaanus Kääp de Clarified Security (CVE-2016-3201)
  - Ke Liu de Tencent's Xuanwu Lab (CVE-2016-3203, CVE-2016-3215)
  - kdot par ZDI de Trend Micro (CVE-2016-3203, CVE-2016-3215)

MS16-081 Vulnérabilité dans Active Directory (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows serveur 2008, 2008R2, 2012, 2012R2
  - Remplace MS13-032
- Exploit:
  - Déni de service
- Crédits:
  - Ondrej Sevecek de GOPAS (CVE-2016-3226)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-082 Vulnérabilité dans Windows Search (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3156387, KB3156421
- Exploit:
  - Déni de service à partir de la recherche Windows
- Crédits:
  - ?

MS16-083 Vulnérabilité dans Adobe Flash Payer (38 CVE) [Exploitabilité]

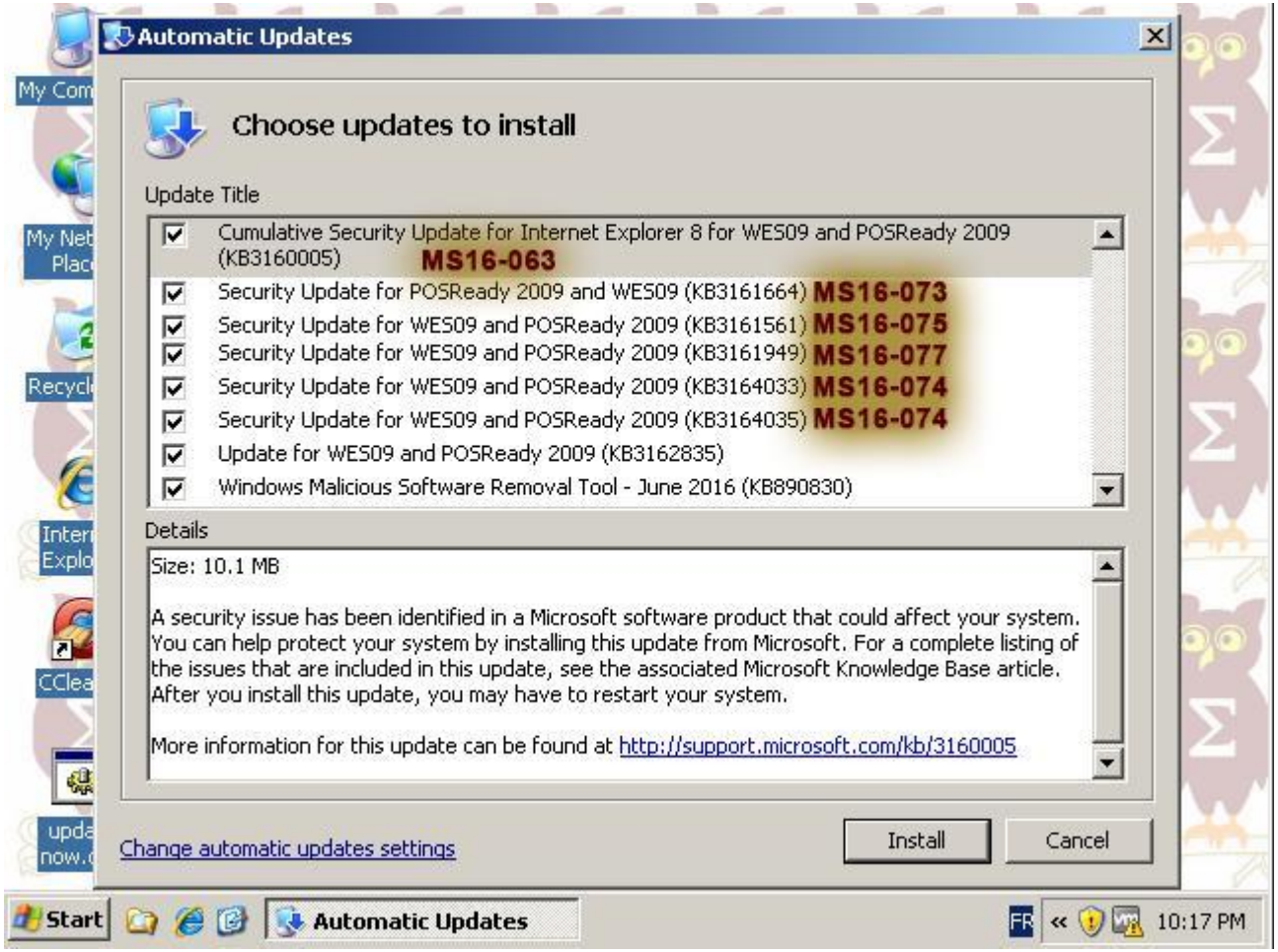
- Affecte:
  - Windows 8.1, 10, 2012, 2012R2
- Exploit:
  - Exécutions de code
- Crédits:
  - ?

