2009 GENEVA vb

Firefox and Malware
„when your browser bites you“

Candid Wüest – Symantec Switzerland

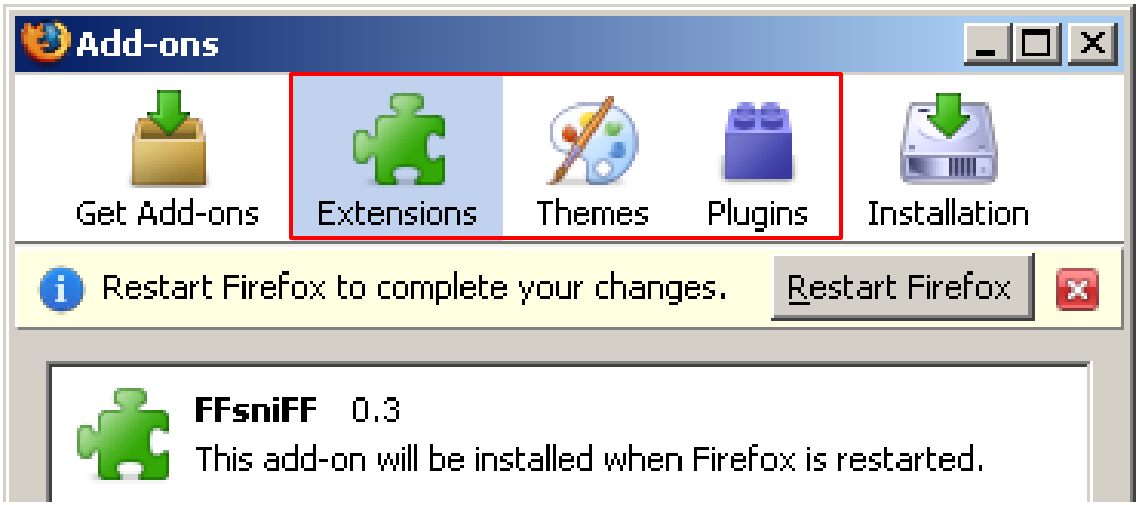
Elia Florio – DPA Italy

Agenda

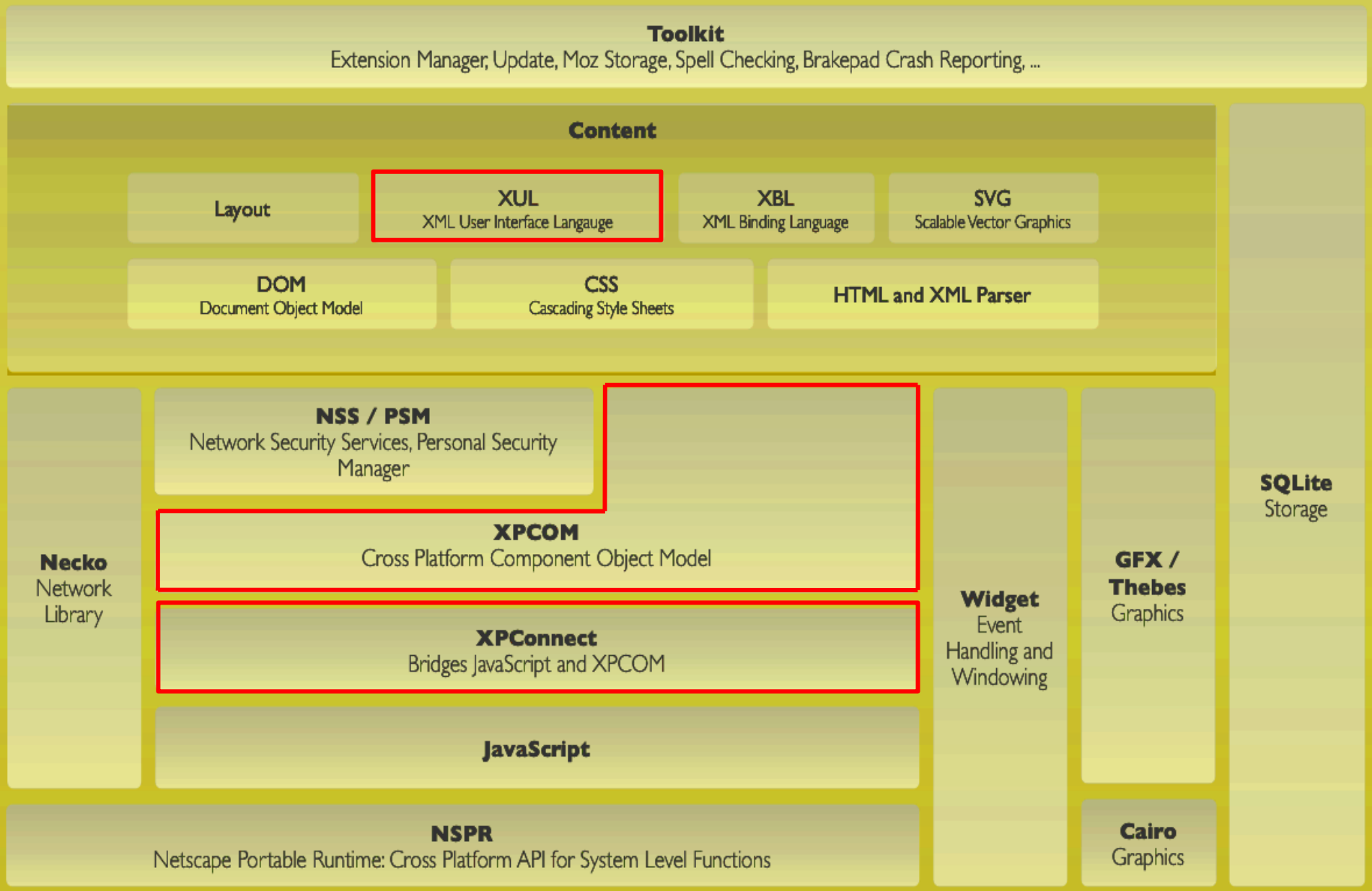
1. What are Firefox Extensions
2. Malicious Firefox Extension Examples
3. Time for Questions & Answers

What are extensions?

