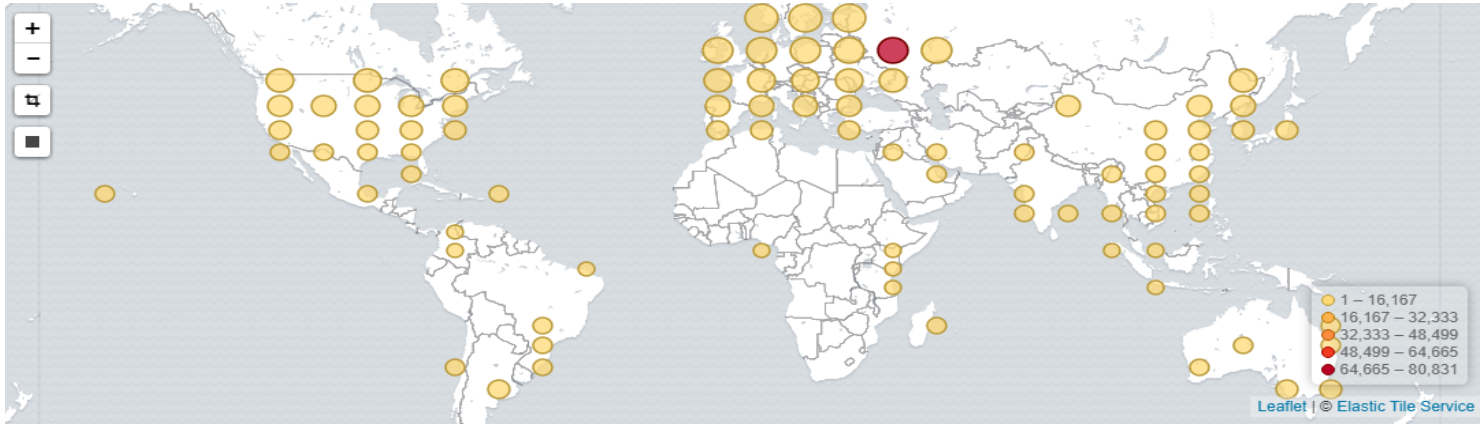
A DGA Odyssey
PDNS Driven DGA Analysis

Yiming Gong
Qitian Su
Zaifeng Zhang

http://netlab.360.com

Quick fact



- We are tracking 38 families, 375 variants
- 5M DNS queries/d
- Subscribers: 57 countries
- Free data feed: http://data.netlab.360.com/dga

Outline

- Background info
- From PDNS Data to Suspicious DGA
- From Suspicious DGA to Malware Sample
- Blocking Experience

Background info

- Traditional non-DGA C2
  - Hardcoded C&C
    - WannaCry

```
.data:004313CE                 align 10h
.data:004313D0 aHttpWww_iuqerf db 'http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com',0
.data:004313D0                                         ; DATA XREF: WinMain(x,x,x,x)+A↑o
.data:00431409                 align 10h
```

```
qmemcpy(&szUrl, aHttpWww_iuqerf, 0x39u);      // Copy hardcoded domain
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// Connect
if ( v5 )                                     // If success
{
```

Background info

- DGA
  - Domain generation algorithms
    - C2s are not hardcoded
    - Generate many candidates based on its algorithm
    - Only register one
      - Example: Necurs, 2048 domains per three days

Background info

- DGA

llvgqpgesb.ga	1	e3	1709212225	0
tffwlwyutc.sh	1	e3	1709212225	0
shwrmrsphrdclbbnx.biz	1	e3	1709212225	0
xghiwdoxxrcteq.so	1	e3	1709212225	0
vykwipbptsebgxhhlrmut.tw	1	e3	1709212225	0
wwlqksmu.us	1	e3	1709212225	0
vavmxfpsotngiq.ug	1	e3	1709212225	0
mehsfqgvjtyie.ru	1	e3	1709212225	0
temtvdgx.com	1	e3	1709212225	0
noaxluqryfewc.sc	1	e3	1709212225	0
sdypfxod.com	1	168.170.0.7	1709212225	
tlbcgfspo.cc	1	e3	1709212225	0
kvmfmkkyjkmnhywvmm.sh	1	e3	1709212225	0
tvudnwwbrwbjrbaueew.net	1	e3	1709212225	0
cemnpvvi.jp	1	e3	1709212225	0
nrkehipvk.jp	1	e3	1709212225	0

