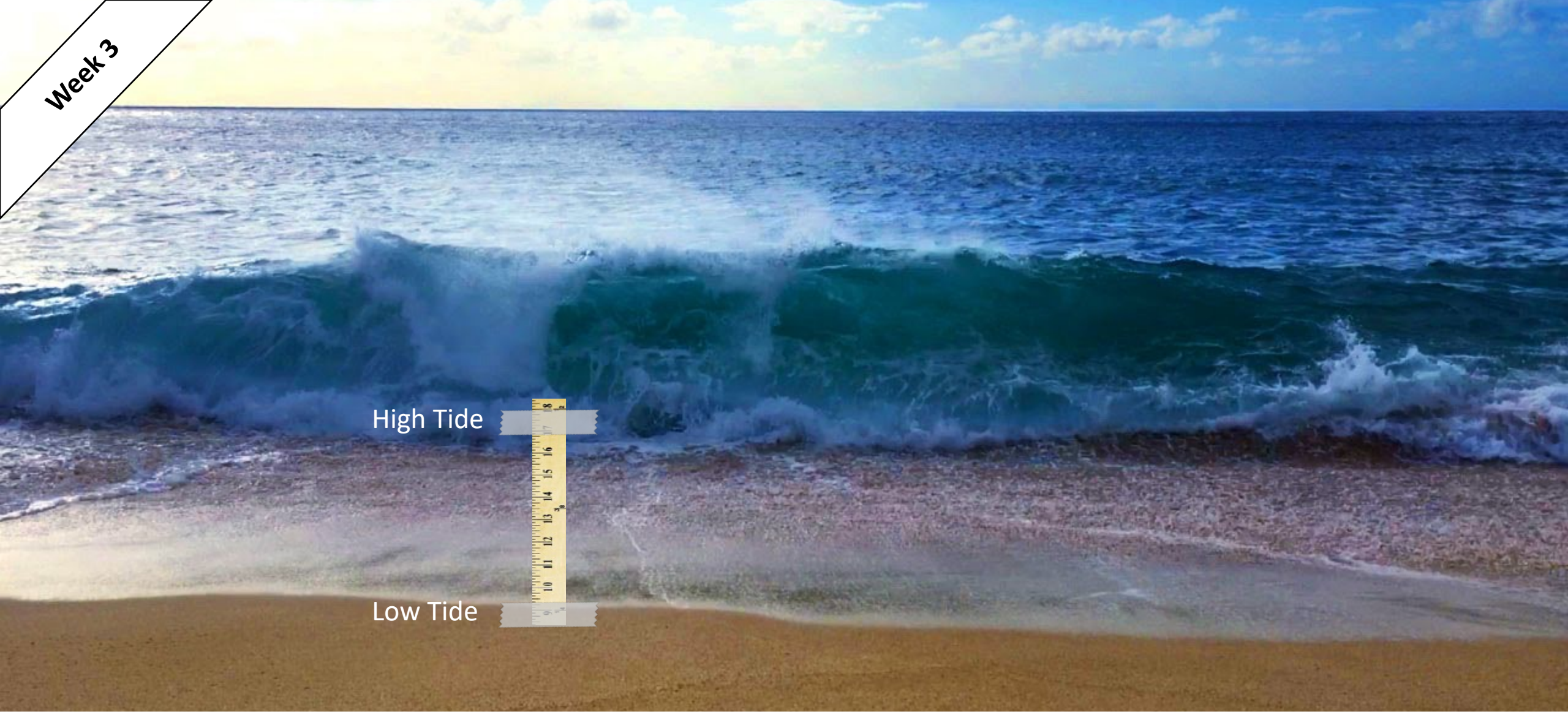
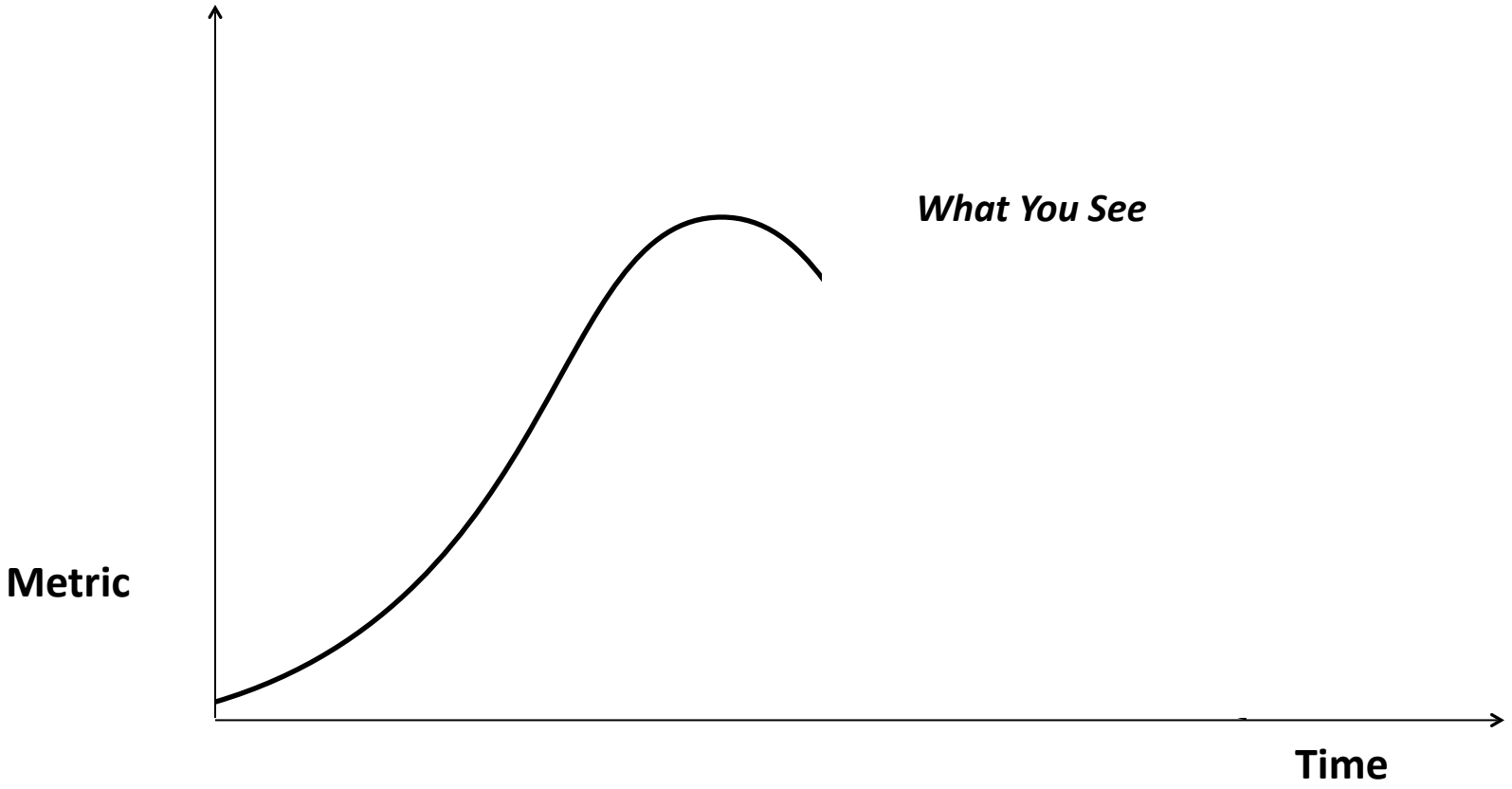


