Revue d'actualité

10/06/2014

Préparée par

Jean-Philippe GAULIER
Ary KOKOS
Vladimir KOLLA
Arnaud SOULLIE

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2014

MS14-021 Vulnérabilité dans Internet Explorer (1 CVE) [Exploitabilité 1]

- Distribué "hors bande" en Mars (Cf. Revue d'avril 2014)

MS14-022 Vulnérabilités dans SharePoint (3 CVE) [Exploitabilité 1,3]

- Affecte:
  - Microsoft SharePoint Server toutes versions supportées (Designer, Web Apps, Foundation et Server en 2007, 2010, 2013)
- Exploit:
  - Corruptions de mémoire aboutissant à une exécution de code à distance pour un utilisateur authentifié et uploadant du contenu spécialement formaté
  - XSS
- Crédits: ?

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2014

MS14-023 Vulnérabilités dans Microsoft Office (2 CVE) [Exploitabilité 1]

- Affecte :
  - Microsoft Office (toutes versions supportées)
  - Sauf Office pour Mac 2011 et Word Viewer
- Exploit:
  - DLL Preloading avec celle concernant la correction grammaticale du Chinois simplifié (CVE-2014-1756)
  - Divulgation (entre autre) du token d'accès aux services en ligne de Microsoft lors de l'ouverture d'un fichier office spécialement formaté et hébergé sur un site malicieux (CVE-2014-1808)
- Crédits:
  - NSFOCUS Security Team (CVE-2014-1756)
  - Arnaud Maillet de l'ANSSI (CVE-2014-1808)

MS14-024 Vulnérabilités dans Microsoft Common Control (1 CVE) [Exploitabilité ?]

- Affecte:
  - Microsoft Office (toutes versions supportées)
  - Sauf Office pour Mac 2011
- Exploit:
  - Mauvaise implémentation du hasard de l'espace mémoire (ASLR / Address Space Layout Randomization) dans la bibliothèque MSCOMCTL.
  - Utilisé dans la nature, cumulée avec des failles comme la CVE-2014-1761 de Mars (Fichiers RTF)
  - http://blogs.technet.com/b/srd/archive/2014/05/13/assessing-risk-for-the-may-2014-security-updates.aspx
- Crédits: ?

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2014

MS14-025 Vulnérabilités dans les Group Policy Preferences (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows Server toutes versions supportées hormis 2003 et Server Core
  - Windows Vista, 7 et 8.1 si "Remote Server Administration Tools" est installé
- Exploit:
  - Possibilité de configurer (entre autre) le mot de passe de l'admin local par des GPO avec les Group Policy Preferences (GPP)
    - Mot de passe dans un XML, accessible à tous \\mon-ad\SYSVOL\mon-domaine\Policies\{uid}\Machine\Preferences\Groups\Groups.xml
    - Chiffré en AES avec une clef publique ;-)
    - http://pastebin.com/TE3fvhEh
    - MetaSploit http://www.rapid7.com/db/modules/post/windows/gather/credentials/gpp
  - Suppression de la possibilité mais uniquement pour les nouveaux comptes
    - "Microsoft is not automatically disabling these Group Policies because we do not want to disrupt existing environments which rely on this feature."*
  - Fourniture fourni d'un script PowerShell pour assurer un changement "sûr" de mot de passe
- Crédits:
  - Selon Microsoft : aucun
  - Selon le reste du monde : en 2012, Emilien Girault / Sogeti
    - à présent à l'ANSSI

http://esec-pentest.sogeti.com/exploiting-windows-2008-group-policy-preferences (Nécéssite un compte)

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2014

MS14-026 Vulnérabilités dans .NET (1 CVE) [Exploitabilité 1]

- Affecte:
  - .NET Framework (toutes versions supportées)
  - Sauf .NET 3.0 SP2, .NET 3.5 SP1, .NET 4.5.2, Windows Server 2008 SP2 Core
- Exploit:
  - Elévation des privilèges si la fonctionnalité .NET "Remoting" est activée (accès à des objets d'autres processus sur le même ordinateur ou sur le réseau) et si elle effectue de la désérialisation (option TypeFilterLevel)
- Crédits:
  - James Forshaw / Context Information Security (CVE-2014-1806)

MS14-027 Vulnérabilités dans l'API ShellExecute (1 CVE) [Exploitabilité 1]

- Affecte:
  - Windows toutes versions supportées
  - Correctif pour Windows XP Embedded POSReady (cf. slide suivant) 
- Exploit:
  - Exploit: Elévation de privilèges locale
  - Technique utilisée par de nombreux malwares (Famille Taterf) qui enregistrent leurs propres extentions (HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks)
- Crédits: ?

Failles / Bulletins / Advisories

Microsoft - Avis Mai 2014

MS14-028 Vulnérabilité iSCSI (2 CVE) [Exploitabilité 3]

- Affecte:
  - Windows Storage Server 2008 et R2, Windows Server 2012 et R2, Server Core
  - Pas de correctif pour Windows Storage Server 2008 car techniquement trop complexe
- Exploit:
  - Déni de service dû à une erreur de traitement de paquets iSCSI spécialement formatés
- Crédits:
  - Pawel Wylecial / Beyond Security's SecuriTeam Secure Disclosure (CVE-2014-0255 et CVE-2014-0256)

MS14-029 Vulnérabilité dans Internet Explorer (2 CVE) [Exploitabilité 1]

- Affecte:
  - Internet Explorer toutes versions supportées sauf Server Core
  - Correctif pour Windows XP Embedded POSReady (cf. slide suivant) 
    - Un “diff” permet d’obtenir une 0-day pour Windows XP “normal”
- Exploit:
  - Corruption de mémoire aboutissant à une exécution de code à l'ouverture d'une page Web spécialement formatée
- Crédits:
  - Fermin J. Serna / Google Security Team (CVE-2014-0310)
  - Anonymous / ZDI (CVE-2014-0310)
  - Clément Lecigne / Google Security Team "Suisse" (CVE-2014-1815)
    - Il y'a quelques mois, a recu $10k d'un Bug Bounty Facebook+Microsoft pour une vulnérabilité dans Flash Payer et a tout reversé à l'association Hackers for Charity.

Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Mai 2014

2871997

- V1.0 L'anti-Mimikatz (ou pas)
  - Un compte local ne peut plus accéder à un système distant avec un hash
    - Mais cela marche toujours pour le compte administrator (SID=500)
  - Fin de la persistance en mémoire des mots de passe RDP en clair
    - après cloture de la session RDP
    - 30 secondes après la cloture (TokenLeakDetectDelaySecs)
    - uniquement si l'utilisateur s'est "proprement" déloggué, sans juste fermer la fenêtre…
      - comme dans 99% des cas ;-)
- Suite aux moqueries, Microsoft publie plus de détails

  http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx
  - Protected Users group
    - Authentification Kerberos obligatoire
    - Plus de cache du mot de passe à partir de Windows 8
    - Chiffrement basé sur AES et non plus DES ou RC4
  - Restricted Admin RDP mode
    - network netlogon, plus de transmission de mot de passe
  - LSA Credential Cleanup
    - cf. plus haut

Failles / Bulletins / Advisories

Microsoft - Advisories et Revisions Mai 2014

2755801

- V24.0 Mise à jour du plugin Flash Player pour Internet Explorer

MS14-029

- V1.2 Changement de détection

Failles / Bulletins / Advisories

Microsoft - Autre

Ecrire dans c:\, vulnérabilité ou fonctionnalité ?

- Répertoire + ADS = fichier
  - Un utilisateur à faible pouvoir ne peut que créer des répertoires dans c:\
  - Il est possible d'écrire dans un ADS dans un répertoire
    - Cela marche aussi avec c:\Windows\system32\tasks

http://seclists.org/fulldisclosure/2014/May/92

http://tyranidslair.blogspot.co.uk/2014/05/abusive-directory-syndrome.html

Fin du support Windows 8.1, le 10 juin prochain

https://isc.sans.edu/diary/This+is+not+a+testtypo%3A+Support+for+Windows+8.1+Ends+in+a+month!/18087

- Pour forcer à migrer « gratuitement » vers Windows 8.1 Update 1

http://blogs.technet.com/b/gladiatormsft/archive/2014/04/12/information-regarding-the-latest-update-for-windows-8-1.aspx

- Si vous disposez de WSUS, vous avez 120 jours
  - Quelle clémence mon seigneur !!!

http://blogs.windows.com/windows/b/springboard/archive/2014/04/16/windows-8-1-update-and-wsus-availability-and-adjusted-timeline.aspx

Failles / Bulletins / Advisories

Microsoft - Autre

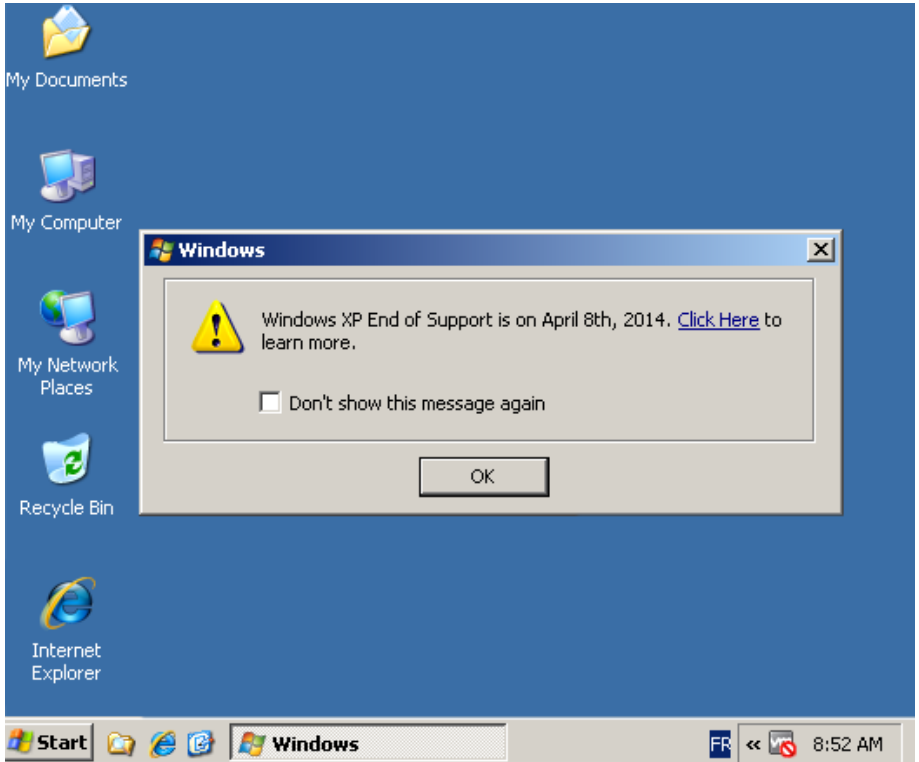
Continuer de mettre à jour Windows XP

- En le faisant passer pour Windows Embedded POSReady 2009
  - Version basée sur Windows XP SP3 dédiée aux machines industrielles, distributeurs de billets…

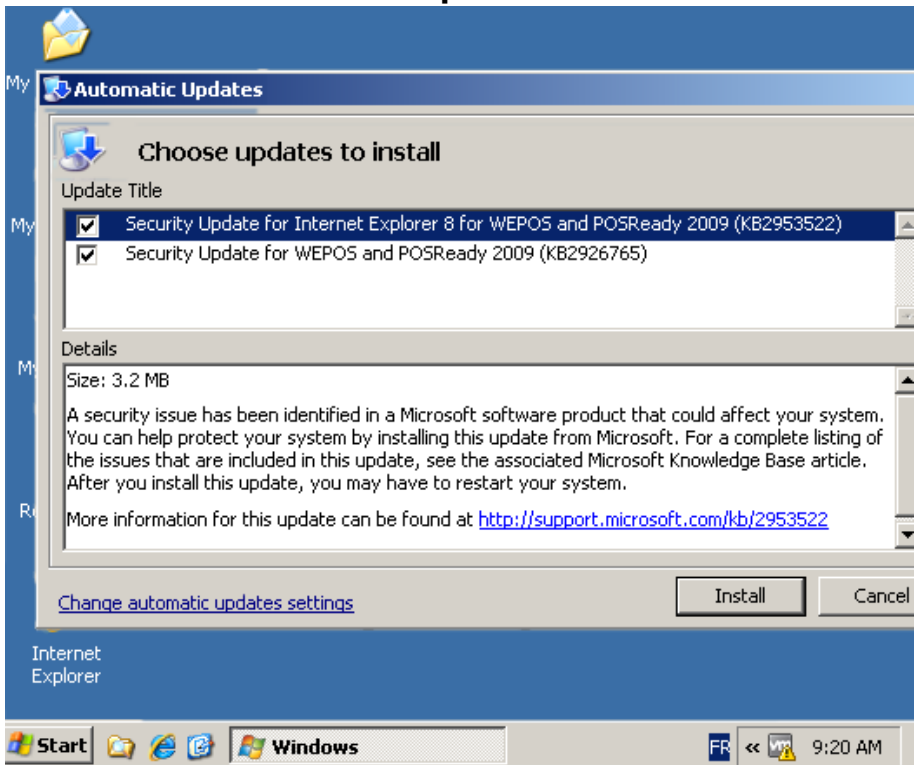
    http://www.ghacks.net/2014/05/24/get-security-updates-windows-xp-april-2019/
  - Mais Microsoft n'en est pas très content ;-)

