

Compte-rendu Insomni'hack 2014

21 mars 2014

OSSIR Paris / 8 avril 2014

Thibaud Binétruy – Consultant Sécurité – Thibaud.Binetruy@Intrinsec.com
Guillaume Lopes – Consultant Sécurité – Guillaume.Lopes@Intrinsec.com

☁ Conférence de sécurité à Genève en Suisse

☁ Organisée par la société SCRT

☁ 7ème édition : 20 et 21 mars 2014

☁ L'évènement est réalisé sur 2 jours

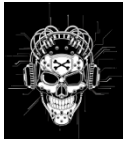
→ 20 mars : Workshops

✓ « Advanced Brup Pro », par Nicolas Grégoire

✓ « Cryptography for developers », par JP Aumasson

✓ « Exploitation Linux », par SCRT

→ 21 mars : Conférences et challenge



Les conférences

Track 1	Track 2	Track 3
	Intro Paul Such Keynote Mikko Hypponen	
When you can't afford 0days. Client-side exploitation for the masses Michele Orru, Krzysztof Kotowicz	Enjeux juridico-organisationnels et Contractuels du Cloud computing Nicolas Rosenthal	Mapping malware infections Ricky "HeadlessZeke" Lawshae
Lurking in clouds: easy hacks for complex apps Nicolas Gregoire	Deploying cyberdefense measures and Policies in a Critical Infrastructure Sector Sébastien Bombal	Wallix
JSMVCOMFG? To sternly look at JavaScript MVC and Templating Frameworks Mario Heiderich	Binary art – funky PoCs & visual docs Ange Albertini	Dalvik Executable (DEX) Tricks Axelle Aprville
RFIDler Adam Laurie	I've got ARGuments for YOU ! Bruno Kerouanton	

🌸 Keynote par Mikko Hypponen

→ Chief Research Officer pour F-Secure depuis 1991

🌸 Mots clés

→ Google / Snowden / NSA



🌸 Retour sur les « récentes » révélations de Snowden

🌸 Très bon orateur, slides minimalistes (gif powered)

🌸 Impossible de résumer une keynote de Mikko

🌸 Retour sur la supériorité IT des Etats Unis

- Difficile de citer 5 grosses sociétés européennes du domaine de l'IT
- Exemple d'une base américaine en Allemagne : « They have American fresh milk ! »

🌸 Quelques phrases choc concernant la surveillance massive :

- « That's not what we build the internet for »

🌸 Troll sur les éditeurs antivirus Américains qui n'ont pas répondu à la lettre leur demandant s'ils avaient passé sous silence des malwares gouvernementaux

🌀 **When you can't afford 0days : Client-side exploitation for the masses**

→ Michele Orru, Krzysztof Kotowicz

🌀 **Problématique : Est-il possible d'exploiter les navigateurs sans posséder de 0 days ?**

- Extensions des navigateurs notamment Chrome
- Applications HTML (utilisation d'ActiveX)
- Documents Office avec des macros
- Contournement de restrictions sur IE

☁ Une extension Chrome

- possède des droits limités
- ne peut effectuer de commandes sur le système
- peut être installée uniquement depuis le Web Store

☁ Pour déployer une extension sur le Web Store, il suffit de

- Avoir une carte crédit
- 5 \$
- un compte Google
- une extension à dupliquer

☁ Enfin, un peu d'ingénierie sociale pour inciter l'utilisateur à installer l'extension

- ☁ Via cette extension, il est possible d'établir un tunnel entre le navigateur du client et l'attaquant
 - Utilisation du navigateur de la victime comme proxy
 - Accès à ces sites en usurpant son identité
 - XSS permanent sur tous les tabs ouverts par l'utilisateur

- ☁ Copie de l'extension « gmail » publiée dans un but de test, des utilisateurs l'ont installé d'eux même...

