

Web Browser Security
Chrome, Chromium & Firefox

Adil Gokturk, Rajinder Singh, Haseeb Rahman

Case Summary - Web Browsers

Google Chromium

Google Chrome

Firefox

Case Summary - Extensions

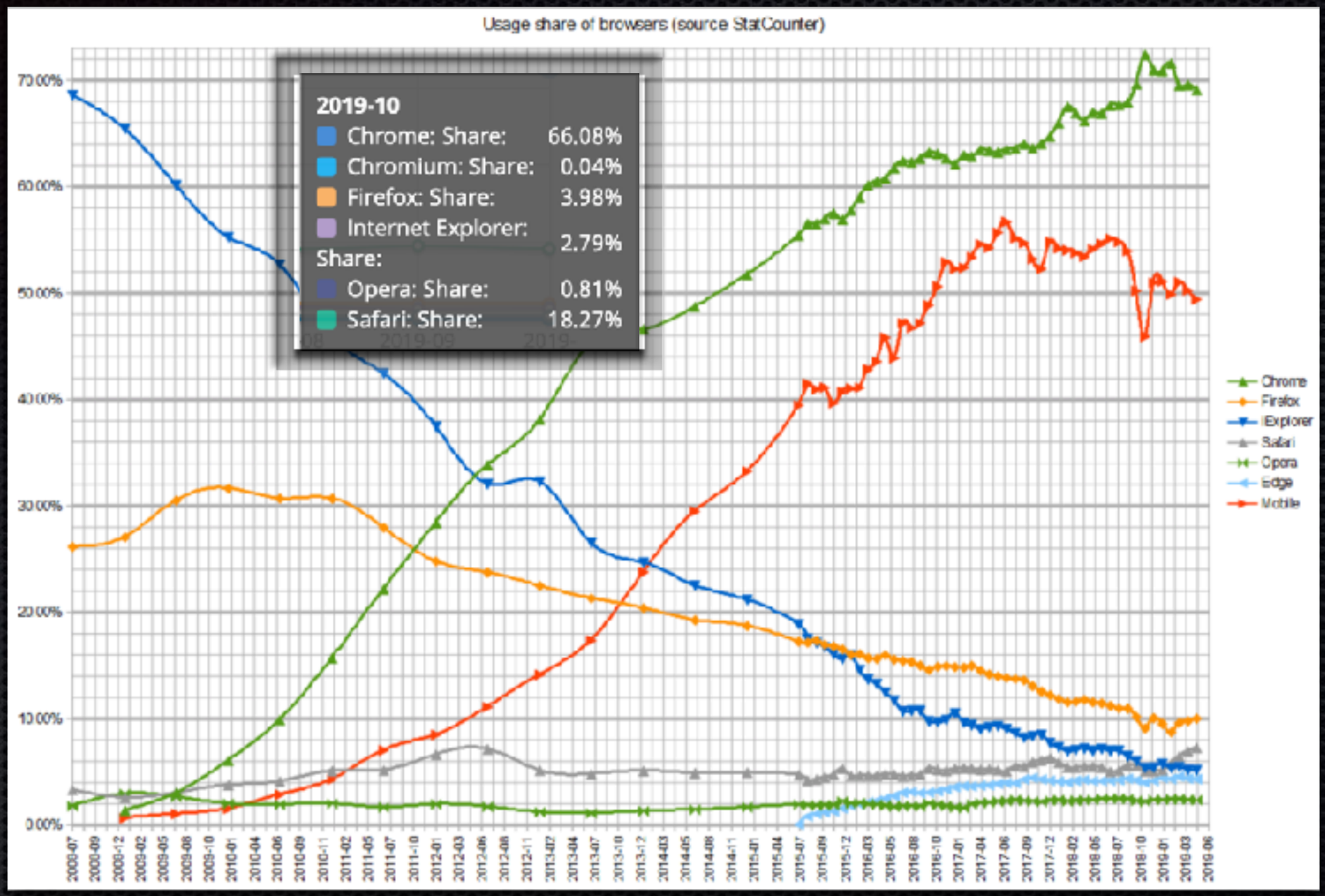
- Extensions:
  - Grammar
  - Evernote
  - Ad blockers
  - YouTube Downloader, etc
- Third party developers provide a set of additional functionalities
  - Malicious tasks:
    - Private information gathering
    - Browsing history retrieval
    - Passwords theft

Case Summary - Malicious Browser Extensions

- Malicious Attacks:
  - Phishing
  - Spying
  - DDoS
  - Email spamming
  - Affiliate fraud
  - Malicious advertising
  - Payment frauds etc.

