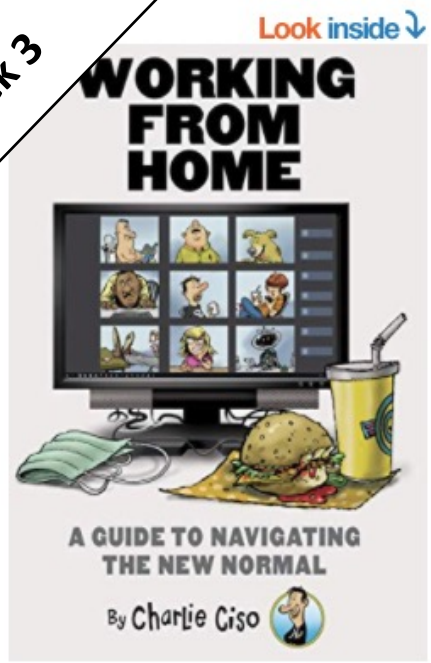
Week 3

An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 3



Working from Home: A Guide to Navigating the New Normal

Kindle Edition

by Edward Amoroso (Author), Rich Powell (Author) | Format: Kindle Edition

★★★★★ 16 ratings

› See all formats and editions

Kindle
$4.99

Read with Our Free App

If you are in need of some Pandemic entertainment and world-class comic relief, then "Working from Home: A Guide to Navigating the New Normal" is for you! This step-by-step guide, written by a fictitious social media sensation (and sometimes cybersecurity expert) named Charlie Ciso, will teach you to:

•Build a fake Zoom backdrop that will get you promoted to senior VP in ten days or less

‹ Read more

Kindle Price: $4.99

Read Now

You already own this item. Read anytime on your Kindle apps and devices.

Buy for others

Give as a gift or purchase for a team or group. Learn more

Quantity: 1 Buy for others

Add to List

Enter a promotion code or Gift Card

Share <Embed>

READ ON ANY DEVICE

›Get free Kindle app

Follow the Author

Edward G. Amoroso

+ Fol

Week 3

Required Text – $9.99 Download from Amazon.com

$25.00 Printed Paperback Book from Amazon.com

From CIA to APT: An Introduction to Cyber Security

Edward G. Amoroso & Matthew E. Amoroso

Week 3

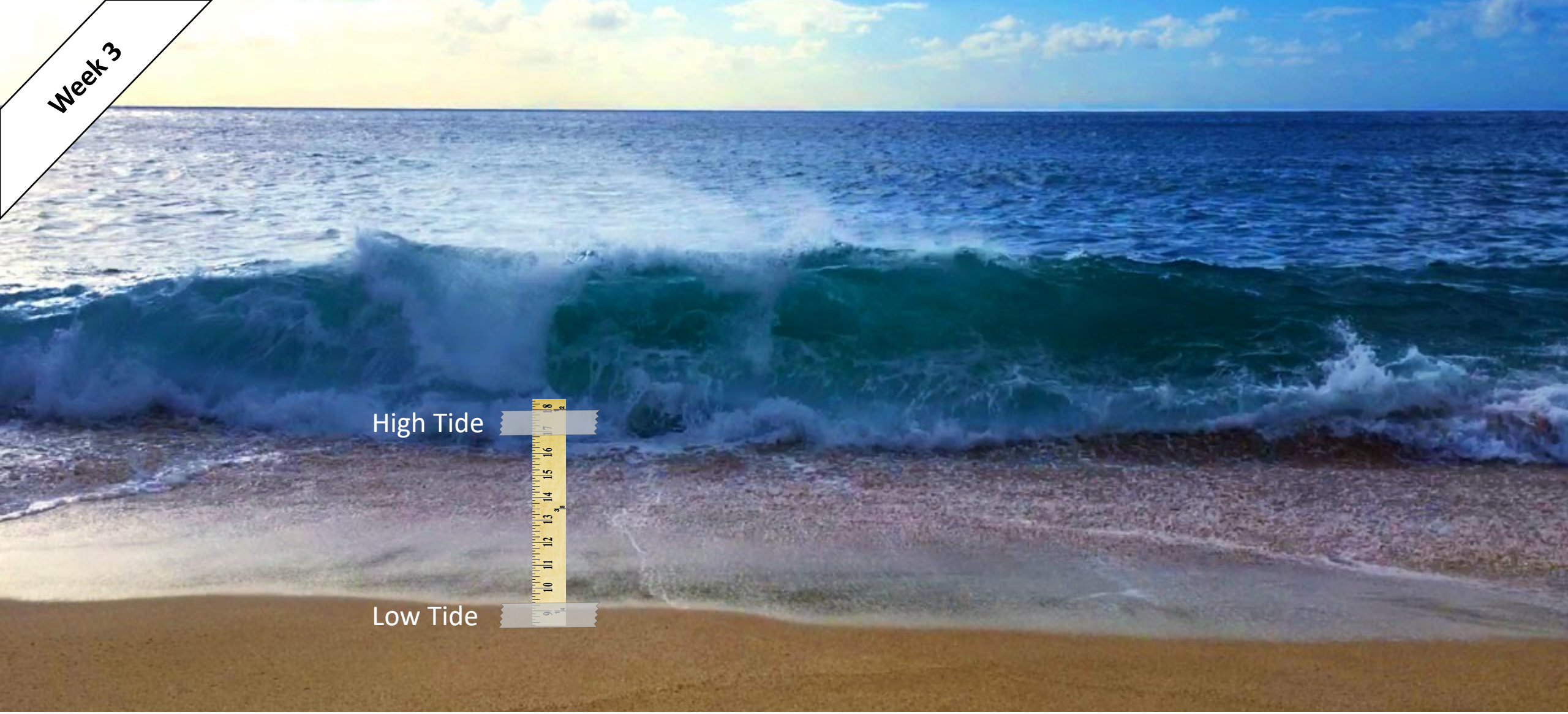
<u>Required Additional Reading</u>: https://www.tag-cyber.com/advisory/quarterly

Week 3

Required Week Three Readings:

1. "The Birth and Death of the Orange Book," Steve Lipner
https://www.stevelipner.org/links/resources/The%20Birth%20and%20Death%20of%20the%20Orange%20Book.pdf

2. **Chapters 8 through 11: *From CIA to APT: An Introduction to Cyber Security*, E. Amoroso & M. Amoroso**



Week 3: Network Security Threats

What Are Some Classic Cyber Attack Approaches?

Week 3

2600

GET THE .PDF

The Hacker Quarterly
NOW ON STANDS!
Current issue: SUMMER 2021
Digital Editions

Magazine | Radio | ...res | Events | 2600 Store

Search 2600

MM.DD.YY	UTC		DISPATCH
09.20.21	0628	!	LOST AUDIO POSTED FO
09.16.21	0127		NEW 'OFF THE HOOK' ON
09.15.21	0111		NEW 'OFF THE WALL' ON
09.07.21	1818	!	SUMMER ISSUE OF 2600
07.13.21	1821	!	LOST AUDIO PROJECT S
06.11.21	1527	!	SPRING ISSUE OF 2600 RELEASED
06.03.21	1857	!	SOME 2600 MEETINGS TO RESUME IN JULY
06.03.21	1745	!	EXTRA HOPE NOT HAPPENING THIS YEAR

Original Hacking Journal

Week 3

Stage 1: IFS Variable

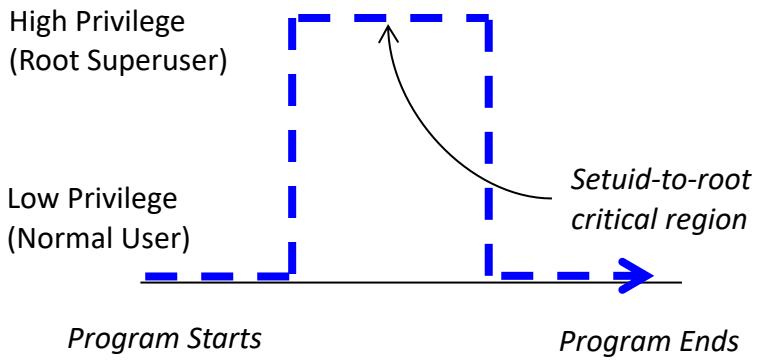
- Set IFS variable to include ‘/’
- “/etc/file” same as “etc file”

Classic Unix Kernel Attack

Week 3

Stage 1: IFS Variable
- Set IFS variable to include '/'
- "/etc/file" same as "etc file"

Stage 2: Find setuid-to-root program
- Allows increase in privilege
- Normal user to Unix "Root"

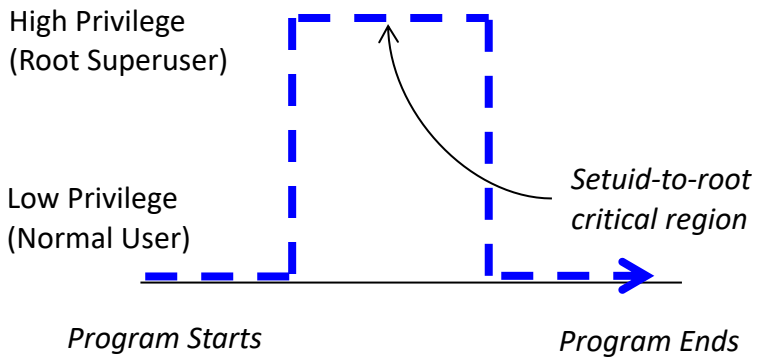


Classic Unix Kernel Attack

Week 3

Stage 1: IFS Variable
- Set IFS variable to include '/'
- "/etc/file" same as "etc file"

Stage 2: Find setuid-to-root program
- Allows increase in privilege
- Normal user to Unix "Root"



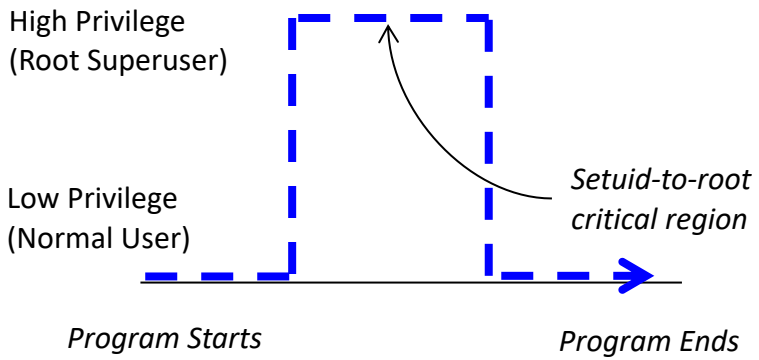
Stage 3: Notice Source Code in "At" Program
- Program has setuid-to-root critical region
- Region includes "exec /etc/protect/file"

Classic Unix Kernel Attack

Week 3

Stage 1: IFS Variable
- Set IFS variable to include '/'
- "/etc/file" same as "etc file"

Stage 2: Find setuid-to-root program
- Allows increase in privilege
- Normal user to Unix "Root"



Stage 3: Notice Source Code in "At" Program
- Program has setuid-to-root critical region
- Region includes "exec /etc/protect/file"

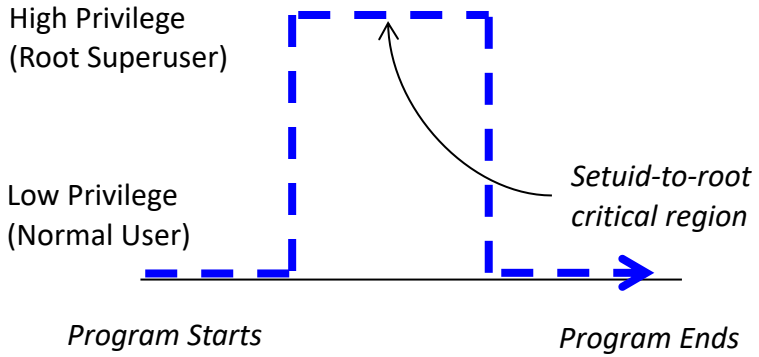
Stage 4: Unix Shell Program
- Allows copying ("cp /bin/sh myshell")
- Copied program inherits privileges

Classic Unix Kernel Attack

Week 3

Stage 1: IFS Variable
- Set IFS variable to include '/'
- "/etc/file" same as "etc file"

Stage 2: Find setuid-to-root program
- Allows increase in privilege
- Normal user to Unix "Root"



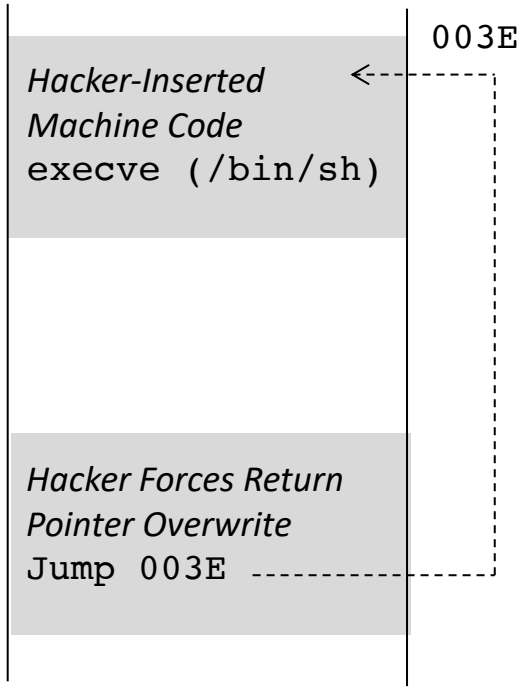
Stage 3: Notice Source Code in "At" Program
- Program has setuid-to-root critical region
- Region includes "exec /etc/protect/file"

Stage 4: Unix Shell Program
- Allows copying ("cp sh myshell")
- Copied program inherits privileges

Unix Kernel Attack:
- Step 1: Set IFS to include '/'
- Step 2: Write shell program called etc and place in local directory. The etc file should to copy /bin/sh to myshell
- Step 3: Run "at" program
- Result: myshell is root shell owed by me!