Week 3: Network Security Threats

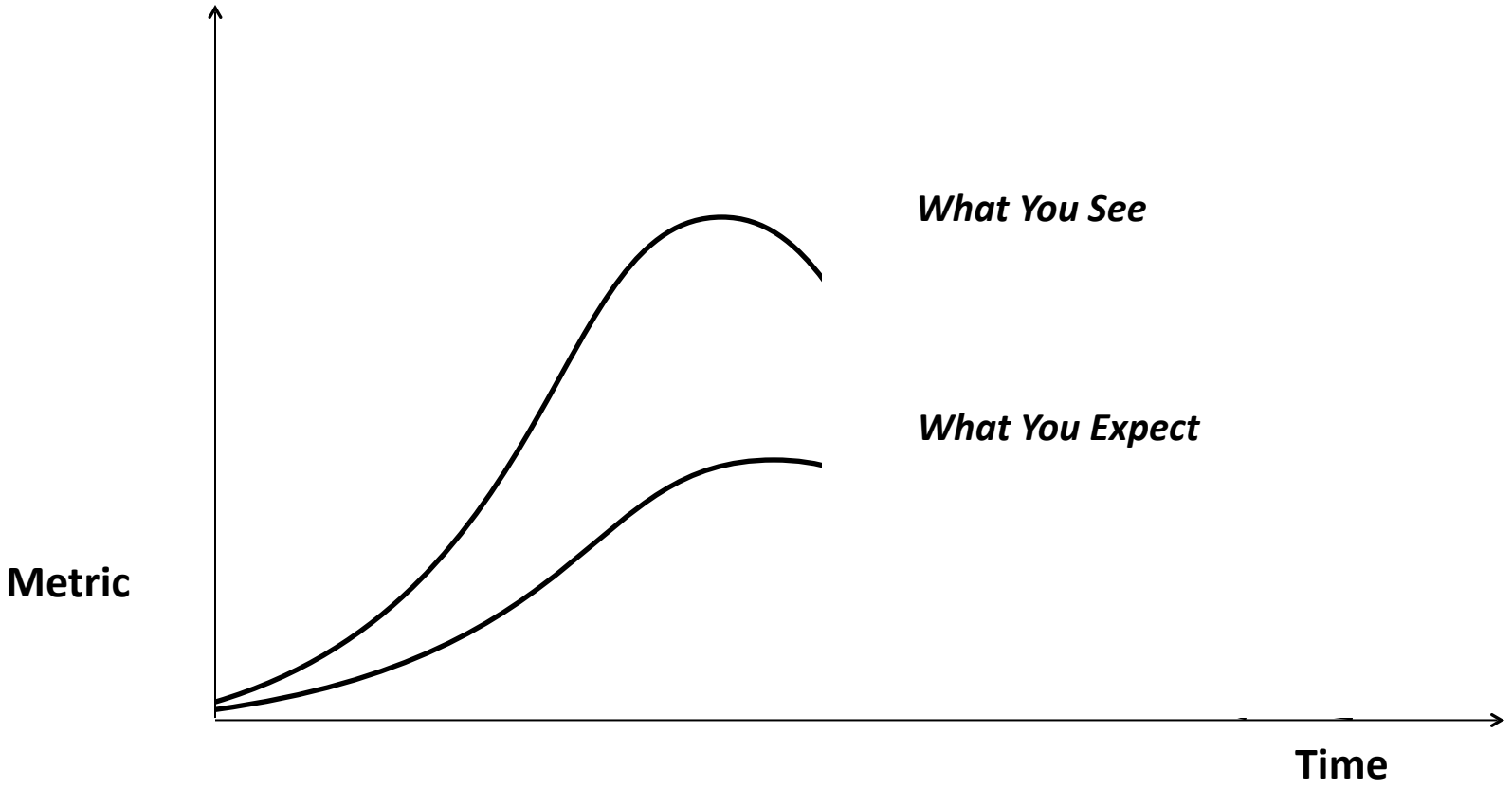
Week 3

Real Time Network Security Behavioral Analytics



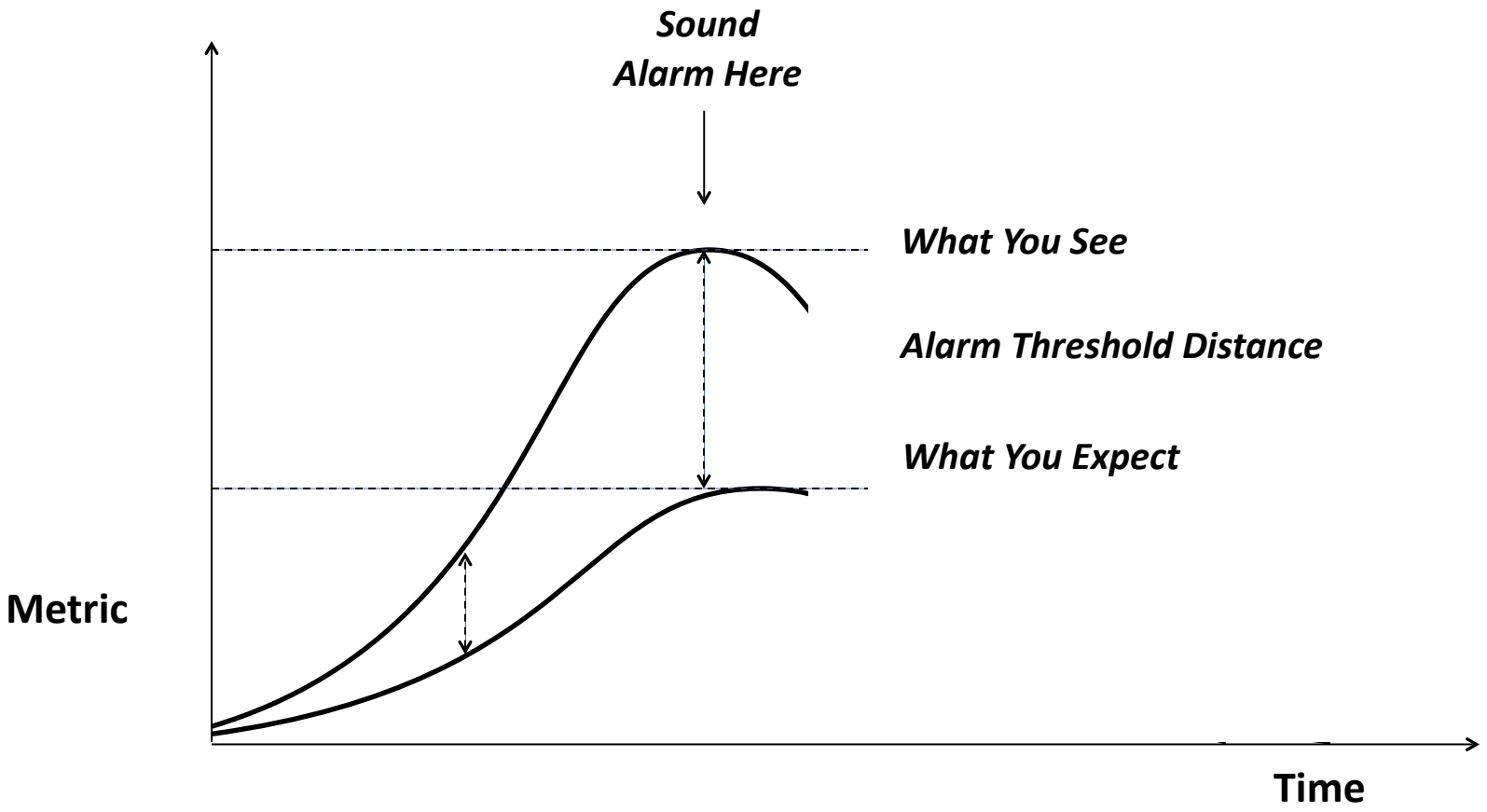
Week 3

Real Time Network Security Behavioral Analytics



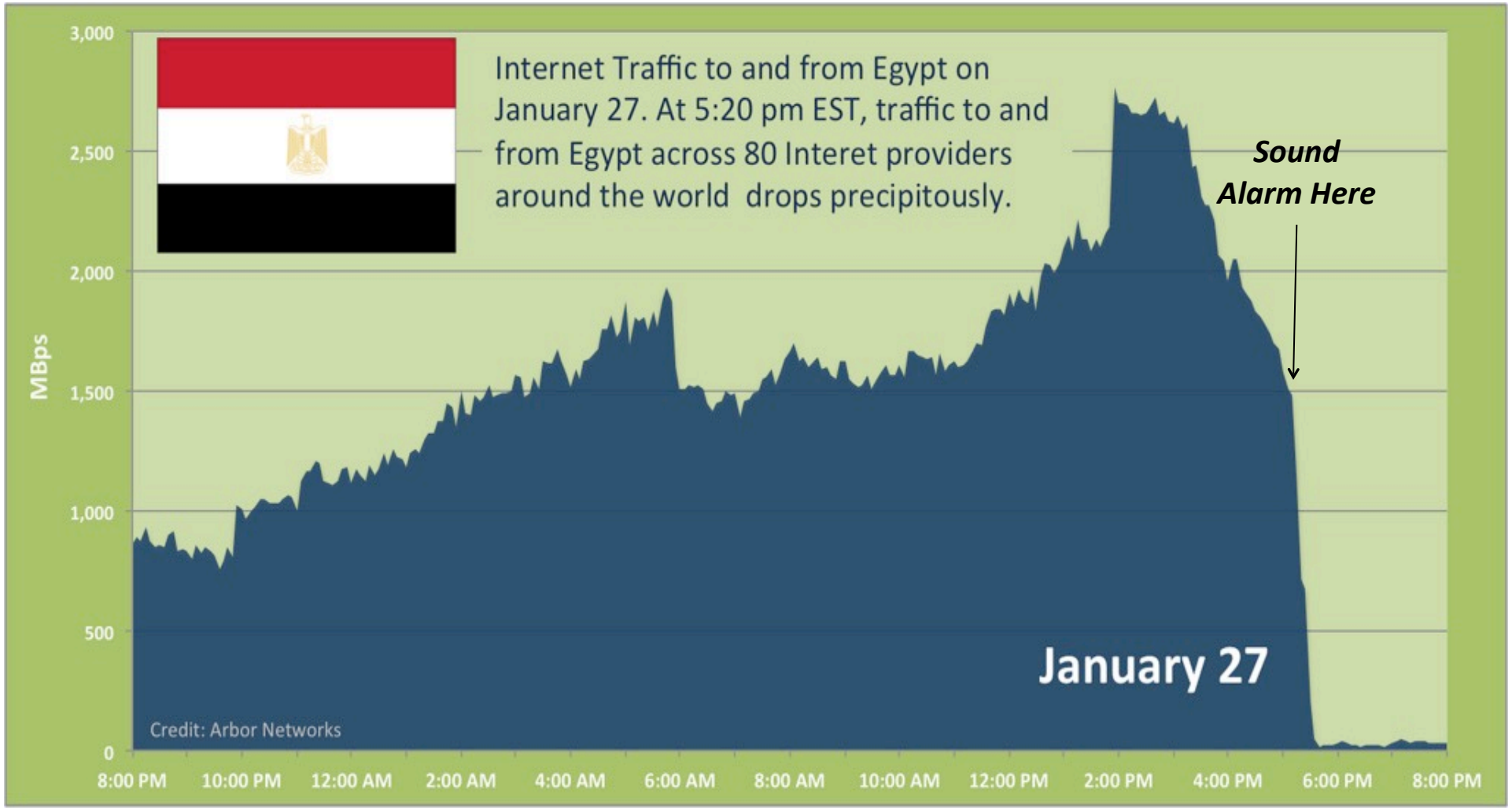
Week 3

Real Time Network Security Behavioral Analytics



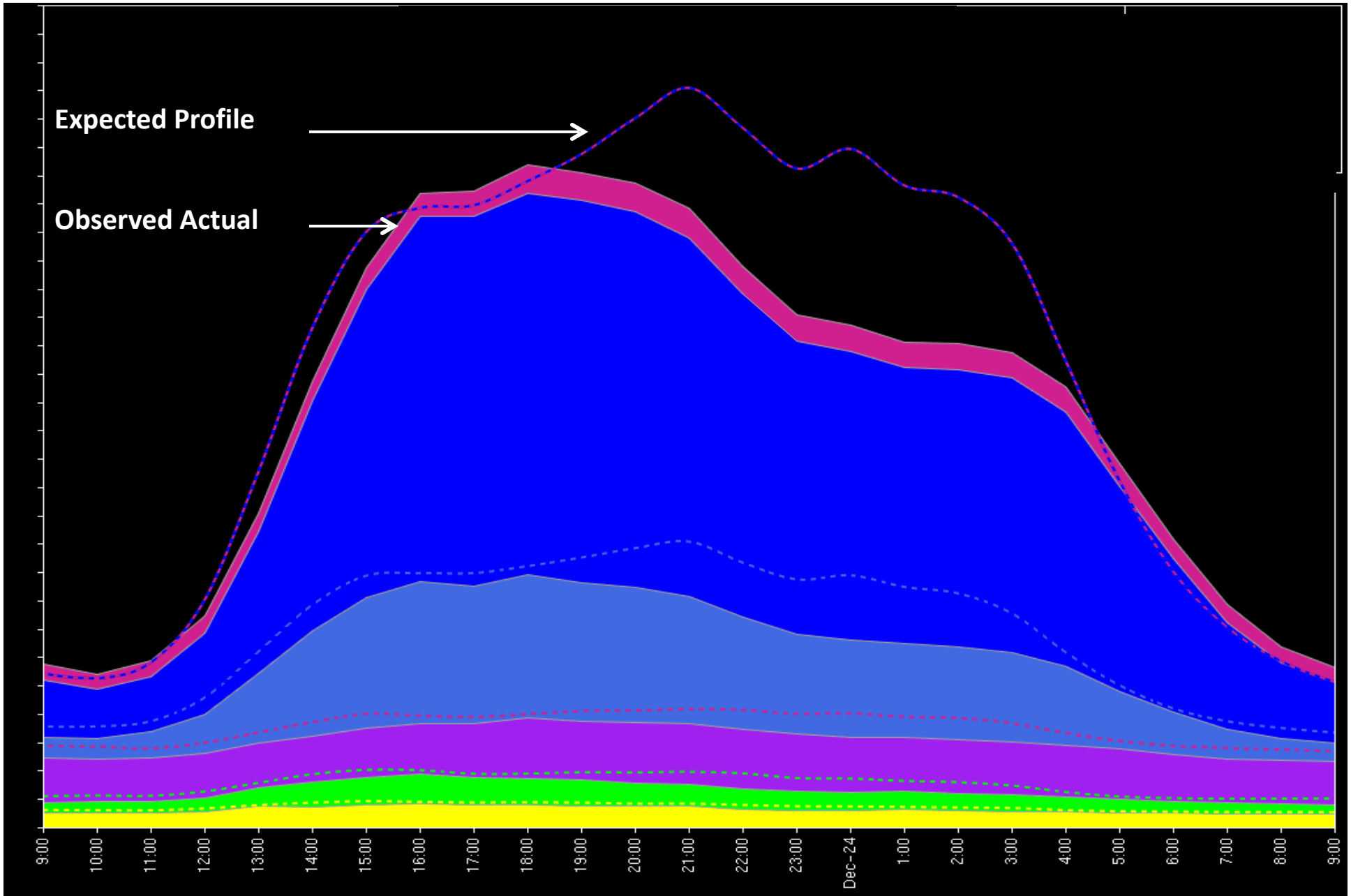
Week 3

Internet Blackout in Egypt – 01/27/11



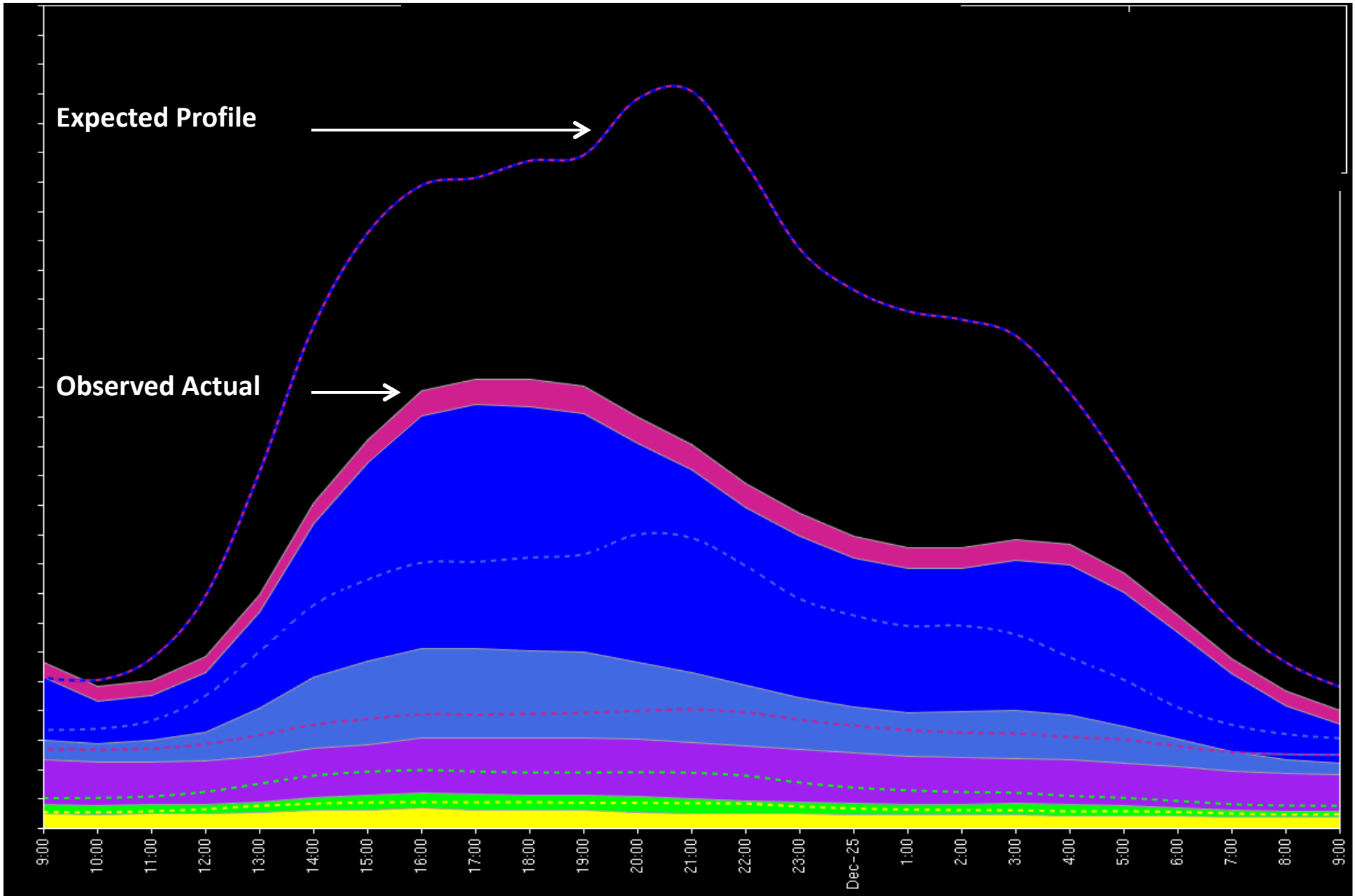
Week 3

Generic View of Public Internet Traffic – 12/23/04



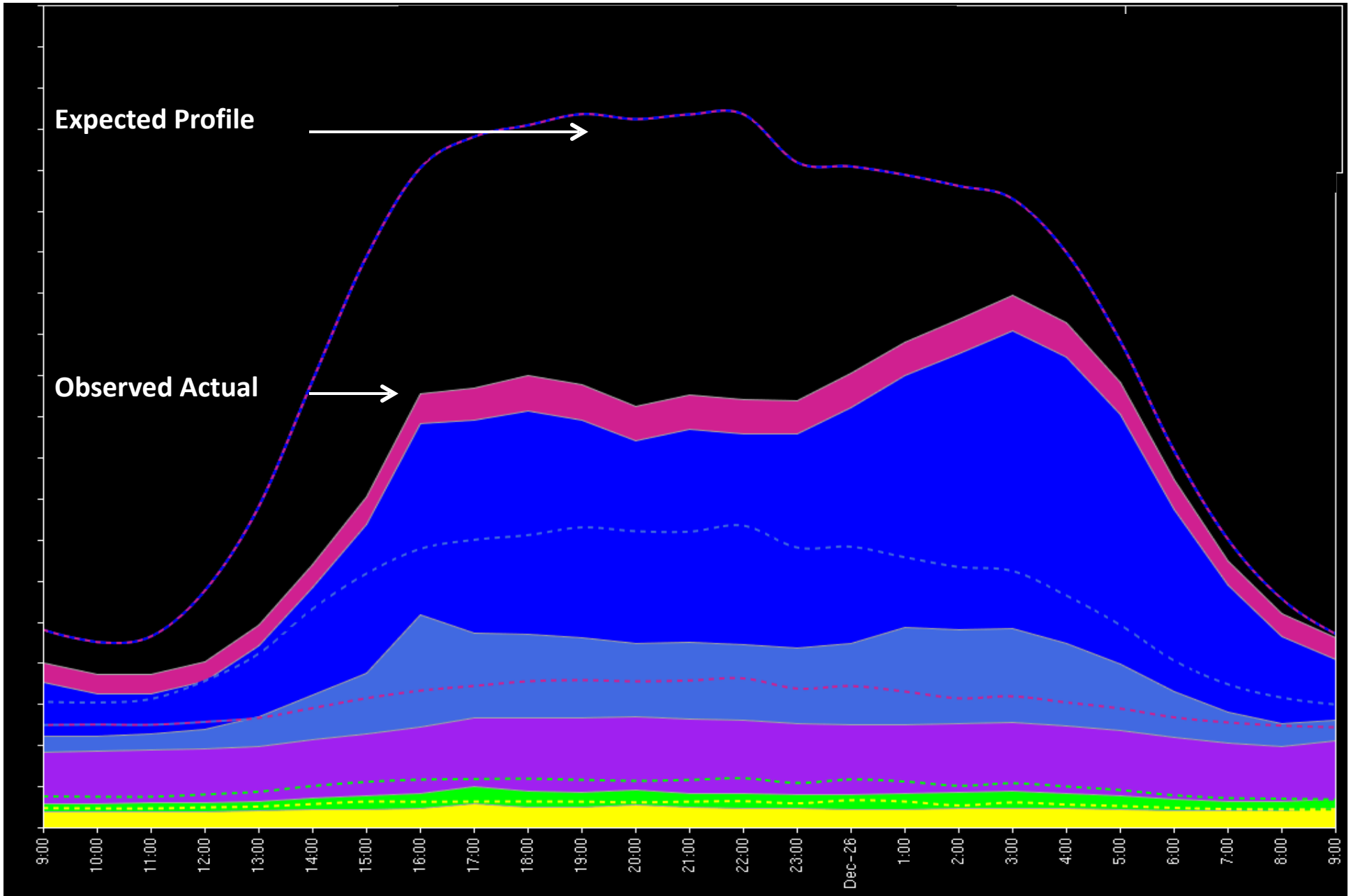
Week 3

Generic View of Public Internet Traffic – 12/24/04



