Content

I  Security Risks with DNS
II  The Biggest Threat - DDoS
III  Current .kr DNS Status
IV  .kr DNS Security Initiative
I. Security Risks with DNS

Data Corruption

Threats causing unauthorized change of information in the DNS
- Authority Impersonation
- Authoritative Server Corruption
- Cache Corruption
- Protocol Corruption

DDoS Attacks

Threats preventing Internet users from using the DNS
- Resource Starvation
- Resource Disruption

Information Exposure

Threats causing disclosure of information about Internet users by examination of their DNS traffic
- Domain Front Running
- Cache Snooping
- Zone Walking
- DNS Query Tracking
- NXDomain Redirection

Threats from DNS

Threats utilizing DNS as a useful tool for attacking 3rd targets
- DNS Amplification Attacks
- Fast Flux DNS
- DNS as a Covert Channel
Ⅱ. The Biggest Threat - DDoS

- **Main Targets of DDoS Attack**: DNS, Government

  - 2012 → 2017: DNS (70%→82%), Web (HTTP, 86%→80%)

  ```
  *
  2012
  2017
  ```

  - 2012 → 2017: Government (15%→37%)

  ```
  ```
Ⅱ. The Biggest Threat - DDoS (cont.)

- Massive Amount of Traffic Attack through **IoT devices**

!![Graph showing DDoS Attack Size Year Over Year]

<table>
<thead>
<tr>
<th>Time</th>
<th>Traffic</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>'15.12</td>
<td>602Gbps</td>
<td>BBC (UK)</td>
</tr>
<tr>
<td>'16.09</td>
<td>665Gbps</td>
<td>Krebs On Security (US)</td>
</tr>
<tr>
<td>'16.09</td>
<td>~ 1Tbps</td>
<td>OVH (France)</td>
</tr>
<tr>
<td>'16.10</td>
<td>~ 1.2Tbps</td>
<td>Dyn (US)</td>
</tr>
<tr>
<td>'18.2</td>
<td>~ 1.35Tbps</td>
<td>Github (US)</td>
</tr>
<tr>
<td>'18.3</td>
<td>~ 1.7Tbps</td>
<td>One of Arbor’s Customers (US)</td>
</tr>
</tbody>
</table>

< **DDoS Attacks through Malware-infected CPE → IoT devices** >
China easily retained pole position by number of attacks: its share remained almost unchanged, up from 59.18% to 59.42%. The US share (17.83%), the second largest, increased by a more noticeable 1.83%. South Korea again took bronze, but its share fell by more than 2%, from 10.21% to 8%. Britain (1.30%) moved from fourth to fifth. Tenth place in Q1 2018 went to Russia, whose share decreased from 1.25% to 0.76%. The Netherlands and Vietnam dropped out of the top ten, but Hong Kong (with a solid 3.67% against 0.67% in Q4 2017) and Japan (1.16%) reappeared.

The top ten countries by number of C&C servers last quarter underwent a major reshuffle: Canada, Turkey, Lithuania, and Denmark dropped out, while Italy, Hong Kong, Germany, and Britain climbed upwards. The top three remained practically unchanged: South Korea (30.92%), the US (29.32%), China (8.03%). Only Russia (2.01%), having shared bronze with China in late 2017, slid down to ninth place.
Ⅲ. Current .kr DNS Status

<table>
<thead>
<tr>
<th>Domain</th>
<th>Stat ('18. 4.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>.kr</td>
<td>1,046,953</td>
</tr>
<tr>
<td>.한국(IDN)</td>
<td>30,179</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP</th>
<th>Stat ('18. 4.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>112,389,888</td>
</tr>
<tr>
<td>IPv6 (/32)</td>
<td>5,253</td>
</tr>
<tr>
<td>ASN</td>
<td>1,024</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>Query &amp; Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>krDNS</td>
<td></td>
</tr>
<tr>
<td>.kr</td>
<td></td>
</tr>
<tr>
<td>.한국 DNS</td>
<td></td>
</tr>
</tbody>
</table>

Table:

<table>
<thead>
<tr>
<th>Index</th>
<th>Average</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>krDNS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IV. .kr DNS Security Initiative

.kr DNS Cloud Service

Anycast Only

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abroad</th>
<th>USA</th>
<th>China</th>
<th>Brazil</th>
<th>USA (Verisign)</th>
<th>Germany</th>
</tr>
</thead>
</table>

Cloud Service

Anycast + Cloud

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abroad</th>
<th>USA</th>
<th>China</th>
<th>Brazil</th>
<th>USA</th>
<th>Germany</th>
</tr>
</thead>
</table>

Solo Site
D.DNS.KR Anycast Sites
E.DNS.KR Anycast Sites
F.DNS.KR Cloud Sites
G.DNS.KR Anycast Sites

Global Internet Cloud
Security Protection & SLA

Global Internet Data Center
IV. .kr DNS Security Initiative (cont.)

.lesson .kr DNS Clean Zone Service

Normal

Internet

Cache DNS

Internet Users

Clean Zone

DDoS Protection (IDS, IPS, ...)

.ISP

.kr DNS

DDoS Attack

Internet

Cache DNS

Internet Users

Zombie PC

Attacker

Clean Zone

DDoS Protection (IDS, IPS, ...)

.ISP

.kr DNS
IV. .kr DNS Security Initiative (cont.)

Data driven .kr DNS Security Project Concept

Malicious Activity:
- Spam-runs
- Botnets like cutwall
- DNS-Amplification attacks
IV. .kr DNS Security Initiative (cont.)

Data driven .kr DNS Project Architecture (concept)
Internet On, Security In!

Thank you!