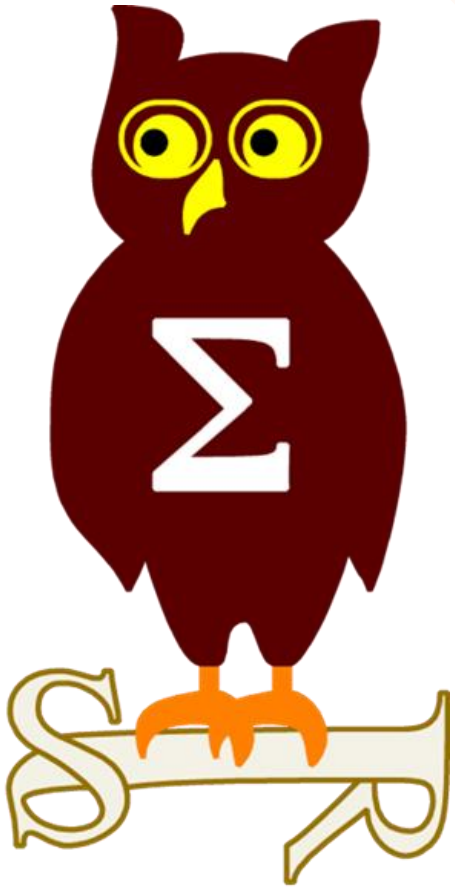
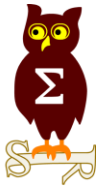


Revue d'actualité

10/05/2016

Préparée par

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



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-037 Cumulative Security Update for Internet Explorer (6 CVE) [Exploitabilité 1,1,2,1,1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3139929, KB3140745, KB3140768
- Exploit:
  - 5 x Corruptions de mémoire aboutissant à une exécution de code
  - 1 x exécution de code au chargement d'une librairie
- Crédits:
  - B6BEB4D5E828CF0CCB47BB24AAC22515 par ZDI (CVE-2016-0159)
  - Henry Li (zenhumany) de Trend Micro par ZDI (CVE-2016-0166)
  - Ladislav Janko par ESET (CVE-2016-0162)
  - Liu Long de Qihoo 360 Vulcan Team (CVE-2016-0154)
  - Sandro Poppi (CVE-2016-0160)
  - Zheng Huang de Baidu Security Lab (CVE-2016-0164)

MS16-038 Cumulative Security Update for Microsoft Edge (6 CVE) [Exploitabilité 1,1,1,1,1,3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3140745, KB3140768
- Exploit:
  - 4 x Corruptions de mémoire aboutissant à une exécution de code
  - 2 x XSS contournement des politiques anti-XSS
- Crédits:
  - Liu Long de Qihoo 360 (CVE-2016-0154, CVE-2016-0155, CVE-2016-0156)
  - QianWen Xiang de Tencent QQBrowser (CVE-2016-0161)
  - Shi Ji (@Puzzor) de VARAS@IIE (CVE-2016-0156)
  - d81b2a7b317c035a8da11d63122964c2 par ZDI (CVE-2016-0157)
  - lokihardt par ZDI (CVE-2016-0158)

Dont 1 commune avec IE:

- CVE-2016-0154

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-039 Vulnérabilités noyau Win32k et GDI32 (4 CVE) [Exploitabilité 1,1,0,0]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3085612, KB3085616...
- Exploit:
  - 1 x Exécutions de code
  - 3 x Elévations de privilèges
    - Exploité dans la nature
- Crédits:
  - Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2016-0167)
  - Kaspersky Lab (CVE-2016-0165)
  - Mateusz Jurczyk de Google Project Zero (CVE-2016-0145)
  - Nils Sommer de bytegeist par Google Project Zero (CVE-2016-0143)
  - Richard Shupak (----------)

MS16-040 Vulnérabilité dans MSXML (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB2993958, KB3046482, KB3140768
- Exploit:
  - Exécution de code lors du traitement de contenu XML
- Crédits:
  - Nicolas Grégoire de Agarri (CVE-2016-0147)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-041 Vulnérabilités dans .NET (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3139929, KB3140745, KB3140768
- Exploit:
  - Exécution de code
- Crédits:
  - Yorick Koster de Securify B.V. (CVE-2016-0148)
  - rgod par Trend Micro's Zero Day Initiative (CVE-2016-0148)

