



ADVANCED THREAT DETECTION AND FORENSICS VIA NETFLOW/IPFIX

Charles Herring

@charlesherring

cherring@lancope.com

<http://f15h.co>



FLOW CONCEPTS



Network Logging Basics

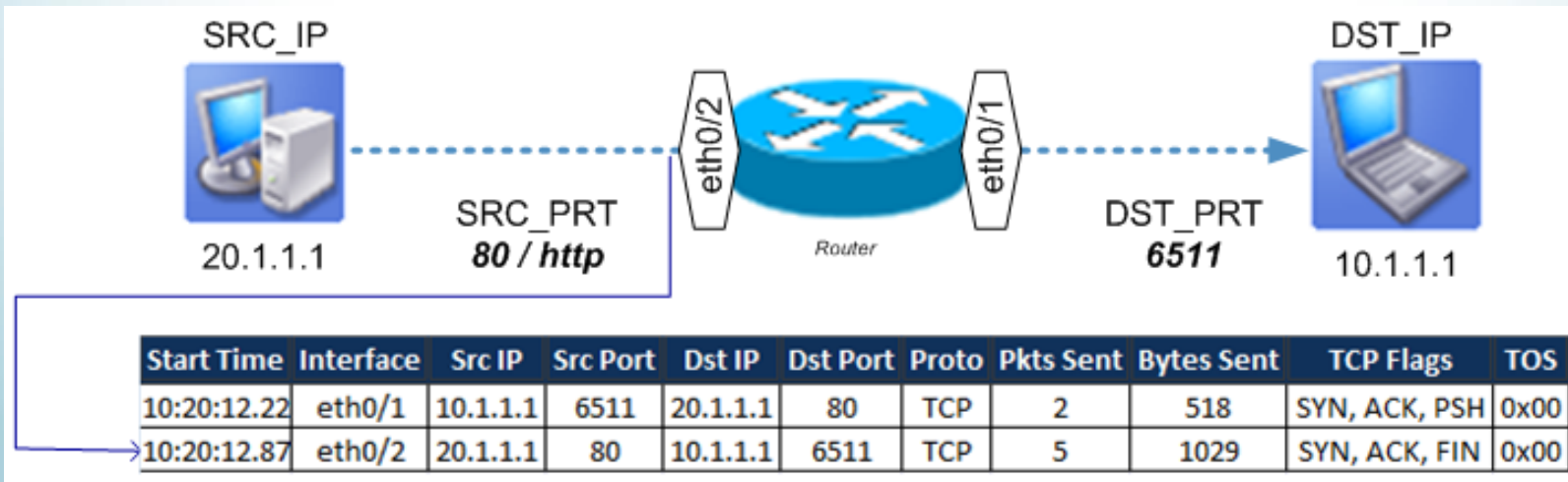
- A record; not a sample
- Can only log available data
- Unidirectional in nature
- Interface specific
- “Phone record” not “Phone tap”
- Category called “NetFlow” or “Flow”
- Devices with one or more Flow producing interfaces are “Exporters”
- Exporters cache and forward records to “Collectors”
- Bandwidth of “basic” Flow export is ~0.1% of monitored traffic



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



Extensible Data Fields



Data sources can provide additional log information

Examples of Extensible Fields

- Network Based Application Recognition
- Performance Metrics (SRT/RRT, Collisions)
- HTTP Headers
- NAT Data
- Security Action (Permit/Deny)
- TTL
- DSCP
- Payload

Packet Capture of IPFIX



```
[-] CISCO NETFLOW/IPFIX
  Version: 10
  Length: 1412
  [+]  
  Timestamp: Nov 6, 2012 08:15:23.000000000 Central Standard Time
  FlowSequence: 1310926
  Observation Domain Id: 22086
  [-] Set 1
    FlowSet Id: (Data) (335)
    FlowSet Length: 608
    [-] Flow 1
      [+]  
      [Duration: 0.000000000 seconds]
      System Init Time: Oct 30, 2012 23:52:35.523000000 Central Daylight Time
      SrcAddr: 74.207.227.45 (74.207.227.45)
      DstAddr: 216.83.162.167 (216.83.162.167)
      SrcPort: 42101
      DstPort: 443
      Source Mac Address: Cisco_00:00:10 (00:08:a4:00:00:10)
      Post Destination Mac Address: Cisco_00:00:06 (00:18:ba:00:00:06)
      Octets: 44
      Packets: 1
      InputInt: 1059
      OutputInt: 1079
      Protocol: 6
      TCP Flags: 0x02
      Vlan Id: 0
      MPLS-Label1: 0 exp-bits: 0
      MinTTL: 49
      IP ToS: 0x00
      Enterprise Private entry: (LANcopel, Inc.) Type 29794: value (hex bytes): 00
      Total TCP syn: 1
      Total TCP ack: 0
      Total TCP fin: 0
      Total TCP rst: 0
```

Stitching & De-duplication



Quick View for Flow

General **Interfaces** Table

Client Exporters IP (IF)

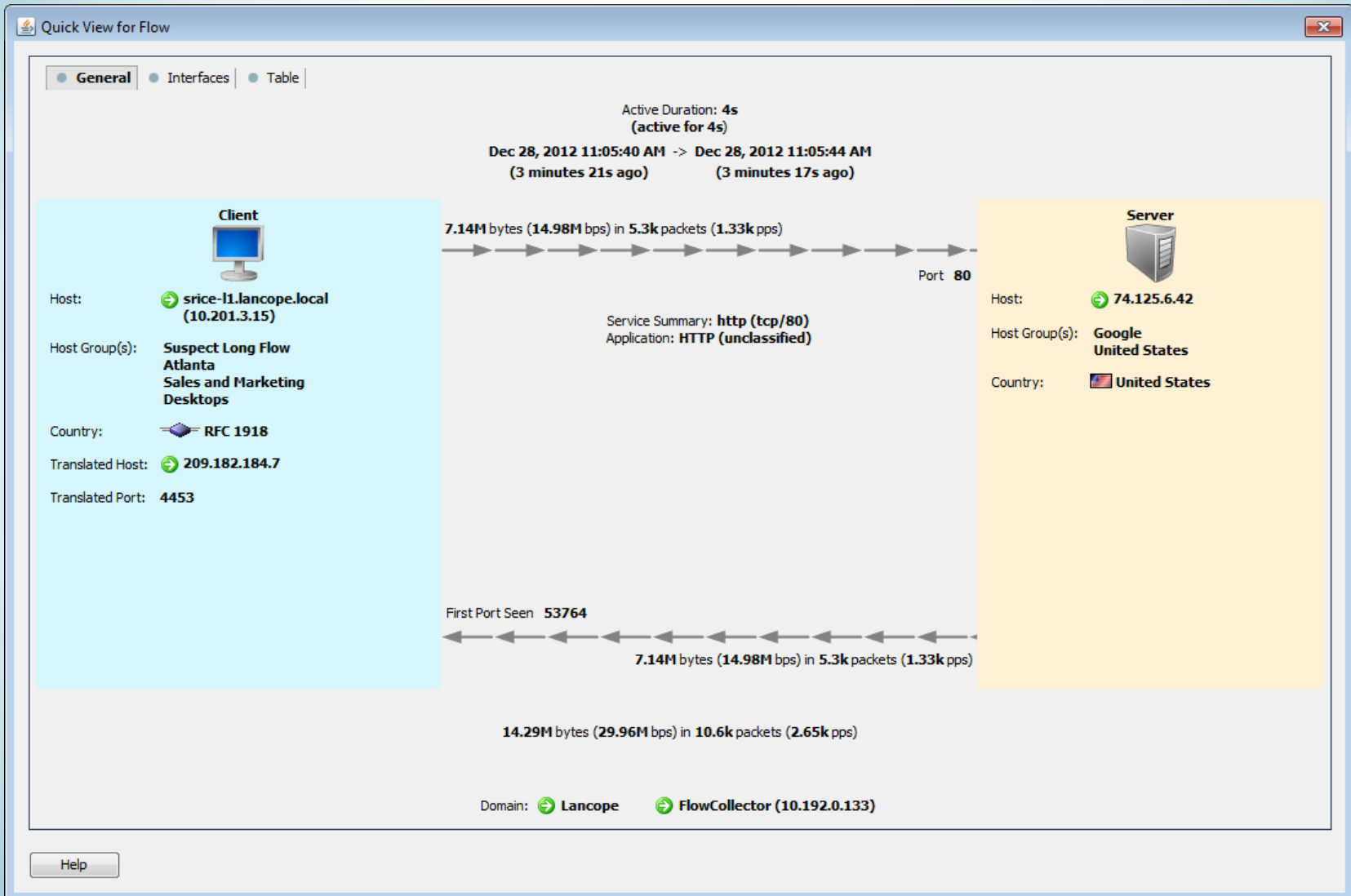
Server Exporters IP (IF)

Exporter	Exporter...	Interface	Direction	TTL	DSCP	Flow Act...
10.240.200.2	Exporter	ifIndex-1	Outbound			
10.240.200.2	Exporter	ifIndex-2	Inbound		best_effort	
10.240.200.1	Cisco ASA	Wan	Outbound			Permitted
10.240.200.1	Cisco ASA	Lan	Inbound			Permitted
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan1	Inbound		best_effort	
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan240	Outbound			

Exporter	Exporter...	Interface	Direction	TTL	DSCP	Flow Act...
10.240.200.2	Exporter	ifIndex-1	Inbound		best_effort	
10.240.200.2	Exporter	ifIndex-2	Outbound			
10.240.200.1	Cisco ASA	Wan	Inbound			Permitted
10.240.200.1	Cisco ASA	Lan	Outbound			Permitted
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan1	Outbound			
lchqgw01.lanco (10.201.0.1)	Exporter	Vlan240	Inbound		best_effort	

Help

Stitching & De-duplication





TOOLS: SILK



SiLK

- Download at <http://tools.netsa.cert.org>
- Stores and processes flow
- Project Managed by Carnegie Mellon CERT

iSiLK



Query Builder (demo-0f0z.isilk)

Basic Query Options | More Filter Options

Data files to search
Data Pool (class/type) Incoming

Sensors All Sensors Choose...

Time Range to Query Current Hour

Apr Apr

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Start hour (GMT): 20 End hour (GMT): 20
Selected 1 hour

IP Addresses and Ports
 Filter based on source and destination

Source
IP x.x.x.x
IP Set (Choose a set)
Clear Choose...

Port 0-65535

Destination
IP x.x.x.x
IP Set (Choose a set)
Clear Choose...

Port 0-65535

```
rwfilter --type=in,inweb --start-date=2013/04/22:20 --proto=0-255 --pass=$output
```

Name Untitled Query Add to demo-0f0z.isilk Return records that FAIL filter

Validate Options Save As Plugin... Close Run Remote Query

iSiLK



Query Builder (demo-0f0z.isilk)

Basic Query Options | More Filter Options

Apply a Prefix Map

File: (Choose a prefix map) [Clear] [Choose...]

saddress: []

daddress: []

Protocol and protocol-specific fields

Protocol: 0-255

TCP Flags: F S R P A U E C [checked] [checked] [checked] [checked] [checked] [checked] [checked] [checked]

ICMP Type: 0-255

ICMP Code: 0-255

Country Codes

Source: []

Dest: []

Flow size fields

Bytes: 1-

Pkts: 1-

b/p: 1-

```
rwfilter --type=in,inweb --start-date=2013/04/22:20 --proto=0-255 --pass=$output
```

Name: Untitled Query | Add to: demo-0f0z.isilk | Return records that FAIL filter

[Validate Options] [Save As Plugin...] [Close] [Run Remote Query]

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)



WHAT CAN LOGGING REVEAL



Signature Matching

- Look for “known bad” conversations
- Match against data collected in NetFlow
- Per Flow Analysis

What Can Intelligent NetFlow Analysis Do?



Reveal BotNet Hosts

	Policy	Start Active Time	Source	Source Host Groups	Target	Target Country	Target Host Groups	Details
	Inside Hosts	Feb 11, 2013 2:40:00 PM (1 hour 53 minutes 27s ago)	209.182.184.8	Atlanta	ns1.dns-domainserve (82.208.40.4)	Czech Republic	Czech Republic, Zeus	Successful communication was detected between this inside host and C&C server using port 80 and the TCP protocol, and http://host1.fileserv.uni.me/css...

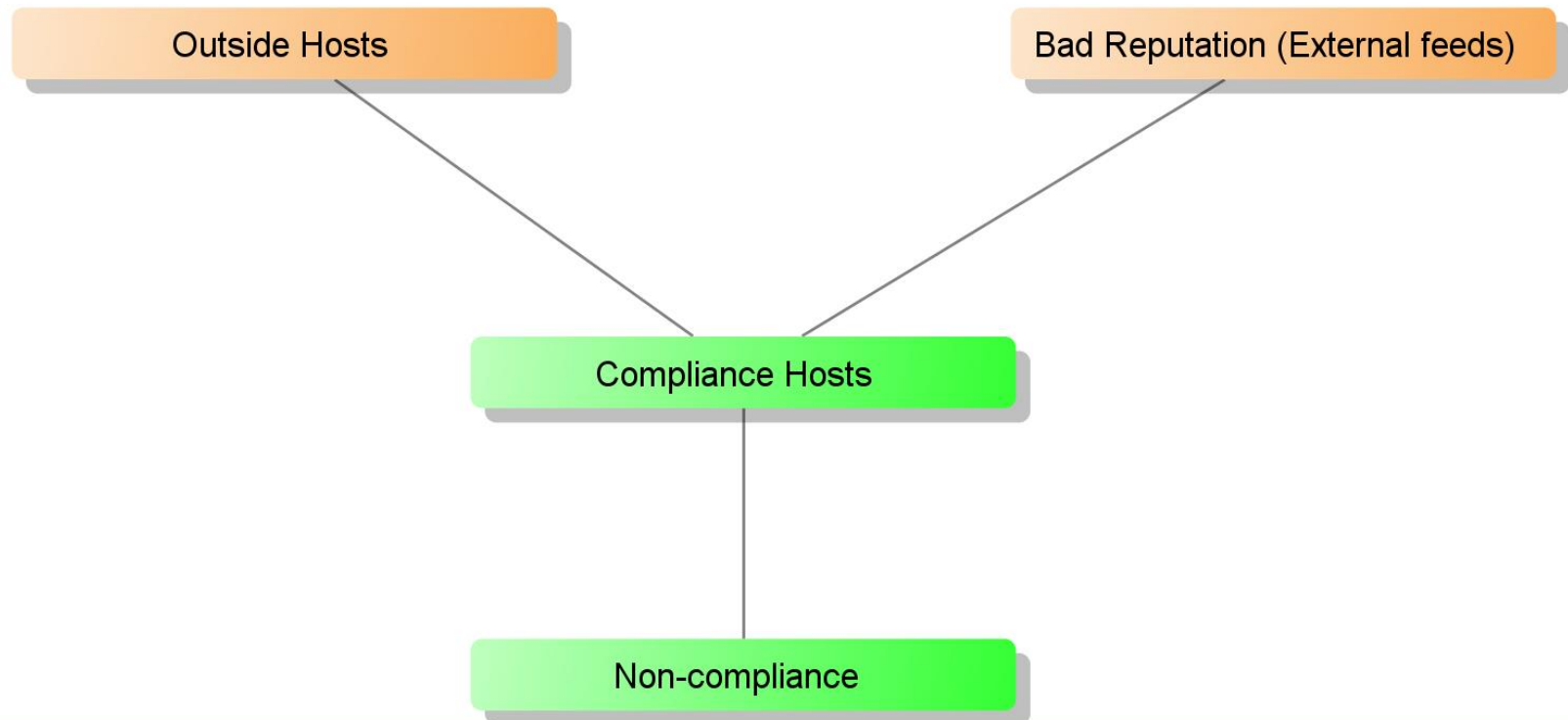
↑
Layer 3

↑
Layer 4
and URL

What Can Intelligent NetFlow Analysis Do?



Report on Compliance

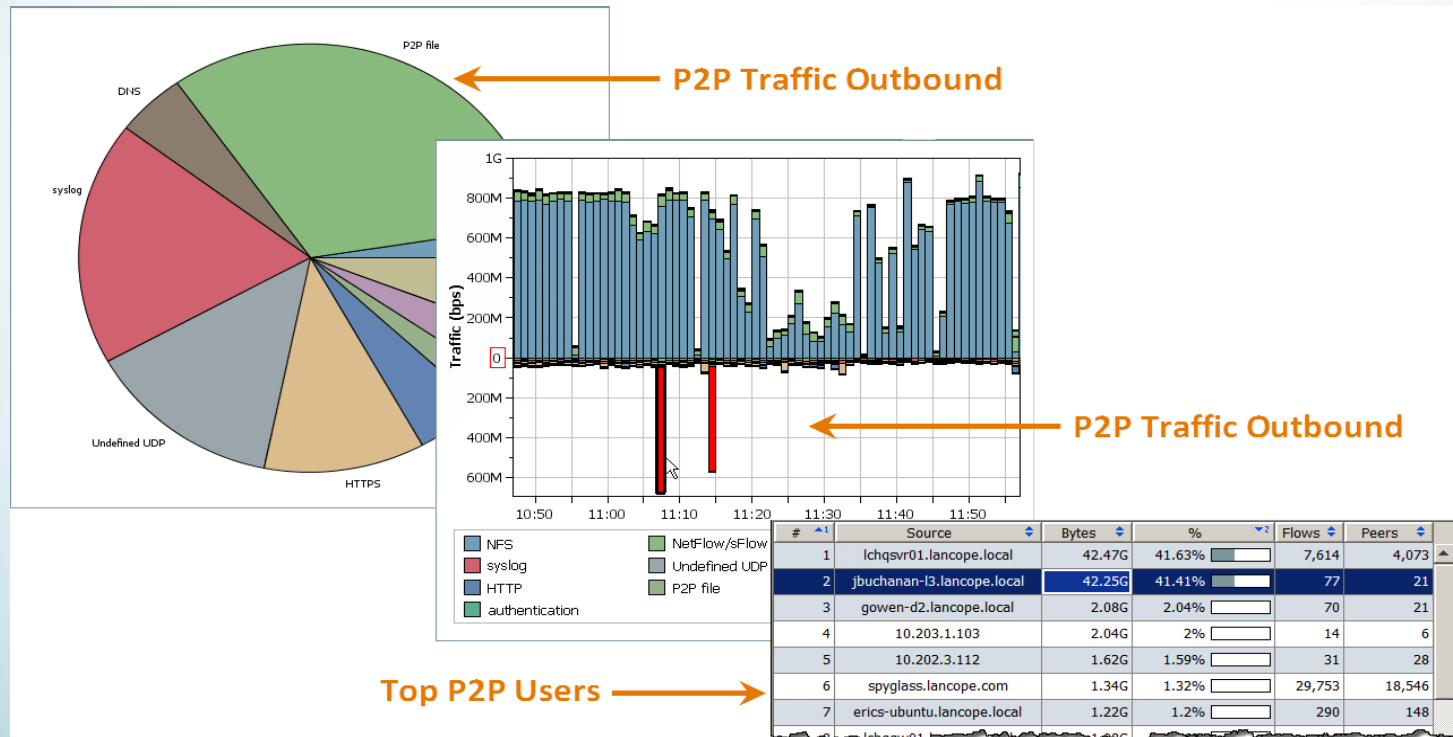


What Can Intelligent NetFlow Analysis Do?



Unsanctioned Device and Application Detection

- ▶ Identify the use of unsanctioned applications
- ▶ Detect rogue servers and other rogue devices



Top P2P Users

What Can Intelligent NetFlow Analysis Do?



- ▶ Audit Firewall rules
- ▶ Immediately detect misconfigurations
- ▶ Ensure regulatory compliance

The screenshot displays two windows from a network analysis tool. The top window, titled "Quick View for Flow", shows a flow between a Client and a Server. The Client is identified as "Host: 10.10.10.65" from the "Networks" group in the "United States". The Server is identified as "Host: 10.10.10.40" from the "Taiwan Suspicious Internet Hosts" group in "Taiwan". The flow details include: "Active Duration: 2 minutes 2s (active for 2 minutes 2s)", "2011/5/4 08:35:08 -> 2011/5/4 08:37:10 (5 minutes 59s ago)", "2.19k bytes (147.15 bps) in 18 pac", "Port: 53", "Service Summary: dnstcp (tcp/53)", "Application: SSH", "1 TCP Connection", and "First Port Seen: 11669". The bottom window, titled "Host Locking Configuration for Domain 'NinjaNet'", is a table with the following data:

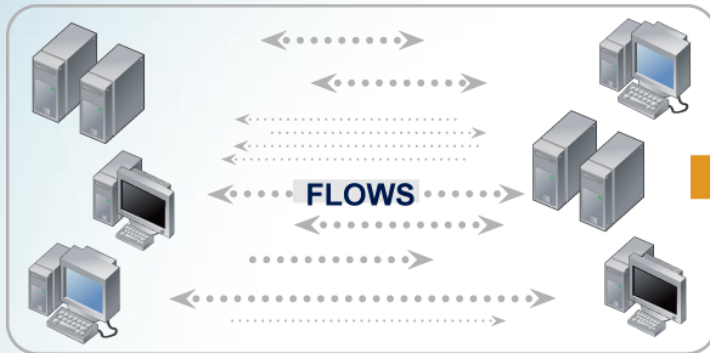
ID	Rule Name	Client Host Group	Server Host Group	Allow/Disallow	Exceptions
5	Restrict Administrative Access	Internal Network	PCI Zone	Disallow All	Services: https,sftp,ssh

Buttons at the bottom of the configuration window include: Add, Remove, Duplicate, Edit, Reverse, Import, Export, Help, Apply, Close, and OK.



Behavior-based Analysis of Network Flows

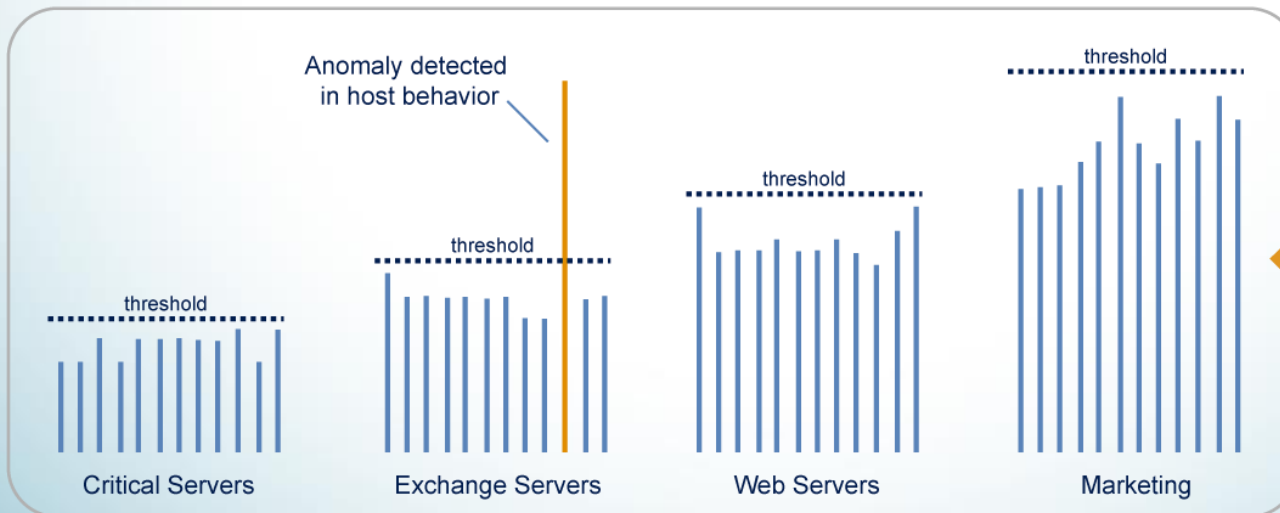
Collect and analyze flows



Establish baseline of behavior

- B
E
H
A
V
I
O
R**
- Number of concurrent flows
 - Packets per second
 - Bits per second
 - New flows created
 - Number of SYNs sent
 - Time of day
 - Number of Syns received
 - Rate of connection resets
 - Duration of the flow
 - Over 80+ other attributes

Alarm on anomalies and changes in behavior



What Can Intelligent NetFlow Analysis Do?



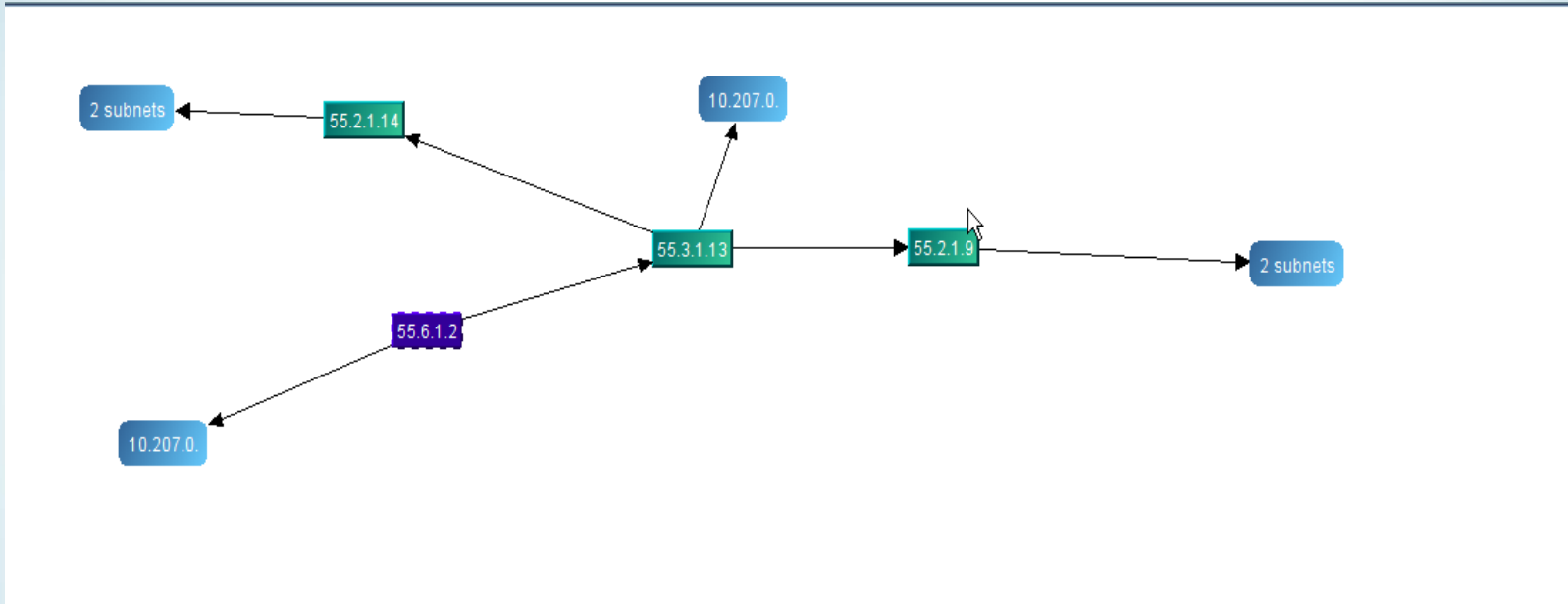
Reveal Recon

Internal Spreading Malware Bot Detection Suspect Data Loss Policy Violation Reconnaissance Detection DDoS Detection Alarms				
Concern Index - 16 records summarized into 16 records				
Host Groups	Host	CI	CI%	Alerts
Atlanta	spyglass.lancope.com (209.182.184.2)	3,520,636	1,174%	Excess_Clients, Port_Scan
Atlanta	209.182.184.1	26,888,520	269%	Rejects, UDP_Scan
Sales and Marketing, Atlanta, Users, Windows	jbuchanan-d2.lancope.local (10.201.3.24)	15,995,525	160%	TCP_Scan
New York, Windows	10.90.10.254	9,132,249	91%	TCP_Scan
New York, Windows	10.30.10.254	8,312,191	83%	TCP_Scan
New York, Windows	10.40.10.254	8,329,626	83%	TCP_Scan
New York, Windows	10.80.10.254	8,344,656	83%	TCP_Scan
New York, Windows	10.70.10.254	8,182,332	82%	TCP_Scan
New York, Windows	10.50.10.254	8,074,116	81%	TCP_Scan
New York, Windows	10.100.10.254	8,020,008	80%	TCP_Scan
New York, Windows	10.20.10.254	7,686,342	77%	TCP_Scan
New York	10.110.10.254	7,608,186	76%	TCP_Scan
New York, Windows	10.60.10.254	7,202,376	72%	TCP_Scan
Atlanta	209.182.176.42	2,144,863	67%	Rejects
SG Private	lcsgrw01.lancope.local (10.192.0.1)	5,972,924	60%	Ping, Ping_Oversized_Packet, Ping_Scan, Rejects
Sales and Marketing, Atlanta, Users, Windows	10.201.3.83	5,903,806	59%	Ping_Oversized_Packet, TCP_Scan

What Can Intelligent NetFlow Analysis Do?



Investigate Infections



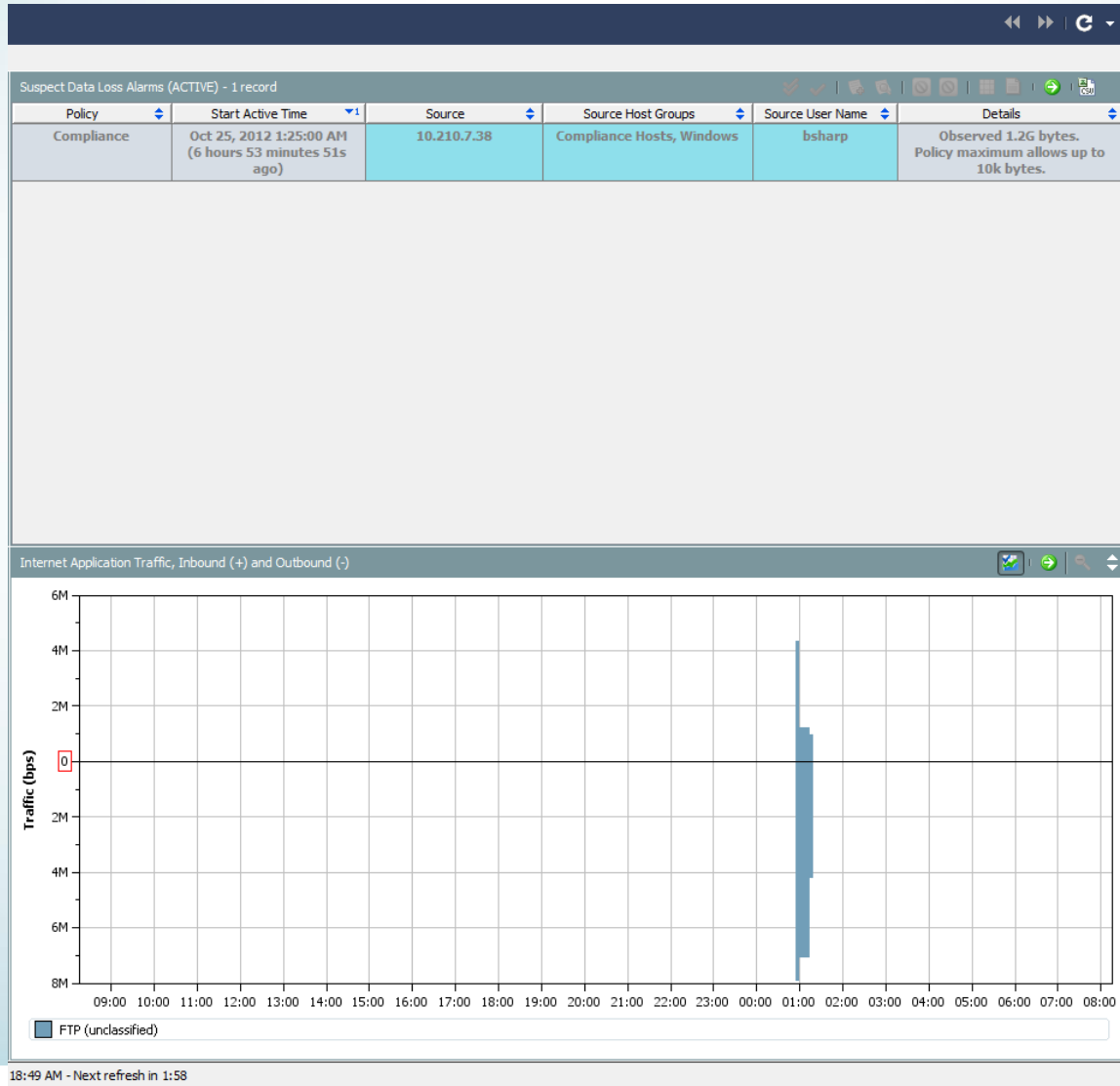
Details - 2 records

Earliest Time	Port	Protocol	Next Hop	Total Hosts Subnet	Propagated Hosts Subnet
05/22/08 01:15:59	445	tcp	55.3.1.13	3	17
05/22/08 01:16:09	445	tcp	Subnet 10.207.0.	1	

What Can Intelligent NetFlow Analysis Do?



Loss of Protected Data





FORENSIC INVESTIGATIONS

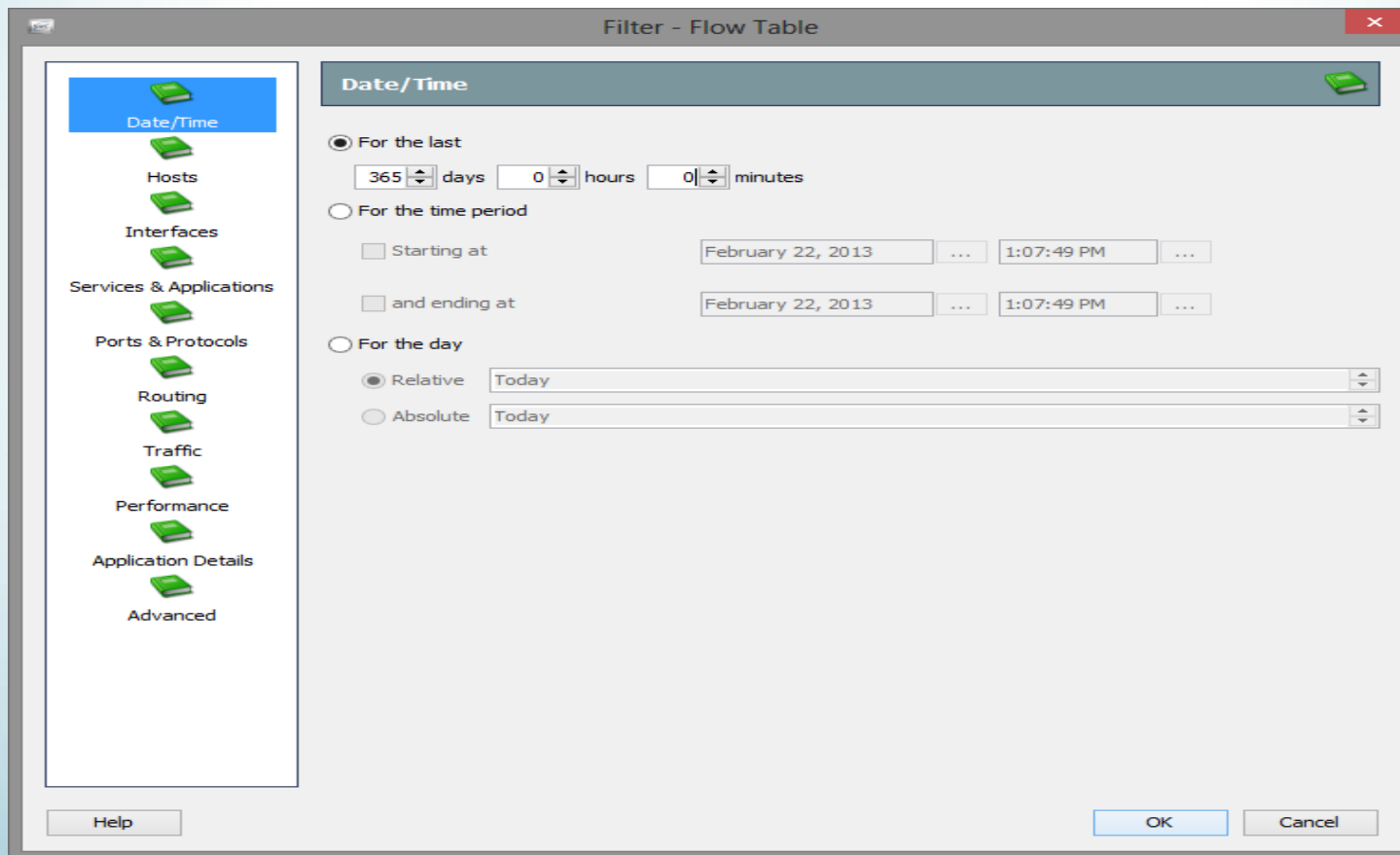


How long has behavior been active? **Historical Traffic Report**

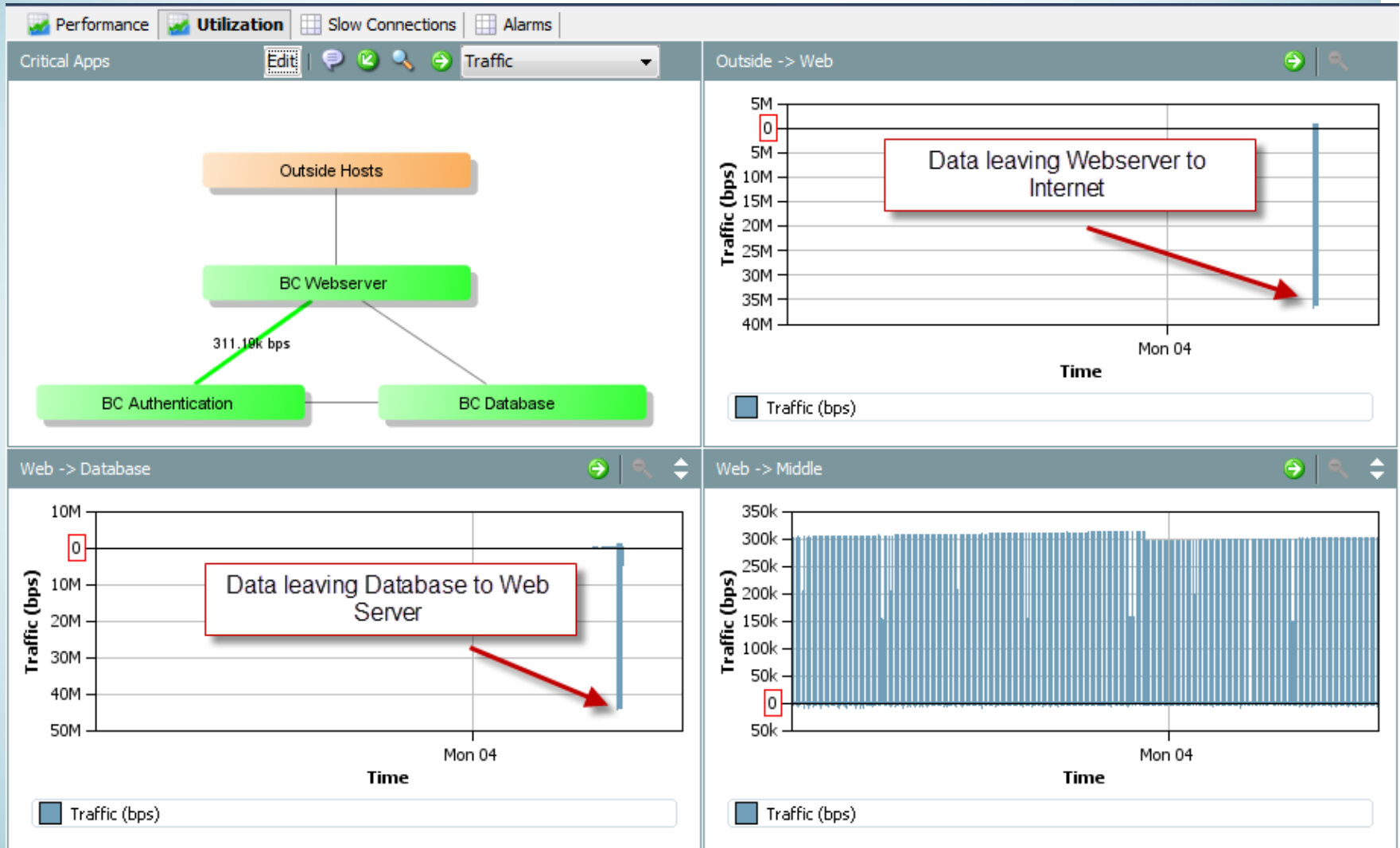
Which hosts have a compromised host “touched?” **Top Peers (filtered to Internal or Critical)**

Has this attack happened in the past? **Flow Table on available data points**

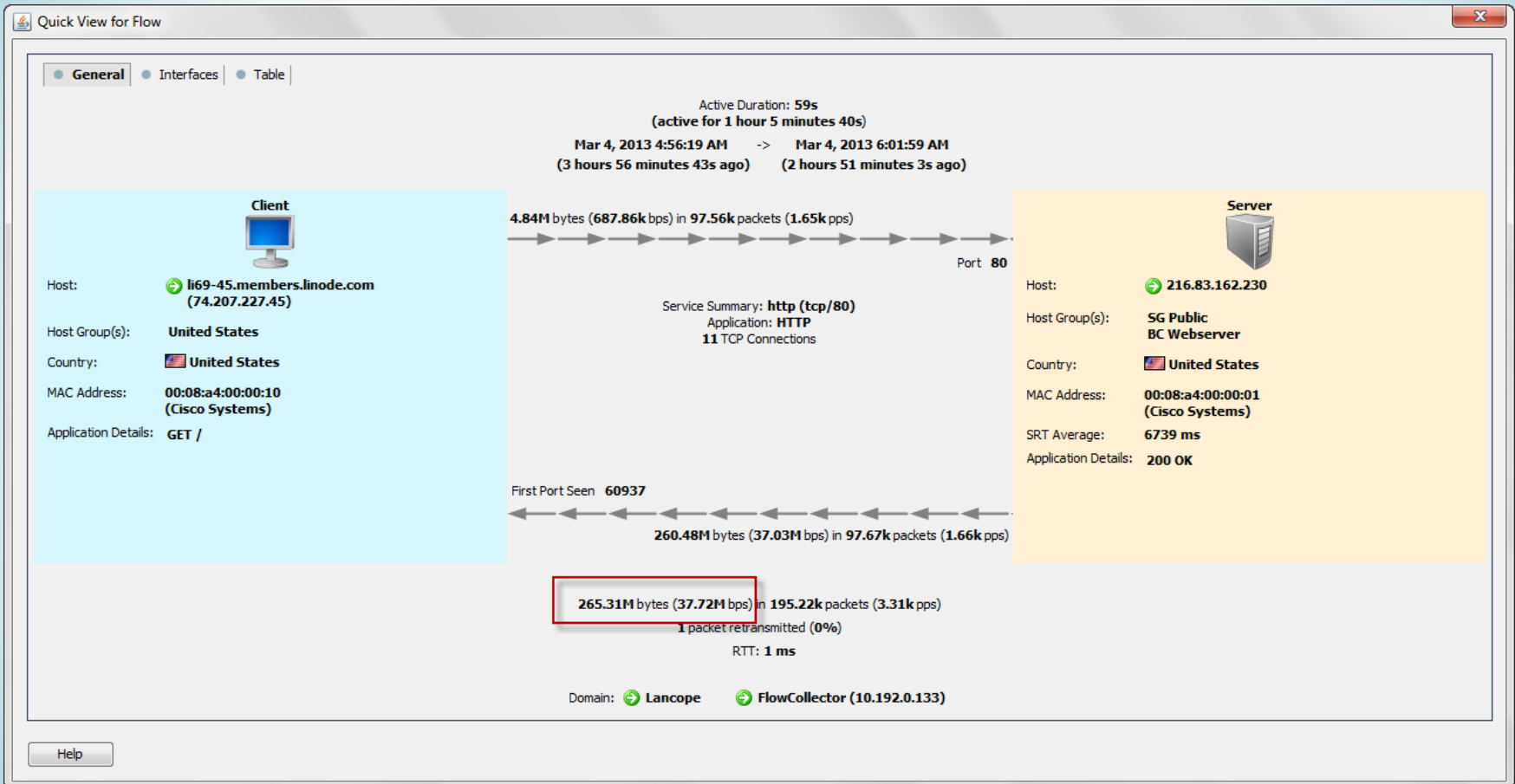
How long has this attacker been lurking around the network? **Historical Traffic on Host**



SQL Injection



SQL Injection



SQL Injection



Filter Domain : Lancopé Time : Today
Host : li69-45.members.linode.com (74.207.227.45)

Identification Alarms Security **CI Events** Top Active Flows Identity, DHCP & Host Notes Exporter Interfaces

Host is Source of CI Events (High CI) - 25 records

Start Active Time	Last Active Time	Target Host Groups	Target Host	Concer...	CI Events
Mar 4, 2013 4:55:57 AM (3 hours 59 minutes 16s ago)	Mar 4, 2013 5:05:14 AM (3 hours 49 minutes 59s ago)	United States	216.83.162.0/24	1,785,588	Ping_Scan(2560), Addr_Scan/tcp-80(492), Addr_Scan/tcp-443(520), Addr_Scan/tcp-8080(6), Ping(10)
Mar 4, 2013 4:56:01 AM (3 hours 59 minutes 12s ago)	Mar 4, 2013 5:16:36 AM (3 hours 38 minutes 37s ago)	SG Public, BC Webserver	216.83.162.230	122,669	Bad_Flag_SYN_FIN-80(200), Bad_Flag_ACK-80(40), Bad_Flag_ACK-443(40), Bad_Flag_ACK-8080(70), Bad_Flag_NoFlg-80(220), Bad_Flag_NoFlg-443(20), Bad_Flag_NoFlg-8080(20), Reset/tcp-8080(1), Timeout/tcp-8080(1), ICMP_Port_Unreach-31233(5), ICMP_Port_Unreach-36977(5), ICMP_Port_Unreach-39977(5), ICMP_Port_Unreach-41448(5), ICMP_Port_Unreach-42605(5), Ping(5)
Mar 4, 2013 5:00:00 AM (3 hours 55 minutes 13s ago)	Mar 4, 2013 5:05:00 AM (3 hours 50 minutes 13s ago)		Multiple Hosts	2,672	ICMP_Flood(2)
Mar 4, 2013 4:55:58 AM	Mar 4, 2013 5:06:41 AM	United States	216.83.162.1	2,041	Bad_Flag_ACK-80(10),

Pre-SQLi suspicious activity
connected with recon



Beron's abnormal disclosure

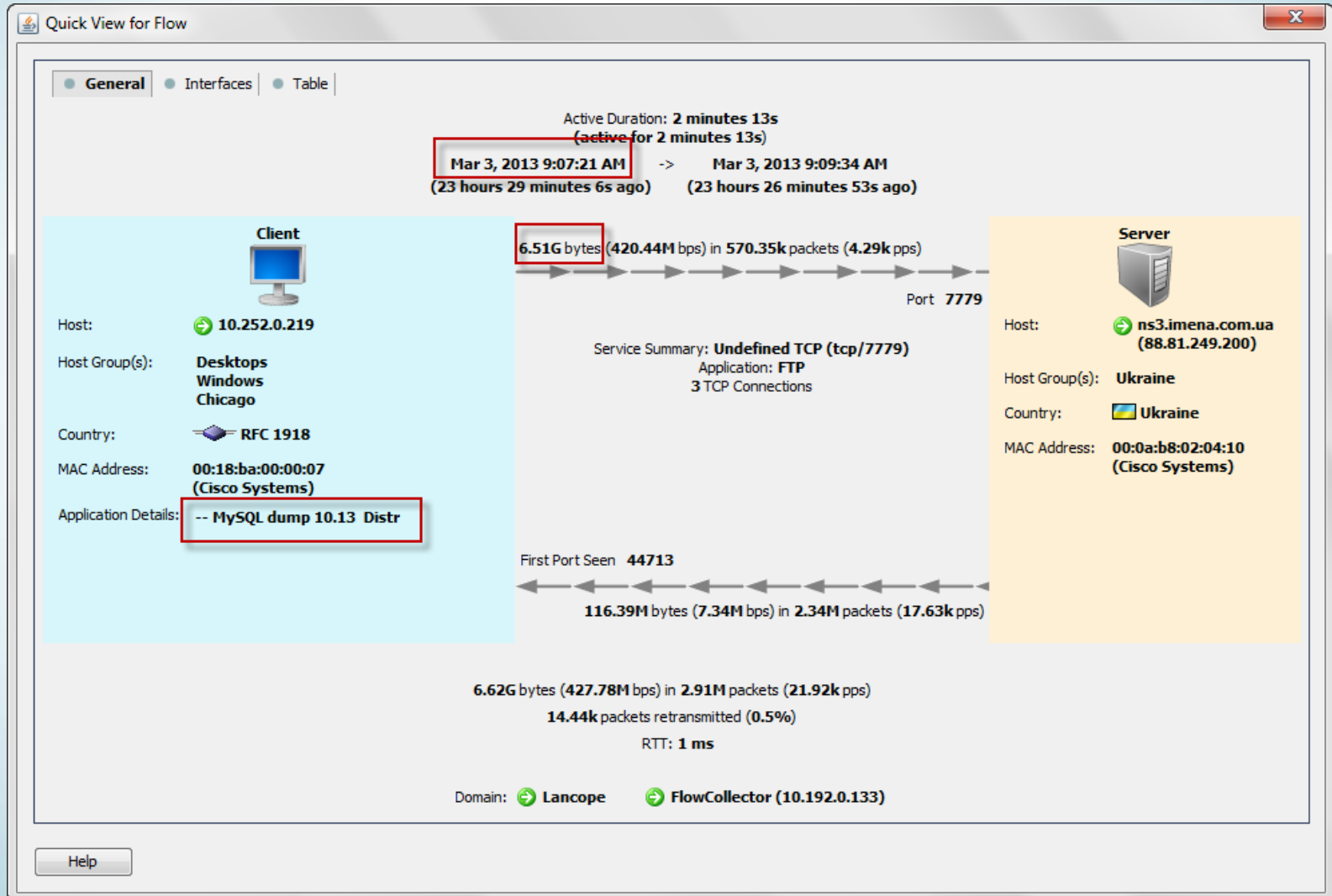
1	2	Policy	Start Active T...	Alarm	Source	Source Host Gr...	Source U...	Target	Target H...	Details
		Compliance Hosts	Mar 3, 2013 7:35:00 AM (1 day 1 hour ago)	Suspect Data Loss	10.210.7.38	Control Servers, Windows	lucy	Multiple Hosts		Observed 2.41G bytes. Policy maximum allows up to 1k bytes.
		Inside Hosts	Mar 3, 2013 9:15:00 AM (23 hours 20 minutes 48s ago)	Suspect Data Loss	10.252.0.219	Desktops, Windows, Chicago	beron	Multiple Hosts		Observed 8.28G bytes. Policy maximum allows up to 500M bytes.

Abnormal Data Upload





What did Beron send? Who received it?





Where could have Beron gotten the data?

Filter Domain : Lancope Direction : Total
Client Host : 10.252.0.219 Time : Last 1 day
Server Host Group : Inside Hosts

Top Peers - 2 records

	% of Bytes	Peer	Peer Host Groups	Peer Role	Average Traffic (b...	Bytes	Flows	Hosts	Peer Bytes Ratio
1	10...	10.252.0.10	BC Database, Chicago	Server	114.68M	10.41G	1	1	98.18%
	10...	Total (1)		Server	114.68M	10.41G	1	1	98.18%



Quick View for Flow

● **General** ● Interfaces ● Table

Active Duration: **11 minutes 14s**
(~~active for 11 minutes 14s~~)

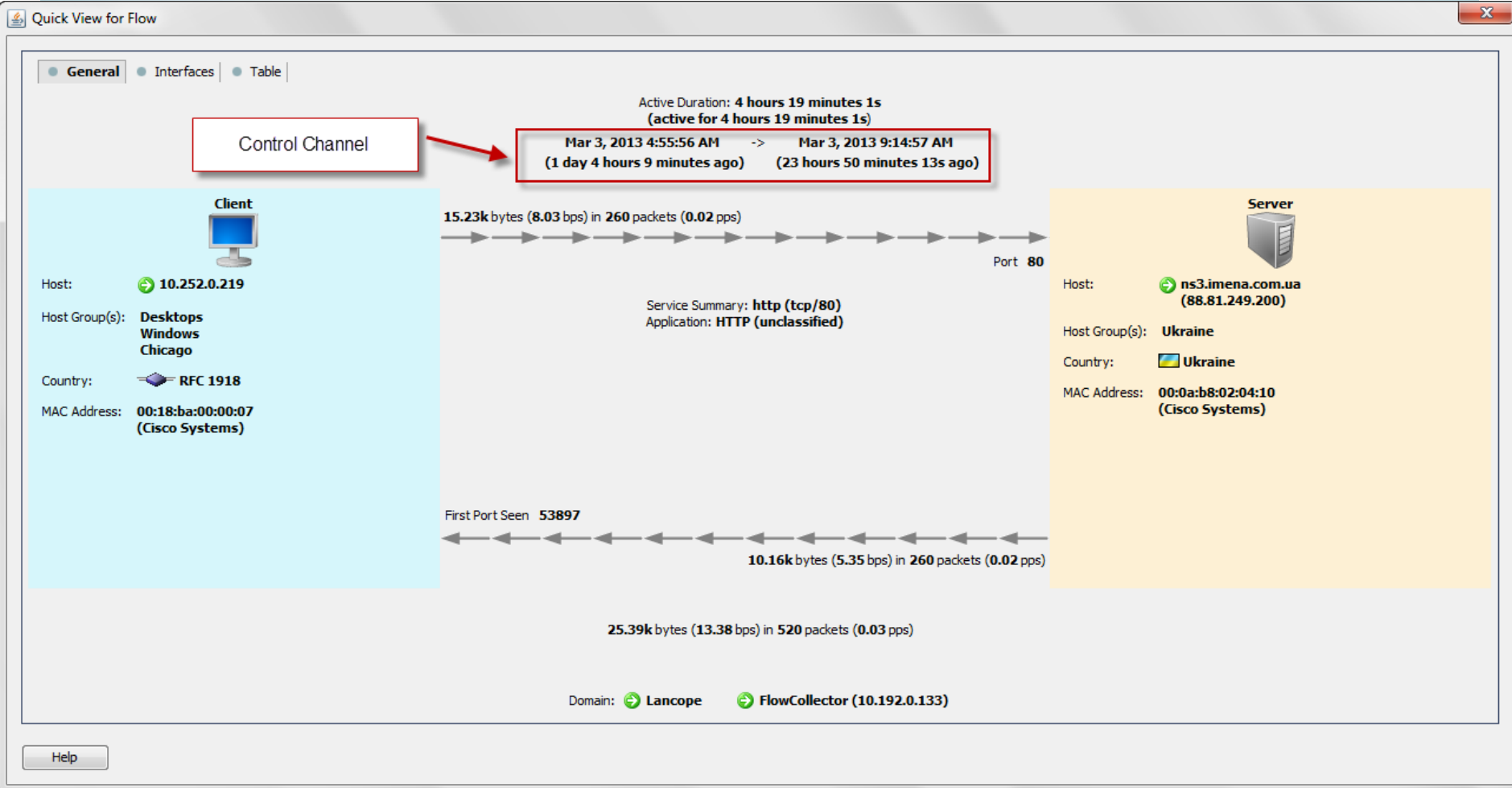
Mar 3, 2013 8:55:57 AM -> **Mar 3, 2013 9:07:11 AM**
(23 hours 42 minutes 24s ago) (23 hours 31 minutes 10s ago)

Client	Flow	Server
Host: 10.252.0.219	194.25M bytes (2.42M bps) in 3.92M pack	Host: 10.252.0.10
Host Group(s): Desktops Windows Chicago	Port 3306	Host Group(s): BC Database Chicago
Country: RFC 1918	Service Summary: mysql (tcp/3306) Application: SQL 15 TCP Connections	Country: RFC 1918
MAC Address: 00:08:a4:00:00:09 (Cisco Systems)		MAC Address: 00:05:dc:1d:10:00 (Cisco Systems, Inc.)
Application Details: !.....!		SRT Average: 1 ms
	First Port Seen 46823	Application Details: 4.....5.1.61!..!..WKP2FL*..
	130.3M bps in 1.99M packets (2.95k pps)	
	10.41G bytes (132.71M bps) in 5.9M packets (8.76k pps)	
	12 packets retransmitted (0%)	
	RTT: 1 ms	
	Domain: Lancop FlowCollector (10.192.0.133)	

Help



Why did Beron do it?





- **Web**

www.lancope.com (Company)
f15h.co (Personal)

- **Twitter**

[@Lancope](https://twitter.com/Lancope) (Company)
[@netflowninjas](https://twitter.com/netflowninjas) (Company Blog)
[@charlesherring](https://twitter.com/charlesherring) (Personal)

- **Charles Herring**

Sr. Systems Engineer, Lancope
cherring@lancope.com

