Proč prevence jako ochrana nestačí?

Flowmon
Driving Network Visibility

Luboš Lunter
lubos.lunter@flowmon.com

Flowmon Networks

- Technologický lídr v NetFlow/IPFIX monitoringu počítačových sítí a behaviorální analýzy
- 3x Deloitte CE Technology Fast 50
- Gartner Magic Quadrant pro NPMD
- Cisco, Check Point, IBM partnerships
- 600+ customers in 30+ countries

Deloitte.
CE Technology Fast 50
Certificate of achievement
INVEA-TECH a.s.

Check Point SOFTWARE TECHNOLOGIES LTD.

RED HERRING EUROPE WINNER 100

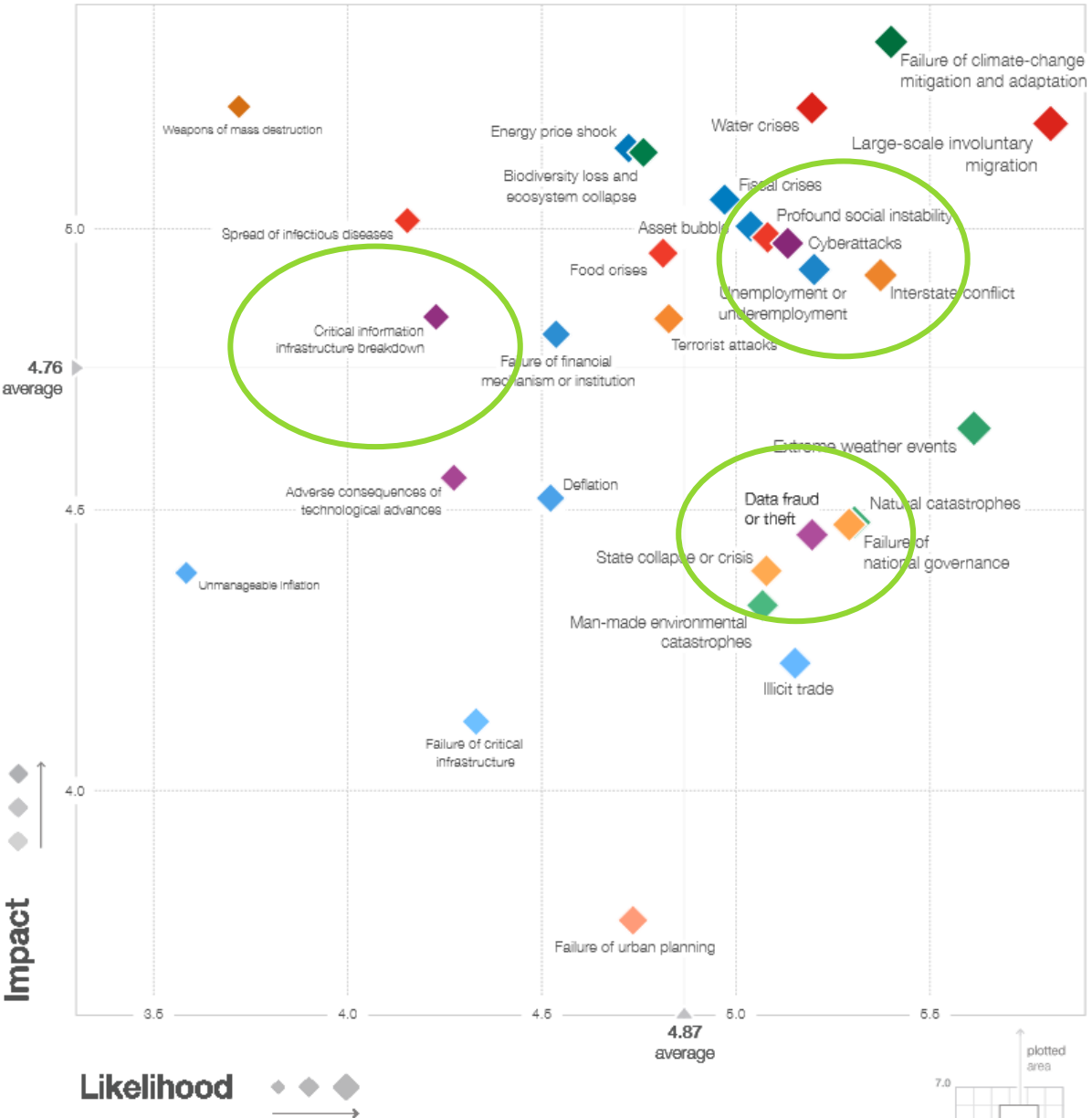
dimension data

NTT Communications


ANTIVIRUS

The Global Risks Landscape

Flowmon Networks



"…zločiny spáchané v kybernetickém prostoru stojí globální ekonomiku odhadem US $445 mld. …"

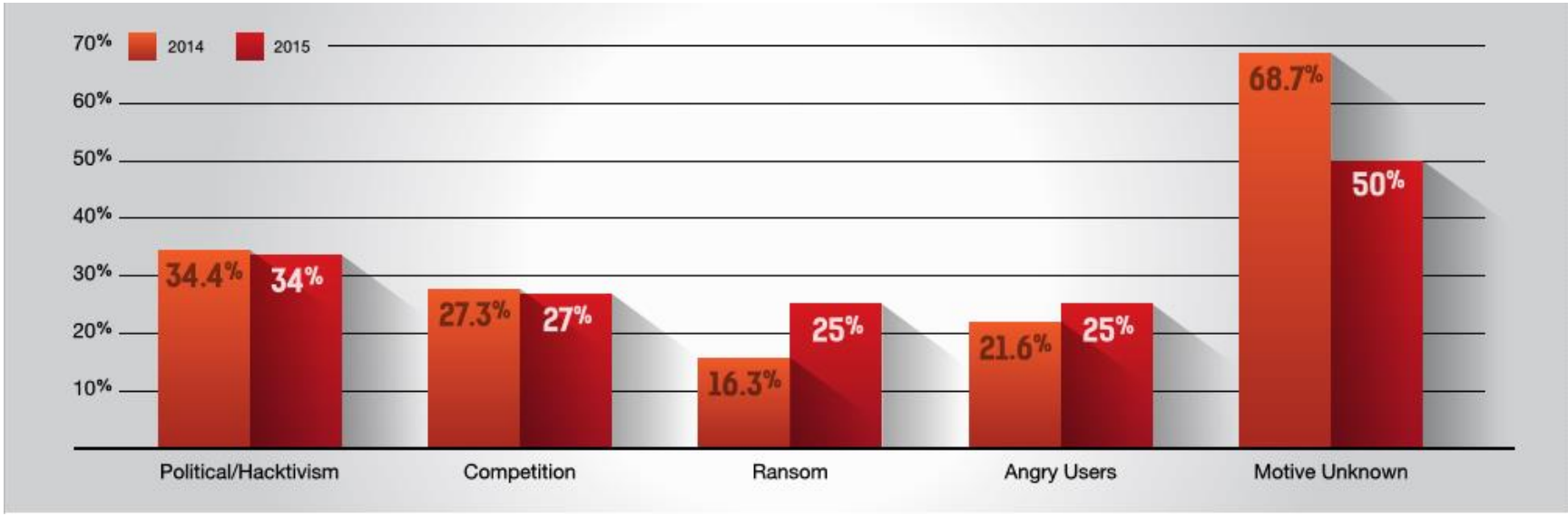
"Každý budoucí konflikt bude obsahovat kybernetickou část a některé budou probíhat čistě v kyberprostoru."

Source:

[The Global Risks Report 2016](#)
(World Economic Forum)

Motives behind cyber attacks

Flowmon Networks



Source:

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2015-2016 (Radware)

Most Pressing Concerns

Flowmon Networks

Figure 11: Top Business Concerns of Cyber Attacks

Source:

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2015-2016 (Radware)

Technologie

Flowmon Networks

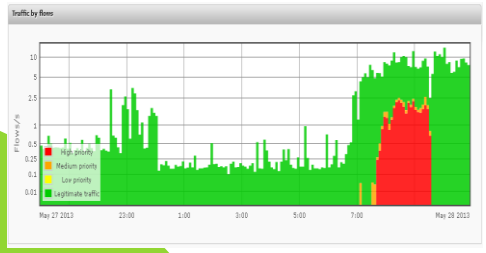
Source: Gartner, Top Security Trends 2015-2016

Flowmon Networks

Detekce anomálií & Analýza chování sítě (NBA)

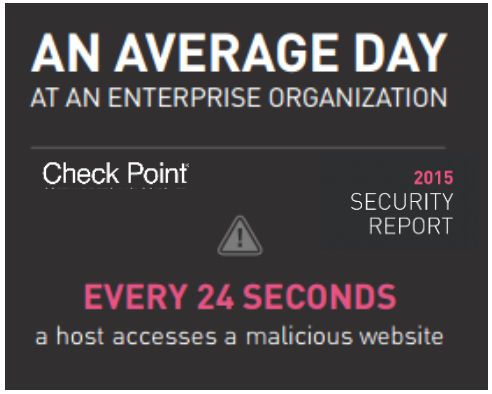
Technologické přístupy

Flowmon Networks



Network Visibility & Security

- Perimeter Security
- Endpoint Security



Adaptivní architektura bezpečnosti

Flowmon Networks

Co je NBA?

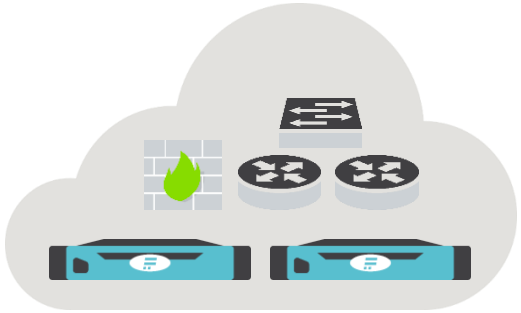
Flowmon Networks

- Behaviorální analýza sítě (NBA) - **zvýšení bezpečnosti** sítě pomocí **monitoringu provozu**, **odhalování neobvyklých aktivit** a odchylek od běžných činností
- Tradiční přístupy (IDS, IPS, FW) se zaměřují na perimetr sítě pomocí inspekce paketů, detekce známých příznaků a blokování v reálném čase
- NBA řešení hlídá, **co se děje uvnitř sítě**, agreguje data z mnoha míst v síti a provádí analýzu

Flowmon
Networks

Flowmon ADS

Architektura řešení Flowmon



LAN/WAN with Flowmon Probes or NetFlow/IPFIX compatible devices

Flowmon Collector

Network Visibility
Troubleshooting

Network Security
Anomaly Detection

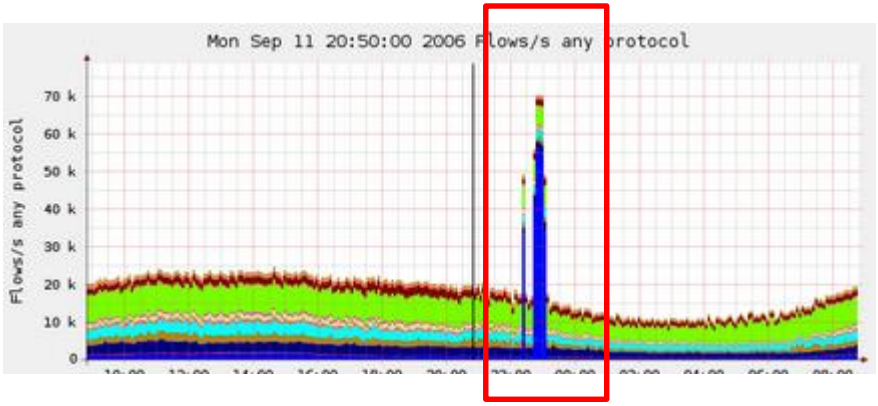
Application Performance
Monitoring

DDoS Protection

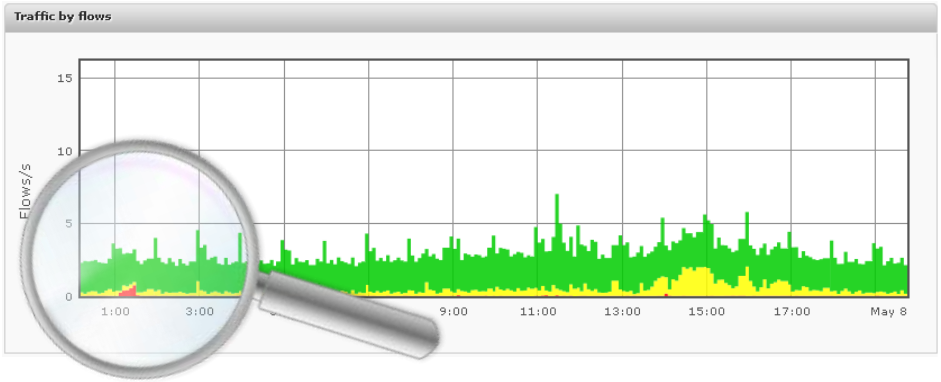
Detekce anomálií

Flowmon Networks

- Jak se náš přístup liší od ostatních nástrojů?



Běžné nástroje používají statistické metody, nimiž detekují špičky a odchylky



Flowmon analyzuje každou jednou komunikaci a jde za hranici tradičních statistických algoritmů

Princip Flowmon ADS

Flowmon Networks

Flowmon ADS

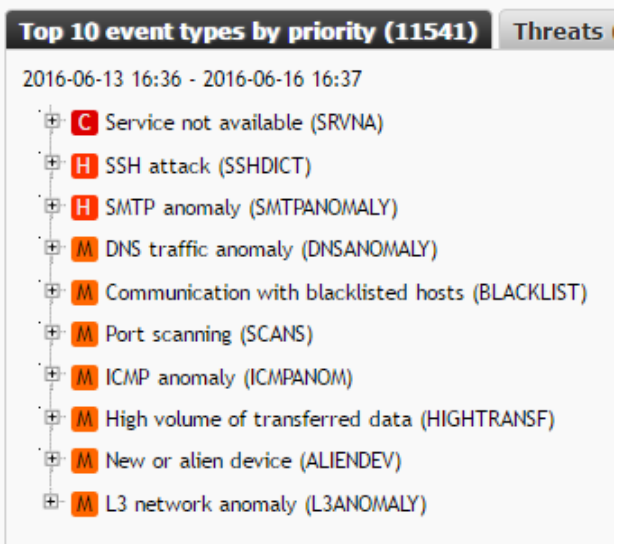
- Strojové učení
- Adaptivní baselining
- Heuristiky
- Vzory chování
- Reputační databáze

#	Zdrojová IP	Typ události	Detail	Čas	Zdroj NetFlow dat	Cíle
1	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 559.	2013-08-24 07:15:21	localhost	1.52.6.170, 1.52.13.199, 1.52.42.167, 1.52.59. 1.52.71.217, 1.52.87.249, 1.52.133.228, 1.52.1 1.52.192.113, 1.52.218.16, ...
2	112.91.30.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 379.	2013-08-24 07:15:21	localhost	1.52.54.212, 1.52.109.106, 1.52.167.73, 1.52.1 1.52.191.229, 1.52.218.123, 1.52.220.241, 1.52 1.52.241.199, 1.53.8.41, ...
3	121.10.112.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 266.	2013-08-24 07:15:21	localhost	1.52.1.176, 1.52.2.100, 1.52.7.105, 1.52.44.16 1.52.77.224, 1.52.128.196, 1.52.128.214, 1.52. 1.52.199.183, 1.52.241.170, ...
4	183.61.138.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 415.	2013-08-24 07:15:21	localhost	1.52.58.25, 1.52.85.224, 1.52.86.18, 1.52.92.1 1.52.174.104, 1.52.183.10, 1.52.184.230, 1.52. 1.52.203.16, 1.52.235.13, ...
5	210.73.221.181	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.36 MiB, packets: 58 086.	2013-08-24 07:15:21	localhost	1.52.28.245, 1.52.44.63, 1.52.112.109, 1.52.14 1.52.177.97, 1.53.40.147, 1.53.58.10, 1.53.89. 1.53.122.157, 1.53.221.26, ...
6	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 5.04 MiB, packets: 125 924.	2013-08-24 05:39:59	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.7 1.52.42.130, 1.52.44.24, 1.52.48.142, 1.52.67. 1.52.83.34, ...
7	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 3.60 MiB, packets: 88 749.	2013-08-24 03:38:31	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.9 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.1 1.52.122.10, ...
8	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.60 MiB, packets: 63 126.	2013-08-24 03:00:34	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.125 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.52. 1.52.203.143, 1.52.209.197, ...

Detekční schopnosti

Flowmon Networks

- Útoky na síťové služby
  - Anomálie v DNS, DHCP provozu
  - Útoky na VoIP, PBX, …
  - Neočakávaný e-mailový provoz a SPAM
- Infikovaná zařízení
  - komunikace botnet C&C, útočící zařízení, …
  - Port scanning apod. symptomy
- Aplikace jako P2P sítě nebo on-line messengers, obcházení PROXY , TOR
- Outages of network services or improper configurations
- Potenciální úniky dat



Flowmon Threat Intelligence

Flowmon Networks

- IP a host-based reputační databáze
- Detekce C&C domén, P2P botnetů, phishing
  - IP addresses
  - HTTP host names
  - Domain names

Flowmon Networks

Use Case: Flowmon ADS + Flowmon Traffic Recorder

Flowmon

FlowMon ADS

en | admin

- Dashboard
- Events
- Reports
- Configuration
  - General settings
  - Traffic processing
- About

Search criteria

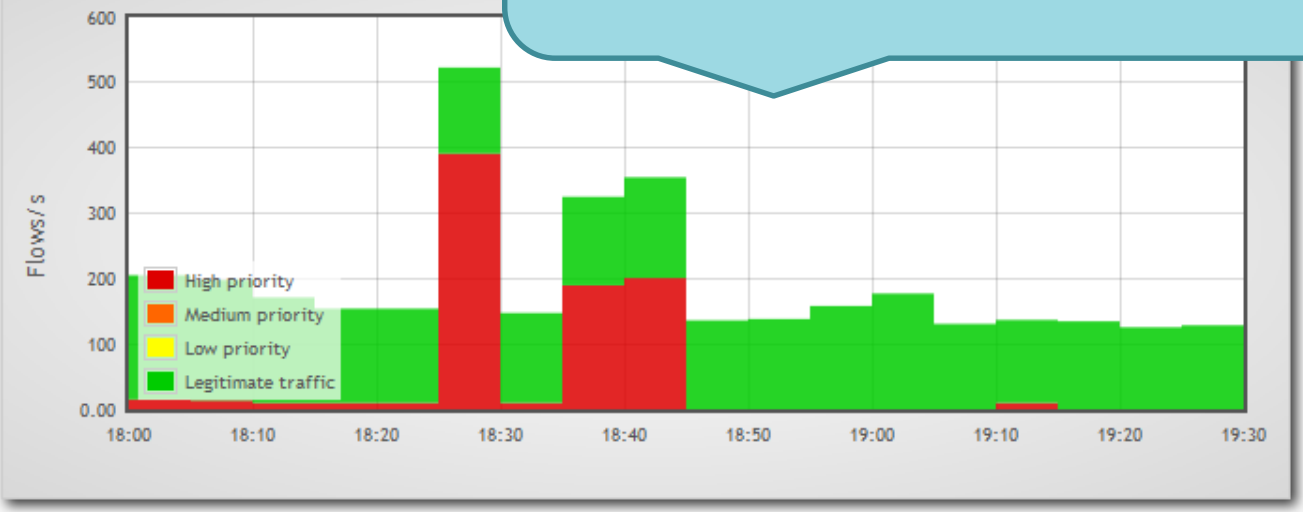
From 2016-02-08 18:00 To 2016-02-08 19:30 Search Reset

Perspective Demo NetFlow s

Přehled provozu, detekované anomálie

Overview | Events

Traffic by flows

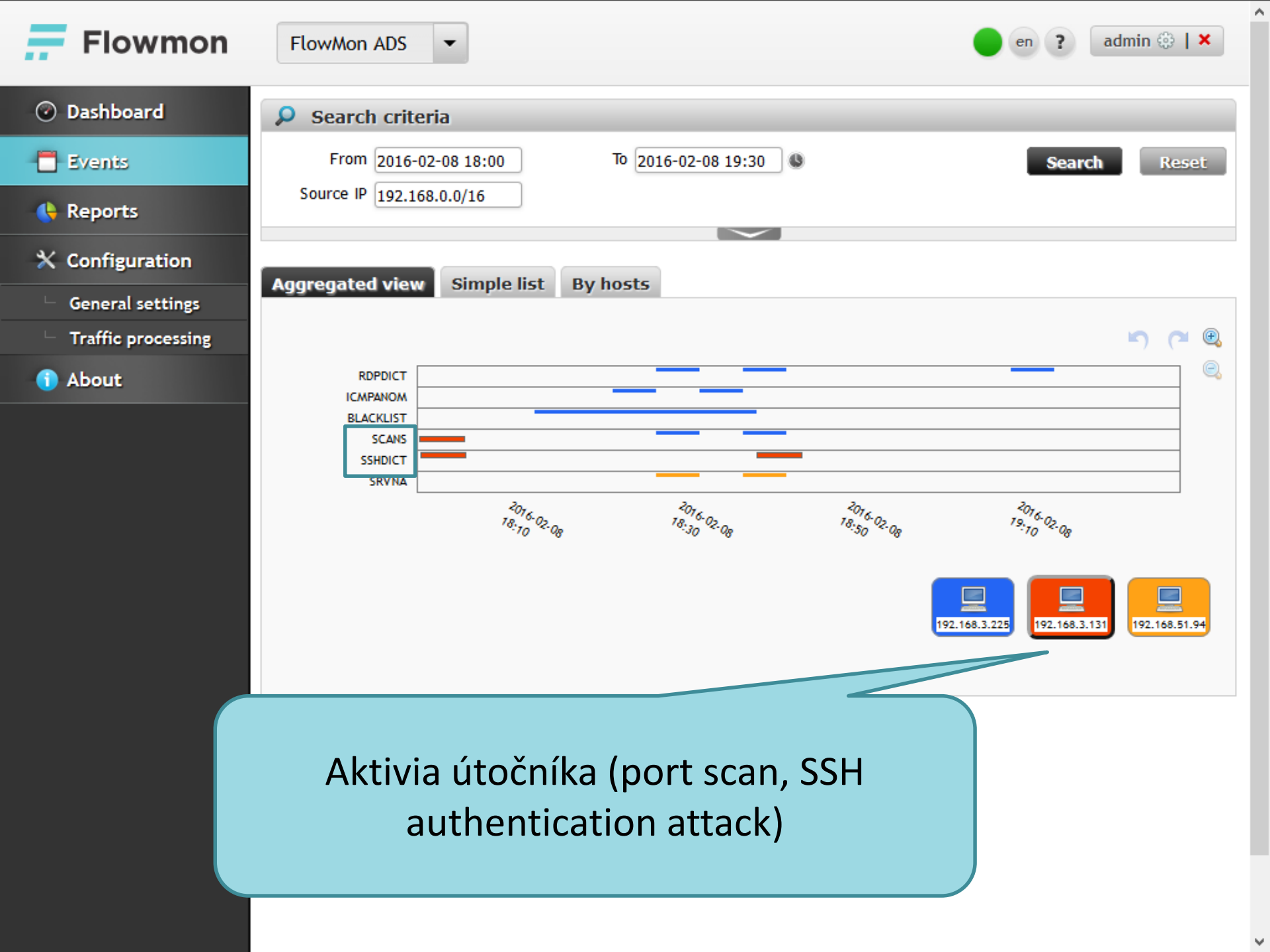


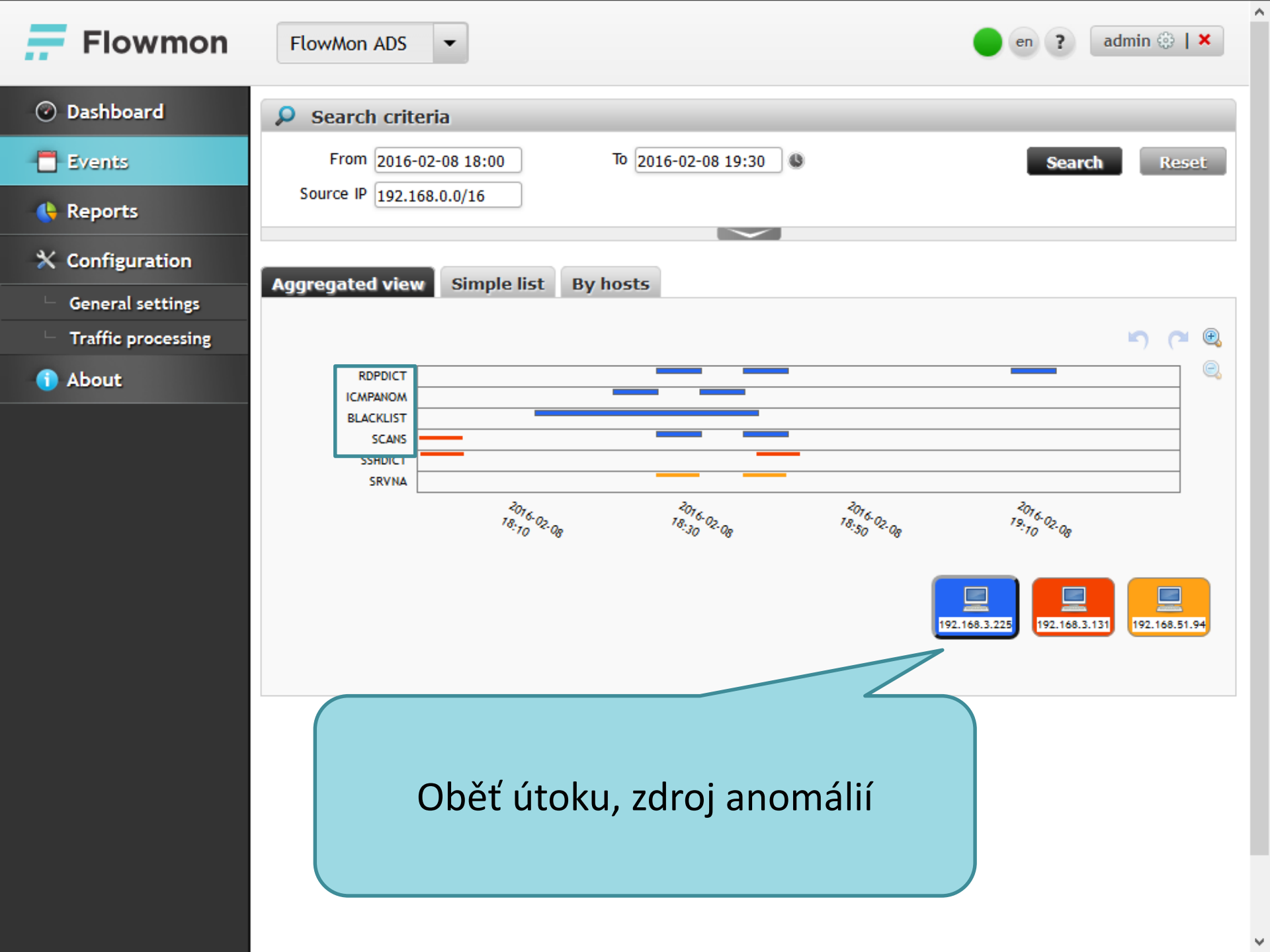
Bytes

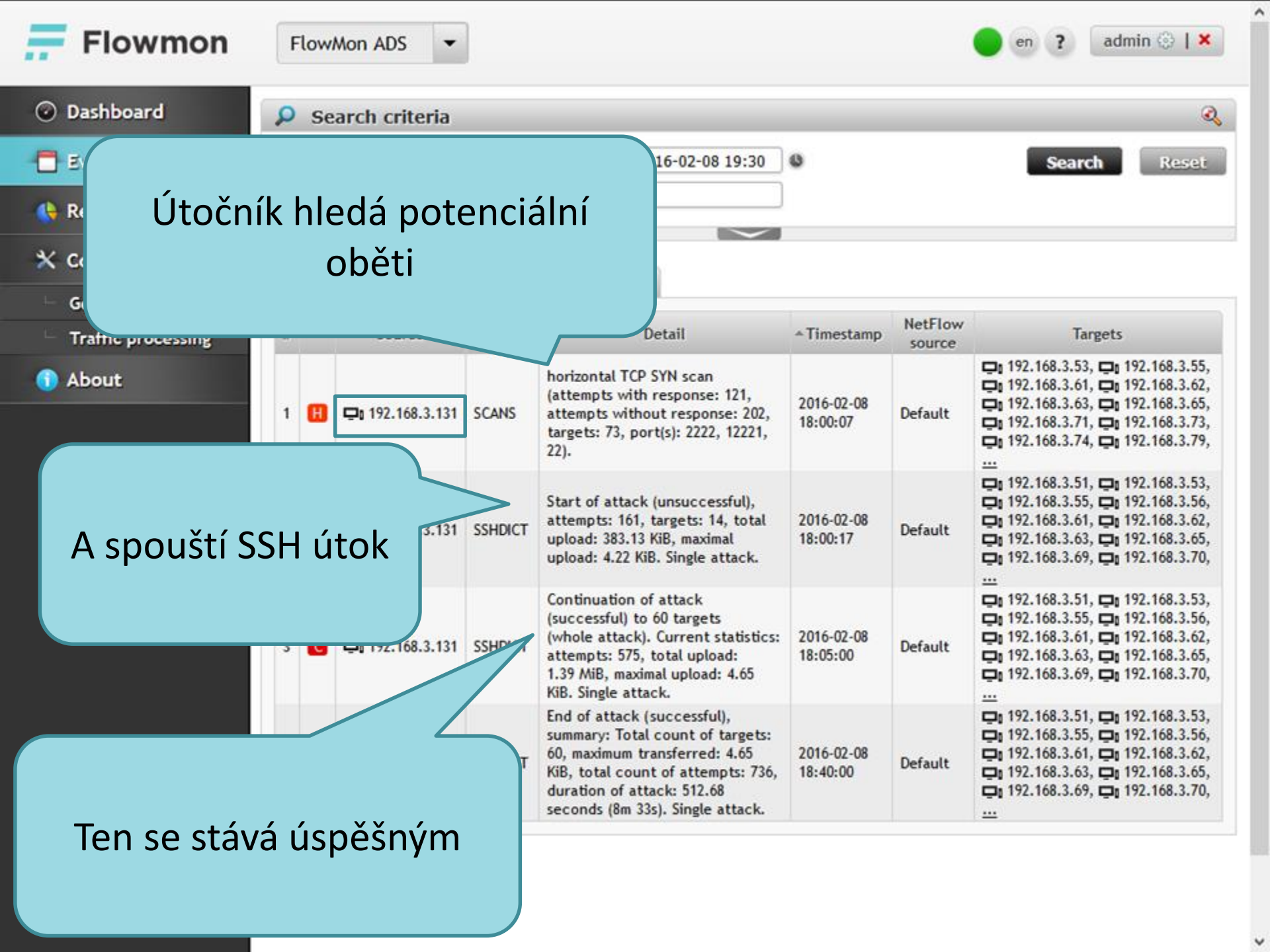
Packets

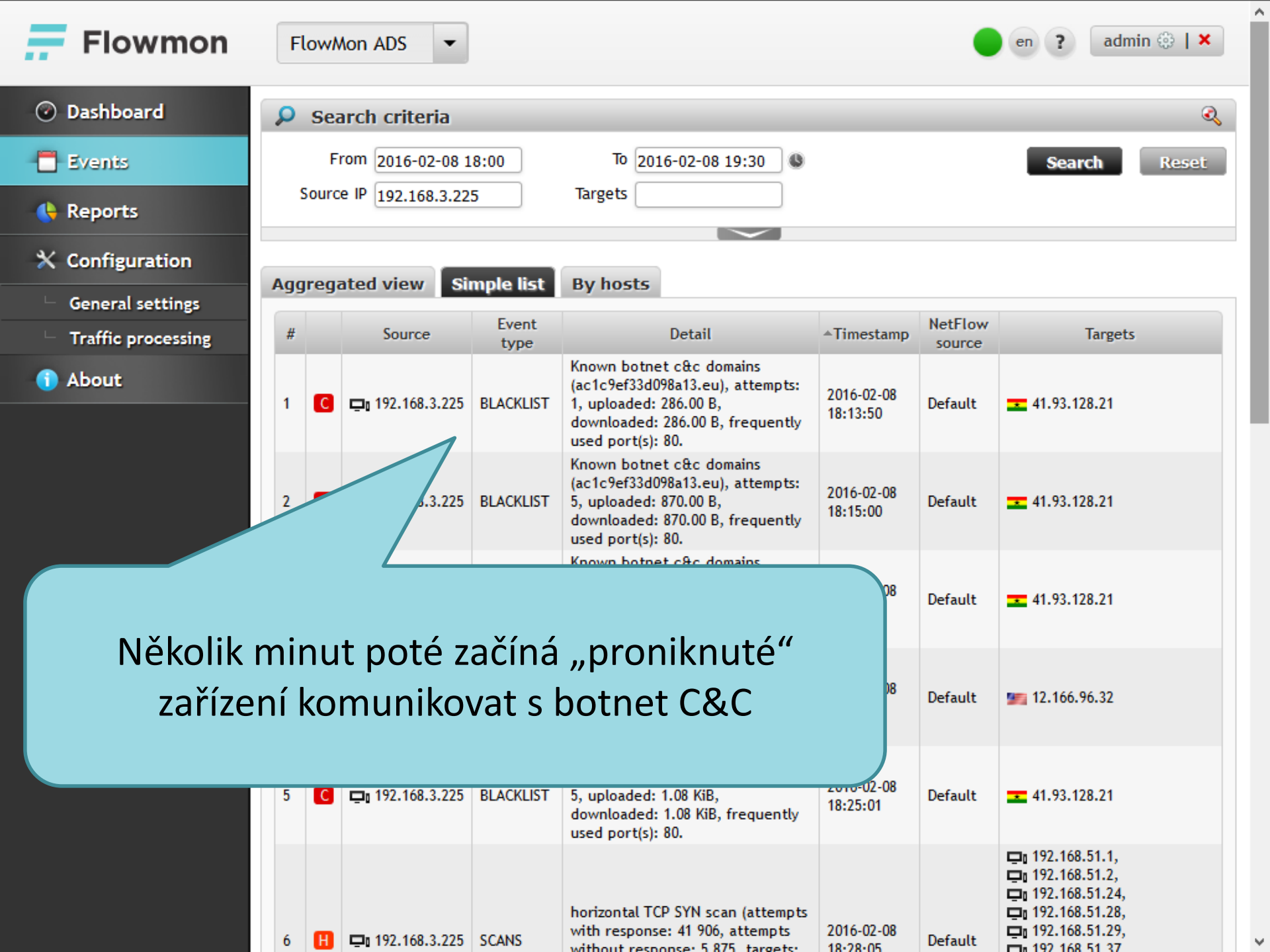
Traffic statistics (2016-02-08 18:00 - 2016-02-08 19:30)

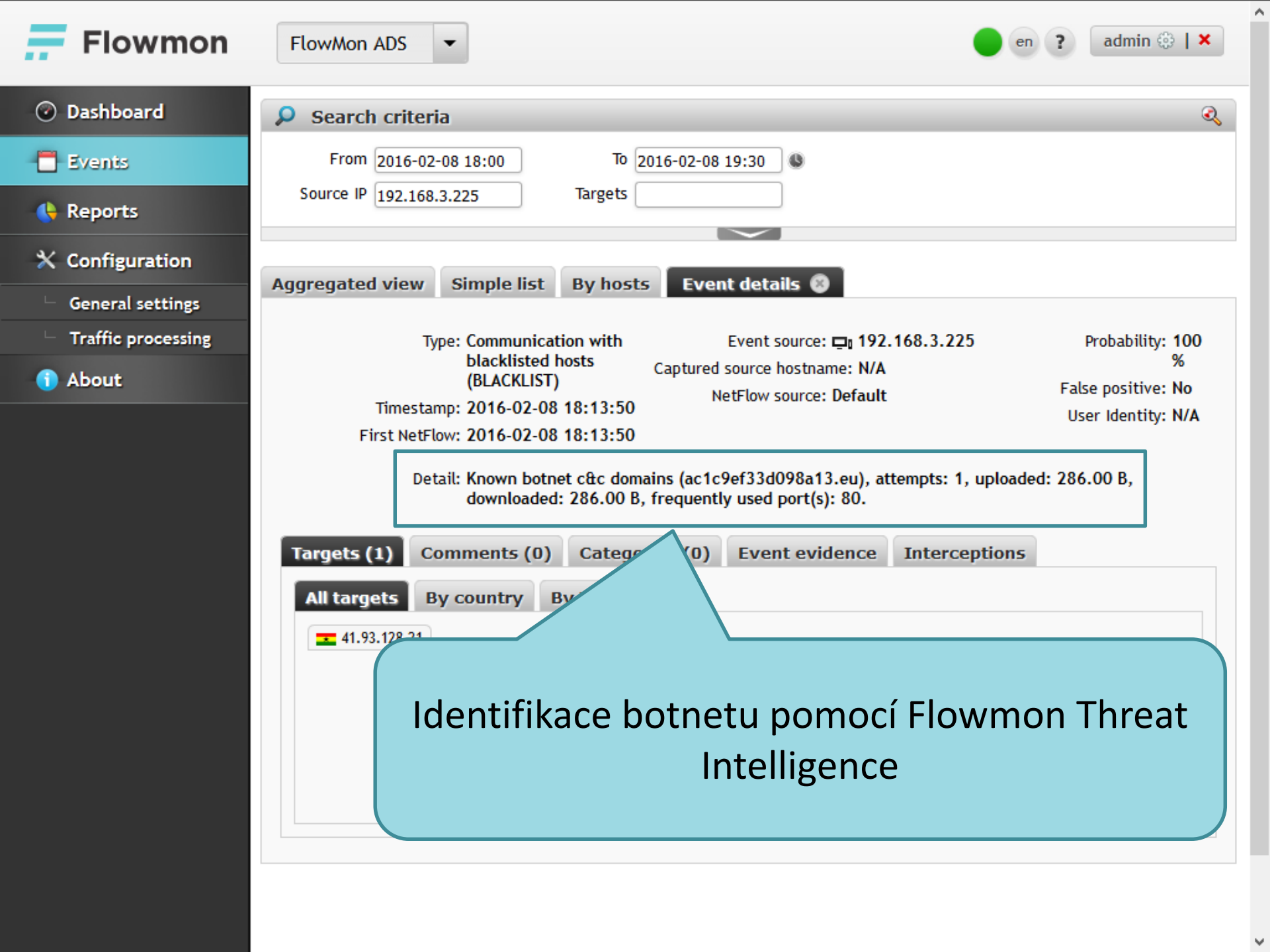
✓	Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
☑	High priority	237.3 K flows	43.935 flows/s	145.1 MiB	27.5 KiB/s	1.9 M packets	356.1 packets/s
☑	Medium priority	0.0 flows	0.000 flows/s	0.0B	0.0B/s	0.0 packets	0.0 packets/s
☑	Low priority	0.0 flows	0.000 flows/s	0.0B	0.0B/s	0.0 packets	0.0 packets/s
☑	Legitimate traffic	791.7 K flows	146.608 flows/s	71.3 GiB	13.5 MiB/s	91.8 M packets	17.0 K packets/s
	Total traffic	1.0 M flows	190.543 flows/s	71.4 GiB	13.5 MiB/s	93.7 M packets	17.4 K packets/s


Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.0.0/16
Search
Reset
Aggregated view
Simple list
By hosts
RDPDICT
ICMPANOM
BLACKLIST
SCANS
SSHDICT
SRVNA
2016-02-08 18:10
2016-02-08 18:30
2016-02-08 18:50
2016-02-08 19:10
192.168.3.225
192.168.3.131
192.168.51.94
Aktivia útočníka (port scan, SSH authentication attack)


Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.0.0/16
Search
Reset
Aggregated view
Simple list
By hosts
RDPDICT
ICMPANOM
BLACKLIST
SCANS
SSHDICT
SRVNA
2016-02-08 18:10
2016-02-08 18:30
2016-02-08 18:50
2016-02-08 19:10
192.168.3.225
192.168.3.131
192.168.51.94
Oběť útoku, zdroj anomálií


Flowmon
FlowMon ADS
en
admin
Dashboard
Search criteria
16-02-08 19:30
Search
Reset
Útočník hledá potenciální oběti
Detail
Timestamp
NetFlow source
Targets
1
192.168.3.131
SCANS
horizontal TCP SYN scan (attempts with response: 121, attempts without response: 202, targets: 73, port(s): 2222, 12221, 22).
2016-02-08 18:00:07
Default
192.168.3.53, 192.168.3.55, 192.168.3.61, 192.168.3.62, 192.168.3.63, 192.168.3.65, 192.168.3.71, 192.168.3.73, 192.168.3.74, 192.168.3.79,
A spouští SSH útok
SSHDICT
Start of attack (unsuccessful), attempts: 161, targets: 14, total upload: 383.13 KiB, maximal upload: 4.22 KiB. Single attack.
2016-02-08 18:00:17
Default
192.168.3.51, 192.168.3.53, 192.168.3.55, 192.168.3.56, 192.168.3.61, 192.168.3.62, 192.168.3.63, 192.168.3.65, 192.168.3.69, 192.168.3.70,
Continuation of attack (successful) to 60 targets (whole attack). Current statistics: attempts: 575, total upload: 1.39 MiB, maximal upload: 4.65 KiB. Single attack.
2016-02-08 18:05:00
Default
End of attack (successful), summary: Total count of targets: 60, maximum transferred: 4.65 KiB, total count of attempts: 736, duration of attack: 512.68 seconds (8m 33s). Single attack.
2016-02-08 18:40:00
Default
Ten se stává úspěšným
About


Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.3.225
Targets
Search
Reset
Aggregated view
Simple list
By hosts
| Source | Event type | Detail | Timestamp | NetFlow source | Targets
1 | 192.168.3.225 | BLACKLIST | Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 1, uploaded: 286.00 B, downloaded: 286.00 B, frequently used port(s): 80. | 2016-02-08 18:13:50 | Default | 41.93.128.21
2 | .3.225 | BLACKLIST | Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 5, uploaded: 870.00 B, downloaded: 870.00 B, frequently used port(s): 80. | 2016-02-08 18:15:00 | Default | 41.93.128.21
Default | 41.93.128.21
Default | 12.166.96.32
5 | 192.168.3.225 | BLACKLIST | 5, uploaded: 1.08 KiB, downloaded: 1.08 KiB, frequently used port(s): 80. | 2016-02-08 18:25:01 | Default | 41.93.128.21
6 | 192.168.3.225 | SCANS | horizontal TCP SYN scan (attempts with response: 41 906, attempts | 2016-02-08 | Default | 192.168.51.1, 192.168.51.2, 192.168.51.24, 192.168.51.28, 192.168.51.29,
Několik minut poté začíná „proniknuté“ zařízení komunikovat s botnet C&C


Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.3.225
Targets
Aggregated view
Simple list
By hosts
Event details
Type: Communication with blacklisted hosts (BLACKLIST)
Timestamp: 2016-02-08 18:13:50
First NetFlow: 2016-02-08 18:13:50
Event source: 192.168.3.225
Captured source hostname: N/A
NetFlow source: Default
Probability: 100 %
False positive: No
User Identity: N/A
Detail: Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 1, uploaded: 286.00 B, downloaded: 286.00 B, frequently used port(s): 80.
Targets (1)
Comments (0)
Event evidence
Interceptions
All targets
By country
Identifikace botnetu pomocí Flowmon Threat Intelligence

Aggregated view | Simple list | By hosts | Event details

Type: Communication with blacklisted hosts (BLACKLIST)
Timestamp: 2016-02-08 18:13:50
First NetFlow: 2016-02-08 18:13:50

Event source: 192.168.3.225
Captured source hostname: N/A
NetFlow source: Default

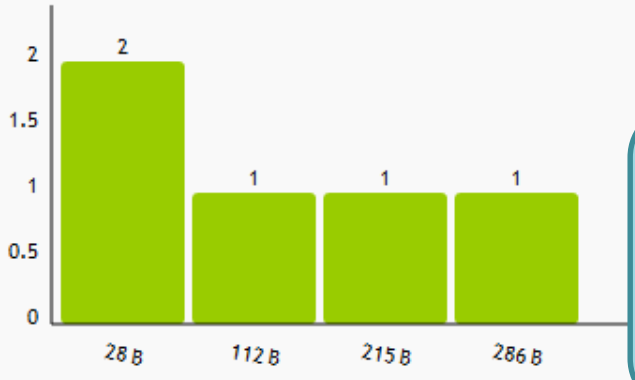
Probability: 100 %
False positive: No
User Identity: N/A

Detail: Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 1, uploaded: 286.00 B, downloaded: 286.00 B, frequently used port(s): 80.

Targets (1) | Comments (0) | Categories (0) | Event evidence | Interceptions

Count of flows due to Transferred

Save as text file
Monitoring center query



Flow data z L2/L3/L4

Filter flows: Show all data

Source IP	Destination IP	Timestamp	Duration	Protocol	Source port	Destination port	Transferred	Packets	Flags
192.168.3.225	41.93.128.21	2016-02-08 18:13:50.058	0	ARP	0	0	28	1	.....
192.168.3.225	41.93.128.21	2016-02-08 18:13:50.059	0.014	ARP	0	0	112	4	.....
41.93.128.21	192.168.3.225	2016-02-08 18:13:50.059	1.002	TCP	80	42711	215	3	...AP.S.
192.168.3.225	41.93.128.21	2016-02-08 18:13:50.059	1.003	TCP	42711	80	286	4	...AP.S.
41.93.128.21	192.168.3.225	2016-02-08 18:13:50.059	0	ARP	0	0	28	1	.....

Aggregated view | Simple list | By hosts | Event details

Type: Communication with blacklisted hosts (BLACKLIST)
Timestamp: 2016-02-08 18:13:50
First NetFlow: 2016-02-08 18:13:50

Event source: 192.168.3.225
Captured source hostname: N/A
NetFlow source: Default

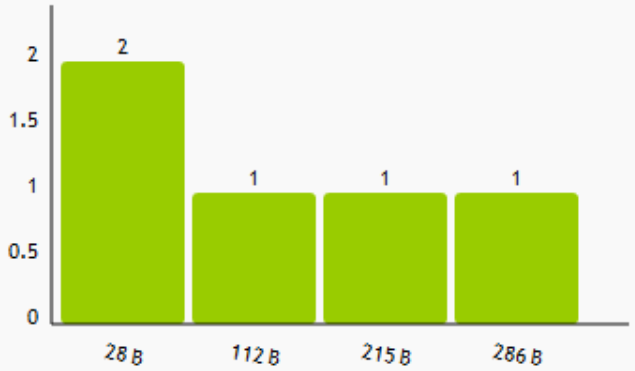
Probability: 100 %
False positive: No
User Identity: N/A

Detail: Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 1, uploaded: 286.00 B, downloaded: 286.00 B, frequently used port(s): 80.

Targets (1) | Comments (0) | Categories (0) | Event evidence | Interceptions

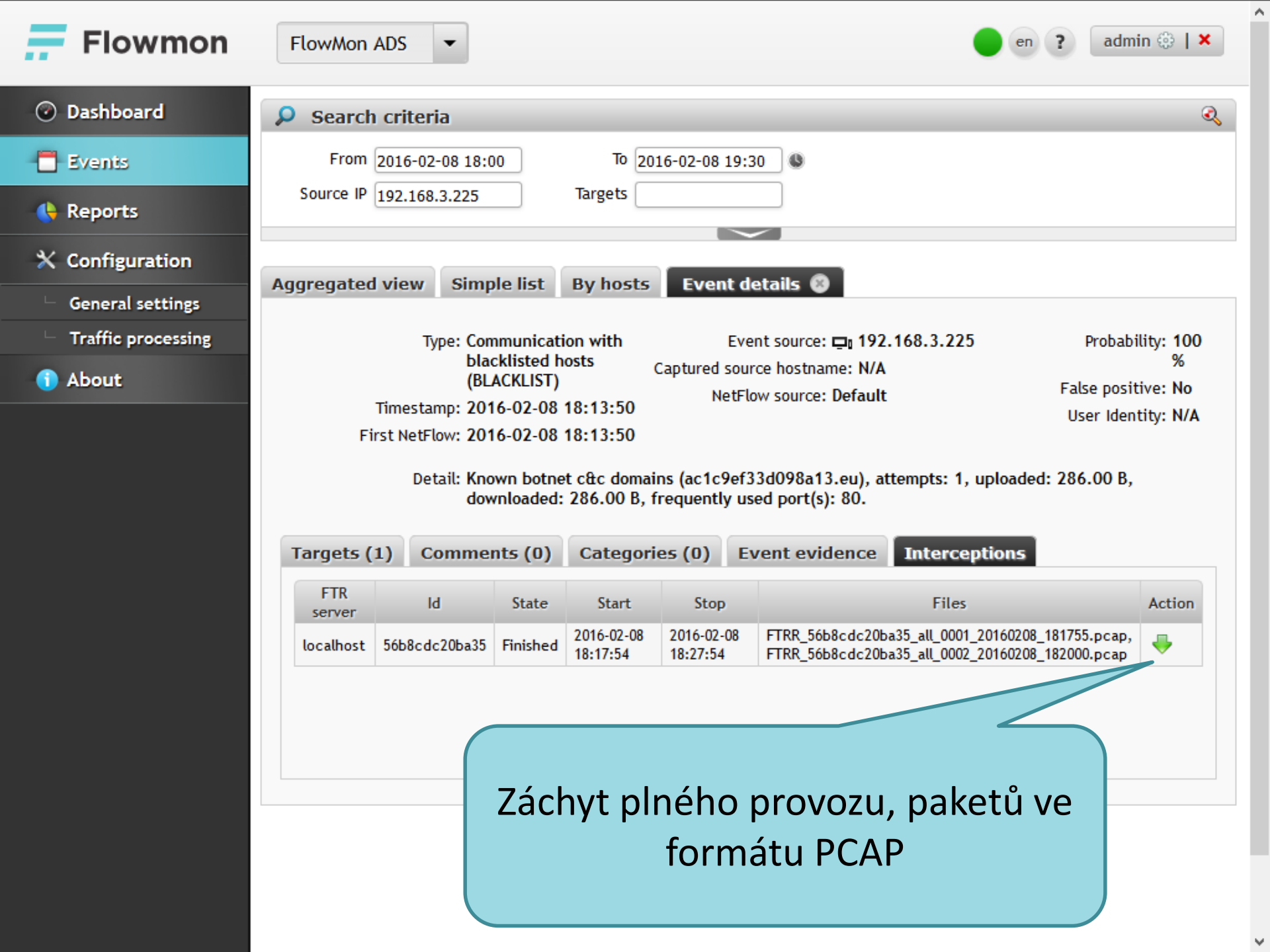
Count of flows due to Transferred

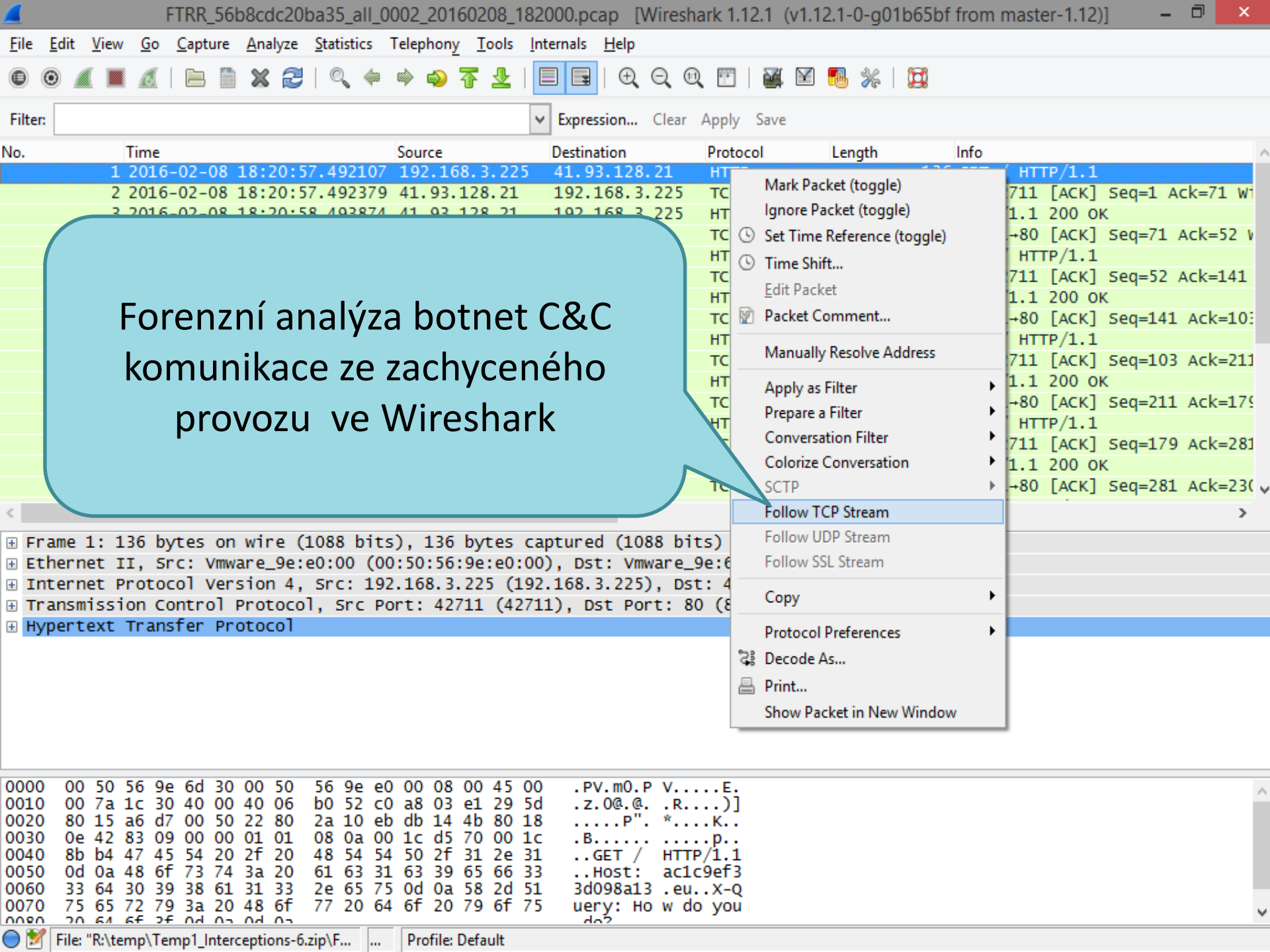
Save as text file
Monitoring center query

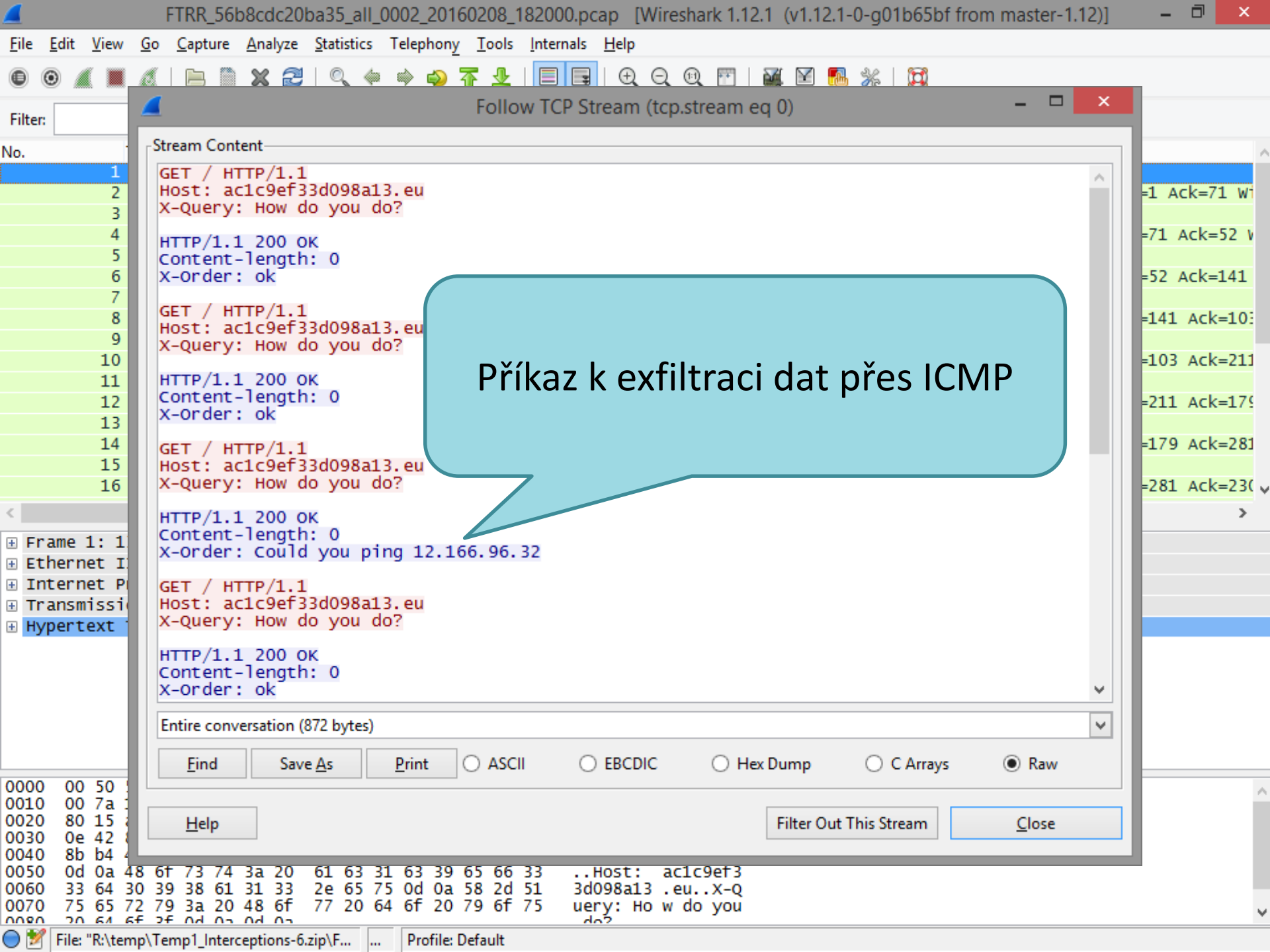


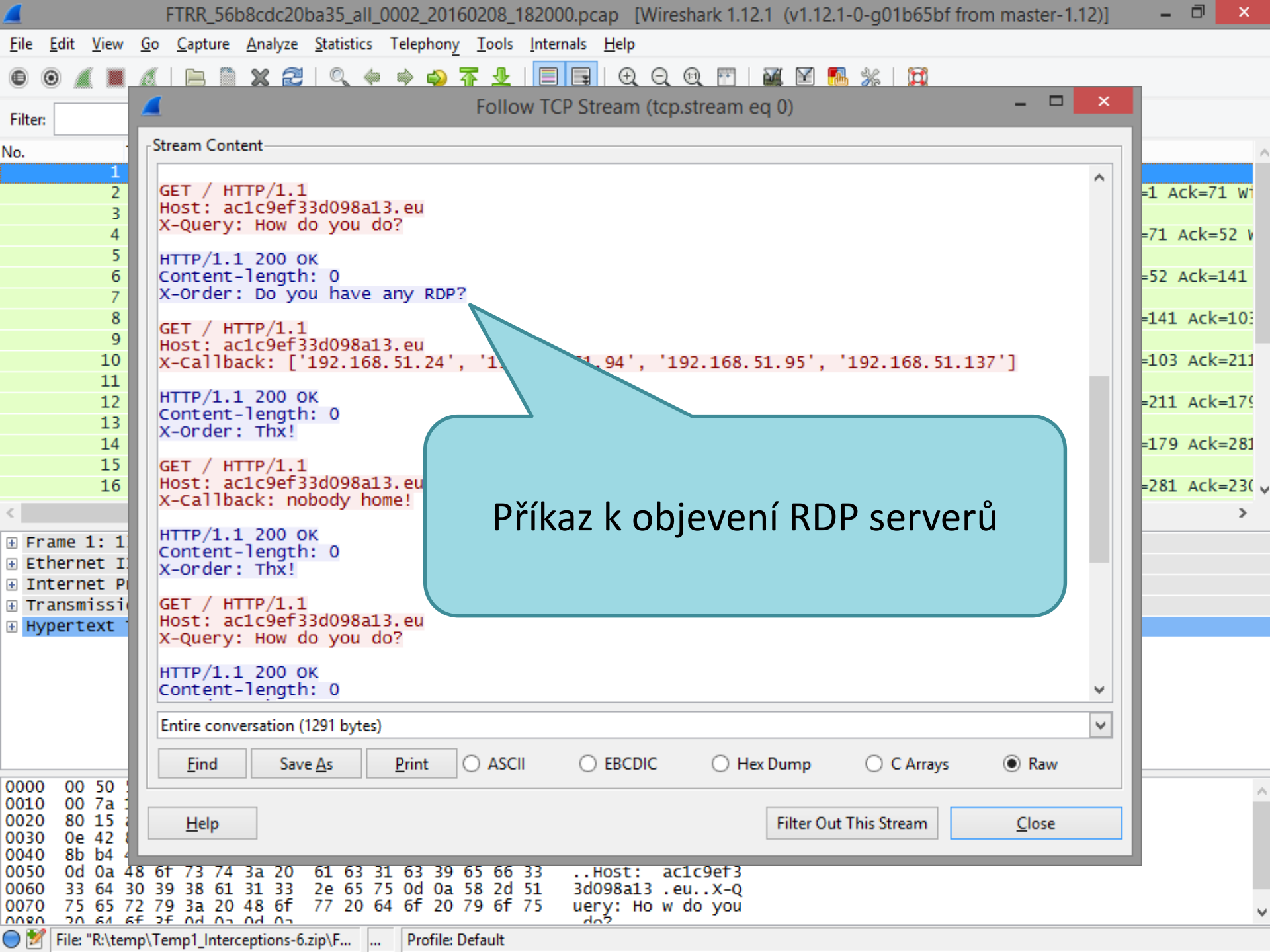
Včetně viditelnosti do L7

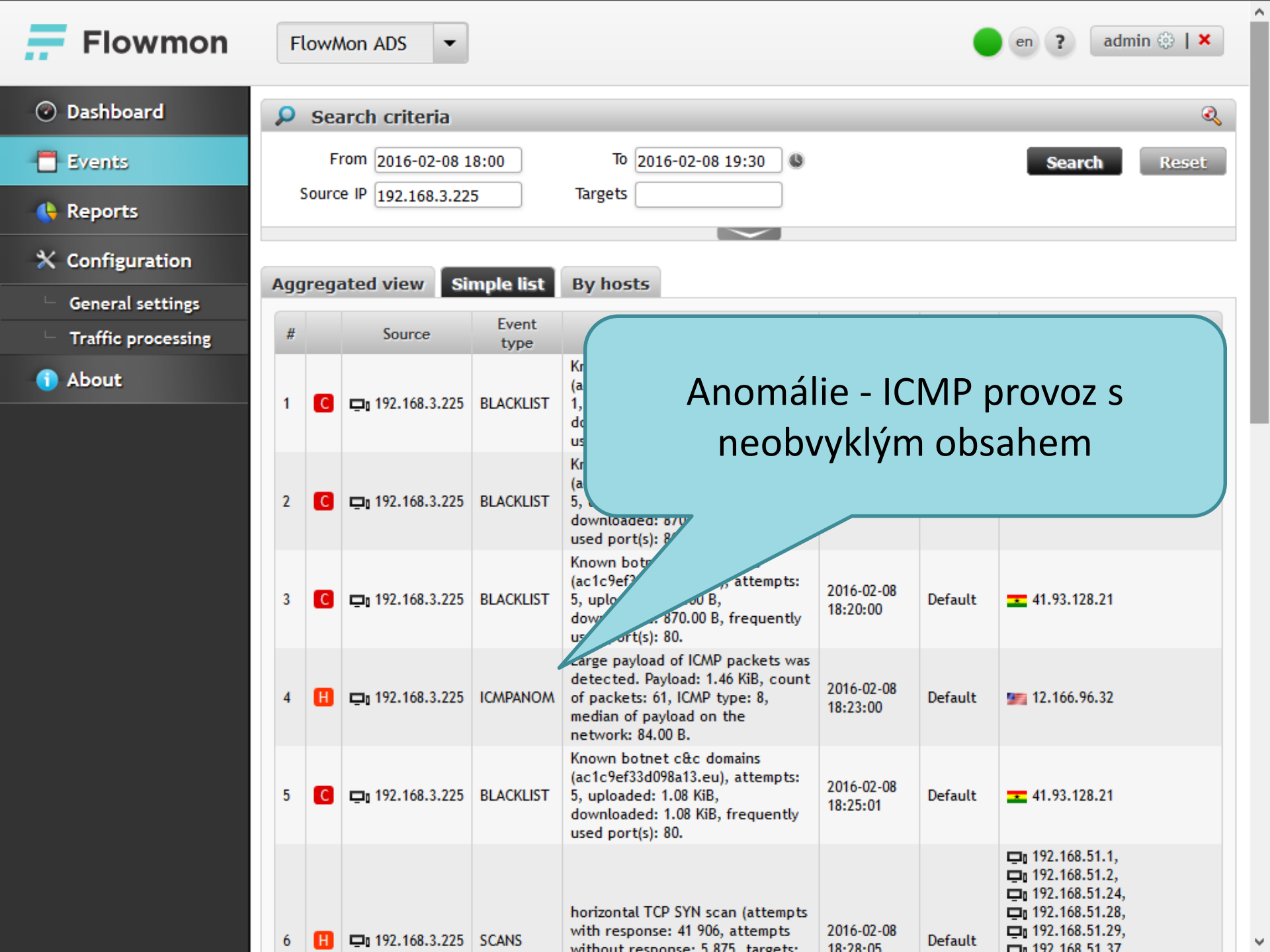
on	Transferred	Packets	Flags	TOS	Source MAC	Destination MAC		HTTP host	URL	Flow source IP address
0	28	1	.....	0	00:50:56:9e:e0:00	00:00:00:00:00:00	0:			192.168.3.242
0	112	4	.....	0	00:50:56:9e:e0:00	00:00:00:00:00:00	0:0			192.168.3.242
11	215	3	...AP.S.	0	00:50:56:9e:6d:30	00:50:56:9e:e0:00	3:80			192.168.3.242
80	286	4	...AP.S.	0	00:50:56:9e:e0:00	00:50:56:9e:6d:30	3:80	ac1c9ef33d098a13.eu	/	192.168.3.242
0	28	1	.....	0	00:50:56:9e:6d:30	00:50:56:9e:e0:00	0:0			192.168.3.242

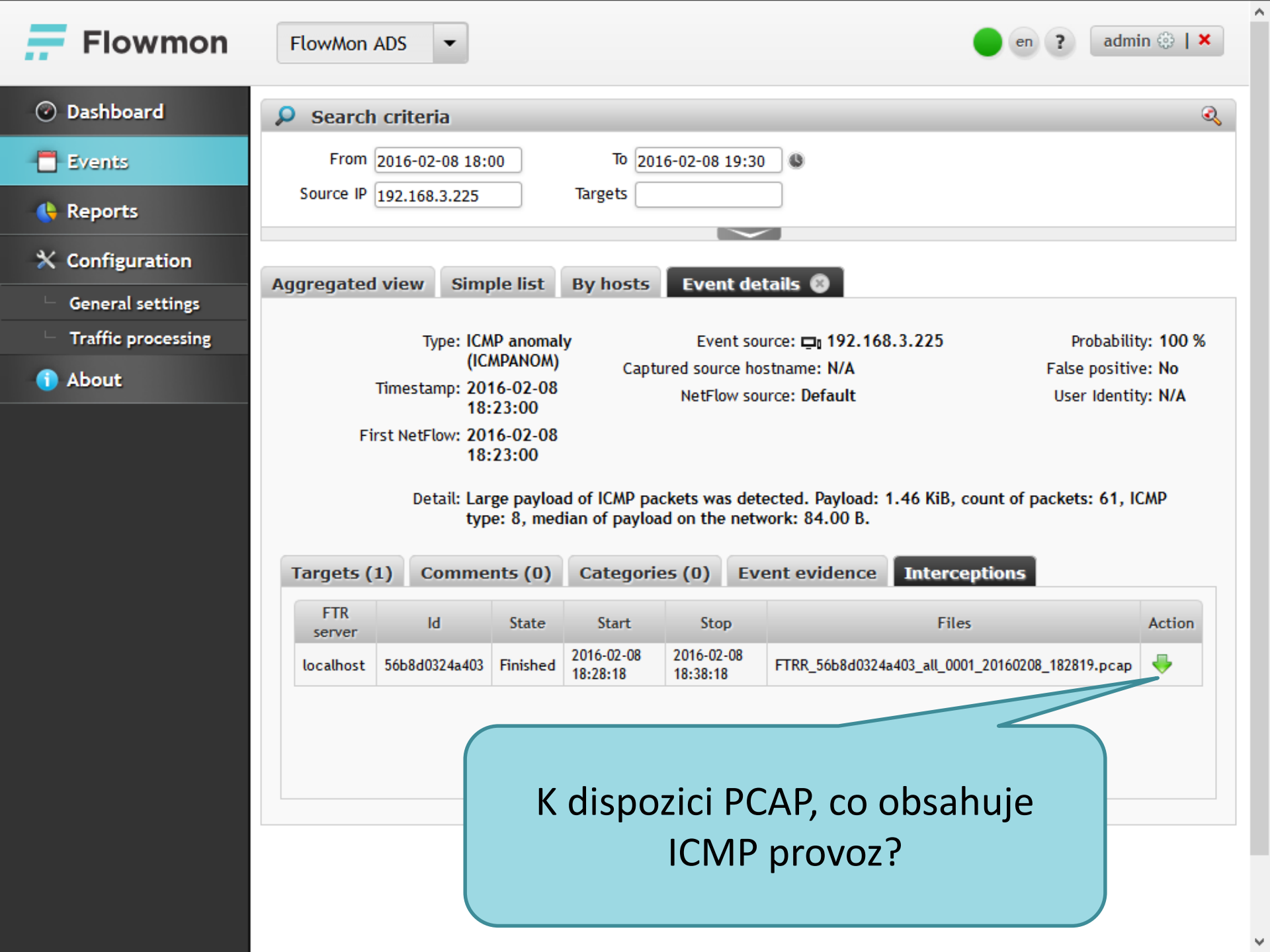

Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.3.225
Targets
Aggregated view
Simple list
By hosts
Event details
Type: Communication with blacklisted hosts (BLACKLIST)
Timestamp: 2016-02-08 18:13:50
First NetFlow: 2016-02-08 18:13:50
Event source: 192.168.3.225
Captured source hostname: N/A
NetFlow source: Default
Probability: 100 %
False positive: No
User Identity: N/A
Detail: Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 1, uploaded: 286.00 B, downloaded: 286.00 B, frequently used port(s): 80.
Targets (1)
Comments (0)
Categories (0)
Event evidence
Interceptions
FTR server
Id
State
Start
Stop
Files
Action
localhost
56b8cdc20ba35
Finished
2016-02-08 18:17:54
2016-02-08 18:27:54
FTRR_56b8cdc20ba35_all_0001_20160208_181755.pcap, FTRR_56b8cdc20ba35_all_0002_20160208_182000.pcap
Záchyt plného provozu, paketů ve formátu PCAP

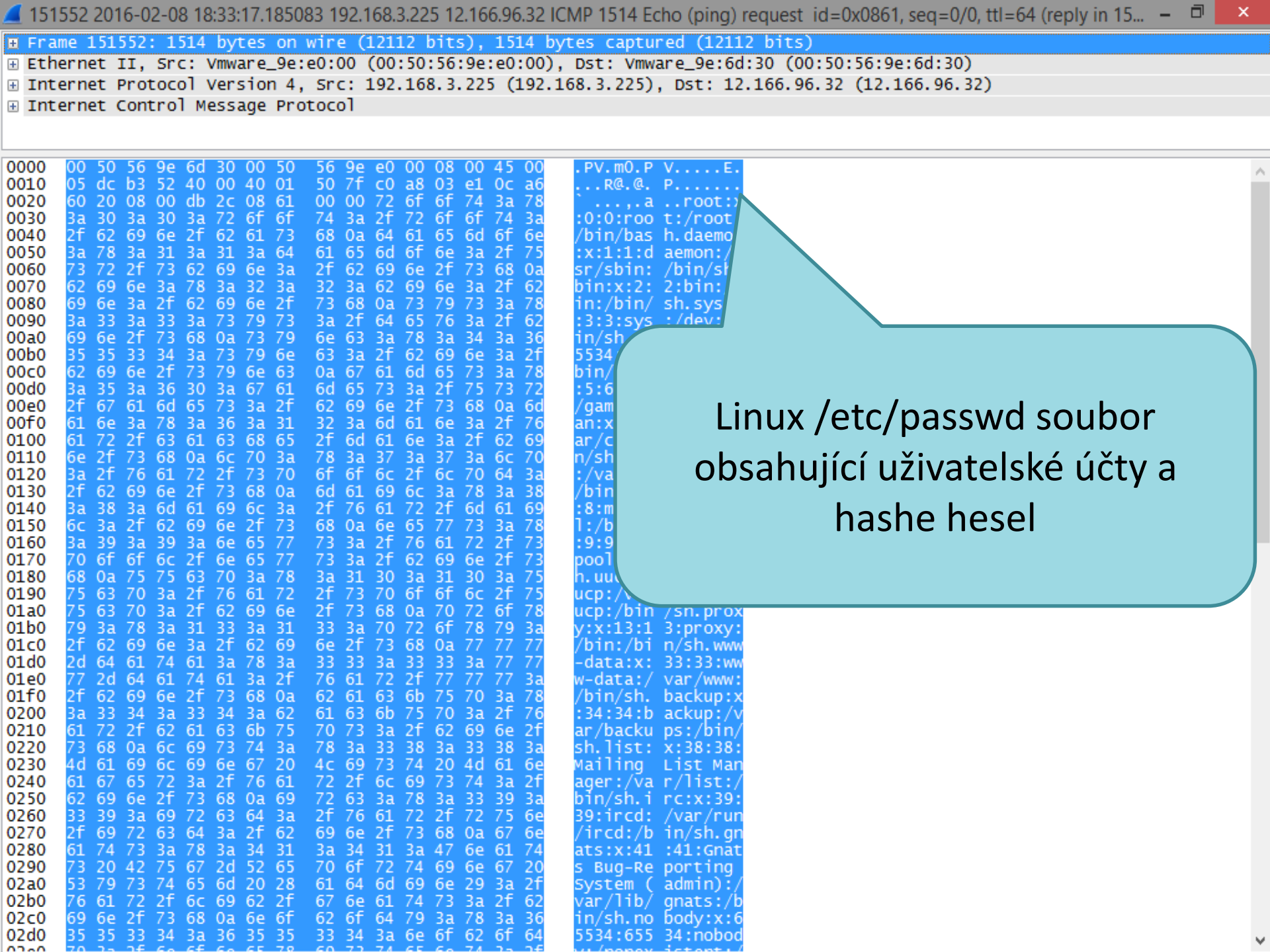

FTRR_56b8cdc20ba35_all_0002_20160208_182000.pcap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 2016-02-08 18:20:57.492107 192.168.3.225 41.93.128.21 HTTP/1.1
2 2016-02-08 18:20:57.492379 41.93.128.21 192.168.3.225
Forenzní analýza botnet C&C komunikace ze zachyceného provozu ve Wireshark
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Protocol Preferences
Decode As...
Print...
Show Packet in New Window
Frame 1: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits)
Ethernet II, Src: Vmware_9e:e0:00 (00:50:56:9e:e0:00), Dst: Vmware_9e:6
Internet Protocol Version 4, Src: 192.168.3.225 (192.168.3.225), Dst: 4
Transmission Control Protocol, Src Port: 42711 (42711), Dst Port: 80 (8
Hypertext Transfer Protocol
0000 00 50 56 9e 6d 30 00 50 56 9e e0 00 08 00 45 00 .PV.m0.P V.....E.
0010 00 7a 1c 30 40 00 40 06 b0 52 c0 a8 03 e1 29 5d .z.0@.@. .R....)]
0020 80 15 a6 d7 00 50 22 80 2a 10 eb db 14 4b 80 18 .....P". *....K..
0030 0e 42 83 09 00 00 01 01 08 0a 00 1c d5 70 00 1c .B..... .....p..
0040 8b b4 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 61 63 31 63 39 65 66 33 ..Host: ac1c9ef3
0060 33 64 30 39 38 61 31 33 2e 65 75 0d 0a 58 2d 51 3d098a13 .eu..X-Q
0070 75 65 72 79 3a 20 48 6f 77 20 64 6f 20 79 6f 75 uery: Ho w do you
File: "R:\temp\Temp1_Interceptions-6.zip\F...
Profile: Default


FTRR_56b8cdc20ba35_all_0002_20160208_182000.pcap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
No.
Follow TCP Stream (tcp.stream eq 0)
Stream Content
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Query: How do you do?
HTTP/1.1 200 OK
Content-length: 0
X-Order: ok
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Query: How do you do?
HTTP/1.1 200 OK
Content-length: 0
X-Order: ok
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Query: How do you do?
HTTP/1.1 200 OK
Content-length: 0
X-Order: Could you ping 12.166.96.32
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Query: How do you do?
HTTP/1.1 200 OK
Content-length: 0
X-Order: ok
Příkaz k exfiltraci dat přes ICMP
Entire conversation (872 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close
Frame 1: 1
Ethernet I
Internet P
Transmissi
Hypertext
0000 00 50
0010 00 7a
0020 80 15
0030 0e 42
0040 8b b4
0050 0d 0a 48 6f 73 74 3a 20 61 63 31 63 39 65 66 33 ..Host: ac1c9ef3
0060 33 64 30 39 38 61 31 33 2e 65 75 0d 0a 58 2d 51 3d098a13 .eu..X-Q
0070 75 65 72 79 3a 20 48 6f 77 20 64 6f 20 79 6f 75 uery: Ho w do you
File: "R:\temp\Temp1_Interceptions-6.zip\F...
Profile: Default


FTRR_56b8cdc20ba35_all_0002_20160208_182000.pcap [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
No.
Follow TCP Stream (tcp.stream eq 0)
Stream Content
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Query: How do you do?
HTTP/1.1 200 OK
Content-length: 0
X-Order: Do you have any RDP?
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Callback: ['192.168.51.24', '1
.94', '192.168.51.95', '192.168.51.137']
HTTP/1.1 200 OK
Content-length: 0
X-Order: Thx!
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Callback: nobody home!
HTTP/1.1 200 OK
Content-length: 0
X-Order: Thx!
GET / HTTP/1.1
Host: ac1c9ef33d098a13.eu
X-Query: How do you do?
HTTP/1.1 200 OK
Content-length: 0
Příkaz k objevení RDP serverů
Entire conversation (1291 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close
Frame 1: 1
Ethernet I
Internet P
Transmissi
Hypertext
0000 00 50
0010 00 7a
0020 80 15
0030 0e 42
0040 8b b4
0050 0d 0a 48 6f 73 74 3a 20 61 63 31 63 39 65 66 33 ..Host: ac1c9ef3
0060 33 64 30 39 38 61 31 33 2e 65 75 0d 0a 58 2d 51 3d098a13 .eu..X-Q
0070 75 65 72 79 3a 20 48 6f 77 20 64 6f 20 79 6f 75 uery: Ho w do you
File: "R:\temp\Temp1_Interceptions-6.zip\F...
Profile: Default


Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.3.225
Targets
Search
Reset
Aggregated view
Simple list
By hosts
Source Event type
1 C 192.168.3.225 BLACKLIST
2 C 192.168.3.225 BLACKLIST
3 C 192.168.3.225 BLACKLIST Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 5, uploaded: 1.08 KiB, downloaded: 870.00 B, frequently used port(s): 80. 2016-02-08 18:20:00 Default 41.93.128.21
4 H 192.168.3.225 ICMPANOM Large payload of ICMP packets was detected. Payload: 1.46 KiB, count of packets: 61, ICMP type: 8, median of payload on the network: 84.00 B. 2016-02-08 18:23:00 Default 12.166.96.32
5 C 192.168.3.225 BLACKLIST Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 5, uploaded: 1.08 KiB, downloaded: 1.08 KiB, frequently used port(s): 80. 2016-02-08 18:25:01 Default 41.93.128.21
6 H 192.168.3.225 SCANS horizontal TCP SYN scan (attempts with response: 41 906, attempts 2016-02-08 Default 192.168.51.1, 192.168.51.2, 192.168.51.24, 192.168.51.28, 192.168.51.29,
Anomálie - ICMP provoz s neobvyklým obsahem


Flowmon
FlowMon ADS
en
admin
Dashboard
Events
Reports
Configuration
General settings
Traffic processing
About
Search criteria
From 2016-02-08 18:00
To 2016-02-08 19:30
Source IP 192.168.3.225
Targets
Aggregated view
Simple list
By hosts
Event details
Type: ICMP anomaly (ICMPANOM)
Timestamp: 2016-02-08 18:23:00
First NetFlow: 2016-02-08 18:23:00
Event source: 192.168.3.225
Captured source hostname: N/A
NetFlow source: Default
Probability: 100 %
False positive: No
User Identity: N/A
Detail: Large payload of ICMP packets was detected. Payload: 1.46 KiB, count of packets: 61, ICMP type: 8, median of payload on the network: 84.00 B.
Targets (1)
Comments (0)
Categories (0)
Event evidence
Interceptions
FTR server
Id
State
Start
Stop
Files
Action
localhost
56b8d0324a403
Finished
2016-02-08 18:28:18
2016-02-08 18:38:18
FTRR_56b8d0324a403_all_0001_20160208_182819.pcap
K dispozici PCAP, co obsahuje ICMP provoz?


151552 2016-02-08 18:33:17.185083 192.168.3.225 12.166.96.32 ICMP 1514 Echo (ping) request id=0x0861, seq=0/0, ttl=64 (reply in 15...
Frame 151552: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Vmware_9e:e0:00 (00:50:56:9e:e0:00), Dst: Vmware_9e:6d:30 (00:50:56:9e:6d:30)
Internet Protocol Version 4, Src: 192.168.3.225 (192.168.3.225), Dst: 12.166.96.32 (12.166.96.32)
Internet Control Message Protocol
0000 00 50 56 9e 6d 30 00 50 56 9e e0 00 08 00 45 00 .PV.m0.P V.....E.
0010 05 dc b3 52 40 00 40 01 50 7f c0 a8 03 e1 0c a6 ...R@.@. P.......
0020 60 20 08 00 db 2c 08 61 00 00 72 6f 6f 74 3a 78 ` ...,.a ..root:x
0030 3a 30 3a 30 3a 72 6f 6f 74 3a 2f 72 6f 6f 74 3a :0:0:roo t:/root:
0040 2f 62 69 6e 2f 62 61 73 68 0a 64 61 65 6d 6f 6e /bin/bas h.daemon
0050 3a 78 3a 31 3a 31 3a 64 61 65 6d 6f 6e 3a 2f 75 :x:1:1:d aemon:/u
0060 73 72 2f 73 62 69 6e 3a 2f 62 69 6e 2f 73 68 0a sr/sbin: /bin/sh.
0070 62 69 6e 3a 78 3a 32 3a 32 3a 62 69 6e 3a 2f 62 bin:x:2: 2:bin:/b
0080 69 6e 3a 2f 62 69 6e 2f 73 68 0a 73 79 73 3a 78 in:/bin/ sh.sys:x
0090 3a 33 3a 33 3a 73 79 73 3a 2f 64 65 76 3a 2f 62 :3:3:sys :/dev:/b
00a0 69 6e 2f 73 68 0a 73 79 6e 63 3a 78 3a 34 3a 36 in/sh.sy nc:x:4:6
00b0 35 35 33 34 3a 73 79 6e 63 3a 2f 62 69 6e 2f 73 5534:syn c:/bin/s
00c0 62 69 6e 2f 73 79 6e 63 0a 67 61 6d 65 73 3a 78 bin/sync .games:x
00d0 3a 35 3a 36 30 3a 67 61 6d 65 73 3a 2f 75 73 72 :5:60:ga mes:/usr
00e0 2f 67 61 6d 65 73 3a 2f 62 69 6e 2f 73 68 0a 6d /games:/ bin/sh.m
00f0 61 6e 3a 78 3a 36 3a 31 32 3a 6d 61 6e 3a 2f 76 an:x:6:1 2:man:/v
0100 61 72 2f 63 61 63 68 65 2f 6d 61 6e 3a 2f 62 69 ar/cache /man:/bi
0110 6e 2f 73 68 0a 6c 70 3a 78 3a 37 3a 37 3a 6c 70 n/sh.lp :x:7:7:lp
0120 3a 2f 76 61 72 2f 73 70 6f 6f 6c 2f 6c 70 64 3a :/var/sp ool/lpd:
0130 2f 62 69 6e 2f 73 68 0a 6d 61 69 6c 3a 78 3a 38 /bin/sh. mail:x:8
0140 3a 38 3a 6d 61 69 6c 3a 2f 76 61 72 2f 6d 61 69 :8:mail: /var/mai
0150 6c 3a 2f 62 69 6e 2f 73 68 0a 6e 65 77 73 3a 78 l:/bin/s h.news:x
0160 3a 39 3a 39 3a 6e 65 77 73 3a 2f 76 61 72 2f 73 :9:9:new s:/var/s
0170 70 6f 6f 6c 2f 6e 65 77 73 3a 2f 62 69 6e 2f 73 pool/new s:/bin/s
0180 68 0a 75 75 63 70 3a 78 3a 31 30 3a 31 30 3a 75 h.uucp:x :10:10:u
0190 75 63 70 3a 2f 76 61 72 2f 73 70 6f 6f 6c 2f 75 ucp:/var /spool/u
01a0 75 63 70 3a 2f 62 69 6e 2f 73 68 0a 70 72 6f 78 ucp:/bin /sh.prox
01b0 79 3a 78 3a 31 33 3a 31 33 3a 70 72 6f 78 79 3a y:x:13:1 3:proxy:
01c0 2f 62 69 6e 3a 2f 62 69 6e 2f 73 68 0a 77 77 77 /bin:/bi n/sh.www
01d0 2d 64 61 74 61 3a 78 3a 33 33 3a 33 33 3a 77 77 -data:x: 33:33:ww
01e0 77 2d 64 61 74 61 3a 2f 76 61 72 2f 77 77 77 3a w-data:/ var/www:
01f0 2f 62 69 6e 2f 73 68 0a 62 61 63 6b 75 70 3a 78 /bin/sh. backup:x
0200 3a 33 34 3a 33 34 3a 62 61 63 6b 75 70 3a 2f 76 :34:34:b ackup:/v
0210 61 72 2f 62 61 63 6b 75 70 73 3a 2f 62 69 6e 2f ar/backu ps:/bin/
0220 73 68 0a 6c 69 73 74 3a 78 3a 33 38 3a 33 38 3a sh.list: x:38:38:
0230 4d 61 69 6c 69 6e 67 20 4c 69 73 74 20 4d 61 6e Mailing List Man
0240 61 67 65 72 3a 2f 76 61 72 2f 6c 69 73 74 3a 2f ager:/va r/list:/
0250 62 69 6e 2f 73 68 0a 69 72 63 3a 78 3a 33 39 3a bin/sh.i rc:x:39:
0260 33 39 3a 69 72 63 64 3a 2f 76 61 72 2f 72 75 6e 39:ircd: /var/run
0270 2f 69 72 63 64 3a 2f 62 69 6e 2f 73 68 0a 67 6e /ircd:/b in/sh.gn
0280 61 74 73 3a 78 3a 34 31 3a 34 31 3a 47 6e 61 74 ats:x:41 :41:Gnat
0290 73 20 42 75 67 2d 52 65 70 6f 72 74 69 6e 67 20 s Bug-Re porting
02a0 53 79 73 74 65 6d 20 28 61 64 6d 69 6e 29 3a 2f System (admin):/
02b0 76 61 72 2f 6c 69 62 2f 67 6e 61 74 73 3a 2f 62 var/lib/ gnats:/b
02c0 69 6e 2f 73 68 0a 6e 6f 62 6f 64 79 3a 78 3a 36 in/sh.no body:x:6
02d0 35 35 33 34 3a 36 35 35 33 34 3a 6e 6f 62 6f 64 5534:655 34:nobod
Linux /etc/passwd soubor obsahující uživatelské účty a hashe hesel

Hledání Windows serverů s RDP

				used port(s): 80.			
3	C	192.168.3.225	BLACKLIST	Known botnet c&c domains (ac1c9ef33d098a13.eu), attempts: 5, uploaded: 870.00 B, downloaded: 870.00 B, frequently	2016-02-08 18:20:00	Default	41.93.128.21
				MP packets was : 1.46 KiB, count MP type: 8, on the	2016-02-08 18:23:00	Default	12.166.96.32
				domains .eu), attempts: KiB, KiB, frequently ed port(s): 80.	2016-02-08 18:25:01	Default	41.93.128.21
6	H	192.168.3.225	SCANS	horizontal TCP SYN scan (attempts with response: 41 906, attempts without response: 5 875, targets: 97, port(s): 3389).	2016-02-08 18:28:05	Default	192.168.51.1, 192.168.51.2, 192.168.51.24, 192.168.51.28, 192.168.51.29, 192.168.51.37, 192.168.51.57, 192.168.51.72, 192.168.51.79, 192.168.51.89, ...
7	C	192.168.3.225	RDPDICT	Continuation of attack to 2 targets (whole attack). Current statistics: attempts: 178, total upload: 785.19 KiB, maximal load: 10.07 KiB. Single attack.	2016-02-08 18:28:08	Default	192.168.51.24, 192.168.51.137
8	C	192.168.3.225	BLACKLIST	Kn tnet c&c domains (ac1c 13.eu), attempts: 4, uploa downloade ently used port(s):	2016-02-08 18:30:13	Default	41.93.128.21
9	H	192.168.3.225	ICMPANOM	La			
10	C	192.168.3.225	BLACKLIST				
							192.168.51.1, 192.168.51.2,

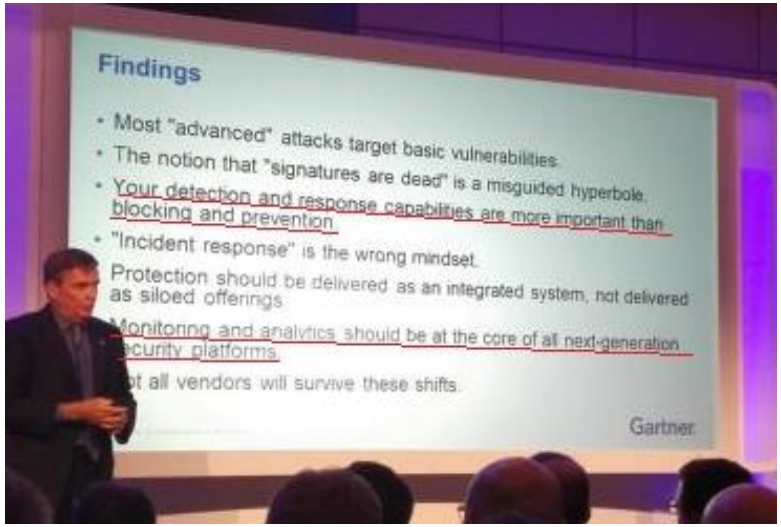
Útok na RDP služby

Shrnutí

Analýza chování sítě

Flowmon Networks

Gartner



Neil MacDonald
VP Distinguished Analyst
Gartner Security & Risk Management Summit

Recommendation

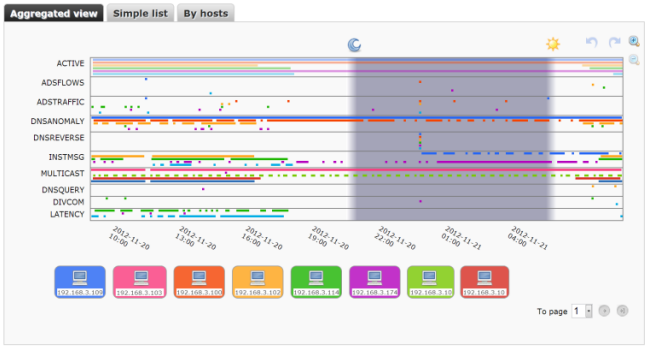
After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques.

- *Schopnost detekce a reakce je důležitější než blokování a prevence.*
- *Monitoring a analýza sítě by měly tvořit základ všech next-generation bezpečnostních platforem.*

Flowmon ADS

Flowmon Networks

- Analýza chování a detekce anomálií
  - Detekce a upozornění na abnormální chování
  - Reporting anomálií a APT
  - Detekce průniků a útoků nerozpoznatelných standardními nástroji využívajícími signatury



Děkuji za pozornost!

Flowmon Networks

Flowmon Networks

Driving Network Visibility

Luboš Lunter
lubos.lunter@flowmon.com
+420 779 970 084

Flowmon Networks a.s.
U Vodarny 2965/2
616 00 Brno, Czech Republic
www.flowmon.com