GuadalajaraCON

20 y 21 de abril del 2012

Laboratorio de Análisis de Malware

@hugo_glez

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Acerca de:

http://atit.upslp.edu.mx/~hugo/

- No hago análisis de malware por motivos económicos/profesionales, tiene que ver más con investigación y cuestiones académicas.
- El público objetivo es básico a intermedio, habrá sesiones de análisis avanzado.

¿ Para qué analizar malware ?

Mi punto es:

- Conocer sobre el malware y su comportamiento.
- Ayudar en la automatización del análisis de malware.
- Contribuir a la seguridad en Internet.
- Resolver problemas del estado de la práctica y del estado del arte. (cripto)

Mi punto es:

- Conocer sobre el malware y su comportamiento.
- Ayudar en la automatización del análisis de malware.
- Contribuir a la seguridad en Internet.
- Resolver problemas del estado de la práctica y del estado del arte. (cripto)
- **¡Conseguir trabajo en un laboratorio de antivirus!**

Laboratorio

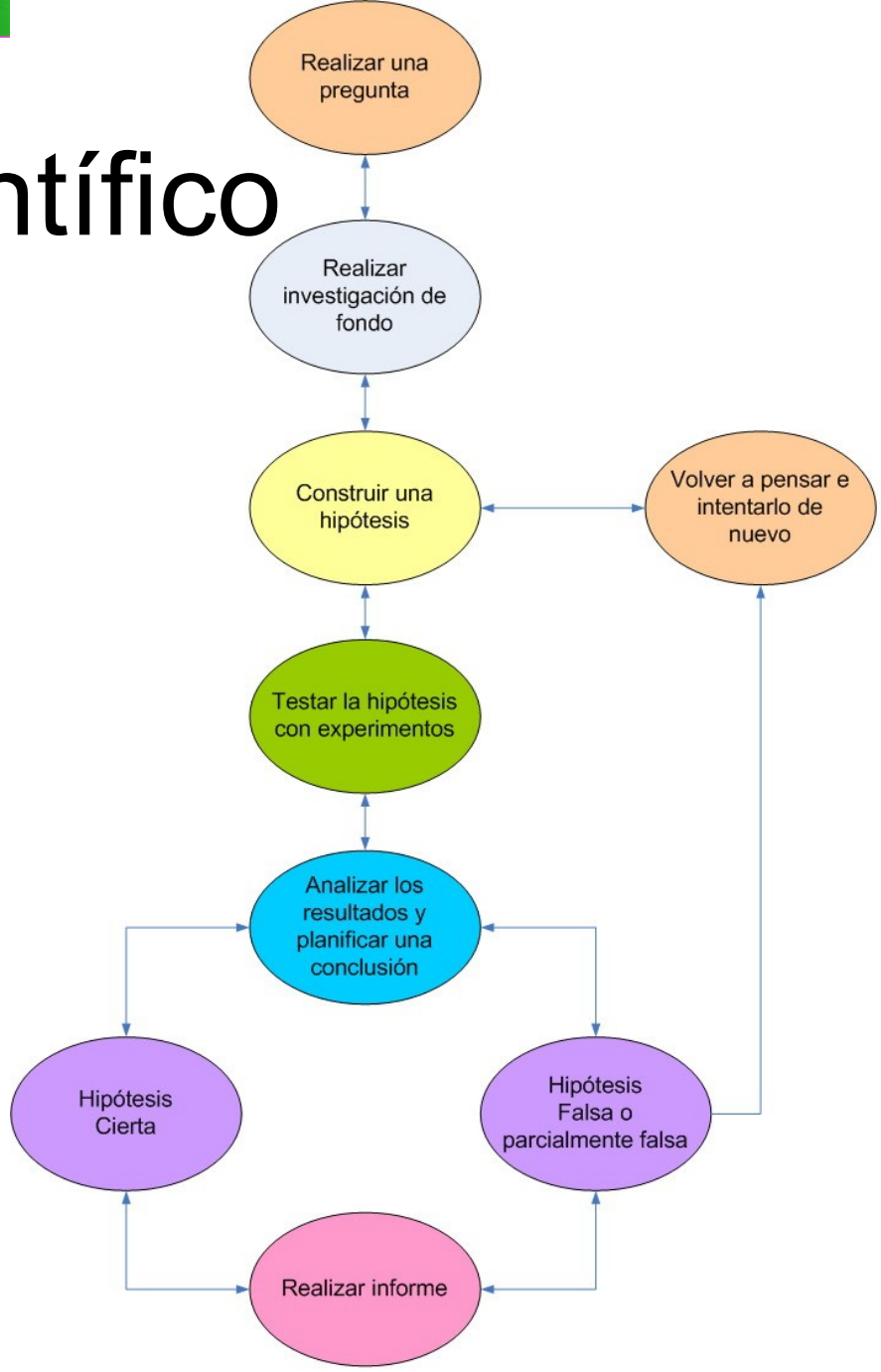
- El laboratorio es un lugar dotado de los medios necesarios para realizar investigaciones, experimentos, prácticas y trabajos de carácter científico, tecnológico o técnico; está equipado con instrumentos de medida o equipos con que se realizan experimentos, investigaciones o prácticas diversas, según la rama de la ciencia a la que se dedique.
  - Se puede asegurar que no se producen influencias extrañas (a las conocidas o previstas) que alteren el resultado del experimento o medición: control.
  - Se garantiza que el experimento o medición es repetible, es decir, cualquier otro laboratorio podría repetir el proceso y obtener el mismo resultado: normalización.
- **http://es.wikipedia.org/wiki/Laboratorio**

