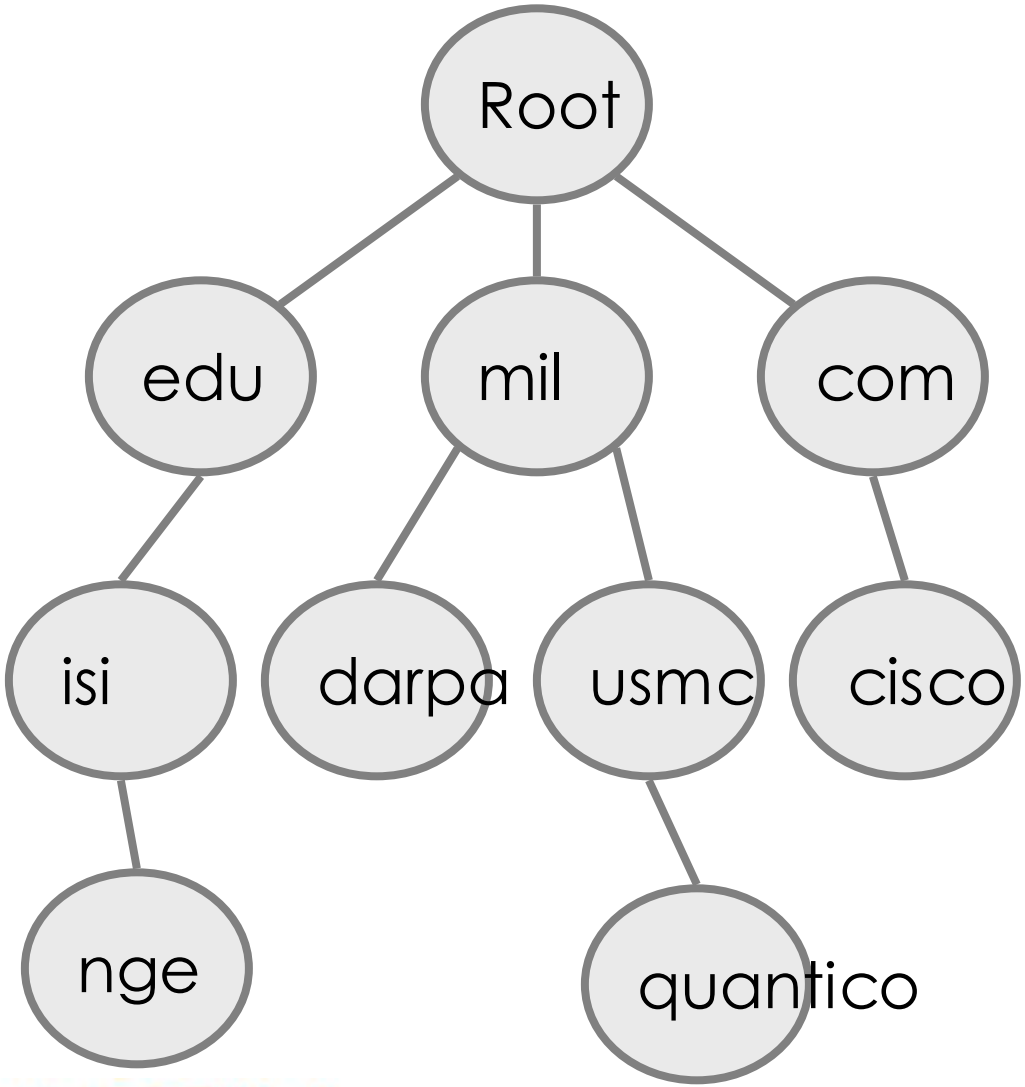
DNS攻击与防御

关于我

- ID:LION_00
- 当当网
- CCIE （Sec） && CISSP

关于DNS



DNS故障.CN域名凌晨大面积瘫痪 或为根服务器受攻击

字号: 小 中 大　　2013-08-25 09:58:31　　更多　评 论 54

关键字 >> 互联网 .CN域名 DNS CN域名无法解析 DNS故障 域名解析 CNNIC IT新浪潮

8月25日凌晨，根据中国最大的DNS解析服务商DNSPod的监控，CN的根域授权DNS全线故障，所有CN域名均无法解析，凌晨4点左右，.CN域名的解析恢复正常。

您的位置：新华网主页 － 新华社会

百度遭黑客攻击陷入瘫痪 DNS解析记录被篡改

2010年01月12日 12:10:47　来源：新华网

【字号 大 中 小】 【留言】 【打印】 【关闭】 【Email推荐： 提交 】

新华网北京１月１２日电（记者顾洪洪）１月１２日７点钟开始，国内最大搜索引擎百度遭到黑客攻击，长时间无法正常访问。据瑞星反病毒专家分析，这次攻击百度的黑客疑似来自境外，利用了ＤＮＳ记录篡改的方式。

