

# Laboratorio de Malware

Jose Moruno Cadima

Agosto 2013

## 1 Whoami

## 2 Introducción

## 3 Como realizar un análisis

## 4 Como realizar un análisis II

## 5 Un análisis REAL

## 1 Whoami

## 2 Introducción

## 3 Como realizar un análisis

## 4 Como realizar un análisis II

## 5 Un análisis REAL



Jose Moruno Cadima A.K.A Snifer

- Consultor, Análisis de Malware, Android .
- Desarrollador en Python, Perl, Ruby.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.



Jose Moruno Cadima A.K.A Snifer

- Consultor, Análisis de Malware, Android .
- Desarrollador en Python, Perl, Ruby.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.



Jose Moruno Cadima A.K.A Snifer

- Consultor, Análisis de Malware, Android .
- Desarrollador en Python, Perl, Ruby.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.



Jose Moruno Cadima A.K.A Snifer

- Consultor, Análisis de Malware, Android .
- Desarrollador en Python, Perl, Ruby.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.



Jose Moruno Cadima A.K.A Snifer

- Consultor, Análisis de Malware, Android .
- Desarrollador en Python, Perl, Ruby.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.

## 1 Whoami

### ■ Yanapti

Whoami  
hackmeeting  
Yanapti

e-security



## 1 Whoami

## 2 Introducción

## 3 Como realizar un análisis

## 4 Como realizar un análisis II

## 5 Un análisis REAL

## 2 Introducción

- Porque la charla
- ¿Que es un laboratorio?
- Malware

# Introducción

hackmeeting  
Porque la charla

e-security

El objetivo de la charla es...

- 1 Conocer un poco de historia.
- 2 Como interactua.
- 3 Como analizarlo, detectarlo.
- 4 Contribuir a la sociedad.
- 5 Aceptar un nuevo reto, resolver problemas!!

# Introducción

hackmeeting  
Porque la charla

e-security

El objetivo de la charla es...

- 1 Conocer un poco de historia.
- 2 Como interactua.
- 3 Como analizarlo, detectarlo.
- 4 Contribuir a la sociedad.
- 5 Aceptar un nuevo reto, resolver problemas!!

# Introducción

hackmeeting  
Porque la charla

e-security

El objetivo de la charla es...

- 1 Conocer un poco de historia.
- 2 Como interactua.
- 3 Como analizarlo, detectarlo.
- 4 Contribuir a la sociedad.
- 5 Aceptar un nuevo reto, resolver problemas!!

# Introducción

hackmeeting  
Porque la charla

e-security

El objetivo de la charla es...

- 1 Conocer un poco de historia.
- 2 Como interactua.
- 3 Como analizarlo, detectarlo.
- 4 Contribuir a la sociedad.
- 5 Aceptar un nuevo reto, resolver problemas!!

# Introducción

hackmeeting  
Porque la charla

e-security

El objetivo de la charla es...

- 1 Conocer un poco de historia.
- 2 Como interactua.
- 3 Como analizarlo, detectarlo.
- 4 Contribuir a la sociedad.
- 5 Aceptar un nuevo reto, resolver problemas!!

# Introducción

hackmeeting  
Porque la charla

e-security

El objetivo de la charla es...

- 1 Conocer un poco de historia.
- 2 Como interactua.
- 3 Como analizarlo, detectarlo.
- 4 Contribuir a la sociedad.
- 5 Aceptar un nuevo reto, resolver problemas!!

## 2 Introducción

- Porque la charla
- ¿Que es un laboratorio?
- Malware

# Introducción

hackmeeting

¿Qué es un laboratorio?

e-security



Un laboratorio de malware que es para ti...

- 1 Investigaciones.
- 2 Experimentos.
- 3 Practicas.
- 4 Integridad.

# Introducción

hackmeeting

¿Qué es un laboratorio?

e-security



Un laboratorio de malware que es para ti...

- 1 Investigaciones.
- 2 Experimentos.
- 3 Prácticas.
- 4 Integridad.