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

- **Rien ce mois-ci**

Failles / Bulletins / Advisories

Microsoft - Autre

Microsoft à payé $10,000 pour une mise à jour de Windows 10

- “Nobody ever asked me if I wanted to update.”

  http://www.seattletimes.com/business/microsoft/microsoft-draws-flak-for-pushing-windows-10-on-pc-users/

- Depuis, Windows demande gentiment

  http://uk.businessinsider.com/microsoft-changes-windows-10-upgrade-notifications-2016-6

Présentation du contournement de HVCI à la BlackHat (MS16-066)

https://www.blackhat.com/us-16/briefings/schedule/index.html#analysis-of-the-attack-surface-of-windows-10-virtualization-based-security-3666

Failles / Bulletins / Advisories

Antivirus

Symantec, encore des vulnérabilités trouvées par Tavis

- Exécution de code noyau à partir de “dépackeur” UPX
- Dépassement de tampon (buffer overflow) dans le “parseur” PowerPoint

  https://googleprojectzero.blogspot.fr/2016/06/how-to-compromise-enterprise-endpoint.html
- Le gouvernement US recommande de mettre à jour au plus vite

  https://www.grahamcluley.com/2016/07/government-tells-symantec-norton-antivirus-users-apply-security-patches-immediately/

Antivirus Armadito

http://seclists.org/fulldisclosure/2016/Jun/69

Failles / Bulletins / Advisories

Système (principales failles)

Wget <= 1.17

- Exécution de code à partir des “302 Redirect” vers un FTP

  https://blogs.securiteam.com/index.php/archives/2701

- Et pour jouer avec les utilisateurs de Wget

```php
<?php
// Wget Troll
if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    if(preg_match("/Wget/", $_SERVER['HTTP_USER_AGENT'])) {
        header("Location: ftp://speedtest.tele2.net/1000GB.zip", true, 302);
        exit;
    }
}
?>
```

https://twitter.com/datasiph0n/status/751008978923028480/photo/1

Firefox, contournement de la Same Origin Policy

- http://37.187.18.85**\x0B**.test.google.com

  http://blog.bentkowski.info/2016/07/firefox-same-origin-policy-bypass-cve.html

Apache, HTTP2 et X509

- Une vulnérabilité dans Apache permettait, lorsque HTTP2 était activé, de contournement le contrôle d’accès via certificat

http://seclists.org/fulldisclosure/2016/Jul/11

Failles / Bulletins / Advisories

Système (principales failles)

Esx, bug non exploitable selon VMWare

- Pourtant bien exploitable selon SpiderLabs 😜

  https://twitter.com/vnik5287/status/746196338346332160/photo/1

VBulletin, une 0day serait en cours d'utilisation dans la nature

https://twitter.com/LeakedSource/status/751604566353936384

Contournement d'un WAF grâce aux entêtes HTTP

- X-forwarded-for, X-remote-IP, X-originating-IP, X-remote-addr

  http://www.securityaegis.com/bypassing-web-application-firewalls-using-http-headers/

```
GET /app?user='or'1'='1';-- HTTP/1.1
Host: www.heisenberg-bank.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0)
Gecko/20100101 Firefox/26.0
Accept: */*
x-forwarded-for: I'm your cache server! (184.189.250.X)
x-remote-IP: I'm your proxy! (184.189.250.X)
x-originating-IP: I'm YOU! (127.0.0.1)
x-remote-addr: Internal user, let me in! (192.168.1.X)
x-remote-ip: I swear I'll be nice (* or %00 or %0A)
```

Sanbox/microvm bromium

- Divers contournement et évasions

  https://twitter.com/taviso/status/741063403985240064

  https://twitter.com/taviso/status/740695221621526528

Failles / Bulletins / Advisories

Système (principales failles)

ThinkPwn, exécution de code UEFI

- Vulnérables : Lenovo Thinkpad, HP Pavilion, des cartes mère Gigabyte, certains Dell Latitude...