据了解，这是自百度建立以来，所遭遇的持续时间最长、影响最严重的黑客攻击，网民访问百度时，会被定向到一个位于荷兰的ＩＰ地址，百度旗下所有子域名均无法正常访问。

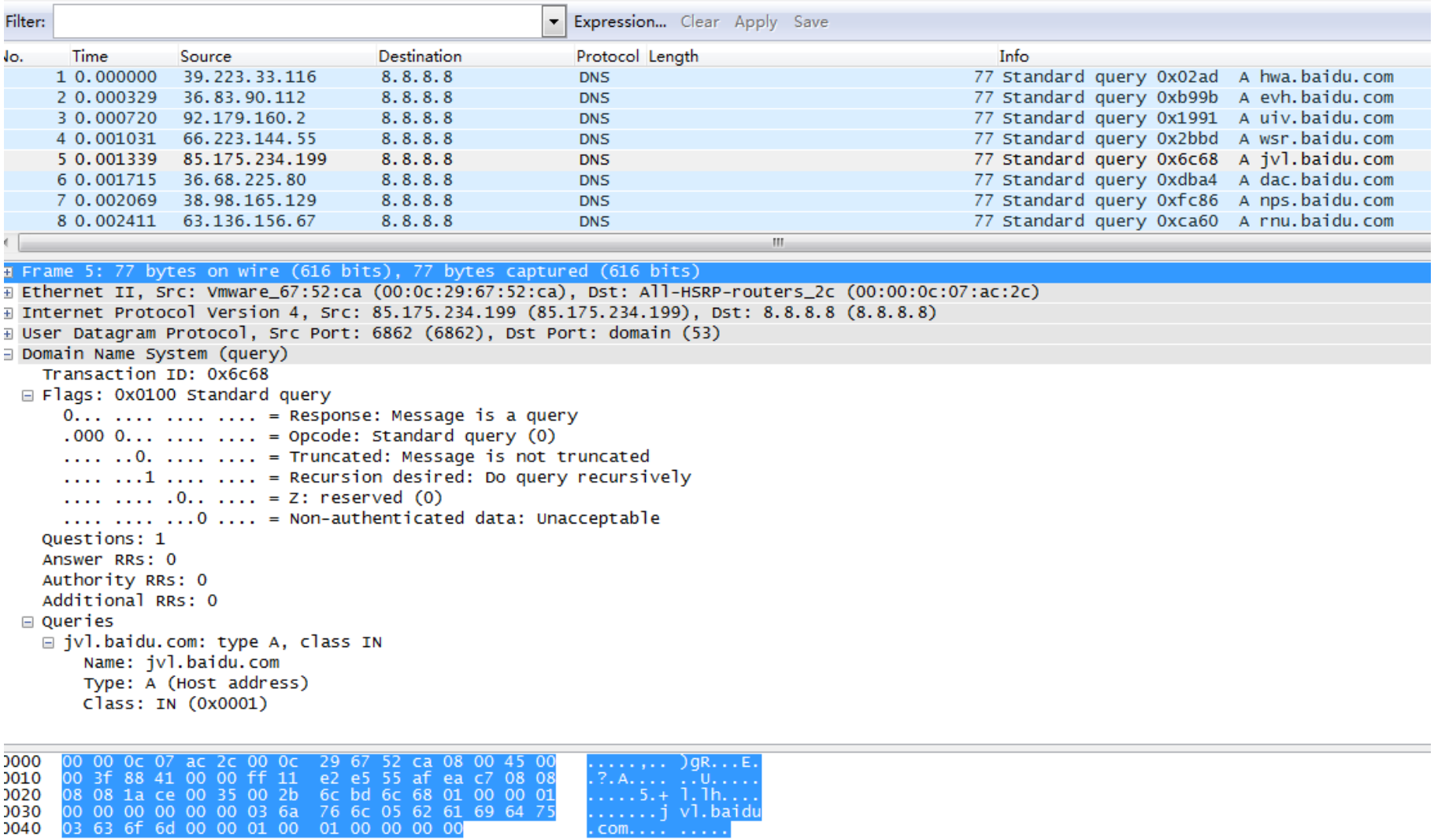
DNS 正常请求

```
⊞ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
⊞ Ethernet II, Src: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24), Dst: D-Link_21:99:4c (00:05:5d:21:99:4c)
⊞ Internet Protocol Version 4, Src: 192.168.0.114 (192.168.0.114), Dst: 205.152.37.23 (205.152.37.23)
⊞ User Datagram Protocol, Src Port: polestar (1060), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x180f
  ⊟ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ wireshark.org: type A, class IN
        Name: wireshark.org
        Type: A (Host address)
        Class: IN (0x0001)
```