2017-09-21
C&C: 168.170.0.7

seydwjdaewafx.in	1	e3	1709241405	0
olpcnkxuxjukvkmr.ac	1	e3	1709241405	0
uwaxayog.ru	1	e3	1709241405	0
nsjydsbjnneuhwuignkfo.ru	1	e3	1709241405	0
lqpqiex.net	1	169.242.240.68	1709241405	36
xvnjcapvp.nu	1	e3	1709241405	0
txmwwuntrrfxxdyhx.tw	1	e3	1709241405	0
begkajmuxxskxwyujsucx.pro	1	e3	1709241405	0
aukwkhiofi.sx	1	e3	1709241405	0
jolxqio.ir	1	e3	1709241405	0
filliineoe.ki	1	e3	1709241405	0
ofwbafao.sx	1	e3	1709241405	0
vlkktytatkxqfubmb.pro	1	e3	1709241405	0
axrsllydhsr.jp	1	e3	1709241405	0
fwgcipduxoyxxxhxmxnpa.de	1	e3	1709241405	0
egfoehki.net	1	e3	1709241405	0
xjcyaqdtyncdvtlt.co	1	e3	1709241405	0

2017-09-24
C&C: 169.242.240.68

Background info

- PDNS
  - Passive DNS

```
$ flint rrset www.nanog.org -p
2014-08-06 11:12:59    2017-03-22 09:34:57    3314    www.nanog.org   A      50.31.151.73

2017-02-23 21:40:23    2017-09-23 16:17:06    716     www.nanog.org   A      104.20.198.50
```

Background info

- PDNS
  - Fast flux

```
$ flint rrset blanytread.com -p
2017-09-24 04:41:18  2017-09-24 04:41:19  2    blanytread.com  A    176.53.209.231
2017-09-24 04:41:18  2017-09-24 04:41:19  2    blanytread.com  A    185.185.181.72
2017-09-24 04:41:18  2017-09-24 04:41:19  2    blanytread.com  A    31.133.76.95
2017-09-24 04:41:18  2017-09-24 04:41:19  2    blanytread.com  A    91.243.212.227
2017-09-24 04:41:18  2017-09-24 04:41:19  2    blanytread.com  A    93.127.86.207

2017-09-24 03:25:49  2017-09-24 03:25:49  1    blanytread.com  A    147.194.1.229
2017-09-24 03:25:49  2017-09-24 03:25:49  1    blanytread.com  A    31.133.63.40
2017-09-24 03:25:49  2017-09-24 03:25:49  1    blanytread.com  A    31.43.79.122
2017-09-24 03:25:49  2017-09-24 03:25:49  1    blanytread.com  A    46.185.100.234
2017-09-24 03:25:49  2017-09-24 03:25:49  1    blanytread.com  A    5.105.27.37
```

Background info

- PDNS has great potential
- PassiveDNS.cn
  - ~10%+ China DNS traffic
  - ~1M+ queries per second
  - ~15+ billion RRsets

Finding Highly Suspicious DGA

- First we need to have daily new Domains
  - Match
    - New Domains in last 7 days
    - Second Level Domain(SLD) not on Alexa top 10K
    - Others
      - virtual hosts provided by registrar
      - Wildcards Domain names
      - …
  - Result
    - Raw data → millions

Finding Highly Suspicious DGA

- noise
  - looks like, but NOT DGAs

Akamai	Cloudflare
p714.10uss.akadns.net	www.webhoster.ag.cdn.cloudflare.net
p716.10uss.akadns.net	www.wpconsulting.agency.cdn.cloudflare.net
p726.10uss.akadns.net	www.xingular.ae.cdn.cloudflare.net

Spamhaus	SURBL
224.134.0.1.zen.spamhaus.org	zol.com.cn.ab.surbl.org
225.128.0.1.zen.spamhaus.org	zol-img.com.cn.ab.surbl.org
225.136.0.1.zen.spamhaus.org	zte.com.cn.ab.surbl.org
226.133.0.1.zen.spamhaus.org	ztesc.com.cn.ab.surbl.org

Finding Highly Suspicious DGA

- noise

000-000-000a-000a-0000-1452593369-fbe2b699ai6l7t3bsclvr0mpf260.am2oob.dashnxdomain.net
000-000-000a-000a-0000-1452605115-66c1ba4bai6o1gog9i2rtf62s45g.am2oob.dashnxdomain.net
000-000-000a-000a-0000-1452613108-ai6pug3r8rpqhno6m220.am2oob.dashnxdomain.net
000-000-000a-000a-0000-1452661195-2db4c5c2ai75dc5mv4qr6aiehdjg.am2oob.dashnxdomain.net
000-000-000a-000a-0000-1452672623-ac948d19ai784i3luh3r3r7iekpg.am2oob.dashnxdomain.net
000-000-000a-000a-0000-1452674129-4f07e17bai78g1sashmonjoc3o90.am2oob.dashnxdomain.net

Elknot	Mirai
ytslujgxynglwb.www.cn856.com	ng5gt6bdun2m.kindjia.com
yutluue.www.cn856.com	jfkhuo16u51c.kindjia.com
yvcnud.www.cn856.com	fcdepfuun7jp.kindjia.com
yvdvbcfprox.www.cn856.com	v4ihpfrgt2hj.kindjia.com
yvizalsxkxqvel.www.cn856.com	qdl4aa5bb6cs.kindjia.com

