

Explotando Add-On's de Mozilla Firefox

Richard Villca Apaza

SixP4ck3r

Hackmeeting 2013
Santa Cruz - Bolivia



Acercas 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!



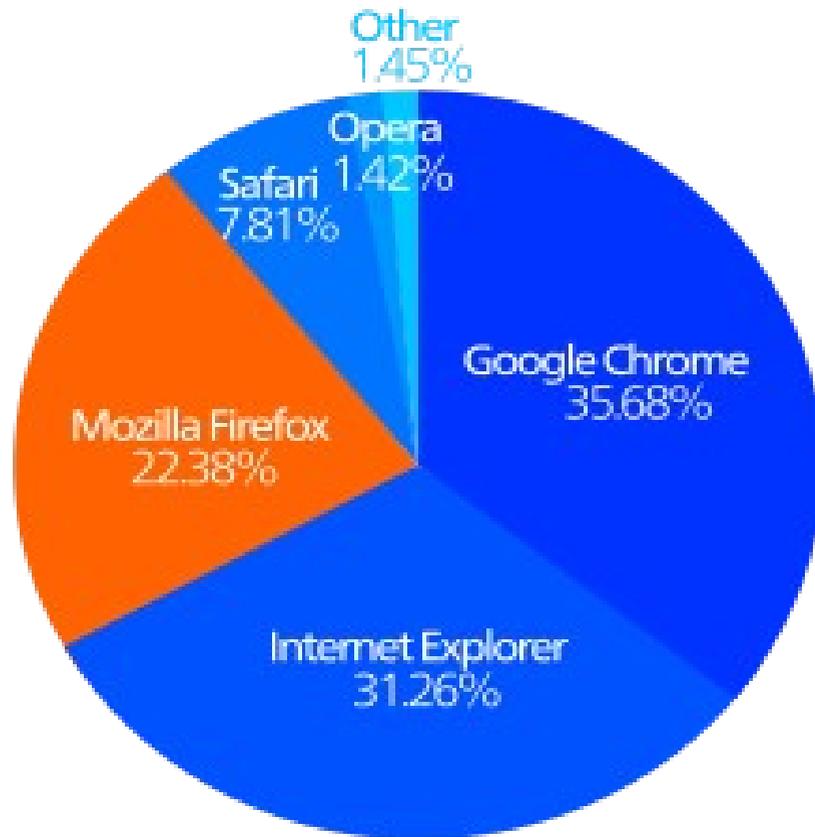
Lo que veremos...

- 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



Introducción

- 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



The screenshot shows the Firefox Add-ons page for the Firebug extension. At the top left is the Firefox logo and the word "COMPLEMENTOS" in large blue letters. Below it are links for "EXTENSIONES", "TEMAS", "COLECCIONES", and "MÁS...". A search bar on the right contains the text "buscar com". Below the navigation is a breadcrumb trail: "Inicio » Extensiones » Firebug". The main content area features the Firebug extension card, which includes a small bug icon, the title "Firebug 1.11.4" with a "SIN REINICIAR" badge, and the authors "por Joe Hewitt, Jan Odvarko, robcee, FirebugWorkingGroup". A description follows: "Firebug integrates with Firefox to put a wealth of development tools at your fingertips while you browse. You can edit, debug, and monitor CSS, HTML, and JavaScript live in any web page...". A prominent green button with a plus sign says "Agregar a Firefox". At the bottom of the card, there is a section titled "¿Te gusta este complemento?" with a developer profile icon, a text box asking for support, and a blue "Colabora" button with a heart icon. Below the button, it says "US\$ 10,00 sugerido".

 **COMPLEMENTOS**
EXTENSIONES | TEMAS | COLECCIONES | MÁS...

🔍 buscar com

🏠 » Extensiones » Firebug

 **Firebug 1.11.4** SIN REINICIAR
por Joe Hewitt, Jan Odvarko, robcee, FirebugWorkingGroup

Firebug integrates with Firefox to put a wealth of development tools at your fingertips while you browse. You can edit, debug, and monitor CSS, HTML, and JavaScript live in any web page...

[+ Agregar a Firefox](#)

 *¿Te gusta este complemento?*
El desarrollador de este complemento pide que muestres tu apoyo realizando un donativo a Mozilla Foundation.

[❤ Colabora](#)
US\$ 10,00 sugerido

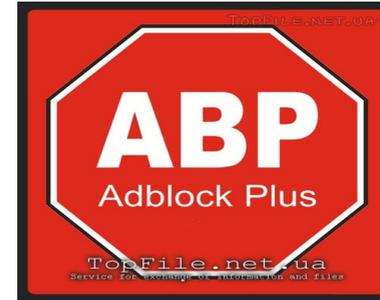


Complementos en Firefox

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.

