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

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

Agenda

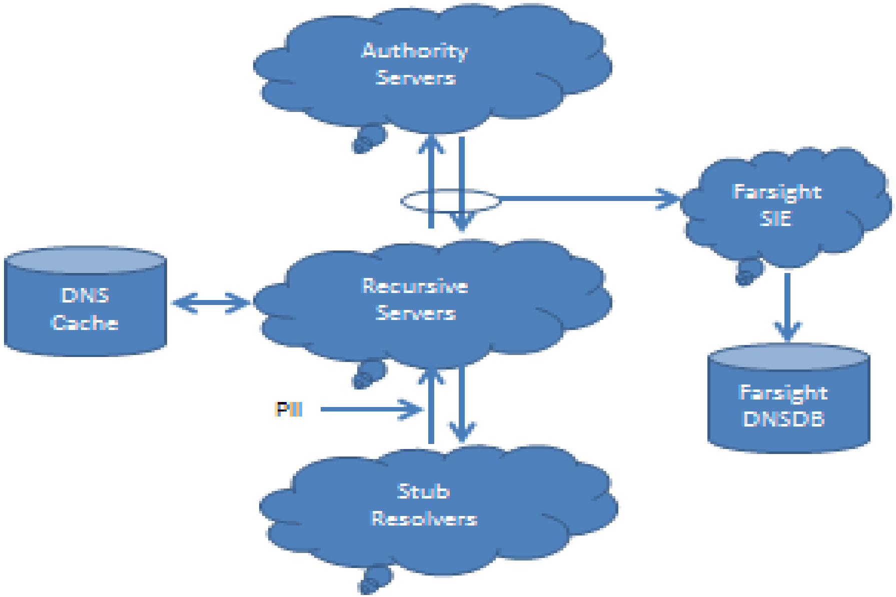
I. Introduction to Passive DNS

II. ProtectWise-Farsight DNSDB Case Study

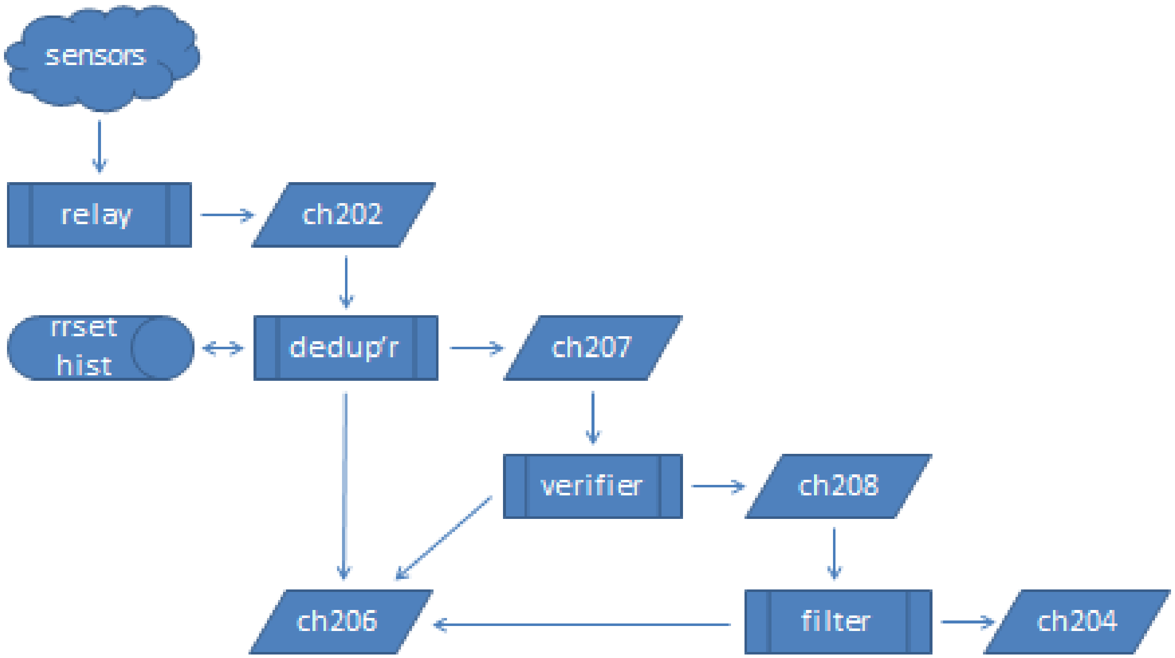
III. Conclusion

Introduction to Passive DNS

Domain Name System Data Flow



SIE pDNS Streaming



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
;; count: 2221563; bailiwick: vix.com.
vix.com.  NS  ns.sql1.vix.com.
vix.com.  NS  ns1.isc-sns.net.
vix.com.  NS  ns2.isc-sns.com.
vix.com.  NS  ns3.isc-sns.info.

;; record times: 2013-10-18 06:30:10 .. 2014-02-28 18:13:10
;; count: 330; bailiwick: vix.com.
vix.com.  NS  buy.internettraffic.com.
vix.com.  NS  sell.internettraffic.com.
```

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
ww.vix.com.                 A  24.104.150.12
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
ap-kit.lah1.vix.com.        A  24.104.150.67
cat.lah1.vix.com.           A  24.104.150.225
vix.com.                    A  24.104.150.231
deadrat.lah1.vix.com.       A  24.104.150.232
ns-maps.vix.com.            A  24.104.150.232
ns.lah1.vix.com.            A  24.104.150.234
```

Data Lookup, By Name

```
$ ./dnsdb_query -n ss.vix.su/mx
vix.su.                  MX  10 ss.vix.su.
dns-ok.us.               MX   0 ss.vix.su.
mibh.com.                MX   0 ss.vix.su.
iengines.com.            MX   0 ss.vix.su.
toomanydatsuns.com.      MX   0 ss.vix.su.
farsightsecurity.com.    MX  10 ss.vix.su.
anog.net.                MX   0 ss.vix.su.
mibh.net.                MX   0 ss.vix.su.
tisf.net.                MX  10 ss.vix.su.
iengines.net.            MX   0 ss.vix.su.
al.org.                  MX   0 ss.vix.su.
vixie.org.               MX   0 ss.vix.su.
redbarn.org.             MX   0 ss.vix.su.
benedelman.org.          MX   0 ss.vix.su.
```

