Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices

Xiaofeng Zheng, Chaoyi Lu, Jian Peng, Qiushi Yang, Dongjie Zhou, Baojun Liu, Keyu Man, Shuang Hao, Haixin Duan and Zhiyun Qian
DNS Forwarder

- Devices standing in between stub and recursive resolvers
  - E.g., home routers, open Wi-Fi networks
  - Can have caching abilities
  - Relies on the integrity of upstream resolvers
DNS Cache Poisoning Attacks

- Forging attacks targeting recursive resolvers
  - Craft a DNS answer which matches the query’s metadata
  - Example: Kaminsky Attack (2008)
  - Mitigation: increase randomness of DNS packet

RFC 5452: DNS resolver implementations should use randomized ephemeral port numbers and DNS transaction IDs
Threat Model: Overview

- Defragmentation attacks targeting DNS forwarders
  - Reliably forces DNS response fragmentation
  - Targets arbitrary victim domain names
Threat Model: Overview

- Defragmentation attacks targeting DNS forwarders
  - Reliably forces DNS response fragmentation
  - Targets arbitrary victim domain names

1. Attacker & DNS forwarder locate in the same LAN (e.g., in open Wi-Fi networks)
2. Use attacker’s own domain name and authoritative server
Insight on Forwarder Roles

- Defragmentation attacks targeting DNS forwarders
  - **Reliably** forces DNS response fragmentation
  - Targets *arbitrary victim domain names*

1. Attacker & DNS forwarder locate in the same LAN (e.g., in open Wi-Fi networks)
2. Use attacker’s own domain name and authoritative server

Relies on recursive resolvers
Target of cache poisoning

Security checks (e.g., DNSSEC)
Attacker’s Oversized DNS Response

- CNAME chain
  - Use dummy **CNAME records** to enlarge attacker’s DNS response

<table>
<thead>
<tr>
<th>1st fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.attacker.com CNAME b.attacker.com</td>
</tr>
<tr>
<td>b.attacker.com CNAME c.attacker.com</td>
</tr>
<tr>
<td>c.attacker.com CNAME d.attacker.com</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>x.attacker.com CNAME y.attacker.com</td>
</tr>
<tr>
<td>y.attacker.com CNAME z.attacker.com</td>
</tr>
<tr>
<td>z.attacker.com A x.x.x.x</td>
</tr>
</tbody>
</table>

> 1,500 Bytes (Ethernet MTU)
Always produce fragments
Attacker’s Oversized DNS Response

- **CNAME chain**
  - Use dummy **CNAME records** to enlarge attacker’s DNS response
  - Use CNAME to **point attacker’s domain to any victim**

---

### What the recursive resolver sees

1st fragment

<table>
<thead>
<tr>
<th>a.attacker.com CNAME b.attacker.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.attacker.com CNAME c.attacker.com</td>
</tr>
<tr>
<td>c.attacker.com CNAME d.attacker.com</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>x.attacker.com CNAME y.attacker.com</td>
</tr>
<tr>
<td>y.attacker.com CNAME z.attacker.com</td>
</tr>
<tr>
<td>z.attacker.com A x.x.x.x</td>
</tr>
</tbody>
</table>

2nd fragment

---

### What the DNS forwarder sees

1st fragment

<table>
<thead>
<tr>
<th>a.attacker.com CNAME b.attacker.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.attacker.com CNAME c.attacker.com</td>
</tr>
<tr>
<td>c.attacker.com CNAME d.attacker.com</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>x.attacker.com CNAME y.attacker.com</td>
</tr>
</tbody>
</table>

2nd fragment

| y.attacker.com CNAME victim.com |
| victim.com A a.t.k.r |

Spoofed 2nd fragment
Attacker’s Oversized DNS Response

- **CNAME chain**
  - Use dummy **CNAME records** to enlarge attacker’s DNS response
  - Use CNAME to **point attacker’s domain to any victim**

<table>
<thead>
<tr>
<th>What the recursive resolver sees</th>
<th>1st fragment</th>
<th>2nd fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.attacker.com CNAME b.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b.attacker.com CNAME c.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c.attacker.com CNAME d.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x.attacker.com CNAME y.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>y.attacker.com CNAME z.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z.attacker.com A x.x.x.x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What the DNS forwarder sees</th>
<th>1st fragment</th>
<th>Spoofed 2nd fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.attacker.com CNAME b.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b.attacker.com CNAME c.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c.attacker.com CNAME d.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x.attacker.com CNAME y.attacker.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>y.attacker.com CNAME victim.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>victim.com A a.t.k.r</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spoofer 2nd fragment</td>
</tr>
</tbody>
</table>
Flow of Defragmentation Attack