Table 1. Malicious extension based attacks (statistics)

Extension (Year): Attack Type	Extension Description	Attack Description
HoverZoom (2013): Keylogging	Browse images on websites by hovering over without clicking	Collecting online form data and selling users' keystrokes.
Tweet This Page (2014): Content Injection	Tweet a Page	Turned into an ad-injecting machine; started hijacking Google searches.
BBC News Reader (2014): Spying	Get latest news and articles	Tracks user browsing data
Autocopy (2014): Spying	Select text and automatically copy to the clipboard	Sends a lot of user data back to its servers.
Hola Unblocker (2015): DDoS	Easy-access to region blocked content	Bandwidth from users of being sold to cover costs (powers botnets for attack)
Marauder's Map (2015): Spying	Plot your friends' location data from Facebook on a map	A hacker can know if you're not home, shops you visit frequently, who you spend most time with.
Viralands (2016): Phishing	"Verify your age" to access restricted content	Access to Facebook access token; login credentials stolen.
iCalc (2016): Webpage Manipulation	Functional Calculator	Creates a proxy and intercept web requests, taking commands and updates from a domain
Dubbed Copyfish (2017): Mal-Ads	Extract text from images, PDFs, videos	Equipped with ad injection capabilities.
Web Developer (2017): Affiliate Fraud	Adds a toolbar button to the browser with web developer tools	Substitute ads on browser, hijacking traffic from legit ad networks.



Usage Share of Web Browsers

https://statcounter.com

Google Chromium

- Free and Open - Source Fully functional Web Browser
- Developed by Google on September 2, 2008
- Current version: Chromium 789
  - running on
    - GNOME Shell and Ubuntu Linux
- Written in C, C++ and JavaScript
- Operating Systems
  - Windows
  - Mac OS X
    - Linux

Google Chromium - Extensions—Add-ons

accessibilityFeatures | alarms | automation | bookmarks | browserAction | browsingData | certificateProvider | commands | contentSettings | contextMenus | cookies | debugger | declarativeContent | declarativeNetRequest | declarativeWebRequestdesktopCapture | devtools.inspectedWindow | devtools.network | devtools.panels | documentScan | downloads | enterprise.deviceAttributes | enterprise.hardwarePlatform | enterprise.platformKeys | events | extension | extensionTypes | fileBrowserHandler | fileSystemProvider | fontSettings | gcm | history | i18n | identity | idle | input.ime | instanceID | management | networking.config | notifications | omnibox | pageAction | pageCapture | permissions | platformKeys | power | printerProvider | privacy | processes | proxy | runtime | sessions | signedInDevicesstorage | system.cpu | system.memory | system.storage | tabCapture | tabs | topSites | tts | ttsEngine | types | vpnProvider | wallpaper | webNavigation | webRequest | windows

Google Mail Checker extension

Chromium Threat models

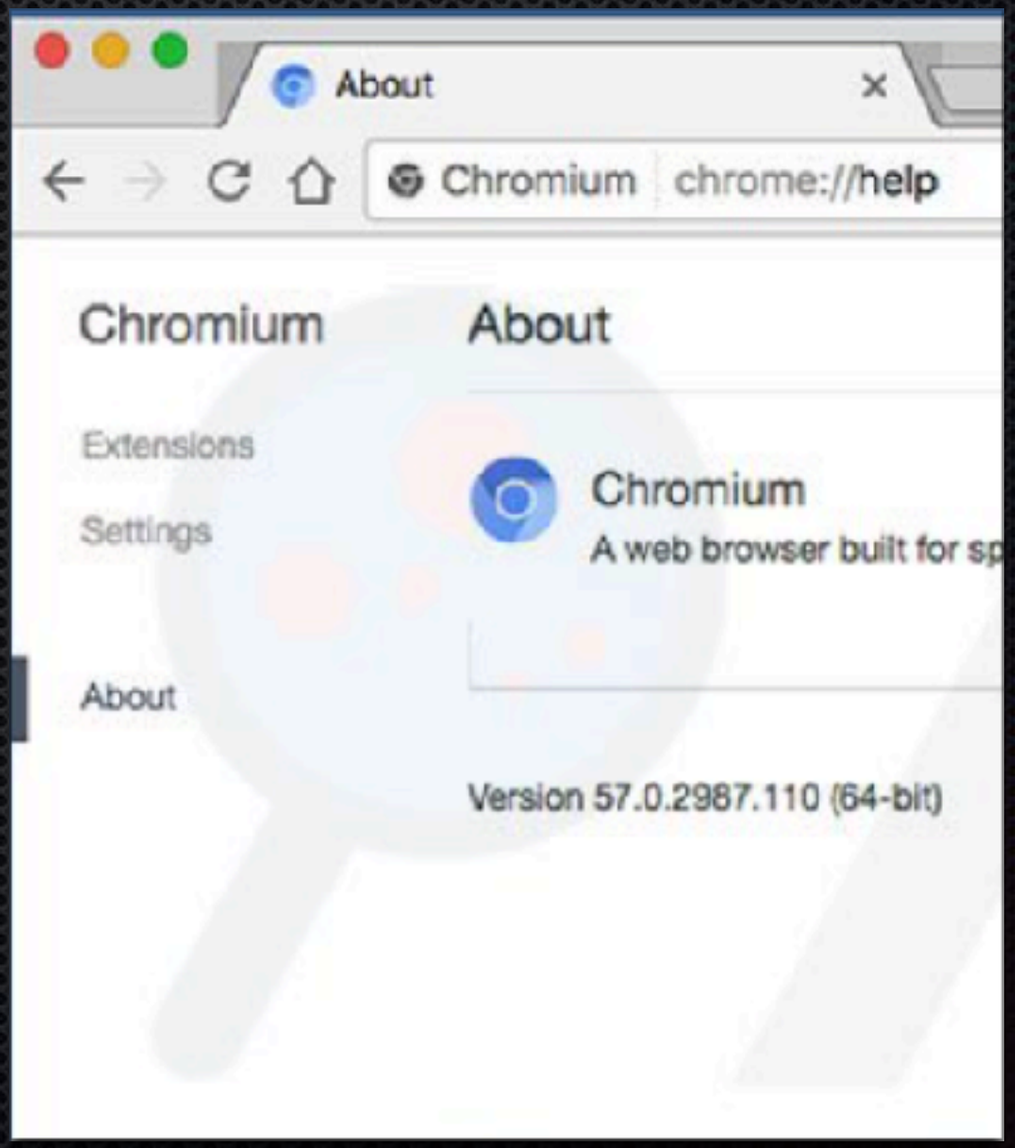
- An opportunistic adversary
- A dedicated adversary

