

# The Inconvenient Truth About the State of Browser Security

Wolfgang Kandek  
Qualys, Inc.



Session ID: SP01-204  
Session Classification: Intermediate

# Agenda

- Browser Security Project
- Browser Plugins
- Resulting Threats
- Actions
- Up and Coming

# BrowserCheck Project

---

- <https://browsercheck.qualys.com>
- Security check for Browsers and Plug-ins

# BrowserCheck Project

Qualys BrowserCheck - Mozilla Firefox

qualys.com https://browsercheck.qualys.com/

Qualys BrowserCheck

**QUALYS BROWSERCHECK**

About FAQ Feedback Qualys.com

Browser Check Complete  
**1 Security Issue Detected**

Firefox 3.6

Follow the recommended actions in the results below to get software updates and resolve security issues.

Re-Scan

Qualys® BrowserCheck Results

	<b>Mozilla Firefox</b> Product Version: 3.6.13	<a href="#">▶ Up To Date</a>
	<b>Adobe Flash Player</b> Product Version: 10.1.102.64	<a href="#">▶ Insecure Version</a> <a href="#">Fix It</a>

Facebook Twitter

**? NEED HELP?**

- [Why is my browser insecure?](#)
- [What do the different status levels mean?](#)
- [How do I fix a security issue?](#)
- [What items are detected by this](#)

# BrowserCheck Project

- <https://browsercheck.qualys.com>
- Security check for Browsers and Plug-ins
- End user focus, free and easy to use

# BrowserCheck Project

- [sXXXXXXXXs@gmail.com](mailto:sXXXXXXXXs@gmail.com): This is really a wonderful tool for browser check I will recommend this to my friends who would be pleased to try it.
- [kXXXXXXXX7@hotmail.com](mailto:kXXXXXXXX7@hotmail.com): thank guyssssssssssssssssssss.....
- [wXXXXXXXXn@suddenlink.net](mailto:wXXXXXXXXn@suddenlink.net): Great Tool! It's scarry that I was running my computer in the dark re online securituy for all of these years. I would like to see feeds added to notify me of changes/upgrades to the programs it is checking.
- [jXXXXXXXX4@earthlink.net](mailto:jXXXXXXXX4@earthlink.net): First, I like that it checks for available updates. Additionally, the links for zero-day issues. Very nice!
- [fXXXXXXXX9@live.com](mailto:fXXXXXXXX9@live.com): This program is the first so far that i have tried that appears to work!!! Thanks
- [bXXXXXXXXs@bmts.com](mailto:bXXXXXXXXs@bmts.com): This little tool is great for us non-techy types. I have told my friends about it as well
- [aXXXXXXXXm@comcast.net](mailto:aXXXXXXXXm@comcast.net): No Linux support? Pathetic



# BrowserCheck Project


Applications Places System Sun Feb 13, 9:04 PM user

Qualys BrowserCheck - Mozilla Firefox

File Edit View History Bookmarks Tools Help

← → ↻ × 🏠 qualys.com https://browsercheck.qualys.com/ ☆ Google 🔍

Qualys BrowserCheck +




 **Browser Check Complete**  
**1 Security Issue Detected**

Follow the recommended actions in the results below to get software updates and resolve security issues.

[Re-Scan](#)

**BETA** Thank you for trying out the beta version of our scanner for your browser. [Click here](#) to see list of fully supported browsers.

Qualys® BrowserCheck Results

 <b>Mozilla Firefox</b> 3.6.13	<a href="#">Up To Date</a>	
 <b>Shockwave Flash</b> 10.1.102	<a href="#">Insecure Version</a>	<a href="#">Fix It</a>
 <b>Totem Player</b> 2.32.0	<a href="#">Update Available</a>	<a href="#">Fix It</a>

[f](#) [t](#)

[?](#) **NEED HELP?**

[Why is my browser insecure?](#)

[What do the different status levels mean?](#)

[How do I fix a security issue?](#)

[What items are detected by this tool?](#)

[!](#) **RATE THIS TOOL**

[Send us your feedback](#)

Qualys BrowserCheck ...

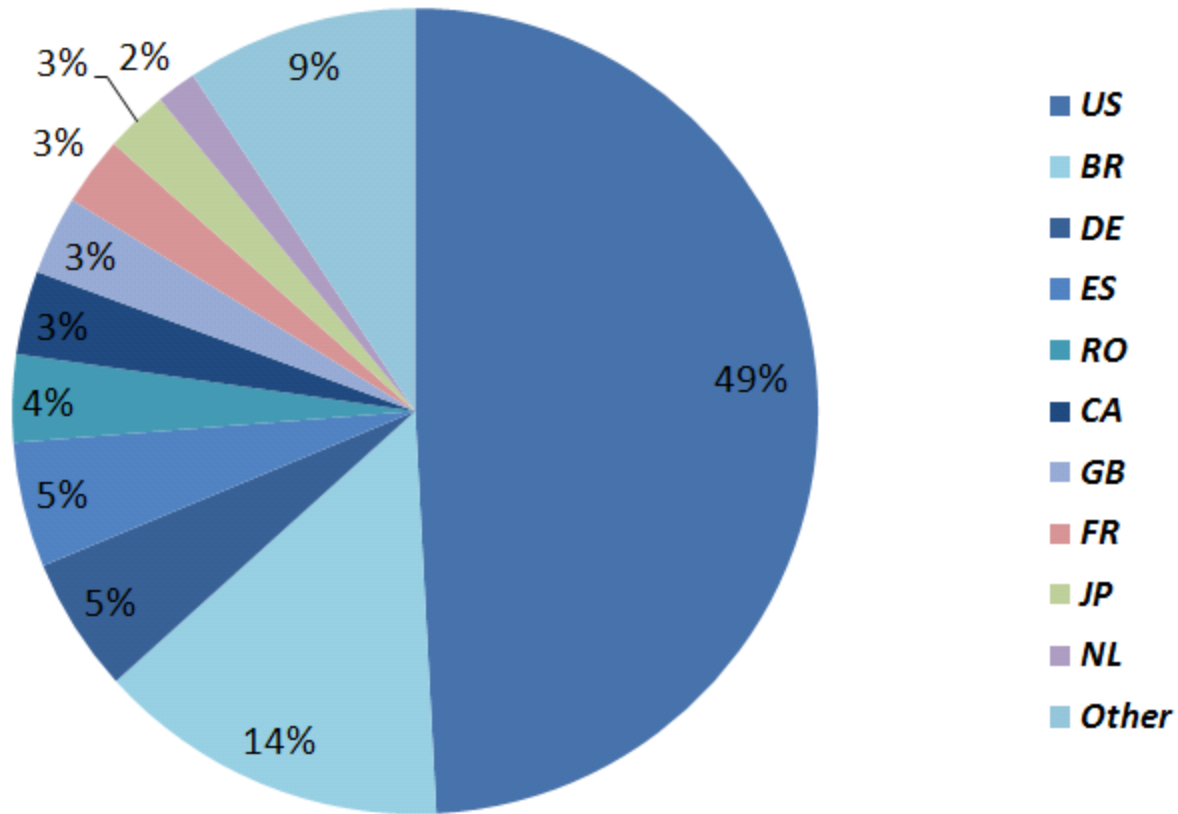
# BrowserCheck Project

- <https://browsercheck.qualys.com>
- Security check for Browsers and Plug-ins
- End user focus, free and easy to use
- Windows, Mac OS X and Linux
- IE, Firefox, Safari, Chrome, Opera
- 200,000 visits – Jul 2010 / Jan 2011



# BrowserCheck Project Stats

## Country Percentages

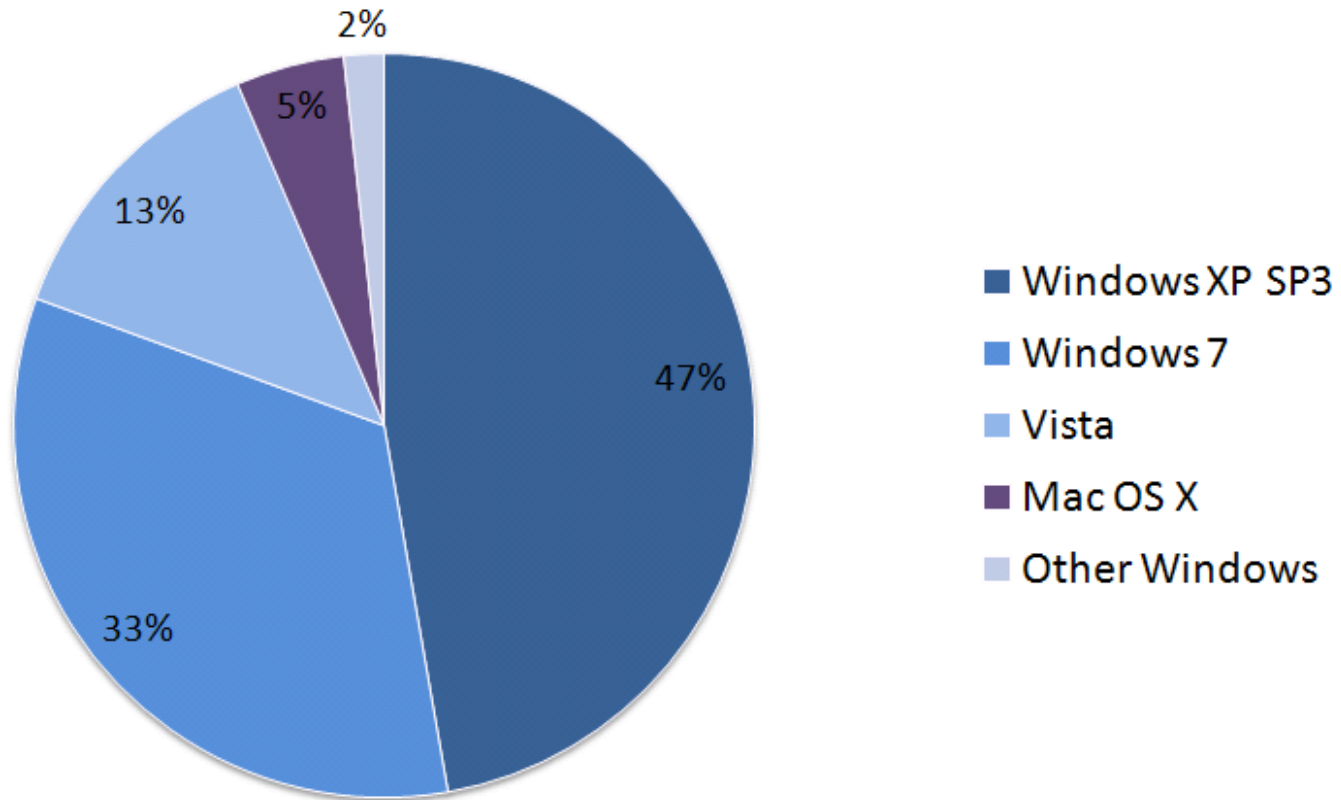


# BrowserCheck Project Stats

- Operating System: ?

