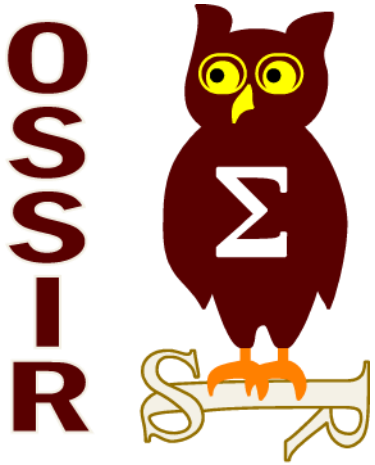

RéSIST : Revue d'actualité

27 Mars 2012

Presented by
Etienne Maynier

Sommaire

- Incidents de sécurité Février / Mars 2012
- Conférences
- Vulnérabilités

Symantec PC Anywhere

- Vulnérabilité critique trouvée dans Symantec PC Anywhere suite à un vol de code source puis divulgation de plusieurs codes source par les « Anonymous »
- Timeline intéressante
  - Avant 2012 : intrusion annoncée mais non reconnue par Symantec
  - W2 : Vol de code source sans importance confirmé par Symantec
  - W4 : Symantec recommande de désactiver PC Anywhere en attendant le patch
  - W6 : Release du code source de PC Anywhere après des négociations échouées ($50 000 en échange du démenti par les Anonymous)
  - W7 : Patch disponible
  - W10 : Publication du code source de Norton Antivirus 2006
- Liens
  - http://www.theregister.co.uk/2012/01/06/symantec_source_code_theft/
  - http://www.symantec.com/theme.jsp?themeid=anonymous-code-claims
  - http://www.h-online.com/security/news/item/Critical-flaw-discovered-in-Symantec-s-pcAnywhere-1421261.html
  - http://www.reuters.com/article/2012/02/07/us-symantec-hackers-idUSTRE8160KB20120207
  - http://www.theinquirer.net/inquirer/news/2158170/anonymous-leaks-symantec-source-code
  - http://www.forbes.com/sites/andygreenberg/2012/02/07/as-hackers-leak-symantecs-source-code-firm-says-cops-set-up-extortion-sting/

VeriSign

- Plusieurs intrusions réussies détectées en 2010 dans le réseau de VeriSign.
- Révélé dans un rapport d'une commission US sur la sécurité
- Le CTO de l'époque Ken Silva a annoncé ne pas avoir eu connaissance de ces attaques

- Rappel : VeriSign a vendu son département « Autorité de Certification » en Aout 2010 à Symantec mais reste gestionnaire du TLD .com

- Liens
  - http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202
  - http://threatpost.com/en_us/blogs/update-verisign-admits-security-breaches-2010-020212

SSL

- Mauvaise période pour SSL
  - Plus d'OCRL dans Chrome, utilisation des mises à jour du navigateur
  - Trustwave a créé un certificat intermédiaire pour permettre à une société de faire du DLP
    - Mozilla en discussion pour bannir la société des autorités de certifications reconnues
  - Démonstration d'une compromission des données Google Maps par analyse de traffic
- Liens
  - http://threatpost.com/en_us/blogs/google-stop-using-online-crl-checks-chrome-020712
  - http://www.theregister.co.uk/2012/02/09/tustwave_disavows_mitm_digital_cert/
  - https://bugzilla.mozilla.org/show_bug.cgi?id=724929#c88
  - http://blog.ioactive.com/2012/02/ssl-traffic-analysis-on-google-maps.html

Lulzsec

- Arrestation de 7 membres de lulzsec (US/UK/Irlande)
- Arrêtés suite au retournement de leur leader Sabu, en coopération avec le FBI depuis plusieurs mois (Juillet 2011)
- Encourt 124 ans de prison…
- Fin de lulzsec

- Liens
  - http://www.bbc.co.uk/news/technology-17270822
  - http://www.reuters.com/article/2012/03/09/us-cyber-arrests-idUSBRE82801P20120309

