HOW TO ROCK WITH DNS
Patterns for Detection and Faster Spotting of Malicious Activities

João Collier de Mendonça
Prague – CZ, October 2016.
$ whoami

- Brazilian living in Germany for a long time
- Since 2010 at Deutsche Telekom CERT / CDC
- Based in Bonn, Germany
- Network Security & Forensics, Incident Response, Collaboration
- I’d rather be sailing :-(
PROBLEM STATEMENT
THE “WHAT”

• Use DNS features※ to spot malicious activities

※ features in the sense of “characteristics”
THE “WHY”

• Networks are ubiquitous, so is DNS
• Malware uses DNS widely
• Organisations frequently do not monitor it properly

Source: Cisco 2016 Annual Security Report
Your blind spot is the attacker’s sweet spot
CONCEPTS

essential to the coming ideas
A DIFFERENT VIEW ON DNS

• Database that can be publicly queried

• Frequently no egress control (internal endpoints use google DNS)

• Query: Record Type, Key

• Response: Record Type, Key, Associated Values
## SOME RECORD TYPES

<table>
<thead>
<tr>
<th>record type</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>IP address record</td>
</tr>
<tr>
<td>NS</td>
<td>Nameserver responsible for the domain</td>
</tr>
<tr>
<td>TXT</td>
<td>Descriptive data about a domain</td>
</tr>
<tr>
<td>CNAME</td>
<td>Alternate name for a resource</td>
</tr>
<tr>
<td>SOA</td>
<td>key data about the zone, eg. default TTL</td>
</tr>
</tbody>
</table>

Nice ref: [http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html](http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html)
CONCEPTS (SUMMARY)

- FQDN (hostname)
- Labels (all besides the dots)
- RFC 1035 2.3.4. Size limits
  - Labels (0-63 chars)
  - FQDN length: up to 255 chars

```
$ dig +all isc.org ANY
...
;; ANSWER SECTION:
isc.org. 7200 IN MX 20 mx.ams1.isc.org.
isc.org. 60 IN AAAA 2001:4f8:0:2::69
isc.org. 7200 IN SPF "v=spf1 a mx
ip4:204.152.184.0/21 ~all"
isc.org. 7200 IN NS ns.isc.afilias-nst.info.
isc.org. 7200 IN TXT "google-site-
verification=6v652rgkk_kI6Ky32tGdxqXjQ4_BAd5DYKsHnRXKUiE"
isc.org. 7200 IN SOA ns-int.isc.org.
hostmaster.isc.org. 2016091300 7200 3600 24796800 3600
isc.org. 7200 IN NS ord.sns-pb.isc.org.
isc.org. 60 IN A 149.20.64.69
```
CONCEPTS

fully qualified domain name (FQDN) or hostname

second-level domain name

top-level domain

host

label

label

label
DNS TUNNELLING

• Misuse of DNS protocol to establish a (semi) covert communication channel with an attacker-controlled DNS server

• DNS Protocol: (Request, Reply)

• Challenge: maximise data transfer rate

• Solution: long FQDNs, CNAME for queries; TXT for replies
FURTHER DNS INTRICACIES: DNS RESPONSE CODES

<table>
<thead>
<tr>
<th>Outcome</th>
<th>Descriptive Code</th>
<th>RCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Query completed successfully</td>
<td>NOERROR</td>
<td>0</td>
</tr>
<tr>
<td>Query Format Error</td>
<td>FORMERR</td>
<td>1</td>
</tr>
<tr>
<td>Server failed to complete the DNS request</td>
<td>SERVFAIL</td>
<td>2</td>
</tr>
<tr>
<td>Domain name does not exist</td>
<td>NXDOMAIN</td>
<td>3</td>
</tr>
</tbody>
</table>

This is not an extensive list

Nice source: https://support.opendns.com/hc/en-us/articles/227986827
DNS AND ITS FEATURES
# DNS AND ITS FEATURES

<table>
<thead>
<tr>
<th>DNS Protocol</th>
<th>IP/Network</th>
<th>Domain Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN length</td>
<td>FQDN lexical features</td>
<td>IP addresses (eg. diversity)</td>
</tr>
<tr>
<td>2nd-level domain length</td>
<td>2nd-level domain lexical features</td>
<td>Parked domains (eg. A record non-routable address)</td>
</tr>
<tr>
<td>TTL values</td>
<td>Response codes</td>
<td></td>
</tr>
<tr>
<td>Timing info</td>
<td>(eg. queries / sec)</td>
<td></td>
</tr>
</tbody>
</table>
PATTERNS

a solid starting point
PATTERN 1

FQDN Length
FQDN LENGTH

• Look for very long FQDNs
• Needed to maximise throughput of a DNS tunnel
• As easy as `len(str)` on a widely available field
• Exclude legitimate use: services using disposable hostnames (CDNs, skype, spotify, antivirus, etc)
FQDN LENGTH

• Field is widely available (and rarely used e.g. on SIEM)

• Inspect all FQDN on requests
  tshark -nn -r $PCAP -T fields -E header=n -E occurrence=a -E quote=n -E separator=',' -e dns.qry.name -Y 'ip and dns and (dns.flags.response==0)'
PATTERN 2
Rate of TXT Records
RATE OF TXT RECORDS

• Look for endpoints with higher rate of queries for TXT records
• Needed to maximise throughput of tunnel
• Detected by aggregation of TXT usage by endpoints
• Beware of legitimate usage: Mail servers (SPF), domain ownership verification
RATE OF TXT RECORDS

- Gather DNS replies with TXT records
  
  `tshark -nn -r $PCAP -Y 'ip and dns and (dns.flags.response==1) and dns.qry.type==0x10'`

- Create a aggregated (queries and responses) list of top talkers using TXT records
  
  `tshark -nn -r $PCAP -Y 'ip and dns and dns.qry.type==0x10' -T fields -E header=n -E occurrence=a -E quote=d -E separator=',' -e ip.dst | sort | uniq -c | sort -rn`
PATTERN 3
Rate of NXDOMAIN
RATE OF NXDOMAIN

• "DGA-infected" endpoints will generate DNS response with higher rate of NXDOMAIN

• Simple rate comparison of NXDOMAIN between endpoints

• Exclude legitimate usage, eg. queries for domain.tld.dbl.spamhaus.org
RATE OF NXDOMAIN

• Inspect all responses with DNS NXDOMAIN
  tshark -nn -r $PCAP -Y 'ip and dns and (dns.flags.response==1) and dns.flags.rcode==3'

• Create a list of unique-domain NXDOMAIN top talkers
  tshark -nn -r $PCAP -Y 'dns and (dns.flags.response==1) and dns.flags.rcode!=0' -T fields -E header=n -E occurrence=a -E quote=d -E separator=',' -e ip.dst | sort | uniq -c | sort -rn
#THANKYOU

HOW TO ROCK WITH DNS
Patterns for Detection and Faster Spotting of Malicious Activities

João Collier de Mendonça
Praha CZ, October 2016.