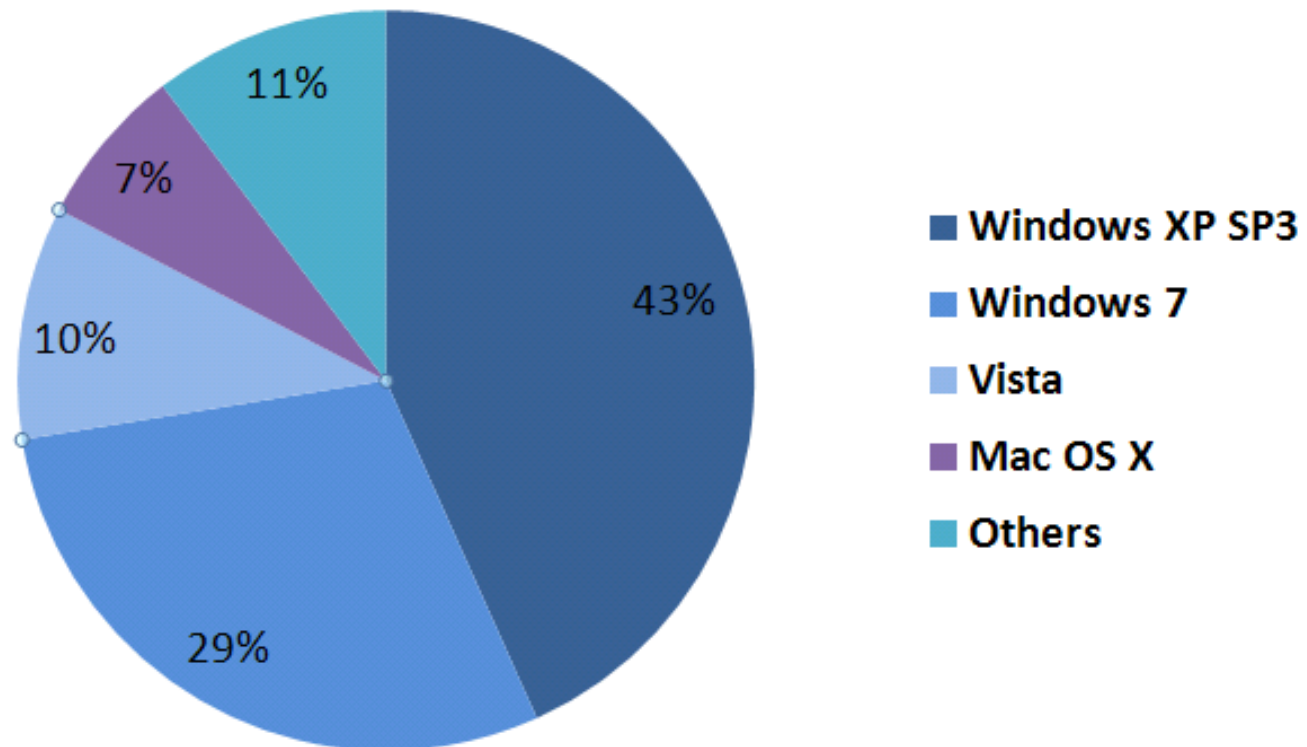
# BrowserCheck Project Stats

OS Distribution



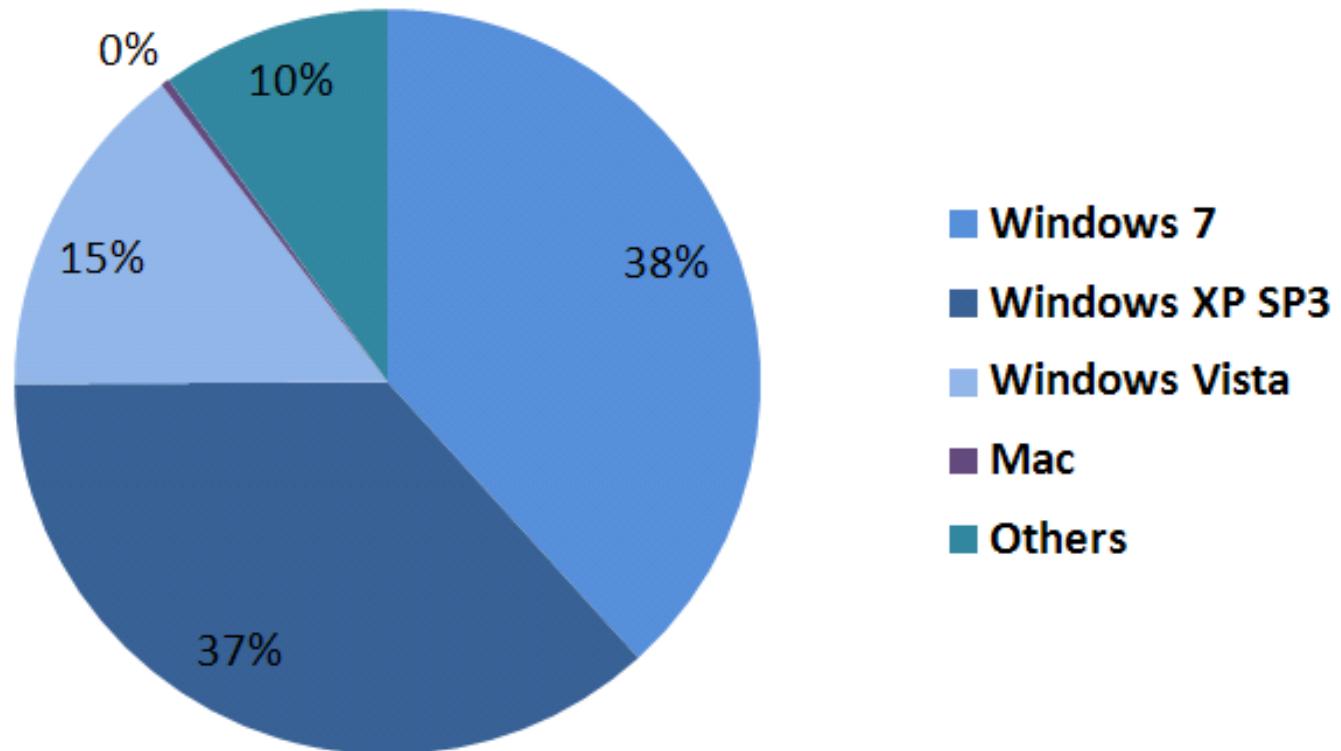
# BrowserCheck Project Stats

OS distribution in USA (US)



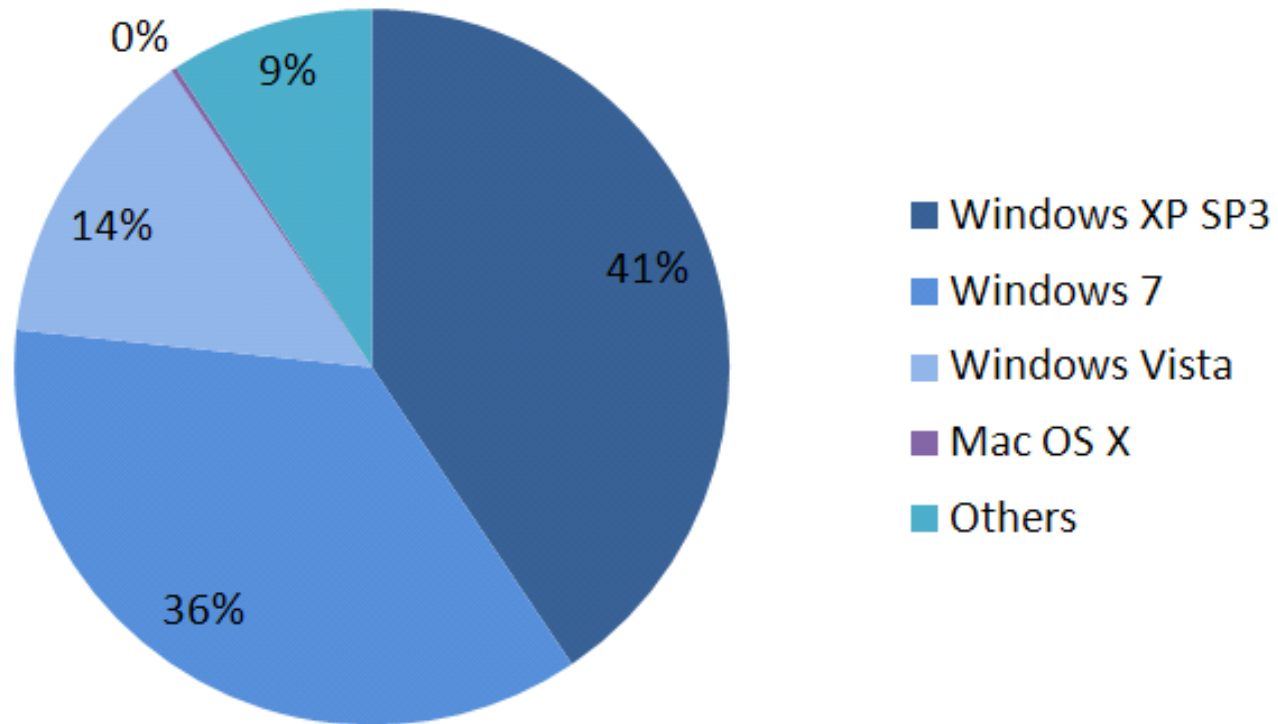
# BrowserCheck Project Stats

OS distribution in Brazil (BR)



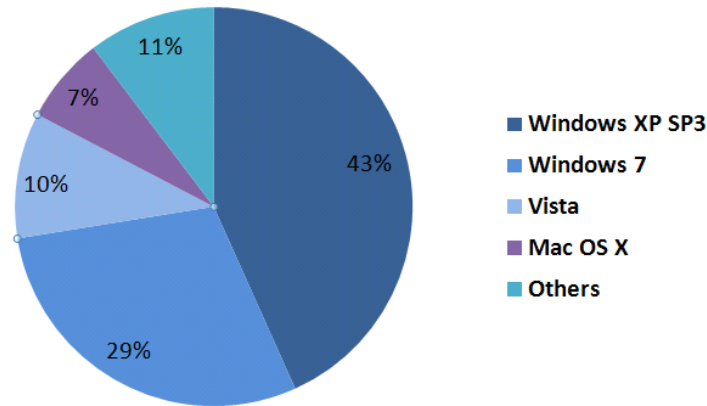
# BrowserCheck Project Stats

OS distribution in Germany (DE)