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - Logic
    - Aggregate the DGAs from same family| variant to same cluster
  - match
    - Time
      - Most DGA queries are generated in a short amount of time
    - Client
      - Clients infected with same family|variant ask for same FQDNs in same time window
  - Result
    - Million → 100,000s

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - Time based clustering
    - Granularity: hour
    - Clustering all accessed domains in same clustering from 1h for same client
  - Client based clustering
    - Domain-IP matrix (A)
    - Calculate transpose of matrix A^T
    - Similarity matrix based on client requests: $B = A * A^T$
    - Louvain algorithm

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - Diagram of client based clustering (1)

$$A = \begin{array}{c} \begin{array}{ccccc} IP_1 & IP_2 & IP_3 & IP_4 & IP_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array} \begin{array}{c} D_1 \\ D_2 \\ D_3 \\ D_4 \end{array}$$

$$A^T = \begin{array}{c} \begin{array}{cccc} D_1 & D_2 & D_3 & D_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array} \begin{array}{c} IP_1 \\ IP_2 \\ IP_3 \\ IP_4 \\ IP_5 \end{array}$$

$$B = A * A^T = \begin{array}{c} \begin{array}{cccc} D_1 & D_2 & D_3 & D_4 \end{array} \\ \begin{pmatrix} 3 & 3 & 1 & 1 \\ 3 & 4 & 2 & 2 \\ 1 & 2 & 3 & 2 \\ 1 & 2 & 2 & 3 \end{pmatrix} \end{array} \begin{array}{c} D_1 \\ D_2 \\ D_3 \\ D_4 \end{array}$$

1 = 1*1 + 1*0 + 0*1 + 1*0 + 0*1

3 = 1*1 + 1*1 + 0*1 + 1*1 + 0*0

Matrix A:

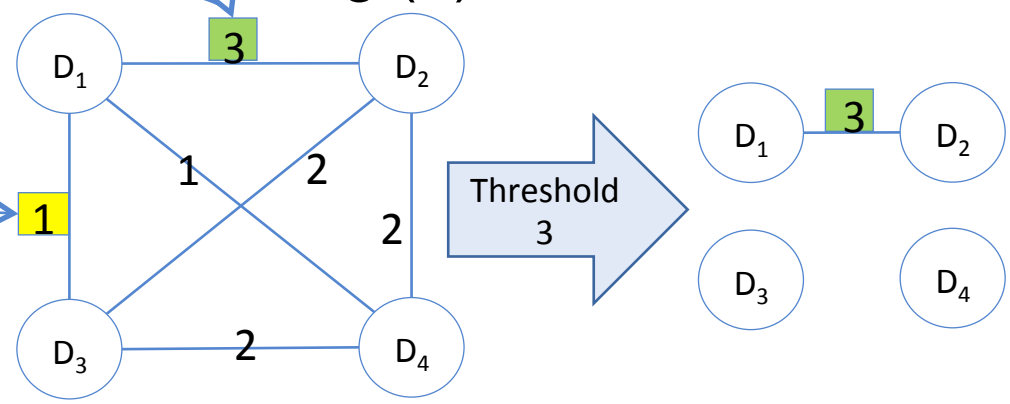
- D means Domain
- Value of 1 indicates that domain has a DNS query from that IP, 0 means none

From the calculation principle, we can see that the element value of matrix B is the coincidence number of client IPs between two domain. Thus, based on the client dimension, the similarity of D_1 &D_2 is higher than D_1 & D_3.

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - Diagram of client based clustering (2)

$$B = A * A^T = \begin{array}{c} \begin{array}{cccc} D_1 & D_2 & D_3 & D_4 \end{array} \\ \begin{pmatrix} 3 & \boxed{3} & \boxed{1} & 1 \\ 3 & 4 & 2 & 2 \\ 1 & 2 & 3 & 2 \\ 1 & 2 & 2 & 3 \end{pmatrix} \end{array} \begin{array}{c} D_1 \\ D_2 \\ D_3 \\ D_4 \end{array}$$



Louvain algorithm:

- Convert matrix B into undirected graph, set a threshold, such as 3, leaving the edge with the weight ≥ the threshold only.
- So, the four domains will eventually be divided into three clusters: D_1 and D_2 a class, D_3, D_4 each class.
- https://perso.uclouvain.be/vincent.blondel/research/louvain.html

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - A long potential candidates list
    - For example, Conficker, DGA

ID	conficker	ID	conficker
26324	njcdeclp.info	26324	hperqjhe.info
26324	xbtyyxdkixd.info	26324	fwdwcymvko.info
26324	yqesnmuf.info	26324	ldebdwssq.info
26324	zhwnrjm.info	26324	scpxhu.info
26324	eocsdlj.info	26324	zwachxy.info
26324	nmwnfrssxab.info	26324	hxbqndbm.info

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - Noise again
    - Example1, domain are **hardcoded** in malware, not DGA.

