

WEB BROWSER SANDBOXING: SECURITY AGAINST WEB ATTACKS

AVAR 2011

by Rajesh Nikam

Quick Heal

Security Simplified

CONTENTS

Rise of Web Attacks

Application Vulnerabilities

Existing Protection Mechanisms

Need for Effective Sandbox

Sandboxing as Mitigation

Challenges

Conclusion

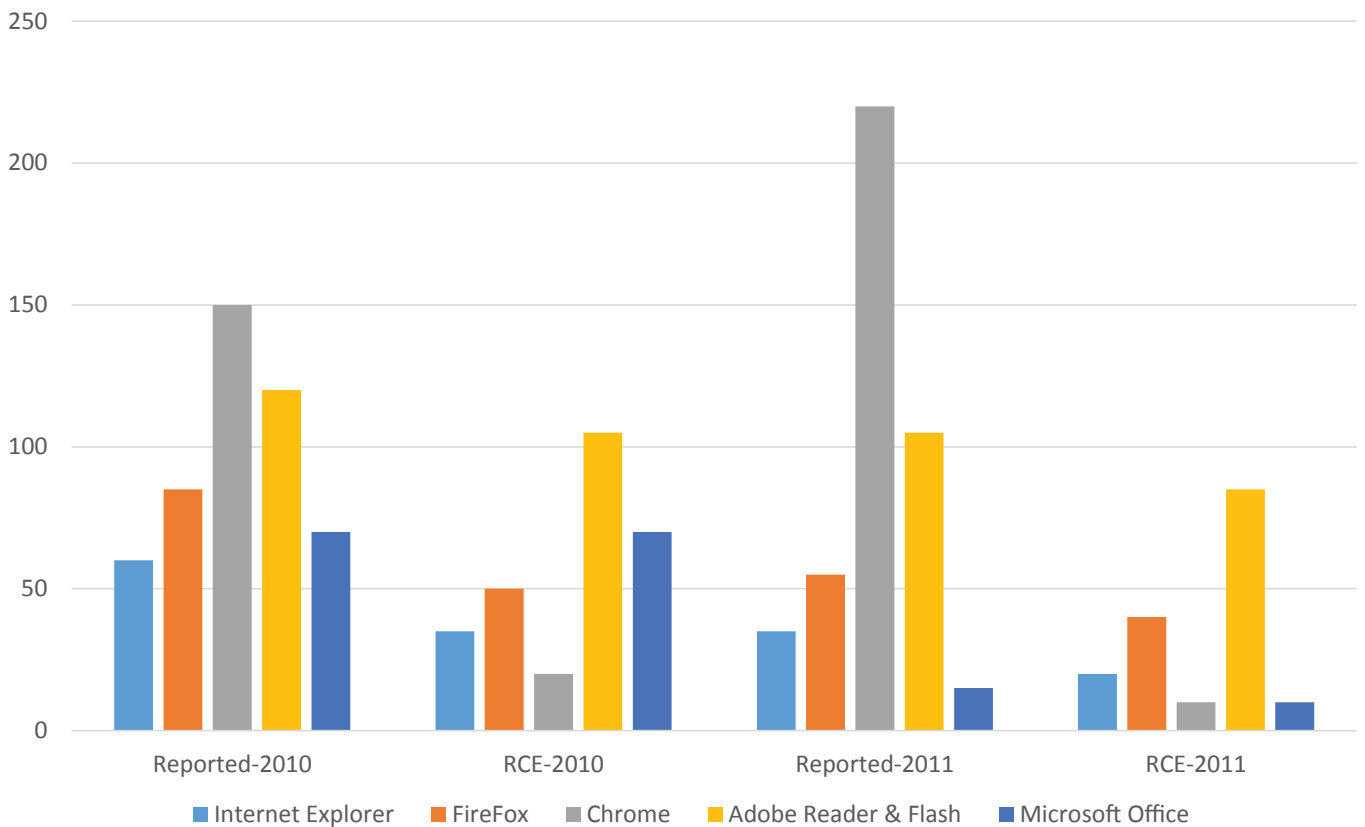
RISE OF WEB ATTACKS

- Rise of Web 2.0 has opened more opportunities for cybercriminals.
- Web Browser has become popular as an attack platform.
- Dozens of Browser Exploit Packs (BEP) are available in the underground community.
 - Eleonore, Phoenix, Zeus, SpyEye, IcePack, BlackHole, YES Exploit Pack, Crimepack, Neosploit ...
- Social Engineering techniques never die!