  https://github.com/Cr4sh/ThinkPwn

  http://www.winbeta.org/news/zero-day-exploit-bypasses-windows-security-features-affects-lenovo-thinkpads
- Plus de détails sur l'exploit :

  http://linkis.com/blog.cr4.sh/2016/06/8pS5X

StartCom essaie de copier LetsEncrypt (en délivrant gratuitement et automatiquement des certificats)

- Et se plante lamentablement :
  - Le chemin du fichier prouvant l'appartenance du site est laissée à la main de l'utilisateur
  - L'API suit les redirect, même vers un autre domaine
  - L'API ne vérifie pas le certificat SSL du site, ni le type MIME du fichier
  - ...

  https://www.computest.nl/blog/startencrypt-considered-harmful-today/

Comodo essaie de voler la marque LetsEncrypt

- "Let's Encrypt", "Let's Encrypt with Comodo", "Comodo Let's Encrypt"
- Mais fini par abandonner, ouf !

  https://letsencrypt.org//2016/06/23/defending-our-brand.html

Failles / Bulletins / Advisories

Réseau (principales failles)

TP-LINK ne renouvelle pas ses noms de domaine

- Pas de risque majeur, mais les anciens noms de domaine sont étiquettés sur les équipements.

  http://seclists.org/bugtraq/2016/Jul/3

Failles / Bulletins / Advisories

Apple, Google, Facebook...

Contournement du chiffrement des mobiles Android utilisant un SoC Qualcomm

- Via une vulnérabilité dans le noyau de la TrustZone

  https://bits-please.blogspot.fr/2016/06/extracting-qualcomms-keymaster-keys.html

Contournement de la double authentification Google

- En demandant poliment le code de sécurité à l'utilisateur
  - et en ayant son identifiant et son mot de passe 😜

  http://www.informanews.net/double-authentification-google-hackers/

Apple oublie de chiffrer le cache noyau d'iOS 10 ?

https://www.technologyreview.com/s/601748/apple-opens-up-iphone-code-in-what-could-be-savvy-strategy-or-security-screwup/

- Non, c'est un choix !

  https://twitter.com/musclenerd/status/750624369756368896

iOS 10 image comparison

	Unencrypted in 10.0b1	Unencrypted in 10.0b2
bootloaders	none	32-bit
ramdisk	none	all except ATV
kernel	64-bit	all
main filesystem	all	all
sep	none	none

Failles / Bulletins / Advisories

Divers

Vulnérabilité dans le framework Java Spring

- Contournement du contrôle d'accès via un défaut de matching d'URL

  http://pivotal.io/security/cve-2016-5007

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Voitures

Vulnérabilités sur les portail officiels de BMW et ConnectDrive

- Permet de contrôler des fonctions de la voiture (chauffage, éclairage) et de gérer les services de l'utilisateur comme les emails

  http://securityaffairs.co/wordpress/49149/hacking/bmw-connecteddrive-hacking.html

Attaque sur TheDAO (Ethereum)

- Exploitation d'une faille dans un smart-contract pour voler des Ethers (crypto-monnaie)
- Détournement de 3,6 millions d'Ether (~$50 000 000)
- Réactions de la communauté pour empêcher le détournement :
  - Hardfork : on annule toutes les transactions depuis une certaine date
  - Softwork : on blackliste l'adresse du "pirate"

    ⇒ Problème : possibilité d'utiliser cette technique pour porter atteinte à la disponibilité des noeuds
- Sans nouvelle décision, le pirate pourra utiliser les fonds détournés à partir de jeudi

http://www.securityinsider-solucom.fr/2016/06/ethereum-x-dao-retours-sur-lattaque-de_30.html

Pirater un compte Facebook ?

- Il suffit d'insister un peu…

https://www.reddit.com/r/technology/comments/4q8ywp/til_that_someone_can_change_your_facebook_email

Piratages, Malwares, spam, fraudes et DDoS

Malware

Conficker remis au goût du jour

- Ciblant des hôpitaux avec des vieux Windows non à jour

  https://threatpost.com/conficker-used-in-new-wave-of-hospital-iot-device-attacks/118985/

