Network Security Monitoring and Behavior Analysis

Pavel Čeleda

celeda@ics.muni.cz

Workshop on Campus Network Monitoring, 24-25 April 2012, Brno, Czech Republic

Part I

Introduction

Security Monitoring and Behavior Analysis Toolset

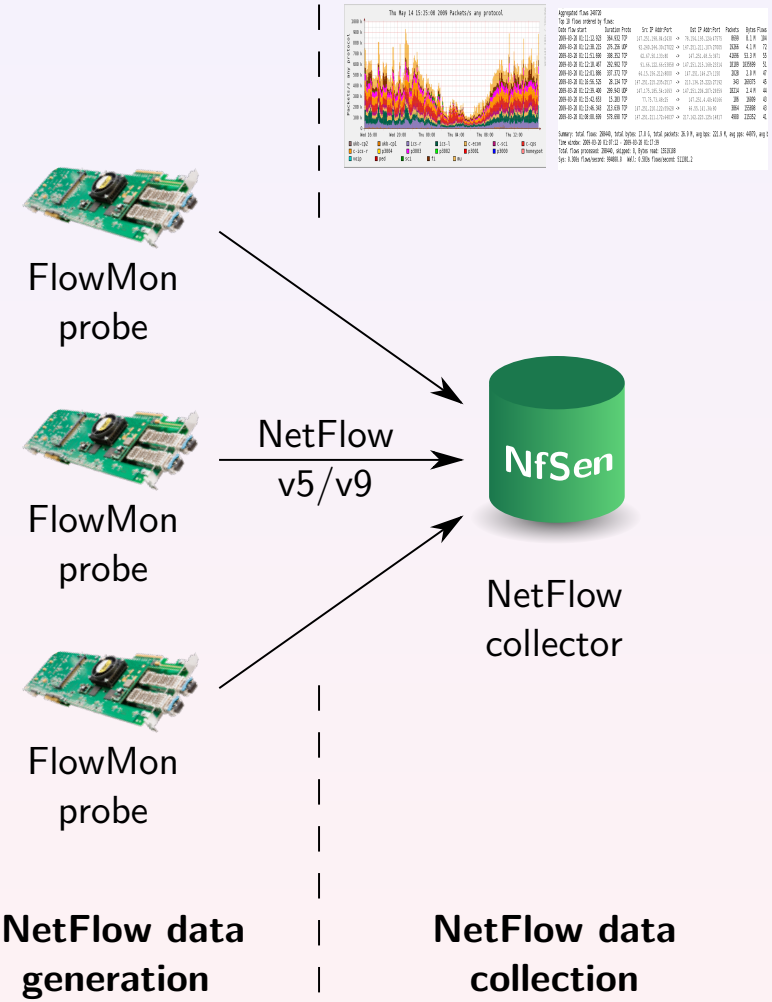
FlowMon probe

FlowMon probe

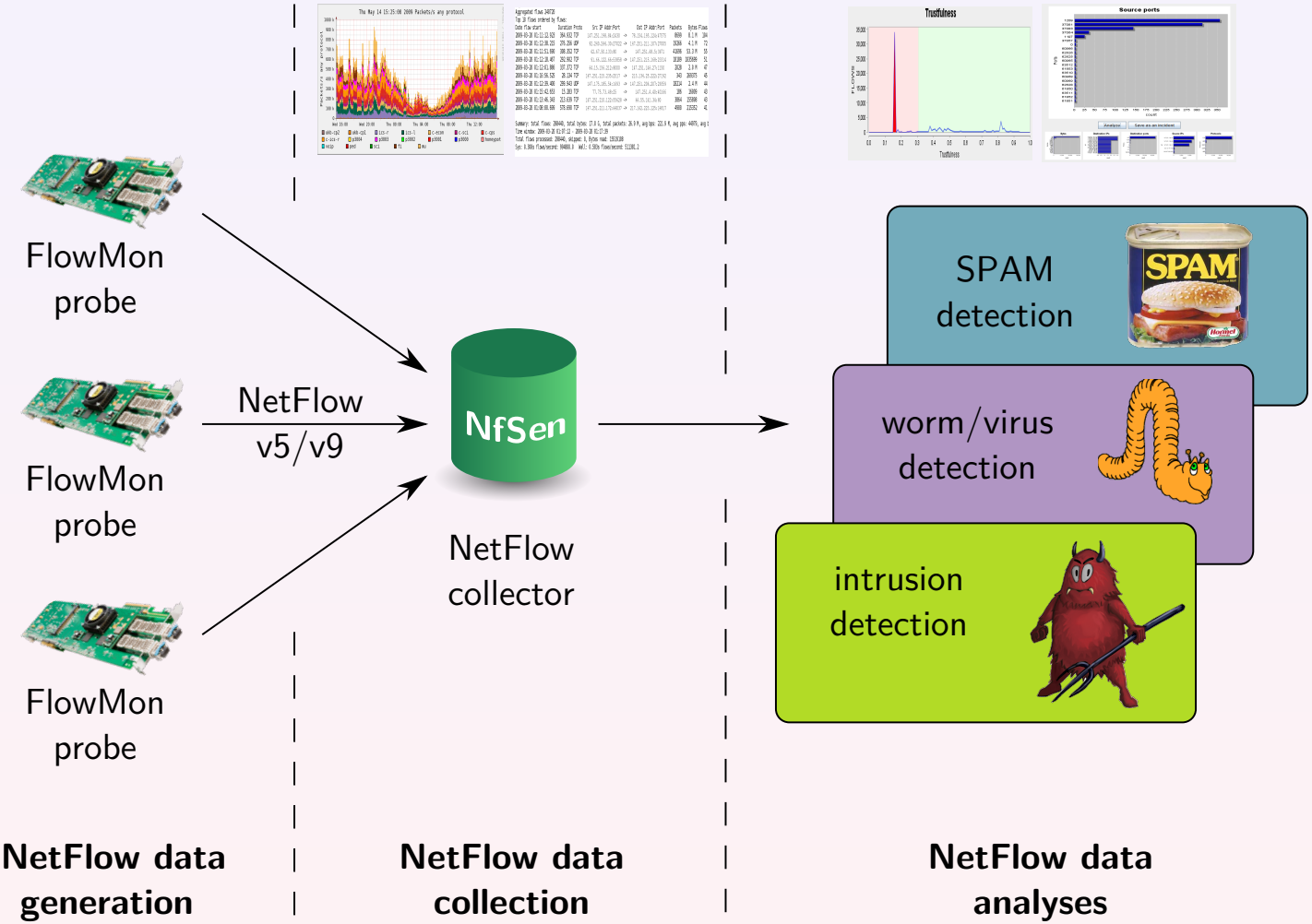
FlowMon probe

NetFlow data generation

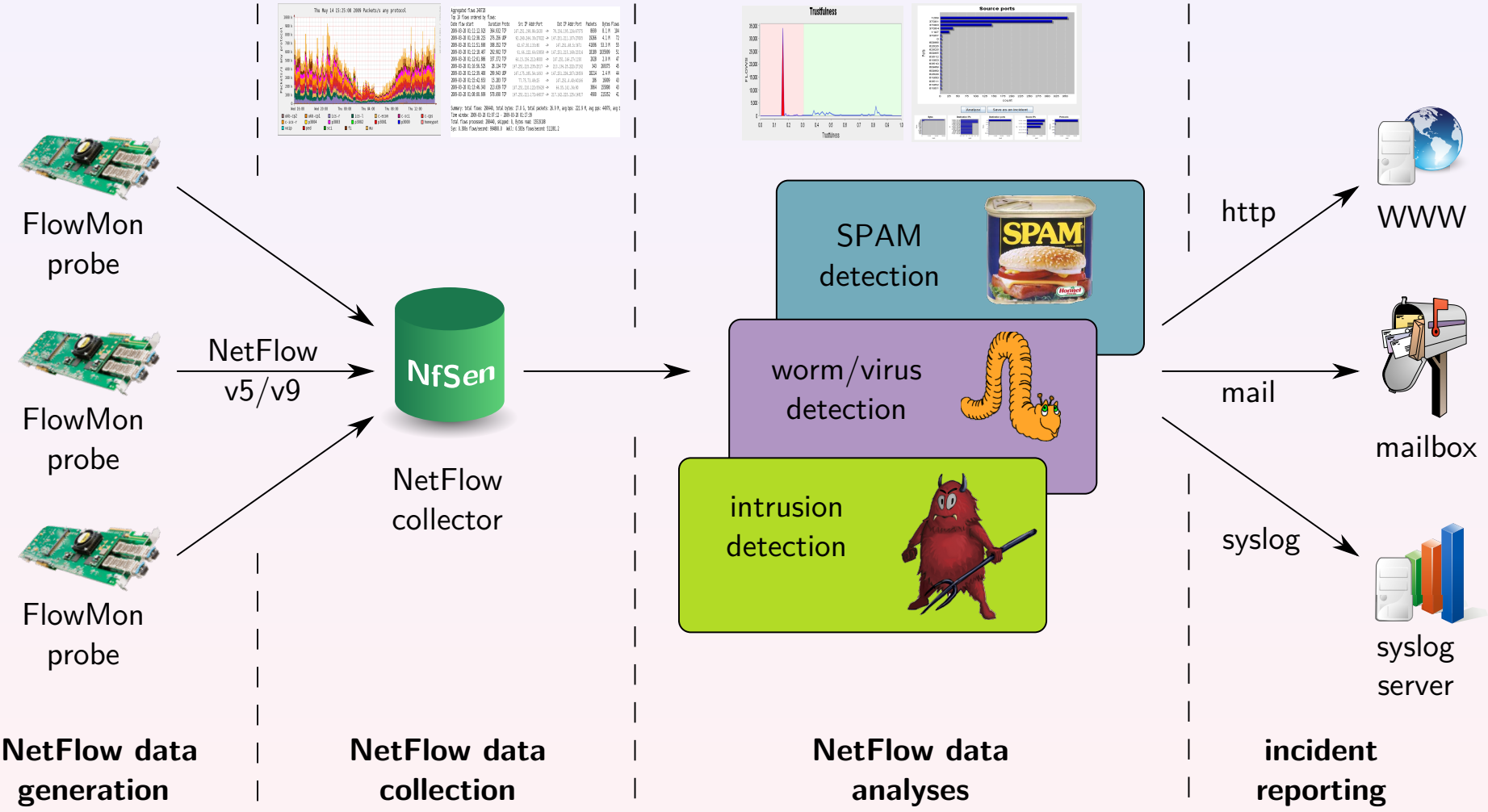
Security Monitoring and Behavior Analysis Toolset



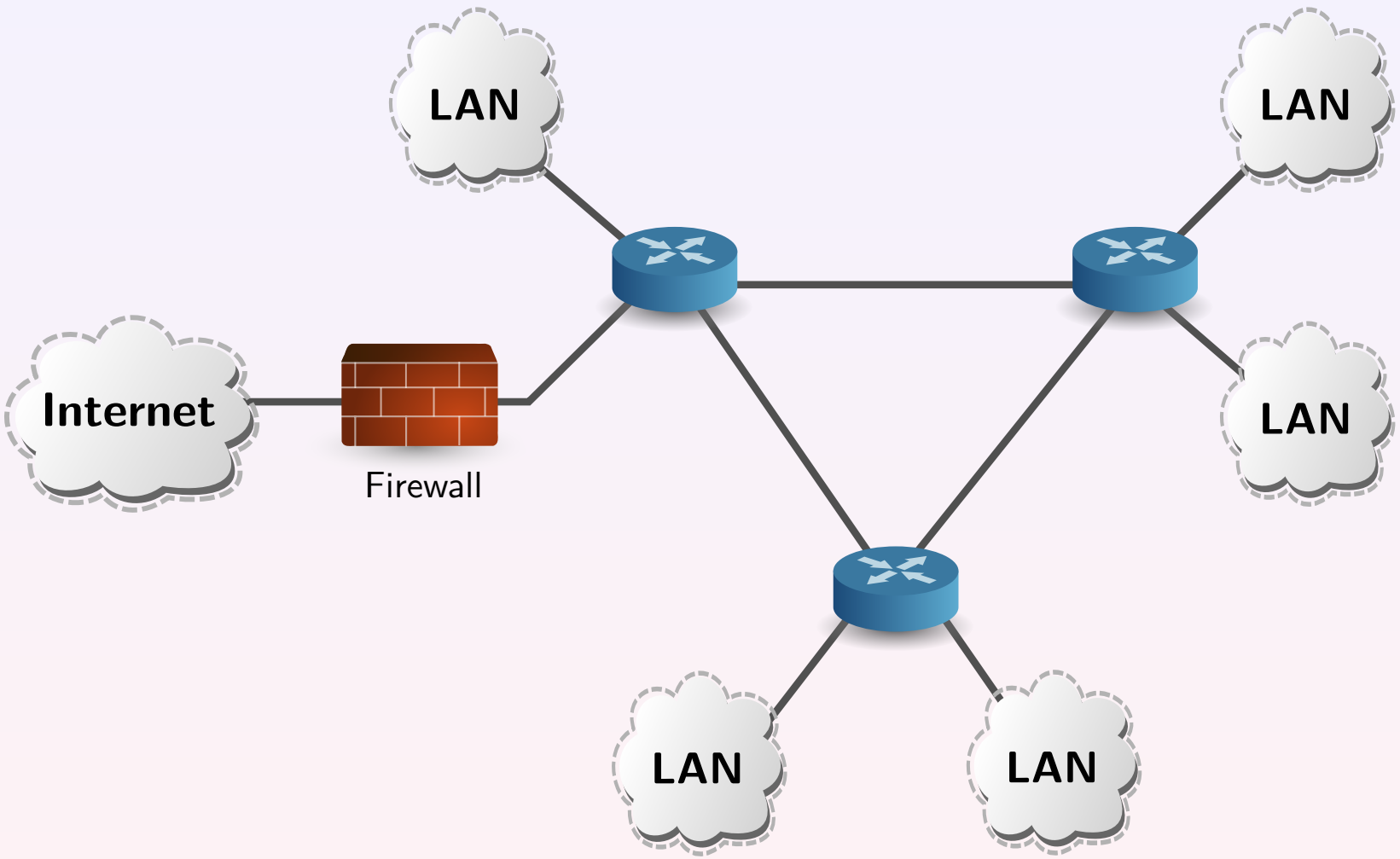
Security Monitoring and Behavior Analysis Toolset