Google et la vie privée

- Changement de la politique de confidentialité
  - Regroupement des informations de tous les services Google
  - *"Les nouvelles règles autoriseraient Google à afficher sur Youtube des publicités liées à l'activité de l'utilisateur sur son téléphone Android et à sa localisation*, note la CNIL
  - Entrée en vigueur le 1er Mars
  - 19 Mars: envoi d'un questionnaire par la CNIL à Google
- Tracking des utilisateurs
  - Bypass des protections privacy de Safari et IE
  - Enquête lancée par les EU et l'Europe
- Dépôt d'un nouveau brevet pour « tenir compte de l'environnement du téléphone » pour cibler les publicités
- Liens
  - http://www.lemonde.fr/technologies/article/2012/01/25/google-annonce-une-grande-revision-de-sa-politique-de-confidentialite_1634068_651865.html
  - http://www.cnil.fr/la-cnil/actualite/article/article/les-nouvelles-regles-de-confidentialite-de-google-soulevent-des-inquietudes/
  - http://www.cnil.fr/nc/la-cnil/actualite/article/article/nouvelles-regles-de-confidentialite-de-google-la-cnil-adresse-un-questionnaire-detaille/
  - http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html
  - http://online.wsj.com/article/SB10001424052702304692804577283821586827892.html
  - http://www.digitaltrends.com/mobile/google-patent-suggests-using-background-noise-to-generate-mobile-ads/

Androïd

- Evolution des menaces sous Androïd
  - Vulnérabilité dans certains smartphones HTC permettant de découvrir les clés wifi (mauvais filtrage du toString)
  - Malware ayant affecté plus de 100 000 smartphones découvert
    - Utilisé pour envoyer des SMS surtaxés
- Google réagit
  - Déploiement d'un outil d'analyse automatique par Google
- Liens
  - http://blog.mywarwithentropy.com/2012/02/8021x-password-exploit-on-many-htc.html
  - http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet
  - http://www.reuters.com/article/2012/02/03/us-google-security-idUSTRE81201U20120203

Vol d'information à Dassault Aviation

- Rencontre Dassault / BEA System pour un partenariat sur un nouveau drone
- Départ de l'équipe de Dassault à la Gare du Nord
  - Deux personnes : une qui distrait, une qui prend la mallette
- Un cas d'école d'intelligence économique !
- Liens
  - http://www.securityvibes.fr/menaces-alertes/dassault-aviation-bae-vol-de-donnees/
  - http://threatpost.com/en_us/blogs/old-school-attack-nabs-joint-uk-french-drone-plans-022312

Clés RSA

- Etude de millions de clés RSA accessibles sur Internet (SSL, PGP)
  - Mauvais PRNGs sur 4% des clés, dans ce cas-là RSA n'offrirait aucune sécurité
  - Après étude, problème uniquement sur les équipements réseau
  - Recommandations CERTA
    - Renouvellement des certificats
    - Changement des mots de passe
    - Revue des logs

- Liens
  - http://eprint.iacr.org/2012/064.pdf
  - http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-008/index.html
  - http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/vulnerabilite-rsa-diagnostic-et-recommandations.html
  - http://www.securityvibes.fr/produits-technologies/epflcles-rsa/

Autre

- Exercice PIRANET2012 de l'ANSSI
  - Simulation d'une attaque de grande ampleur sur l'Internet français et contre les réseaux des administrations
- Plantage du cloud Microsoft Azure le 29 Février
  - 4% des applications touchées
- Publication par Wikileaks des emails de Stratfor (Lien)
- Vol d'un PC de la NASA contenant des algorithmes de contrôle d'ISS (Lien)
- Création d'un faux profil Facebook d'un général de l'OTAN (Lien)

Conférences

- Trois conférences :
  - CanSecWest et son fameux Pwn2Own (Vancouver)
  - La conférence RSA (San Francisco)
  - BlackHat Europe (Amsterdam)

CanSecWest 2012

- 13ème édition
  - Nouvelles règles pour Pwn2Own
    - Focus uniquement sur IE/Chrome/Firefox/Opera sous 7/Lion
    - Mode CTF : deux vulnérabilités non-patchées révélées au début
    - Des points gagnés pour chaque exploit
    - Il faut au minimum un 0day pour gagner
    - Forfait de Charlie Miller
  - Lancement de Google Pwnium sur Google Chrome
    - $60 000 par 0day
    - Obligation de révéler la vulnérabilité à Google
- Liens
  - http://www.zdnet.com/blog/security/cansecwest-pwn2own-hacker-challenge-gets-a-105000-makeover/10182
  - http://pwn2own.zerodayinitiative.com/rules.html
  - http://www.zdnet.com/blog/security/charlie-miller-skipping-pwn2own-as-new-rules-change-hacking-game/10554
  - http://blog.chromium.org/2012/02/pwnium-rewards-for-exploits.html

CanSecWest 2012

- Résultats:
  - Deux 0-day trouvées dans Chrome (VUPEN & Sergey Glazunov)
  - Un 0day dans IE9 par VUPEN
  - VUPEN a indiqué ne pas partager ces exploits à Google mais les réserver à ses clients…
  - Après Full Disclosure, Responsible Disclosure, No Disclosure !