- Defragmentation attacks targeting DNS forwarders

1. Craft spoofed 2nd fragment
Flow of Defragmentation Attack

- Defragmentation attacks targeting DNS forwarders

1. Craft spoofed 2nd fragment
2. Issue a DNS query
Flow of Defragmentation Attack

- Defragmentation attacks targeting DNS forwarders

1. Craft spoofed 2nd fragment
2. Issue a DNS query
3. Authoritative returns oversized response (> Ethernet MTU)
Flow of Defragmentation Attack

- Defragmentation attacks targeting DNS forwarders

1. Craft spoofed 2nd fragment
2. Issue a DNS query
3. Authoritative returns oversized response (> Ethernet MTU)
4. Defragment by forwarder
Flow of Defragmentation Attack

- Defragmentation attacks targeting DNS forwarders

1. Craft spoofed 2nd fragment
2. Issue a DNS query
3. Authoritative returns oversized response (> Ethernet MTU)
4. Defragment by forwarder

- **Lack Security Checks**

Diagram showing the flow:

- **Attacker**
- **DNS Forwarder**
- **Recursive resolver**
- **Authoritative Server** (attacker.com)

Steps:

0a. Any query (to recursive)

1. Spoofed 2nd fragment
   - Header: victim.com A a.t.k.r

2a. Query a.attacker.com

2b. Query a.attacker.com

2c. Query a.attacker.com

2d. Follow aliases (CNAME)

3a. Responses

3b. Aggregated by resolver
   - (CNAME chain)
   - attacker.com A x.x.x.x

0b. Response

- Fragment cached

- Reassembled rogue response
Conditions of Successful Attacks

- **DNS caching by record**
  - The tampered record can be cached separately

- **EDNS(0) support**
  - Allows transfer of DNS messages larger than 512 Bytes

- **No active truncation of DNS response**
  - Ensures that the entire oversized response is transferred

- **No response verification**
  - DNS forwarders rely on upstream resolvers
Vulnerable DNS Software

- **Home routers**
  - 16 models are tested (by real attacks in controlled environment)
  - **8 models** are vulnerable

- **DNS software**
  - **2 kinds of popular DNS software** are vulnerable

<table>
<thead>
<tr>
<th>Brand</th>
<th>Model</th>
<th>EDNS(0)</th>
<th>No Truncation</th>
<th>Cache by Record</th>
<th>Vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-Link</td>
<td>DIR 878</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ASUS</td>
<td>RT-AC66U B1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Linksys</td>
<td>WRT32X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Motorola</td>
<td>M2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Xiaomi</td>
<td>3G</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GEE</td>
<td>Gee 4 Turbo</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wavlink</td>
<td>A42</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Volans</td>
<td>VE984GW+</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>EDNS(0) &amp; No truncation</th>
<th>Cache by Record</th>
<th>No Verification</th>
<th>Vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>dnsmaq</td>
<td>2.7.9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS DNS</td>
<td>2019</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
**Vulnerable DNS Software**

- **Home routers**
  - 16 models are tested (by real attacks in controlled environment)
  - 8 models are vulnerable

- **DNS software**
  - 2 kinds of popular DNS software are vulnerable

- **Responsible Disclosure**
  - ASUS and D-Link release firmware patches
  - Linksys accepts issue via BugCrowd
Measuring Clients Potentially Under Risk

- Collect vantage points
  - Implement measurement code in a network diagnosis tool
  - **20K clients**, mostly located in China

- Check the forwarder conditions
  - Ethical considerations: no real attack
  - 40% do not support EDNS(0) yet
  - **Estimated vulnerable clients: 6.6%**
Discussion

- **Mitigation for DNS forwarders**
  - Perform response verification (e.g., DNSSEC)
  - **DNS caching by response (short-term solution)**

- **Lack clear guidelines of DNS forwarders**
  - What role should they play?
  - What features should be supported?
- An attack targeting DNS forwarders
- Affects forwarder implementations extensively
- Call for more attention on DNS forwarder security

Any Questions?

zxf19@mails.tsinghua.edu.cn