Malicious Recommendations 

By .sh aka @fkshell

@fuckwebsec 

NORTH PALMYRA
INTELLIGENCE GUILD

В чем плюсы?

Что получает клиент?

> персонализированный экспириенс

>> адаптивность ресурса под конкретный браузер

Что получает хостер?

> анализ действий посетителей

> эффективный маркетинг

> продвижение

Как это работает

Тег Google Аналитики

> как подключить на сайт >>тык<<

```
<!-- Google Analytics -->
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','https://www.google-analytics.com/analytics.js','ga');

ga('create', 'UA-XXXXX-Y', 'auto');
ga('send', 'pageview');
</script>
<!-- End Google Analytics -->
```

Yandex

Тег Яндекс Метрики

```
<script type="text/javascript">
(function(m,e,t,r,i,k,a){m[i]=m[i]||function(){(m[i].a=m[i].a||[]).push(arguments)};
m[i].l=1*new Date();k=e.createElement(t),a=e.getElementsByTagName(t)[0],k.async=1,k.src=r
,a.parentNode.insertBefore(k,a)})
(window, document, "script", "https://mc.yandex.ru/metrika/tag.js", "ym");

ym(XXXXXX, "init", {<параметры инициализации>});
</script>
```

Почему понять как работает скрипт сложно?

>обфускация кода

> Что происходит согласно документации

Файл устанавливает специфичные файлы cookie на домен, к которому подключается с помощью тега

Куки 🍪

HTTP cookie (web cookie, куки браузера) - это небольшой фрагмент данных, который сервер отправляет браузеру пользователя.

Для чего нужны куки метрик

- различать уникальных пользователей
- ограничивать частоту запросов
- запомнить число и время предыдущих посещений
- записать источник трафика
- определить начало и конец сеанса

…

Сбор данных

REFERER

>из поиска

>ввел ссылку в браузере

>перешел по ссылке с другого сайта

Действия внутри домена

>клики мышкой

>движение курсора

>ссылки и якоря по которым переходит пользователь

>время проводимое на ресурсе

>начало и конец сеанса

Данные пользователя

>локаль

>время

>геопозиция

>харакетеристики девайса

> ОС и ее версия

>браузер и его версия

>высота и ширина экрана

Идентификация Yandex

название	срок действия	описание	домен, на который устанавливается
_ym_uid	1 год	позволяет различать посетителей	домен, на котором установлен счетчик

> Яндекс Метрика автоматически присваивает ClientID каждому уникальному посетителю сайта.

> Этот идентификатор — анонимный: он создается случайным образом и определяет браузер

> в котором посетитель просматривает сайт.

Идентификация Google

название	срок действия	описание	домен, на который устанавливается
_ga	2 года	позволяет различать посетителей	домен, на котором установлен счетчик

> Чтобы сообщить Google Analytics, что два обращения относятся к одному и тому же

> пользователю, вместе с каждым из этих обращений в поле clientId отправляется

> уникальный идентификатор.

> Он генерируется случайным образом.

Google

Request

Pretty | Raw | Hex | Hackvertor

```
1  GET /start HTTP/2
2  Host: test.domain.com
3  Cookie: _ga=GA1.3.224669696.1696300277
4  Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
5  Accept: application/json, text/javascript
6  Content-Type: application/x-www-form-urlencoded
7  X-Requested-With: XMLHttpRequest
8  Sec-Ch-Ua-Mobile: ?0
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132
   Safari/537.36
10 Sec-Ch-Ua-Platform: "macOS"
11 Origin: https://www.daraz.com.np
12 Sec-Fetch-Site: same-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://www.daraz.com.np/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
```

Yandex

Request

Pretty | Raw | Hex | Hackvertor

```
1  GET /start HTTP/1.1
2  Host: domain.test.com
3  Cookie: _ym_uid=1690810991995178587
4  Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
5  Sec-Ch-Ua-Mobile: ?0
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.63
   Safari/537.36
7  Sec-Ch-Ua-Platform: "macOS"
8  Accept: */*
9  Sec-Fetch-Site: none
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
14 Connection: close
```

Другие куки

* нажми на тык чтобы узнать больше об устанавливаемых куки

>>тык<<

_gat	1 минута	ограничивает частоту запросов
AMP_TOKEN	от 30 секунд до 1 года	содержит токен, с помощью которого можно получить Client ID от сервиса AMP
gac<property-id>	90 дней	содержит информацию о кампании для пользователя
…	…	…

