Leveraging Passive DNS for Incident Response

Daniel Schwalbe
Deputy CISO & VP/Eng
About the Presenter

Daniel Schwalbe

Daniel Schwalbe is Deputy Chief Information Security Officer and Vice President of Engineering for Farsight Security, Inc.

He is a veteran information security professional with 20 years of experience leading incident response and digital forensics efforts in large enterprise settings. Prior to joining Farsight, he served as Associate Chief Information Security Officer at the University of Washington, where his focus areas were threat intelligence, information sharing, and incident response.

He is an active contributor and speaker in the information security community, and previously served on the board of directors for the REN-ISAC.
Remember Phone Books?
CASEY Robt L 32 Scott Cir Ded. 326-2370
Robt & Lauren 8 Otis Av Ded. 326-0635
Robt W 71 Herbert Rd Bra. 848-5137
Rose 617 Broad Wey. 331-6948
Ruth B 208 Atlnc Av Hul. 925-2525
Sean 141 Carroll Av Wswd. 329-9412
Stacie 30 Chapman Wey. 331-3652
Stephen & Katherine
590 Middle Wey. 340-6658
Stephen R 17 Draper Can. 828-1108
ification 17 Binnacle Ln Qui. 479-4923
Thos 65 Dickens Qui. 328-6078
Thos A Jr 194 School Wswd. 326-2474
Thos R 1 Wentworth Rd Can. 828-6969
Timothy P 30 French Qui. 326-1140
Timothy P 637 Pleasant Mil. 328-4662
Tom & Judy 63 Hollis Av Qui. 328-0734
V 9 Fore River Av Wey. 749-5746
Walter J Jr 17 Autumn Cir Hin. 331-5746
William C 212 Central Av Humrck. 749-5746
Ben & Bill 11 King Wswd. 331-5746
Benjamin B 11 Klaas Wswd. 331-5746
Arthur A 36 Bayley Wswd. 749-5746
James D 36 Bayley Wswd. 749-5746

4
DNS

Powers Everything

(...and everything in DNS is “public”)

Copyright © 2021 Farsight Security, Inc. Not for distribution or publication.
Historical Passive DNS – Critical for Incident Response

• Regular DNS is all about \textit{what's defined NOW}, not what was true last week, last month, or at the time when an incident may have occurred

• Passive DNS bridges that gap and provides \textit{historical information}, including changes over time, which are invaluable during Incident Response & Breach Investigations.

• The ability to go back in time and look at the DNS as it existed \textbf{before}, \textbf{during}, and \textbf{after} an incident is \textbf{critical} to a successful Incident Response, Investigation, and Remediation.
DNS – How does it work again?

I want to visit farsightsecurity.com

Your computer

Recursive DNS Server

farsightsecurity.com

Root Name Server

TLD Name Server

Authoritative Name Server
The DNS is optimized to turn names into IP addresses

$ dig farsightsecurity.com

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> farsightsecurity.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42297
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
farsightsecurity.com. IN A

;; ANSWER SECTION:
farsightsecurity.com. 3395 IN A 104.244.14.13
The DNS is optimized to turn names into IP addresses

$ dig farsightsecurity.com

;; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> farsightsecurity.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42297
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;farsightsecurity.com.          IN      A

;; ANSWER SECTION:
farsightsecurity.com. 3395 IN A 104.244.14.13
Sometimes, IP addresses can be turned into names using the DNS...

