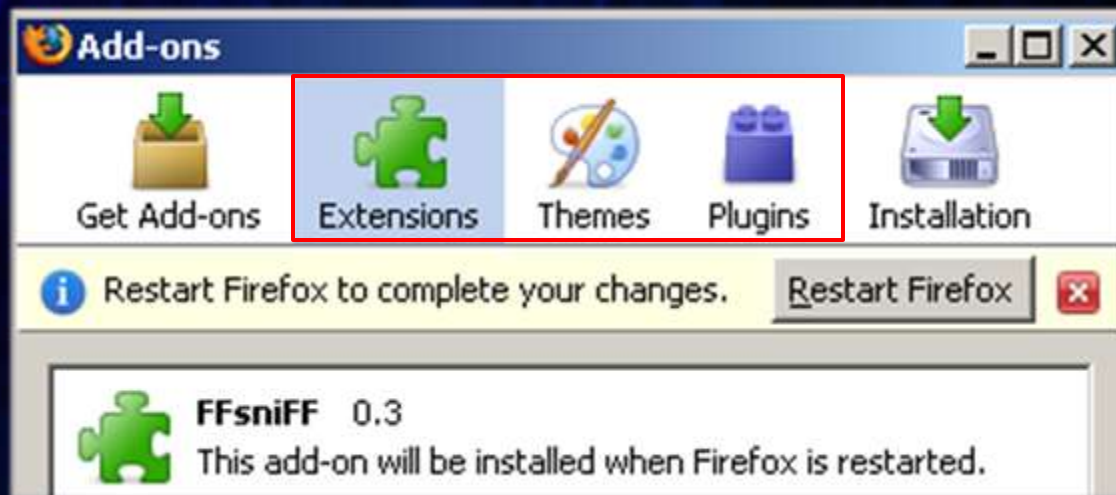


Fun with Firefox Extension Malware

candid wüest
Sr. threat researcher

What are we talking about?

- Software add-ons for the Mozilla Firefox Browser
- Similar to ActiveX (history repeating?! Focus here on FF)
- 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