MS16-042 Vulnérabilités dans Microsoft Office (4 CVE) [Exploitabilité 1,2,1,1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3114401, KB3114432...
- Exploit:
  - Exécution de code
- Crédits:
  - Lucas Leong de Trend Micro (CVE-2016-0127)
  - Steven Seeley de Source Incite (CVE-2016-0139)
  - Steven Seeley de Source Incite par VeriSign iDefense Labs (CVE-2016-0136)
  - Sébastien Morin de COSIG (CVE-2016-0122)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-044 Vulnérabilités pour Windows OLE (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3072633, KB3140410
- Exploit:
  - Exécution de code
- Crédits:
  - Debasish Mandal de Intel Security IPS Vulnerability Research Team (CVE-2016-0153)

MS16-045 Vulnérabilités dans Windows Hyper-V (3 CVE) [Exploitabilité 3,3,3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3087088, KB3140745
- Exploit:
  - Exécution de code
- Crédits:
  - Kostya Kortchinsky de Google Security Team (CVE-2016-0088, CVE-2016-0089, CVE-2016-0090)
  - Thomas Garnier (CVE-2016-0088, CVE-2016-0089, CVE-2016-0090)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-046 Vulnérabilités dans le service d'ouverture de session secondaire (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3140745, KB3140768
- Exploit:
  - Élévation de privilège
- Crédits:
  - Tenable Network Security (CVE-2016-0135)

MS16-047 Vulnérabilités dans SAM et le protocole distant LSAD (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3050514, KB3050514, KB3072595, KB3101246, KB3101246, KB3121918, KB3121918, KB3140745, KB3140768
- Exploit:
  - Élévation de privilège
- Crédits:
  - This vulnerability was discovered et researched by Stefan Metzmacher de SAMBA+ et the Samba Team, which also helped design a fix for the problem.For more information about the vulnerability named "BADLOCK," see Badlock Bug. (CVE-2016-0128)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-048 Vulnérabilités dans CSRSS (1 CVE) [Exploitabilité 2]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3023266, KB3121212, KB3140745, KB3140768
- Exploit:
  - Security Feature Bypass
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2016-0151)

MS16-049 Vulnérabilité dans HTTP.sys (1 CVE) [Exploitabilité 3]

- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3050514, KB3050514, KB3072595, KB3101246, KB3101246, KB3121918, KB3121918, KB3140745, KB3140768
- Exploit:
  - Déni de service
- Crédits:
  - Dhanesh Kizhakkinan de FireEye, Inc. (CVE-2016-0150)
  - Noam Mazor de Imperva (CVE-2016-0150)

Failles / Bulletins / Advisories

Microsoft - Avis

MS16-050 Vulnérabilités dans Adobe Flash Player (0 CVE) [Exploitabilité]