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

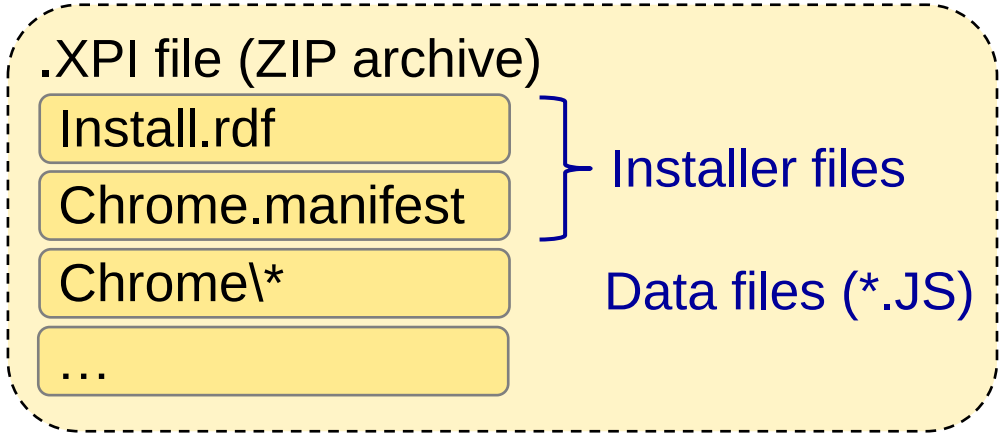


The Mozilla Platform



Installation File

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

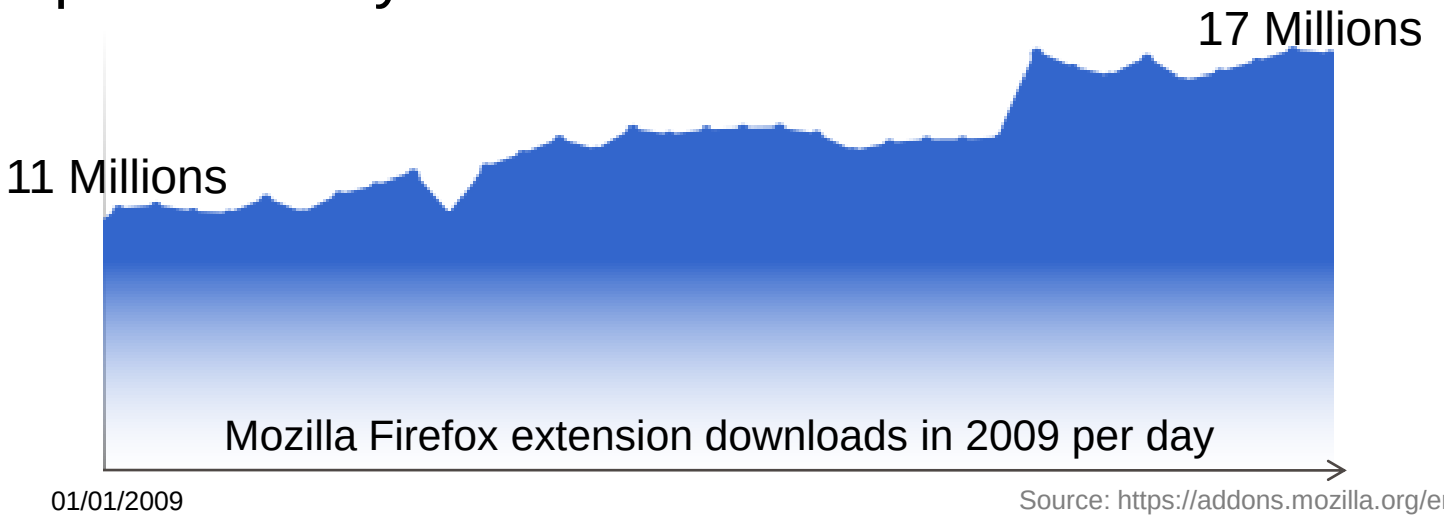


Are there many Extensions?

Firefox 3.x - 22% market share

Firefox Extensions:

- 17 Million downloads / day (1.5 Billons total)
- 150 new / day
- 450 updated / day



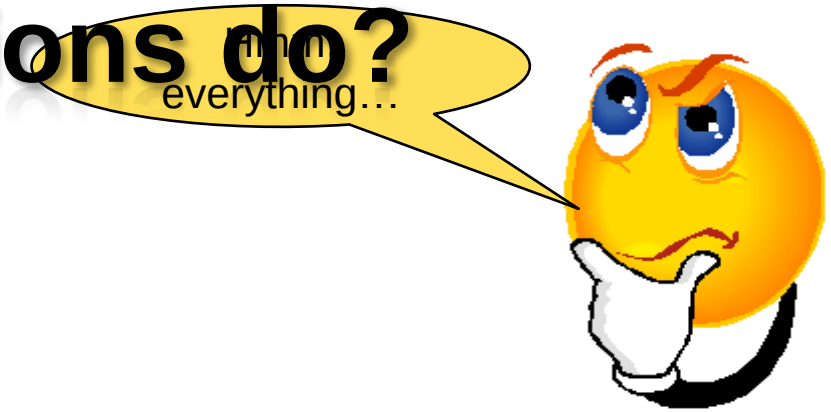
Source: https://addons.mozilla.org/en-US/statistics

What can extensions do?