Laboratorio de análisis de malware

Con software libre !!

Método científico

- Observación
- Inducción
- Hipótesis
- Experimentación
- Demostración
- Tesis o Teoría (Conclusiones)



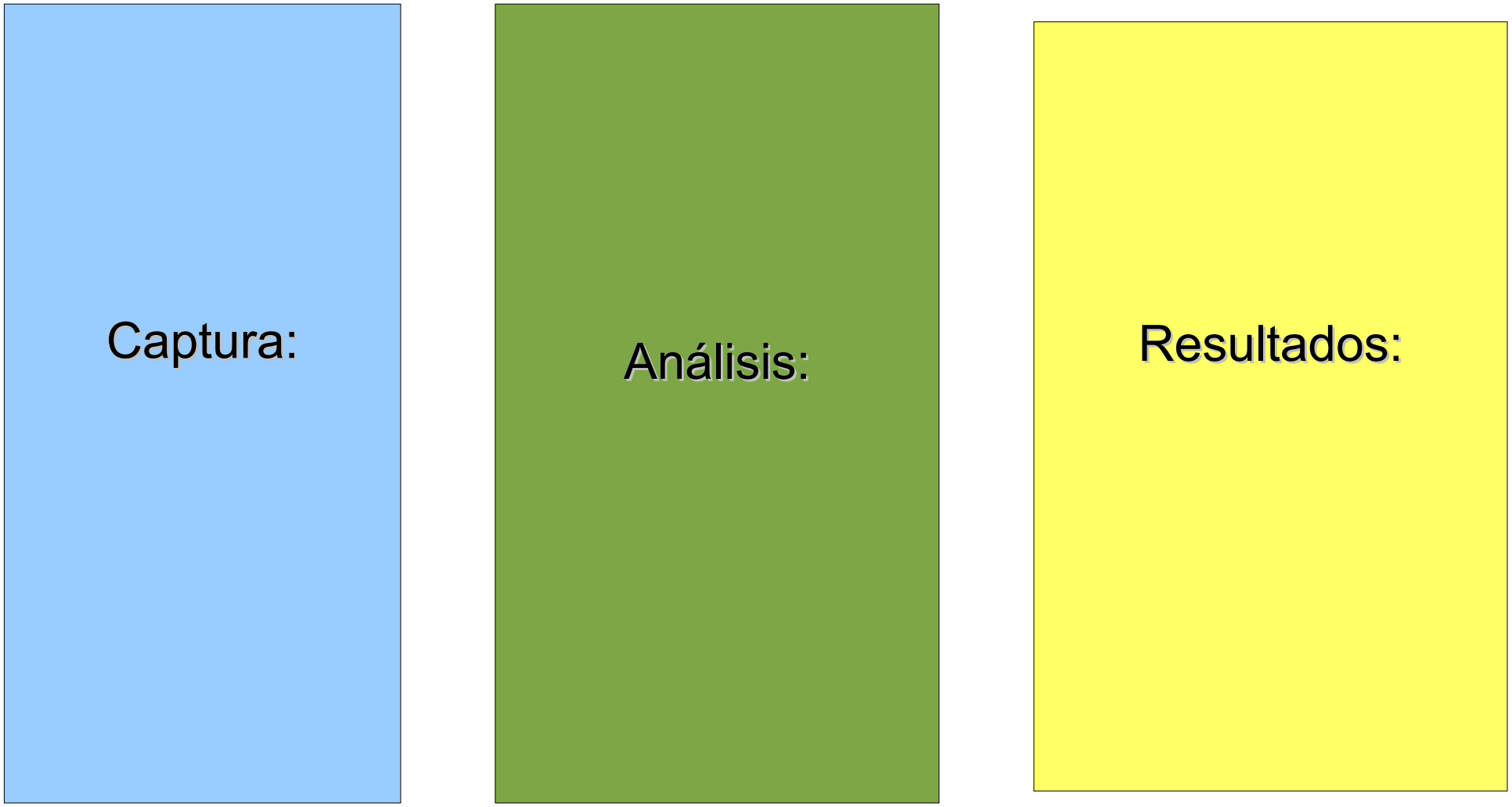
Modelo simplificado de las etapas del método científico

