

BEC 10.24.23

- Link from Travis sent to employees at Rea

```
(https://)sabrelifeorg(.)com/user_authentication.php(?)
674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418
```

- lookup.icann.org information below reveals the domain was registered 2023-10-18, 6 days ago

ICANN | LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

sabrelifeorg.com

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

The client was unable to process information from the Registrar RDAP server. The information below is shown as provided by the TLD Registry RDAP service.

Domain Information

Name: SABRELIFEORG.COM

Registry Domain ID: 2822747788_DOMAIN_COM-VRSN

Domain Status:
[clientTransferProhibited](#)

Nameservers:
BARBARA.NS.CLOUDFLARE.COM
KIP.NS.CLOUDFLARE.COM

Dates

Registry Expiration: 2024-10-18 17:43:14 UTC

Updated: 2023-10-18 18:17:40 UTC

Created: 2023-10-18 17:43:14 UTC

- Dig TLD sabrelifeorg.com reveals 2 ips associated with it

```
boost@SCMODS:~$ dig +short A sabrelifeorg.com
172.67.147.217
104.21.57.168
```

```

boost@SCMODS:~$ dig A sabrelifeorg.com
;; communications error to 127.0.0.53#53: timed out

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> A sabrelifeorg.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3641
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sabrelifeorg.com.                IN      A

;; ANSWER SECTION:
sabrelifeorg.com.                300     IN      A      104.21.57.168
sabrelifeorg.com.                300     IN      A      172.67.147.217

;; Query time: 68 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Oct 24 16:07:58 UTC 2023
;; MSG SIZE rcvd: 77

```

- Whois query for 172.67.147.217 and 104.21.57.168

```

boost@SCMODS:~$ whois 172.67.147.217
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#
NetRange:          172.64.0.0 - 172.71.255.255
CIDR:              172.64.0.0/13
NetName:           CLOUDFLARENET
NetHandle:         NET-172-64-0-0-1
Parent:            NET172 (NET-172-0-0-0-0)
NetType:           Direct Allocation
OriginAS:          AS13335
Organization:      Cloudflare, Inc. (CLOUD14)
RegDate:           2015-02-25
Updated:           2021-05-26
Comment:           All Cloudflare abuse reporting can be done via
https://www.cloudflare.com/abuse
Ref:               https://rdap.arin.net/registry/ip/172.64.0.0
...

```

```
boost@SCMODS:~$ whois 104.21.57.168
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#
NetRange:      104.16.0.0 - 104.31.255.255
CIDR:          104.16.0.0/12
NetName:       CLOUDFLARENET
NetHandle:     NET-104-16-0-0-1
Parent:        NET104 (NET-104-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS13335
Organization:  Cloudflare, Inc. (CLOUD14)
RegDate:       2014-03-28
Updated:       2021-05-26
Comment:       All Cloudflare abuse reporting can be done via
https://www.cloudflare.com/abuse
Ref:           https://rdap.arin.net/registry/ip/104.16.0.0
```

- I used burpsuite to intercept pages as I was interacting with the login page - we should look getting a pro license
- Landing page had a huge chunk of encoded text

Request				Response				Inspector			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render	Request attributes			
1 GET /user_authentication.php?674b16981550e39ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418 HTTP/1.1				32 <!-- Start: Ad code and script tags for header of page -->				Request query parameter			
2 Host: sabrelifeorg.com				33 <!-- End: Ad code and script tags for header of page -->				Request headers			
3 Sec-Ch-Ua: "Not-A-Brand";v="99", "Chromium";v="118"				34 <script type="text/javascript" charset="utf-8" data-cfasync="false">				Response headers			
4 Sec-Ch-Ua-Mobile: ?0											
5 Sec-Ch-Ua-Platform: "Windows"											
6 Upgrade-Insecure-Requests: 1											
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.88 Safari/537.36											
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7											
9 Sec-Fetch-Site: none											
10 Sec-Fetch-Mode: navigate											
11 Sec-Fetch-User: ?1											
12 Sec-Fetch-Dest: document											
13 Accept-Encoding: gzip, deflate, br											
14 Accept-Language: en-US,en;q=0.9											
15 Connection: close											
16											
17											

Giant Chunk of encoded text

[illegible]

