

GuadalajaraCON

20 y 21 de abril del 2012

Laboratorio de Análisis de Malware

@hugo_glez

This work is licensed under the Creative Commons
Attribution-NonCommercial-ShareAlike 3.0 Unported License.

To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>



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.



Disclaimer

¿ 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.

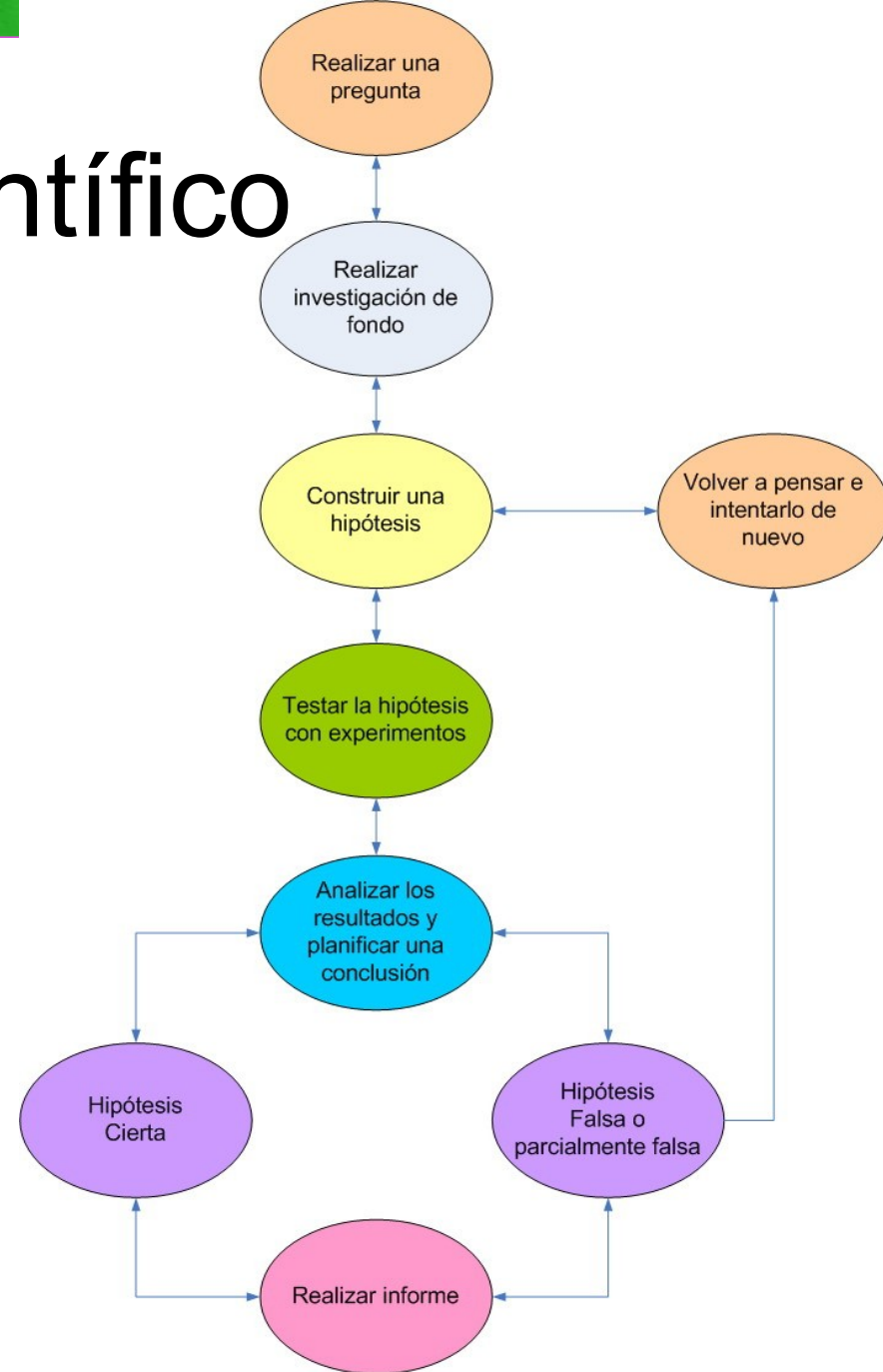
Laboratorio de análisis de malware

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

Captura:

Análisis:

Resultados:

Arquitectura genérica



Captura:

Nepenthes

Dionaea

Spampot

ContagioDUMP

USB en el ciber

Listas

Otras fuentes.

dionaea catches bugs

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

- Development
- Compiling & Installation
- Update
- Running
- Configuration
- Honors
- Links
- FAQ
- Segfault
- Support
- Blog

How it works

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

Security

contagio
malware dump

Monday, April 16, 2012

Java OSX CVE-2012-0507, CVE-2011-3544 and Flashback.35U sample

Dr. Web published GoodBoor/Flashback.35 (Flashback.35) with variants epidemic chronology to analyze the chronology of the...
 SAMPLE 1 is java.signed.appl01.s0061.em.phishing.csp.08 (see Michael Sobier's comment below) and 3 is JAVA.CVE.2011.3544 and another Flashback.35.02.