APPLICATION VULNERABILITIES

Vulnerability	Description	Affected versions
CVE-2009-0658	Adobe JBIG2Decode Memory Corruption Exploit	Adobe Reader 9.0
CVE-2011-0609	Adobe Flash Player AVM Bytecode Verification Vulnerability	Adobe Flash Player 10.2.152.33
CVE-2011-0611	Adobe Flash Player SWF Memory Corruption Vulnerability	Adobe Flash Player 10.2.153.1
CVE-2010-3971	IE CSS Recursive Import Use After Free	IE 6,7,8
CVE-2010-0806	IE DHTML Behaviors Use After Free	IE 6, 7
CVE-2009-1671	Java buffer overflows in the Deployment Toolkit ActiveX control in deploytk.dll	JRE 6 Update 13
CVE-2010-4452	Java Applet2ClassLoader Remote Code Execution Exploit	JRE 6 Update 23

Application Vulnerabilities

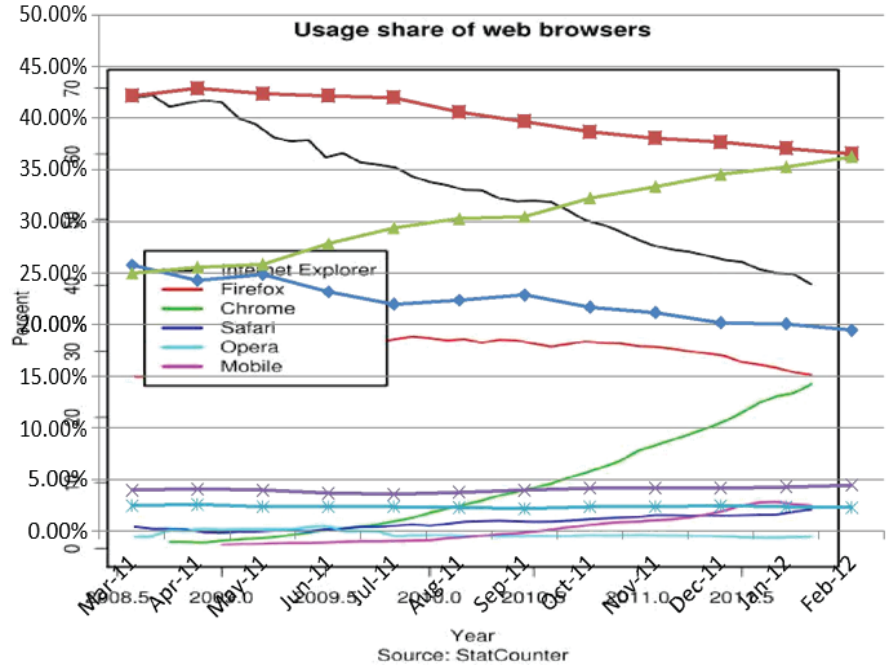


CVE - Common Vulnerabilities and Exposures, RCE - Remote Code Execution
Source: <http://cve.mitre.org>

