Catching Breaches with NBAD

Charles Herring
@charlesherring
http://f15hb0wn.com
CHerring@Lancope.com

Agenda

- Definitions
- NBAD Specific Detection Approaches
- Example Breaches

Overview - Definitions

- What is NBAD?
- What is NetFlow?
- Detection Schools

What is NBAD?

- Network Behavioral Anomaly Detection
- Data source = Network MetaData (NetFlow)
- Probe locations = Core or deeper
- Quantity/Metric Centric (not Pattern/Signature Centric)
- Sometimes used to refer to NetFlow Security Tools

OSS NBAD - SiLK/PySiLK

```
# Import the global variables needed for processing the record
global smtpports, counts

# Pull data from the record
sip = rec.sip
bytes = rec.bytes

# Get a reference to the current data on the IP address in question
data = counts.setdefault(sip, [0, 0])

# Update the total byte count for the IP address
data[0] += bytes

# Is the flow mail related?  If so add the byte count to the mail bytes
if (rec.protocol == 6 and rec.sport in smtpports and
    rec.packets > 3 and rec.bytes > 120):
    data[1] += bytes
    return True

# If not mail related, fail the record
return False
```

Commercial Solutions

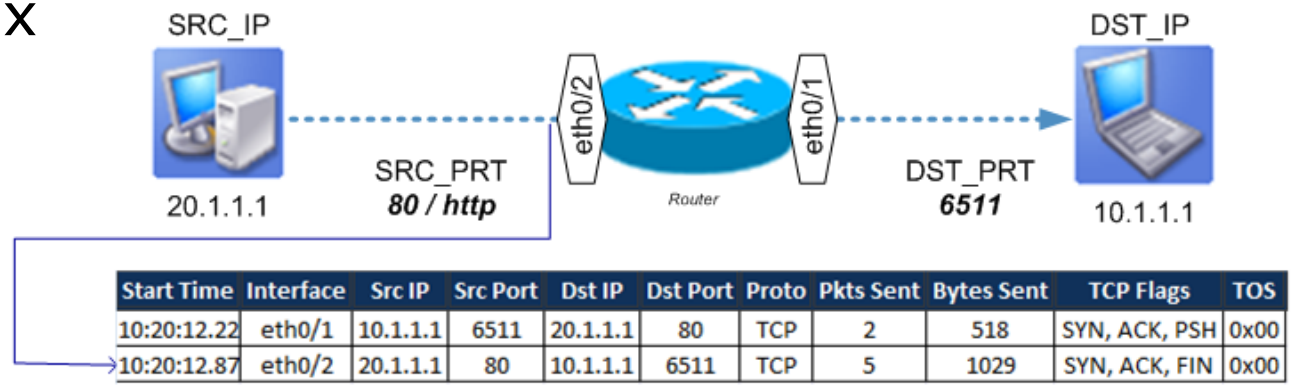
- Arbor PeakFlow
- IBM Qradar
- Invea-Tech FlowMon
- Lancope StealthWatch
- ManageEngine
- McAfee NTBA
- Plixer Scrutinizer
- ProQSys FlowTraq
- Riverbed Cascade (formerly Mazu)

* For comparison see Gartner Network Behavior Analysis Market December 2012 (G00245584)

Network Logging Standards

- NetFlow v9 (RFC-3950)
- IPFIX (RFC-5101)
- Rebranded NetFlow
  - Jflow – Juniper
  - Cflowd – Juniper/Alcatel-Lucent
  - NetStream – 3Com/Huawei
  - Rflow – Ericsson
  - AppFlow - Citrix

Basic/Common Fields



Start Time	Interface	Src IP	Src Port	Dst IP	Dst Port	Proto	Pkts Sent	Bytes Sent	TCP Flags	TOS
10:20:12.22	eth0/1	10.1.1.1	6511	20.1.1.1	80	TCP	2	518	SYN, ACK, PSH	0x00
10:20:12.87	eth0/2	20.1.1.1	80	10.1.1.1	6511	TCP	5	1029	SYN, ACK, FIN	0x00

Detection Methods

- **Signature** = Inspect Object against blacklist
  - IPS
  - Antivirus
  - Content Filter
- **Behavioral** = Inspect Victim behavior against blacklist
  - Malware Sandbox
  - NBAD/UBAD
  - HIPS
  - SEIM
- **Anomaly** = Inspect Victim behavior against whitelist
  - NBAD/UBAD

Comparison of Detection Methods

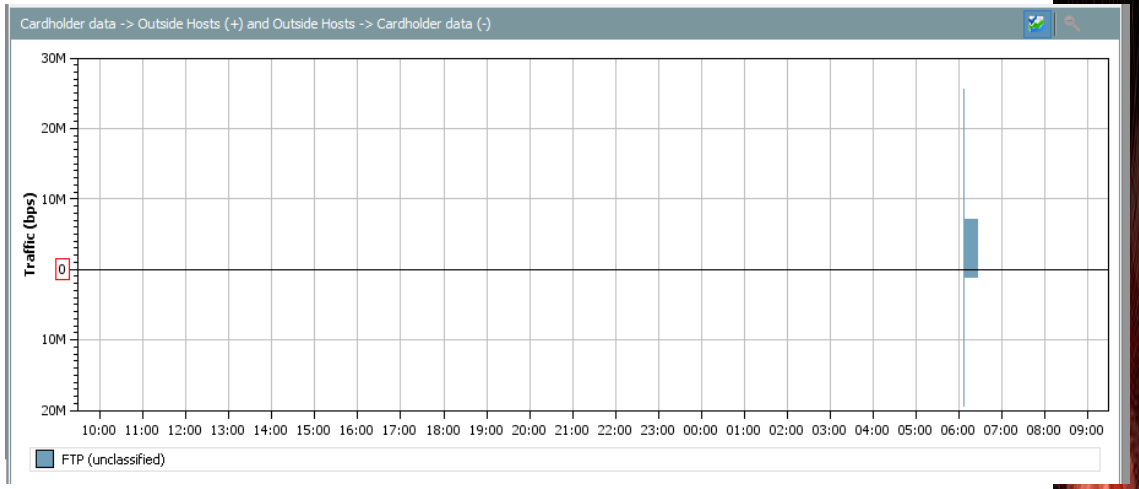
	Signature	Behavior	Anomaly
Known Exploits	**Best**	Good	Limited
0-Day Exploits	Limited	**Best**	Good
Credential Abuse	Limited	Limited	**Best**

Overview – NBAD Detection Approaches

- Signature
- Behavioral
- Anomaly

NBAD Detection - Signature

- Segmentation Enforcement
- Policy Violations
- C&C Connections



Apr 20, 2014 11:56:00 AM (14 minutes 6s ago)	Bot Infected Host - Successful C&C Activity	10[redacted]	Atlanta, Sales and Marketing, Desktops, Windows, PCI Unauthorized		web8.r01.ru (195[redacted])	Russian Federation, Blackenergy	Successful communication was detected between this inside host and C&C server using port 80 and the TCP protocol, and http://xa[redacted]/stat.php.

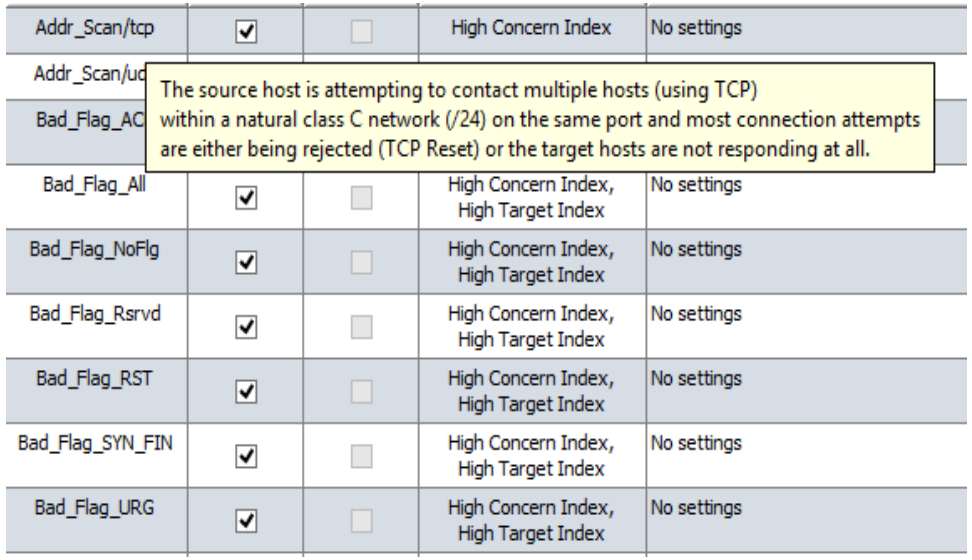
- **Pro's**: Certainty can be established; Easy to set up; Deep visibility (without probes)
- **Con's**: Only detects "Known Threats"

Boolean Detection

- Requires understanding of “bad” scenario
- Dependent on reliable (non-compromised) data sources
- Data sources rely on signature (known bad) detection
- NetFlow usage limited to communication tracking

NBAD Detection - Behavioral

- Scanning
- SYN Flood
- Flag Sequences



Addr_Scan/tcp	☑	☐	High Concern Index	No settings
Addr_Scan/ud				
Bad_Flag_AC				
Bad_Flag_All	☑	☐	High Concern Index, High Target Index	No settings
Bad_Flag_NoFlg	☑	☐	High Concern Index, High Target Index	No settings
Bad_Flag_Rsrvd	☑	☐	High Concern Index, High Target Index	No settings
Bad_Flag_RST	☑	☐	High Concern Index, High Target Index	No settings
Bad_Flag_SYN_FIN	☑	☐	High Concern Index, High Target Index	No settings
Bad_Flag_URG	☑	☐	High Concern Index, High Target Index	No settings

The source host is attempting to contact multiple hosts (using TCP) within a natural class C network (/24) on the same port and most connection attempts are either being rejected (TCP Reset) or the target hosts are not responding at all.

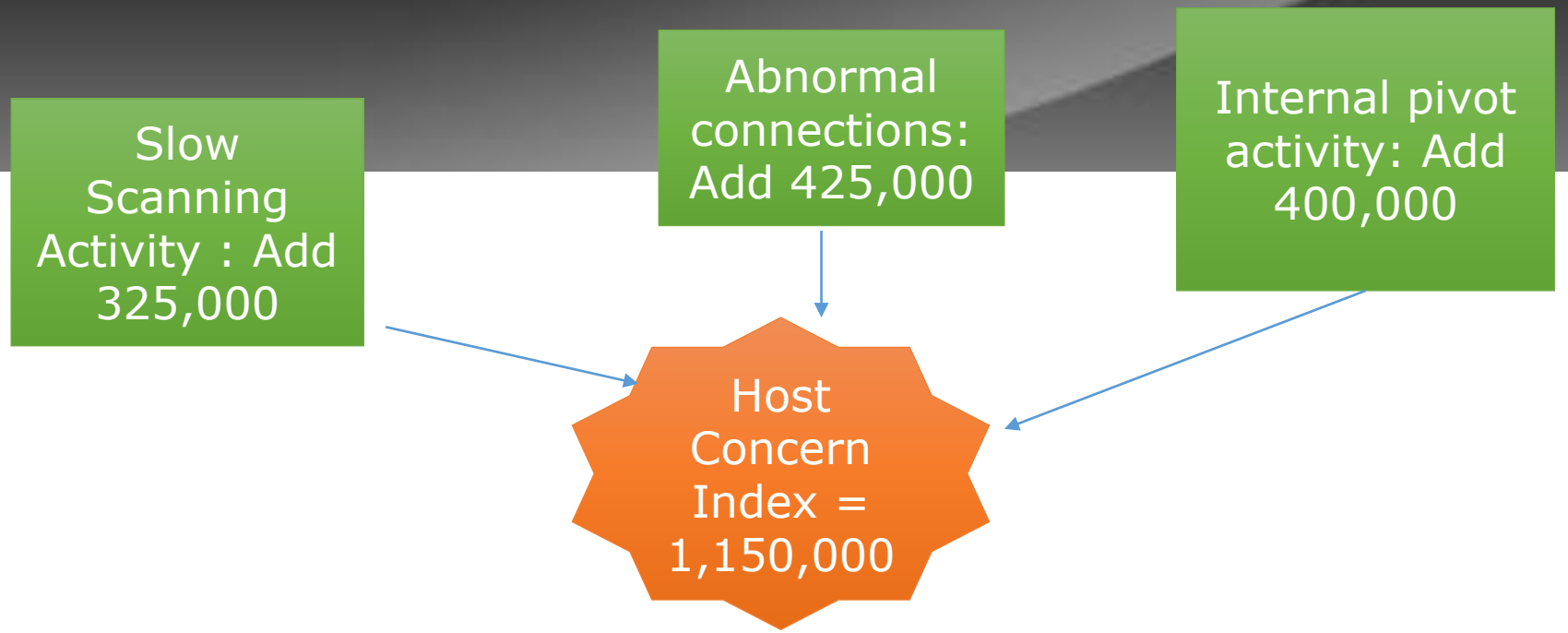
- **Pro's**: Doesn't need to know exploit
- **Con's**: Must establish host counters

NBAD Detection – Anomaly

- **Pro's**: Can Catch Sophisticated/Targeted/Unknown Threats

- **Con's**:
  - Requires Host and User Profiles
  - Requires Specific Baselines/Policies
  - Output requires interpretation
  - Requires massive data collection/processing
  - Requires Algorithmic Calculation

Algorithmic Detection



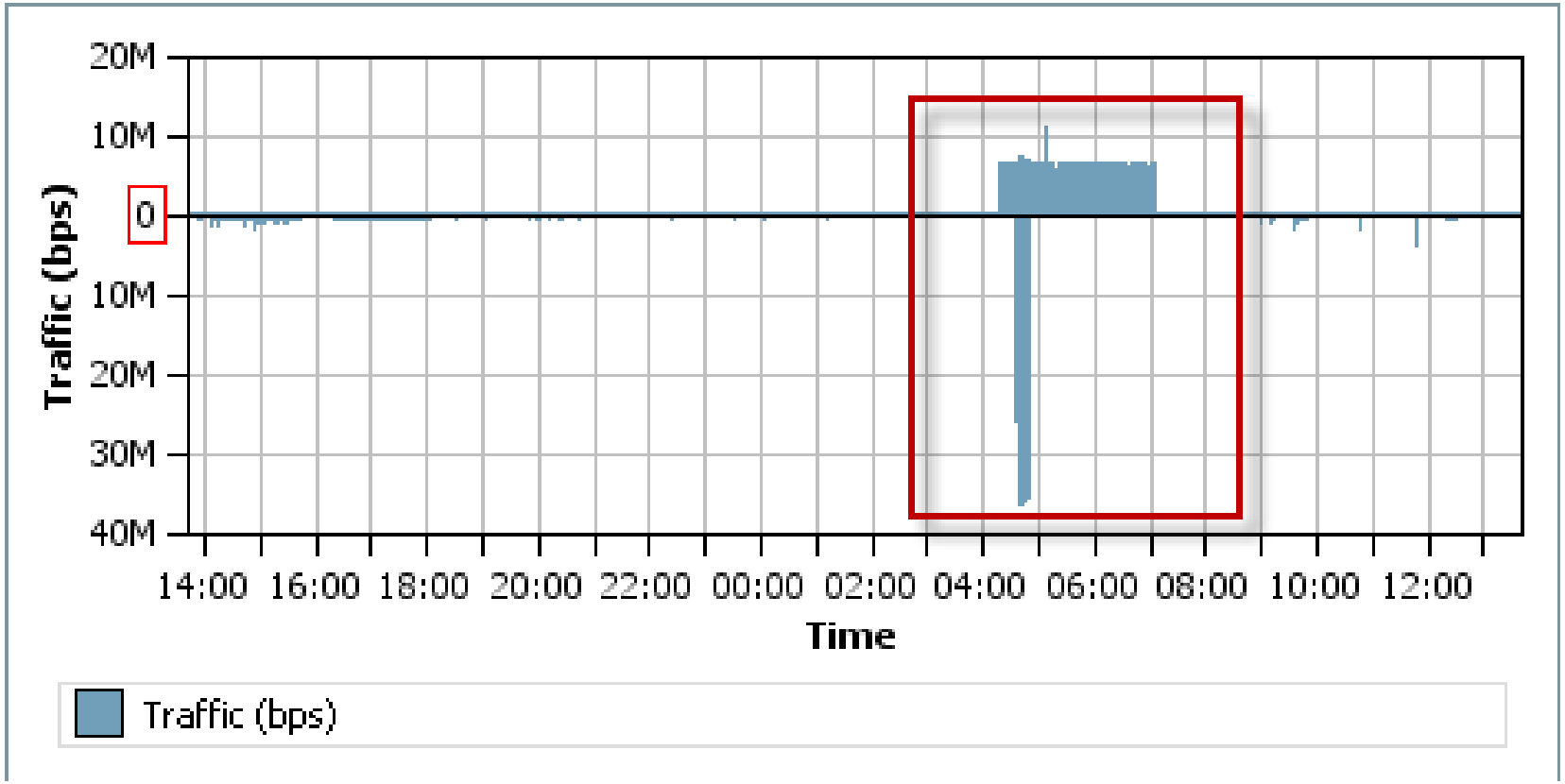
- Based on knowing normal
- Dependent on raw NetFlow MetaData (multiple sources)
- Does not require understanding of attack
- Output is security indices focused on host activity

NBAD Detection – Anomaly Types

- Service Traffic Threshold Anomaly
- Service Type Anomaly
- Geographic Traffic Anomaly
- Time of Day Anomaly
- Geographic User Anomaly
- Data Hoarding
- Data Disclosure

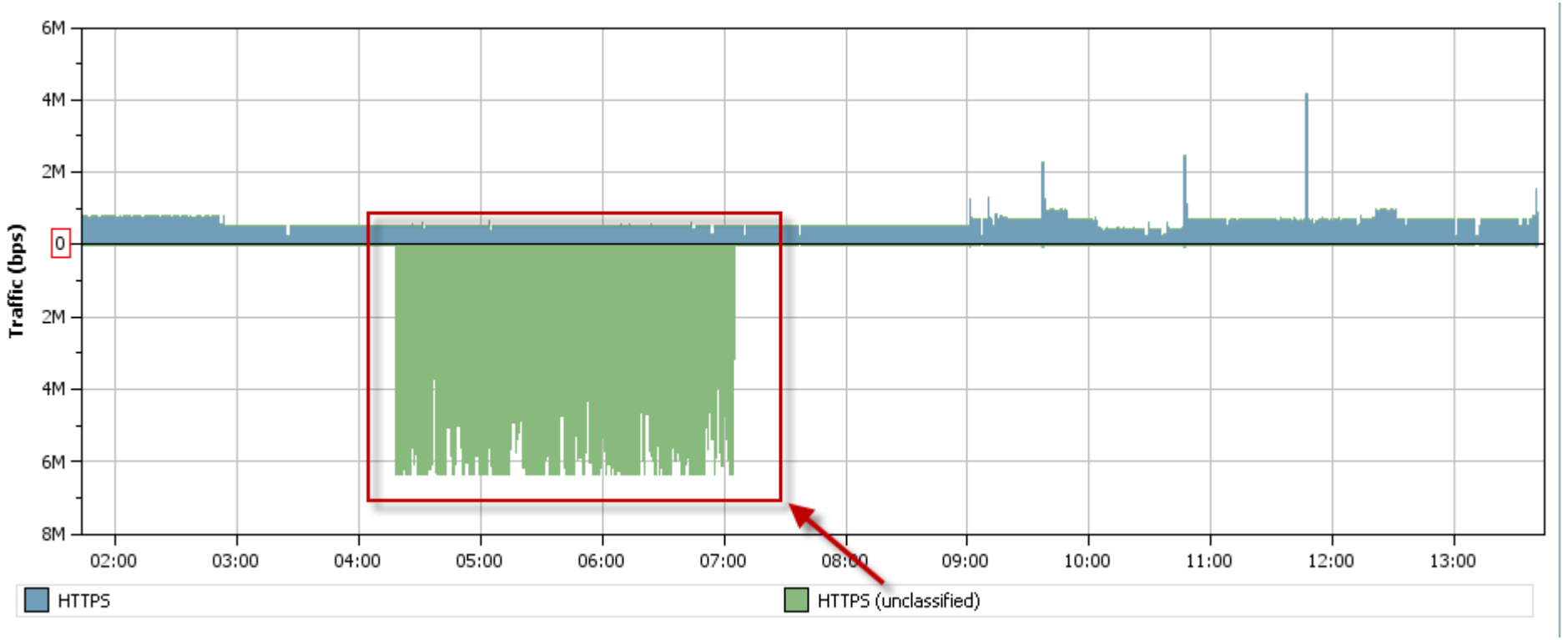
NBAD Detection - Anomaly

- Service Traffic Threshold Anomaly



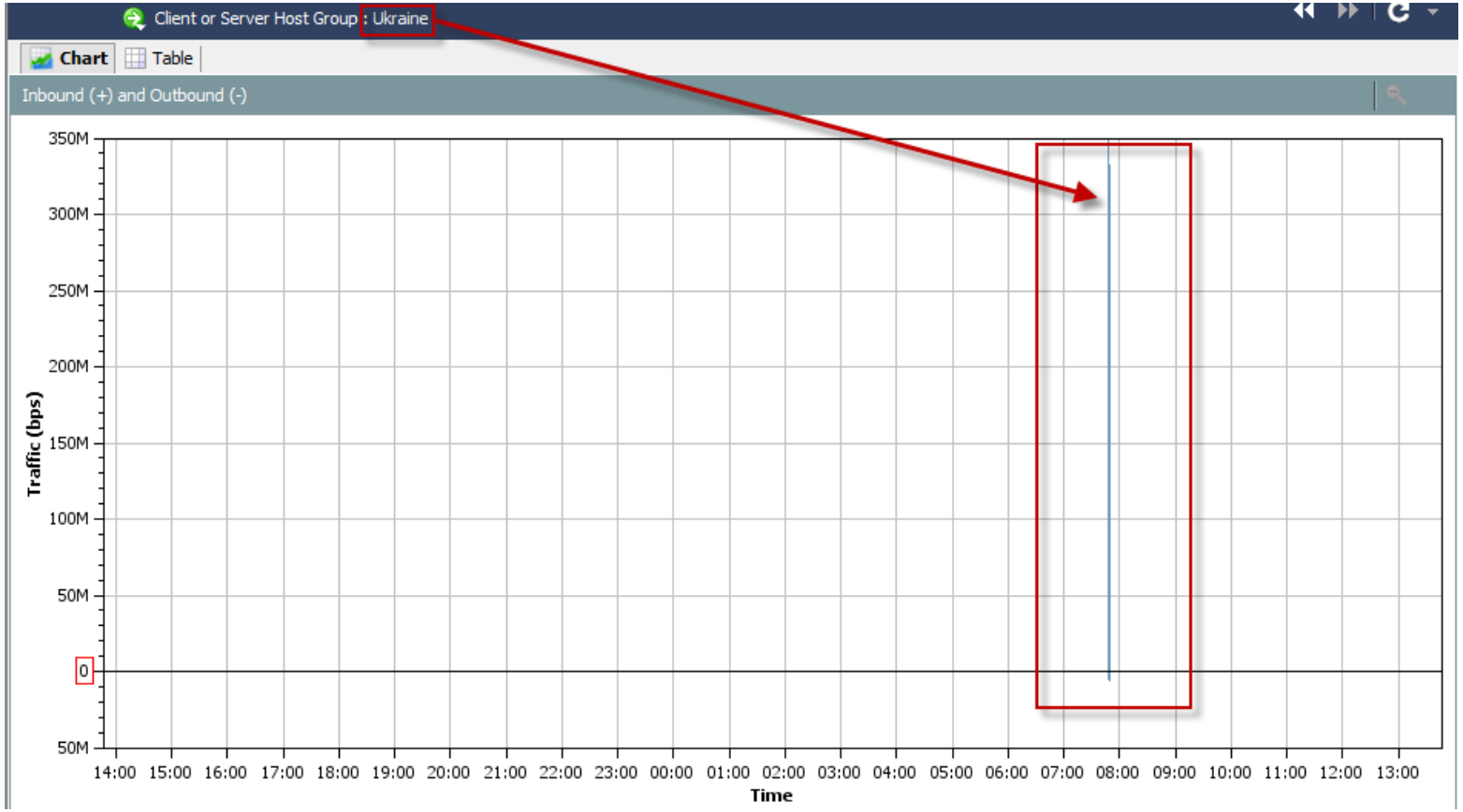
NBAD Detection - Anomaly

- Service Type Anomaly



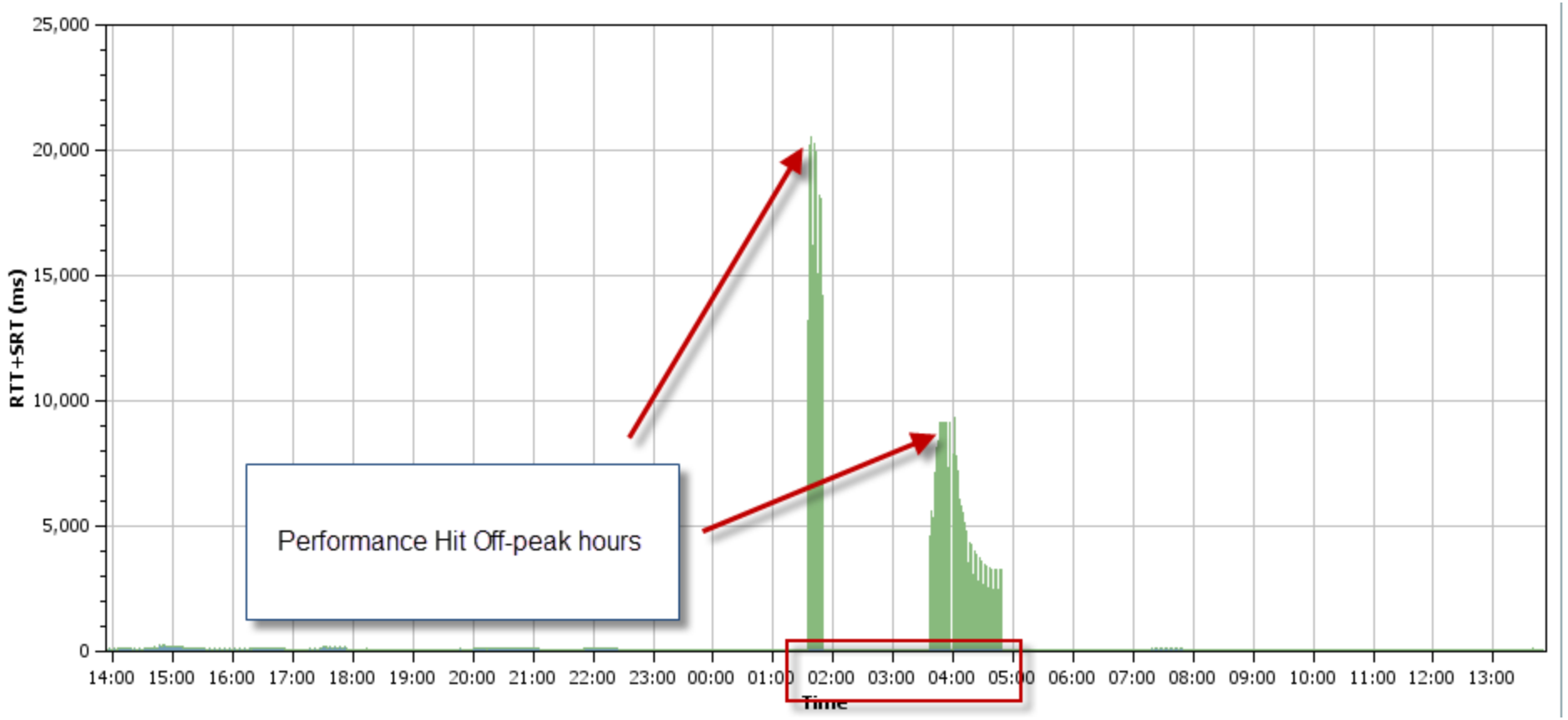
NBAD Detection - Anomaly

- Geographic Traffic Anomaly



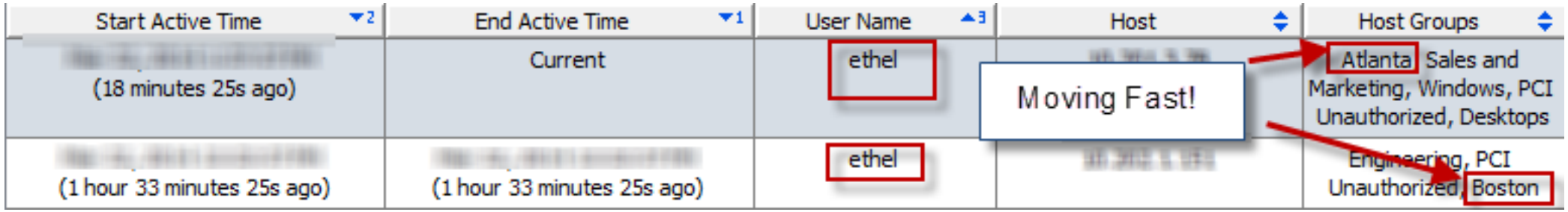
NBAD Detection - Anomaly

- Time of Day Anomaly



NBAD Detection - Anomaly

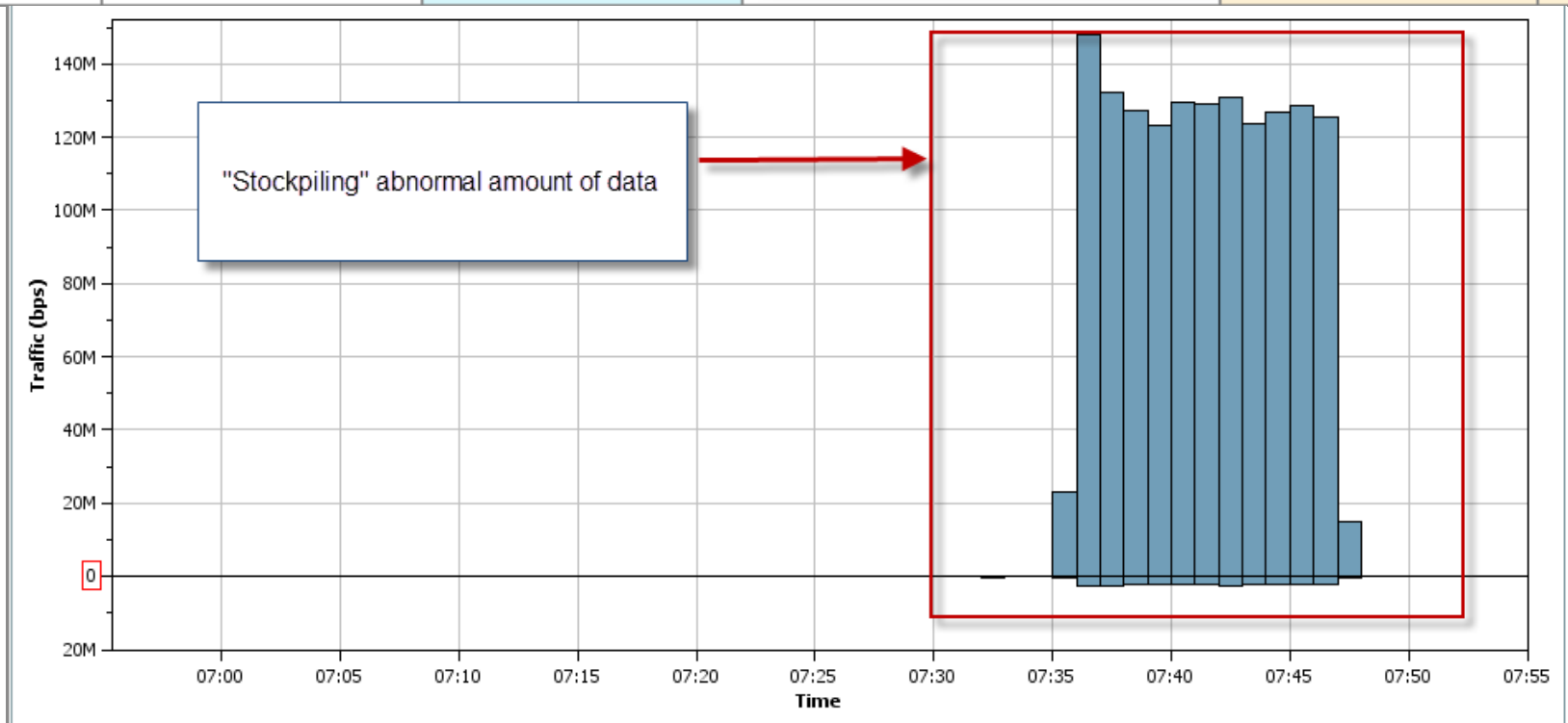
- Geographic User Anomaly



NBAD Detection - Anomaly

- Data Hoarding

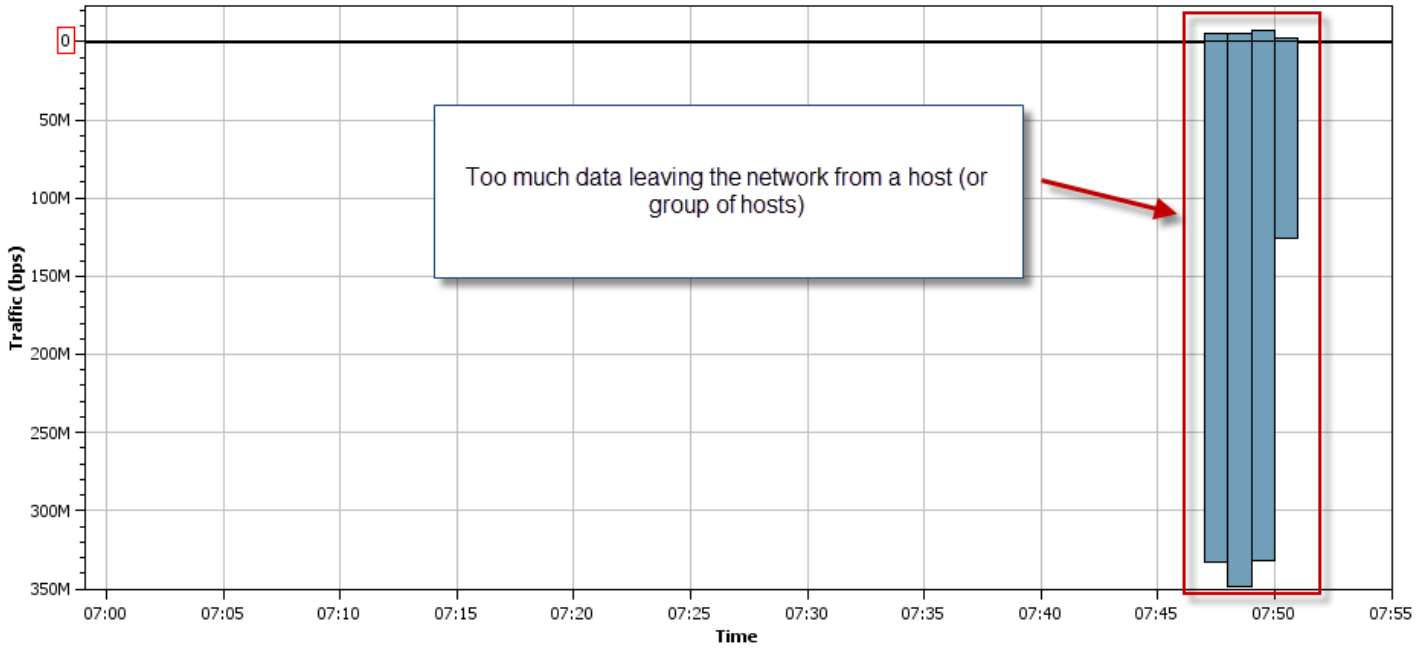
(6 hours 12 minutes 55s ago)	Suspect Data Hoarding	10.252.	Observed 10.9G bytes. Policy maximum allows up to 100M bytes.		Multiple Hosts



NBAD Detection - Anomaly

- Data Disclosure

[redacted] (6 hours 15 minutes 55s ago)	Suspect Data Loss	10.252.[redacted]	Observed 8.35G bytes. Policy maximum allows up to 500M bytes.



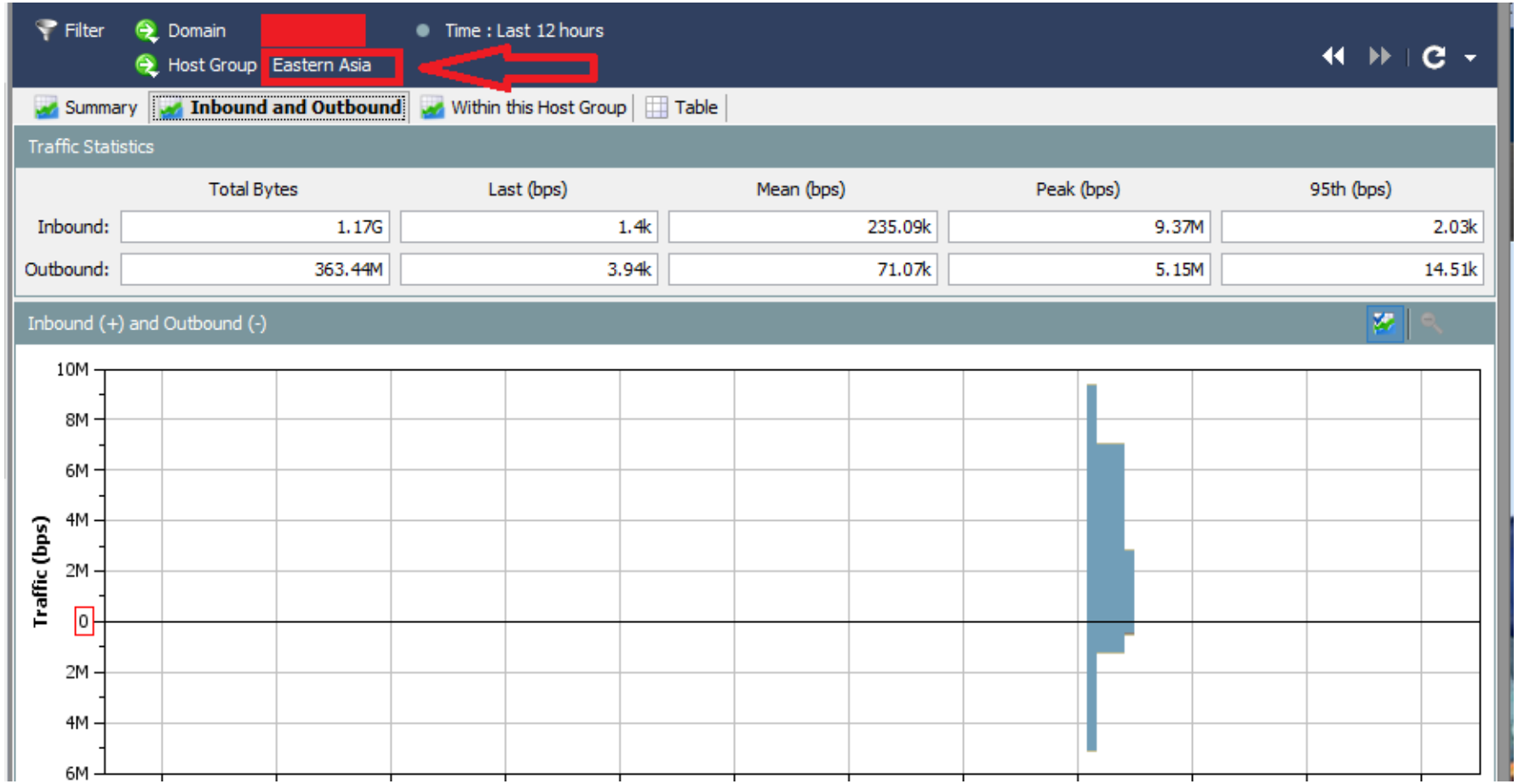
Overview – Specific NBAD Breaches

- Health Care vs. State Sponsored
- State/Local Government vs. Organized Crime
- Agriculture vs. State Sponsored
- Higher Education vs. State Sponsored
- Manufacture vs. Activists

Patient Data to East Asia

- **Victim Vertical**: Healthcare
- **Probable Assailant**: State Sponsored
- **Objective**: Theft of patient healthcare records
- **Motivation**: Geopolitical/Martial
- **Methodology**:
  - Keylogging Malware
  - Configuration change of infrastructure
- **NBAD Type**: Enforcement Monitoring

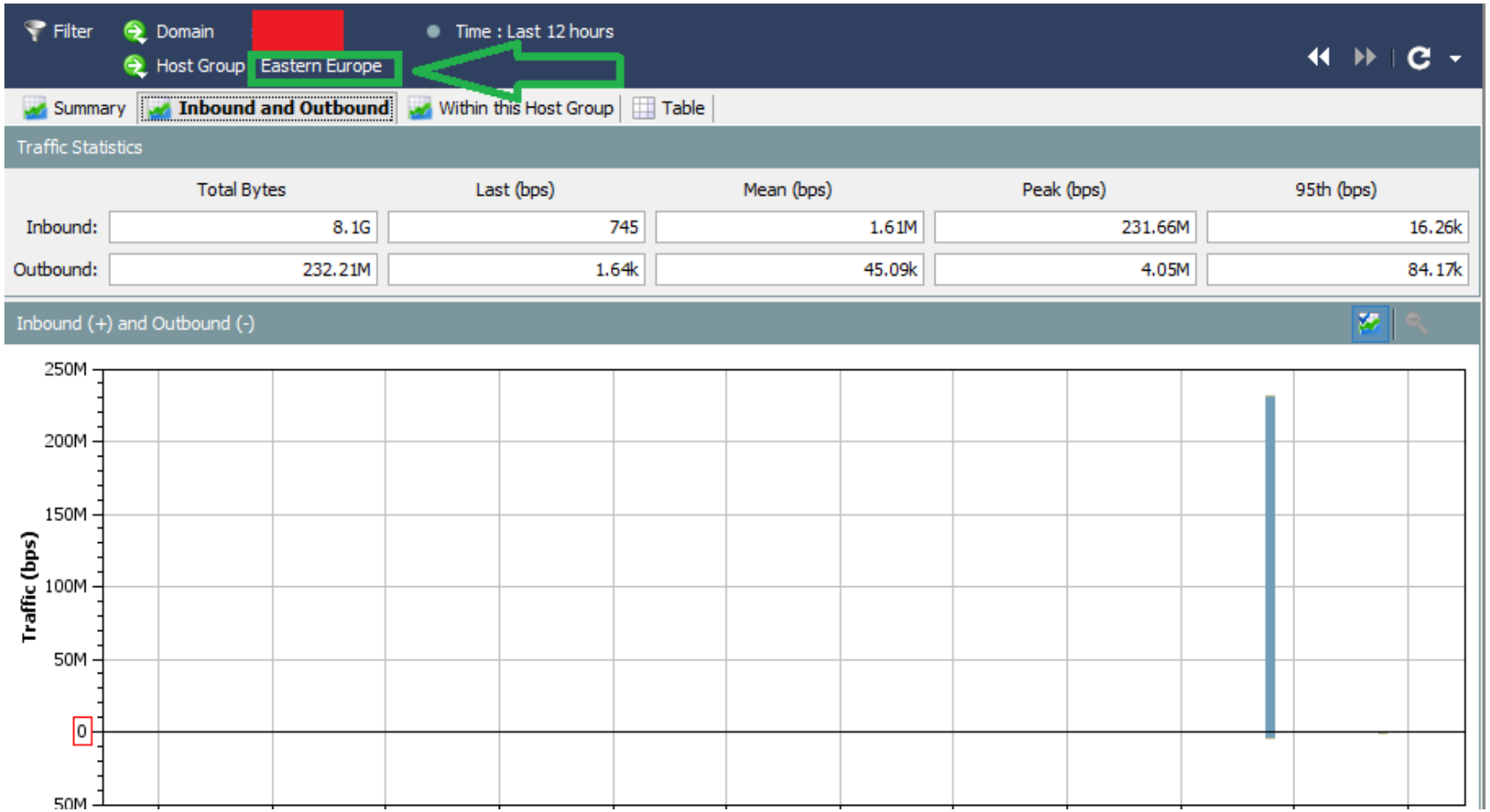
Geographical Anomaly



Cardholder Data to East Europe

- **Victim Vertical**: State/Local Government
- **Probable Assailant**: Organized Crime
- **Objective**: Theft of cardholder data
- **Motivation**: Profit
- **Methodology**:
  - Coldfusion exploit of payment webserver
  - Recoded Application
  - Staged data on server; uploaded to East Europe FTP server
- **NBAD Type**:
  - Geographic Anomaly
  - Traffic Anomaly

Geographical Traffic Anomaly



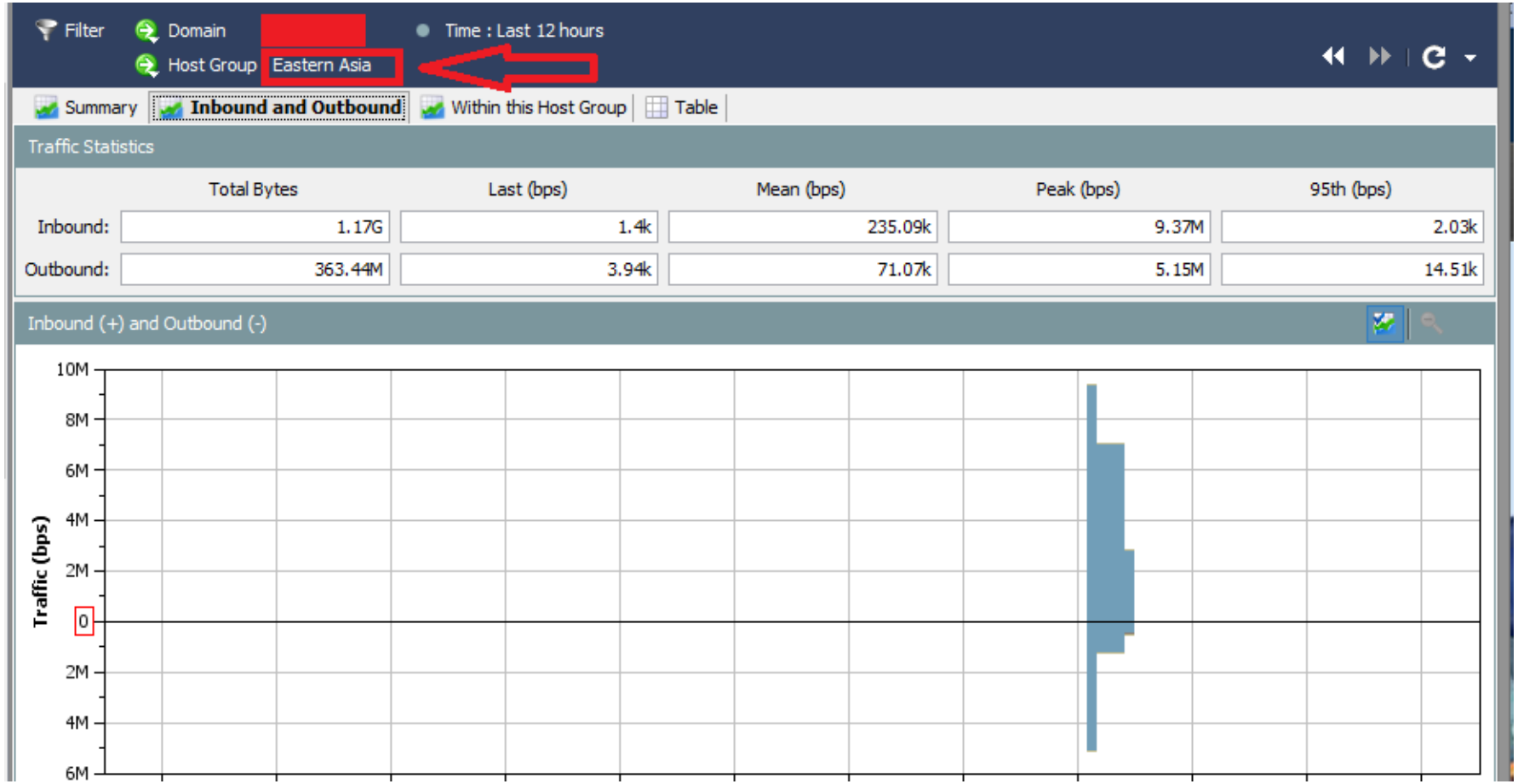
Intellectual Property to East Asia

- **Victim Vertical**: Agriculture
- **Probable Assailant**: State Sponsored
- **Objective**: Theft of food production IP
- **Motivation**: Profit/National Competition
- **Methodology**:
  - Spearphish of administrator
  - Pivot via VPN
  - Pivot via monitoring servers
  - Direct exfiltration
- **NBAD Type**:
  - Geographic Traffic Anomaly
  - Geographic User Anomaly
  - Traffic Anomaly

Recon from Monitoring Servers

Target Host	Concern Index ▼1	Security Events
10. [redacted]	2,885,766	Addr_Scan/tcp-445(5766)
10.	2,852,699	Addr_Scan/tcp-445(5699)
10.	2,822,644	Addr_Scan/tcp-445(5644)
10.	2,816,622	Addr_Scan/tcp-445(5622)
10.	2,804,603	Addr_Scan/tcp-445(5603)
10.	2,783,558	Addr_Scan/tcp-445(5558)
10.	2,774,549	Addr_Scan/tcp-445(5549)
10.	2,774,538	Addr_Scan/tcp-445(5538)
10.	1,827,655	Addr_Scan/tcp-445(3655)

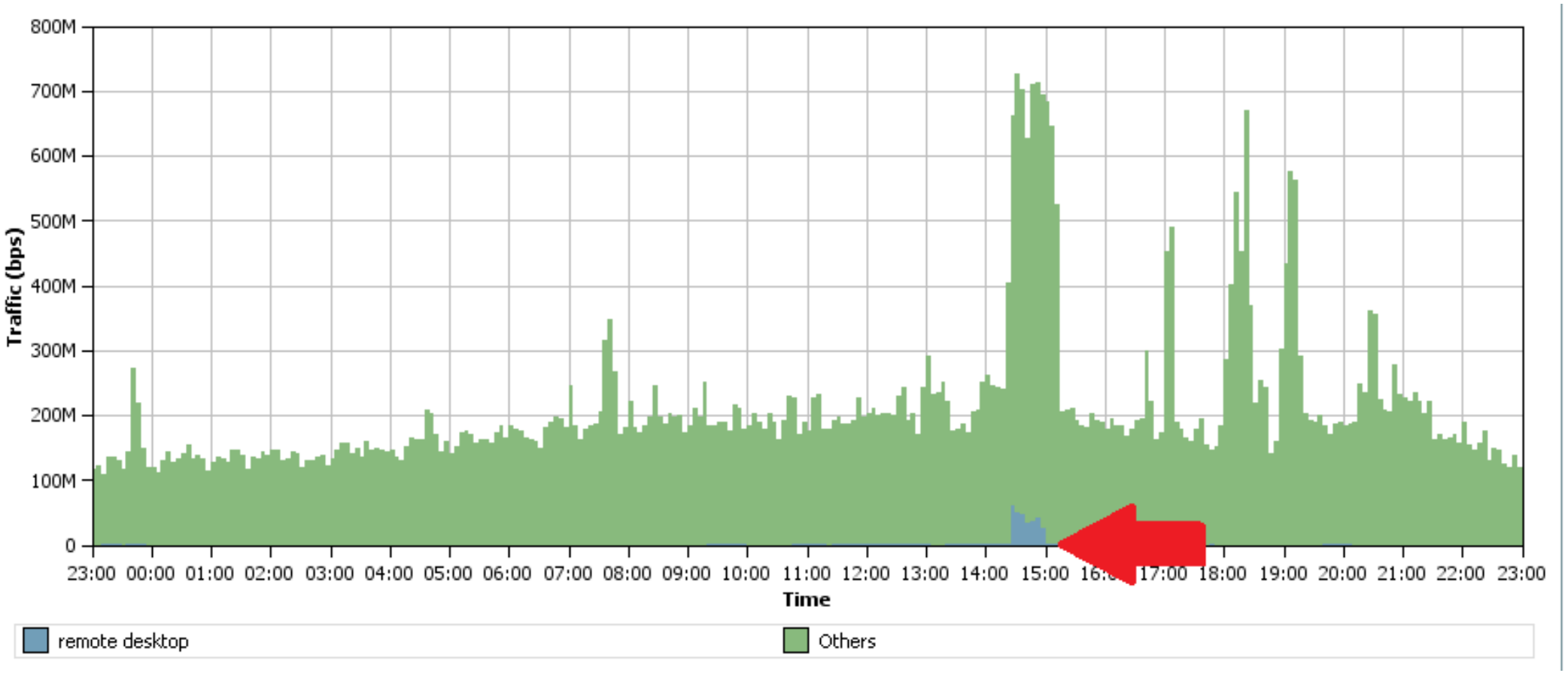
Geographical Anomaly



Theft of Research Data

- **Victim Vertical**: Higher Education
- **Probable Assailant**: State Sponsored
- **Objective**: Theft sensitive research data
- **Motivation**: Geopolitical/Martial
- **Methodology**:
  - Direct access to exposed RDP Servers
  - Bruteforce of credentials
- **NBAD Type**:
  - Service Traffic Anomaly
  - Geographic Traffic Anomaly

Traffic Anomaly



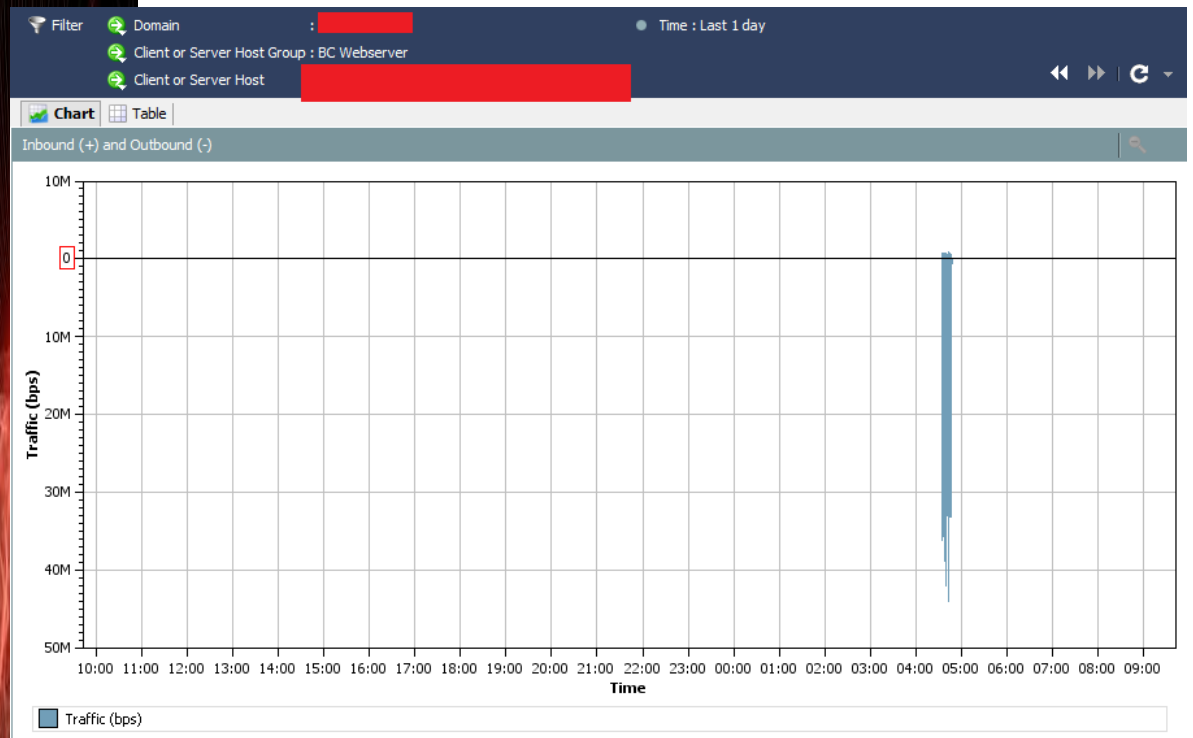
Theft of Customer Data

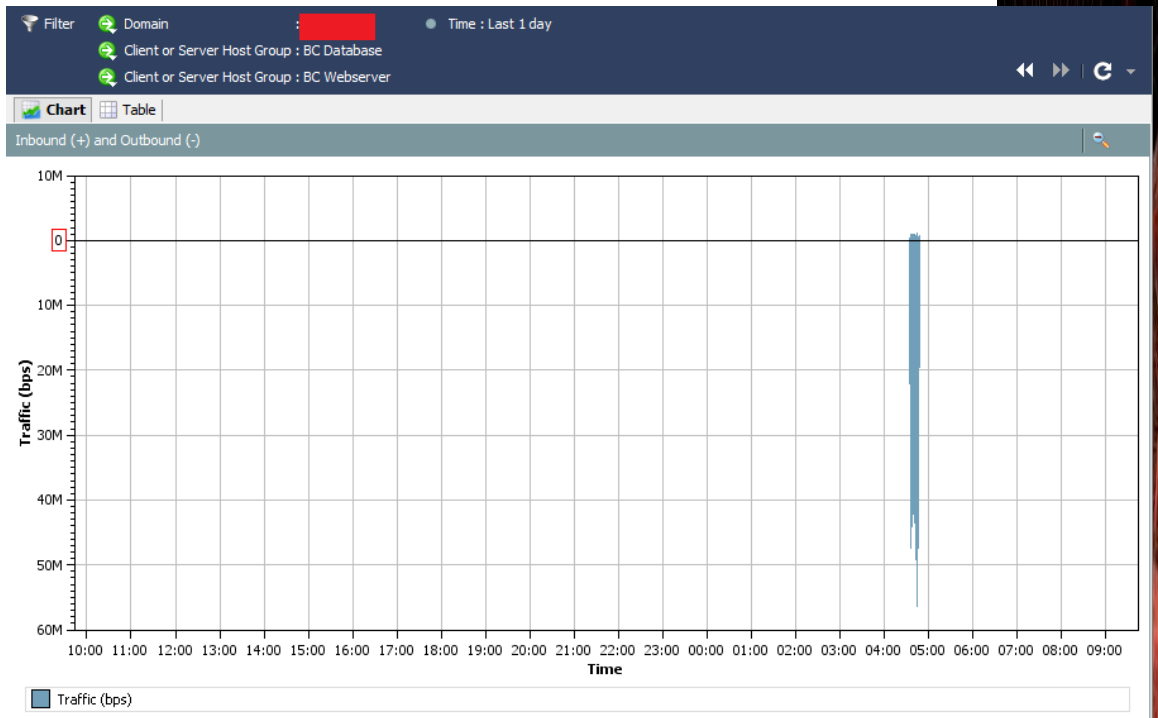
- **Victim Vertical**: Manufacturing
- **Probable Assailant**: Activist
- **Objective**: Publish stolen customer data
- **Motivation**: Embarrassing Victim
- **Methodology**:
  - SQL Injection to Customer Portal
- **NBAD Type**:
  - Recon detection
  - Traffic Anomaly to Internet
  - Traffic Anomaly to Webserver from DB

Recon before SQLi

Target Host ▲2	Concern Index ▼3	Security Events ▲1
21[redacted]/24	285,576	Addr_Scan/tcp-443(576), Addr_Scan/tcp-443(576)
21[redacted]/24	246,500	Addr_Scan/tcp-80(500), Addr_Scan/tcp-80(500)
21[redacted]/24	691,392	Ping_Scan(1392), Ping_Scan(1392)

Anomalous Data Exfiltration





Catching Breaches with NBAD

Questions?

Charles Herring
@charlesherring
http://f15hb0wn.com
CHerring@Lancope.com