I am posting here 2 Java exploits used to distribute Flashback variants:
 SAMPLE 1: JAVA.CVE-2012-0507 is a stored Applet file, and appears to be a distributed Flashback.35.02 - as seen from the physical.

I don't know which domains distributed these exploits, but who knows if you do, but I guess we are seeing the malware distribution scheme common for Windows targeting exploit packs.

De	Asunto	Fecha
Ivan González Jaso	RE: descarga de archivos	jue 15/12/2011 17:43
ROBERT ZERKLE	FRAUD ALERT for ACH	jue 17/11/2011 23:33
Nicole Jackson	Bill payment canceled	mar 15/11/2011 15:38
Robert Dabo	Bill payment canceled	mar 15/11/2011 7:16
no reply	FDC message center	jue 22/09/2011 10:55
ach 01	ACH Payment 95456101 Failed	vie 16/09/2011 14:55
account manager	NACHA security notification	jue 08/09/2011 9:09
account manager	NACHA security notification	jue 08/09/2011 4:35
account manager	ACH Payment 0230301 Canceled	jue 01/09/2011 5:07
UAE Central	UAE Central Bank Warning: E-mail scam alert	mié 31/08/2011 21:48
account manager	ACH Payment 0232539 Canceled	mié 31/08/2011 1:22
account manager	ACH Payment 5638143 Canceled	vie 26/08/2011 8:29
no-reply 1	Uniform traffic ticket	jue 22/08/2011 14:56
no-reply 2	Uniform traffic ticket	vie 19/08/2011 13:21
info-493	Uniform traffic ticket	mié 17/08/2011 5:08
info 6	UPS notification	mar 16/08/2011 2:32
support 7	UPS notification	vie 12/08/2011 2:03
support 6	UPS notification	jue 11/08/2011 17:50
Reservation Department	Hotel One Hal Harbour Resort & Spa made wrong transaction	jue 28/07/2011 6:27
Notification robot	Your Credit Card is one week overdue	mar 26/07/2011 9:26
Notification robot	Credit Card is one week overdue	mar 12/07/2011 1:57
Global Express Guaranteed	Parcel delivered to the office of Postal Service 996360	mar 05/07/2011 14:14
Notification robot	Credit Card Overdue	vie 01/07/2011 3:16
Notification robot	Credit Card Overdue	mar 28/06/2011 11:24
McDonald's Company	A ticket for five portions	mié 22/06/2011 20:45

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

Development
Compiling & Installation
Update
Running
Configuration
Honors
Links
FAQ
Segfault
Support
Blog

libemu
x86 emu

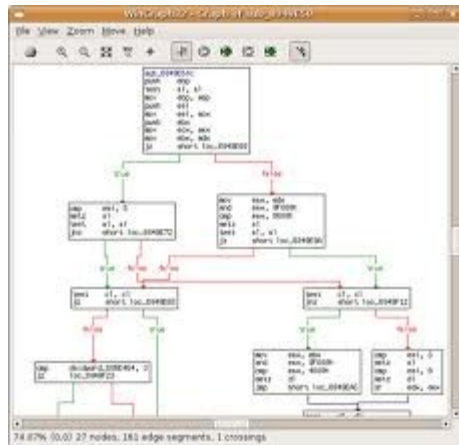
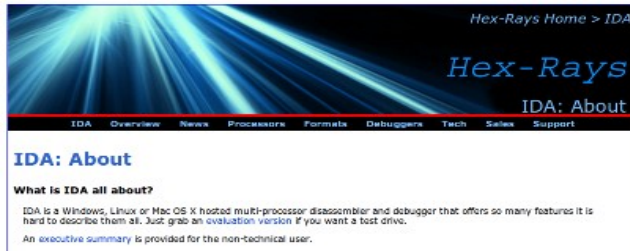
How IT WORKS

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



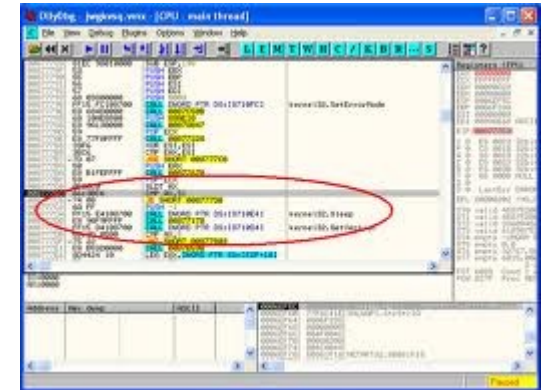
Análisis:

Estático
Strings
Decompilar
Desensamblar

Dinámico
Depurar (Ollydbg, IDA)

Comportamiento
Ejecutarlo
Máquina Virtual
Máquina Real

Otros ?





