27th ANNUAL

FIRST CONFERENCE BERLIN

14-19 JUNE 2015

UNIFIED SECURITY: IMPROVING THE FUTURE

Fact Tables: A Case Study in Reducing Reactive Time-to-Know by 95%

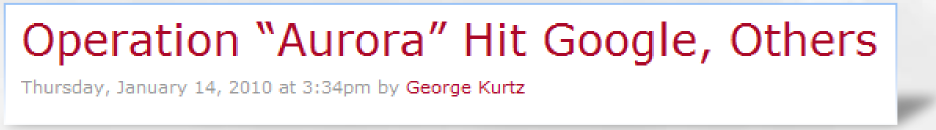
Jeff Boerio, Sr. Advanced Intrusion Analyst, Intel Corp.

Victor Colvard, Security Systems Engineer, Intel Corp.

Today’s Talk

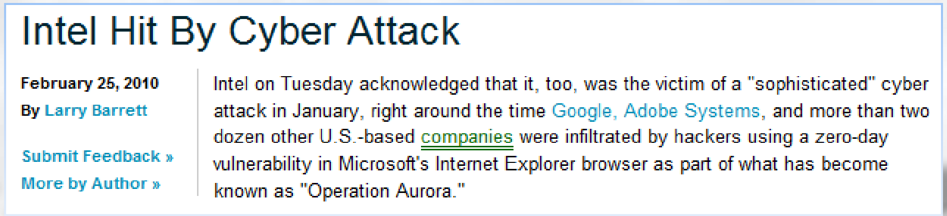
- Our wake-up call
- What we had in terms of “SBI”
- Where we are today
- What is this “Order-1” or “Fact Table” concept
- How it fits in our workflow
- Other use cases

Where it Started – Operation Aurora



Operation “Aurora” Hit Google, Others

Thursday, January 14, 2010 at 3:34pm by George Kurtz



Intel Hit By Cyber Attack

February 25, 2010
By Larry Barrett

Submit Feedback »
More by Author »

Intel on Tuesday acknowledged that it, too, was the victim of a "sophisticated" cyber attack in January, right around the time Google, Adobe Systems, and more than two dozen other U.S.-based companies were infiltrated by hackers using a zero-day vulnerability in Microsoft's Internet Explorer browser as part of what has become known as "Operation Aurora."

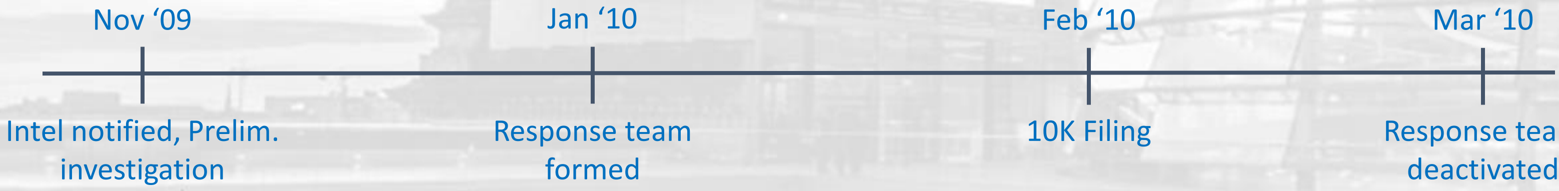
Highly resourced, coordinated attack campaign affecting dozens of US-based companies in the technology, finance, media, & chemical sectors

What Went Well

- Intel ahead of most peers in response
- Required expertise largely existed in-house

What Didn’t

- People, Process, Tool issues
  - New team unknown to some data owners
  - Accessibility/Availability of data
  - Geo challenges
  - No real time monitoring
- Challenges to sustaining response
  - Day jobs didn’t go away
  - If another APT event had occurred …



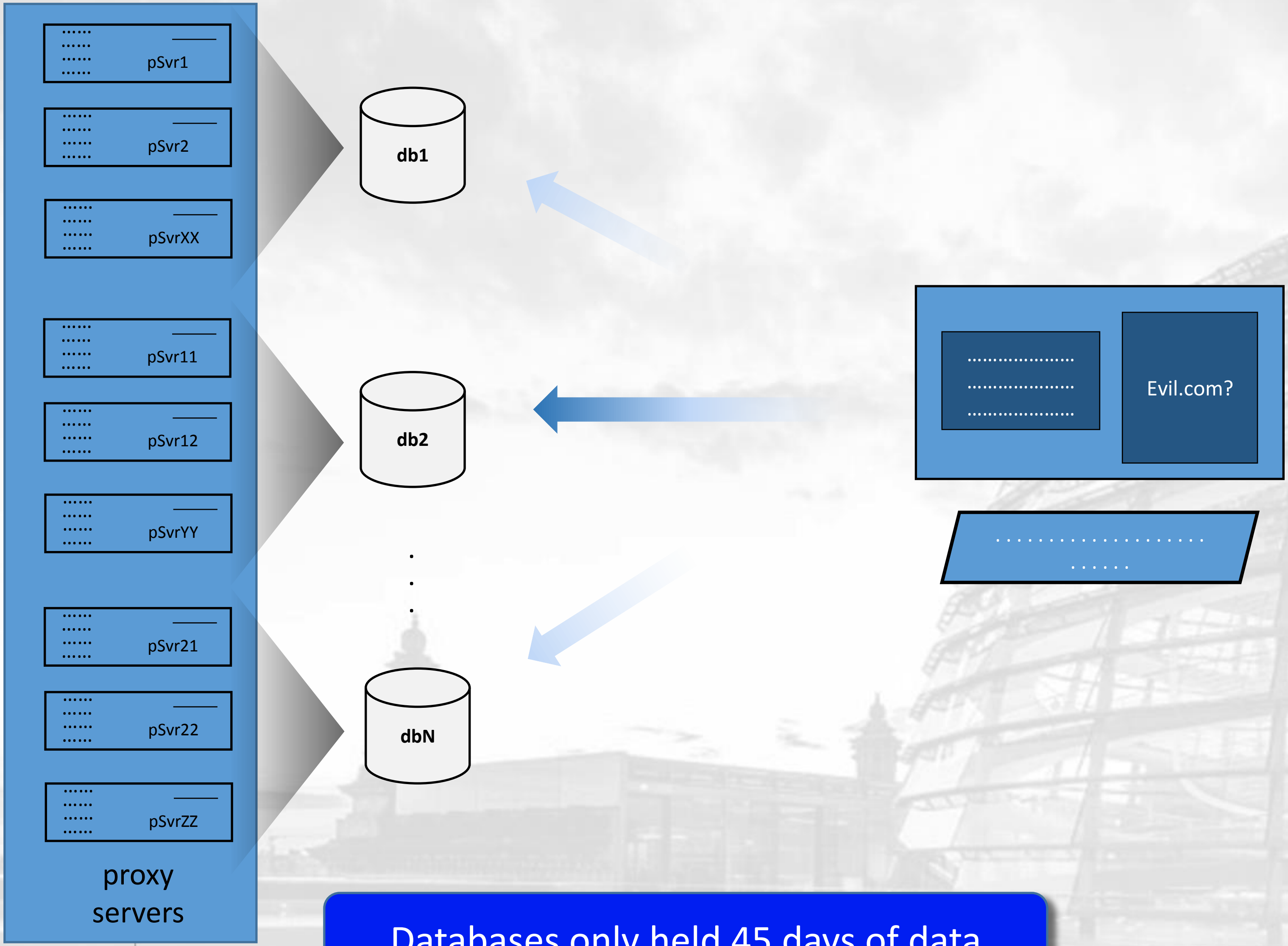
Nov ‘09
Intel notified, Prelim. investigation

Jan ‘10
Response team formed

Feb ‘10
10K Filing

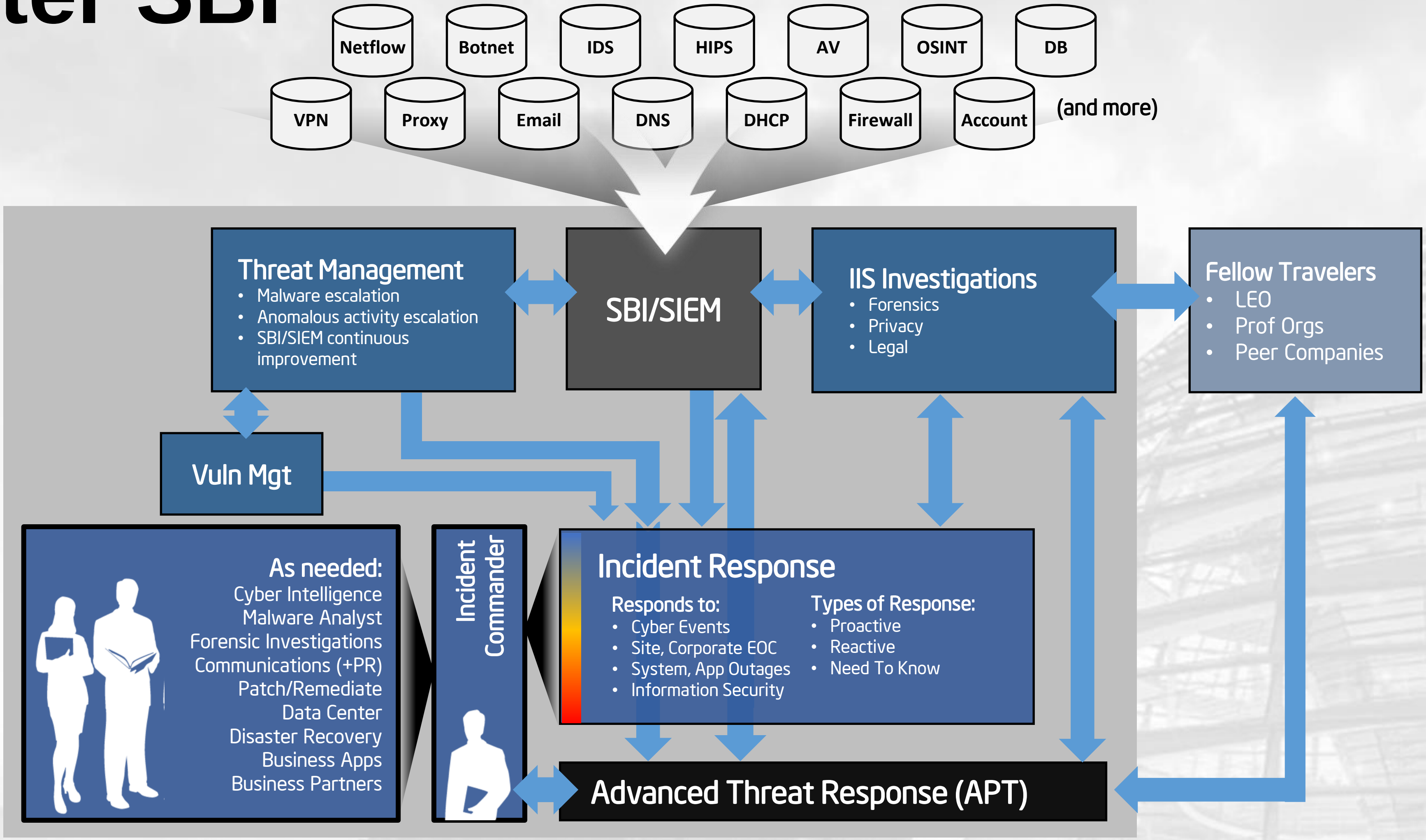
Mar ‘10
Response team deactivated

Pain



Databases only held 45 days of data

Enter SBI



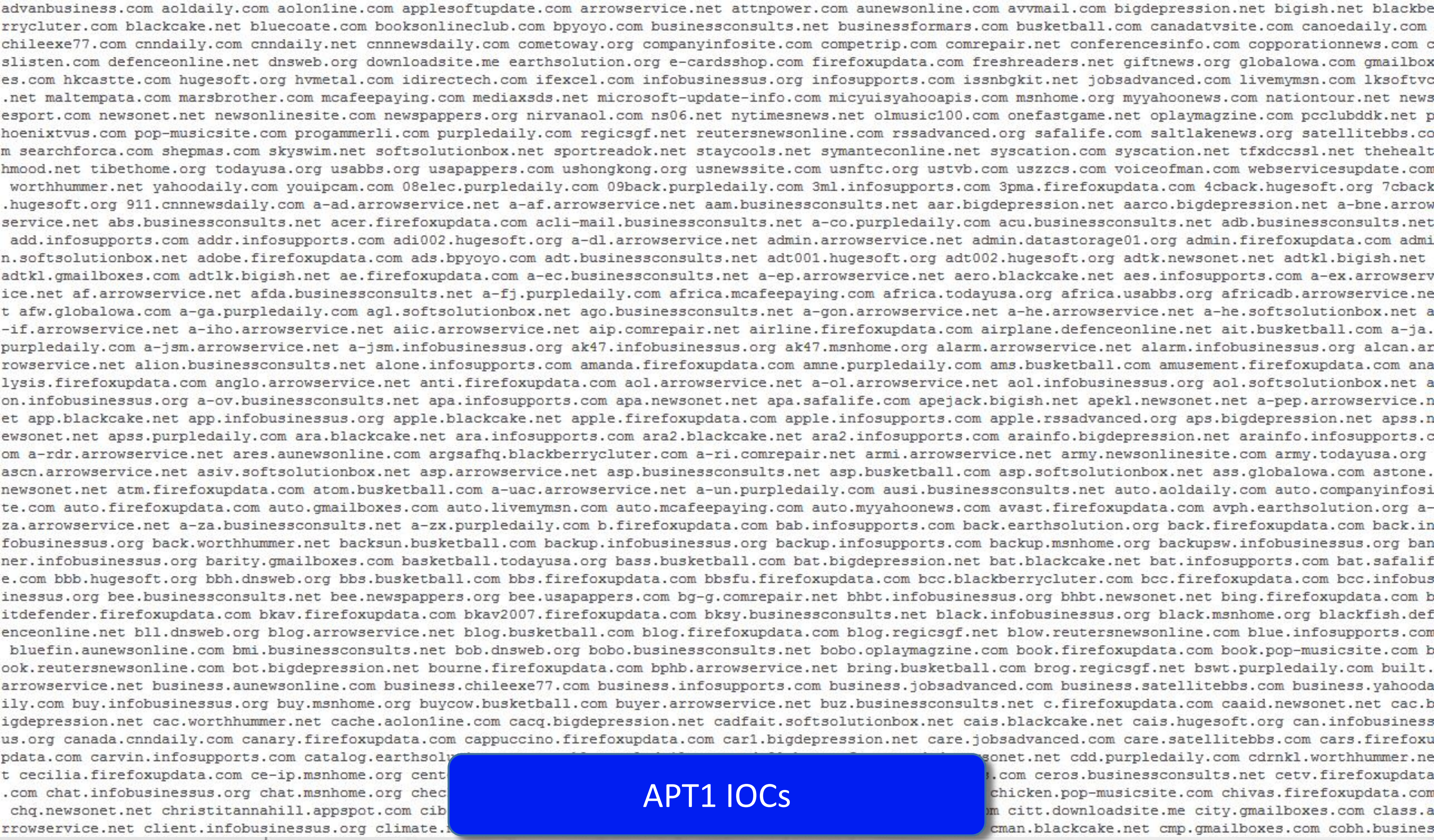
1yr data for all event sources – but there's a LOT of data

Order(1) Proxy Searches

IOC – Have You Seen It?

evil.com

IOCs – Have You Seen These?



```
advanbusiness.com aoldaily.com aolon1ine.com applesoftupdate.com arrowservice.net attnpower.com aunewsonline.com avvmail.com bigdepression.net bigish.net blackbe
rrycluter.com blackcake.net bluecoate.com booksonlineclub.com bpyoyo.com businessconsults.net businessformars.com busketball.com canadatvsite.com canoedaily.com
chileexe77.com cnndaily.com cnndaily.net cnnnewsdaily.com cometoway.org companyinfosite.com competrip.com comrepair.net conferencesinfo.com copporationnews.com c
slisten.com defenceonline.net dnsweb.org downloadsite.me earthsolution.org e-cardsshop.com firefoxupdata.com freshreaders.net giftnews.org globalowa.com gmailbox
es.com hkcastte.com hugesoft.org hvmetal.com idirectech.com ifexcel.com infobusinessus.org infosupports.com issnbgkit.net jobsadvanced.com livemymsn.com lksoftvc
.net maltempata.com marsbrother.com mcafeepaying.com mediaxsds.net microsoft-update-info.com micyuisyahooapis.com msnhome.org myyahoonews.com nationtour.net news
esport.com newsonet.net newsonlinesite.com newspappers.org nirvanaol.com ns06.net nytimesnews.net olmusic100.com onefastgame.net oplaymagzine.com pcclubddk.net p
hoenixtvus.com pop-musicsite.com progammerli.com purpledaily.com regicsgf.net reutersnewsonline.com rssadvanced.org safalife.com saltlakenews.org satellitebbs.co
m searchforca.com shepmas.com skyswim.net softsolutionbox.net sportreadok.net staycools.net symanteconline.net syscation.com syscation.net tfxdccssl.net thehealt
hmood.net tibethome.org todayusa.org usabbs.org usapappers.com ushongkong.org usnewssite.com usnftc.org ustvb.com uszzcs.com voiceofman.com webservicesupdate.com
 worthhummer.net yahoodaily.com youipcam.com 08elec.purpledaily.com 09back.purpledaily.com 3ml.infosupports.com 3pma.firefoxupdata.com 4cback.hugesoft.org 7cback
.hugesoft.org 911.cnnnewsdaily.com a-ad.arrowservice.net a-af.arrowservice.net aam.businessconsults.net aar.bigdepression.net aarco.bigdepression.net a-bne.arrow
service.net abs.businessconsults.net acer.firefoxupdata.com acli-mail.businessconsults.net a-co.purpledaily.com acu.businessconsults.net adb.businessconsults.net
 add.infosupports.com addr.infosupports.com adi002.hugesoft.org a-dl.arrowservice.net admin.arrowservice.net admin.datastorage01.org admin.firefoxupdata.com admi
n.softsolutionbox.net adobe.firefoxupdata.com ads.bpyoyo.com adt.businessconsults.net adt001.hugesoft.org adt002.hugesoft.org adtk.newsonet.net adtkl.bigish.net
adtkl.gmailboxes.com adtlk.bigish.net ae.firefoxupdata.com a-ec.businessconsults.net a-ep.arrowservice.net aero.blackcake.net aes.infosupports.com a-ex.arrowserv
ice.net af.arrowservice.net afda.businessconsults.net a-fj.purpledaily.com africa.mcafeepaying.com africa.todayusa.org africa.usabbs.org africadb.arrowservice.ne
t afw.globalowa.com a-ga.purpledaily.com agl.softsolutionbox.net ago.businessconsults.net a-gon.arrowservice.net a-he.arrowservice.net a-he.softsolutionbox.net a
-if.arrowservice.net a-iho.arrowservice.net aiic.arrowservice.net aip.comrepair.net airline.firefoxupdata.com airplane.defenceonline.net ait.busketball.com a-ja.
purpledaily.com a-jsm.arrowservice.net a-jsm.infobusinessus.org ak47.infobusinessus.org ak47.msnhome.org alarm.arrowservice.net alarm.infobusinessus.org alcan.ar
rowservice.net alion.businessconsults.net alone.infosupports.com amanda.firefoxupdata.com amne.purpledaily.com ams.busketball.com amusement.firefoxupdata.com ana
lysis.firefoxupdata.com anglo.arrowservice.net anti.firefoxupdata.com aol.arrowservice.net a-ol.arrowservice.net aol.infobusinessus.org aol.softsolutionbox.net a
on.infobusinessus.org a-ov.businessconsults.net apa.infosupports.com apa.newsonet.net apa.safalife.com apejack.bigish.net apekl.newsonet.net a-pep.arrowservice.n
et app.blackcake.net app.infobusinessus.org apple.blackcake.net apple.firefoxupdata.com apple.infosupports.com apple.rssadvanced.org aps.bigdepression.net apss.n
ewsonet.net apss.purpledaily.com ara.blackcake.net ara.infosupports.com ara2.blackcake.net ara2.infosupports.com arainfo.bigdepression.net arainfo.infosupports.c
om a-rdr.arrowservice.net ares.aunewsonline.com argsafhq.blackberrycluter.com a-ri.comrepair.net armi.arrowservice.net army.newsonlinesite.com army.todayusa.org
ascn.arrowservice.net asiv.softsolutionbox.net asp.arrowservice.net asp.businessconsults.net asp.busketball.com asp.softsolutionbox.net ass.globalowa.com astone.
newsonet.net atm.firefoxupdata.com atom.busketball.com a-uac.arrowservice.net a-un.purpledaily.com ausi.businessconsults.net auto.aoldaily.com auto.companyinfosi
te.com auto.firefoxupdata.com auto.gmailboxes.com auto.livemymsn.com auto.mcafeepaying.com auto.myyahoonews.com avast.firefoxupdata.com avph.earthsolution.org a-
za.arrowservice.net a-za.businessconsults.net a-zx.purpledaily.com b.firefoxupdata.com bab.infosupports.com back.earthsolution.org back.firefoxupdata.com back.in
fobusinessus.org back.worthhummer.net backsun.busketball.com backup.infobusinessus.org backup.infosupports.com backup.msnhome.org backupsw.infobusinessus.org ban
ner.infobusinessus.org barity.gmailboxes.com basketball.todayusa.org bass.busketball.com bat.bigdepression.net bat.blackcake.net bat.infosupports.com bat.safalif
e.com bbb.hugesoft.org bbh.dnsweb.org bbs.busketball.com bbs.firefoxupdata.com bbsfu.firefoxupdata.com bcc.blackberrycluter.com bcc.firefoxupdata.com bcc.infobus
inessus.org bee.businessconsults.net bee.newspappers.org bee.usapappers.com bg-g.comrepair.net bhbt.infobusinessus.org bhbt.newsonet.net bing.firefoxupdata.com b
itdefender.firefoxupdata.com bkav.firefoxupdata.com bkav2007.firefoxupdata.com bksy.businessconsults.net black.infobusinessus.org black.msnhome.org blackfish.def
enceonline.net bll.dnsweb.org blog.arrowservice.net blog.busketball.com blog.firefoxupdata.com blog.regicsgf.net blow.reutersnewsonline.com blue.infosupports.com
 bluefin.aunewsonline.com bmi.businessconsults.net bob.dnsweb.org bobo.businessconsults.net bobo.oplaymagzine.com book.firefoxupdata.com book.pop-musicsite.com b
ook.reutersnewsonline.com bot.bigdepression.net bourne.firefoxupdata.com bphb.arrowservice.net bring.busketball.com brog.regicsgf.net bswt.purpledaily.com built.
arrowservice.net business.aunewsonline.com business.chileexe77.com business.infosupports.com business.jobsadvanced.com business.satellitebbs.com business.yahooda
ily.com buy.infobusinessus.org buy.msnhome.org buycow.busketball.com buyer.arrowservice.net buz.businessconsults.net c.firefoxupdata.com caaid.newsonet.net cac.b
igdepression.net cac.worthhummer.net cache.aolon1ine.com cacq.bigdepression.net cadfait.softsolutionbox.net cais.blackcake.net cais.hugesoft.org can.infobusiness
us.org canada.cnndaily.com canary.firefoxupdata.com cappuccino.firefoxupdata.com car1.bigdepression.net care.jobsadvanced.com care.satellitebbs.com cars.firefoxu
pdata.com carvin.infosupports.com catalog.earthsol                              sonet.net cdd.purpledaily.com cdrnkl.worthhummer.ne
t cecilia.firefoxupdata.com ce-ip.msnhome.org cent                              .com ceros.businessconsults.net cetv.firefoxupdata
.com chat.infobusinessus.org chat.msnhome.org chec                              chicken.pop-musicsite.com chivas.firefoxupdata.com
 chq.newsonet.net christitannahill.appspot.com cib                              m citt.downloadsite.me city.gmailboxes.com class.a
rrowservice.net client.infobusinessus.org climate.                              cman.blackcake.net cmp.gmailboxes.com cobh.busines
```

APT1 IOCs

Fact Table

```
PROXYDB
timestamp
client_IP
username
category
method
scheme
host
port
uriPath
uriQuery
user-agent
bytesSent
bytesRcv
response
proxy_IP
...
```

Requirements

- Have we seen attempts to *blah*?
- How many?
- What date range?
- Keep for a long time (2-5 yrs)
- Speed

Fact Table

PROXYDB
timestamp
client_IP
username
category
method
scheme
host
port
uriPath
uriQuery
user-agent
bytesSent
bytesRcv
response
proxy_IP
...

```
select
       host,
       min(timestamp) as “First Seen”,
       max(timestamp) as “Last Seen”,
       count*
from proxyDB
group by 1
```

Host	First Seen	Last Seen	Count
example.com	1970-01-01 09:15:31 UTC	1970-01-01 23:05:31 UTC	84
…			
example.com	1974-01-12 18:32:08 UTC	1974-01-12 18:32:08 UTC	2

Take all the sites we saw on $day and add to O1db

Uses

Have we ever seen traffic to example.com or example2.com?

```
select Destination, min(MIN_TS) as “First Seen”, max(MAX_TS) as “Last Seen”,
sum(Count) from proxy01DB where Destination in “example.com,example2.com” and
MIN_TS=”01-01-1970 00:00:00” and MAX_TS=”12-31-2008 23:59:59” group by 1
```

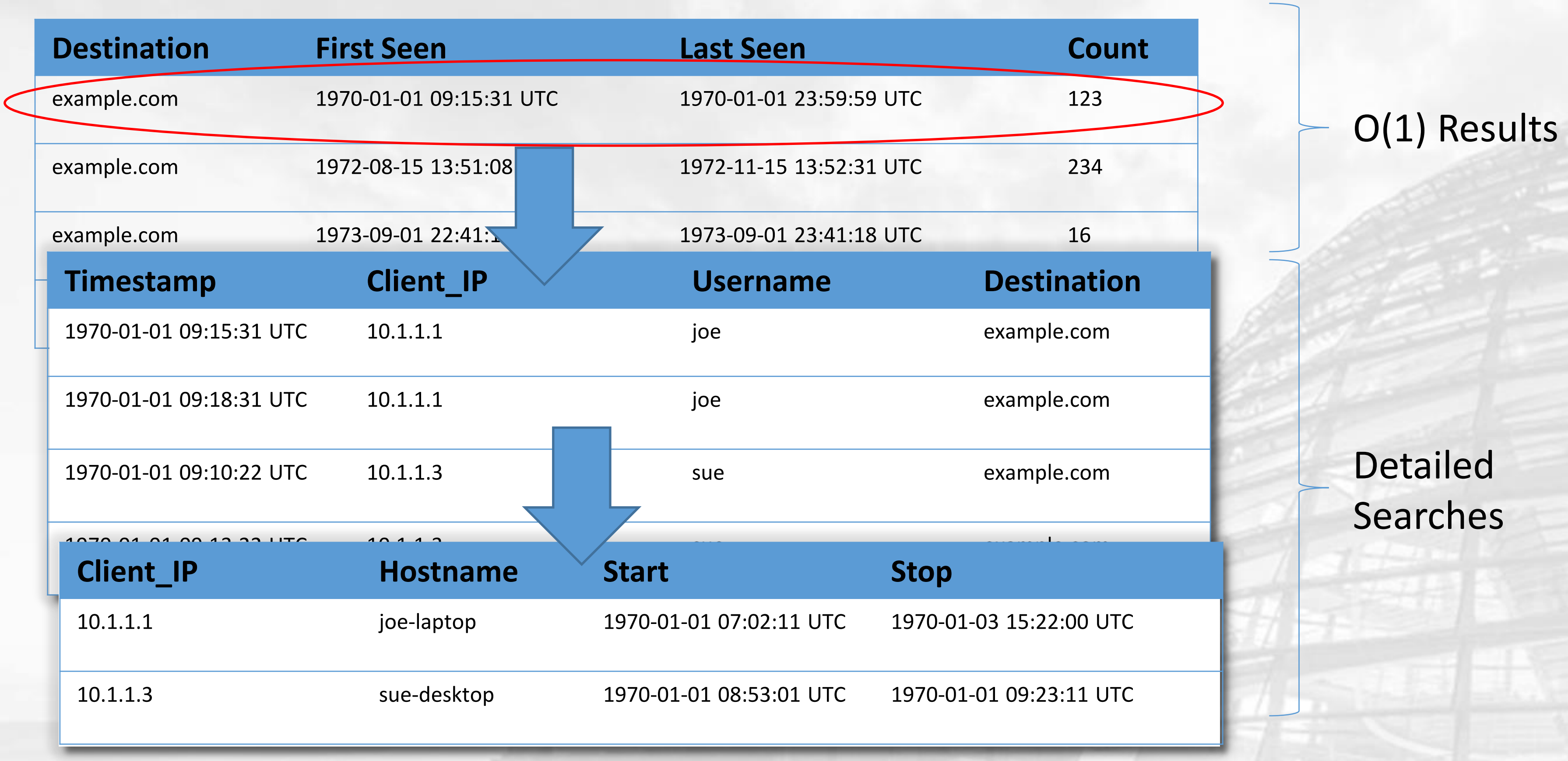
Destination	First Seen	Last Seen	Count
example.com	1970-01-01 09:15:31 UTC	1974-01-12 18:32:08 UTC	854
example2.com	1998-11-21 19:13:01 UTC	2008-12-02 04:12:01 UTC	20

When did we see traffic to example.com?

```
select Destination, min(MIN_TS) as “First Seen”, max(MAX_TS) as “Last Seen”,
sum(Count) from proxy01DB where Destination = “example.com” and MIN_TS=”01-01-
1970 09:15:31” and MAX_TS=”01-12-1974 18:32:08” group by 1
```

Destination	First Seen	Last Seen	Count
example.com	1970-01-01 09:15:31 UTC	1970-01-01 23:59:59 UTC	123
example.com	1972-08-15 13:51:08 UTC	1972-11-15 13:52:31 UTC	234
example.com	1973-09-01 22:41:15 UTC	1973-09-01 23:41:18 UTC	16
example.com	1974-01-12 03:00:01 UTC	1974-01-12 18:32:08 UTC	481

Now We Have Something to Pivot On



Destination	First Seen	Last Seen	Count
example.com	1970-01-01 09:15:31 UTC	1970-01-01 23:59:59 UTC	123
example.com	1972-08-15 13:51:08	1972-11-15 13:52:31 UTC	234
example.com	1973-09-01 22:41:1	1973-09-01 23:41:18 UTC	16

Timestamp	Client_IP	Username	Destination
1970-01-01 09:15:31 UTC	10.1.1.1	joe	example.com
1970-01-01 09:18:31 UTC	10.1.1.1	joe	example.com
1970-01-01 09:10:22 UTC	10.1.1.3	sue	example.com
1970-01-01 09:13:22 UTC	10.1.1.3	sue	example.com

Client_IP	Hostname	Start	Stop
10.1.1.1	joe-laptop	1970-01-01 07:02:11 UTC	1970-01-03 15:22:00 UTC
10.1.1.3	sue-desktop	1970-01-01 08:53:01 UTC	1970-01-01 09:23:11 UTC

O(1) Results

Detailed Searches

What used to take weeks now takes <1 day

DNS Use Case

Requirements essentially the same

- Have we seen attempts to *blah*?
- How many?
- What date range?
- Keep for a long time (2-5 yrs)
- Exclude Intel lookups
- Speed

Our O(1) DNS only stores non-intel.com queries

Improvements, Automation, Additional Work

Proxy/DNS "Firehose"

Current

- Provide IOCs to engine
- Engine queries on O(1) tables

Future

- Automatically open a case
- Engine automatically pulls proxy/DHCP
  - And employee entitlements/access

Do all the work an analyst currently does manually
Generate shareable threat intelligence

DNS Tunnel Detection

- Query O(1) DNS table
- Remove Alexa Top 1 Million
- Count primary domains
- High counts could indicate tunnels

Detected pen testing vendor

Other Use Cases

- User-Agent
  - Many malware uses specific U-A strings
- Observed Malware
  - How many times are you seeing a malware family
- Email
  - Phishing campaigns based on sender, subject, etc
- VPN
  - Identify geo-spatial issues or anomalies

Be mindful of privacy requirements

Acknowledgements

Steve Mancini	Idea development
Victor Colvard	Solution engineering
Stacy Purcell	SBI evangelist

Questions?

Jeff Boerio, Sr. Advanced Intrusion Analyst, Intel Corp.
Email: jeff.boerio@intel.com
Victor Colvard, Security Systems Engineer, Intel Corp.
See Jeff for Contact Details