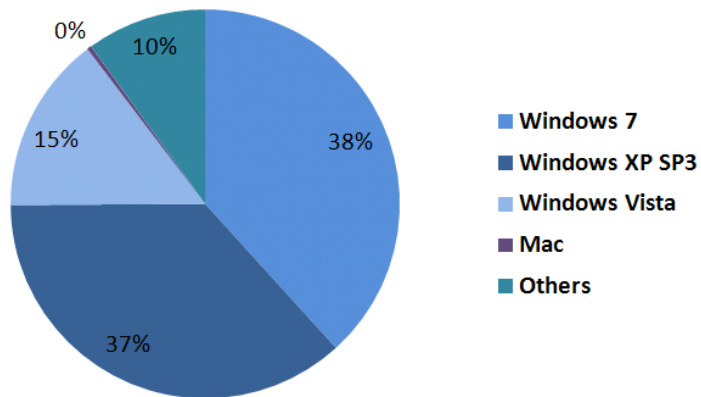


# BrowserCheck Project Stats

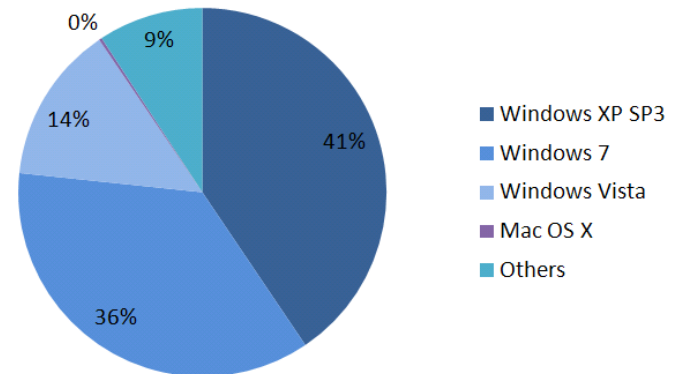
OS distribution in USA (US)



OS distribution in Brazil (BR)



OS distribution in Germany (DE)



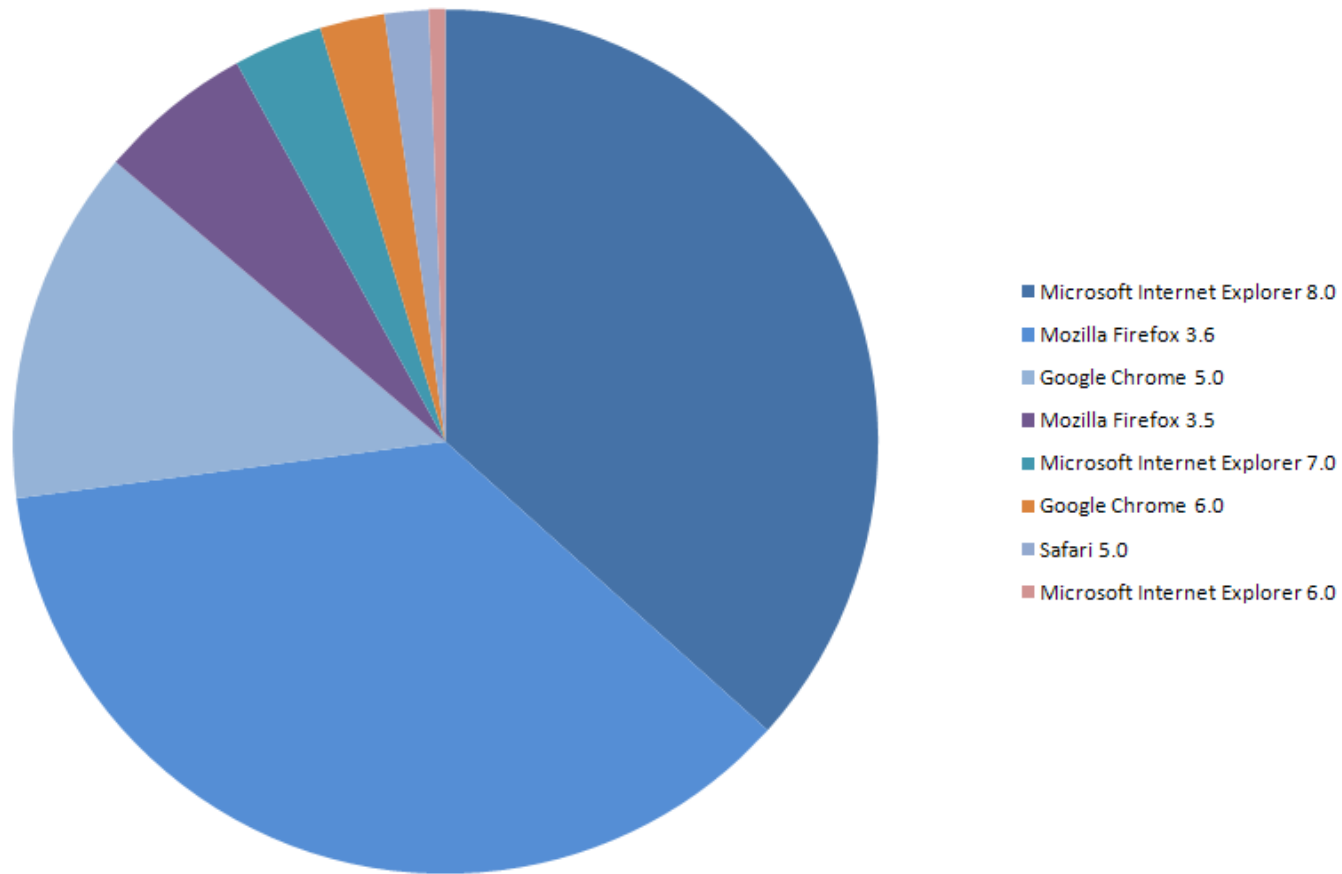
# BrowserCheck Project Stats

- Operating System:
  - Windows XP – 47 %
  - Windows 7 – 32 %
- Browser: ?