Navigation: About Download Documentation Donations Blog Contacts

Cuckoo Sandbox - Report f75900bf77405cb6dcd19b91312c853

Browser: http://localhost:8080/analysis/3

Network Analysis

DNS Requests

Hostname	IP Address
epsyun.com	50.63.39.1
sites.securepaynet.net	64.202.165.42

HTTP Requests

URL	Data
http://epsyun.com/zeus/config.bin	GET /zeus/config.bin HTTP/1.1 Accept: /* Connection: Close User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Host: epsyun.com Cache-Control: no-cache
http://sites.securepaynet.net/redirect_0.html	GET /redirect_0.html HTTP/1.1 Accept: /* Connection: Close User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Host: sites.securepaynet.net

Network analysis of a Zeus binary

Cuckoo Sandbox

AUTOMATED MALWARE ANALYSIS SYSTEM



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.

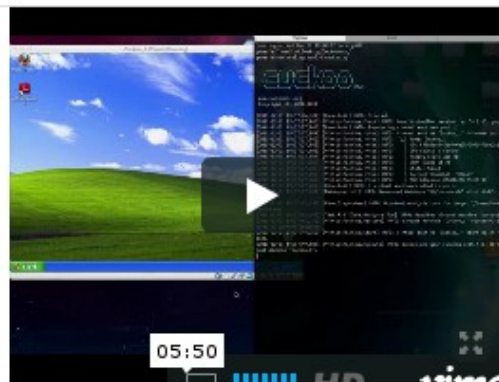
But it can do much more...
It's up to you to discover what and how.

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

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



[Cuckoo eats Zeus v2](#)

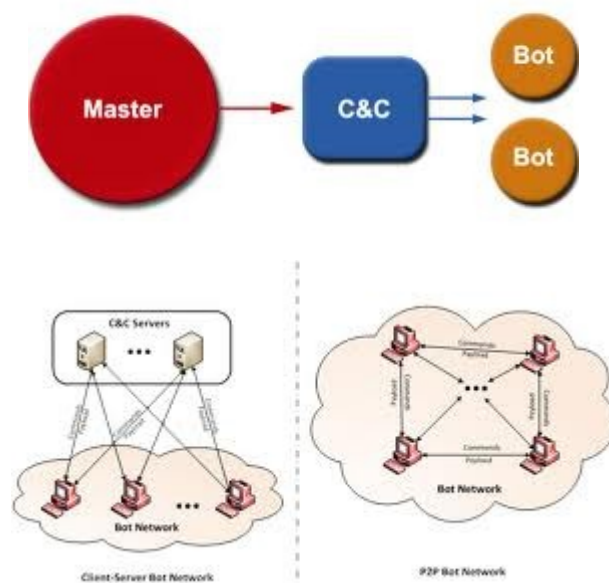
Download

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



Video

Arquitectura genérica



Resultados:

Más análisis

Reporte

Clasificación

Comparación

Método de limpieza

Firma para AV

Conocimiento !!

Ponga aquí lo que le agrada

Observaciones y datos

2. Observation and Data Reduction

2.1. NAOS-CONICA

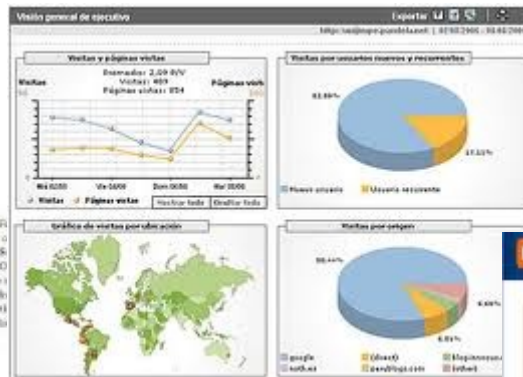
High angular resolution near infrared imaging of IC 348 was performed on February 20, 2008 and February 23, 2008 using NAOS-CONICA (NACO) at Yepun, one of 8.2 m main telescopes of the Very Large Telescope (VLT) installed at the European Southern Observatory's (ESO) site on Cerro Paranal, Chile. NAOS (Nasmyth Adaptive Optics System) is an adaptive optics (AO) system that consists imaging at wavelengths in the 0.8-2.5 μm by directing light from the telescope partially into a (faster) optical or infrared beam splitter. The remaining light is directed into the CONICA infrared camera which is equipped with a 1024×1024 pixel Aladdin 6-50 array detector (Larkin et al. 2008; Ili et al. 2008).