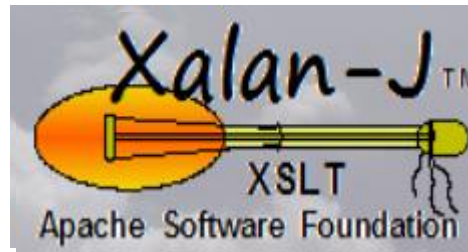
- ☁ Slides
 - insomnihackdotme.files.wordpress.com/2014/04/when_you_dont_have_0days-kotowicz-antisnatchor-insomnihack2014.pdf

☁ **Lurking in clouds: easy hacks for complex apps**

→ Nicolas Grégoire / Fondateur d'Agarri

☁ Démonstration de découvertes de vulnérabilités sur 4 solutions

ORACLE



☁ Pas de techniques avancées: Keep It Simple 😊

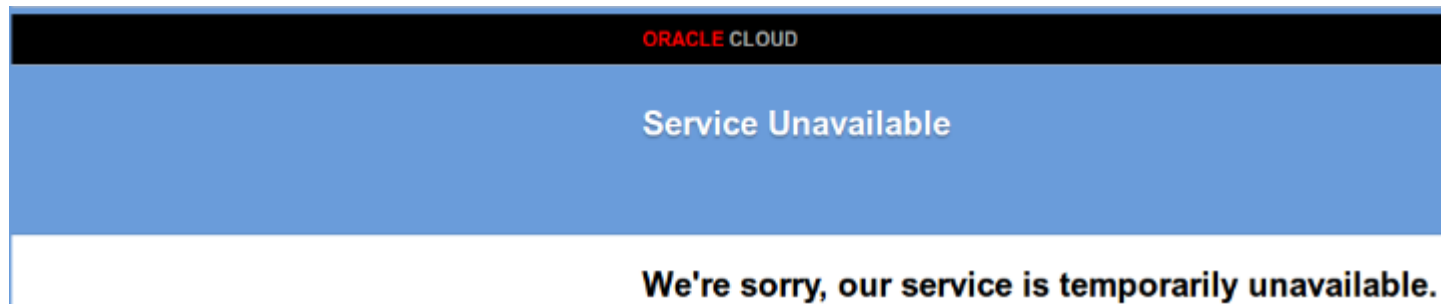
☁ Bug Bounty intéressants !

Oracle Database Cloud Service

- Utilisation d'une version vulnérable connue depuis 2013
- CVE-2013-3751 : Parseur XML

PRODUCT	VERSION	STATUS
NLSRTL	11.2.0.3.0	Production
Oracle Database 11g Enterprise Edition	11.2.0.3.0	64bit Production
PL/SQL	11.2.0.3.0	Production
TNS for Linux:	11.2.0.3.0	Production

Résultat : Déni de service



☁️ Yahoo Query Language

- Syntaxe similaire au SQL
- Vulnérabilités XXE découvertes
 - ✓ Yahoo Pipes / YQL Console / REST interface

☁️ Résultat : Exécution de commandes

```
Content stolen via XXE... /etc/hostname: engine3.yql.bf1.yahoo.com /etc/passwd:  
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/sbin/nologin shutdown:x:6:0:shutdown:/sbin:/sbin/nologin  
halt:x:7:0:halt:/sbin:/sbin/nologin mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
news:x:9:13:news:/etc/news:/sbin/nologin uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
oprofile:x:16:16:Spectal user account to be used by OProfile:/home/oprofile:/sbin/nologin  
nscd:x:28:28:NSCD Daemon:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
rpc:x:32:32:Portmapper RPC user:/sbin/nologin rpm:x:37:37:/var/lib/rpm:/sbin/nologin  
ntp:x:38:38:/etc/ntp:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin  
mailnull:x:47:47:/var/spool/mqueue:/sbin/nologin smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin  
bind:x:53:53:Bind Sandbox:/sbin/nologin nslcd:x:65:55:LDAP Client User:/sbin/nologin  
haldaemon:x:68:68:HAL daemon:/sbin/nologin vcsa:x:69:69:virtual console memory  
owner:/dev:/sbin/nologin avahi:x:70:70:Avahi daemon:/sbin/nologin tcpdump:x:72:72:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
pcap:x:77:77:/var/arpwatch:/sbin/nologin dbus:x:81:81:system message bus:/sbin/nologin  
postfix:x:89:89:/var/spool/postfix:/sbin/nologin extm:x:93:93:/var/spool/extm:/sbin/nologin  
nobody:x:99:99:Nobody:/sbin/nologin avahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-  
autoipd:/sbin/nologin saslauthd:x:489:489:"Saslauthd user"/var/empty/saslauthd:/sbin/nologin  
yahoo:x:1000:100:Yahoo:/home/yahoo:/usr/local/bin/push flo:x:1001:100:David Filo:/home/filo:/bin/bash
```

