www.vektort13.pro

Угроза – Mozilla 51 ft. WebGL 2.0

То, что раньше было доступно лишь в версиях Mozilla Nightly теперь доступно каждому пользователю, и не только доступно но и напрямую угрожает безопасности пользователя.

WebGL 2.0 на основе технологии OpenGL ES 3.0 – вот имя новой угрозы анонимности каждого пользователя. Технология, которая позволит намного лучше и красочнее обрабатывать 3Д объекты в нашем браузере так-же будет получать информацию о нашей системе.

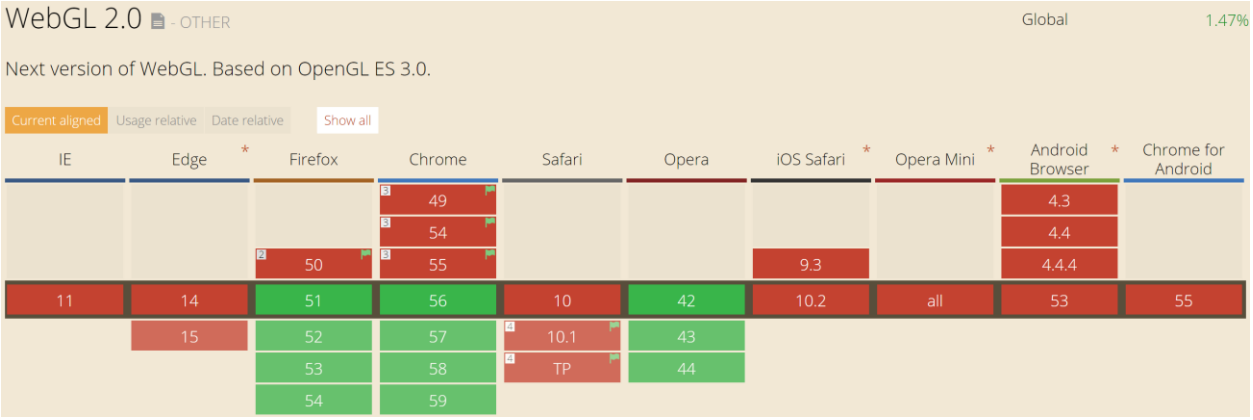
WebGL Support Detection :

This browser supports WebGL	✓ True
This browser supports WebGL 2	✓ True (88 of 88 new functions implemented) more

WebGL Context Info :

Supported Context Name(s)	**webgl2**, webgl, experimental-webgl
GL Version	WebGL 2.0
Shading Language Version	WebGL GLSL ES 3.00
Vendor	Mozilla
Renderer	Mozilla
Antialiasing	True
ANGLE	True, Direct3D 11
Major Performance Caveat	False

Помимо нововведения в виде WebGL 2.0 добавлена была технология FLAC audio codec.



К сожалению с каждым днем Mozilla превращается из гибкого многофункционального инструмента в некое подобие других браузеров, которые в первую очередь сконцентрированы на получении прибыли.

СМИ:
https://hacks.mozilla.org/2017/01/webgl-2-lands-in-firefox/
http://caniuse.com/#feat=webgl2

Техническая документация:
https://developer.mozilla.org/ru/docs/Web/API/WebGL2RenderingContext

Тесты:
https://browserleaks.com/webgl

Защита:
Для защиты от технологии снятия отпечатка WebGL пользователю необходимо отключить JavaScript в своем браузере.

Подмена:
Для подмены рекомендуется использовать софт vGPU или более старые версии браузеров.

Угроза – Canvas

Элемент Canvas используется для отрисовки графики на странице. Используется сайтами по назначению довольно редко, а для отслеживания - часто.

За счёт того, что отрисовка объектов в разных системах и в разных библиотеках (браузерах) немного различается, сайт может получить дополнительную информацию, позволяющую вас дополнительно идентифицировать, возможно, из нескольких сотен или даже тысяч пользователей.

СМИ:

https://habrahabr.ru/post/230679/
http://www.pcworld.com/article/2458280/canvas-fingerprinting-tracking-is-sneaky-but-easy-to-halt.html

Техническая документация:

https://en.wikipedia.org/wiki/Canvas_fingerprinting

Тесты:

https://browserleaks.com/canvas

Защита:

Отключить Canvas в браузере вручную или воспользоваться плагинами для отключения.