# Introducción

hackmeeting

¿Qué es un laboratorio?

e-security



Un laboratorio de malware que es para ti...

- 1 Investigaciones.
- 2 Experimentos.
- 3 Prácticas.
- 4 Integridad.

# Introducción

hackmeeting

¿Qué es un laboratorio?

e-security



Un laboratorio de malware que es para ti...

- 1 Investigaciones.
- 2 Experimentos.
- 3 Practicas.
- 4 Integridad.

# Introducción

hackmeeting

¿Qué es un laboratorio?

e-security



Un laboratorio de malware que es para ti...

- 1 Investigaciones.
- 2 Experimentos.
- 3 Practicas.
- 4 Integridad.

## 2 Introducción

- Porque la charla
- ¿Que es un laboratorio?
- Malware

# Introducción

hackmeeting  
Malware

e-security

Es un software dañino cuyo objetivo es infiltrarse o dañar un equipo.

Breve historia del Malware

Mejor lo vemos en un video!!

# Introducción

hackmeeting  
Malware

e-security

Es un software dañino cuyo objetivo es infiltrarse o dañar un equipo.

## Breve historia del Malware

Mejor lo vemos en un video!!

# Introducción

hackmeeting  
Malware



e-security

## Primer Virus

El primer virus fue creado en los laboratorios BELL, con la intención de realizar un juego llamado Core War el cual consistía en llenar la memoria RAM del contrincante en el menor tiempo posible.

## Robert Tappan Morris

Es conocido por crear el Gusano Morris en 1988, considerado como el primer gusano de ordenador de la era de Internet.

# Introducción

hackmeeting  
Malware

e-security

Actualmente se usa para cometer actos ilegales

- 1 Robo de información, DoS, SPAM etc.
- 2 Sabotaje
- 3 Stuxnet
- 4 Virus de la policía (Lo veremos luego)

# Introducción

hackmeeting  
Malware

e-security

Actualmente se usa para cometer actos ilegales

- 1 Robo de información, DoS, SPAM etc.
- 2 Sabotaje
- 3 Stuxnet
- 4 Virus de la policía (Lo veremos luego)

# Introducción

hackmeeting  
Malware

e-security

Actualmente se usa para cometer actos ilegales

- 1 Robo de información, DoS, SPAM etc.
- 2 Sabotaje
- 3 Stuxnet
- 4 Virus de la policía (Lo veremos luego)

# Introducción

hackmeeting  
Malware

e-security

Actualmente se usa para cometer actos ilegales

- 1 Robo de información, DoS, SPAM etc.
- 2 Sabotaje
- 3 Stuxnet
- 4 Virus de la policía (Lo veremos luego)

# Introducción

hackmeeting  
Malware

e-security

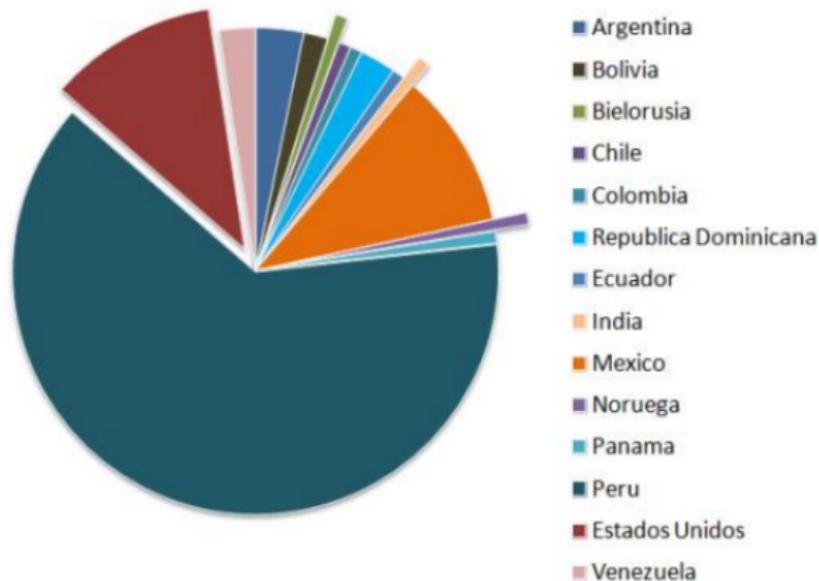
Keyloggers, Bootnets, Troyanos, Rogue Rasonware, Rootkits, Backdoors.