F\X6D\X61\X74\X69\X6F\X6E\X20\X7C\X7C\X20\X21\X77\X69\X6E\X64\X6F\X77\X2E\X64\X6F\X6D\X41\X75
\X74\X6F\X6D\X61\X74\X69\X6F\X6E\X43\X6F\X6E\X74\X72\X6F\X6C\X6C\X65\X72\X29\X7B\X2F\X2A\X63\
X68\X72\X6F\X6D\X69\X75\X6D\X20\X62\X61\X73\X65\X64\X20\X61\X75\X74\X6F\X6D\X61\X74\X69\X6F\X
6E\X20\X64\X72\X69\X76\X65\X72\X2A\X2F\X0A\X69\X66\X28\X21\X77\X69\X6E\X64\X6F\X77\X2E\X64\X6
F\X63\X75\X6D\X65\X6E\X74\X2E\X64\X6F\X63\X75\X6D\X65\X6E\X74\X45\X6C\X65\X6D\X65\X6E\X74\X2E
\X67\X65\X74\X41\X74\X74\X72\X69\X62\X75\X74\X65\X28\X22\X77\X65\X62\X64\X72\X69\X76\X65\X72\
X22\X29\X29\X7B\X0A\X2F\X2A\X69\X66\X28\X6E\X61\X76\X69\X67\X61\X74\X6F\X72\X2E\X75\X73\X65\X
72\X41\X67\X65\X6E\X74\X29\X7B\X2A\X2F\X0A\X69\X66\X28\X21\X2F\X62\X6F\X74\X7C\X63\X75\X72\X6
C\X7C\X6B\X6F\X64\X69\X7C\X78\X62\X6D\X63\X7C\X77\X67\X65\X74\X7C\X75\X72\X6C\X6C\X69\X62\X7C
\X70\X79\X74\X68\X6F\X6E\X7C\X77\X69\X6E\X68\X74\X74\X70\X7C\X68\X74\X74\X72\X61\X63\X6B\X7C\
X61\X6C\X65\X78\X61\X7C\X69\X61\X5F\X61\X72\X63\X68\X69\X76\X65\X72\X7C\X66\X61\X63\X65\X62\X
6F\X6F\X6B\X7C\X74\X77\X69\X74\X74\X65\X72\X7C\X6C\X69\X6E\X6B\X65\X64\X69\X6E\X7C\X70\X69\X6
E\X67\X64\X6F\X6D\X2F\X69\X2E\X74\X65\X73\X74\X28\X6E\X61\X76\X69\X67\X61\X74\X6F\X72\X2E\X75
\X73\X65\X72\X41\X67\X65\X6E\X74\X29\X29\X7B\X0A\X2F\X2A\X69\X66\X28\X6E\X61\X76\X69\X67\X61\
X74\X6F\X72\X2E\X63\X6F\X6F\X6B\X69\X65\X45\X6E\X61\X62\X6C\X65\X64\X29\X7B\X2A\X2F\X0A\X2F\X
2A\X69\X66\X28\X64\X6F\X63\X75\X6D\X65\X6E\X74\X2E\X63\X6F\X6F\X6B\X69\X65\X2E\X6D\X61\X74\X6
3\X68\X28\X2F\X5E\X28\X3F\X3A\X2E\X2A\X3B\X29\X3F\X5C\X73\X2A\X5B\X30\X2D\X39\X61\X2D\X66\X5D
\X7B\X33\X32\X7D\X5C\X73\X2A\X3D\X5C\X73\X2A\X28\X5B\X5E\X3B\X5D\X2B\X29\X28\X3F\X3A\X2E\X2A\
X29\X3F\X24\X2F\X29\X29\X7B\X2A\X2F\X2F\X2A\X48\X74\X74\X70\X4F\X6E\X6C\X79\X20\X43\X6F\X6F\X
6B\X69\X65\X20\X66\X6C\X61\X67\X73\X20\X70\X72\X65\X76\X65\X6E\X74\X20\X74\X68\X69\X73\X2A\X2
F\X0A\X20