- Liens
  - http://googlechromereleases.blogspot.fr/2012/03/chrome-stable-channel-update.html
  - http://www.zdnet.com/blog/security/pwn2own-2012-google-chrome-browser-sandbox-first-to-fall/10588
  - http://threatpost.com/en_us/blogs/ie-9-falls-pair-zero-days-pwn2own-030812
  - http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

RSA Conference

- *"The current risks to internet freedom, openness, and innovation don't come from the bad guys – they are political and technical. I suppose I should call this talk 'Layer eight and nine threats',"* Bruce Schneier
- Arrivée massive du Bring Your Own Device
- Manque de sécurité des systèmes de vote électronique
- La Chine est tout aussi vulnérable aux attaques informatiques

- Liens
  - http://www.theregister.co.uk/2012/02/29/schneier_warns_government_business_threat/
  - http://www.net-security.org/secworld.php?id=12508
  - http://www.theregister.co.uk/2012/03/01/electronic_voting_hacked_bender/
  - http://www.securityvibes.fr/cyber-pouvoirs/chine-cyberguerre-espionnage/

BlackHat EU

- Quelques sujets abordés
  - Problèmes de sécurité due aux proxy intercepteurs
    - Site de test https://ssltest.offenseindepth.com/
  - Analyse détaillée des sandbox sous MAC OS X
  - Outil d'injection Xpath
    - https://github.com/orf/xcat
  - Recommandations pour gérer le passage de la frontière US
  - Sécurité SAP
  - Gestion de la fragmentation en IPv6
  - Sécurité des Secure Password Managers de smartphones

- Archives en lignes !

Vulnérabilités

- Google Chrome < 17.0.963.79
  - Plusieurs CVE menant à des arbitrary code execution (CVE-2011-3961 CVE-2011-3047) et DoS (CVE-2011-3953 CVE-2011-3955 CVE-2011-3957 CVE-2011-3959 CVE-2011-3966 CVE-2011-3015 CVE-2011-3016 CVE-2011-3017 CVE-2011-3018 CVE-2011-3020 CVE-2011-3021 CVE-2011-3026 CVE-2011-3027 CVE-2011-3031 CVE-2011-3032 CVE-2011-3033 CVE-2011-3034 CVE-2011-3035 CVE-2011-3036 CVE-2011-3037 CVE-2011-3038 CVE-2011-3039 CVE-2011-3041 CVE-2011-3042 CVE-2011-3043 CVE-2011-3044 CVE-2011-3046)
- PHP < 5.3.10
  - Mauvaise gestion de la mémoire des tableaux menant à une remote code execution[1] (CVE-2012-0830)
  - Bypass des magic quotes possibles (CVE-2012-0831)
- RealPlayer < 15.02.71
  - 7 vulnérabilités arbitrary code execution (CVE-2012-0922 CVE-2012-0923 CVE-2012-0924 CVE-2012-0925 CVE-2012-0926 CVE-2012-0927 CVE-2012-0928)
- Notes
  - 1 - http://thexploit.com/sec/critical-php-remote-vulnerability-introduced-in-fix-for-php-hashtable-collision-dos/

Vulnérabilités

- Adobe Flash Player < 10.3.183.16 / 11.1.102.63
  - 7 arbitrary code execution (CVE-2012-0751 CVE-2012-0752 CVE-2012-0753 CVE-2012-0754[1] CVE-2012-0755 CVE-2012-0756 CVE-2012-0768)
- Adobe Shockwave player < 11.6.4.634
  - Six arbitrary code execution (CVE-2012-0757 CVE-2012-0758 CVE-2012-0759 CVE-2012-0760 CVE-2012-0761 CVE-2012-0762 CVE-2012-0763 CVE-2012-0764 CVE-2012-0766)
- Notes
  - 1 – Exploit public http://www.exploit-db.com/exploits/18572/

