Dark Side of the DNS Force

ERIK WU

ACALVIO, INC.

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

DNS

104.20.66.243

DNS

blackhat.com. DNS 104.20.66.243

Alexa Rank: 60244

20

Start of Authority
mname: may.ns.cloudflare.com rname: dns.cloudflare.com
serial: 2021007381
refresh: 10000 retry: 2400
expire: 604800 minimum: 3600

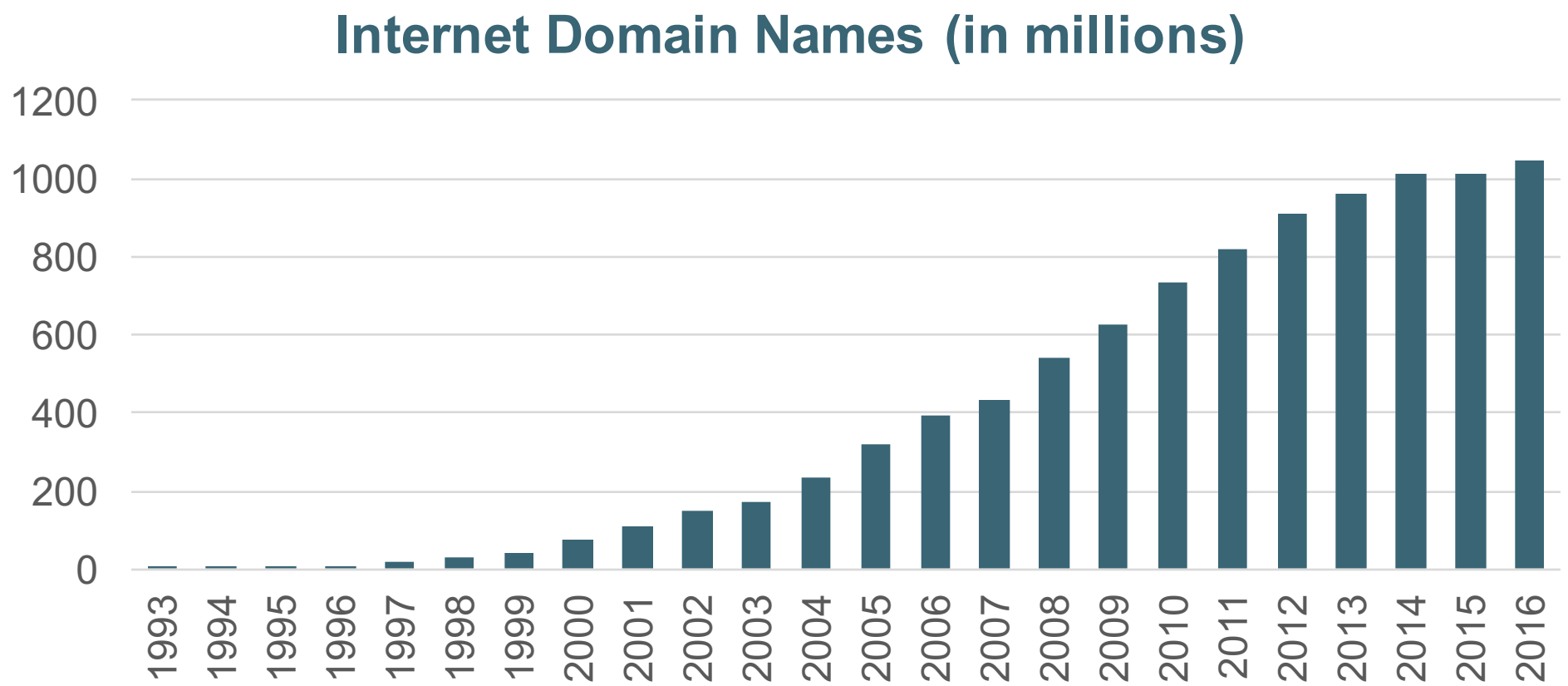
Nameservers
may.ns.cloudflare.com, rick.ns.cloudflare.com

Mail Exchangers
aspmx.l.google.com(1), alt1.aspmx.l.google.com(5), alt2.aspmx.l.google.com(5), aspmx2.googlemail.com(10), aspmx3.googlemail.com(10)