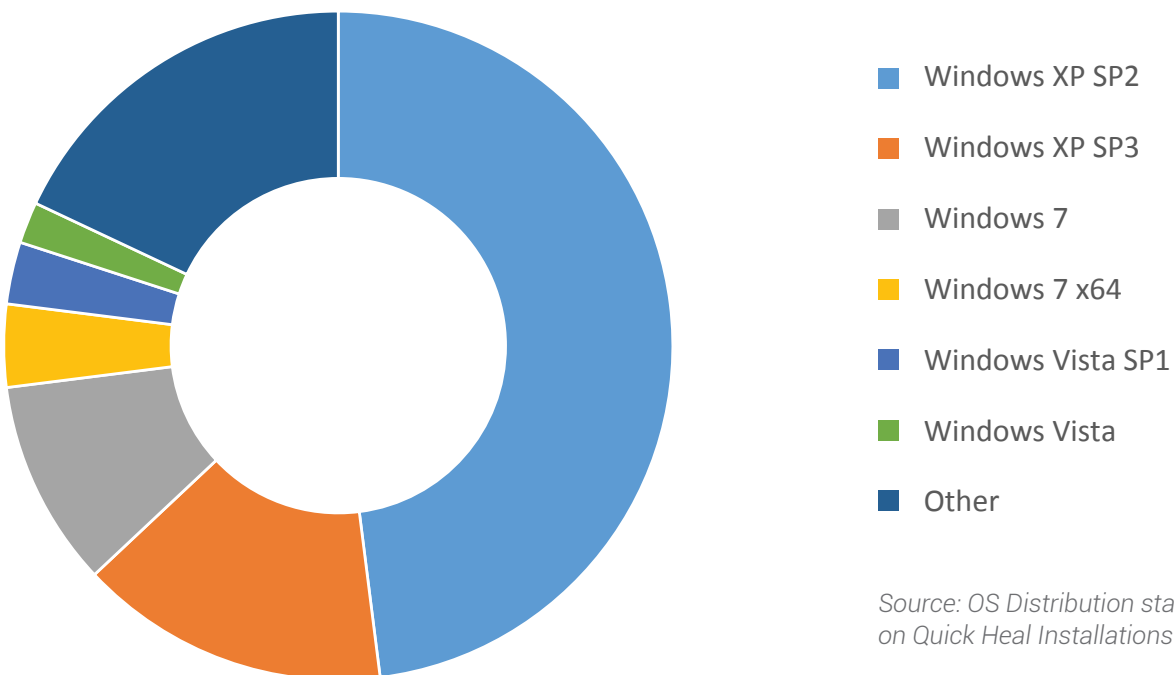
EXISTING PROTECTION MECHANISMS

- Phishing Protection
- Parental Control
- Firewall & IPS
- Pop-up Blocker
- URL Classification
 - Google Safe Browsing
 - SmartScreen Filter with Internet Explorer
- InPrivate Browsing with Microsoft Internet Explorer
- Protected Mode is supported on IE7+ on Windows Vista and above
- Firefox supports Private Browsing mode
- Google Chrome promises better security with Sandboxing
- Microsoft Office 2010 supports Protected Mode
- Adobe Reader X supports Sandboxing

