2013

Wrap-Up

Quack1

http://quack1.me/tag/sstic-2013.html

SSTIC 2013

5, 6 & 7 Juin 2013

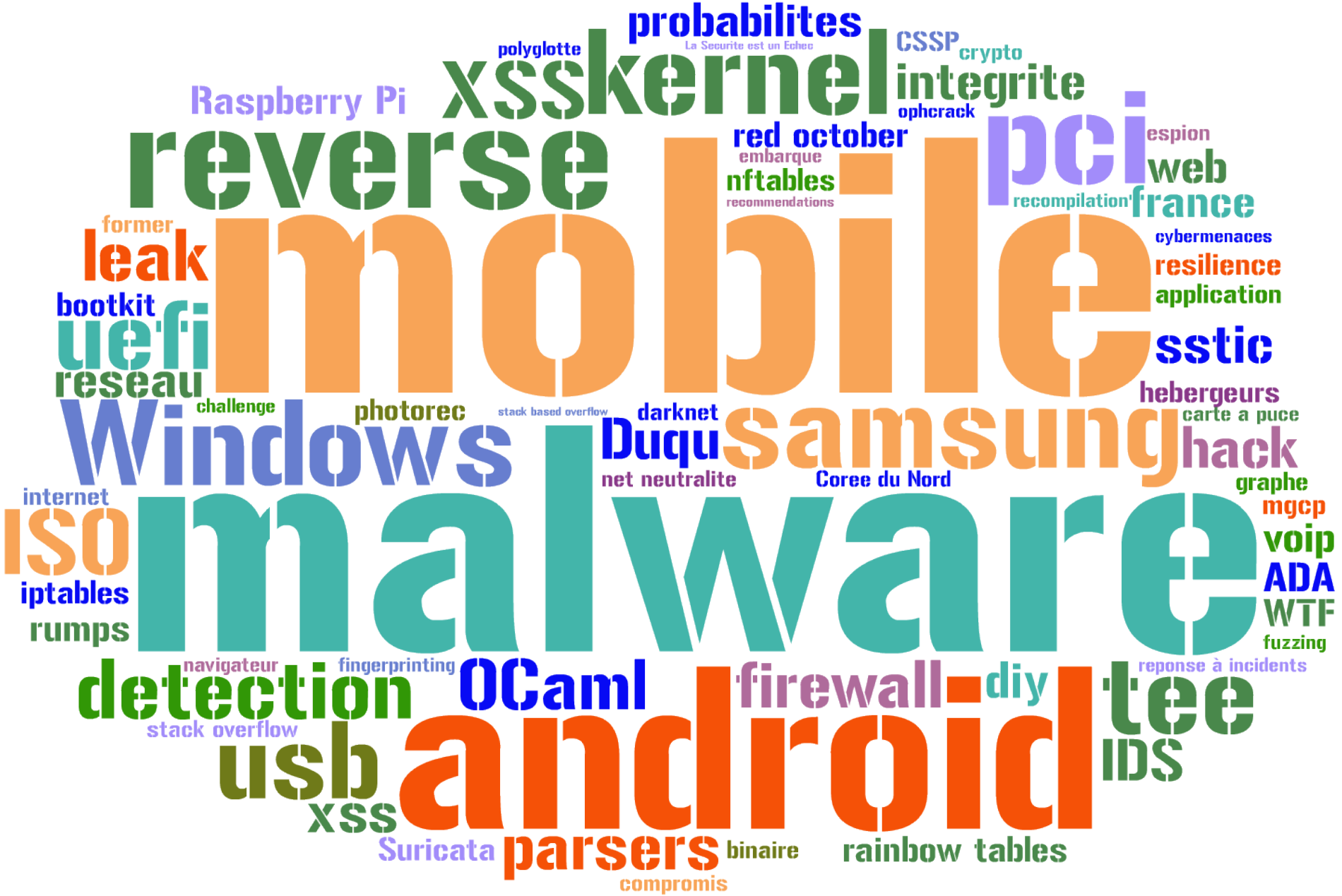
11ème édition

Rennes

29 présentations (+ 21 *Rumps*)

430 participants

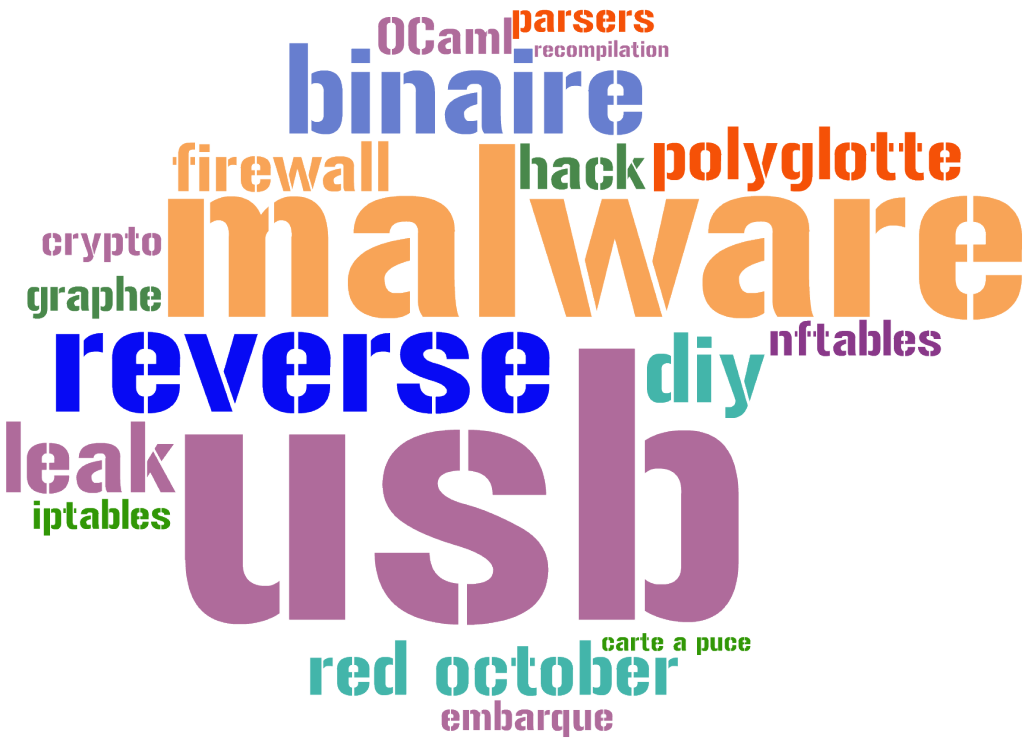
(Et de la bière, des 0day, des crêpes, du troll...)


probabilites
polyglotte
La Securite est un Echec
CSSP
crypto
xss
kernel
integrite
Raspberry Pi
ophcrack
reverse
red october
pci
espion
embarque
nftables
web
recommendations
recompilation
france
former
leak
mobile
cybermenaces
resilience
bootkit
application
uefi
sstic
reseau
hebergeurs
challenge
photorec
stack based overflow
darknet
Windows
samsung
carte a puce
Duqu
hack
net neutralite
Coree du Nord
graphe
internet
malware
mgcp
ISO
voip
iptables
ADA
rumps
WTF
fuzzing
navigateur
fingerprinting
reponse à incidents
detection
OCaml
firewall
diy
tee
stack overflow
android
IDS
usb
xss
Suricata
parsers
binaire
rainbow tables
compromis

1er jour

Mon TOP :

1. Polyglottes binaires et implications
2. Attaques applicatives via périphériques USB modifiés
3. (L')Embarqué entre Confiance et Défiance ?



Innovations en crypto symétrique

Joan Daemen (MTElectronics)

« On m'a demandé de vous expliquer comment on faisait des standards.