TXT Records
google-site-verification=Ehd8tYFdHXyRhk6rRoTYXw-u3KDVmcv2bvCLt4hvAGE

A Records
104.20.65.243, 104.20.66.243

Registered Internet Domains



Source Statista

Cloudflare/Spamhaus DDoSed via open DNS resolvers

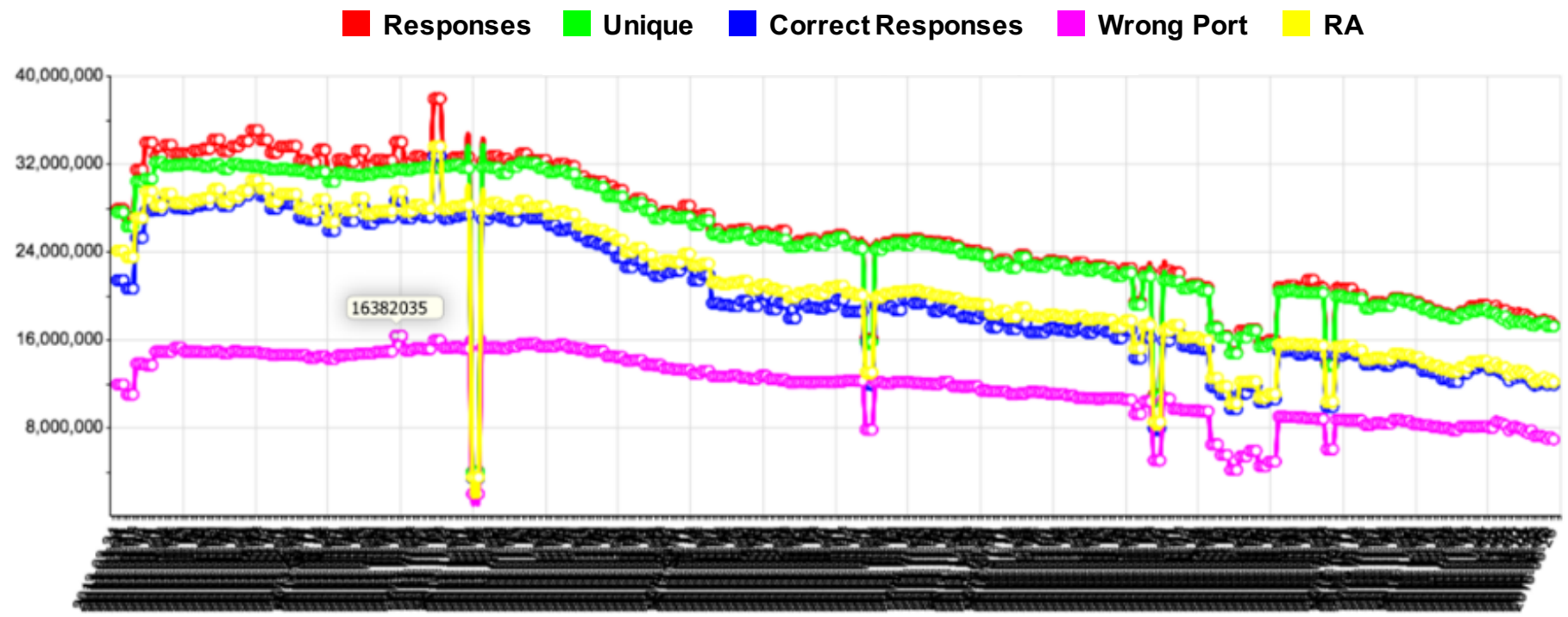
ACALVIO

FLASHING IN MARCH 2013

300gbps DNS amplification attacks

27.2M open DNS resolvers (in 2013)

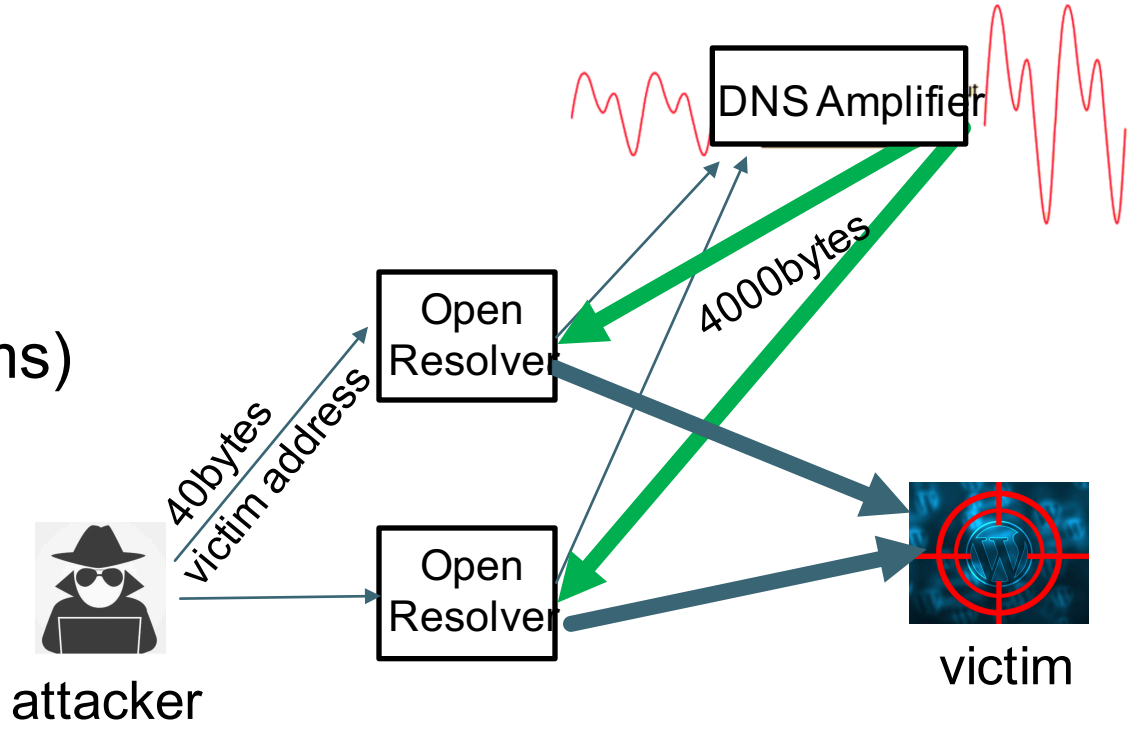
17.6M of today (>3yrs later)



Source openresolverproject.org

DNS amplification DDoS attacks

- Enablers
  - Open DNS resolvers
  - DNS amplifiers
    - Legit
    - Purpose-built
  - Spoofed sending addresses (of victims)



