# Explotando Add-On's de Mozilla Firefox

Richard Villca Apaza

SixP4ck3r

**Hackmeeting 2013**

Santa Cruz - Bolivia

# Acerca de mi

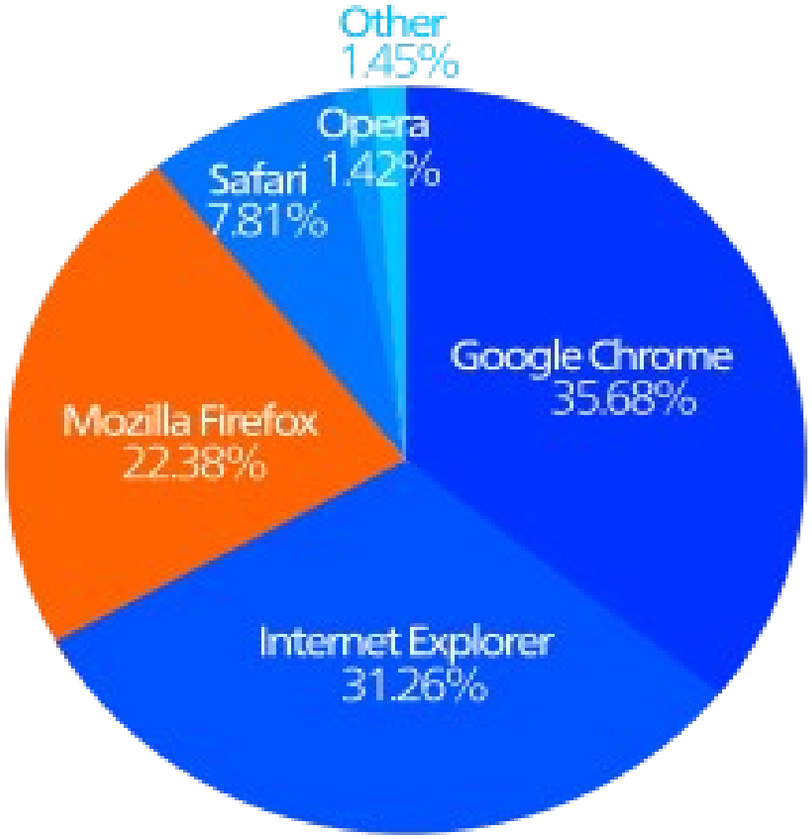
- Estudiante de 2do. año de sistemas.
- Amante de la tecnología y el Software Libre.
- Programador... me encanta programar en el viejo C, Java, PHP, node.js, .NET y Python.
- Uno poco mas de 5 años en el mundo del Hacking
- Escritor de pappers.
- Me encanta compartir conocimientos.
- Un autodidacta mas en la red!

# Lo que veremos...

- Intro
- Complementos, Ad-Ons, Plugins ...
- Seguridad en los Complementos de Mozilla Firefox
- Debilidades... y explotando...
- Demos (Keylogger, MiTM-GET-POST,remoteExec, Botnet)
- Add-OnFirefox + Beef = Botnet
- Entonces como puedo protegerme!
- Conclusión

# Introduccíon

- Mozilla Firefox es el tercer navegador mas usado!




# ¿Complementos ó Plugins?

Los plug-in's son pequeños programas auxiliares o dispositivos de hardware que permiten a sistemas mayores extender sus capacidades normales o aportar una función, generalmente muy específica.

Gracias a sus miles de add-ons hacen a Mozilla Firefox un navegador potente.

# Todos usamos plugins

- Plataformas Web, CMS's
  - Joomla, WordPress, Drupal, SMF y otros
  - Plugins, Complementos
  - Y otros...