Everything

What can extensions do?

that Firefox could do

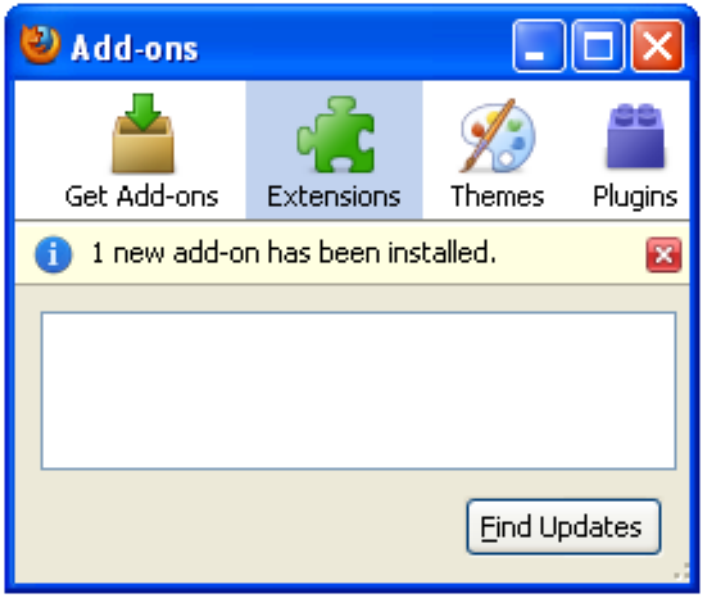


- Read/write file access
- Network sockets
- Control browser UI
- Control submitted information
- Control registry (on Windows)