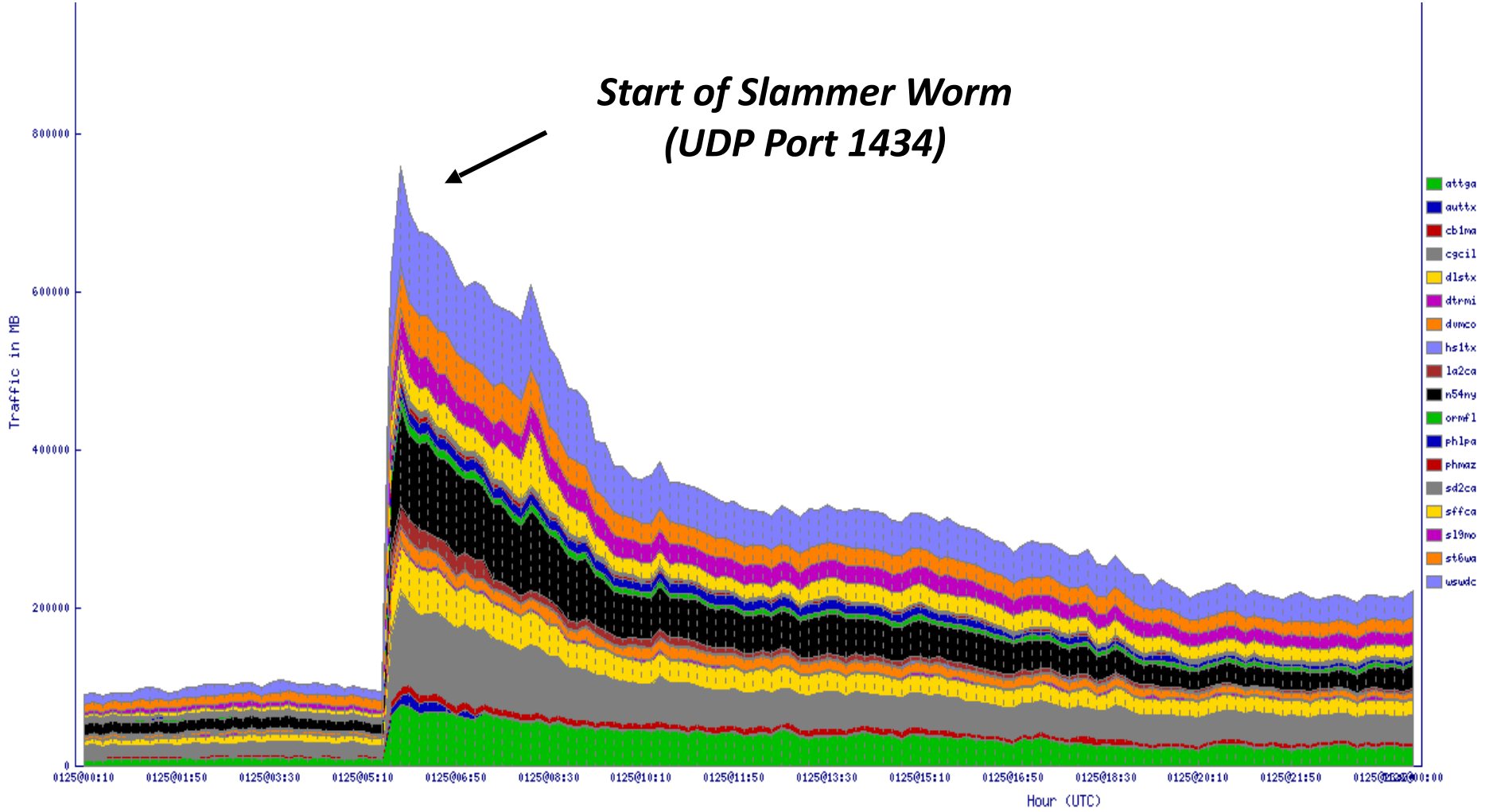
Week 3

Generic View of Public Internet Traffic – 12/25/04



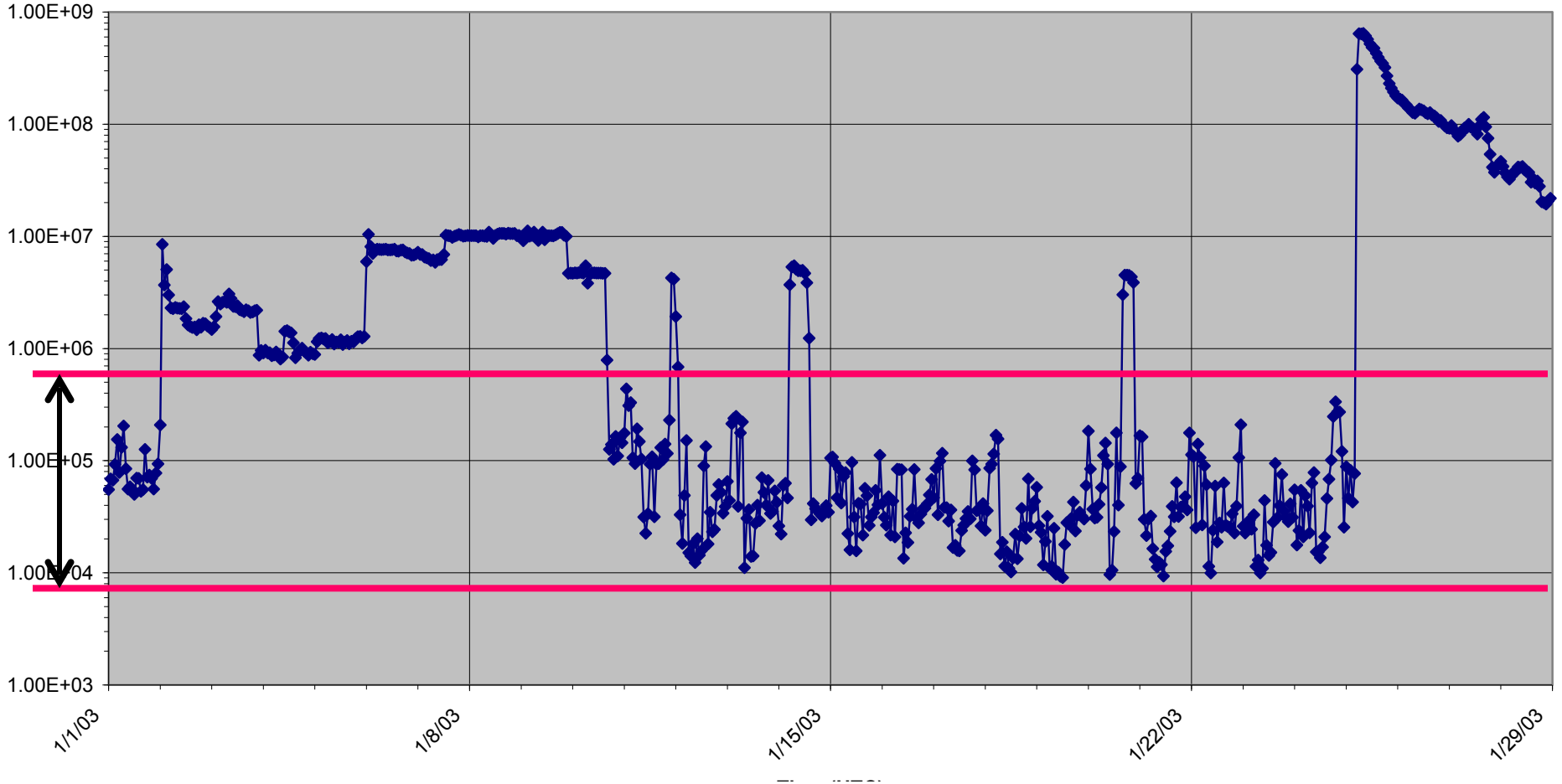
Week 3

Internet View of Slammer Worm – UDP Port 1434: 01/25/03



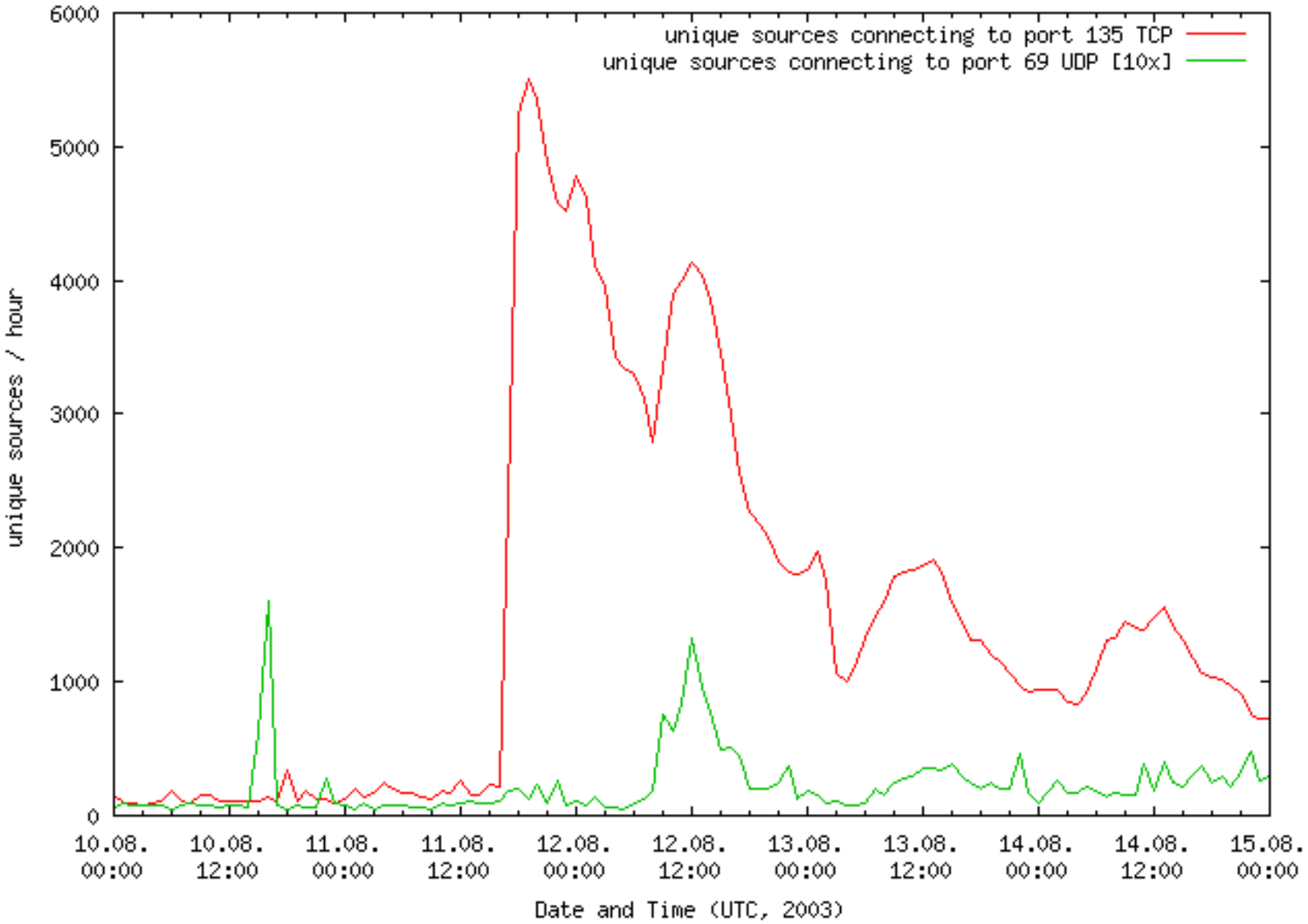
Week 3

Internet View of Slammer Worm – 01/03/03 – 01/25/03



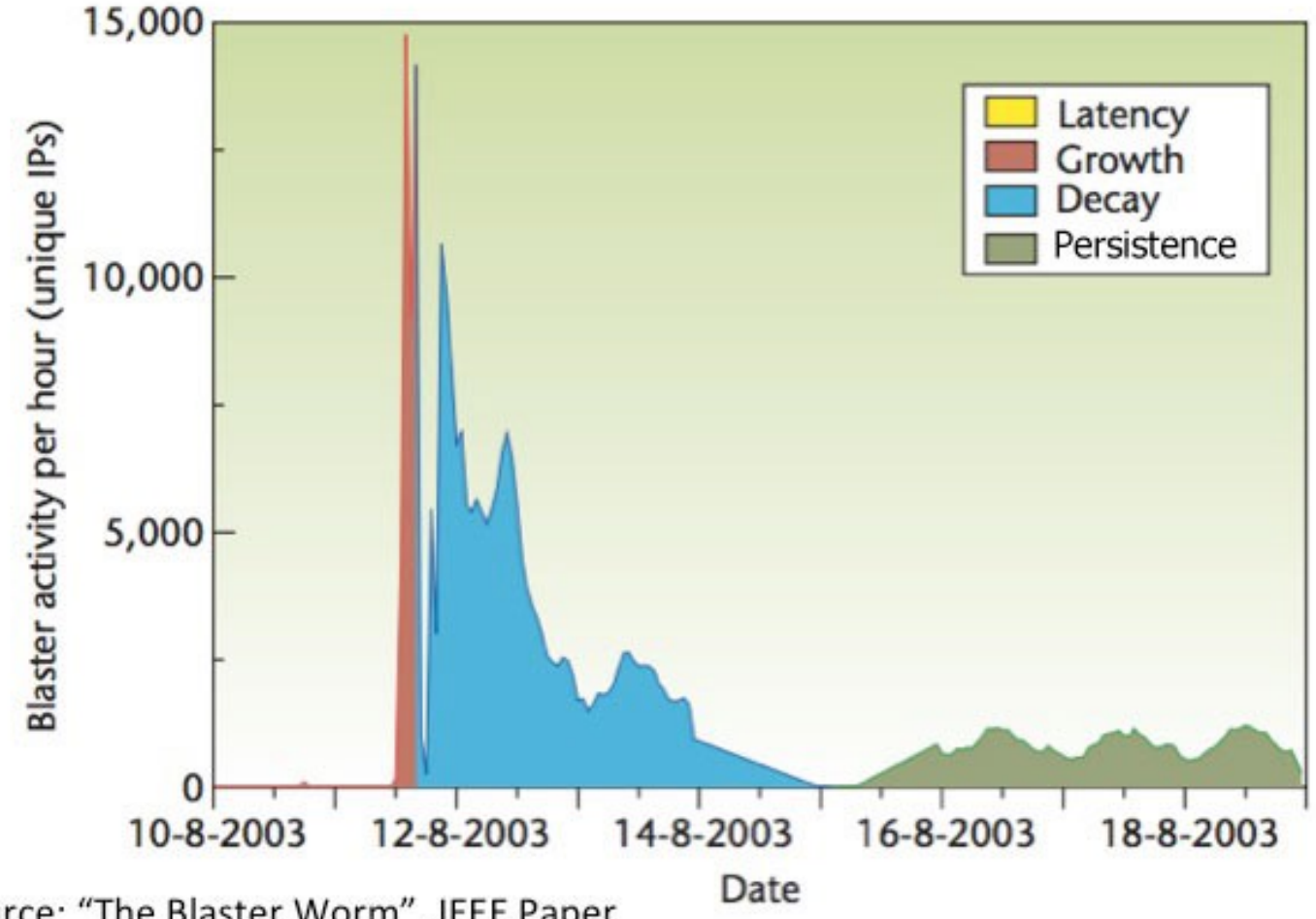
Week 3

Sharp Spike from Blaster Worm – 8/11/03



Week 3

Sharp Spike from Blaster Worm – 8/11/03

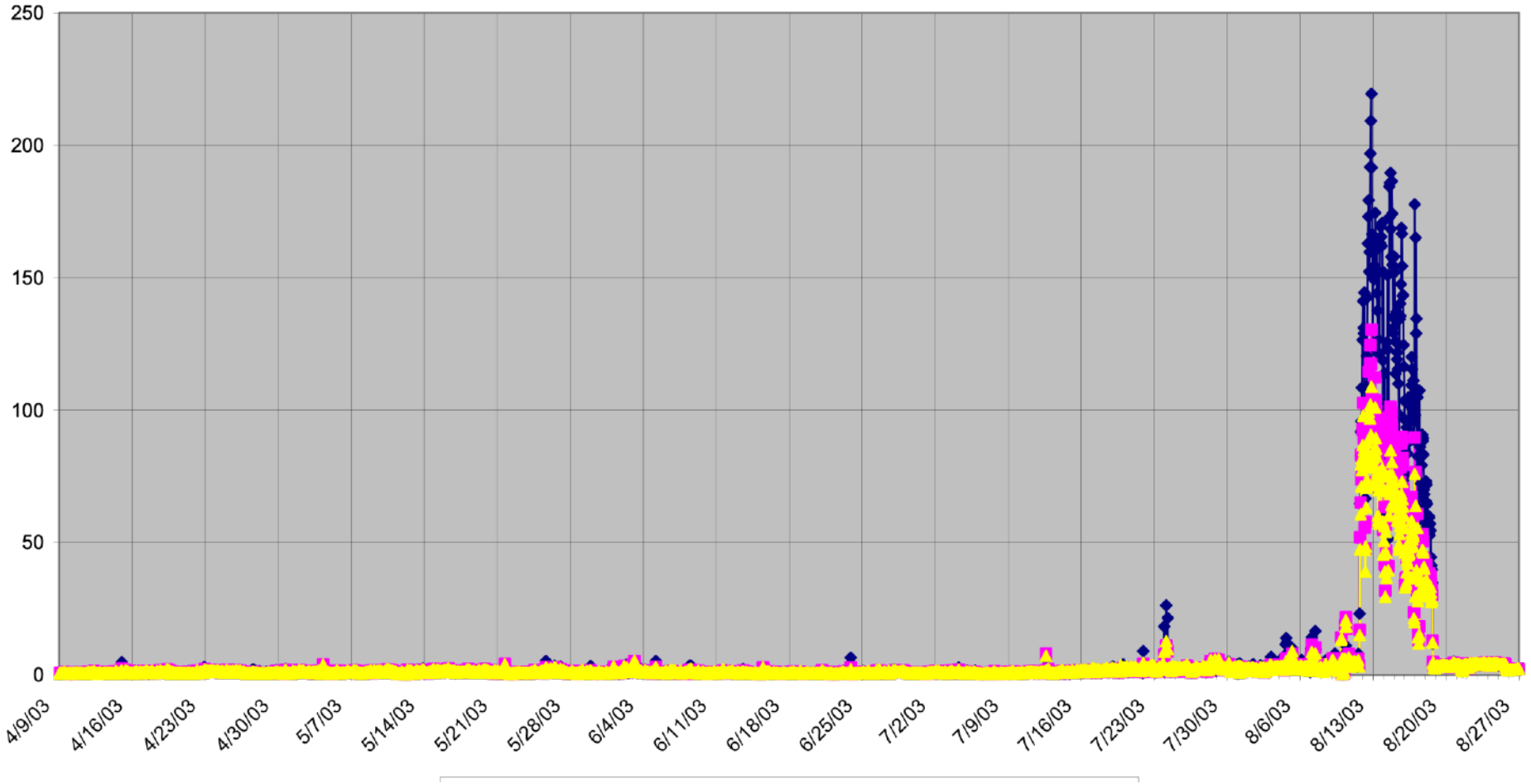


Source: "The Blaster Worm", IEEE Paper

ARBOR NETWORKS

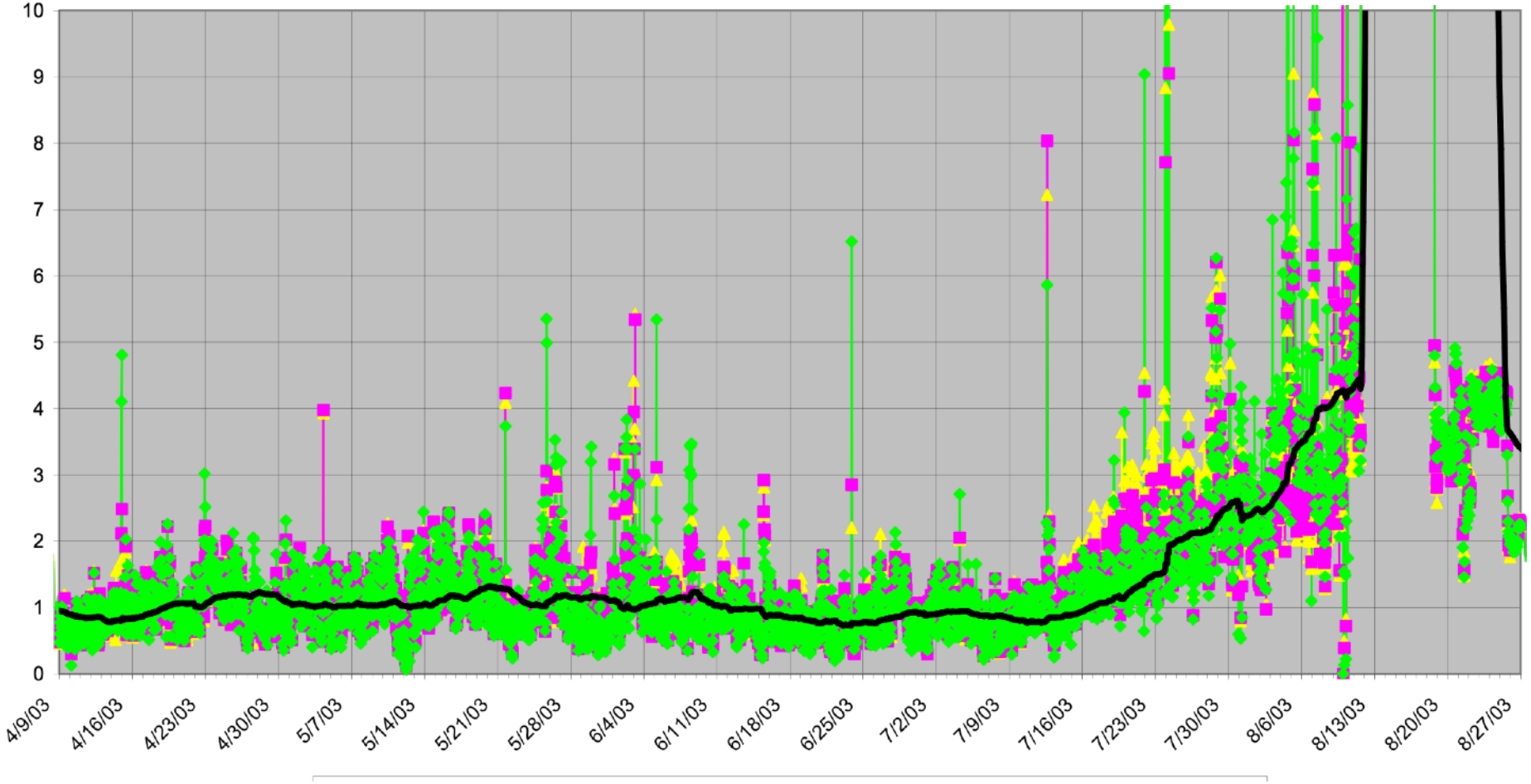
