阿里云 | 云盾先知 安全情报

DNS中的“奇葩数据”解析

先知白帽大会
开放创新·先知先行

关于我们

- 360网络安全研究院
  - netlab.360.com
  - 数据
    - 挑选数据，产出数据，数据分析与挖掘
- 部分开放平台
  - PDNS：passivedns.cn
  - DoS监控：ddosmon.net
  - 全网扫描监控：scan.netlab.360.com
  - 开放数据：data.netlab.360.com

Netlab 360.com

Home DGA EK MalConn Mirai Scanner Mirai C2 DRDoS Reflector

Netlab OpenData Project

By Network Security Research Lab at 360

Description

The Netlab OpenData project was presented to the public first at ISC' 2016 on August 16, 2016. We currently provide multiple data feeds, including DGA, EK, MalCon, Mirai-Scanner and Mirai C2, and DRDoS Reflector.

We share these data feeds to the security community, looking forward to improve the cyberspace security. And contributor are welcome to provide us more data to expand the diversity of current data feeds.

Outliner

- Domain
  - DGA
  - DNS suffix
  - 组合
  - IDN域名
- IP
  - Sinkhole
  - NXDOMAIN
  - 特殊用途IP
  - 开源情报（OSINT）

“奇葩Domain”

- 先看几组域名

```
o594de30e878a211a56c90acab08de7adc.cc
hcf35c452fc744b36653774b05859d5502.cn
u6f28440b8649db41985e1bf036dd65226.cc
o52946f088a5dc2f51985f57b1cd70f2e0.cc
p78f75b5dbae6f80a67762f51e8c2be058.ws
he614eb55d093977f6aa9582671fdd64f6.cn
o6ffa5d75a147c189a80490bb96c335af0.to
e2790713da0820b43fb0a4c85a734a22fb.cc
d8654ecea0a8a5f22ef2732abedba902f6.ws
bccd4cabb8bd14546af2bf4c3aaca91093.ws
k1a9b8bbb1d6567d55c898f442c467805f.tk
ffd30a8f13e0b114f364bbd1ecf8c9f1cd.cn
h7372c048d9d661b1ca07514d6c0005967.in
e4e38df5e87a39c284d107b9317e3eff97.to
w06b9180d42309a5b0ae21956f8881d7d4.to
h05baeb41e72d3686ad9913d74c3f83635.cn
```

```
xmawhfglbcm.you
qpztqimfv.you
vofizwdpscvusnw.you
adixjvamwepsyrn.you
fikzjru.you
obwjfrcxebod.you
jvjygzxrundqk.you
afpcrzea.you
rwcyotobkwgzwe.you
odukeitxzfql.you
ekjzdnq.you
aioswetntayrd.you
cugmplyn.you
life.china.com.cn.you
mmmzgbovvhiric.you
dwutyxszuziwvkk.you
```

```
vwhwijlsuo5q1kv5wct0vc2tvd.cnn.com
qw4kootxrtchltjslatqv5umba.com
xblnrfzxsidruofhaksmcwkwtg.com
mmgatj1roq510kjshsqgffc3oh.com
ljfw0jdqj331tcnelpscsawc4a.com
iks4zlfrrannez31gzsc50zyea.com
mitnwtfxwtladeb21lqgacwqbc.com
gvrwn4huo4ih0jcwf1todfbame.com
l4dvr5fwpd2ajrphecq0gpvqwf.com
a2kji42ry3ueqittyrrcfrcgpb.com
fsnfzczwv33d3nyu5xrgzytdld.com
0mzd2hiwrpggxx1wgrsmv0il5a.ask.com
of3y4perr1v3kyqy24qe1n2knd.com
fhrgodpsdticfdututsiiurfhh.blogger.com
4vd2lofvx34yw2zc1bqg32zyuh.com
reudbnzvds25pk50lrryntuxde.go.com
```