$ dig -x 104.244.14.13

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> -x 104.244.14.13
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35844
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;13.14.244.104.in-addr.arpa. IN  PTR

;; ANSWER SECTION:
13.14.244.104.in-addr.arpa. 85596 IN  PTR siel.iad1.fsi.io.
Sometimes, IP addresses can be turned into names using the DNS...

```bash
$ dig -x 104.244.14.13

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> -x 104.244.14.13
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35844
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: 0, udp: 4096
;; QUESTION SECTION:
;13.14.244.104.in-addr.arpa.  IN  PTR

;; ANSWER SECTION:
13.14.244.104.in-addr.arpa. 85596 IN   PTR sie1.iad1.fsi.io.
```
...but not always (and forward and reverse don’t have to match)

```
$ dig sie1.iad1.fsi.io

;; <<<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<<>> sie1.iad1.fsi.io
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23046
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sie1.iad1.fsi.io. IN A

;; AUTHORITY SECTION:
fsi.io. 2502 IN SOA fsi.io. hostmaster.fsi.io
```
...but not always (and forward and reverse don’t have to match)

$ dig sie1.iad1.fsi.io

;; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> sie1.iad1.fsi.io
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23046
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sie1.iad1.fsi.io.              IN      A

;; AUTHORITY SECTION:
fsi.io.                 2502    IN      SOA fsi.io. hostmaster.fsi.io
“Regular” DNS has its limitations

• Regular DNS assumes authoritative DNS has been **properly configured**

• Regular DNS can return **deceptive answers** one moment, and go back to legitimate answers the next

• Answers to regular DNS queries **may vary depending on your location**
Passive DNS is all about making connections

• Passive DNS is all about collecting real DNS data and saving it in a highly optimized format

• This allows efficient searching of the data to discover those otherwise often overlooked relationships

• Passive DNS is all about objective connections between domains and IPs, and name servers and domains.

• Passive DNS is not about “goodness” or “badness”, it does not attach a value statement to the data that gets collected
Passive DNS

I want to visit farsightsecurity.com

Your computer

Recursive DNS Server

Cache miss

farsightsecurity.com

DNSDB

Root Name Server

TLD Name Server

Authoritative Name Server
Passive DNS: Answer the questions that regular DNS never could

- Regular DNS is great at answering the questions it was meant to answer, most commonly, "What IP is www.example.com on?"

- Regular DNS cannot, and isn't intended to, answer questions like:
  - When was www.example.com first used on the Internet? Between then and now, what IP addresses have been used by www.example.com?
  - It looks like www.example.com has resolved to 192.0.2.59. What are all the OTHER domain names that also resolve to IP address 192.0.2.59? (or maybe what are all the domains that live in a CIDR prefix, such as 192.0.2.0/24?)
  - Can you please tell me virtually ALL the domains that use ns1.example.com as a name server?
Basic Passive DNS search strategy

• **If you've got IP addresses**, look for domain names associated with those IPs

• **If you've got domain names**, look for IP addresses associated with those domain names

• **If you've got name server FQDNs**, look for domain names known to use those name servers

**Note:** Key point – don’t stop after just one query!
Passive DNS Synthesizes Implicit Relationships

• If passive DNS sees www.example.com ➔ 192.0.2.59, passive DNS will also impute the reverse relationship (192.0.2.59 ➔ www.example.com). We will do this even if that inverse relationship is NOT explicitly defined.

• Regular DNS knows the name servers that a given domain uses. However, regular DNS cannot tell you all the OTHER domains that ALSO use those same name servers. Passive DNS can.

• Passive DNS tracks not just what it sees, but WHEN it sees it. This means that we can ask for only records from a particular time period, excluding ("fencing off") all other time periods. It also means that we can watch a domain as it hops from one IP address to another over time.
We'll be Using DNSDB Scout for Today’s Hands-On part

DNSDB Scout is best known as a browser extension for Chrome, Brave, Edge, and Firefox, which are available through their respective web stores.

DNSDB Scout also exists as a standalone webpage, accessible from popular browsers. This eliminates the need for you to install a browser extension, if your environment restricts changes to the browser.

DNSDB Scout Web Edition can be accessed at

https://scout.dnsdb.info

You can also use our command line client, dnsdbq, which is available on GitHub at https://github.com/dnsdb/dnsdbq
TIME TO GET HANDS-ON
Questions?

Daniel Schwalbe
dfs@fsi.io