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!“

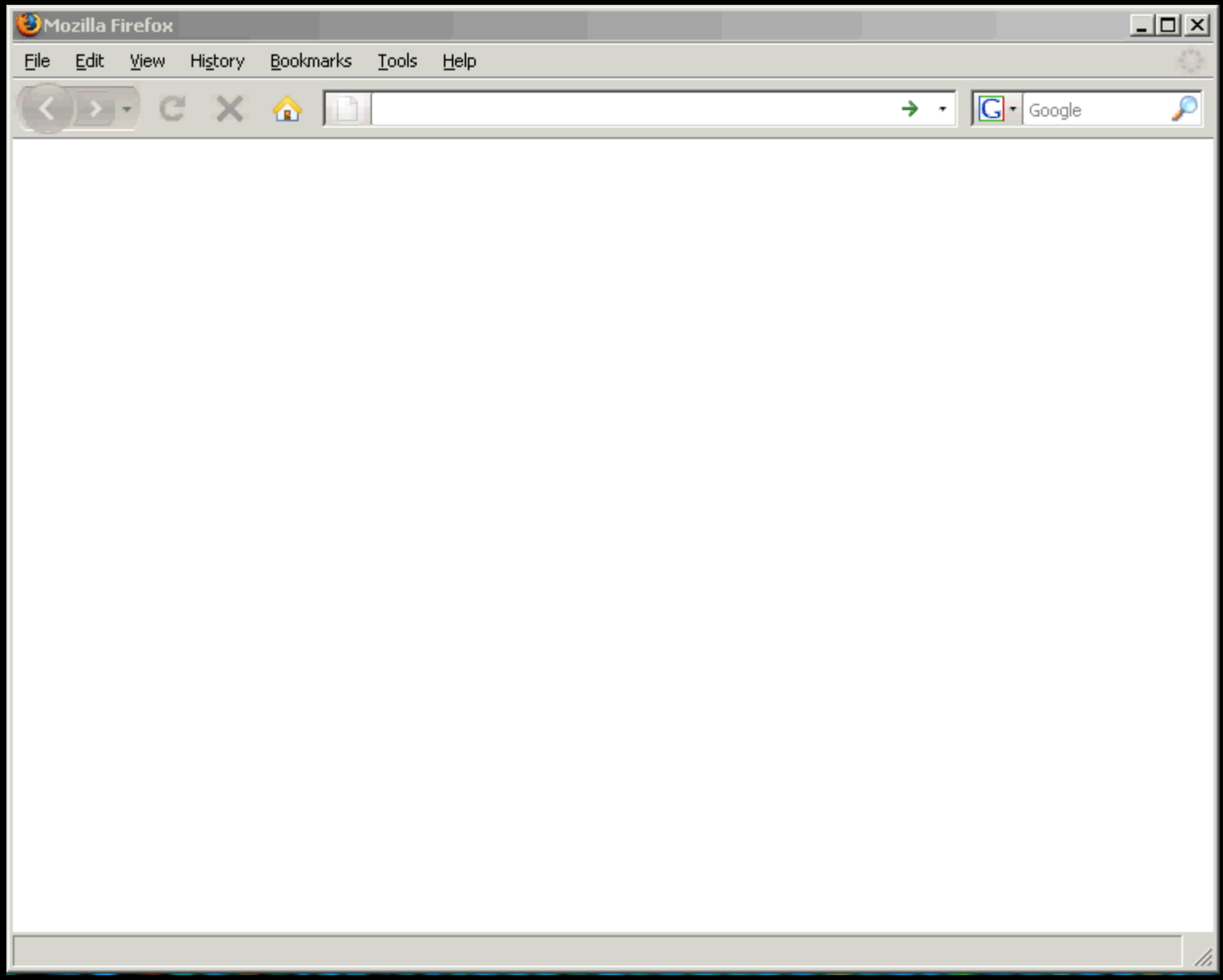


Hiding Extensions

Many ways to hide an extension on the system:

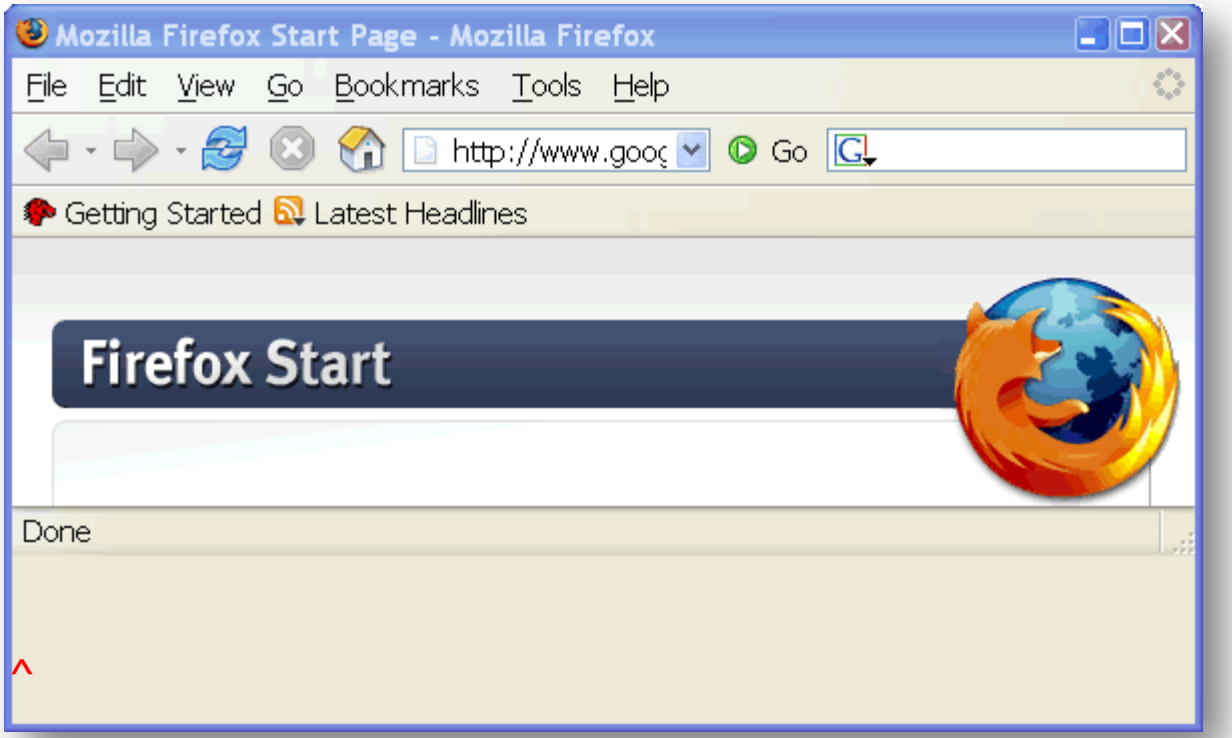
- „Hidden“ tag in *install.rdf*
- Set add-on type to zero in *install.rdf*
- Remove itself from the extension listing at runtime
- Modify *extension.rdf* file after installation
- Hijack other extensions (even signed ones!)
- Hijack Firefox core files