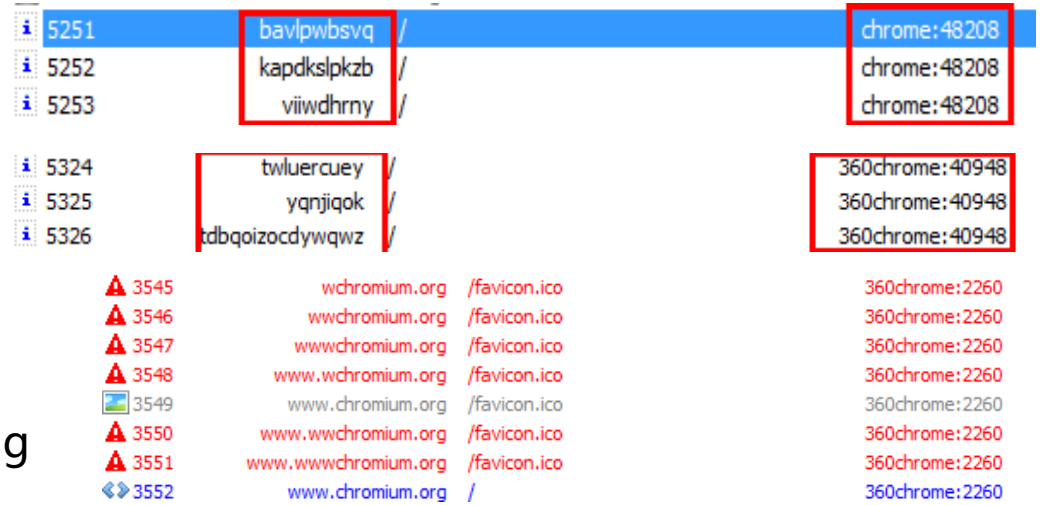
“奇葩Domain”

- DGA
  - Malware
    - Example: Dyre
  - 垃圾站群
    - 批量购买二级域名
    - 前缀生成器生成子域

eslttkc.1xq3f.faith	41	1	1703181440	1703181440	23.89.10.147
xgmhkjxjg.1xq3f.faith	41	1	1703181040	1703181040	23.89.10.147
lhckjjglsjl.1xq3f.faith	41	1	1703180925	1703180925	23.89.10.147
nbjdsms.1xq3f.faith	41	1	1703180800	1703180800	23.89.10.147
cdrjsdj.1xq3f.faith	41	1	1703181425	1703181425	23.89.10.147
xgsszztwqr.1xq3f.faith	41	1	1703180840	1703180840	23.89.10.147
xgmhbjctk.1xq3f.faith	41	1	1703181455	1703181455	23.89.10.147
hdxptyx.1xq3f.faith	41	1	1703181445	1703181445	23.89.10.147
ptyxgslt.1xq3f.faith	41	1	1703181205	1703181205	23.89.10.147
lhstdygs.1xq3f.faith	41	1	1703180855	1703180855	23.89.10.147
ssqxglhct.1xq3f.faith	41	1	1703180525	1703180525	23.89.10.147
xgsmhhdx.1xq3f.faith	41	1	1703180845	1703180845	23.89.10.147

“奇葩Domain”

- DGA
  - Chrome 探测
    - Pattern
    - 周期
  - DNS benchmark
    - pattern
  - others
    - Omnibox prefetching
    - 特定CNAME
    - …



“奇葩Domain”

- DNS suffix
  - PC
    - 个人
    - 公司/组织
  - 路由器
    - 用于区分内外网

```
C:\Documents and Settings\zzf>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : zzf-f037f78939b
        Primary Dns Suffix  . . . . . . . : fortest.com
        Node Type . . . . . . . . . . . . : Unknown
```

```
C:\Documents and Settings\zzf>nslookup www.360.cn
Server:  [redacted]
Address:  192.168.0.222

Non-authoritative answer:
Name:    www.360.cn
Address:  106.120.167.67
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	192.168.0.222	DNS	82	Standard query A www.360.cn.fortest.com
2	0.000649	192.168.0.222	10.0.2.15	DNS	144	Standard query response, No such name
3	0.001003	10.0.2.15	192.168.0.222	DNS	70	Standard query A www.360.cn
4	0.001543	192.168.0.222	10.0.2.15	DNS	86	Standard query response A 106.120.167.67

“奇葩Domain”

- 组合
  - DGA + DNS suffix
  - Host + DNS suffix

source: http://img2.iautos.cn/upload/2014/11/3/289080141103115106.jpg

“奇葩Domain”

- DGA + DNS suffix
  - Chrome + DNS suffix
    - DNS suffix == TLD
    - DNS suffix == router AP
    - DNS suffix == 公司域名

```
jonsmfhzivmg.tendaap
fnqrctlzbrbrglu.tendaap
lmtqsvhrntdefzn.tendaap
adtgkyt.tendaap
wlgqsujhei.tendaap
whavgvplwluanqf.tendaap
sssetbeuq.tendaap
wvffrhagix.tendaap
ofnmlvuslg.tendaap
gzpyyzbtwi.tendaap
```