Chromium - Mitigating Remote System Compromise

- A plugin, tricking the user into giving a malicious web app
  - **<u>Unwarranted access to HTML5/Extension APIs</u>**
- Trying to subvert our autoupdate process in order to get some malicious code onto the device.

Google Chromium
- Malicious Extensions and Behaviors

- Chromium's appearance barely differs from the Google Chrome
- Significant advantage for an attacker to exploit:
  - IP addresses
  - URLs visited
  - Pages viewed
  - Search queries



Google Chromium
- Malicious Extensions —a Rogue Chromium variant
How did Chromium install on a computer?

- Deceptive marketing method
- Bundling - stealth installation of third party applications together with regular free program

Google Chromium - Malicious Extensions —Chromium potentially unwanted application

- Threat Type
  - Mac Malware, Mac Virus
- Symtoms:
  - Mac became slower than normal, you see unwanted pop-up ads, you get redirected to shady websites.
  - Deceptive pop-up ads, free software installers (bundling), fake flash player installers, torrent file downloads.
- Damage:
  - Internet browsing tracking (potential privacy issues), displaying of unwanted ads, redirects to shady websites, loss of private information.
- Solution:
  - Eliminate and remove Chromium from the MAC
  - Scan it.

Google Chromium - Security Features - OS Hardening

- Process sandboxing
  - Mandatory access control implementation that limits resource, process, and kernel interactions
  - Control group device filtering and resource abuse constraint
  - Chrooting and process namespacing for reducing resource and cross-process attack surfaces
  - Media device interposition to reduce direct kernel interface access from Chromium browser and plugin processes
- Toolchain hardening to limit exploit reliability and success
  - NX, ASLR, stack cookies, etc
- Kernel hardening and configuration paring
- Additional file system restrictions
  - Read-only root partition
  - tmpfs-based /tmp
  - User home directories that can't have executables, privileged executables, or device nodes
- Longer term, additional system enhancements will be pursued, like driver sandboxing