Classic Unix Kernel Attack

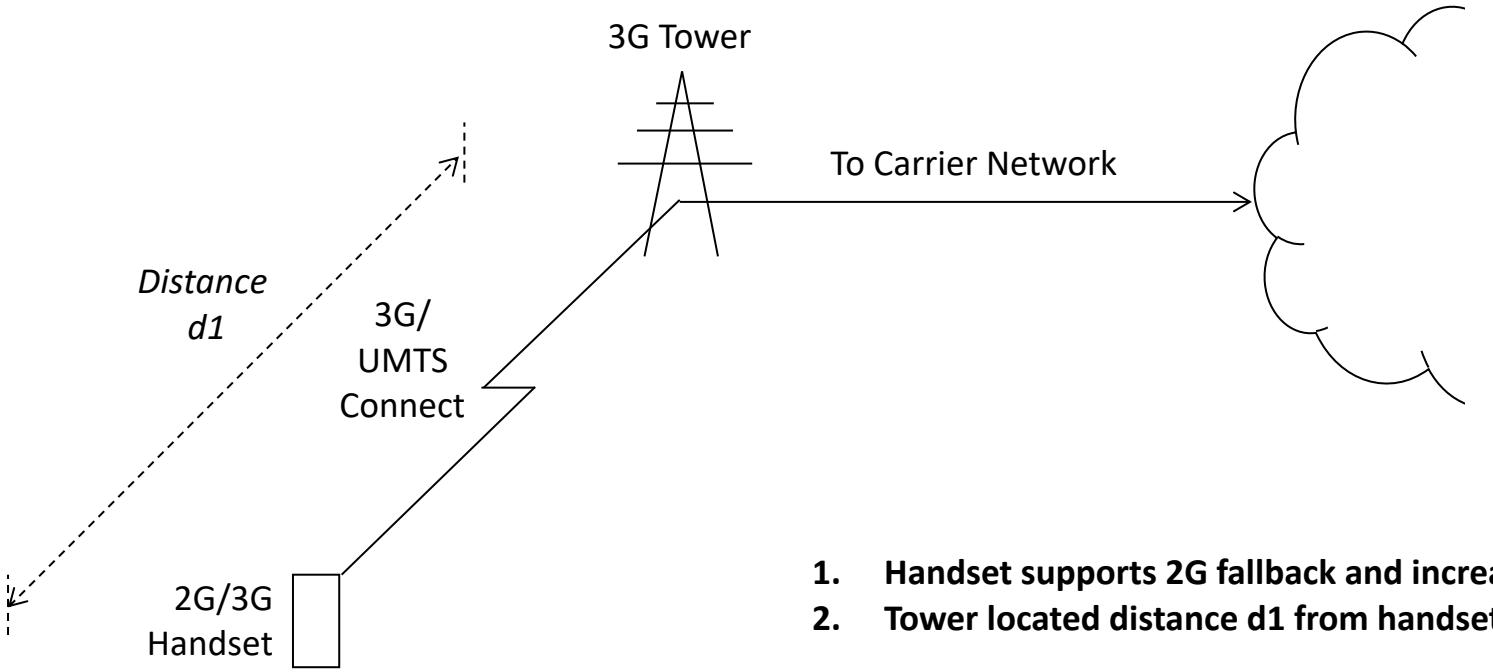
Week 3




```
void overflow_function(char *string)
    {
            char buffer[16];
            strcpy(buffer, string);
            return;
    }

void main()
    {
            char buffer[256];
            int i;

            for(i=0; i<255; i++)
                  large_buffer[i]='A';

                  overflow_function(large_buffer);
    }
```

Classic Buffer Overflow Attack Code

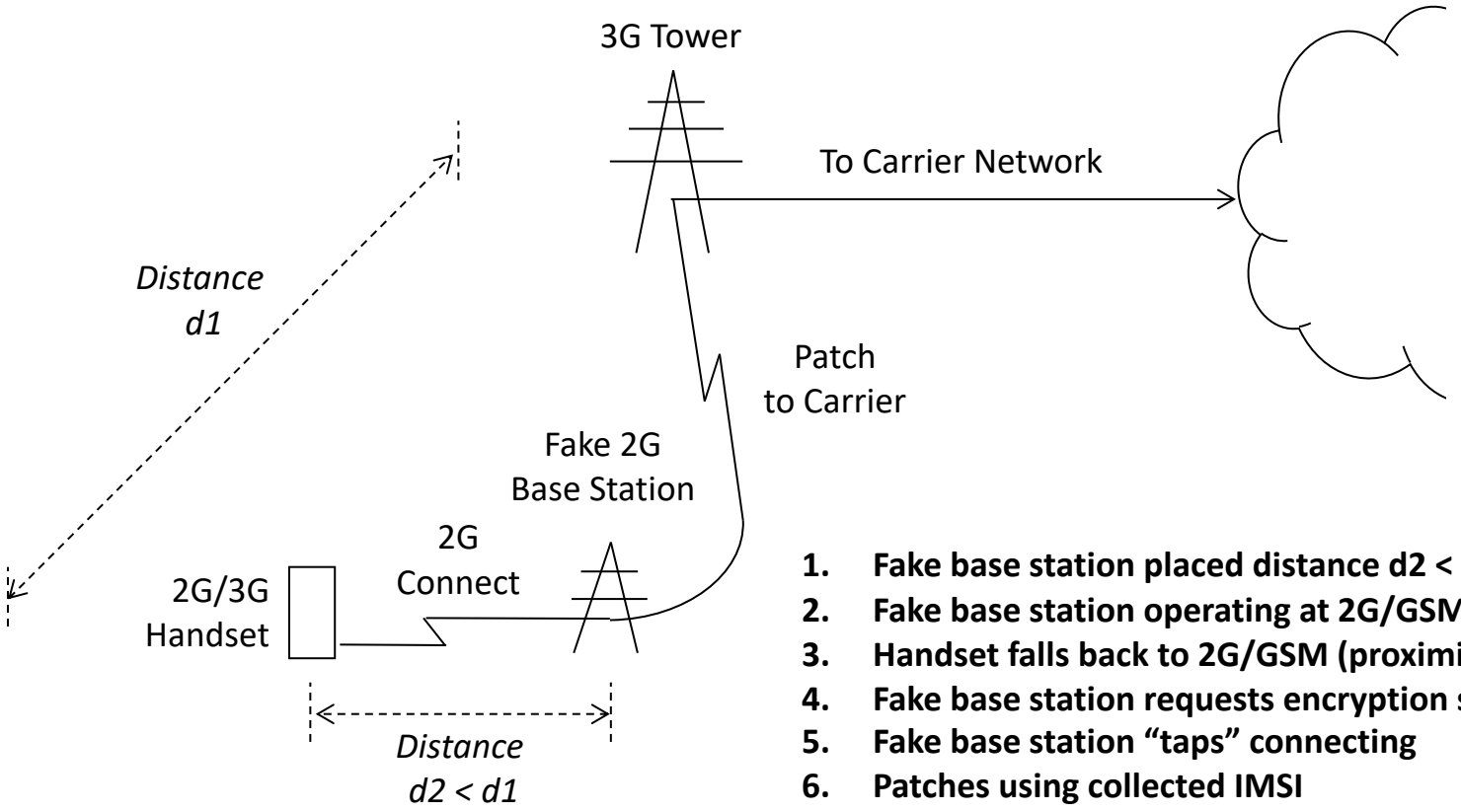
Week 3



1. **Handset supports 2G fallback and increased coverage**
2. **Tower located distance d1 from handset**

Classic 3G Mobile Intercept Attack (Fake Base Station)

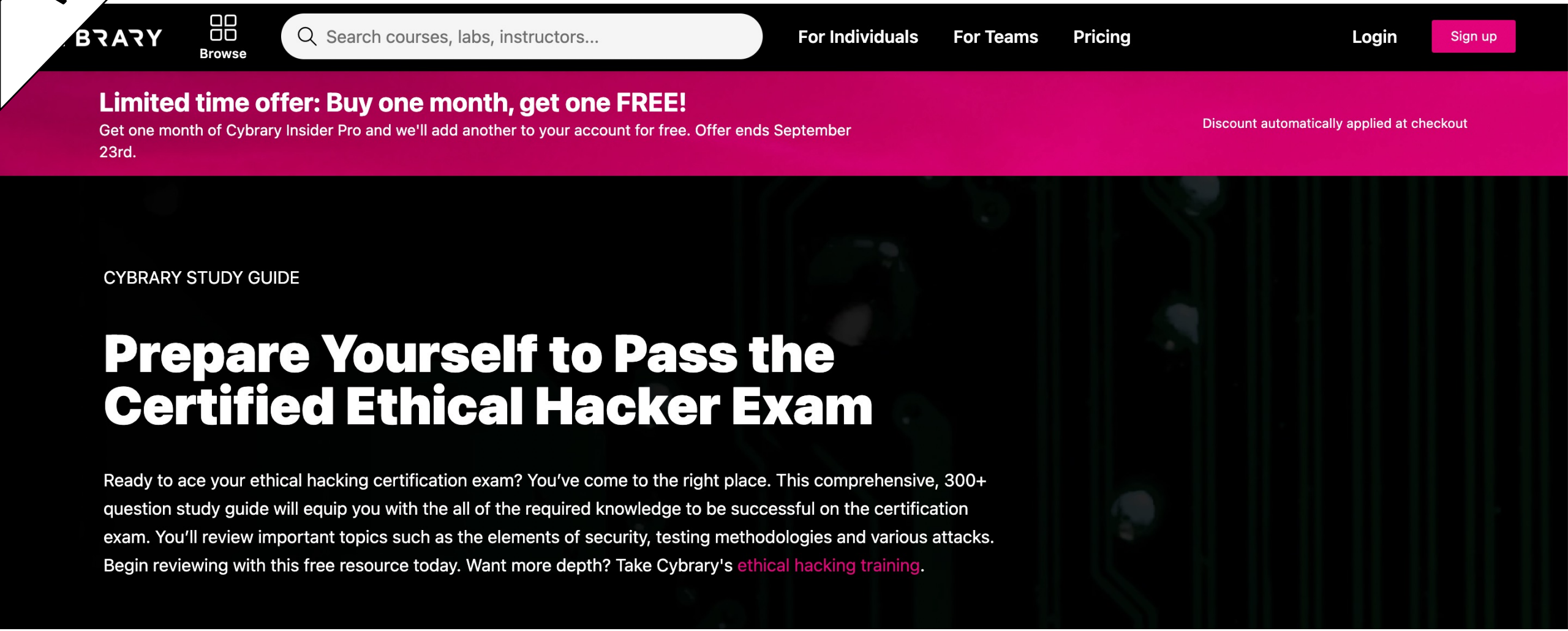
Week 3



1. **Fake base station placed distance d2 < d1 from handset**
2. **Fake base station operating at 2G/GSM**
3. **Handset falls back to 2G/GSM (proximity rule)**
4. **Fake base station requests encryption suppression**
5. **Fake base station "taps" connecting**
6. **Patches using collected IMSI**