Xalan-J

→ Analyseur XSLT de la fondation Apache

Résultat : Exécution de commandes à distance

→ Utilisation du langage de script fourni par Xalan-J

```
xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"  
xmlns:xalan="http://xml.apache.org/xalan"  
xmlns:foo="bar" version="1.0">  
<xalan:component prefix="foo">  
<xalan:script lang="(xslt | jython | ...) ">  
<![CDATA[  
...  
Whatever you want to execute  
...  
]]>  
</xalan:script>  
</xalan:component>  
</xsl:stylesheet>
```

Prezi

- Outil de création de présentations en Flash
- Deux éditeurs disponibles
 - ✓ Application Web (gratuite)
 - ✓ Application lourde (payante)

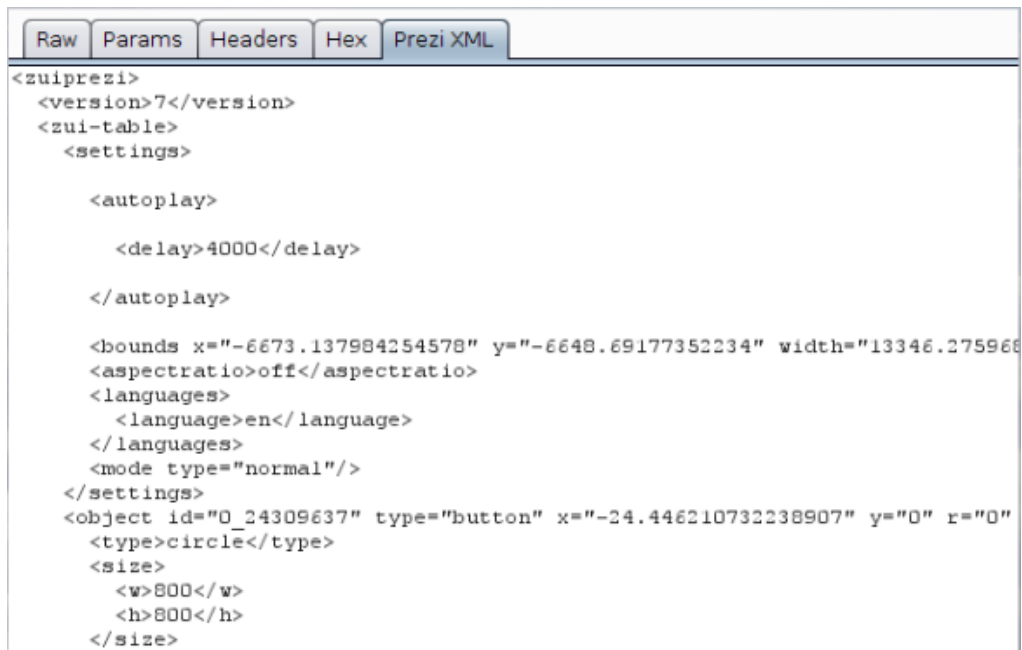
Etude du fonctionnement de l'application Web avec Burp Suite Pro

- Identification d'un paramètre contenant du XML
 - ✓ XML = zlibDecompress(base64Decode(urlDecode(VALUE)))
- Création de deux extensions Burp :
 - ✓ PUSH : Permet de décoder et modifier la valeur du paramètre
 - ✓ PULL: Permet uniquement de décoder la paramètre sans modification

Sans l'extension

```
b64%5Fzipped%5Fxml%5Fcontent=e...zDwMlv2OYS/hwD/g8bHtBeP4jk7vLVoYWzXbcIkLZB63xogyBYkUuJZOpUSSqKXPS/3%2bxSFJcvkiWluOI  
u2mWw4dbnmYdmZ0dKgnff/eT3800b=/SOSpY5fOrQ%2b8uLF0HL%2bx8fXj/8iuIsw0h7En%2b0cWeBIM3gZVgsWVGsI7H8Af4G9UbjC4SCTzwwkmw  
xdgOjfvivEoDMq2ST14gmeC16WyWJaV18IbX8FbFVmy5RtavluBdYiLhYs0zQDo3rfvQqMrn29MM1Wi6hAn6%2b1ke04VMfU9T2L2JbtehraSLH16Y6  
PXZfahFBLQ%2bSkKmfXGqbUcnT12r7j2aaPbVdDM55MZ6VYI76rU4/almtaluNpxngXSrHkYZmsMenGWRvDNkVQK6VsMV2xKS%2baWHayMV8Exu5hF  
2LPJJhnEUf1ZsmvtUWWz1laowINs9BNvk3QEBJdK2ZH41FTd%2bhEE510ImVZbbQJEnEOiEcgk2XAhmeb7qSJVNDufxZQOyObgMn1PSwR6hrORoKU  
6iMay1M0jDl2g6f2H5cCQNDPtOrRfLElcljXY00kd62IZpVo1sSv2gRzXjJFe5GVP2RREic8ut28K3g%2bjvNsPir5HIqiBO99hc24yXK%2bKB%2b2u
```