    http://www.theguardian.com/technology/2014/may/27/microsoft-windows-xp-security-hack-update
  - Un "diff" de chaque nouveau bulletin permettra d'obtenir une 0-day pour Windows XP

Avant



Après



Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco

- Nexus
  - Prise de contrôle totale du système à distance ("Smart Call Home" + serveur SMTP)
  - Déni de service
  - ...

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140521-nxos

- IOS
  - Déni de service par l'envoi de messages RTCP (Real-Time Control Protocol)

  http://software.cisco.com/download/navigator.html?mdfid=281458045

Checkpoint

- Firewall >= R75.40
  - Déni de service à distance, "peut-être" lors de traitements sur SSL (sans plus de détails)
  - Fait rare : beaucoup de clients ont été contacté directement par Checkpoint
    - Cela doit donc sentir très mauvais **;-)**

https://supportcontent.checkpoint.com/solutions?id=sk100431

Failles / Bulletins / Advisories

Autre (principales failles)

VMWare

- vCenter
  - Contournement du CHROOT à distance pour un utilisateur authentifié

  http://www.zerodayinitiative.com/advisories/ZDI-14-159/
- VMware Workstation, Player, Fusion (pour Mac) et ESXi
  - "Null déréférencement" aboutissant à une élévation de privilèges dans la machine virtuelle

  https://www.vmware.com/security/advisories/VMSA-2014-0005.html

Oracle

- MySQL
  - Plusieurs CVE dont une éxecution de code à distance pour un utilisateur non authentifié (CVE-2014-2440)

  http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html#AppendixMSQL
- Java
  - Plusieurs vulnérabilités dont une éxecution de code à distance sur Java SE, Java SE Embedded et JRockit.

  http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html#AppendixJAVA

Google

- Chrome 34.0.1847
  - “Use-after-free” et execution de code lors de l'utilisation des WebSockets.

  http://googlechromereleases.blogspot.com/2014/05/stable-channel-update.html

Failles / Bulletins / Advisories

Autre (principales failles)

Webapps

- All in One SEO Pack plugin (Wordpress)
  - XSS et escalade de privilèges

http://www.theregister.co.uk/2014/06/02/flaws_open_gates_to_wordpress_enmasse_seo_beatdown/

Failles / Bulletins / Advisories

Internet of (insecure) things

Plusieurs vulénrabilités dans les prise intelligentes D-LINK

http://www.devttys0.com/2014/05/hacking-the-d-link-dsp-w215-smart-plug/#more-2103

http://www.devttys0.com/2014/05/hacking-the-dsp-w215-again-again/

http://www.devttys0.com/2014/05/hacking-the-dspw215-again/

Des failles dans un appareil photo intelligent

http://op-co.de/blog/posts/hacking_the_nx300/

Failles / Bulletins / Advisories

Divers

Serait-on en train de « re-découvrir » les fonctionnalités de SNMP !!?

- SNMP exposé sur Internet = Fuite d'informations sensibles

  https://community.rapid7.com/community/metasploit/blog/2014/05/12/r7-2014-01-r7-2014-02-r7-2014-03-disclosures-exposure-of-critical-information-via-snmp-public-community-string

- SNMP exposé sur Internet = DDoS par reflexion

  http://news.techworld.com/security/3521487/ddos-attacks-using-snmp-amplification-on-the-rise

  - A quand la découverte de la possibilité de configurer des équipemens par SNMP ? ;-)

Contourner l'authentification 2-facteurs de Google, Facebook et autres

- La plupart des sites grand public permettent de recevoir un OTP (One-Time Password)
  - Servant de second facteur d'authentification, par téléphone.
- Niveau de sécurisation faible des boîtes vocales (on se rappelle notamment des scandales anglais de 2009)
  - Un attaquant peut utiliser ce moyen afin de récupérer un OTP valide

  http://shubh.am/how-i-bypassed-2-factor-authentication-on-google-yahoo-linkedin-and-many-others/

Les appareils iOS victimes d'un rançongiciel en Australie

- Verrouillés via la fonction "Find my phone", une rançon de 100$ est demandée
- Pas d'info précise sur les moyens employés par le(s) pirate(s)
  http://www.darkreading.com/mobile/apple-users-fend-off-ransom-attacks-against-iphones-and-macs/d/d-id/1269206