Objetivo:

Aprender más sobre el malware
Publicar ...

- Recolección de malware
- Análisis
  - Estático
  - Dinámico
  - De comportamiento
- Resultados

Arquitectura genérica



Arquitectura genérica

Captura:

Nepenthes

Dionaea

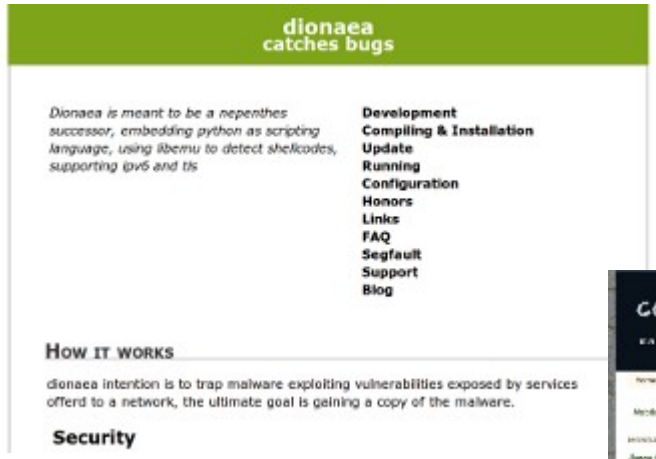
Spampot

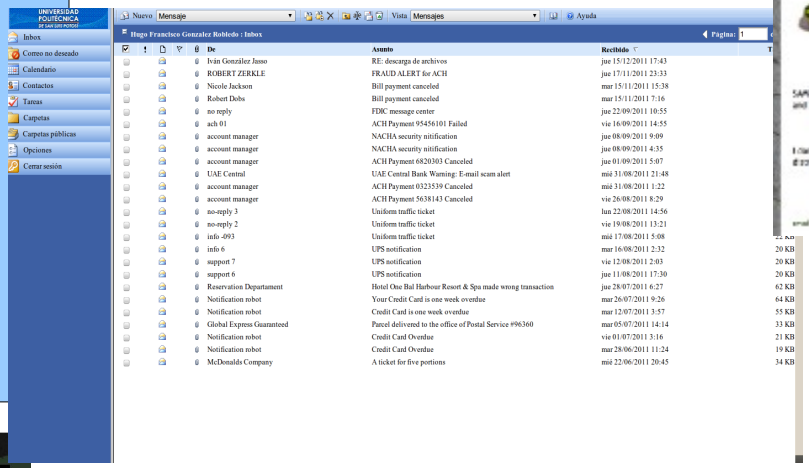
ContagioDUMP

USB en el ciber

Listas

Otras fuentes.





GuadalajaraCON
20 y 21 de abril del 2012

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Dionaea

http://dionaea.carnivore.it

dionaea
catches bugs

Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls

libemu
x86 emu

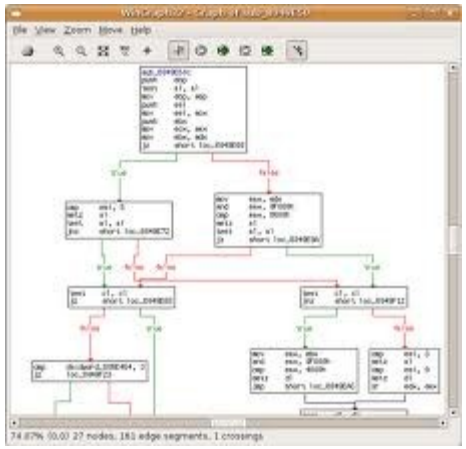
How it works

dionaea intention is to trap malware exploiting vulnerabilities exposed by services offerd to a network, the ultimate goal is gaining a copy of the malware.