ID	fakeAV sites	ID	fakeAV sites
367	zujytuhehok.com	367	nixyxakuluna.com
367	rinysegaci.com	367	cimuxorazag.com
367	dakygyzav.com	367	bodiqynyjyjof.com
367	fyqesegyz.com	367	pinoguzeseme.com
367	qobirawif.com	367	horiqomep.com
367	cajarihejeluw.com	367	……

DNS Resolutions

- zujytuhehok.com
- lohyfyrasokiso.com
- lohyfyrasokiso.com.ovh.net
- mijywujysa.com
- mijywujysa.com.ovh.net
- miferyciq.com
- miferyciq.com.ovh.net
- fuxuvugyvupi.com

Refer: https://www.virustotal.com/#/file/cbfc857edb70dd5fef15a9498b96010ed16f3b139f6fa5c2cce84fe785b04996/behavior

Finding Highly Suspicious DGA

- Clustering the candidate DGAs
  - Noise again
    - example2, link farm, not DGA

ID	link farm
5491	www.av936.info
5491	www.av934.info
5491	www.av933.info
5491	www.av935.info
5491	www.av931.info
5491	www.av932.info

view-source:www.av942.info

```
<h5>友情链接</h5>
<ul>
<li><a href="http://www.av931.info/" target="_blank">神马影院</a></li>
<li><a href="http://www.av932.info/" target="_blank">罗马影院</a></li>
<li><a href="http://www.av933.info/" target="_blank">天仙影院</a></li>
<li><a href="http://www.av934.info/" target="_blank">玉兰影院</a></li>
<li><a href="http://www.av935.info/" target="_blank">水仙影院</a></li>
<li><a href="http://www.av936.info/" target="_blank">情色中心</a></li>
```

Finding Highly Suspicious DGA

- So we need to narrow down the result
  - Match
    - Each domain name
      - Only SLD+TLD && length(SLD) > 5
      - Number of rdata < 5
    - Each cluster
      - NXDOMAIN≥ 20%
      - Number of Domain names ≥ 4
  - Result
    - 100,000s to 10,000s

Finding Highly Suspicious DGA

- Result (still a super long list)
  - Example (2017-08-21)

ID	Susp_DGA1
37	n8g3weynq0.com
37	cry5vh1scj.com
37	0eh9qthmcn.com
37	jiz34u3weg.com
37	6w3u15y0c2.com
37	jofvwkk8kc.com
37	yv7n1woyl3.com

ID	Conficker
118	tlaqgqgw.ws
118	gaizhknmnyq.net
118	sidgrylw.com
118	suswyfwy.info
118	piopoku.cc
118	mfogpe.net
118	tovilt.cn

ID	Susp_DGA2
864	holqtz.com
864	efwyjr.com
864	bdxlpe.com
864	weobdt.com
864	wzwabg.com
864	npwoce.com
864	stkaoy.com

- So we are facing a list with ~10,000s highly suspicious DGA Domain names
- We could stop here
- Or not?

Locating Malware Sample

- We run malware samples in our sandbox
  - VT:~100K/d samples
  - 360:~ even more than VT
- MD5-domain pairs

```
[hdp-netlab d2m_sandbox]$ hadoop fs -text /home/hdp-netlab/md5_domain/vt.20170923.lzo \
> | grep 2f6e458c3d81fe9a155b05effe72ca3d | less
17/09/25 14:34:33 INFO util.NativeCodeLoader: Loaded the native-hadoop library
17/09/25 14:34:33 INFO compress.LzmaCodec: Successfully loaded & initialized native-lzma library
17/09/25 14:34:33 INFO lzo.GPLNativeCodeLoader: Loaded native gpl library
17/09/25 14:34:33 INFO lzo.LzoCodec: Successfully loaded & initialized native-lzo library
2f6e458c3d81fe9a155b05effe72ca3d        gacyryw.com
2f6e458c3d81fe9a155b05effe72ca3d        gacyzuz.com
2f6e458c3d81fe9a155b05effe72ca3d        gadyfuh.com
2f6e458c3d81fe9a155b05effe72ca3d        gadyniw.com
2f6e458c3d81fe9a155b05effe72ca3d        gahyhob.com
2f6e458c3d81fe9a155b05effe72ca3d        gahyqah.com
2f6e458c3d81fe9a155b05effe72ca3d        galykes.com
2f6e458c3d81fe9a155b05effe72ca3d        galyqaz.com
2f6e458c3d81fe9a155b05effe72ca3d        ganypih.com
2f6e458c3d81fe9a155b05effe72ca3d        gaqycos.com
```

Locating Malware Sample

- For suspicious domains
  - Have MD5
    - marked (by any vendor as malicious)
    - Unmarked (reverse engineering, most time consuming)
  - No MD5