3. Source Identification and Photometry

3.1. PhotVis Identification

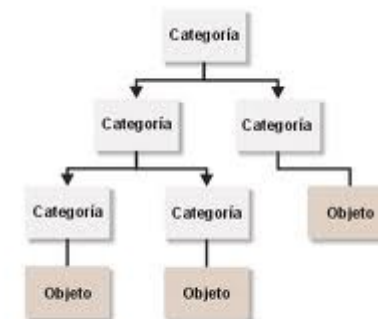
Star source detection and photometry was accomplished using GrismMatch (Dell'Amico et al. 2006) and VisMatch (Dell'Amico et al. 2006). PhotVis uses point sources from simulated regions containing significant amounts of variability with a modification to the standard DAOPHOT algorithm. PhotVis is heavily dependent on the FITS procedures and DAOPHOT routines supplied by the IRAF Astronomy Users Library (Landsman 1994).

Given the detection was accurate for all sources and sources with a likelihood of false detection (FDR) greater than 2.5 percent (2%) were discarded. The images were also visually inspected to ensure false positive due to large artifacts. Four observations



Motor antivirus	Versión	Última actualización	Resultado
n-antivirus	4.5.0.24	2009.08.14	Trojan-Dropper.9432.Hwndwn.DK
F-Secure	8.0.14470.0	2009.08.14	Trojan-Dropper.JL.wtg
Avast	5.1.1.2.44.0	2009.08.14	Trojan-Dropper.9432.Hwndwn
Symantec	7.0.0.125	2009.08.14	Trojan-Dropper.JL.wtg
McAfee/Scansite	8708	2009.08.13	Suspicio-29144821A056287
McAfee-DF-Engine	6.5.3	2009.08.14	Behavioral.Behavioral.Malicious.Trojan.D
Norton	6.01.09	2009.08.14	Win/Dropper.TMG
Panda	10.0.0.14	2009.08.14	Suspicious.File
BitDefender	4.6.2.0	2009.08.13	WTD.Symantec.Dns
VirusBuster	4.6.3.0	2009.08.14	WTD.Symantec.Dns

Malware UNAM - CERT



Clasificación Jerárquica Simple

The dialog box includes the following elements:

- Follow this Blog:** Header with a Blogger logo.
- Start following The Blog:** Sub-header with the URL <http://www.wdweers/pickup.blogspot.com/>.
- Follow publicly as Denmark:** Selected radio button option.
 - Follow publicly to tell the blog's author and the world that you're a fan.
 - Stay updated with this blog's posts on your Blogger Dashboard.
- Follow anonymously:** Unselected radio button option.
 - Keep your subscription private.
 - Stay updated with this blog's posts on your Blogger Dashboard.
- Followers:** A small grid of user avatars.
- Your picture:** A placeholder for the user's profile picture.
- Buttons:** 'FOLLOW' (orange) and 'CANCEL' (blue).

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

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

- Inbox
- Correo no deseado
- Calendario
- Contactos
- Tareas
- Carpetas
- Carpetas públicas
- Opciones
- Cerrar sesión

Nuevo Mensaje

Vista Mensajes

Ayuda

Hugo Francisco Gonzalez Robledo : Inbox

Página: 1 de 2

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

Casos

- InetSim

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

INetSim: Internet Services Simulation Suite



Home

About

Features

News

Requirements

Documentation

Downloads

Feedback

Contact

Welcome to the INetSim project homepage!

INetSim is a software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples.

Current version is 1.2.2, released on 2010-11-24.

Android malware



[Project Home](#) [Downloads](#) [Wiki](#) [Issues](#) [Source](#)

[Summary](#) [People](#)

Project Information

+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



[Project Home](#) [Downloads](#) [Wiki](#) [Issues](#) [Source](#)

[Summary](#) [People](#)

Project Information

Recommend this on Google

Starred by 50 users
[Project feeds](#)

Code license
GNU GPL v2

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-x3UUUY> (English Site) or <http://www.tudou.com/programs/view/loT493jK-zk/> (Chinese Site)



The HoneyNet Project

[Home](#) > [Blogs](#) > [christian.seifert's blog](#)

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.honey.net.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/>