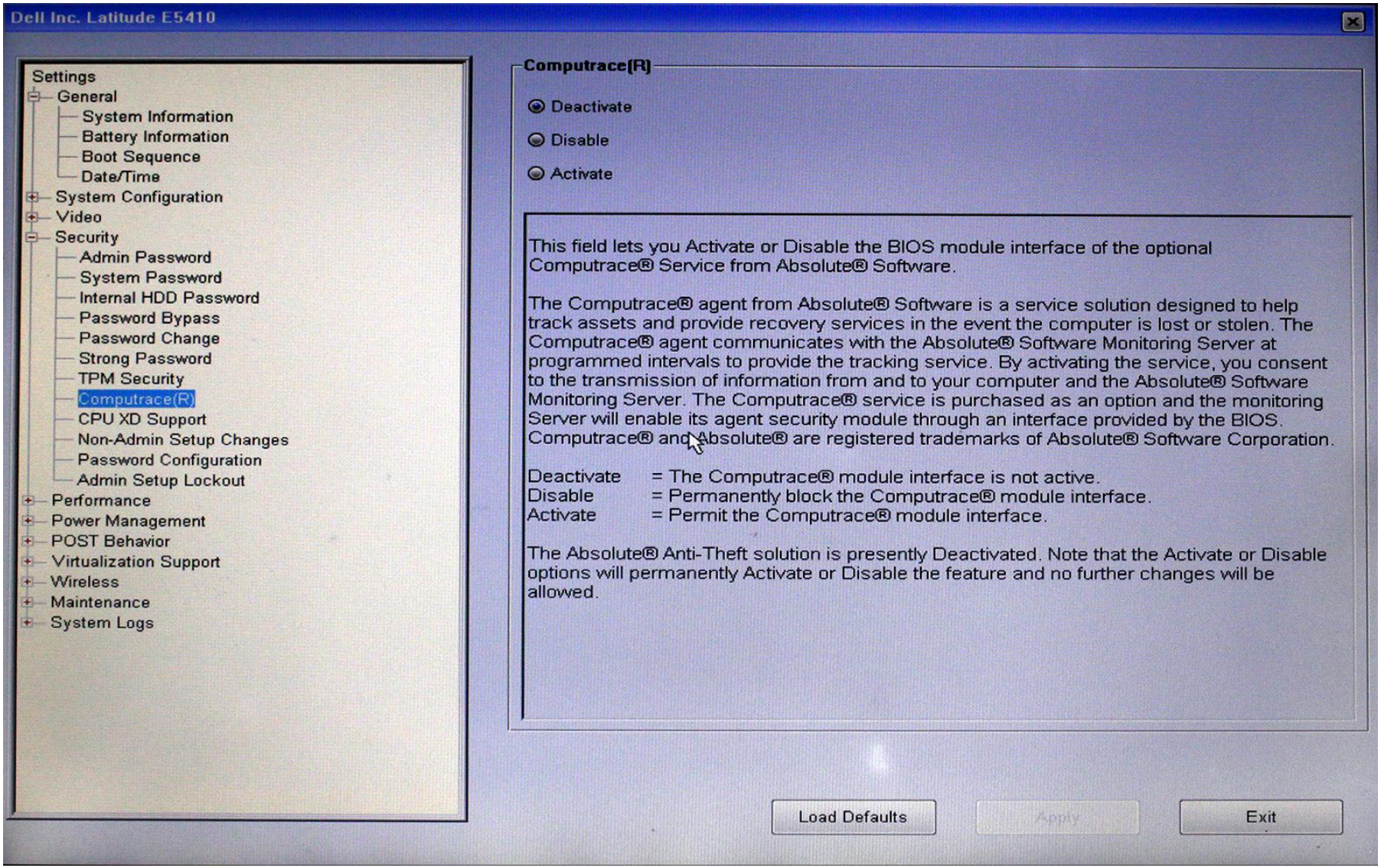
Piratages, Malwares, spam, fraudes et DDoS
Malwares

La Backdoor Absolute Computrace

- Dévouvert par Kaspersky
  - Suite à des plantages répétés d'un PC

    https://www.securelist.com/en/analysis/204792325/Absolute_Computrace_Revisited
- Système de traçabilité antivol
  - Présent dans le BIOS depuis des années
    - Sur la majorité des ordinateurs Acer, Asus, Dell, HP, Lenovo, Toshiba...
  - Activable à distance (c'est mieux pour un système antivol ^_^)
  - Non detecté par les antivirus (idem)
  - Utilise des techniques de malware
    - Injection dans l'OS depuis le BIOS
    - ...en écrasant des outils Microsoft légitimes (autocheck.exe)
    - ...et s'injectant dans des processus comme internet explorer
- Photo sur le slide suivant

La Backdoor Absolute Computrace (suite)



Piratages, Malwares, spam, fraudes et DDoS

Malwares

Nemanja, nouveau malware de terminaux de paiement

- A déjà infecté plus de 1500 GAB / DAB / ATM
- Dans 36 pays différents

http://www.theregister.co.uk/2014/05/27/keylogging_botnet_menaces_retailers/

CryptoDefense, le nouveau “rançongiciel chiffrant”

- Désactive le system restore et efface les shadow copies
  - ~1000€ de rançon

http://labs.bromium.com/2014/05/27/cryptodefense-the-ransomware-games-have-begun/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Récupération du contenu des pages web depuis le GPU

- C'est beau mais irréaliste ;-)

  http://www.ieee-security.org/TC/SP2014/papers/StealingWebpagesRenderedonYourBrowserbyExploitingGPUVulnerabilities.pdf

Android, développer "légitimement" une application qui prend des photos

- A l'insu de l'utilisateur

  http://www.isssource.com/apps-take-photos-with-no-one-knowing/

Exploitation de la faille HeartBleed

- Contre les terminaux Android 4.1, sur un réseau Wifi
  - Cf. Revue d'avril 2014 « Reparlons d'HeartBleed »

  http://www.itespresso.fr/securite-it-heartbleed-menace-android-reseaux-wi-fi-75935.html

Piratages, Malwares, spam, fraudes et DDoS

Sites piratés

eBay : Vol des données personnelles de près de 145 millions de clients

http://www.darkreading.com/attacks-breaches/ebay-database-hacked-with-stolen-employee-credentials-/d/d-id/1269093

http://www.ebayinc.com/in_the_news/story/ebay-inc-ask-ebay-users-change-passwords

- Quelques jours après, diffusion de :
  - XSS, exécution de code à distance, rejeu de sessions…

http://www.undernews.fr/hacking-hacktivisme/ebay-multiples-vulnerabilites-et-piratages-les-clients-encore-en-danger.html

Faille XSS chez Deezer

- 2500 cookies interceptés fin Mai

http://www.undernews.fr/alertes-securite/alerte-securite-faille-xss-persistante-sur-deezer-deja-2500-cookies-interceptes.html

Défacement un site des nouvelles cartes d'identité : suivi-cni.interieur.gouv.fr

- Par un hackeur (d3b~X) ayant utilisé un outil de mass-défacement
  - donc non-ciblé ;-)

http://www.undernews.fr/reseau-securite/le-site-dedie-aux-cartes-nationales-didentite-hors-service-suite-a-un-piratage.html

