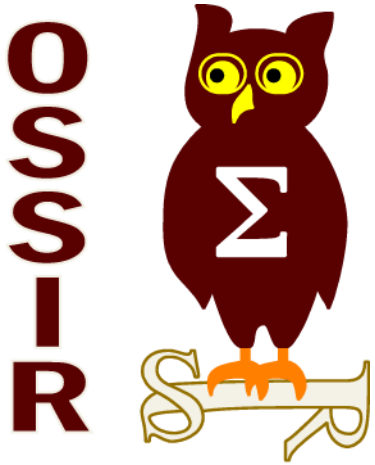

RéSIST : Revue d'actualité

15 Mai 2012

Presented by
Etienne Maynier

Sommaire

- Incidents de sécurité Avril / Mai 2012
- Conférences
- Vulnérabilités

Flashback

- Vulnérabilité critique dans Java (CVE-2012-0507) non patchée par Apple pendant six semaines
- Botnet de 550 000 machines découvert par Dr Web début Avril
  - Malware « Flashback » commandé par un C&C pour installer d'autres binaires
  - Mise à jour par Apple dix jours plus tard
- Un mois après difficile de dire l'effet de la mise à jour
  - 500 000 bots selon Dr Web / 180 000 selon Symantec
- Fin de l'histoire : Flashback était utilisé pour détourner les mots clés google vers d'autres publicités payées par clic
  - 0.8 centimes par click -> 10 000$ par jour
- Liens
  - http://news.drweb.com/show/?i=2341
  - http://www.h-online.com/security/news/item/Apple-releases-Java-update-with-Flashback-removal-tool-Update-1520431.html
  - http://www.h-online.com/security/news/item/Flashback-numbers-not-going-down-still-over-half-a-million-1547542.html
  - http://www.symantec.com/connect/blogs/osxflashbackk-motivation-behind-malware

Incidents de sécurité (1/2)

- Global Payments Inc :
  - Vol d'1,5 million de numéros de cartes bancaires
- Ministère de la défense britannique
  - *"The number of serious incidents is quite small, but it is there"*
  - *"If we want to know really what is happening, we really have to listen to the young kids out in the street."*
- Sociétés américaines opérant des pipelines de gaz naturel
  - Apparemment phishing ciblé utilisé
  - Fin mars, l'ICS-CERT recommande de ne pas prendre encore de mesures si cela ne met pas des systèmes critiques en danger
- Liens
  - http://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/
  - http://www.forbes.com/sites/greatspeculations/2012/04/03/global-payments-data-breach-exposes-card-payments-vulnerability/
  - www.guardian.co.uk/technology/2012/may/03/hackers-breached-secret-mod-systems
  - http://www.csmonitor.com/USA/2012/0505/Alert-Major-cyber-attack-aimed-at-natural-gas-pipeline-companies

Incidents de sécurité (2/2)

- Twitter
  - 55 000 login/password sur Pastebin
  - Après analyse par Twitter, 20 000 doublons, des comptes de spam bloqués et des données erronées
  - Les autres comptes ont eu le mot de passe réinitialisé
- SOCA : UK's Serious Organised Crime Agency
  - DDoS sur le site web public
  - Deux adolescents norvégiens arrêtés la semaine suivante
- Liens
  - http://www.lemonde.fr/technologies/article/2012/05/09/une-fuite-dans-twitter_1698237_651865.html
  - http://www.theinquirer.net/inquirer/news/2173569/twitter-reassures-users-personal-details-safe-security-breach
  - http://www.bbc.com/news/technology-17936962
  - http://www.bbc.com/news/technology-18005505

Chine

- Huawei
  - Refus d'accepter la réponse de la société à un appel d'offre public par le gouvernement australien à cause des cyber-attaques venant de chine
  - Symantec rompt son partenariat pour ne pas nuire à son marché américain
- Exercices de cybersécurité entre USA et Chine
  - Exercices militaires pour comprendre les réactions opposées dans différents scénarios. Ex : attaque type Stuxnet venant de la Chine
- Annonce officielle de collaboration USA/Chine début mai
  - Objectif : éviter une guerre froide informatique
- Liens
  - http://www.smh.com.au/business/gillard-defends-huawei-nbn-bar-as-prudent-20120326-1vtyx.html
  - http://www.linformaticien.com/actualites/id/24228/symantec-rompt-son-alliance-avec-huawei.aspx
  - http://www.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games
  - http://www.bbc.com/news/technology-17989560

Botnets

- Microsoft et Zeus
  - Saisie de serveurs de C&C d'un botnet utilisant une variante de Zeus
  - Une partie du botnet toujours en vie (147 des 156 serveurs de C&C arrêtés)
  - Des critiques de la communauté pour avoir utilisé des informations confidentielles pour lancer cette opération sans grand effet
- Kaspersky et Kelihos
  - Démantèlement du botnet P2P Kelihos B
  - En réalité botnet encore en activité
- Liens
  - http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx
  - http://blog.fireeye.com/research/2012/04/zeus-takeover-leaves-undead-remains.html
  - http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/
  - http://www.securelist.com/en/blog/208193431/Botnet_Shutdown_Success_Story_again_Disabling_the_new_Hlux_Kelihos_Botnet
  - http://blog.seculert.com/2012/03/kelihosb-is-still-live-and-social.html