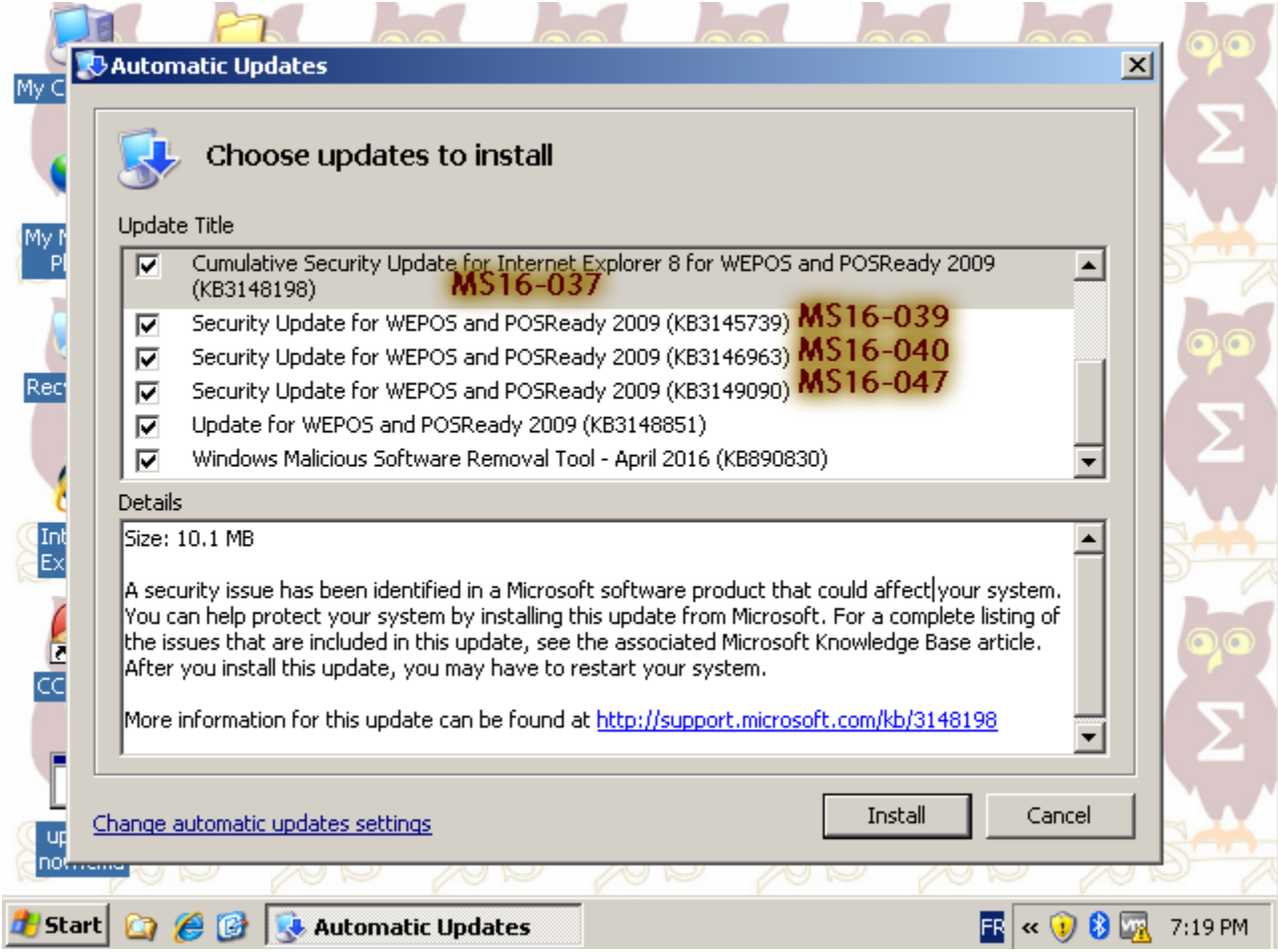
- Affecte:
  - Windows (toutes versions supportes)
  - Remplace KB3144756
- Exploit:
  - Exécution de code
- Crédits:
  - ?

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 - Autre

Hyperviseur Hyper-V

- 3x Évasions de la machine virtuelle et exécution de code sur l'hyperviseur
  https://bugs.chromium.org/p/project-zero/issues/detail?id=688
  https://bugs.chromium.org/p/project-zero/issues/detail?id=689
  https://bugs.chromium.org/p/project-zero/issues/detail?id=690
- Cela donne à réfléchir quand on voit l'importance d'Azure

Failles / Bulletins / Advisories

Système (principales failles)

Badlock, execution de code à distance sur Samba

- Encore de la com' :
  - ✔ Un nom : Badlock
  - ✔ Un site web http://badlock.org/
  - ✔ Un logo

- Annonce sans détails, fortement critiquée par la communauté
  - Tous les détails seront donnés le 12 avril ?

http://malwarejake.blogspot.fr/2016/03/badlock-what-you-need-to-know-today.html

- Au final :
  - Possibilités de MitM sur Windows (sauf si la signature SMB est activée)
  - Déni de service sur Linux
  - Score CVSS de 7.1
  - Correctifs pour Windows dans le bulletin MS16-047
    https://technet.microsoft.com/library/security/MS16-047