Le forum d'Avast piraté, près de 400 000 authentifiants volés

http://blog.avast.com/2014/05/26/avast-forum-offline-due-to-attack/

Crypto

TrueCrypt, que se passe-t-il ? Il est urgent d'attendre

- Les developpeurs
  - Livrent une nouvelle version 7.2, signée avec leur clef
  - Rétro compatible mais ne permettant plus de créer des des volumes chiffrés !!?
  - Ils suppriment toutes les anciennes versions
  - www.truecrypt.org renvoie sur SourceForce
    - Avec un message d'alerte : WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues
  - Les developpeurs (anonymes) disent arrêter le projet
    - Et proposant de migrer vers Microsoft BitLocker
      - Malgré l'existence d'une clef de "recouvrement" de 48 bytes, même avec une puce TPM
- Urgence ? Risque ?
  - Certification DCSSI-CSPN-2008/03 et ANSSI-CSPN-2013/09
  - Résultats de l'audit de code d'iSec corrects
- Une explication ?
  - Les developpeurs "auraient" voulu arrêter projet sans qu'il n'y ait de reprise
    - Pas à cause de l'effet OpenSSL, ni de l'audit d'iSec
    - En oubliant l'existence de la communauté et des miroirs

      https://www.grc.com/misc/truecrypt/truecrypt.htm

      http://krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/
- La Suite ?
  - **iSec** continue l'audit formel de la partie Crypto
    - Prévu pour cet été
  - Une relève possible : http://truecrypt.ch
  - L'ANSSI recommande Cryhod, Zed !, ZoneCentral, Security Box ou encore StormShield.

    http://www.ssi.gouv.fr/fr/menu/actualites/possible-abandon-de-truecrypt-par-ses-developpeurs.html

Cryptographie Homomorphiques

- Accélération des NTRU (Nth degree Truncated polynomial Ring Units) avec GPU

  http://www.confianzit.org/searchdl/public/book_series/CSS/2/46.pdf
  - Une bonne nouvelle pour vendre du Cloud Américain aux autres pays
  - Une mauvaise nouvelle pour le Cloud franco-francais
- Des informations interessantes dans les commentaires :

  http://linuxfr.org/news/le-chiffrement-homomorphe

Quand on vous disait que la crypto-monnaie BitCoin n'était pas anonyme…

- Déjà abordé par Renaud LIFCHITZ en 2011

  http://prezi.com/tikwkjt9ouey/bitcoin-une-monnaie-electronique-pour-tous/

- A présent, par des universitaires Luxembourgeois

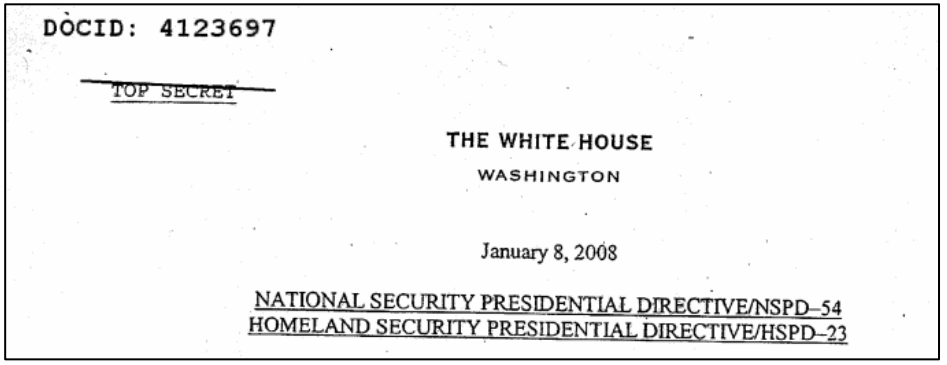
  http://arxiv.org/pdf/1405.7418.pdf

SCADA
Divers

“SCADA piratés sur 3 continents”

- Un document confidentiel daté de janvier 2008 mentionne le piratage de systèmes industriels sur 3 continents

  http://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf



DOCID: 4123697

~~TOP SECRET~~

THE WHITE HOUSE

WASHINGTON

January 8, 2008

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-54
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-23

- Une présentation par un membre de ScadaStrangeLove sur les protocoles de communication industriels et leur (absence) de mécanismes de sécurité http://www.slideshare.net/AlexanderTimorin/scada-deep-inside-protocols-and-security-mechanisms

- La participation de la team ScadaStrangeLove à la conférence PHDays à Moscou http://www.scadastrangelove.blogspot.fr/2014/06/at-positive-hack-days-iv-www.html#more

Nouveautés (logiciel, langage, protocole...)

Open Source

Mimikatz 2.0 alpha 20140525

- No more DLL needed to inject code in LSASS for lsadump::lsa /inject !

  http://blog.gentilkiwi.com/mimikatz

Nouveautés (logiciel, langage, protocole...)

Divers

HackerOne : Nouveau programme de bug bounty

- Par l'ancien responsable de l'équipe sécurité de Facebook
  - Avec une levée de fonds de $9 millions

  http://blogs.wsj.com/venturecapital/2014/05/28/hackerone-emerges-with-9-million-to-root-out-software-bugs/
- Les prix "minimum" par programmes

  https://hackerone.com/programs

Hex-Rays IDA v6.6

- Support x64 pour la décompilation

  https://www.hex-rays.com/products/ida/6.6/index.shtml

  https://www.hex-rays.com/products/decompiler/news.shtml#140604

Business
France

Atos rachète Bull

- Objectifs: s'emparer d'une expertise dans les surpercalculateurs et récupérer des compétences uniques en ingéniérie informatique
  - Quid des activités d'Amesys / Trustway ?

http://www.challenges.fr/high-tech/20140526.CHA4232/pourquoi-atos-rachete-bull.html

Consolidation du marché du WAF Français (Web Application Firewall)

- DenyAll acquière Beeware
  - Il n'y a que dans ce domaine que Paris peut "acquérir" Montpellier **;-)**
- Pour créer le « Next Generation Application Security »

http://www.lemagit.fr/actualites/2240220821/Consolidation-sur-le-marche-francais-du-WAF

Thales s'accapare les divisions cybersécurité d'Alcatel-Lucent

http://www.zdnet.fr/actualites/thales-s-accapare-les-divisions-cybersecurite-d-alcatel-lucent-39801541.htm

L'OS Made in France (Montebourg inside)

http://www.journaldunet.com/solutions/dsi/un-systeme-d-exploitation-made-in-france-0514.shtml

