# HUM
# Homemade Undetectable Malware

by
Adrián Puente Z.



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# ¿Qué es el Malware?

- **Tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.**
- **El término malware incluye virus, gusanos, troyanos, la mayoría de los rootkits, spyware, adware intrusivo, crimeware y otros software maliciosos e indeseables.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Tipos de Malware

- Virus
- Gusanos
- Troyano
- Backdoors
- Adware
- Spyware
- Dialer
- Hijacker
- Joke
- Rootkit
- Herramienta de Hacking
- Keylogger
- Hoax
- Spam
- FakeAVs & Rogues



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# ¿Para qué se emplea?

- **Acceso remoto**
- **Fraude electrónico**
- **Espionaje Industrial y Gubernamental**
- **Anonimato**
- **Ciberterrorismo**
- **Phishing, SPAM, BotNets**
- **Guerra Cibernetica**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Una Amenaza Real

- **La firma inglesa Sophos estima que el 40% del spam es enviada por equipos zombies.**
- **Akamai culpa a los equipos zombie por los ataques de negacion de servicios.**
- **Reuters reporta que adolescentes hackers rentan sus botnets por $100 la hora.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Nos Vigilan

- **“Sony BMG Music Entertainment distribuía un esquema de protección contra copia en sus Cds musicales que instalaba en secreto un rootkit en los ordenadores.”**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# El Gran Hermano

- **"Se habla que cooperamos con algunos gobiernos para crear una puerta trasera, mediante la cual los gobiernos puedan acceder a datos cifrados de BitLocker; pero esto ocurrirá sobre mi cadáver"**

  **— Niels Ferguson**
  **Desarrollador jefe de Microsoft**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Ciberguerra

- **En Estonia en 2007, unos millones de computadores fueron usados para bloquear los Websites del gobierno y el comercio de ello. El ataque venía de Rusia.**
- **Se presume que el mismo ataque fue perpetrado en Georgia en el 2008.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

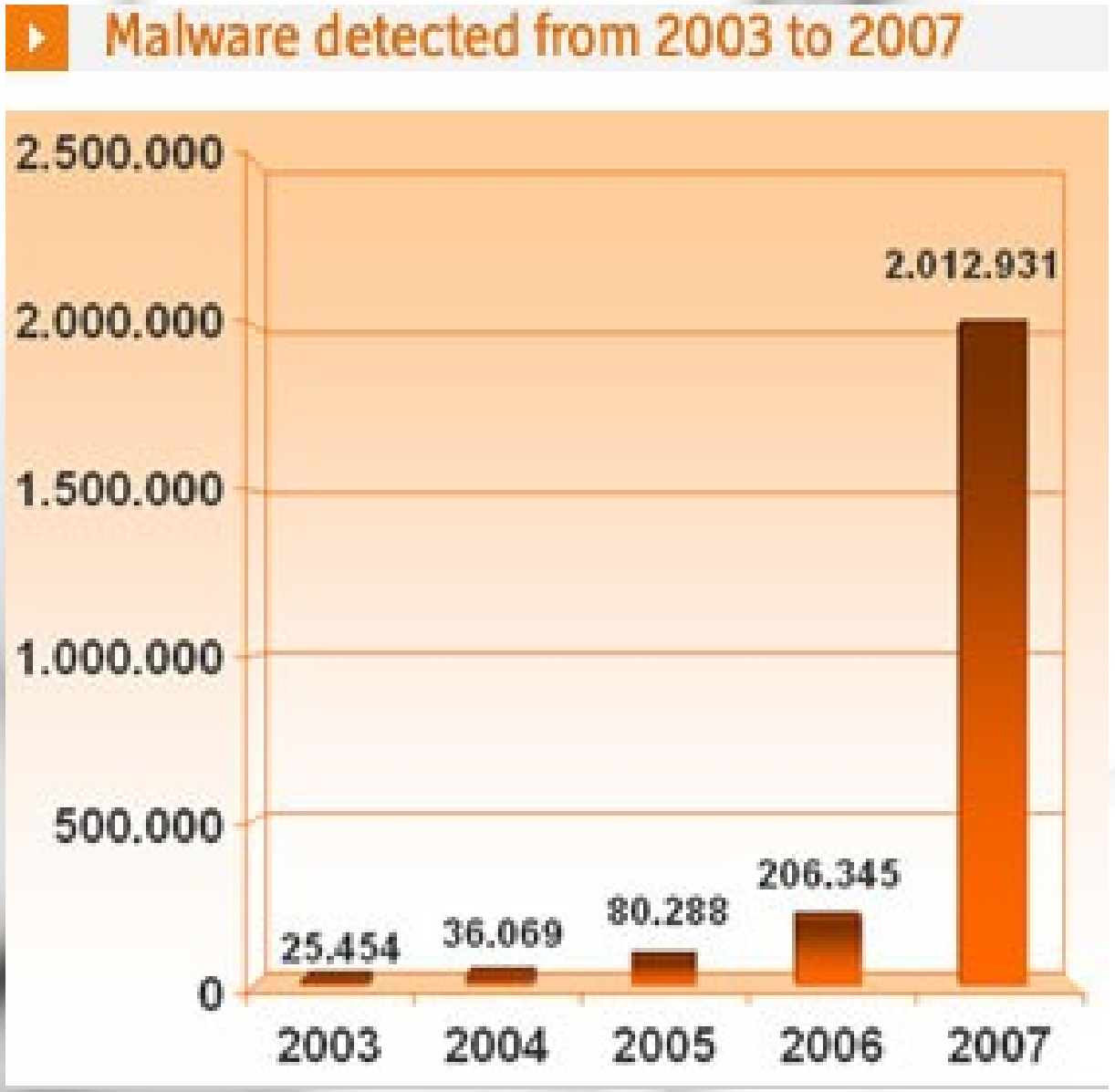
# ¿Qué Infecta?