Week 3

Internet View of TCP 135 – Blaster Worm – 2003



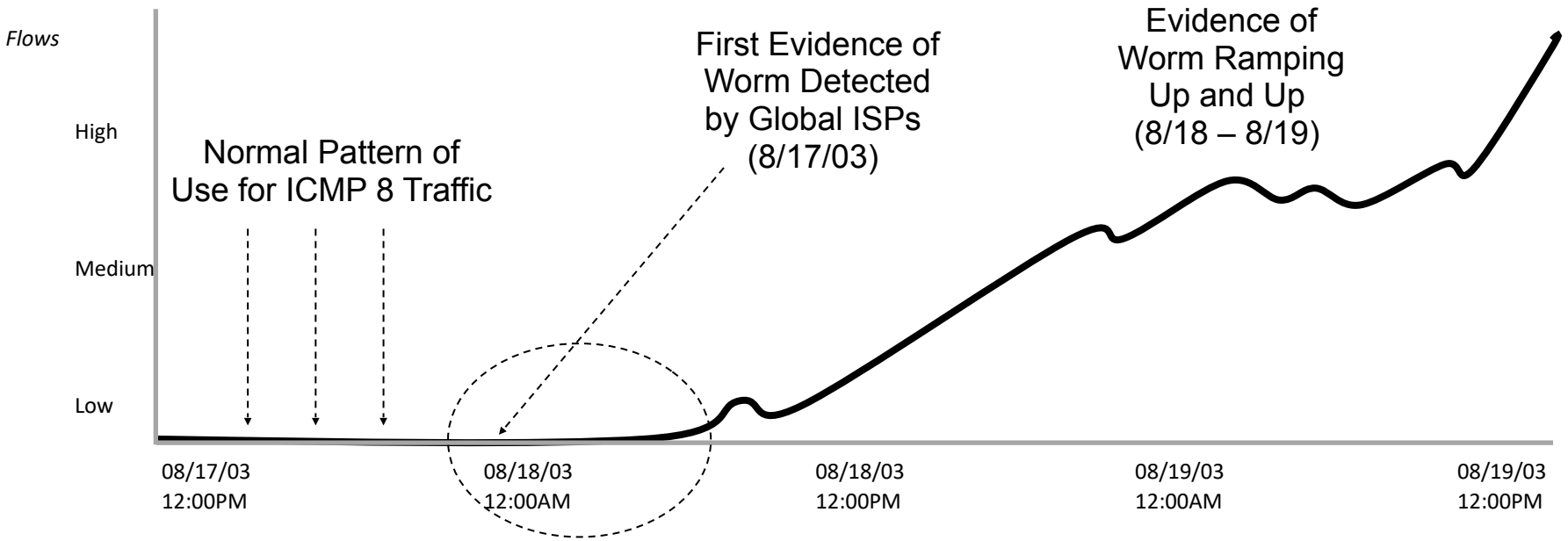
Week 3

Deeper Internet View of TCP 135 Activity – Blaster Worm



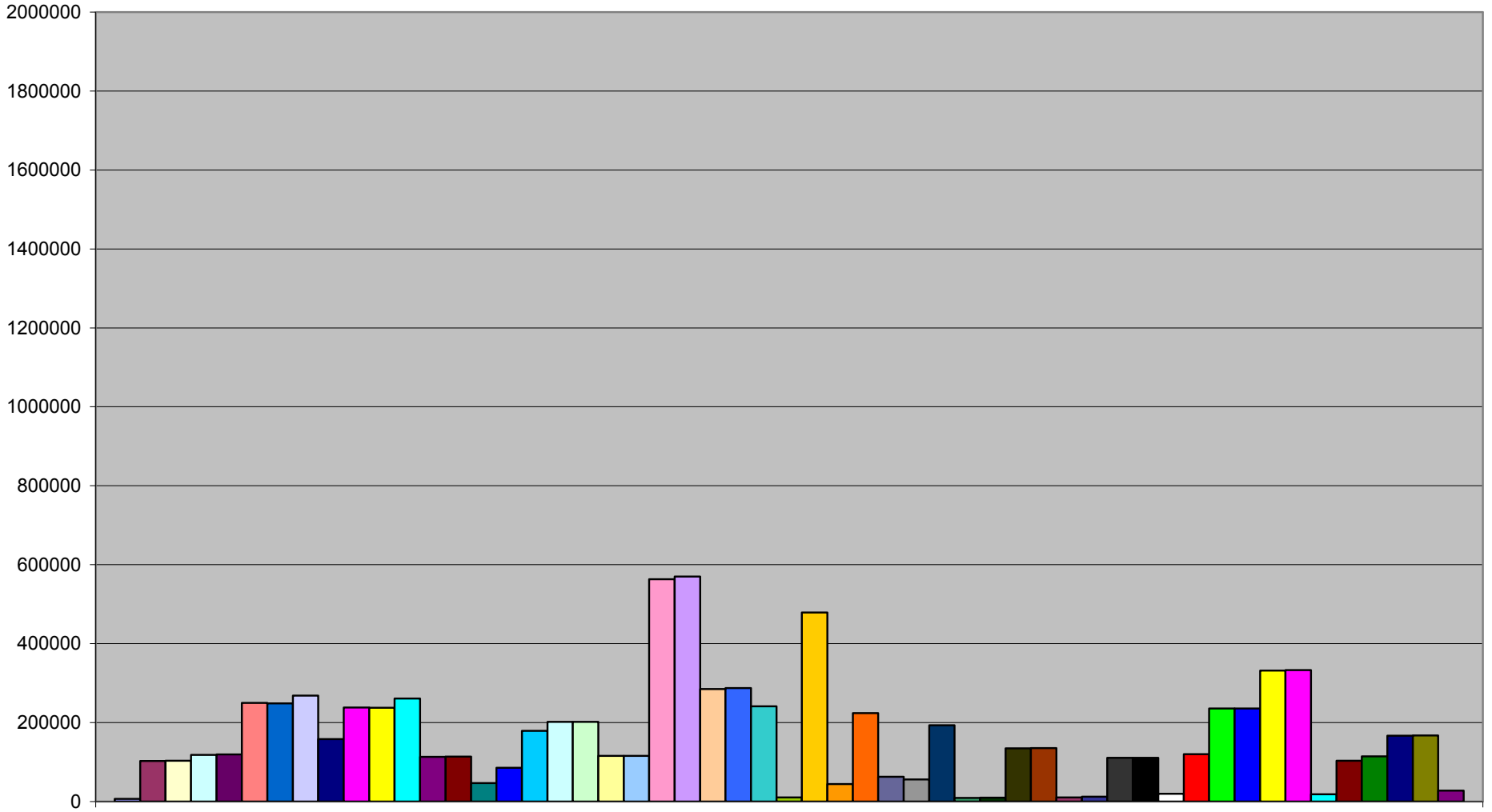
Week 3

Nachi Worm of 2003



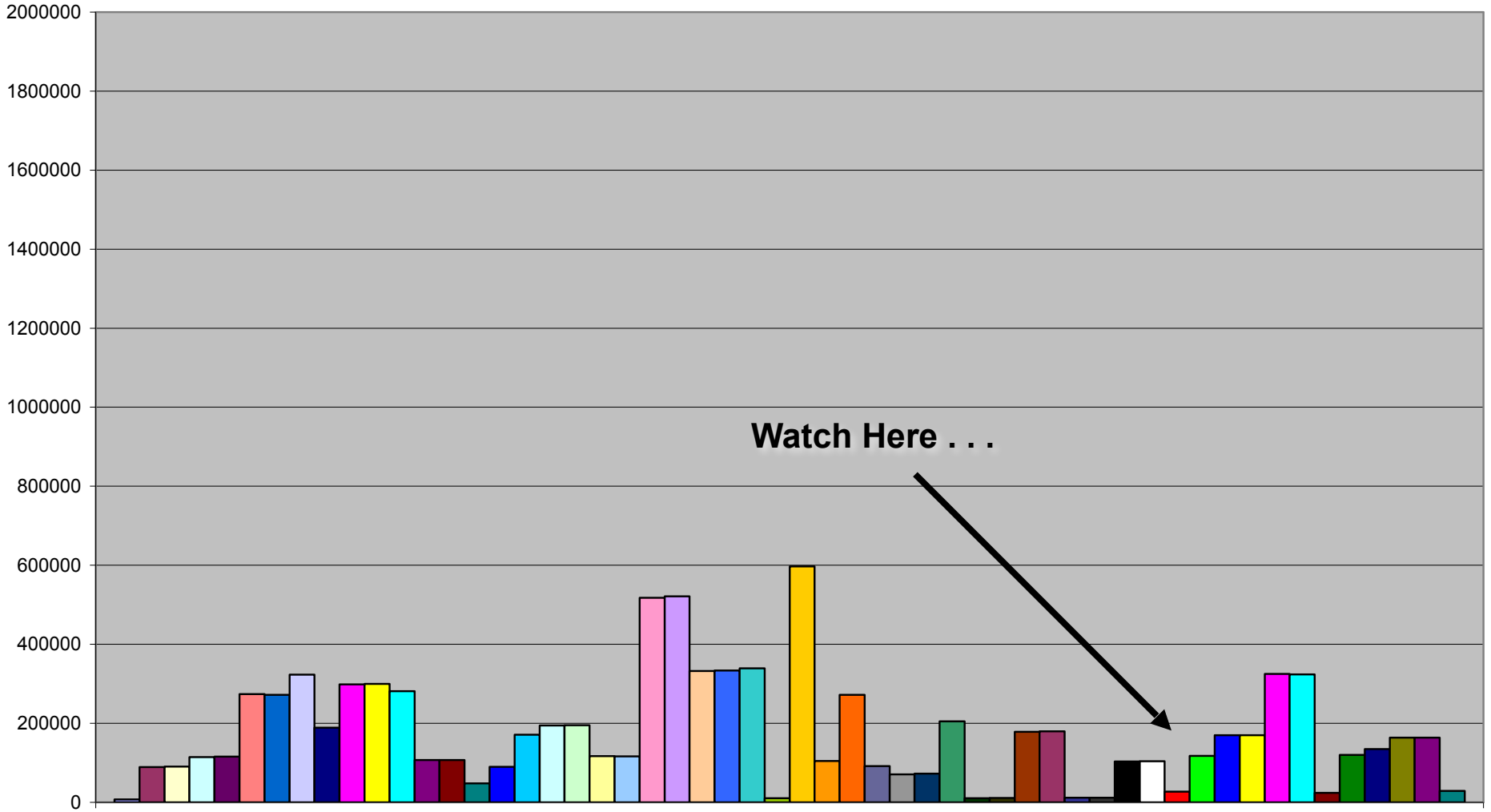
Week 3

Nachi 8/17/03 10:00PM



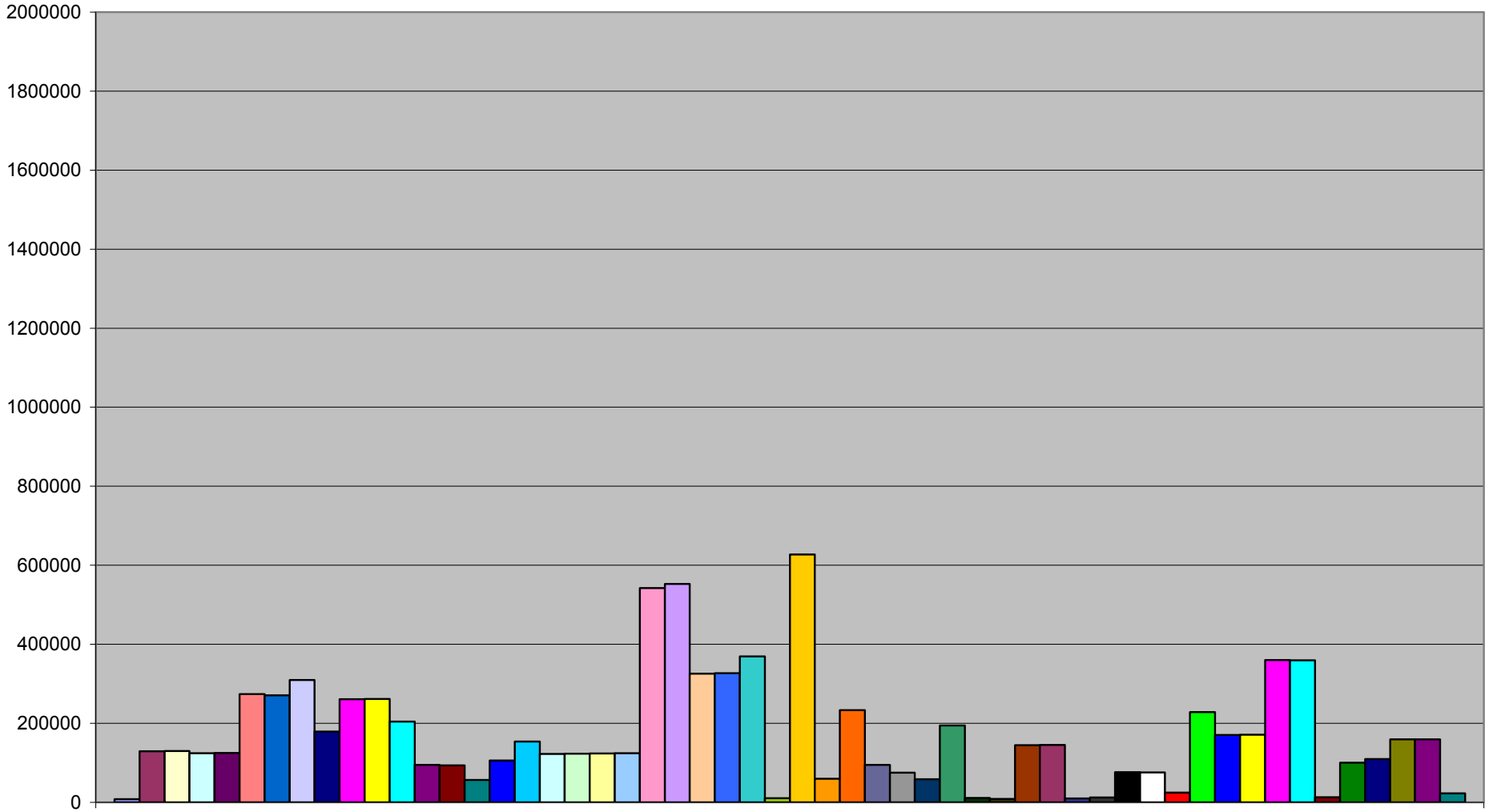
Week 3

Nachi 8/17/03 11:00PM



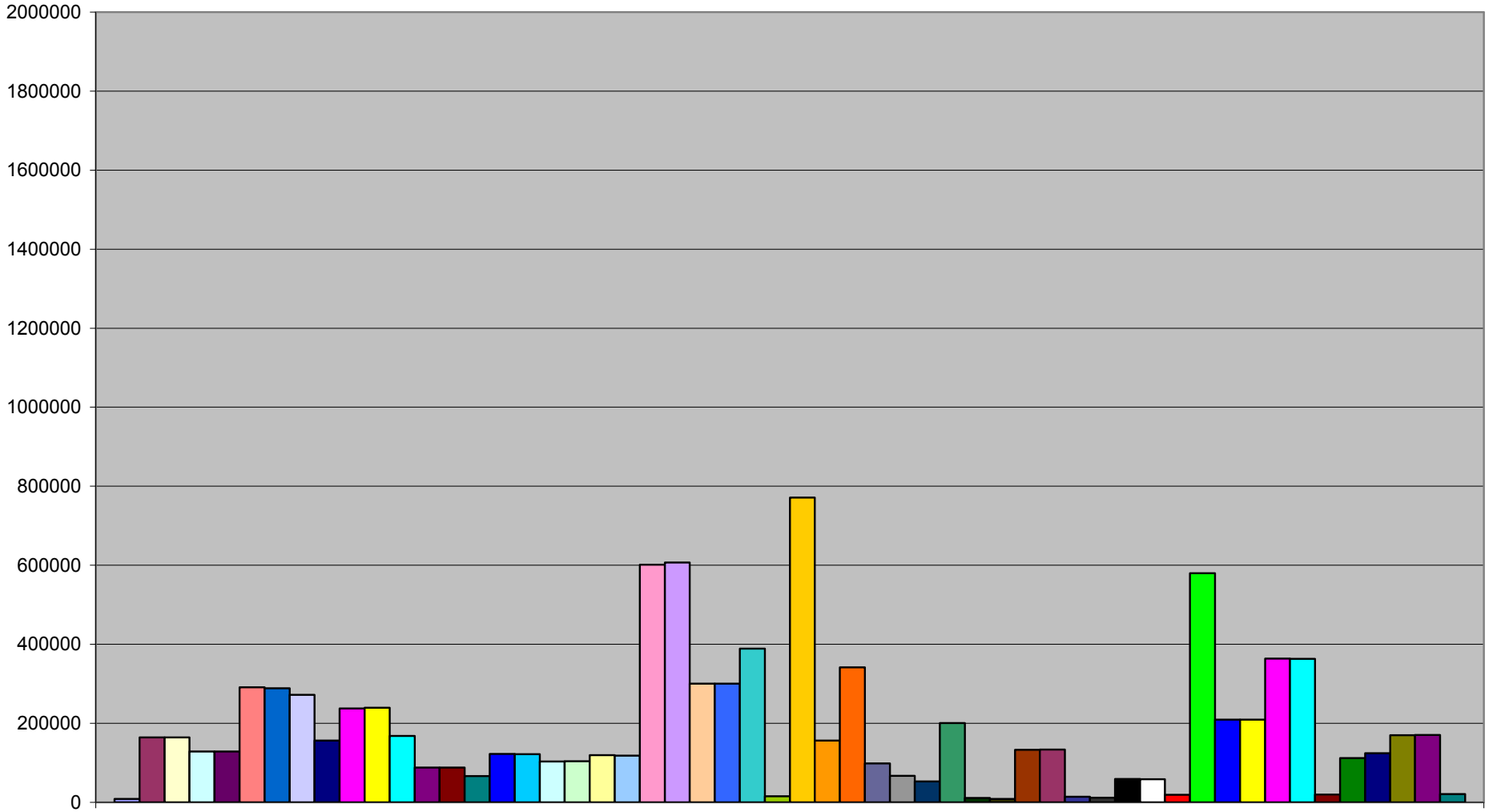
Week 3

Nachi 8/17/03 Midnight



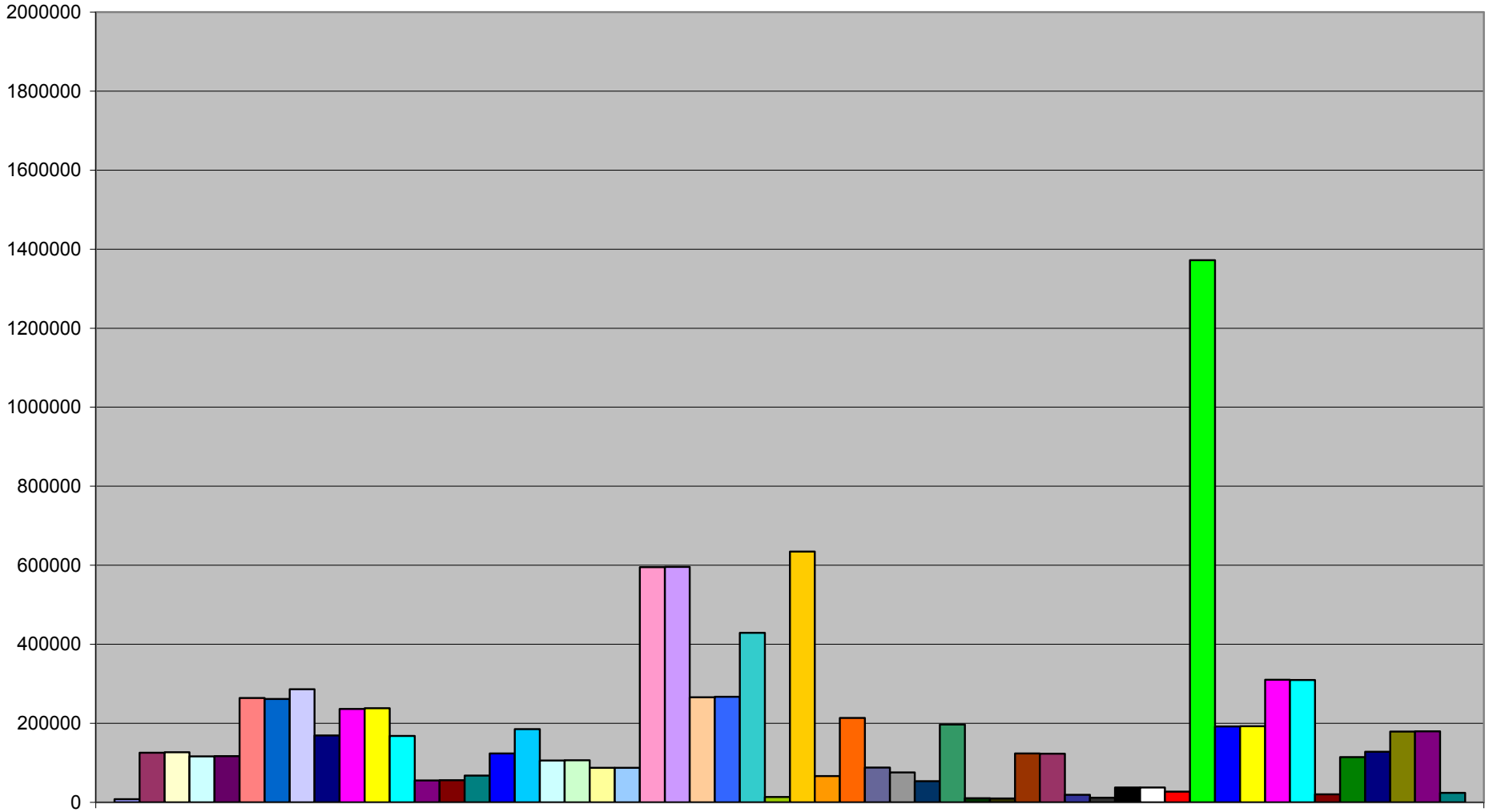
Week 3

Nachi 8/18/03 1:00AM



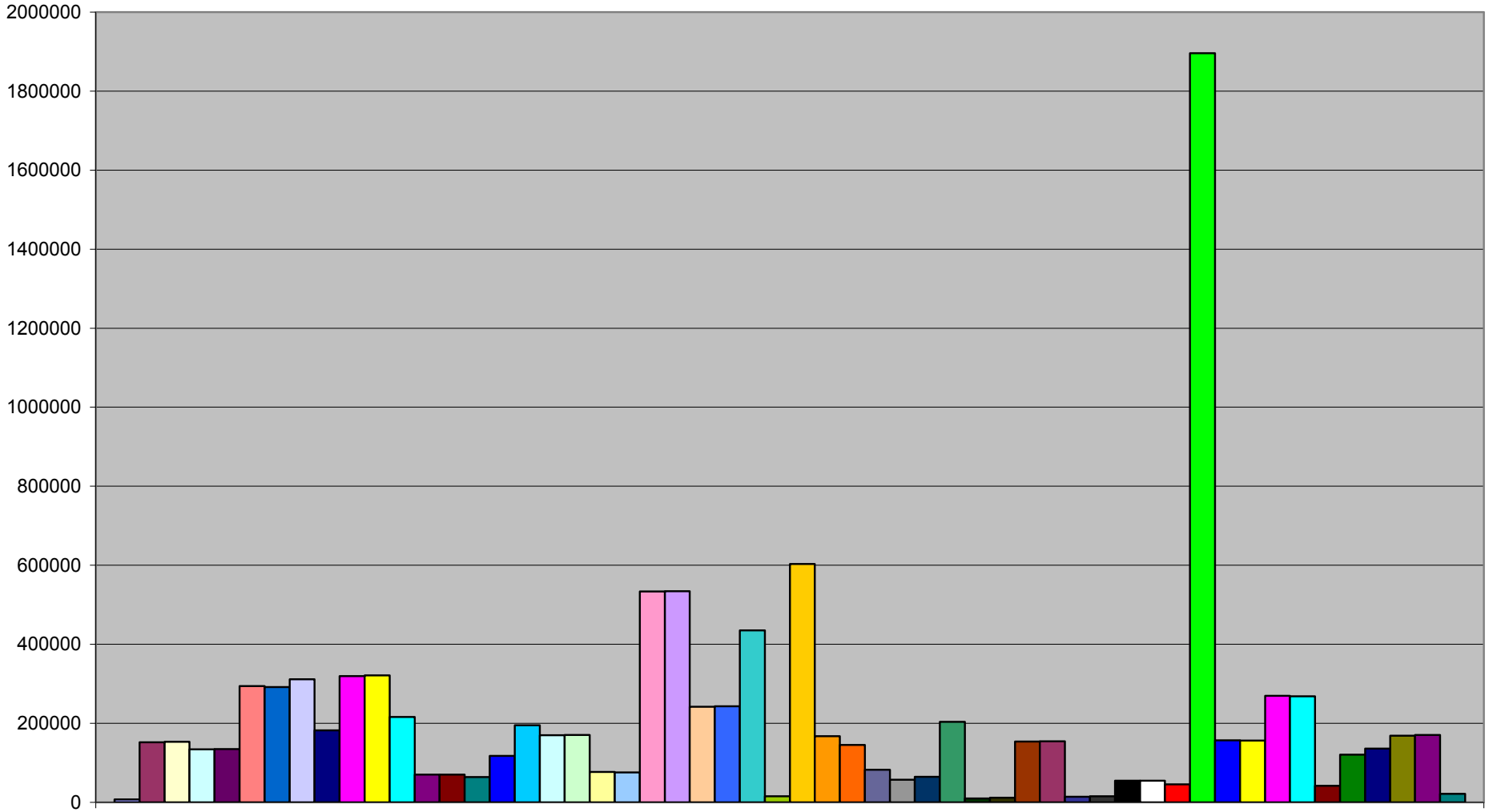
Week 3