Failles / Bulletins / Advisories

Voiture connectées

Les risques liés aux ports de diagnostique ODBII

Projet de recherche de l'ICS-CERT

- *Insecure firmware updates and downloads*
- *Hardcoded or non-existent Bluetooth PINs*
- *Weak WPA2 passwords*
- *Hardcoded credentials*
- *An Internet-enabled administrative interface*

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=453871

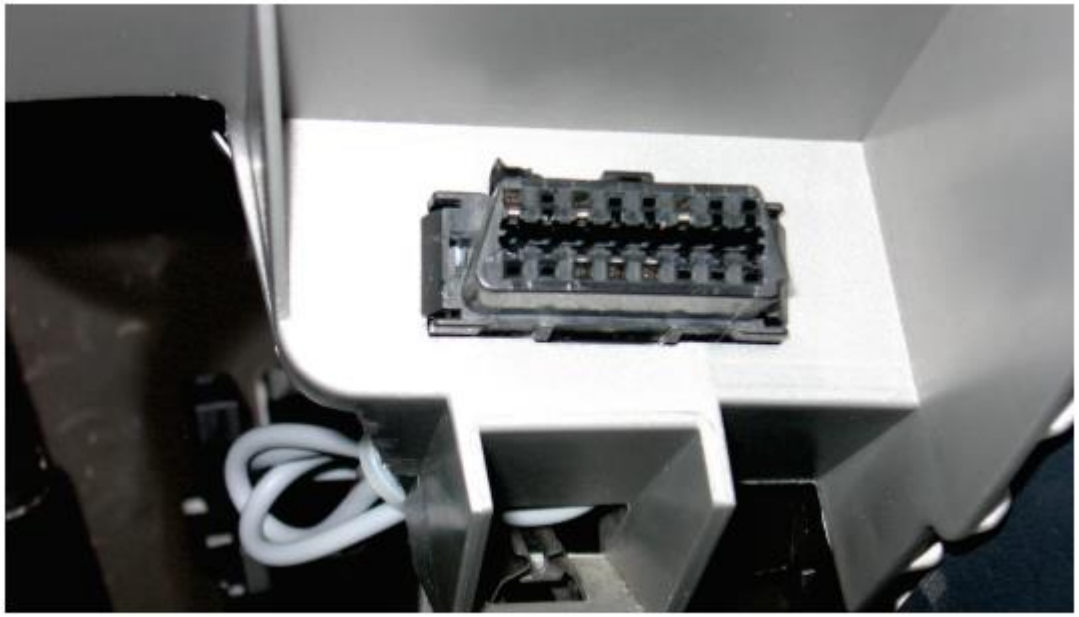


Figure 1: OBD-II Connector (Image courtesy Wikipedia/Michiel1972.)

Failles / Bulletins / Advisories

Apple

Quicktime, vulnérable à des executions de code à distance

- Abandonné sous Windows, donc vulnérable à jamais

- La défense américaine recommande de le désinstaller
  https://www.us-cert.gov/ncas/alerts/TA16-105A

Failles / Bulletins / Advisories

Google

Bulletins de sécurité Android pour le mois de mai 2016

Issue	CVE	Severity	Affects Nexus?
Remote Code Execution Vulnerability in Mediaserver	CVE-2016-2428 CVE-2016-2429	Critical	Yes
Elevation of Privilege Vulnerability in Debuggerd	CVE-2016-2430	Critical	Yes
Elevation of Privilege Vulnerability in Qualcomm TrustZone	CVE-2016-2431 CVE-2016-2432	Critical	Yes
Elevation of Privilege Vulnerability in Qualcomm Wi-Fi Driver	CVE-2015-0569 CVE-2015-0570	Critical	Yes
Elevation of Privilege Vulnerability in NVIDIA Video Driver	CVE-2016-2434 CVE-2016-2435 CVE-2016-2436 CVE-2016-2437	Critical	Yes
Elevation of Privilege Vulnerability in Kernel	CVE-2015-1805	Critical	Yes
Remote Code Execution Vulnerability in Kernel	CVE-2016-2438	High	Yes
Information Disclosure Vulnerability in Qualcomm Tethering Controller	CVE-2016-2060	High	No
Remote Code Execution in Bluetooth	CVE-2016-2439	High	Yes

Et bien d'autres !