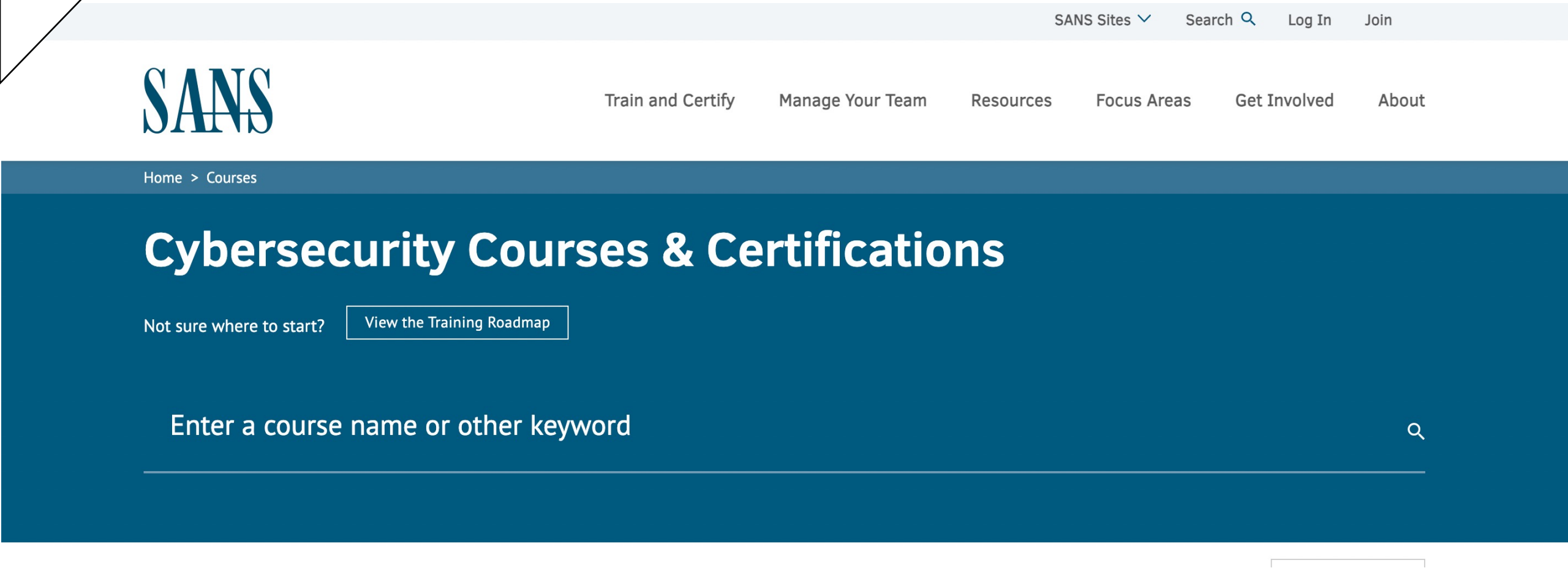
Classic 3G Mobile Intercept Attack (Fake Base Station)

Week 3



Cybrary Ethical Hacker Program

Week 3



SANS Ethical Hacker Program

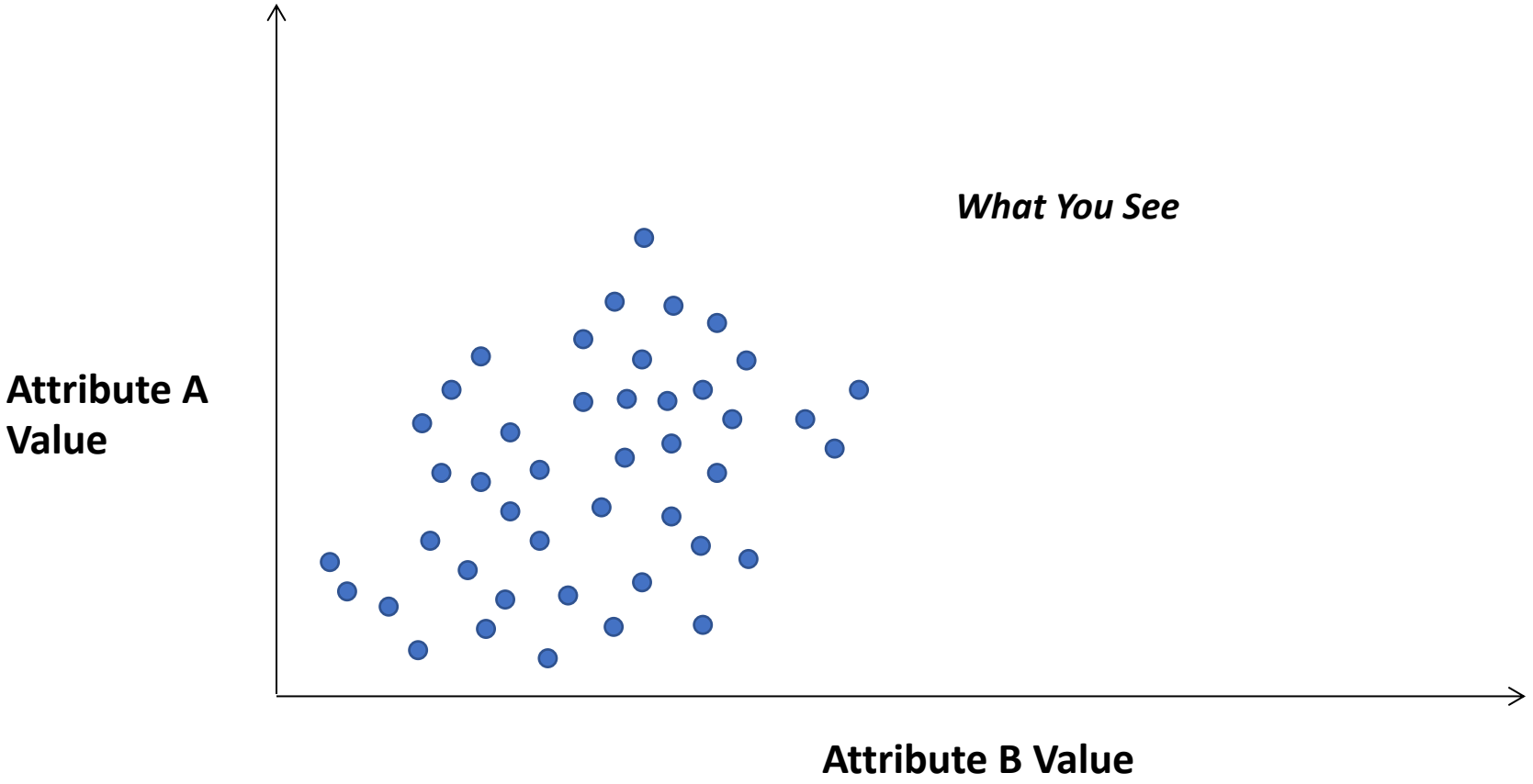
Week 3

InfoSec Institute Ethical Hacker Program

How Can Machine Learning be Used for Network Security?

