



Confidence in a connected world.



2009
GENEVA 



Firefox and Malware *„when your browser bites you“*

Candid Wüest – Symantec Switzerland
Elia Florio – DPA Italy



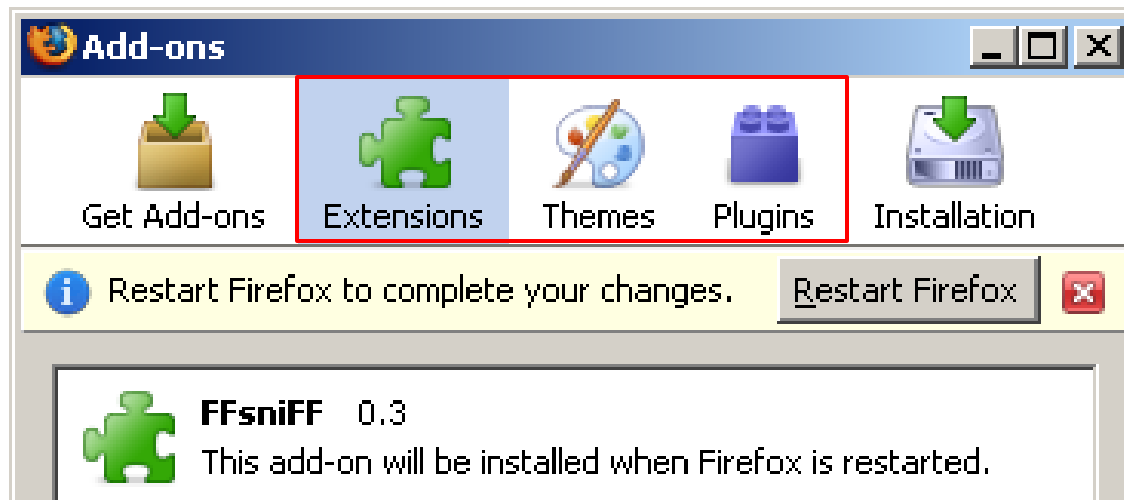


- 1 What are Firefox Extensions
- 2 Malicious Firefox Extension Examples
- 3 Time for Questions & Answers



What are extensions?

- Software add-ons for the Mozilla Firefox Browser
- Similar to ActiveX
- Coded in JavaScript or C++ etc
- Cross platform (if correctly implemented ;-)



The Mozilla Platform

Toolkit

Extension Manager, Update, Moz Storage, Spell Checking, Brakepad Crash Reporting, ...

Content

Layout

XUL

XML User Interface Language

XBL

XML Binding Language

SVG

Scalable Vector Graphics

DOM

Document Object Model

CSS

Cascading Style Sheets

HTML and XML Parser

NSS / PSM

Network Security Services, Personal Security Manager

XPCOM

Cross Platform Component Object Model

XPConnect

Bridges JavaScript and XPCOM

JavaScript

NSPR

Netscape Portable Runtime: Cross Platform API for System Level Functions

Neko
Network Library

Widget
Event Handling and Windowing

GFX / Thebes
Graphics

Cairo
Graphics

SQLite
Storage

Installation File

- Distributed as XPI
 - cross platform installer
- Most XPI are unsigned

.XPI file (ZIP archive)

Install.rdf

Chrome.manifest

Chrome*

...

Installer files

Data files (*.JS)