Face au pillage de ses dessins exposés sur Internet, Manu Larcenet clôt son site

http://www.manularcenet.com/blog/articles/10876/closing-time

Business
France

7 start up invitées à s'installer en Auvergne

- Tous frais payés

  http://pro.01net.com/editorial/620394/les-7-startups-invitees-a-s-installer-en-auvergne-tous-frais-payes/

Mouvements dans les télécoms

- Orange « examine les opportunités »

  http://www.nextinpact.com/news/87585-mouvements-dans-telecoms-orange-examine-opportunites.htm

Business
International

FireEye souhaite acheter nPulse Technologies

- Spécialiste du forensique réseau

http://www.fireeye.com/blog/corporate/2014/05/fireeye-enters-agreement-to-acquire-npulse-technologies.html

HP investit 1 milliard de dollard dans OpenStack

http://www.silicon.fr/hp-mise-milliard-dollars-cloud-openstack-94208.html

Twitter chute de plus de 10%

- après l'expiration du "lock-up"
  - Période de 6 mois interdisant aux actionnaires historiques de céder leurs titres

http://www.boursorama.com/actualites/twitter-chute-de-plus-de-10-apres-l-expiration-du-lock-up-a2ef1b1c776865b11399a1f7fc65bd17

L'Open Internet Project demande le démantèlement de Google

http://www.nextinpact.com/news/87406-antitrust-open-internet-project-demande-demantelement-google.htm

Pourquoi Yahoo continue à tuer tout ce qu'elle achète

- Car ils tendent à tout consolider/centraliser dans leur portail

http://www.wired.com/2014/05/yahoo-blink/

Business
International

Bill Gates cède son fauteuil d'actionnaire majoritaire de Microsoft

- Suite à la vente de 4,6 millions d'actions
- Steve Ballmer devient numéro 1

http://www.developpez.com/actu/70862/Bill-Gates-cede-son-fauteuil-d-actionnaire-majoritaire-de-Microsoft-suite-a-la-vente-de-4-6-millions-d-actions/

Avec Ion, Blackberry se positionne sur le marché des objets connectés

http://www.zdnet.fr/actualites/avec-ion-blackberry-se-positionne-sur-le-marche-des-objets-connectes-39801485.htm

Droit / Politique

France

L'ARCEP ouvre cinq enquêtes

- Déploiement 3G pour Free
- Déploiement 3G pour SFR
- Qualité de service des offres régulées d'Orange pour les entreprises
- Qualité de service de la téléphonie fixe d'Orange
- 3G en zone rurale pour les 4 opérateurs

http://www.nextinpact.com/news/87770-larcep-annonce-enquetes-sur-orange-bouygues-free-mobile-et-sfr.htm

Contre le terrorisme, des députés UMP envisagent le blocage de Twitter

http://www.nextinpact.com/news/87294-le-delit-consultation-sites-terroristes-retour-a-l-assemblee-nationale.htm

Le site du ministère de la Culture passe (presque) sous Creative Commons

http://www.nextinpact.com/news/87550-le-site-ministere-culture-passe-presque-sous-creative-commons.htm

King s'attaque à Bubblies, un groupe de rock toulousain

- Et manque son coup

http://www.nextinpact.com/news/87367-king-sattaque-a-bubblies-groupe-rock-toulousain-et-manque-son-coup.htm

Droit / Politique

France

Hadopi attribue cinq nouveaux « LOL »

http://www.nextinpact.com/breve/87744-la-hadopi-attribue-cinq-nouveaux-lol.htm

Et de 3 millions d'avertissements envoyés par la Hadopi

http://www.numerama.com/magazine/29420-et-de-3-millions-d-avertissements-envoyes-par-la-hadopi.html

Régulation du Net : le CSA esquisse sa frontière avec l'Arcep

http://www.nextinpact.com/news/87362-regulation-net-csa-esquisse-sa-frontiere-avec-arcep.htm

Bouygues, Free, Orange et SFR devront bloquer trois sites ukrainiens

http://www.nextinpact.com/news/87689-bouygues-free-orange-et-sfr-devront-bloquer-trois-sites-ukrainiens.htm

La justice condamne un logiciel d'enregistrement de flux en streaming

- Developpé par un étudiant de Sup Info de Montpellier

http://www.nextinpact.com/news/87781-la-justice-condamne-logiciel-d-enregistrement-flux-en-streaming.htm

Droit / Politique
Europe

L’Europe dit non au vote électronique par Internet

- Pour les prochaines élections en Estonie

  https://estoniaevoting.org/findings

L'Allemagne ne veut plus du matériel réseau des entreprises américaines

http://www.nextinpact.com/news/87697-lallemagne-ne-veut-plus-materiel-reseau-entreprises-americaines.htm

Droit / Politique
International

Google doit dominer le e-commerce

- Pour montrer que ses publicités fonctionnent vraiment

  http://www.wired.com/2014/05/google-serious-shopping/

Google prévoit l'apparition de publicité à des endroits inattendus

- Comme les thermostats !!?

  http://blogs.wsj.com/digits/2014/05/21/google-predicts-ads-in-odd-spots-like-thermostats/

Google sommé de respecter le droit à l'oubli

http://www.lefigaro.fr/secteur/high-tech/2014/05/13/01007-20140513ARTFIG00132-google-somme-de-respecter-le-droit-a-l-oubli.php

Silent Circle déménage en Suisse (Blacksphone et mails sécurisés Dark Mail Alliance)

- Qui se veut un bunker pour la vie privée

  http://www.numerama.com/magazine/29454-silent-circle-demenage-en-suisse-qui-se-veut-un-bunker-pour-la-vie-privee.html

- Tout comme le WebMail **Proton**
  - Victime de sons succès

  http://www.01net.com/editorial/620152/protonmail-le-webmail-anti-nsa-deja-victime-de-son-succes/

Droit / Politique
International

Aux États-Unis, la première plainte pour crowdfunding non honoré

http://www.nextinpact.com/news/87366-aux-etats-unis-premiere-plainte-pour-crowdfunding-non-honore.htm

Apple publie un guide pour les procédures judiciaires

- Liste de données pouvant être fournies légalement aux autorités américaines

http://www.developpez.com/actu/71018/Apple-publie-un-guide-pour-les-procedures-judiciaires-qui-etablit-une-liste-de-donnees-pouvant-etre-fournies-legalement-aux-autorites-americaines/

Snapchat a-t-il menti à ses utilisateurs ?