Week 3

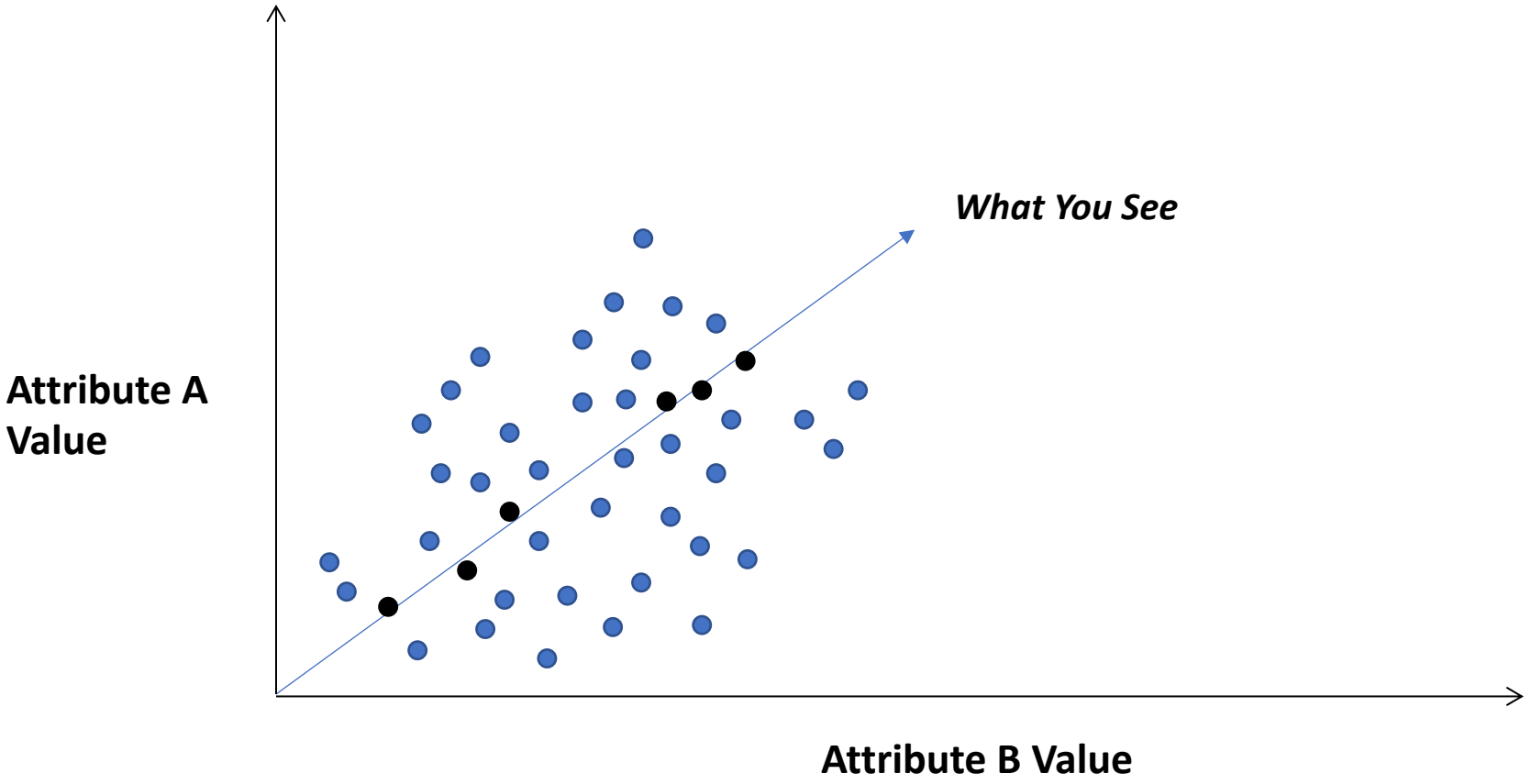
Supervised Machine Learning



Week 3

Supervised Machine Learning

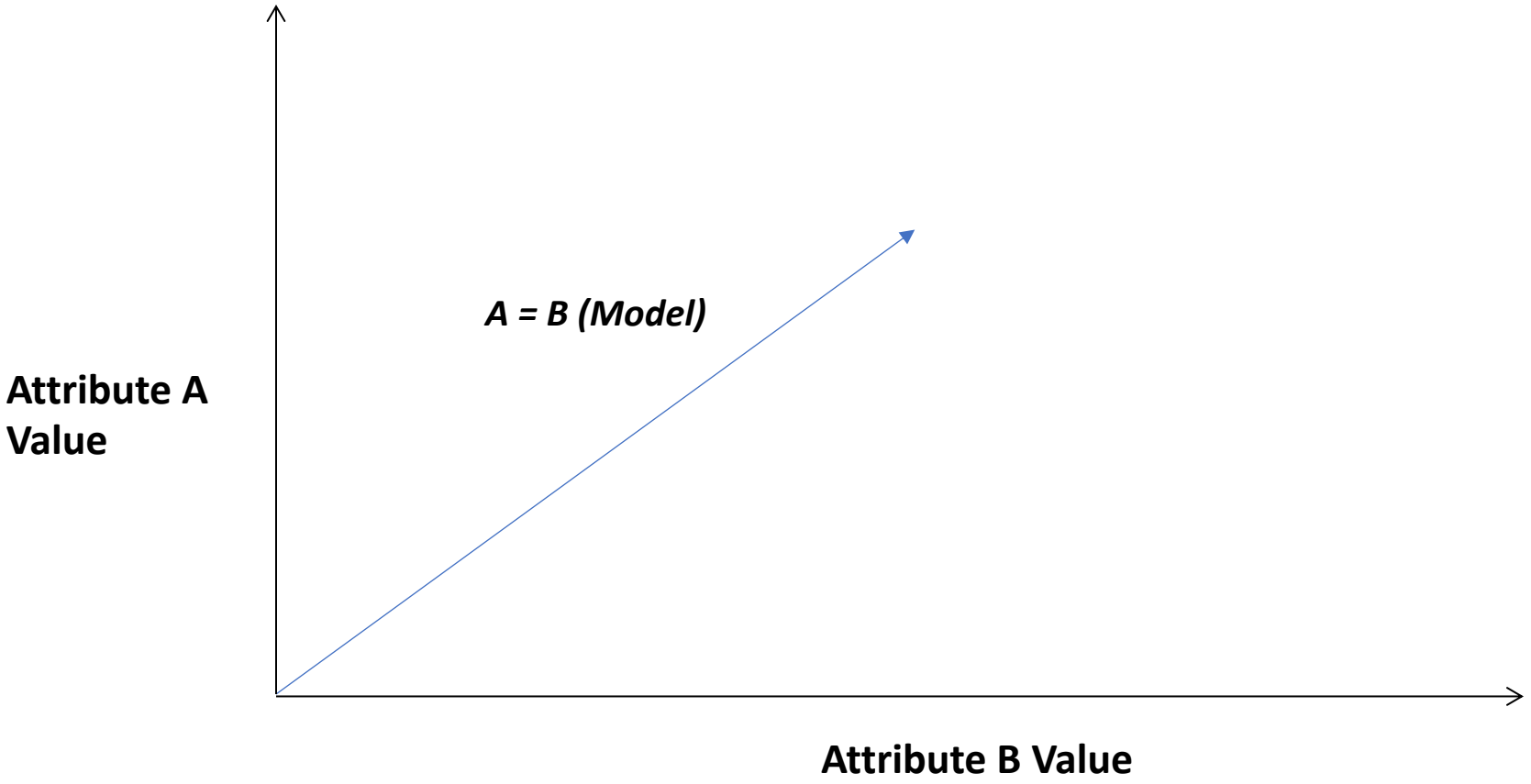
Initial Training:
Attribute A Value = Attribute B Value Implies Some Desired Condition