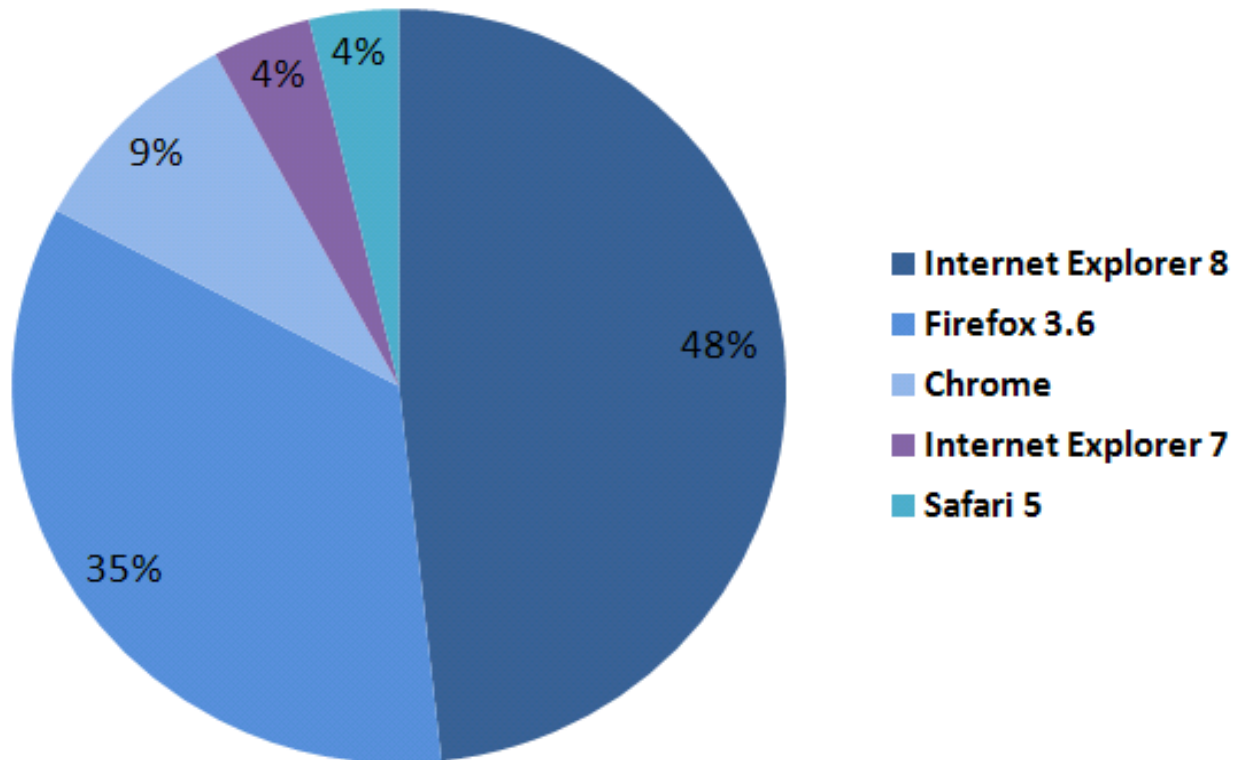
# BrowserCheck Project Stats

Browser Distribution



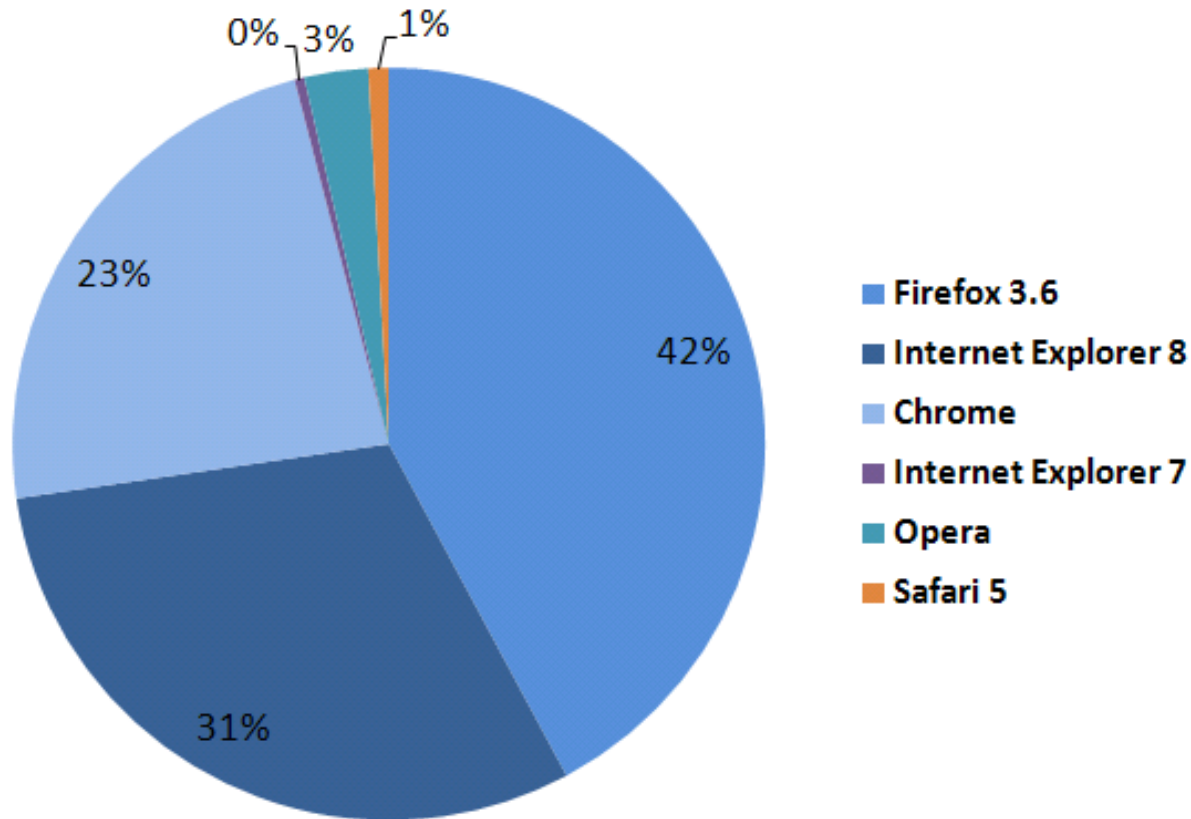
# BrowserCheck Project Stats

Browser distribution in USA (US)



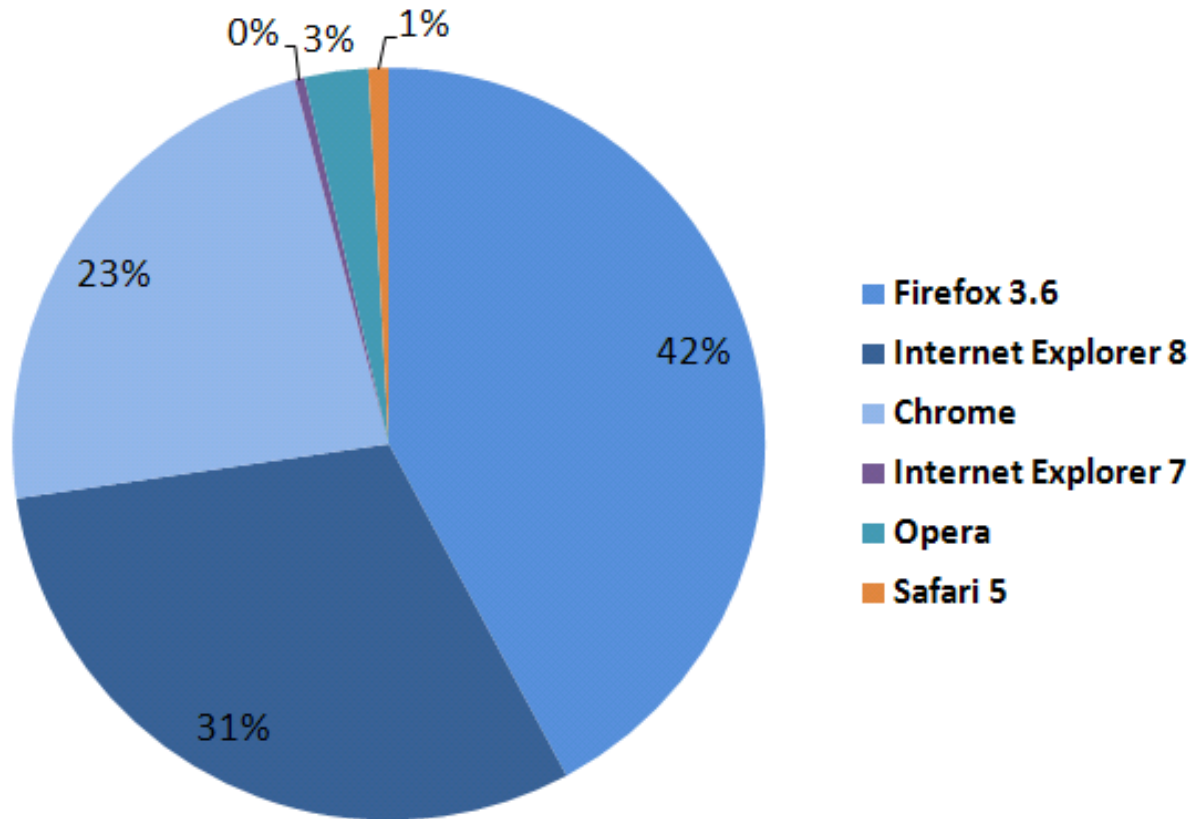
# BrowserCheck Project Stats

Browser distribution in Brazil (BR)



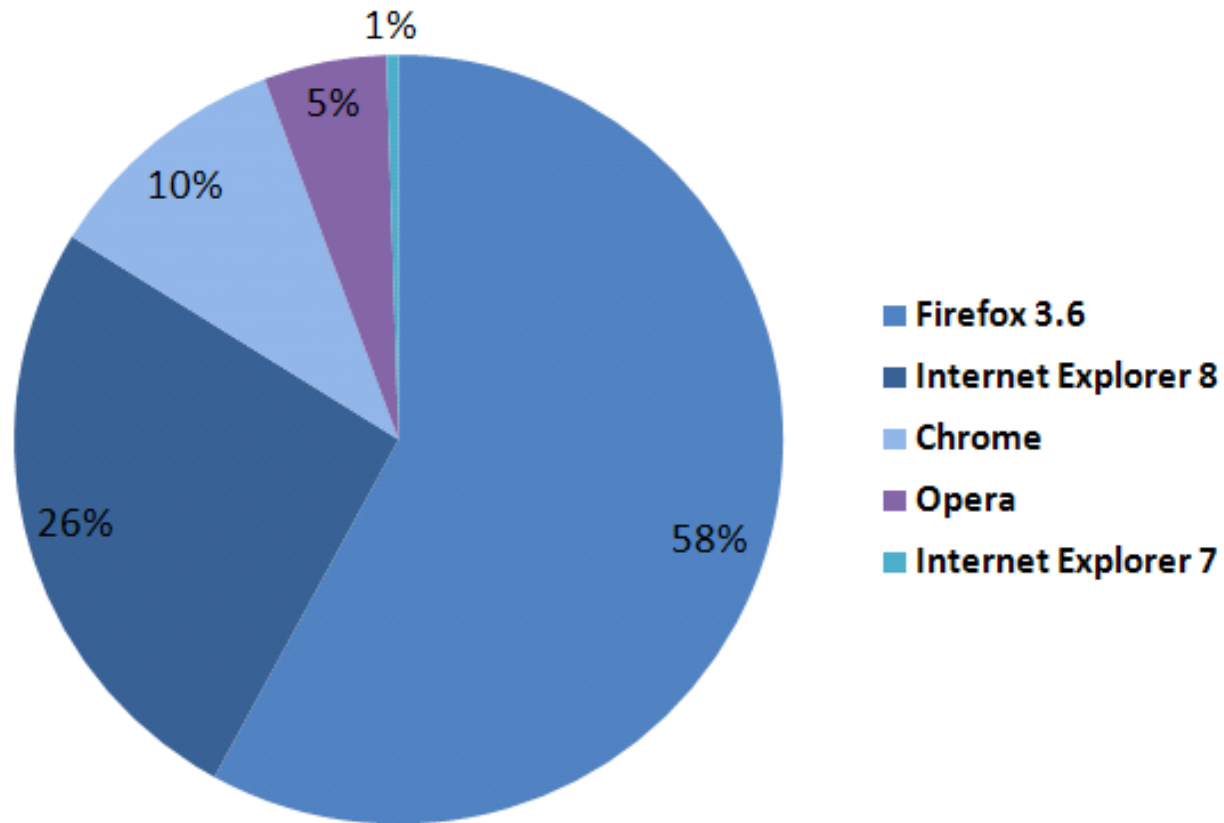
# BrowserCheck Project Stats

Browser distribution in Brazil (BR)



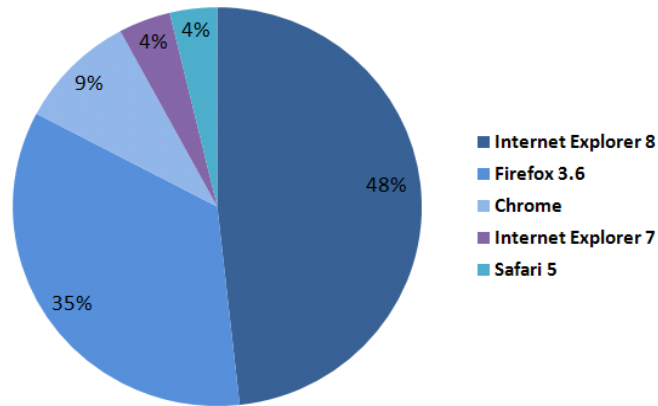
# BrowserCheck Project Stats

Browser distribution in Germany (DE)