Locating Malware Sample

- TID DGA
  - Time-independent and deterministic
    - Generates same domains all the time when it runs

```
67 2017-01-11 … DNS Standard query 0x2364 A bjvsjkday.com
68 2017-01-11 … DNS Standard query 0x19fc A pkwkbiggxlqvakqqxn.com
69 2017-01-11 … DNS Standard query 0x21da A mvpsefgsjvh.com
70 2017-01-11 … DNS Standard query 0xa86f A jgysjyvnchanx.com
76 2017-01-11 … DNS Standard query 0x0261 A kkujkajkeiobts.com
77 2017-01-11 … DNS Standard query 0x8bc6 A pjxmmfnykuiuuvefdic.com
78 2017-01-11 … DNS Standard query 0x6950 A meeaexhvlnhfalqyrc.com
79 2017-01-11 … DNS Standard query 0x1e19 A pkwkbiggxlqvakqqxn.com
80 2017-01-11 … DNS Standard query 0xfe97 A mvpsefgsjvh.com
```

2017-01-11

```
10 2017-09-25 … DNS Standard query 0xf6c9 A bjvsjkday.com
11 2017-09-25 … DNS Standard query 0x7692 A mvpsefgsjvh.com
12 2017-09-25 … DNS Standard query 0x02bd A pkwkbiggxlqvakqqxn.com
13 2017-09-25 … DNS Standard query 0x09f2 A jgysjyvnchanx.com
14 2017-09-25 … DNS Standard query 0x00df A fbtmdswerb.com
19 2017-09-25 … DNS Standard query 0xf97d A pjxmmfnykuiuuvefdic.com
20 2017-09-25 … DNS Standard query 0x7692 A mvpsefgsjvh.com
21 2017-09-25 … DNS Standard query 0xf6c9 A bjvsjkday.com
22 2017-09-25 … DNS Standard query 0x09f2 A jgysjyvnchanx.com
```

2017-09-25

Locating Malware Sample

- TID DGA
  - Exact match MD5
  - TID DGA family: 13/38

Banjori | Dircrypt | Fobber | Gspy | Matsnu
Pykspa | Ramnit | Rovnix | Shifu | Simda
Tempedreve | Tinba | Vawtrak

Locating Malware Sample

- TID DGA
  - New domains

/ltca2/related/cid_type/client_cid/val/201642/date/20160

20160106	-3	201642	12	612540	lcudlnkpyoj.com
20160106	-3	201642	12	612540	ofheubnonpg.com
20160106	-3	201642	12	612540	vwnaoeynisd.com
20160106	-3	201642	12	612540	xtlctubpuyy.com
20160106	-3	201642	12	612540	thbihlxurob.com
20160106	-3	201642	50	612542	wigwdjpfb.com
20160106	-3	201642	12	612540	ecemuammark.com
20160106	-3	201642	12	612540	wbylawgnume.com

lcudlnkpyoj.com
ofheubnonpg.com
vwnaoeynisd.com
xtlctubpuyy.com
thbihlxurob.com
wigwdjpfb.com
ecemuammark.com

Locating Malware Sample

- TID DGA

```
amac:netlab yiming$ fdark -d lcudlnkpyoj.com | sort -k 1

2016/05/10 18:42:24    234f13eb1713521c3c0d1ec62e301d10    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com
2016/05/11 14:55:10    41e68fdb73938237d5e3019cf6bc25e7    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com
2016/05/14 11:34:09    8bd626b116b110a81b1515f65575d764    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com
2016/05/15 19:09:33    c37b3bc4949e7093968bad9ea7f97071    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com
2017/04/06 22:46:14    cdddd7400e10010531f9ccad43e36fe7    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com    src=sandbox3    dga=1
2017/06/16 18:37:34    90b74ea0e5ff79a95c40c0356dcd2da2    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com    src=sandbox2    dga=1
2017/08/18 01:22:05    9c423856410559e0492764ae4db4763b    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com    src=sandbox2    dga=1
2017/09/09 06:28:50    05083a2417d66866a4f8aa776f46691d    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com    src=sandbox2    dga=1
2017/09/19 07:52:52    57fb7dada7336dc269d51f4f739dc525    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com    src=sandbox2    dga=1
2017/09/19 07:52:52    57fb7dada7336dc269d51f4f739dc525    dns_nx    server=172.16.1.1    domain=lcudlnkpyoj.com    src=sandbox3    dga=1
```

Locating Malware Sample

- TID DGA

234f13eb1713521c3
c0d1ec62e301d10
41e68fdb73938237
d5e3019cf6bc25e7
8bd626b116b110a8
1b1515f65575d764
…
6 samples

Ad-Aware	Win32.Ramnit.Y
ALYac	Win32.Ramnit.Y
Avast	Win32:Ramon
Avira	TR/AD.CeeInject.M.asgl
BitDefender	Win32.Ramnit.Y
ClamAV	Win.Virus.Ramnit-1850
Cyren	W32/Ramnit.Q

Results from Virustotal:
Ramnit, known DGA

New variant???