- **Equipos personales, no importa si es Linux, Windows o MAC**
- **Tarjetas de Video**
- **Equipos Celulares**
- **Firmaware de BIOS, cómo hace poco pasó con Servidores Dell.**
- **Consolas de video juegos**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Crecimiento Exponencial






Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Dónde Conseguirlo

- **Foros y sitios en internet dan tutoriales y código fuente.**
- **Se pueden comprar versiones personalizadas**
- **Se pueden rentar botnets y pagar con dinero irrastreable.**



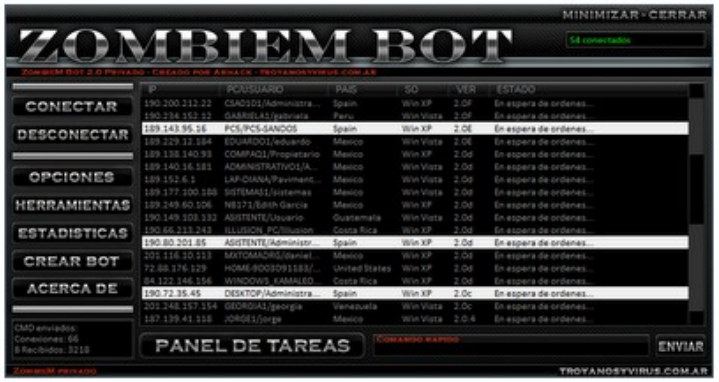
Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Mostrando las entradas más recientes con la etiqueta **PRODUCTOS PRIVADOS / PAGO** Mostrar las entradas más antiguas

# ZombieM Bot 2.0 PRIVADO

Publicado por MAURO
Etiquetas: BOT/BOTNETS/IRC, PRODUCTOS PRIVADOS / PAGO

**ZombieM Bot** es un nuevo bot programado por **Arhack**, diseñado para testear la seguridad de redes y administrar pcs bajo sistema operativo windows de forma remota y masiva.




**Tareas**
Una de las caracteristicas que hacen que ZombieM se destaque del resto es la gran cantidad de tareas que puede realizar y la efectividad de las mismas, a continuacion se explicaran brevemente las mas importantes.