Week 3

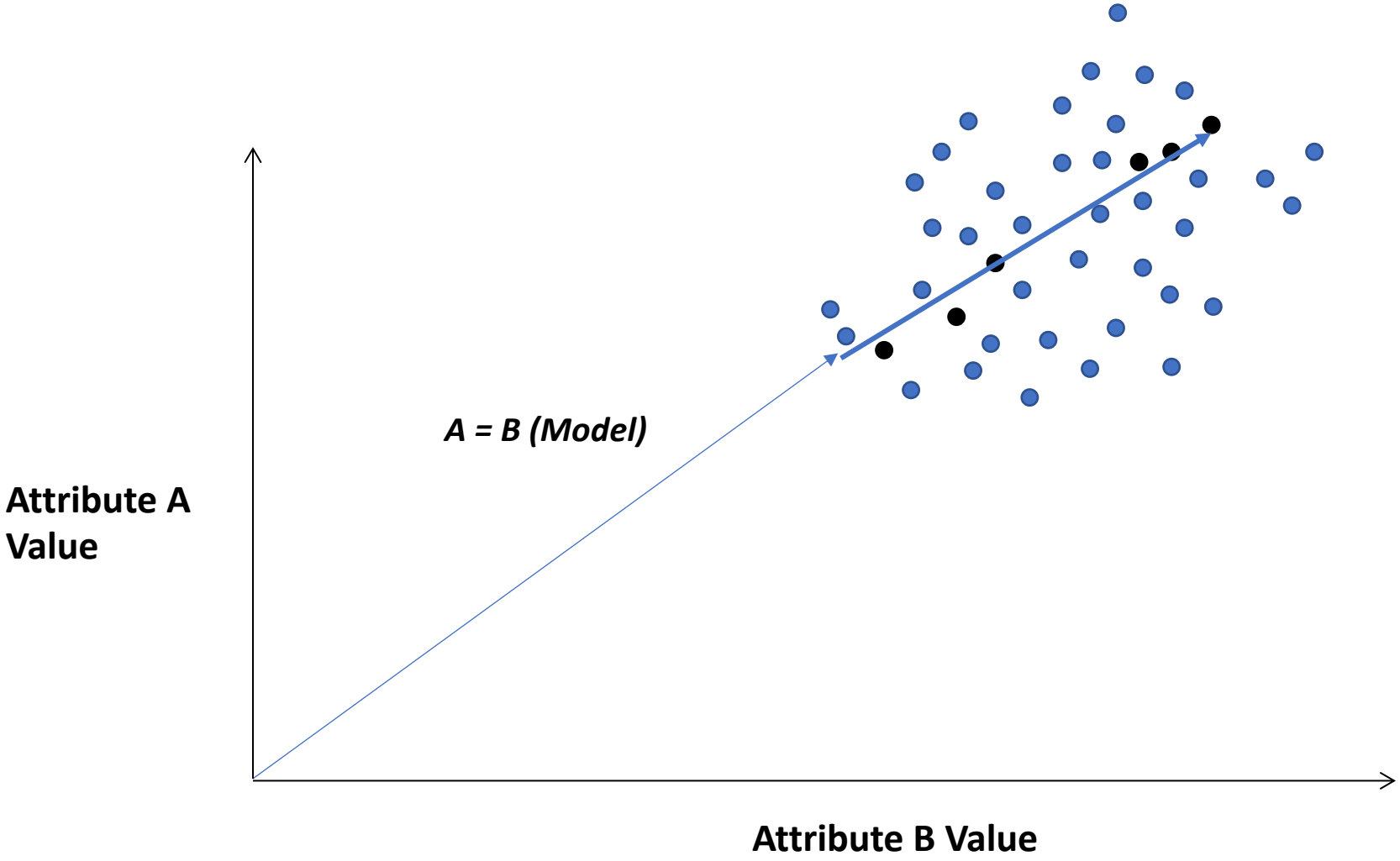
Supervised Machine Learning

New Training:
Observe Slight Variation



Week 3

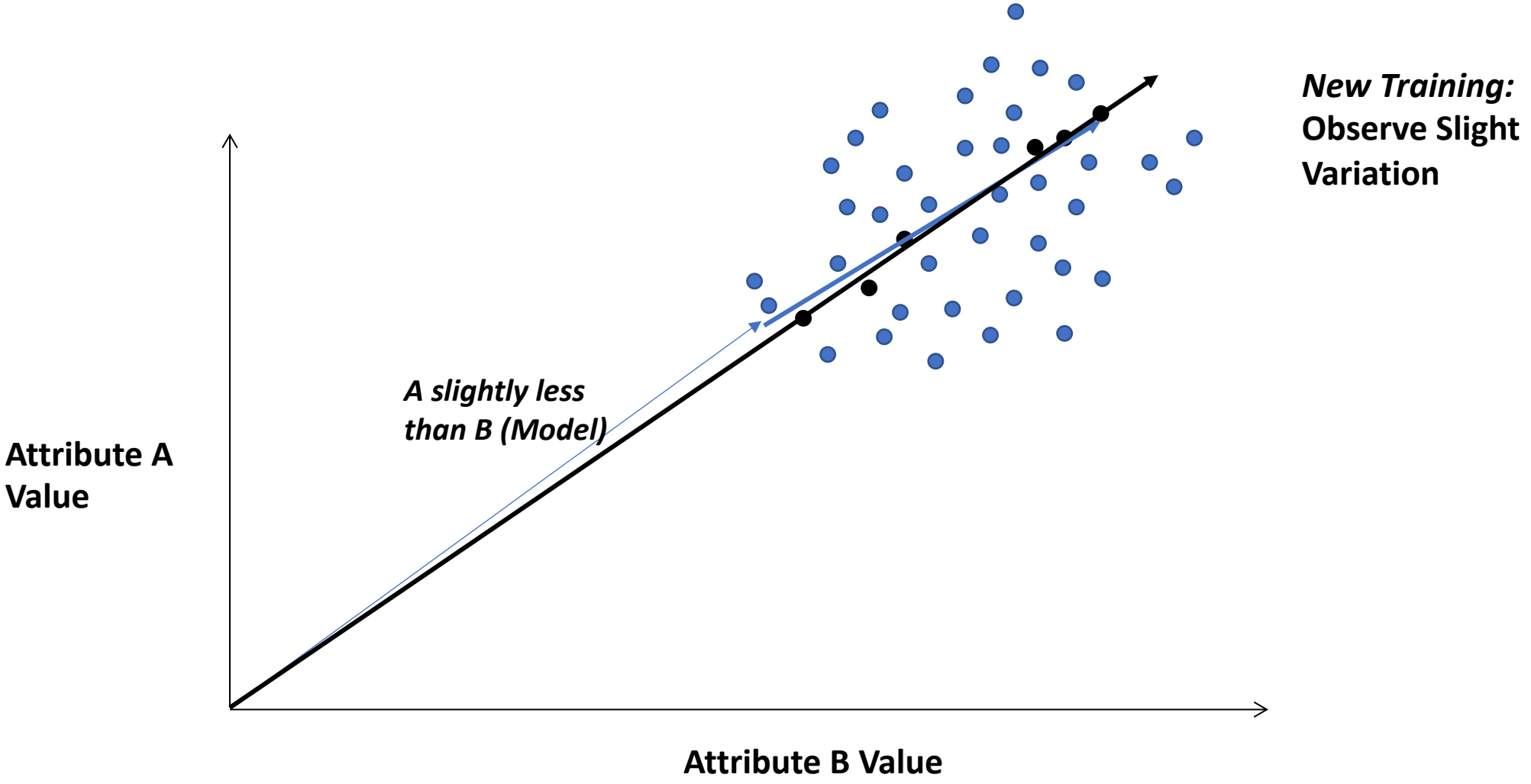
Supervised Machine Learning



New Training:
Observe Slight Variation

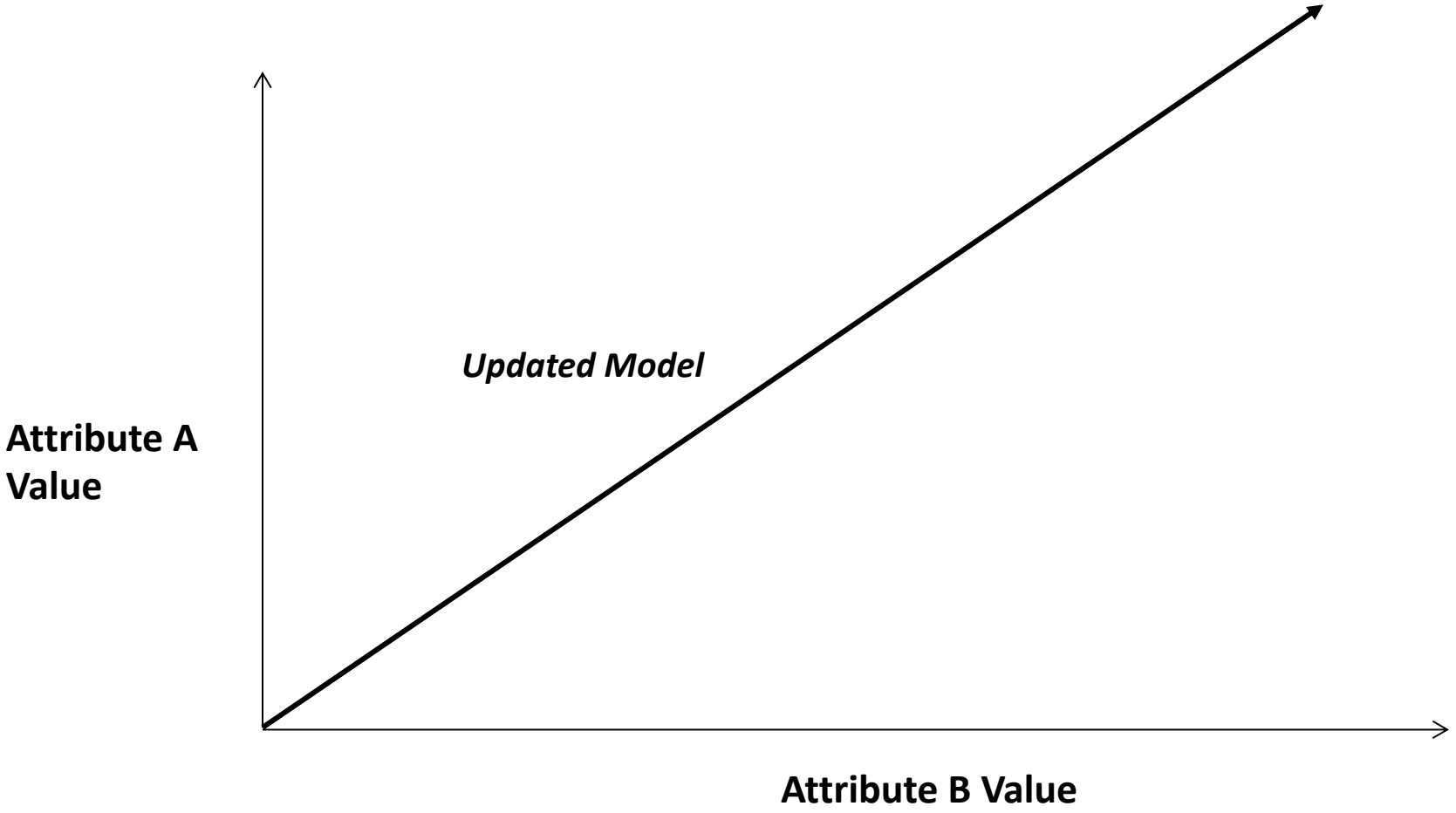
Week 3

Supervised Machine Learning



Week 3

Supervised Machine Learning



Week 3

Supervised Machine Learning for Security – Concepts

Week 3

Supervised Machine Learning for Security – Concepts

Training Data for App Security (One Factor)

Input Feature X1: Size Difference Between Largest and Smallest App Data Transfer / Past Month	Output Value: Number of Vulnerabilities Found In the App / Past Month
20GB	127
26GB	150
200MB	56

Week 3

Supervised Machine Learning for Security – Concepts

Training Data for App Security (Two Factors)

Input Feature X1: Size Difference Between Largest and Smallest App Data Transfer / Past Month	Input Feature X2: Number of Permissions Errors Found / Last Month	Output Value: Number of Vulnerabilities Found In the App / Past Month
20GB	12	127
26GB	4	150
200MB	0	56

Week 3

Supervised Machine Learning for Security – Concepts

Training Data for App Security (Two Factors)

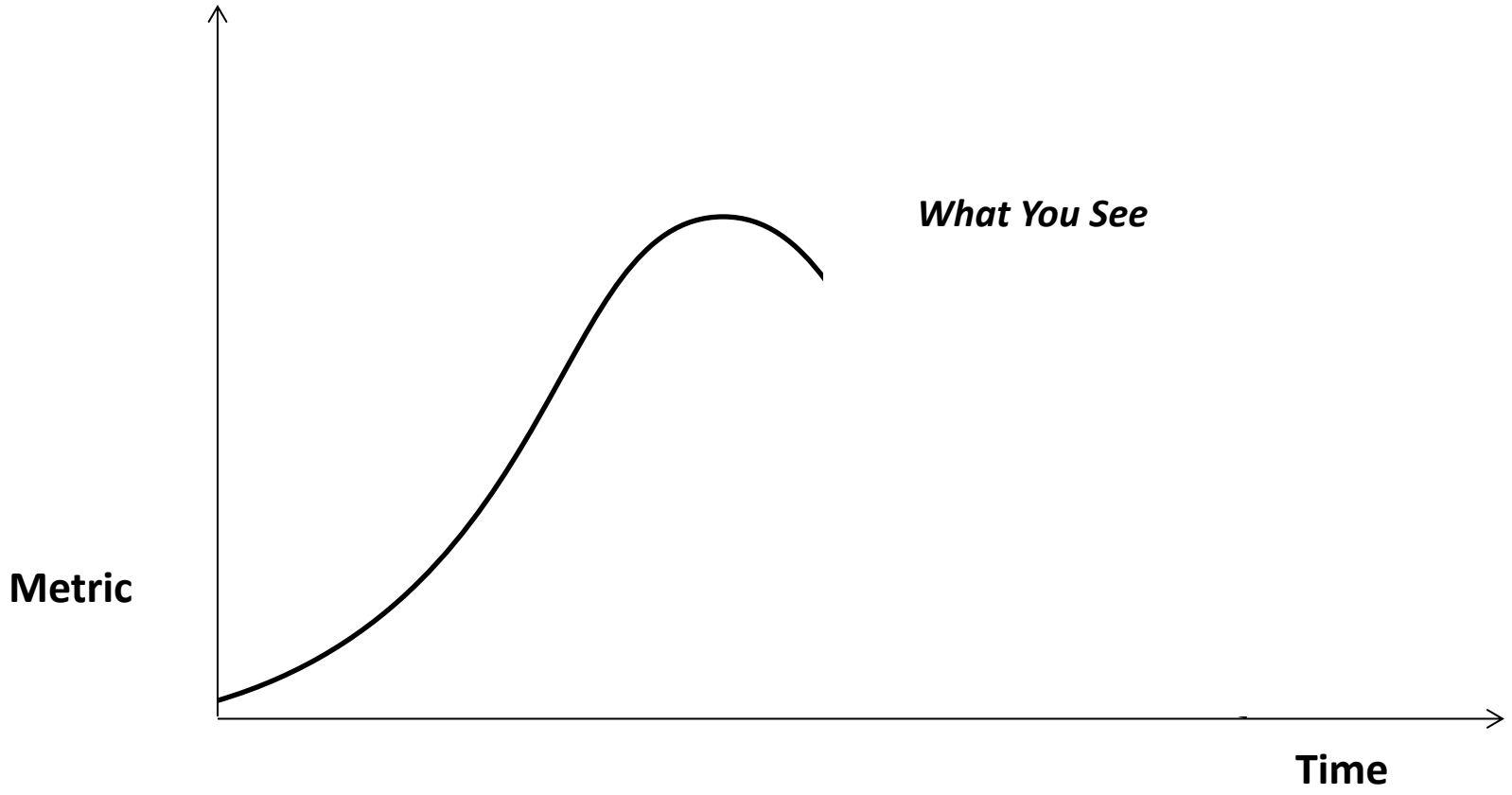
Input Feature X1: Size Difference Between Largest and Smallest App Data Transfer / Past Month	Input Feature X2: Number of Permissions Errors Found / Last Month	Output Value: Number of Vulnerabilities Found In the App / Past Month
20GB	12	127
26GB	4	150
200MB	0	56

Linear Regression Strategy: Graph the Data and Use to Predict Number of Vulnerabilities from Two Input factors

How Can Network Security Attacks Be Visualized?