DNS amplification DDoS attacks

DNS AMPLIFIER

Legit | Purpose-built

```
;access-board.gov.                      IN      ANY

;; ANSWER SECTION:
access-board.gov.                                                       gov. 2016010101 21600 3600 604800 21600
access-board.gov.                                                       102034616 2960 access-board.gov. TSkZe/pObXZ3/XeT/IWt/7L9MT9p1qmfQ6/SrJwr69sZ2iqN2qappUFC Z2R4lkaLZXofZKkkWJbNu3hBGWRoglHk
MyF0v0Qbk9t4mh3SCACEZ                                                  yts9xzpJ3YUBekKIsKZr/skL2ayRcN6XdMZx1gkM9vW8mx5GIace4Rpj DCWZns9YEZ4g34MMzYag9seGEBftNJ8XhABgUk1Hm+YUcFldpeq9aw1Y xvaMMLG6
4ehXyCANrQAa4e3L9Doxb
access-board.gov.
access-board.gov.
access-board.gov.                                                       02034616 2960 access-board.gov. cJtzv0ucihLXYaEpLXRlGmETBd9SHmpUPvma+dRhDSoXDZraR7sTTFhh ZVFkSf+BvcXiB/ziLIasG95mbPTyRYaej
COONnQ0m+vuWBAYMOVAmUtn oTDfTA6DoLj7zPPZ732RrKWRK0athKE4/idoooQ2n9NMasoSN3Y0qxmR mM+XTvbn/7Q5aPSFsqhtSSnILYl2a+vvsoaxXfy5GrQucJf27gMT+ViG GhNzkY+3rvfMcmreMW0UdDpDRcNquaG2TUKhNd3kD8pajO8tJkeNSPJl 7Cp2Mkdr9
+632DHePCK4nAtQSX5VaVjRUdCmAk4mSoV+KEfVGt+1XAkT NaQpPQ==
access-board.gov.       11234   IN      A       128.241.229.190
access-board.gov.       11234   IN      RRSIG   A 5 2 86400 20160401034616 20160102034616 2960 access-board.gov. PHq/jLjfcFW5E34VI4SAiT7hRzo2pHHvq/BLskTpMT0xKDkcoiLBWvaj Fm8faBrLeWu0Homq9ReTwoNCbt0Ij+7+qb
9WW5qBhPQQ/gBhWsKBkQwI NjIQkW5fhccNV9KNc3RDbCvMl6ZvWxKVRAIBEAsxLPMlU5oOHh+ka18C 1KoaVO5nB7OGqtzhe+LLuwWWBKT2kf/7zdBxJY8kdvxCj+s1ecEsVIqW 1/w2AHBcyCwqNSMwytE36IqsBXjr7Uw2+CpseYAGW4DOY2Apuwivv1yD 7SP/F4+Yyx
bs8VGtQBEikZeJuxSbC0b4zrkXGA+H2etj+ta9hkqzuTRA 2lYU2w==
access-board.gov.       11234   IN      MX      10 accessboard-gov01e.mail.eo.outlook.com.
access-board.gov.       11234   IN      MX      20 accessboard-gov01e.mail.eo.outlook.com.
access-board.gov.       11234   IN      RRSIG   MX 5 2 86400 20160401034616 20160102034616 2960 access-board.gov. jweNey5dykpzz88vIBncQiR4JLJCBWsbQ1duRYE36C/anD0CKPVc102y zJZ42ggD5iBEgtx8+WATvY2JfcYOYsA6C
lXMCRtDRfQE3ydKD66bkBbR esLLzJe5KCBNXbJH7L9Elfbbm43QvxD+2enu1P/dTIizYH6BhBZo/6dS A+s84qBqvCG/ZzLZHtXmdtHhW8w8CB0ejVdf0xGL/jXSk+TkA7AWxEb1 ZzLnyLKnr55Yof3R9JeLB9TB1IpuLF+GRUwmazDwjVTikuL/yCNJJ3uS Za/Jjg1Wf
jg0yNBAOlp0yS4VtLqsRXVu4BjLSBwdp2cZUJl1+dmK8Pft VkqBSA==
access-board.gov.       11234   IN      TXT     "v=spf1 include:outlook.com ~all"
access-board.gov.       11234   IN      TXT     "MS=ms18981696"
access-board.gov.       11234   IN      RRSIG   TXT 5 2 86400 20160401034616 20160102034616 2960 access-board.gov. LjLFR9O2t+L5Nwon+K6CUm4uNmQUxP0vF4eDakMy4hWvbMn+XwgAf6mP K1bgUyWnfCezkbjLLP4zbgOD+jJ5lSZQ
lZkccvR//YE50BPxHOE3YSZ9 LDithnUPKN3kKmacIiM//Hp/HO0bMWPJ7z4419uXkofSEHBKeZ7zGHd1 i/4xpQoa9B8d6VKmFJZjALtO63tc7trwINO+Y+2HjTPtBBeOPc8StB++ zp087awTu2sSgk0/oVCR6cYA6o64Mcl6c7ckVuq38oIAXXR6Dt6SkuWG 1ljs1kne
hqppUg4+C4YXbgbGFq4cff5g25OP/MmKF/gNYCwqw/fdcD3m z1MaaQ==
access-board.gov.       11234   IN      AAAA    2001:418:dc01:4::80f1:e5bb
access-board.gov.       11234   IN      RRSIG   AAAA 5 2 86400 20160401034616 20160102034616 2960 access-board.gov. X4Afu4WgYqqBpmEYVCmODyjGHBaDx3abNkxYe/WUTHH26XJLIxWuPdX3 f2YnNfBYgxr6C8ZN/Tdr/62jDgVL1vW