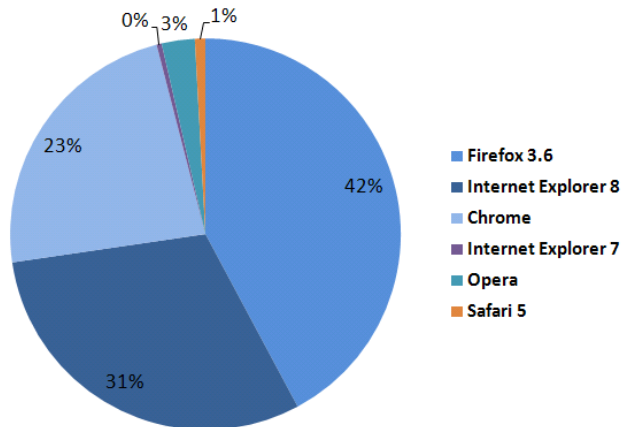


# BrowserCheck Project Stats

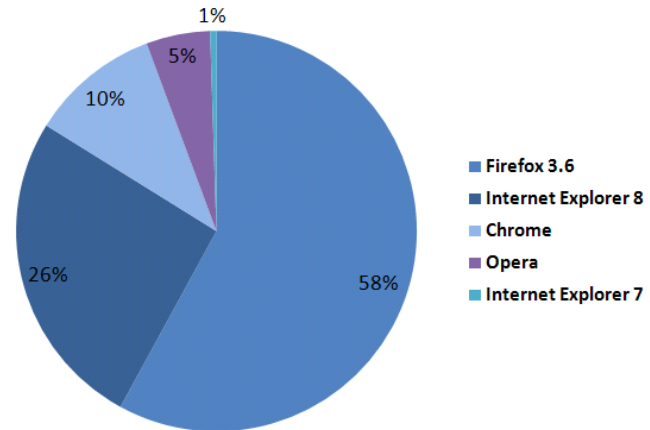
Browser distribution in USA (US)



Browser distribution in Brazil (BR)



Browser distribution in Germany (DE)

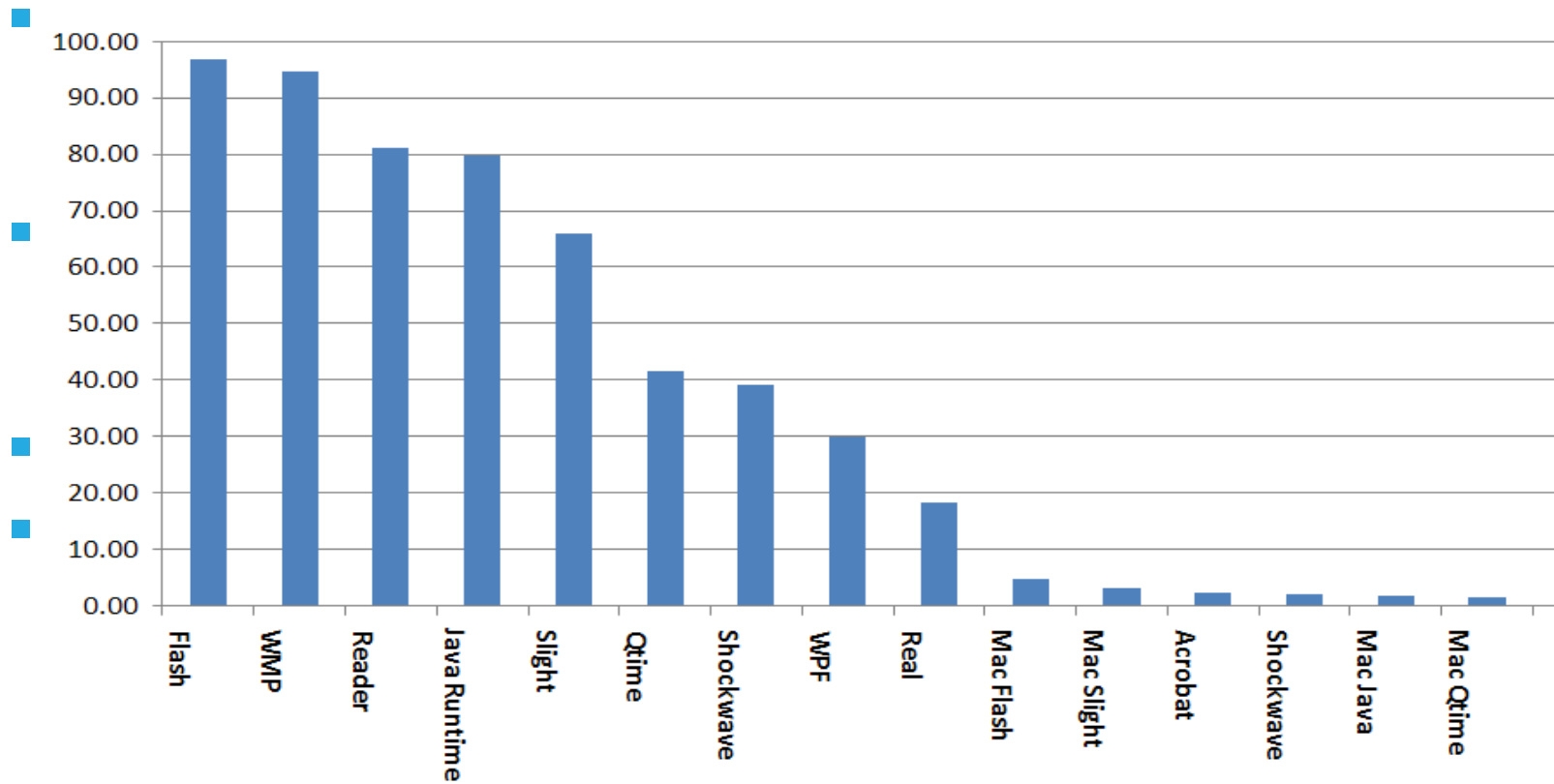


# BrowserCheck Project Stats

- Operating System:
  - Windows XP – 47 %
  - Windows 7 – 32 %
- Browser:
  - IE 8 – 36 %
  - Firefox 3.6 – 34 %
- Plug-in: ?

# BrowserCheck Project Stats

## Browsercheck Plug-ins



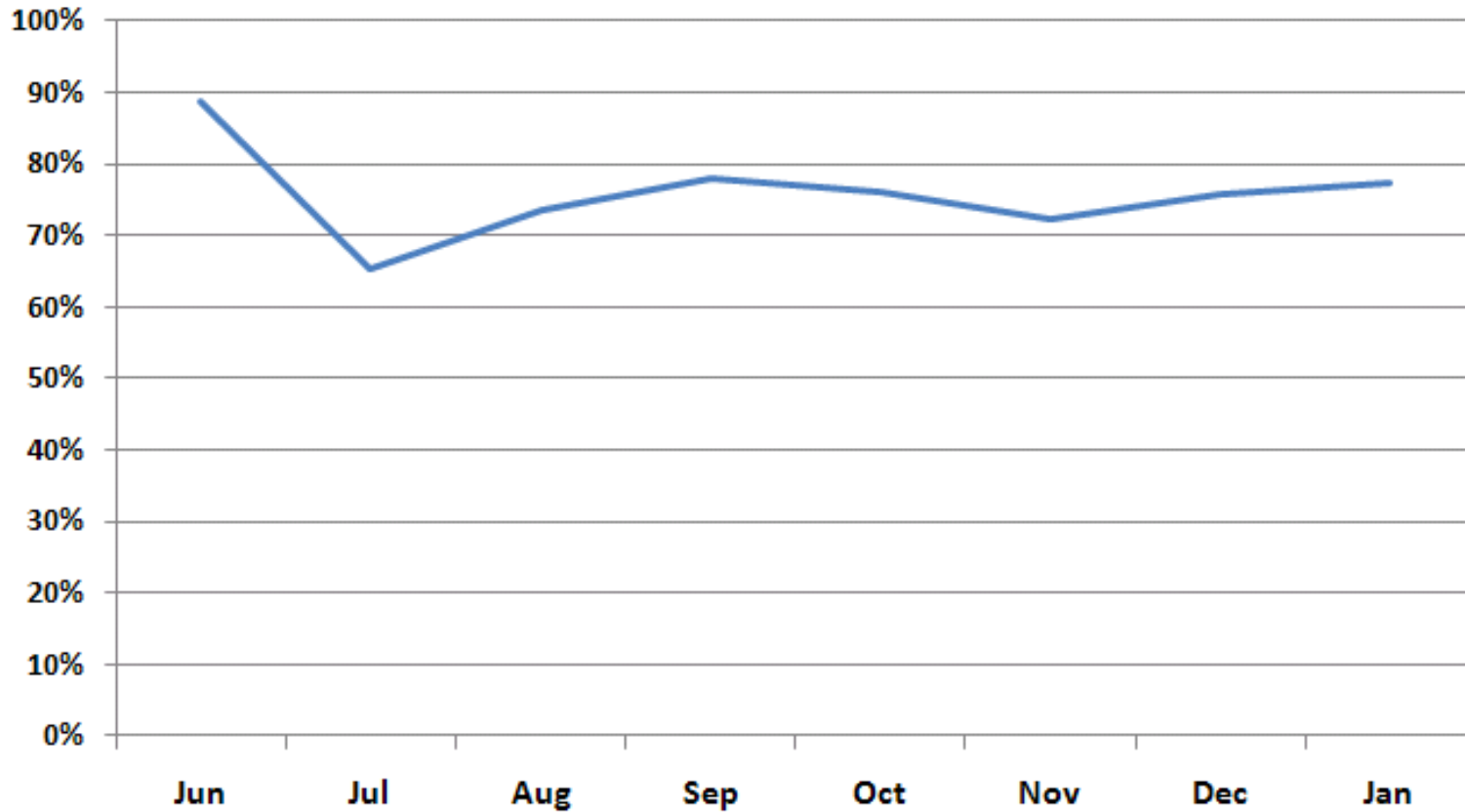


# BrowserCheck Project Stats

- Operating System:
  - Windows XP – 47 %
  - Windows 7 – 32 %
- Browser:
  - IE 8 – 36 %
  - Firefox 3.6 – 34 %
- Plug-in:
  - Adobe Flash – 97 %
  - Windows Media Player – 95%

