



OSSIR

2008/04/07

Compte-Rendu BlackHat Europe 2008

Francois Ropert

fropert (à) cisco.com

Cisco

Jeremy Lebourdais

jeremy.lebourdais (à) edelweb.fr

EdelWeb / Groupe ON-X



- diffusion publique -



BlackHat Europe 2008

❑ **Lieu: Amsterdam**

❑ **Quelques chiffres**

- ✓ 400 personnes
- ✓ 2 jours
- ✓ 24 présentations

❑ **Sujets variés**

- ✓ De la sécurité physique
- ✓ Aux failles dans PDF
- ✓ En passant par le Web 2.0, les codes malveillants, etc

Keynote

❑ L'échec prévu des systèmes rationnels

- ✓ Incapacité à gérer l'exception
- ✓ Sécurité ne peut être étudiée et gérée par les statistiques
- ✓ Nombreuses citations et exemples
- ✓ Vidéo illustrant ses propos
- ✓ Vouloir tout contrôler est voué à l'échec
- ✓ Il faut apprendre à gérer les exceptions

Client Side Security

❑ Techniques d'attaques côté client (PDP – GnuCitizen)

✓ Plusieurs exemples d'attaque

- CSRF (Gmail, Boitiers BT), CS File Upload (Flash, FORM)
- UPnP, QuickTime, Second Life, Citrix, RDP

❑ Au final

✓ « 4^{ème} génération » de rootkits seront sur les navigateurs ?

✓ Navigateur = Cible privilégiée :

- ajout de fonctionnalités facile, accès au web
- code multiplateforme, XML et JS polymorphiques ? (obfuscation plutôt)

✓ Des problèmes, mais pas de solutions proposées ...

Attacking antivirus (1/2)

❑ Recherche de vulnérabilités dans les antivirus

- ✓ Constat : Trop de confiance dans les antivirus
- ✓ Installés sur une majorité des postes de travail et sur les serveurs mail
- ✓ Or les antivirus sont sujets aux erreurs car il y a de nombreux formats à analyser
- ✓ Axes de recherche
 - Augmentation de privilèges (localement)
 - Composants ActiveX (contrôle d'un poste en ligne)
 - Moteur
 - Console d'administration

Attacking antivirus (2/2)

❑ **Comment faire ?**

- ✓ Analyse du composant ActiveX et du réseau
- ✓ Audit du code source, reverse engineering, fuzzing

❑ **Présentations de plusieurs exemples**

❑ **Conclusion**

- ✓ Les éditeurs doivent prendre la sécurité de leur solution plus sérieusement (audit interne, SDL, fuzzing)
- ✓ Avant, il fallait scanner tout fichier suspect, maintenant il faut réfléchir avant de faire le contrôle ;-)

Crackstation

□ Comment se faire acheter une PlayStation 3 par son entreprise ;-)

- ✓ Architecture Cell, avec processeur PPU, connecté à 8 SPU
- ✓ Code scalaire : performances équivalentes à un Centrino 2 duo à 2,2GHz (env **5 millions MD5/s**)
- ✓ Code vectoriel (SIMD) permet d'appliquer une opération à plusieurs données : **1,9 milliards de calculs MD5/s !**
- ✓ Architecture Cell a un bon rapport qualité/prix, mais SSE implémente aussi SIMD (augmentation moindre des performances, env x3)

Iron Chef: John Henry Challenge

❑ Comparaison interactive de deux méthodes d'analyse de code

- ✓ Challenge entre deux équipes, analyse d'un programme en 3/4h
- ✓ Outils automatisés
 - Dynamique (modification des variables pour ajouter des marqueurs)
 - Statique (analyse du flux d'exécution)
- ✓ Analyse « manuelle »
 - Expérience nécessaire
 - Recherche orientée
- ✓ Résultat : égalité (à l'applaudimètre ;-)

□ Présentation du framework Dtrace

- ✓ « Capteurs » implantés dans le noyau
- ✓ Déclenchement d'un évènement lors de l'exécution d'un capteur
- ✓ Création de scripts sur ces évènements
- ✓ Pas un débogueur, impact faible sur les performances
- ✓ Langage D trop limité, création du framework « RE:Trace » (Ruby)
- ✓ Facilite la vie du « reverser »:
 - Surveillance des « stack overflow », des « heap overflow »
 - Analyse du flux d'exécution dynamiquement (et plugin IDA)