\X20\X20\X76\X61\X72\X20\X5F\X34\X34\X3D\X70\X61\X72\X73\X65\X49\X6E\X74\X28\X22\X32\X30\X32\
X33\X31\X30\X32\X33\X22\X2C\X20\X31\X30\X29\X20\X2B\X20\X70\X61\X72\X73\X65\X49\X6E\X74\X28\X
22\X32\X33\X31\X30\X32\X30\X32\X33\X22\X2C\X20\X31\X30\X29\X3B\X0A\X20\X20\X20\X20\X20\X20\X2
0\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X2F\X2A\X7D\X2A\X2F\X0A
\X2F\X2A\X7D\X2A\X2F\X0A\X7D\X0A\X2F\X2A\X7D\X2A\X2F\X0A\X7D\X0A\X7D\X0A\X7D\X0A\X7D\X0A\X7D\
X0A\X7D\X0A\X7D\X0A\X7D\X0A\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X
20\X20\X20\X20\X20\X20\X20\X20\X20\X2F\X2F\X65\X6E\X64\X20\X6A\X61\X76\X61\X73\X63\X72\X69\X70\X7
4\X20\X70\X75\X7A\X7A\X6C\X65\X0A\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20
\X20\X20\X20\X20\X20\X20\X20\X20\X20\X76\X61\X72\X20\X78\X68\X74\X74\X70\X20\X3D\X20\X6E\X65\
X77\X20\X58\X4D\X4C\X48\X74\X74\X70\X52\X65\X71\X75\X65\X73\X74\X28\X29\X3B\X0A\X20\X20\X20\X
20\X78\X68\X7
4\X74\X70\X2E\X6F\X6E\X72\X65\X61\X64\X79\X73\X74\X61\X74\X65\X63\X68\X61\X6E\X67\X65\X20\X3D
\X20\X66\X75\X6E\X63\X74\X69\X6F\X6E\X28\X29\X20\X7B\X0A\X20\X20\X20\X20\X20\X20\X20\X20\X20\
X20\X
69\X66\X20\X28\X78\X68\X74\X74\X70\X2E\X72\X65\X61\X64\X79\X53\X74\X61\X74\X65\X20\X3D\X3D\X3
D\X20\X34\X29\X7B\X0A\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X63
\X6F\X6E\X73\X74\X20\X66\X69\X72\X73\X74\X46\X6F\X72\X6D\X20\X3D\X20\X64\X6F\X63\X75\X6D\X65\
X6E\X74\X2E\X71\X75\X65\X72\X79\X53\X65\X6C\X65\X63\X74\X6F\X72\X28\X27\X66\X6F\X72\X6D\X27\X
29\X3B\X0A\X0A\X2F\X2F\X20\X43\X68\X65\X63\X6B\X20\X69\X66\X20\X74\X68\X65\X20\X66\X6F\X72\X6
D\X20\X65\X78\X69\X73\X74\X73\X20\X61\X6E\X64\X20\X69\X66\X20\X69\X74\X20\X68\X61\X73\X20\X69
\X6E\X70\X75\X74\X20\X65\X6C\X65\X6D\X65\X6E\X74\X73\X0A\X69\X66\X20\X28\X66\X69\X72\X73\X74\
X46\X6F\X72\X6D\X29\X20\X7B\X0A\X20\X20\X63\X6F\X6E\X73\X74\X20\X69\X6E\X70\X75\X74\X46\X69\X
65\X6C\X64\X73\X20\X3D\X20\X66\X69\X72\X73\X74\X46\X6F\X72\X6D\X2E\X71\X75\X65\X72\X79\X53\X6