Sondage : qui a eu un patch ?

https://source.android.com/security/bulletin/2016-05-01.html

Failles / Bulletins / Advisories

Divers

Image Tragick

Vulnérabilités dans la bibliothèque de manipulation d'image ImageMagick

- Exécution de code via le nom du fichier lors de l'appel à une fonction externe
- SSRF
- Modification / suppression de fichiers locaux
- Lecture de fichiers locaux

file_read.mvg

```
push graphic-context
viewbox 0 0 640 480
image over 0,0 0,0 'label:@/etc/passwd'
pop graphic-context
```

```
$ convert file_read.mvg out.png
```

produces file with text rendered from /etc/passwd

http://www.openwall.com/lists/oss-security/2016/05/03/18
https://imagetragick.com/

Failles / Bulletins / Advisories

Divers

Controverses au sujet du rapport DBIR de Verizon

- Censé contenir des informations et statistiques sur les attaques de par le monde
- Il semblerait que les statistiques soient en fait basée sur
  - Des scans de vulnérabilités
  - Des logs de sondes IDS
  - ➔ Aucune réalité refletée dans ces statistiques

1. 2015-03-05 – CVE-2015-1637 – Microsoft Windows Secure Channel (Schannel) RSA Temporary Key Handling EXPORT_RSA Ciphers Downgrade MitM (FREAK)
2. 2015-01-06 – CVE-2015-0204 – OpenSSL RSA Temporary Key Handling EXPORT_RSA Ciphers Downgrade MitM (FREAK)
3. 2012-02-25 – CVE-2012-1054 – Puppet k5login File Symlink File Overwrite Local Privilege Escalation
4. 2011-07-19 – CVE-2011-0877 – Oracle Enterprise Manager Grid Control Instance Management Unspecified Remote Issue (2011-0877)
5. 2004-02-10 – CVE-2003-0818 – Microsoft Windows ASN.1 Library (MSASN1.DLL) BER Encoding Handling Remote Integer Overflows
6. 2002-01-15 – CVE-2002-0126 – BlackMoon FTP Server Multiple Command Remote Overflow
7. 2001-12-26 – CVE-2002-0953 – PHPAddress globals.php LangCookie Parameter Remote File Inclusion
8. 2001-12-20 – CVE-2001-0876 – Microsoft Windows Universal Plug and Play NOTIFY Directive URL Handling Remote Overflow
9. 2001-04-13 – CVE-2001-0680 – QVT/Net / Term FTP Server LIST Command Traversal Remote File Access
10. 1999-11-22 – CVE-1999-1058 – Vermillion FTPD Long CWD Command Handling Remote Overflow DoS

TOP10 des vulnérabilités selon le rapport Verizon DBIR 2016

http://blog.erratasec.com/2016/05/freaking-out-over-dbir.html#.VzB8ZYSLSCo

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Analyse d'un malware lié au piratage d'une banque au Bangladesh

- Surveillance des connexions, des transactions
- Modification des confirmation de transactions imprimées

http://baesystemsai.blogspot.fr/2016/04/two-bytes-to-951m.html

Possible compromission de Jenkins

- Pas de modification des binaires

https://jenkins.io/blog/2016/04/22/possible-infra-compromise/

Bug Bounty Facebook : il découvre d'autres attaquants

- Focus sur une appliance de transfert de fichier : SQLi pre-auth
- Découvertes d'autres webshells

http://devco.re/blog/2016/04/21/how-I-hacked-facebook-and-found-someones-backdoor-script-eng-ver/