DNS 正常回应

```
⊞ Frame 2: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
⊞ Ethernet II, Src: D-Link_21:99:4c (00:05:5d:21:99:4c), Dst: HonHaiPr_6e:8b:24 (00:16:ce:6e:8b:24)
⊞ Internet Protocol Version 4, Src: 205.152.37.23 (205.152.37.23), Dst: 192.168.0.114 (192.168.0.114)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: polestar (1060)
⊟ Domain Name System (response)
    [Request In: 1]
    [Time: 0.091164000 seconds]
    Transaction ID: 0x180f
  ⊟ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ wireshark.org: type A, class IN
        Name: wireshark.org
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ wireshark.org: type A, class IN, addr 128.121.50.122
        Name: wireshark.org
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 4 hours
        Data length: 4
        Addr: 128.121.50.122 (128.121.50.122)
```

DNS Query



DNS Query

- 难度 ★
- 破坏力 ★

DNS Amplification

< 特征 >	< 时间戳 >	< 来源 地址 >
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:30:07	81.177.141.202:64934
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:30:00	99.164.189.237:36896
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:56	192.169.80.130:51224
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:47	174.5.148.97:6553
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:45	87.72.75.71:39222
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:45	63.142.111.71:7229
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:43	78.83.29.137:17842
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:41	5.254.100.146:27070
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:39	192.169.81.94:62774
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:31	68.35.245.3:1470
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:30	119.63.38.52:37261
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:29	179.98.25.210:61692
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:25	125.253.114.8:33717
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:06	112.78.14.6:57805
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:02	177.35.121.174:48794
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:29:00	99.155.176.65:14492
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:55	69.162.101.102:2810
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:54	192.169.80.130:57675
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:53	31.170.161.250:6033
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:36	50.97.182.19:54194
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:36	78.83.29.137:56699
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:26	198.50.239.98:54433
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:26	192.184.11.133:27685
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:25	192.169.81.94:25432
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:25	125.253.114.8:48969
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:24	119.63.38.52:44825
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:18	87.72.75.71:64197
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:18	81.177.141.202:18979
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:17	71.93.188.198:65521
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:14	174.5.148.97:58400
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:09	179.98.25.210:59916
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:05	95.211.220.42:52658
ET CURRENT_EVENTS DNS Amplification Attack Inbound	2013-10-15 14:28:04	5.254.100.146:40831

DNS放大攻击

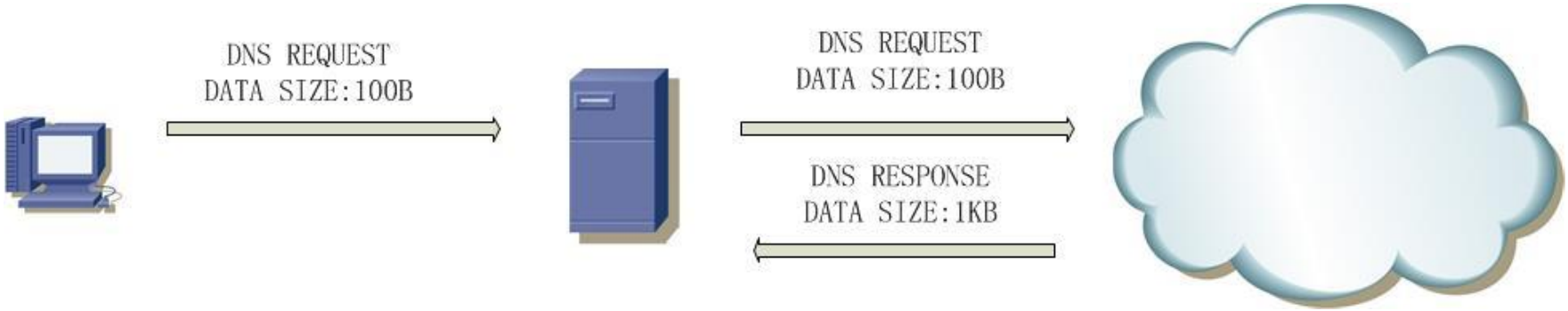
```
    3 0.000473   192.168.248.248    199.223.126.187    DNS
```

```
Answers
  irlwinning.com: type A, class IN, addr 1.1.1.143
  irlwinning.com: type A, class IN, addr 1.1.1.144
  irlwinning.com: type A, class IN, addr 1.1.1.145
  irlwinning.com: type A, class IN, addr 1.1.1.146
  irlwinning.com: type A, class IN, addr 1.1.1.147
  irlwinning.com: type A, class IN, addr 1.1.1.148
  irlwinning.com: type A, class IN, addr 1.1.1.149
  irlwinning.com: type A, class IN, addr 1.1.1.150
  irlwinning.com: type A, class IN, addr 1.1.1.151
  irlwinning.com: type A, class IN, addr 1.1.1.152
  irlwinning.com: type A, class IN, addr 1.1.1.153
  irlwinning.com: type A, class IN, addr 1.1.1.154
  irlwinning.com: type A, class IN, addr 1.1.1.155
  irlwinning.com: type A, class IN, addr 1.1.1.156
```