Árbol de archivos	Nombre de archivo ▲
chrome	install.rdf
components	chrome.manifest
▼ defaults	local
preferences	defaults
▼ local	components
modules	chrome



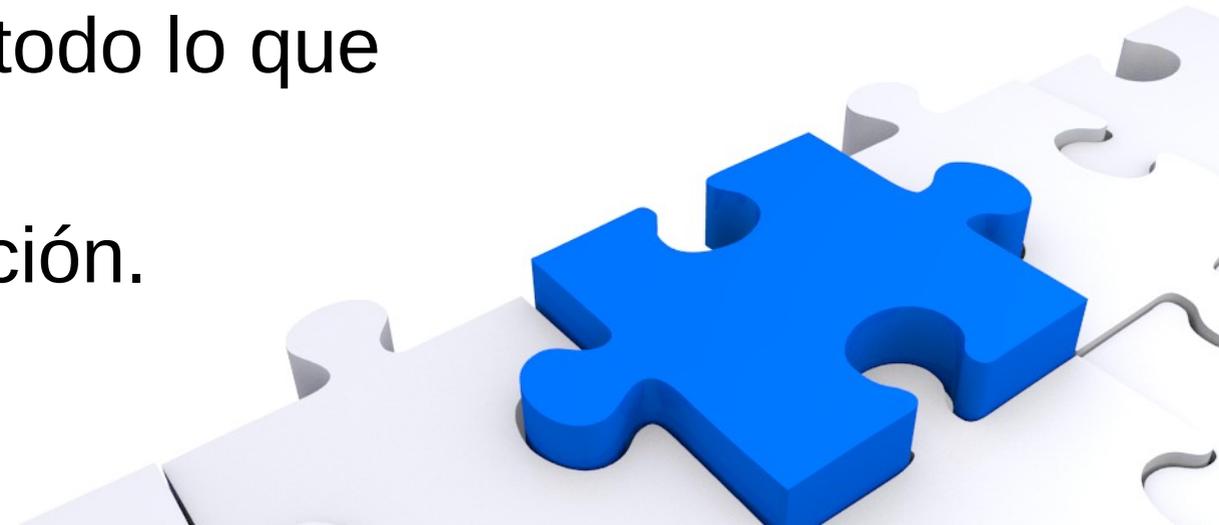
Esctructura de un Add-On

- **chrome.manifest:** Encargado de manejar la ubicacion de los ficheros del componente.
- **install.rdf:** Encargado de gestionar los nombres del desarrollador, 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 sitios, 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.