- Les “snaps” ne sont pas éphémères

http://www.lesinrocks.com/2014/05/09/actualite/snapchat-ce-se-passe-internet-reste-internet-11503344/

Retour sur la journée internationale contre les DRM du 6 mai 2014

http://linuxfr.org/news/nouvelle-depeche-35346

Les DRM et le défi de servir les utilisateurs

https://blog.mozilla.org/blog/2014/05/14/drm-and-the-challenge-of-serving-users/

Droit / Politique
International

Quand les majors obtiennent le déréférencement de The Pirate Bay-AFK

http://www.nextinpact.com/news/79819-quand-majors-obtiennent-dereferencement-the-pirate-bay-afk.htm

Neutralité du net

- La FCC américaine adopte les "voies rapides"

  http://www.zdnet.fr/actualites/neutralite-du-net-la-fcc-americaine-adopte-les-voies-rapides-39801225.htm

Droit / Politique
International

Un ancien directeur de la NSA admet

- "Nous tuons des gens en nous basant sur les métadonnées" et à l'aide de drones

  http://thehackernews.com/2014/05/ex-nsa-director-admits-we-kill-people.html

Les US se feraient espionner massivement par…

- Israel !

  http://www.courrierinternational.com/article/2014/05/21/espionnage-nos-allies-israeliens-ont-depasse-les-bornes

- Mais la France serait “seconde” à dérober des secrets US
  - Selon un ex-directeur de la Cia, également ex-secrétaire à la Défense des Etats-Unis
  - Derrière la chine
  - En entrant par effraction dans les chambres d’hôtel ;-)

  http://www.01net.com/editorial/620360/la-france-deuxieme-cyber-ennemi-des-etats-unis

  - Quand ils ne se font pas attraper comme en 2011 **;-)**

  http://www.ladepeche.fr/article/2010/12/15/970868-les-chinois-victimes-d-espions-francais.html

Droit / Politique
International

Microsoft vs USA : accès aux données du cloud en Irlande

- Dans une affaire criminelle, il a été demandé à Microsoft de fournir des données de son Cloud, hébergée en Irlande.
  - Microsoft a refusé
    - Réglementation européenne oblige
    - 4eme amendement : n'autorise les perquisitions qu'en cas de présomption « sérieuse » avec obligation d'avoir un mandat.

  http://www.networkworld.com/community/blog/judge-microsoft-hand-over-cloud-data-no-matter-where-world-it-stored
- Le 25 Avril, un juge fédéral a rejeté le refus de Microsoft
  - Si l'entreprise est domiciliée aux USA, alors les lois Américaines lui sont applicables.

  http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398
- Le G29 a statué et soutient Microsoft
  - Il est du devoir de Microsoft de veiller à la conformité de leurs dispositions contractuelles avec les exigences de l'UE en matière de protection des données.
- Et finalement, s'oppose avec succès à la requête du FBI

http://www.nextinpact.com/news/87707-microsoft-soppose-avec-succes-a-requete-fbi.htm

Cinq militaires chinois sont accusés d'espionnage par les États-Unis

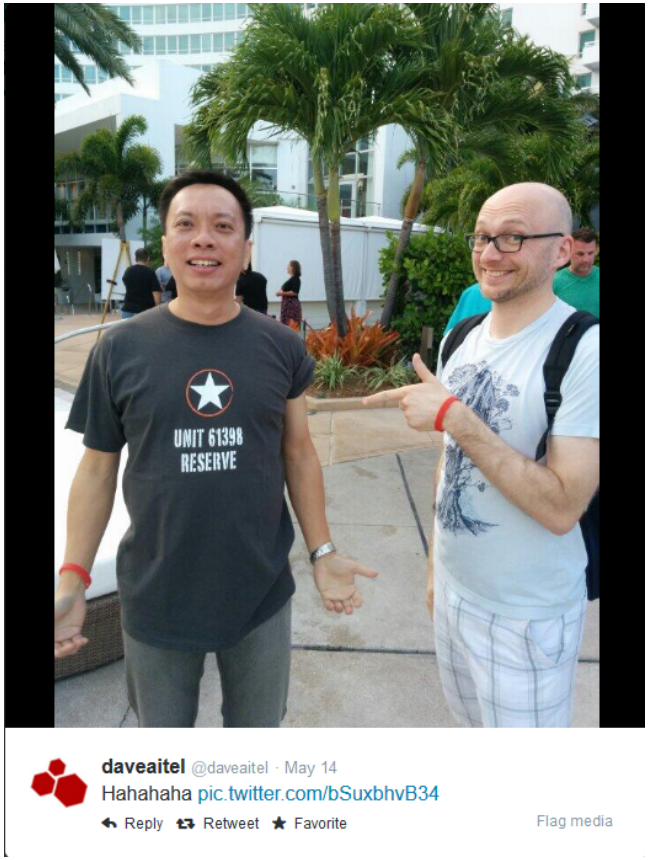
http://arstechnica.com/tech-policy/2014/05/indicted-chinas-army-hacked-into-us-companies-stole-trade-secrets/

http://www.justice.gov/opa/pr/2014/May/14-ag-528.html

http://www.networkworld.com/news/2014/052214-china-to-block-it-products-281827.html

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Heureusement qu'il reste l'humour ;-)



Conférences

Passées

- SSTIC - 4 au 6 juin 2014 à Rennes
  - Compte-rendu en séance

A venir

- Hack in Paris - 23 au 27 juin 2014 chez Mickey
- HACK.LU - 21 au 24 octobre 2014
  - CFP ouvert jusqu'au 15 juillet
- No Such Con - 19 au 21 novembre 2014 à Paris
- Bot Conf - 3 au 5 Décembre 2014 à Nantes

Divers / Trolls velus

Qui protège le mieux vos données personnelles contre les états ?

- Selon l'EFF ce sont :
  - Apple, Credo, Dropbox, Google, Facebook, Microsoft, Twitter et Yahoo. Qui l'eut cru !

  https://www.eff.org/who-has-your-back-2014
- Mauvais élèves : Amazon, Snapchat et ATT.