SemC7yRgC4tz05WhcuaC9b0SD rE6rjzvPYzcBwMQwqm9k8QBwhGU24wift3jeCAEnWlfQfp0dq0u3csYX MOJI7b+im1gTXmUoo2pymvS56Nzu3htHEpXYGsCW1Ejs9dbBhJ4knolI 86U0NtEDKaqJ/DkEKOZ1EEzK+W7LQ64FBe0FEqKa1BlYKIrQ3O/xWms+ CUJc0Yq
q1X1bPLL+aCZH3oX5WdK62dzsCl6RXIcGkey5G1juee1n37tZ ovCu/Q==
access-board.gov.       11234   IN      NSEC    autodiscover.access-board.gov. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
access-board.gov.       11234   IN      RRSIG   NSEC 5 2 21600 20160401034616 20160102034616 2960 access-board.gov. Px3RJ/hoJ1oRBG5qir55+mWdjhzAkT4XidTuDycHejsqssuZdTZnlZTx 7RkAhRIp3ykrGKCOyXMnCct/DtUWnOt
U14E6njIZPEP261dNipHYRldE t5606N7+g3bueXdkCg+VxI8O27Q48Dz83cG9atpCrrZqD3tj4/nSnYh1 gytXgEd2qNsOyw6f6WVOyFgLGl8+tARgZ0BOQpaora5ZnK11daliRtof tiCDsljju9fVh6JnmVQCRzqb25NJIoCGOjOHGuWw5AfaMNaIFBW4gaNN BYEAuoJ
xM0F8kHgo6Q8OmYlXncStuRLgy+xewE6iGpBVFOkFT5YInepT W/v3DA==
access-board.gov.       11234   IN      DNSKEY  256 3 5 AwEAAeTliR5ccvdixTwIMqVubCoS6WbzZgk+0YqjAQfCKsq981kQOVgy HS1G9XXe0GZI64rDzWPs4eHjRorjNoaxBufm5ObXmw1P/GBmgxDhdXlF kbb/g1y92LeDH/RilObxyF3V7++7idJM29
ML2gbqSBWhCtwGi5lCV/EY LFL2O9VMHvdWHNZHAf5MIruiq+LfIyEyyN8wv9n+Fe1lqJ9h1z1czUKM es4sO+kG9ftd+5m7jAoqsaDLpWZnrW7zAHJ0ZZ0eRkR9P6I/mPZvm+LO kajsXvXwDqrZaYBrRm2AiyfQFJV6g2TB7iPqotCsKyb71dbEmYaZpIqe e1/4LcomXZ
c=
access-board.gov.       11234   IN      DNSKEY  256 3 5 BQEAAAAB0jCdi71rcFx2y14Sb9ekrBD7F74jpdWhe0plHq1oY5u5TB9W iYAl3d9MrZHGqydU0dC/nm5XE1X04+KwXnTZQjYkzdK0MZY+mRTyrOts pKMamBzI/eWO9jcn10uYz+7v4ICrznAVmS
5UtCYt18kIBkT83/Sv5mmy YX5HYFq4D9uk06HNmq4jYYQzO9BaJ2pDO7pyJMteRFFYX3/s1UUlj3Im l+gN65rJ6AHn2f6nMEX/7SKsSyJNEiLZVdz+lCUapfXL7SsZbY4aSiX3 BbmhqMA8d+gNlwUpoFaw5ImfytpSrZcLvIYpOTa5f1bHLcQCtfIvT7H2 D2fwRfvdwm
/5uw==
access-board.gov.       11234   IN      DNSKEY  257 3 5 AwEAAadqsq50DH2j8ozV4qHttBI2Da9ezLKJZzuQ0hn8enzJnWzpU4es xtaYCArMiVwzmA1dAe+ofpSNjA3kLYev2f5iINpopM7rhhuSDcLwisRR TVc2Sre2gepMIJH9Me0bPN1u5ZQUtsJXkd
8boeChFVaMTCBuYCk+RTRX GRjS+oXVtKkByJqa5fZiHEhkYby8Rg2cy9jMNDNxn3eqpWiTuPdb1g/E AhQfxn5fDi5gle24UqMxXh86gaurgwWy93mqUXP+Tq4zo3nn9n8PO66I VmK3Mq+QrKOHV4uQD9GptItibfeTMjyE4KNTJKkMdh+nsd5iF8J6aEgV 32NssAgLdM
s=
access-board.gov.       11234   IN      RRSIG   DNSKEY 5 2 86400 20160401034616 20160102034616 2960 access-board.gov. yVnCZF7csrBb0dI3TtwfRWrbimxNHgXEFO1r/hElI/Kd0sjvjZ66D0Ai oDCnv149dhWQPgkVfcz1hggC5FWGh
LOeKOiCPOU9q3peMAnUvY2Hm5Rb 9zAFcKz6XYv28ZqrG6bGWZmp6CHhy5hDEo4G0QWOx//WafEP5b/CXkpN K9SSP6qBAtoxj1Eh0paKRnoSxiis5/0DX48d3oZoOlXH7hRxLBA1w5dx tVljKVc4Iu28KVhNetuxpapESwVB6jwp+zOdqClZkIZKQs2p9QX2JRhD 2hWluu
VLVWYWMmS6truISfHoOwA0mfVyUJl8jtwmfRo4GUDgYVkjSA/Cz Po0JIQ==
access-board.gov.       11234   IN      RRSIG   DNSKEY 5 2 86400 20160401034616 20160102034616 44299 access-board.gov. TYCMDBNo4hqE9lpqAd0Mt8UzpQp9wBpTmRT7cK8wk5HnXV4odHV6gPOb 63NpW2HbXbzBgdv+0DKg51U6SsNJ
2Wj2+2vLSoLn2eMbuAw6YBs1OCUq QOx4qOG/T7WyspXnrwFFQwFA2qRx69oC23XL+SHCVBTNJlFS7i29NWEp RxwISq6bN6iGN1gYHSRejFCXCQ68Cla9Gml32os8ii65HCzBdG6SMI5Y oaACAx5ORo6pEe6N0O4EXOudBUiGHJCAtrteWENlMpHgjYXRfcBpm3QE CFl7
f/uD5k4kCzZ6d0ZyhfLj+xkHMBkCIx5l6i6BTQGlRadQschQgNMF yinv3A==

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Jan 16 22:42:38 2016
;; MSG SIZE  rcvd: 3924
```

DNS amplification DDoS attacks

DNS AMPLIFIER

Legit | Purpose-built

```
xM0F8kHgo                                    iGp8VFOkFT5YInepT W/v3DA==
access-bo                                    IN      DNSKEY  256 3 5 AwEAAeTliR5ccvdixTwIMqV
ML2gbq5Bk                                    vdWHNZHAf5MIruiq+LfIyEyyN0wv9n+Fe1lqJ9h1z1czUKM
c=
access-board.gov.       11234   IN      DNSKEY  256 3 5 BQEAAAAB0jCdi71rcFx2y14
5UtCYt18kI8kT83/Sv5mmy YX5HYFq4D9uk06HNmq4jYYQzO9BaJ2pDO7pyJMteRFFYX3/s1UUlj3Im
/5uw==
access-board.gov.       11234   IN      DNSKEY  257 3 5 AwEAAadqsq50DH2j8ozV4qH
8boeChFVaMTCBuYCk+RTRX GRjS+oXVtKk8yJqa5fZiHEhkYby8Rg2cy9jM0DNxn3eqpWiTuPdb1g/E
s=
access-board.gov.       11234   IN      RRSIG   DNSKEY 5 2 86400 20160401034616
LOeKOiCPOU9q3peMAnUvY2Hm5Rb 9zAFcKz6XYv28ZqrG6bGWZmp6CHhy5hDEo4G0QW0x//WafEP5b/
VLVWYWMmS6truISfHoOwA0mfVyUJl8jtwmfRo4GUDgYVkjSA/Cz Po0JIQ==
access-board.gov.       11234   IN      RRSIG   DNSKEY 5 2 86400 20160401034616
2Wj2+2vLSoLn2eMbuAw6Y8s1OCUq Q0x4qOG/T7WyspXnrwFFQwFA2qRx69oC23XL+SHCVBTNJlFS7i
f/uD5k4kCzZ6d0ZyhfLj+xkHM8kCIx5l6i6BTQGlRadQschQgNMF yinv3A==

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Jan 16 22:42:38 2016
;; MSG SIZE  rcvd: 3924
```

DNS amplification DDoS attacks

DNS AMPLIFIER

Legit | Purpose-built

```
;; ANSWER SECTION:
hajjamservices.us.      21582   IN      A       204.46.43.230
hajjamservices.us.      21582   IN      A       204.46.43.231
hajjamservices.us.      21582   IN      A       204.46.43.232
hajjamservices.us.      21582   IN      A       204.46.43.233
hajjamservices.us.      21582   IN      A       204.46.43.234
hajjamservices.us.      21582   IN      A       204.46.43.235
hajjamservices.us.      21582   IN      A       204.46.43.236
hajjamservices.us.      21582   IN      A       204.46.43.237
hajjamservices.us.      21582   IN      A       204.46.43.238
hajjamservices.us.      21582   IN      A       204.46.43.239
hajjamservices.us.      21582   IN      A       204.46.43.240
hajjamservices.us.      21582   IN      A       204.46.43.241
hajjamservices.us.      21582   IN      A       204.46.43.242
hajjamservices.us.      21582   IN      A       204.46.43.1
hajjamservices.us.      21582   IN      A       204.46.43.2
hajjamservices.us.      21582   IN      A       204.46.43.3
hajjamservices.us.      21582   IN      A       204.46.43.4
hajjamservices.us.      21582   IN      A       204.46.43.5
hajjamservices.us.      21582   IN      A       204.46.43.6
hajjamservices.us.      21582   IN      A       204.46.43.7
hajjamservices.us.      21582   IN      A       204.46.43.8
hajjamservices.us.      21582   IN      A       204.46.43.9
hajjamservices.us.      21582   IN      A       204.46.43.10
hajjamservices.us.      21582   IN      A       204.46.43.11
hajjamservices.us.      21582   IN      A       204.46.43.12
hajjamservices.us.      21582   IN      A       204.46.43.13
hajjamservices.us.      21582   IN      A       204.46.43.14
hajjamservices.us.      21582   IN      A       204.46.43.15
hajjamservices.us.      21582   IN      A       204.46.43.16
hajjamservices.us.      21582   IN      A       204.46.43.17
hajjamservices.us.      21582   IN      A       204.46.43.18
hajjamservices.us.      21582   IN      A       204.46.43.19
hajjamservices.us.      21582   IN      A       204.46.43.20
hajjamservices.us.      21582   IN      A       204.46.43.21
:
```

```
hajjamservices.us.      21582   IN      A       204.46.43.193
hajjamservices.us.      21582   IN      A       204.46.43.194
hajjamservices.us.      21582   IN      A       204.46.43.195
hajjamservices.us.      21582   IN      A       204.46.43.196
hajjamservices.us.      21582   IN      A       204.46.43.197
hajjamservices.us.      21582   IN      A       204.46.43.198
hajjamservices.us.      21582   IN      A       204.46.43.199
hajjamservices.us.      21582   IN      A       204.46.43.200
hajjamservices.us.      21582   IN      A       204.46.43.201
hajjamservices.us.      21582   IN      A       204.46.43.202
hajjamservices.us.      21582   IN      A       204.46.43.203
hajjamservices.us.      21582   IN      A       204.46.43.204
hajjamservices.us.      21582   IN      A       204.46.43.205
hajjamservices.us.      21582   IN      A       204.46.43.206
hajjamservices.us.      21582   IN      A       204.46.43.207
hajjamservices.us.      21582   IN      A       204.46.43.208
hajjamservices.us.      21582   IN      A       204.46.43.209
hajjamservices.us.      21582   IN      A       204.46.43.210
hajjamservices.us.      21582   IN      A       204.46.43.211
hajjamservices.us.      21582   IN      A       204.46.43.212
hajjamservices.us.      21582   IN      A       204.46.43.213
hajjamservices.us.      21582   IN      A       204.46.43.214
hajjamservices.us.      21582   IN      A       204.46.43.215
hajjamservices.us.      21582   IN      A       204.46.43.216
hajjamservices.us.      21582   IN      A       204.46.43.217
hajjamservices.us.      21582   IN      A       204.46.43.218
hajjamservices.us.      21582   IN      A       204.46.43.219
hajjamservices.us.      21582   IN      A       204.46.43.220
hajjamservices.us.      21582   IN      A       204.46.43.221
hajjamservices.us.      21582   IN      A       204.46.43.222
hajjamservices.us.      21582   IN      A       204.46.43.223
hajjamservices.us.      21582   IN      A       204.46.43.224
hajjamservices.us.      21582   IN      A       204.46.43.225
hajjamservices.us.      21582   IN      A       204.46.43.226
hajjamservices.us.      21582   IN      A       204.46.43.227
hajjamservices.us.      21582   IN      A       204.46.43.228
hajjamservices.us.      21582   IN      A       204.46.43.229

;; Query time: 3 msec
;; SERVER: 10.10.0.8#53(10.10.0.8)
;; WHEN: Wed Jul 13 18:49:23 2016
;; MSG SIZE  rcvd: 3907
```