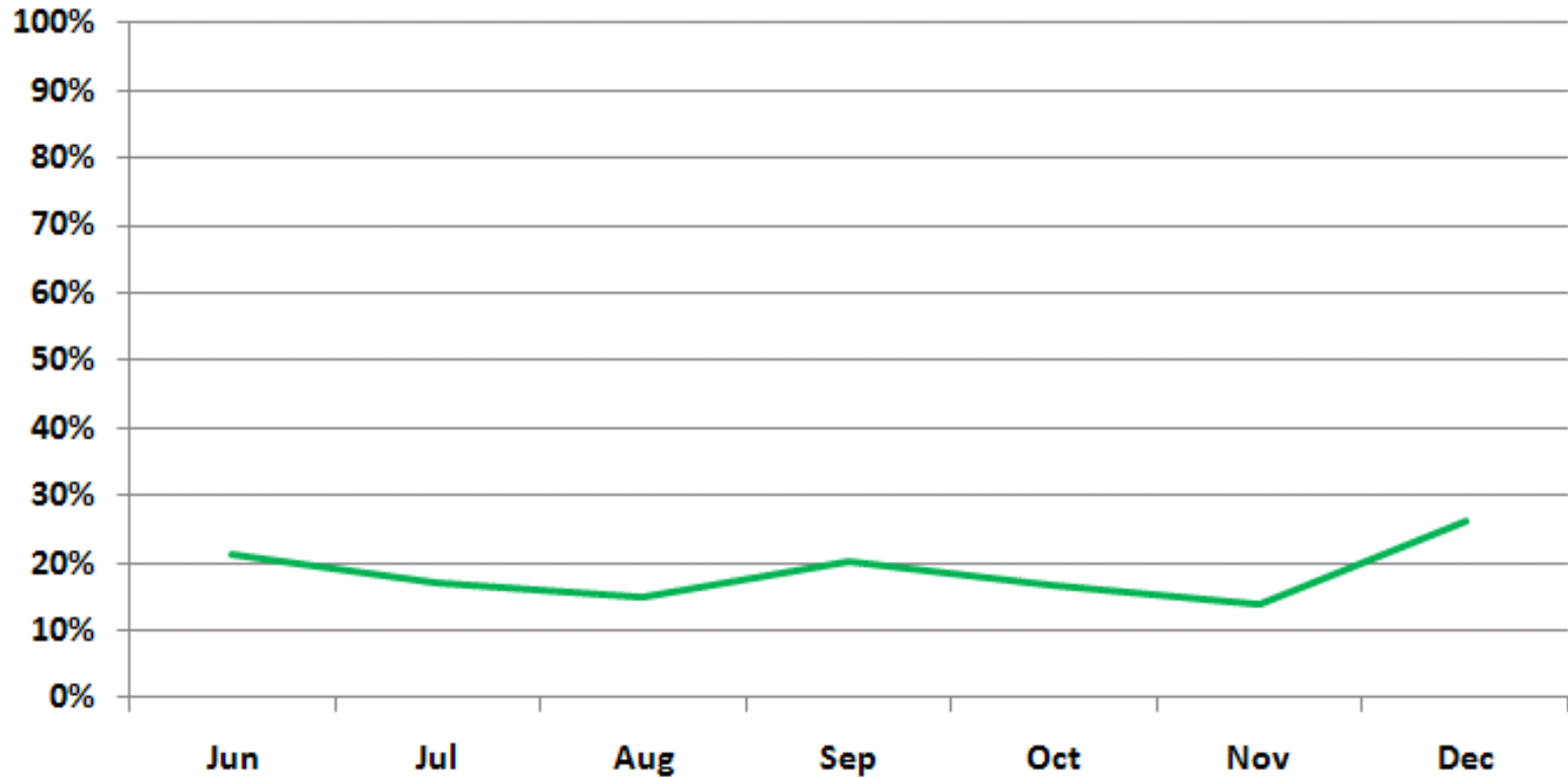
# BrowserCheck Project Stats

## Insecure Browsers



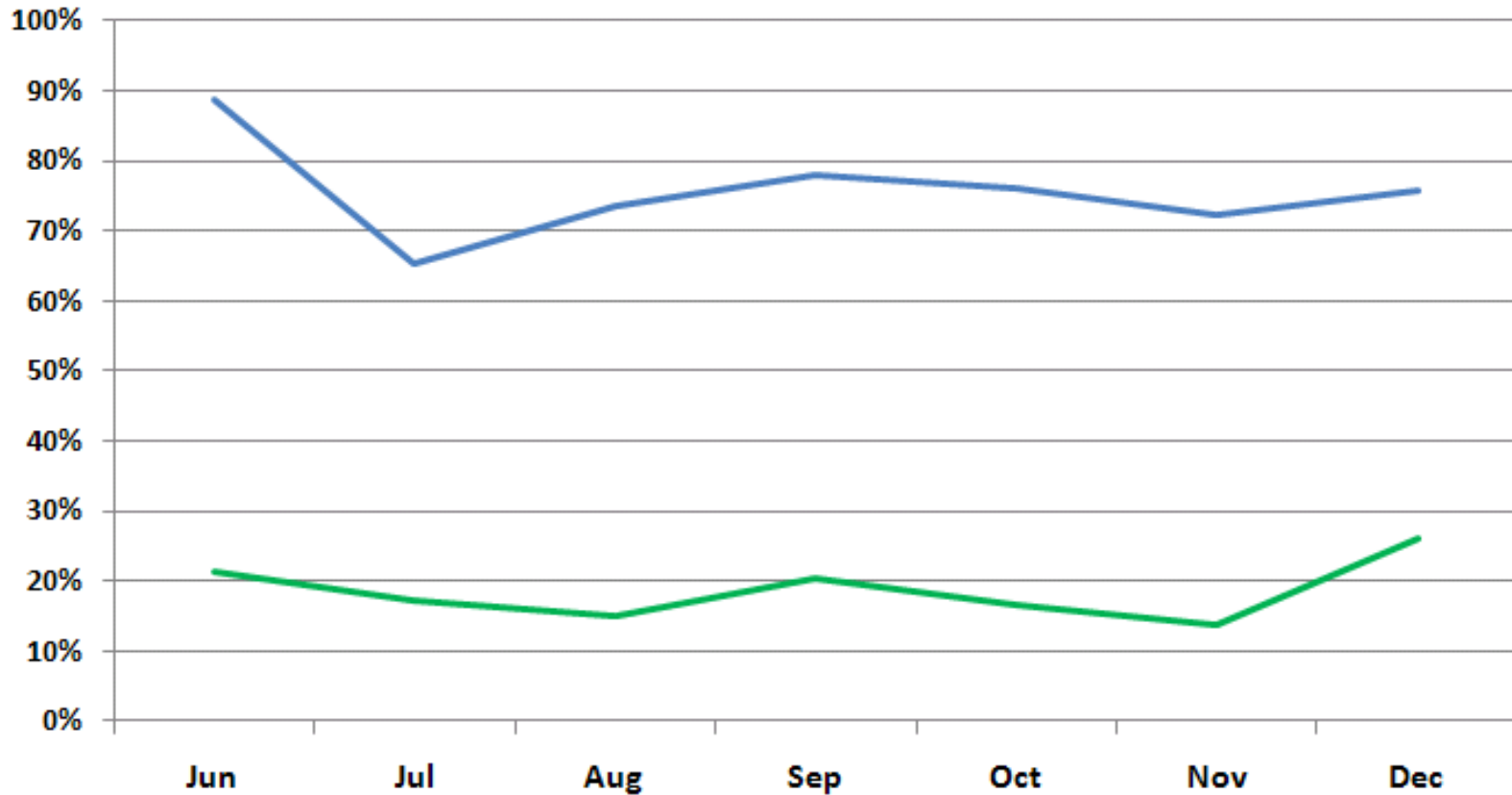
# BrowserCheck Project Stats

## Natively Insecure Browsers



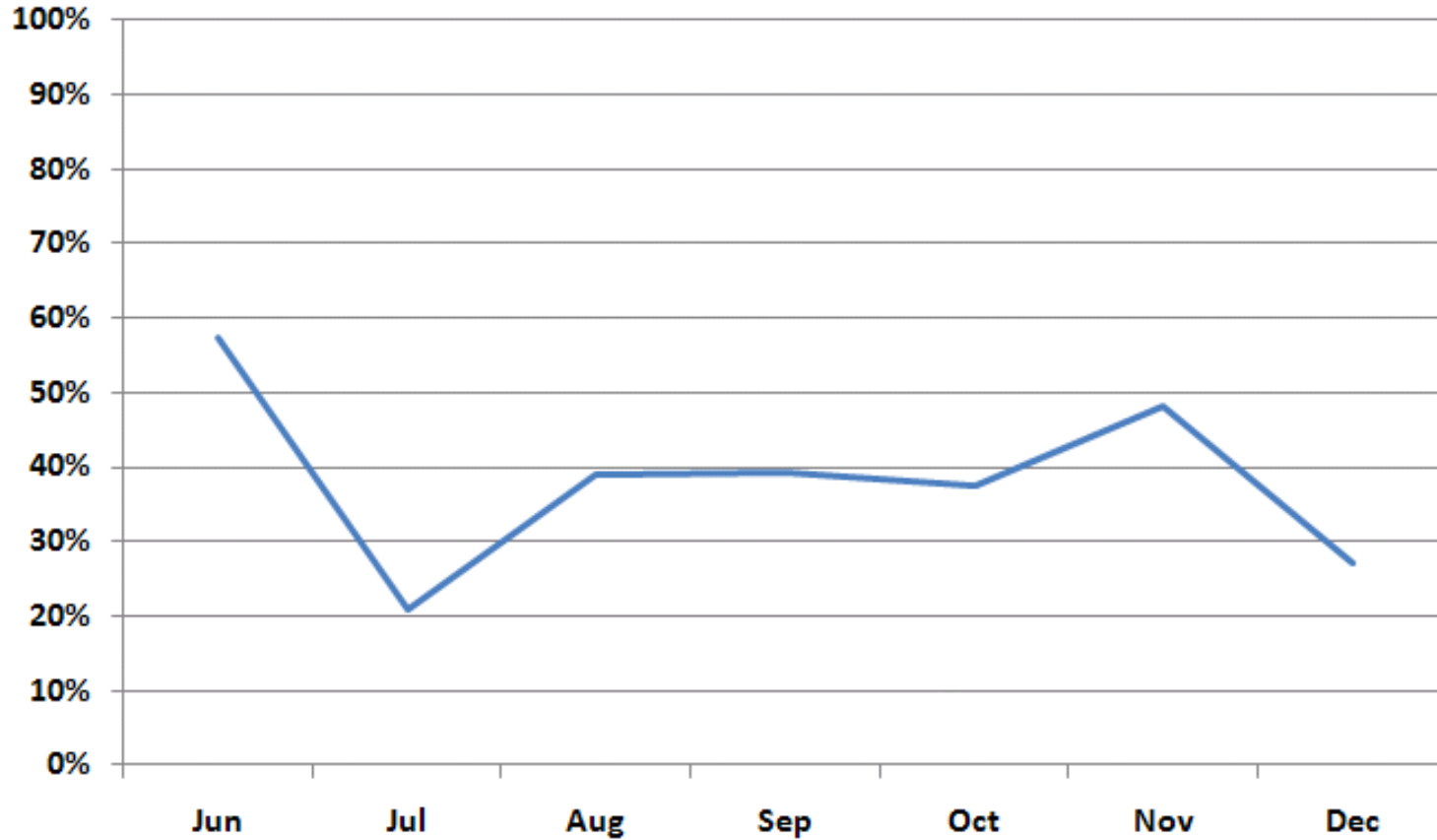
# BrowserCheck Project Stats

## Browsers Insecure By Association



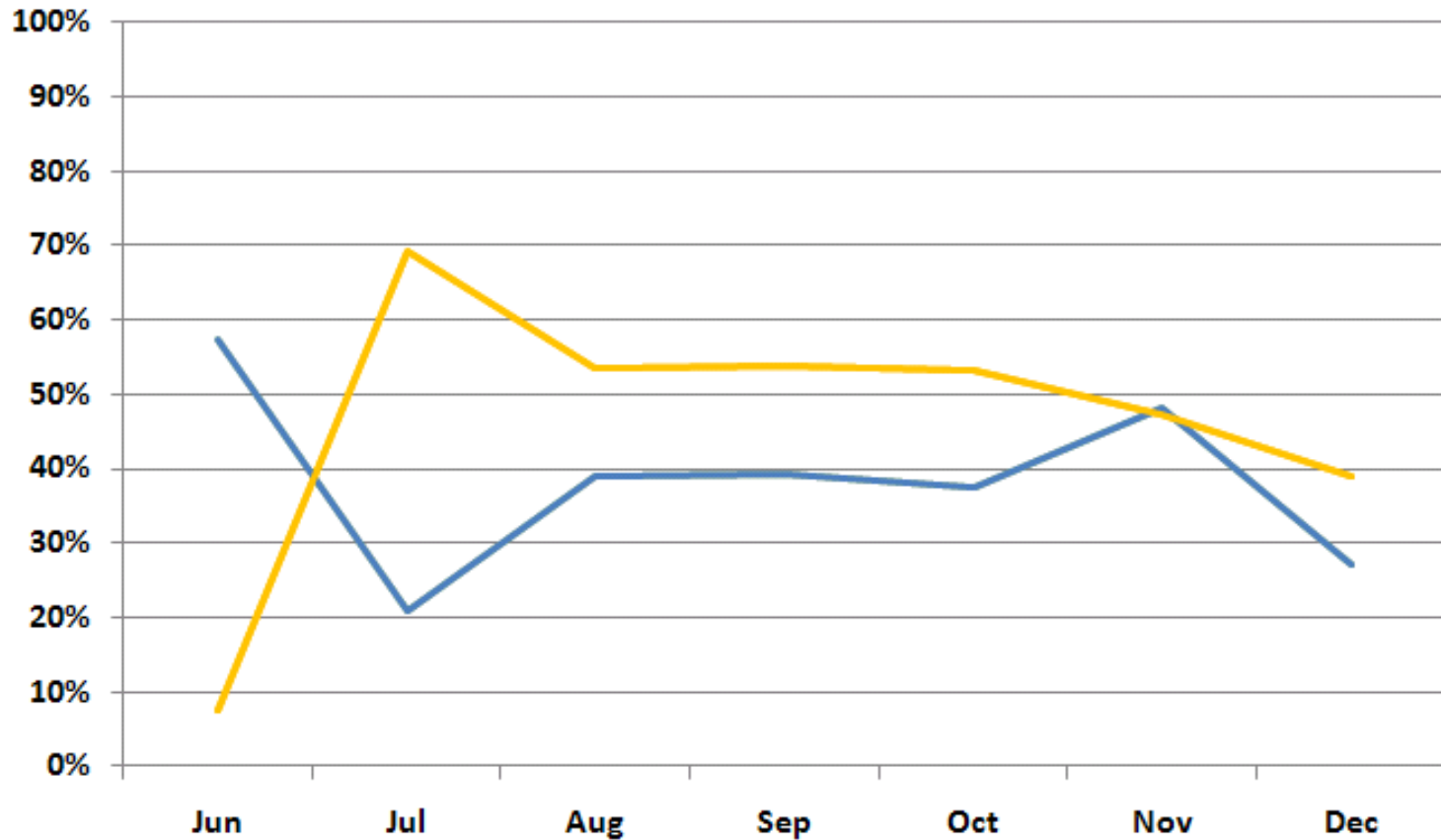
# BrowserCheck Project Stats

## Insecure Adobe Flash



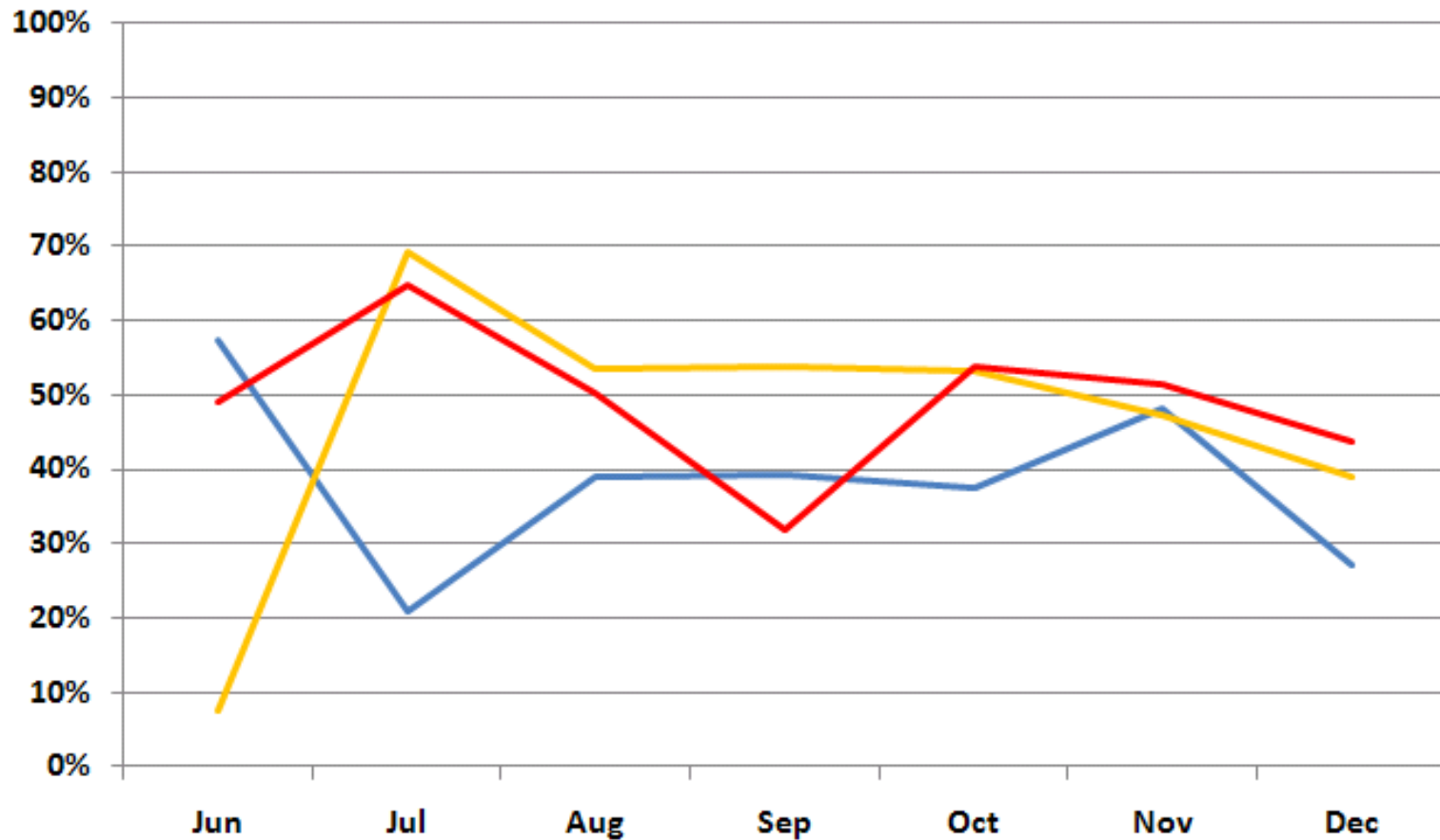
# BrowserCheck Project Stats

## Insecure Adobe Flash & Reader

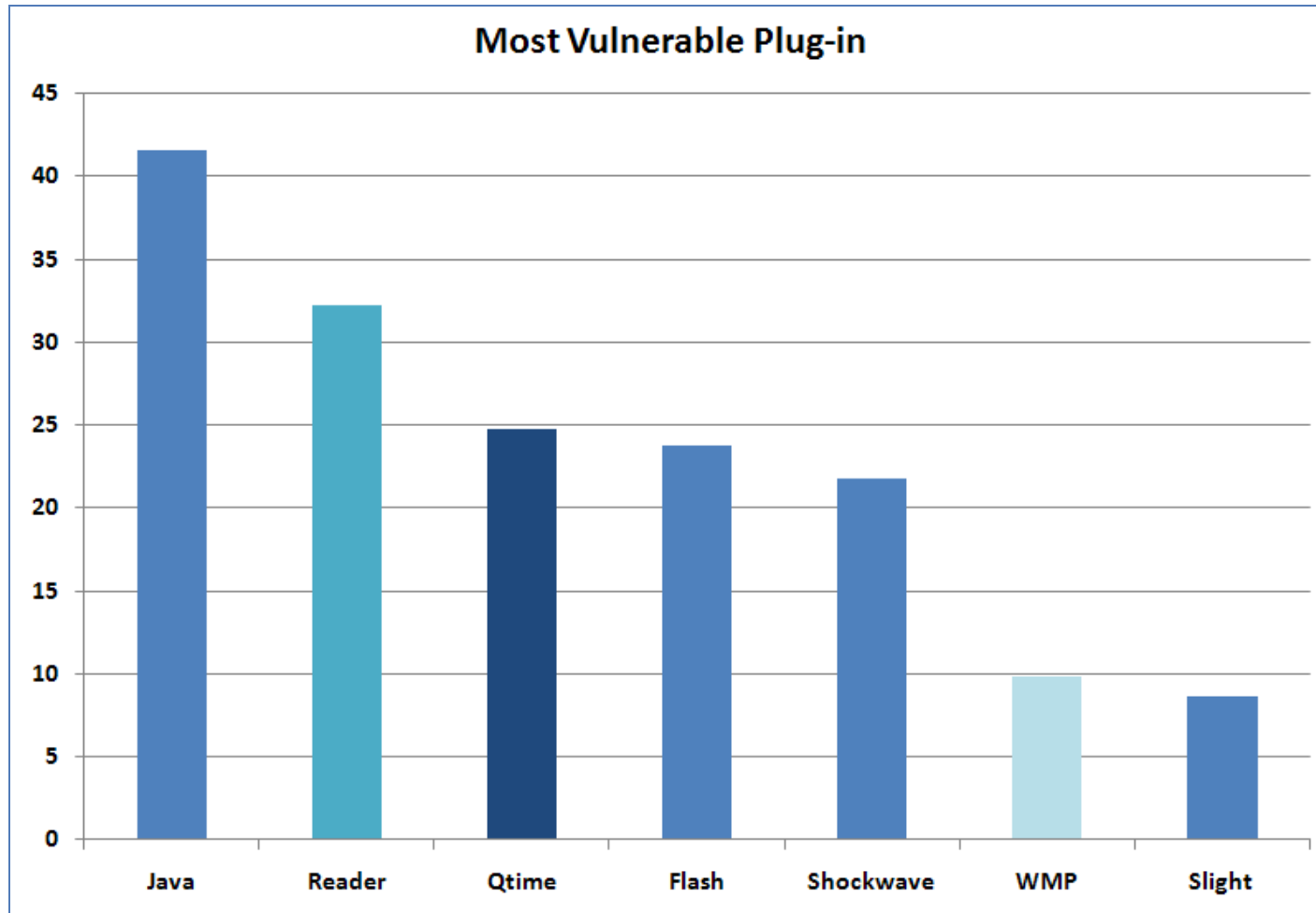


# BrowserCheck Project Stats

## Insecure Adobe Flash & Reader and Sun Java



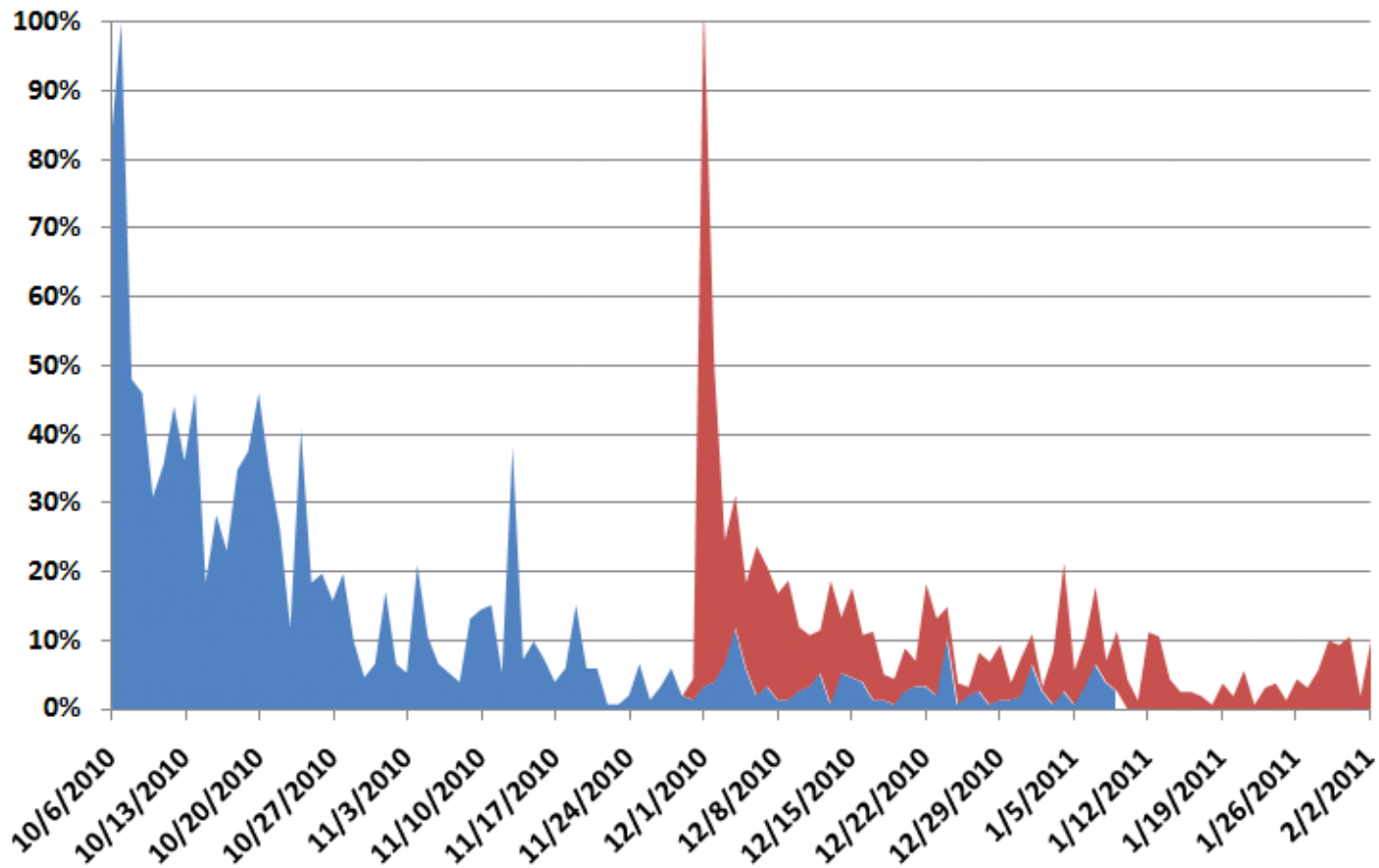
# BrowserCheck Project Stats





# BrowserCheck Project Stats – MVP – Adobe Reader

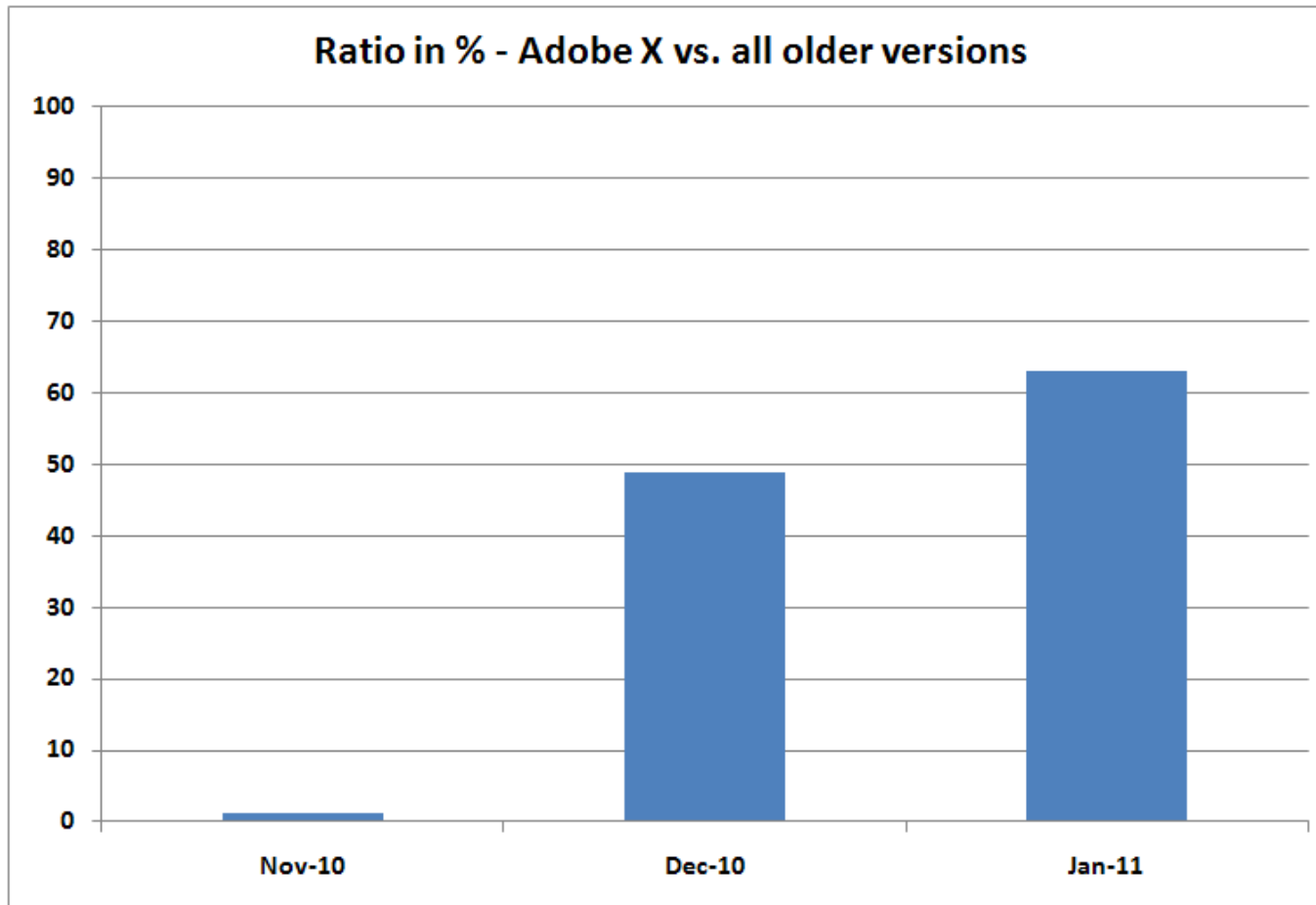
## Adobe Reader 9.3.4/9.4.0 Cycles



# BrowserCheck Project Stats

- Speed of Adoption of new Software versions
- Adobe Reader X
  - Introduced in mid November 2010
  - Improved Usability
- Security Enhancements
  - Sandbox (protected mode)
  - Secure defaults

# BrowserCheck Project Stats



# Summary

- Browser Security is in a shaky state
- Browsers and plug-ins frequently outdated and easily attackable
- Malware authors have adapted and most new attacks are against browser plug-ins

# Consequences

- Browsers are in use by your employees
  - 10% of all users come from corporate networks
  - 5-8% of all machines in corporate networks show signs of malware infection
- Browsers are in use by your clients
  - Credentials are in danger
  - Transaction integrity threatened

# Actions

- Assure Browsers are updated
  - Aggressive Patch roll-out
- Assure Browser Plugins are updated
  - Enumerate, Evaluate
  - Plan for Updates
- Browser Help (include updates for plugins)
- Vendor Help Ask Microsoft to open up and include
  - Adobe Patches
  - Sun, Apple Patches

# Actions

- Server: Implement 2-factor authentication
  - Username/Password are obsolete
  - 2-factor: token, phone
  - SaaS Services make management easier
- Server: Investigate client integrity
  - VPN plus local checks
  - Transparent services

# Up and Coming

- New Platforms
  - Smartphones, Tablets
  - Integrated machines
- Tight vendor management ++
- Loss of Control --
  
- CloudNAC
  - Client Health Repository





**Thank you !**

**The Inconvenient Truth  
About the State of  
Browser Security**

wkandek@qualys.com  
<http://laws.qualys.com>  
Twitter: @wkandek