Veille légale

- Europe
  - Projet de loi sur la cybersécurité
    - Attaque plus sévèrement punies
    - La possession et distribution d'outils également…
  - Création d'un centre européen de lutte contre la cybercriminalité

- USA
  - Loi CISPA : loi favorisant l'échange de données entre sociétés et agences gouvernementales et autorisant la surveillance de données personnelles
  - Forte opposition notamment de l'EFF

- Liens
  - http://www.europarl.europa.eu/news/de/pressroom/content/20120326IPR41843/html/Hacking-IT-systems-to-become-a-criminal-offence
  - http://www.linformaticien.com/actualites/id/24250/bruxelles-propose-la-creation-d-un-centre-europeen-de-lutte-contre-la-cybercriminalite.aspx
  - http://www.lemonde.fr/technologies/article/2012/04/09/cispa-un-projet-de-loi-sur-la-cybersecurite-controverse_1682559_651865.html
  - https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it

Autre (1/2)

- Etude sur la vente d'exploits au marché noir après les discussions sur VUPEN et pwn2own

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

- Projet EuroCybex : exercices de cyber-crises entre agences européennes (dont l'ANSSI)

- Liens
  - http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/
  - http://www.ceis.eu/fr/bureau-europeen/actu/exercice-de-cyber-crise-publication-du-rapport-eurocybex

Autre (2/2)

- Mise en garde du FBI sur la sécurité des wifi publics
  - Malware utilisant ces réseaux wifi pour créer des pop-up de fausse demande de mise à jour
- Le FBI voudrait promouvoir un projet de loi donnant un accès aux autorités américaines dans le services web en ligne (réseau sociaux, emails…)
  - Des discussions seraient en cours entre le FBI et plusieurs sociétés américaines
- Un rapport indique que le nombre de faux semi-conducteurs serait en train d'augmenter
- Seconde version du RGS en cours de préparation à l'ANSSI
- Liens
  - http://krebsonsecurity.com/2012/05/fbi-updates-over-public-net-access-bad-idea/
  - http://www.bbc.com/news/technology-17665527
  - http://www.ssi.gouv.fr/fr/menu/actualites/l-anssi-prepare-la-seconde-version-du-rgs.html
  - http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/

Conférence

- Une seule conférence

- Présentation de la sécurité des cartes bancaires NFC
  - Pas d'authentification ni de chiffrement
  - Accès aux données de la carte, copie de la carte…
- Backdoor matérielle
  - Rakshasa : BIOS malveillant
- http://2012.hackitoergosum.org/blog/schedule/talks

Vulnérabilités

- Microsoft :
  - MS12-027 : RCE dans Office, SQL Server, MS Commerce... Déjà exploité “into the wild”
  - MS12-023 : 4 RCE dans Internet Explorer. Exploit prévu sous 30 jours
  - MS12-029 : RCE dans Office
  - MS12-034, MS12-035 : RCE dans .NET / Silverlight
- Samba :
  - CVE-2012-1182 : RCE root dans toutes les versions de Samba ! PoC déjà public
- Oracle :
  - Patch d’avril : 88 vulnérabilités dont 33 RCE dans 30 produits
  - Une vulnérabilité communiquée à Oracle (CVE-2012-1675) mais non patchée. Après une communication sur FD, Oracle a sorti un patch.

Vulnérabilités

- Chrome
  - Vulnérabilités critiques dans Chromes
- PHP CVE-2012-1823
  - Découvert par le groupe Eindbazen
  - Uniquement avec php-cgi, permet de récupérer le code source php
- Adobe
  - CVE-2012-0779 : arbitrary code execution dans Flash déja exploitée dans la nature
  - Reader : CVE-2012-0774, CVE-2012-0775, CVE-2012-0776, CVE-2012-0777
  - Illustrator et Photoshop : la version mise à jour sera payante !
  - Shockware player : arbitrary code execution

Vulnérabilités

- Apple
  - Fichier debug dans FileVault loggant les mots de passe en clair.
  - IOS 5.1.1 : URL spoofing dans Safari, RCE dans webkit
- RuggedCom Rugged Operating System
  - Equipements réseau industriels
  - Mot de passe dérivé de l'adresse MAC…
  - CVE-2012-1803 et CVE-2012-2441

Sujets du jour

- *The story of how I hacked into your TV*
  - M. Rikke Kuipers, Codenomicon
- *Traçabilité des administrateurs internes et externes : une garantie pour la conformité*
  - Wallix