DNS amplification DDoS attacks

DNS AMPLIFIER

Legit | Purpose-built

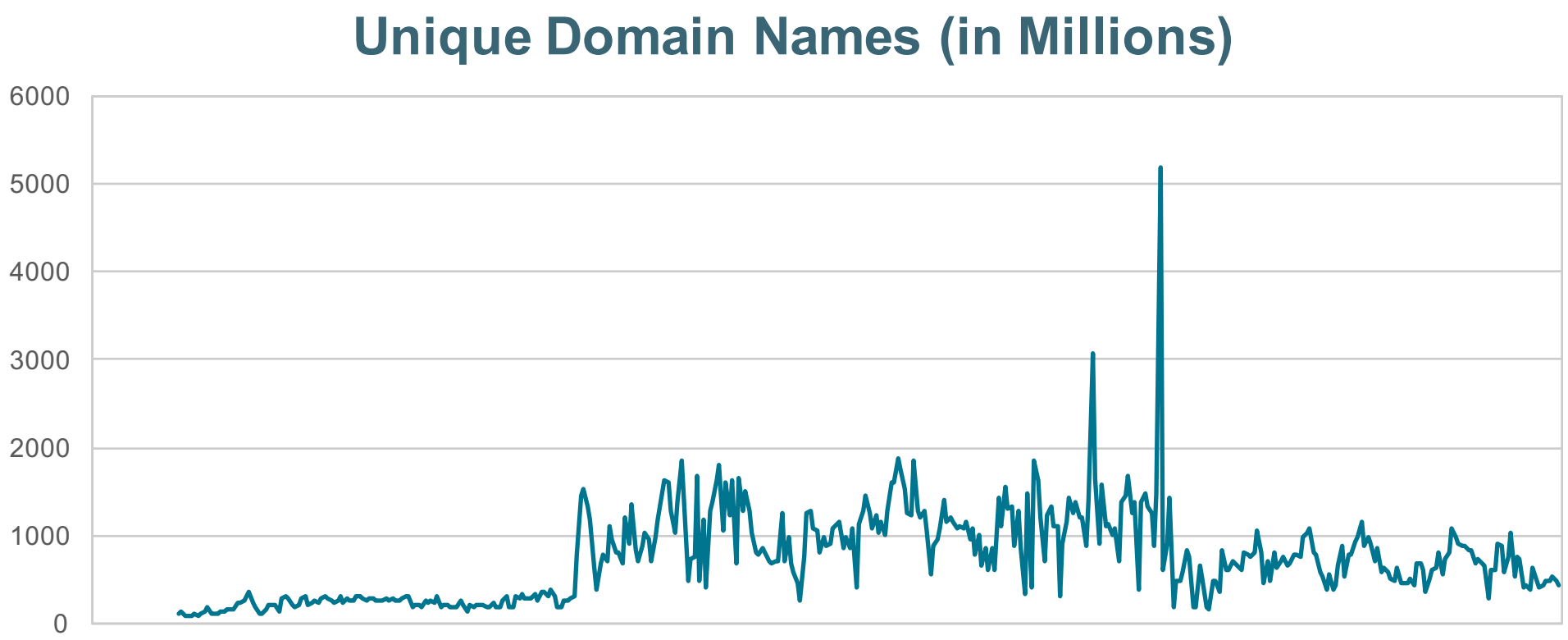
```
hajjamservices.us.      21582   IN      A       204.46.43.212
hajjamservices.us.      21582   IN      A       204.46.43.213
hajjamservices.us.      21582   IN      A       204.46.43.214
hajjamservices.us.      21582   IN      A       204.46.43.215
hajjamservices.us.      21582   IN      A       204.46.43.216
hajjamservices.us.      21582   IN      A       204.46.43.217
hajjamservices.us.      21582   IN      A       204.46.43.218
hajjamservices.us.      21582   IN      A       204.46.43.219
hajjamservices.us.      21582   IN      A       204.46.43.220
hajjamservices.us.      21582   IN      A       204.46.43.221
hajjamservices.us.      21582   IN      A       204.46.43.222
hajjamservices.us.      21582   IN      A       204.46.43.223
hajjamservices.us.      21582   IN      A       204.46.43.224
hajjamservices.us.      21582   IN      A       204.46.43.225
hajjamservices.us.      21582   IN      A       204.46.43.226
hajjamservices.us.      21582   IN      A       204.46.43.227
hajjamservices.us.      21582   IN      A       204.46.43.228
hajjamservices.us.      21582   IN      A       204.46.43.229

;;  Query time: 3 msec
;;  SERVER: 10.10.0.8#53(10.10.0.8)
;;  WHEN: Wed Jul 13 18:49:23 2016
;;  MSG SIZE  rcvd: 3907
```

DNS amplification DDoS attacks

- Mitigation options
  - Filter spoofed sending addresses
  - Disarm amplifiers
  - Close open resolvers

High spikes of unique domains seen on Internet



Source: Nominum

What's wrong with subdomains?

blackhat.com.

www.blackhat.com.
m.blackhat.com.
media.blackhat.com.

104.20.66.243

wwww.blackhat.com.
mwww.blackhat.com.
mmww.blackhat.com.
mmmw.blackhat.com.
mmmm.blackhat.com.