DEMO – Startup Method


Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Google

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

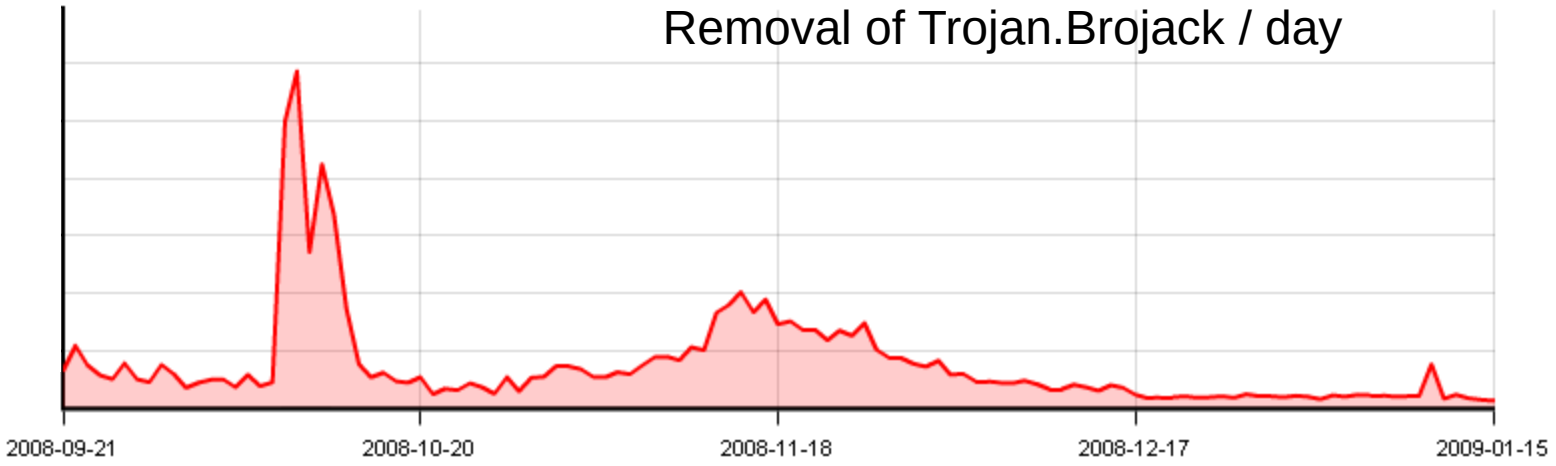


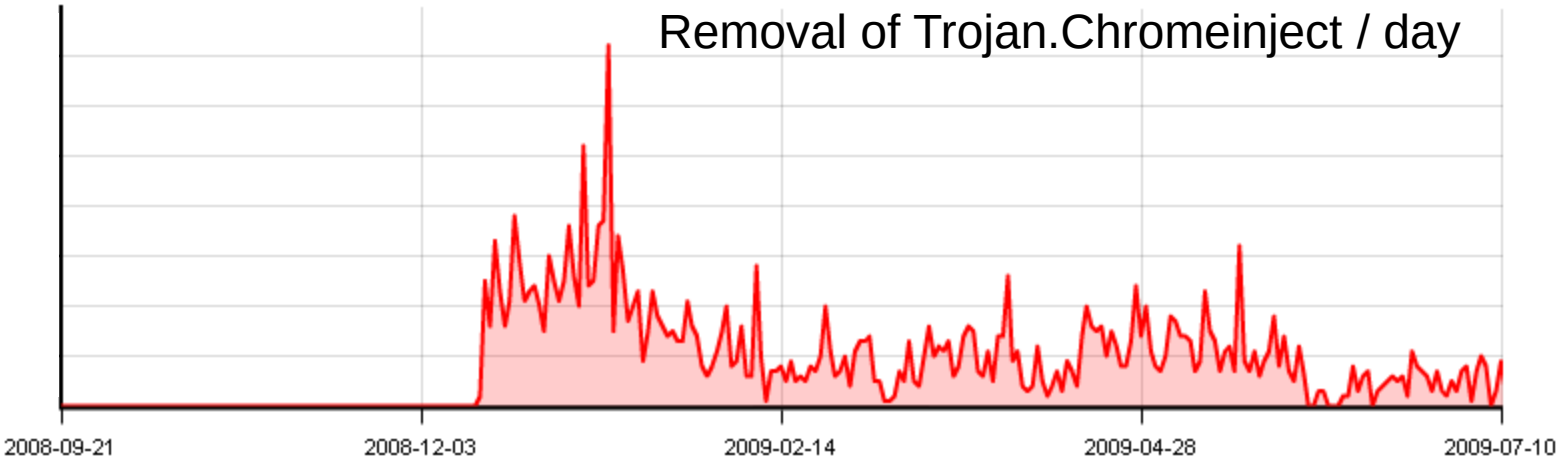
Generated by an error

^

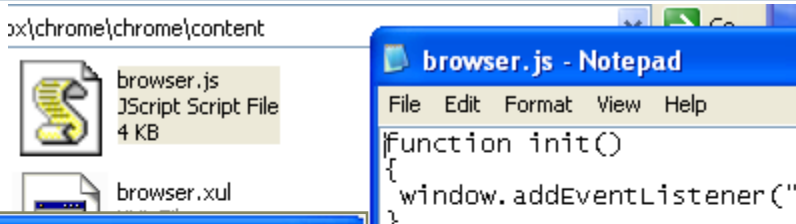