Подмена:

Для подмены можно воспользоваться либо vGPU либо расширением для браузера Mozilla:
https://vektort13.pro/useragent.xpi
Сайт автора плагина - http://fxprivacy.8vs.ru/

Угроза – Font Fingerprint

Стандартная технология четкое время появления которой доподлинно неизвестно, однако благодаря своей простоте и эффективности технология снятия отпечатка шрифтов нашла свое применение практически во всех крупных антифрод компаниях. Как нетрудно догадаться из названия данная технология получает список шрифтов установленных на ПК пользователя.
Разработчики Mozilla Firefox официально заявили, что в версии Mozilla 52 будет встроена защита от данной технологии, однако для тех кто пытается осуществить подмену данного отпечатка, это скорее всего будет печальной новостью.
http://news.thewindowsclub.com/firefox-52-font-fingerprinting-protection-87818/

СМИ:

https://blues.cs.berkeley.edu/blog/2015/01/21/fingerprinting-web-users-through-font-metrics-fc-15/

Техническая документация:

http://fc15.ifca.ai/preproceedings/paper_83.pdf

Тесты:

https://browserleaks.com/fonts

Защита:

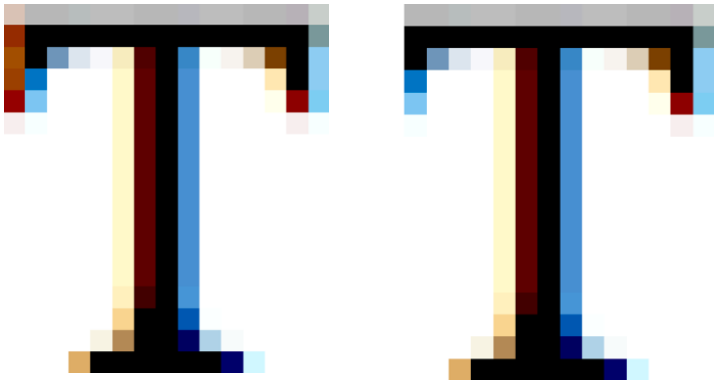
Для защиты от технологии снятия отпечатка шрифтов пользователю необходимо отключить Adobe Flash и JavaScript в своем браузере.

Подмена:

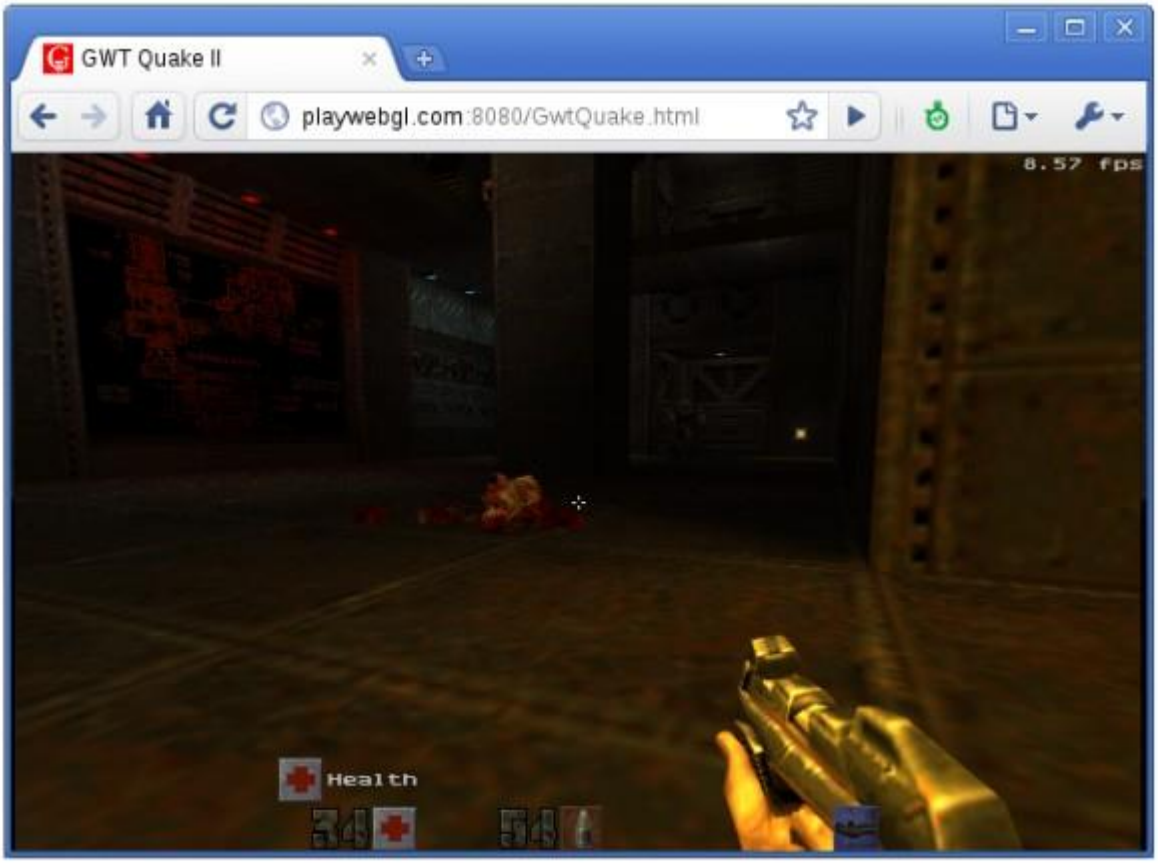
Для подмены установить новые или удалить старые имеющиеся в системе шрифты либо расширением для браузера Mozilla:
https://vektort13.pro/useragent.xpi
Сайт автора плагина - http://fxprivacy.8vs.ru/