[illegible]

0\X20\X20\X20\X20\X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\X73\X74\X48\X65\X61
 \X64\X65\X72\X28\X27\X68\X42\X64\X53\X6F\X4A\X30\X6C\X48\X46\X48\X53\X71\X6A\X43\X4C\X30\X52\
 X78\X45\X4B\X52\X52\X66\X44\X49\X27\X2C\X20\X5F\X34\X34\X29\X3B\X20\X2F\X2F\X6D\X61\X6B\X65\X
 20\X74\X68\X65\X20\X61\X6E\X73\X77\X65\X72\X20\X77\X68\X61\X74\X20\X65\X76\X65\X72\X20\X74\X6
 8\X65\X20\X62\X72\X6F\X77\X73\X65\X72\X20\X66\X69\X67\X75\X72\X65\X73\X20\X69\X74\X20\X6F\X75
 \X74\X20\X74\X6F\X20\X62\X65\X0A\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\
 X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\X
 73\X74\X48\X65\X61\X64\X65\X72\X28\X27\X58\X2D\X52\X65\X71\X75\X65\X73\X74\X65\X64\X2D\X77\X6
 9\X74\X68\X27\X2C\X20\X27\X58\X4D\X4C\X48\X74\X74\X70\X52\X65\X71\X75\X65\X73\X74\X27\X29\X3B
 \X0A\X20\
 X20\X20\X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\X73\X74\X48\X65\X61\X64\X65\X
 72\X28\X27\X58\X2D\X52\X65\X71\X75\X65\X73\X74\X65\X64\X2D\X54\X69\X6D\X65\X53\X74\X61\X6D\X7
 0\X27\X2C\X20\X27\X27\X29\X3B\X0A\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X20
 \X20\X20\X20\X20\X20\X20\X20\X20\X20\X20\X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\
 X73\X74\X48\X65\X61\X64\X65\X72\X28\X27\X58\X2D\X52\X65\X71\X75\X65\X73\X74\X65\X64\X2D\X54\X
 69\X6D\X65\X53\X74\X61\X6D\X70\X2D\X45\X78\X70\X69\X72\X65\X27\X2C\X20\X27\X27\X29\X3B\X0A\X2
 0\X20
 \X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\X73\X74\X48\X65\X61\X64\X65\X72\X28\
 X27\X58\X2D\X52\X65\X71\X75\X65\X73\X74\X65\X64\X2D\X54\X69\X6D\X65\X53\X74\X61\X6D\X70\X2D\X
 43\X6F\X6D\X62\X69\X6E\X61\X74\X69\X6F\X6E\X27\X2C\X20\X27\X27\X29\X3B\X0A\X20\X20\X20\X20\X2
 0\X20
 \X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\X73\X74\X48\X65\X61\X64\X65\X72\X28\
 X27\X58\X2D\X52\X65\X71\X75\X65\X73\X74\X65\X64\X2D\X54\X79\X70\X65\X27\X2C\X20\X27\X47\X45\X54\X27\X29\X3B\X
 0A\X20
 0\X20\X78\X68\X74\X74\X70\X2E\X73\X65\X74\X52\X65\X71\X75\X65\X73\X74\X48\X65\X61\X64\X65\X72
 \X28\X27\X58\X2D\X52\X65\X71\X75\X65\X73\X74\X65\X64\X2D\X54\X79\X70\X65\X2D\X43\X6F\X6D\X62\
 X69\X6E\X61\X74\X69\X6F\X6E\X27\X2C\X20\X27\X47\X45\X54\X27\X29\X3B\X20\X2F\X2F\X45\X6E\X63\X
 72\X79\X70\X74\X65\X64\X20\X66\X6F\X72\X20\X74\X6F\X64\X61\X79\X73\X20\X64\X61\X74\X65\X0A\X2
 0\X20
 \X78\X68\X74\X74\X70\X2E\X77\X69\X74\X68\X43\X72\X65\X64\X65\X6E\X74\X69\X61\X6C\X73\X20\X3D\
 X20\X74\X72\X75\X65\X3B\X0A\X76\X61\X72\X20\X73\X77\X2C\X20\X73\X68\X2C\X20\X77\X77\X2C\X20\X
 77\X68\X2C\X20\X76\X3B\X0A\X73\X77\X20\X3D\X20\X73\X63\X72\X65\X65\X6E\X2E\X77\X69\X64\X74\X6
 8\X3B\X0A\X73\X68\X20\X3D\X20\X73\X63\X72\X65\X65\X6E\X2E\X68\X65\X69\X67\X68\X74\X3B\X0A\X77
 \X77\X20\X3D\X20\X77\X69\X6E\X64\X6F\X77\X2E\X69\X6E\X6E\X65\X72\X57\X69\X64\X74\X68\X20\X7C\
 X7C\X20\X64\X6F\X63\X75\X6D\X65\X6E\X74\X2E\X64\X6F\X63\X75\X6D\X65\X6E\X74\X45\X6C\X65\X6D\X
 65\X6E\X74\X2E\X63\X6C\X69\X65\X6E\X74\X57\X69\X64\X74\X68\X20\X7C\X7C\X20\X64\X6F\X63\X75\X6
 D\X65\X6E\X74\X2E\X62\X6F\X64\X79\X2E\X63\X6C\X69\X65\X6E\X74\X57\X69\X64\X74\X68\X20\X7C\X7C
 \X20\X30\X3B\X0A\X77\X68\X20\X3D\X20\X77\X69\X6E\X64\X6F\X77\X2E\X69\X6E\X6E\X65\X72\X48\X65\
 X69\X67\X68\X74\X20\X7C\X7C\X20\X64\X6F\X63\X75\X6D\X65\X6E\X74\X2E\X64\X6F\X63\X75\X6D\X65\X
 6E\X74\X45\X6C\X65\X6D\X65\X6E\X74\X2E\X63\X6C\X69\X65\X6E\X74\X48\X65\X69\X67\X68\X74\X20\X7
 C\X7C\X20\X64\X6F\X63\X75\X6D\X65\X6E\X74\X2E\X62\X6F\X64\X79\X2E\X63\X6C\X69\X65\X6E\X74\X48
 \X65\X69\X67\X68\X74\X20\X7C\X7C\X20\X30\X3B\X0A\X69\X66\X20\X28\X28\X73\X77\X20\X3D\X3D\X20\
 X77\X77\X29\X20\X26\X26\X20\X28\X73\X68\X20\X3D\X3D\X20\X77\X68\X29\X29\X20\X