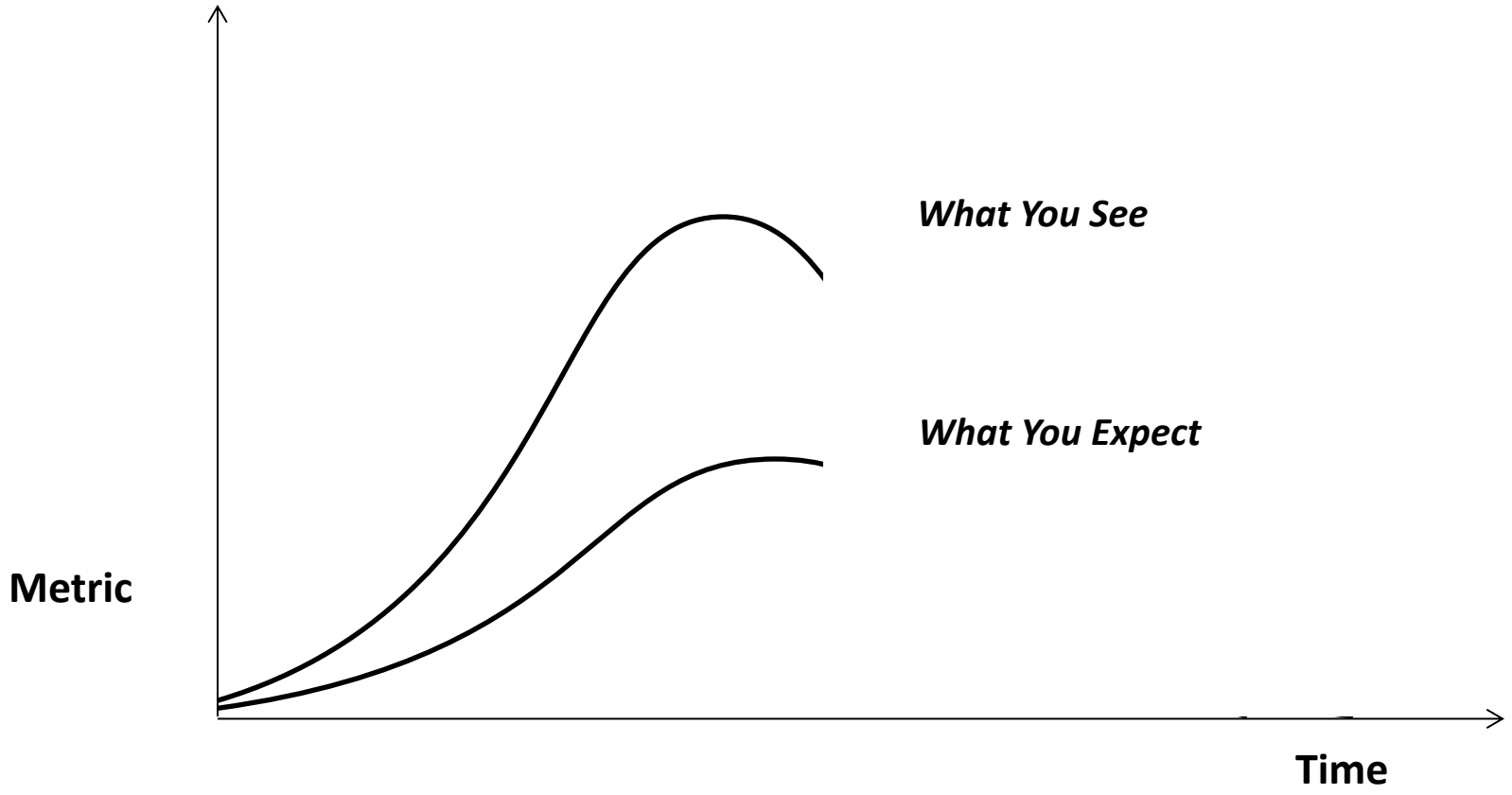
Week 3

Real Time Network Security Behavioral Analytics



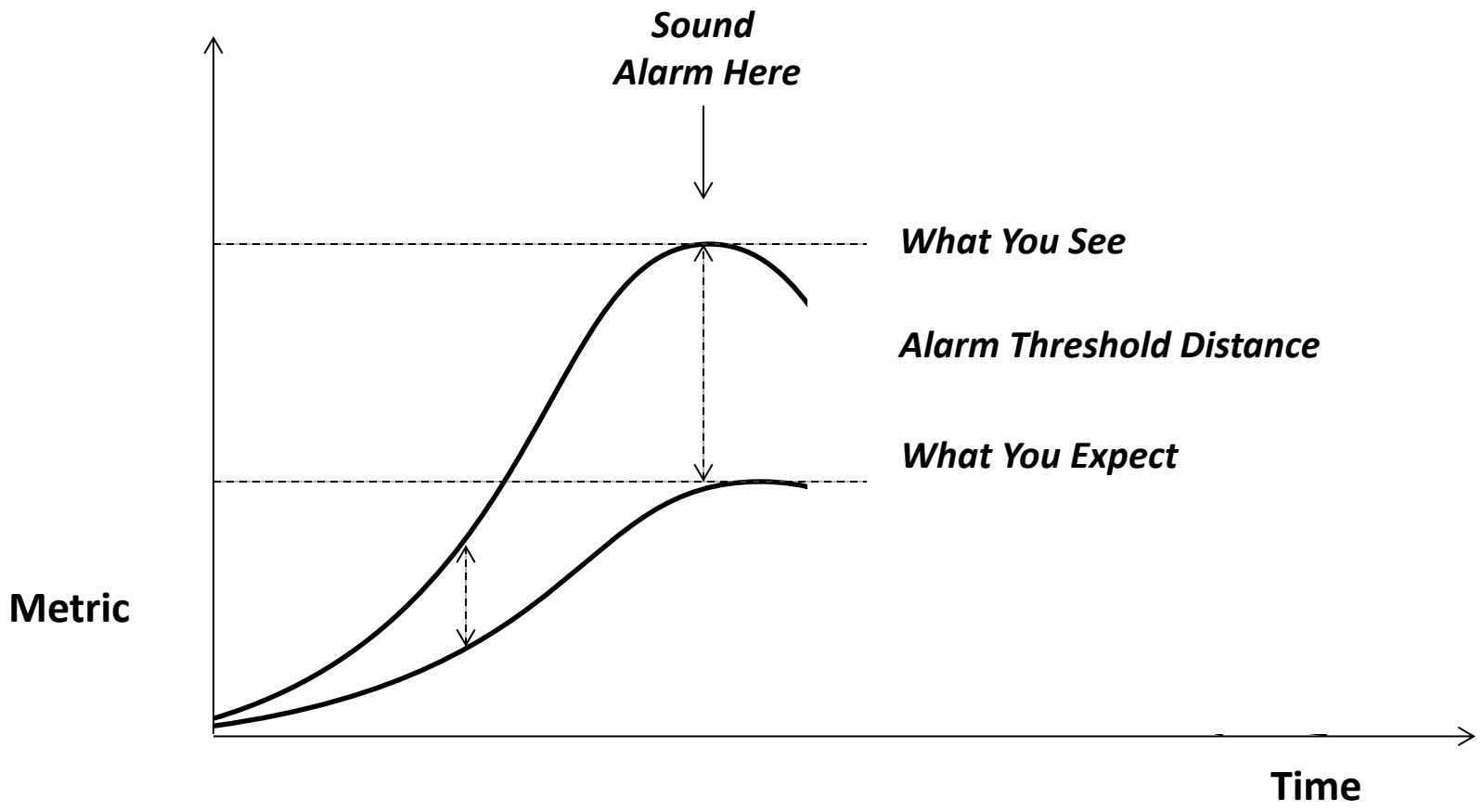
Week 3

Real Time Network Security Behavioral Analytics



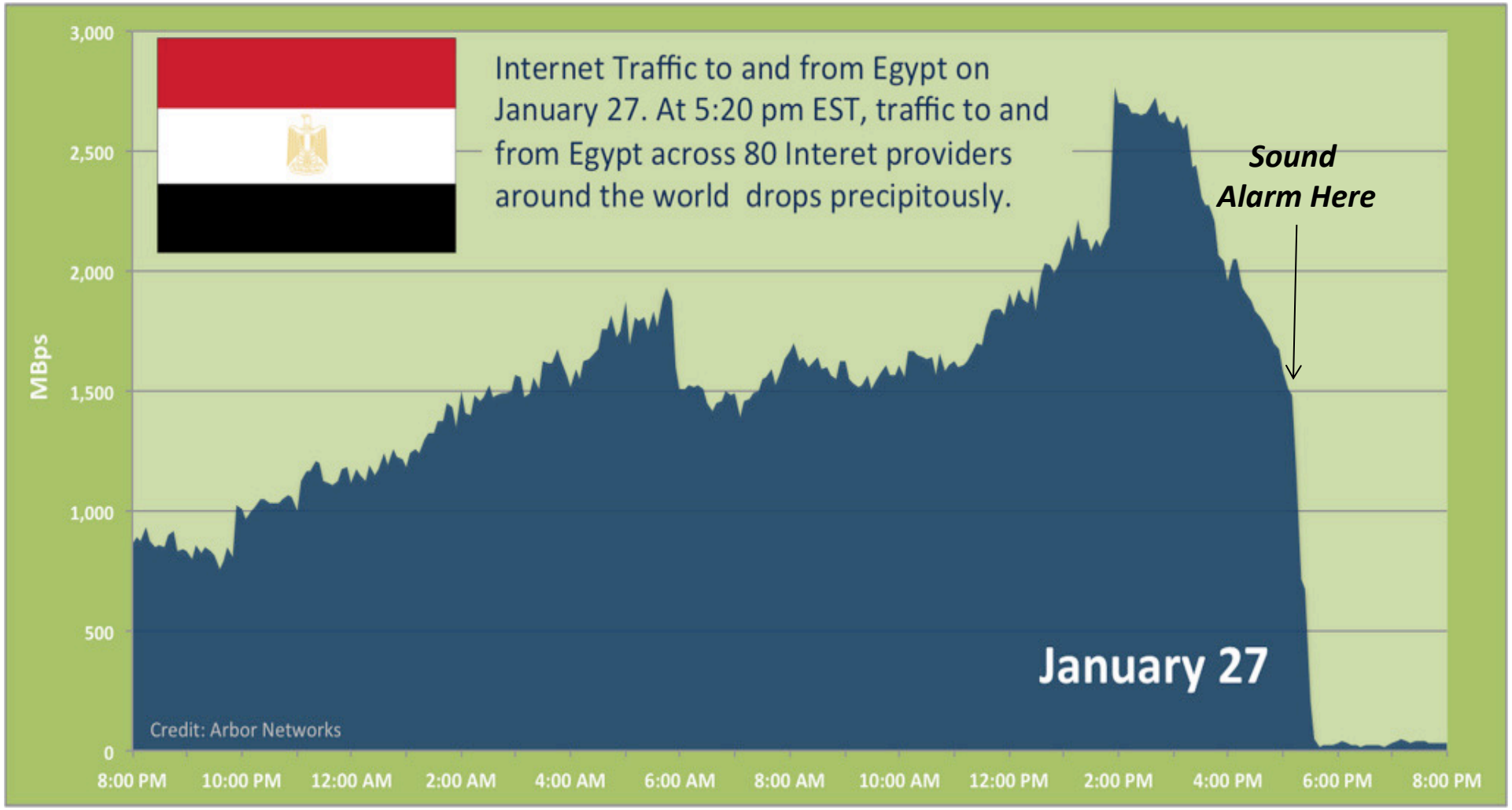
Week 3

Real Time Network Security Behavioral Analytics



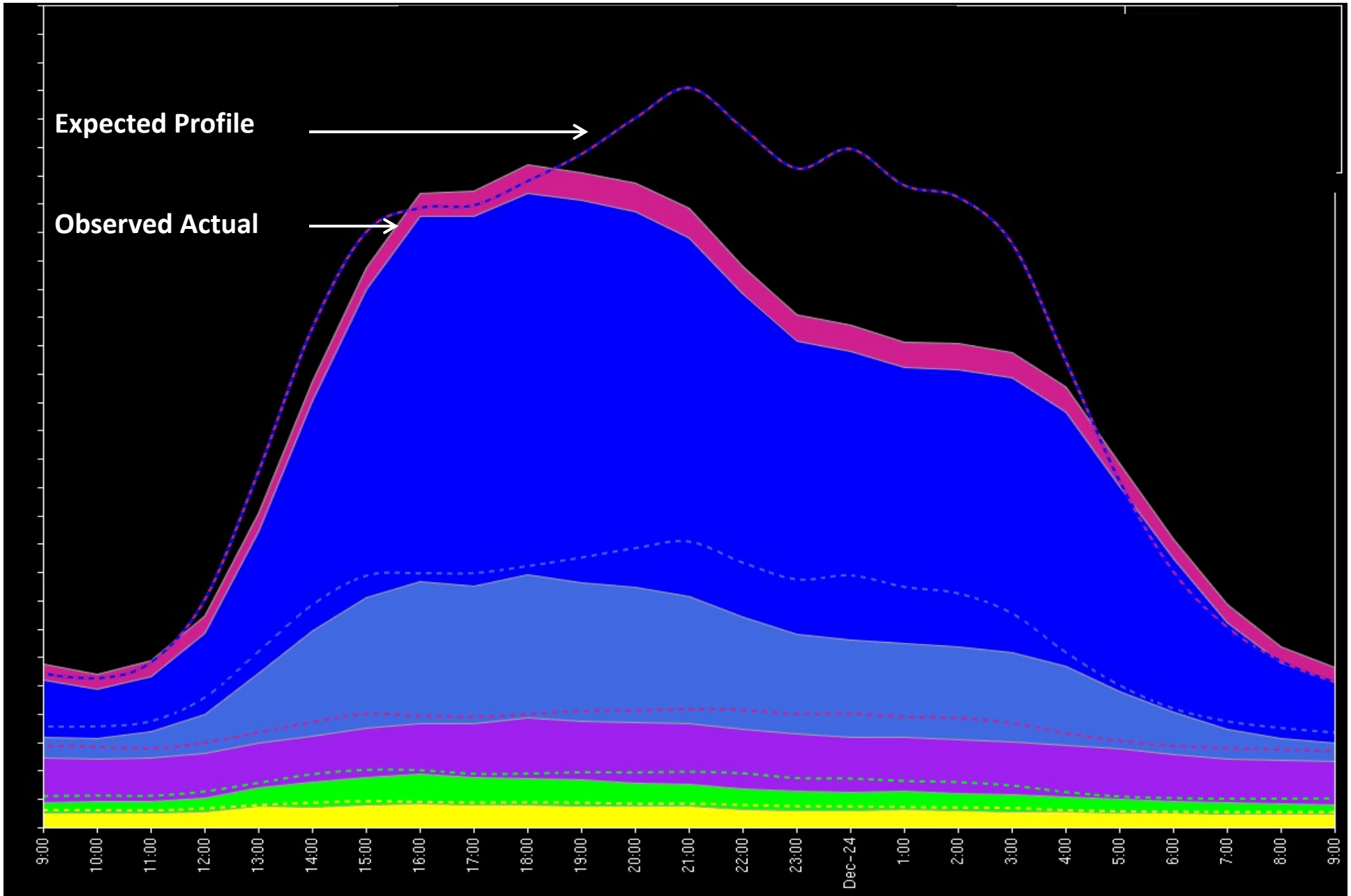
Week 3

Internet Blackout in Egypt – 01/27/11