The Fundamentals of Physical Security

□ **Présentation du « Lockpicking » et des différentes serrures**

- ✓ Très interactif (caméra pour montrer les manipulations)
- ✓ Comment retirer des menottes avec un bout de métal
- ✓ Ou bien ouvrir un cadenas avec une cannette découpée
- ✓ Présentation des différentes technologies de serrures
- ✓ Analyse des vulnérabilités mais aussi recommandations associées (par exemple les serrures à disque)
- ✓ Atelier pratique à la fin, avec prêt/vente de petits kits et utilisation de serrures avec difficulté croissante

Bad Sushi - Beating Phishers at Their Own Game

□ Analyse des sites et compétences des Phishers

- ✓ Les phishers ne prennent pas le temps de sécuriser leurs serveurs
- ✓ Exemples de scripts kiddies
- ✓ Peu de créateurs de framework mais beaucoup « d'utilisateurs »
- ✓ Partis d'un site de phishing, arrivés à un trafic de « ATM skimmers »
- ✓ Ce qui était vrai hier ne l'est plus aujourd'hui
 - Recopie des sites légitimes (plus de Referer)
 - Sécurisation des serveurs
 - Transmission et stockage des informations récoltées avec chiffrement
- ✓ Présentation des attaques et vulnérabilités, pas des solutions

Uri use and abuse

□ **Comment exploiter les URIs et gestionnaires associés**

- ✓ Utilisation des URIs comme point d'entrée
- ✓ Beaucoup de gestionnaires, et pas tous sécurisés ...
- ✓ Nombreux exemples :
 - Stack Overflow dans Trillian, MS07-035 (Iframe.dll)
 - Picasa, Gtalk
 - iPhoto (for Fun and Profit)
- ✓ Même Windows Mobile est concerné (sera l'objet d'une présentation à la BlackHat Las Vegas)

LDAP Injection & Blind LDAP Injection

□ Quelles sont les attaques d'injection sur LDAP ?

- ✓ Rappel sur LDAP (protocole d'accès, orienté objet, standard)
- ✓ L'AD de Microsoft et OpenLDAP n'utilisent que le premier filtre fourni, les autres sont ignorés
- ✓ Différents exemples d'attaques
 - Injection « classique » (désactivation du filtrage, condition toujours vraie)
 - Blind LDAP Injection (identique au SQL)
- ✓ Recommandations: les mêmes que pour le SQL: filtrer les variables en entrée, bien construire les requêtes, etc

□ **Présentation du framework Maltego, version 2**

- ✓ Utilisation de moyens gratuits (moteurs de recherche, Whois, ...) afin de corréler des informations
- ✓ Comment associer une adresse mail à un numéro de téléphone ?
- ✓ Principes
 - Récupération des informations selon certains critères (confiance dans la source,
 - Transformation de celles-ci en d'autres (cœur du framework)
 - Extension simple
- ✓ Interface graphique (entités, liens, poids, ...)
- ✓ A suivre !

Security failures in security devices

□ Etat de l'art de la sécurité des circuits intégrés

- ✓ Les datasheets mentent
 - « The most secure hardware token in the world »
 - « Security optimized layout and layout scrambling »
- ✓ Le master password « Write7 »
- ✓ Le bulk-erase est contournable et on récupère les données
- ✓ Le scrambling du bus de données est inefficace
- ✓ Aujourd'hui toutes les techniques de protection des IC ont été cassées

Side channel analysis on embedded systems

□ **Attaques et contremesures des systèmes de sécurité embarqués**

- ✓ Cassage de clé DES/RSA et attaques DPA/SPA
 - Et contre-mesures
 - ✓ Limiter le nombre d'opérations
 - ✓ Générer du « bruit »
 - ✓ Shuffling, Masking, Nop sled, tolérance de fuites
 - ✓ Licences CRI

Development in Cisco IOS forensics

□ Analyse post-mortem de dumps mémoire IOS

✓ Analyse du core dump

- Reconstruction de la heap
- Liste des processus
- Signatures d'images IOS
- Extraction du trafic en CPU switching

✓ Manque de maturité

- Dans le nombre d'information récupérées
- Dans le nombre de plateformes supportées

Exposing vulnerabilities in media software

□ Fuzzing des formats de fichiers audio et vidéo

✓ Vecteurs d'attaques

- Metadonnées

- ✓ Commentaires, titre de l'album, ...

- Trame

- ✓ Sample rate, nombre de trames, channels, ...

✓ Fuzzbox

- Etude de cas du format libre Ogg Vorbis

- ✓ Chaînes aléatoires, bugs de format

- ✓ Chaque trame Ogg a un CRC

- ✓ PT_DENY_ATTACH pour anti-anti-debugging iTunes

0-day patch – Exposing vendors (in)security perfs

□ Une nouvelle métrique pour la sécurité des OS

✓ 0-day patch

- Pleins de sources différentes en base de vulnérabilités
- Réduction du temps entre disclosure et patch
- Exemple Microsoft vs Apple

Biologger – A biometric keylogger

□ Sécurité des systèmes biométriques

- ✓ Entre le lecteur et le serveur stockant les empreintes, la communication est en UDP et non chiffrée
 - Man in the middle
 - Scripts de quelques lignes en python
 - Paint c'est super
 - Biométrie != Sécurité

Mobile phone spying tools

□ Espionner l'usage d'un téléphone portable

✓ On peut récupérer

- SMS/MMS, e-mail, statistiques des appels , enregistrement des conversations dans la carte mémoire, écoute distante avec un appel silencieux, coordonnées GPS, enregistrement des frappes de touches

✓ Détecter un téléphone espionné

- Aucun outil ne peut échapper à la facture de l'opérateur
- Reniflage des paquets TCP/IP + présence icône GPRS
- Analyse du système de fichiers et des processus

Malware on the net – Behind the scenes

□ Transition du malware vers le crimeware

- ✓ Vecteurs d'attaques invisibles pour
 - Antivirus, IPS, pare-feux, filtrage d'URL, bases de réputation
- ✓ Et difficiles à arrêter
 - Obfuscation de code dynamique
 - Mises à jour automatiques
- ✓ Ca rapporte combien ?
 - Pas mal ...
- ✓ Idées pour le futur
 - Web 2.0, Flux RSS, gadgets Vista



- diffusion publique -



Spam-Evolution

□ Etat de l'art du SPAM

✓ Des problèmes difficiles à résoudre

- Le facteur humain, zombies, ...
- Réputation de gmail, yahoo, hotmail,...

✓ Technologies antispam

- Sécurité sur les postes de travail ou dans l'infrastructure
- Listes Black/Grey/White IP/DNS, SPF, DKIM, hashCash, filtres sur contenu, signatures, OCR, systèmes de réputation
- N'oubliez pas de filtrer les mails en sortie ...



- diffusion publique -



Intercepting mobile phone/GSM traffic

□ La sécurité est entre le téléphone et le BTS

✓ Réception

- Avec un téléphone, USRP
- IMSI
- A5/x

✓ Déchiffrement de communications A5/1

- En 6 minutes
- 68 pico E-16 FPGA
- Rainbow tables (2To !) – 3 mois pour les générer

Antiphishing security strategy

□ Les établissements financiers sont toujours la cible favorite

- ✓ Nouvelles méthodes utilisées par les phishers
 - Hyperliens vers un serveur malicieux depuis un vrai site web, URL obfusquées, malwares installant un BHO, corruption du fichier hosts
- ✓ Stratégies de défense basées sur le poste de travail
 - Blacklists
 - Similarités visuelles
 - Circulation des informations (DomAntiPhish)

Hacking Second Life

□ Second life en tant que proxy

✓ Architecture client/serveur

- Clients SL viewer « open-source »
- Password.dat
- Aucune best practice appliquée sur les serveurs

✓ Lancement d'attaques depuis SL

- Spam
- Injections SQL
- Slikto
- Méfiez-vous des objets

New viral threats of PDF language

□ Le langage PDF n'est pas sécurisé

✓ Détournement des primitives

- OPENACTION
- ACTION
- Positions dans le PDF, lancement d'exécutables, vol de données, phishing

✓ Du point de vue de l'OS

- Attaques sur fichiers acord32.dll, rdlang32.xxx
- Diverses clés dans la base de registre

Pour finir

- ❑ **A part la keynote, pas de grande nouveauté**
- ❑ **Présentations variées, plutôt techniques**
- ❑ **Pas toujours des recommandations**
- ❑ **Mais un événement très intéressant !**
- ❑ **Merci à l'OSSIR**

Questions