NXDOMAIN

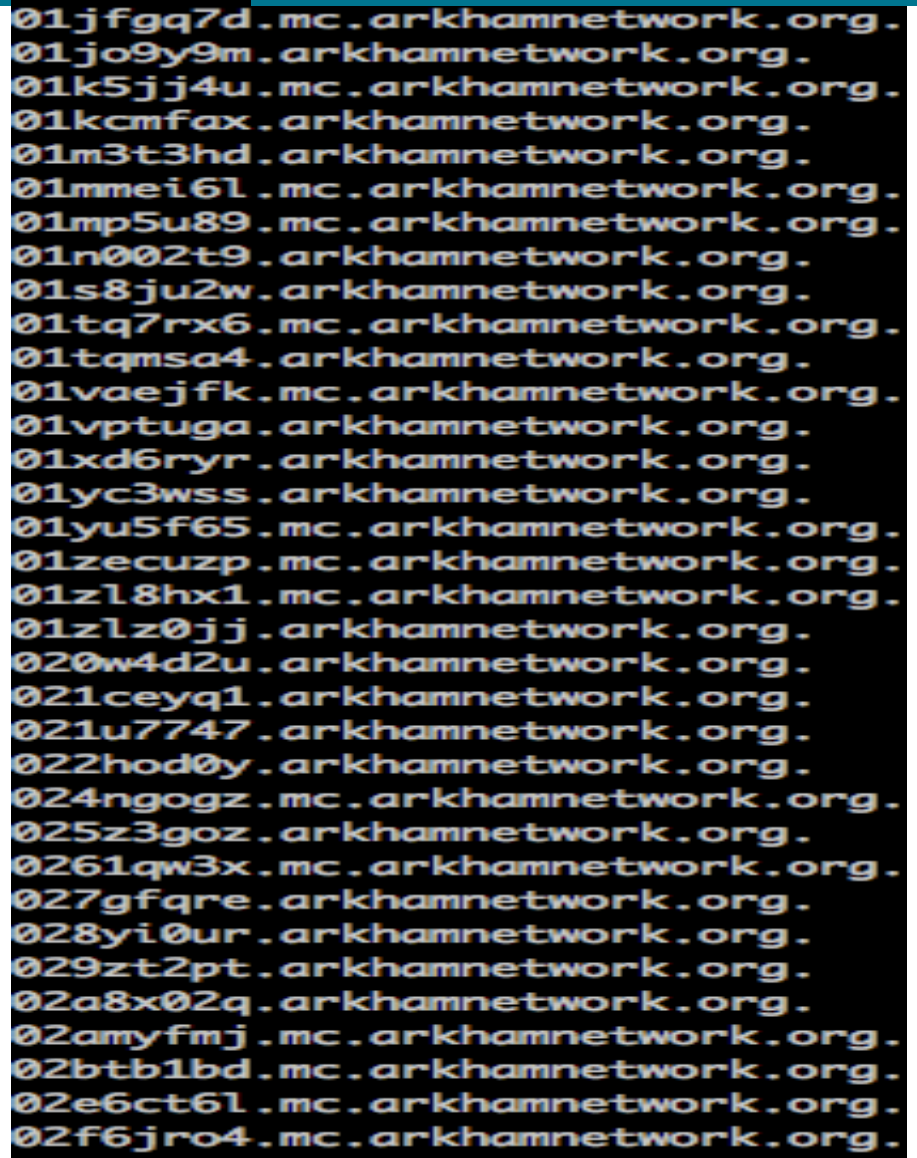
Subdomain attack as a competitive edge

ACALVIO

- Online gaming sites' availability is a key metrics
  - Subdomain attack was a novel abuse of DNS back in 2011/2012
  - Initially simple sequence number strings were used as prefixes to a competitor gaming site domain name to destruct the service of that gaming site:

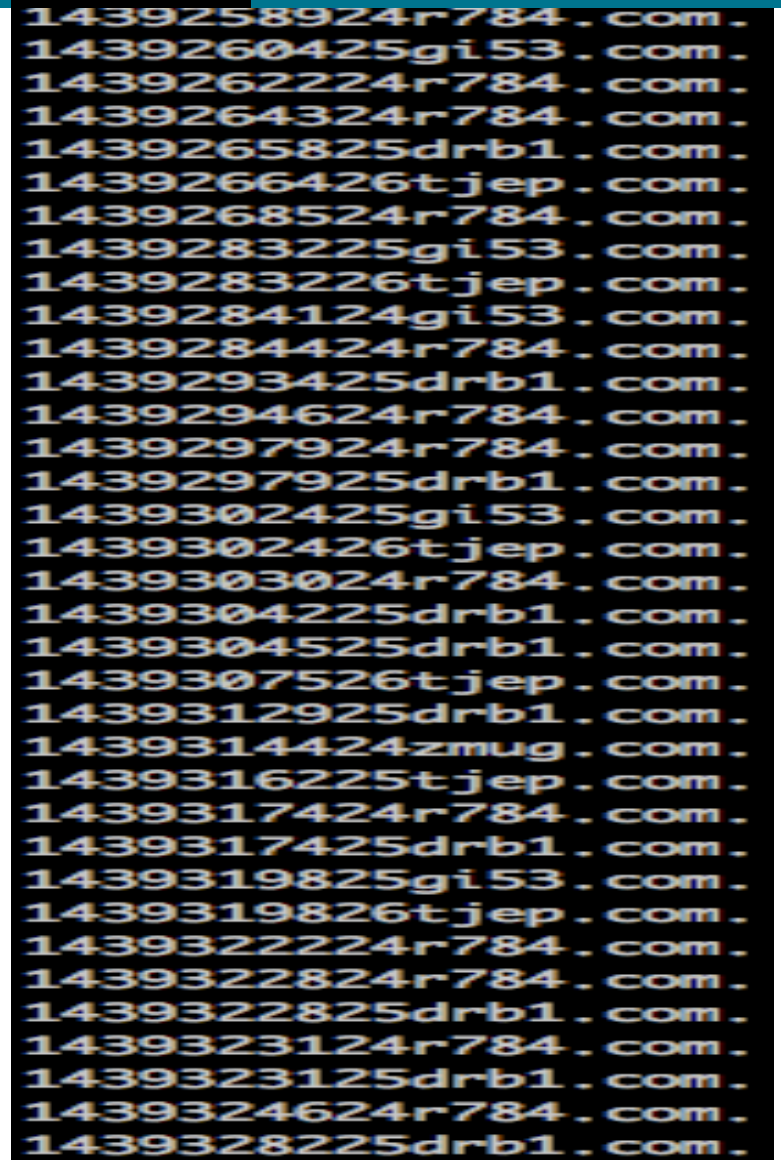
100000000.sf520.com.
100000001.sf520.com.
100000010.sf520.com.
100000011.sf520.com.
100000100.sf520.com.
100000101.sf520.com.
100000110.sf520.com.
100000111.sf520.com.
100001000.sf520.com.