Locky, nouvelle technique anti-sandbox

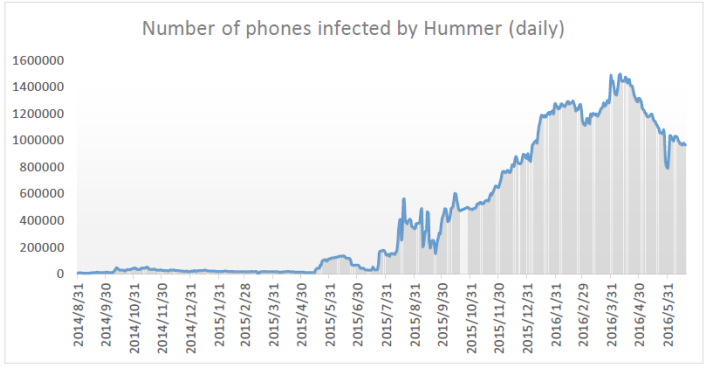
- Déchiffrement à partir d'une clef passé en paramètre

  https://blog.fortinet.com/2016/06/30/cracking-locky-s-new-anti-sandbox-technique

Hummer infecte 1,4 millions Android par jour

- Soit 500 000 dollars par jour pour le groupe Chinois
- Pays concernés: Inde, Chine, Malaisie, Turquie, ...

  http://www.cmcm.com/blog/en/security/2016-06-29/995.html



Malware angler en fin de vie?

- De mois en moins d'activité

  https://nakedsecurity.sophos.com/2016/06/16/is-angler-exploit-kit-dead/

Piratages, Malwares, spam, fraudes et DDoS

Malware

Généralisation des Macro Office détectant les sandbox

http://joe4security.blogspot.fr/2016/07/rise-of-vbs-evading-sandboxes.html

Un ransomware 100% en Javascript

- On n'arrête pas le progrès

https://nakedsecurity.sophos.com/2016/06/20/ransomware-thats-100-pure-javascript-no-download-required/

Un malware pour Mac OS Xfait son apparition: Eleonor

- S'installe par une application non signé: Easy Doc Converter. Auto-install un service Tor et un serveur web PHP.
- L'activation de la protection Gatekeeper permet de se prémunir du malware

https://labs.bitdefender.com/2016/07/new-mac-backdoor-nukes-os-x-systems/

Premier ransomware pour Mac OS X ?

- Signé comme une véritable application
- Apple a réagit rapidement en révoquant le certificat et en mettant à jour son antivirus
  - Un antivirus sur Mac !!? Il y'aurait donc des virus !!!

https://techcrunch.com/2016/03/07/apple-has-shut-down-the-first-fully-functional-mac-os-x-ransomware/

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Vulnérabilité dans une prise connectée

- Possibilité d'allumer/éteindre si on connaît l'adresse MAC
- Menaces de la part du fabricant à l'encontre d'une personne ayant indiqué cette information dans un commentaire sur Amazon

  https://techcrunch.com/2016/07/01/security-researcher-gets-threats-over-amazon-review/

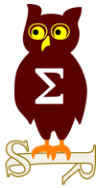
Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Fuite de données chez Amazon

- Un serveur Amazon Kindle contenant 80 000 logins piraté. Des données personnelles disponibles: nom, numéro de téléphone, mot de passe, adresse/ville/pays, adresse IP, ...

  http://securityaffairs.co/wordpress/49192/data-breach/hacker-breached-amazon-server.html



Nouveautés, outils et techniques

Mettre une porte dérobée dans Diffie-Hellman

- En choisissant p et q pour réduire la complexité du logarithme discret
- En choisissant p et q pour que p-1 et q-1 soient factorisable par la méthode Pollard

https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/2016/june/how-to-backdoor-diffie-hellmanpdf

Récupérer les relations hiérarchiques de l'Active Directory

- Plus efficace que l'outil présenté lors de la précédente revue

  http://nicolaslang.blogspot.fr/2015/07/obtenir-un-organigramme-hierarchique.html

Un framework pour backdoorer du code source ou des exécutables

https://github.com/TreyCorp/Keyhole

Un fork d'AFL pour fuzzer les binaires Windows

https://github.com/ivanfratric/winafl

Framework de récupération d'infos sensibles en mémoire

- Écrit en PowerShell
- Focalisé sur l'espace utilisateur

  https://github.com/putterpanda/mimikittenz

Attacking KeePass

- Using Powershell of course

  http://www.harmj0y.net/blog/redteaming/a-case-study-in-attacking-keepass/

  http://www.harmj0y.net/blog/redteaming/keethief-a-case-study-in-attacking-keepass-part-2/

Pentest
Techniques & outils

Exploiter MS16-032 (élévation de privilèges) en PowerShell depuis Empire

- La procédure : https://warroom.securestate.com/leveraging-ms16-032-powershell-empire/
  - L'exploit : https://www.exploit-db.com/exploits/39719/

Contourner l'UAC sous Windows 10

- Uniquement fonctionnel avec une configuration par défaut de l'UAC

  https://github.com/hfiref0x/UACME

  https://astr0baby.wordpress.com/2016/06/26/windows-10-uac-bypass-with-custom-meterpreter-payloads/