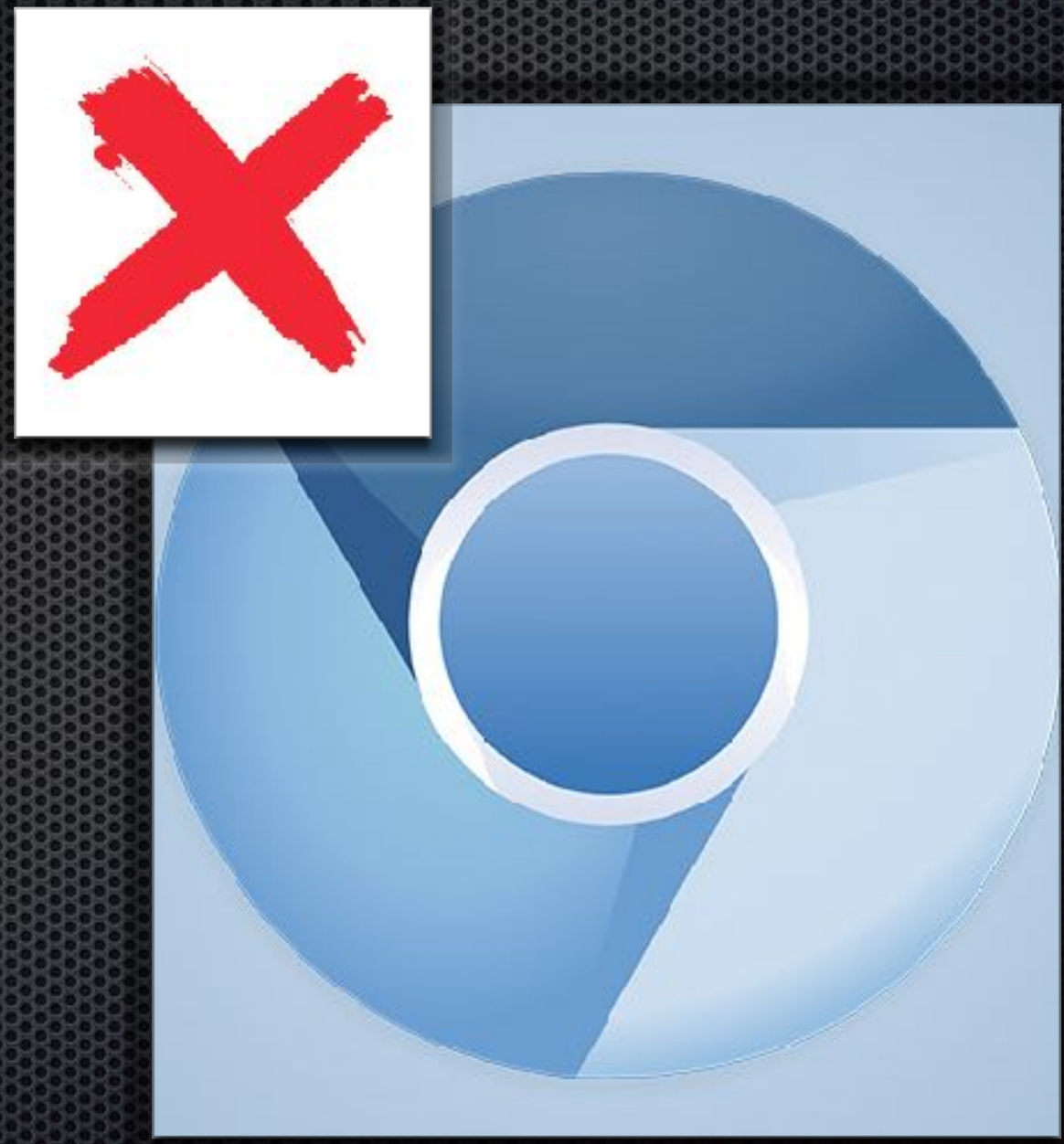
Google Chromium - Security Features

- Making the browser more modular
  - Plugins
  - Standalone network stack
  - Per-domain local storage
- Secure autoupdate
- Verified boot
  - Firmware-based verification
  - Kernel-based verification

Google Chromium - Pros

- An open-source fully functional browser
- Developed by Google
- Privacy:
  - Gives the user more privacy than Chrome
  - None of the data is sent to Google
- Update every 14-21 days

Google Chromium - Cons



- Security
- No Automatic Updates
- Relatively high malware threats
- Privacy
  - Unable to disable WebRTC
  - Vulnerable to WebRTC leaks

Google Chrome

- Is a web browser developed and maintained by Google, released in 2008.
- Uses the open web browser Chromium source code and adds a bunch of features developed by Google.
- It is available for Windows, Mac OS X, Linux, Android ad iOS operating systems.
- The Google Chrome browser takes a sandboxing-based approach to Web security. Each open website runs as its own process, which helps prevent malicious code on one page from affecting others.

Google Chrome

- In 2010, Google launched the Chrome Web Store, an online marketplace where users can buy and install Web-based applications to run inside the browser. These apps are available as either browser extensions or links to websites.
- **Differentiator to Chromium- Auto Updates, Chrome Web Store, Reopen the accidentally closed tabs, Restoring tabs after the unexpected exit or crash, Killing unresponsive web pages, Fixing up the corrupt chrome files without deleting the profile, Wipe the slate clean reset flags and default settings, Usage tracking, Crash reporting, Media Codec Support.**
- Seems to be best choice for security, based on a very good engine and has a history of getting new security patches applied the most quickly.