Security Monitoring and Behavior Analysis Toolset

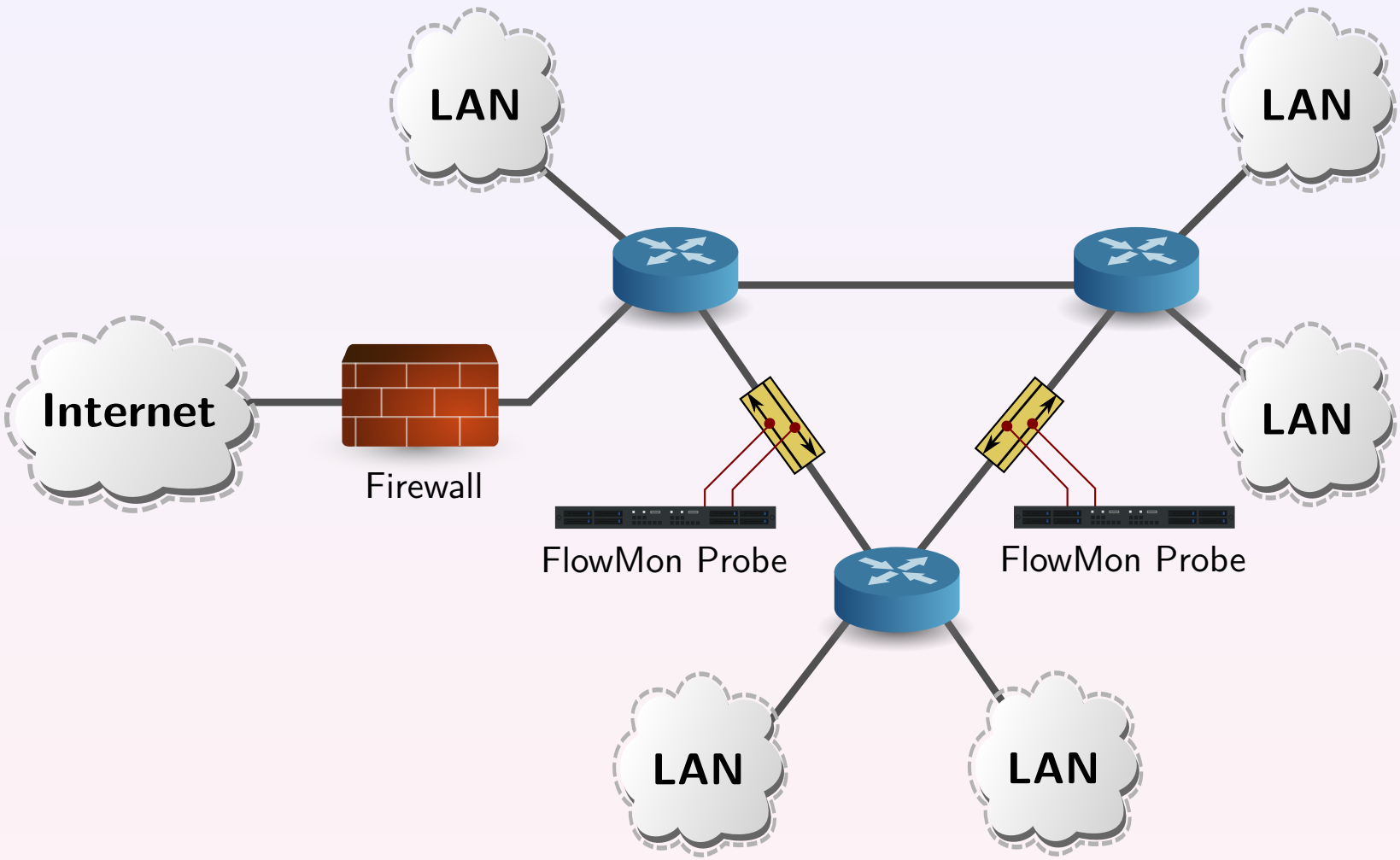


Traffic Monitoring System



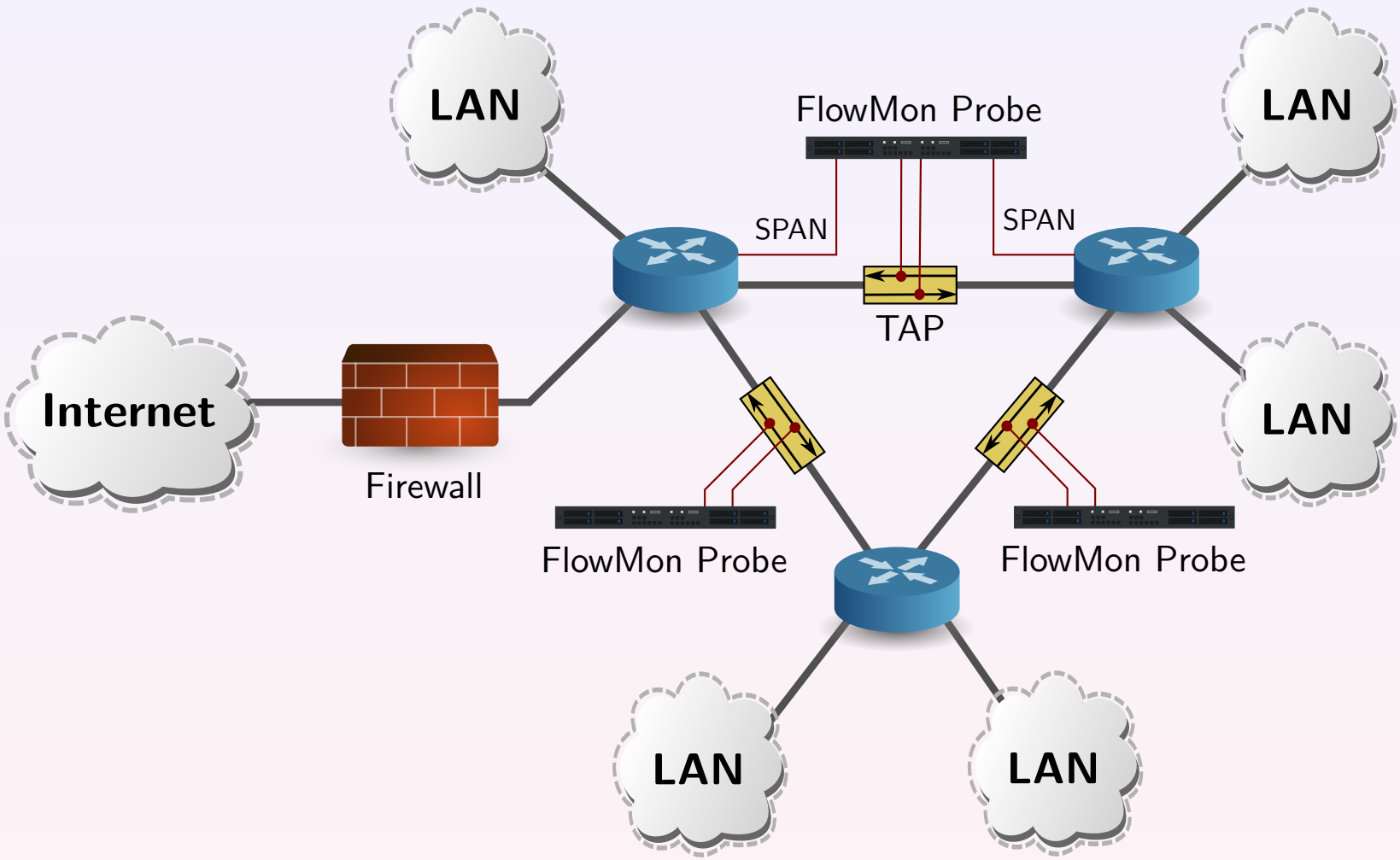
Network without any flow monitoring system.

Traffic Monitoring System



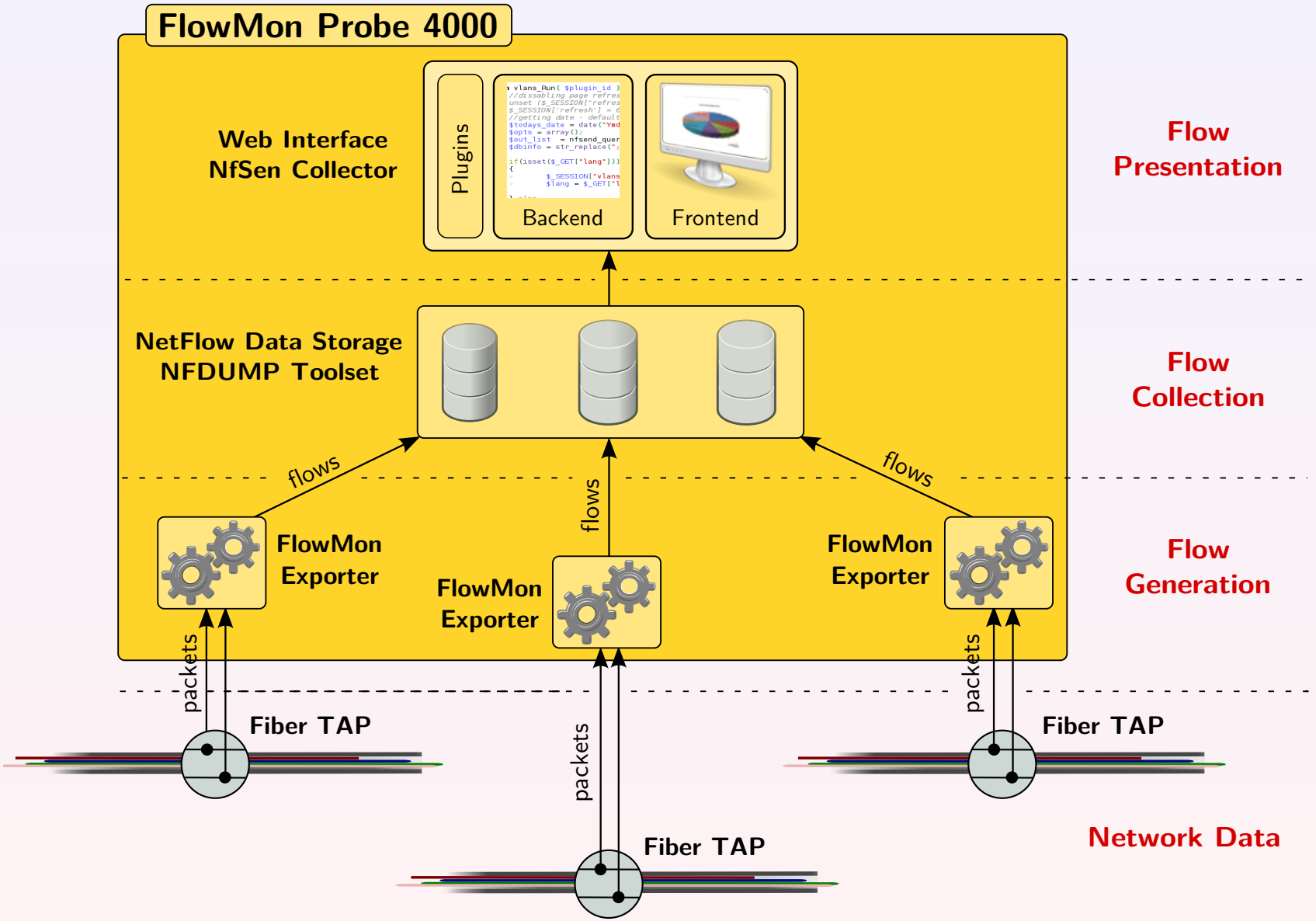
FlowMon probe connected to in-line TAP.

Traffic Monitoring System

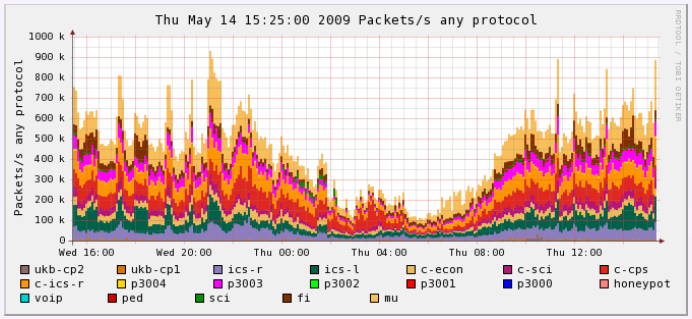


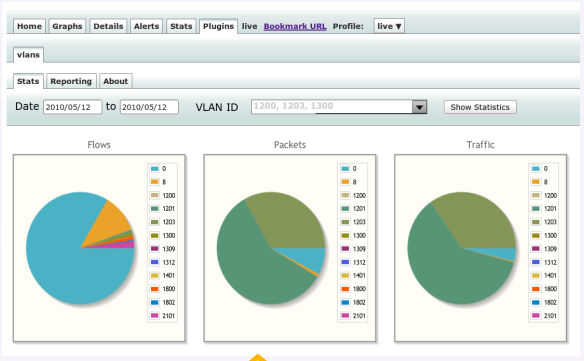
FlowMon observes data from TAP and SPAN ports.

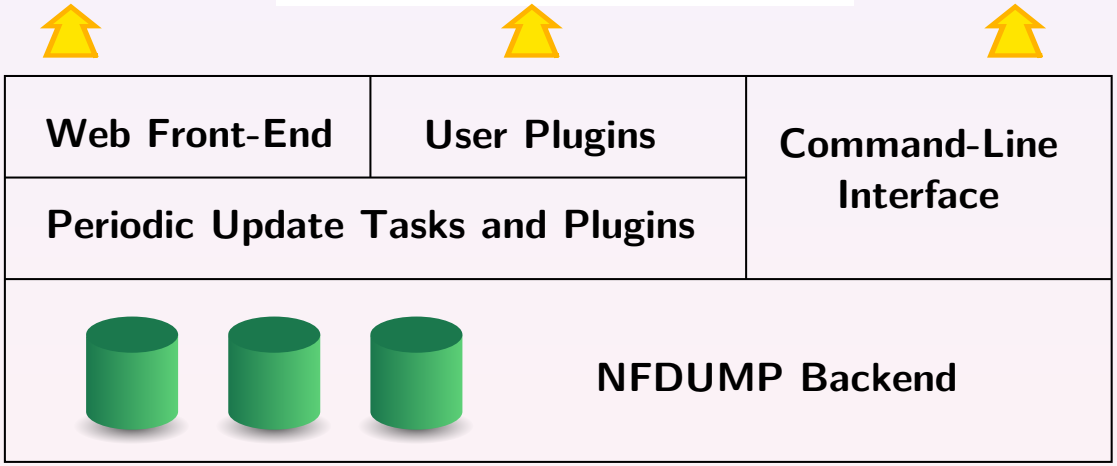
FlowMon Probe Architecture



NfSen/NFDUMP Collector Toolset Architecture







- **NfSen – NetFlow Sensor** – http://nfsen.sf.net/
- **NFDUMP – NetFlow display** – http://nfdump.sf.net/

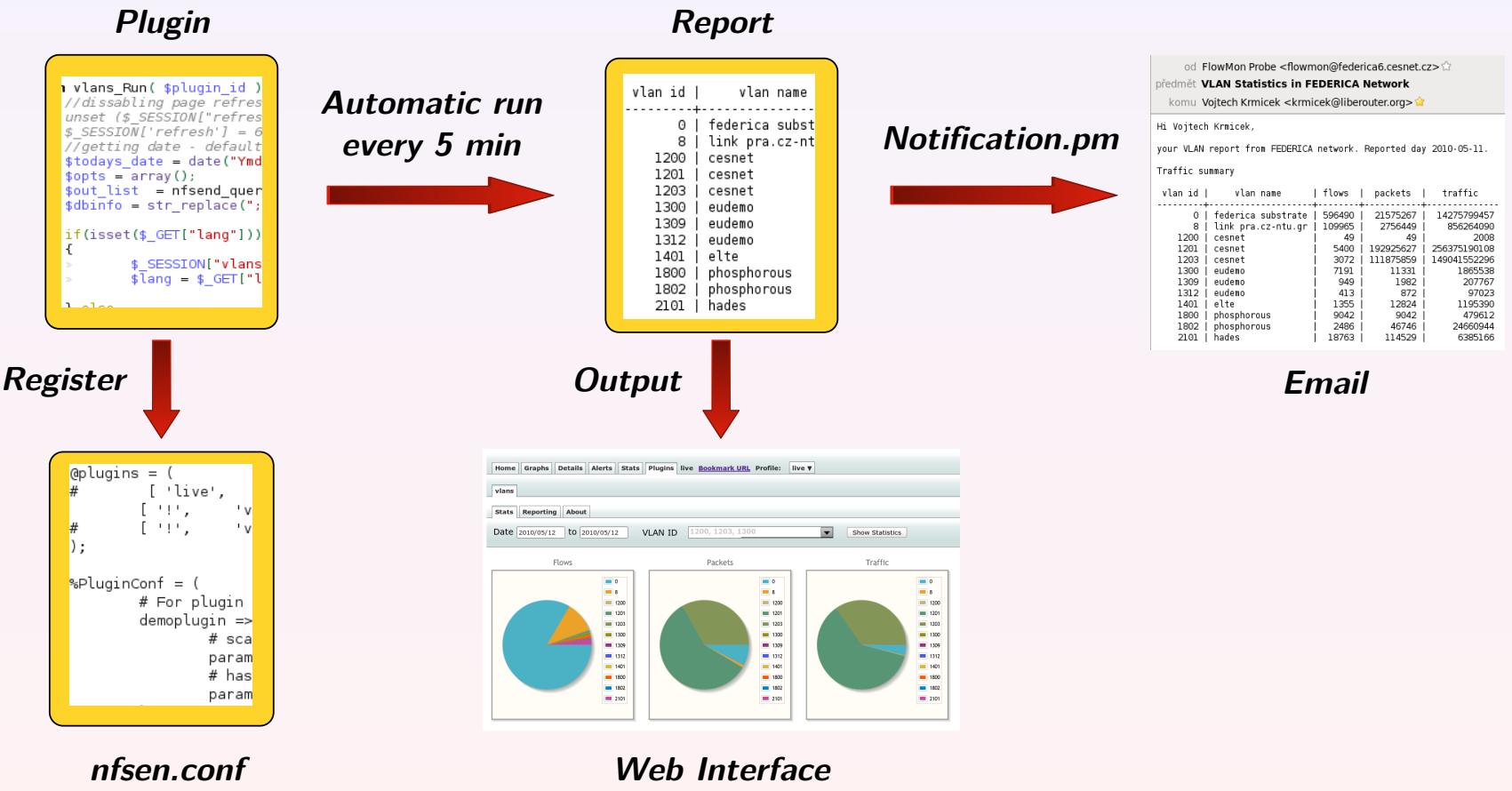
Available Flow Statistics

- Raw NetFlow data.
- Top N statistics.
- Flow filtering (via IP addresses, protocols, VLAN, MAC, ...).
- Flow aggregation (IP addresses, protocols, VLAN, MAC, ...).