Piratages, Malwares, spam, fraudes et DDoS

Scada

Vulnérabilité dans des compteurs électriques intelligents

- Absence d'authentification sur l'interface web, stockage en clair des mots de passe

https://ics-cert.us-cert.gov/advisories/ICSA-16-105-02

Vulnérabilité dans un utilitaire de création d'interface web

- On retrouve tout le TOP10 de l'OWASP

https://ics-cert.us-cert.gov/advisories/ICSA-16-105-03

Vulnérabilité liée à glibc dazns certains produits Siemens

https://ics-cert.us-cert.gov/advisories/ICSA-16-103-01

Piratages, Malwares, spam, fraudes et DDoS

Internet des Objets

Piratage de capteurs de trafic routier

https://www.rsaconference.com/writable/presentations/file_upload/tech-t09-smart-megalopolises.-how-safe-and-reliable-is-your-data.pdf

https://securelist.com/blog/research/74454/how-to-trick-traffic-sensors/

Des modems câble vulnérables

Absence d'authentification sur l'interface d'administration, CSRF

Facilement exploitable, la victime visite un site web et le routeur *reboot*

http://www.securityforrealpeople.com/2016/04/arris-motorola-surfboard-modem.html

Un malware présent sur des webcams achetées sur Amazon

http://artfulhacker.com/post/142519805054/beware-even-things-on-amazon-come

Prise connectée, application Android malveillante

Envoi de SMS surtaxés

http://www.new-deal.com/support-fr/

https://play.google.com/store/apps/details?id=com.ruiqu.slwifi.plug.other

Piratages, Malwares, spam, fraudes et DDoS

Sites Piratés

Francs maçons : vol de 3Go de données de la Grande Loge de France

- Spear Phishing ?
- Vol des identifiants de leur Cloud et publication de documents internes et du Cloud
- L'auteur des faits ne dissimule même pas son identité !!?

  http://stopmensonges.com/franc-maconnerie-papers-la-grande-fuite-de-lhistoire-6000-documents-secrets-divulgues/