Nachi 8/18/03 2:00AM



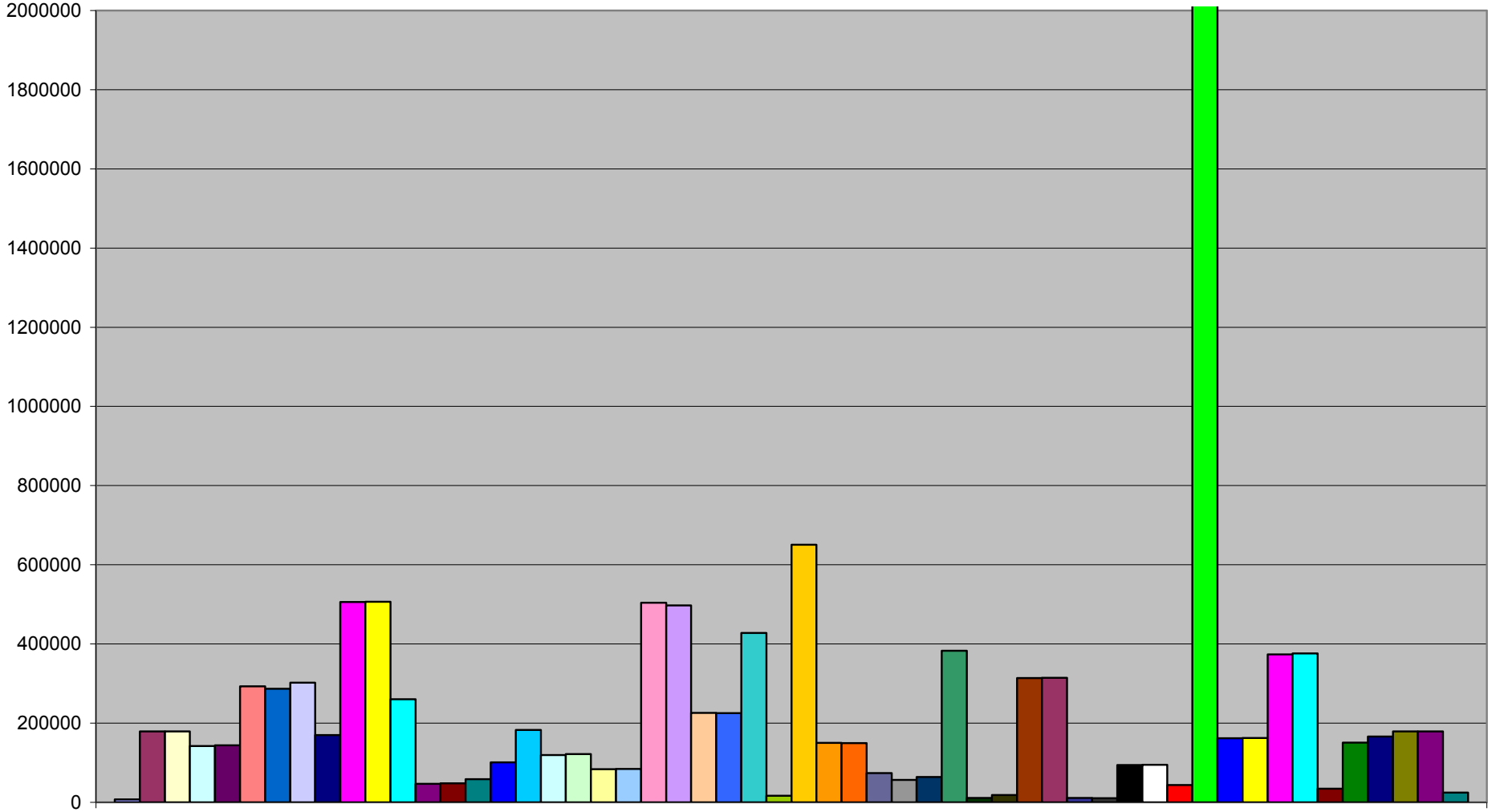
Week 3

Nachi 8/18/03 3:00AM



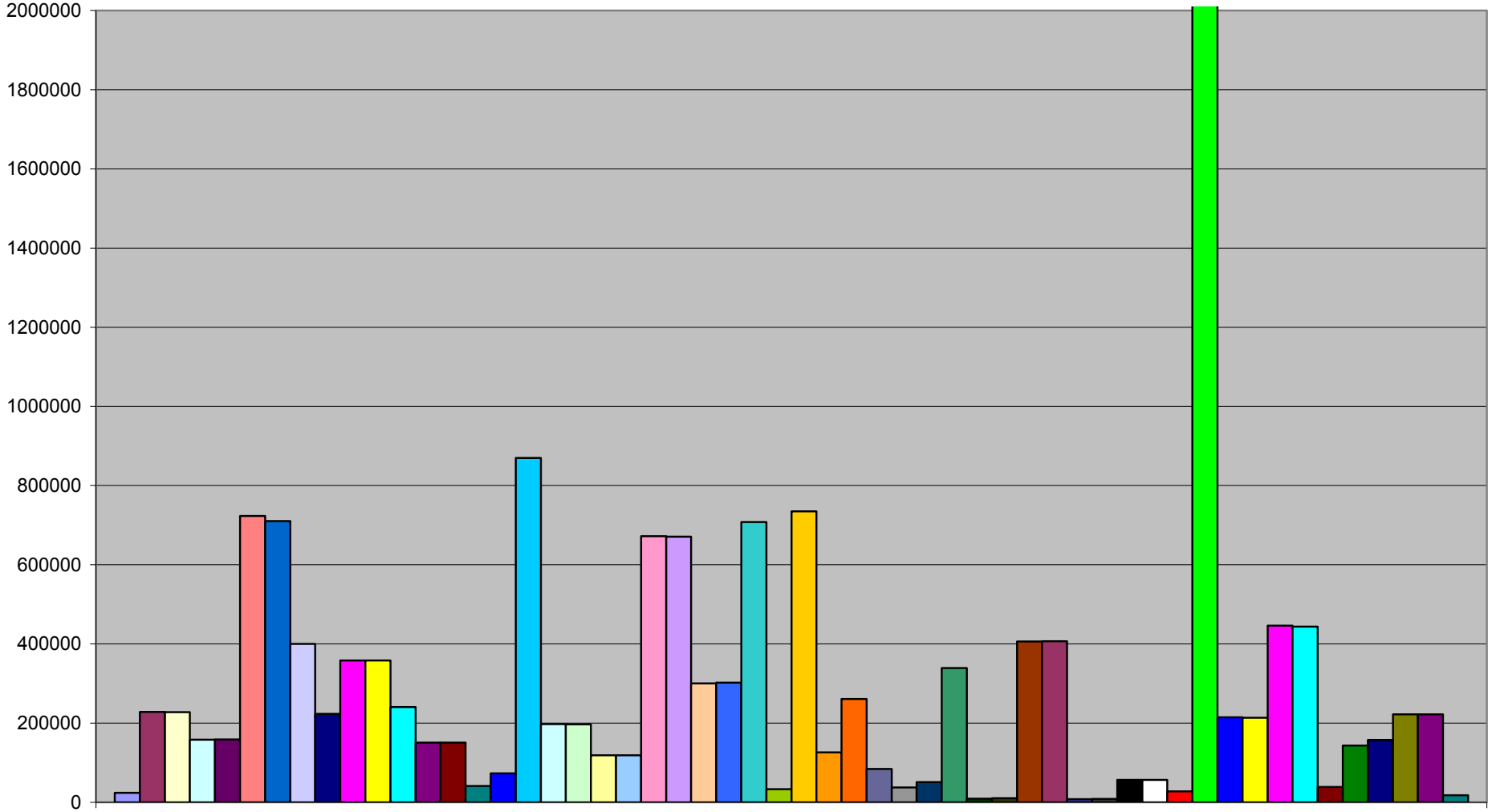
Week 3

Nachi 8/18/03 4:00AM



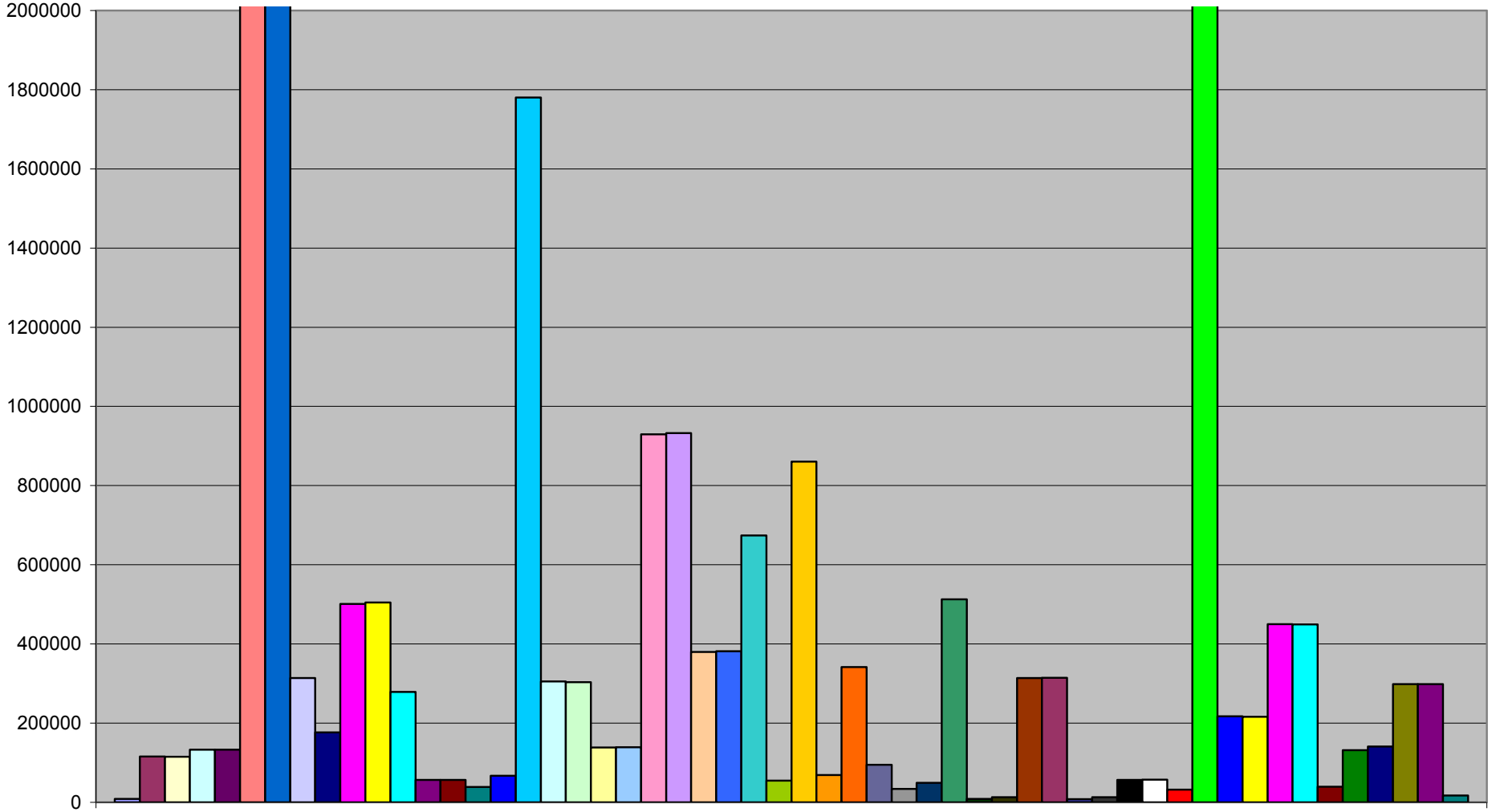
Week 3

Nachi 8/18/03 5:00AM



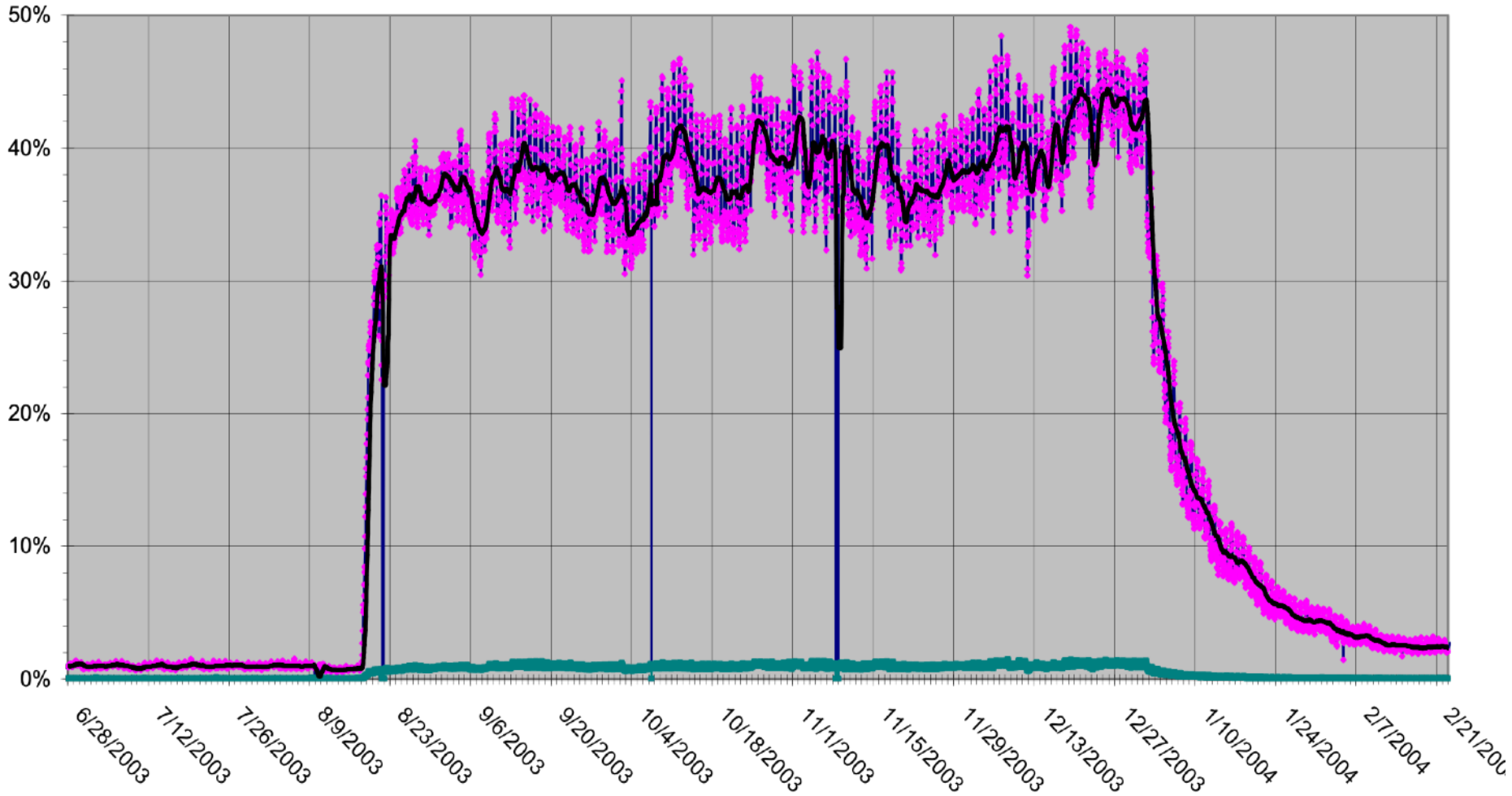
Week 3

Nachi 8/18/03 6:00AM



Week 3

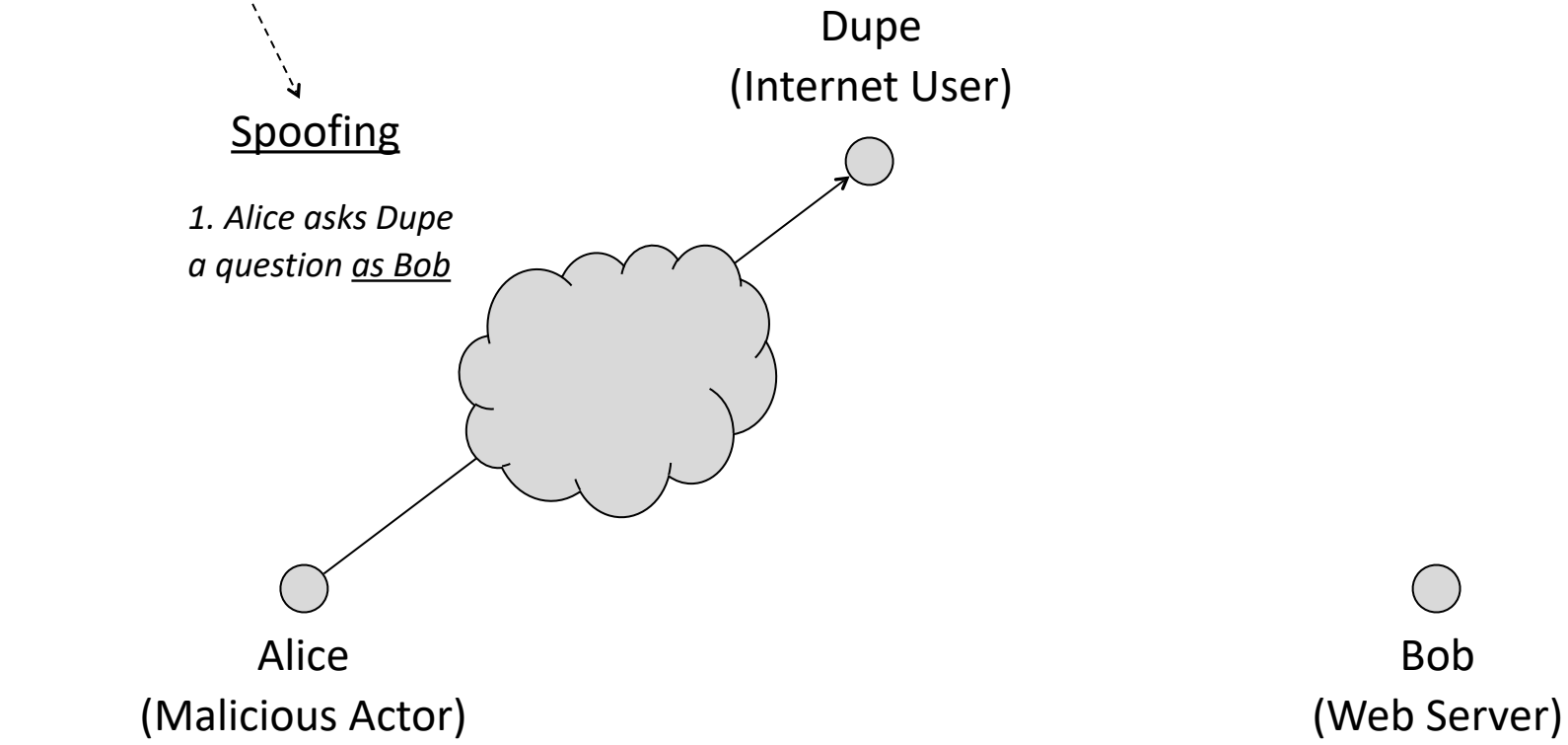
Nachi Worm (08/03 – 01/04)



Week 3

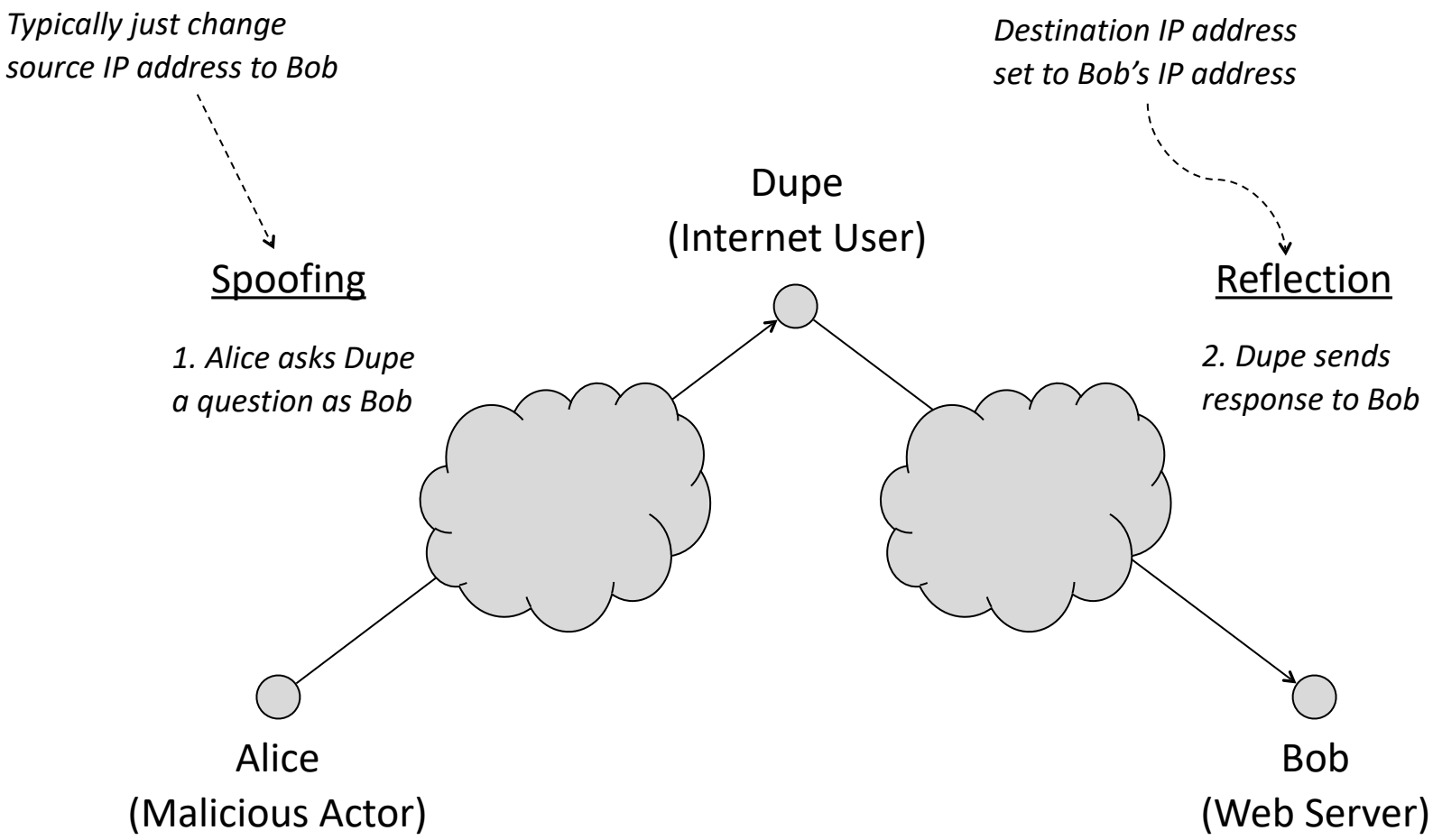
Spoofing and Reflection

Typically just change source IP address to Bob



Week 3

Spoofing and Reflection

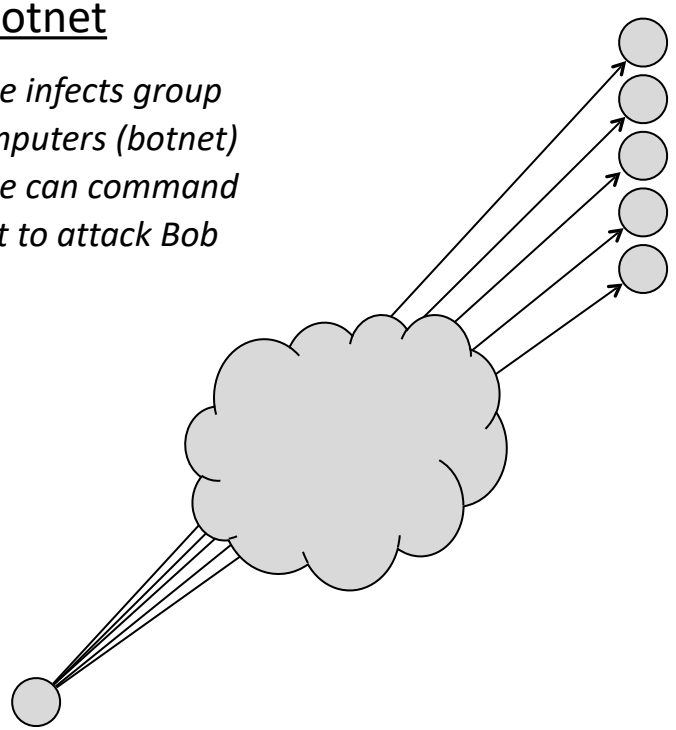


Week 3

Distribution and Amplification

Botnet

1. Alice infects group of computers (botnet)
2. Alice can command botnet to attack Bob



Alice
(Malicious Actor)

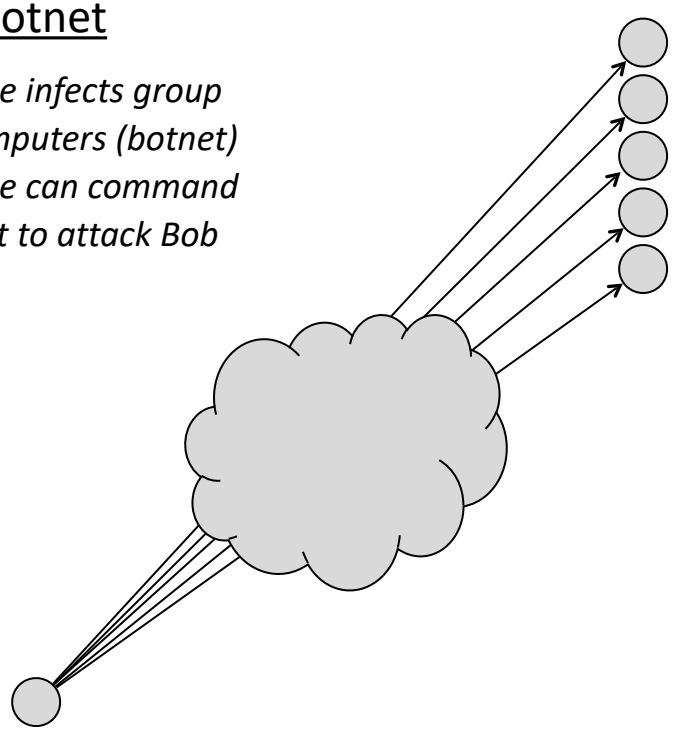
Bob
(Web Server)

Week 3

Distribution and Amplification

Botnet

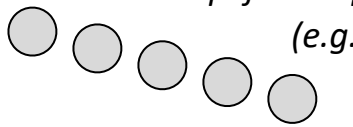
1. Alice infects group of computers (botnet)
2. Alice can command botnet to attack Bob

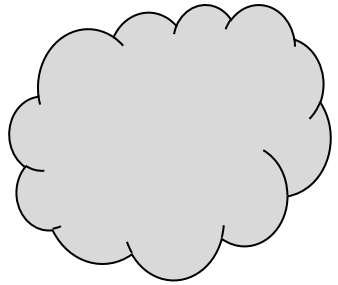


Alice
(Malicious Actor)

Amplifying Service

3. Botnet targets service that amplifies responses (e.g., DNS)

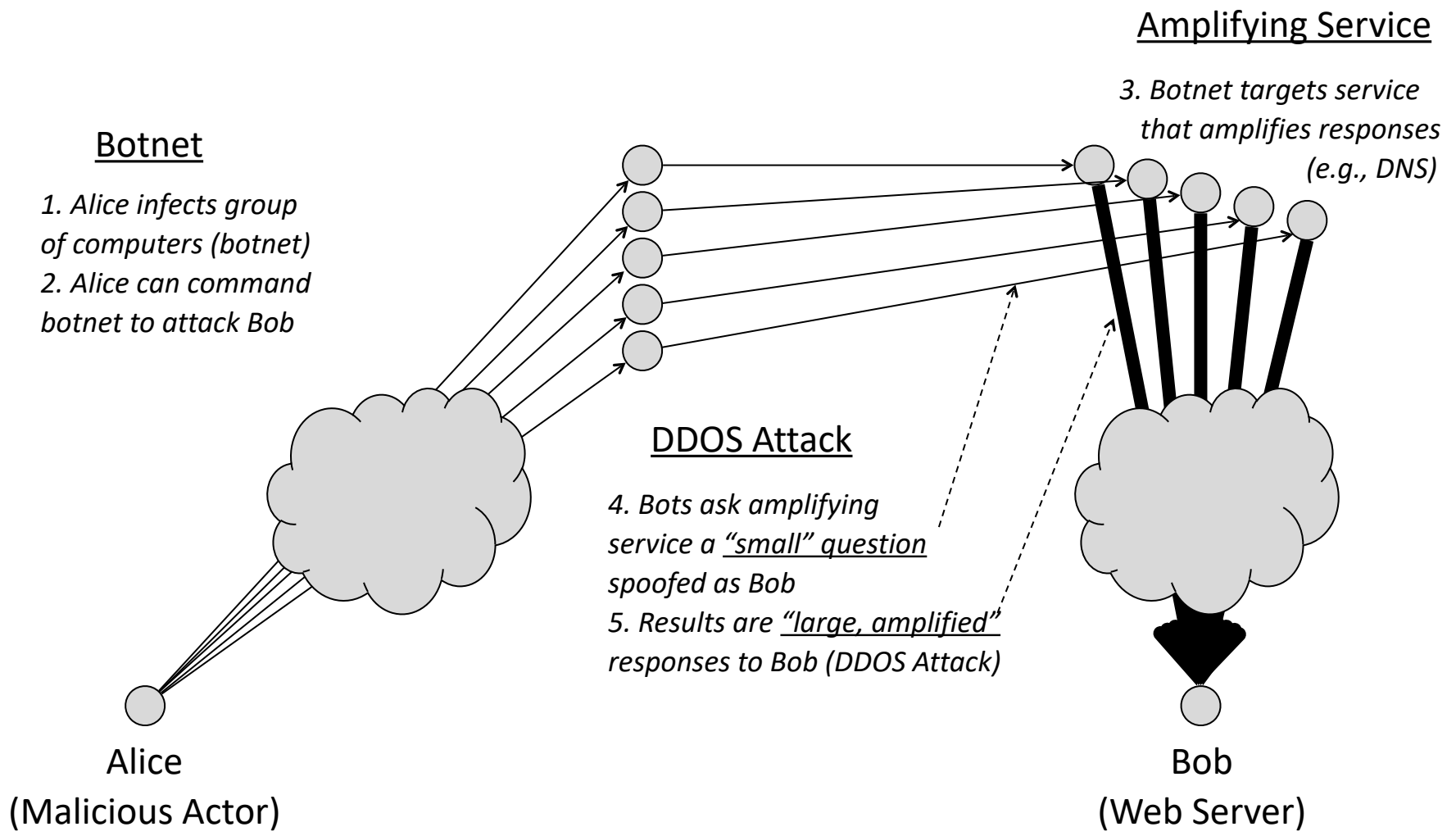




Bob
(Web Server)