Google Chrome - Security Features

- **The Chromium security team** aims to provide Chrome and Chrome OS users with the most secure platform to navigate the web. Chromium is the open-source project behind Google Chrome.
- **Integrated sandbox** that reduces the impact of most common vulnerabilities, and is much stronger than approaches used by other browsers.
- Have **Site Isolation** to protect website data from compromised renderer processes and side channel attacks.
- Infrequent **critical security vulnerabilities** relatively compared to other browsers.
- Have **leading sandbox protection for the Adobe Flash plug-in.**
- Have **unique techniques** for significantly mitigating the security risks posed by plug-ins.
  - More powerful plug-in controls: Google Chrome now has the ability to disable individual plug-ins or to operate in a “domain whitelist” mode whereby only trusted domains are permitted to load plug-ins .
  - Autoupdate for Adobe Flash Player: By including Adobe Flash Player -- the most popular plug-in -- with Google Chrome, we can re-use Google Chrome’s powerful auto update strategy and minimize the window of risk for patched vulnerabilities.
- Have leading HTTPS security through features such as **mixed script blocking**.
- A “mixed scripting” vulnerability affects HTTPS websites that are improperly implemented; these vulnerabilities are serious because they eliminate most of the security protections afforded by HTTPS.

Google Chrome - Pros

- Google Chrome is a **simple web browser** that's easy to navigate, and it is one of the best options for Android users who want to access the internet on their cell phones and tablets.
- It is also compatible with Apple computers and mobile devices, which makes **Chrome versatile** and is the reason many prefer this internet browser.
- One of the **most secure web browsers** available. Does not allow harmful ransomware, Trojans and viruses to automatically download and it recognized and warned user about most phishing schemes.
- **Is much better in overall performance**. As you write, edit, save, and publish your work, the speed of the browser outperforms other browsers. It also loads articles faster.

Google Chrome - Cons

- This web browser is **a little bigger compared to other browsers.**
  - Need over a megabyte of space to download the program.
- New users who are used to something like Internet Explorer may need some time to adjust to not seeing menus and icons at the top of the browser.

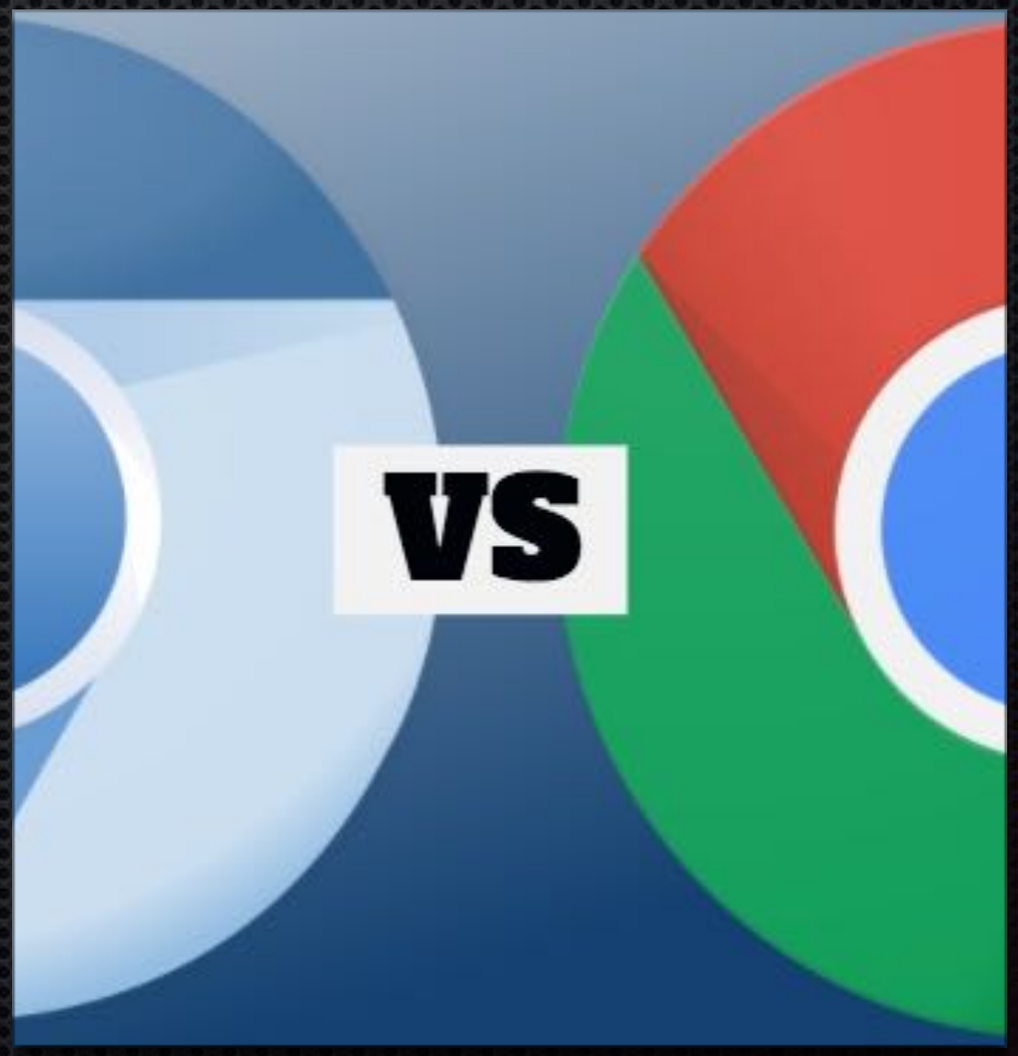
Google Chrome - Add-ons

- Google Chrome comes with **built-in security features – incognito mode** and **options to control data collection by various websites.** For additional security there are third-party Chrome security extensions.