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Intf	VLAN
06:49:55.049	299.996	ICMP	192.168.3.2:0	->	192.168.3.1:0.0	969	1.3 M	8	1203
06:49:55.657	299.997	ICMP	192.168.3.1:0	->	192.168.3.2:8.0	969	1.3 M	9	1203
06:51:10.255	299.752	ICMP	192.168.3.2:0	->	192.168.1.1:8.0	968	1.3 M	8	1203
06:51:10.255	299.752	ICMP	192.168.1.1:0	->	192.168.3.2:0.0	968	1.3 M	9	1203
06:51:36.593	299.824	ICMP	192.168.1.3:0	->	192.168.1.1:0.0	1936	2.6 M	6	1201
06:51:37.189	299.848	ICMP	192.168.1.1:0	->	192.168.1.3:8.0	1936	2.6 M	7	1201
06:54:55.355	299.997	ICMP	192.168.3.2:0	->	192.168.3.1:0.0	969	1.3 M	8	1203
06:54:55.964	299.996	ICMP	192.168.3.1:0	->	192.168.3.2:8.0	969	1.3 M	9	1203
06:56:10.317	299.781	ICMP	192.168.1.1:0	->	192.168.3.2:0.0	968	1.3 M	9	1203
06:56:10.317	299.781	ICMP	192.168.3.2:0	->	192.168.1.1:8.0	968	1.3 M	8	1203
06:56:36.649	299.916	ICMP	192.168.1.3:0	->	192.168.1.1:0.0	1936	2.6 M	6	1201
06:56:37.245	299.941	ICMP	192.168.1.1:0	->	192.168.1.3:8.0	1936	2.6 M	7	1201
06:57:01.952	0.000	UDP	194.132.52.193:138	->	194.132.52.195:138	2	513	5	1200

NfSen Plugins

- The plugins allow to extend NfSen with new functionality.
- The plugins run automated tasks every 5 minutes.
- The plugins allow display any results of NetFlow measurement.



Part II

Anomaly Detection and Behavior Analysis

Network Behavior Analysis

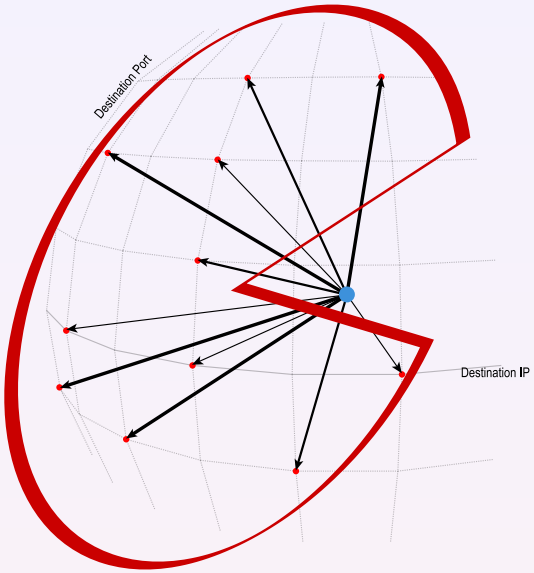
NBA Principles

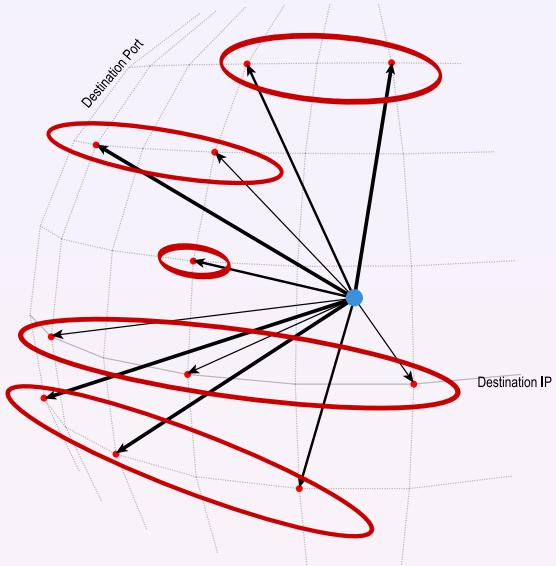
- identifies malware from **network traffic statistics**
- watch what's happening **inside the network**
- single purpose **detection patterns** (*scanning*, *botnets*, ...)
- **complex models** of the network behavior
- **statistical modeling**, PCA – Principal Component Analysis

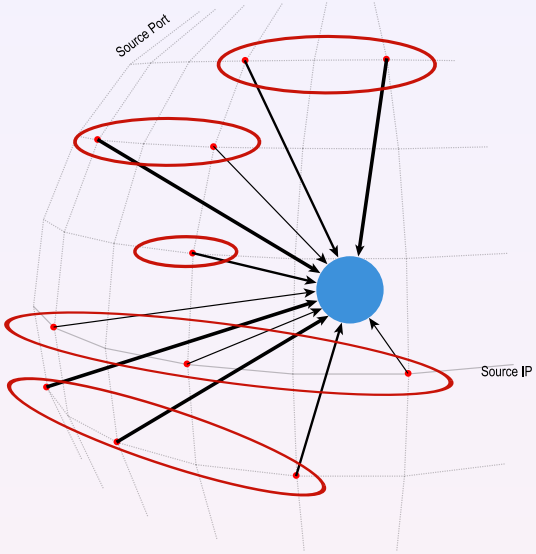
NBA Advantages

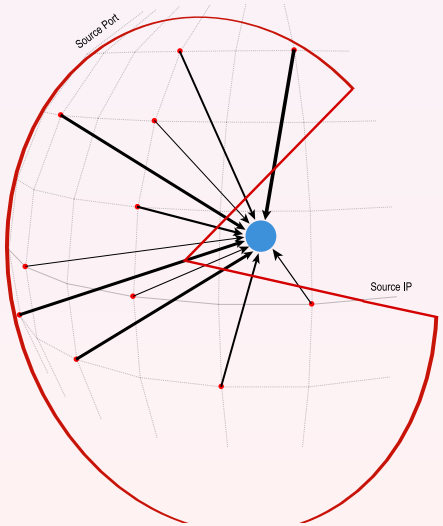
- good for spotting **new malware** and **zero day exploits**
- suitable for **high-speed networks**
- should be used **as an enhancement** to the protection provided by the standard tools (*firewall*, *IDS*, *AVS*, ...)

NBA Example - MINDS Method







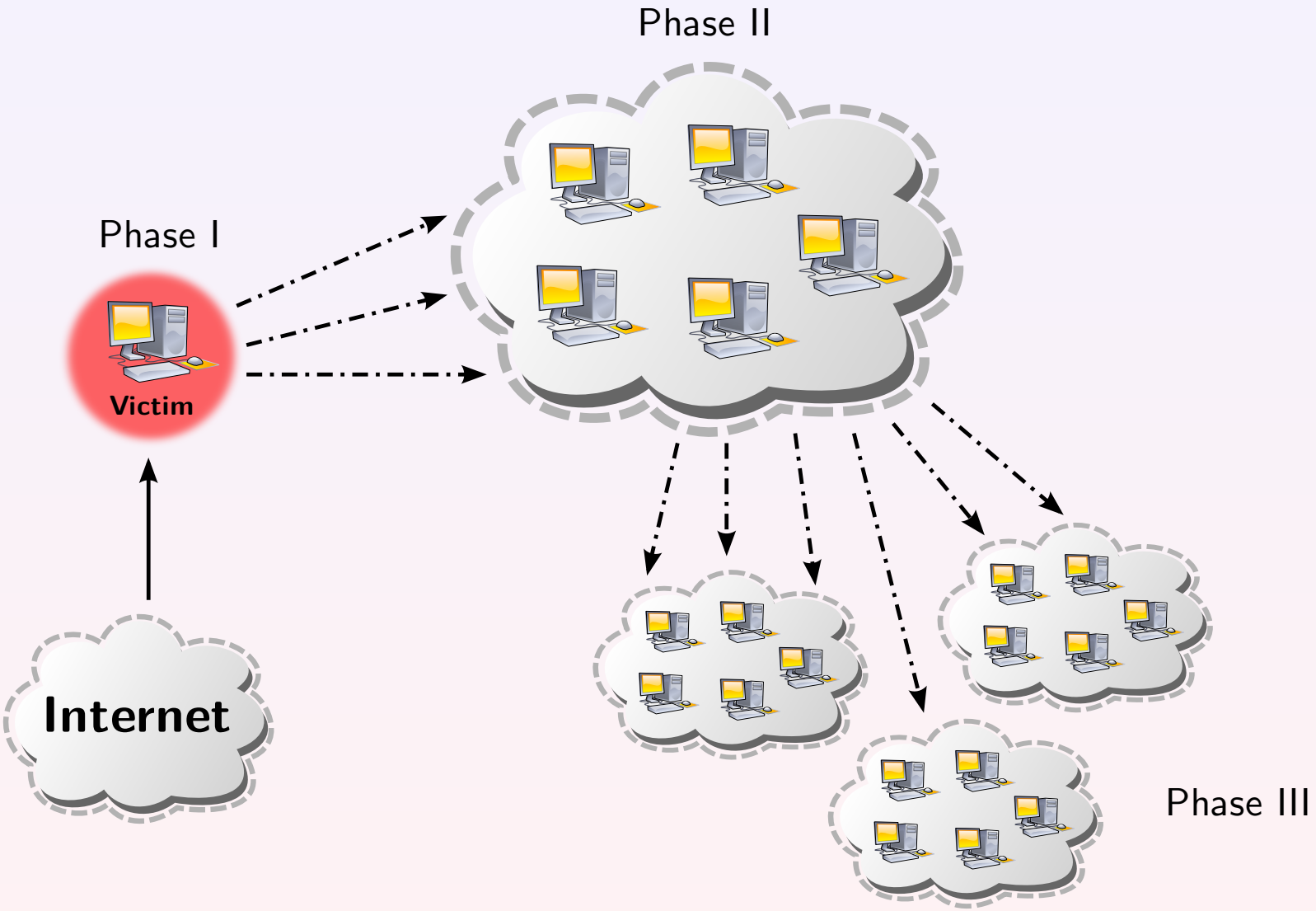


- **Features:** Flow counts from/to important IP/port combinations.
- **Malware identification:** Comparison with windowed average of past values.

Part III

Anomaly Detection – Use Case I. Conficker Worm

Conficker Worm Spreading

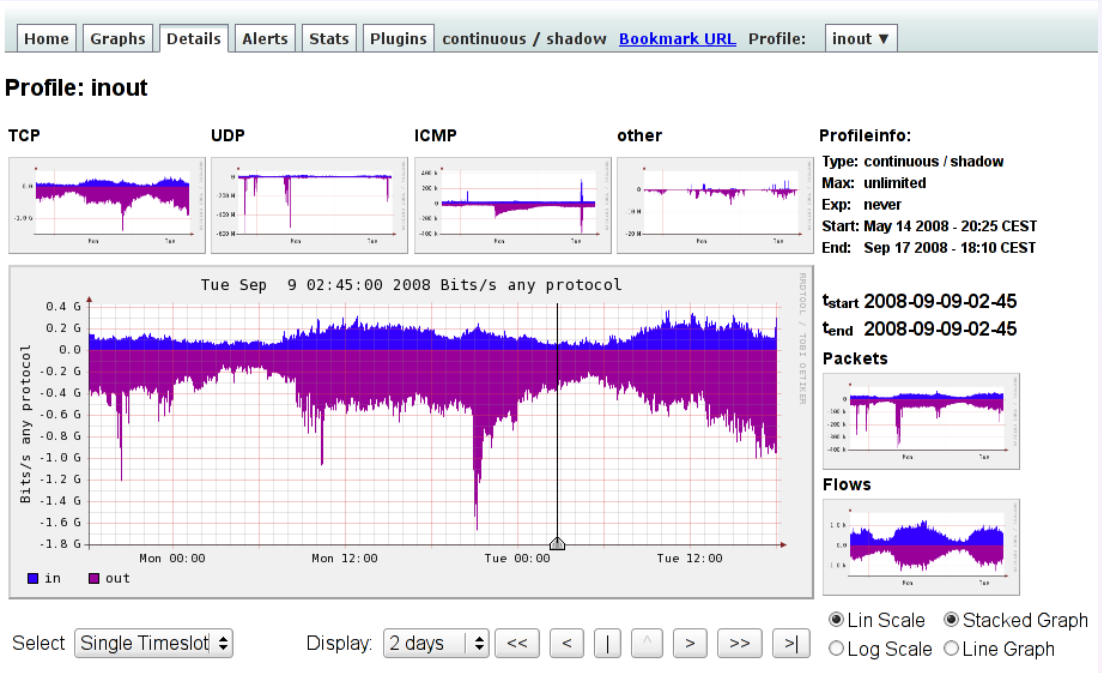


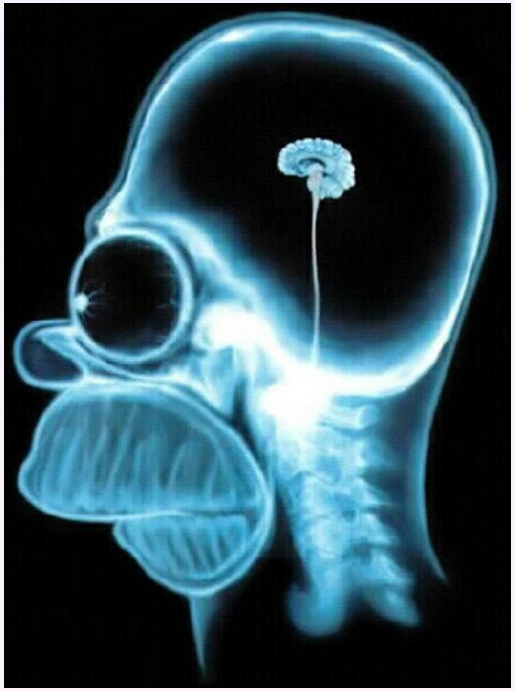
Traditional NetFlow Analysis Using NFDUMP Tool

Traditional NetFlow Analysis Using NFDUMP Tool

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
09:41:14.446	30.150	ICMP	172.16.92.1:0	->	172.16.96.48:3.10	.....	25	3028	1
09:41:24.470	0.049	UDP	172.16.96.48:138	->	172.16.96.255:138	.....	3	662	1
09:41:26.069	31.846	UDP	172.16.96.48:60443	->	239.255.255.250:1900	.....	14	2254	1
09:41:40.404	0.000	UDP	172.16.96.48:60395	->	172.16.92.1:53	.....	1	50	1
09:41:40.405	0.000	UDP	172.16.92.1:53	->	172.16.96.48:60395	.....	1	125	1
09:41:43.244	0.000	UDP	172.16.96.48:50664	->	172.16.92.1:53	.....	1	62	1
09:41:43.244	0.000	UDP	172.16.92.1:53	->	172.16.96.48:64291	.....	1	256	1
09:41:43.246	0.384	TCP	172.16.96.48:49158	->	207.46.131.206:80	A.RS.	4	172	1
09:41:43.437	0.192	TCP	207.46.131.206:80	->	172.16.96.48:49158	AP.SF	3	510	1
09:41:43.631	0.000	UDP	172.16.96.48:63820	->	172.16.92.1:53	.....	1	62	1
09:41:43.673	0.000	UDP	172.16.92.1:53	->	172.16.96.48:63820	.....	1	256	1

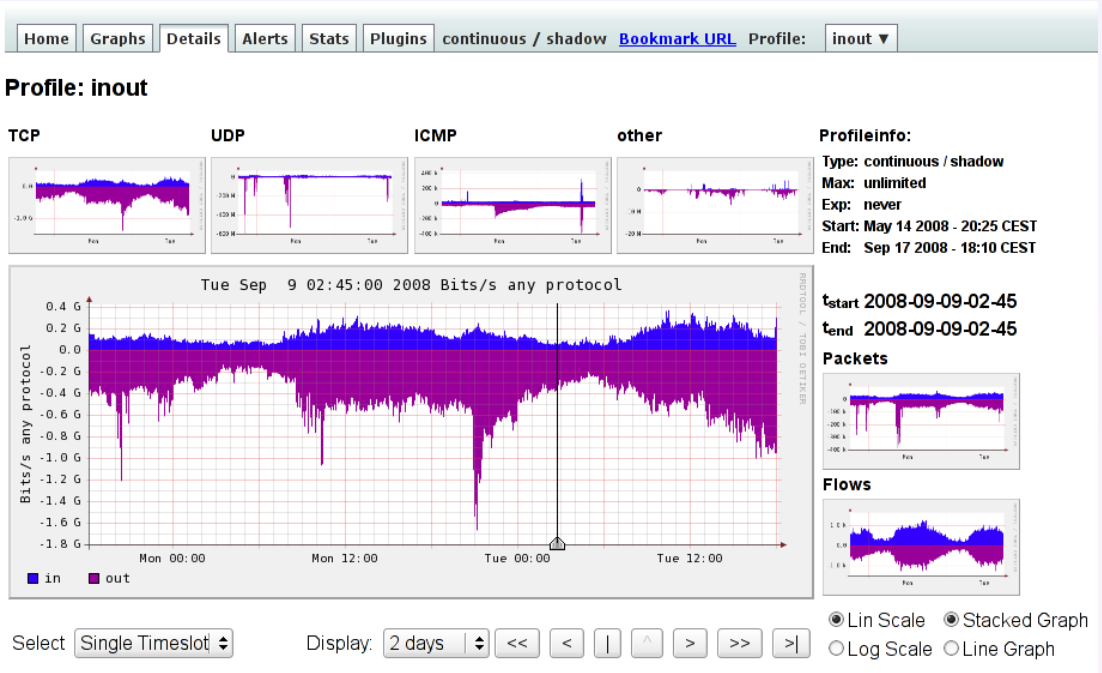
Traditional NetFlow Analysis Using NFDUMP Tool

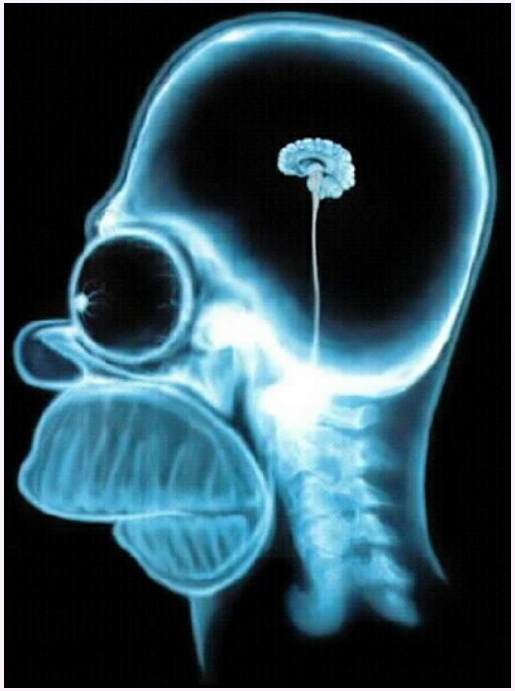




```
Flow start   Duration Proto Src IP Addr:Port          Dst IP Addr:Port  Flags Packets Bytes Flows
09:41:14.446  30.150  ICMP  172.16.92.1:0      ->    172.16.96.48:3.10  .....   25    3028     1
09:41:24.470   0.049  UDP  172.16.96.48:138    ->   172.16.96.255:138   .....    3     662     1
09:41:26.069  31.846  UDP  172.16.96.48:60443  -> 239.255.255.250:1900  .....   14    2254     1
09:41:40.404   0.000  UDP  172.16.96.48:60395  ->     172.16.92.1:53    .....    1      50     1
09:41:40.405   0.000  UDP   172.16.92.1:53     ->    172.16.96.48:60395 .....    1     125     1
09:41:43.244   0.000  UDP  172.16.96.48:50664  ->     172.16.92.1:53    .....    1      62     1
09:41:43.244   0.000  UDP   172.16.92.1:53     ->    172.16.96.48:64291 .....    1     256     1
09:41:43.246   0.384  TCP  172.16.96.48:49158  ->  207.46.131.206:80    A.RS.    4     172     1
09:41:43.437   0.192  TCP  207.46.131.206:80   ->    172.16.96.48:49158 AP.SF    3     510     1
09:41:43.631   0.000  UDP  172.16.96.48:63820  ->     172.16.92.1:53    .....    1      62     1
09:41:43.673   0.000  UDP   172.16.92.1:53     ->    172.16.96.48:63820 .....    1     256     1
```

Traditional NetFlow Analysis Using NFDUMP Tool





Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
09:41:14.446	30.150	ICMP	172.16.92.1:0	->	172.16.96.48:3.10	.....	25	3028	1
09:41:24.470	0.049	UDP	172.16.96.48:138	->	172.16.96.255:138	.....	3	662	1
09:41:26.069	31.846	UDP	172.16.96.48:60443	->	239.255.255.250:1900	.....	14	2254	1
09:41:40.404	0.000	UDP	172.16.96.48:60395	->	172.16.92.1:53	.....	1	50	1
09:41:40.405	0.000	UDP	172.16.92.1:53	->	172.16.96.48:60395	.....	1	125	1
09:41:43.244	0.000	UDP	172.16.96.48:50664	->	172.16.92.1:53	.....	1	62	1
09:41:43.244	0.000	UDP	172.16.92.1:53	->	172.16.96.48:64291	.....	1	256	1
09:41:43.246	0.384	TCP	172.16.96.48:49158	->	207.46.131.206:80	A.RS.	4	172	1
09:41:43.437	0.192	TCP	207.46.131.206:80	->	172.16.96.48:49158	AP.SF	3	510	1
09:41:43.631	0.000	UDP	172.16.96.48:63820	->	172.16.92.1:53	.....	1	62	1
09:41:43.673	0.000	UDP	172.16.92.1:53	->	172.16.96.48:63820	.....	1	256	1

Conficker Detection Using NFDUMP Tool - I

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
09:55:42.963	0.000	TCP	172.16.96.48:49225	->	100.9.240.76:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49226	->	209.13.138.30:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49224	->	71.70.105.4:445	...S.	1	48	1
09:55:42.964	0.000	TCP	172.16.96.48:49230	->	150.18.37.52:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49238	->	189.97.157.63:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49235	->	46.77.154.99:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49237	->	187.96.185.74:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49234	->	223.62.32.43:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49236	->	176.77.174.109:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49239	->	121.110.84.84:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49243	->	153.34.211.79:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49244	->	59.34.59.14:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49245	->	172.115.82.70:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49246	->	196.117.5.44:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49258	->	78.33.209.5:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49248	->	28.36.5.3:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49259	->	91.39.4.28:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49254	->	112.96.125.115:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49262	->	197.63.38.5:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49268	->	36.85.125.20:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49261	->	170.88.178.77:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49260	->	175.42.90.106:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49263	->	15.70.58.96:445	...S.	1	48	1

We focus on TCP traffic.

Conficker Detection Using NFDUMP Tool - I

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
09:55:42.963	0.000	TCP	172.16.96.48:49225	->	100.9.240.76:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49226	->	209.13.138.30:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49224	->	71.70.105.4:445	...S.	1	48	1
09:55:42.964	0.000	TCP	172.16.96.48:49230	->	150.18.37.52:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49238	->	189.97.157.63:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49235	->	46.77.154.99:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49237	->	187.96.185.74:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49234	->	223.62.32.43:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49236	->	176.77.174.109:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49239	->	121.110.84.84:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49243	->	153.34.211.79:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49244	->	59.34.59.14:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49245	->	172.115.82.70:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49246	->	196.117.5.44:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49258	->	78.33.209.5:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49248	->	28.36.5.3:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49259	->	91.39.4.28:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49254	->	112.96.125.115:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49262	->	197.63.38.5:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49268	->	36.85.125.20:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49261	->	170.88.178.77:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49260	->	175.42.90.106:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49263	->	15.70.58.96:445	...S.	1	48	1

Traffic comes out from single host – every new connection generates flow.

Conficker Detection Using NFDUMP Tool - I

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
09:55:42.963	0.000	TCP	172.16.96.48:49225	->	100.9.240.76:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49226	->	209.13.138.30:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49224	->	71.70.105.4:445	...S.	1	48	1
09:55:42.964	0.000	TCP	172.16.96.48:49230	->	150.18.37.52:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49238	->	189.97.157.63:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49235	->	46.77.154.99:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49237	->	187.96.185.74:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49234	->	223.62.32.43:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49236	->	176.77.174.109:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49239	->	121.110.84.84:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49243	->	153.34.211.79:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49244	->	59.34.59.14:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49245	->	172.115.82.70:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49246	->	196.117.5.44:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49258	->	78.33.209.5:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49248	->	28.36.5.3:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49259	->	91.39.4.28:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49254	->	112.96.125.115:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49262	->	197.63.38.5:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49268	->	36.85.125.20:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49261	->	170.88.178.77:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49260	->	175.42.90.106:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49263	->	15.70.58.96:445	...S.	1	48	1

Infected host connects to various remote machines (horizontal scan) – same destination port 445.

Conficker Detection Using NFDUMP Tool - I

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
09:55:42.963	0.000	TCP	172.16.96.48:49225	->	100.9.240.76:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49226	->	209.13.138.30:445	...S.	1	48	1
09:55:42.963	0.000	TCP	172.16.96.48:49224	->	71.70.105.4:445	...S.	1	48	1
09:55:42.964	0.000	TCP	172.16.96.48:49230	->	150.18.37.52:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49238	->	189.97.157.63:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49235	->	46.77.154.99:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49237	->	187.96.185.74:445	...S.	1	48	1
09:55:42.965	0.000	TCP	172.16.96.48:49234	->	223.62.32.43:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49236	->	176.77.174.109:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49239	->	121.110.84.84:445	...S.	1	48	1
09:55:42.966	0.000	TCP	172.16.96.48:49243	->	153.34.211.79:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49244	->	59.34.59.14:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49245	->	172.115.82.70:445	...S.	1	48	1
09:55:42.967	0.000	TCP	172.16.96.48:49246	->	196.117.5.44:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49258	->	78.33.209.5:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49248	->	28.36.5.3:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49259	->	91.39.4.28:445	...S.	1	48	1
09:55:42.968	0.000	TCP	172.16.96.48:49254	->	112.96.125.115:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49262	->	197.63.38.5:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49268	->	36.85.125.20:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49261	->	170.88.178.77:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49260	->	175.42.90.106:445	...S.	1	48	1
09:55:42.969	0.000	TCP	172.16.96.48:49263	->	15.70.58.96:445	...S.	1	48	1

TCP SYN flag set, single packet with uniform size.

Conficker Detection Using NFDUMP Tool - II

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
10:48:10.983	29.934	TCP	172.16.96.31:50076	->	145.107.246.69:445	AP.S.	30	1259	1
10:48:25.894	30.189	TCP	172.16.96.47:51875	->	169.41.101.97:445	AP.S.	29	1298	1
10:48:26.001	32.111	TCP	172.16.96.49:63778	->	43.28.146.45:445	AP.S.	18	906	1
10:48:26.948	10.745	TCP	172.16.96.50:52225	->	104.24.33.123:445	AP.S.	10	537	1
10:48:27.466	24.770	TCP	172.16.96.35:55484	->	109.18.23.97:445	AP.SF	102	146397	1
10:48:28.443	28.866	TCP	172.16.96.37:53098	->	102.124.181.67:445	AP.S.	15	804	1
10:48:28.473	10.572	TCP	172.16.96.38:60340	->	222.50.79.96:445	AP.S.	23	4549	1
10:48:28.797	30.748	TCP	172.16.96.37:53174	->	212.82.132.58:445	AP.S.	19	861	1
10:48:29.267	32.783	TCP	172.16.96.34:64769	->	34.56.183.93:445	AP.S.	17	1696	1
10:48:29.409	7.773	TCP	172.16.96.34:64756	->	89.109.215.111:445	AP.S.	17	3037	1
10:48:29.492	34.993	TCP	172.16.96.44:57145	->	32.113.4.81:445	AP.S.	15	2562	1
10:48:29.749	26.004	TCP	172.16.96.43:52707	->	138.8.147.38:445	AP.S.	16	1725	1
10:48:30.159	12.609	TCP	172.16.96.49:63902	->	203.101.75.18:445	AP.S.	22	2316	1
10:48:31.116	3.004	TCP	172.16.96.31:50766	->	194.125.49.68:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50768	->	193.114.216.37:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50769	->	37.107.5.111:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50770	->	126.96.239.95:445	...S.	2	96	1
10:48:31.118	3.002	TCP	172.16.96.31:50776	->	43.87.170.91:445	...S.	2	96	1
10:48:31.119	3.001	TCP	172.16.96.31:50778	->	103.13.70.122:445	...S.	2	96	1
10:48:31.127	2.993	TCP	172.16.96.31:50784	->	200.68.202.35:445	...S.	2	96	1
10:48:31.129	2.991	TCP	172.16.96.31:50791	->	56.39.208.87:445	...S.	2	96	1
10:48:31.131	2.990	TCP	172.16.96.31:50797	->	59.104.110.104:445	...S.	2	96	1

Infected hosts from the same subnet.

Conficker Detection Using NFDUMP Tool - II

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
10:48:10.983	29.934	TCP	172.16.96.31:50076	->	145.107.246.69:445	AP.S.	30	1259	1
10:48:25.894	30.189	TCP	172.16.96.47:51875	->	169.41.101.97:445	AP.S.	29	1298	1
10:48:26.001	32.111	TCP	172.16.96.49:63778	->	43.28.146.45:445	AP.S.	18	906	1
10:48:26.948	10.745	TCP	172.16.96.50:52225	->	104.24.33.123:445	AP.S.	10	537	1
10:48:27.466	24.770	TCP	172.16.96.35:55484	->	109.18.23.97:445	AP.SF	102	146397	1
10:48:28.443	28.866	TCP	172.16.96.37:53098	->	102.124.181.67:445	AP.S.	15	804	1
10:48:28.473	10.572	TCP	172.16.96.38:60340	->	222.50.79.96:445	AP.S.	23	4549	1
10:48:28.797	30.748	TCP	172.16.96.37:53174	->	212.82.132.58:445	AP.S.	19	861	1
10:48:29.267	32.783	TCP	172.16.96.34:64769	->	34.56.183.93:445	AP.S.	17	1696	1
10:48:29.409	7.773	TCP	172.16.96.34:64756	->	89.109.215.111:445	AP.S.	17	3037	1
10:48:29.492	34.993	TCP	172.16.96.44:57145	->	32.113.4.81:445	AP.S.	15	2562	1
10:48:29.749	26.004	TCP	172.16.96.43:52707	->	138.8.147.38:445	AP.S.	16	1725	1
10:48:30.159	12.609	TCP	172.16.96.49:63902	->	203.101.75.18:445	AP.S.	22	2316	1
10:48:31.116	3.004	TCP	172.16.96.31:50766	->	194.125.49.68:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50768	->	193.114.216.37:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50769	->	37.107.5.111:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50770	->	126.96.239.95:445	...S.	2	96	1
10:48:31.118	3.002	TCP	172.16.96.31:50776	->	43.87.170.91:445	...S.	2	96	1
10:48:31.119	3.001	TCP	172.16.96.31:50778	->	103.13.70.122:445	...S.	2	96	1
10:48:31.127	2.993	TCP	172.16.96.31:50784	->	200.68.202.35:445	...S.	2	96	1
10:48:31.129	2.991	TCP	172.16.96.31:50791	->	56.39.208.87:445	...S.	2	96	1
10:48:31.131	2.990	TCP	172.16.96.31:50797	->	59.104.110.104:445	...S.	2	96	1

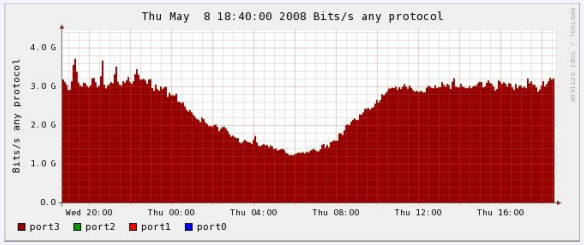
Successful TCP communication – high source ports and identical destination port 445.