```
wfkvfjyi.cn.juniper.net
cawjhwwonat.cn.juniper.net
lbzfrntkdveq.cn.juniper.net
rvuswdjz.cn.juniper.net
qdfnzqzafnaqo.cn.juniper.net
gcuoulns.cn.juniper.net
zqggsdqnac.cn.juniper.net
kvmsaqegsbpvyod.cn.juniper.net
xnafjknptw.cn.juniper.net
awjzjvczw.cn.juniper.net
wkczlcxrjqx.cn.juniper.net
```

“奇葩Domain”

- DGA + DNS suffix
  - Malware + DNS suffix
    - 泛解析

```
zokskmhs.org.yadon.com
nvvaemrbwr.biz.yadon.com
yovcgrv.org.yadon.com
ppmyevvfydj.net.yadon.com
xyamjrygba.biz.yadon.com
tipdgbk.info.yadon.com
ivxlxtsc.info.yadon.com
ztkfd.cc.yadon.com
xnyxss.org.yadon.com
vnuvrsi.net.yadon.com
xakemgpi.net.yadon.com
zkjij.cc.yadon.com
tmmgjzak.biz.yadon.com
ibuayj.net.yadon.com
psebnaw.net.yadon.com
ntvnasy.cc.yadon.com
```

“奇葩Domain”

- Host + DNS suffix
  - Nested domain
    - VS Phishing domain

正常域名