- TweakPass- Secure Your Passwords While Browsing
- StopAllAds – Best Security Extension for Chrome
- Ghostery – Best Privacy Chrome Extension
- Adblock Plus – Block Intrusive Ads
- PureVPN – Browse Web Anonymously
- Blur – Protect Your Personal Informations
- TeamPassword- Manage Multiple Passwords
- Click&Clean – Secure PC from Online Threats

Google Chromium vs Chrome

- Which is better?
  - **Google Chrome is better** option for both Windows and MacOS since the software releases are more stable compared to Chromium.
  - Chromium is best Browser for the Linux, Ubuntu and other open-sources platform
- Conclusion
  - Chromium open source software are better than others because we can do a lot more customization in it. On the other hand, there are some basic features that are missing. Chrome have some the advantages like Auto update and Add-on which can increase productivity.
  - Finally, It **depends on the users** what kind of Operating system they are using.



Firefox

- The first name for the Browser was “Mozilla”
  - That was a slang term for “Mosaic Killer”
- The No. 1 Browser today is Internet Explorer with 65% of the Market. No. 2 is Firefox with just over 15%. The remainder of the market is highly fractured. Apple's Safari has only 1%.
- Firefox is the fastest growing browser software
- IRecently Google added Firefox to it's recommended list of free downloads

Firefox - Security

- Firefox doesn't allow the user to set the Security Level. The developers designed it for maximum security level
- Firefox uses Googles Blacklist of Phishing and Malware Sites
- permissions
- private browsing

Firefox - Pros & Cons

- Easy to use.
  - Takes some getting used to because some commands are a little different than Internet Explorer.
- Firefox complements Internet Explorer,
  - so you can keep them both on your desktop and use either one.
- Firefox doesn't render pictures quite as well as IE.
  - You can see a little graininess in some website pictures.
- There are innumerable Add-Ons that people have developed.

Firefox - Add-ons

- Firefox is an “Open Source” program which allows individuals to code and offer enhancements
- There are a large number of Add-ons offered for free on the internet, most of which have no value to you
- Many are fun to try and may be quite useful
- Examples are mapping tools, screensavers, etc.
- There is no oversight of Add-ons by Mozilla so some could create security leaks.
- Stay with Add-ons listed at Mozilla’s site
  - addons.mozilla.org/en-US/firefox/

Download and run the Lightbeam add-on in your Firefox browser.

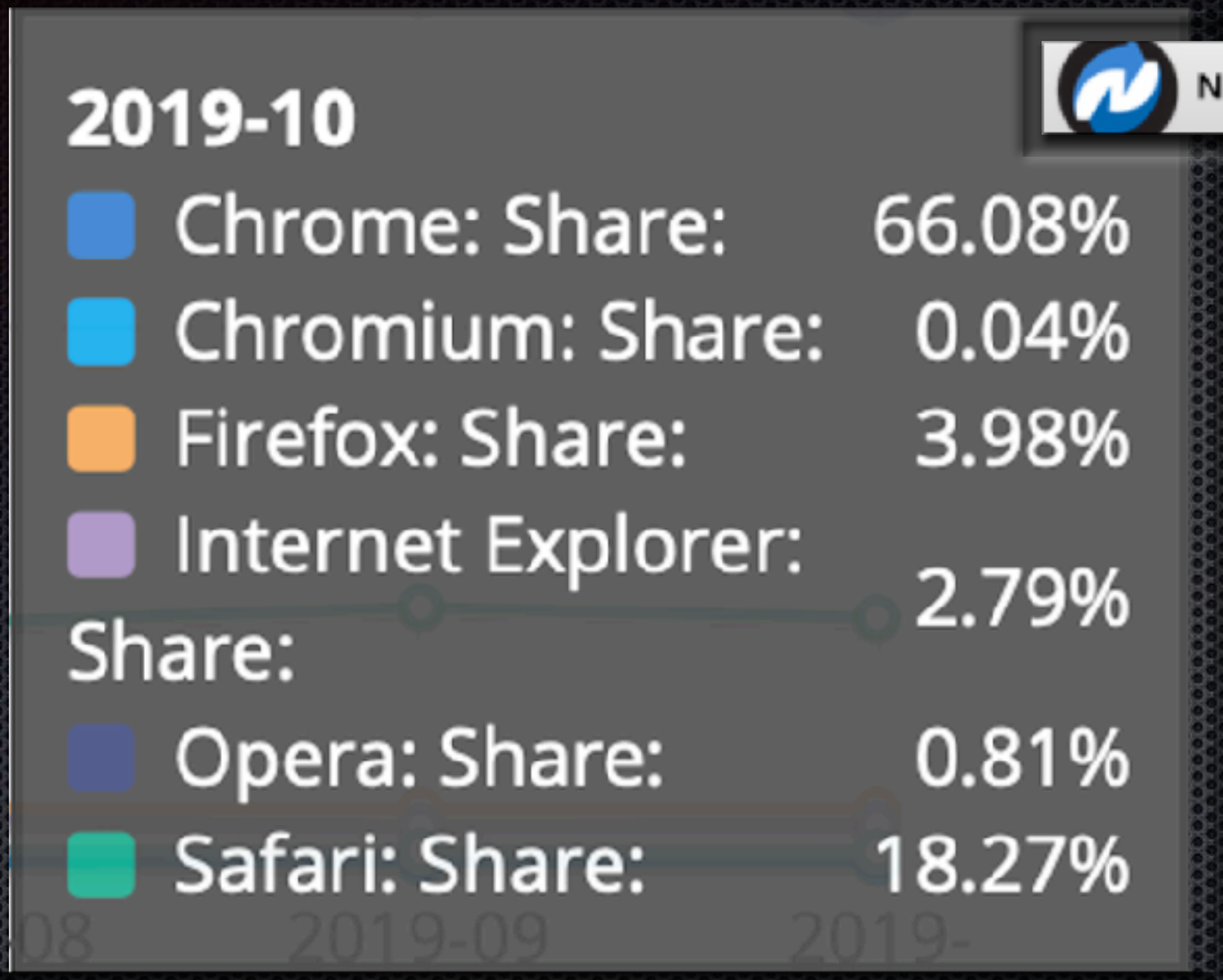
Lightbeam will create a record of events for every site you visit and every third party site that is stored locally on your browser.

