Passive DNS Replication

Florian Weimer

17th Annual FIRST Conference, Singapore, 2005

Outline

A very brief introduction to DNS

Case Study: Botnet mitigation

Architecture and implementation

Results
A very brief introduction to DNS

Outline

A very brief introduction to DNS

Case Study: Botnet mitigation

Architecture and implementation

Results

DNS as a huge table

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.enyo.de">www.enyo.de</a></td>
<td>A</td>
<td>212.9.189.164</td>
</tr>
<tr>
<td>static.enyo.de</td>
<td>A</td>
<td>212.9.189.164</td>
</tr>
<tr>
<td>mail.enyo.de</td>
<td>A</td>
<td>212.9.189.167</td>
</tr>
<tr>
<td>enyo.de</td>
<td>MX</td>
<td>10 mail.enyo.de</td>
</tr>
<tr>
<td><a href="http://www.first.org">www.first.org</a></td>
<td>A</td>
<td>163.1.2.77</td>
</tr>
<tr>
<td><a href="http://www.first.org">www.first.org</a></td>
<td>A</td>
<td>192.25.206.20</td>
</tr>
<tr>
<td><a href="http://www.first.org">www.first.org</a></td>
<td>A</td>
<td>210.148.223.8</td>
</tr>
<tr>
<td>164.189.9.212.in-addr.arpa</td>
<td>PTR</td>
<td><a href="http://www.enyo.de">www.enyo.de</a></td>
</tr>
</tbody>
</table>
A very brief introduction to DNS

DNS summary

- You can query only by the primary key, the domain/class/type triple.
- Queries on secondary keys can be emulated if the key is encoded in a domain name (as in 164.189.9.212.in-addr.arpa).
- There are no consistency guarantees.
- Reverse lookups (based on PTR records) are optional and not reliable: Both www and static point to 212.9.189.164, but there is only one PTR record.

Case Study: Botnet mitigation

Outline

A very brief introduction to DNS

Case Study: Botnet mitigation

Architecture and implementation

Results
An IDS alert

- The intrusion detection system detects a botnet command:
  T 2005/04/21 18:06:33.188392
  192.0.2.166:6667 -> 212.9.189.171:1037
  :abc!DeFgH@SOME.TLA.GOV
  TOPIC #133t/.advscan dcom135 100 5 0 -r..
- 212.9.189.171 is a compromised host on our network.
- 192.0.2.166 is the botnet controller.
- The captured command instructs 212.9.189.171 to scan for further victims.

Response to the report

- Filter 212.9.189.171, the victim host.
- Filter 192.0.2.166, the botnet controller.
- Contact the owner of the 212.9.189.171 machine and force him to clean it.
- ... and hope for the best.
  - The victims continue to scan the internal network, discovering new victims.
  - Filtering the botnet controller prevents them from joining the botnet. (???)
Case Study: Botnet mitigation

Contacting the botnet controller

- The bot may contain one or more domain names instead of hard-coded IP addresses.
- Each domain can resolve to multiple IP addresses.
- Blocking a single IP address often does not prevent hosts from joining the botnet.
- If you know the domain name, better filters are possible.
  - You can adjust the filters when the domain name changes.
  - You can filter the domain name on your resolvers (in theory).

How to recover domain names from IP addresses

- Reverse engineer the bot.
  - Disassembling needs time and expertise.
  - And a copy of the malware.
- The security team often cannot access the caching resolvers which store a copy of the DNS record.
- Zone file transfers do not work, the traditional DNS replication mechanism, do not work.
Case Study: Botnet mitigation

From domain names to IP addresses

- Capture DNS packets and look for the IP address you are interested in.
- DNS caches may delay the reappearance of resource records for hours.
- Idea: Capture DNS records in advance and store them in a database for later reference.
- This leads to "passive DNS replication".

Outline

A very brief introduction to DNS

Case Study: Botnet mitigation

Architecture and implementation

Results
dnslogger architecture

Sensor placement
Challenges

- Privacy concerns
- Security concerns
- Truncated and EDNS0 responses
- What about bogus DNS data captured by the sensors?
- The data rate itself is fairly low on medium-sized campus networks.
- But keeping lots of historic data is problematic.

\textit{dnslogger implementation}

- Two sensor implementations:
  - Perl: simple and obviously correct
  - C: higher performance, fewer dependencies
- The remaining parts of the\textit{dnslogger} software are written in Ada.
- Berkeley DB from Sleepycat is used as the underlying database technology.
  - The schema design is highly denormalized and clustered on reversed domain names.
  - All database updates are idempotent and commute, which makes replication particularly easy.
Outline

A very brief introduction to DNS

Case Study: Botnet mitigation

Architecture and implementation

Results

Examples

- Identify botnet controllers
- Track DNS-driven botnets (Blaster)
- Correlate domains
- Dating DNS anomalies (new or just newly discovered?)
### Example: The kimble.org fiasco