Sauf que je sais pas comment on fait. »

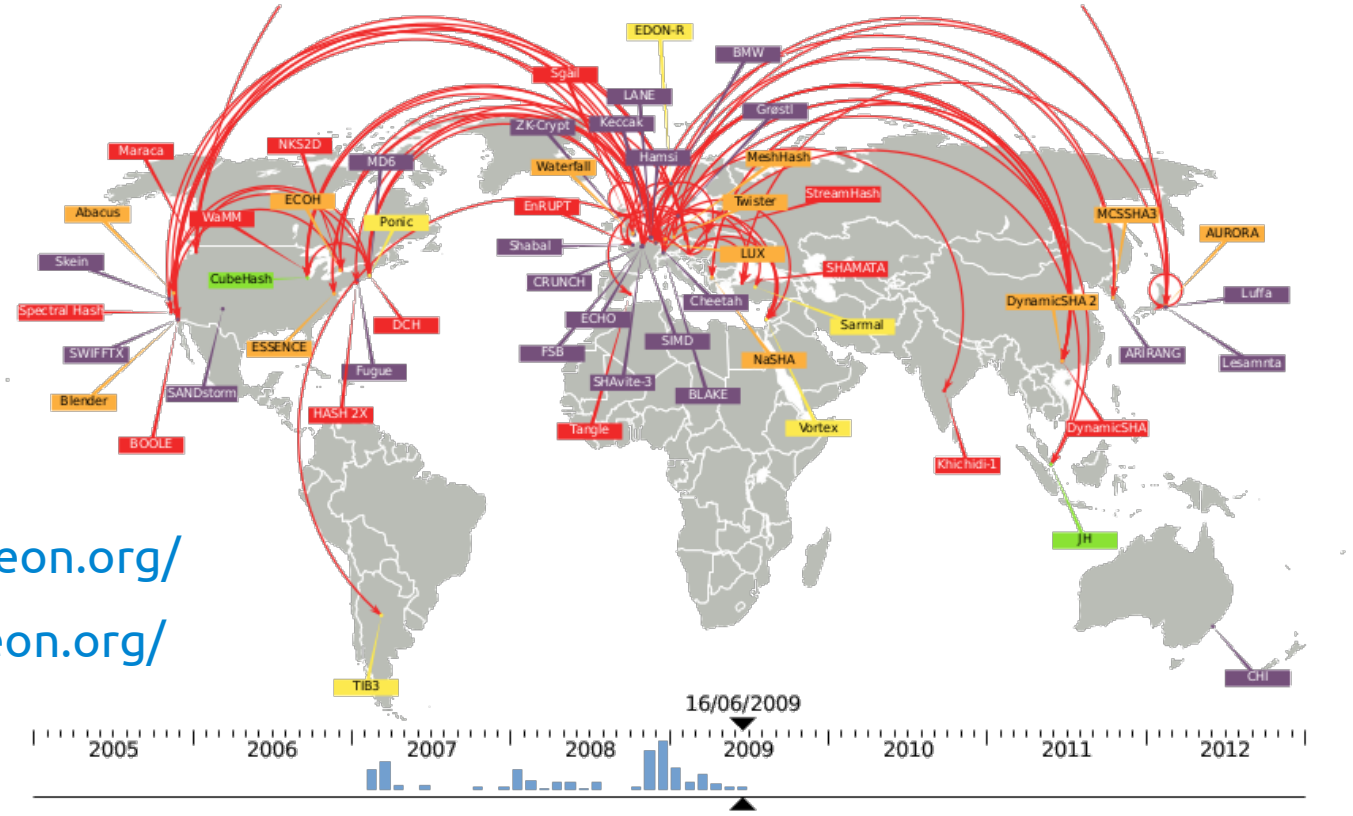
Et pourtant...

2 défis du NIST

- Rijndael → AES
- Keccak → SHA-3

Quelques liens :

- http://sponge.noekeon.org/
- http://keccak.noekeon.org/



[courtesy of Christophe De Cannière]

Ingrédients pour faire de bons protocoles :

→ Essayer beaucoup d'idées

Jeter la plupart d'entre elles

Garder les bonnes

→ Avoir une équipe avec des compétences complémentaires

Confronter ses idées

→ Pas trop d'ego

→ Tout ré-écrire plutôt que patcher

Privilégier la simplicité

Mise à plat de graphes de flot de contrôle et exécution symbolique

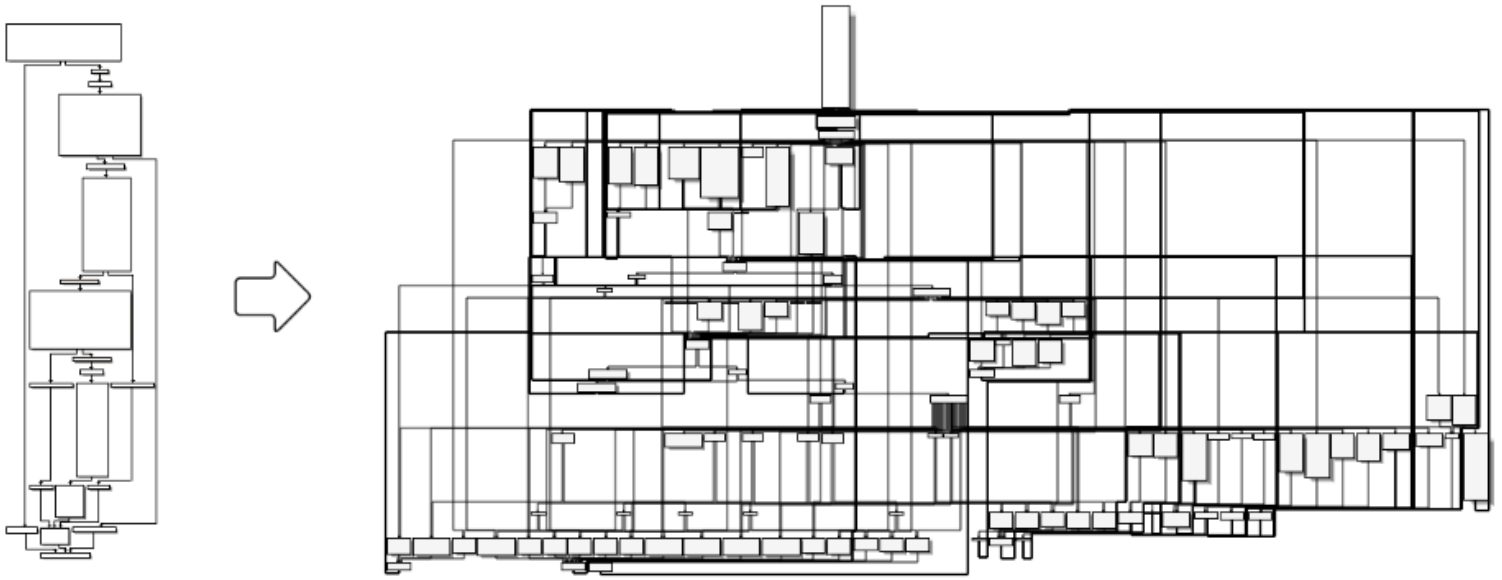
Eloi Vanderbéken (OPPIDA)

Code « brouillé » → Reconstruction du graphe de flot

Analyses dynamiques (exécution, données) vs Analyse statique

Analyse complète du code

Réécriture d'un exécutable « propre »



Polyglottes binaires et implications

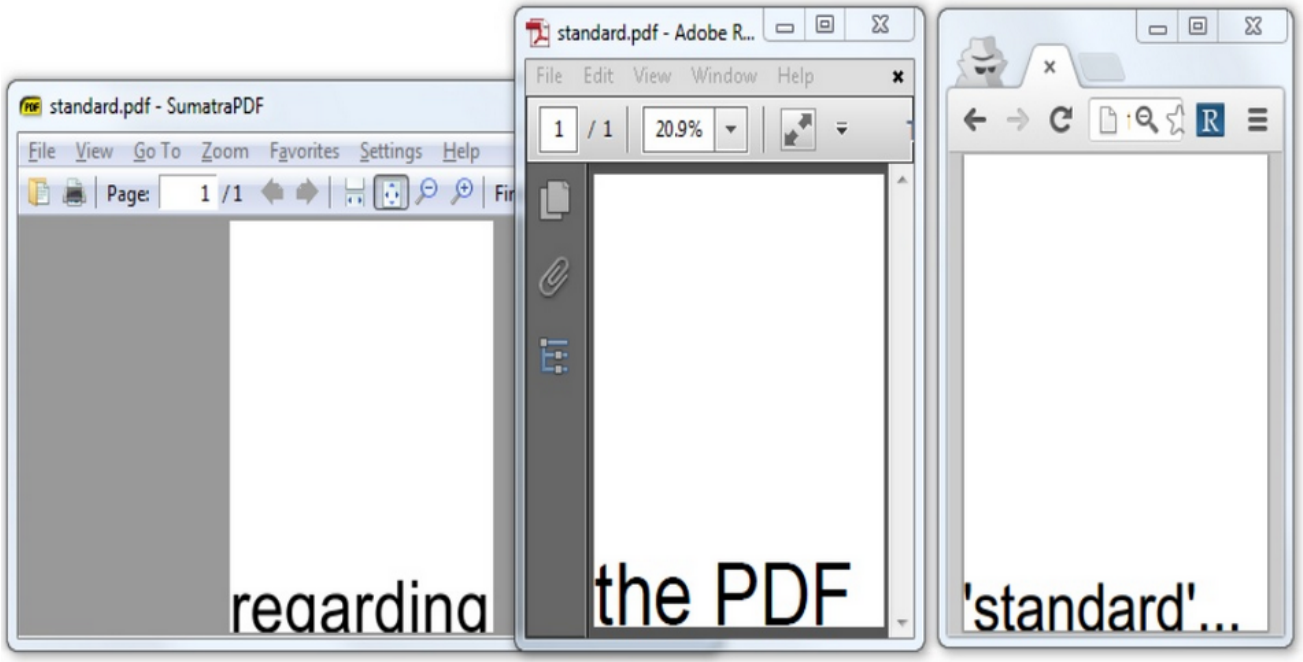
Ange Albertini (Corkami.com)

Fichier polyglotte : plusieurs fichiers de types différents en un

Plusieurs fichiers du même type (PDF) affiché différemment selon le lecteur

« Chrome, c'est n'importe quoi,Sumatra c'est n'importe quoi,

Adobe c'est n'importe quoi, mais c'est le moins pire de tous. »



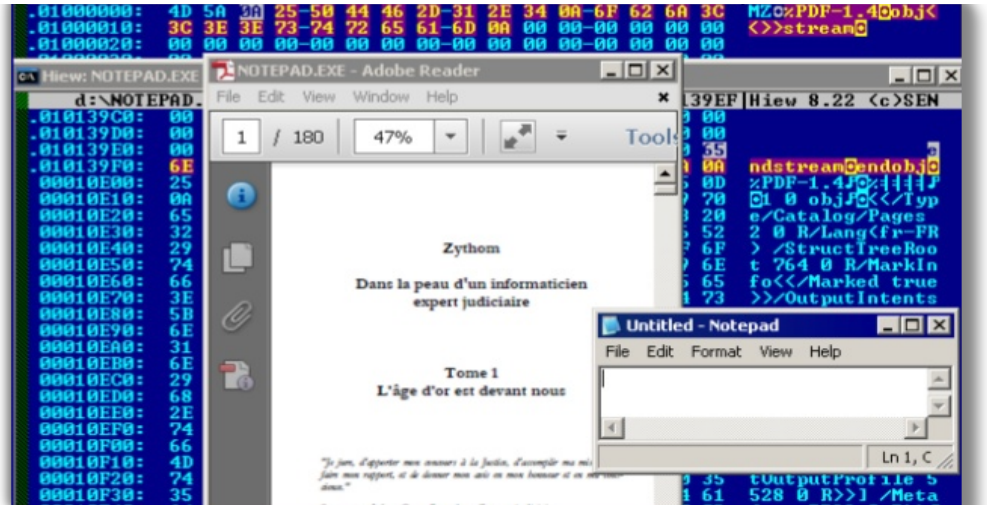
Dans la pratique

PE + PDF + HTML/Javascript + Java

Laxisme

- des formats de fichiers
- des interpréteurs

Contournement d'antivirus/firewall



Recompilation de codes binaires hostiles

Sébastien Josse (DGA)

- Pas d'outil universel d'analyse de malware
- Outil de désobfuscation/analyse :
  - Unpacking
  - Recompilation pour une machine virtuelle
  - Analyse du malware
- Ré-utilisation d'outils existants

Présentations Courtes

Persifal, ou comment écrire des parsers robustes — *Olivier Levillain (ANSSI)*

- Simplifier l'écriture de parsers
- 1 classe Ocaml ↔ 1 protocole
- https://github.com/ANSSI-FR/parsifal

nftables : bien plus que %s/ip/nf/g/ — *Eric Leblond (OISF)*

- Coreteam iptables & Suricata
  - Mainteneur du Firewall OpenOffice : https://www.wzdftpd.net/blog/index.php?post/2010/06/16/46-le-pare-feu-openoffice
- Refonte du core d'iptables + Nouveau format de règles
- Meilleures performances

Mode ligne de commande

```
nft add rule ip filter input tcp dport 80 drop
nft list table filter -a
nft delete rule filter output handle 10
```

Compromission d'un terminal sécurisé via l'interface carte à puce

Guillaume Vinet (SERMA)

Nouveau paradigme :

- Attaques sur la carte vs Attaques sur le terminal

Émulateur de carte à puce

- Arduino + Python
- Difficilement détectable

Attaques « classiques »

- Buffer Overflow
- Failles dans l'implémentation des protocoles

Plusieurs failles :

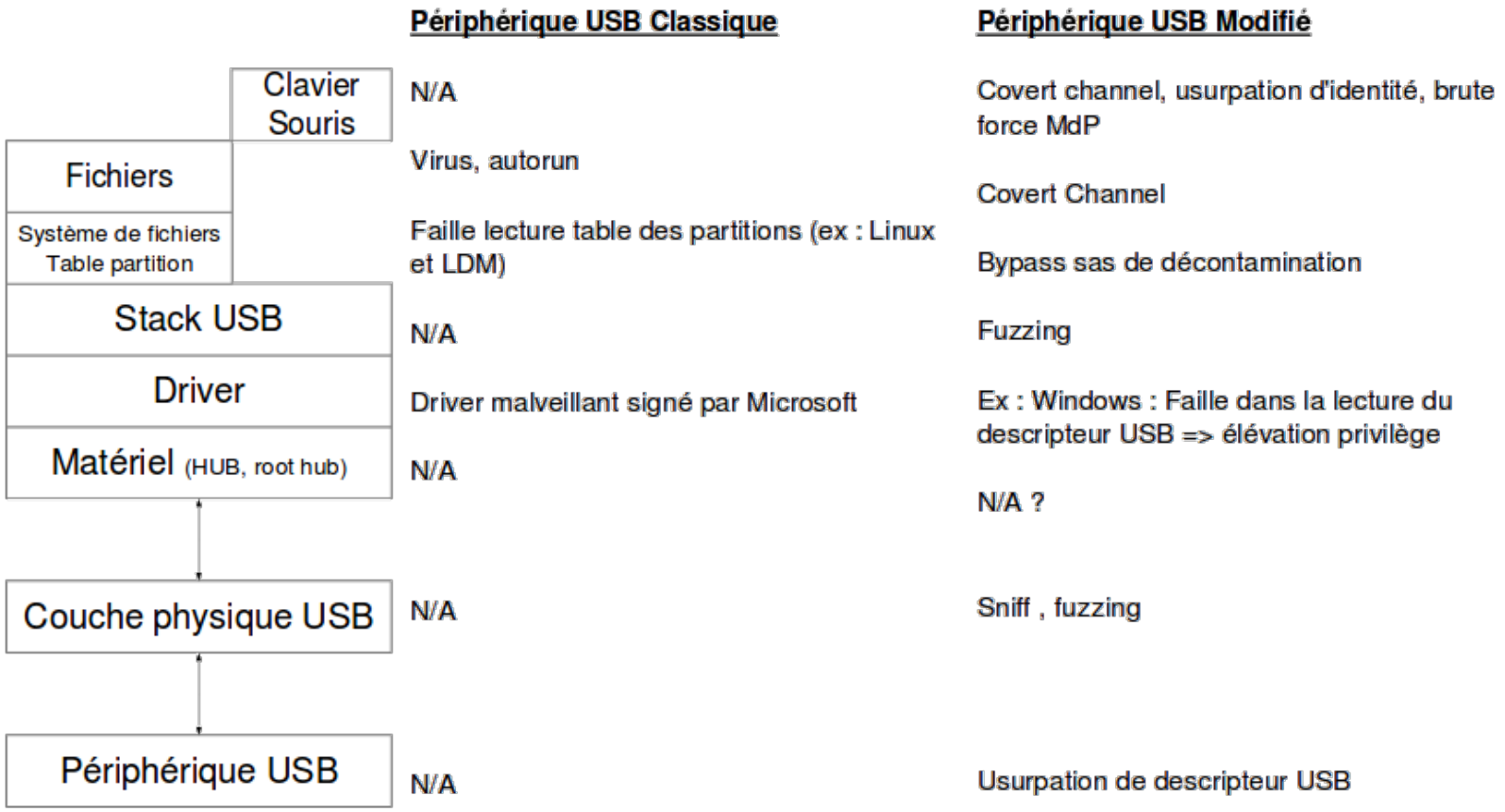
- Dump du firmware
- Dump de la RAM

Attaques applicatives via périphériques USB modifiés : infection virale et fuite d'informations

Benoît Badrignans (SECLAB FR)

USB limité en entreprise

Clé USB modifiée : surface d'attaque augmentée



Écriture sur une clé en *Read-Only*

GNU/Linux custom sur clé

Lecture à l'adresse 0xCAFEDECA sur la clé

La clé écrit sur elle-même la donnée 0xCAFEDECA

```
#opening comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1

for i in `cat $1 | hexdump -v -e '/1 "%02u\n"'`
do
    echo $i
    dd iflag=direct if=$OUTPUT_FILE of=/dev/null bs=512 count=1 skip=$i
done

#closing comm
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1 skip=1
dd iflag=direct if=$CMD_FILE of=/dev/null bs=512 count=1
```

Infection automatisée d'une machine sans *autorun*

Ø d'antivirus – Ø accès au SI – Sas de décontamination USB

Sas de décontamination

Efface les fichiers vérolés

→ Affichage des « malwares » après *X* branchements

Autorun

→ Clé usb → Clavier/Souris USB

Le « clavier » USB tape les commandes qui vont exécuter le programme stocké sur la clé

Red October

Nicolas Brulez (Kaspersky)

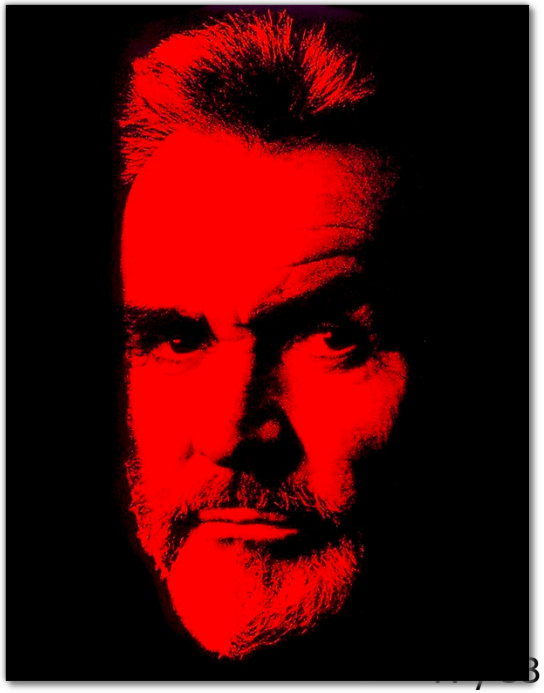
Attaque par malwares

2007 → 2013

Gouvernements / Services diplomatiques

Recueillement d'informations

C&C : 60 noms de domaines



Infrastructure d'une attaque

Processus

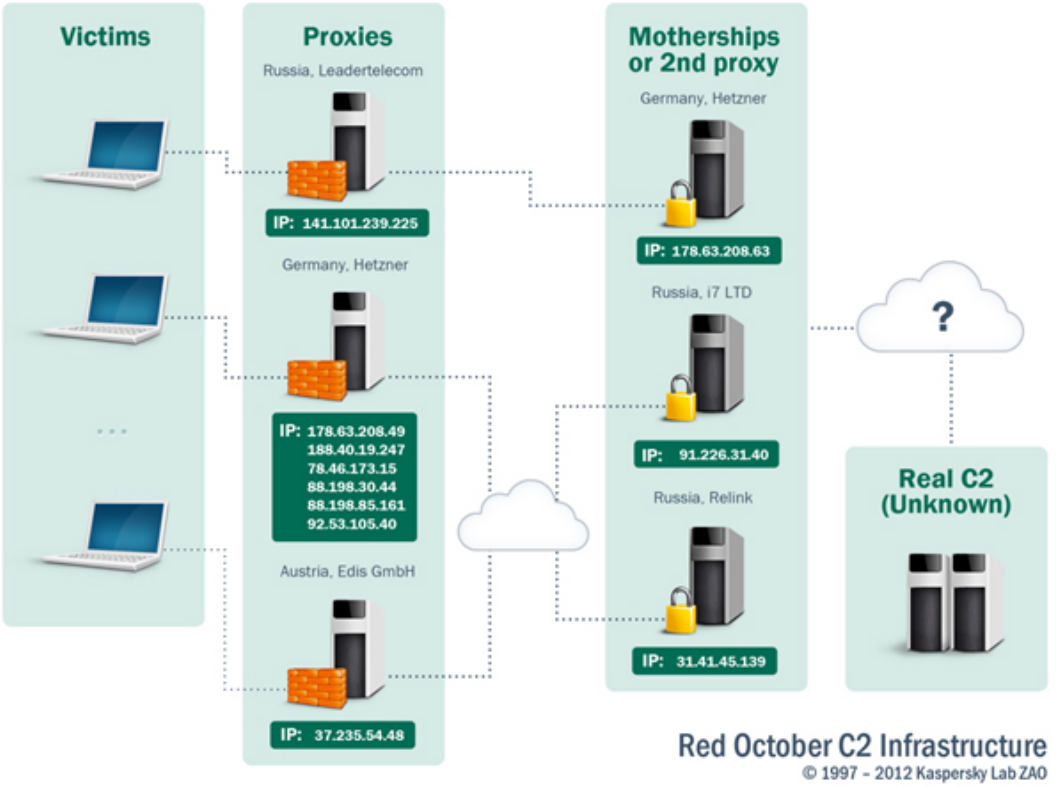
- Spear-Phishing
- Failles/Exploits connus (Ø 0-Day) Word/Excel

Grande ampleur

- 10 vagues d'attaques (espacées de ~2 mois)
- 1000 fichiers malveillants
- 30 modules

Multi-plateforme

- Windows
- Blackberry
- iPhone



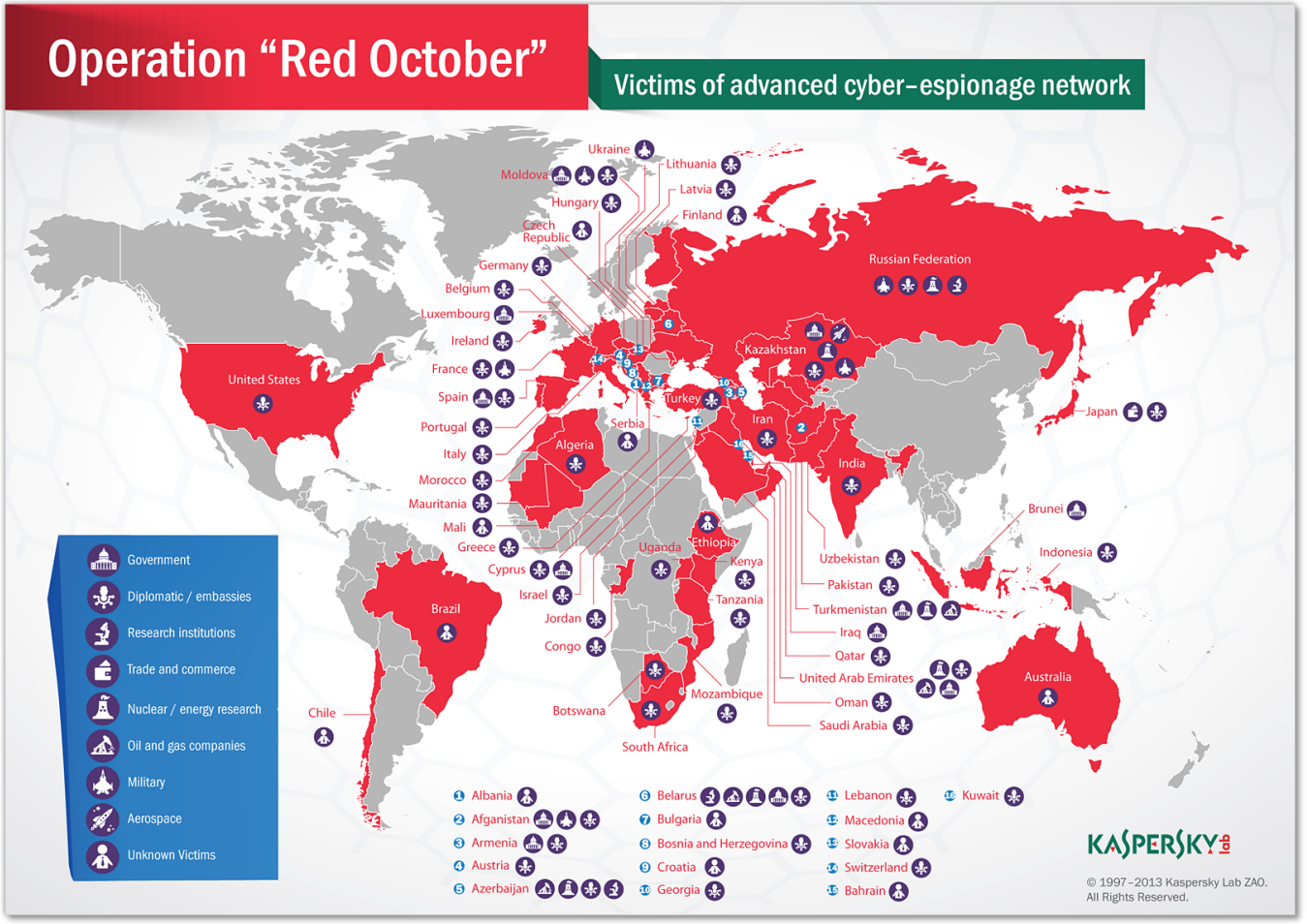
Cibles

300 entités infectées (4 en France)

Statistiques : *Sinkhole*

1 nom de domaine (C&C) mal enregistré par les attaquants

Enregistrement par Kaspersky pour stats



(L')Embarqué entre Confiance et Défiance ?

Aurelien Francillon (Eurecom)

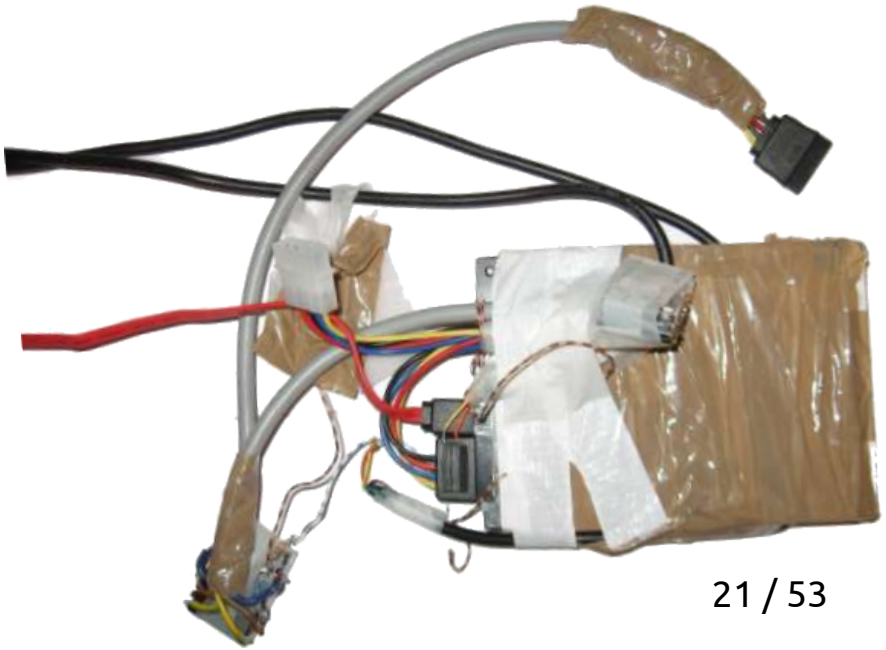
Confiance dans l'embarqué ?

Backdoor gouvernementale dans le *Baseband* du HTC G1

- Un stagiaire qui s'ennuyait y a fait tourner un kernel GNU/Linux

Firmware des disques durs non signés

- Modifiables (presque) en un claquement de doigts



Please, drive me to the next level...

Clé de voiture *contactless*

P0wn3d

Si quelqu'un a une voiture avec une clé comme ça, on essaiera de faire une démo ;-)

ADS-B (Aviation)

Aucune sécurité

Cf BlackHat 2012

http://www.andreicostin.com/papers/adsb_blackhat12us_slides.pdf

2ème jour

Mon TOP :

1. Rumps
2. Compromission d'un environnement VoIP Cisco
3. La Couleur du Net
4. Social Event

UEFI

Dreamboot → Bootkit Windows 8 — *Sébastien Kaczmarek (QuarksLab)*

- Bypass authentification locale
- Escalade de privilèges
- Hooking du noyau

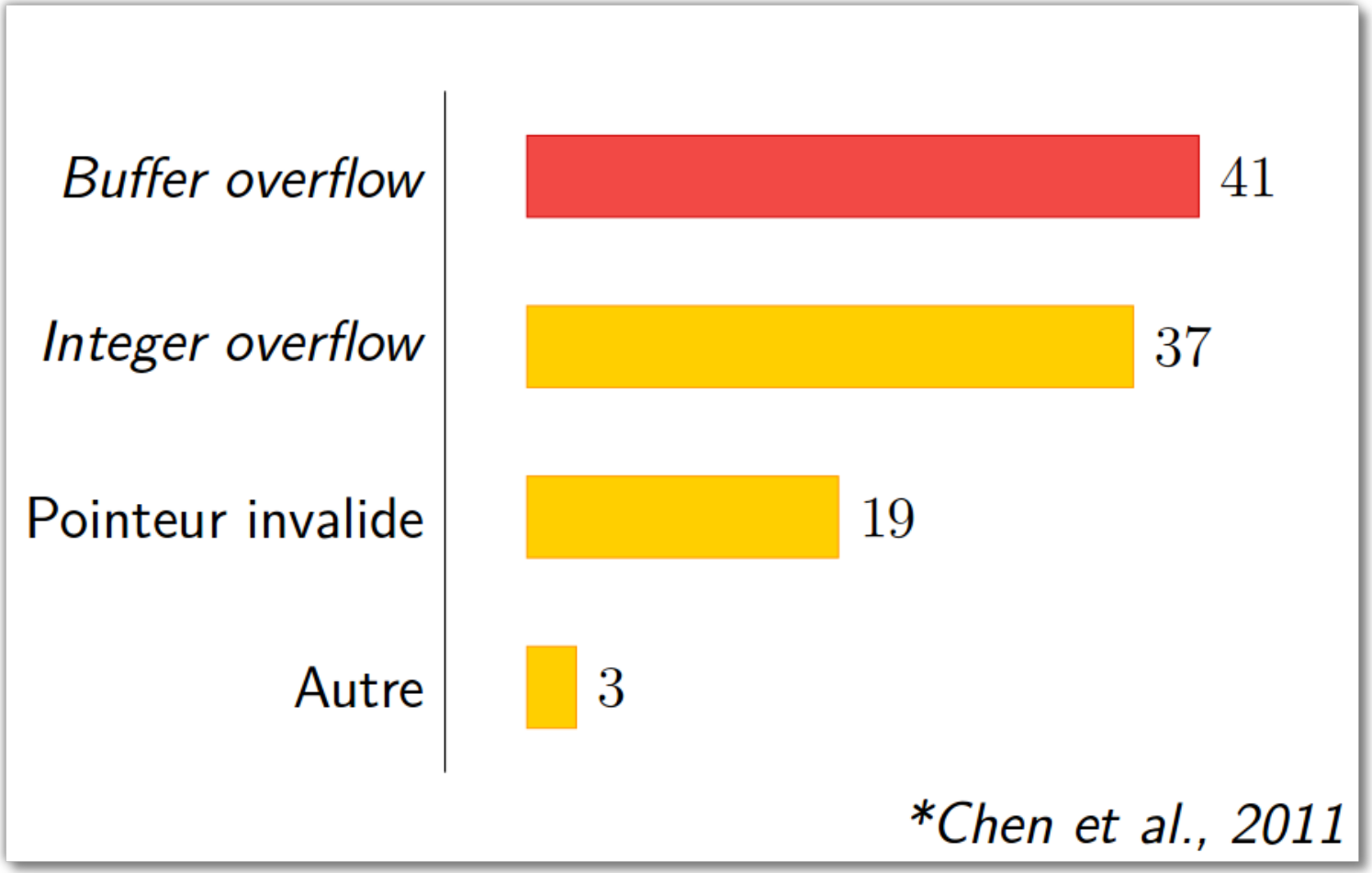
UEFI et Bootkits PCI — *Pierre Chifflier (ANSSI)*

- Bootkit via une carte graphique
- Difficulté d'accès à la ROM (*La route du ROM)*
- Modification de la ROM d'origine (Une ROM arrangée)

Développement d'un noyau sécurisé en Ada

Arnauld Michelizza (ANSSI)

Vulnérabilités critiques des OS ?