**Funciones Basicas**
ZombieM bot posee las funciones basicas para administrar los archivos de las pcs conectadas:
-Descargar archivo / Descargar y ejecutar
-Ejecutar archivo / Comandos
-Crear carpetas
-Borrar archivo
-Borrar carpeta
-Genera archivos con contenido (bat, txt, inf, reg,etc)
-Actualizar servidor

BUSQUEDA!

Entradas (RSS) Comentarios (RSS)

## TROYANOSYVIRUS.COM.AR

Bienvenidos a troyanosyvirus, blog dedicado al estudio del malware, desde el punto de vista del "atacante". Todo lo que encuentres en el blog es solo para uso instructivo y para su correspondiente analisis, el autor ni nadie se hace responsable por el mal uso que le des a lo publicado en este blog. Para Consultas, criticas, sugerencias o lo que sea escribime desde la PAGINA DE CONTACTO

*** Productos destacados ***

* ZombieM Bot 2.0 - 180 EUROS

## Etiquetas

ACCESO REMOTO (7)
ANONIMATO (2)
BINDERS/JOINERS (14)
BOT/BOTNETS/IRC (6)
CODIGO FUENTE (11)
DOS/DDOS/NUKERS (10)
DOWNLOADERS (2)
ENCRIPTADORES (28)
GUSANOS/WORMS (10)
INDETECTABLES (28)
KEYLOGGERS/STEALERS/PASSWORDS (13)
KILLERS (1)
LANZADORES (1)
MANEJO DE ARCHIVOS (4)
MANUALES (29)
MEDIOS DE INFECCION (5)
MSN (9)
OTROS (7)

## Suscribite a TYV

Suscribite via mail

Ingresa tu correo electronico:

Suscribirme

O via RSS mediante el siguiente boton

3469 readers
BY FEEDBURNER

## Vínculos de suscripción

Entradas
Todos los comentarios

## Seguidores

eset virus radar on-line

Mayores amenazas en las últimas 24 hs

1. Win32/Netsky.Q worm
2. a variant of Win...
3. Win32/Zafi.B worm
4. Win32/Netsky.C worm
5. Win32/Mydoom.Q worm

## Afiliados

Arhack RHACK.COM.AR
Gmail?
HackStore
SCB LAB'S

# Nuclear Winter Crew

Main | Products | Buy | Community | Partners | Development | Search | About | Support | Articles



**Our group is specialized in hacking, keylogging, spy, security, auditing and related software. You may find binders, keyloggers, uploaders, webdownloaders, remote administration tools, socks daemons, tools related in general. You may also check the open source section, with complete open sourced programs. We can code a custom application for you, visit the "Buy" section for more information. This website uses Javascript and cookies to work, so please enable both**

## **Xmas Discounts on Bandook** posted by Princeali on December 2nd 2009

Greetings everybody , it has been a long time since i posted here , however i would like to take the opportunity to announce discounts on **Bandook 1.37 Private** editions (VIP , VIP Plus , Business)during this month , the offer is valid only until the new year , i would like also to let u know that i will have a new program released on new year , i will leave it as a surprise for u guys ,i wish all u all a merry Christmas and happy new year from now :)

## **What?!** posted by caesar2k on November 4th 2009

Don't panic, NR 3.0 decreased the "%" done because I've decided to redo to a more flexible and reliable data communication (without using text), and to take advantage of traffic compression. I'm reusing most of memory possible, the opposite from version 2.1, that copy all data everywhere, everytime. That's one reason because (after years of programming) you realize using text for communication is bad! Another thing, I've removed the programs that will never be completed, because either the coder died or the project won't just never be completed, some mine as well.

## Top 5 Popular Products

1. Nuclear RAT 2.1.0 [108670]
2. Bandook RAT v1.35 [NEW] [69273]
3. Maya Pws v1.1 [49731]
4. Seed 1.1 [17029]
5. Pretator Binder v1.6 [14200]

## Lastest 5 Releases

1. Nuclear Messenger Loader 1.1
2. Nuclear RAT 2.1.0
3. Bandook RAT v1.35 [NEW]
4. TntControls Converter
5. Nuclear Conversation v1.0

## Poll

**On the next Nuclear RAT upgrade, what you would like to see?**

- Faster and better screencap and webcam

princeali@[redacted] Tue, Jun 8, 2010 at 11:40 AM

To: [redacted]

Reply | Reply to all | Forward | Print | Delete | Show original

Bandook version 1.38 is the current private edition , its the result on 3 years of developement after 1.35 , it contain many changes like Vista , windows 7 Support, 64bits Compatibility , Unicode support , Multi Language interface , network manager , ports monitor and a long list of additions and fixes .