- Aplicaciones de Escritorio
  - Plugins para Photoshop
  - Complementos para MS-Power Point
  - Y muchos mas.
  -

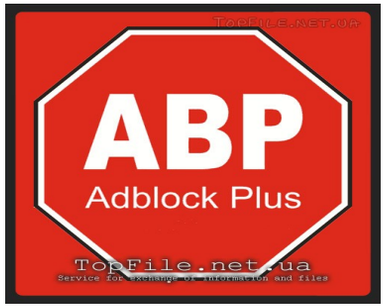
# Complementos en Firefox


# Complementos en Firefox

**MÁS POPULARES**

Todos »

1. Adblock Plus
   14.615.542 usuarios
2. Video DownloadHelper
   6.055.212 usuarios
3. Firebug
   2.812.061 usuarios
4. Easy YouTube Video Do
   1.948.270 usuarios
5. NoScript
   1.937.132 usuarios

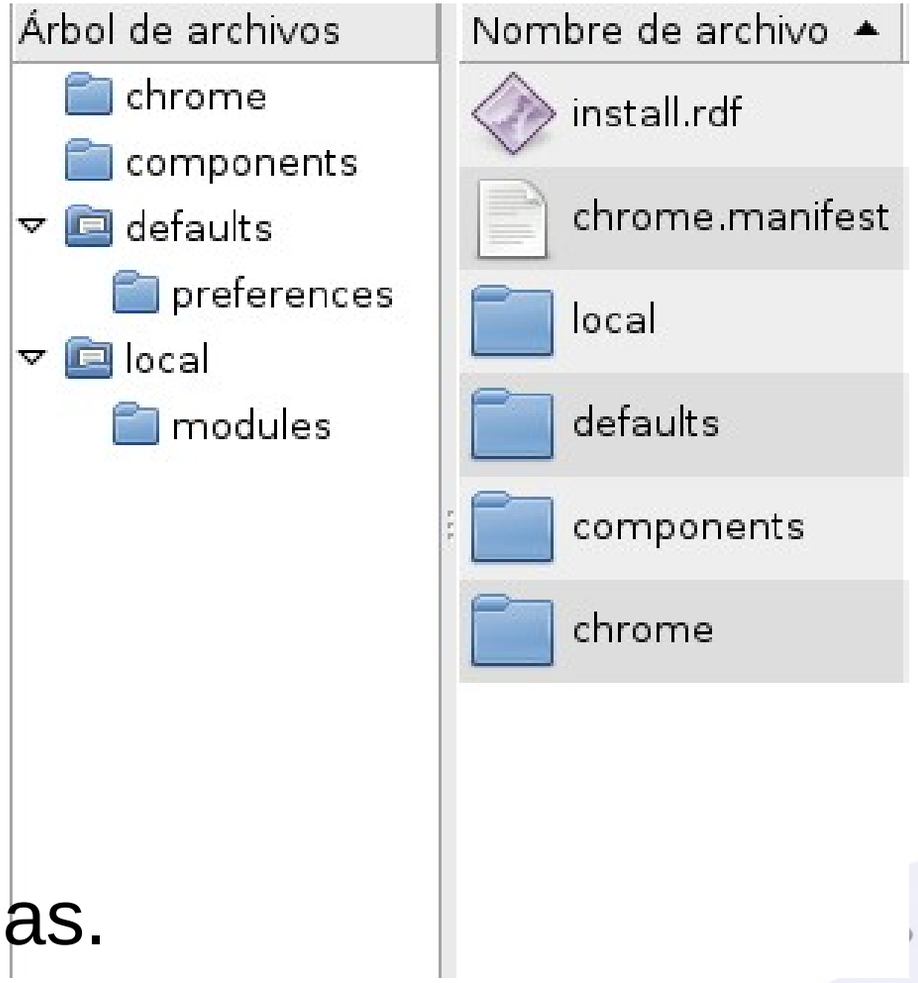





# Esctructura de un Add-On

Soporta:

- JavaScript
- HTML5
- Ajax
- XUL -> GUI
- XML
- Y una variedad mas.




# Esctructura de un Add-On

- **chrome.manifest**: Encargado de manejar la ubicacion de los ficheros del componente.
- **install.rdf**: Encargado de gestionar los nombres del desarollador, nombre del Add-On, Descripción, Version.
- **Overlay.js**: Los scripts que hacen posible el funcionamiento de un Add-On.
- **Overlay.xul**: GUI -> Encargado de manejar toda la interfaz grafica del Add-On.

# Seguridad en los Add-On's

- No hay mecanismos para restringir los privilegios de un Add-On.
- Los codigos de un Add-On no son verificados.
- Ninguna restricción para comunicarse desde un Add-On hacia Internet.
- XPConnect con privilegios, haces todo lo que quieres.
- Cuestion de creatividad e imaginación.