Kernel sans bogues ?

Être un Dieu de la programmation

Preuves formelles

- 200k lignes de preuve pour 8500 lignes de C
- 11 années-hommes

Langage sans *Overflow* → 80 % de bogues en moins

- Algol ?
- Java ?
- SafeC ?

Et si on le faisait en ADA ?

Kernel en ADA ?

Conception

- 11k lignes de code
- 1 an de développement
- amd64 / Multitâches / elf64
- Écran / clavier / disques ATA / Réseau / ext2 / IPv6

Performances ?

- 15 % cycles d'horloge en plus
- Taille : +70 %

Sécurité ?

- 80 % de vulnérabilités en moins
- Erreurs visibles
- Débogage facile

Challenge SSTIC

Émilien Girault (ANSSI)

PCAP

- Fichier chiffré over FTP
- Clé : canaux cachés

FPGA

- Implémentation d'un CPU « Harvard »
- Désassembler le programme exécuté
- Bruteforce de la clé

Postscript

- « Petit » programme à reverser

Vcard

- Dé-obfuscation
- Adresse email

Ça valait bien un ChromeBook:-)

La Couleur du Net

Laurent Chemla (Gandi)

Idée et réflexions sur la Liberté/Neutralité du Net

« Régulation » du Net

- Droits d'auteur
- Pédonazis
- Haine raciale
- Arnaques
- ...

Changements apportés à la société par Internet

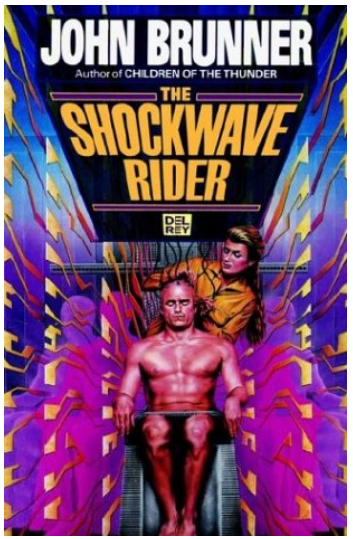
- Liberté d'expression
- Logiciel Libre

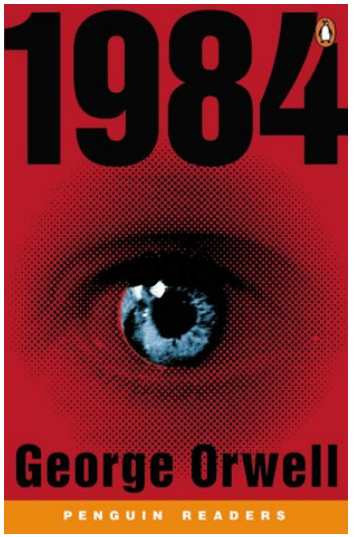
Neutre techniquement

Pas neutre socialement

Quelques phrases en vrac

« L'imprimerie a permis au gens de lire, Internet leur a permis d'écrire »





Présentations courtes

Hack Android/Samsung : à l'attaque du kernel — *Étienne Comet (Lexfo)*

- Linux 3.4 / ARM / Options de compilation «non auditées »
- Patchs kernel constructeurs
- *Détails techniques dans les slides*

Francisco (Lexfo)

Compromission d'un environnement de VoIP Cisco

- Call Manager
- 0-day
  - SQLi Informix
  - *Remote Code Execution*
  - Élévation de privilèges

Observatoire de la résilience de l'Internet Français — *Guillaume Valadon (ANSSI)*

- BGP → Usurpation de préfixes IP
- DNS → Beaucoup (80%) de zones DNS sur 1 seul AS
- IPv6 → 13 %

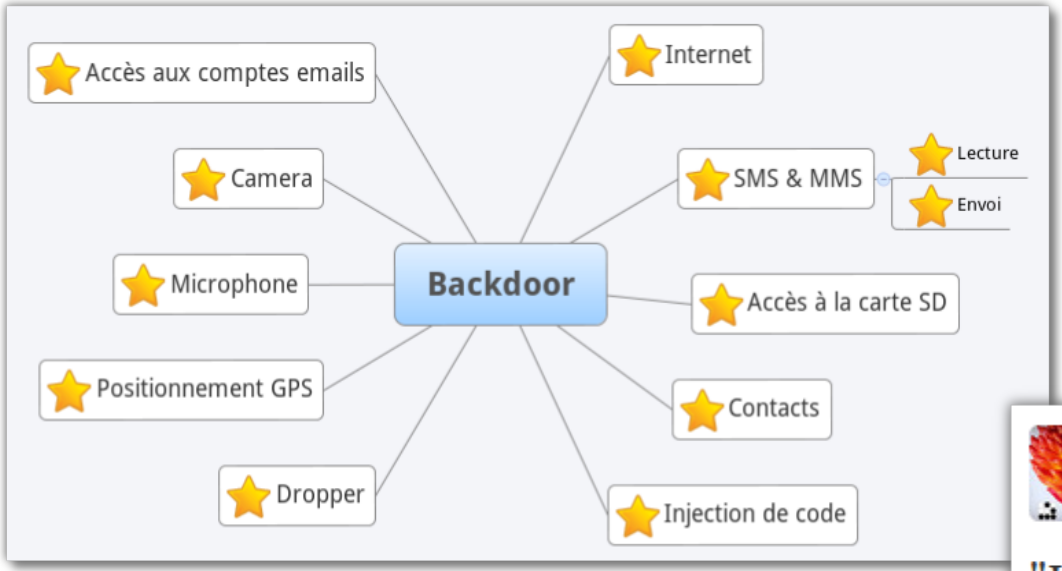
Sécurité des applications Android constructeurs et réalisation de backdoors sans permissions

André Moulu (QuarksLab)

Android bien sécurisé de base

Samsungs : 216 apps vs Nexus 4 : 91 apps

Surcouche trouée



Limites des Rainbow Tables et comment les dépasser en utilisant des méthodes probabilistes avancées

Cédric Tissières (Objectif Sécurité)

- Ophcrack
  - 2To
  - 8 caractères
  - 6 mois de calcul pour 3 ATI Radeon HD6990
- Méthodes probabilistes pour limiter
  - Taille des tables
  - Temps de calcul
- IA
  - Algorithme du Sac à Dos
  - Modèles de Markov
- Pas de stats :(

Rumps (1)

Trucs en stock sur le SSTIC — *SSTIC*

- Soumettez !
- Inscriptions très rapides (150places/~4 minutes)
- 1/3 de nouveaux cette année

MGCP : Un protocole VOIP oublié — *Joffrey Czarny*

- Aucune sécurité intégrée au protocole
- MitM sur la gateway

Quel est l'OS de Kim Jong-Un ? — *Pierre Capillon*

- http://java-0day.com
- president.whitehouse.gov → Ubuntu/Firefox
- IP APT1
- Syrie (Windows NT 6.2), Iran (Ubuntu 10.04), Cuba (Windows NT 6.2)
- Corée du Nord → Mac OSX

Rumps (2)

La sécurité est un _ _ _ _ _ _

Nicolas Ruff (EADS)

- Failles dans un produit certifié CSPN par l'ANSSI
- `sudo tar <input>`
- Clés privées ssh
- Hash de mots de passe dans le code
- Indice : U _ _ _ _ A

La certification est un échec ?