Vulnérabilités Microsoft

- Internet Explorer : Arbitrary code execution (CVE-2012-0011[1] CVE-2012-0155 CVE-2012-1544[2])
- .Net framework / Silverlight : arbitrary code execution (CVE-2012-0014 CVE-2012-0015)
- Visio Viewer : arbitrary code execution (CVE-2012-0019 CVE-2012-0020 CVE-2012-0136 CVE-2012-0137 CVE-2012-0138)
- Windows 7 : Privilege escalation (CVE-2012-0148 CVE-2012-0150 CVE-2012-0157)
- Windows server 2003 : Privilege escalation (CVE-2012-0149)
- RDP : Remote code execution[3] (CVE-2012-0002)
  - Course à l'exploit, révélé à Microsoft en Aout 2011, fuite du PoC
  - Potentiel ver RDP à prévoir
- Notes
  - 1 - Exploit public et disponible http://www.exploit-db.com/exploits/18642/
  - 2 – Exploit démontré à Pwn2Own par VUPEN
  - 3 - http://www.metasploit.com/modules/auxiliary/dos/windows/rdp/ms12_020_maxchannelids
  - 4 - http://seclists.org/nmap-dev/2012/q1/att-662/rdp-ms12-020.nse

Vulnérabilités

- Mozilla Firefox < 10.0.3
  - Arbitrary code execution (CVE-2012-0452 CVE-2012-0454 CVE-2012-0457 CVE-2012-0459 CVE-2012-0461 CVE-2012-0462 CVE-2012-0463 CVE-2012-0464)
- Oracle Java < SE 7 Update 2 / 6 Update 30
  - Arbitrary code execution (CVE-2012-0497 CVE-2012-0498 CVE-2012-0499 CVE-2012-0500 CVE-2012-0503 CVE-2012-0504 CVE-2012-0505 CVE-2012-0508
- Cisco ASA 5500/6500
  - Denial of Service (CVE-2012-0353 CVE-2012-0354 CVE-2012-0355 CVE-2012-0356)
  - Arbitrary code execution dans le client VPN(CVE-2012-0358)

Vulnérabilités Apple

- Apple Safari < 5.1.2
  - Use after free vulnerability leading to arbitrary code execution (CVE-2011-3443 CVE-2011-3845)
- iTunes < 10.6 / iOS < 5.1
  - Arbitrary code execution in Webkit (CVE-2011-2833 CVE-2011-2866 CVE-2011-2867 CVE-2011-2868 CVE-2011-2869 CVE-2011-2870 CVE-2011-2871 CVE-2011-2872 CVE-2011-2873 CVE-2012-0591 CVE-2012-0592 CVE-2012-0593 CVE-2012-0594 CVE-2012-0595 CVE-2012-0596 CVE-2012-0597 CVE-2012-0598 CVE-2012-0599 CVE-2012-0600 CVE-2012-0601 CVE-2012-0602 CVE-2012-0603 CVE-2012-0604 CVE-2012-0605 CVE-2012-0606 CVE-2012-0607 CVE-2012-0609 CVE-2012-0610 CVE-2012-0611 CVE-2012-0612 CVE-2012-0613 CVE-2012-0614 CVE-2012-0615 CVE-2012-0616 CVE-2012-0617 CVE-2012-0618 CVE-2012-0619 CVE-2012-0620 CVE-2012-0621 CVE-2012-0622 CVE-2012-0623 CVE-2012-0624 CVE-2012-0625 CVE-2012-0626 CVE-2012-0627 CVE-2012-0628 CVE-2012-0629 CVE-2012-0630 CVE-2012-0631 CVE-2012-0632 CVE-2012-0633 CVE-2012-0634 CVE-2012-0635 CVE-2012-0636 CVE-2012-0637 CVE-2012-0638 CVE-2012-0639 CVE-2012-0648)
  - iOS (CVE-2012-0642 CVE-2012-0643 CVE-2012-0646)

Sujets du jour

- *AET, Advanced Evasion Threats*
  - Léonard DAHAN, Stonesoft
- *Bilan Cert-IST sur les attaques informatiques de l'année 2011*
  - Philippe BOURGEOIS, CERT-IST