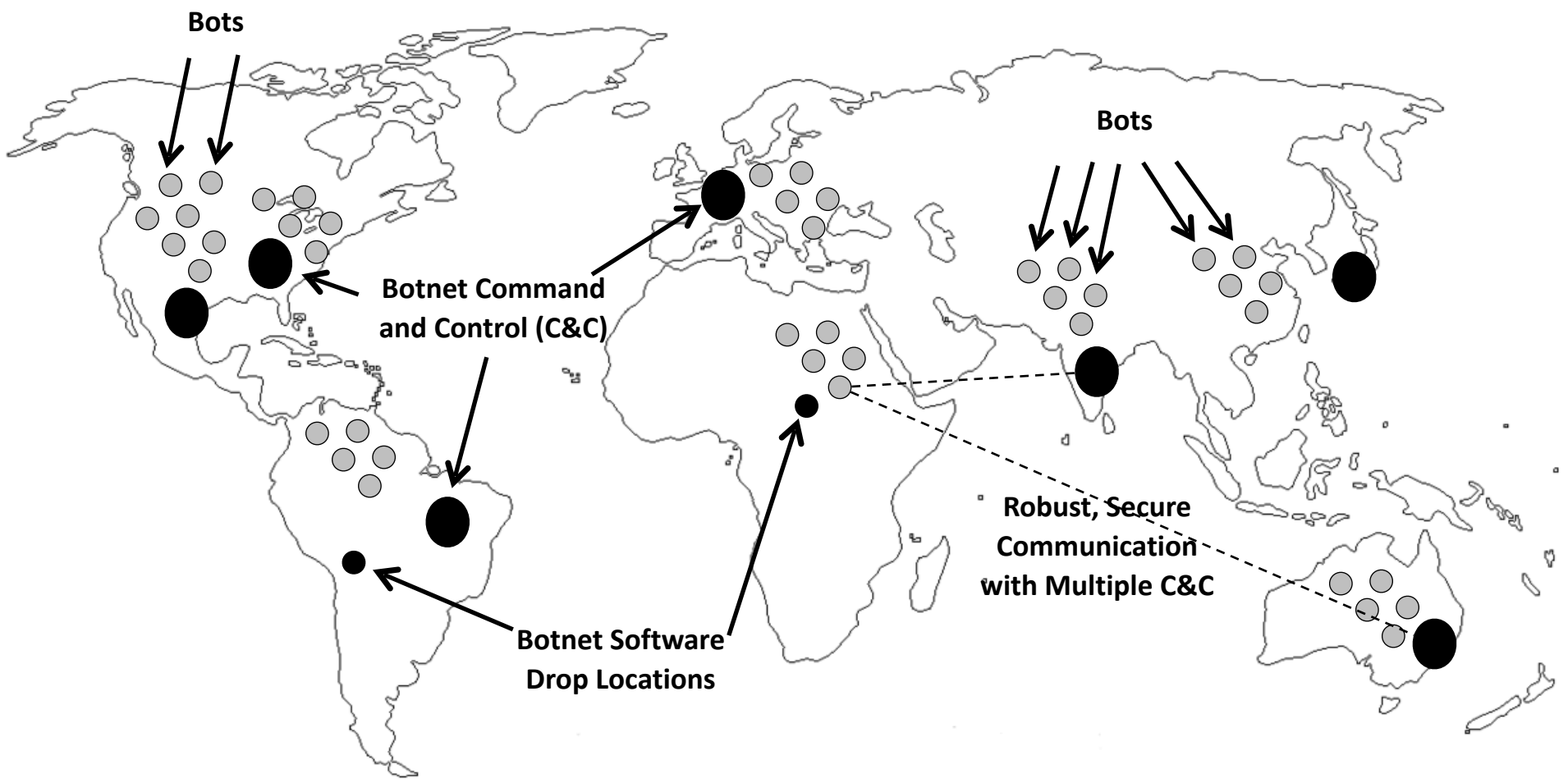
Week 3

Distribution and Amplification



Week 3

Botnets

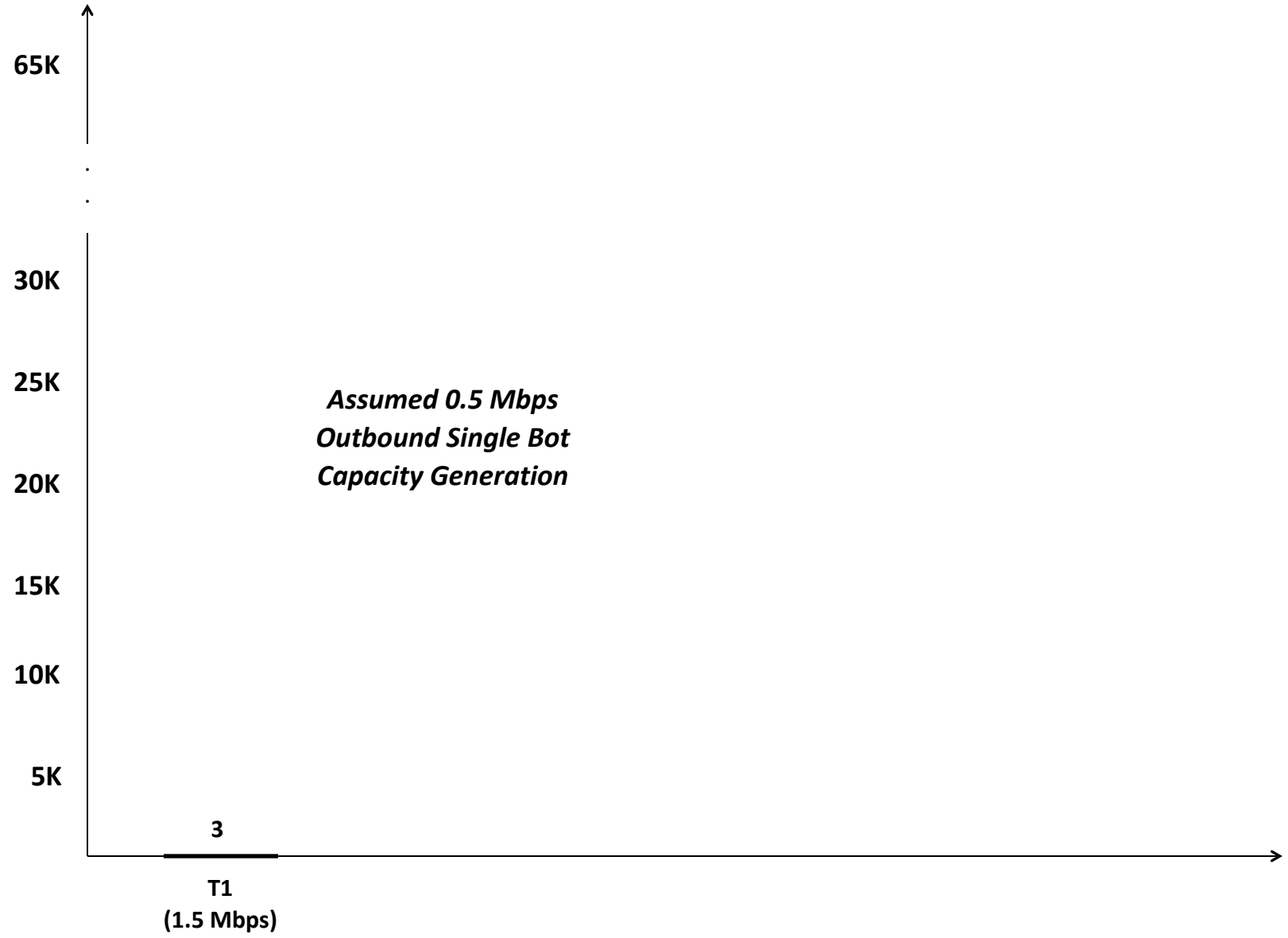


Week 3

Typical Botnet Visualization

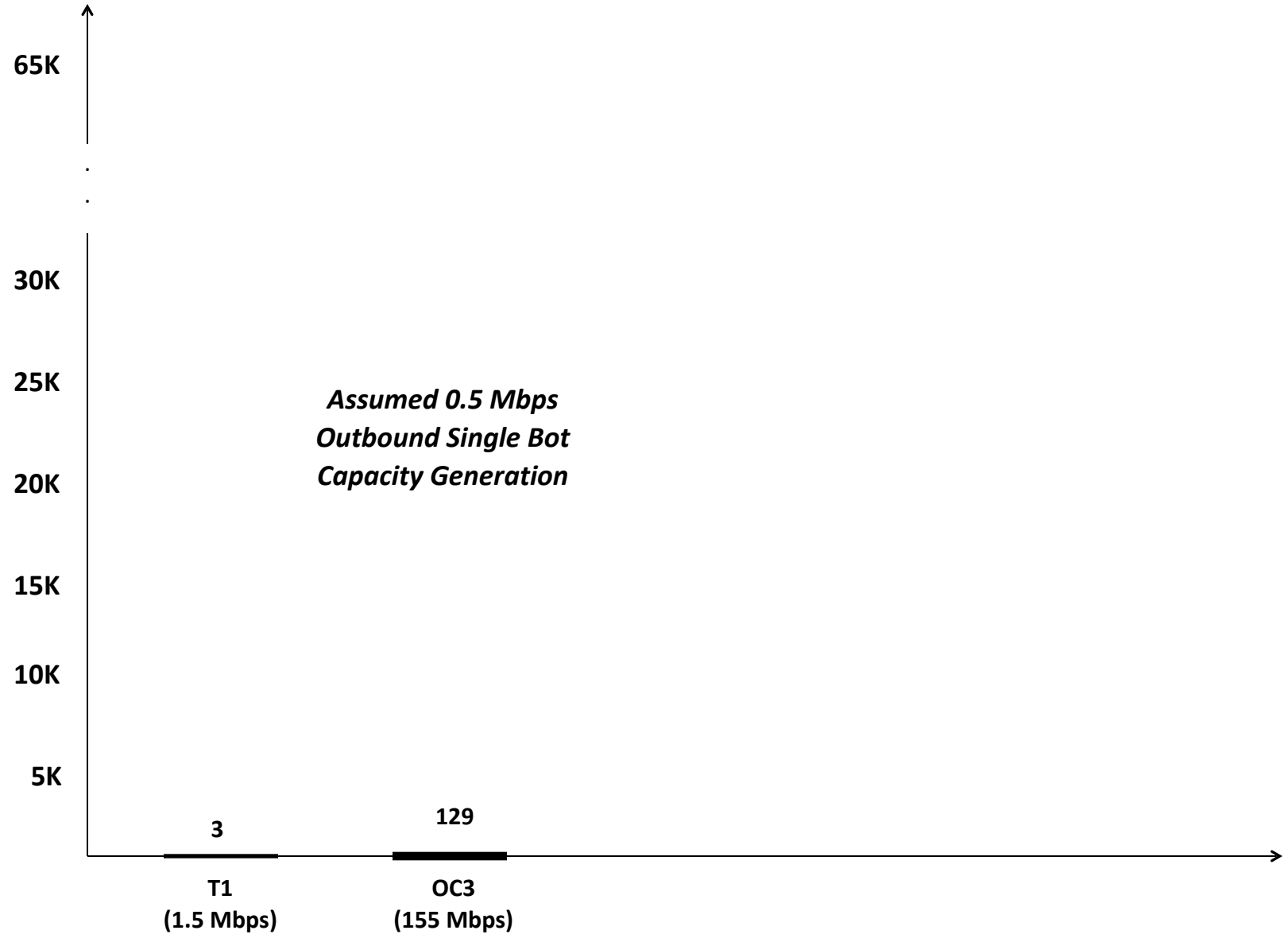
Week 3

Bot Capacity Generation (500Kbps)



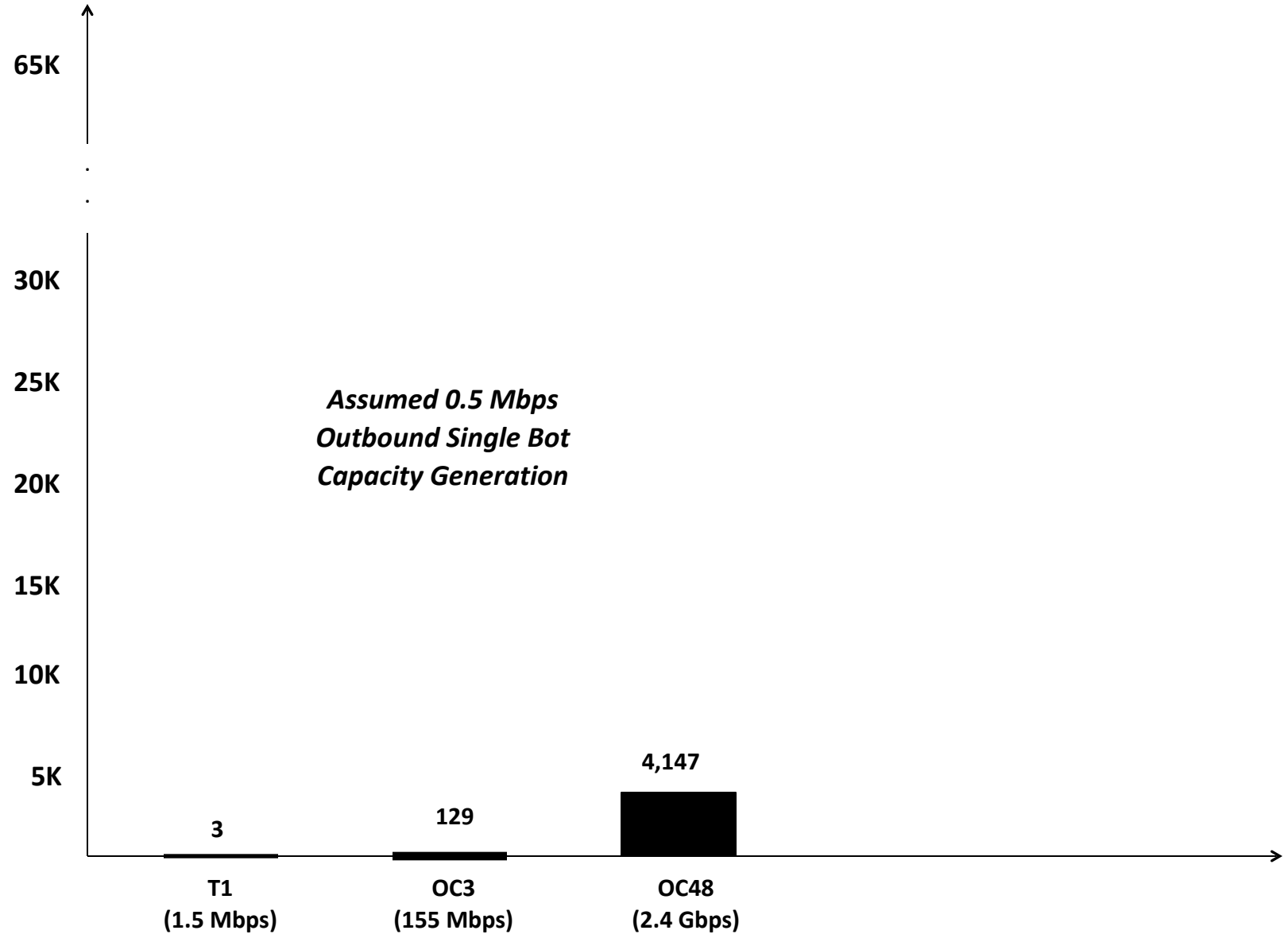
Week 3

Bot Capacity Generation (500Kbps)



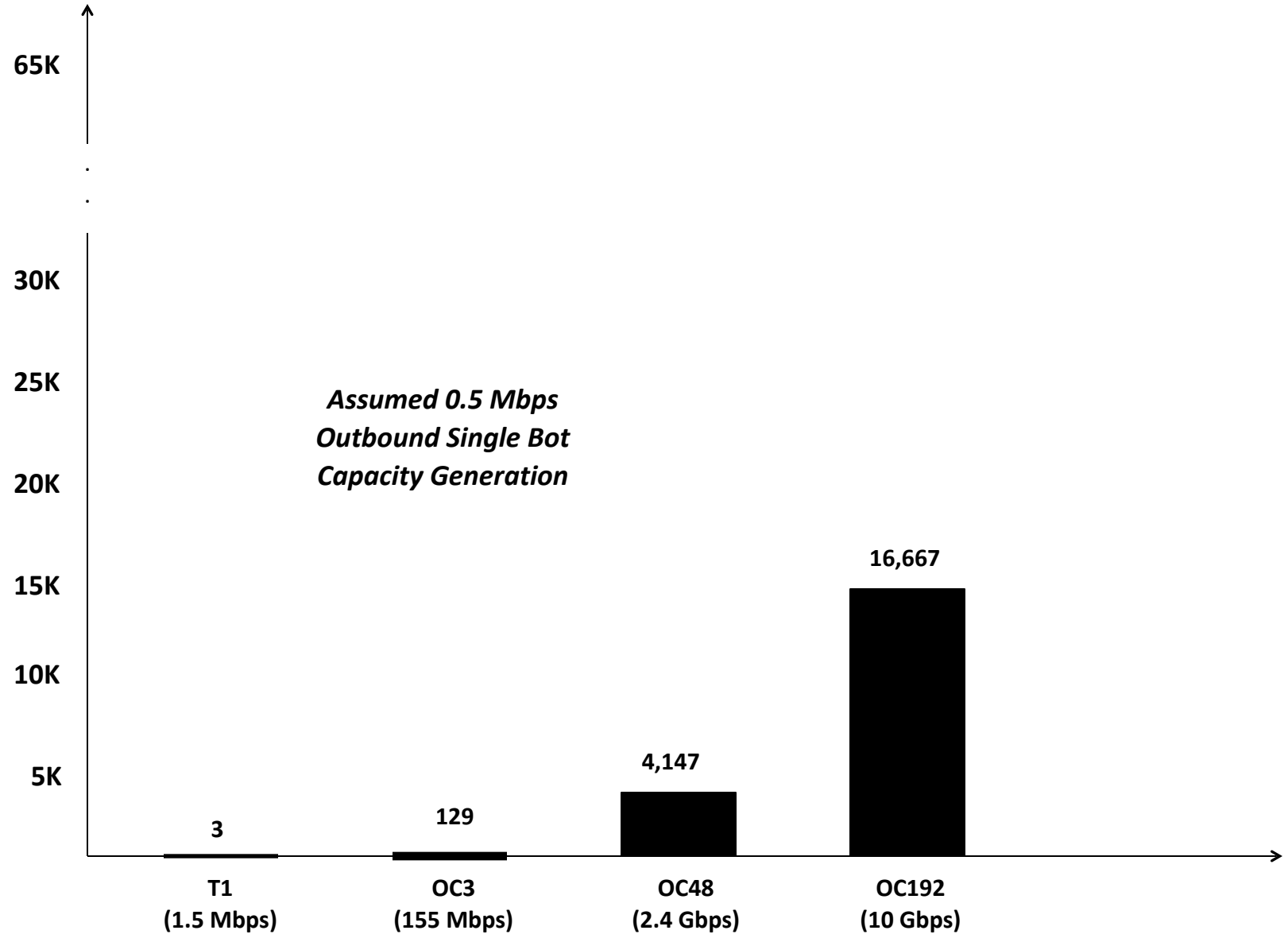
Week 3

Bot Capacity Generation (500Kbps)