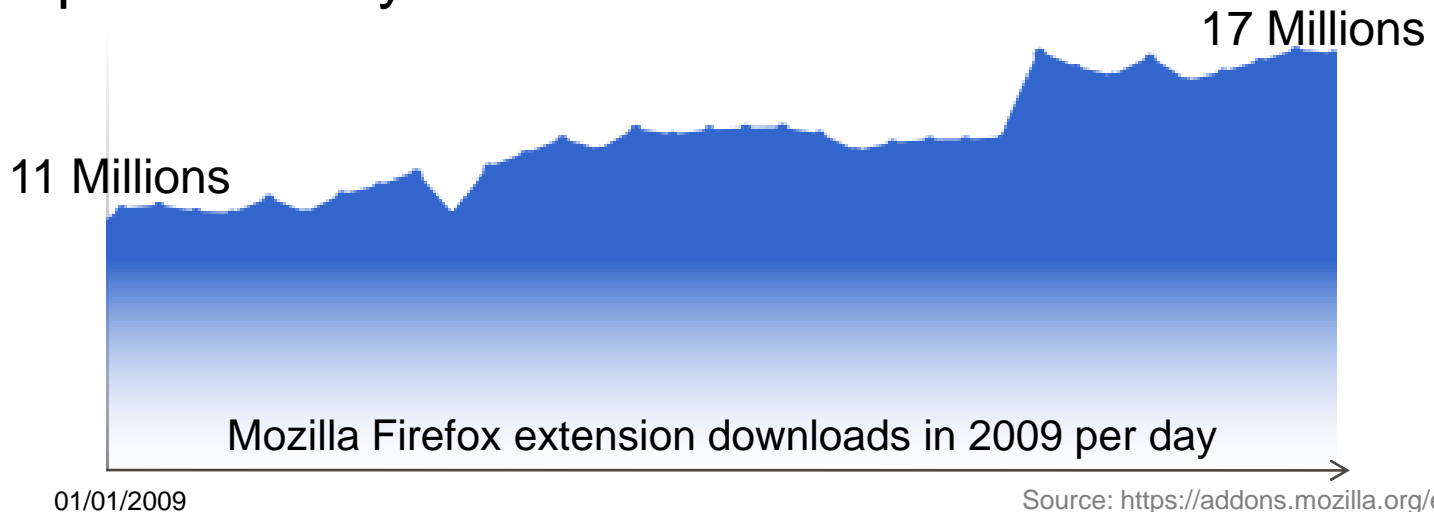
Are there many Extensions?

Firefox 3.x - 22% market share

Firefox Extensions:

- 17 Million downloads / day
- 150 new / day
- 450 updated / day

(1.5 Billions total)



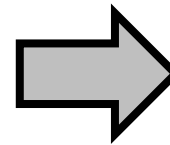
Source: <https://addons.mozilla.org/en-US/statistics>

Everything that Firefox could do

mm
everything...



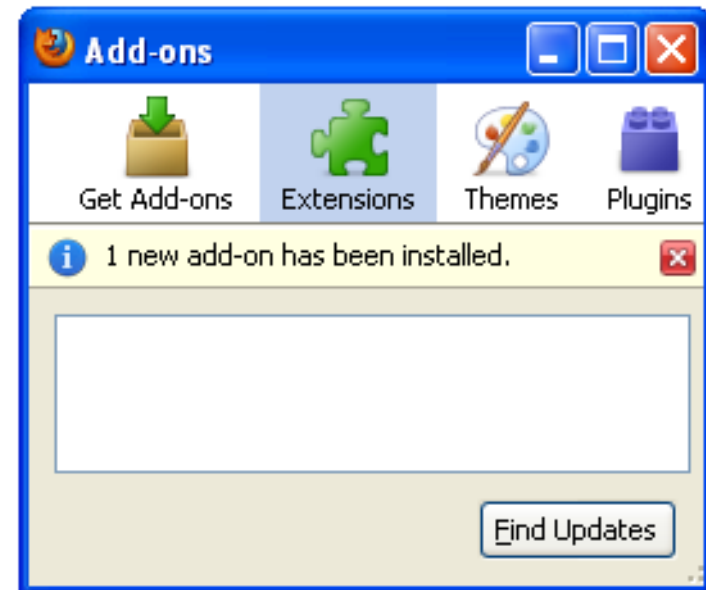
- Read/write file access
- Network sockets
- Control browser UI
- Control submitted information
- Control registry (on Windows)