Un whitepaper sur l'exploitation des mécanismes de résolution de noms locaux

- NBNS / LLMNR

  https://www.nccgroup.trust/uk/our-research/local-network-compromise-despite-good-patching/?research=Whitepapers

Déchiffrer les mots de passe du navigateur via la clé de recouvrement DPAPI de l'AD

http://fr.slideshare.net/ItaiGrady/protecting-browsers-secrets-in-adomainenvironment

PSAttack v1.2

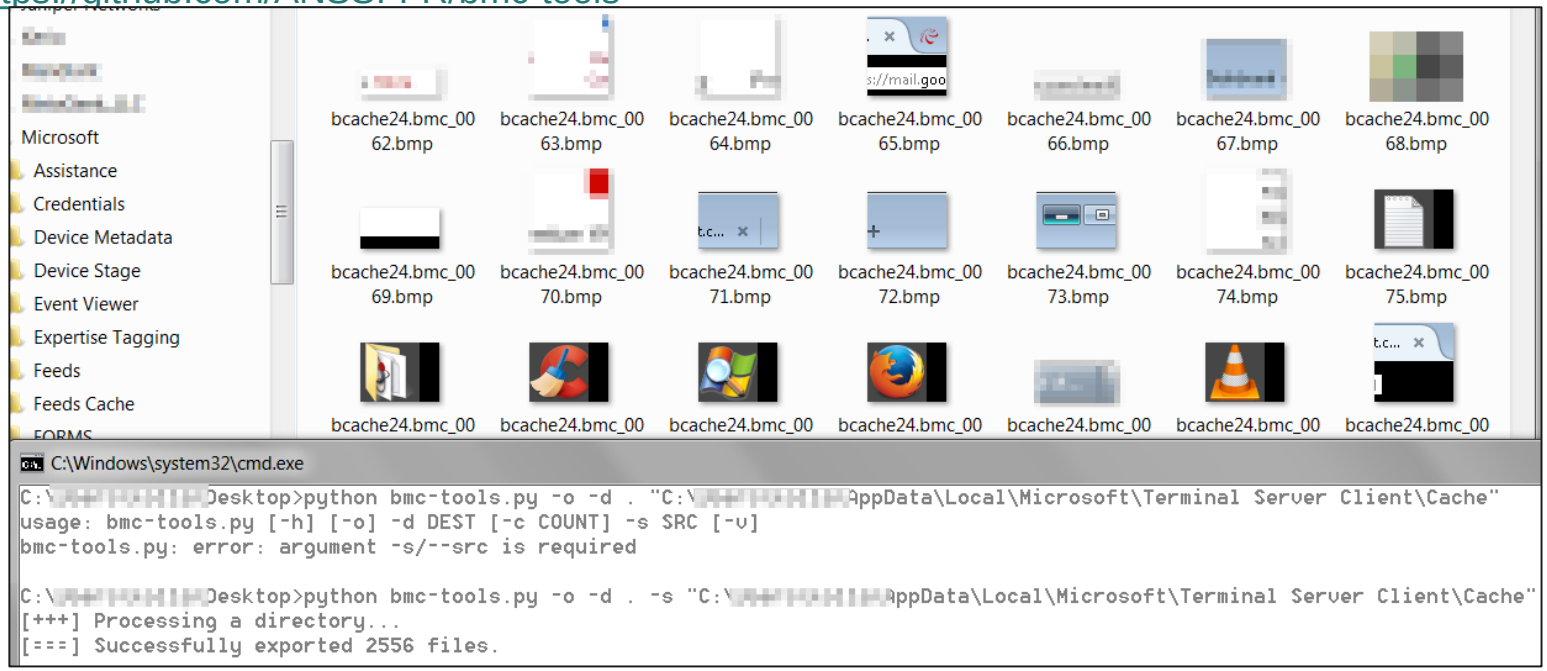
- Outil de post-exploitation intégrant tous les classiques

  https://github.com/jaredhaight/PSAttack/releases/tag/v1.2

BMC Tool de l'ANSSI

- pour extraire le contenu des fichiers cache RDP

https://github.com/ANSSI-FR/bmc-tools



Obfuscation par injection de Jump

https://breakdev.org/x86-shellcode-obfuscation-part-3/

Comprendre le tas (Heap) de Windows 10

https://www.corelan.be/index.php/2016/07/05/windows-10-x86wow64-userland-heap/

Publication de “Control-Flow Enforcement Technology” d’Intel

- Pour bloquer les ROP

  https://blogs.intel.com/evangelists/2016/06/09/intel-release-new-technology-specifications-protect-rop-attacks/
- Mais pas LOP (Loop Oriented Programming)
  - Les gadgets sont ici des fonctions completes

  https://marcoramilli.blogspot.fr/2016/06/from-rop-to-lop-bypassing-control-flow.html