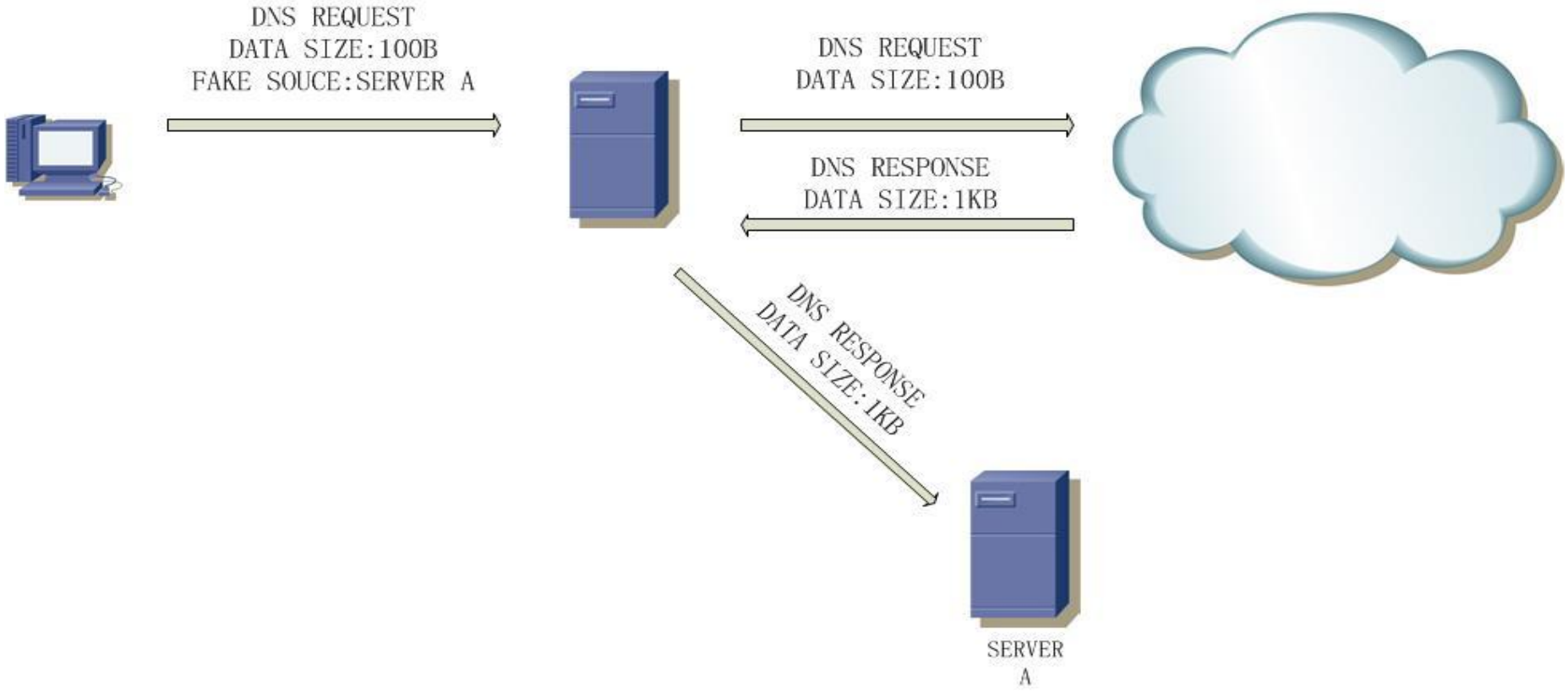
```
0000  00 1c 54 ff 08 15 6c 9c  ed 4f 39 41 08 00 45 00   ..T...l. .O9A..E.
0010  04 07 6c 13 01 72 3f 11  0a 25 c0 a8 f8 f8 c7 df   ..l..r?. .%......
0020  7e bb 10 52 00 04 01 01  01 54 c0 0c 00 01 00 01   ~..R.... .T......
0030  00 00 10 52 00 04 01 01  01 55 c0 0c 00 01 00 01   ...R.... .U......
0040  00 00 10 52 00 04 01 01  01 56 c0 0c 00 01 00 01   ...R.... .V......
0050  00 00 10 52 00 04 01 01  01 57 c0 0c 00 01 00 01   ...R.... .W......
0060  00 00 10 52 00 04 01 01  01 58 c0 0c 00 01 00 01   ...R.... .X......
```