Une autre perspective aux Darknets

Alexandre Dulaunoy (CIRCL)

- Darknet → Préfixe IP non utilisé
- 193.168.0.0/16 (~RFC 1918)
- Serveurs/Machines
- Imprimantes
- Routeurs

Exploitation d'une faille vieille de 20 ans

Joffrey Czarny

- Exploit PATHALLOC
- Windows NT → Windows 8
- Publique
- Non patchée
- http://blog.cmpxchg8b.com/2013/05/introduction-to-windows-kernel-security.html

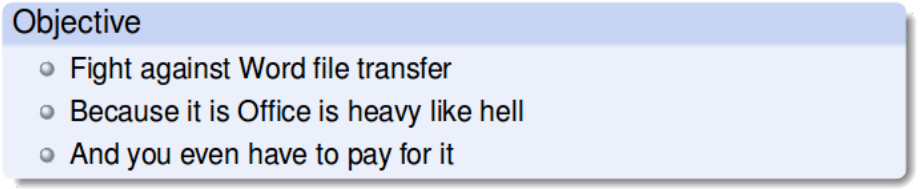
Rumps (3)

Cloud ISO 14001 — *Arnaud Ebalard (EADS)*

- Serveur léger
- Sécurisé
  - GNU/Linux
  - grsec
- NAS Netgear

Suricata WTF — *Eric Leblond (OISF)*

- Marquage des paquets avec Suricata
- QoS avec Netfilter/tc



Pubs

- BotConf – http://botconf.eu
  - 5&6 Décembre 2013 à Nantes
- GreHack
  - 15 Novembre à Grenoble
- OWASP Tour 2013
  - 24 Juin à Sophia Antipolis

Rumps (4)

Raspberry Spy

Antoine Cervoise (Devoteam)

- « Keylogger » réseau
- Raspberry + tcpdump

Me@YourHome: Cambriolage 2.0

- Réseaux Sociaux
- Venir vous cambrioler quand vous êtes absent

Yara-IOC : Mon cœur balance

Yvan Fontarensky (Cassidian)

- Éditeur graphique de règles YARA
- Détection des machines infectées avec outils Mandiant

Stack Overflow != Stack Based Overflow

- Stack Based Buffer Overflow : Débordement sur des données
- Stack Overflow : Pile déborde sur d'autres sections de la mémoire

Rumps (5)

Analyse d'AD — *Philippe Biondi (EADS)*

- Python
- Parsing du fichier ntds.dll
- Extraction des données de l'AD
- Base de données MongoDB

Panda OCR — *Panda*

- Reconnaissance de caractères minimaliste
- Python
- CAPTCHA

Hack my CCTP — *Anonymous*

- Hacker les appels d'offre publics

RW2 : Des photos sans Photorec — *Raphaël Rigo (Syscall.eu)*

- Distorsion sur les photos RAW

Rumps (6)

QPhotorec — *Christophe Grenier*
- Récupération de fichiers
- 500 formats
- Ligne de commande
- Interface graphique

Je choisis l'option offensive ! — *Florent Chabaud (ANSSI)*
- Livre Blanc 2013
- Offensive autorisée
- Encadrement
- <troll>Challenge ? L'État recrute </troll>

TNS Bit Flip Attack — *Joffrey Czarny*
- TNS : Protocole de réseau P2P / Oracle
- Proxy/MitM
- SQLi → Bypass authentification
- Projet Houracle

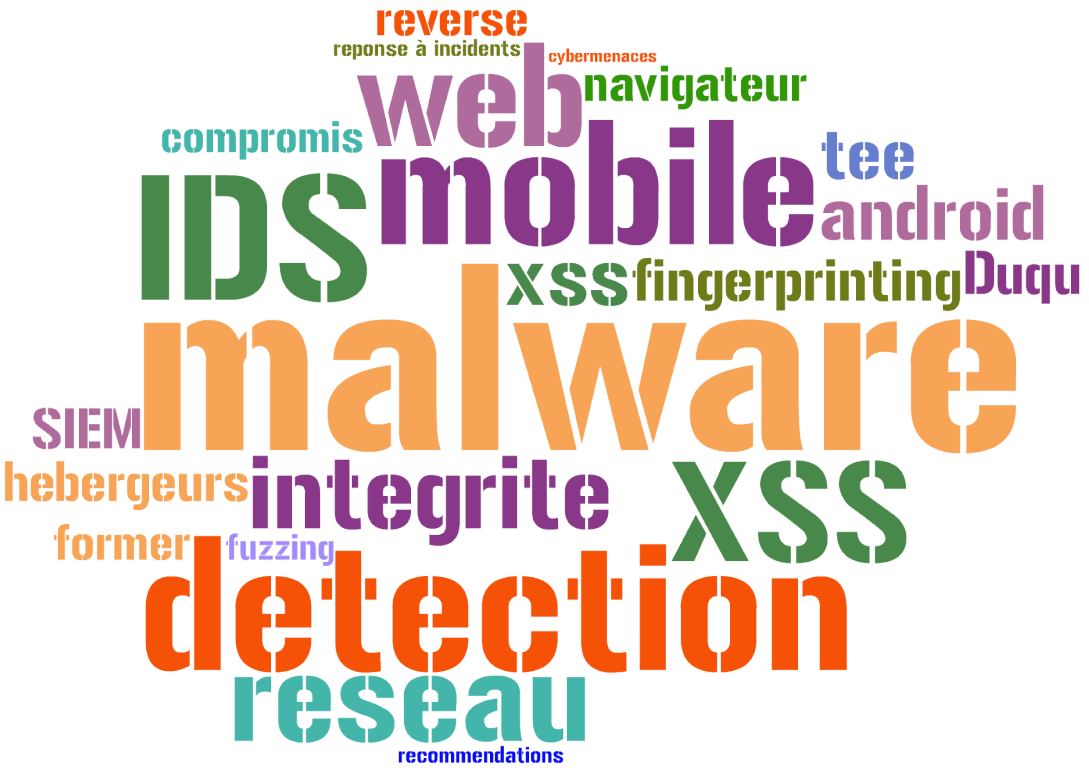
3ème jour

Mon TOP :

1. La réponse aux incidents, ou quelques recommendations pratiques pour les auteurs de malwares

2. Faire face aux cybermenaces ⇒ Détecter (les attaques) ∧ Former (des experts en SSI)

3. Fingerprinting de navigateurs



Fuzzing Intelligent d'XSS Type-2 Filtrées selon Darwin : KameleonFuzz

Fabien Duchene (LIG Lab)

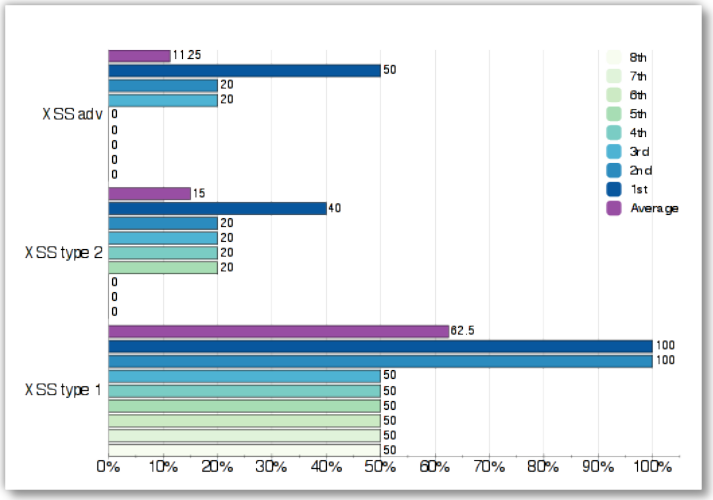
XSS Persistante

Fuzzing intelligent

- Inférence de modèle → Apprentissage automatique (crawl) du système cible
- Fuzzing évolutionniste
  - Dictionnaire limité
  - Détecte les XSS, si on est « proche » d'une XSS → Vérification manuelle

KameleonFuzz

- Plus efficace que 4 outils (XSS Sniper, Wapiti, w3af, skipfish, ~~XSSF~~)



Fingerprinting de navigateurs

Erwan Abgrall (Télécom Bretagne)

Obtenir « à coup sûr » la version du navigateur/plugins utilisés

↳ Envoyer le bon payload

Comportement des navigateurs

↳ XSS

Exécution de *n* vecteurs de XSS

↳ Arbre de décision

↳ Distance de Hamming

Duqu contre Duqu

Aurélien Thierry (Inria)

Duqu

- Malware (2011)
- 0day dans une *font* TrueType
- Lié à Stuxnet

Reversing du driver Duqu

Réutilisation de Duqu pour détecter Duqu

La TEE, nouvelle ligne de défense contre les mobiles (?)

Hervé Sibert (ST Ericsson)

- Trusted Execution Environment
- Exécution des fonctions sensibles dans la TEE
  - Boot
  - Stockage
  - IHM
  - SIM / SecureElement
  - Sandboxing du code
  - Clés de sécurité
  - Séparation Code/Données
- « Pipeau commercial » pour TrustZone

La réponse aux Incidents : Conseils aux auteurs de Malwares

Alexandre Dulaunoy (Circl)

« Keep it simple »

Binaire signé ?

- Voler/Acheter des clés privés ?
- Faire signer son malware / Compromettre la CA ?
  - 600 CA/sub-CA
- Utiliser des binaires signés (exemple : PlugX)
  - Modifier le binaire pour lui faire charger son binaire malveillant (*LoadLibrary*)

Réseau ?

