



TLP WHITE

DNS-BASED THREAT HUNTING:

learn, share and improve. repeat.

João Collier de Mendonça
Zurich, September 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 :-)



AGENDA

- Problem statement
- DNS and its features
- Patterns: learn, share and improve. repeat.

PROBLEM STATEMENT

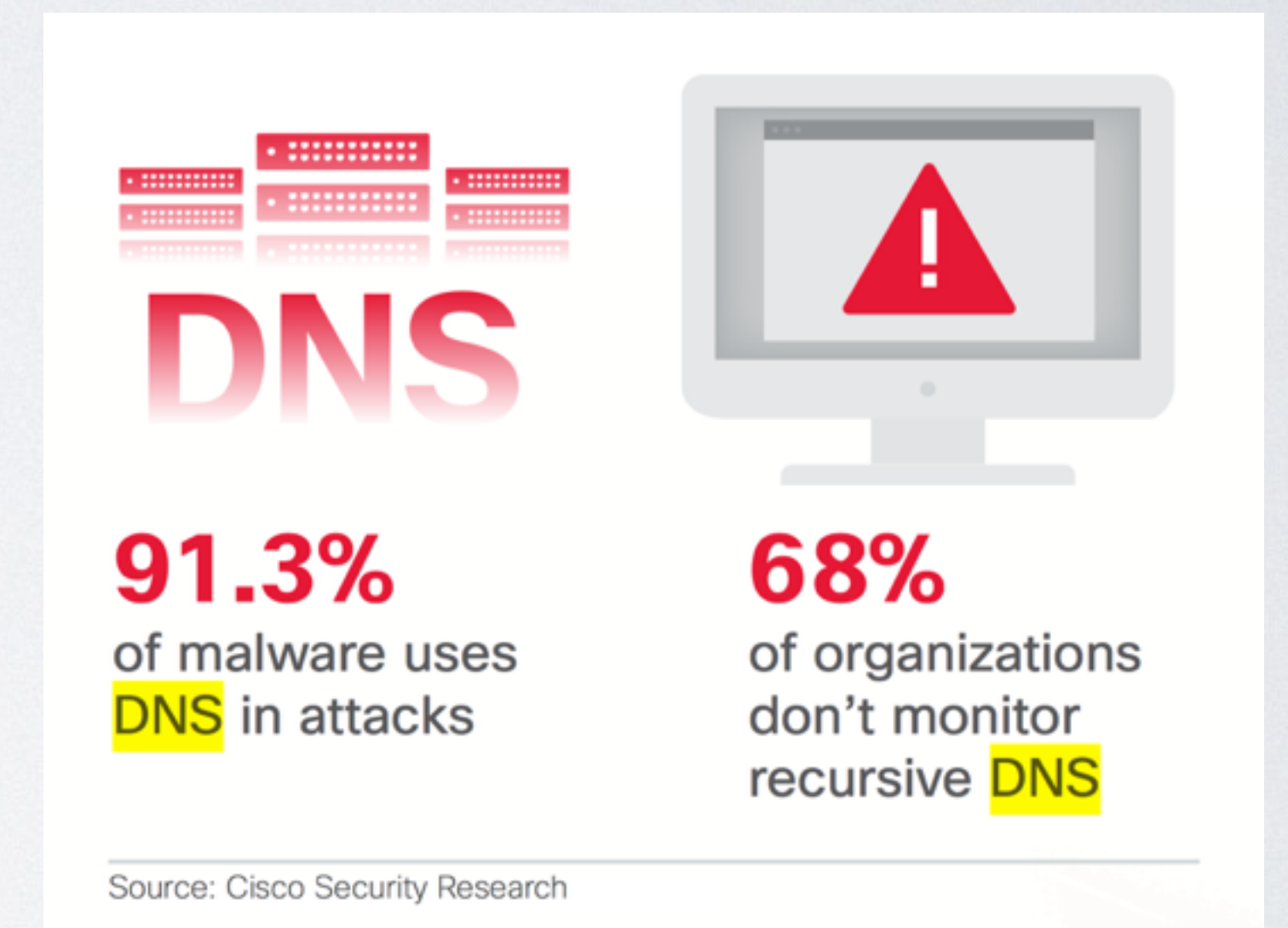
THE “WHAT”

- 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
- **Your blind spot is the attacker's sweet spot**



Source: Cisco 2016 Annual Security Report

MIND OUR SETTINGS

- Incident Response
- Environment for which there is no traffic baseline
- How can I leverage DNS data for detection?

DNS AND ITS FEATURES

DNS AND ITS FEATURES

METADATA

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

PATTERNS

a solid starting point

PATTERN I

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!=0'
```

- 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
```

SHARE A LEARNING

while using FQDN Length

FQDN LENGTH: LEARNING


kinkasayolmhvmw2ribnf2u24lrjuavaqkzcvua27amab4wyukrifiqspij.eqwinlrjqafq
abnaqqq2xcabveckykybacak5lqkecdamj4cvavsydvfuqbs.
7by.counterbalancegenusonychomys.com.

oiltycoonparotid.in
lymantriacypresdoctrine.biz
counterbalancegenusonychomys.com



FQDN LENGTH: LEARNING

- Don't chase your tail
(like I did)

- secretmedia.com: 
ad-blocker bypassing
service

```
$ dig
kinkasayolmhvmw2ribnf2u24lrjuavaqkzcvua27amab4wyukrifiqs
piij.eqwinlrjqafqabnaqqq2xcabveckykybacak5lqkecdamj4cvav
sydvfuqbs.7by.counterbalancegenusonychomys.com.
;; Truncated, retrying in TCP mode.
[snip]
;; ANSWER SECTION:
kinkas...counterbalancegenusonychomys.com. 1000 IN CNAME
front11.secretmedia.com.
front11.secretmedia.com. 3600 IN A 185.42.119.171
front11.secretmedia.com. 3600 IN A 185.42.119.107
front11.secretmedia.com. 3600 IN A 185.42.119.41
front11.secretmedia.com. 3600 IN A 185.42.119.139
```



THANK YOU FOR YOUR TIME

and for ideas during the hop-on, hop-off

João Collier de Mendonça
Zurich, September 2016.

 @sec_joao



DNS-BASED THREAT HUNTING:

learn, share and improve. repeat.

João Collier de Mendonça
Zurich, September 2016.

 @sec_joao

HOP-ON HOP-OFF

- Initial Idea was to provide patterns for detection
- Feedback to the initial ideas very was nice, thank you!
- Hopefully, you will add this patterns to your toolbox!

HOP-ON HOP-OFF

- Further patterns collected during hop-on hop-off
 - Endpoints querying for CNAME and NS record types
 - Inspect Entropy of FQDNs together with length
 - For entropy calculation, quick'n'dirty™, just drop the dots (.) and the calculation over the entire FQDN



THANK YOU FOR YOUR TIME

and for ideas during the hop-on, hop-off

João Collier de Mendonça
Zurich, September 2016.

 @sec_joao