DNS放大攻击

DNS放大攻击


DNS REQUEST
DATA SIZE:100B
DNS REQUEST
DATA SIZE:100B
DNS RESPONSE
DATA SIZE:1KB

DNS放大攻击


DNS REQUEST
DATA SIZE:100B
FAKE SOUCE:SERVER A
DNS REQUEST
DATA SIZE:100B
DNS RESPONSE
DATA SIZE:1KB
DNS RESPONSE
DATA SIZE:1KB
SERVER
A

DNS放大攻击

- 难度 ★ ★ ★
- 破坏力 ★ ★ ★ ★

DNS Refuse

No.	Time	Source	Destination	Protocol	Length	Info
400	0.167164	188.162.160.71		DNS		91 Standard query response 0xafd2 Refused
542	0.219396	143.89.15.72		DNS		89 Standard query response 0xb004 Refused
708	0.280743	143.89.15.72		DNS		89 Standard query response 0xb005 Refused
840	0.341190	143.89.15.72		DNS		89 Standard query response 0xb006 Refused
5242	2.347840	83.233.79.37		DNS		89 Standard query response 0xb026 Refused
6359	2.783110	83.233.79.37		DNS		89 Standard query response 0xb027 Refused
9671	4.202994	74.95.161.65		DNS		64 Standard query response 0xb071 Refused
10280	4.494970	74.95.161.65		DNS		64 Standard query response 0xb072 Refused
14735	6.688643	202.156.1.28		DNS		89 Standard query response 0xb0e5 Refused
15724	7.202353	202.156.1.28		DNS		89 Standard query response 0xb0e6 Refused
15800	7.235333	66.129.96.228		DNS		90 Standard query response 0xb0e9 Refused
16040	7.328336	88.215.63.129		DNS		90 Standard query response 0xb0e3 Refused
16913	7.730559	202.156.1.28		DNS		89 Standard query response 0xb0e7 Refused
16952	7.744777	88.215.63.129		DNS		90 Standard query response 0xb0e4 Refused
18369	8.368736	203.115.0.46		DNS		89 Standard query response 0xb110 Refused
18540	8.449715	130.203.1.4		DNS		88 Standard query response 0xb151 Refused
19437	8.814782	203.115.0.46		DNS		89 Standard query response 0xb111 Refused
20262	9.170345	112.126.32.234		DNS		64 Standard query response 0xb187 Refused
20277	9.177745	112.126.32.234		DNS		64 Standard query response 0xb188 Refused
20290	9.184605	112.126.32.234		DNS		64 Standard query response 0xb189 Refused
20916	9.488437	130.203.1.4		DNS		88 Standard query response 0xb153 Refused
23018	10.345644	220.152.32.145		DNS		91 Standard query response 0xb1ba Refused
23512	10.529830	220.152.32.145		DNS		91 Standard query response 0xb1bb Refused
23988	10.710831	220.152.32.145		DNS		91 Standard query response 0xb1bc Refused

```
⊞ Frame 23988: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
⊞ Ethernet II, Src: Cisco_1f:ad:c3 (04:fe:7f:1f:ad:c3), Dst:
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 4094
⊞ Internet Protocol Version 4, Src: 220.152.32.145 (220.152.32.145), Dst:
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 47081 (47081)
⊞ Domain Name System (response)
```

```
0000  00 01 d7 b8 7d 83 04 fe                          ....}... ........
0010  08 00 45 00 00 49 a3 96                          ..E..I.. @...2A..
0020  20 91 c0 a8 fb f9 00 35                           ......5 ...5....
0030  80 05 00 01 00 00 00 00                          ........ ...145.3
0040  32 03 31 35 32 03 32 32                          2.152.22 0.in-add
0050  72 04 61 72 70 61 00 00                          r.arpa.. ...
```