Le NIST publie un guide de durcissement de Mac OS X

http://csrc.nist.gov/publications/drafts/800-179/sp800_179_draft.pdf

Détectez les mouvements latéraux grâce logs d’évènement Windows

- En se concentrant sur les authentications (succès, echec, kerberos, ntlm et attribution de droits d’admin)

  https://t.co/OMT6UBVTFY
- Pensez également à tracer les exécutions de PowerShell “avec” les paramètres

  http://www.redblue.team/2016/01/powershell-traceless-threat-and-how-to.html

Un HIPS en PowerShell et WMI pour protéger son poste

- L'outil permet de détecter :
  - Si quelqu'un stoppe un service
  - Les changement des clefs « RUN » de la base de registre
  - Les processus démarrant de répertoires louches (temp, corbeille…)
  - La création, l'effacement, le renommage de fichiers dans les répertoires système

http://www.cyberforce.be/blog/2016/6/5/building-your-own-host-intrusion-detection-system-with-wmi-and-powershell

Nouveautés (logiciel, langage, protocole...)

Open Source

TinyAntivirus

- Objectif : détecter les virus polymorphes

https://github.com/develbranch/TinyAntivirus

Ayaabu, All Your Antivirus Are Belong to Us

- Simulez l'installation de tous les antivirus

https://github.com/mynameisv/Ayaabu

Revue de "smart contracts"

- Visualiser le control flow d'un contrat solidity

https://github.com/raineorshine/solgraph

Suricata 3.1

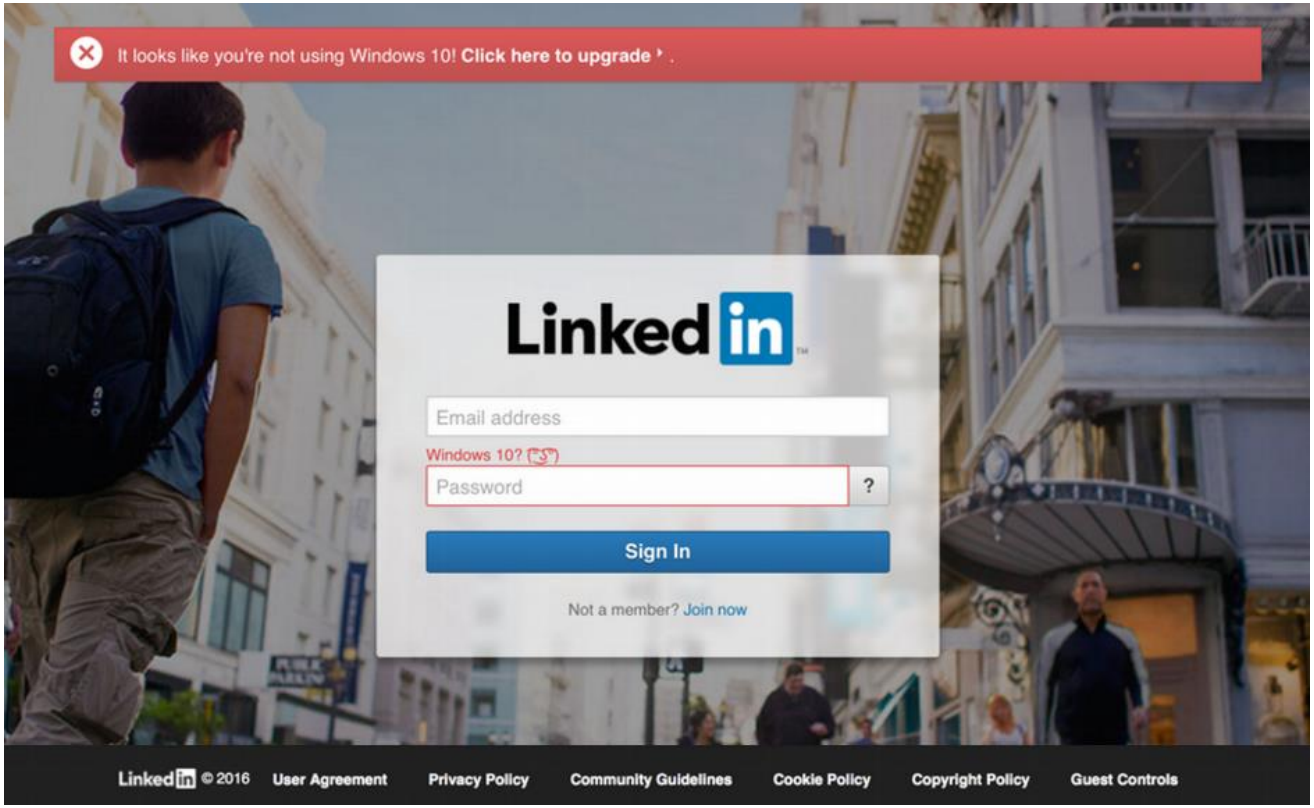
https://suricata-ids.org/2016/06/20/suricata-3-1-released/