Security

Video

Arquitectura genérica



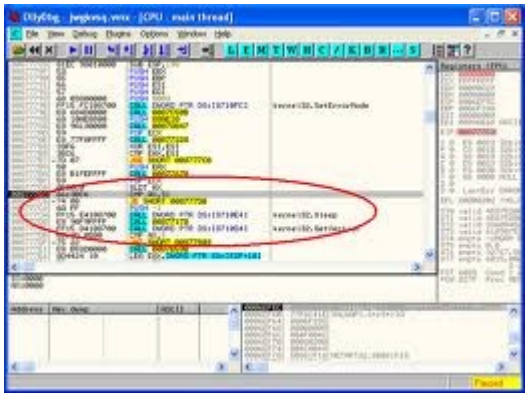
Análisis:

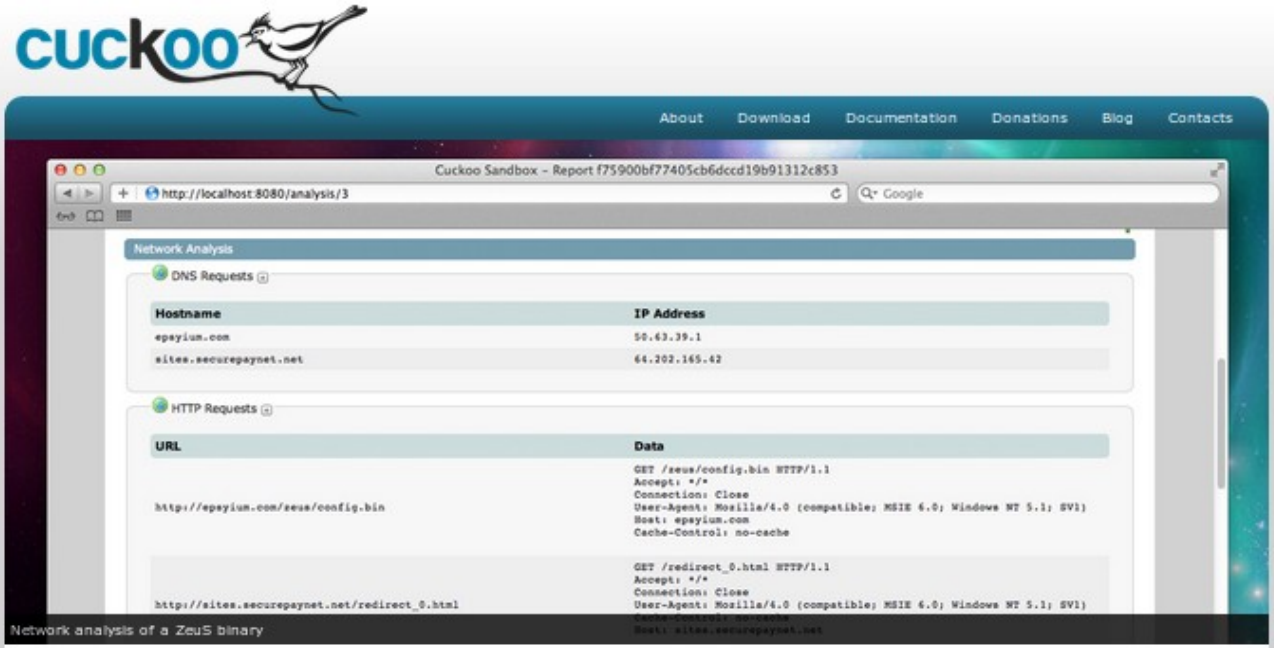
Estático
Strings
Decompilar
Desensamblar

Dinámico
Depurar (Ollydbg, IDA)

Comportamiento
Ejecutarlo
Máquina Virtual
Máquina Real

Otros ?





Network analysis of a ZeuS binary

Cuckoo Sandbox

AUTOMATED MALWARE ANALYSIS SYSTEM

~

RAPID7 powered

About

In three words, **Cuckoo Sandbox** is a *malware analysis system*.

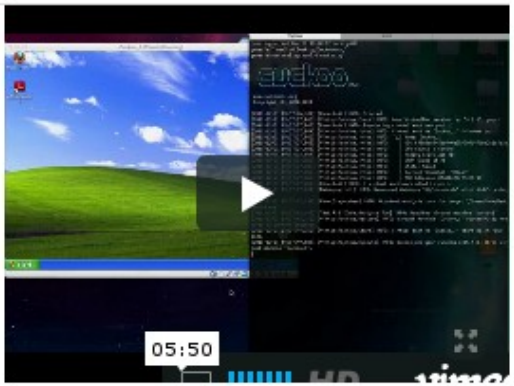
Its goal is to provide you a way to automatically analyze files and collect comprehensive results describing and outlining what such files do while executed inside an isolated environment.