DNS Refuse

- 难度 ★ ★ ★
- 破坏力 ★ ★ ★

DNS污染

- 为什么不能访问facebook （一）

```
C:\Users\lion>nslookup www.facebook.com 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
名称:    www.facebook.com
Addresses:  59.24.3.173
          78.16.49.15


C:\Users\lion>nslookup -vc www.facebook.com 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
名称:    star.c10r.facebook.com
Addresses:  2a03:2880:f00d:501:face:b00c:0:1
          31.13.70.17
Aliases:  www.facebook.com
```

203.98.7.65
78.16.49.15
243.185.187.39
93.46.8.89
37.61.54.158
59.24.3.173
159.106.121.75
8.7.198.45
46.82.174.68

DNS污染

- 为什么不能访问facebook （二）

No.	Time	Source	Destination	Protocol	Length	Info
74	5.322182000	192.168.102.4	8.8.8.8	DNS	76	Standard query 0x0007 A www.facebook.com
75	5.360146000	8.8.8.8	192.168.102.4	DNS	108	Standard query response 0x0007 A 93.46.8.89
76	5.360583000	192.168.102.4	8.8.8.8	DNS	76	Standard query 0x0008 AAAA www.facebook.com
77	5.360657000	8.8.8.8	192.168.102.4	DNS	92	Standard query response 0x0007 A 203.98.7.65
78	5.360698000	192.168.102.4	8.8.8.8	ICMP	120	Destination unreachable (Port unreachable)
79	5.399914000	8.8.8.8	192.168.102.4	DNS	108	Standard query response 0x0008 A 203.98.7.65
82	5.514752000	8.8.8.8	192.168.102.4	DNS	116	Standard query response 0x0007 CNAME star.c10r.facebook.com A 31.13.70.81
84	5.555076000	8.8.8.8	192.168.102.4	DNS	128	Standard query response 0x0008 CNAME star.c10r.facebook.com AAAA 2a03:2880:f

```
C:\Users\lion>ping 8.8.8.8

正在 Ping 8.8.8.8 具有 32 字节的数据:
来自 8.8.8.8 的回复: 字节=32 时间=217ms TTL=33
来自 8.8.8.8 的回复: 字节=32 时间=219ms TTL=33
```

TCP劫持

- 为什么不能访问facebook

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.8.146	31.13.70.81	TCP	66	49324 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.177806000	31.13.70.81	192.168.8.146	TCP	66	http > 49324 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
3	0.177882000	192.168.8.146	31.13.70.81	TCP	54	49324 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.187382000	192.168.8.146	31.13.70.81	HTTP	360	GET / HTTP/1.1
5	0.370427000	31.13.70.81	192.168.8.146	TCP	60	http > 49324 [ACK] Seq=1 Ack=307 Win=17920 Len=0
6	0.447381000	31.13.70.81	192.168.8.146	HTTP	302	HTTP/1.1 301 Moved Permanently
7	0.449384000	31.13.70.81	192.168.8.146	TCP	60	http > 49324 [RST] Seq=249 Win=11941376 Len=0

```
  7 0.449384000 31.13.70.81     192.168.8.146       TCP
```

```
    Time to live: 53
    Protocol: TCP (6)
  ⊞ Header checksum: 0xf775 [correct]
    Source: 31.13.70.81 (31.13.70.81)
    Destination: 192.168.8.146 (192.168.8.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port
    Source port: http (80)
    Destination port: 49324 (49324)
    [Stream index: 0]
    Sequence number: 249    (relative sequence number)
    Header length: 20 bytes
  ⊟ Flags: 0x004 (RST)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not se
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
    ⊟ .... .... .1.. = Reset: Set
      ⊟ [Expert Info (Chat/Sequence): Connection reset (RST)]
          [Message: Connection reset (RST)]
```

```
  6 0.447381000 31.13.70.81     192.168.8.146       HTTP
  7 0.449384000 31.13.70.81     192.168.8.146       TCP
```

```
⊞ Frame 6: 302 bytes on wire (2416 bits), 302 bytes captured (24
⊞ Ethernet II, Src: Cisco_ed:a9:3f (28:94:0f:ed:a9:3f), Dst: Del
⊟ Internet Protocol Version 4, Src: 31.13.70.81 (31.13.70.81), D
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN
      0000 00.. = Differentiated Services Codepoint: Default (0x
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not
    Total Length: 288
    Identification: 0x6dae (28078)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 82
    Protocol: TCP (6)
  ⊞ Header checksum: 0x8b91 [correct]
    Source: 31.13.70.81 (31.13.70.81)
    Destination: 192.168.8.146 (192.168.8.146)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port:
    Source port: http (80)
    Destination port: 49324 (49324)
```