Avec l'extension



```
Raw Params Headers Hex Prezi XML  
<zuiprezi>  
<version>7</version>  
<zui-table>  
<settings>  
  
<autoplay>  
  
<delay>4000</delay>  
  
</autoplay>  
  
<bounds x="-6673.137984254578" y="-6648.69177352234" width="13346.275966" height="13346.275966">  
<aspectratio>off</aspectratio>  
<languages>  
<language>en</language>  
</languages>  
<mode type="normal"/>  
</settings>  
<object id="O_24309637" type="button" x="-24.446210732238907" y="0" r="0">  
<type>circle</type>  
<size>  
<w>800</w>  
<h>800</h>  
</size>
```

☁ Faiblesse dans l'exportation des présentations sous format Prezi

- Pointeur vers un fichier local
- Exporter la présentation
- Ouverture du ZIP et obtention des données

```

nagios:x:109:118::/var/lib/nagios:/bin/false
stunnel4:x:110:119:stunnel:/var/run/stunnel4:/bin/false
publisher:x:1018:100:Prezi Publisher:/home/publisher:/bin/bash
mzagon:x:1022:100:Mihaly ZAGON:/home/mzagon:/bin/bash
kepten:x:1023:100:Robert KISS:/home/kepten:/bin/bash
zsellera:x:1024:100:Attila ZSELLER:/home/zsellera:/bin/bash

```


 Correction effectuée par Prezi

→ Restriction des ressources externes au protocole http://

 Néanmoins toujours possible d'accéder à une IP interne

→ Prezi utilise les instances Amazon EC2

→ 169.254.169.254 est utilisé par la VM afin d'accéder à certaines métadonnées

 Possibilité de récupérer les métadonnées stockées dans

→ <http://169.254.169.254/latest/user-data/>

 Slides

→ insomnihackdotme.files.wordpress.com/2014/04/easy_hacks_for_complex_apps-ins14.pdf

☁ Deploying cyberdefense measures and Policies in a Critical Infrastructure Sector

- Sébastien Bombal / RSSI chez AREVA
- @sbombal sur Twitter

☁ Bonnes pratiques à mettre en œuvre :

- Mélange de technique et d'organisationnel (pas uniquement l'un ou l'autre)
- Renforcer son SI et se doter de capacité de détection et de réaction
- Vous n'échapperez pas aux crises, donc autant être préparés 😊

☁ Quelques facteurs de succès :

- Avoir mis en place un cycle de décision rapide au bon niveau
- Assurer la confidentialité de l'opération tout en étant prêt à communiquer (« be prepared to answer a lot of question from your customers, authorities... »)
- Avoir une équipe de réaction appropriée, dans le pire des cas il vous faudra une équipe pour maintenir le RUN et une équipe pour construire un nouveau SI
- Etre prêt à dérouler le plan de secours à tout moment
- Tracer toutes les décisions et les actions « au cas où »

- ☁ « Crisis is not a fatality, turn it into an opportunity »:
 - surfez sur le « plus jamais ça » pour obtenir ce qu'on vous refuse depuis longtemps

- ☁ Prioriser les sessions de sensibilisation sur les utilisateurs avec pouvoir

- ☁ Slides:
 - <http://insomnihackdotme.files.wordpress.com/2014/04/sebastien-bombal-v3-3.pdf>

☁ Dalvik Executable (DEX) Tricks

→ Axelle Apvrille / Analyste de malwares chez Fortinet

→ @Cryptax sur Twitter

☁ Découverte d'une « vulnérabilité » Android permettant de masquer une méthode aux yeux d'un décompilateur

☁ Objectif de la présentation démontrer qu'il est possible de masquer une méthode et de l'exécuter quand même

☁ Technique idéale pour un auteur de malware Android

- ☁ Mise au point d'un « détecteur » :
 - A utiliser lors d'une analyse de malware Android
 - L'auteure n'a jamais découvert d'échantillons utilisant cette technique

- ☁ Défaut signalé à Google, normalement corrigé dans les versions à venir (temps de réaction assez long)

- ☁ Publication de l'outil de détection
 - <https://github.com/cryptax/dextools>

- ☁ Slides
 - insomnihackdotme.files.wordpress.com/2014/04/hidex-insomni.pdf

☁ I've got ARGuments for YOU !