Business et Politique

Business
International

Microsoft va acquérir Linkedin pour 26 milliard de dollars

- Linkedin et sa futur page de connexion



Avast achète l'antivirus AVG

- 1,3 milliard de dollars sur la table ont été mis

Business
International

Silent Circle (Blackphone) va mal

- Bataille en justice contre son ancien partenaire espagnol Geeskphone
- Échec commercial du premier Blackphone
- Licenciement de 15% des effectives (20 personnes)

http://www.forbes.com/sites/thomasbrewster/2016/07/06/silent-circle-blackphone-losses-layoffs-geekphone-lawsuit/#29dad58660df

Quelques exemples concrets de problèmes de sûreté sur l'intelligence articificielle

https://openai.com/blog/concrete-ai-safety-problems/

McAfee et Intel, c'est déjà fini ?

http://www.clubic.com/pro/entreprises/mcafee/actualite-810430-intel-chercherait-debarrasser-mcafee.html

Samsung acquière Joyent

- Mainteneur de Node.js et hébergeur Cloud avec SmartOS, sa version d'OpenSolaris

http://www.silicon.fr/samsung-electronics-met-la-main-sur-le-specialiste-du-cloud-joyent-150439.html

Les fuites de données coûteraient en moyenne $4,000,000

- Une équipe de réponse à incident ferait économiser $400,000 

http://www.silicon.fr/fuite-donnees-cout-moyen-4-millions-dollars-ibm-ponemon-150520.html

Droit / Politique

France

Règlement Général sur la Protection des Données

- Il sera adopté en 2018
- Amende jusqu'à 4% du CA ou 20 millions d'euros
- et il va falloir se mettre à jour !

http://www.zdnet.fr/actualites/rgpd-les-entreprises-vont-devoir-massivement-investir-surtout-dans-le-secteur-de-la-sante-39838460.htm

Martine part en vacances en Israël

- Et « aurait » laissé son téléphone sans surveillance
- Téléphone qui tombera en panne quelques jours après
  - Pas de commentaire de l'ANSSI
  - Israël dit ne pas espionner ses amis

http://www.lexpress.fr/actualite/politique/israel-soupconne-d-avoir-espionne-le-telephone-de-manuel-valls_1809369.html

Droit / Politique
International

Sauvez la planète sécurité

- Votez pour que l'Europe paie un pentest à votre logiciel Open Source favoris (1m€ max)
  https://ec.europa.eu/eusurvey/runner/EU-FOSSA-software-choice

Pour la NSA, si vous lisez Linux Journal ou utilisez Tor et Tails Linux…

- Alors vous êtes un extrémiste !

```
$TAILS_terms=word('tails' or 'Amnesiac Incognito Live System') and word('linux'
 or ' USB ' or ' CD ' or 'secure desktop' or ' IRC ' or 'truecrypt' or ' tor ');
 $TAILS_websites=('tails.boum.org/') or ('linuxjournal.com/content/linux*');
```

- Si vous utilisez VeraCrypt… ca va

  http://www.in.techspot.com/news/security/nsa-classifies-li  journal-readers-tor-and-tails-linux-users-as-extremists/articleshow/47743699.cms

Les exigences de la Chine, vis à vis des développeurs d'application

- Une sur deux est légitime, l'autre est là pour espionner :
  1. L'application doit vérifier l'identité de l'utilisateur
  2. Les données de l'utilisateur doivent être protégées
  3. La censure doit être améliorée et punir ceux qui la contournent
  4. Les utilisateurs doivent être informés de leurs droits et des données collectées
  5. Il ne faut pas pirater les concurrents
  6. Il faut enregistrer les activités de l'utilisateur au moins 60 jours

  http://french.people.com.cn/n3/2016/0629/c31357-9078863.html

Droit / Politique

International

Un ex de la CIA chez Tor ?