Necko
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

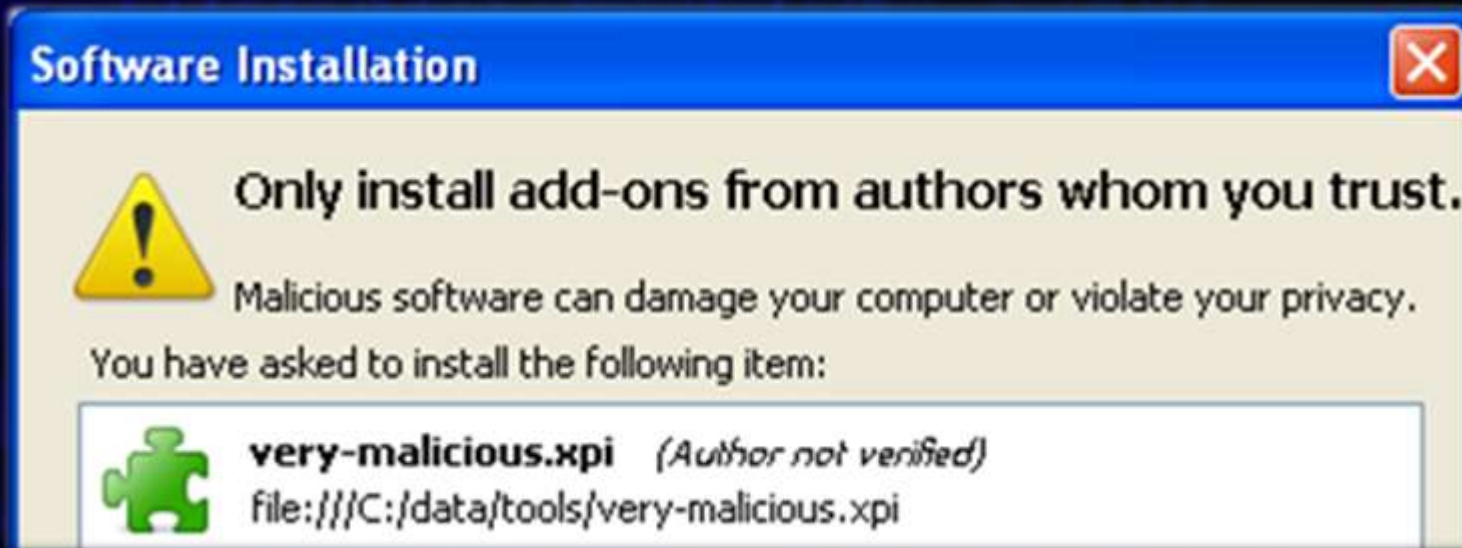
Chrome.manifest

Chrome*

...

Installer files

Data files (*.JS)



Are there many Extensions?

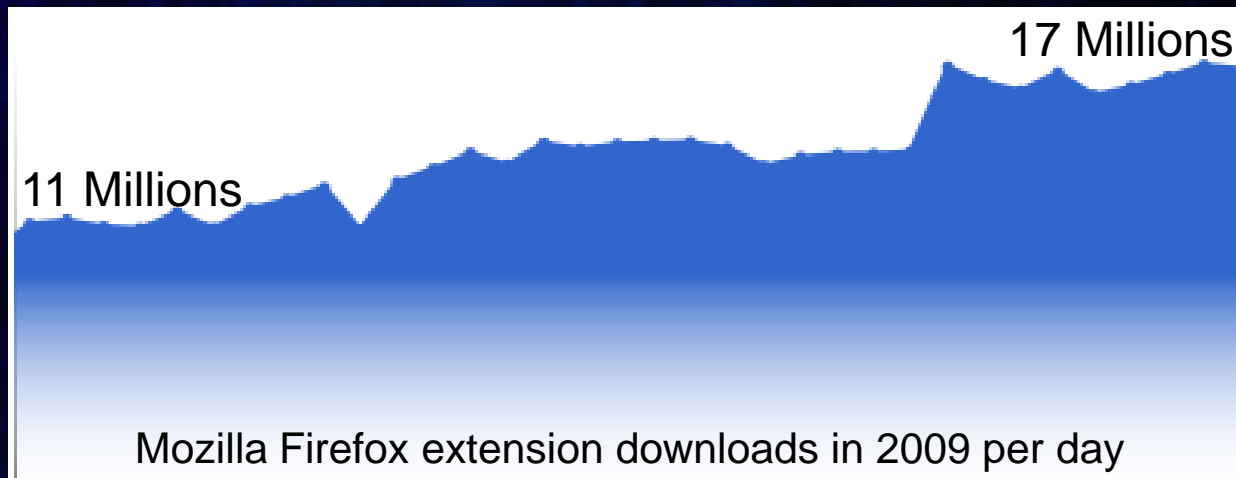
010101001011010100110011011010100101011010100010110110011101101001010101110101011010110011100101010110101100010101101100110

Firefox 3.x - 22% market share



Firefox Extensions:

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



01/01/2009

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

010101001011010100110011011010100101011010100010110110011101101001010101110101011010110011100101010110101100010101101100110

What can extensions do?

What can extensions do?