It's mostly used to analyze Windows executables, DLL files, PDF documents, Office documents, PHP scripts, Python scripts, Internet URLs and almost anything else you can imagine.

But it can do much more...
It's up to you to discover what and how.

Some of the results that Cuckoo generates are:

- Trace of performed relevant win32 API calls
- Dump of network traffic generated during analysis
- Creation of screenshots taken during analysis
- Dump of files created, deleted and downloaded by the malware during analysis
- Trace of assembly instructions executed by malware process



Cuckoo eats ZeuS v2

In addition, Cuckoo allows you to:

- Automate submission of analysis tasks
- Create analysis packages to define custom operations and procedures for performing an analysis
- Run multiple virtual machines concurrently
- Script the process and correlation of analysis results data
- Script and automate the generation of reports in the format you prefer

Download

Current Cuckoo Sandbox's version is **0.3.2**.

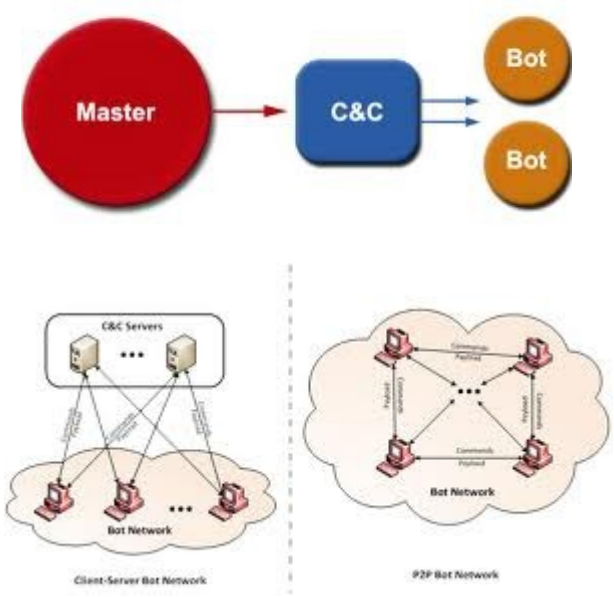
python

SQLite

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Video

Arquitectura genérica



Resultados:

Más análisis

Reporte

Clasificación

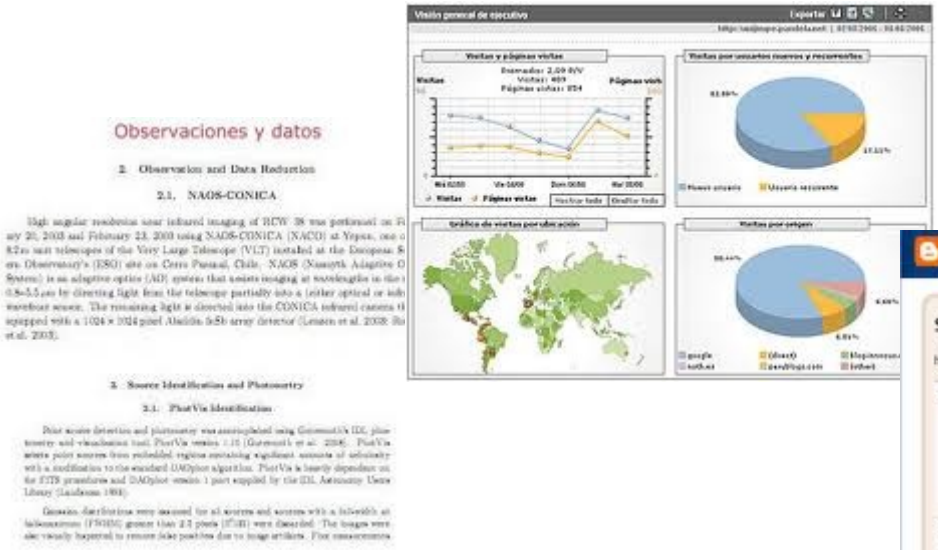
Comparación

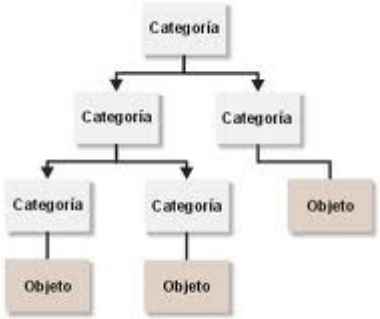
Método de limpieza

Firma para AV

Conocimiento !!