VIP ( 300 $ ) : Bandook 1.38 Undetected with support [ 1 Time only]

VIP Plus ( 500 $ ) : Bandook 1.38 and all Future versions (released privatly) Undetected with Support and upgrades

Business Edition ( 2000 $ ) : Bandook 1.39 and all future versions , plus direct replacement on detection , extra features like Certificate manager , polymorphic plugin , minimized windows capture , bluetooth notification , IE Form Grabber , Smart Video Recorder , firefox form grabber and more

When purchasing a Copy u get Access to a Private Customers Portal where u can get support , download ur version , and more (Currently down under maintenance but will be up soon)

Payment methods accepted :
---

-Western Union
-Money Gram
-WebMoney
-Bank Transfer

regards

- Show quoted text -

Sent on the move from my BlackBerry® smartphone from mtc touch

Reply | Reply to all | Forward | Print | Delete | Show original

- Yeeeiiii!!
- Pero yo no vine a esto!
- A que hora h4x0r34m05?

# Cómo son Detectados

- **Por comparación del archivo contra una firma de antivirus.**
- **Proactiva**
  - **Es la técnica de las firmas pero en memoria durante la ejecución.**
- **Por Heurística**
  - **Consiste en revisar poco a poco cada pedazo del código para ver instrucciones que diferencían a un virus de un programa normal.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# ¿Instrucciones?

- **Pedazos de código que hacen llamadas al sistema o APIs que nos dan acceso a cierta funcionalidad.**




Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Lenguajes

- **Mientras mas alto nivel mas complicado es hacerlo indetectable**
  - **Mucho Malware es programado es C/C++ o Pascal/Delphi pero el favorito es ASM**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Ensam... WTF?

- **Muy complicado pero te permite crear tus rutinas y poder modificar al vuelo la funcionalidad del malware para evitar ser detectado.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Herramientas de Ocultación
## — Binders —

- **Unen nuestro malware con uno o mas programas inocentes.**
- **Crece el tamaño del programa.**
- **Una vez ejecutado descomprime ambos programas en disco y el antivirus detecta y detiene nuestro malware.**
- **Muchos binders ya son detectados por antivirus.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Herramientas de Ocultación
## — Crypters —

- **Toman nuestro malware y lo cifran evitando que el antivirus lo detecte.**
- **Aumenta un poquito de tamaño nuestro malware.**
- **Al ser ejecutado carga y ejecuta directamente en memoria nuestro malware**
- **Muchos crypters ya son detectados por antivirus.**



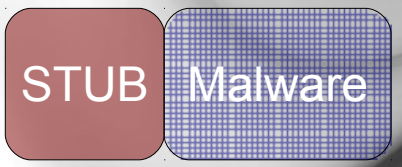
Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

HACK arandas

# Cómo Trabajan

- **Binders**


- **Crypters**






Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Porqué no Funcionan


- **Porque el STUB ya está marcado como Malware dentro de los Antivirus.**
- **Habría que crear un STUB que fuera indetectable y ese emplearlo en el Binder o Crypter.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

HACK arandas

# Técnicas de Ocultación
## — HEX —

- **El mas simple de hacer, solo se necesita un notepad, un hex editor y mucha paciencia.**
- **Consiste en modificar a nivel hexadecimal un malware para destruir las firmas intentando no dañar el flujo del programa.**
- **Se vuelve un infierno si tiene más de una firma el malware**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Técnicas de Ocultación
# — RIT —

- **Es mas complicado pero con la práctica se vuelve automático**

- **Consiste mover las funciones/firmas de un programa a espacios en blanco y modificar el flujo del programa para no dañarlo.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Técnicas de Ocultación
## — MEEPA —

- **Requiere conocimiento básico del ensamblador y de la funcionalidad del arranque del programa.**