Everything that Firefox could do



It is missing a granular privilege system

- 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

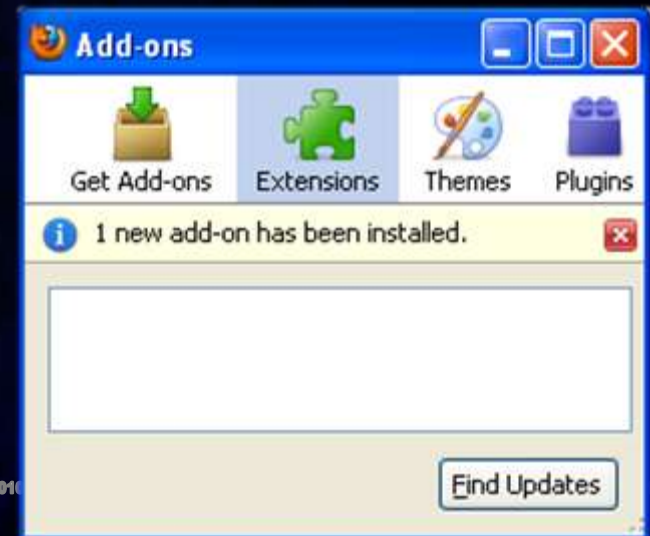
- **Malicious updates from trusted source**
 - As seen with NoScript or Vietnamese language pack
- **Dropped through vulnerabilities**
 - Talk by Roberto Suggi Liverani / Nick Freeman (Defcon 17)
 - JavaScript with Chrome privileges → Game Over
- **Dropped by local malware**
 - Easy to build and hard to trace (Same as with IE BHO)
- **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



01010100101101010011001101101010010101101010001011011001110110100101010101101010110101011010110011100101010110101100010101101100110

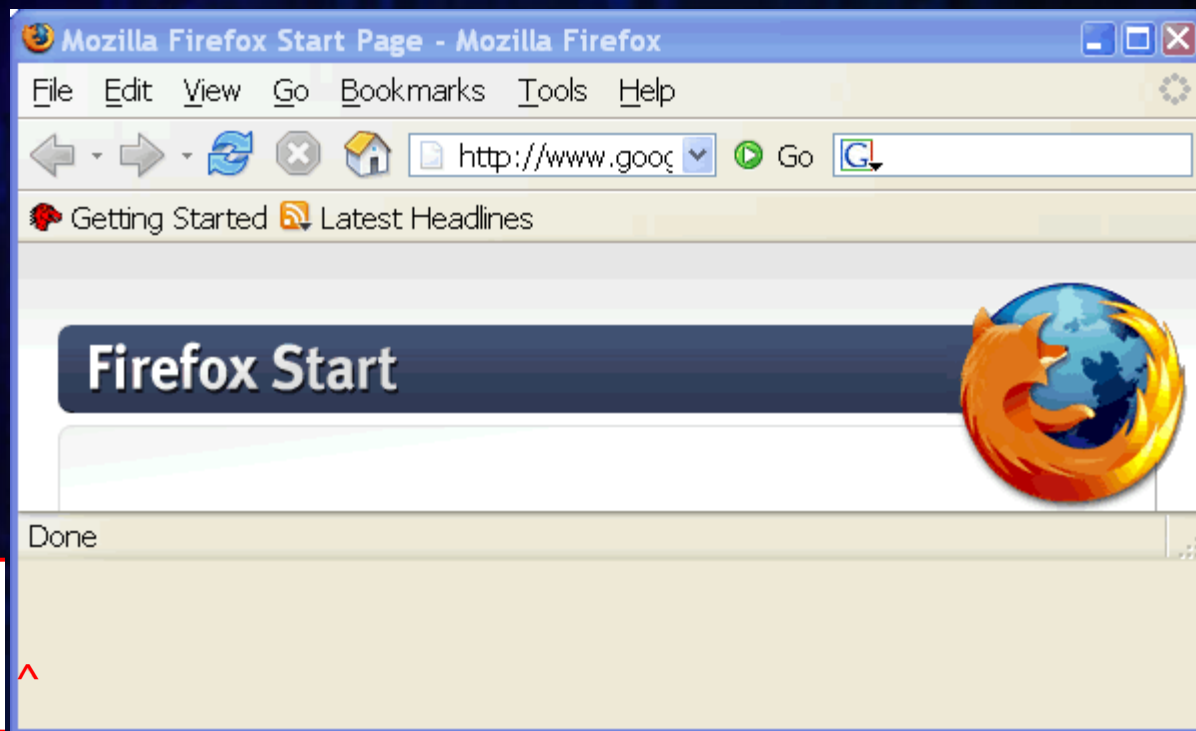
DEMO – 1



01010100101101010011001101101010010101101010001011011001110110100101010101101010110101011010110011100101010110101100010101101100110