Locating Malware Sample

- TID DGA

lcudlnkpyoj.com
ofheubnonpg.com
vwnaoeynisd.com
xtlctubpuyv.c
thbihl
wigwdj
ecemua
wbylawg

234f13
21c3c0d
7d5e3
116b110a81b1
515f65575d764
…
6 samples

New variant of Ramnit
0xc17317b9

Locating Malware Sample

- TDD DGA
  - Time-dependent and deterministic
    - Generated different domains at different times

```
 1 2016-02-18 … DNS Standard query 0xaa2d A b24au7e7151avtyp.com
 3 2016-02-18 … DNS Standard query 0xa740 A i1vf61nyzrf9z20k.biz
 5 2016-02-18 … DNS Standard query 0x3800 A kib7zddueubzgmxv.info
 7 2016-02-18 … DNS Standard query 0xcae5 A 9pebg3k6rbk3deus.cn
 9 2016-02-18 … DNS Standard query 0x11de A 8viexhpdkf1ch40p.cn
11 2016-02-18 … DNS Standard query 0x90ac A voo1gpro3voghqqc.info
13 2016-02-18 … DNS Standard query 0x6bcb A wyaicoewvbgsrgr9.net
15 2016-02-18 … DNS Standard query 0x494a A 103wgmf8bgll67tj.info
17 2016-02-18 … DNS Standard query 0xcd19 A 8r4r95tpniaqsh3w.cn
19 2016-02-18 … DNS Standard query 0x7de2 A kdh9cbx8cte2jodp.info
21 2016-02-18 … DNS Standard query 0x06a6 A a7tjk8ltz4lj2agv.ru
23 2016-02-18 … DNS Standard query 0x4a60 A 11oxnlk9a0knq8fh.org
25 2016-02-18 … DNS Standard query 0x3a23 A i9hhskre1a6hguhd.info
27 2016-02-18 … DNS Standard query 0x56d9 A doh0rrp53e5h0h5g.org
```

2016-02-18

```
 1 2017-09-25 … DNS Standard query 0xbfc9 A zfjhpoc1zi63xnhb.ru
 3 2017-09-25 … DNS Standard query 0xa29a A pvgh2u4jixs6w1uf.ru
 5 2017-09-25 … DNS Standard query 0x4673 A 5msjm4yggahk5c35.org
 7 2017-09-25 … DNS Standard query 0xae1e A cvet68rs7t6ap5ea.ru
 9 2017-09-25 … DNS Standard query 0xf61f A yhyltqa9m2tkohgf.com
11 2017-09-25 … DNS Standard query 0xa1d2 A 3of5lfdnnfxiddo0.ru
13 2017-09-25 … DNS Standard query 0x167e A jx5bfftuxzhvhejf.ru
15 2017-09-25 … DNS Standard query 0x8ec7 A knip60but5zy5hwc.com
17 2017-09-25 … DNS Standard query 0x1cdc A lsy34bnm27aixm5g.net
19 2017-09-25 … DNS Standard query 0x9185 A rgaubcrqc13zechm.net
21 2017-09-25 … DNS Standard query 0xfb00 A rs69jgid6fqj45kp.org
23 2017-09-25 … DNS Standard query 0xa9f1 A 0fn1ladna8yd11zb.com
25 2017-09-25 … DNS Standard query 0x2b7b A kmslavk6fzdb8lqg.com
27 2017-09-25 … DNS Standard query 0x8147 A cyllpsnpl2g7va3a.com
```

2017-09-25

Locating Malware Sample

- TDD DGA

Family	Domains	Characteristics	e.g
Virut	10000 per day	TLDs: [com] SLD: Fix length of 6 a-z	hgznsb.com yvvioe.com zuzmoq.com
Ranbyus	40 per day	TLDs: [in, me, cc, su, tw, net, com, pw, org] SLD: A fix length of 14|17 a-y, missing z	oswwsbsmibofdi.net nslxbdyiofityx.com pnejirjyxjmycx.pw
Vidro	100 per week	TLDs: [dyndns.org, com, net] SLD: A length of 7-12 a-z	jfxetiogrvo.dyndns.org ckdypldcxi.com ilaalsylt.net
CCleaner	1 per month	TLDs: [com] SLD: A length of 11-13 mix a-f and 0-9	ab1145b758c30.com ab890e964c34.com ab3d685a0c37.com

In general, because of the difference in algorithms, domains generated by different families have different characteristics; But the domains generated by the same family at different times have the same characteristics.