- Utiliser le format correspondant au port utilisé
- Domaines différents
- Types d'enregistrements DNS

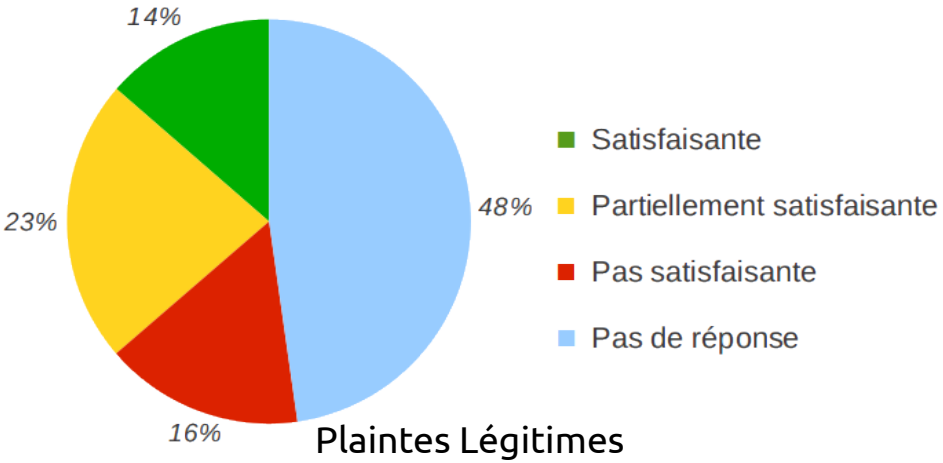
Présentations courtes (1)

Le rôle des hébergeurs dans la détection de sites web compromis

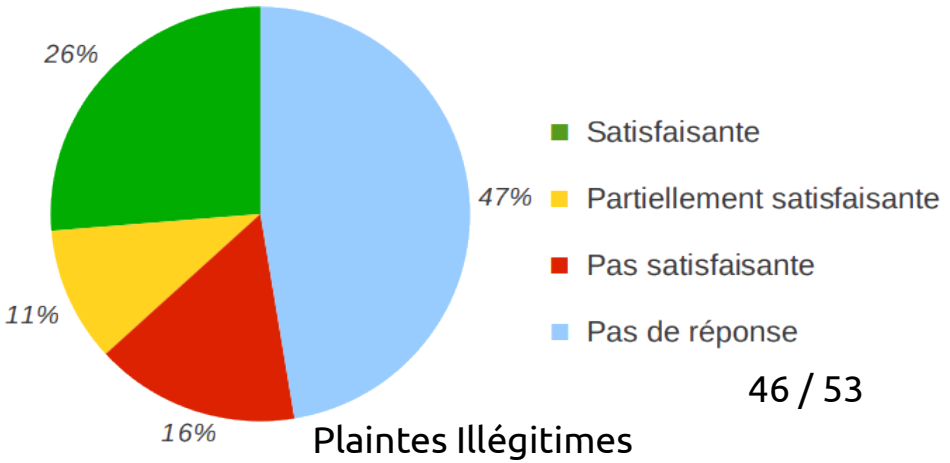
Davide Canali (Eurecom)

- Hébergement mutualisé
- 12 hébergeurs mondiaux (US) / 10 régionaux
- 110 tests (botnet, SQLi, Phishing, RCE, Auth bypass)
- Attente de réaction
  - 1 seul hébergeur détecte
- Plaintes
  - 50 % réponses
  - 64 % réponses dans la journée
  - Temps moyen
  - Globaux → 28h
  - Régionaux → 79h

TL;DR ;
Protection contre les inscriptions abusives.
Détection basique des attaques (URL blacklists)
Pas de détection des signes évidents de p0wn4ge



Plaintes Légitimes



Plaintes Illégitimes

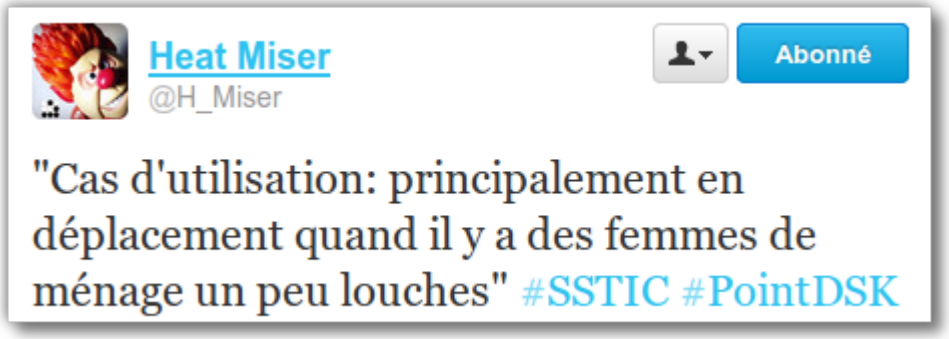
Présentations courtes (2)

Détection comportementale de malwares P2P — *Xiao Han (Orange Labs)*

- Le « bon » P2P et le « mauvais » P2P
- → Isolation P2P pur
- → Isolation trafic malveillant
  - ↳ Algorithme SVM
- → 97,2 % précision

Attestation distante d'intégrité sous Android — *Dimitri Kirchner (Amossys)*

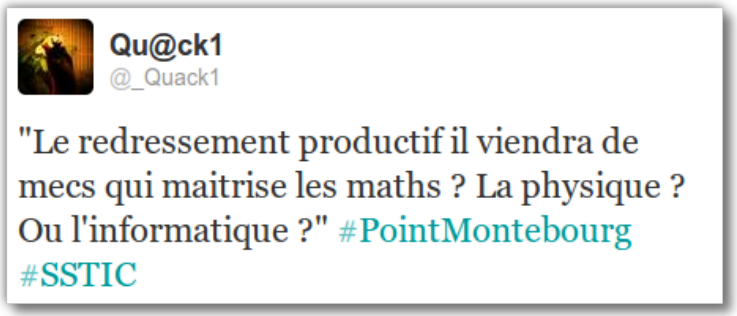
- Vérifier l'intégrité d'un PC au démarrage
- Smartphone Android



Faire face aux cybermenaces ⇒ Détecter (les attaques) ∧ Former (des experts en SSI)

Ludovic Mé (Supelec)

- Livre Blanc 2013
  - Détecter les attaques
  - Y répondre
- Détection
  - Détection / Supervision importantes
  - Trop de faux positifs
  - SIEM / Amélioration des outils
- Formation
  - Sensibilisation à tous les niveaux
  - Bonnes pratiques
  - Formateurs ?
  - Formation à l'attaque ?

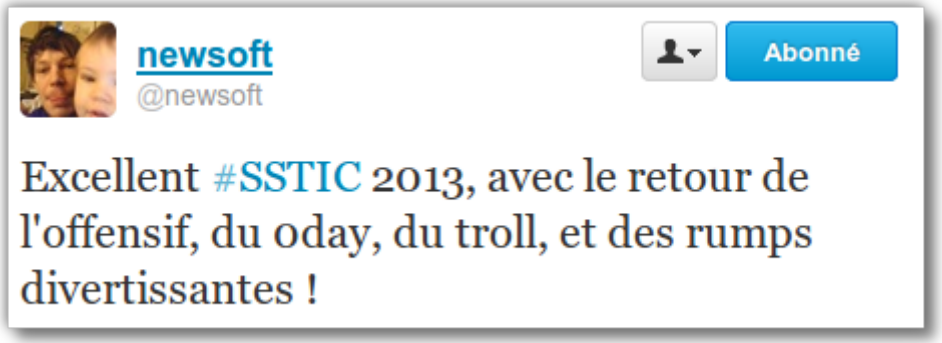


En conclusion

0-day
Offensif
Troll
Lol

Très bonne conférence
Haut niveau des confs
Excellente organisation
Il a fait beau ☀
Des rencontres (merci)

On y retourne l'année prochaine ?



→ Fichiers polyglottes

PoC : http://quack1.me/fichiers_polyglottes.html

→ Fingerprinting de navigateurs

Article à venir...

→ Exécution de malwares non signés

Si vous en voulez plus

Articles sur mon blog : http://quack1.me/tag/sstic-2013.html

Un gros best-of : http://www.sebnet.org/article/sstic-edition-2013/

Les slides/papers : https://www.sstic.org/2013/actes/