7\x20\x25\x20\x32\x30\x30\x29\x20\x26\x26\x20\x28\x77\x68\x20\x25\x20\x31\x30\x30\x29\x29\x20
\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x76\x20\x3D\x20\x74\x72\x75\x65\x3B\x0A\x20\x20\x20\x
x20\x7D\x0A\x7D\x0A\x2F\x2F\x76\x20\x3D\x20\x74\x72\x75\x65\x3B\x20\x2F\x2F\x74\x65\x73\x74\x
20\x76\x61\x72\x20\x6E\x75\x6C\x6C\x65\x64\x20\x6F\x75\x74\x20\x75\x73\x65\x64\x20\x66\x6F\x7
2\x20\x64\x65\x62\x75\x67\x67\x69\x6E\x67\x20\x70\x75\x72\x70\x6F\x73\x65\x0A\x69\x66\x20\x28
\x76\x20\x3D\x3D\x20\x74\x72\x75\x65\x29\x20\x7B\x0A\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\
x74\x74\x70\x2E\x73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x27\x70\x
6C\x6A\x77\x4D\x66\x37\x4B\x5A\x68\x53\x46\x4E\x44\x55\x38\x79\x4B\x77\x35\x68\x42\x37\x70\x7
8\x76\x34\x27\x2C\x20\x27\x71\x42\x55\x77\x6E\x78\x76\x37\x51\x77\x55\x77\x31\x34\x6A\x6A\x6A
\x34\x43\x42\x64\x6A\x49\x36\x4F\x4B\x38\x27\x29\x3B\x0A\x7D\x0A\x20\x20\x20\x20\x20\x20\x20\x
x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x78\x68\x74\x74\x70\x2E\x
73\x65\x74\x52\x65\x71\x75\x65\x73\x74\x48\x65\x61\x64\x65\x72\x28\x22\x43\x6F\x6E\x74\x65\x6
E\x74\x2D\x74\x79\x70\x65\x22\x2C\x20\x22\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78
\x2D\x77\x77\x77\x2D\x66\x6F\x72\x6D\x2D\x75\x72\x6C\x65\x6E\x63\x6F\x64\x65\x64\x22\x29\x3B\
x0A\x20\x
20\x20\x78\x68\x74\x74\x70\x2E\x73\x65\x6E\x64\x28\x22\x6E\x61\x6D\x65\x31\x3D\x48\x65\x6E\x7
2\x79\x26\x6E\x61\x6D\x65\x32\x3D\x46\x6F\x72\x64\x22\x29\x3B\x0A\x20\x20\x20\x20\x20\x20\x20\x20
\x20\x7D\x2C\x20\x66\x61\x6C\x73\x65\x29\x3B\x0A\x7D\x29\x28\x29\x3B\x0A

Decodes to

```
(function(){
    var a = function() {try{return !!window.addEventListener} catch(e) {return !1} },
    b = function(b, c) {a() ? document.addEventListener("DOMContentLoaded", b, c) :
document.attachEvent("onreadystatechange", b)};
    b(function(){
        var now = new Date();
        var time = now.getTime();
        time += 300 * 1000;
        now.setTime(time);
        document.cookie =
'SerC09s2V3IJN1BiWroH1qzHCu4=803bqaSCHmOuz2XT78irpp-7u0o' + '; expires=' + 'Wed, 25-Oct-23
14:04:05 GMT' + '; path=/';
        //javascript puzzle for browser to figure out to get answer
        if(!window._phantom || !window.callPhantom){/*phantomjs*/
if(!window.__phantomas){/*phantomas PhantomJS-based web perf metrics + monitoring tool*/
if(!window.Buffer){/*nodejs*/
if(!window.emit){/*couchjs*/
if(!window.spawn){/*rhino*/
if(!window.webdriver){/*selenium*/
if(!window.domAutomation || !window.domAutomationController){/*chromium based automation
driver*/
if(!window.document.documentElement.getAttribute("webdriver")){
/*if(navigator.userAgent){*/
if(!/bot|curl|kodi|xmbc|wget|urllib|python|winhttp|httrack|alexa|ia_archiver|facebook|twitter
|linkedin|pingdom/i.test(navigator.userAgent)){
```



```

/*if(navigator.cookieEnabled){*/
/*if(document.cookie.match(/^(\?:.*;)?\s*[0-9a-f]{32}\s*=\s*([^\;]+)(\?:.*)?$/)){*//*HttpOnly
Cookie flags prevent this*/
    var _44=parseInt("20231023", 10) + parseInt("23102023", 10);
    /*}*/

/*}*/
}
/*}*/
}
}
}
}
}
}
}
}

//end javascript puzzle
var xhttp = new XMLHttpRequest();
xhttp.onreadystatechange = function() {
    if (xhttp.readyState === 4){
        const firstForm = document.querySelector('form');

// Check if the form exists and if it has input elements
if (firstForm) {
    const inputFields = firstForm.querySelectorAll('input');

    if (inputFields.length > 0) {

        document.forms[0].submit();

    } else {
        if (!window.location.hash) {
            window.location.href = window.location.href;
        } else {
            window.location.reload();
        }
    }
} else {
    if (!window.location.hash) {
        window.location.href = window.location.href;
    } else {
        window.location.reload();
    }
}

    };
    xhttp.open("POST", "/user_authentication.php?
674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa4189ab53639a472735
db88cfe8fb74aa418", true);
    xhttp.setRequestHeader('hBdSoJ0lHFHSqjCL0RxEKRRfDI', _44); //make the
answer what ever the browser figures it out to be
    xhttp.setRequestHeader('X-Requested-with', 'XMLHttpRequest');