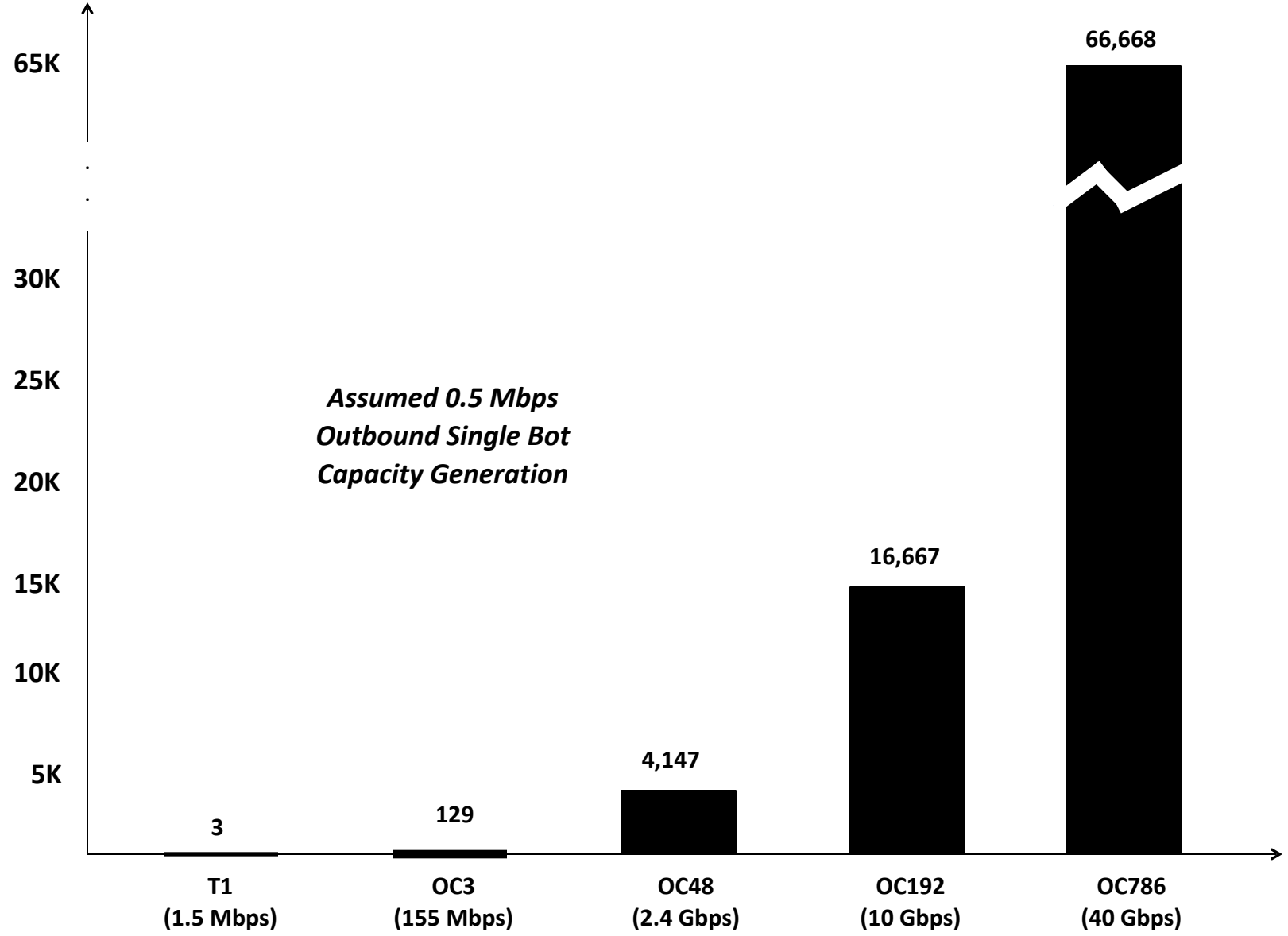
Week 3

Bot Capacity Generation (500Kbps)



Week 3

Bot Capacity Generation (500Kbps)



Week 3

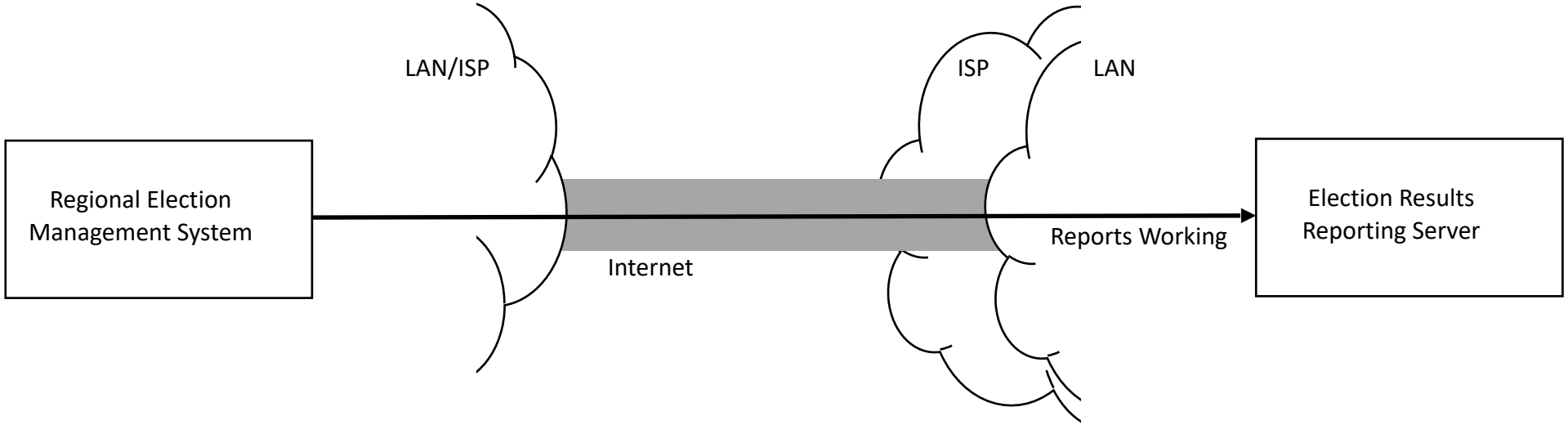
Botnet Capacity Generation (750 Kbps – 1.0 Mbps)

Number of Bots	Outbound Capacity	Size of Attack	Network Size
2	750 Kbps	1.5 Mbps	T1
1,200	1.0 Mbps	1.2 Gbps	OC-24
2,400	1.0 Mbps	2.4 Gbps	OC-48
10,000	1.0 Mbps	10.0 Gbps	OC-192
40,000	1.0 Mbps	40.0 Gbps	OC-768
80,000	1.0 Mbps	80.0 Gbps	
100,000	1.0 Mbps	100 Gbps	*Starts to fill typical ISP backbone*
1,000,000	1.0 Mbps	1000 Gbps	

Week 3

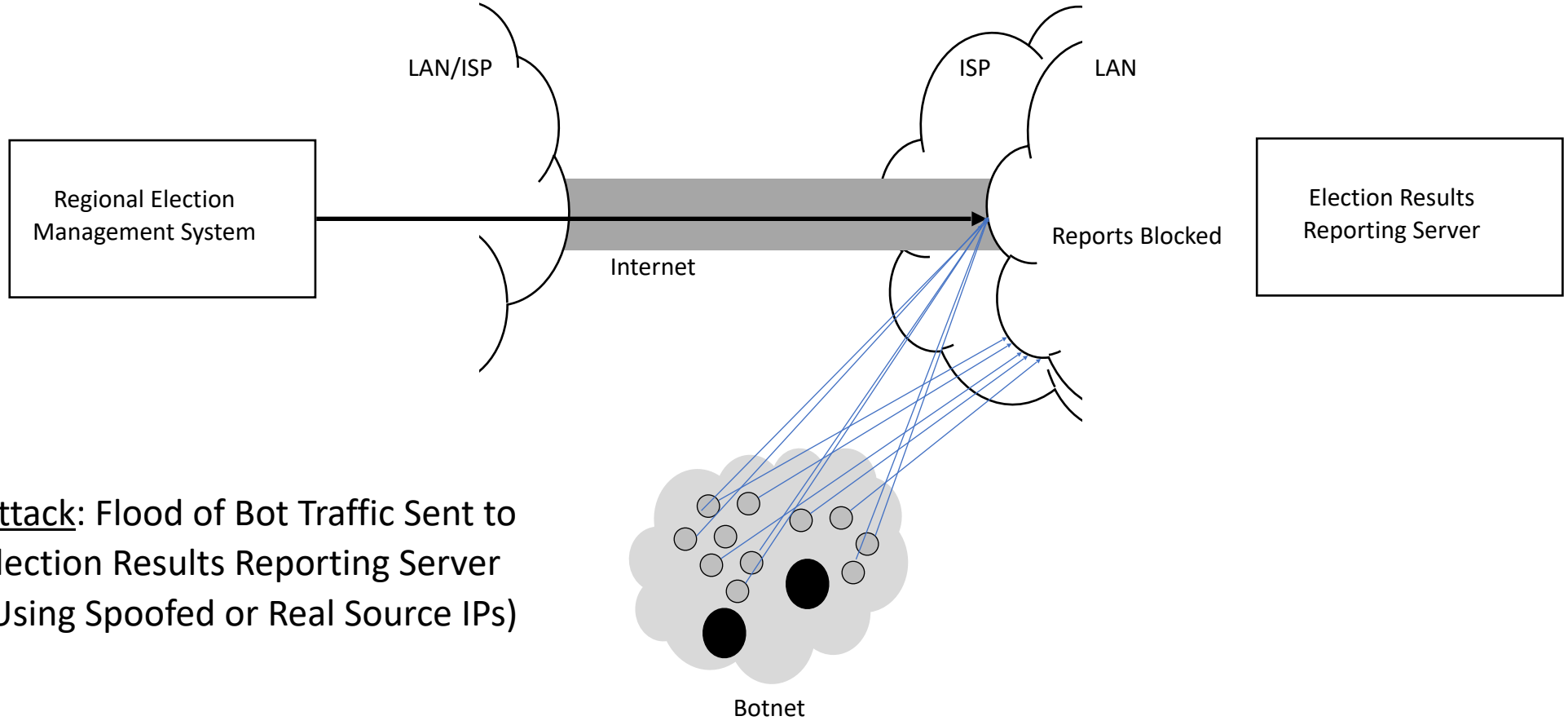
Week 3

Case Study: Mitigating Inbound Election Reporting DDOS



Week 3

Case Study: Mitigating Inbound Election Reporting DDOS

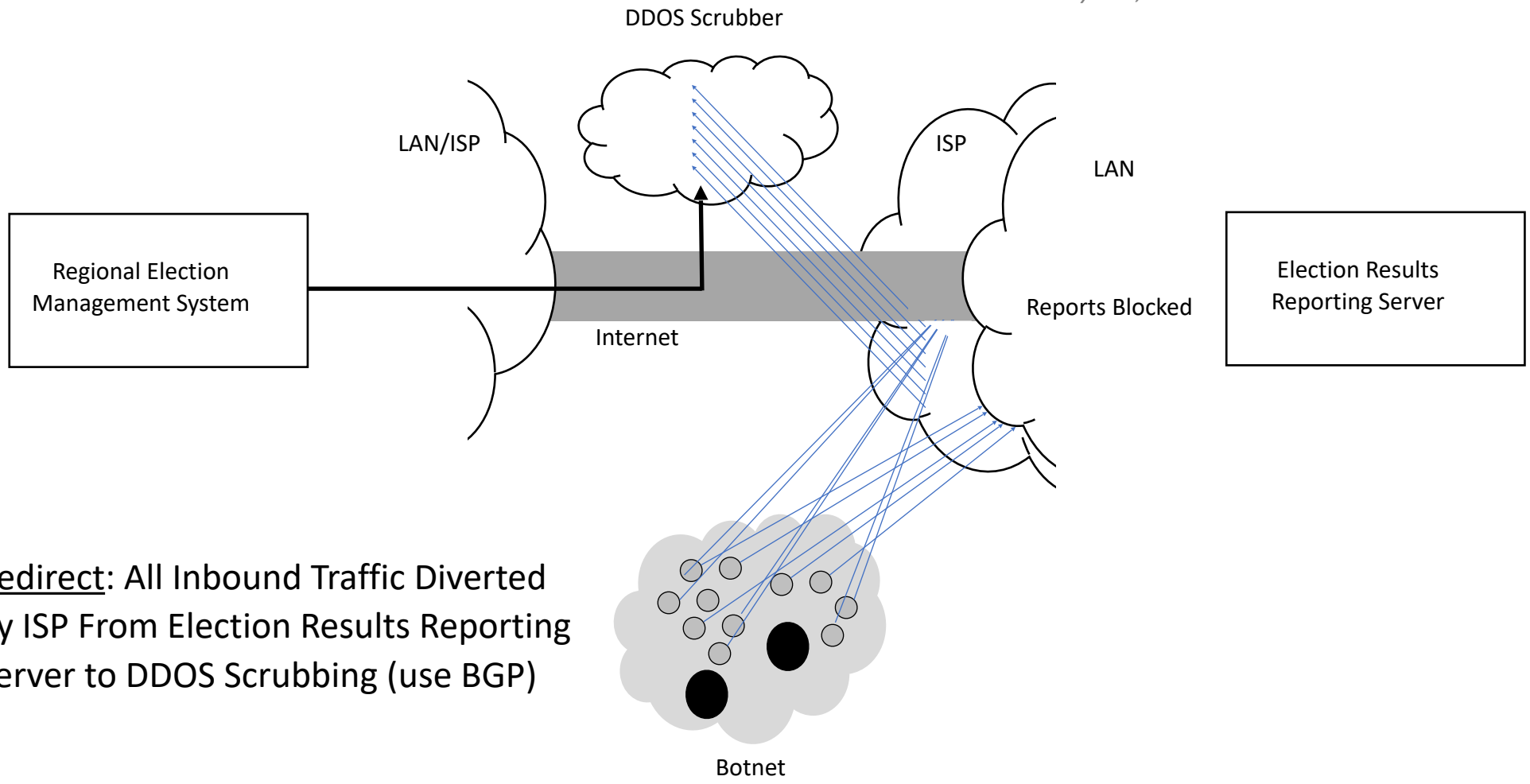


Attack: Flood of Bot Traffic Sent to Election Results Reporting Server (Using Spoofed or Real Source IPs)

Week 3

Case Study: Mitigating Inbound Election Reporting DDOS

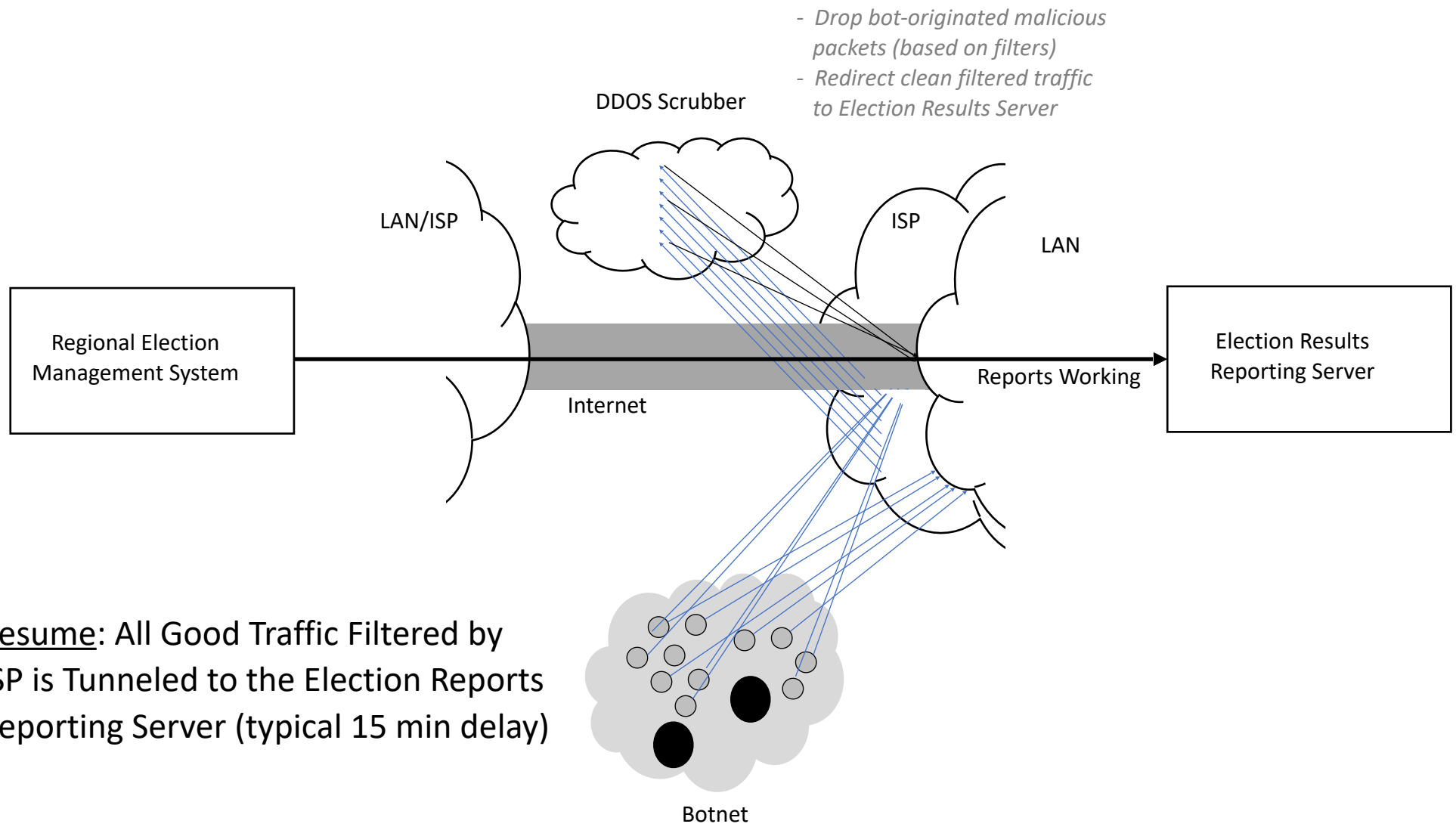
- Filter on Common Source IP
- Filter on Common Packet Size
- Filter on Common Payload, etc.



Redirect: All Inbound Traffic Diverted by ISP From Election Results Reporting Server to DDOS Scrubbing (use BGP)

Week 3

Case Study: Mitigating Inbound Election Reporting DDOS



Resume: All Good Traffic Filtered by ISP is Tunneled to the Election Reports Reporting Server (typical 15 min delay)