Dark Side of the DNS Force

ERIK WU
ACALVIO, INC.
104.20.66.243
blackhat.com. 104.20.66.243

Alexa Rank: 30244

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

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

Mail Exchangers
aspmx1.google.com(1), alt1.aspmx1.google.com(5), alt2.aspmx1.google.com(5), aspmx2.googlemail.com(10), aspmx3.googlemail.com(10)

TXT Records
google-sitem-verification=En8tYFDrHxRk6fRcTYXw-u3KDVCv2bvCL4hvAGE

A Records
104.20.66.243, 104.20.66.243
Registered Internet Domains

Internet Domain Names (in millions)

Source: Statista
FLAShING IN MARCH 2013

300gbs 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
DNS amplification DDoS attacks

DNS AMPLIFIER

Legit | Purpose-built

---

DNSKEY 256 3 5 AwEAAeTliR5ccvdixTwIMqViMl2gbqSBwLc=
access-board.gov. 11234 IN DNSSKEY 256 3 5 BQEEEAAAB0jCd171rcFx2y14!
5UtCYt18kIBkT83/Sv5mmyYX5HYFq4D9uk86Hnmq4jYYQz09BaJ2p0D7pyjMteRFFYX3/sIuUlj3Im
/5uw==
access-board.gov. 11234 IN DNSSKEY 256 3 5 AwEAAadqsq50DH2j8ozV4qH:
8boeChFVaMTCBuYck+RTRXGRjs+oXVttKk8yJqa5fZiHEhKYby8Rg2cy9jMNNOnxn3eqpWiTuPdb1g/E=
access-board.gov. 11234 IN DNSSKEY 256 3 5 AwEAAadqsq50DH2j8ozV4qH:
8boeChFVaMTCBuYck+RTRXGRjs+oXVttKk8yJqa5fZiHEhKYby8Rg2cy9jMNNOnxn3eqpWiTuPdb1g/E=
access-board.gov. 11234 IN RRSIG DNSSKEY 5 2 86400 20160401034616
L0eK01CPOO9q3peMANuVvY2Hm5Rb 9zAFcKz6XYv28ZqrG6bGWZmp6CHHy5hDEo4G00W0x/WafEP5b/I
VLVWYWMMs6truISfH0qwAwH8mfVvYUJ8jtwmFro4GUDqYVkJsA/CzP0oJlQ==
access-board.gov. 11234 IN RRSIG DNSSKEY 5 2 86400 20160401034616
2Wwj2+2vL5oLn2eMbuAw6YBs10CuQ Q0x4q0G/T7WyspXnrwFFqWFa2qRx690c23XL+5HCvBTNiJfS7i:
f/uD5k4kCzG6dQZyhfLj+xxKHMbKCIx56l68TQGlRadQschOgMNF yinv3A==
DNS amplification DDoS attacks

DNS AMPLIFIER

Good | Bad | Ugly

DNS AMPLIFIER

<table>
<thead>
<tr>
<th>ANSWER SECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.230</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.232</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.233</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.234</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.235</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.236</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.237</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.238</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.239</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.240</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.241</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.242</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.1</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.2</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.3</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.4</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.5</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.6</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.7</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.8</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.9</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.10</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.11</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.12</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.13</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.14</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.15</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.16</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.17</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.18</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.19</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.20</td>
</tr>
<tr>
<td>hajjamservices.us. 21582 IN A 246.46.43.21</td>
</tr>
</tbody>
</table>
DNS amplification DDoS attacks

DNS AMPLIFIER

<table>
<thead>
<tr>
<th>Legit</th>
<th>Purpose-built</th>
</tr>
</thead>
</table>

---

Intro
Subdomain
Mechanism
Impact
Outro

Good
Bad
Ugly

DNS  amplifier  DDoS  attacks

---

Query time: 3 msec
SERVER: 10.10.0.8#53(10.10.0.8)
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

Unique Domain Names (in Millions)

Source: Nominum
What’s wrong with subdomains?

blackhat.com.

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

104.20.66.243

wwwwww.blackhat.com.
mwww.blackhat.com.
mmmwww.blackhat.com.

NXDOMAIN

mmmww.blackhat.com.
mmmmm.blackhat.com.
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
  - zdecc7nnx
- Time stamps:
  - 1465560729
  - 1465561210
- Random strings
  - WO423WWWOX5C
  - FN88RBHXWX9J
- Random numbers
  - 2967230841
  - 4343234574
- Sequence numbers
  - 1165885261118
  - 1165885261119
- Dictionary words
  - glassmaking
  - dishwasher
SUBDOMAIN POSITION:

- Left most
- 2nd left most
- 3rd left most
- Any position on the left side of target domain


n.m.zdecc7nnx.www.blackhat.com.
SUBDOMAIN COMPOSITION:

• Single subdomain string
  FN88RBHXWX9J.blackhat.com.

• Multiple subdomain strings

• Combination of constant and random strings
• 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
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
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?
SIMPLE PROTOCOL ABUSE CAN BECOME A MAJOR SECURITY HEADACHE AND COSTLY MITIGATION:

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