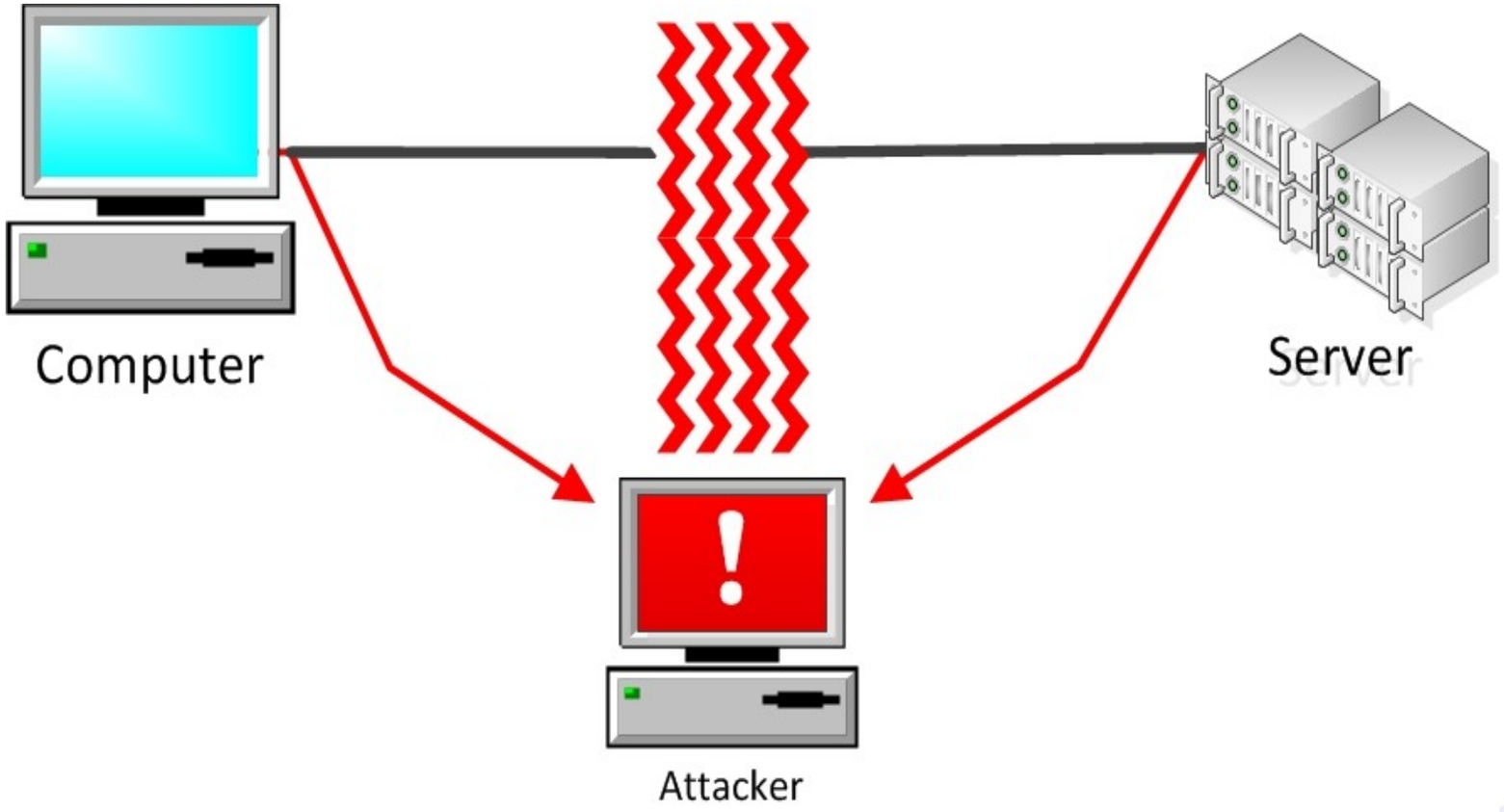
# Pensando como atacante!

- Leer ficheros del S.O.
- Keylogger Local, Remoto y robo de Cookies.
- MiTM control sobre el trafico POST y GET
- Reddireccion a otros sitos, control total sobre el contenido de una web.
- Distributed Denial of Service Attack (DDoS)
- Creando una BotNET con Beef
- En todos los S.O. Donde Mozilla Firefox este corriendo.