Locating Malware Sample

- TDD DGA
  - Fuzzy match MD5
  - TDD DGA family: 25/38

Bamital	Blackhole	CCleaner	Chinad	Conficker
Cryptolocker	Emotet	Dyre	Gameover	Murofet
Necurs	Locky	Madmax	Mirai	Qadars
Suppobox	Nymaim	Padcrypt	Proslikefan	Symmi
Vidro	Ranbyus	Tofsee	Virut	XshellGhost

Locating Malware Sample

- TDD DGA
  - Chinad

/ltca2/related/cid_type/cid/val/622578/date/20160807/

LTCA2 | cid(622578)

date	server_cid (1)	client_cid (1)	domain_cid (1)	cid (1)	domain
20160807	-5	0	171	622578	0fzxftj2p9pteghq.info
20160807	-5	0	171	622578	17jjcz1ww4weqtjc.com
20160807	-5	0	171	622578	1b8vtddz6iaamnc2.info
20160807	-5	0	171	622578	1bbca0ps2egaceeu.net
20160807	-5	0	171	622578	1kb33oizszsc9zll.info

0fzxftj2p9pteghq.info
17jjcz1ww4weqtjc.com
1b8vtddz6iaamnc2.info
1bbca0ps2egaceeu.net
1kb33oizszsc9zll.info
……

Locating Malware Sample

- TDD DGA
  - Find the naming pattern, fuzzy match

0fzxftj2p9pteghq.info
17jjcz1ww4weqtjc.com
qowhi81jvoid4j0m.biz
1bbca0ps2egaceeu.net
53ptxfec6a4mwbrl.org
ou16nagv4pashauc.ru
d9tan26jpjpz9snt.cn ……

TLDs: [org, ru, cn, net, info, biz, com]
SLD： 16
SLD： a-z, 0-9

Locating Malware Sample

- TDD DGA
  - Search the sandbox dns-md5 pairs

```
[hdp-netlab          ]$ cat search_by_featrue.output
55c447191d9566c7442e25c4caf0d2fe        am3kuucsxqldkfqg.info
55c447191d9566c7442e25c4caf0d2fe        w14iwr0xptbg5hxy.biz
55c447191d9566c7442e25c4caf0d2fe        0aa05rcmqxnz7vzj.net
55c447191d9566c7442e25c4caf0d2fe        akylgdz7hvtdbv27.cn
55c447191d9566c7442e25c4caf0d2fe        5rdjt2j29u80vmaq.ru
55c447191d9566c7442e25c4caf0d2fe        a147xjazb4oq5geg.info
55c447191d9566c7442e25c4caf0d2fe        tjklzgosi2xivjs4.biz
55c447191d9566c7442e25c4caf0d2fe        e8xm3w0md5eig27n.biz
55c447191d9566c7442e25c4caf0d2fe        a2jwc2n6cs6xexfs.org
55c447191d9566c7442e25c4caf0d2fe        qxwvtrcqcav8bnr1.info
55c447191d9566c7442e25c4caf0d2fe        3qa9i5r626pd0wtq.biz
55c447191d9566c7442e25c4caf0d2fe        b5ucw6o72p1f2yec.cn
55c447191d9566c7442e25c4caf0d2fe        gagy110933myxtng.com
```

Locating Malware Sample

- TDD DGA

55c447191d9566c7
442e25c4caf0d2fe

New DGA???

Results from Malwarebytes blog:
Chinad, unknown

Locating Malware Sample

- TDD DGA

0fzxftj2p9pteghq.info
17jjcz1ww4weqtjc.com
qowhi81jv
1bbca0ps2e
53ptxfec6a4
ou16nagv4pa
d9tan26jpjpz9snt.cn
……

91d9566c7
2e25c4caf0d2fe

New DGA family
Chinad

Practical Blocking Experience

- DGA database
  - 90M records
  - TDD DGA pre-generated 30days
- DGA block list
  - 1M active domains

Practical Blocking Experience

- False positive
  - Domain collision: DGA domains are same with legit domains
  - Virut
    - TLD: com; SLD: 6 letters, a-z
    - 10000 domains/d

Some collision example	Effective date
aliyun.com	2000-06-27
google.com	2000-07-14
xiaomi.com	2002-02-06
amazon.com	2003-03-24

Practical Blocking Experience

- False positive
  - fix
    - Same client accesses many active DGAs in one day
    - Popular rank

Some collision example	Popular rank
aliyun.com	7.5
google.com	8.7
xiaomi.com	6.4
amazon.com	7.6

Practical Blocking Experience

- False positive
  - IP block
    - From block list to non-C&C IP
    - Sinkhole
      - DNS sinkhole
      - https://en.wikipedia.org/wiki/DNS_sinkhole
    - Parking
      - Domain Parking
      - https://en.wikipedia.org/wiki/Domain_parking
    - Wildcard Domain Name
      - https://en.wikipedia.org/wiki/Wildcard_DNS_record