# Introducción

hackmeeting  
Malware

e-security

Un pequeno análisis.



## 1 Whoami

## 2 Introducción

## 3 Como realizar un análisis

## 4 Como realizar un análisis II

## 5 Un análisis REAL

# Como realizar un análisis

hackmeeting

e-security

- 1 Reconocimiento – Tecnología
- 2 Análisis
- 3 Experimentación
- 4 Conclusión

# Como realizar un análisis

hackmeeting

e-security

- 1 Reconocimiento – Tecnología
- 2 Análisis
- 3 Experimentación
- 4 Conclusión

# Como realizar un análisis

hackmeeting

e-security

- 1 Reconocimiento – Tecnología
- 2 Análisis
- 3 Experimentación
- 4 Conclusión

# Como realizar un análisis

hackmeeting

e-security

- 1 Reconocimiento – Tecnología
- 2 Análisis
- 3 Experimentación
- 4 Conclusión

## 1 Whoami

## 2 Introducción

## 3 Como realizar un análisis

## 4 Como realizar un análisis II

## 5 Un análisis REAL

# Como realizar un análisis II

hackmeeting

e-security

Las etapas que se pueden seguir son:

- Recolección
- Análisis



- Conclusion

## 4 Como realizar un análisis II

### ■ Recolección

# Como realizar un análisis II

hackmeeting  
Recolección

e-security



Pablo Contreras > Programadores en Visual Basic  
<http://bitly.com/1cB8yVZ>

Like · Comment · Share · 4 hours ago via mobile ·

# Como realizar un análisis II

hackmeeting  
Recolección

e-security

## 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 !!

## 1 Whoami

## 2 Introducción

## 3 Como realizar un análisis

## 4 Como realizar un análisis II

## 5 Un análisis REAL

# Un análisis REAL

hackmeeting

e-security

- Creación de un ambiente controlado
- Análisis Estático
- Análisis Dinámico

# Un análisis REAL

hackmeeting

e-security

- Creación de un ambiente controlado
- Análisis Estático
- Análisis Dinámico

# Un análisis REAL

▶ hackmeeting

▶ e-security

- Creación de un ambiente controlado
- Análisis Estático
- Análisis Dinámico

# Un análisis REAL

▶ hackmeeting

▶ e-security

- Creación de un ambiente controlado
- Análisis Estático
- Análisis Dinámico

## 5 Un análisis REAL

- Distribuciones
- Lo que hacemos hoy...

# Un análisis REAL

hackmeeting  
Distribuciones

e-security

## REMnux

REMnux es la distribución de GNU/Linux basada en Ubuntu de Lenny Zeltser para el análisis e Ingeniería Inversa del Malware (Reverse-Engineering Malware – REM).

## Bugtraq y MOBISEC

Bugtraq distribución española la cual tiene una sección para el análisis de Malware.

Mobisec distribución orientada al análisis de malware para dispositivos Android.

## 5 Un análisis REAL

- Distribuciones
- Lo que hacemos hoy...

# Un análisis REAL

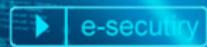
hackmeeting

Lo que hacemos hoy...

e-security

LOS ACTOS PRESENTES DERIVAN LA SITUACION FUTURA.

SOMOS JOVENES Y TENEMOS QUE APRENDER A TENER UNA MEDIDA A NUESTRAS TRAVESURAS, LA INQUIETUD DEBEMOS DE SABER CANALIZAR Y CONTROLARLA.



# Gracias por su atención

**Jose Moruno Cadima**  
snifer@h-sec.org

Presentación compuesta con L<sup>A</sup>T<sub>E</sub>X