SANS EMEA

DFIR PRAGUE 2016

HOW TO ROCK WITH DNS

Patterns for Detection and Faster Spotting of Malicious Activities

João Collier de Mendonça
Prague – CZ, October 2016.

@sec_joao

$ 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

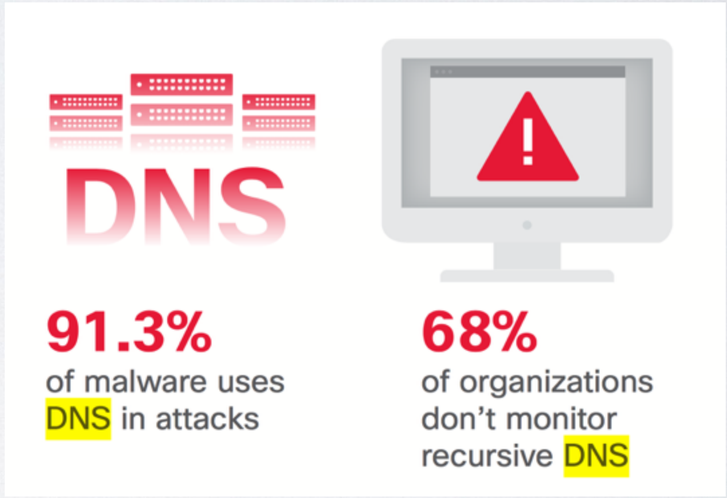
FEEDERBOT

MORTO

PLUGX

WEKBY

SAURON



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

record type	value
A	IP address record
NS	Nameserver responsible for the domain
TXT	Descriptive data about a domain
CNAME	Alternate name for a resource
SOA	key data about the zone, eg. default TTL

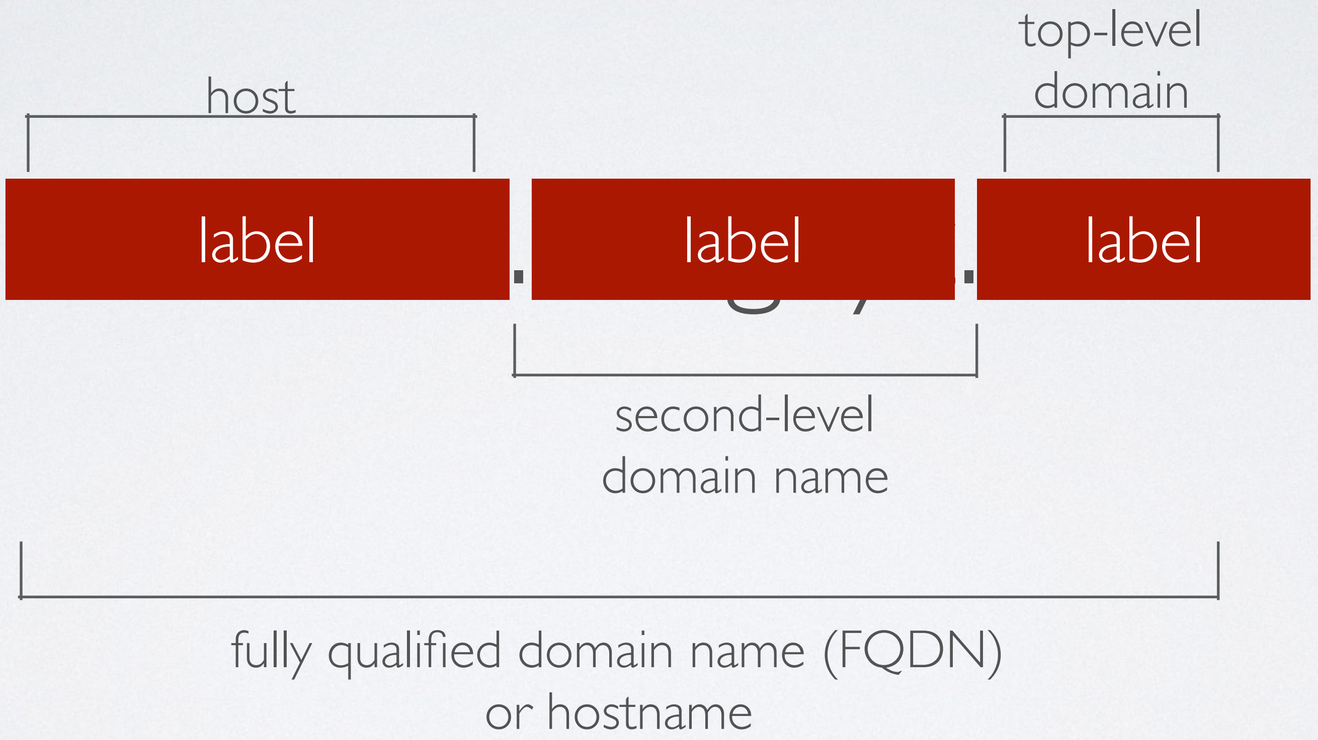
Nice ref: http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

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_kI6Ky32iGdxqXjQ4_BAd5DYKsrnRXKUi
E"
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


top-level
domain
host
label
label
label
second-level
domain name
fully qualified domain name (FQDN)
or hostname

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

Outcome	Descriptive Code	RCode
DNS Query completed successfully	NOERROR	0
Query Format Error	FORMERR	1
Server failed to complete the DNS request	SERVFAIL	2
Domain name does not exist	NXDOMAIN	3
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~~ METADATA

DNS Protocol		IP/Network		Domain Registration	
FQDN length	FQDN lexical features	IP addresses (eg. diversity)	ASNs (eg. diversity)	Contacts: registrar, registrant	Creation date
2nd-level domain length	2nd-level domain lexical features	Parked domains (eg. A record non-routable address)	CNAME, NS, SOA, MX associations	Expiration date	Last update
TTL values	Response codes			Country / Geoloc	
Timing info (eg. queries / sec)					

PATTERNS

a solid starting point

PATTERN 1

FQDN Length

DNS protocol

DNS tunnelling

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)

DNS protocol

DNS tunnelling

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

DNS protocol

DNS tunnelling

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

DNS protocol

DNS tunnelling

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

DNS protocol

DGAs

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`

DNS protocol

DGAs

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
```

SANS EMEA

DFIR PRAGUE 2016

#THANKYOU

HOW TO ROCK WITH DNS

Patterns for Detection and Faster Spotting of Malicious Activities

João Collier de Mendonça
Praha CZ, October 2016.

@sec_joao