Cisco CSIRT’s Passive DNS Collection and Searching System

Henry Stern
Two Separate Problems: Questions and Answers
DNS Answers

• Complex data:
  Time, source, destination, question, answer, additional records.

• What did a name resolve to and when?
• What else resolved to this IP?
• What else is served by this name server?
• Solution: Passive DNS Replication

  • https://dnsdb.isc.org/
  • http://www.bfk.de/bfk_dnslogger.html
  • http://www.enyo.de/fw/software/dnslogger/
DNS Questions

• Simple data:
  - Source IP.
  - Destination IP.
  - Question – qname and qtype.

• Great for forensics.

• Who looked up this name?

• Who is a member of this botnet?

• What did this host look up?
DNS traffic capture design
How Much Data?

• 130k active Windows hosts at any given time.
• 90k active Linux hosts at any given time.
• 10 billion Netflows captured at zone boundaries.
• IDS sensors at all zone boundaries.
• 1 Tb of security event log data.

• 13 data centres, DMZs covered with PDNS.
• 4 billion DNS and NetBIOS packets captured per day.
• 300gb of traffic captured per day.
DNS Question Search Tool

• Data captured with ncaptool.
• Search engine written in Python+Pyrex.
• Uses libbind/Strangle, pyncap, IPy, pySubnetTree, list2re, pybloomfilter.
• Files are indexed with a Bloom filter.
  - Quickly determines whether a file contains entries that match a query.
  - Pre-computation by cron job.
• Distributed search client/server.
  - JSON-based protocol.
  - Use SSL certs for authentication.
  - Future: Switch to HTTPS+SRP.
Command Line Interface

## Demo – Mariposa Infections

$ pdns-search --qname bfisback.no-ip.org --max-results 4

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Source</th>
<th>Destination</th>
<th>QName</th>
<th>QType</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-08-21</td>
<td>ELIDED</td>
<td>64.102.255.44</td>
<td>bfisback.no-ip.org</td>
<td>A</td>
</tr>
<tr>
<td>2012-08-21</td>
<td>64.102.255.43</td>
<td>69.65.40.108</td>
<td>bfisback.no-ip.org</td>
<td>A</td>
</tr>
<tr>
<td>2012-08-21</td>
<td>ELIDED</td>
<td>64.102.255.44</td>
<td>bfisback.no-ip.org</td>
<td>A</td>
</tr>
<tr>
<td>2012-08-21</td>
<td>64.102.255.43</td>
<td>69.72.255.8</td>
<td>bfisback.no-ip.org</td>
<td>A</td>
</tr>
</tbody>
</table>

Search: 100% | ####################################################| Time: 0:00:03 Files: 780/780
Using Our Tools

• Fill in gaps in Netflow coverage.
• Alert on queries for dangerous domain names.
• Look for patterns in queries to discover C2 servers.
• Monitor queries about high-value targets.
• Watch for new names hosted on dangerous networks.
• Discover new dangerous networks.
Future

• Tell us when DNS responses have changed.
• Automatically feed the data to other systems.
• Integrate our searches with external systems.
  Logs (Splunk)
  Flows (Lancope)
  SenderBase Network Participation