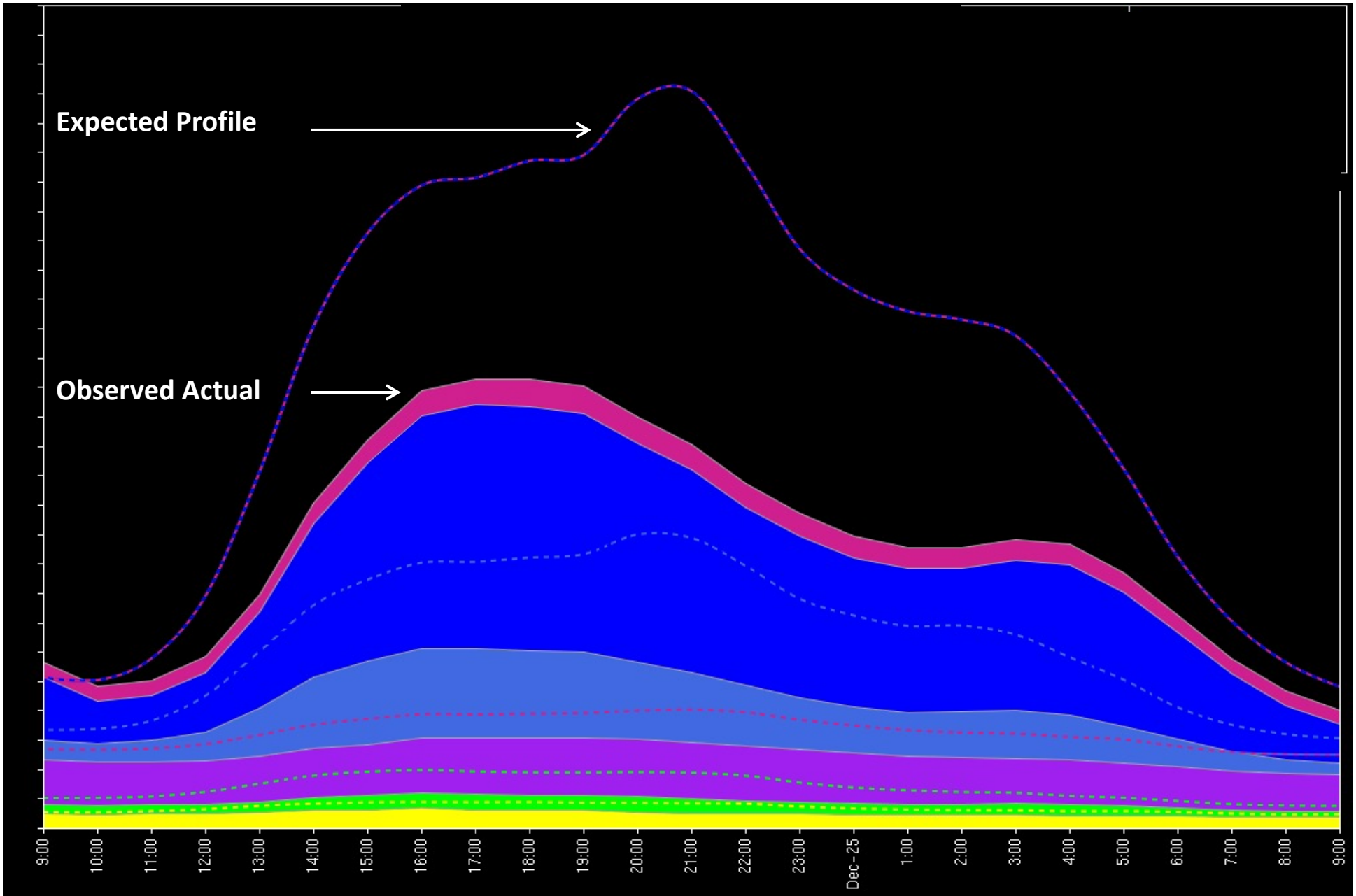
Week 3

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



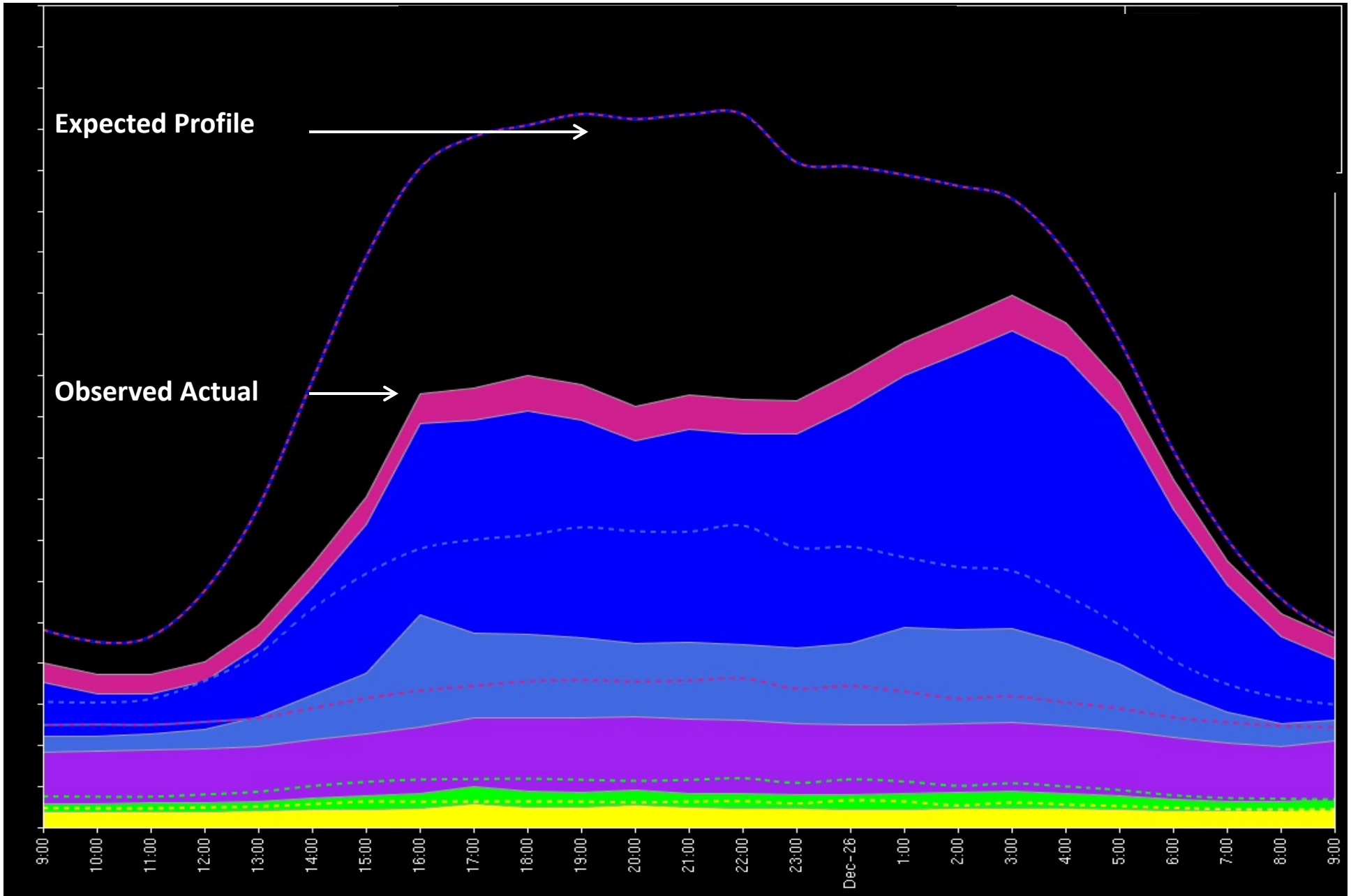
Week 3

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



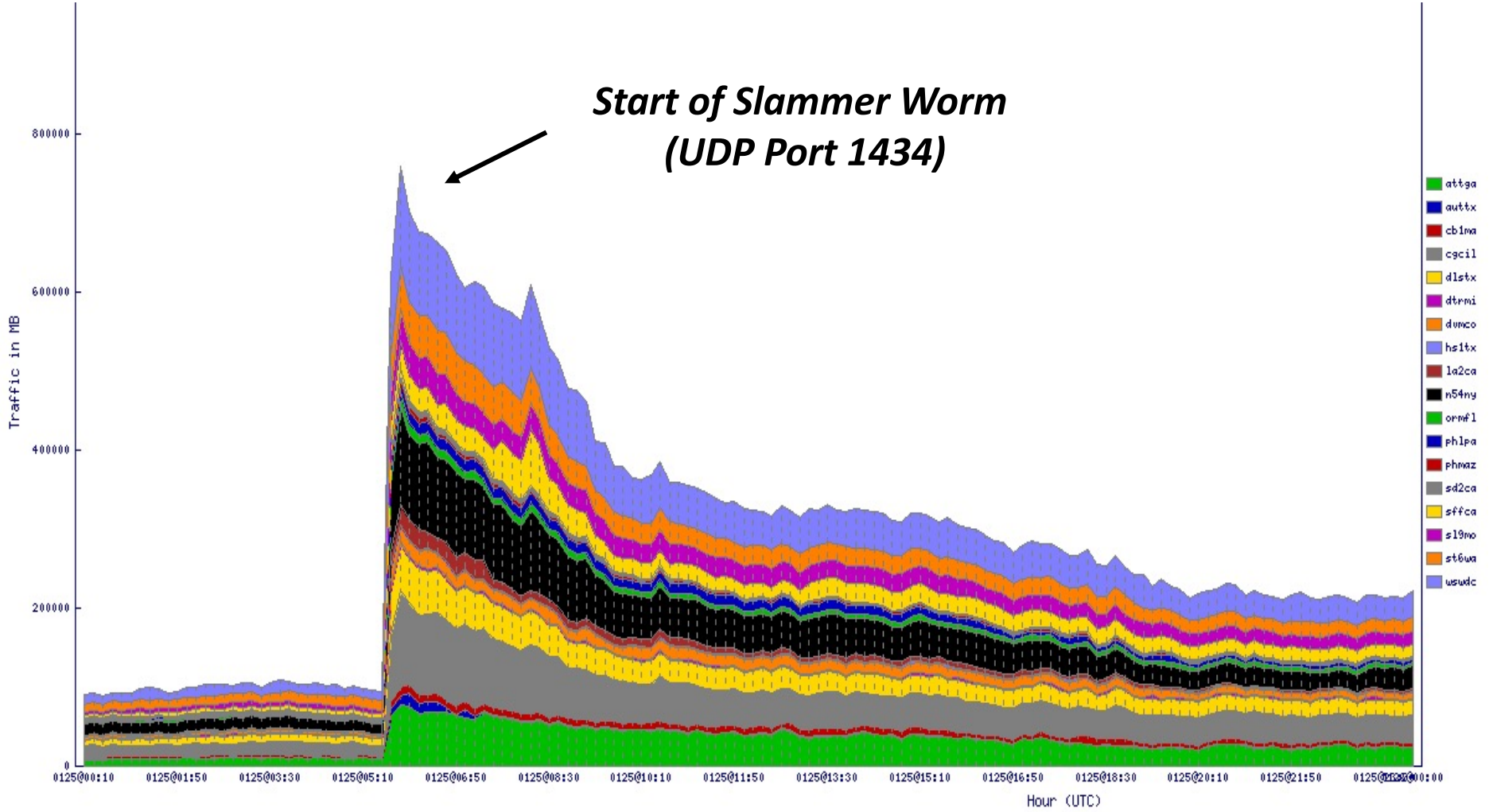
Week 3

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



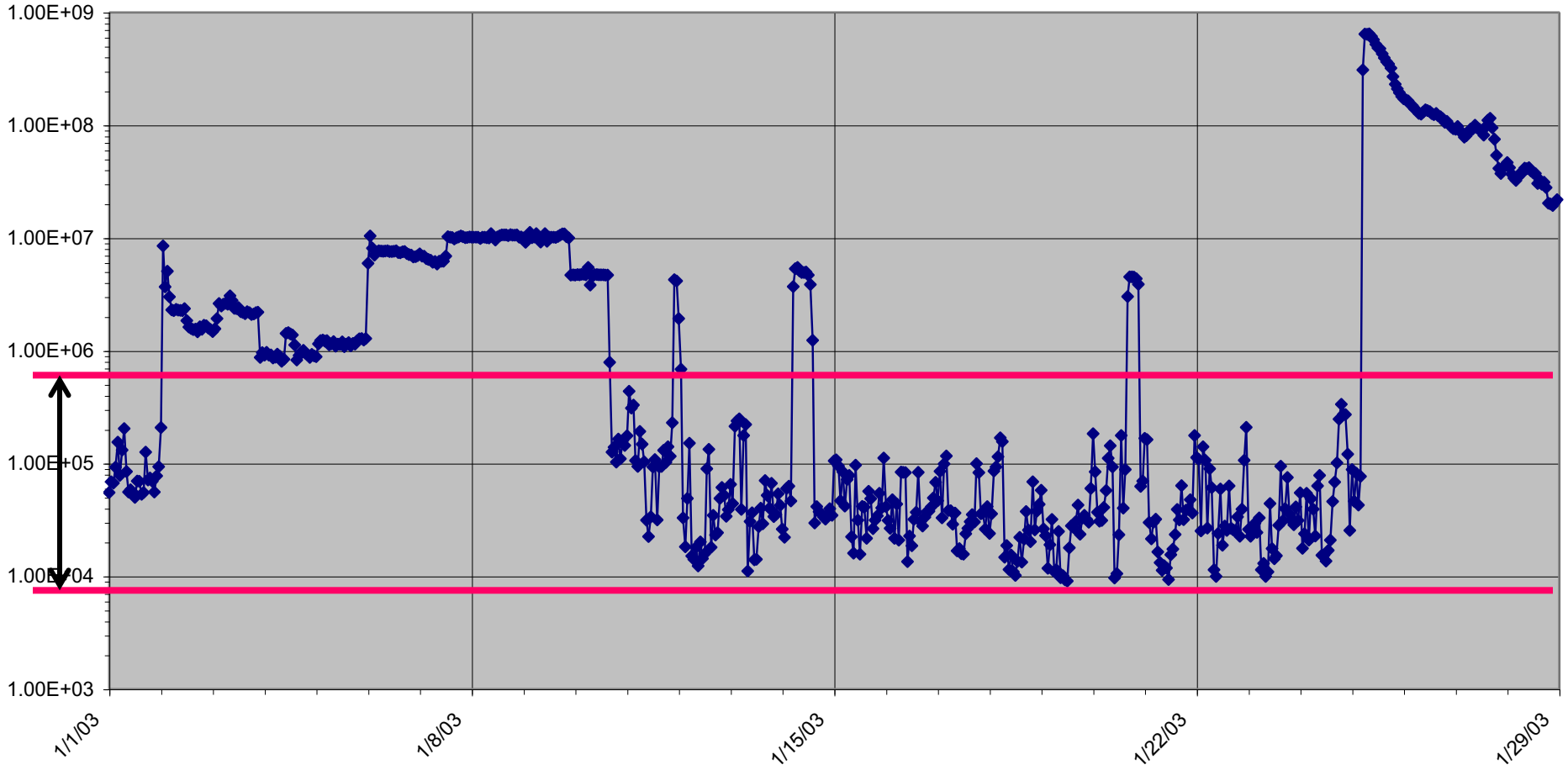
Week 3