>>тык<<

_ym_isad	2 дня	используется для определения наличия у посетителя блокировщиков рекламы
_ym_d	1 год	хранит дату первого визита посетителя на сайт
_ym_hostIndex	1 сутки	позволяет ограничить количество запросов
ymex	1 год	хранит вспомогательную информацию для работы метрики
usst	1 год	хранит вспомогательную информацию для синхронизации идентификаторов посетителей между разными доменами Яндекса
…	…	…

Атрибуты безопасности

Name	Value	HttpOnly	Secure
_ga	GA1.3.1652678156.1675634651		

На такие куки не принято выставлять атрибуты безопасности (Secure и HttpOnly)

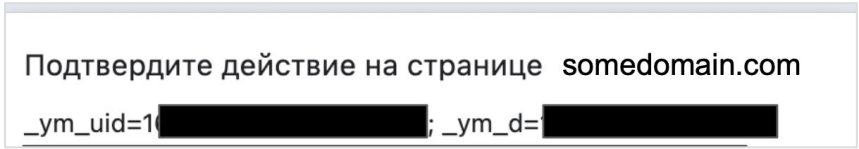
> secure куки отсылаются на сервер только тогда, когда запрос отправляется по протоколу SSL и HTTPS

> куки HttpOnly не доступны из JavaScript через свойство document.cookie API, что помогает избежать межсайтового скриптинга (XSS)

XSS

Файлы cookie могут быть украдены с помощью вредоносного JavaScript кода

*если ресурс уязвим к XSS



вывод значений куки с помощью alert(document.cookie)

XSS

При удачном обходе защиты файлов cookie от передачи их на сторонний домен их можно отправить с помощью примерно такого пэйлоада:

Импакт

Privacy Violation

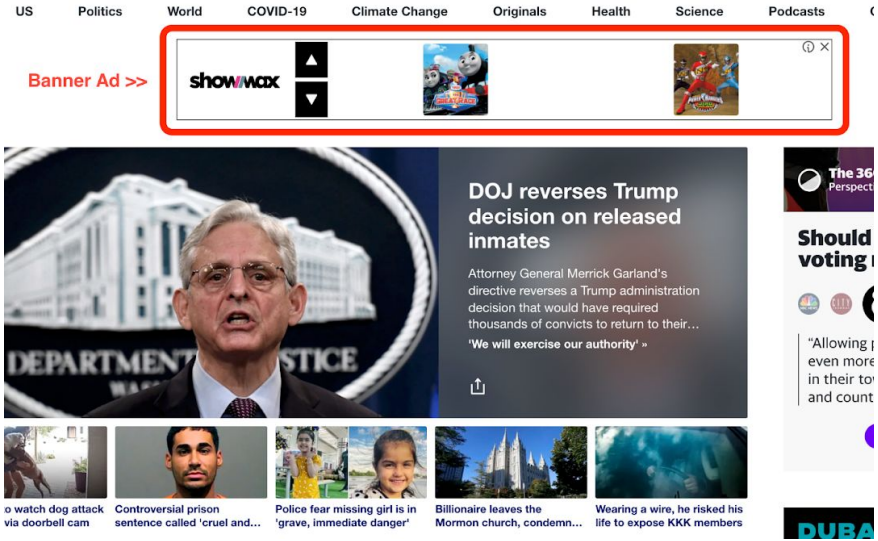
_gac_*

Summary

Cookie is used by:	Google Ads
The functionality is:	**to** store and track audience reach.
The purpose is:	Marketing

ℹ Expiration period: 90 days

> использовать значение `_gac_*` cookie для получения персонализированной рекламы



Уязвимости в аналитике и метрике

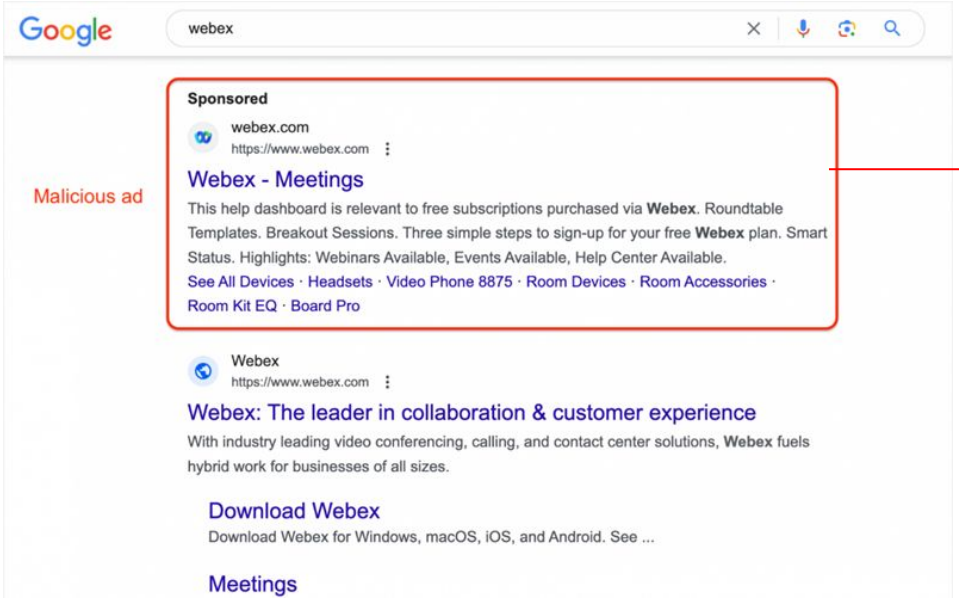
Вообще по сути файлы аналитики это библиотеки, написанные на JavaScript, поэтому они тоже могут быть уязвимы:

> CVE для Google Analytics

> CVE для Yandex Metrics

SEO Poisoning

> злоумышленник создает вредоносный веб-сайт и используют механизмы SEO для повышения их рейтинга и отображения в числе первых результатов поиска



ссылка на загрузку вредоносного ПО

больше об инциденте можно прочитать [>>тут<<]

Google converse

Картинки | Покупки | 2023 | Api | Online | One Star | All Star | Новости | Chuck 70

Результатов: примерно 528 000 000 (0,48 сек.)

Результаты: **Москва** · Изменить регион

кеды «Конверс
https://moscow-converse.ru

Кеды CONVERSE (Конверс) купить в Москве ...

Оригинальные кеды Конверс официальном интернет-магазине, **Converse** All Star купить в Москве дешево, быстрая и бесплатная доставка при покупке двух пар.
Converse интернет магазин · Converse на высокой подошве · Converse Dior

SCAM

Street Beat
https://street-beat.ru › cat › converse

Продажа и цены на Converse в магазинах Street Beat

Покупайте оригинальные кеды **Converse** из последних коллекций в Сети фирменных магазинов Street Beat. Заказывайте с доставкой по всей России.
Кеды · Женщинам · Розовые товары Converse... · Женские кеды Converse...

Converse
https://www.converse.com

Converse Official Site. Converse.com

Shop **Converse**.com for shoes, clothing, gear and the latest collaboration. Find Classic Chuck, Chuck 70, One Star, Jack Purcell & More.
Converse Color · Boys' Converse · Girls Converse · Converse Pride

Почему так происходит

BlackHat SEO

техники:

> **Keyword stuffing** - наполнение текста веб-страницы ключевыми словами, чтобы ввести в заблуждение алгоритмы поисковых систем и заставить веб-сайт получить более высокий рейтинг

> **Cloaking** - предоставление сканерам поисковых систем материала, отличного от того, что отображается пользователю при нажатии на ссылку

> **Манипулирование рейтингом** - искусственное увеличение рейтинга кликов веб-сайта для повышения его рейтинга в поисковых системах

> ранжирование

>> более точно подходит под поисковой запрос (наличие ключевых слов в странице)

>> авторитетность источника

>>> наличие бэклинков

>>> SSL-сертификат

>> индексация

>> адаптивная вёрстка

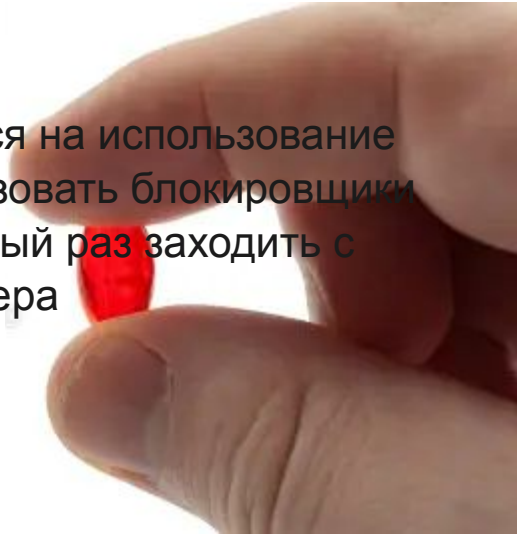
** учитывается локаль, геопозиция и остальные персональные характеристики, поэтому атака может быть также и узконаправленной

А че делать

Ваш user experience может быть либо удобным либо безопасным

забить

не соглашаться на использование cookie использовать блокировщики рекламы каждый раз заходить с чистого браузера



Коллектив Северной Пальмиры
Сообщество специалистов в сфере OSINT

<- Хочешь сделать доклад? напиши им! ->

«Schwarz_osint»
Энтузиаст, проказник,
Шалопай.
Специалист в сфере
Open Source Intelligence