Угроза – WebGL

WebGL это контекст элемента Canvas, который отвечает за ускорение и работу с графикой. Различные видеокарты, их драйвера и операционные системы обрабатывают графику по разному и если в обычном Canvas нам предоставляют простую графику, типа:



то при использовании WebGL графические элементы становятся намного сложнее:



В своей работе, как и большинство других элементов направленных на взаимодействие с пользователем WebGL основываеться на

JavaScript. Для анонимности пользователя WebGL несет угрозу не только как крайне опасный элемент для осуществления атак на пользователя:
http://www.cyberstyle.ru/newsline/11067-microsoft-webgl-directx-technet-chronos-group.html
но так-же и как элемент который имеет свои уникальные отпечатки, а так-же сообщает информацию о видеокарте пользователя.

СМИ:
http://freebrowsers.ru/technology/webgl

Техническая документация:
https://www.khronos.org/files/webgl/webgl-reference-card-1_0.pdf
https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf
http://www.reedbushey.com/85Webgl%20Up%20and%20Running.pdf

Тесты:
https://browserleaks.com/webgl

Защита:
Отключить WebGL в браузере вручную или воспользоваться плагинами для отключения.

Подмена:
Для подмены можно воспользоваться либо vGPU либо расширением для браузера Mozilla:
https://vektort13.pro/useragent.xpi

Сайт автора плагина - http://fxprivacy.8vs.ru/

Угроза – Generic Headers Signature

Каждый браузер уникален, а если быть точнее каждая платформа браузера уникальна. По анализу совокупности факторов получаемых сайтом с помощью технологий JavaScript и CSS можно определить с большой долей вероятности какой браузер использует пользователь, или же определить его подмену в случае применения каких-либо программных средств защиты.

Техническая документация:

http://people.scs.carleton.ca/~paulv/papers/acsac2016-device-fingerprinting.pdf

Тесты:

http://codepen.io/run-time/pen/XJNXWV
http://ip-check.info/?lang=en

Защита:

Отключение CSS и Javascript

Подмена:

Для подмены подписи браузера пользователю необходимо либо воспользоваться сторонними плагинами, например – BeeFree либо использовать Request Proxy.

Угроза – Графический движок браузера

Это и есть самая главная часть любого веб браузера, его сердце и мозг. Графический движок отображает на экране содержимое запрашиваемого ресурса.

Именно эта часть браузера анализирует полученный HTML или XML, при этом учитывает влияние CSS и Javascript, а так же других объектов, расположенных на веб странице (например, изображения или flash). На основе всех этих данных, движок создает макет (разметку) страницы, который видит пользователь на экране.

Ключевыми компонентами графического движка являются HTML и CSS парсеры — сложные программные комплексы, поскольку они позволяет графическому движку отобразить документ даже при наличии ошибок в HTML и CSS.

Самые распространенные движки браузеров на сегодня:

Trident — Internet Explorer;

Gecko — браузеры Mozilla;

Webkit — Chrome, Safari;

Presto — Opera.

СМИ:

http://browsermania.ru/engine

Техническая документация:

http://grosskurth.ca/papers/browser-archevol-20060619.pdf

Тесты:

https://audiofingerprint.openwpm.com/

VEKTOR T13

АНОНИМНОСТЬ И БЕЗОПАСНОСТЬ В СЕТИ

- Настройка защищенного и анонимного удаленного рабочего места.
- Поднятие своего VPN на моих или ваших серверах.
- Поднятие своего VOIP на моих или ваших серверах.
- Поднятие своего Jabber на моих или ваших серверах.
- Поднятие Email на моих или ваших серверах.
- Поднятие облачного хранилища на моих или ваших серверах.

Стоимость: уточняйте у саппорта.

jabber help@VektorT13.pro | telegram @VektorT13_pro
mail help@VektorT13.pro | skype VektorT13.pro