Simple analysis using pDNS

Irena Damsky

Damsky.tech

@DamskyIrena

Hack.lu 2018 | October 17th 2018 | Luxembourg

AGENDA

- DNS
  - Quick reminder –DNS
  - How does it work
  - Record types
- pDNS
  - What is it
  - What can you do with it
  - Where can you get it
- Queries
  - Get IP for domain
  - Get Subdomains
  - Discover TLDs
- Research
  - Analysis of malicious name servers
  - Finding Phishing

PART I

Quick reminder - DNS

QUICK REMINDER - DNS

- Domain Name System (not Domain Name Server)
- First RFC (882, 883) published in November 1983 by Paul Mockapetris
- Port 53 traffic

EXAMPLE OF DNS RESOLUTION ROUTE

```
dig +trace 2018.hack.lu
```

DNS RECORD TYPES

Type	Description	Simply put
A	Address mapping	IPv4
AAAA	Address mapping	IPv6
CNAME	Canonical name record	Redirect / alias
NS	Authoritative Name Server	
MX	Mail exchanger	
PTR	Reverse lookup pointer	
TXT	Text	Arbitrary non-formatted text
RRSIG	DNSSEC Signature	

https://en.wikipedia.org/wiki/List_of_DNS_record_types

PART II

pDNS – Passive DNS

What is pDNS?

- Invented in 2004 by Florian Weimer
- Historical DB of DNS resolutions
- Collected using multiple sensors on the internet.
  - Passively collected – only real world traffic is monitored
    - Only Cache misses are collected
  - Another option – scraping zone files
- Data changes based on the DB!

What can you do with pDNS?

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?

Where can you get pDNS?

FARSIGHT SECURITY	RISKIQ	Netlab 360.com
CIRCL Passive DNS	BFK	VirusTotal Inside VirusTotal's back pocket
SPAMHAUS	mnemonic	

Where can you get pDNS?

- VT - http://blog.virustotal.com/2013/04/virustotal-passive-dns-replication.html
- CIRCL - https://www.circl.lu/services/passive-dns/
- PASSIVETOTAL - https://www.riskiq.com/products/passivetotal/
- FSI - DNSDB - https://www.dnsdb.info/
- 360 – https://passivedns.cn/login/?next=%2F
- MNEMONIC - https://passivedns.mnemonic.no/search
- BFK - http://www.bfk.de/bfk_dnslogger.html
- SPAMHAUS - https://www.spamhaustech.com/protecting-networks/threat-intelligence-data/passive-dns/

PART III

Simple stuff

GET IP FOR DOMAIN

Current

```
dig hack.li
dig +short hack.lu
```

GET (HISTORICAL) IP FOR DOMAIN

Current

```
dig hack.lu
dig +short hack.lu
```

Historical

- `./dnsdb-query rrset hack.lu`

GET SUBDOMAINS

- Current
  - Brute force?

- Passive DNS

```
./dnsdb-query rrset *.hack.lu  |
      grep -v ";;" |
      cut -f 1 -d" " |
      sort |
      uniq
```

FIND NEW TLDS

- ```
  ./dnsdb-query rrset hack.*/A  |
      "IN A" |
      cut -f 1 -d" " |
      sort |
      uniq
  ```

- Adds a filter to get only “A” records
  ```

PART IV

let's do some research

FIND PHISHING

- What are we looking for?
  - bankofamerica ?
  - “appleid” ?
- Going to take a lot of time
  - Phishing has a short life span → Limit on time → --after -1w / -1d
- Limitations:
  - Only right/left hand joker is allowed
- Do some analysis and filtering
  - Highly subdomained stuff – awk -F"." 'NF>=4’
  - Suspicious words - grep “\.com\.”
  - Check for suspicious tlds – grep “\.xyz”
  - And more

FIND MALICIOUS NAME SERVERS

- Get the name servers associated with the domain:

- ./dnsdb-query rrset <malicious-domain> | grep NS | cut -f 4 –d" " | sort |uniq

- Find what else is on that nameserver:
- ./dnsdb-query rdata name <name-server>
- You can joker (remove the subdomain) and filter this using “/NS”

(RE)SOURCES

- How the DNS works by Verisgn - https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml
- Full list of DNS Record Types - https://en.wikipedia.org/wiki/List_of_DNS_record_types
- Merike Kaeo presentation - http://meetings.apnic.net/__data/assets/pdf_file/0017/45521/05-Merike-Kaeo-Passive-DNS.pdf
- What is pDNS - https://help.passivetotal.org/passive_dns.html
- Ben April's great blog post on hunting malware using pDNS - https://www.farsightsecurity.com/2017/10/18/bapril-threathuntingtips/
- Dnsdb-query on github - https://github.com/dnsdb/dnsdb-query

QUESTIONS?

irena@damsky.tech

@DamskyIrena