Source: http://kb.mozillazine.org/Gray_bar_below_status_bar

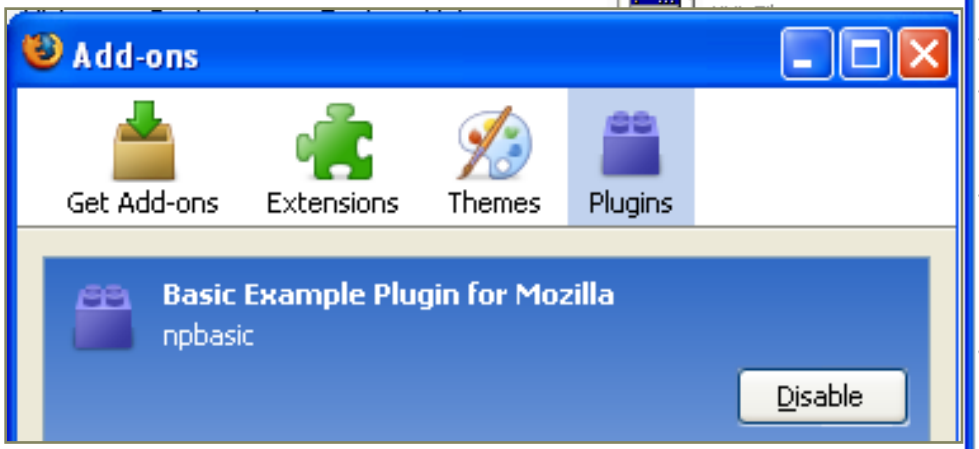
Prevalence


Removal of Trojan.Brojack / day
2008-09-21
2008-10-20
2008-11-18
2008-12-17
2009-01-15


Removal of Trojan.Chromeinject / day
2008-09-21
2008-12-03
2009-02-14
2009-04-28
2009-07-10