Conficker Detection Using NFDUMP Tool - II

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes	Flows
10:48:10.983	29.934	TCP	172.16.96.31:50076	->	145.107.246.69:445	AP.S.	30	1259	1
10:48:25.894	30.189	TCP	172.16.96.47:51875	->	169.41.101.97:445	AP.S.	29	1298	1
10:48:26.001	32.111	TCP	172.16.96.49:63778	->	43.28.146.45:445	AP.S.	18	906	1
10:48:26.948	10.745	TCP	172.16.96.50:52225	->	104.24.33.123:445	AP.S.	10	537	1
10:48:27.466	24.770	TCP	172.16.96.35:55484	->	109.18.23.97:445	AP.SF	102	146397	1
10:48:28.443	28.866	TCP	172.16.96.37:53098	->	102.124.181.67:445	AP.S.	15	804	1
10:48:28.473	10.572	TCP	172.16.96.38:60340	->	222.50.79.96:445	AP.S.	23	4549	1
10:48:28.797	30.748	TCP	172.16.96.37:53174	->	212.82.132.58:445	AP.S.	19	861	1
10:48:29.267	32.783	TCP	172.16.96.34:64769	->	34.56.183.93:445	AP.S.	17	1696	1
10:48:29.409	7.773	TCP	172.16.96.34:64756	->	89.109.215.111:445	AP.S.	17	3037	1
10:48:29.492	34.993	TCP	172.16.96.44:57145	->	32.113.4.81:445	AP.S.	15	2562	1
10:48:29.749	26.004	TCP	172.16.96.43:52707	->	138.8.147.38:445	AP.S.	16	1725	1
10:48:30.159	12.609	TCP	172.16.96.49:63902	->	203.101.75.18:445	AP.S.	22	2316	1
10:48:31.116	3.004	TCP	172.16.96.31:50766	->	194.125.49.68:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50768	->	193.114.216.37:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50769	->	37.107.5.111:445	...S.	2	96	1
10:48:31.117	3.003	TCP	172.16.96.31:50770	->	126.96.239.95:445	...S.	2	96	1
10:48:31.118	3.002	TCP	172.16.96.31:50776	->	43.87.170.91:445	...S.	2	96	1
10:48:31.119	3.001	TCP	172.16.96.31:50778	->	103.13.70.122:445	...S.	2	96	1
10:48:31.127	2.993	TCP	172.16.96.31:50784	->	200.68.202.35:445	...S.	2	96	1
10:48:31.129	2.991	TCP	172.16.96.31:50791	->	56.39.208.87:445	...S.	2	96	1
10:48:31.131	2.990	TCP	172.16.96.31:50797	->	59.104.110.104:445	...S.	2	96	1

Further worm propagation – port 445 horizontal scan/buffer overflow attempt.

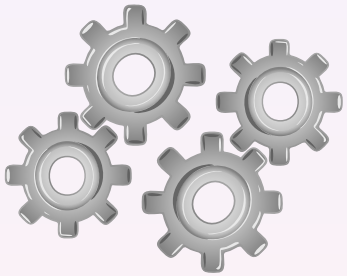
Worm Detection And Analysis With CAMNEP - I



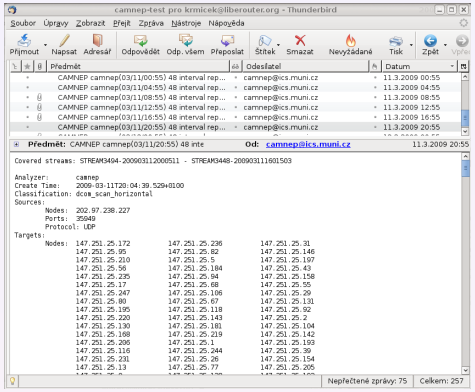
Milions of Flows per Day

CAMPUS Network

Threat

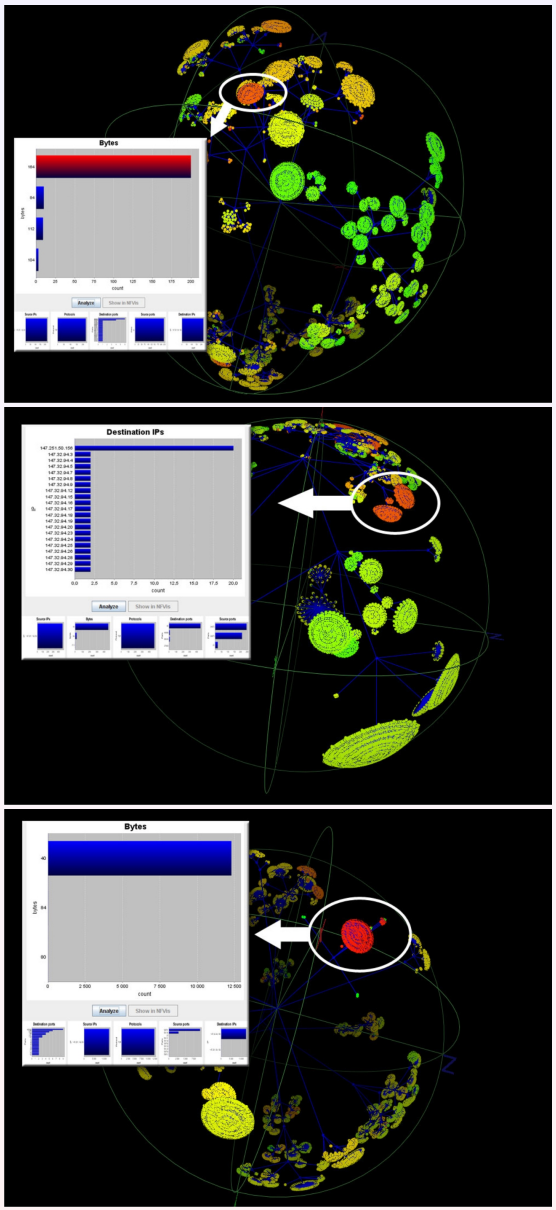


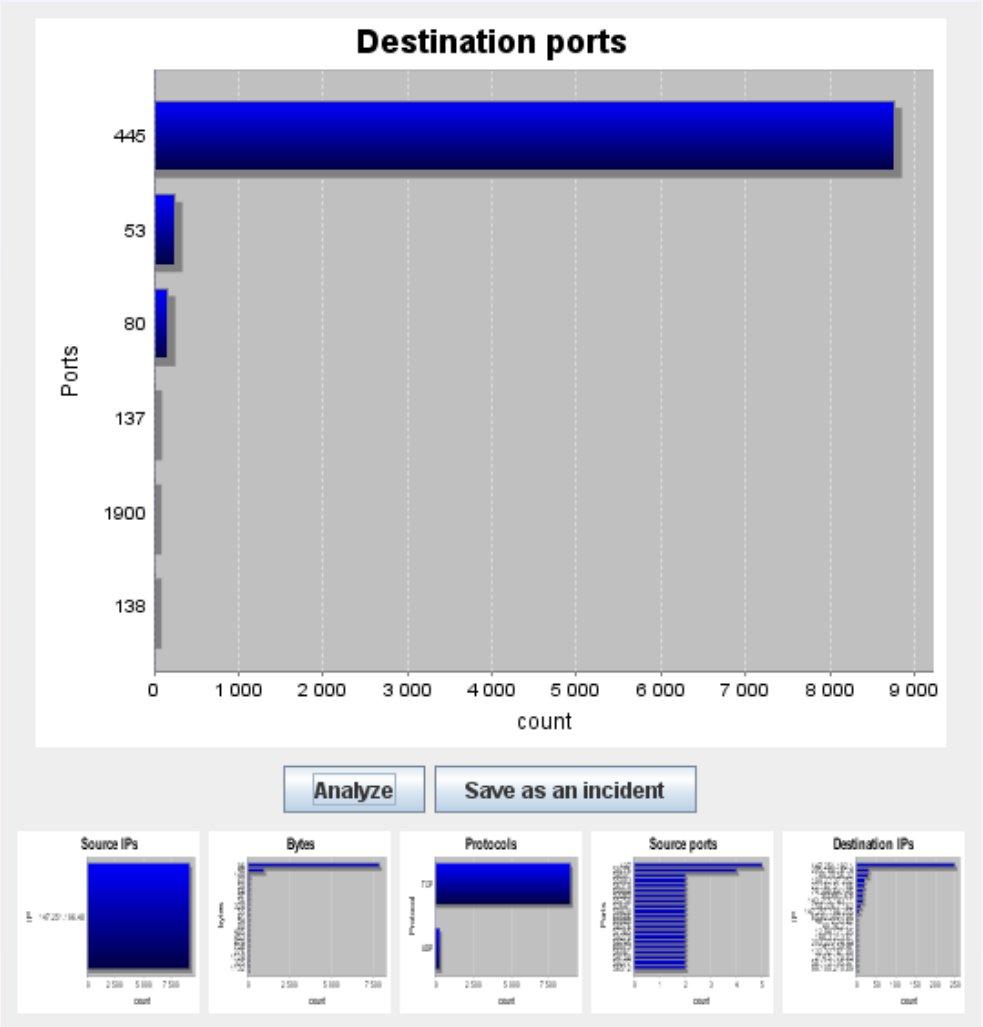
Network Behavioral Analysis



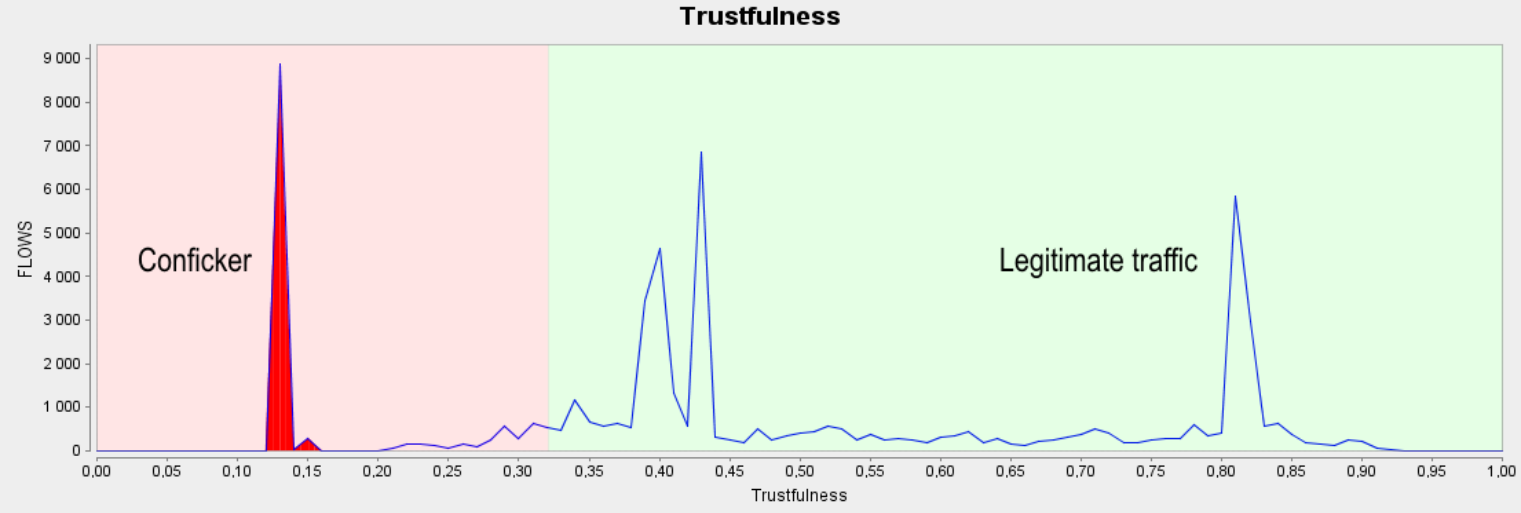
CSIRT Early Action

Worm Detection And Analysis With CAMNEP - II





Worm Detection And Analysis With CAMNEP - III




```
Analyzer:       CamnepKB111
Create Time:    2009-02-11T09:58:49.977+0100
Classification: conficker, also similar to: web_requests,dns_requests,port_scan_horizontal
Flows:  5045, Bytes:  484505, 1 sources, 5016 targets
Sources:
        Nodes:  172.16.96.48 [anonymized, random IP address in the list]
        Ports:  0,137,1900,49190-49195,49197-49198,49200-49227,49229-49341,49343-49381,49383-49462,
                [ ... ]
                63052,63808,63815,65015,65288
        Protocol: UDP, ICMP, TCP
Targets:
        Nodes:  17.108.162.71           215.77.118.108          155.59.237.22
                [ ... ]
                40.15.162.105           40.127.21.51            40.72.221.37
 and more (5016 in total)
        Ports:  53,80,137,139,445,1900,2048,3702,5355,52358
        Protocol: UDP, ICMP, TCP
```

Part IV

Anomaly Detection – Use Case II. Chuck Norris Botnet

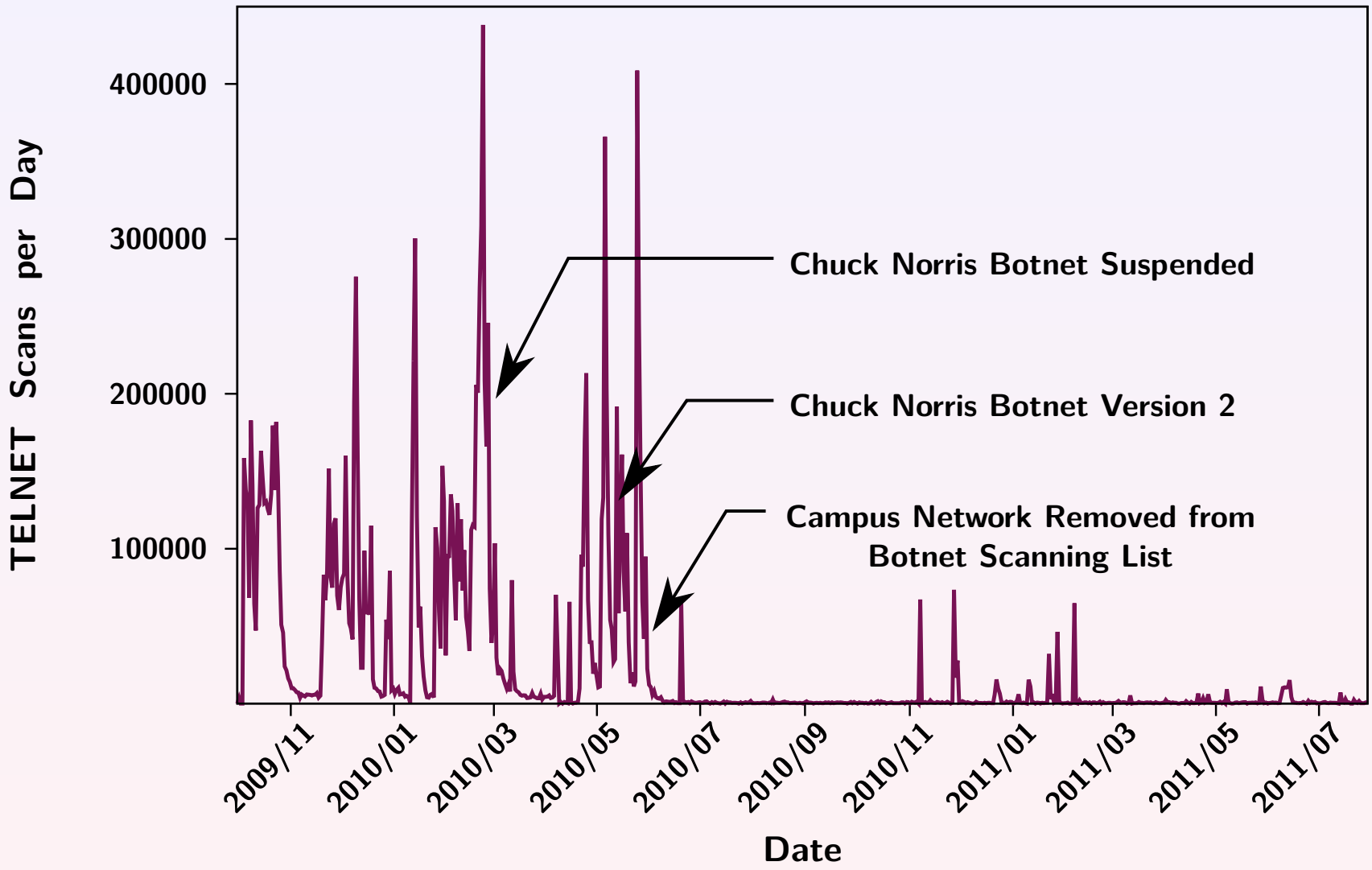
Chuck Norris Botnet in Nutshell

- **Linux malware** – IRC bots with central C&C servers.
- Attacks **poorly-configured** Linux **MIPSEL** devices.
- Vulnerable devices – **ADSL modems** and **routers**.

- Uses **TELNET brute force** attack as infection vector.
- Users are **not aware** about the malicious activities.
- **Missing** anti-malware **solution** to detect it.