Ponga aquí lo que le agrade





Clasificación Jerárquica Simple

Motor antivirus	Versión	Última actualización	Resultado
a-squared	4.5.0.24	2009.08.14	Trojan-Downloader.Win32.Murlo!IK
F-Secure	8.0.14470.0	2009.08.14	Trojan-Downloader.JS.Qeo
Ikarus	T3.1.1.64.0	2009.08.14	Trojan-Downloader.Win32.Murlo!gen
Kaspersky	7.0.0.125	2009.08.14	Trojan-Downloader.JS.Qeo
McAfee+Artemis	5706	2009.08.13	Suspect-29!45EF13D76437
McAfee-GW-Edition	6.8.5	2009.08.14	Heuristic.BehavesLike.Win32.Trojan.C
Norman	6.01.09	2009.08.14	W32/Qiuadar.TIAU
Panda	10.0.0.14	2009.08.14	Suspicious file
PCTools	4.4.2.0	2009.08.12	HTML.Prime.Gen
ViRobot	4.4.5.0	2009.08.14	HTML.Prime.Gen

Malware UNAM - CERT

Arquitectura genérica

Captura:

Nepenthes

Dionaea

Spampot

ContagioDUMP

USB en el ciber

Listas

Otras fuentes.

Análisis:

Estático
Strings
Decompilar
Desensamblar

Dinámico
Depurar (Ollydbg, IDA)

Comportamiento
Ejecutarlo
Máquina Virtual
Máquina Real

Otros ?

Resultados:

Más análisis

Reporte

Clasificación

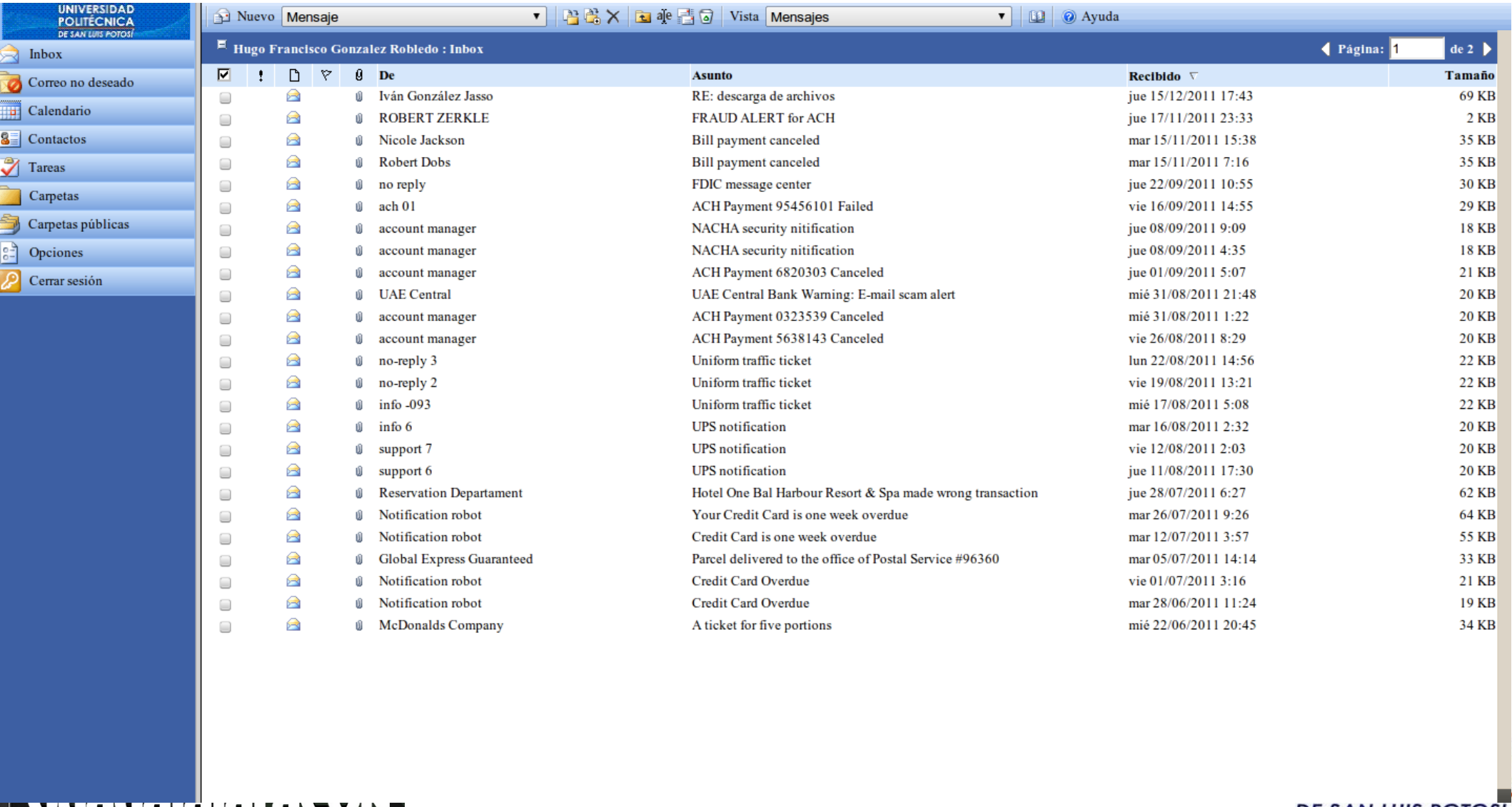
Comparación

Método de limpieza

Firma para AV

Conocimiento !!

Spampot

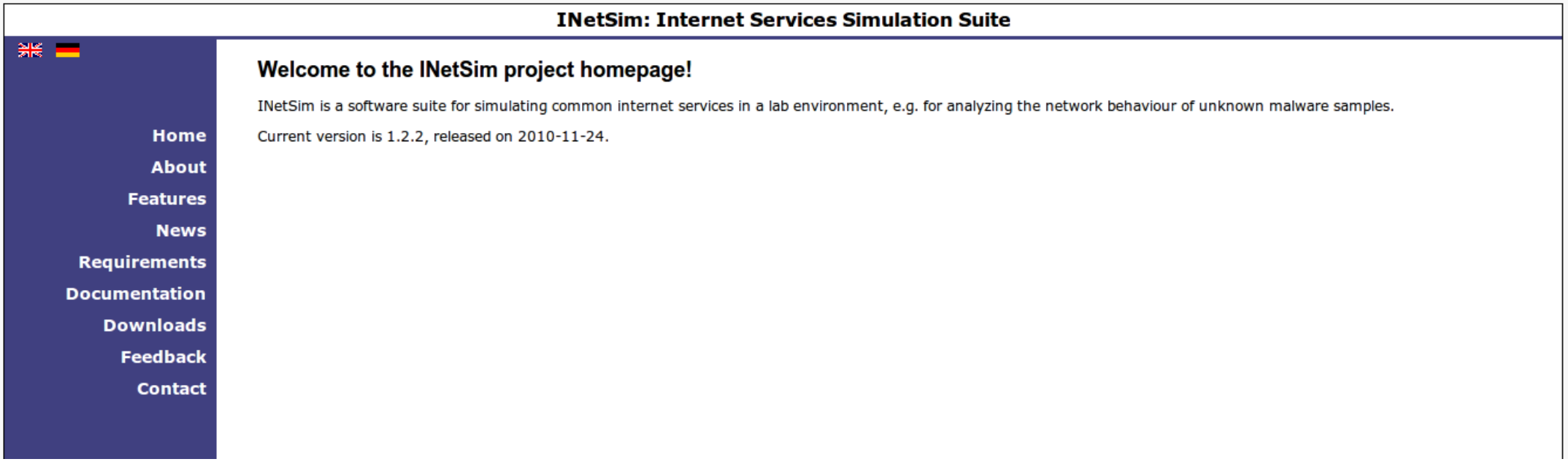


De	Asunto	Recibido	Tamaño
Iván González Jasso	RE: descarga de archivos	jue 15/12/2011 17:43	69 KB
ROBERT ZERKLE	FRAUD ALERT for ACH	jue 17/11/2011 23:33	2 KB
Nicole Jackson	Bill payment canceled	mar 15/11/2011 15:38	35 KB
Robert Dobs	Bill payment canceled	mar 15/11/2011 7:16	35 KB
no reply	FDIC message center	jue 22/09/2011 10:55	30 KB
ach 01	ACH Payment 95456101 Failed	vie 16/09/2011 14:55	29 KB
account manager	NACHA security nitification	jue 08/09/2011 9:09	18 KB
account manager	NACHA security nitification	jue 08/09/2011 4:35	18 KB
account manager	ACH Payment 6820303 Canceled	jue 01/09/2011 5:07	21 KB
UAE Central	UAE Central Bank Warning: E-mail scam alert	mié 31/08/2011 21:48	20 KB
account manager	ACH Payment 0323539 Canceled	mié 31/08/2011 1:22	20 KB
account manager	ACH Payment 5638143 Canceled	vie 26/08/2011 8:29	20 KB
no-reply 3	Uniform traffic ticket	lun 22/08/2011 14:56	22 KB
no-reply 2	Uniform traffic ticket	vie 19/08/2011 13:21	22 KB
info -093	Uniform traffic ticket	mié 17/08/2011 5:08	22 KB
info 6	UPS notification	mar 16/08/2011 2:32	20 KB
support 7	UPS notification	vie 12/08/2011 2:03	20 KB
support 6	UPS notification	jue 11/08/2011 17:30	20 KB
Reservation Departament	Hotel One Bal Harbour Resort & Spa made wrong transaction	jue 28/07/2011 6:27	62 KB
Notification robot	Your Credit Card is one week overdue	mar 26/07/2011 9:26	64 KB
Notification robot	Credit Card is one week overdue	mar 12/07/2011 3:57	55 KB
Global Express Guaranteed	Parcel delivered to the office of Postal Service #96360	mar 05/07/2011 14:14	33 KB
Notification robot	Credit Card Overdue	vie 01/07/2011 3:16	21 KB
Notification robot	Credit Card Overdue	mar 28/06/2011 11:24	19 KB
McDonalds Company	A ticket for five portions	mié 22/06/2011 20:45	34 KB