Examples



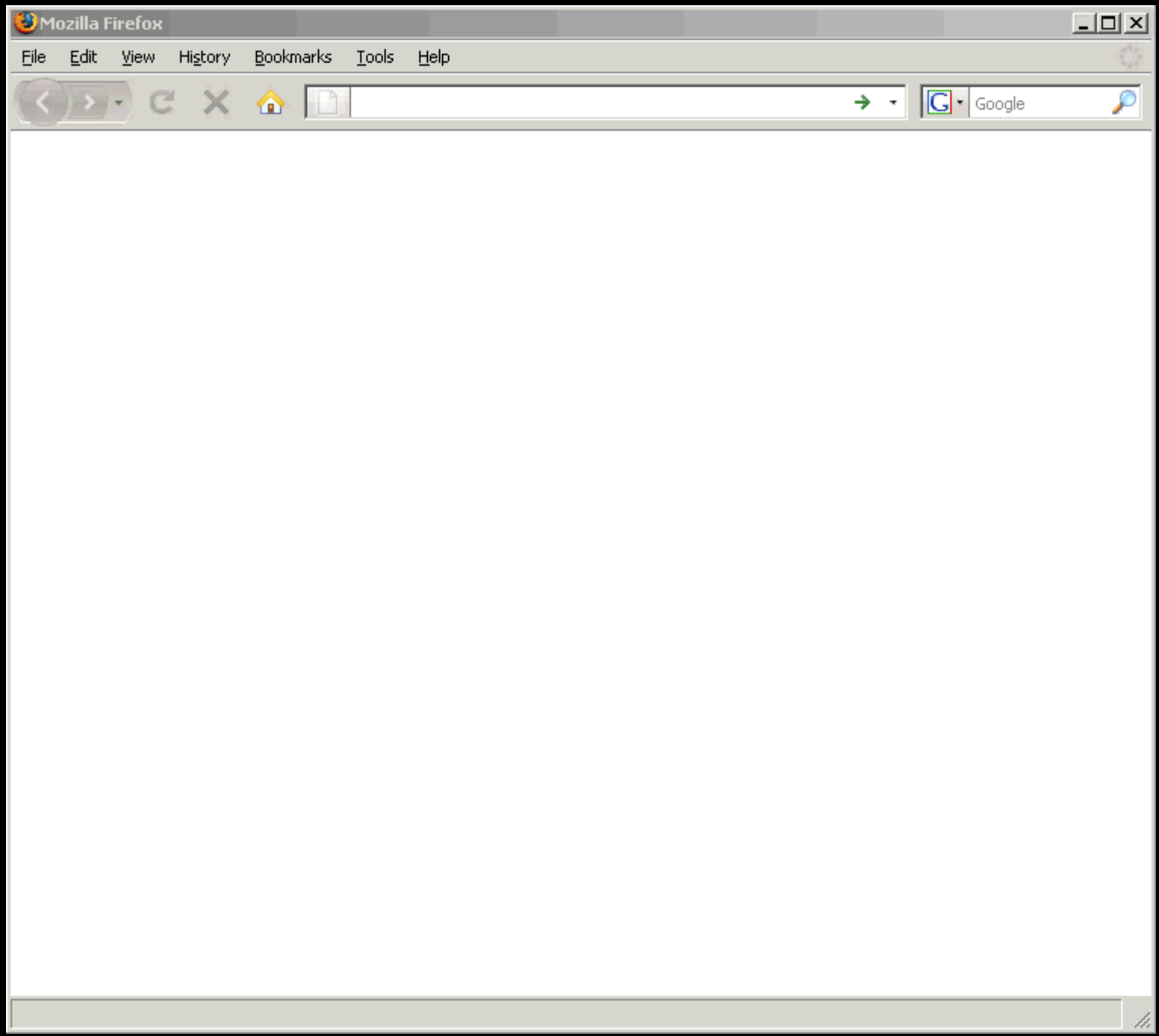


- Loads malicious dl
- Steals credentials f
- Hides from Extensi

```
[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


Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
Google

Conclusion

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

Questions ?

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

We hope you had a good time in Geneva

Thank You!

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

We hope you had a good time in Geneva