Expanding The Hunt: Pivoting Using Passive DNS and Full PCAP
A Case Study

Dr. Paul Vixie, CEO Farsight Security
Gene Stevens, CTO ProtectWise
Agenda

I. Introduction to Passive DNS

II. ProtectWise-Farsight DNSDB Case Study

III. Conclusion
Introduction to Passive DNS
Domain Name System Data Flow

- DNS Cache
- Authority Servers
- Recursive Servers
- Stub Resolvers
- Farsight SIE
- Farsight DNSDB

Flow:
- DNS Cache to Recursive Servers
- Recursive Servers to Authority Servers
- Authority Servers to Farsight SIE
- Farsight SIE to Farsight DNSDB
- Farsight DNSDB to DNS Cache
Owner Lookup, Show History

$ dnsdb_query -r vix.com/ns/vix.com
...
;; record times: 2010-07-04 16:14:12 .. 2013-05-12 00:55:59
vix.com. NS ns1.isc-sns.net.

;; record times: 2013-10-18 06:30:10 .. 2014-02-28 18:13:10
Owner Wildcards, Left Hand

$ dnsdb_query -r \*.vix.com/a | fgrep 24.104.150
internal.cat.lah1.vix.com.   A 24.104.150.1
ss.vix.com.                 A 24.104.150.2
gutentag.vix.com.           A 24.104.150.3
lah1z.vix.com.               A 24.104.150.4
mm.vix.com.                  A 24.104.150.11
external.cat.lah1.vix.com.   A 24.104.150.33
wireless.cat.lah1.vix.com.   A 24.104.150.65
wireless.ss.vix.com.         A 24.104.150.66
cat.lah1.vix.com.            A 24.104.150.225
vix.com.                     A 24.104.150.231
ns.lah1.vix.com.             A 24.104.150.234
<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>Preference</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vix.su</td>
<td>MX</td>
<td>10</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>dns-ok.us</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>mibh.com</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>iengines.com</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>toomanydatsuns.com</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>farsightsecurity.com</td>
<td>MX</td>
<td>10</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>anog.net</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>mibh.net</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>tisf.net</td>
<td>MX</td>
<td>10</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>iengines.net</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>al.org</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>vixie.org</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>redbarn.org</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
<tr>
<td>benedelman.org</td>
<td>MX</td>
<td>0</td>
<td>ss.vix.su</td>
</tr>
</tbody>
</table>
Data Lookup, by IP Address

$ dnsdb_query -r ic.fbi.gov/mx
ic.fbi.gov. MX 10 mail.ic.fbi.gov.

$ dnsdb_query -r mail.ic.fbi.gov/a
mail.ic.fbi.gov. A 153.31.119.142

$ dnsdb_query -i 153.31.119.142
ic.fbi.gov. A 153.31.119.142
mail.ic.fbi.gov. A 153.31.119.142
mail.ncijtf.fbi.gov. A 153.31.119.142
**Data Lookup, by IP Address Block**

```
$ dnsdb_query -i 153.31.119.0/24 | grep -v infragard

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn.dev2.leo.gov.</td>
<td>153.31.119.70</td>
</tr>
<tr>
<td>mail.leo.gov.</td>
<td>153.31.119.132</td>
</tr>
<tr>
<td><a href="http://www.biometriccoe.gov">www.biometriccoe.gov</a>.</td>
<td>153.31.119.135</td>
</tr>
<tr>
<td><a href="http://www.leo.gov">www.leo.gov</a>.</td>
<td>153.31.119.136</td>
</tr>
<tr>
<td>cgate.leo.gov.</td>
<td>153.31.119.136</td>
</tr>
<tr>
<td><a href="http://www.infraguard.net">www.infraguard.net</a>.</td>
<td>153.31.119.138</td>
</tr>
<tr>
<td>infraguard.org.</td>
<td>153.31.119.138</td>
</tr>
<tr>
<td><a href="http://www.infraguard.org">www.infraguard.org</a>.</td>
<td>153.31.119.138</td>
</tr>
<tr>
<td>mx.leo.gov.</td>
<td>153.31.119.140</td>
</tr>
<tr>
<td>ic.fbi.gov.</td>
<td>153.31.119.142</td>
</tr>
<tr>
<td>mail.ic.fbi.gov.</td>
<td>153.31.119.142</td>
</tr>
<tr>
<td>mail.ncijtf.fbi.gov.</td>
<td>153.31.119.142</td>
</tr>
</tbody>
</table>
```
Technical Formatting Notes

• These slides use the “terminal interface”
  – Actual agents use a web browser interface
• These slides show a DNS output conversion
  – The real output is in JSON format, i.e.:

```bash
$ dnsdb_query -r f.root-servers.net/a/root-servers.net
;; record times: 2010-06-24 03:10:38 .. 2014-03-05 01:22:56
;; count: 715301521; bailiwick: root-servers.net.
f.root-servers.net.  A  192.5.5.241

$ dnsdb_query -r f.root-servers.net/a/root-servers.net -j
{"count": 715301521, "time_first": 1277349038, "rrtype": "A", "rrname": "f.root-servers.net.", "bailiwick": "root-servers.net.", "rdata": ["192.5.5.241"], "time_last": 1393982576}
```
ProtectWise-Farsight DNSDB Case Study
How ProtectWise Works

**NETWORK SENSORS**
- Egress
- Core
- Cloud
- Remote
- Industrial

**OPTIMIZED NETWORK REPLAY**
- Ingest

**SECURITY DVR PLATFORM**
- Visualizer
- Time Machine
- Secure Vault
A Time Machine for Threat Detection

- Behavioral Analysis
- Machine Learning
- Heuristics
- Signatures
- Predictive Analysis

Traditional Real Time Analysis

Network Traffic

Automated Retrospective Analysis

24 hours

1 month

6 months

1 year

Collective Correlation

C1

C2

C3
December 2015:

Alarm fires indicating compromised host is beaconing

Communication to: akamie.com / 121.54.168.216 via a backdoor associated with the Codoso APT group

Forensic analysis of the packets determined the full scope of the command and control activity
DNSDB Query Example

```plaintext
;; bailiwick: akamie.com.
;;      count: 315
;; first seen: 2015-01-02 02:21:24 -0000
;; last seen: 2015-03-27 14:30:42 -0000
www.akamie.com. IN A 106.185.34.182

;; bailiwick: akamie.com.
;;      count: 2
;; first seen: 2015-09-17 17:58:43 -0000
;; last seen: 2015-09-17 17:58:43 -0000
www.akamie.com. IN A 121.127.228.77

;; bailiwick: akamie.com.
;;      count: 3
;; first seen: 2016-03-09 04:57:18 -0000
;; last seen: 2016-03-09 04:57:18 -0000
www.akamie.com. IN A 141.8.225.244

;; bailiwick: akamie.com.
;;      count: 16
;; first seen: 2015-08-20 17:41:28 -0000
;; last seen: 2015-11-23 21:23:02 -0000
www.akamie.com. IN A 198.74.125.235

;; bailiwick: akamie.com.
;;      count: 11
;; first seen: 2016-03-17 23:07:53 -0000
;; last seen: 2016-04-10 11:07:56 -0000
www.akamie.com. IN A 204.11.56.48
```
Hunt 1: Customer Specific Search

HuntNetflowCustomer (106.185.34.182, 121.127.228.77, 141.8.225.244, 198.74.125.235, 204.11.56.48)

Historic data revealed successful HTTP connections to 198.74.125.235, 121.127.228.77.

Connections to 198.74.125.235 dated as early as **July 15th, 2015**.

Packet level forensics confirm HTTP connection attempts and successful C2 traffic.

**Fully established timeline of APT activity**
Strong Packet Validation

You can't get this with logs

Deep packet visibility is critical in understanding attacker actions
Hunt 2: Pivot Across Customers

Search all customers for newly identified IP addresses

\[ \text{HuntNetflowCustomersAll (} 106.185.34.182, \\
121.127.228.77, \\
141.8.225.244, \\
198.74.125.235, \\
204.11.56.48 \) \]

Search uncovered latent infrastructure in second customer
Machines Identified & Mitigated

Check domain resolution history for each IP and repeat!
Conclusion

Farsight DNSDB coupled with Retrospective Analysis of raw network traffic can discover the previously unknown, offering deep forensic exploration and providing new intelligence about past activity.
Appendix
Additional Exploit Kit Example

- Angler EK Alarm Fires at Customer A
- Pull full PCAP to examine contents of landing page
- Initial indicator search did not uncover any other hits
- HTTP request referer was suspicious and part of the Exploit Kit's redirection process.
- At the time of investigation the resolution of the referring host did not resolve.
- Netflow hunting for resolution of referrer yielded no results
- Using passive DNS we found the most recent resolution of the referrer in question.
- Retrospecting this new IP yielded that a host at customer B also visited the referrer in question and was redirected to a different Exploit Kit landing page that we were unaware of
- Hosts at both customers were identified and remediated