Avalon and DNSDB™ to expose the Emotet Malware
INTRODUCTION

▪ DANIEL SCHWALBE, DIRECTOR OF ENGINEERING & DEPUTY CISO AT FARSIGHT SECURITY

▪ AARON GEE-CLOUGH, CTO, KING & UNION
AGENDA

- DNS AND SENSOR OVERVIEW
- INTRODUCTION TO PIVOTING WITH PASSIVE DNS
- AVALON THREAT ANALYTICS PLATFORM OVERVIEW
- INVESTIGATION AND COLLABORATION ON AVALON
- EMOTET BACKGROUND AND DEMO
- Q&A
UNDERSTANDING DNS
DNS AS A MAP

- Most everything we do on the Internet...
  - B2C Web, B2B Web, E-mail, I-M, ...
    relies on TCP/IP, and begins with a DNS lookup

- Mobile Internet is dominated by search...
  - ...but search itself relies extensively upon DNS
    DNS has a rigorous internal structure

- Things that are in fact related, are related in DNS
  - You can NOT have whois privacy or email privacy
  - but there is no DNS privacy – DNS is the basis of truth
We observe and record DNS resolutions worldwide as they happen and store all associated record types, i.e. MX, NS…
DNS RECURSION / PASSIVE DNS

- DNS Servers
- Root Servers
- Registry Servers
- Farsight Security
- Recursive Server
- Cache
- www.example.com
- 93.184.216.34
- Devices & Users
DNS DATA WORLDWIDE - OUR SENSOR ARRAY

GLOBAL COVERAGE

DIVERSE SOURCES
- Consumer
- Government
- Education
- Enterprise
- ISPs & Mobile
- Social media

REAL-TIME & HISTORIC
- 200k+ DNS records / sec
- 5+ TB / Day
- 100+ Billion DNS Resolutions
TWO WAYS TO EMPOWER SECURITY OPERATIONS

I. SECURITY INFORMATION EXCHANGE

• Proactively detect and block
• Empower your Firewall & Mail Servers
• 200,000+ observations/second
• Compliant with leading protocols for easy ingestion

II. DNS INTELLIGENCE DATABASE – DNSDB

• World’s largest historic database of DNS resolution and all records
• Empower your SIEM and Threat Platform
• Started 2007, rebuilt in 2010, updated in real-time, 100+ Billion resolutions recorded
• API and On-Prem Solution
PIVOTING:

UNDERSTANDING PIVOTING
WITH
PASSIVE DNS
PIVOTING: GUILT BY ASSOCIATION – PASSIVE DNS

KNOWN BAD HOSTNAME OR IP ADDRESS

- WHAT OTHER HOST NAMES AT THE SAME ADDRESS AT THE SAME TIME?

- WHAT OTHER INFRASTRUCTURE IS HOSTED IN THE SURROUNDING NETWORK BLOCK?

KNOWN BAD DOMAIN

- WHAT OTHER HOSTS ARE IN THE DOMAIN?

- WHAT OTHER DOMAINS ARE SERVED BY THE SAME NAMESERVER?
PIVOTING: GUILT BY ASSOCIATION – PASSIVE DNS

SIMILAR NAMING PATTERNS
- FAST-FLUX BOTNET INFRASTRUCTURE
- UNCOMMON NAMES USED IN MANY DOMAINS
- DOMAIN GENERATION ALGORITHMS

SIMILAR LOOKING ANSWERS
- SOA RECORDS?
- TXT RECORDS?
- SPF RECORDS?
PIVOTING PASSIVE DNS: REDUCING FALSE POSITIVES

INDICATOR FOR A HOSTNAME OR IP ADDRESS

- KNOWN REVERSE PROXY SERVICE?
- KNOWN SINKHOLE?
- HOSTING SERVICE?
- DOMAIN PARKING SERVICE?
- DYNAMIC DNS SERVICE?
- WIDELY USED CDN INFRASTRUCTURE?
WHERE TO USE FARSIGHT DNS INTELLIGENCE

- Threat Platforms
- Firewalls
- Mail Servers
- Orchestration / Automation
- Bulk Queries
- Machine Learning
- SIEMs
KEY USE CASES

- Indicator of Compromise correlation
- Historical resolution lookups
- Time-based analysis
- Fully qualified domain name lookups
- SIEM event enrichment
- Domain or IP enrichment to proactively hunt for threats
INTRODUCTION

KING & UNION
Companies can no longer approach cyber security alone...
INDUSTRY OBSERVATIONS

- Insufficient Collaboration Amongst Security Analysts
- Missing Context Around Cyber Security Threats
- Manual Workflows
- Inability to Manage Overwhelming Threat Intelligence Data
Eva Galperin – Dir of Cybersecurity at EFF
@ Shmoocon - Intelligence work happens in teams, not solo.

Dave Aitel – CTO at IMMUNITY Incorporated
on Twitter - …there is only one generational divide: Collaborative workers, who can use Google Docs, and individual workers, who use Microsoft Office and email, and are about a thousand times less productive

Our tools right now are "collaborative" in the same way email is: it’s technically sharing, but it’s just not the same.

We should be moving to the Google Docs model of collaboration.
Workflows in Threat Intel are very manual:

- Search Google, whois, data providers, etc, one by one.
- Make a big spreadsheet or notepad file.
- Iterate.
- Profit?

We work with computers, we should be able to automate this.

(Having an expensive & busy analyst type "whois" on the command line 100 times is not a good use of their time.)
The output from TI work is often a text report (or a non-machine-parsable PDF).

Difficult to take results & consume them in IDS/SIEM.

The results of an investigation should be automatically consumable by a SIEM/IDS/etc.

(Reports are nice, but it makes no sense to have a SOC analyst re-typing IOCs out of a report.)
WHAT AVALON PROVIDES

- Threat Analysis Platform to Foster Collaboration
- Automate Manual Analyst Workflow Processes
- Custom Dynamic Graphing & Threat Visualization
- Import/Export Data to Platform & Analysis
1050 connected nodes. This is a great start. Saved me hours of manual work in seconds.

Aaron 9/25/17 at 11:32 AM
That cluster on the right looks interesting.

Comcast_user 9/25/17 at 11:32 AM
The 192.64.119.254 IP? Yeah. Looks like it belongs to Namecheap.

Webhoster?

Aaron 9/25/17 at 11:33 AM
Possibly. Am more interested in the 5.56.133.87 IP in the bottom left.

Aaron 9/25/17 at 11:33 AM
'k. Let's add that enrichment, see where it goes.

Comcast_user 9/25/17 at 11:34 AM
That added all kinds of interesting stuff.

Say something..
Let’s look at how an analysis would work in an automated, collaborative environment.

Emotet Background:
- Banking trojan that’s been around for a while now.
- Changing C2 & downloader URLs often.
- Groups tracking the new C2 & downloader URLs, posting those to Pastebin, etc.

Let’s build on one of those reports, with 3 twists:
- use Avalon to automate lookups,
- use DNSDB’s info,
- Work with more than one person at once.
Avalon Demo - Taunting the Demo Gods
Avalon returns security operators/analysts to their true purpose: identifying and neutralizing potential threats together.
CONCLUSION

▪ Passive DNS (both forward and reverse) is a hugely powerful tool in identifying relationships between infrastructure on the internet.
▪ Realtime collaboration is essential for modern investigations.
▪ Visual/graphical representation of data is invaluable in understanding the relationships in your data.
▪ Automation is key to making analysts as efficient as possible.
HOW TO GET YOUR DNSDB™ TRIAL API KEY

1. Farsightsecurity.com

2. Get Started
3. Free DNSDB Trial API

**Free DNSDB™ Trial API**

Get your free DNSDB™ API Key and use it in any of your preferred platform(s)

100 Queries / day

30-days free

**GET YOUR API KEY**
HOW TO GET YOUR DNSDB™ TRIAL API KEY

4. Fill out registration form

5. Receive email with your API Key
ADD DNSDB™ to Avalon

1. Log into Avalon
2. Go to your profile
3. Go to the license management page
4. Click to add a license
**ADD DNSDB™ to Avalon**

### Step 6: Select Farsight as the service

In the service selection column, choose Farsight.

### Step 7: Paste key in "API Key" field

After selecting Farsight, input the API key in the designated field labeled as "API Key."
THANK YOU FOR YOUR ATTENTION

Questions?

King & Union
Contact: info@kingandunion.com
Avalon Free Trial: https://www.kingandunion.com/early-adoption-request.html

Farsight Security
Contact: info@farsightsecurity.com
DNSDB™ Free Trial: https://www.farsightsecurity.com/trial-api/