ARBOR NETWORKS

Zero-Day Attack – Finding Advanced Threats in ALL of Your Data

C F Chui, Arbor Networks

Arbor Networks Overview

90% Percentage of world's Tier 1 service providers who are Arbor customers

107 Number of countries with Arbor products deployed

90 Tbps Amount of global traffic monitored by the ATLAS security intelligence initiative right now!

14 Number of years Arbor has been delivering innovative security and network visibility technologies & products

Arbor market position in Carrier, Enterprise and Mobile DDoS equipment market segments – **49% of total market**
[Infonetics Research Q1 2014]

$19B 2013 GAAP revenues [USD] of Danaher – Arbor's parent company providing deep financial backing

ARBOR NETWORKS

ATLAS Intelligence

ATLAS

ATLAS Portal

Models: *Free, Participant*

- Up-to-date threat dashboard showing what Arbor is tracking around the globe
- Details, network specific visibility for Provider partners with sensors deployed

ATLAS Intelligence Feeds

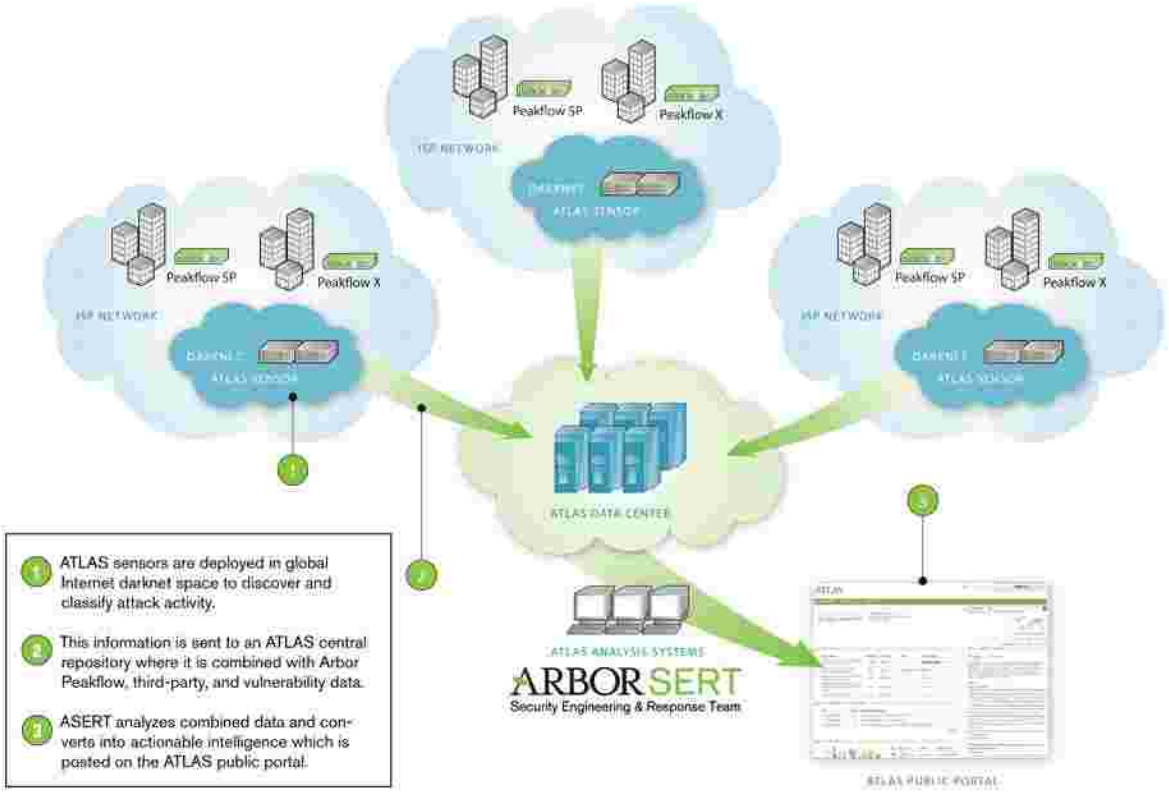
Models: *Basic, Advanced*

- Threat updates going to Arbor Products to detect:
  - Geography, Web Crawler ID, Malware, C&C, Mobile, Targeted Campaign's & other threats

Fingerprint Sharing

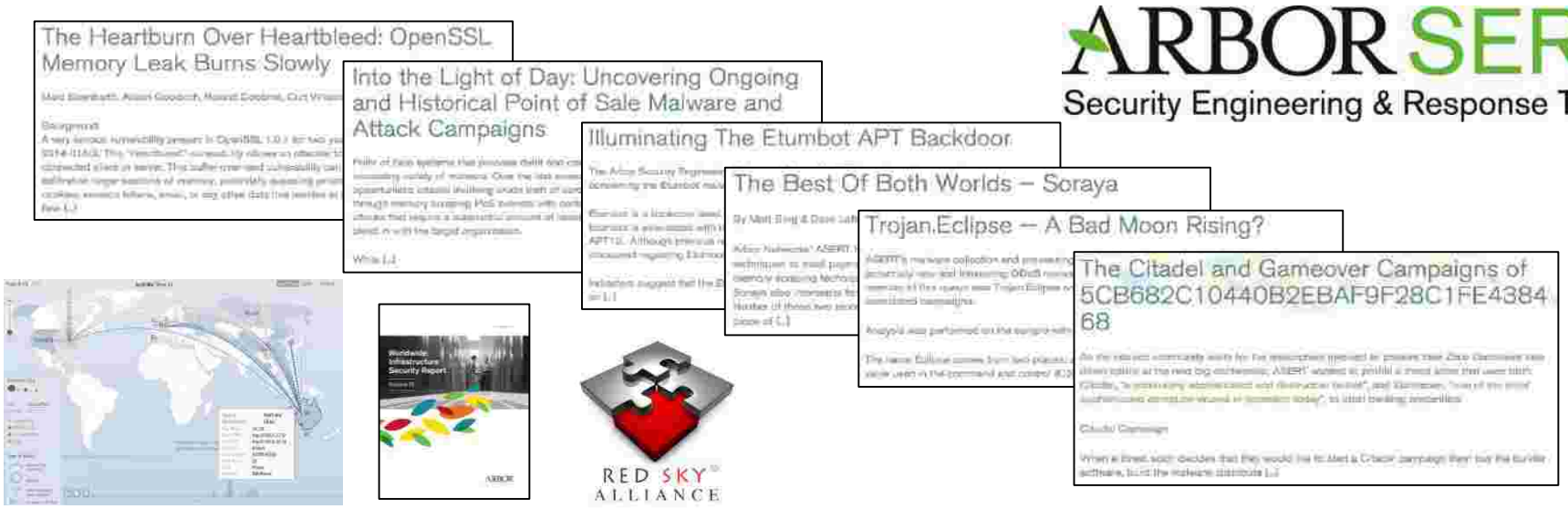
- Enable ISP's to coordinate response to DDoS attacks

ARBOR NETWORKS



- 300 service providers around the globe share data
  - Monitors 90TB/sec of Internet traffic
  - Over 100,000 malware samples seen every day
- Unique and timely threat data used to update Arbor Products with intelligence, alert customers and the market to new threats and partner with third-parties

ASERT Research



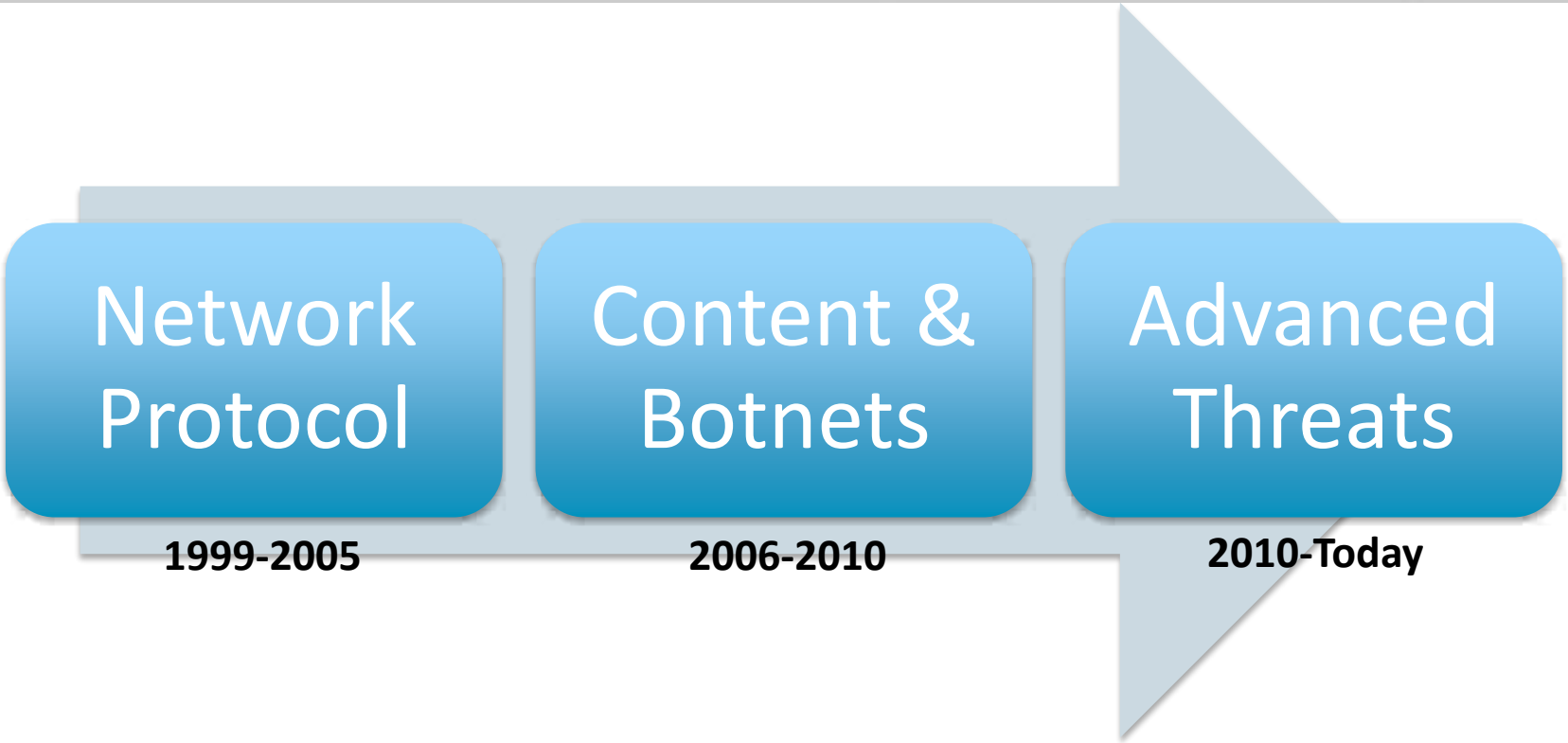
ARBOR SERT
Security Engineering & Response Team

Unmatched Security Research and Community Leadership

- Over a hundred national CERT teams
- Large cross-section of the security industry, through various sharing groups
- Founding member of the Red Sky Alliance
- ATLAS portal has 711 unique users, registering 6,006 ASNs for reporting
- We share up to 5GB of samples per day, which have no re-use restrictions
- ASERT's Malware Corral has seen 9.1M unique IPv4 addresses over 90 days
- ASERT has data for 44,570 of 45,369 ASNs
- ASERT has monitored 2.63B unique IPv4 addresses
- ASERT actively monitors 1.76M "dark" IPv4 addresses

ARBOR NETWORKS

Threat Landscape Era's



- Synflood (Trinoo/TFN)
- Code Red
- Slammer
- Zotob
- Conficker (2008)

- Web Browser
- Web Applications
- Doc/PDF/etc.
- Flash/Shockwave
- Java

- Aurora
- Operation Payback
- Stuxnet/Flame/Duqu
- Red October
- Cyber Warfare

ARBOR NETWORKS

Targeted Attacks In The Headlines

Target hacked: news and updates on the massive retail breach that affected millions

By Chris Welch on January 16, 2014 01:42 pm Email

Between November 27th and December 15th, 2013, retail gian
sophisticated hack that compromised data on tens of millions o
on approximately 40 million credit and debit card accounts was stolen during the breach,
and this sensitive financial data quickly appeared on the black market. Target would later reveal that names, mailing addresses, and phone numbers for up to 70 million customers had also been taken during the attack. The retailer is cooperating with the US Secret Service and Department of Justice to find those responsible; those perpetrators currently remain at large. Target's holiday breach ranks as one of the largest retail hacks in history. In response to the ordeal, the company offered affected customers one year of

Adobe hack: At least 38 million accounts breached

Adobe has confirmed that a recent cyber-attack compromised many more customer accounts than first reported.

The software-maker said that it now believed usernames and encrypted passwords had been stolen from about 38 million

Adobe said source code for Photoshop had been stolen

Business Disruption
Loss of Customer Trust
Financial Costs
Legal Issues

omputer glitch

The government still has an 82% stake in RBS

Royal Bank of Scotland (RBS) has put aside £125m to pay compensation to customers affected by the recent breakdown in its computer systems.

Account holders at RBS and its NatWest and Ulster Bank subsidiaries faced disruption for up to two weeks in June after a software upgrade at the bank.

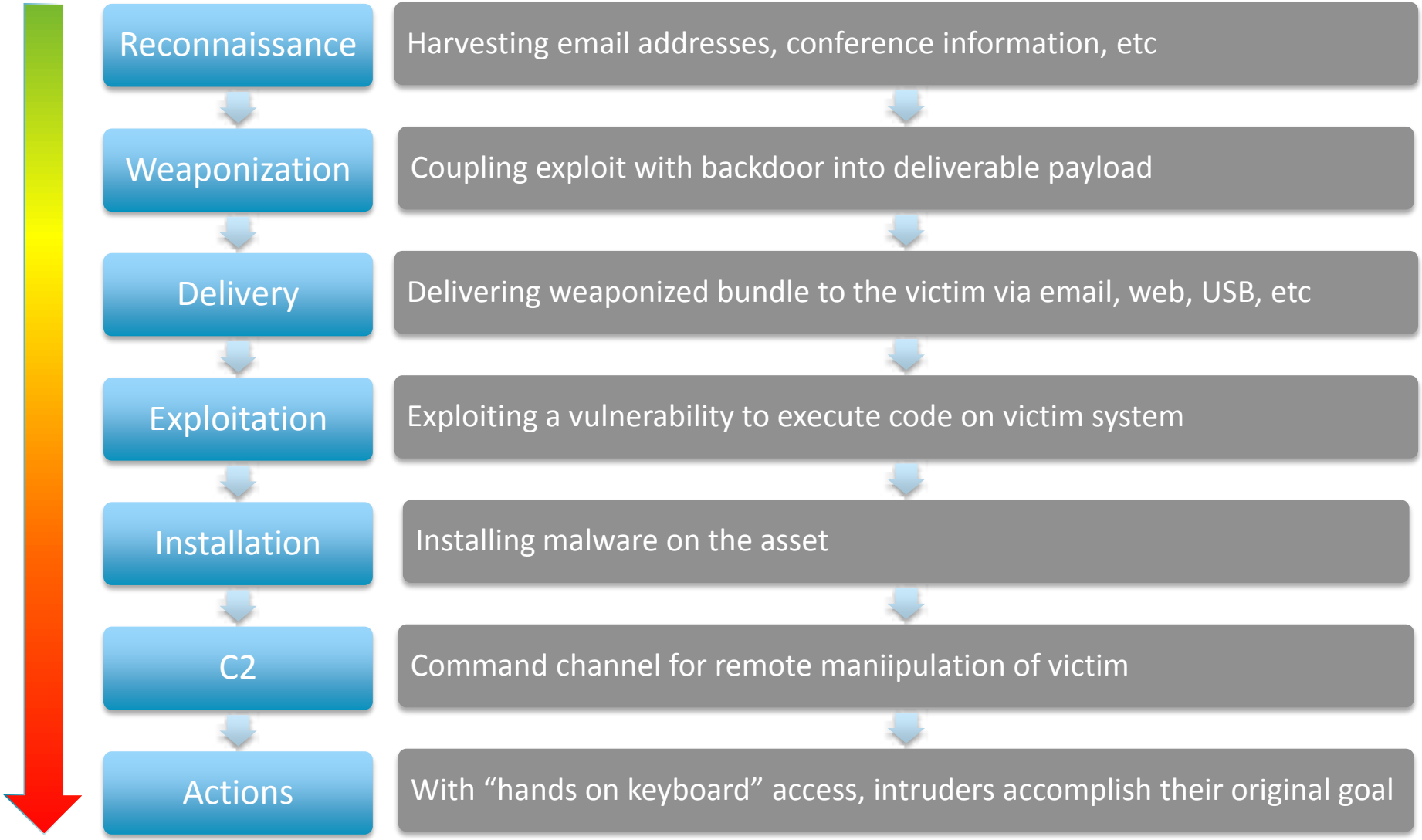
ARBOR NETWORKS

What are Advanced Threats?

- Target **specific victims** for **data exfiltration**
- **Well organized criminal** or government entities
- **Multi-vector**: implants advanced malware in email or other means, triggered via spear-phishing, connects to C&C
- Goal: **long-term control** of compromised systems
- Make use of **Advanced Malware**

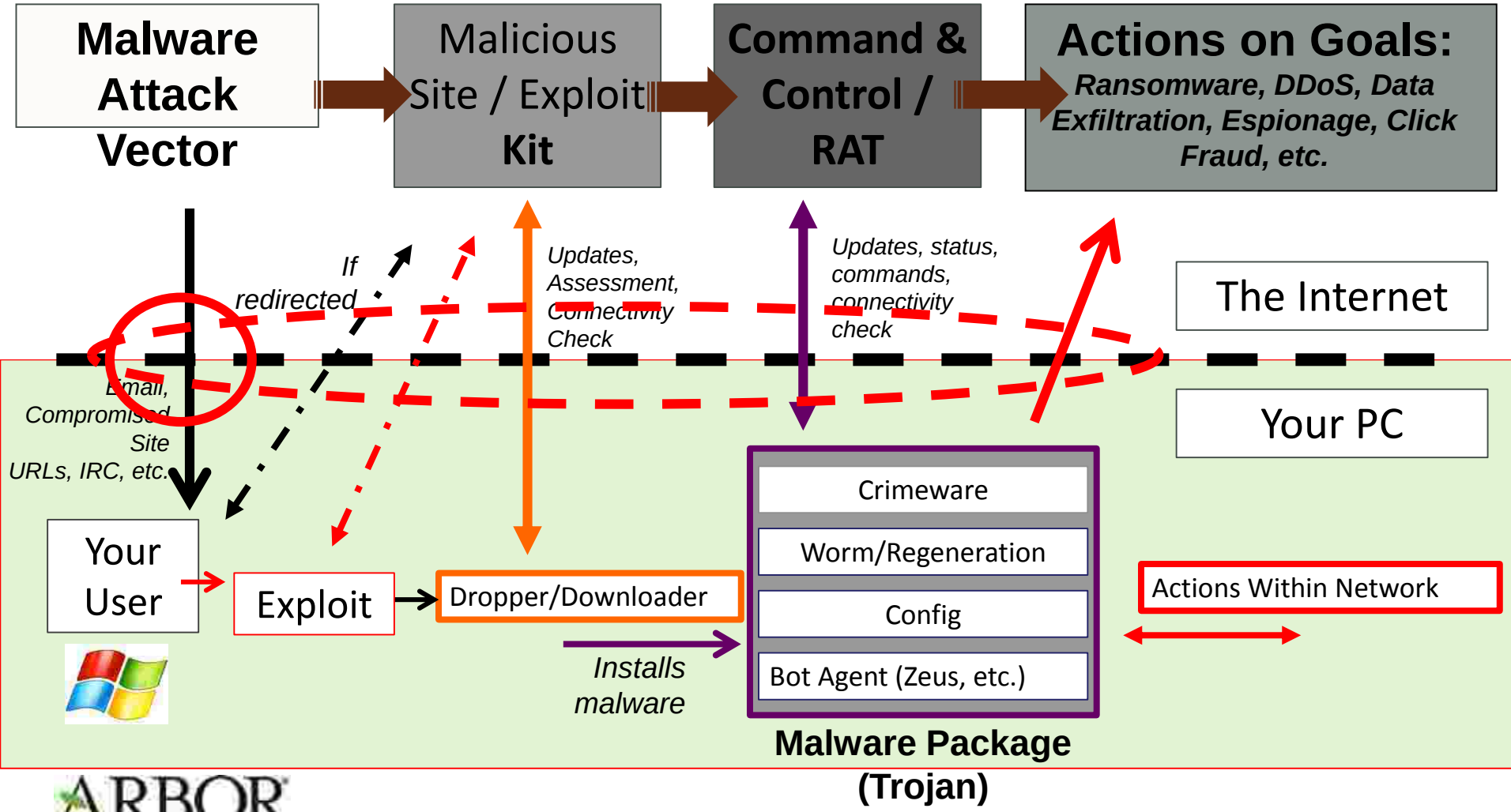
ARBOR NETWORKS

Cyber Intrusion Kill Chain



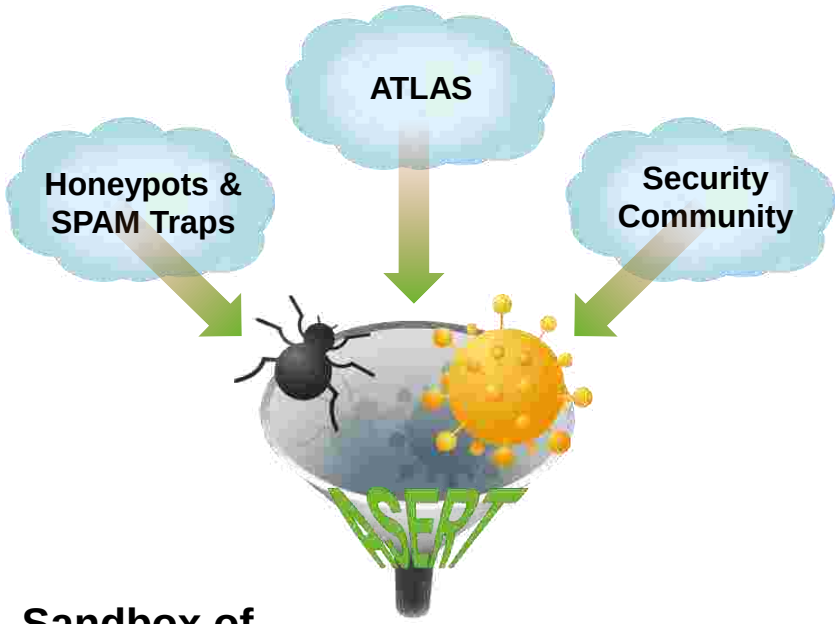
ARBOR NETWORKS

Malware Is An Ecosystem, Not Just A Sample



ARBOR NETWORKS

Who is ASERT: Large-Scale Analysis



Sandbox of Virtual Machines
run malware
(look for Botnet C&C, Files, Network Behavior)

Security Content

Report and PCAP stored in database

"Tracker" DDoS Attack Auto-classification and analysis every 24 hrs.

ARBOR NETWORKS

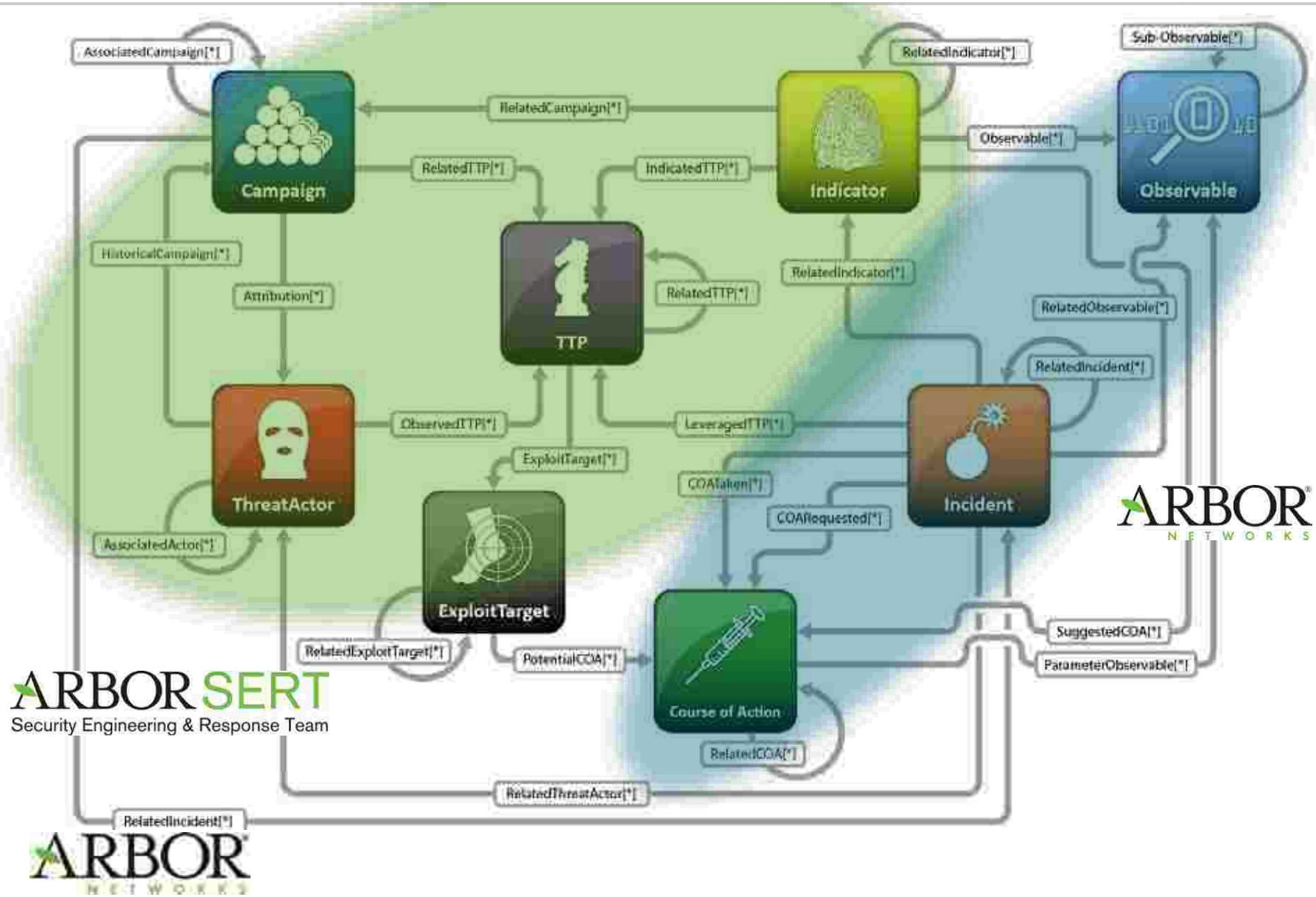
Who is ASERT: Reverse Engineering

- Goals of Data Collection
  - Broad coverage required to focus on specific use-cases, such as DDoS
  - Multiple infection vectors, CnC mechanisms, backscatter analysis, etc.
  - Generate unique indicators: honeypots, CnCs themselves, harvesting, etc.

- Goals of Reverse Engineering
  - Reverse engineering of botnet CnC protocol
  - Emulation of full CnC protocol for direct CnC and peer (zombie) analysis
  - Unique approach to static and dynamic analysis techniques

- Goals of Large-Scale Analysis
  - Understand both latest capabilities and attacker resources
  - Internet-scale correlation, i.e. relate a .eml to originating executable
  - End-to-end threat lifecycle, i.e. **observe** actor ordering an attack through a infiltrated CnC then **verify** the attack from flow data

Historical, Campaign-Focused Approach



ARBOR NETWORKS

ARBOR SERT
Security Engineering & Response Team

ARBOR NETWORKS

ATLAS Data – Darknet

- Honeypot Output

```
start    - UTC timestamp
sid      - Snort signature ID
src      - IP address string
proto    - IP protocol number
dport    - destination port number
           (or type for ICMP)
attacks  - number of attacks
cc       - country code
asn      - AS number
```

```
[
  {
     "asn": "4725",
     "attacks": "1",
     "cc": "JP",
     "dport": "447",
     "proto": "17",
     "sid": "2008109”,
     "src":"220.212.51.179",
     "start": "1400355000
  }
]
```

sid 2008109 -> ET CURRENT_EVENTS Possible Bobax/Kraken/Oderoor UDP 447 CnC Channel Outbound

ARBOR NETWORKS

ATLAS Data – Botnet

- Botnet Data

```
now     -- C&C Timestamp when added
ip      -- C&C IP address string
port    -- C&C Port
cc      -- C&C Country Code
asn     -- C&C AS number
```

```
{
   "cc": "DE",
   "ip": "80.82.209.199",
   "now": "1405473000",
   "port": "6667",
   "asn": "24961"
}
```

ARBOR NETWORKS

ATLAS Data – Botnet

- Botnet Infiltration Data
  - Data used for threat intel and special event engagements


```
{
        "added": "2013-04-29T15:55:00",
        "family": "dirtjumper",
        "hostname": "18-11-1996.cc",
        "ips": [
            {
                "cc": "JP",
                "ip": "36.55.239.170"
            }
        ],
        "last_success": null,
        "md5": [],
        "targets": [],
        "uri": "/panel/diwar.php",
        "urls": []
    },
```


ARBOR NETWORKS

ATLAS Data – Botnet

- Botnet Infiltration Data


```
{  "added": "2014-01-05T19:22:51",
   "family": "drive",
   "hostname": "beanonymouse.biz",
   "ips": [ {
                "cc": "UA",
                "ip": "31.28.169.22"
            },
   "last_success": "2014-06-08T03:55:04",
   "md5": ["6915142fa489e75ac64e69a60104a36f”],
   "targets": [ {
                     "attack_type": "post2",
                     "target_asn": 16509,
                     "target_cc": "jp",
                     "target_host": "aossms.com"
              } ],
   "uri": "/forum/",
```


ARBOR NETWORKS

ATLAS Data – Bot emulation

Show 50 entries
Search:

ts	Family	CnC	command	target	port	uri	asn	cc	nb_name
2014-11-06 17:15:06	kernelbot_hk	nitori-tour.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw
2014-11-06 17:15:06	kernelbot_hk	ninekobe.com	DDOS_UdpFlood	202.85.162.116	-1	None	9729	hk	iadvantage limi
2014-11-06 17:15:08	kernelbot_hk	mizma.co.jp	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw
2014-11-06 17:15:09	kernelbot_hk	wizapply.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw
2014-11-06 18:15:05	kernelbot_hk	wizapply.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	209	us	akamai technolo
2014-11-06 18:15:07	kernelbot_hk	mizma.co.jp	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	209	us	akamai technolo
2014-11-06 18:15:07	kernelbot_hk	ninekobe.com	DDOS_UdpFlood	202.85.162.116	-1	None	9729	hk	iadvantage limi
2014-11-06 18:15:08	kernelbot_hk	nitori-tour.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	209	us	akamai technolo
2014-11-06 19:15:06	kernelbot_hk	nitori-tour.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	209	us	akamai technolo
2014-11-06 19:15:07	kernelbot_hk	nine					9729	hk	iadvantage limi
2014-11-06 19:15:08	kernelbot_hk	miz				deo/0	209	us	akamai technolo
2014-11-06 19:15:09	kernelbot_hk	wiz				deo/0	209	us	akamai technolo
2014-11-06 20:15:05	kernelbot_hk	wiz				deo/0	209	us	akamai technolo
2014-11-06 20:15:06	kernelbot_hk	miz				deo/0	209	us	akamai technolo
2014-11-06 20:15:07	kernelbot_hk	nine					9729	hk	iadvantage limi
2014-11-06 21:15:17	kernelbot_hk	nine					9729	hk	iadvantage limi
2014-11-06 21:15:18	kernelbot_hk	miz				deo/0	209	us	akamai technolo
2014-11-06 21:15:18	kernelbot_hk	wiz				deo/0	209	us	akamai technolo
2014-11-06 22:15:05	kernelbot_hk	wizapply.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	2914	us	ntt america in
2014-11-06 22:15:06	kernelbot_hk	mizma.co.jp	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	2914	us	ntt america in
2014-11-06 22:15:07	kernelbot_hk	ninekobe.com	DDOS_UdpFlood	202.85.162.116	-1	None	9729	hk	iadvantage limi
2014-11-06 23:15:16	kernelbot_hk	ninekobe.com	DDOS_UdpFlood	202.85.162.116	-1	None	9729	hk	iadvantage limi
2014-11-06 23:15:17	kernelbot_hk	mizma.co.jp	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	2914	us	ntt america in
2014-11-06 23:15:18	kernelbot_hk	wizapply.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	2914	us	ntt america in
2014-11-07 00:15:06	kernelbot_hk	wizapply.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw
2014-11-07 00:15:07	kernelbot_hk	mizma.co.jp	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw
2014-11-07 00:15:07	kernelbot_hk	ninekobe.com	DDOS_UdpFlood	202.85.162.116	-1	None	9729	hk	iadvantage limi
2014-11-07 01:15:16	kernelbot_hk	ninekobe.com	DDOS_UdpFlood	202.85.162.116	-1	None	9729	hk	iadvantage limi
2014-11-07 01:15:17	kernelbot_hk	mizma.co.jp	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw
2014-11-07 01:15:18	kernelbot_hk	wizapply.com	DDOS_ScriptFlood	hk.dv.nextmedia.com	80	/video/videolist/20141105/hit/video/0	3491	us	beyond the netw

ASERT methodically tracks and monitors wide range of botnet activity

ARBOR NETWORKS

Threat-Centric Approach

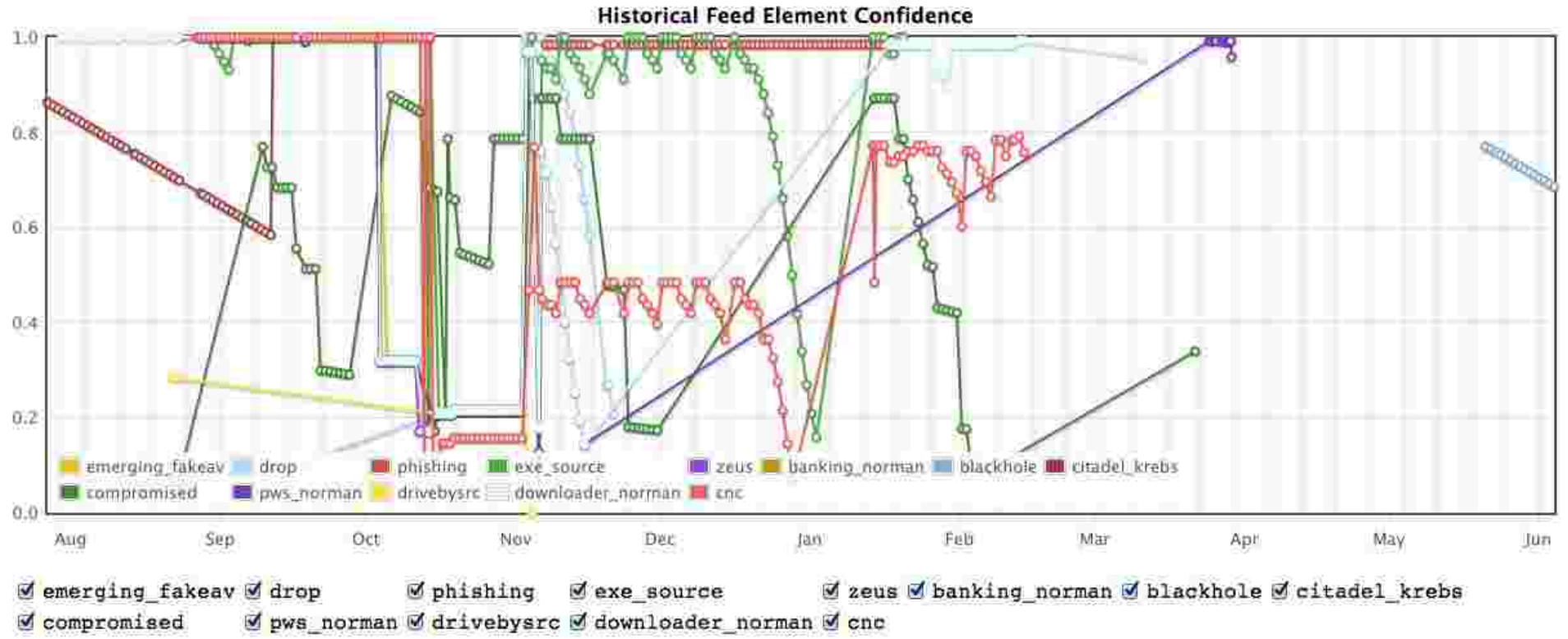
- What is the malware designed to do?
- Not necessarily where it's been, but where is it going?
- Don't look at just active behavior, but potential behavior

Mischief Detection(s):

Accesses Windows Address Book [Severity: 6]
Adds autostart object [Severity: 5]
Creates Entry in Autostart Folder or File [Severity: 5]
Creates file in drivers folder [Severity: 5]
Creates malicious events: P2P Zeus [Banking] [Severity: 10]
Creates malicious events: Zeus [Banking] [Severity: 10]
Creates process in suspicious location [Severity: 5]
Creates threads in system processes [Severity: 7]
Downloads executable [Severity: 4]
Dumps and runs batch script [Severity: 6]
Injects thread into Windows process [Severity: 7]
Installs service [Severity: 6]

ARBOR NETWORKS

Historical, Campaign-Focused Approach



☑ emerging_fakeav ☑ drop ☑ phishing ☑ exe_source ☑ zeus ☑ banking_norman ☑ blackhole ☑ citadel_krebs
☑ compromised ☑ pws_norman ☑ drivebysrc ☑ downloader_norman ☑ cnc

ARBOR NETWORKS

Network-Based Indicators of Compromise

Network-Observables

- IP/Port/CIDR/AS
- Domain
- URL
- File Hash
- Social Networking
- Geo Location
- Credentials
- Certificates

ARBOR NETWORKS

Arbor Networks Zero-day Threat Solution

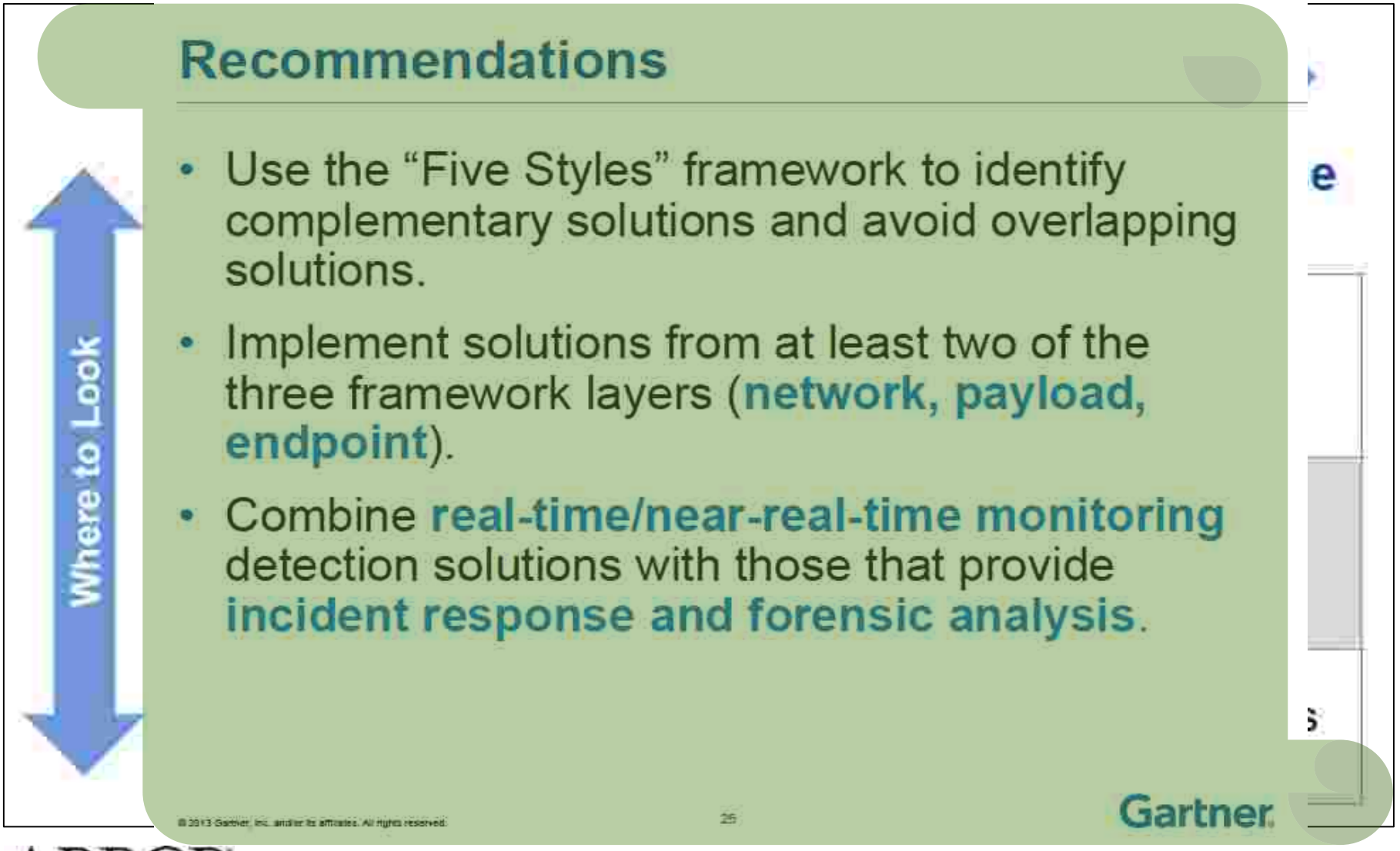
ARBOR NETWORKS

Advanced Threat: What we know today….

- Organizations face an ever growing and sophisticated level of threats
- There are not enough skilled security analysts to interpret and act on these threats
- Its not getting any easier

ARBOR NETWORKS

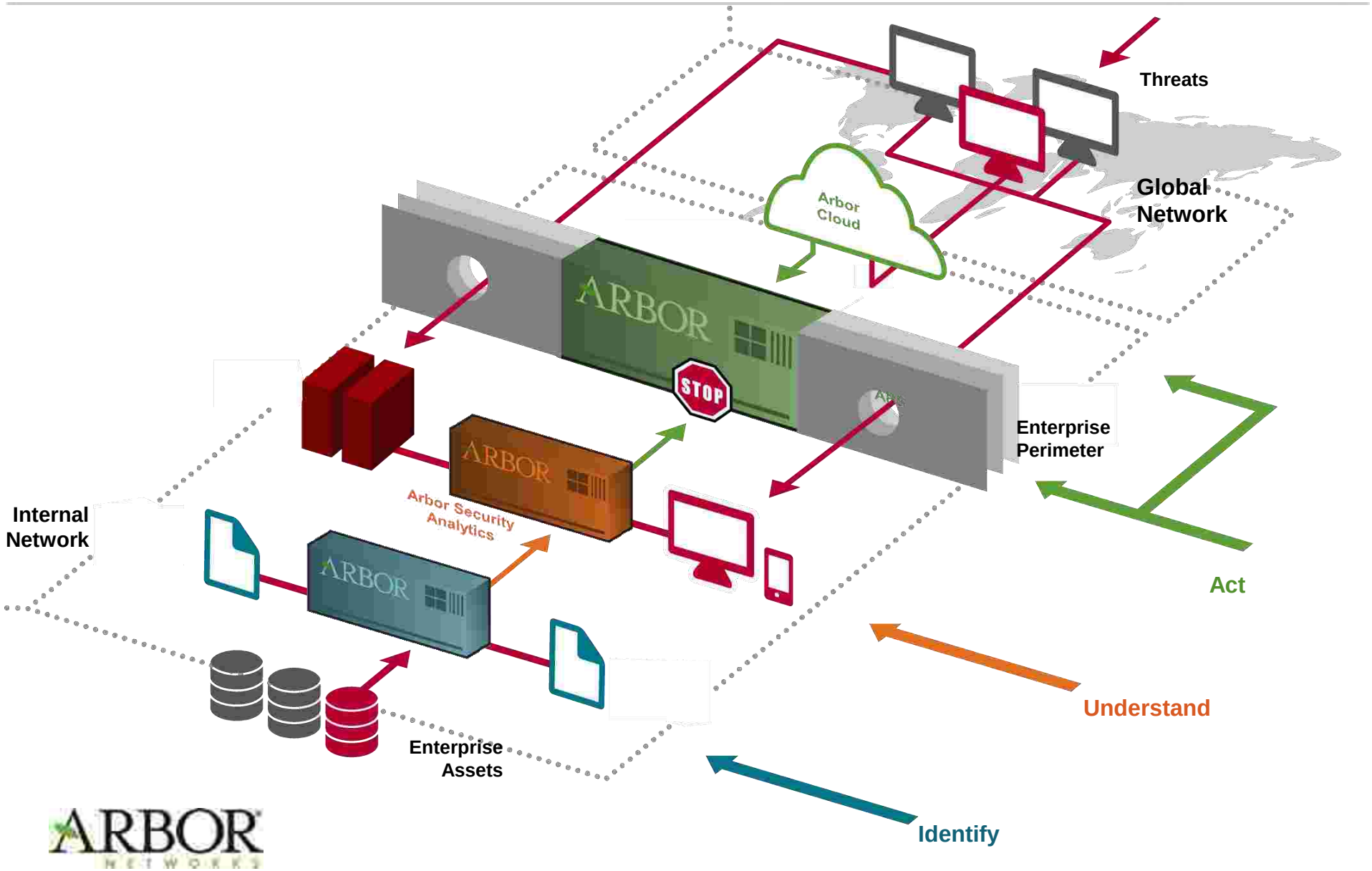
Five Styles of Advanced Threat Defense



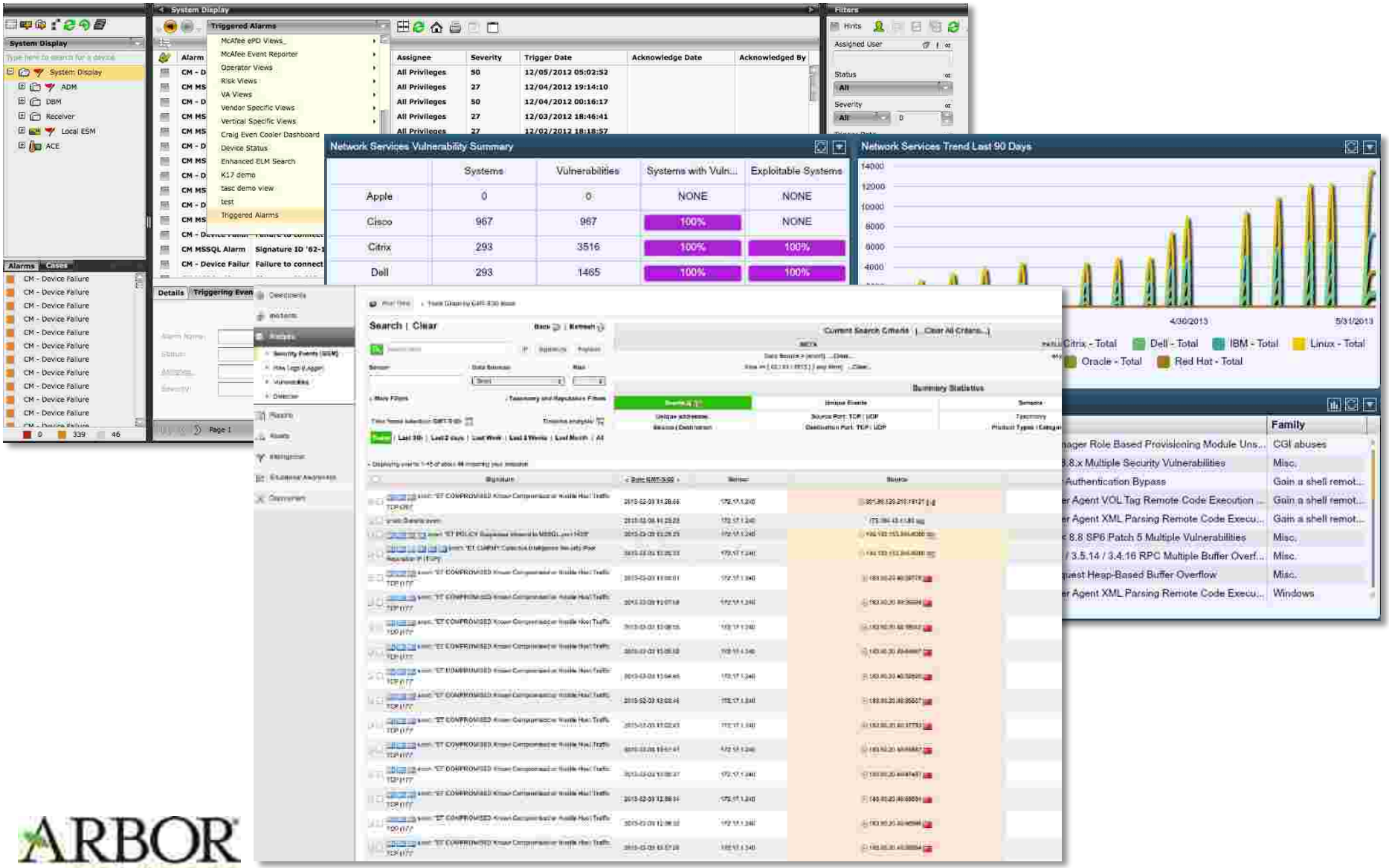
ARBOR NETWORKS

Source: 2013 Gartner, Inc and/or its affiliates. All rights reserved

Arbor Solution View

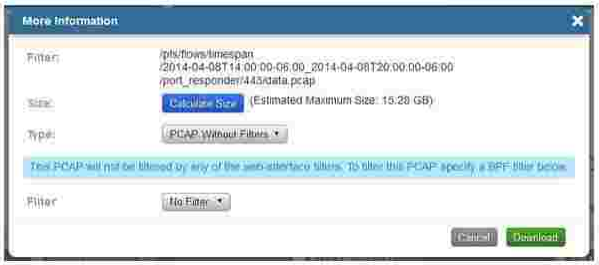


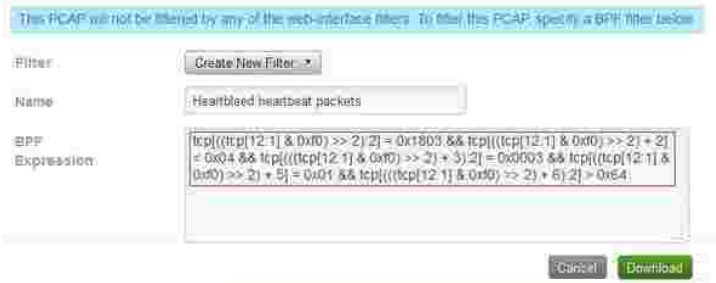
SIEM – Rows and Columns of Threats



ARBOR NETWORKS

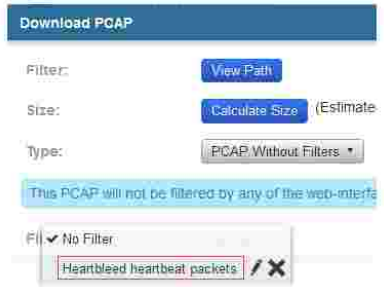
Finding a Zero-day Attack – the hard way



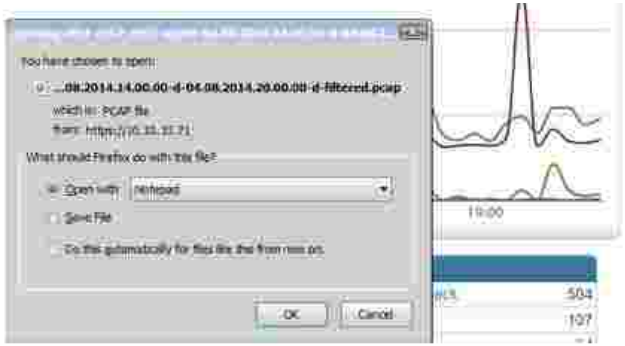


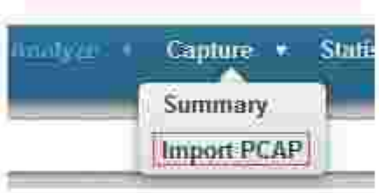
The BPF filter text is:

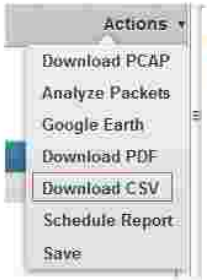
```
tcp[((tcp[12:1] & 0xf0) >> 2):2] = 0x1803 && tcp[((tcp[12:1] & 0xf0) >>
2) + 2] < 0x04 && tcp[((tcp[12:1] & 0xf0) >> 2) + 3:2] = 0x0003 &&
tcp[((tcp[12:1] & 0xf0) >> 2) + 5]
2) + 6):2] > 0x64
```

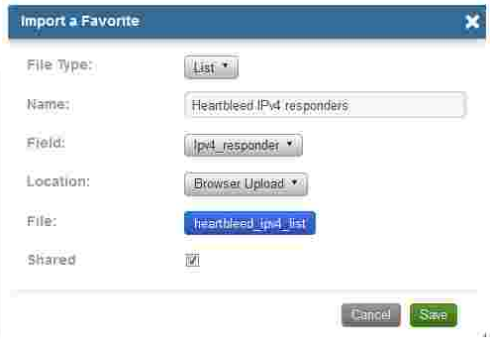


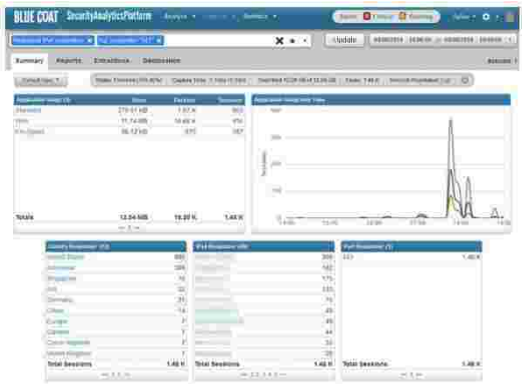
12 ‘Simple’ steps to find Heartbleed











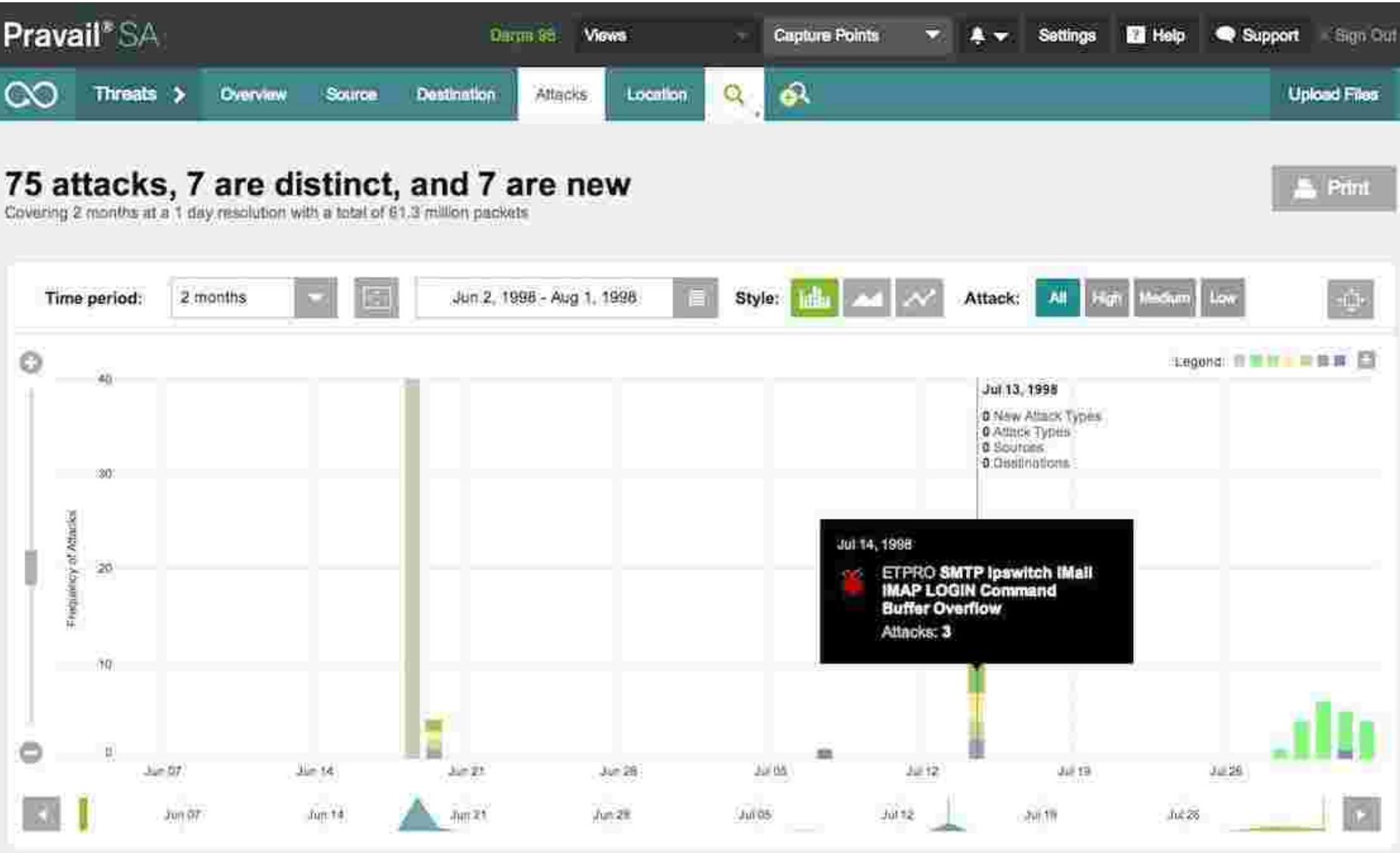
Enterprise-Wide Visibility

The Enterprise Visibility Needed To Secure the Network
"You Simply Can't Secure It if You Can't See It"

- *Detect* who is accessing your network, when and what they are doing.
- *Analyze* where your risks are and how to stop them.
- *Address* problems, armed with context and security intelligence

ARBOR NETWORKS

Attack Timelines is Critical



ARBOR NETWORKS

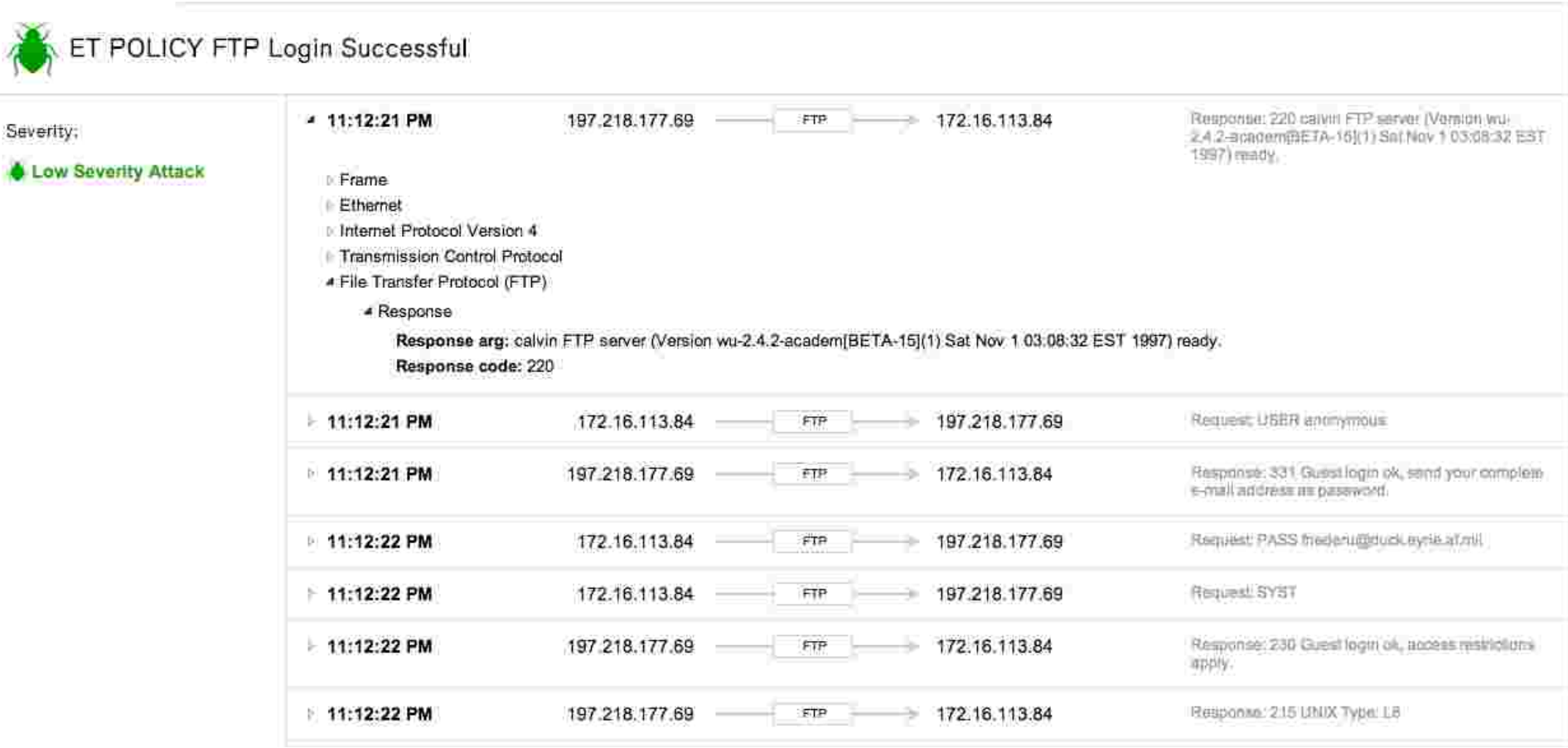
Zoom from months and years to seconds

IP Address and Port Details aren't enough

Time	S...	L...	Origin	A...	Source	Destination	Service	Rule	Policy Name	Description
26/Oct/2013 09:30:47			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
26/Oct/2013 09:33:04			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
20/Oct/2013 21:27:09			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
26/Oct/2013 09:37:30			GW-Nevada		10.2.29.177	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1
26/Oct/2013 09:37:23			GW-Nevada		10.2.29.177	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1
26/Oct/2013 09:37:11			GW-Nevada		10.6.20.54	10.9.190.53	UDP/138	2	my_policy1	Accepted on rule 2
26/Oct/2013 09:37:11			GW-Nevada		10.2.29.177	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1
26/Oct/2013 09:36:59			GW-Nevada		10.2.29.177	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1
26/Oct/2013 09:36:50			GW-Nevada		10.4.83.55	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1
20/Oct/2013 18:15:20			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
20/Oct/2013 22:18:54			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
19/Oct/2013 18:09:08			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
26/Oct/2013 08:02:02			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
21/Oct/2013 13:15:57			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
23/Oct/2013 21:28:29			GW-Nevada		10.6.20.54	10.11.186.54	TCP/80	4	my_policy1	Accepted on rule 4
26/Oct/2013 09:35:50			GW-Nevada		10.2.29.177	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1
26/Oct/2013 09:35:45			GW-Nevada		10.2.29.177	10.3.203.128	TCP/18192	1	my_policy1	Accepted on rule 1

ARBOR NETWORKS

Need to know Attacks details



ARBOR NETWORKS

Packet Capture or it didn't happen…..

- **Full Packet Capture is the richest source of data but it isn't BIG DATA**

- Contains **ALL** of the network data, and can be taken from **ANYWHERE** in the network via TAP or SPAN
- Can be processed whenever you like – years later or as a real time stream
- Security analytics content derived from each capture is cumulative, building a long running history of searchable and comparable attack data…**this is BIG DATA**
- Like CCTV for your network – Play, Pause and Rewind your data
- Enables base lining of metrics between data sets and trend comparison of different periods

ARBOR NETWORKS

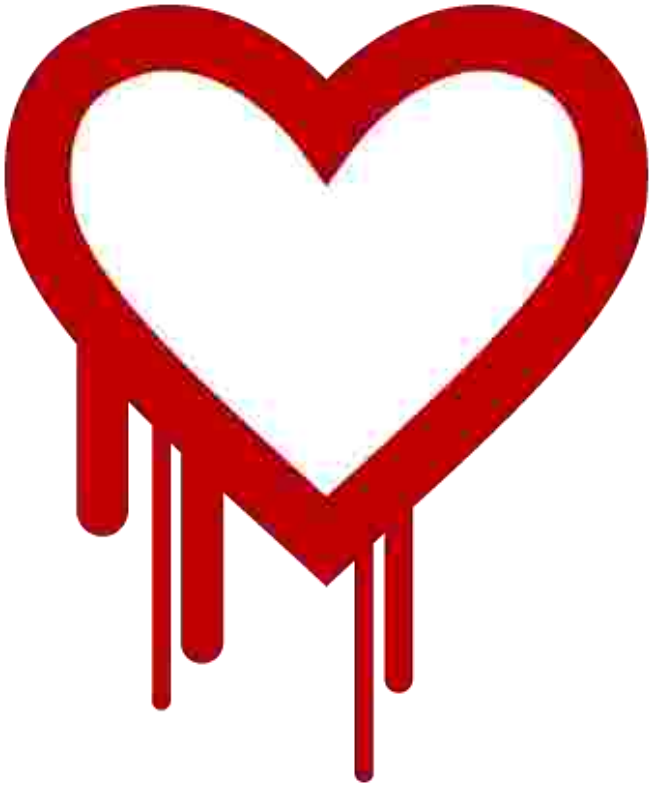
Learning from the Past

- Find out if an attacker used a zero day attack previously
- Find out what systems were compromised
- Find out what happened next?
  - What other systems were compromised laterally
  - What data was accessed
  - What data was exfiltrated
- Find out if the attacker is still active, still in your network
- Understand the effectiveness of existing controls
- Understand what new controls are required

ARBOR NETWORKS

Were you affected by Heartbleed?

- **So you have patched all your OpenSSL based systems. Is that it?**



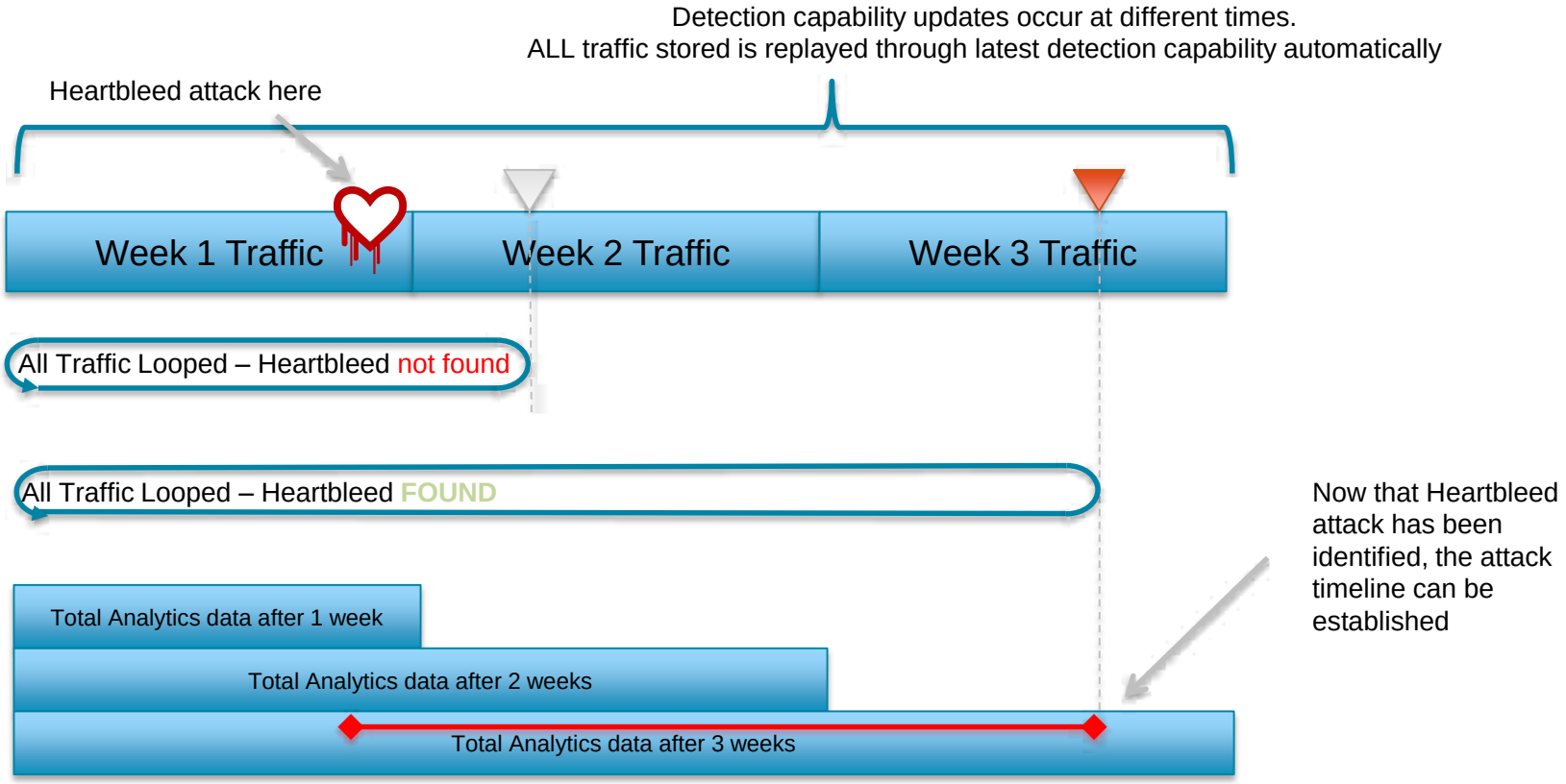
- Heartbleed could have been used against you before you applied the necessary updates, or even before the vulnerability became known to the public
- There are no application layer logs that would allow you to check if you were attacked or what data was stolen
- Any sensitive data stored in server memory could be disclosed to attacker
  - Private SSL keys
  - Unencrypted passwords
  - Business critical documents

ARBOR NETWORKS

Looping for Zero Day Attacks such as Heartbleed

Detection capability update but without signature for the Heartbleed attack

Detection capability update INCLUDING signature for the Heartbleed attack



ARBOR NETWORKS

Problem: Response-Driven Operations

- Security operations remains a passive, response-driven process
- Never enough resources to investigate & close every alert
  - Average enterprise SOC sees ~10,000 alerts per day
  - Splunk Enterprise Security app: 12,000 events per 1 Gbps of traffic

  - Avg. “dwell time” of targeted, advanced threatr continues to grow as teams chase too many events

Despite false positives, teams remain focused on these events – as opposed to FINDING THREATS

ARBOR NETWORKS

Problem: Slow Response & Decision Paralysis

- Once real incident identified, IR teams struggle to quickly get a clear view of the threat
  - Disparate data logs: SIEM, packet archives, event logs
  - Slow SIEM query response time that requires the analyst to specify exact data they want
  - Too many pie charts and event logs – as opposed to visually presenting data as trends and timelines
- Kill chain often delayed as teams seek information with little context to what happened pre/post event

ARBOR NETWORKS

Enterprises are adapting to these Challenges

Today's enterprise security leaders:

- ✓No longer rely on firewall, AV & IPS
- ✓Create "hunter" teams of their best security analysts
- ✓Apply big data analytics
- ✓Recognize that perimeter-dominated security no longer effective, so apply solutions that focus on network & host activity

ARBOR NETWORKS

Arbor Networks Assumptions

- There will never be enough budget
  - Technology should be “scalable”
- Defense in depth, best practices, & compliance aren’t getting it done
  - If you aren’t doing more than this bad things are already happening
- You have a skilled headcount problem, not just a CapX problem
- There are more networking people in the world than threat experts

ARBOR NETWORKS

Arbor Networks Product Strategy

- Leverage netflow, packet capture, & inline capability for broad visibility
  - Prevent, Detect, Respond
- Put the power back in the hands of the analysts
  - Network & Threat Visibility
  - Incident Response Workflow
- Technology should enable personnel & process investment
  - Regardless of how many you have
  - Or skillset

ARBOR NETWORKS

ARBOR NETWORKS

Thank You