DNS 缓存毒化

```
root@bt:~# ping www.baidu.com
PING www.a.shifen.com (61.135.169.105) 56(84) bytes of data.


^C^C^Z
[1]+  Stopped                 ping www.baidu.com
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# ping www.baidu.com
PING www.baidu.com (1.2.3.4) 56(84) bytes of data.
```

DNS 缓存毒化

```
⊞ Frame 3: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
⊞ Ethernet II, Src: Vmware_67:52:ca (00:0c:29:67:52:ca), Dst: All-HSRP-routers_2c (00:00:0c:07:ac:2c)
⊞ Internet Protocol Version 4, Src: 10.4.4.4 (10.4.4.4), Dst: 192.168.103.111 (192.168.103.111)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: ddt (1052)
⊟ Domain Name System (response)
    [Request In: 2]
    [Time: 0.003366000 seconds]
    Transaction ID: 0x38df
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ⊟ Queries
    ⊟ www.sina1.com: type A, class IN
        Name: www.sina1.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ www.sina1.com: type A, class IN, addr 192.168.103.111
        Name: www.sina1.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 1 minute, 9 seconds
        Data length: 4
        Addr: 192.168.103.111 (192.168.103.111)
  ⊟ Additional records
    ⊟ <Root>: type Unknown (887), class Unknown (30583)
        Name: <Root>
        Type: Unknown (887)
        Class: Unknown (0x7777)
        Time to live: 1045 days, 12 hours, 39 minutes, 5 seconds
        Data length: 25717
        Data
```

```
0030  00 01 00 00 00 01 03 77  77 77 05 73 69 6e 61 31   .......w ww.sina1
0040  03 63 6f 6d 00 00 01 00  01 c0 0c 00 01 00 01 00   .com.... ........
0050  00 00 45 00 04 c0 a8 67  6f 00 03 77 77 77 05 62   ..E....g o..www.b
0060  61 69 64 75 03 63 6f 6d  00 00 01 00 01 00 33 33   aidu.com ......33
0070  ae 00 04 01 02 03 04                              .......
```

DNS 缓存毒化数据包

源IP	NSSERVER
目的IP	DNSSERVER
源端口	53
目的端口	？？？
协议	UDP
Transaction ID	？？？

DNS 缓存毒化难点

- Transaction ID (0XFFFF)
- PORT (0XFFFF) （dig porttest.dns-oarc.net TXT @dns_server_ip）

```
[root@localhost Iptest]# dig +short porttest.dns-oarc.net TXT @8.8.8.8
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"74.125.16.80 is GREAT: 8 queries in 2.9 seconds from 8 ports with std dev 11017"
```