Practical Blocking Experience

- False positive
  - IP blocking - sinkhole
  - 2017-08-18

Family	FQDN	IP	Whois
Conficker	adbvjdtitzi.biz lfphs.biz zlgqkebcgei.biz	104.244.14.252 38.102.150.27	NS.CONFICKER-SINKHOLE.COM NS.CONFICKER-SINKHOLE.NET NS.CONFICKER-SINKHOLE.ORG
Gameover	l7lps31x4atfg17cd65alabnoi.org	208.100.26.251	Sinkhole Security
Chinad	na3jbmyctela409i.org	208.100.26.251	Sinkhole Security
Locky	wkrlygtpwvuw.org juhpyworipo.fr	208.100.26.251	Sinkhole Security
Suppobox	leaveneedle.net materialcompany.net	208.100.26.251	Sinkhole Security

Practical Blocking Experience

- False positive
  - IP blocking - parking
    - Our blog: Conficker domain rare being abused
    - http://blog.netlab.360.com/conficker-domain-abuse/

IP	Domain	Total
195.22.126.212(Poland)	aqiapn.org blbgfa.org azzaf.info …	511
166.78.101.108(USA)	ejzyy.org hsgan.info qrltvy.org …	159
213.184.126.162(Israel)	ankpw.info axwmn.org atcmg.org …	552

Practical Blocking Experience

- False positive
  - IP blocking - Wildcard Domain Name

Family	Time	FQDN	IP
Necurs	2017-08-18	ctfghwiipaqhc.pw kiieglmrxhemwluwpdi.pw	141.8.226.58
Dyre	2017-08-21	v58471dbc9934f47df4eceb33ab16ce461.ws n0fc8598e7859b48c0728361cdddc835a9.ws p48699fe54790b358f577c69eb722c8c45.ws	64.70.19.203
Bamital	2017-08-21	6e7614809cbe50cf6f33960d51bd3c2c.cz.cc 87bb73904ee5f2e266b079ef6394b228.co.cc	43.229.108.32 175.126.123.219
Locky	2017-08-21	agaenaxwfsjxct.pw xddxtlkwlrupl.pw	141.8.226.58

Practical Blocking Experience

- False positive
  - White list

Category	API
Sinkhole	api.netlab.corp.qihoo.net/sinkdb
Parking	api.netlab.corp.qihoo.net/dparking
Wildcard Domain Name	api.netlab.corp.qihoo.net/dwa

Practical Blocking Experience

- False negative
  - Timing
    - TDD DGA vs DNS time

Family	Query time	DNS	Effective time
Conficker	2017-08-20	vmfxswkzuch.com vfvtspc.ws texwccgg.info	2014-07-10 08:00:00 ~ 2014-07-11 07:59:59
Necurs	2017-05-21	hyktbhrkwkptfpwke.com tmahdoh.net wbdoxbwihylcaobhpb.com	2017-05-24 00:00:00 ~ 2017-05-27 23:59:59
Gameover	2015-12-11	qcrgptwrwtlvtohetxwprpnuw.org zxlxkfmgihaxwuwjfucijr.org mrdyhwlnzfuqwxyhnvhwkjlto.org	2016-12-21 00:00:00 ~ 2016-12-27 23:59:59

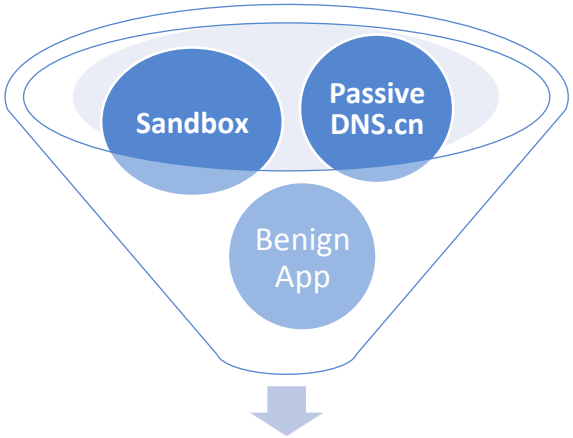
Practical Blocking Experience

- False negative
  - Bug in algorithms
    - Rovnix
      - TID DGA, SLD length: 18, a-z and 1-8
      - We generate 10000 FQDNs for every variant
      - There is not exit condition, there will always be new FQDNs if the malware keeps running

Seed	FQDN	Sequence (>10000)	PDNS records
0x3c51	yqgurqe4xu2skkldr7.cn zqdwjaaaqa82yb2hsy.cn	10005 11958	105 uniq client IPs 98 uniq client Ips
0x59da	yiefhxjbsuget1kvbv.cn kx7ibskwdh2bo38iz7.cn	10005 10681	17 uniq client Ips 18 uniq client Ips
0x4719	q2hhw4gxndjafagk6o.cn 1438j6m57cbk7g44q2.cn	10017 10668	2 uniq client IPs 2 uniq client Ips

Want to Make Contributions?

- GitHub repository
  - Suspicious DGA domains from PDNS
  - Uncertain DGA samples from sandbox
  - DGA in benign App



https://github.com/360netlab/DGA

Q&A