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
vpn.dev2.leo.gov.           A  153.31.119.70
mail.leo.gov.               A  153.31.119.132
www.biometriccoe.gov.       A  153.31.119.135
www.leo.gov.                A  153.31.119.136
cgate.leo.gov.              A  153.31.119.136
www.infraguard.net.         A  153.31.119.138
infraguard.org.             A  153.31.119.138
www.infraguard.org.         A  153.31.119.138
mx.leo.gov.                 A  153.31.119.140
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
```

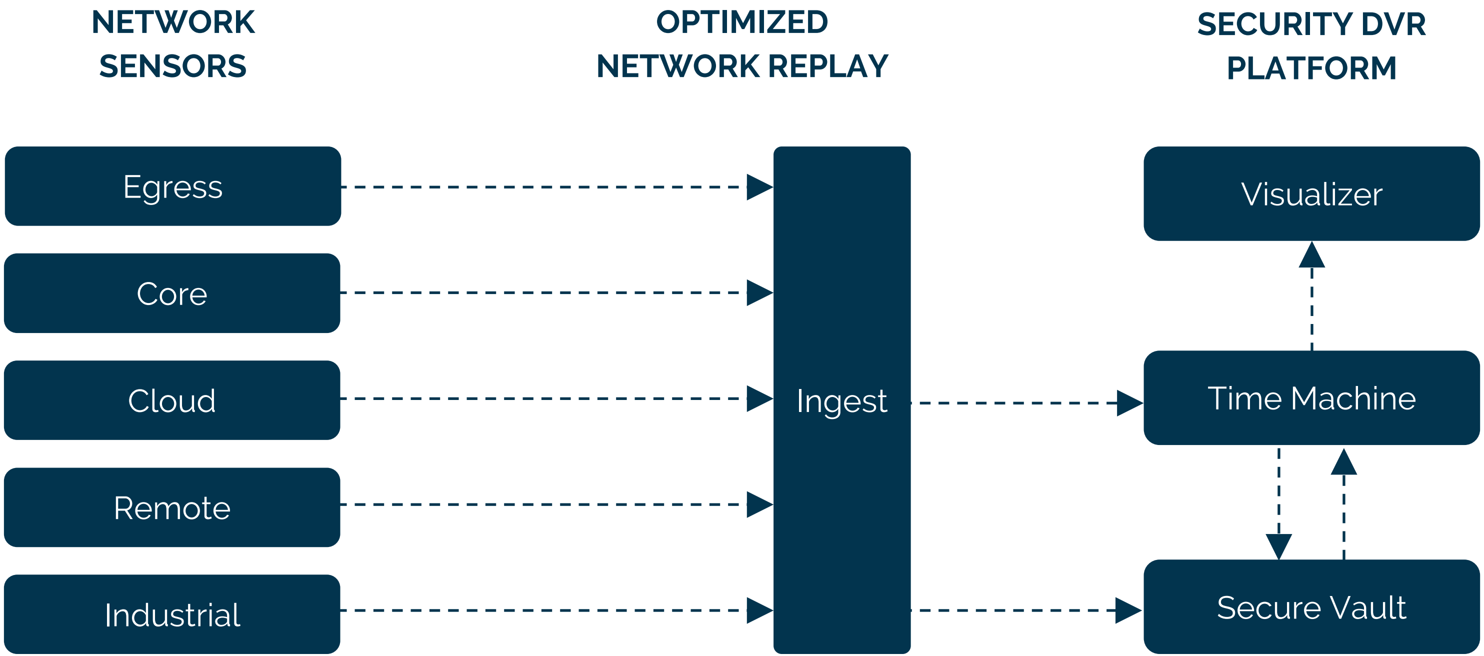
Technical Formatting Notes

- 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.:

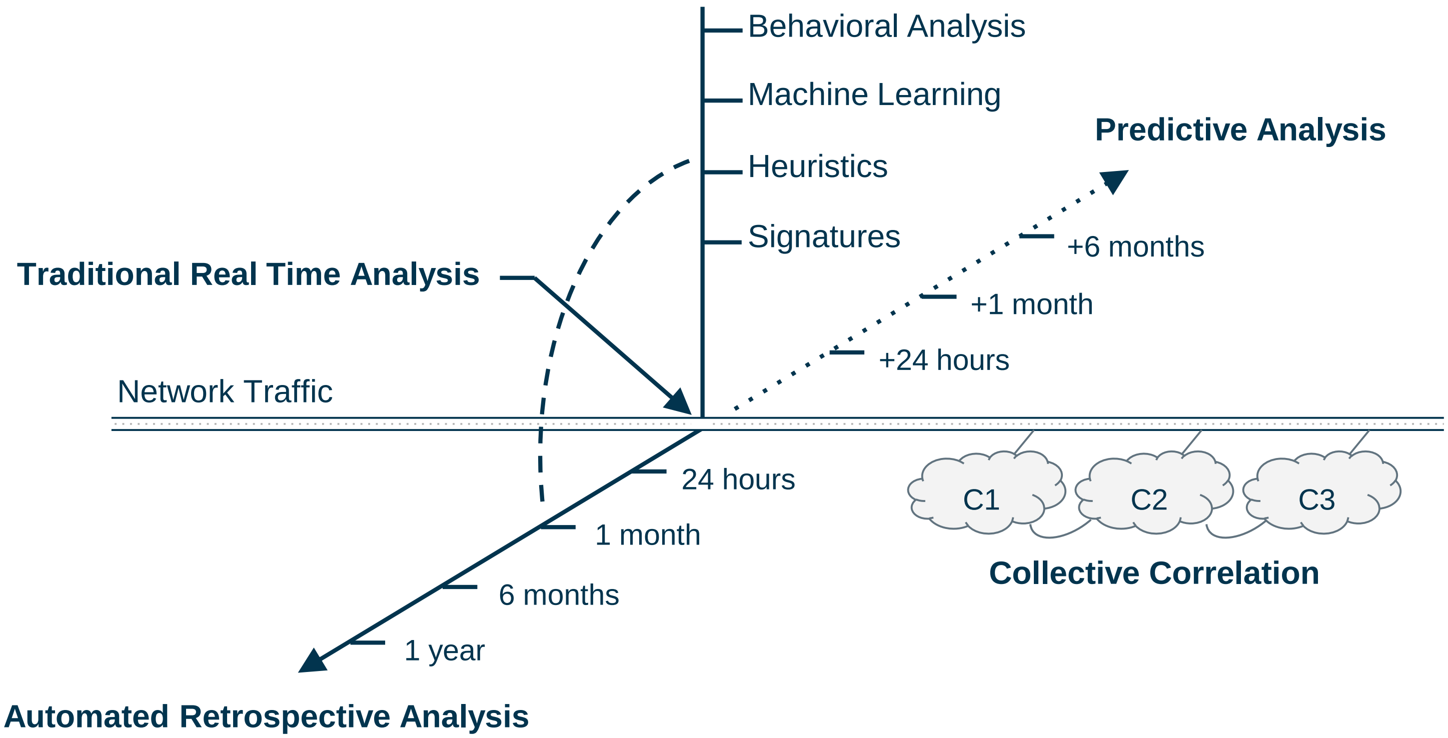
```
$ dnsdb_query -r f.root-servers.net/a/root-servers.net
;; record times: 2010-06-24 03:10:38 .. 2014-03-05 01:22:56
;; count: 715301521; bailiwick: root-servers.net.
f.root-servers.net.  A  192.5.5.241

$ 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



A Time Machine for Threat Detection



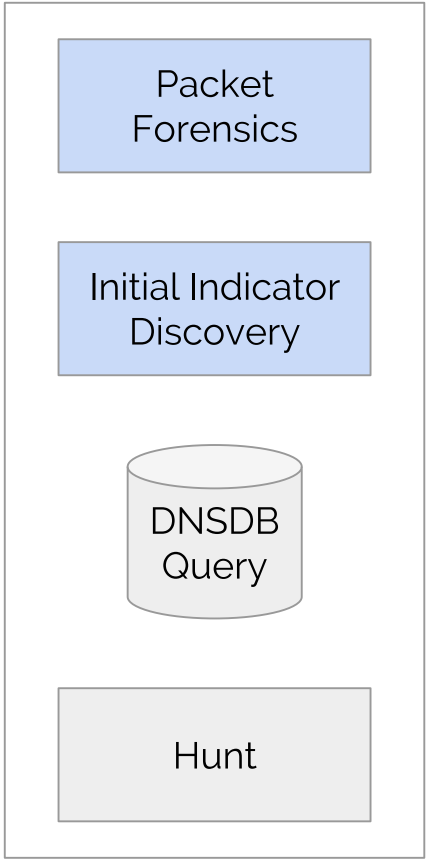
Hunting with DNS

December 2015:

Alarm fires indicating compromised host is beaconing

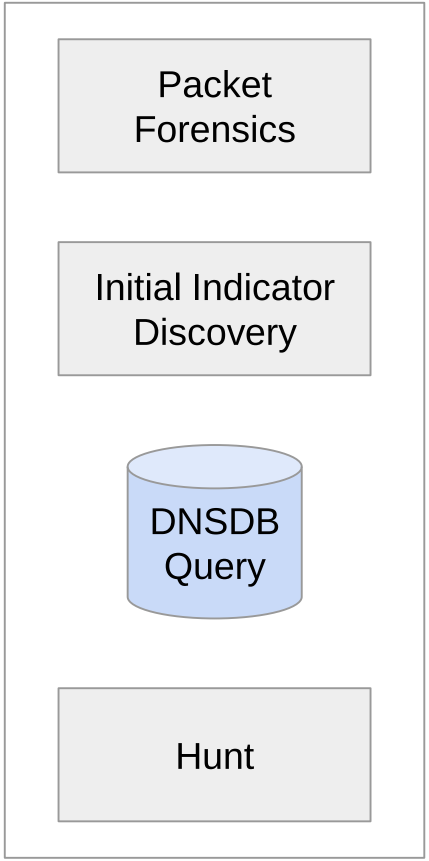
Communication to : akamie.com / 121.54.168.216 via a backdoor associated with the Codoso APT group

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



DNSDB Query Example

```
 ;;  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
```



Packet Forensics

Initial Indicator Discovery

DNSDB Query

Hunt

Hunt 1: Customer Specific Search

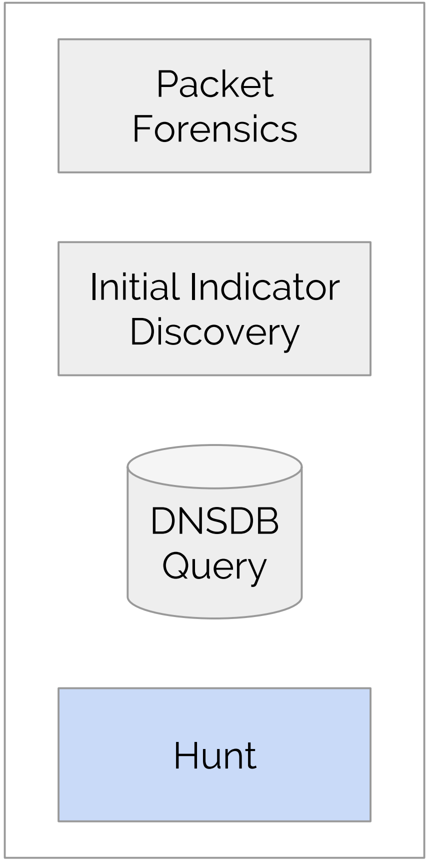
```
HuntNetflowCustomer   ( 106.185.34.182,
                        121.127.228.77,
                        141.8.225.244,
                        198.74.125.235,
                        204.11.56.48 )
```

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



Packet Forensics

Initial Indicator Discovery

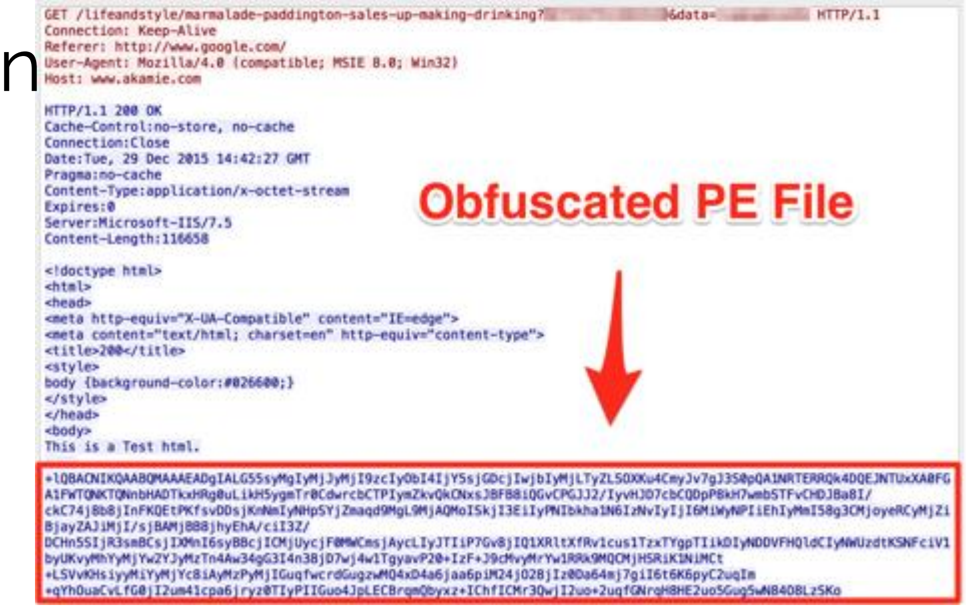
DNSDB Query

Hunt

Strong Packet Validation

You can't get this with logs

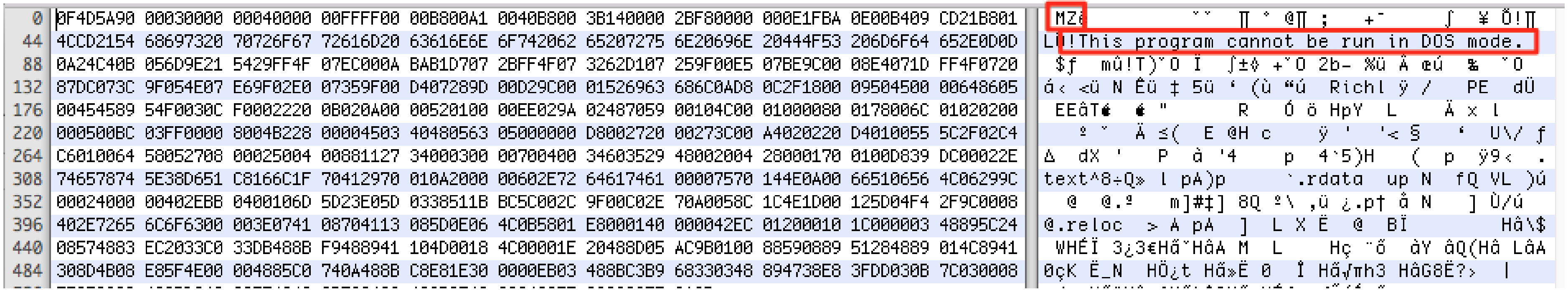
Deep packet visibility is critical in understanding attacker actions



```
GET /lifeandstyle/marmalade-paddington-sales-up-making-drinking?[redacted]&data=[redacted] HTTP/1.1
Connection: Keep-Alive
Referer: http://www.google.com/
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: www.akamie.com

HTTP/1.1 200 OK
Cache-Control:no-store, no-cache
Connection:Close
Date:Tue, 29 Dec 2015 14:42:27 GMT
Pragma:no-cache
Content-Type:application/x-octet-stream
Expires:0
Server:Microsoft-IIS/7.5
Content-Length:116658

<!doctype html>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta content="text/html; charset=en" http-equiv="content-type">
<title>200</title>
<style>
body {background-color:#026600;}
</style>
</head>
<body>
This is a Test html.
```

```
+lQBACNIKQAABQMAAAEADgIALG55syMgIyMjJyMjI9zcIyObI4IjY5sjGDcjIwjbIyMjLTyZL5OXKu4CmyJv7gJ3S0pQA1NRTERRQk4DQEJNTUxXA0FG
A1FWTQNKTQNnbHADTkxHRg0uLikH5ygmTr0CdwrcbCTPIymZkvQkCNxsJBFB8iQGvCPGJJ2/IyvHJD7cbCQDpP8kH7wmb5TFvCHDJBa8I/
ckC74j8b8jInFKQEtPKfsvDDsjKnNmIyNHp5YjZmaqd9MgL9MjAQMoISkjI3EiIyPNIbkha1N6IzNvIyIjI6MiWyNPIiEhIyMmI58g3CMjoyeRCyMjZi
BjayZAJiMjI/sjBAMjB8BjhyEhA/ciI3Z/
DCHn5SIjR3smBCsjIXMnI6syBBcjICMjUycjF0MWCmsjAycLIyJTIiP7Gv8jIQ1XRltXfRv1cus1TzxTYgpTIikDIyNDDVFHQldCIyNWUzdtKSNFciV1
byUKvyMhYyMjYw2YJyMzTn4Aw34gG3I4n3BjD7wj4w1TgyavP20+IzF+J9cMvyMrYw1RRk9MQCMjH5RiK1NiMCt
+LSVvKHsiyyMiYyMjYc8iAyMzPyMjIGuqfwcrdGugzwMQ4xD4a6jaa6piM24jO28jIz0Da64mj7giI6t6K6pyC2uqIm
+qYhOuaCvLfG0jI2um41cpa6jryz0TIyPIIGuo4JpLECBrqmQbyxz+IChfICMr3QwjI2uo+2uqfGNrqH8HE2uo5Gug5wN84OBLz5Ko
```

Obfuscated PE File



```
  0 0F4D5A90 00030000 00040000 00FFFF00 00B800A1 0040B800 3B140000 2BF80000 000E1FBA 0E00B409 CD21B801   MZê          ˇˇ   ∏ ˚ @∏ ;   +¯       ∫  ¥ Õ!∏
 44 4CCD2154 68697320 70726F67 72616D20 63616E6E 6F742062 65207275 6E20696E 20444F53 206D6F64 652E0D0D  LÕ!This program cannot be run in DOS mode.
 88 0A24C40B 056D9E21 5429FF4F 07EC000A BAB1D707 2BFF4F07 3262D107 259F00E5 07BE9C00 08E4071D FF4F0720   $ƒ  mû!T)ˇO Ï  ∫±◊ +ˇO 2b– %ü Â œú  ‰ ˇO
132 87DC073C 9F054E07 E69F02E0 07359F00 D407289D 00D29C00 01526963 686C0AD8 0C2F1800 09504500 00648605  á‹ <ü N Êü ‡ 5ü ‘ (ù “ú  Richl ÿ /   PE  dÜ
176 00454589 54F0030C F0002220 0B020A00 00520100 00EE029A 02487059 00104C00 01000080 0178006C 01020200   EEâT   "        R   Ó ö HpY  L    Ä x l
220 000500BC 03FF0000 8004B228 00004503 40480563 05000000 D8002720 00273C00 A4020220 D4010055 5C2F02C4     º ˇ   Ä ≤(  E @H c    ÿ '   '< §   ‘  U\/ ƒ
264 C6010064 58052708 00025004 00881127 34000300 00700400 34603529 48002004 28000170 0100D839 DC00022E  ∆  dX '   P  à '4    p  4`5)H   (  p  ÿ9‹  .
308 74657874 5E38D651 C8166C1F 70412970 010A2000 00602E72 64617461 00007570 144E0A00 66510656 4C06299C  text^8÷Q» l pA)p      `.rdata  up N  fQ VL )ú
352 00024000 00402EBB 0400106D 5D23E05D 0338511B BC5C002C 9F00C02E 70A0058C 1C4E1D00 125D04F4 2F9C0008    @  @.º    m]#‡] 8Q º\ ,ü ¿.p† å N  ] Ù/ú
396 402E7265 6C6F6300 003E0741 08704113 085D0E06 4C0B5801 E8000140 000042EC 01200010 1C000003 48895C24  @.reloc  > A pA  ] L X Ë  @  BÏ          Hâ\$
440 08574883 EC2033C0 33DB488B F9488941 104D0018 4C00001E 20488D05 AC9B0100 88590889 51284889 014C8941   WHÉÏ 3¿3€Hãˇ HâA M  L    Hç ¨ő  àY âQ(Hâ LâA
484 308D4B08 E85F4E00 004885C0 740A488B C8E81E30 0000EB03 488BC3B9 68330348 894738E8 3FDD030B 7C030008  0çK Ë_N  HÖ¿t Hã»Ë 0  Î Hã√πh3 HâG8Ë?›  |
```

Hunt 2: Pivot Across Customers

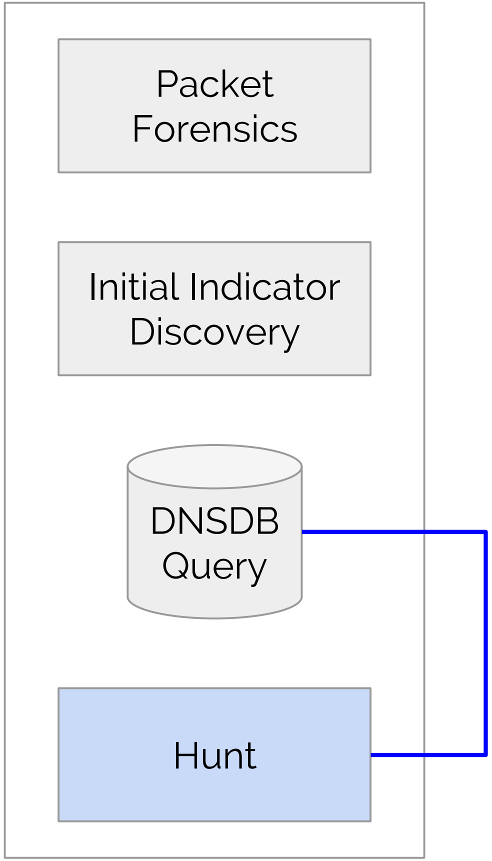
Search all customers for newly identified IP addresses

```
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.

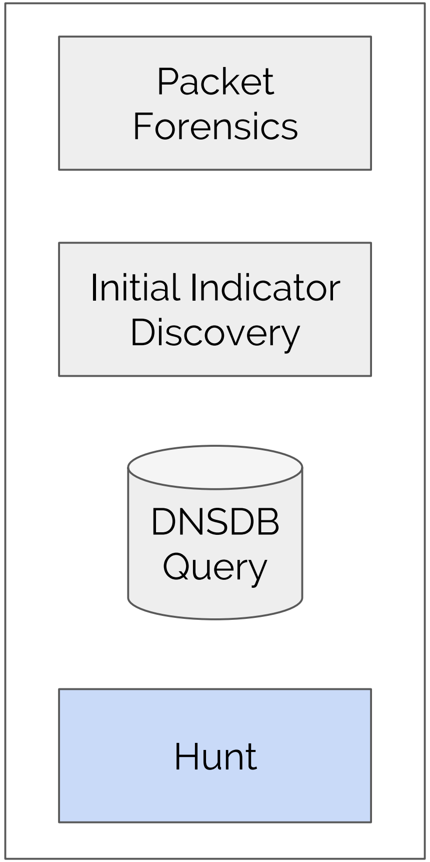
PROTECTWISE

FARSIGHT
SECURITY

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**


Packet Forensics
Initial Indicator Discovery
DNSDB Query
Hunt