DNS 缓存毒化

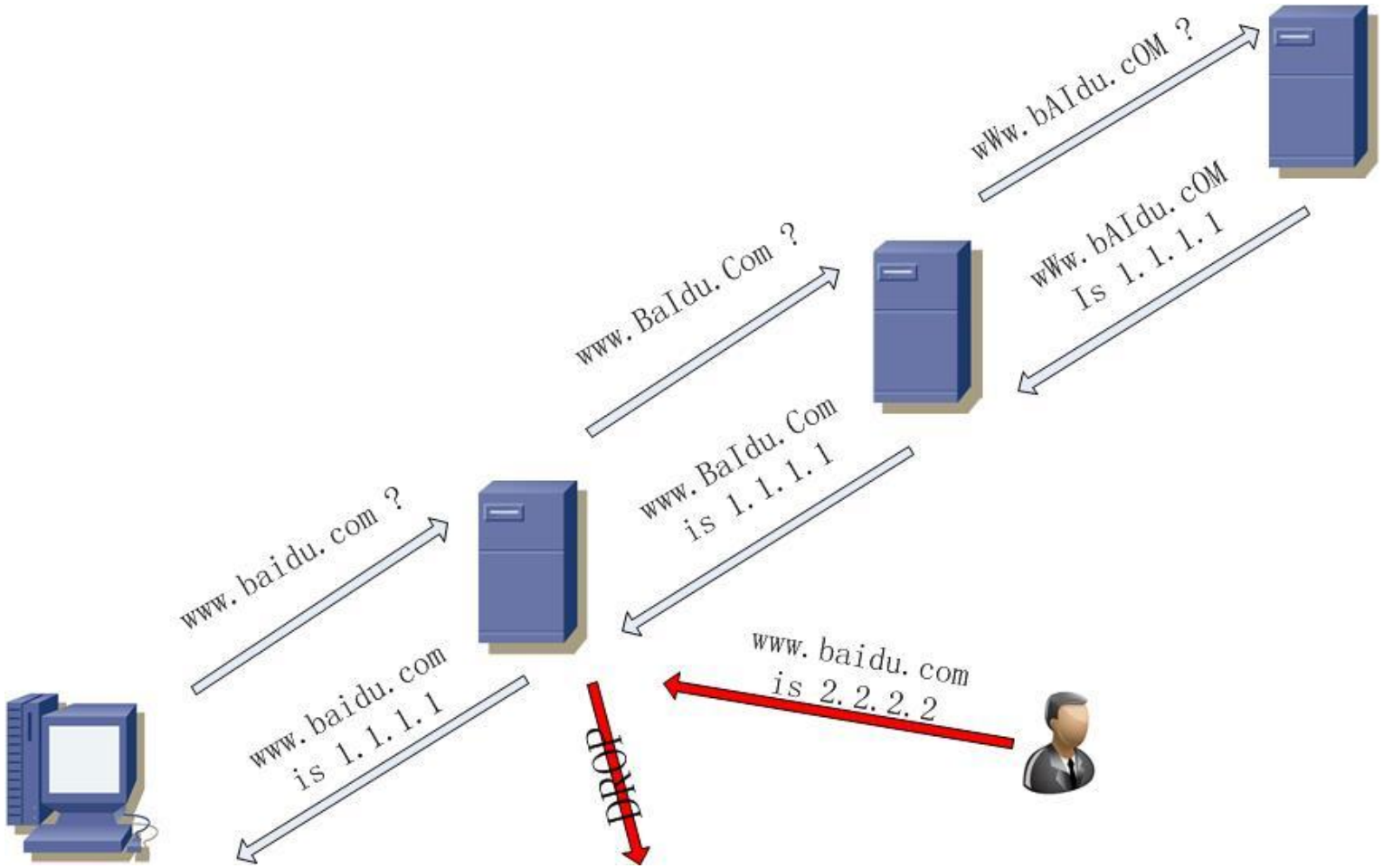
- 难度 ★ ★ ★ ★ ★
- 破坏力 ★ ★ ★ ★ ★

DNSSEC 与 0X20

- DNSSEC:是Internet工程任务组 （IETF）的对确保由域名系统 （DNS）中提供的关于互联网协议 （IP）网络使用特定类型的信息规格套件。它是对DNS提供给DNS客户端（解析器）的DNS数据来源进行认证，并验证不存在性和校验数据完整性验证，但不提供或机密性和有效性。
- 优点:防止欺骗
- 缺点: 性能，无法阻止DDOS 等

- 0X20:随机化大小写验证技术
- http://tools.ietf.org/html/draft-vixie-dnsext-dns0x20-00

0x20


wWw.bAIdu.cOM ?
www.BaIdu.Com ?
wWw.bAIdu.cOM
Is 1.1.1.1
www.BaIdu.Com
is 1.1.1.1
www.baidu.com ?
www.baidu.com
is 1.1.1.1
www.baidu.com
is 2.2.2.2
DROP

DNS面临的其他问题

- 针对根攻击　　（DNSSec）
- 缓存中毒　　（端口随机，0X20)
- 针对授权服务器　　（暴风影音,DNSPOD）
- 域名供应商
- DDOS

DNS？？危害？？

- 业务无法访问
- 钓鱼
- 挂马
- CPS
- 僵尸网络
- 。。。

THANKS