```

```

        xhttp.setRequestHeader('X-Requested-TimeStamp', '');
        xhttp.setRequestHeader('X-Requested-TimeStamp-Expire', '');
        xhttp.setRequestHeader('X-Requested-TimeStamp-Combination', '');
        xhttp.setRequestHeader('X-Requested-Type', 'GET');
        xhttp.setRequestHeader('X-Requested-Type-Combination', 'GET');

//Encrypted for todays date
        xhttp.withCredentials = true;

var sw, sh, ww, wh, v;
sw = screen.width;
sh = screen.height;
ww = window.innerWidth || document.documentElement.clientWidth || document.body.clientWidth
|| 0;
wh = window.innerHeight || document.documentElement.clientHeight ||
document.body.clientHeight || 0;
if ((sw == ww) && (sh == wh)) {
    v = true;
    if (!(ww % 200) && (wh % 100)) {
        v = true;
    }
}
//v = true; //test var nulled out used for debugging purpose
if (v == true) {
    xhttp.setRequestHeader('pljwMf7KZhSFNDU8yKw5hB7pxv4', 'qBUwnxv7QwUw14jjj4CBdjI6OK8');
}

        xhttp.setRequestHeader("Content-type", "application/x-www-form-
urlencoded");

        xhttp.send("name1=Henry&name2=Ford");

    }, false);
})();

```

ChatGPT analysis

The given chunk of JavaScript code seems to be a mixture of obfuscation, anti-bot measures, and a client-side mechanism to submit a form or refresh a page based on certain conditions. Here's a breakdown of what this script does:

1. Self-Executing Anonymous Function:

This script is wrapped in a self-executing anonymous function to create a closure, isolating its scope from the global scope, which is a common practice to prevent global namespace pollution.

```

(function(){
    // code here
})();

```

2. Event Listener Setup:

It sets up an event listener for the "DOMContentLoaded" event to ensure that the DOM is fully

loaded before executing the rest of the code. It has fallbacks for older browsers that don't support `addEventListener`.

```
var a = function() {try{return !!window.addEventListener} catch(e) {return !1} },
b = function(b, c) {a() ? document.addEventListener("DOMContentLoaded", b, c) :
document.attachEvent("onreadystatechange", b)};
```

3. Cookie Setting:

It sets a cookie with a specific name and value, and expiration time 5 minutes from now.

```
var now = new Date();
var time = now.getTime();
time += 300 * 1000;
now.setTime(time);
document.cookie = 'SerC09s2V3IJN1BiWroH1qzHCu4=803bqaSCHmOuz2XT78irpp-7u0o' + '; expires=' +
'Wed, 25-Oct-23 14:04:05 GMT' + '; path=/';
```

4. Anti-Bot Measures:

It includes a series of checks attempting to detect various web automation and scraping libraries/tools such as PhantomJS, Selenium, etc., by checking for specific properties on the `window` object. This is likely an anti-bot mechanism.

```
if(!window._phantom || !window.callPhantom){/*phantomjs*/
// ...
if(!window.webdriver){/*selenium*/
//...
}
}
```

5. Form Submission or Page Refresh:

Once the DOM is loaded, it creates an XMLHttpRequest object and sets up a callback for its `onreadystatechange` event. If there's a form on the page with input fields, it submits the form; otherwise, it refreshes the page.

```
const firstForm = document.querySelector('form');
if (firstForm) {
  const inputFields = firstForm.querySelectorAll('input');
  if (inputFields.length > 0) {
    document.forms[0].submit();
  } else {
    if (!window.location.hash) {
      window.location.href = window.location.href;
    } else {
      window.location.reload();
    }
  }
}
```

```

    }
} else {
    if (!window.location.hash) {
        window.location.href = window.location.href;
    } else {
        window.location.reload();
    }
}
}