Lightbeam visually graphs these events to highlight the interactions between sites you intentionally visit and the third parties.

Lightbeam will continue to add to your graph as you browse the Web. You can stop Lightbeam at any time by disabling it or uninstalling the add-on. Your Lightbeam data can be easily saved or deleted.

Lightbeam





netmarketshareAsofNovember2019

Investigation Facts - Browser Market Share

As of November 8, 2019

Investigation Facts - Browser Market Share

Browser Type	Market Share	Updates Frequency	Security Features	Security Plugins	Browser Extensions
Google Chrome	67.15%	15 days	Sandboxing Function	Yes	Yes
Google Chromium	0.12%	Continues Major and minor updates 14-21 days	Sandboxing Function	Yes	Yes
Mozilla Firefox	9.14%	15-28 days	Anti-tracking Browsing Mode	Yes	Yes

Investigation Facts - Browser Security Comparison

Security Features			
Market Share	67.15%	0.12%	9.14%
Sandboxing	Yes	Yes	Yes
Site Isolation	Yes	Yes	Yes
Private Browsing	Yes (Incognito mode)	Yes (Incognito mode)	Yes
Default Plug-ins	Yes	Yes	No
Netscape Plug-in Application Programming Interface (NPAPI)	No	No longer used by Native Client	Yes
Pepper plug-in API (PPAPI)	Yes	Yes	No
Autoupdate for Adobe Flash Player	Yes	Yes	Yes
Password accessible through browser	Yes	Yes	Yes
Master Password	No	No	Yes
Google Safe browsing	Yes	Yes	Yes
Updates Frequency	15 days	14-21 Days	15 – 28 days

Lesson Learned

- The current countermeasures are insufficient or erroneously implemented (Iskander Sanchez-Rola, 2017).
  - In particular, Sanchez-Rola argues that, a **time side-channel attack** against the access control settings used by the Chromium browser family .

Lesson Learned

- Chrome security features include anti-phishing and anti-malware that's built-in with the browser, which helps prevent users from being exposed to fraudulent websites.
- Its built-in plug-in system removes the necessity to install 3rd party plug-ins, reducing the risks of an attack.
- The default plug-ins and Sandboxing are the most influential security features as they prevent a large array of attack vectors without burdening the user in any way.
- Chrome still hasn't added the concept of master password and all the saved and synced data is tied to the Google account which is a concern as its acts as a single point of entry for accessing all that sensitive information.

Conclusion

- Despite continues updates and efforts non-of these browsers and their extensions—add-ons are 100% secure.
  - Sanchez-Rola argues that both Google Chrome and Chromium families are still open novel-time side-channel attack against the access control settings (Iskander Sanchez-Rola, 2017).
  - Firefox WebExtensions and Microsoft Edge follow the same API and design, proving that they may be prone to be vulnerable to the similar attacks (Iskander Sanchez-Rola, 2017).
- It would be good idea to research several different browsers before make a decision on your web browser preference.
- Download the software verified sources.
- Do necessary security perimeter adjustments regarding on your personalized preferences and needs.
- Keep the we browser and its extensions are updated
- Be careful when visiting a website, even clicking a link.