- Bruno Kerouanton / RSSI du Canton du Jura
- @Kerouanton sur Twitter
- Présentation hallucinante, speaker fou 😊

☁ Alternate Reality Game

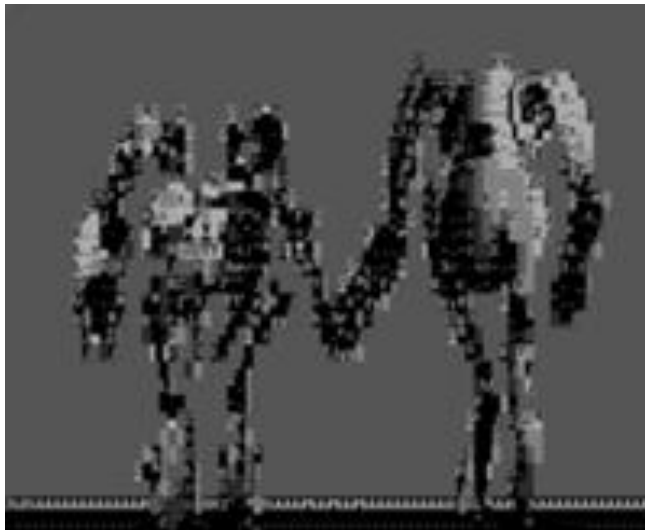
- Canaux cachés dans un support pour diffuser des informations
- A destination des « power users » qui s'ennuient 😊

☁ Deux exemples traités

- La série « The IT Crowd »
- Le jeu vidéo « Portal »

Portal

- Les radios peuvent diffuser des signaux
- Utilisation du morse et du SSTV
- Récupération de texte et d'images
- Récupération d'un numéro de BBS
- Accès à des infos concernant Portal 2



☁ The IT Crowd

- Programmes diffusés en base64 dans les sous titres
- Diffusion de code via un flash lumineux sur la TV
 - ✓ Une piste cachée explique comment construire un récepteur
- ...





Le challenge

- ☁ Plus de 200 participants
- ☁ 8 personnes par équipe au maximum
- ☁ Possibilité de jouer en solo
- ☁ Le challenge a duré de 18h à 4h
- ☁ Différentes catégories d'épreuves à résoudre
→ Web / Stégano / Reverse / Hardware / etc.

🌀 Les trois premières équipes remportaient 20 grammes d'or



🌀 Classement final

PLEASE EXERCISE COMMON COURTESY AND DISABLE YOUR MOBILE PHONE IN THE OBSERVATION SPACE

Team results			Individuals results		
Rank	Team	Score	Rank	Name	Score
#1	Dragon Sector	6620	#1	eint0	
#2	StratumAuhuur	5360	#2	david	
#3	HackingForBeers	4760	#3	thecis0	
#4	More Smoked Leet Chicken	4060	#4	britney	
#5	Int3pids	4020	#5	FuZ	
#6	dcua	3160	#6	K9A	
#7	FIXME	2195	#7	lmeonthehack	
#8	HoneyBadgerz	1900	#8	Riber	
#9	Dulac	1835	#9	theciso	
#10	mushd00m	1550			
#11	insomniacs_II	1455			
#12	Porc Scanner	1410			
#13	Hackdumb	1300			
#14	SeBC	1260			
#15	Bullshit Security	1200			
#16	cr4zy g0at 0verf10w	1200			



Conclusion

☁ Très bonne conférence

- Intervenants de qualité
- Large panel de sujets (techniques ou non)
- Un challenge très sympa et gratuit

☁ Un peu dur de suivre 3 tracks en parallèle

☁ Rendez vous en 2015 😊

Supports mis en ligne :

→ <http://insomnihack.ch/2014/04/02/slides-of-some-of-the-2014-conferences/>

Vidéos :

→ <http://insomnihack.ch/2014/03/26/insomnihack-2014-video/>

Photos :

→ <http://insomnihack.ch/2014/03/26/thank-you/>



Merci de votre attention
Questions ?