Discovered at Masaryk University on 2 December 2009. The malware got the Chuck Norris moniker from a comment in its source code `[R]anger Killato : in nome di Chuck Norris !`

TELNET Malware Activities – 2009/11 - 2011/7



Detection of CNB Scanning

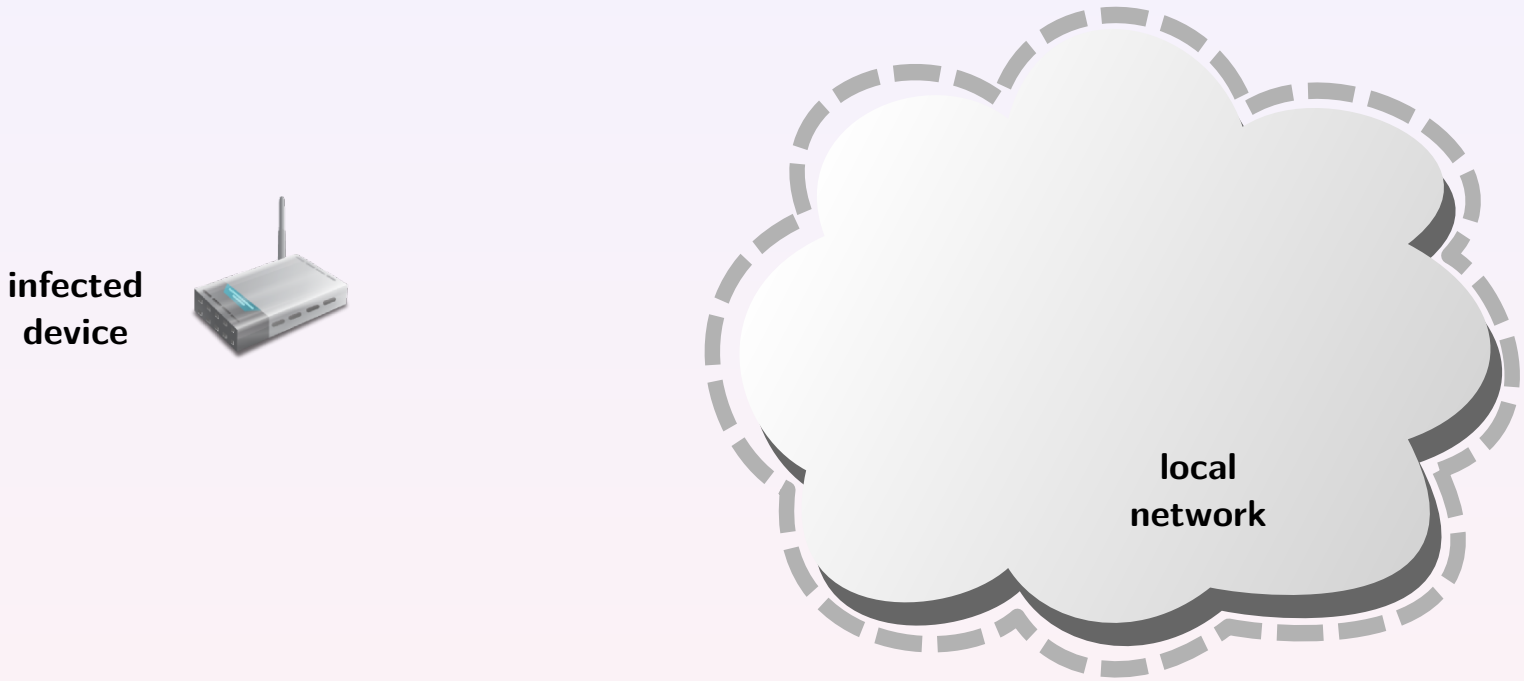
- Incoming and outgoing **TCP SYN scans** on port 22 and 23.

infected device

NFDUMP detection filter

Detection of CNB Scanning

- Incoming and outgoing **TCP SYN scans** on port 22 and 23.



NFDUMP detection filter

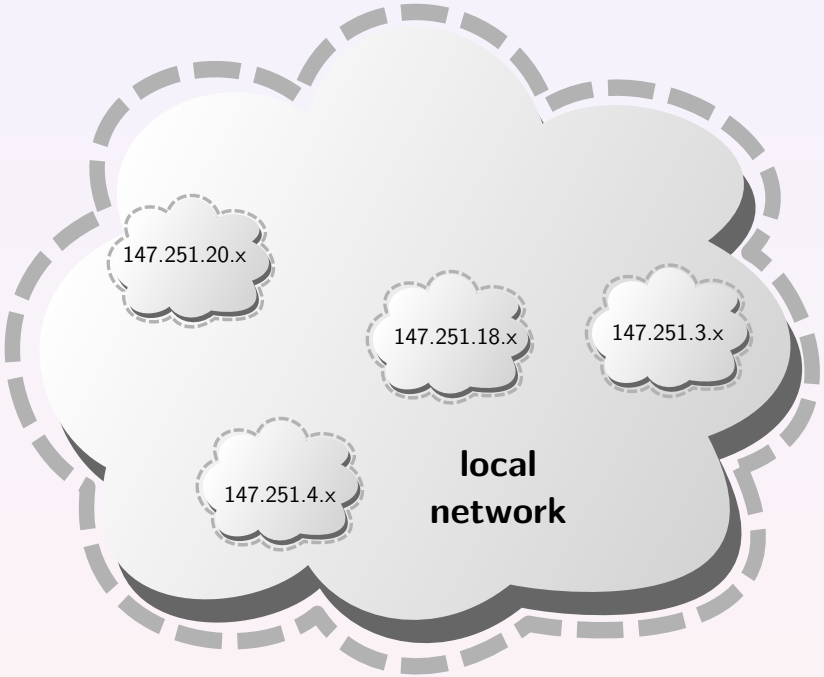
(net *local_network*)

Detection of CNB Scanning

- Incoming and outgoing **TCP SYN scans** on port 22 and 23.

list of C class networks to scan

infected device

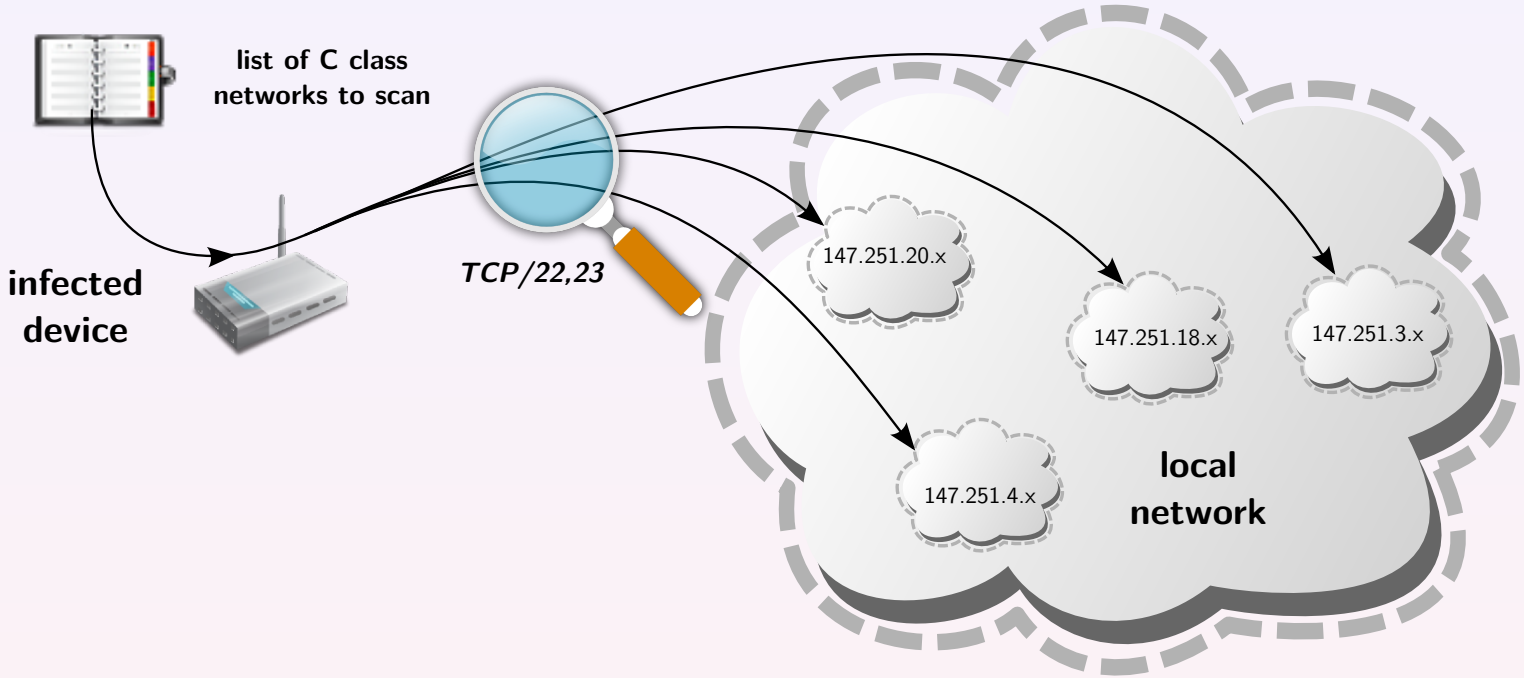


NFDUMP detection filter

(net *local_network*)

Detection of CNB Scanning

- Incoming and outgoing **TCP SYN scans** on port 22 and 23.

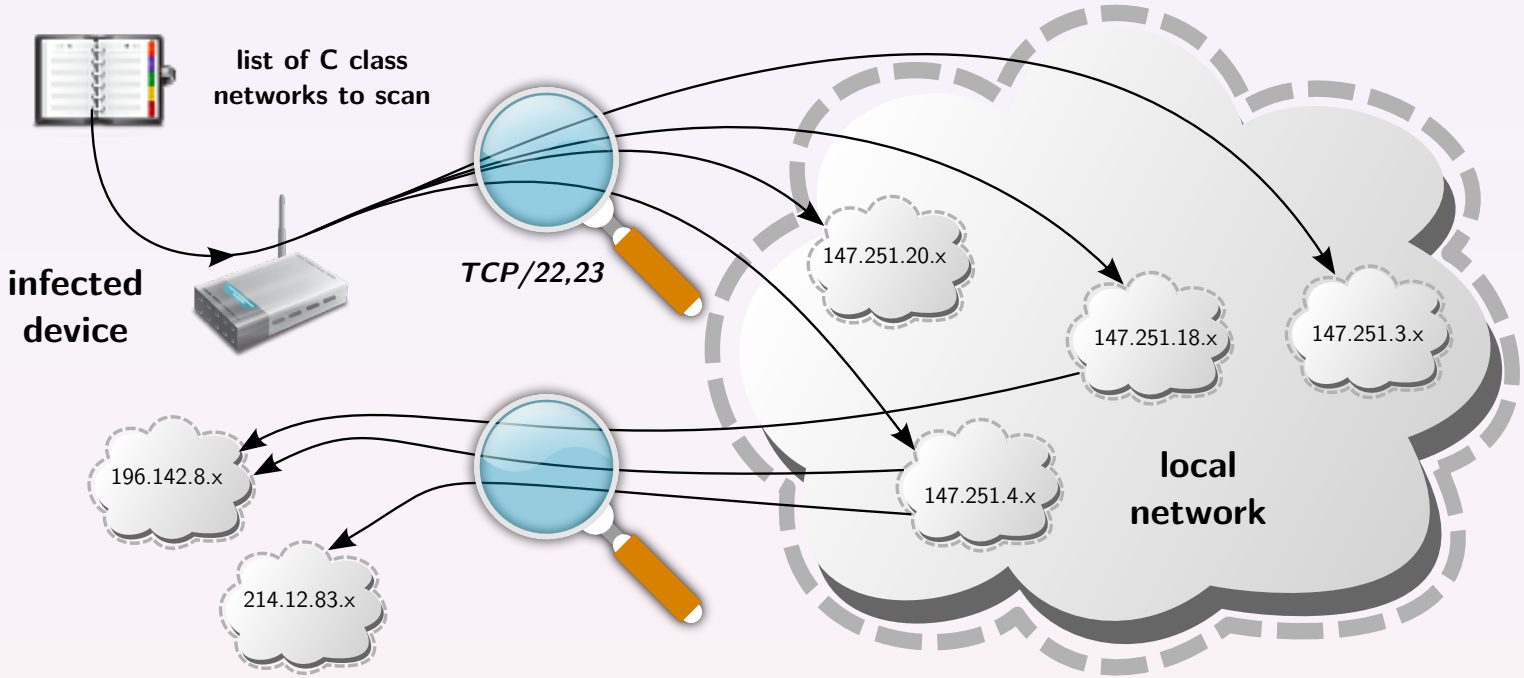


NFDUMP detection filter

(net *local_network*) and (dst port 22 or dst port 23) and (proto TCP)

Detection of CNB Scanning

- Incoming and outgoing **TCP SYN scans** on port 22 and 23.

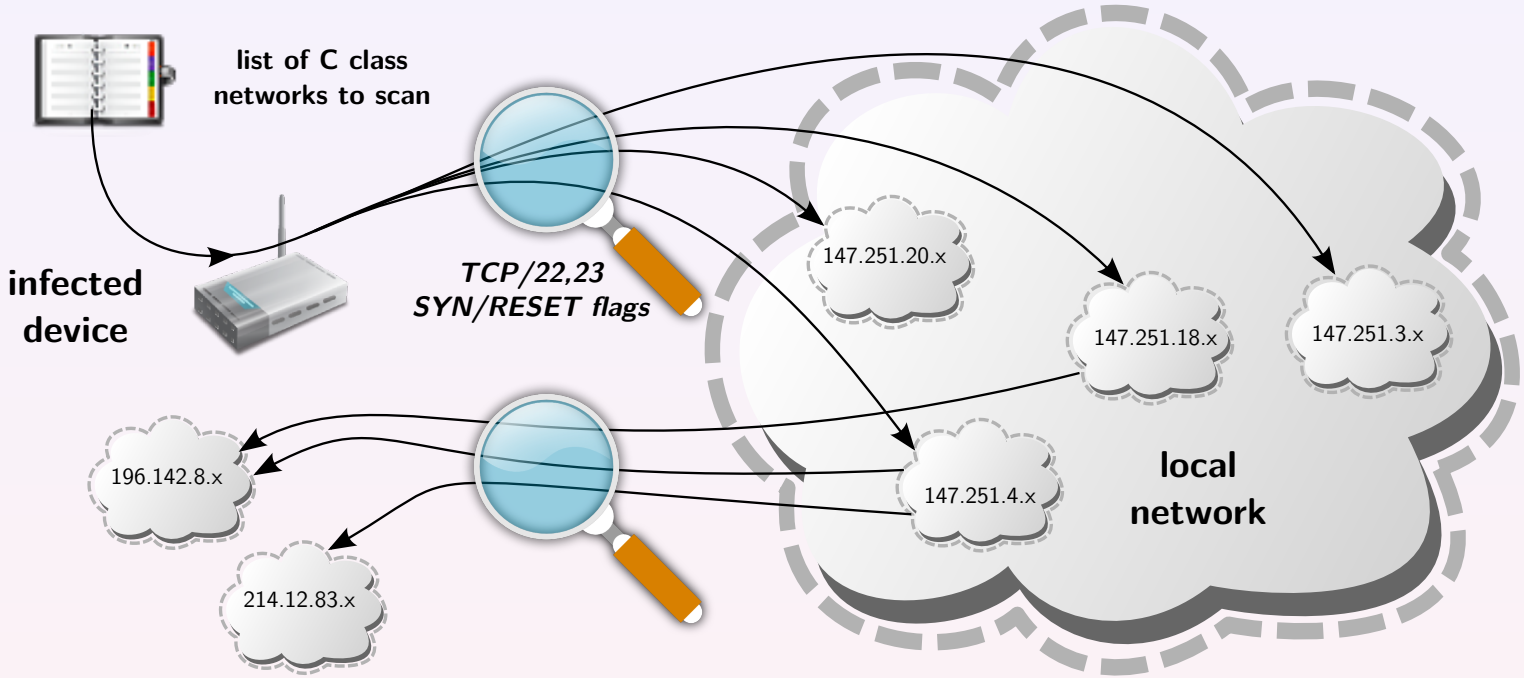


NFDUMP detection filter

(net *local_network*) and (dst port 22 or dst port 23) and (proto TCP)

Detection of CNB Scanning

- Incoming and outgoing **TCP SYN scans** on port 22 and 23.



NFDUMP detection filter

(net *local_network*) and (dst port 22 or dst port 23) and (proto TCP) and ((flags S and not flags ARPUF) or (flags SR and not flags APUF))

Detection of CNB Initialization and Update

- Bot's **web download requests** from infected host.

NFDUMP detection filter

Detection of CNB Initialization and Update

- Bot's **web download requests** from infected host.

NFDUMP detection filter

(src net *local_network*)

Detection of CNB Initialization and Update

- Bot's **web download requests** from infected host.

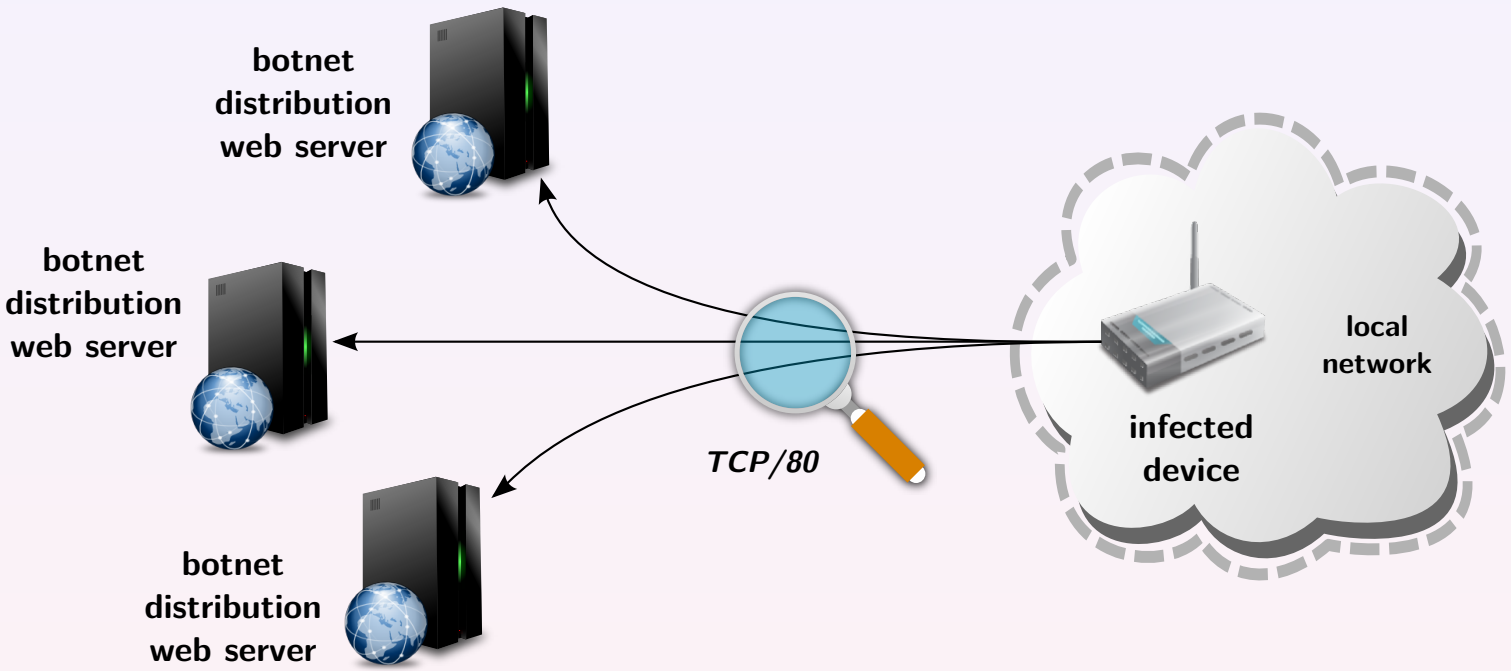
NFDUMP detection filter

(src net *local_network*) and (dst ip *web_servers*[1])

[1] IP addresses of attacker's botnet distribution web servers

Detection of CNB Initialization and Update

- Bot's **web download requests** from infected host.



NFDUMP detection filter

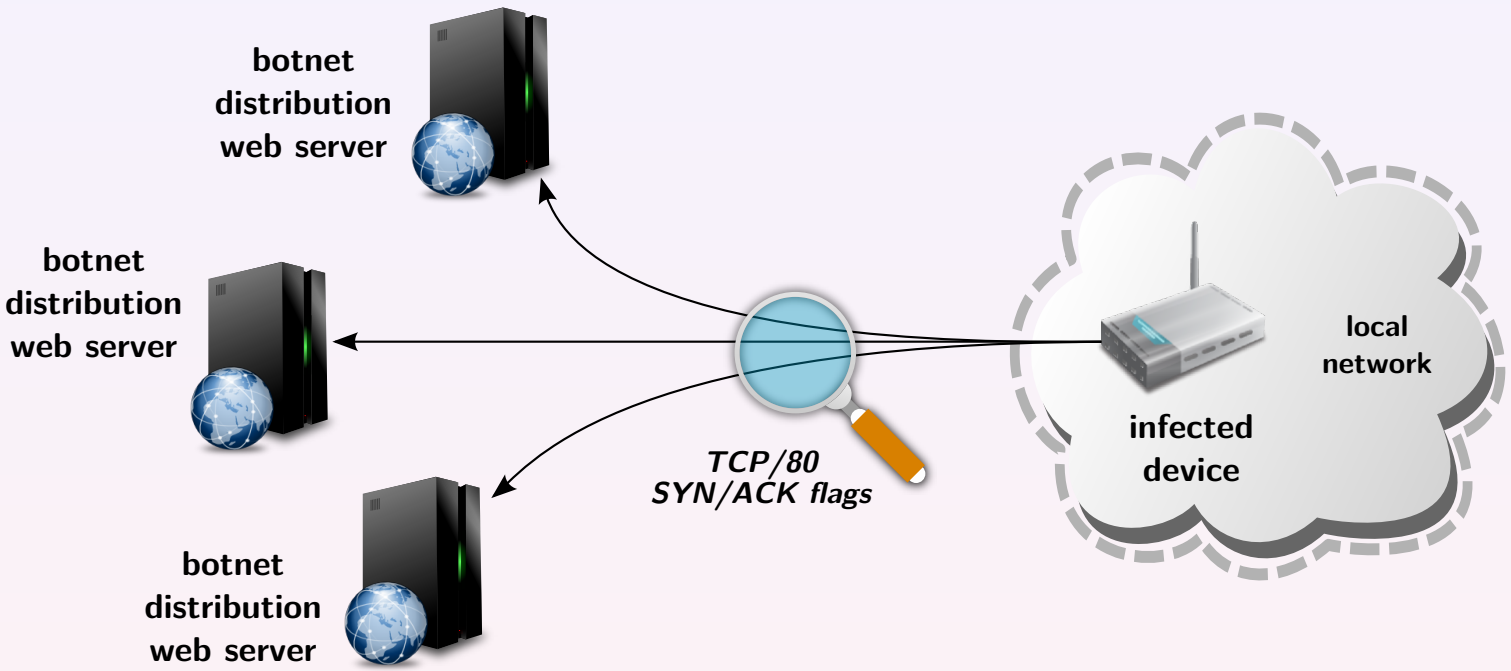
(src net *local_network*) and (dst ip *web_servers*[1]) and

(dst port 80) and (proto TCP)

[1] IP addresses of attacker's botnet distribution web servers

Detection of CNB Initialization and Update

- Bot's **web download requests** from infected host.



NFDUMP detection filter

(src net *local_network*) and (dst ip *web_servers*[1]) and

(dst port 80) and (proto TCP) and (flags SA and not flag R)

[1] IP addresses of attacker's botnet distribution web servers

Detection of CNB DNS Spoofing Attack

Detecting Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's DNS**.

NFDUMP detection filter

Detection of CNB DNS Spoofing Attack

Detecting Attacker's DNS or OpenDNS Queries

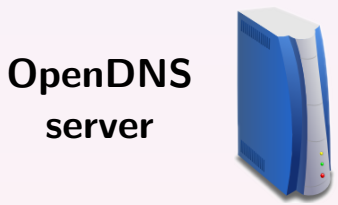
- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's DNS**.

NFDUMP detection filter
(src net *local_network*)

Detection of CNB DNS Spoofing Attack

Detecting Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's DNS**.



NFDUMP detection filter

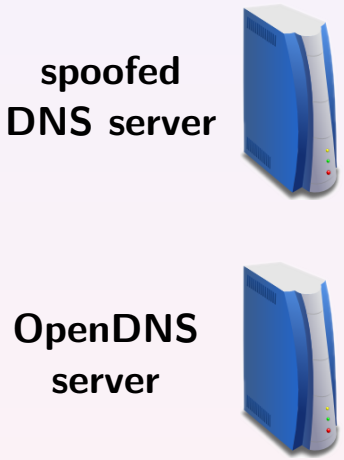
(src net *local_network*) and ((dst ip *OpenDNS servers*[2]) or

[2] IP addresses of a common OpenDNS servers

Detection of CNB DNS Spoofing Attack

Detecting Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's DNS**.



NFDUMP detection filter

(src net *local_network*) and ((dst ip *OpenDNS servers*[2]) or (dst ip *DNS servers*[3]))

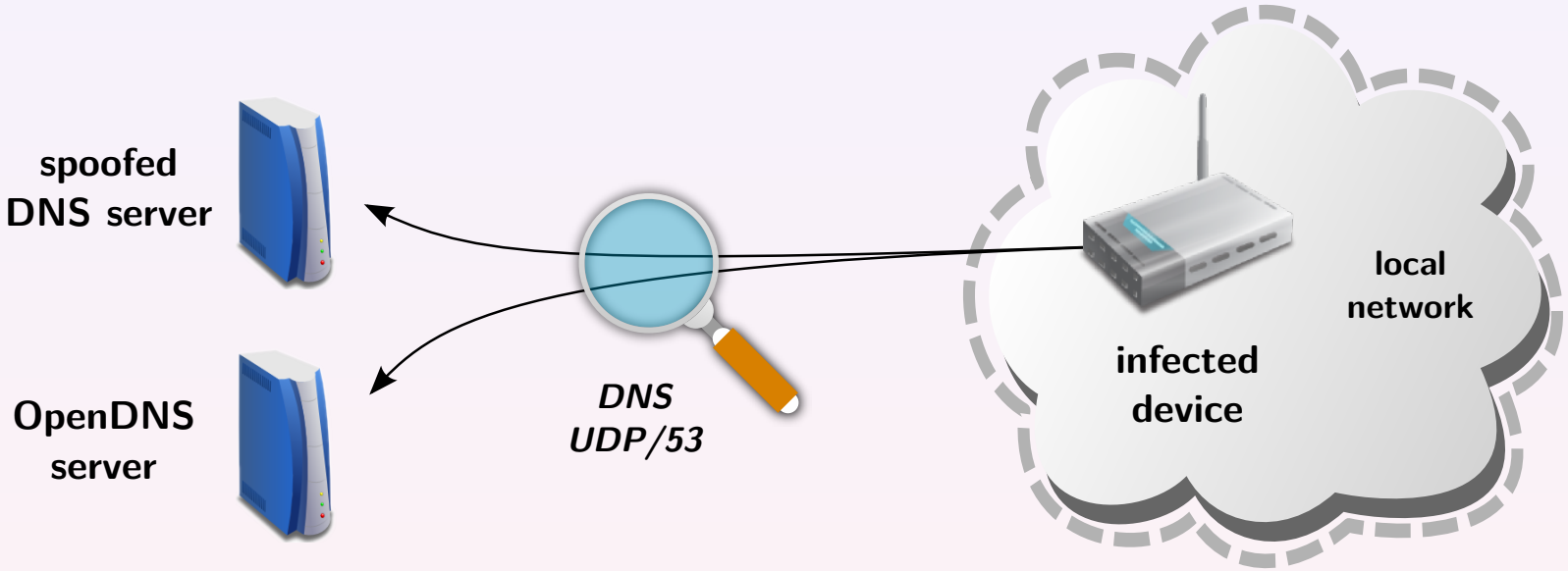
[2]IP addresses of a common OpenDNS servers

[3]IP addresses of a spoofed attacker's DNS servers

Detection of CNB DNS Spoofing Attack

Detecting Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's DNS**.



NFDUMP detection filter

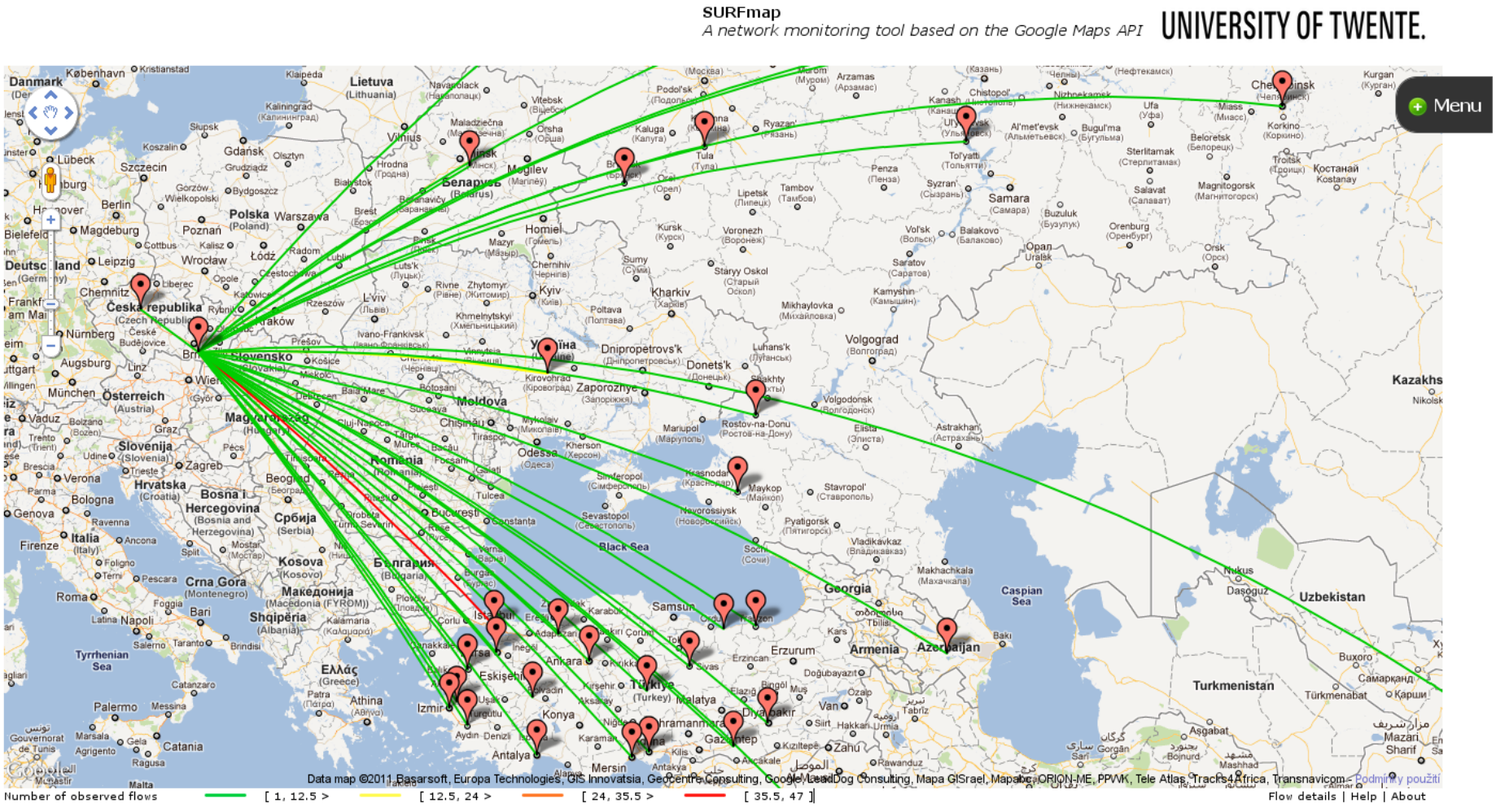
(src net *local_network*) and ((dst ip *OpenDNS servers*[2]) or (dst ip *DNS servers*[3])) and (proto UDP) and (dst port 53)

[2]IP addresses of a common OpenDNS servers

[3]IP addresses of a spoofed attacker's DNS servers

Chuck Norris Will Never Die or Cyber War ?

TELNET scans against single host – 2011-10-20.



SURFmap – http://surfmap.sf.net

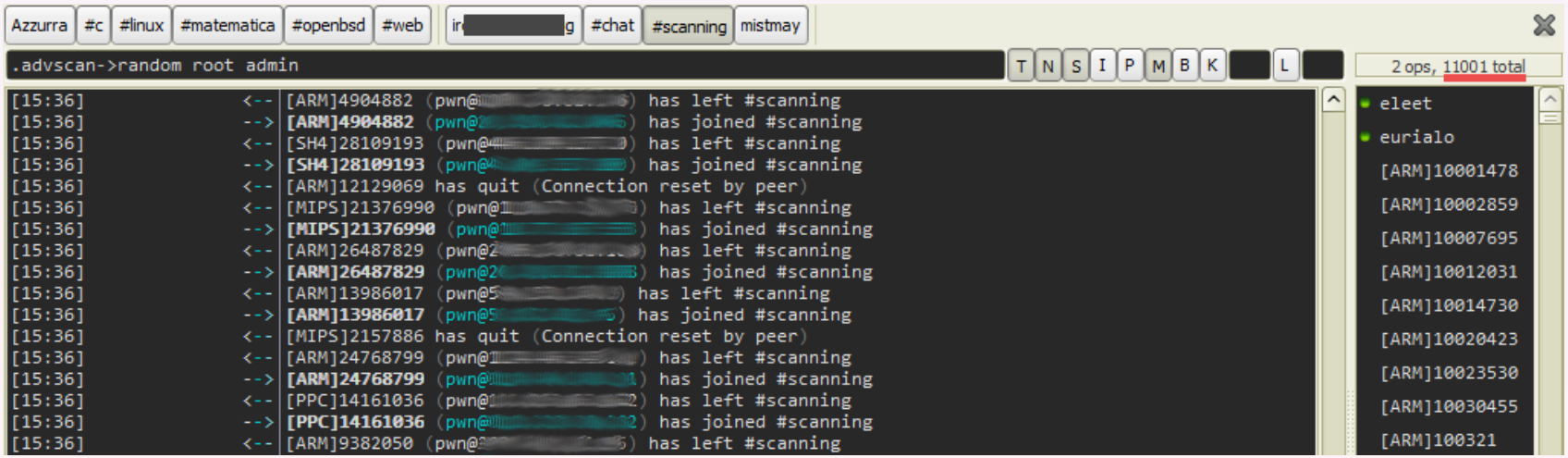
Part V

Anomaly Detection – Use Case III. Attack from Building Automation System

AIDRA Botnet in Nutshell

- **Linux malware** – IRC bots with central C&C servers.
- Based on source code of **Hydra** botnet.
- Attacks poorly-configured **ARM, MIPS, MIPSEL, PPC** and **SH4** Linux embedded devices (default Telnet credentials).
- First attacks observed at Masaryk University on 2011-12-04.

AIDRA in action (screenshot of 2011.1 private version)

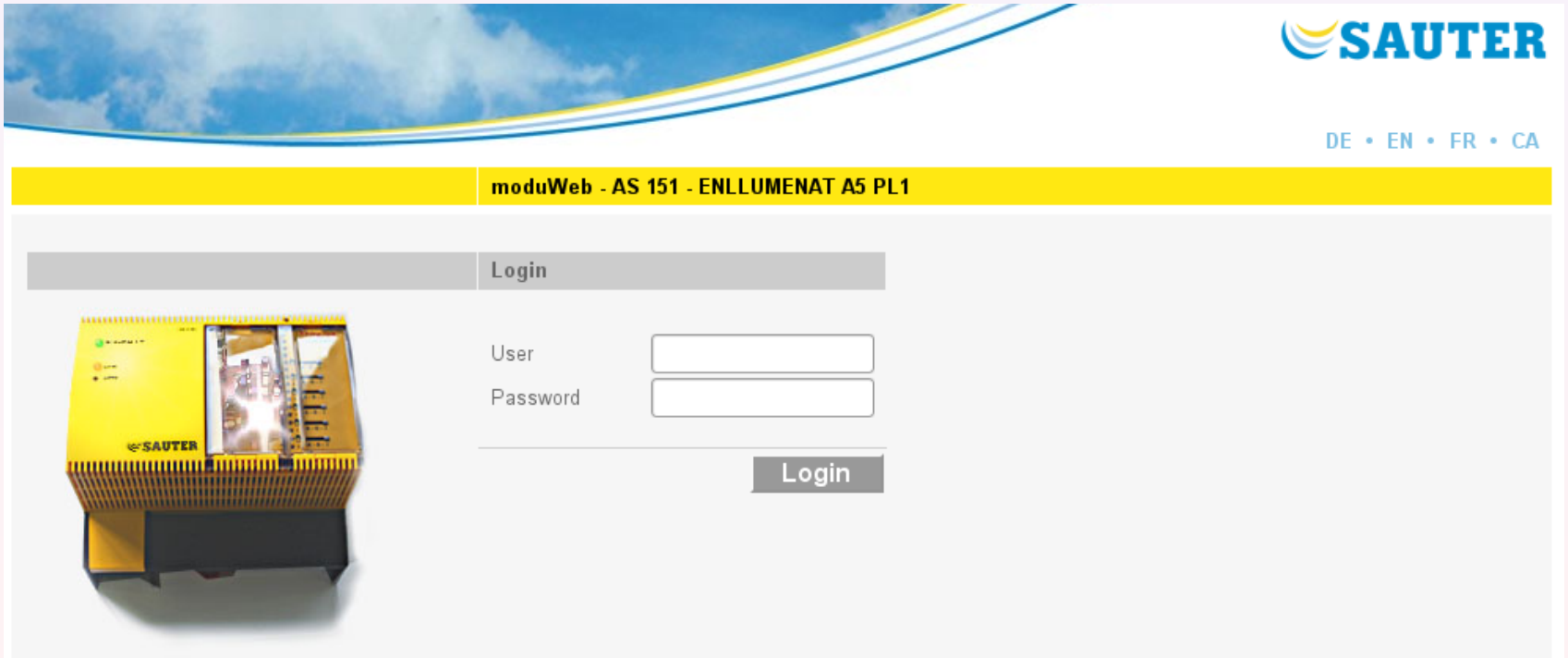


source – http://www.ahacktivia.org (2011-12-08)

Beyond Modems – AIDRA Infected Device

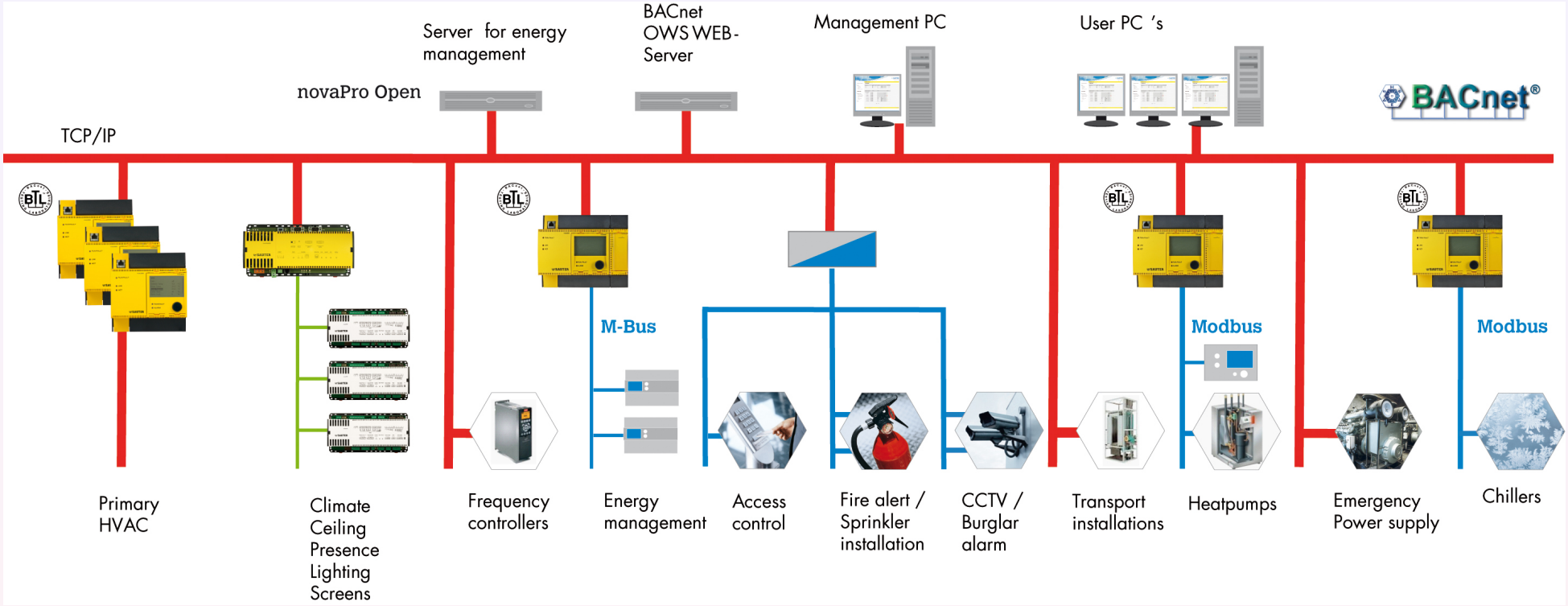
Modular Automation Station for Intelligent Buildings

- Control and monitoring of technical installations, e.g. HVAC.
- Communication: **BACnet/IP** (EN ISO 16484-5).
- Linux based (PPC) – integrated web and telnet server.



New Emerging Target – Intelligent Building

Topology of the Rabobank building management system

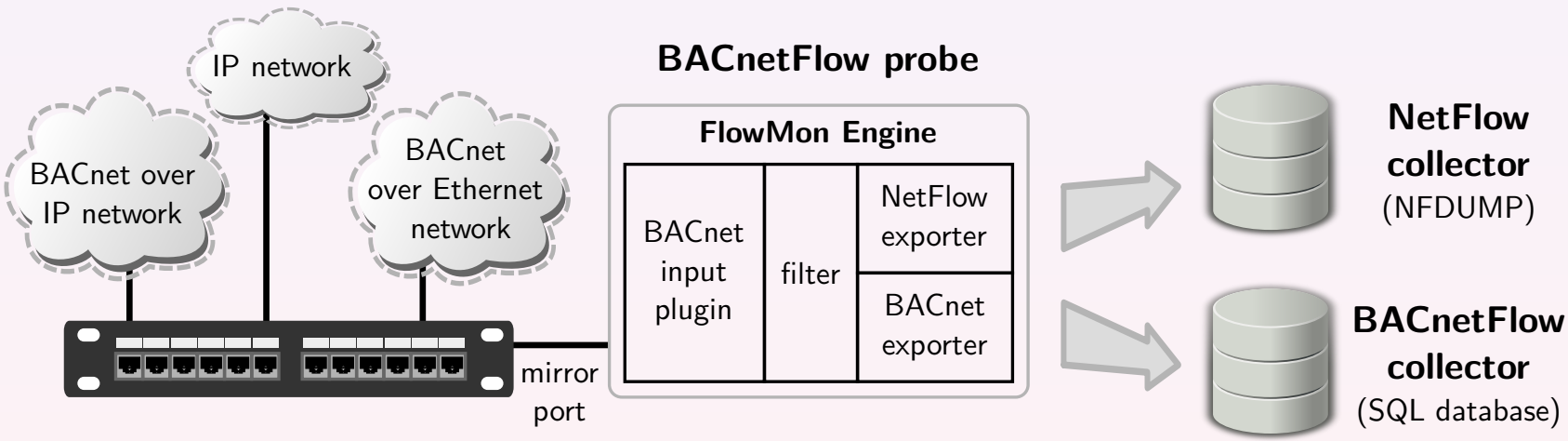


source – http://www.sauter-controls.com

AIDRA botnet does not support any targeted attacks against intelligent buildings!

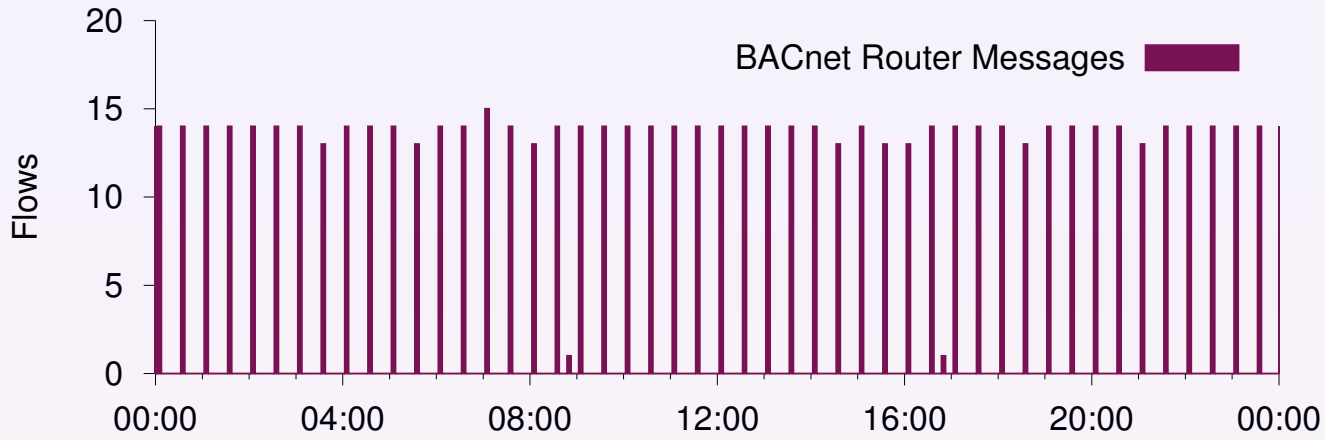
BACnet – Building Automation and Control Networking

- We introduced BACnetFlow[4] to get flow data from BACnet.
- BACnetFlow provides L2, L3, L4 and L7 visibility.
- BACnetFlow data can help detect BACnet attacks.

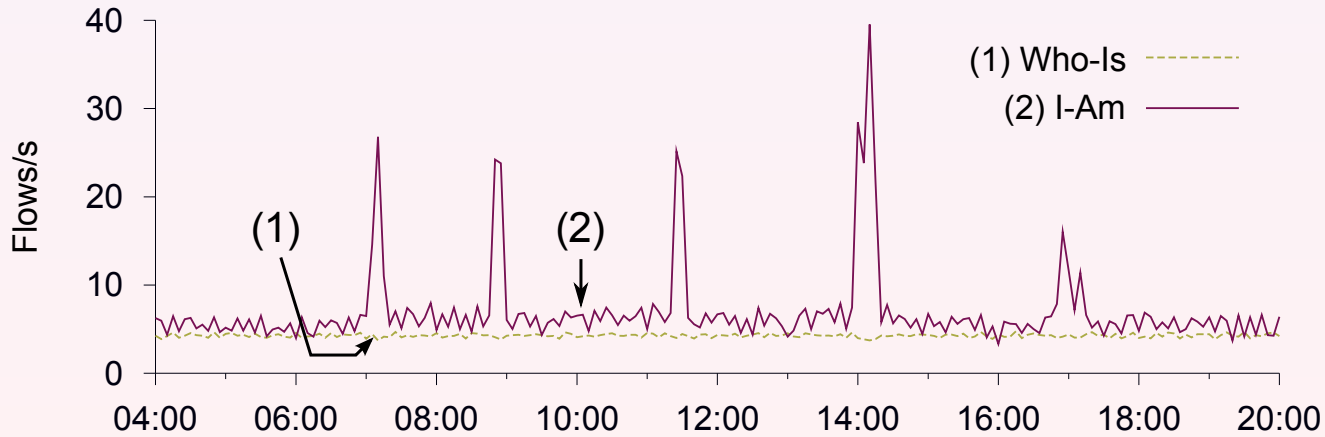


[4] Krejčí, R. et al.: *Traffic Measurement and Analysis of Building Automation and Control Networks*. Paper to appear in AIMS 2012.

BACnet Router Traffic - detection of router spoofing attacks



BACnet Device Discovery Traffic - detection of DoS attacks



Part VI

Conclusion

Conclusion

Why we need NSM and NBA?

- Networks are **complex** and prone to **failures** and **attacks**.
- Networks are difficult to manage without detailed information.
- IP flows present **scaleable** and **long-time** monitoring solution.

- Everybody leaves **traces in network traffic** (you can't hide).
- Observe and **automatically inspect 24x7** your network data.
- **Detect attacks before** your hosts are **infected**.

Experiences

- **Better network knowledge** after you deploy NSM and NBA.
- NSM and NBA are **essential in liberal** network environments.

Thank You For Your Attention!

Network Security Monitoring and Behavior Analysis

Pavel Čeleda et al.

celeda@ics.muni.cz

Project CAMNEP
http://www.muni.cz/ics/camnep

Project CYBER
http://www.muni.cz/ics/cyber