References - Adil Gokturk

- A. P. Sivanesan, A. Mathur and A. Y. Javaid, "A Google Chromium Browser Extension for Detecting XSS Attack in HTML5 Based Websites," 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, 2018, pp. 0302-0304.doi: 10.1109/EIT.2018.8500284 URL: http://ieeexplore.ieee.org.libezproxy2.syr.edu/stamp/stamp.jsp?tp=&arnumber=8500284&isnumber=8500077
- Caleb. (2019, https://www.expressvpn.com/blog/best-browsers-for-privacy/). Ranked: Security and privacy for the most popular web browsers in 2019. Retrieved from https://www.expressvpn.com/blog/best-browsers-for-privacy/
- Chromium (Producer). (2019). The Chromium Projects. Retrieved from http://www.chromium.org/chromium-os/chromiumos-design-docs/security-overview#Secure_Autoupdate_514579947008_3042258492955804
- Iskander Sanchez-Rola, I. S., Davide Balzarotti. (August 16–18, 2017). Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies. Paper presented at the 26th USENIX Security Symposium, Vancouver, BC, Canada. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-sanchez-rola.pdf
- Khan, Z. H. (2019). Evaluating Popular Web Browsers in Terms of Security and Privacy. Retrieved December 7, 2019 https://readwrite.com/2019/03/29/evaluating-popular-web-browsers-in-terms-of-security-and-privacy/
- N. Mazher, I. Ashraf and A. Altaf, "Which web browser work best for detecting phishing," 2013 5th International Conference on Information and Communication Technologies, Karachi, 2013, pp. 1-5. doi: 10.1109/ICICT.2013.6732784 URL: http://ieeexplore.ieee.org.libezproxy2.syr.edu/stamp/stamp.jsp?tp=&arnumber=6732784&isnumber=6732770
- Net Marketshare, October, 2019 market share reports are now live. Retrieved December 8, 2019 URL: https://netmarketshare.com/browser-market-share.aspx?options=%7B%22filter%22%3A%7B%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22browser%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22browsersDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222018-11%22%2C%22dateEnd%22%3A%222019-10%22%2C%22plotKeys%22%3A%5B%7B%22browser%22%3A%22Firefox%22%7D%2C%7B%22browser%22%3A%22Internet%20Explorer%22%7D%2C%7B%22browser%22%3A%22Opera%22%7D%2C%7B%22browser%22%3A%22Chromium%22%7D%2C%7B%22browser%22%3A%22Safari%22%7D%2C%7B%22browser%22%3A%22Chrome%22%7D%5D%2C%22pageLength%22%3A25%2C%22segments%22%3A%22-1000%22%7D
- Varshney, G., Bagade, S., & Sinha, S. (2018, 10-12 Jan. 2018). Malicious browser extensions: A growing threat: A case study on Google Chrome: Ongoing work in progress. Paper presented at the 2018 International Conference on Information Networking (ICOIN).

References - Rajinder Singh

- What Is The Difference Between Google Chrome And Chromium Browser?
  - By Aditya Tiwari - March 28, 2018, https://fossbytes.com/difference-google-chrome-vs-chromium-browser/
- Chromium vs. Google Chrome
  - https://www.diffen.com/difference/Chromium_vs_Google_Chrome

References - Haseeb Rahman

- Cameron, B (Minister for Corrections, Victoria) 2017 https://expandedramblings.com/index.php/firefox-statistics/10 Interesting Firefox Statistics and Facts (2019) | By the NumbersHere are a few of the most interesting Firefox statistics I was able to dig up. As always, be sure to check back in the future as I will be updating this post as new and updated stats become available.expandedramblings.com, Victoria, 28 March,
viewed 16 April 2017, <http://www.dpc.vic.gov.au>.

- Khan, Z. H. (2019). Evaluating Popular Web Browsers in Terms of Security and Privacy. Retrieved December 7, 2019 https:// readwrite.com/2019/03/29/evaluating-popular-web-browsers-in-terms-of-security-and-privacy/

- Douglas, N, Douglas, G & Derrett, R (eds) 2018, Browsers that are the furture, John Wiley & Sons, Brisbane, Qld.

- Farley, J 2018, 'The role of browsers in today's society, Conservation Information Security, vol. 22, no. 6, pp. 1399-1408.

- Guidebook to Firefox extensions CCH Australia, North Ryde, NSW.

- Hatch, JA 2018, Mozilla Firefox turns 10, State University of New York, Albany.

“Any Questions.”

Thank you!

–Adil Gokturk, Rajinder Singh, Haseeb Rahman