https://motherboard.vice.com/read/-tor-project-battled-over-hiring-ex-cia-agent-chat-logs-show

Hack the Pentagonn BugBounty par HackerOne

- 1,410 hackers sélectionnés
- 138 vulnérabilités éligibles
- Budget de $150,000 au lieu de $1,000,000 pour un audit équivalent
  - C’est le Uber du pentest

http://www.defense.gov/News/News-Releases/News-Release-View/Article/802929/defense-secretary-ash-carter-releases-hack-the-pentagon-results

Conférences

Conférences

Passées

- SSTIC - 1 au 3 juin 2016 à Rennes
  - Compte rendu… il y’a quelques instants
- BeeRump, des rumps et la bière - 16 juin 2016 à EPITA
  http://www.rump.beer/
- Hack in Paris - 27 juin au 1er juillet 2016 à la Maison de la Chimie
- Nuit du Hack - 2 juillet 2016 chez Mickey

A venir

- BlackHat - 30 juillet au 4 aout 2016 à Las Vegas
- BSides Las Vegas : 2 & 3 août à Las Vegas
- Defcon - 4 au 7 aout à Las Vegas
- Botconf - 30 novembre au 2 décembre 2016 à Lyon

Divers / Trolls velus

Divers / Trolls velus

Quels sont les mots les plus utilisés dans les CVE

- Cela donne presque une phrase : allow remote attackers via arbitrary vulnerability

  http://www.foo.be/cve/

Google My Activity

- Constatez l'ampleur des données collectées

  https://myactivity.google.com/

Autralie, vente aux enchères de 24 518 bitcoins

- Saisis en 2013 par la police et vendus par l'intermédiaire d'Ernst and Young

  http://mashable.france24.com/tech-business/20160628-bitcoins-australie-vente-aux-encheres

Divers / Trolls velus

Récupérer les mots de passe malgrès Credential Guard

- En compromettant UEFI/BIOS
- A partie de 31min, démo à 33min50 et il faut arrêter avant 36min 

http://focus.intelsecurity.com/focus2015/player.html?xml=02-DAY2-SG_SAKW.xml

Collision MD5 avec mimikatz.exe

https://github.com/subTee/MimikatzMD5Collision

Auriez-vous à nouveau votre brevet ?

http://cache.media.eduscol.education.fr/file/DNB/81/2/DNB_2017_Sujet_zero_MathsSciences1_MPCSVT_563812.pdf

Palantir embauche une RedTeam

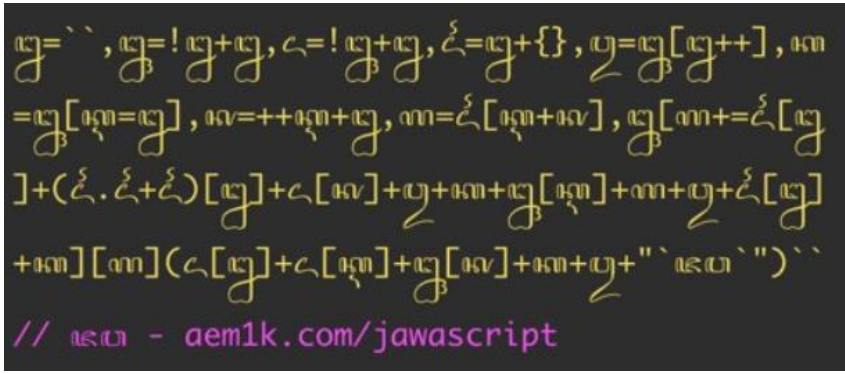
- Et le résultat n'est pas décevant: Contrôle complet du domaine, à partir d'un spear-phishing

https://www.buzzfeed.com/williamalden/how-hired-hackers-got-complete-control-of-palantir

Divers / Trolls velus

Javascript et Unicode…

https://twitter.com/aemkei/status/751905848725737472



Comment Google Zero fait du Fuzzing sur Windows

https://googleprojectzero.blogspot.fr/2016/07/a-year-of-windows-kernel-font-fuzzing-2.html

La Corée du Nord « aurait » une armée de 6 000 hackers

- Gagnant (volant) $866 millions par an

https://thestack.com/security/2016/07/08/6000-strong-north-korean-hacker-army-collects-866-million-per-year

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 13 septembre 2016

After Work

- Fin octobre

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous

Bonnes Vacances