# DEMO: Keylogger Remoto

- PHP
- Ajax
- Una Base de Datos
- Y a divertirse!

# DEMO: MiTM Control POST GET




# DEMO: Ejecución de un *.EXE




# DEMO: Add-On + Beef = BotNET


**Authentication**

Username: SixP4ck3r

Password: ●●●●●●●●●●●●●●●

Login

# Y que dicen los AV's

virustotal

| | |
|---|---|
| SHA256: | 1a8043510ac60fedeb9f1996603eb0ce30f85fc71fd625112333 |
| Nombre: | remoteExec.xpi |
| Detecciones: | 0 / 45 |
| Fecha de análisis: | 2013-08-10 09:00:20 UTC ( hace 2 minutos ) |

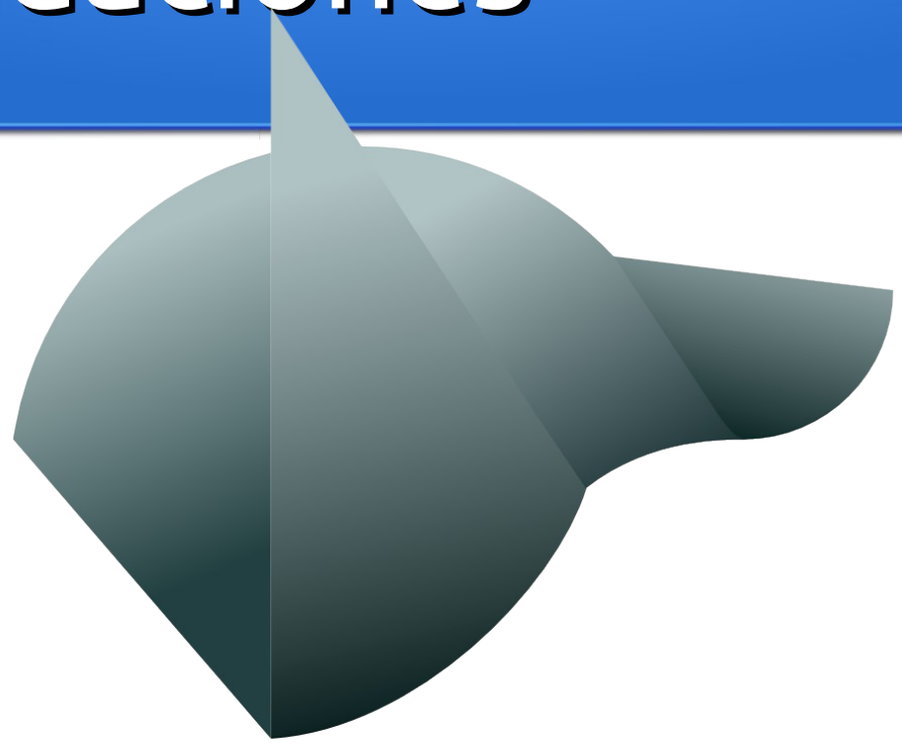
Más detalles

# Recomendaciones

- Jamas instales Add-Ons desde sitios dudosos.
- Cierra cualquier session que hayas iniciado, elimina tus cookies.
- Mirar en el panel de complementos de Firefox, que complementos tienes intalados, algun complemento desconocido dale en **ELIMINAR**.
- Mantener Firefox actualizado.
- Solo Instalar solo componentes que conoscais.

# Recomendaciones

- Usa Linux!
- Usa Lykan-OS



LYKANOS

# Conclusiones

- A pesar de que Mozilla Firefox es un navegador potente igual tiene sus debilidades.
- Si alquien te instalo un Add-On y tu no sabes ni como funciona ni donde estan ubicados para poder desinstalarlo, tienes todas las de perder.
- Como el codigo no es examinado puede venir camuflado en un Add-On valido, por ejemplo dentro del **Firebug**.
- Que los Add-Ons para Mozilla Firefox pueden convertirse potencialmente en Malware.

# Preguntas y Despedida

- En la Informatíca y el AMOR nada es imposible!

  “Han podido acceder a nuestros servidores y han obtenido todas los datos.“ Los Administradores de **DropBOX**

# Contacto

E-Mail -> SixP4ck3r AT Bolivia DOT com

Blog -> http://sixp4ck3r.blogspot.com/

Twitter -> @SixP4ck3r