Vulnérabilité RCE sur le site uber.com

- Divulguée via le programme HackerOne

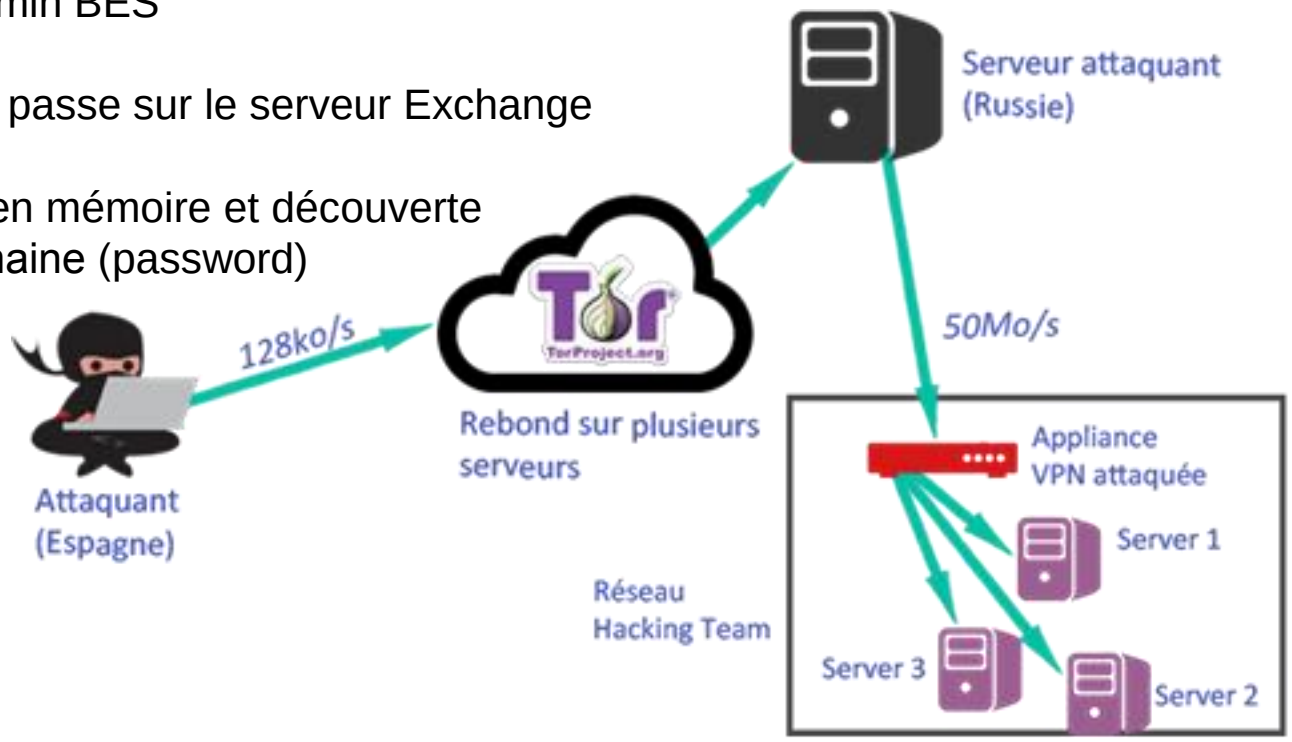
https://hackerone.com/reports/125980

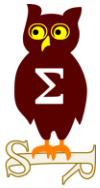
Piratages, Malwares, spam, fraudes et DDoS

Hacking Hacking Team

Compte-rendu complet de l'attaque, par l'attaquant
http://pastebin.com/raw/0SNSvyjJ

- 0day sur l'appliance VPN
- Accès sans authentification à une base MongoDB
- Accès sans authentification au SAN en iscsi
- Accès au mot de passe admin BES
- Connexion avec ce mot de passe sur le serveur Exchange
- Dump des mots de passe en mémoire et découverte d'un compte admin de domaine (password)





Nouveautés, outils et techniques

Crypto

Divers

Analyse du PRNG d'OpenSSL

https://eprint.iacr.org/2016/367.pdf

Pentest

Techniques & outils

Par où démarrer l'audit d'applications Android
http://blog.ostorlab.co/2016/05/first-better-steps-pentesting-android.html?utm_content=buffer06ae8&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

Visualiser les organigrammes métier à partir de l'Active Directory
https://labs.mwrinfosecurity.com/blog/visualising-organisational-charts-from-active-directory/

Analyse de firmware sur routeur
http://jcjc-dev.com/2016/04/29/reversing-huawei-router-2-scouting-firmware/

Créer une AC, l'ajouter à la cible, déployer un binaire signé
https://labs.mwrinfosecurity.com/blog/masquerading-as-a-windows-system-binary-using-digital-signatures/
https://github.com/stufus/certerator

Retrouver le mot de passe du compte PATROL
http://www.contextis.com/resources/blog/subverting-agent-network-patrol/

Scada

Divers

Rétro-ingenierie de protocoles radio SCADA
http://www.securitytube.net/video/15705

Nouveautés (logiciel, langage, protocole...)

Open Source

Améliorations des performances des VM Windows

- Par la suppression des fonctionnalités gourmandes en grpahique et accès disque

https://github.com/artemdinaburg/optimizevm

Reconstruction de flux vidéo RDP à partir du trafic réseau (pcap)

http://www.contextis.com/resources/blog/rdp-replay/

Fermeture de la base de vulnérabilité OSVDB

https://blog.osvdb.org/2016/04/05/osvdb-fin/

Nouveautés (logiciel, langage, protocole...)

Divers

Google détaille son apporche de la sécurité, qui s'éloigne de la sécurité périmétrique
http://research.google.com/pubs/pub43231.html

Conférences

Conférences

Texte en gris = déjà traité précédemment

Passées

- JSSI 2016 - 8 mars 2016 à Paris
  http://www.leparisien.fr/transports/sncf-et-ratp-des-greves-se-profilent-pour-le-9-mars-26-02-2016-5579575.php
- Insomni'Hack - 17 et 18 mars 2016 à Genève
- STHACK – 08 avril 2016 à Bordeaux

A venir

- SSTIC - 1 au 3 juin 2016 à Rennes
- Hack in Paris - 27 juin au 1er juillet 2016 chez Mickey
- Nuit du Hack - 2 juillet 2016 chez Mickey
- RMLL Sécurité – 4 au 6 juillet à Paris

  https://sec2016.rmll.info/programme/

Prochains rendez-vous de l’OSSIR

Prochaine réunion

- Mardi 14 juin 2016

After Work

- Lundi 30 mai ou Mardi 31 mai 2016 (à confirmer, décalage du fait de la conférence SSTIC).

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous