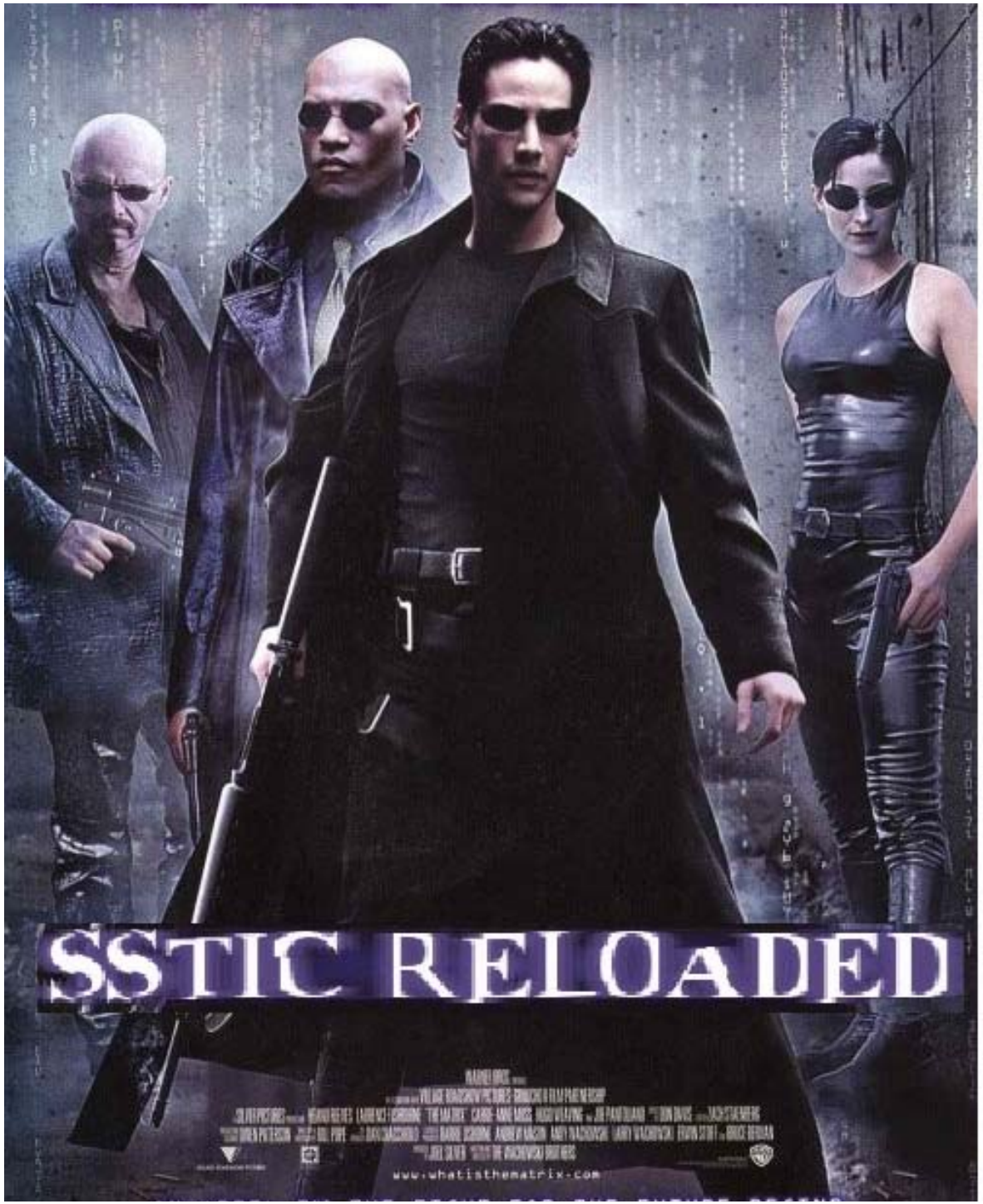


OSSIR Bretagne
17 juin 2008

Présentation résumée du SSTIC 2008

J.P. Gaulier
O. Heen

http://www.ossir.org/bretagne

Objectif

« Réconforter » ceux qui n’ont pas pu assister

Montrer la diversité des thèmes abordés

Donner une idée de l’ambiance

Renvoyer vers les actes et les présentations en ligne sur http://actes.sstic.org/SSTIC08/

Avertissement : en une heure il est impossible de faire une restitution exacte, certaines présentations que nous jugeons pourtant excellentes ne seront donc pas évoquées…


Avenue Charles Tillon
Rennes 1 - Amphi Louis Antoine - SSTIC 2008
Avenue des Préales
Rue de Nantes
Rue de l'Alma
Rennes 1 - Amphi Louis Antoine - SSTIC 2008
Rennes 1 - Amphi Louis Antoine - SSTIC 2008
ouis Antoine - SSTIC 2008

22 présentations

Répartition par source (cf. http://digikod.net)

- 12 sociétés privées
- 8 institutions publiques
- 2 indépendants

Répartition par technicité (subjectif…)

- Technique : 9 (débogage, retro-ingé…)
- Peu technique : 7
- Non technique : 6 (juridique, organisationnel…)

430 participants

3 jours de sécurité intensive

Sécurité : anatomie d'un désastre annoncé M. RANUM

Identification et exploit. des failles humaines […] M. IWOCHEWITSCH

Activation des C.À.P. sans contact à l'insu […] C. MOURTEL

L'expertise judiciaire des téléphones mobiles D. NACCACHE

Outils d'intrusion automatisée : risques et protections M. BLANC

Bogues ou piégeages des processeurs […] L. DUFLOT

[…] observations in vivo d'un banker F. CHARPENTIER, Y. HAMON

GenDbg : un débogueur générique J.M. FRAYGEFOND, D. EYMERY

Avertissement : Seuls les noms des présentateurs sont indiqués, pour la liste complète des auteurs, consulter http://www.sstic.org/SSTIC08/programme.do. les titres abrégés sont signalés par […]

3 jours de sécurité intensive

Sécurisation, […] Green Data Centers	C. WEISS
Déprotection semi-autom. de binaire	A. GAZET, Y. GUILLOT
ERESI: plate-forme d'analyse binaire […]	A. DESNOS, S. ROY
Cryptographie : attaques tous azimuts	J.B. BEDRUNE
Sécurité dans les réseaux de capteurs	C. CASTELLUCCIA
Dépérimétrisation	C. BLANCHER

Pentests : "Réveillez-moi, je suis en plein cauchemar !"

Marie BAREL

Rump sessions

Avertissement : Seuls les noms des présentateurs sont indiqués, pour la liste complète des auteurs, consulter http://www.sstic.org/SSTIC08/programme.do. les titres abrégés sont signalés par […]

3 jours de sécurité intensive

Une Architecture de Bureaux Graphiques Distants […] J. ROUZAUD-CORNABAS

Walk on the Wild side G. ARCAS

SinFP, unification de la prise d'empreinte […] P. AUFFRET

Recueil et analyse de la preuve numérique […] N. DUVINAGE

Voyage au coeur de la mémoire D. AUMAITRE

R&D en sécurité des SI […] F. CHABAUD

Dynamic Malware Analysis for dummies P. LAGADEC

Avertissement : Seuls les noms des présentateurs sont indiqués, pour la liste complète des auteurs, consulter http://www.sstic.org/SSTIC08/programme.do. les titres abrégés sont signalés par […]

Zoom 1 : Damien Aumaitre
Voyage au cœur de la mémoire

Présentation d'une « Lunch time attack »

- Bref accès physique

Basée sur un accès DMA

- Direct Memory Access
- Basée sur les travaux de M. Dornseif (2005)
- et A. Boileau (2006)
- Mais réellement publiée, complète, plus facile mettre en œuvre, plus rapide…

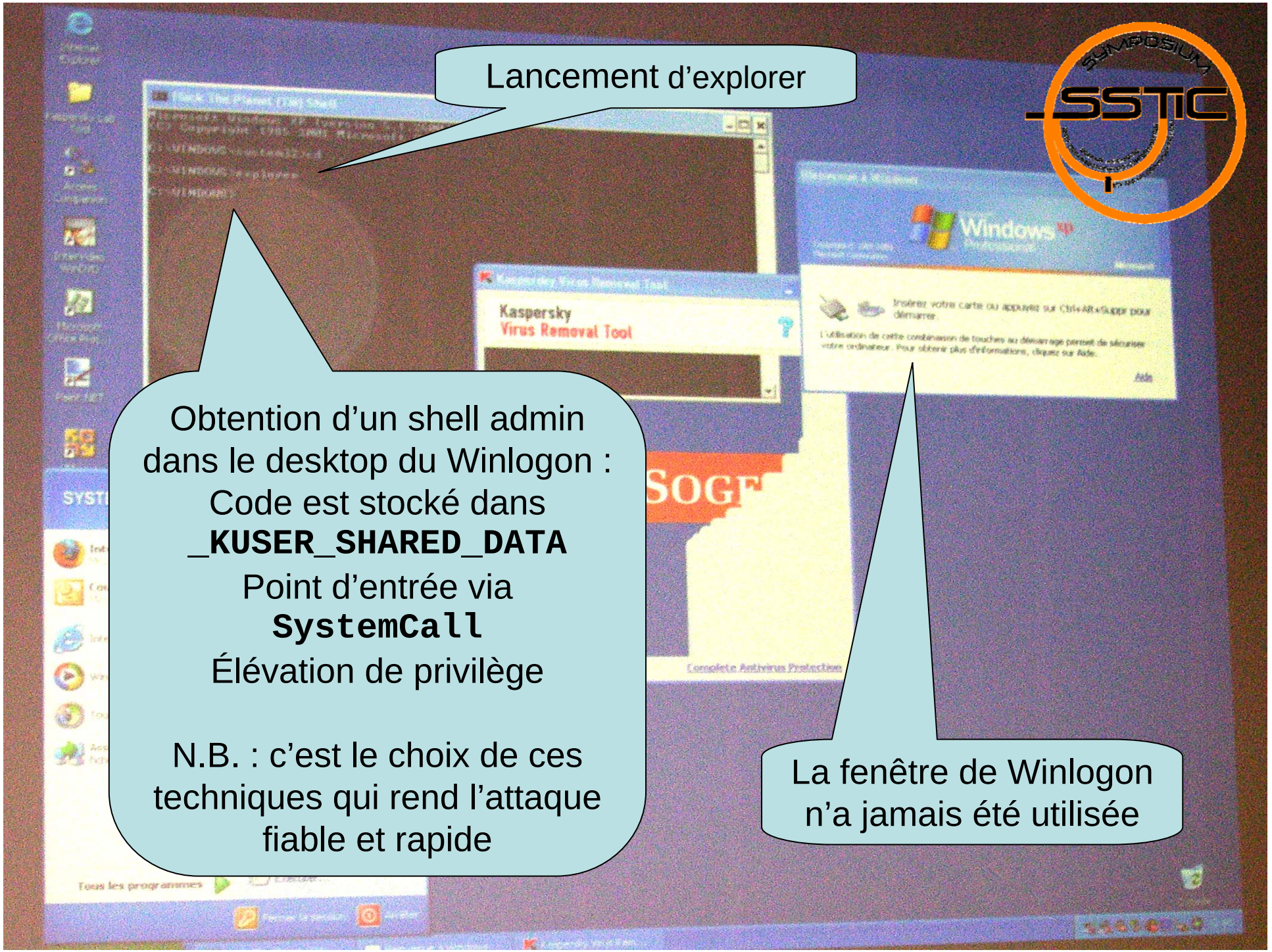
Voir aussi le résumé par Ludovic Blin sur http://www.secuobs.com/news/15062008-dma_firewire.shtml

Zoom 1 : Damien Aumaitre
Voyage au cœur de la mémoire

Principe

1. Firewire utilise le DMA pour faire communiquer un périphérique avec la mémoire d'un PC
2. Le DMA en mode *bus mastering* donne le contrôle de la mémoire au périphérique, afin d'éviter de solliciter le microprocesseur
3. L'accès est interdit par défaut sous Windows, sauf pour les périphériques de masse (e.g. iPod)
4. Un PC peut changer sa « carte d'identité » Firewire via **`raw1394_update_config_rom`**

Et donc…


Lancement d'explorer
Obtention d'un shell admin dans le desktop du Winlogon :
Code est stocké dans
_KUSER_SHARED_DATA
Point d'entrée via
SystemCall
Élévation de privilège
N.B. : c'est le choix de ces techniques qui rend l'attaque fiable et rapide
La fenêtre de Winlogon n'a jamais été utilisée
Kaspersky
Virus Removal Tool
Windows XP
SSTIC
SYMPOSIUM

Zoom 2 : Michel IWOCHEWITSCH

Identification et exploitation des failles humaines par les prédateurs informationnels : un risque sous-estimé par les entreprises ?

Deux types de prédateur

- One-shot
- long-terme

Les « valeurs » de l'information

- pécuniaire
- intégrité de l'information
- confidentialité
- disponibilité
- coût de nuisance
- l'opposition

Zoom 2 : Michel IWOCHEWITSCH

Identification et exploitation des failles humaines par les prédateurs informationnels : un risque sous-estimé par les entreprises ?

Les acronymes de la manipulation

MICE Money ; Ideology ; Coercion; Ego

ASIE Argent, Sexe, Intellect, Ego

SANSOUCIS Solitude, Argent, Nouveautés, Sexe, Orgueil, Utilité, Contrainte, Idéologie, Suffisance

Le profil des cibles

La personne immature, Le « héros »

L'amateur d'intrigue, L'insatisfait

Le solitaire, L'intellectuel

Zoom 2 : Michel IWOCHEWITSCH

Identification et exploitation des failles humaines par les prédateurs informationnels : un risque sous-estimé par les entreprises ?

Process d'acquisition d'une cible

1- Spotting
2- Assessing
3- Development
4- Pitching
5- Formalizing
6- Producing
7- Terminating

Peut-on se protéger ?

oui, en partie…

RUMP Sessions

Annonce de C&ESAR 2008
SSTIC, canal historique
CSRF, nouveau DoS
NF3D, le Netfilter Hero
Nouvelle section SSI à supélec
Muff'in, plug-in IDA
Hybrid Network System (hynesym)
EAP, vulnérabilité sur les AAA
Les impôts et openssl
Exefilter && blind FTP
Faiblesses dans les extensions de firefox

Cracker, crypto packer
Photorec, la suite
Weatherwall
Documentation de Scapy
DRP en Suisse
Le SOC
Hack du cerveau
Visualisation cubique
Un test de QI
HP m'a tuer
La spirale infernale

Zoom 3 : Florent CHABAUD

Recherche et développement en sécurité des systèmes d'information : orientations et enjeux

Un problème de souveraineté : *"Protéger l'autonomie de décision de l'État au delà des frontières, même numériques"*

- Cisco contrefait en Chine et livré au gouvernement US
- Espiogiciel MS Windows et clé USB forensic
- Vol de numéro de CB pendant des mois (Hannaford)
- Marché noir de la cyberdélinquance

Zoom 3 : Florent CHABAUD

Recherche et développement en sécurité des systèmes d'information : orientations et enjeux

Mais que fait la recherche ?

Points forts

- Crypto
- Méthodes formelles

Points faibles

- OS
- Protocoles réseaux
- Architecture matérielle

"La recherche ne doit pas attendre l'industrie"

Zoom 3 : Florent CHABAUD

Recherche et développement en sécurité des systèmes d'information : orientations et enjeux

Six idées stupides (propositions de réponse)

Tout ce qui n'est pas autorisé est interdit !

Recenser oui... quand il y a peu de vulnérabilités !

Corriger oui... mais quand cela a du sens et qu'on en a les moyens techniques !

Cela n'empêche pas d'étudier les méthodes d'attaque !

Sensibiliser les utilisateurs non, les décideurs oui !

Mais ne rien faire dans des pans entiers de la SSI c'est suicidaire !

Zoom 3 : Florent CHABAUD

Recherche et développement en sécurité des systèmes d'information : orientations et enjeux

214/2008

Programme Systèmes Embarqués et Grandes Infrastructures
Défi Sécurité – Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute

- Edition 2008 -

Liste des projets sélectionnés (par ordre alphabétique) :

Acronyme et titre du projet	Coordinateur
OSOSOSOS : Système d'(O)exploitation Sécurisé Open Source (O) et Simple	Louis GRANBOULAN
Safe OS : Système d'exploitation Sécurisé	Thomas HÉRAULT
SPACLik : Sécurité et Propriétés des Applications Contrôlées au sein d'un Linux Kernel	Christian TOINARD

Source http://www.agence-nationale-recherche.fr/documents/aap/2008/selection/SEC-SI-2008.pdf

Pour en savoir plus

Blogs, photos(*), commentaires…

http://www.sstic.org/SSTIC08/presse.do

Lectures

http://actes.sstic.org/SSTIC08/

Infos OSSIR Bretagne

ossirb-request@ossir.org

http://www.ossir.org/bretagne/

(*) Dont certaines photos utilisées dans cette présentation

Dernière minute : on nous signale un mouvement subversif sur http://www.sstic-canalhistorique.org/