Aimed at high-value targets



~200M unique subdomains
of arkhamnetwork.org.

Aimed at high-value targets



Subdomain strings

SUBDOMAIN STRINGS:

- Fixed or varying length:

z5kr836ws	qjkn
zdecc7nnx	styzcphur

- Time stamps:

1465560729	1465561210

- Random strings

WO423WWWOX5C	FN88RBHXWX9J

- Random numbers

2967230841	4343234574

- Sequence numbers

1165885261118	1165885261119

- Dictionary words

glassmaking	dishwater

Subdomain position

SUBDOMAIN POSITION:

- Left most — zdecc7nnx.www.blackhat.com.
- 2nd left most — m.zdecc7nnx.www.blackhat.com.
- 3rd left most — n.m.zdecc7nnx.www.blackhat.com.
- Any position on the left side of target domain

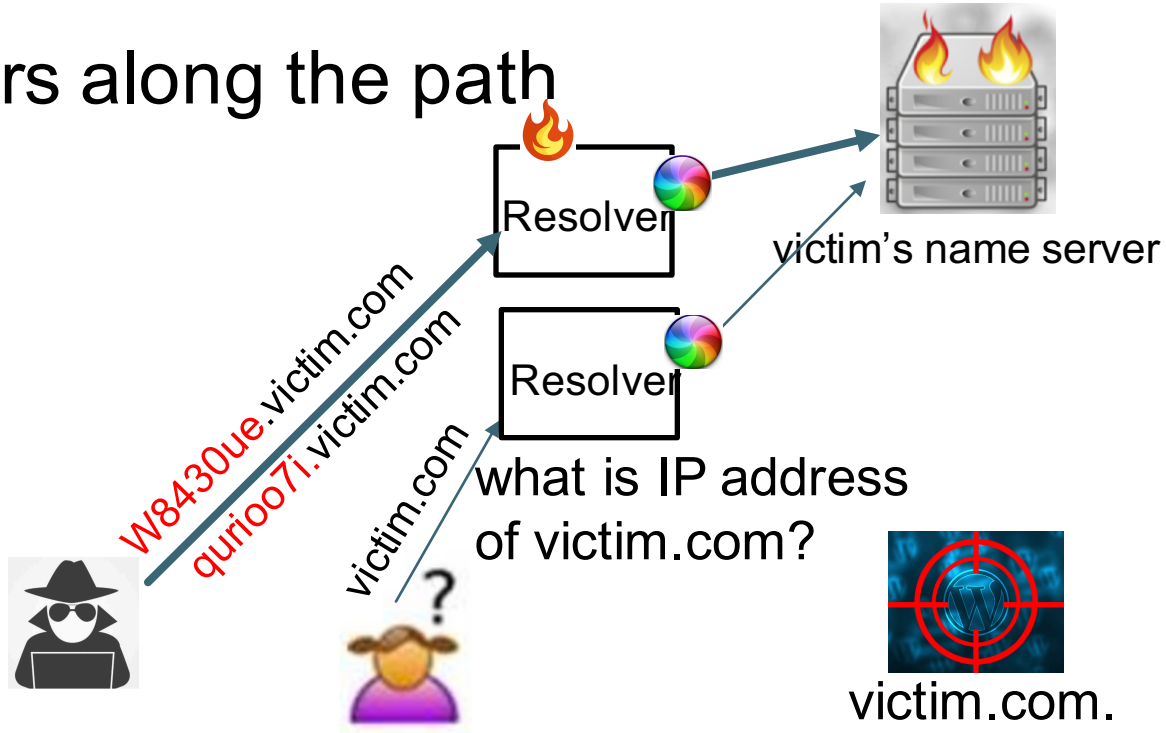
Subdomain composition

SUBDOMAIN COMPOSITION:

- Single subdomain string — FN88RBHXWX9J.blackhat.com.
- Multiple subdomain strings — WO423WW1WX5.FN88RBHXWX9J.blackhat.com.
- Combination of constant and random strings — a.FN88RBHXWX9J.blackhat.com.
  b.WO423WW1WX5.blackhat.com.

Impact

- Attacking target domain's authoritative name servers
- Collateral damages of DNS resolvers along the path
- Enablers:
  - Subdomain generator
  - (optional) Open resolvers
  - (optional) Spoofed sending addresses



ACALVIO

Operation Disruption

Authoritative name server often serves more than one domain, so does DNS resolver (cache/recursive)

A major ISP operation may be taken down by small-scale subdomain attacks

- 2gbps vs 300gbps

ACALVIO

Mitigation Option

- SUBDOMAIN ATTACKS MAY BE MITIGATED WITH VARYING RESULTS:
- Drop queries with random strings
- Limit queries with random strings
- Limit queries per IP address
- Limit queries per domain
- Drop queries per domain
  - What about high-value targets?

Dark Side Innovation

SIMPLE PROTOCOL ABUSE CAN BECOME A MAJOR SECURITY HEADACHE AND COSTLY MITIGATION:

- DNS cache poisoning
- DNS changer
- DNS amplification
- DNS subdomain
- DNS tunneling

Dark Side Innovation

ARMS RACE BETWEEN THE DARK-SIDE INNOVATIONS AND OURS IN CYBER SECURITY DEFENSE:

The dark-side has repeatedly won the fight

Any **glitch** in our defense is a winning **amplifiable opportunity** for the dark-side, while vice versa is not true

Rethinking of our defense strategy

Deception to help rebalance the asymmetric warfare situation between the dark-side and us

Thanks and Questions