Powerful Malware

How do they get on the system

- **Malicious updates from trusted source**
 - As seen with NoScript or Vietnamese language pack
- **Dropped through vulnerabilities**
 - Talk by Roberto Suggi Liverani / Nick Freeman (Defcon 17)
 - JavaScript with Chrome privileges → Game Over
- **Dropped by local malware**
 - Easy to build and hard to trace
- **Social Engineering**
 - „you really need this cool extension!“



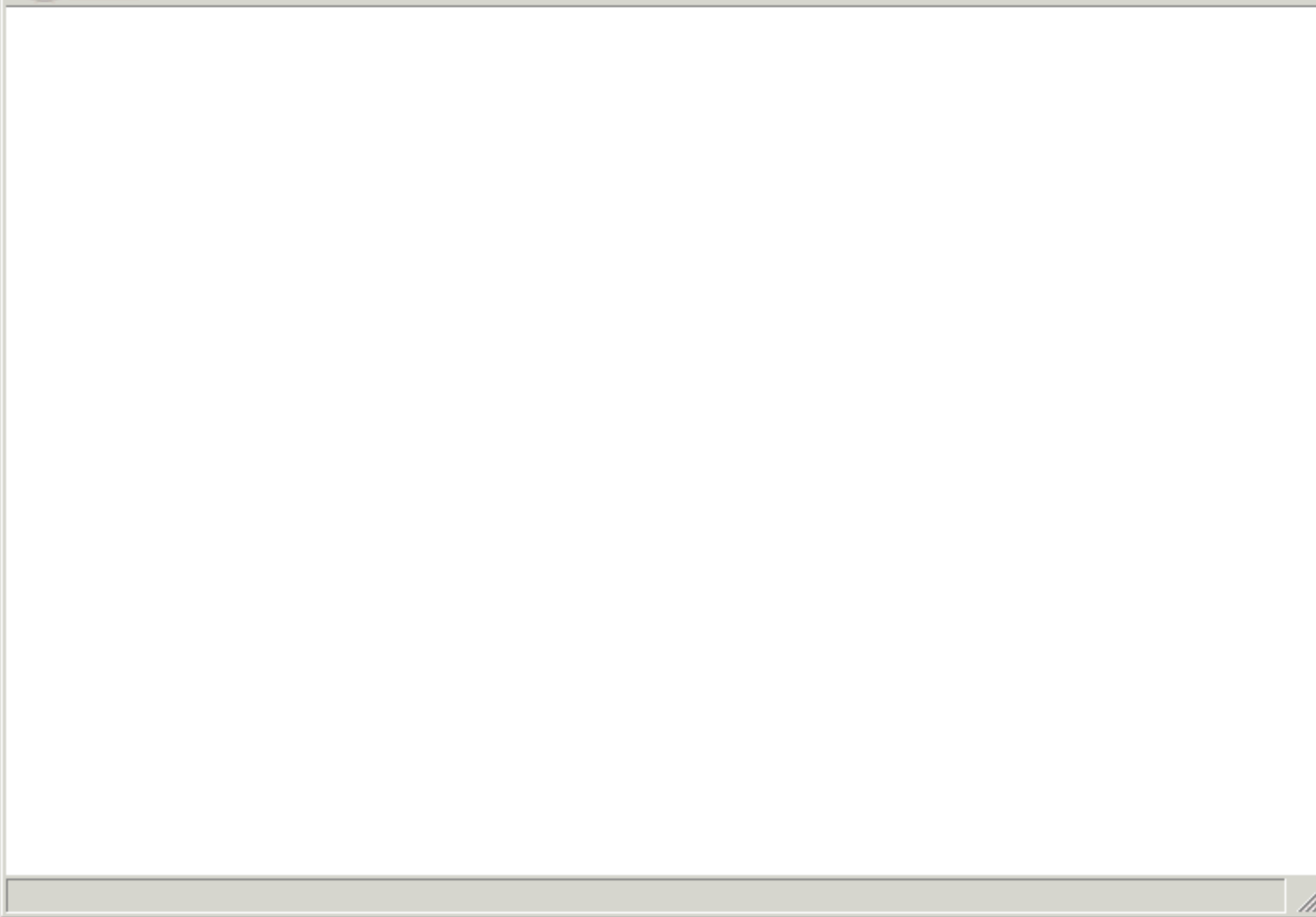
Many ways to hide an extension on the system:

- „Hidden“ tag in *install.rdf*
- Set add-on type to zero in *install.rdf*
- Remove itself from the extension listing at runtime
- Modify *extension.rdf* file after installation
- Hijack other extensions (even signed ones!)
- Hijack Firefox core files



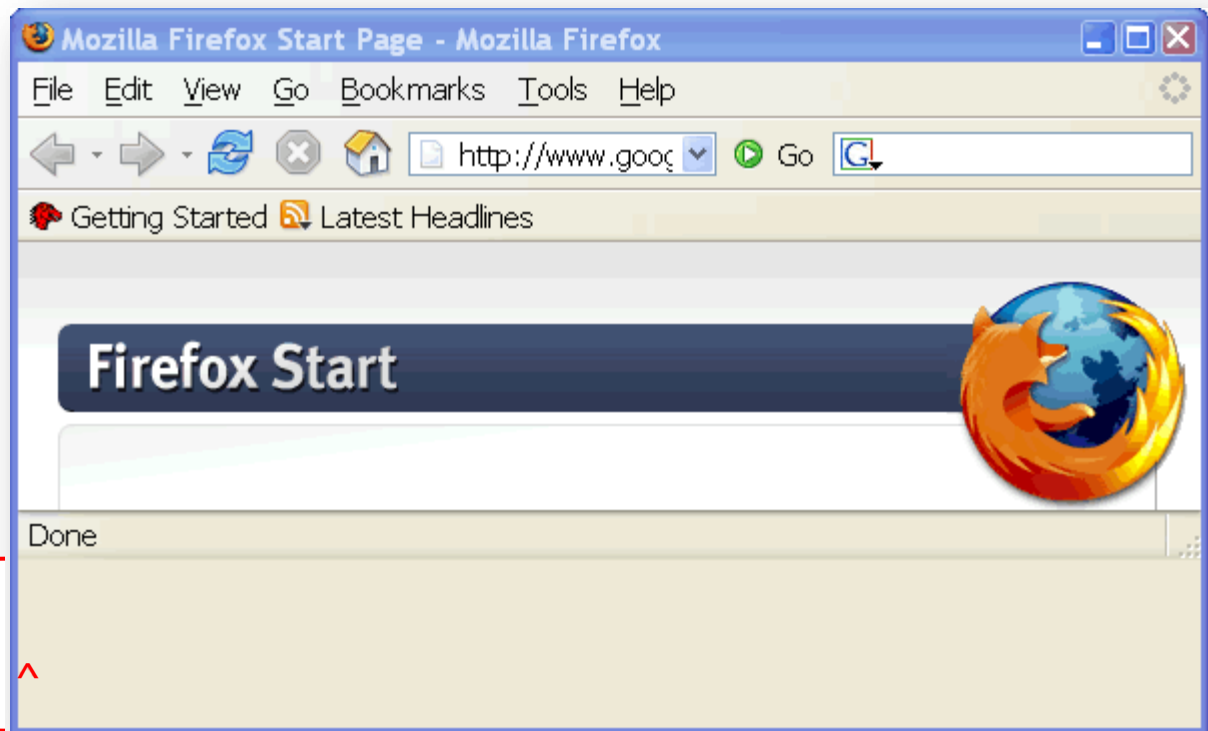
DEMO – Startup Method





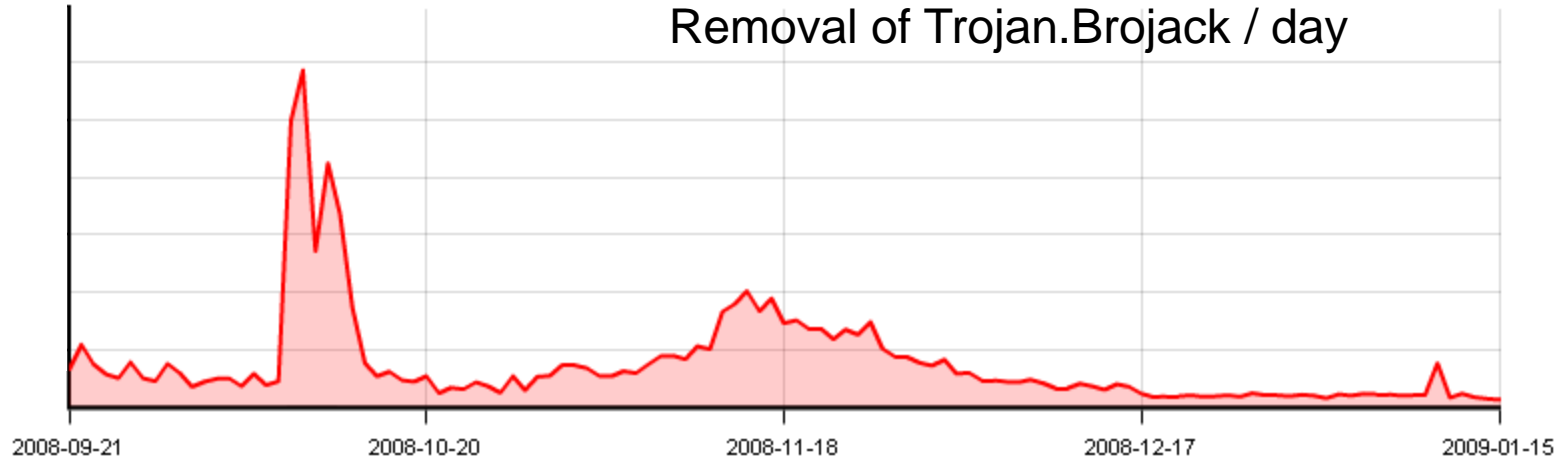
The Grey Bar Experience

- C:\Program Files\Mozilla Firefox\chrome\m3ffxtbr.manifest
- Dropped by MyWebSearch Toolbar
- Automatically removed by Firefox 1.5.0.2 and later