<table>
<thead>
<tr>
<th>First seen</th>
<th>Domain</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-06-23 13:58:51</td>
<td>kimble.org</td>
<td>A</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>2004-08-07 16:14:00</td>
<td>kimble.org</td>
<td>A</td>
<td>207.234.155.17</td>
</tr>
<tr>
<td>2004-10-20 07:15:58</td>
<td>kimble.org</td>
<td>A</td>
<td>212.100.234.54</td>
</tr>
<tr>
<td>2004-10-20 16:12:56</td>
<td>kimble.org</td>
<td>A</td>
<td>64.203.97.121</td>
</tr>
<tr>
<td>2004-10-21 17:15:01</td>
<td>kimble.org</td>
<td>A</td>
<td>212.113.74.58</td>
</tr>
<tr>
<td>2004-10-21 17:45:01</td>
<td>kimble.org</td>
<td>A</td>
<td>195.130.152.100</td>
</tr>
<tr>
<td>2004-10-31 14:45:01</td>
<td>kimble.org</td>
<td>A</td>
<td>195.225.218.59</td>
</tr>
<tr>
<td>2004-11-02 23:15:01</td>
<td>kimble.org</td>
<td>A</td>
<td>206.132.83.2</td>
</tr>
<tr>
<td>2004-11-04 18:15:01</td>
<td>kimble.org</td>
<td>A</td>
<td>213.139.139.206</td>
</tr>
<tr>
<td>2004-11-21 03:15:02</td>
<td>kimble.org</td>
<td>A</td>
<td>216.7.173.212</td>
</tr>
<tr>
<td>2004-11-25 22:45:02</td>
<td>kimble.org</td>
<td>A</td>
<td>38.112.165.60</td>
</tr>
</tbody>
</table>

### Example: Hijacking of ebay.de

<table>
<thead>
<tr>
<th>First seen</th>
<th>Domain</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-06-23 08:21:57</td>
<td>ebay.de</td>
<td>NS</td>
<td>crocodile.ebay.com</td>
</tr>
<tr>
<td>2004-06-23 08:21:57</td>
<td>ebay.de</td>
<td>NS</td>
<td>sjc-dns1.ebaydns.com</td>
</tr>
<tr>
<td>2004-06-23 08:21:57</td>
<td>ebay.de</td>
<td>NS</td>
<td>sjc-dns2.ebaydns.com</td>
</tr>
<tr>
<td>2004-08-28 05:34:01</td>
<td>ebay.de</td>
<td>NS</td>
<td>ns1.goracer.de</td>
</tr>
<tr>
<td>2004-08-28 05:34:01</td>
<td>ebay.de</td>
<td>NS</td>
<td>ns2.goracer.de</td>
</tr>
</tbody>
</table>
Example: Network Solution’s “Site Finder Light”

<table>
<thead>
<tr>
<th>First seen</th>
<th>Domain</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-09-19 05:01:53</td>
<td>misslink.net</td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 05:57:49</td>
<td>ns.bighornent.com</td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 06:13:44</td>
<td>ns13.magnum-inap4.net</td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 06:24:28</td>
<td>host2.7thgate.com</td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 07:25:26</td>
<td><a href="http://www.zydigo.com">www.zydigo.com</a></td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 08:08:33</td>
<td>muslimsonline.com</td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 08:28:26</td>
<td><a href="http://www.animatiehuis.com">www.animatiehuis.com</a></td>
<td>CNAME</td>
<td>†</td>
</tr>
<tr>
<td>2004-09-19 08:57:19</td>
<td><a href="http://www.urbanvoicesonline.com">www.urbanvoicesonline.com</a></td>
<td>CNAME</td>
<td>†</td>
</tr>
</tbody>
</table>

† = resalehost.networksolutions.com

Example: Correlating domains

- An email messages references dkchaotichigh.com ("MegaPowerPills.com").
- An ordinary DNS lookup reveals that ns1.m-dns.us is used as a name server.
- Additional domains are hosted on this name server:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>outfacegood.com</td>
<td>NS</td>
<td>ns1.m-dns.us</td>
</tr>
<tr>
<td>outregood.com</td>
<td>NS</td>
<td>ns1.m-dns.us</td>
</tr>
<tr>
<td>megalithgood.com</td>
<td>NS</td>
<td>ns1.m-dns.us</td>
</tr>
<tr>
<td>medverdigrisgood.com</td>
<td>NS</td>
<td>ns1.m-dns.us</td>
</tr>
</tbody>
</table>

...
Example: Unauthorized name servers for .com

<table>
<thead>
<tr>
<th>First seen</th>
<th>Domain</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-06-24 00:52:37</td>
<td>com</td>
<td>NS</td>
<td>ns1.hi2000.net</td>
</tr>
<tr>
<td>2004-06-30 23:26:21</td>
<td>com</td>
<td>NS</td>
<td>tempsvr.wam.wamusa.com</td>
</tr>
<tr>
<td>2004-07-01 04:32:18</td>
<td>com</td>
<td>NS</td>
<td>ns7.domainredirect.com</td>
</tr>
<tr>
<td>2004-07-05 04:18:36</td>
<td>com</td>
<td>NS</td>
<td>ns1.infoglobe.net</td>
</tr>
<tr>
<td>2004-07-05 07:35:14</td>
<td>com</td>
<td>NS</td>
<td>ns1.cntrading.com</td>
</tr>
<tr>
<td>2004-07-05 16:40:27</td>
<td>com</td>
<td>NS</td>
<td>ns1.spacesurfer.com</td>
</tr>
<tr>
<td>2004-07-08 00:34:29</td>
<td>com</td>
<td>NS</td>
<td>ns.tradenames.com</td>
</tr>
</tbody>
</table>

Observations

- DNS usage is very localized and specific to the network in which the sensor is placed.
- For many applications, you have to run your own sensor, instead of using data collected on other networks.
- But sharing the data with others does not hurt.
Summary

▶ Passive DNS replication provides new ways to access and process DNS data.
▶ This data can support various security-related processes.
▶ It also provides new insights into the operation of the domain name system.
▶ Questions?