- **Consiste modificar valores dentro del programa y restaurarlos al vuelo dentro de la ejecución en memoria.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Demo

- **Funcionó?**

**SI** **NO**



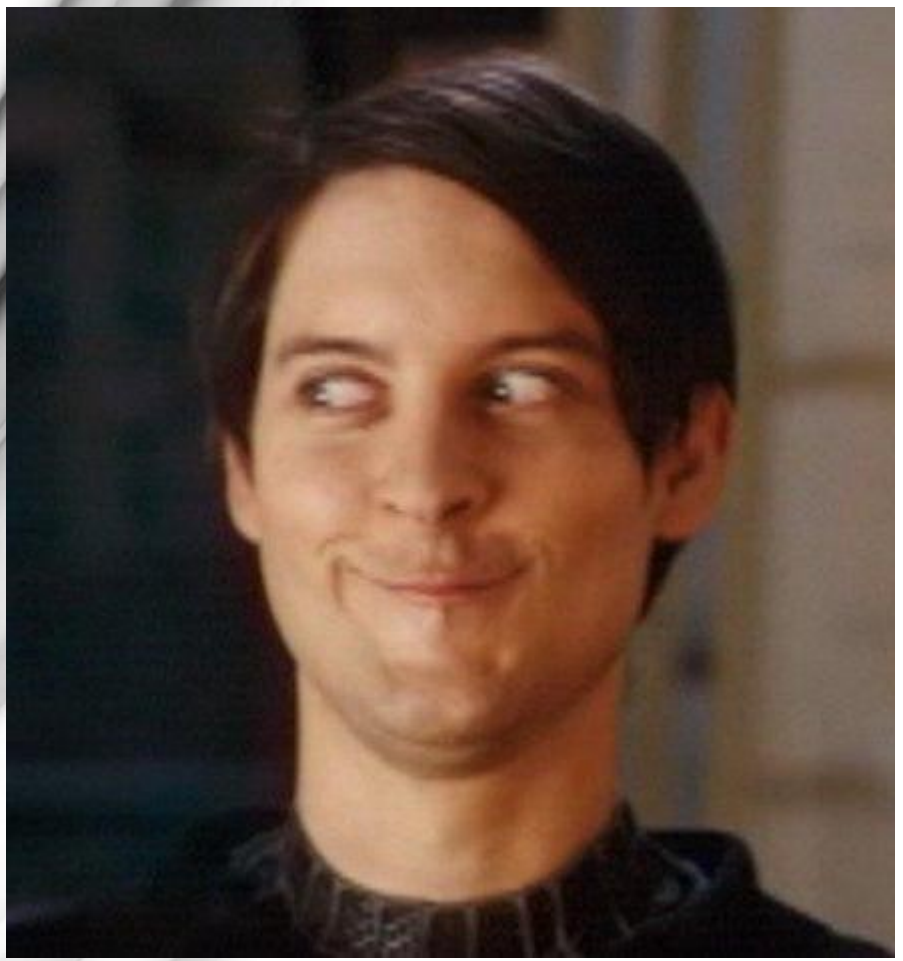
Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# FFFFFUUUUUU!!!!



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# YEEEEEIIII!!!!



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

hackarandas

# Pentest

- **Quien realice el test, intentará mostrar como desde una PC corriente con conexión a Internet es posible ingresar a la red interna de la organización, utilizando las mismas técnicas que seguiría un atacante o espía informático. Este intento se encuentra autorizado y planificado, si bien muy pocos empleados son notificados del mismo.**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

HACK arandas

# Metodos de Propagación

- **Correo**
  - **Correo electrónico con Phishing**
- **Explotación**
  - **Ataque directo al navegador**
- **Java**
  - **Applet de Java malicioso**
- **PDF**
  - **Ataque a Adobe Reader**
- **Office**
  - **Macro de VBS Malicios**

# Ingeniería Social


Apreciable Usuario:

Nos ponemos en contacto con usted, para hacerle saber que existen nuevas actualizaciones en nuestro sitio Microsoft Windows Update:

- Herramienta de eliminación de software malintencionado (gratuito)