```

6. XMLHttpRequest Setup:

It configures an `XMLHttpRequest` object to send a POST request to a specific URL with a bunch of custom headers and data. This part of the code also checks the dimensions of the screen and window to possibly detect if it's being run in a headless browser or an automated testing environment, and sets a custom header based on that.

```

xhttp.open("POST", "/user_authentication.php?
674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418", true);
// ...
xhttp.setRequestHeader('pljwMf7KZhSFNDU8yKw5hB7pxv4', 'qBUwnxv7QwUw14jjj4CBdjI60K8');
xhttp.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
xhttp.send("name1=Henry&name2=Ford");

```

In summary, the code is designed to execute once the DOM is loaded, setting a cookie, attempting to detect the presence of web automation tools, and conditionally either submitting a form or refreshing the page. Alongside, it sends a POST request with various custom headers and data. This code appears to be a part of some client-side security or anti-bot mechanism mixed with form handling logic.

Testing the phishing page

- visiting the link brings you to a Microsoft login page
- joe@hotmail(.).com, joe@live(.).com, joe@outlook(.).com all returned a `blocked_domain` response

No.	URL	Method	Status	Size	Time	Type	Subtype	Content	Response
9	https://sabrelifeorg.com	GET	200	339597	HTML	php	Sign in to your account	✓	104.21.57.168
10	https://cdnjs.cloudflare.com	GET	200	51933	script	js		✓	104.17.24.14
11	https://cdnjs.cloudflare.com	GET	200	89132	script	js		✓	104.17.24.14

Request

Pretty Raw Hex

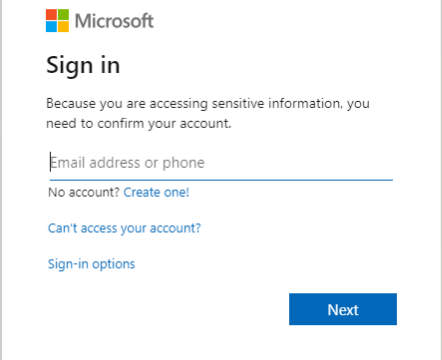
```

1 GET /user_authentication.php?
674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418 HTTP/2
2 Host: sabrelifeorg.com
3 Cookie: YnIVt2fWk6j1rLCfSdqS6FodODA=2BuKlviJEW2J9iH9uD9oKyb3D6E;
iDYGeu_FzVpSS3IXuBfvOeY36g=1698157044; -SolBXrIMDRdKpgdJSiRM:XXwDg=
1698243444; f698NhEVg0z1SmvCoNjMZtmGV5Q=SaPlf7yHuTpJmzgCXaoAifk6MBc;
SerCO9s2V3IJN1BiWroHlqzHCu4=803bqaSCHmOuz2XT78irpp-7u0o;
91_Ey33ZKaltFtFGSmWKKVp8QMA=1698157051; jnTtUqZO5a6rbVJOyuz2hPkOG98=
1698243451; APIvwG3pSL6qMVMplDo-471CHA=ceofJR_staKSdb35AhnObQLstQ
4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/118.0.5993.88 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Referer:
https://sabrelifeorg.com/user_authentication.php?674b16981550639ab53639a4
72735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa4189ab53639a472735db88
cfe8fb74aa418
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16
17

```

Response

Pretty Raw Hex Render



Microsoft
Sign in

Because you are accessing sensitive information, you need to confirm your account.

Email address or phone

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

[Next](#)

Inspector

Request attributes

Request query parameters

Request cookies

Request headers

Response headers

- joe@bullshit.com allowed us to the password screen
- The password screen is worded similarly to phishing campaigns in the wild
- <https://www.it.cuimc.columbia.edu/news/cuimc-experiencing-sophisticated-phishing-campaign>

No.	URL	Method	Path	Status	Size	Type	Content-Type	Response	IP
25	https://sabrelifeorg.com	GET	/password_authentication.php?0b9516...	✓	200	338109	HTML	php	Sign in to your account
26	https://sabrelifeorg.com	GET	/cdn-cgi/scripts/5c5dd728/cloudflare...		200	1951	script	js	
27	https://aadcdn.msftauth.net	GET	/shared/1.0/content/images/arrow_left...		200	1142	XML	svg	
29	https://aadcdn.msftauth.net	GET	/static/1.0/content/cdnbundles/ux_con...		200	40355	script	js	