WEB BROWSER STATISTICS



OPERATING SYSTEM DISTRIBUTION



Source: OS Distribution statistics based on Quick Heal Installations

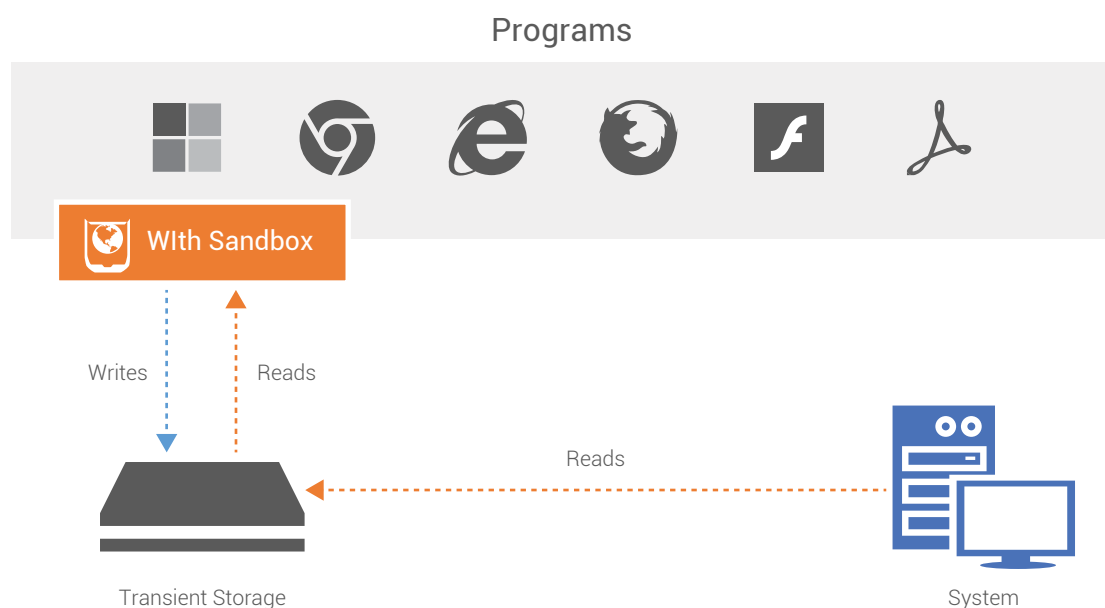
NEED FOR EFFECTIVE SANDBOX

- Protected Mode for Internet Explorer
 - Only supported on Windows Vista and above
- Update, Update, Update!
 - 65% users are using unpatched OS and Web Browsers
 - 60% users are using vulnerable Adobe versions
- Allows read access to all user files
 - Gap in privacy as data can be sent over the network
- Web browsers do not sandbox all their plugins
- Protection feature as default options
- Java and other third-party plugins are not sandboxed
- Social engineering techniques succeed in breaking depth of Security Layers!

Effective Sandbox needs to be designed, developed and tested by Security vendors!

WHAT IS SANDBOXING?

- Provides a restricted environment
 - To run vulnerable and untrusted applications while making it difficult for malware to damage the host operating system
- Isolates untrusted code
- Reduces attack surface
- Acts as containment for attacks that exploit application vulnerabilities



CHALLENGES

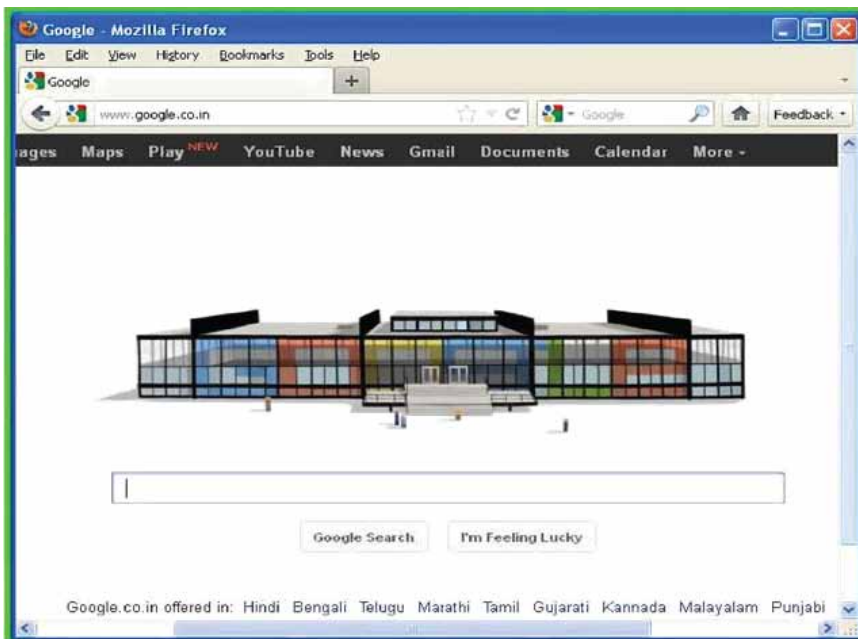
Compatibility

User
Experience

Security

Privacy

QUICK HEAL BROWSER SANDBOX



- Supported Web Browsers:
 - Internet Explorer, Firefox, Chrome
- Compatibility tests
 - Add-ons and toolbars
 - Email attachment download and upload
 - Social Networking Sites
- Security Testing
 - Shopping Sites
 - Banking Sites
 - Visiting Live Malicious URLs
 - Run Exploits using Metasploit

SANDBOX LIMITATIONS

- File system protection features requires NTFS i.e. FAT32 and USB volumes would remain unprotected
- Network access to Sandboxed applications is allowed
- Active exploits in a Sandboxed application will persist until the application is restarted

CONCLUSION

- Sandboxing is a positive step forward for better security
- Increases difficulty and possibility of exploitation
- Reduces the impact on an exploited system
- Effectively stops persistent threats
- Sandbox adds one extra layer of protection to **Quick Heal Web Security!**