Casos

- InetSim

  http://www.inetsim.org/index.html



Android malware

droidbox

Android Application Sandbox

Project Home | Downloads | Wiki | Issues | Source

Summary | People

Project Information

+1 +2 Recommend this on Google

Starred by 62 users

Project feeds

Code license

GNU GPL v2

Introduction

DroidBox is developed to offer dynamic analysis of Android applications. The following information is shown in the results, generated when analysis is ended:

- Hashes for the analyzed package
- Incoming/outgoing network data
- File read and write operations

apkinspector

APKinspector is a powerful GUI tool for analysts to analyze the Android applications.

Project Home | Downloads | Wiki | Issues | Source

Summary | People

Project Information

+1 Recommend this on Google

Starred by 50 users

Project feeds

Code license

The goal of this project is to aide analysts and reverse engineers to visualize compiled Android packages and their corresponding DEX code. The primary focus of this project is to provide a visualization layer that's typically missing in existing Android reverse engineering tools, as well as to create a unified platform that combines several existing Android reverse engineering tools into a single unified view and context. For example this would include taking the control flow graph output from Androguard and unifying it with the code output from apktool, or dex2jar.

Please watch a quick overview video that was created to highlight some of the features of APKInspector: http://www.youtube.com/watch?v=X538N-x3UUY (English Site) or http://www.tudou.com/programs/view/IoT493jK-zk/ (Chinese Site)

The Honeynet Project

Navigation

- About us
- Blogs
  - Honeynet Project Blog
- Funding/Donations
- Challenges
- Chapters
- Papers
- Projects
- Code of Conduct
- Google SoC 2009
- Google SoC 2010
- Google SoC 2011
- Google SoC 2012
  - GSoC 2012 Project Ideas
  - GSoC 2012 Student Template
- Latest images
- Security Workshops
  - 2011 - Paris
  - 2012 - SF Bay Area

Android Reverse Engineering (A.R.E.) Virtual Machine available for download now!

Tue, 11/01/2011 - 03:11 — christian.seifert

The Honeynet Project is happy to announce the release of the Android Reverse Engineering (A.R.E.) Virtual Machine.

Do you need to analyze a piece of Android malware, but dont have all your analysis tools at hand? The Android Reverse Engineering (A.R.E.) Virtual Machine, put together by Anthony Desnos from our French chapter, is here to help. A.R.E. combines the latest Android malware analysis tools in a readily accessible toolbox.

Tools currently found on A.R.E. are:

- Androguard
- Android sdk/ndk
- APKInspector
- Apktool
- Axmlprinter
- Ded
- Dex2jar
- DroidBox
- Jad
- Smali/Baksmali

You can download A.R.E. for free from http://redmine.honeynet.org/projects/are/wiki.

christian.seifert's blog android

Ejemplos

- Dionaea + cuckoo = reportes
- Dionaea + Vbox (capture tcpdumps) = cluster
- Contagiodump + vbox (MacOS)

Conclusiones

- Estudiar malware por diversión !
- Existen muchas herramientas que ayudan, pero todavía falta mejorar la automatización, la interacción entre ellas.
- El malware actual es ingeniería aplicada! Criptografía, canales de comunicaciones, anti-depuración, anti-virtualización, nuevas protecciones.
- Wadalec, Duqu / Stuxnet.
- Android malware.

¿ Preguntas ?

@hugo_glez

Reto de analisis forense para android en:

http://atit.upslp.edu.mx/~hugo/guadalajaracon/