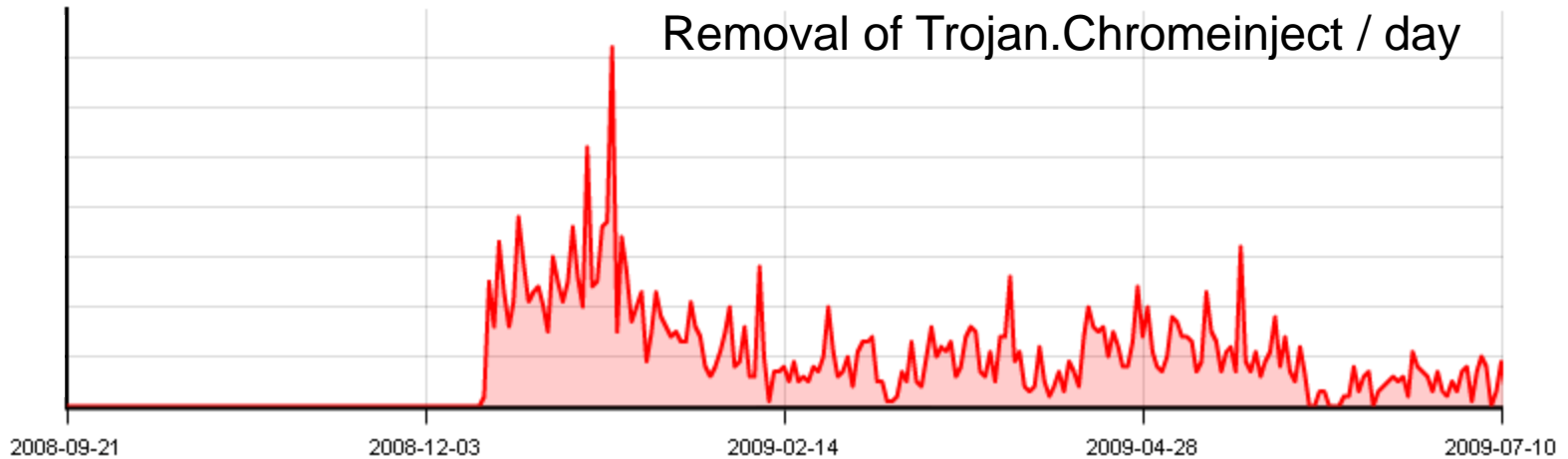


Generated
by an error

Removal of Trojan.Brojack / day



Removal of Trojan.Chromeinject / day



Examples

xx\chrome\chrome\content



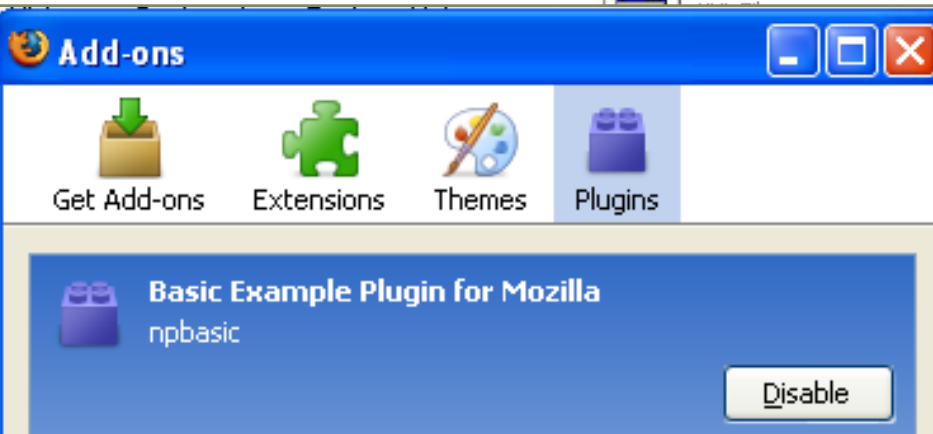
browser.js - Notepad

File Edit Format View Help

```
function init()
{
  window.addEventListener("load", chromeLoad, false);
}
function chromeLoad()
{
  var appContent = document.getElementById("appcontent");
  appContent.addEventListener("DOMContentLoaded", contentLoad)
}

function check(loc, dom)
{
  var domains=['127.0.0.3', '127.0.0.2'];
  var urls=['das', 'http://127.0.0.2/'];
  var urlsr=['yandeeex.ru', 'sss.re'];

  var zurl=['*akbank.com*',
  '*caixasabadell.net*',
  '*credem.it*',
  '*areasegura.banif.es*',
  '*banca.cajaen.es*',
```



- Loads malicious dl
- Steals credentials
- Hides from Extens

```
[SMTP] <0>.
[SMTP] https://my.secure.bank/login.php <0>.
[SMTP] type:name:value <0>.
[SMTP] ----- <0>.
[SMTP] text:Account_ID:candid_101 <0>.
[SMTP] password:TAN:1977 <0>.
[SMTP] password:PASS:31337 <0>.
[SMTP] submit:submit:login <0>.
[SMTP] ----- <0>.
[SMTP] <0>.
[SMTP] . <0>.
[SMTP] QUIT <0>.
```

ct

DEMO – Infostealer.Ebod





Google





Firefox extensions are very powerful (like ActiveX)



Firefox extensions have been misused for years



Most users don't check what they install



Adware is predestinated to use Firefox extensions



Most security tools can not detect or remove them





Confidence in a connected world.

Questions ?

Elia Florio – Italian Data Protection Authority
Candid Wüest – Symantec Switzerland

We hope you had a good time in Geneva





Confidence in a connected world.

Thank You!

Elia Florio – Italian Data Protection Authority
Candid Wüest – Symantec Switzerland

We hope you had a good time in Geneva