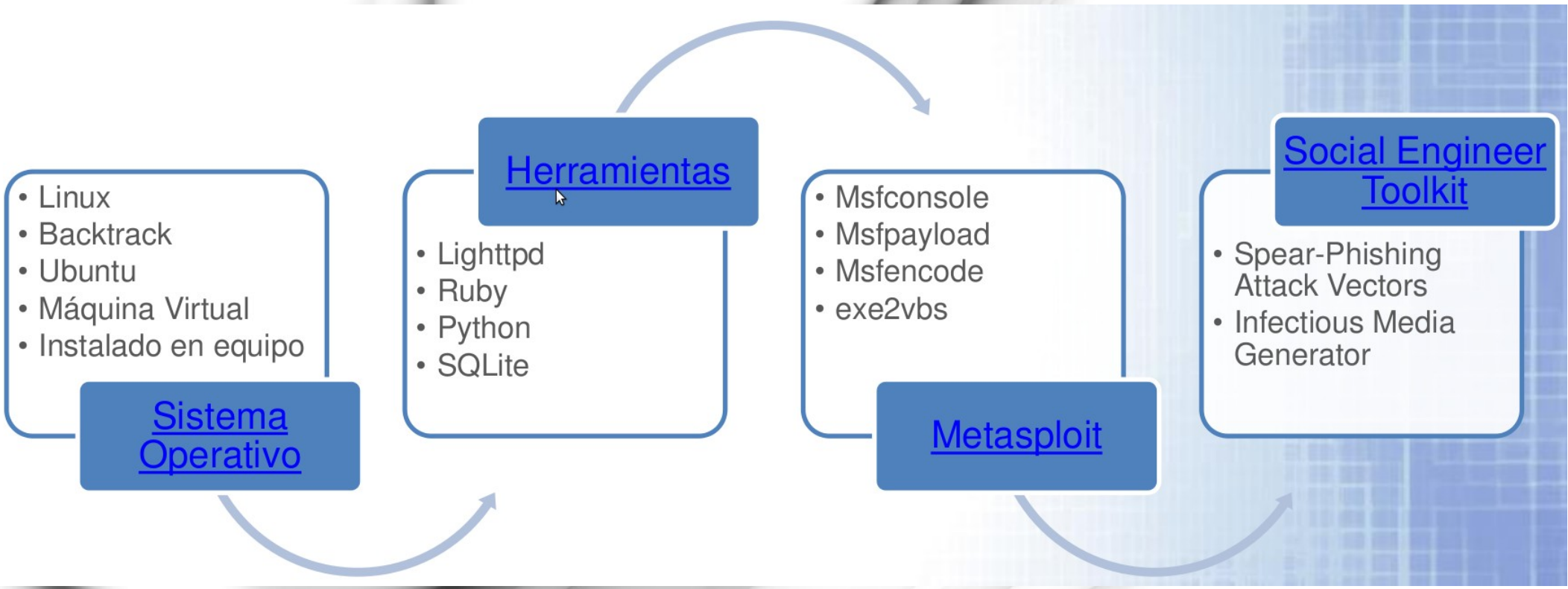
Entre aquí y en el sitio espejo para bajar las actualizaciones correspondientes.




Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

HACK arandas

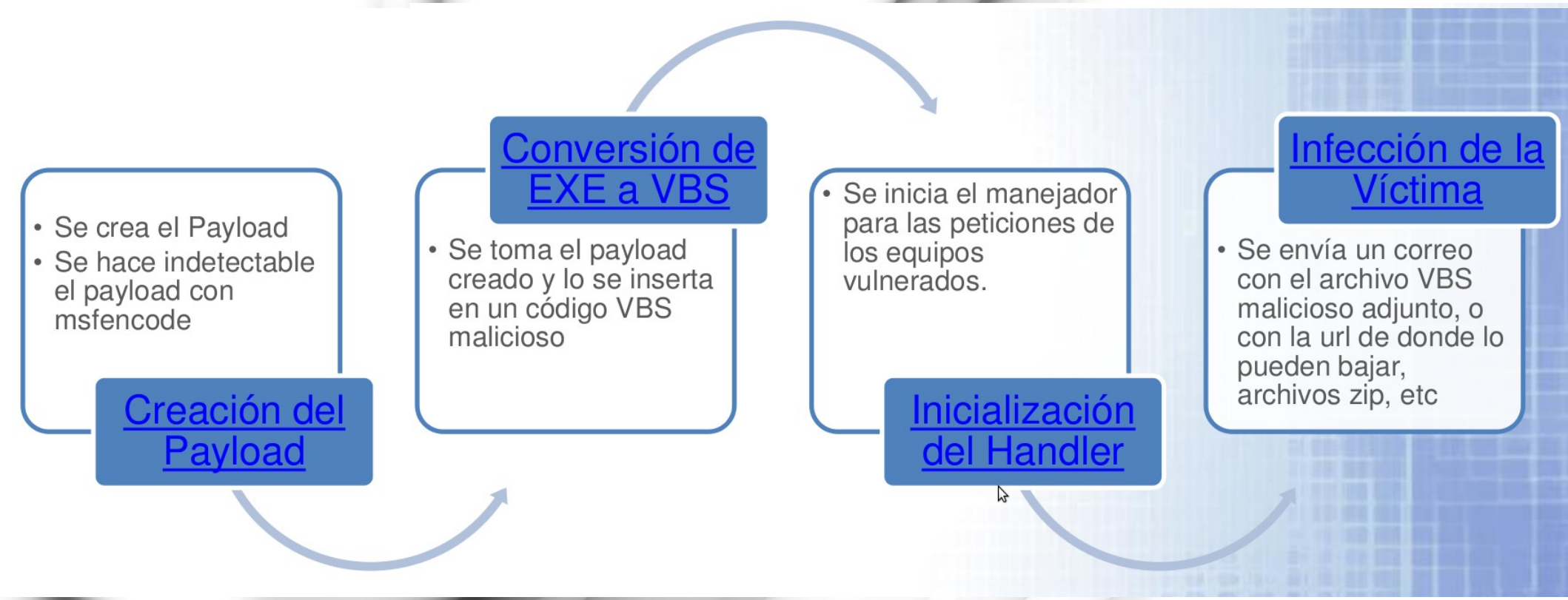
# Creación de Entorno






Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

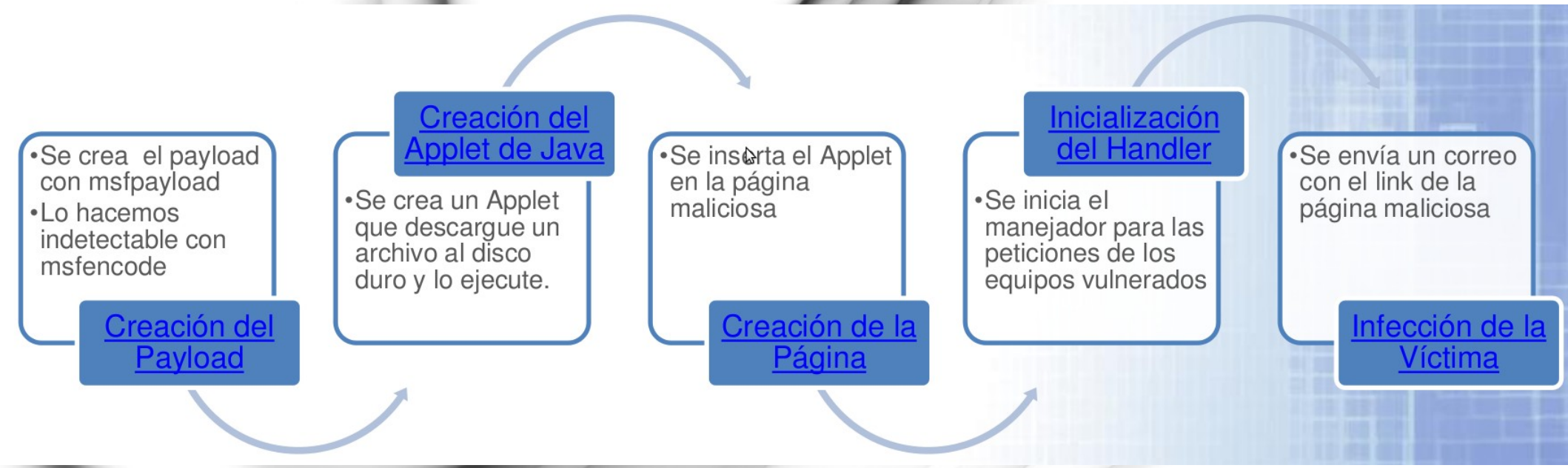
# Ataque de VBS






Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

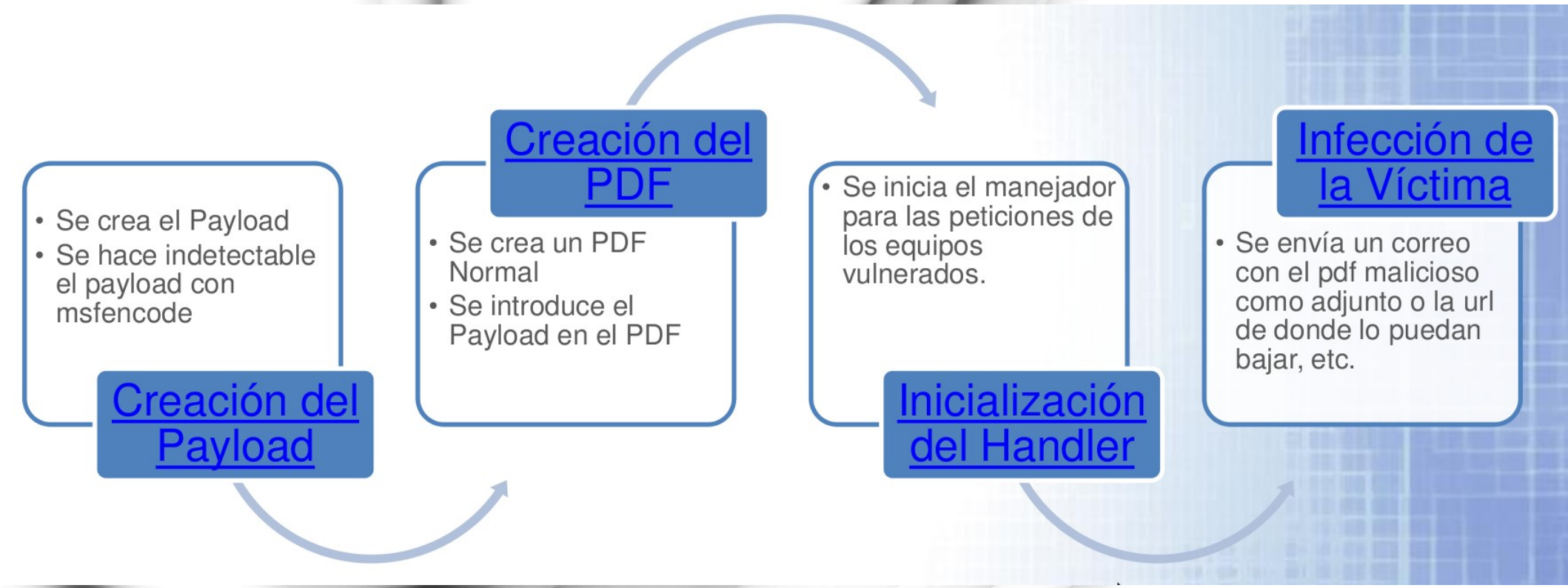
# Applet de Java






Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# PDF Malicioso






Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

HACK arandas

# Referencias

- **Todas las referencias pueden ser vistas en:**

**http://www.delicious.com/ch0ks/conferencia+HUM**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Agradecimientos


- **Profesor Arturo Garcia**
  - **Por la invitación a dar la conferencia**
- **ITESM CCM**
  - **Por las facilidades**
- **Psymera**
  - **Por toda su paciencia y conocimiento**




Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

# Gracias

```
if(you == understand.this){
    get.a.girlfriend;
}
```

**www.hackarandas.com**

**@ch0ks**



Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

HACK arandas