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

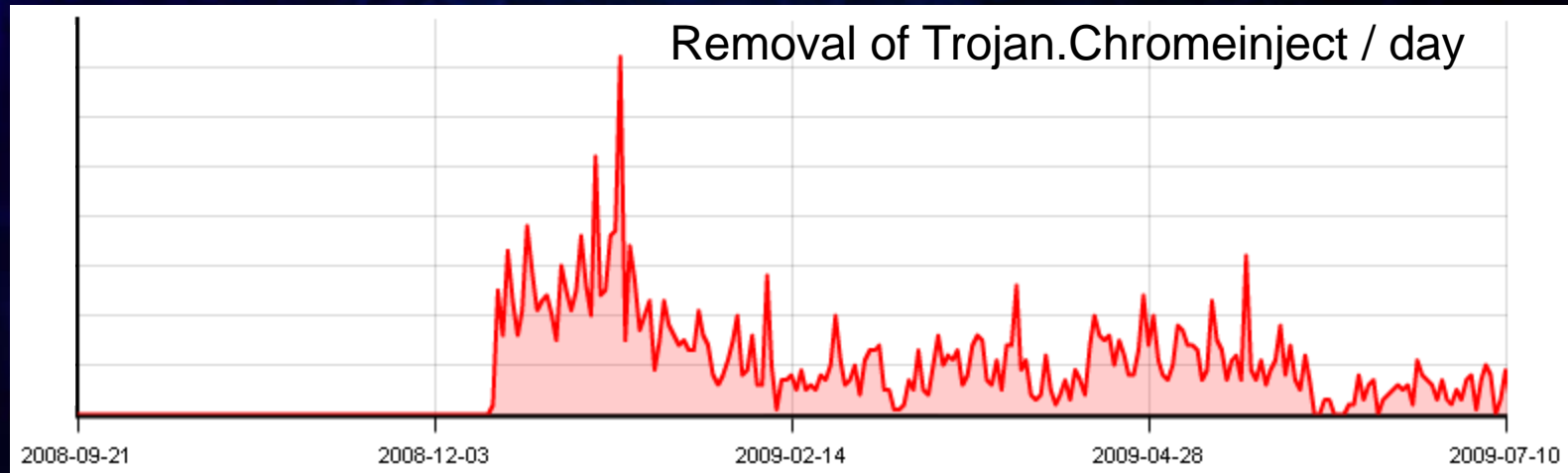
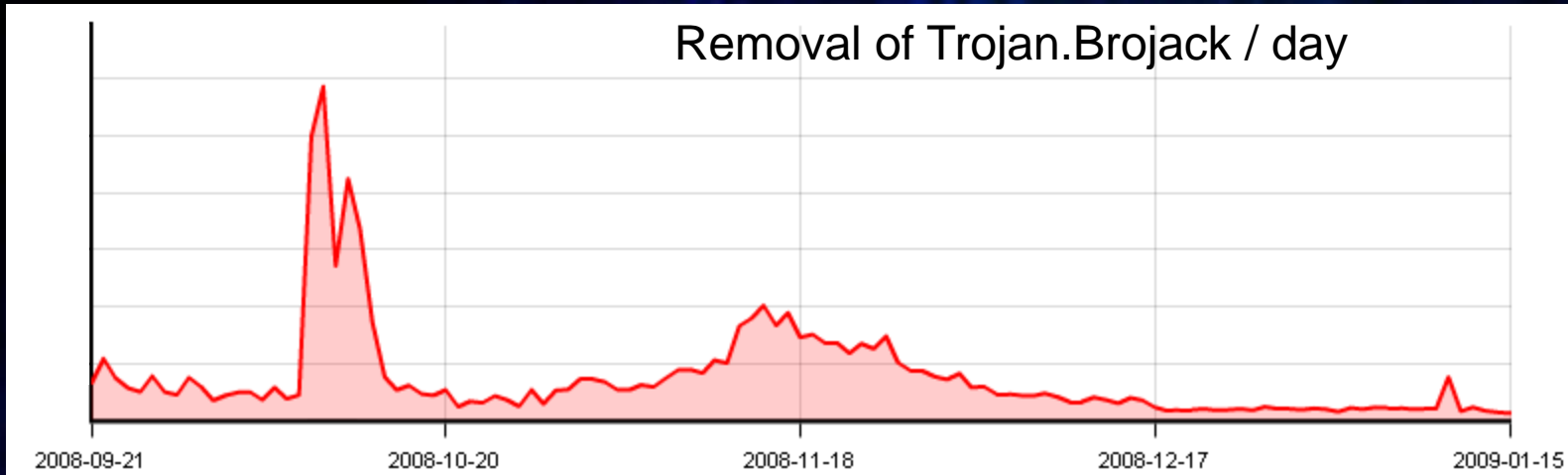


