Internet-wide Scanning and Notifications to Prevent Cybercrime

Orçun Çetin
Orcun.Cetin@sabanciuniv.edu
Internet-wide Scanning

- Scanning:
  - Vulnerabilities
    - DNS
  - Malicious behaviour or malware
    - Cryptojacking, hacked websites
  - Honeypots
    - Elastichoney 193.110.211.14 -> Genel Kurmay Baskanligi
Zone Poisoning Vulnerability

- Cause: nameservers configured to allow non-secure dynamic updates.
- Anyone can manipulate DNS entries with single packet.
- Consequences: running **fake website/mail server** for phishing or espionage purposes.

```bash
~$ nsupdate
> server 192.2.2.101
> zone example.com
> update add paypal.example.com 86400 A 10.10.10.10
> send
```
# Zone Poisoning Vulnerability

<table>
<thead>
<tr>
<th>Type</th>
<th>in #</th>
<th>in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>181</td>
<td>31</td>
</tr>
<tr>
<td>Entertainment</td>
<td>92</td>
<td>15.7</td>
</tr>
<tr>
<td>Educational</td>
<td>90</td>
<td>15.3</td>
</tr>
<tr>
<td>Governmental</td>
<td>56</td>
<td>9.5</td>
</tr>
<tr>
<td>News services</td>
<td>41</td>
<td>7</td>
</tr>
<tr>
<td>Adult</td>
<td>13</td>
<td>2.2</td>
</tr>
<tr>
<td><strong>Financial services</strong></td>
<td><strong>9</strong></td>
<td><strong>1.5</strong></td>
</tr>
<tr>
<td>Health care</td>
<td>8</td>
<td>1.4</td>
</tr>
<tr>
<td>Other</td>
<td>95</td>
<td>16.2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>587</td>
<td>100</td>
</tr>
</tbody>
</table>
Notifications

- All notified groups did better than the control group.
- Still, overall remediation rates were low.
Does it help to demonstrate the vulnerability?

- Short answer: no.
Thank you for listening!

- More info: Orcun.Cetin@sabanciuniv.edu
- More info on underlying study: