

Leveraging Passive DNS for Network Defense

Kathy Wang

Splunk, Inc.

kawang@splunk.com

Whoami

- Last DEFCON I spoke at was DEFCON 12!
- Since then, I've had lots of adventures...

This is a Joint Project

- Steve Brant and I worked on this together

Agenda

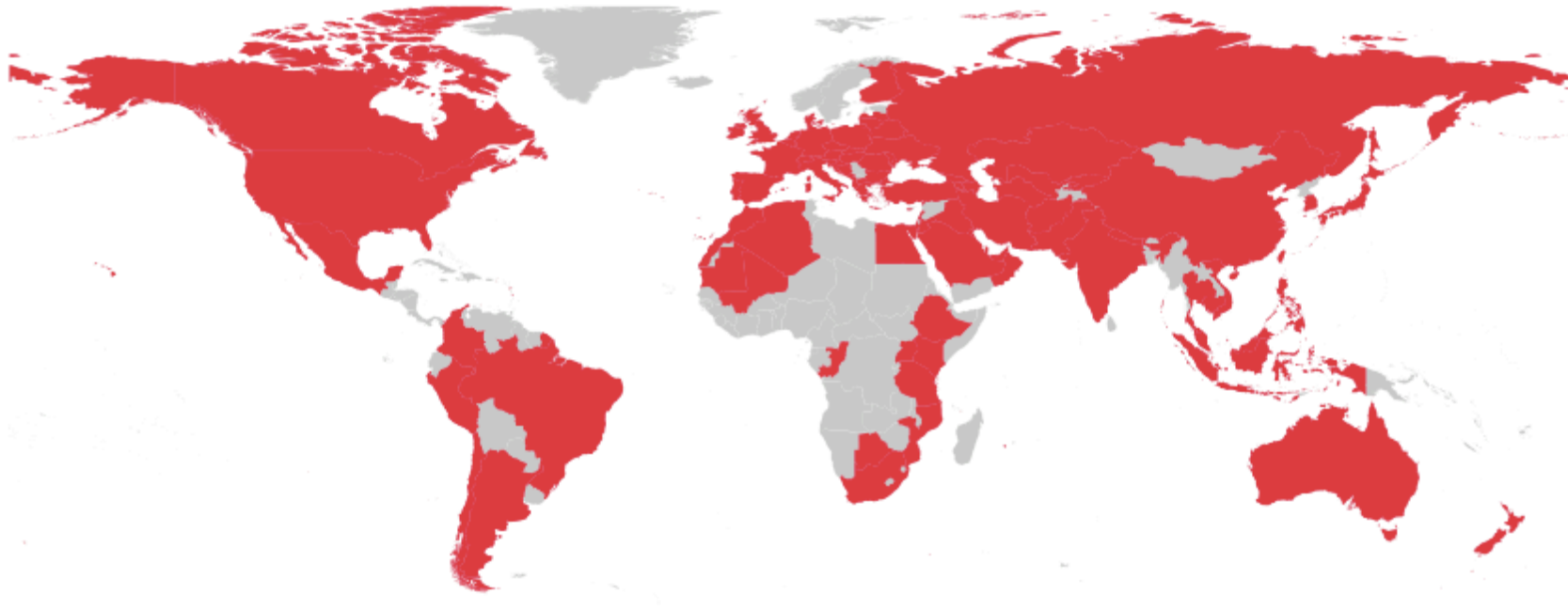
- Threat Intelligence – Current Problems
- Why is TI important?
- Gaps in TI triaging
- Why internal passive DNS sources?
- Our solution/approach
- How can we make analyst investigations easier?
- Creating the tool
- Next steps

Threat Intelligence - Problem Statement

- **Current Problem:** Threat intelligence is sparsely shared among network defenders and always in an inconsistent format.
- There already exist schemas/formats for sharing threat information, but they are not used currently.
- Why is that? It is because we lack tools to enable defenders to easily translate what they know, **visually**, into a format that can be used **tactically**.

Why is this important?

Everyone is a target (and victim):



Source: Verizon DBIR (2014)

Number of security incidents by victim industry and organization size

Industry	Total	Small	Large	Unknown
Accommodation [22]	212	115	34	63
Administrative [56]	16	8	7	1
Agriculture [11]	4	0	3	1
Construction [23]	4	2	0	2
Education [61]	33	2	10	21
Entertainment [71]	20	8	1	11
Finance [52]	856	43	189	624
Healthcare [62]	26	6	1	19
Information [51]	1,132	16	27	1,089
Management [55]	10	1	3	6
Manufacturing [31,32,33]	251	7	33	211
Mining [21]	11	0	8	3
Professional [54]	360	26	10	324
Public [92]	47,479	26	47,074	379
Real Estate [53]	8	4	0	4
Retail [44,45]	467	36	11	420
Trade [42]	4	3	0	1
Transportation [48,49]	27	3	7	17
Utilities [22]	166	2	3	161
Other [81]	27	13	0	14
Unknown	12,384	5,498	4	6,822
Total	63,437	5,819	47,425	10,193

Source: Verizon DBIR 2014

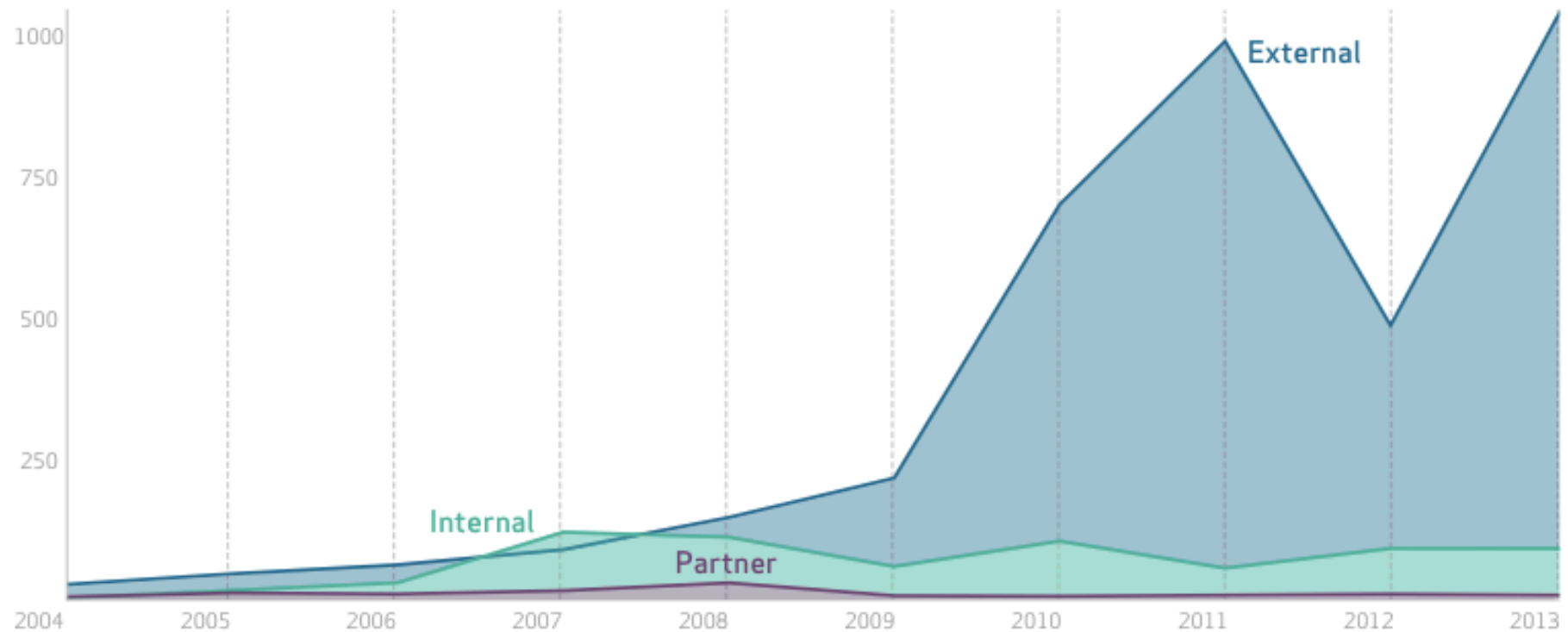
Number of security incidents with confirmed data loss by victim industry and organization size

Industry	Total	Small	Large	Unknown
Accommodation [22]	137	113	21	3
Administrative [56]	7	3	3	1
Construction [23]	2	1	0	1
Education [61]	15	1	9	5
Entertainment [71]	4	3	1	0
Finance [52]	465	24	36	405
Healthcare [62]	7	4	0	3
Information [51]	31	7	6	18
Management [55]	1	1	0	0
Manufacturing [31,32,33]	59	6	12	41
Mining [21]	10	0	7	3
Professional [54]	75	13	5	57
Public [92]	175	16	26	133
Real Estate [53]	4	2	0	2
Retail [44,45]	148	35	11	102
Trade [42]	3	2	0	1
Transportation [48,49]	10	2	4	4
Utilities [22]	80	2	0	78
Other [81]	8	6	0	2
Unknown	126	2	3	121
Total	1,367	243	144	980

Small = organizations with less than 1,000 employees,
Large = organization with 1,000+ employees

External Attacks are Increasing

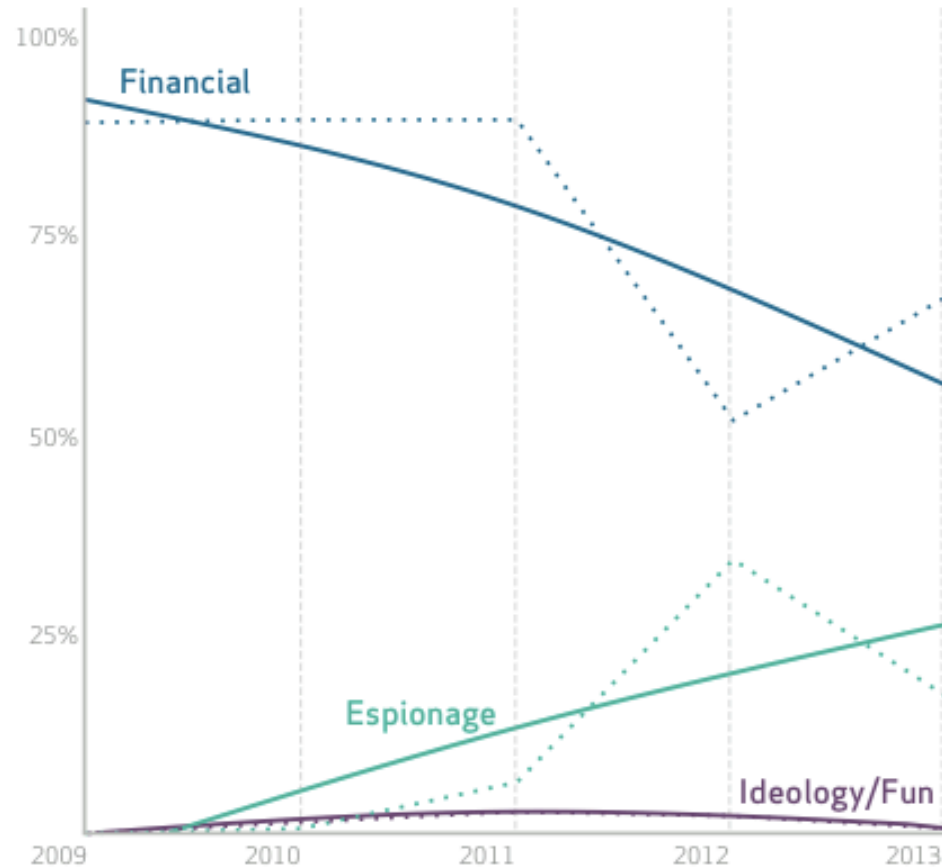
Number of breaches per threat actor category over time



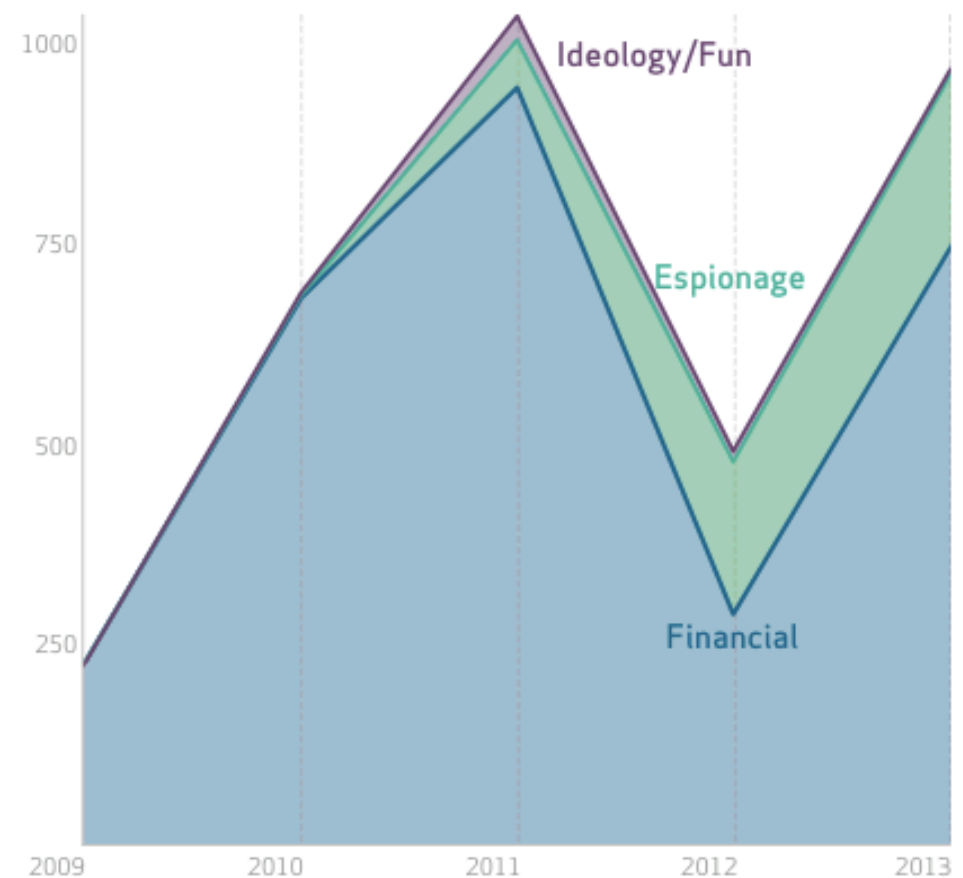
Source: Verizon DBIR 2014

Nation State Attacks are Increasing

Percent of breaches per threat actor motive over time



Number of breaches per threat actor motive over time

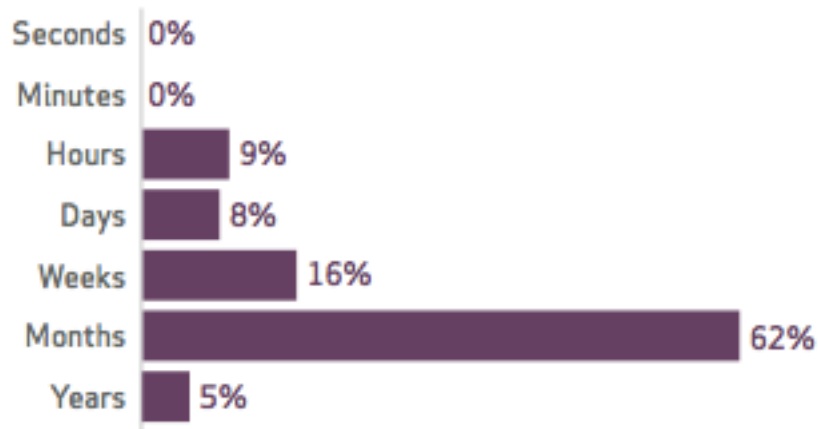


Source: Verizon DBIR 2014

Threat Intel is required to defend against Nation State attacks

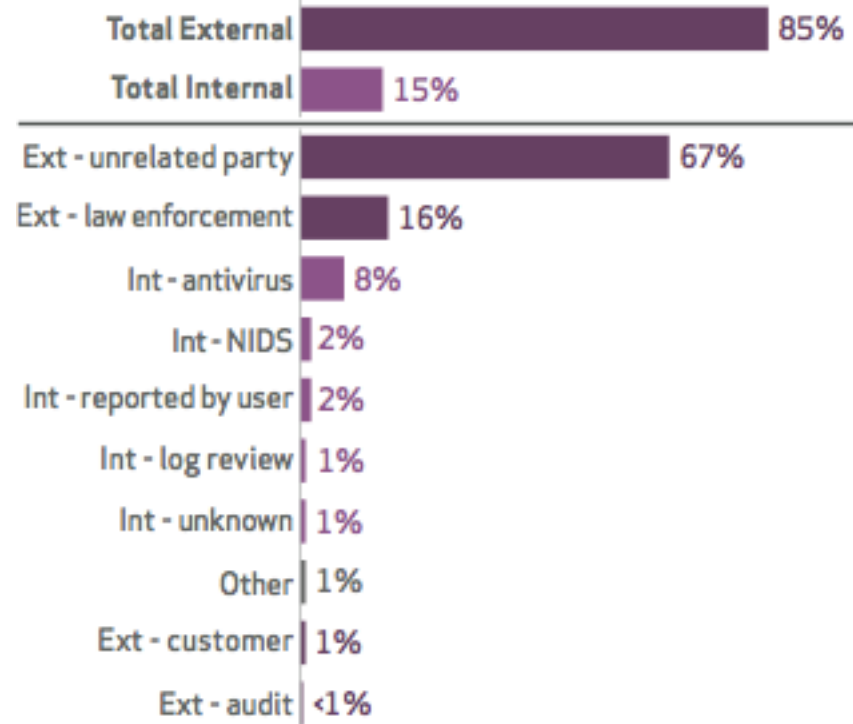
Without threat intel, discovery can take months/years:

Discovery timeline within Cyber-espionage (n=101)

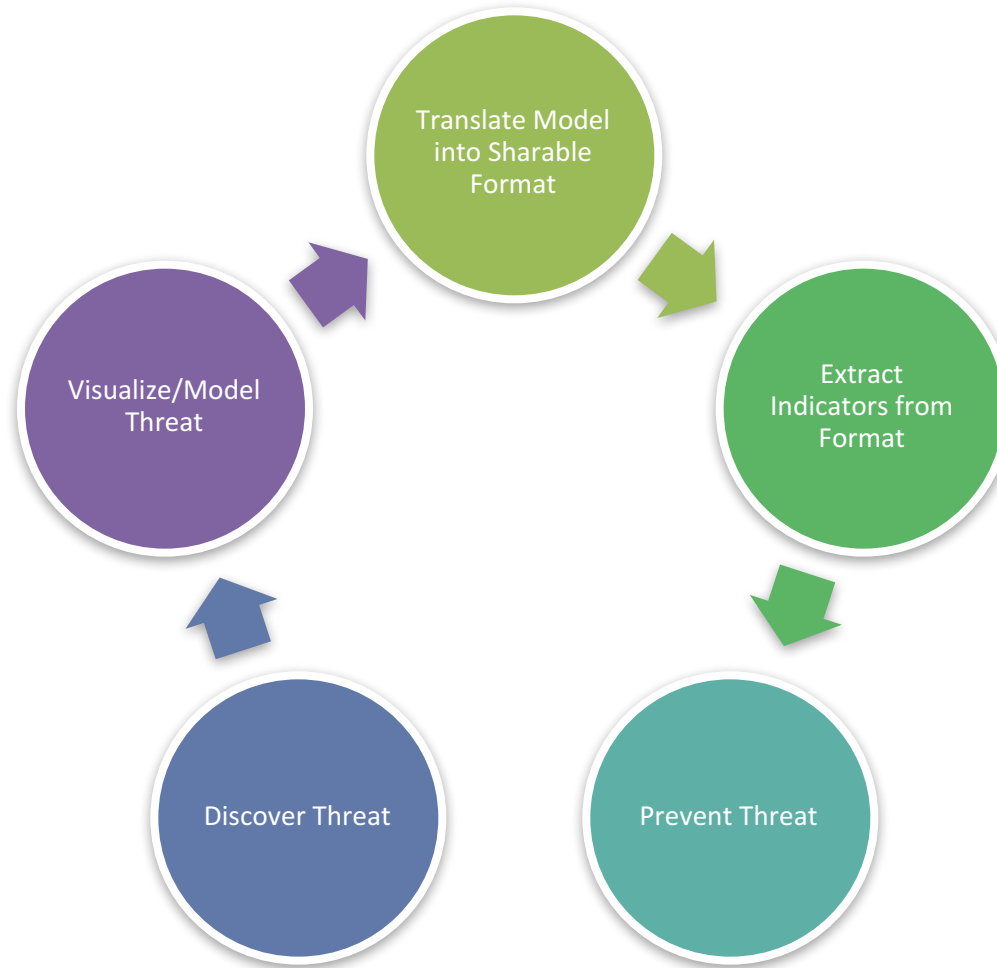


External parties want to share threat intel, but lack tools to help make **collaboration** easier:

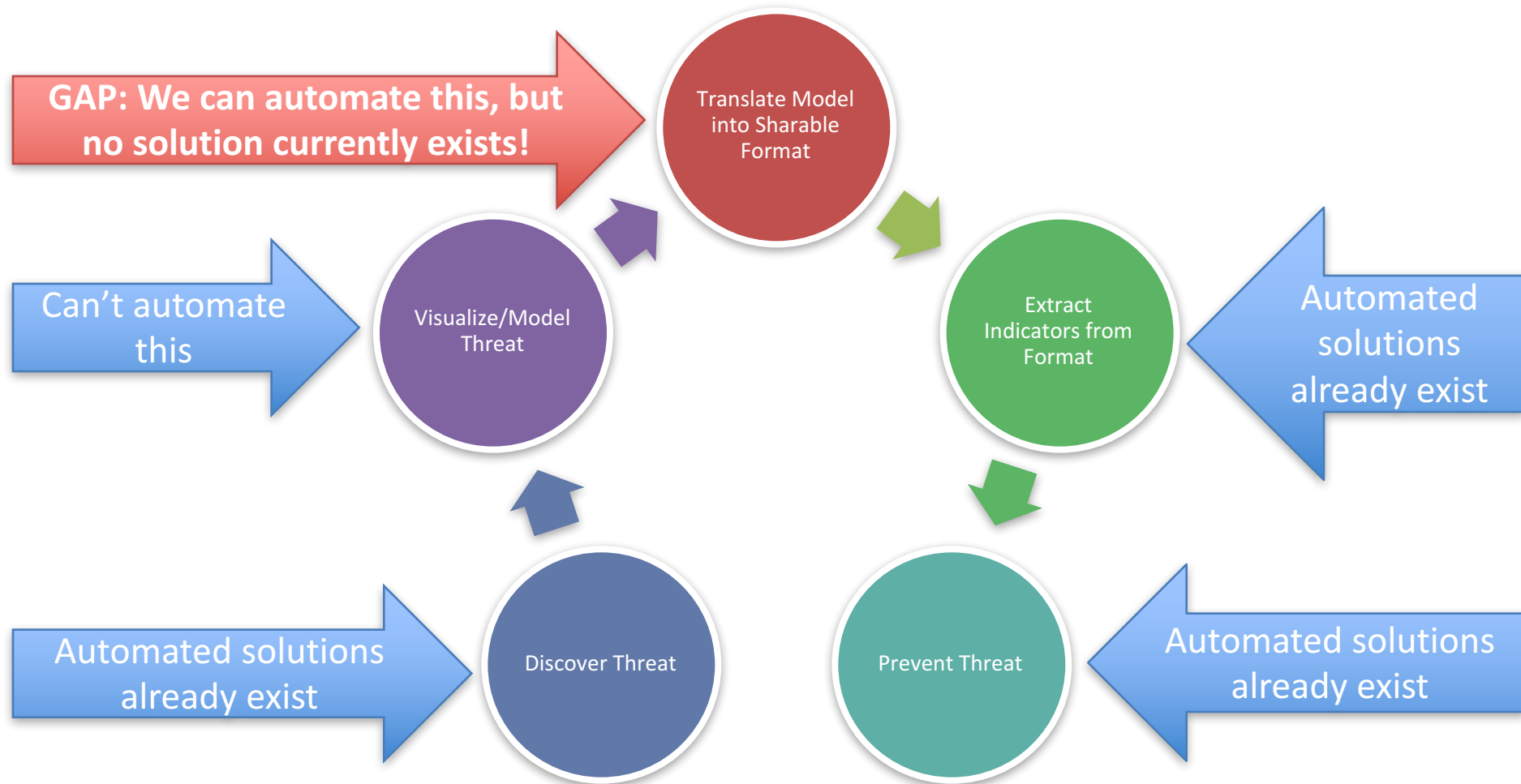
Top 10 discovery methods within Cyber-espionage (n=302)



Current Gap in Threat Intel Workflows



Current Gap in Threat Intel Workflows



Where Can the Process be Improved?

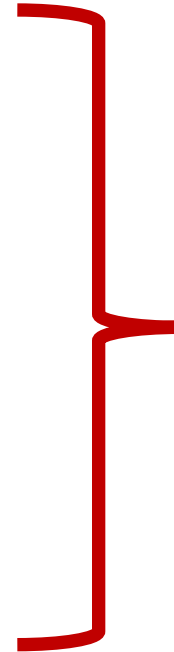
- Better Visibility of Malicious Domains

- Automation

- YARA Rules
- Machine Learning

- Visualization/Modeling

- Sharing (people problem)



We will not discuss these today!

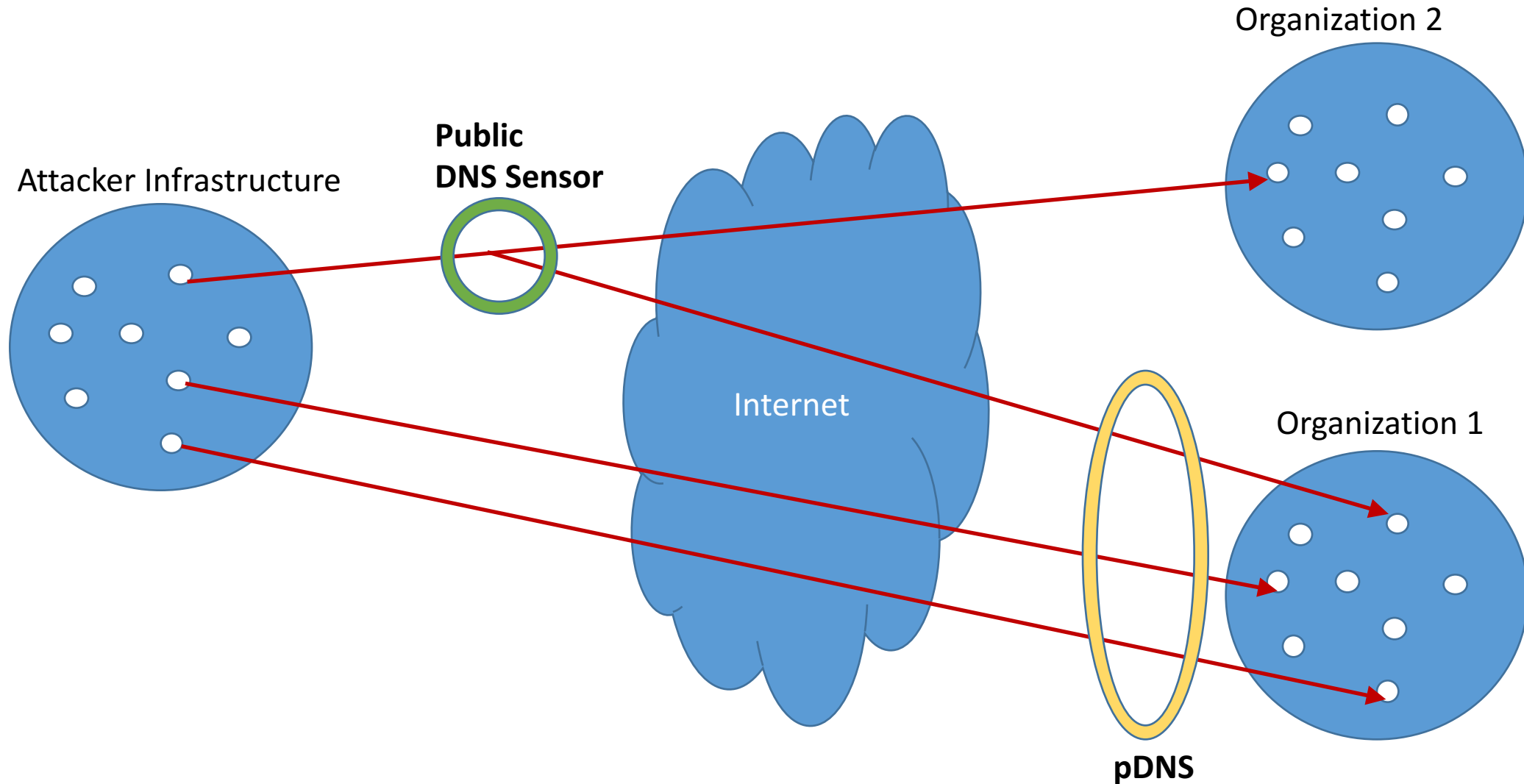
Why Passive DNS Analysis for Threat Intel?

- For normal intrusions, many malware uses ephemeral domains as C2
 - When conducting IR from even events one week old, there are no results on the domain name queries
 - Many analysts use a passiveDNS service (not free) like Farsight DNSDB or PassiveTotal
 - These services may not provide needed data either
 - Having a local passive DNS repository provides that needed data for more thorough analysis

Triaging Threat Intelligence for Network Defense – Problem Statement

- Tailored and targeted attacks are difficult to triage
- External intelligence sources can provide piecemeal information about TTPs used by attackers
 - May not provide full insight as to the methods used in a targeted attack against your organization
- Augmenting external sources with internal sources helps tremendously
 - Blanket solutions like full packet capture can be costly to maintain, and analyze quickly
- Maintaining an internal lightweight sensor focused on DNS data can help gain incremental visibility without a huge maintenance burden

So What? – Why Internal Passive DNS Sources?



What is an Analyst Building?

- Both public and local passive DNS sources are helpful in gaining visibility
 - These are not mutually exclusive approaches

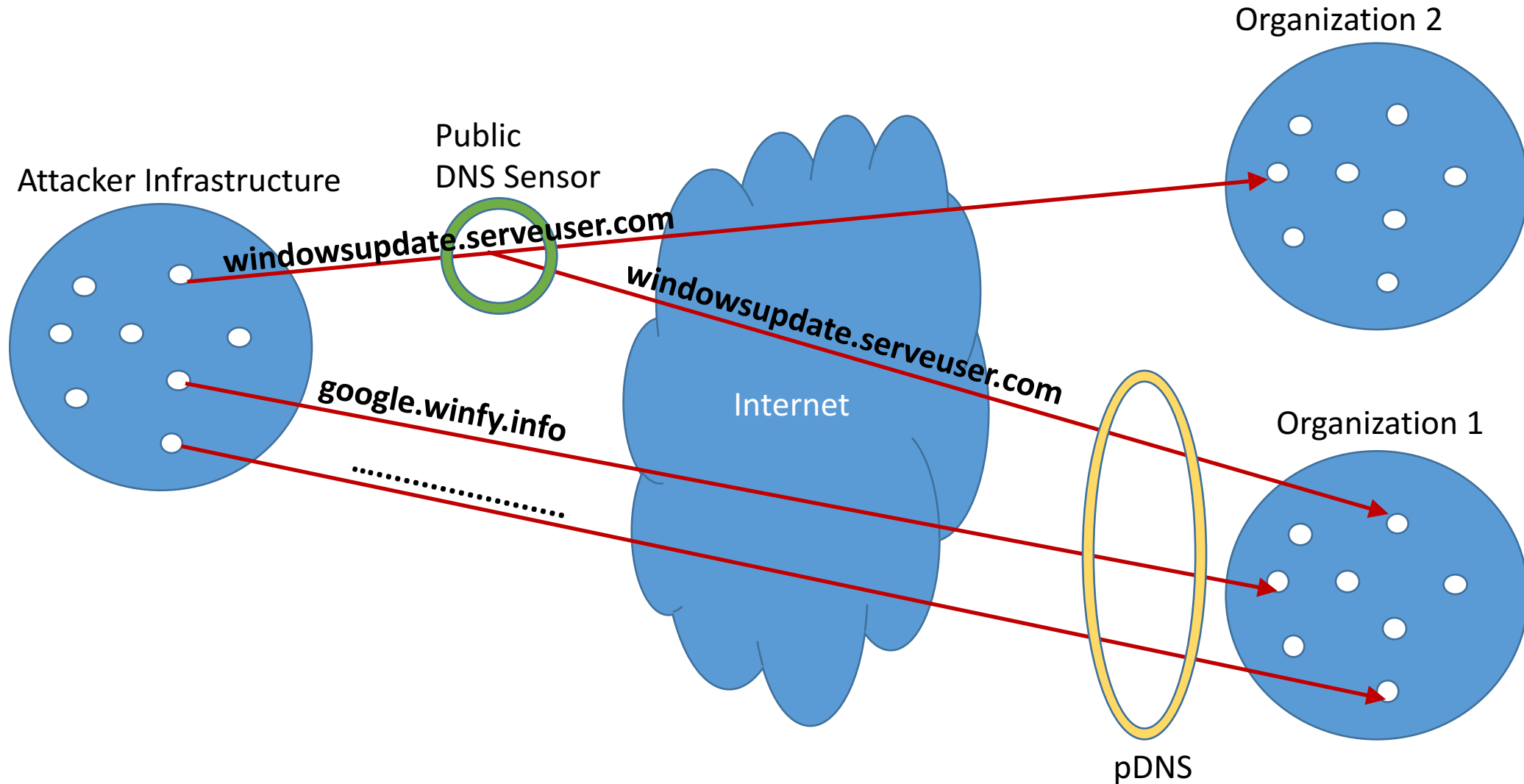
Public Passive DNS Sensors

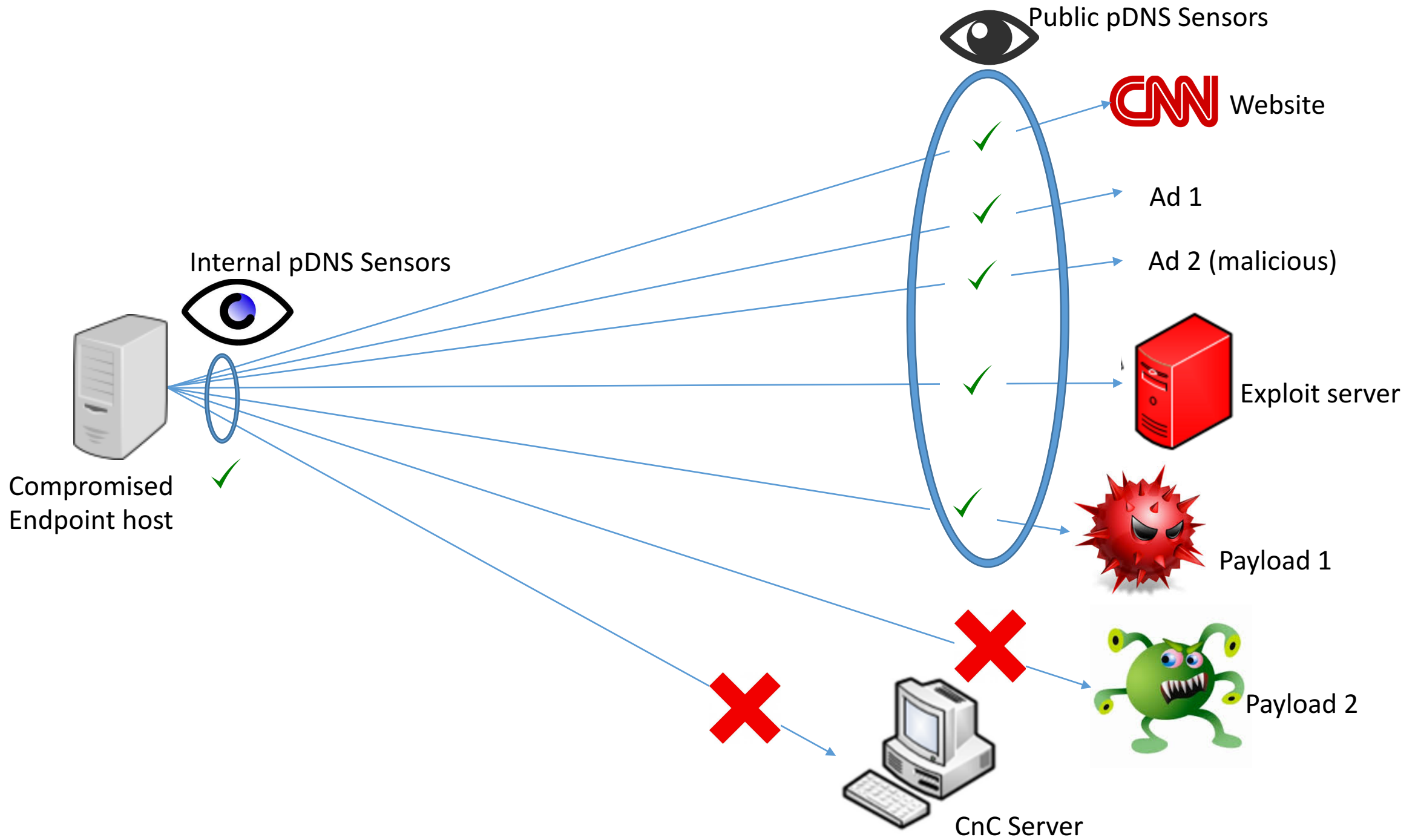
Domain	IP Address
windowsupdate.serveuser.com	xxx.xxx.xxx.xxx
defcontractor2.xxxxx.com	xx.xx.xxx.x
.....

Local/Private Passive DNS Sensors

Domain	IP Address
google.winfy.info	xxx.xx.xxx.xxx
defcontractor.xxxx.com	xx.xxx.x.xxx
windowsupdate.serveuser.com	xxx.xxx.xxx.xxx

So What? – Why Internal Passive DNS Sources?





Solution

- Relying on external sensors alone does not provide full visibility
- Relying on full packet capture solutions is burdensome and inefficient
- **We need a middle ground**
- Local lightweight sensor that provides visibility for quick triaging of attacker TTPs

We Want to Make Analyst Investigations Easier

- What can we build to make triaging of local passive DNS data easier?

First Goal

- Build an app to facilitate local collection of passive DNS data
 - Data will assist in conducting threat intelligence analysis
 - Data can be outputted in simple format for sharing purposes
 - Application is free
 - Current solutions (e.g., Farsight DNSDB, PassiveTotal) has limited visibility
 - Not necessarily inside your network

What is Stream?

- Underlying capture tool that pDNS app utilizes
- Captures real-time streaming wire data
- Netflow-like data, including DNS traffic
- Free – download and install on Splunk

Inputs

- DNS-specific packet captures from Stream application

Outputs

- Analyst UI that allows query of IP addresses or domain names to find relevant DNS traffic that matches query

Starting Point – High Density Data

Timestamp (when DNS query was made)	Internal_IP (srcIP)	External_IP (dstIP)	External DNS (blacklisted)
2016-03-29 12:00:00	192.168.1.1	104.145.233.85	joaservice.com
2016-03-29 12:04:00	192.168.1.1	128.253.180.2	ckt4.cn
2016-03-29 12:06:00	192.168.1.2	128.253.180.2	0551fs.COM
2016-03-29 12:07:00	192.168.1.3	128.253.180.2	foo.com (blacklisted)
2016-03-29 12:08:00	192.168.1.5	128.253.180.3	bar.com (blacklisted)

Three different IPs internally made DNS requests to foo.com, which is blacklisted, during a short timeframe. We need to collapse the entries to what's on the next slide...

Example UI Dashboards


Start Time	End Time	Domain	IP of Resolv. DNS	Count of Unique Client IPs
2016-03-29 12:00:00	2016-03-29 12:07:00	joaservice.com	104.145.233.85	3
2016-03-29 12:08:00	2016-03-29 12:08:00	bar.com	128.253.180.3	1

(Drilldown of 'Count of Unique Client IPs' on next slide)

This is the result of collapsing the previous slide results. We now 'click' on the '3' in the right column, and that leads to the next slide. This would be the starting point for the analyst – the previous table is too information dense for analysts to process.

Drilldown of previous column

Start	End	Client IP	Count of DNS Requests
2016-03-29 12:00:00	2016-03-29 12:04:00	192.168.1.1	2
2016-03-29 12:06:00	2016-03-29 12:06:00	192.168.1.2	1
2016-03-29 12:07:00	2016-03-29 12:07:00	192.168.1.3	1



(Drilldown of 'Count of DNS Requests' on next slide)

Note that we leave out the bar.com result in slide 6, because it's a different domain than foo.com, which is what we're expanding on in this table. Now, we 'click' on the number '2' on the right column to drill down to the next slide.

Drilldown of previous column

Timestamp (when DNS query was made)	Internal_IP (srcIP)	External_IP (dstIP)	External DNS
2016-03-29 12:00:00	192.168.1.1	128.253.180.2	foo.com (blacklisted)
2016-03-29 12:04:00	192.168.1.1	128.253.180.2	foo.com (blacklisted)

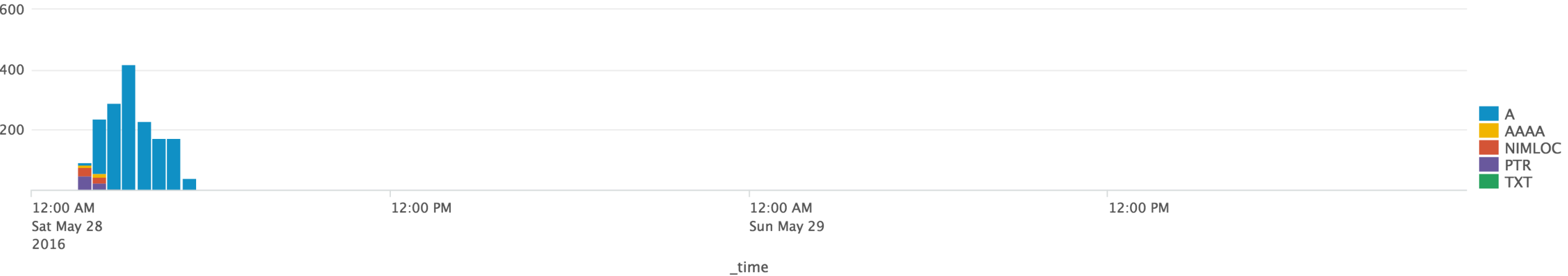
Click row to drill down on query detail

First Query ↕	Last Query ↕	upper_dom ↕	Number of Queries ↕	Distinct Answers ↕	Distinct Subdomains ↕	Distinct Clients ↕	Max Subdomain Length ↕	Blacklist Type ^	Blacklist Reference ↕
2016-06-26 21:02:50	2016-06-26 21:02:50	AMERARANI.COM	8	1	1	1		attackpage	safebrowsing.clients.google.com
2016-05-28 02:31:57	2016-05-28 02:31:57	ASTHANABROTHERS.COM	8	1	1	1		attackpage	safebrowsing.google.com
2016-05-28 02:44:29	2016-05-28 02:44:29	AUTCONTROL.IR	8	1	1	1		attackpage	safebrowsing.clients.google.com
2016-06-26 20:41:46	2016-06-26 20:41:46	BAOLINYOUXIPINGTAI.COM	8	1	1	1		attackpage	safebrowsing.clients.google.com
2016-05-28 02:44:48	2016-05-28 02:44:48	BJHYCD.NET	8	1	1	1		attackpage	safebrowsing.clients.google.com
2016-05-28 02:44:54	2016-05-28 02:44:54	BJXDZG.COM	8	1	1	1		attackpage	safebrowsing.clients.google.com
2016-05-28 02:27:15	2016-05-28 02:27:15	BLACKFALCON3.NET	8	1	1	1		attackpage	www.google.com.ph/safebrowsing
2016-05-28 02:37:56	2016-05-28 02:37:56	BXZXW.NET	8	1	1	1		attackpage	safebrowsing.clients.google.com

Click row to drill down on query detail

First Query ⚙	Last Query ⚙	upper_dom ⚙	Number of Queries ⚙	Distinct Answers ⚙	Distinct Subdomains ⚙	Distinct Clients ⚙	Max Subdomain Length ⚙	Blacklist Type ⚙	Blacklist Reference ⚙
2016-05-28 02:44:48	2016-05-28 02:44:48	BJHYCD.NET	8	1	1	1		attackpage	safebrowsing.clients.google.com


Volume of DNS Events By All Types, Over Selected Time Period



Click row to drill down on query detail

First Query ▾	Last Query ▾	upper_dom ▾	Number of Queries ▾	Distinct Answers ▾	Distinct Subdomains ▾	Distinct Clients ▾	Max Subdomain Length ▾	Blacklist Type ▾	Blacklist Reference ▾
2016-05-28 02:44:48	2016-05-28 02:44:48	BJHYCD.NET	8	1	1	1		attackpage	safebrowsing.clients.google.com

Queries Against Domain: bjhycd.net (click row for further detail)

DNS.query ▾	Trend of Queries ▾	Number of Answers ▾	Number of Queries ▾	Number of Distinct Systems ▾	Systems Making the Request ▾
bjhycd.net		1	8	1	172.31.15.15

Subdomains Queried: bjhycd.net (Click for further detail)

	First Seen ↕	Last Seen ↕	DNS.query ↕	Query Answers ↕	Number of Queries ↕
1	2016-05-28 02:44:48	2016-05-28 02:44:48	bjhycd.net	unknown	4

Clients Querying: bjhycd.net (Click for further detail)

First Seen ↕	Last Seen ↕	DNS.src ↕	Query Count ↕
2016-05-28 02:44:48	2016-05-28 02:44:48	172.31.15.15	2

Subdomains Queried: bjhycd.net (Click for further detail)

	First Seen ⚙	Last Seen ⚙	DNS.query ⚙	Query Answers ⚙	Number of Queries ⚙
1	2016-05-28 02:44:48	2016-05-28 02:44:48	bjhycd.net	unknown	4

Clients Querying: bjhycd.net (Click for further detail)

First Seen ⚙	Last Seen ⚙	DNS.src ⚙	Query Count ⚙
2016-05-28 02:44:48	2016-05-28 02:44:48	172.31.15.15	2

Query Detail for bjhycd.net on Client 172.31.15.15 (Click for drill down to raw events)

timestamp ⚙	Source of Request ⚙	Query Answer ⚙	Queried Domain ⚙
2016-05-28T06:44:43.287019Z	172.31.15.15	unknown	bjhycd.net bjhycd.net

Future Features

- Integrate with 3rd party passive DNS sources
 - FarSight DNSDB service – In progress!
 - PassiveTotal/RiskIQ - Reviewing
 - ShadowServer
 - VirusTotal/Google Safe Browsing

Download

- PassiveDNS GitHub - <https://github.com/sbrant/pdns>
- Splunk Enterprise (500M/day limit) - http://www.splunk.com/en_us/download-21.html
- Splunk Stream - <https://splunkbase.splunk.com/app/1809/>

Questions?