```
img.wsdl.vivo.com.cn.jsahvc.edu.cn
ynuf.alipay.com.jsahvc.edu.cn
h5.m.taobao.com.jsahvc.edu.cn
ifs.tanx.com.jsahvc.edu.cn
dorangesource.alicdn.com.jsahvc.edu.cn
ww1.sinaimg.cn.jsahvc.edu.cn
s1.ananas.chaoxing.com.jsahvc.edu.cn
log.voicecloud.cn.jsahvc.edu.cn
i9.pdim.gs.jsahvc.edu.cn
```

钓鱼域名

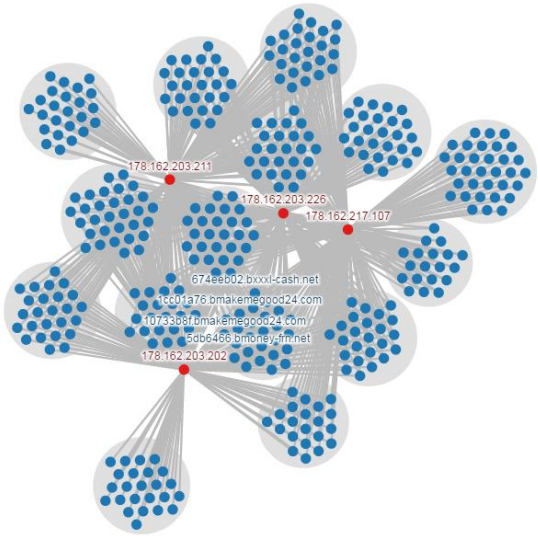
```
touzi.sina.com.cn.444nnn444nnn.top
licaishi.sina.com.cn.rgtzp.loan
licaishi.sina.com.cn.wcyyk.loan
apple.com.inacr.cn
licaishi.sina.com.cn.99ua.top
licaishi.sina.com.cn.qhstm.trade
licaishi.sina.com.cn.nhckf.loan
licaishi.sina.com.cn.hptkt.loan
licaishi.sina.com.cn.wxkch.trade
```

“奇葩Domain”

- IDN域名
  - 初衷
    - 方便非英语国家上网
  - 问题
    - 隐私泄漏（IM）

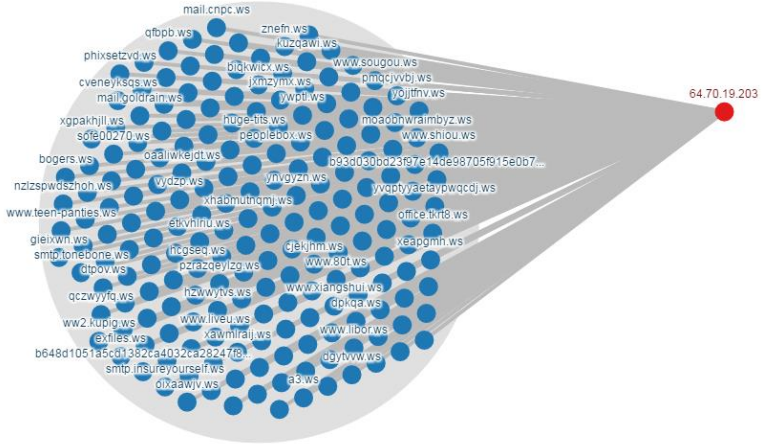
“奇葩IP”

- Sinkhole
  - 对恶意软件的C2域名进行接管的IP地址
  - 遇到sinkhole IP 说明什么
    - 分析落后于人
    - 可能被分析
  - Sinkhole的列表
    - abuse.ch
    - 360netlab



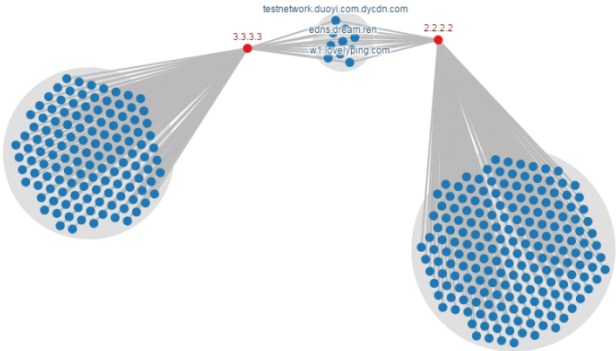
“奇葩IP”

- NXDomain → fake IP
  - ISP的问题
    - chrome 随机串
  - 安全厂商/安全DNS提供商
    - OpenDNS, OneDNS
  - 官方泛解析
    - ccTLD
      - WS/SY/PH
      - Dyre中的*.ws
    - 动态域名
      - *. cba.pl ， *.3322.net



“奇葩IP”

- 特定用途的IPs
  - 1.1.1.1/2.2.2.2/8.8.8.8/114.114.114.114…
    - 原因及危害
    - 建议设置
  - 保留地址
    - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
    - **192.0.2.0/24, 198.51.100.0/24 …**
  - ICANN
    - 127.0.53.53
    - URS



“奇葩IP”In OSINT

- “奇葩IP”在OSINT中的命中情况
  - Sinkhole：48%
  - NXDOMAIN: **93.3%**
  - Reserved：3.2%
  - Root server：**100% [shock]**

“奇葩IP” In OSINT

- 来源分布

	Team-cymru	bambenekconsulting	emergingthreats	alienvault	abuse.ch	talosintel	autoshun	dshield	spamhaus	malwaregroup	surriel
sinkhole	20	69	16	23	25	12	3	6	6	2	3
NXDOMAIN	18	7	2	7	4	3	2	11	27	0	0
Reserved	2	3	1	0	0	0	0	29	28	0	2
Root server	0	0	0	0	0	0	0	13	0	0	0

“奇葩IP” In OSINT

- 时间分布

	2014	2015	2016	2017
sinkhole	32	99	96	19
NXDOMAIN	20	65	79	22
Reserved	4	42	65	26
Root server	0	0	13	13

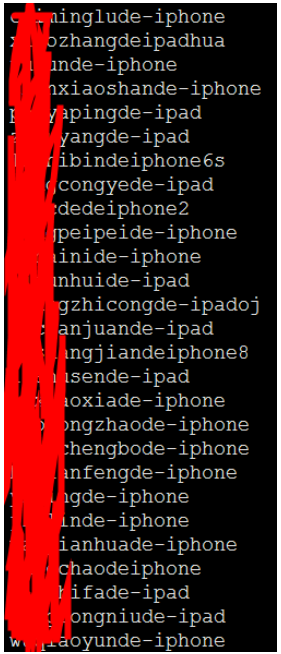
Reference

- https://en.wikipedia.org/wiki/Domain_generation_algorithm
- https://en.wikipedia.org/wiki/Reserved_IP_addresses
- https://en.wikipedia.org/wiki/DNS_sinkhole
- https://sinkdb.abuse.ch/
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dyre-emerging-threat.pdf
- https://www.icann.org/news/announcement-2-2014-08-04-zh
- https://mikewest.org/2012/02/chrome-connects-to-three-random-domains-at-startup
- https://www.icann.org/en/system/files/files/name-collision-mitigation-final-28oct15-en.pdf
- https://www.grc.com/dns/benchmark.htm

构建安全大厦，从造砖，搬砖开始

微博：zhangzaifeng1 ，招砖家：http://netlab.360.com/careers

从DNS看apple设备...




阿里云
云盾先知
安全情报
THANKS!