Même Symantec reconnait l'innéficacité des antivirus :-D

http://www.01net.com/editorial/619276/l-antivirus-est-mort-dit-symantec/

Divers / Trolls velus

Atelier “backdooring” de routeurs Cisco

- Glenn Greenwald sort son livre sur la NSA : « No place to hide »
  - Pour en assurer la promotion, il diffuse des photos de la TAO (Tailored Access Operations)
  - En train d’installer des backdoor dans des routeurs Cisco

http://glenngreenwald.net/

Divers / Trolls velus

Est-ce un oiseau ? Est-ce un avion ? Non, c'est une invasion extraterrestre...

- Ou simplement un balon sonde de Google **;-)** (projet Loon)

  http://www.clubic.com/insolite/actualite-706009-insolite-ballons-wi-fi-google-pris-invasion-alien-usa.html

Oeil pour Oeil, Bitcoin pour Bitcoin

- Victime d'un chantage, un riche entrepreneur du Bitcoin met une prime sur la tête du hackeur

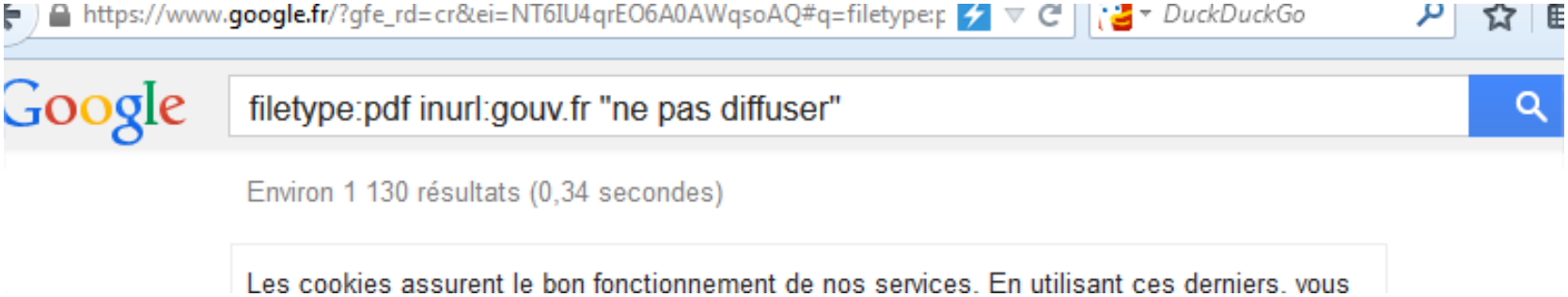
  https://www.facebook.com/rogerkver/posts/10152072000675737

  - Avec succès ;-)
    - Le hackeurs a été complètement "doxé" http://pastebin.com/gWV31yuB

  http://www.wired.com/2014/05/dfwtbj/

filetype:pdf inurl:gouv.fr "ne pas diffuser"

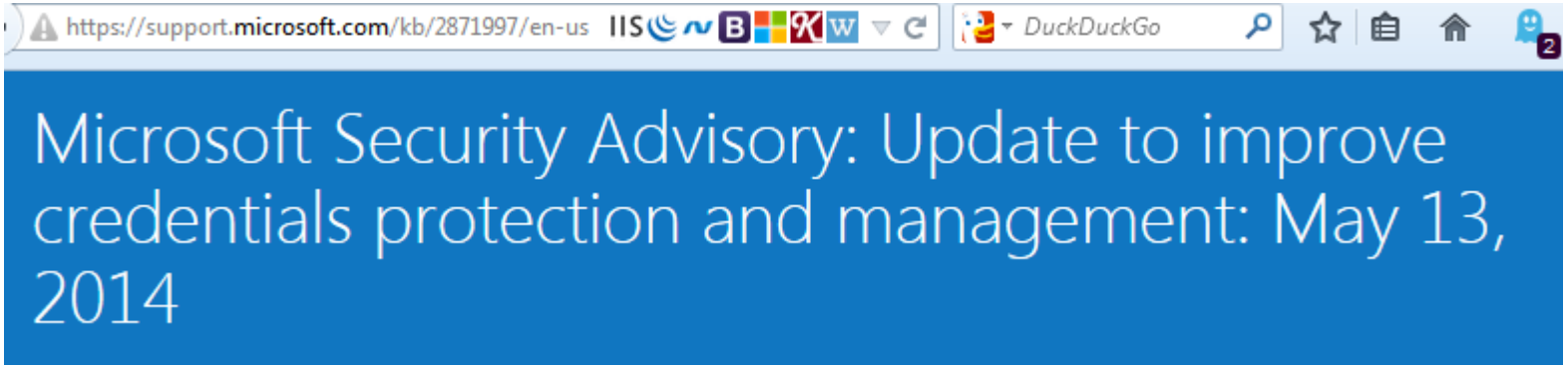
- Mais beaucoup de faux positifs ;-)
  - <<Les opérateurs de services s'engagent à ne pas diffuser les données>>
  - <<important de ne pas diffuser le cri trop longtemps>>



Divers / Trolls velus

Traduction, quand tu nous tiens…

- corrigé depuis ;-)
  - Avis de sécurité Microsoft : Mise à jour permettant d'améliorer la gestion et la protection des informations d'identification datée du 13 mai 2014



Divers / Trolls velus

<<...la naïveté me paraît colossale.>>

- Comptes rendus publics des auditions de travaux de commissions de l'assemblée
  - Extrait de celle du Mercredi 30 avril 2014 :

  <<Certains groupes industriels ont subi des attaques informatiques de grande ampleur. Des mesures correctrices ont été prises, mais ces épisodes ont montré que la conscience et la connaissance de la menace informatique ne sont pas ce qu'elles devraient être ; beaucoup de progrès restent à faire, et la **naïveté** me paraît **colossale**.>>

  http://www.assemblee-nationale.fr/14/cr-cdef/13-14/c1314047.asp

- Autres extraits :
  - << Notre pays semble disposer en la matière d'une avance qui nous placerait même devant les États-Unis.>>
  - << les besoins en énergie et en refroidissement toujours croissants risquent de nous conduire à une impasse en 2022 ou 2025 : il faudrait alors construire un ou plusieurs EPR autour d'un supercalculateur pour l'alimenter en énergie et le refroidir...>>

Questions ?

Prochaines réunions

- Mardi 8 juillet 2014

- Août
  - Congés, repos, soleil !

- 9 septembre 2014
  - Reprise

Des questions ?