Generated
by an error

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

Prevalence

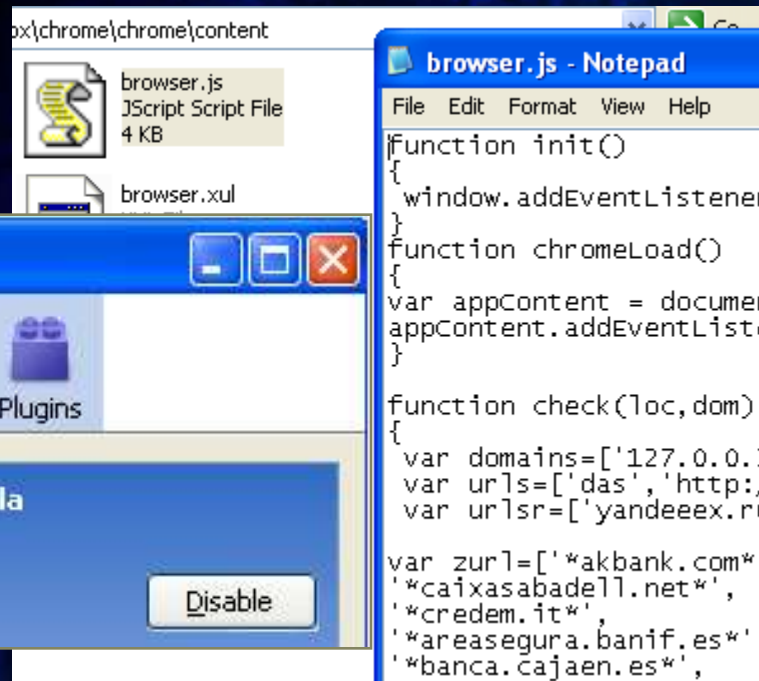
01010100101101010011001101101010010101101010001011011001110110100101010101101010110101011001110010101011010110001010101100110



01010100101101010011001101101010010101101010001011011001110110100101010101101010110101011001110010101011010110001010101100110

Examples

01010100101101010011001101101010010101101010001011011001110110010101010110101011010110011100101010110101100010101101100110



```
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 dll for certain URLs
- Steals credentials for financial sites
- Hides from Extension Manager

Trojan.Chromeinject

01010100101101010011001101101010010101101010001011011001110110010101010110101011010110011100101010110101100010101101100110

01010100101101010011001101101010010101101010001011011001110110100101010101101010110101011010110011100101010110101100010101101100110

DEMO – Malware



01010100101101010011001101101010010101101010001011011001110110100101010101101010110101011010110011100101010110101100010101101100110

Conclusion

0101010010110101001100110110101001010110101000101101100111011010010101011010101101010110011100101010110101100010101101100110



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



0101010010110101001100110110101001010110101000101101100111011010010101011010101101010110011100101010110101100010101101100110

?

Questions



Thank you for listening
candid wüest

Thanks to co-author Elia Florio

The whitepaper can be found here:

http://www.symantec.com/business/security_response/whitepapers.jsp