Practical Comprehensive Bounds on Surreptitious Communication Over DNS

Vern Paxson\textsuperscript{1,2} Mihai Christodorescu\textsuperscript{3} Mobin Javed\textsuperscript{1} Josyula Rao\textsuperscript{4} Reiner Sailer\textsuperscript{4} Douglas Schales\textsuperscript{4} Marc Ph Stoecklin\textsuperscript{4} Kurt Thomas\textsuperscript{1} Wietse Venema\textsuperscript{4} Nicholas Weaver\textsuperscript{2,5}

\textsuperscript{1}UC Berkeley  \textsuperscript{2}ICSI \textsuperscript{3}Qualcomm Research \textsuperscript{4}IBM research \textsuperscript{5}UC San Diego
DATA EXFILTRATION

ENTERPRISE

DNS resolver

DNS requests

HTTP, FTP, etc.

Hijacked system

INTERNET

DNS server controlled by attacker

REMOTE ACCESS

ENTERPRISE

DNS resolver

DNS requests

DNS responses

Hijacked system

INTERNET

SSH
Our work in a nutshell

- Bound information content of DNS query sequences.
- 4 kB/day per client and domain (site.com, site.co.uk).
- Lossless (reversible) compression: no false negatives.
- 1-2 Alerts/week for enterprise-scale networks.
- 59 Confirmed DNS tunnels in 230B lookups.
Next: information embedding examples.

- Query content.
- Query timing.
Information vector: DNS query name content
Actual queries, slightly altered for privacy

- **Tunnel:** SSH over Iodine (TCP/IP over DNS).

  0ebba82?2db??Y?wl??bb??X?Ey0bdj?gZqH??4?1NM????0?aQ
  l????????db??4.????Zz????4BJ?hLv?????4a??i?G.t.porcupinc
  e.org (\(?\) = non-ASCII or non-printable octet)

- **Non-tunnel:** software installer.

  x--00453809-004d-0046-00523-004e-0051-0034004243-0
  051-0055-.00583-0051-0053-0050-0056.val.linux.10-2
  0-191-136.9_5-3532-6097.sn.msgserv.ZeroG.com

- **Capacity:** up to 255 bytes/query.

- **59 Confirmed name-content tunnel detections.**
Information vector: DNS query name codebook
Actual queries, slightly altered for privacy

<table>
<thead>
<tr>
<th>query name</th>
<th>type</th>
<th>time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a0.twimg.com</td>
<td>A</td>
<td>1286949054.503602</td>
</tr>
<tr>
<td>a3.twimg.com</td>
<td>A</td>
<td>1286949216.242019</td>
</tr>
<tr>
<td>a3.twimg.com</td>
<td>A</td>
<td>1286949251.387366</td>
</tr>
<tr>
<td>a1.twimg.com</td>
<td>A</td>
<td>1286949277.589322</td>
</tr>
<tr>
<td>a2.twimg.com</td>
<td>A</td>
<td>1286949295.694136</td>
</tr>
<tr>
<td>a3.twimg.com</td>
<td>A</td>
<td>1286949310.772878</td>
</tr>
<tr>
<td>a1.twimg.com</td>
<td>A</td>
<td>1286949310.816623</td>
</tr>
<tr>
<td>a3.twimg.com</td>
<td>A</td>
<td>1286949418.455759</td>
</tr>
<tr>
<td>a1.twimg.com</td>
<td>A</td>
<td>1286949418.627365</td>
</tr>
<tr>
<td>a3.twimg.com</td>
<td>A</td>
<td>1286949448.813207</td>
</tr>
<tr>
<td>a0.twimg.com</td>
<td>A</td>
<td>1286949461.172023</td>
</tr>
</tbody>
</table>

- Capacity: up to $\log_2$ (codebook size) bits/query.
- No confirmed tunnel detections.

Is this a name tunnel? e.g.,
00 → a0
01 → a1
10 → a2
11 → a3
Information vector: DNS query type
Actual queries, slightly altered for privacy

<table>
<thead>
<tr>
<th>query name</th>
<th>type</th>
<th>time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>AAAA</td>
<td>1363620228.803181</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>A</td>
<td>1363620228.837213</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>AAAA</td>
<td>1363620228.862057</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>A</td>
<td>1363620228.878191</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>A</td>
<td>1363620229.149720</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>AAAA</td>
<td>1363620229.239968</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>A</td>
<td>1363620229.269800</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>AAAA</td>
<td>1363620229.319941</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>AAAA</td>
<td>1363620229.377394</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>A</td>
<td>1363620229.406241</td>
</tr>
<tr>
<td><a href="http://www.e-port.ru">www.e-port.ru</a></td>
<td>AAAA</td>
<td>1363620229.412821</td>
</tr>
</tbody>
</table>

- Capacity: up to 16 bits/query (IANA defines 79 types).
- No confirmed tunnel detections.
Information vector: DNS query timing

Actual queries

- Capacity: $O(100)$ bits/second at 10 msec resolution\(^1\).
- No confirmed detections, but source of most alerts.

\(^1\)Conservative resolution based on median 23msec DNS timing variations observed with Netalyzr.
Next: measuring **all** information content in DNS queries.

- Regardless of encoding in names, types or timing.
- First, focus on query names.
Measuring information in DNS query names, step 1
Result: 2174 alerts for IndLab dataset

“foo.example.com” + “bar.example.com” + …

- **Naive approach: concatenate all query names.**
  - Problem: too many alerts.
Measuring information in DNS query names, step 2
Result: 2174→145 alerts for IndLab dataset

- Use lossless (reversible) data compression.
  - Output length ≥ information content. No false negatives.
    - Insensitive to encoding details (8-bit, base64, etc.).
      - Append “..” to names, for reversible compression.

```bash
gzip(“foo.example.com..” + “bar.example.com..” +…)
```
Use smallest result from different lossless compressors.

- Different compressors, different worst cases.
Use codepoints (besides straight compression):

- Transform names $A \rightarrow$ table of distinct names $D$ + sequence of table indices $I$ (codepoints). Then compress $D$ and $I$.
  - Exploit repetition at the granularity of entire query names.
    - Minor benefit for time-interval and query-type results (small symbols).
Combined DNS query information measurement

Use same procedure to separately measure:

- Sequence of query names; sequence of query types;
- sequence of inter-query time intervals (10 msec units\(^1\)).

\(^1\)Conservative resolution based on median 23msec DNS timing variations observed with Netalyzr.
Validation with synthetic traffic

Exfiltration scenario
Next: detecting DNS tunnels in mostly-benign traffic.

- From 45M→4089 queries without introducing false negatives.
Searching a haystack of 230B lookups

<table>
<thead>
<tr>
<th>Site</th>
<th>Vantage point</th>
<th>Clients</th>
<th>Days</th>
<th>Lookups (daily)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IndLab(^1)</td>
<td>Internal DNS server</td>
<td>10k</td>
<td>1212</td>
<td>57B (47M)</td>
</tr>
<tr>
<td>LBL(^2)</td>
<td>Internal DNS server</td>
<td>6.8k</td>
<td>2776</td>
<td>79B (28M)</td>
</tr>
<tr>
<td>NERSC(^3)</td>
<td>Internal DNS server</td>
<td>1.3k</td>
<td>1642</td>
<td>14B (9M)</td>
</tr>
<tr>
<td>UCB campus</td>
<td>Network perimeter</td>
<td>2.1k</td>
<td>45</td>
<td>1.7B (38M)</td>
</tr>
<tr>
<td>China campus</td>
<td>Caching resolver</td>
<td>61k</td>
<td>5</td>
<td>69M (14M)</td>
</tr>
<tr>
<td>SIE(^4)</td>
<td>Reply mirrors</td>
<td>123</td>
<td>53</td>
<td>77B (1.5B)</td>
</tr>
</tbody>
</table>

\(^1\) Undisclosed Industrial Research Laboratory, USA.
\(^2\) Lawrence Berkeley National Laboratory, USA.
\(^3\) National Energy Research Supercomputing Center, USA.
\(^4\) ISC Security Information Exchange, contributions mainly from USA and Europe.
Input filters
Numbers for 1 day of IndLab traffic

1: Eliminate queries that hit the local DNS resolver cache.
   - Model local DNS resolver cache (requires reply TTLs).

2: Eliminate “uninteresting” queries.
   - Non-existent top-level domains (Mozilla “effective TLD” list).
   - Local/sister/reserved domains and (PTR) address ranges.
3: Aggregate queries by (client, query name suffix).

- 1 Query name suffix ≤ 1 organization.
  
  • site.com, site.co.uk (Mozilla “effective TLD” list).
  
  • in-addr.arpa at /16 and /24 boundaries, ip6.arpa at /48.
Quick information estimate before data compression
Numbers for 1 day of IndLab traffic

4: Eliminate (client, name suffix) based on per-day totals.
- Worst-case Shannon entropies: assume uniform distributions over distinct inter-query time intervals, names, and types.
- Plus length of distinct query names and types.
5: Eliminate (client, suffix) with too little information.

- Compressor and codepoint bakeoff.
- 4 kB bound for targeted environments (individual clients).
  - 10 kB bound for aggregated query streams.
6: Eliminate already-inspected domains.

- Each flagged query name suffix is inspected only once.
  - If a benign domain becomes malicious after inspection:
    - It is a major site (Google, etc.) → we have worse problems.
    - It keeps mimicking benign behavior → it remains undetected.
    - It exposes itself to signature-based detection.
Alert rate sensitivity to parameter settings
IndLab data set, 1212 days
## Detection breakdown

<table>
<thead>
<tr>
<th>Dominant source</th>
<th>Individual clients</th>
<th>Aggregates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>IndLab</td>
<td>LBL</td>
</tr>
<tr>
<td>Lookups (days)</td>
<td>57B(1212)</td>
<td>79B(2776)</td>
</tr>
<tr>
<td>Information bound</td>
<td>4kB</td>
<td>4kB</td>
</tr>
<tr>
<td>Confirmed tunnel</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Benign</td>
<td>286</td>
<td>306</td>
</tr>
<tr>
<td>Malware</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Misconfiguration</td>
<td>49</td>
<td>62</td>
</tr>
<tr>
<td>IPv4 PTR</td>
<td>11</td>
<td>29</td>
</tr>
<tr>
<td>IPv6 PTR</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Unknown</td>
<td>14</td>
<td>27</td>
</tr>
<tr>
<td>Total alerts</td>
<td>362</td>
<td>433</td>
</tr>
<tr>
<td>Alerts/typ. week</td>
<td>2.0</td>
<td>1.1</td>
</tr>
</tbody>
</table>
Conclusion

- Novel procedure to measure the information content of DNS query streams.
- 1-2 Alerts/week for enterprise-scale networks.
  - 4 kbytes/day threshold per local client and remote domain.
  - Lossless compression, no false negatives.
- 59 Confirmed DNS tunnels in 230B queries.
  - All conventional name-content based.