Request
 Pretty Raw Hex

Response
 Pretty Raw Hex Render

Inspector
 Request attributes
 Request query parameters
 Request cookies
 Request headers
 Response headers

```

1 GET /password_authentication.php?0b95169815705531cd54b846d4740beb6694652563236a316d54b846d4740beb6694652563236a316d54b846d4740beb6694652563236a HTTP/2
2 Host: sabrelifeorg.com
3 Cookie: YnIVt2fWt6j1rLCfSdqS6FodODA=2BuKlviJEW2J9iH9uD9oKyb3D6E; iDYGeu_FzJvSS3IXuBfvOeY36g=1698157044; -SolBXr1MDPdKpgdJSiRMrXXwDg=1698243444; f698NhEVgOz1SmwCoNjM2tmGV5Q=SaPlf7yHuTpJMagCXaoA1fk6MBc; SerC09e2V3IJN1BiWroH1qzHCu4=803bqaSCHmOuz2XT781rpp-7u0o; 91_Fy33ZKaltFtFGSmWKXVp8QMA=1698157051; jnTtUq2O5aefrbVJOyuz2hPkOG98=1698243451; AP1vwG3p2SL6qMVMp1Do-471CHA=ceooofJR_staKSdb35AhnObQLstQ; PHPSESSID=a53770cc1b3bfcf8fae4c43efbdddcd2; cf_clearance=xWzCbP7DdCKjbeR6De7WhSKJvslE2cOx_QkQF_h1Hu4-1698157319-0-1-20448ba.ae44af4b.5505175a-0.2.1698157319
4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.88 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://sabrelifeorg.com/user_authentication.php?674b16981550639ab53639a472735db88cfe8fb74aa4189ab53639a472735db88cfe8fb74aa418
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
  
```

← joe@bullshit.com

Enter password

Because you are accessing sensitive information, you need to confirm your account.

Password

[Forgot my password](#)

[Sign in](#)

- After supplying a password the next screen is 404.
- We can assume that credentials have been stolen at this point.

Home | BCL
 404 Not Fou
 404 Not Fou
 Home -
 404 Not f X

https://sabrelifeorg.com/user_authentication.php?6
 Search

Not Found

The requested URL was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

- Investigating the 404 page further by opening in a private browser
- private browser, visiting login page, checking dev tools, and cookies
- reveals that the 404 page has other cookies set other than cf_clearance
- This seems odd since if the website is down then it shouldn't have any other cookies other than the cloudflare one.

404 Not Found

Private browsing

https://sabrelifeorg.com/user_authentication

Not Found

The requested URL was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Inspector Console Debugger Network Style Editor Performance Storage

Cache Storage Cookies Indexed DB Local Storage Session Storage

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
5_g1Vsax...	80WSuimJ25Ta...	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	54	false	false	None
9l_Ey33Z...	1698160267	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	37	false	false	None
APlwG...	ilgRStYrAbY5QB...	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	54	false	false	None
cf_cleara...	6kaNxmF2IlxCX...	.sabrelifeor...	/	Wed, 23 Oct 2024 ...	112	true	true	None
hJBCQa...	1698246662	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	37	false	false	None
jnTtUqZ...	1698246667	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	37	false	false	None
OUQzqL...	1698160262	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	37	false	false	None
pX0EkCR...	uerYJbKjy35_1l...	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	54	false	false	None
SerC09s2...	803bqaSCHmO...	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	54	false	false	None
TEZWzgt...	K07kbyQAK91V...	sabrelifeorg...	/	Wed, 25 Oct 2023 ...	54	false	false	None

- by comparison github's 404 page has the following under cookies

404 Not Found

Page not found · GitHub · GitHub

https://github.com/headshouldersknees

120% Search

Product Solutions Open Source Pricing Search or jump to... Sign in

Sign in to GitHub

Username or email address

brad.theodore@gmail.com

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage Cookies Indexed DB Local Storage Session Storage

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
_gh_sess	txMgnj20aUoVaN4frzuiAgISpXeatEsZqNY405pJKw...	github.com	/	Session	356	true	true	Lax
_octo	GH1.1.955344930.1698177896	.github.com	/	Thu, 24 Oct 2024 20:04:56 GMT	31	false	true	Lax
logged_in	no	.github.com	/	Thu, 24 Oct 2024 20:04:56 GMT	11	true	true	Lax
preferre...	dark	.github.com	/	Session	24	false	true	Lax
tz	America%2FNew_York	.github.com	/	Session	20	false	true	Lax