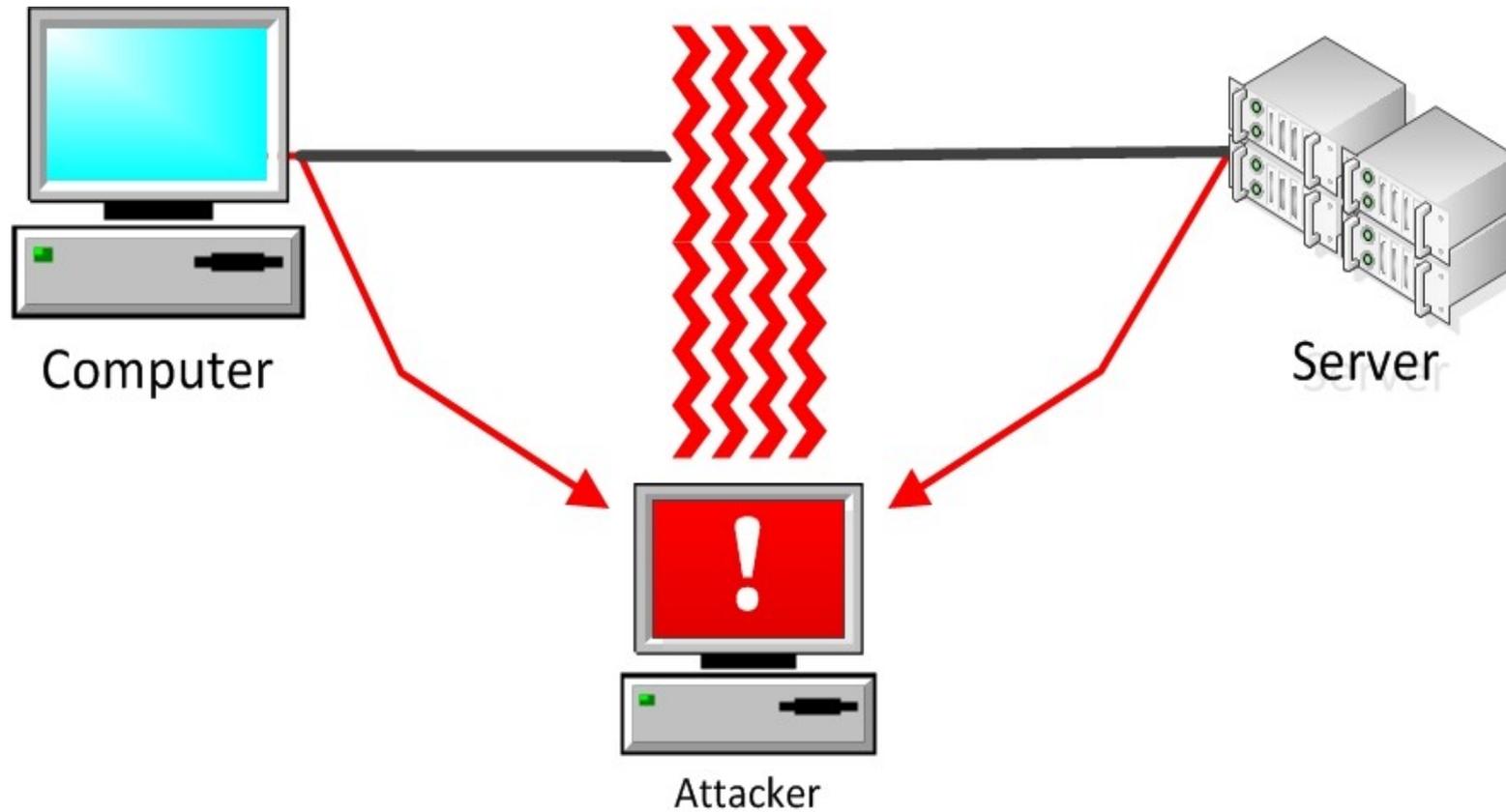


DEMO: Keylogger Remoto

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



DEMO: MiTM Control POST GET



DEMO: Ejecución de un *.EXE

```
.M""bgd `7MM""YMM MMP""MM""YMM
,MI  "Y  MM  `7 P'  MM  `7
`MMb.   MM  d    MM
`YMMNq. MMmmMM   MM
`MM     MM  Y    MM
Mb     dM  MM    ,M  MM
P"Ybmd" .JMMmmmmMM .JMML.
```

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Development Team: JR DePre (pr1me) [---]
[---] Development Team: Joey Furr (j0fer) [---]
[---] Development Team: Thomas Werth [---]
[---] Version: 2.5.1 [---]
[---] Codename: 'Rippin and Tearin' [---]
[---] Report bugs: davek@social-engineer.org [---]
[---] Follow me on Twitter: dave_relik [---]
[---] Homepage: http://www.secmaniac.com [---]
```

Welcome to the Social-Engineer Toolkit (SET). Your one stop shop for all of your social-engineering needs..



DEMO: Add-On + Beef = BotNET



Authentication

Username:

Password:



Y que dicen los AV's



SHA256: 1a8043510ac60fedeb9f1996603eb0ce30f85fc71fd62511233:

Nombre: remoteExec.xpi

Detecciones: 0 / 45

Fecha de análisis: 2013-08-10 09:00:20 UTC (hace 2 minutos)


Más detalles



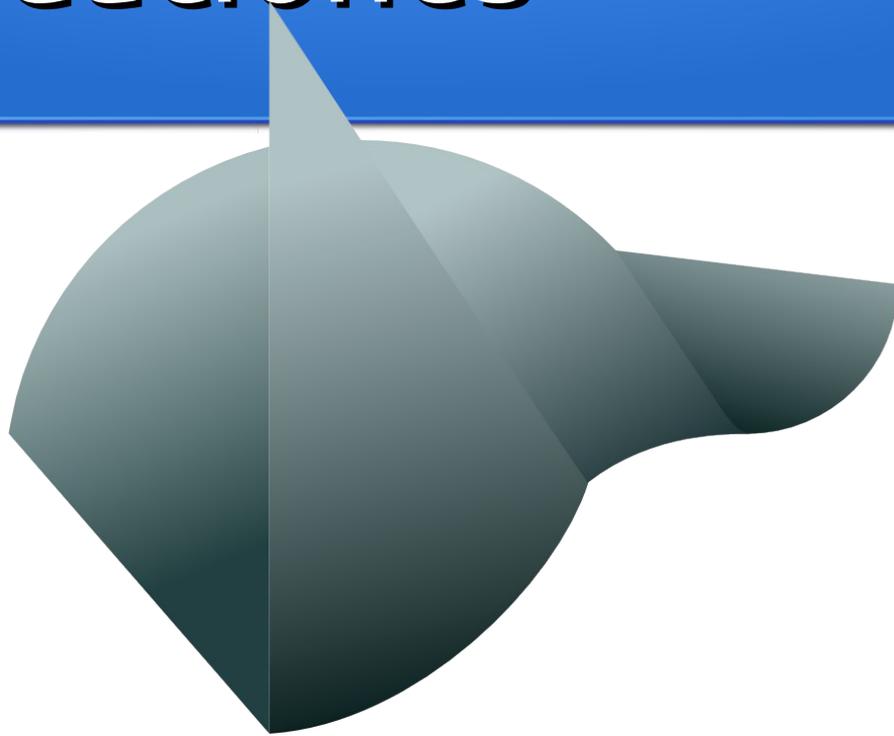
Recomendaciones

- 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 conocais.



Recomendaciones

- Usa Linux!
- Usa Lykan-OS



LYKANOS



Conclusiones

- A pesar de que Mozilla Firefox es un navegador potente igual tiene sus debilidades.
- Si alguien 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 Informática 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