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



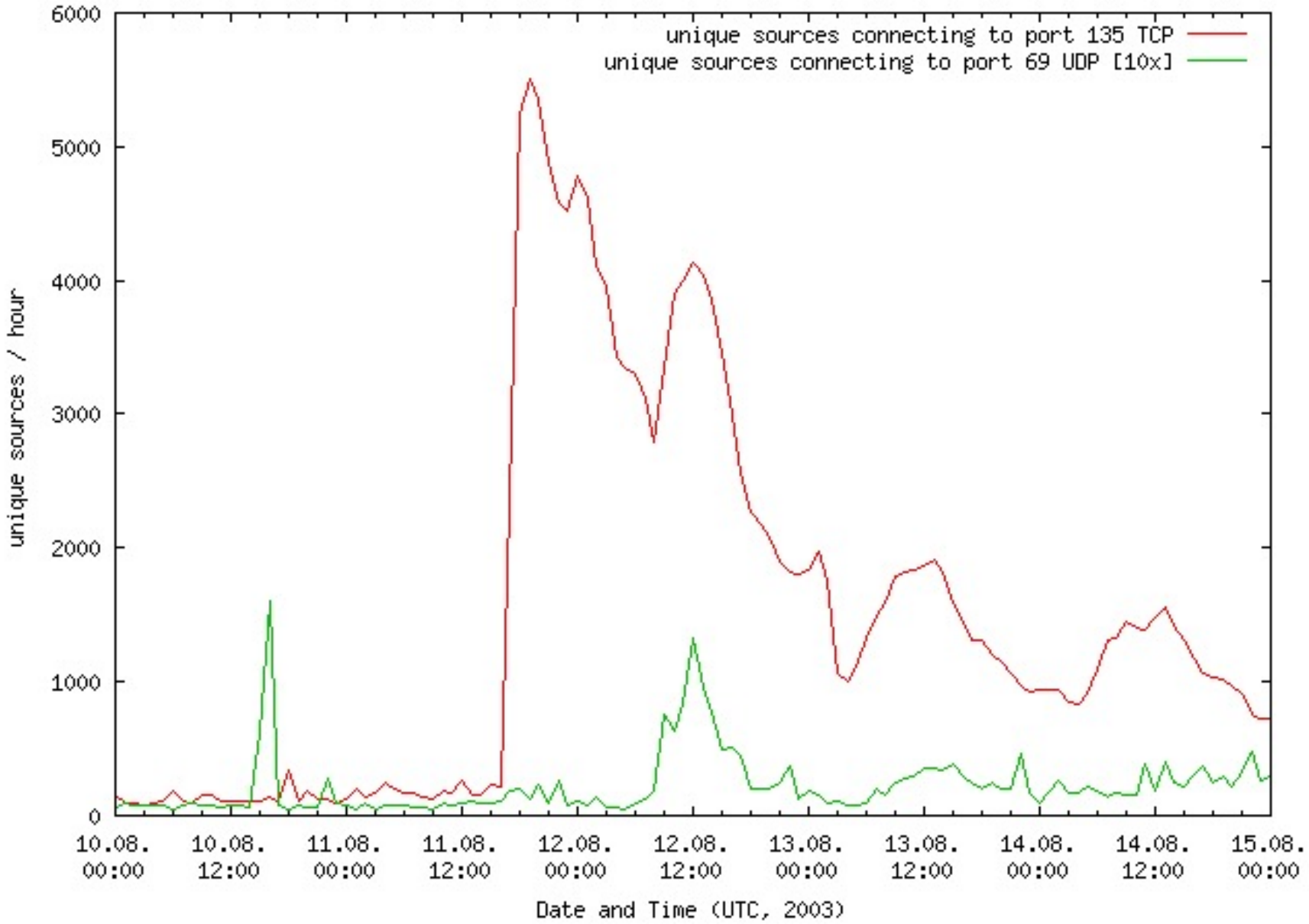
Week 3

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



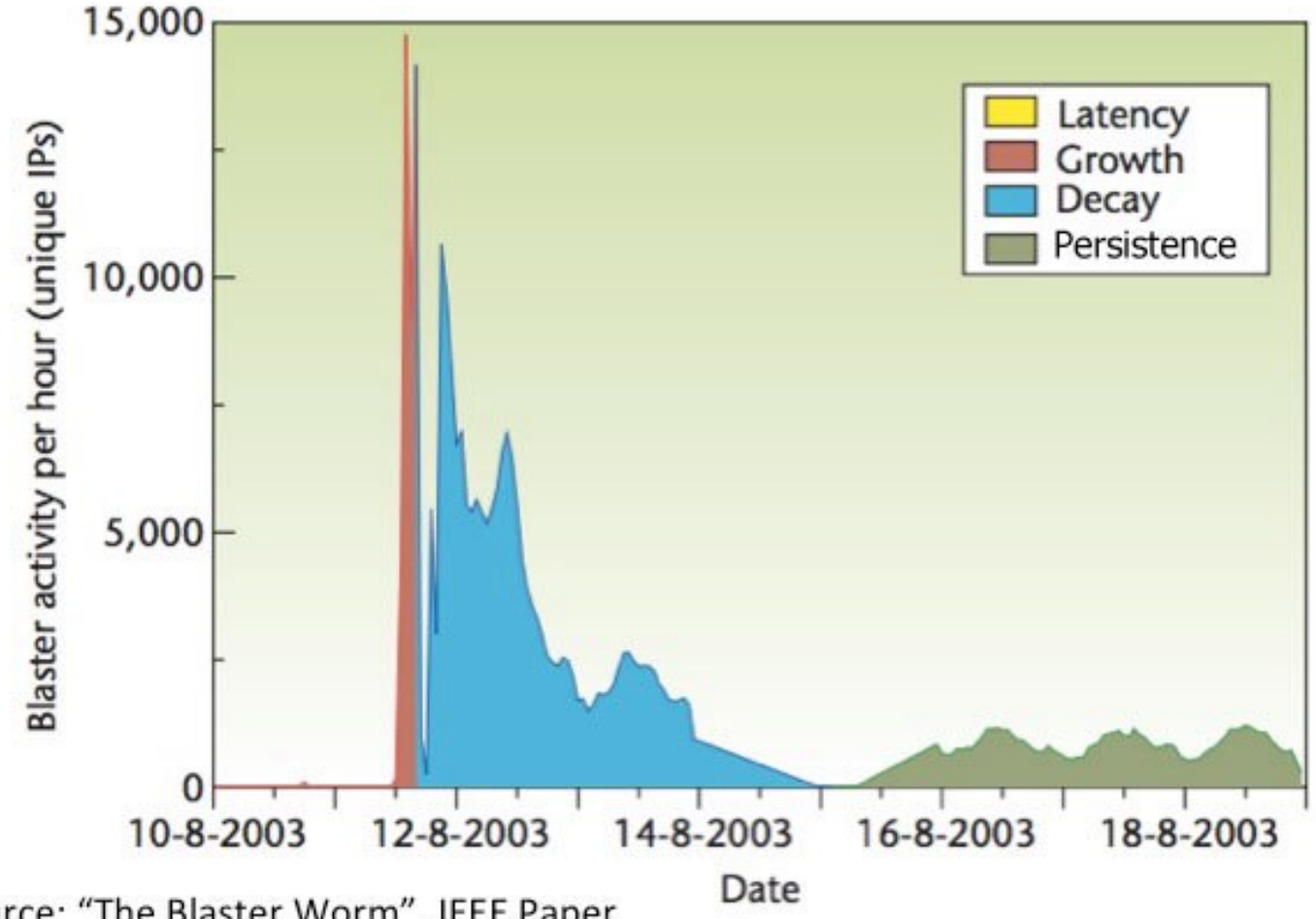
Week 3

Sharp Spike from Blaster Worm – 8/11/03



Week 3

Sharp Spike from Blaster Worm – 8/11/03

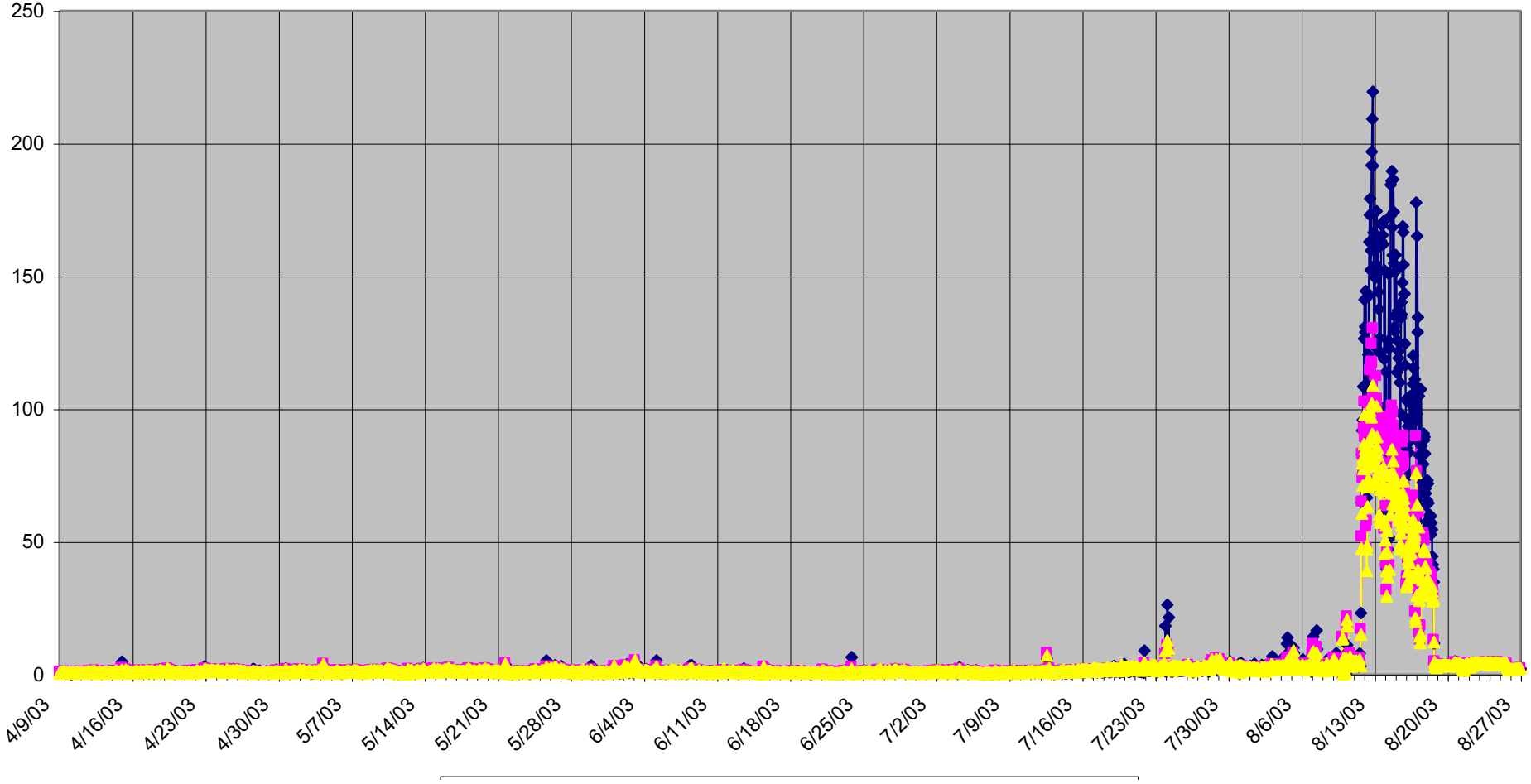


Source: "The Blaster Worm", IEEE Paper

ARBOR NETWORKS

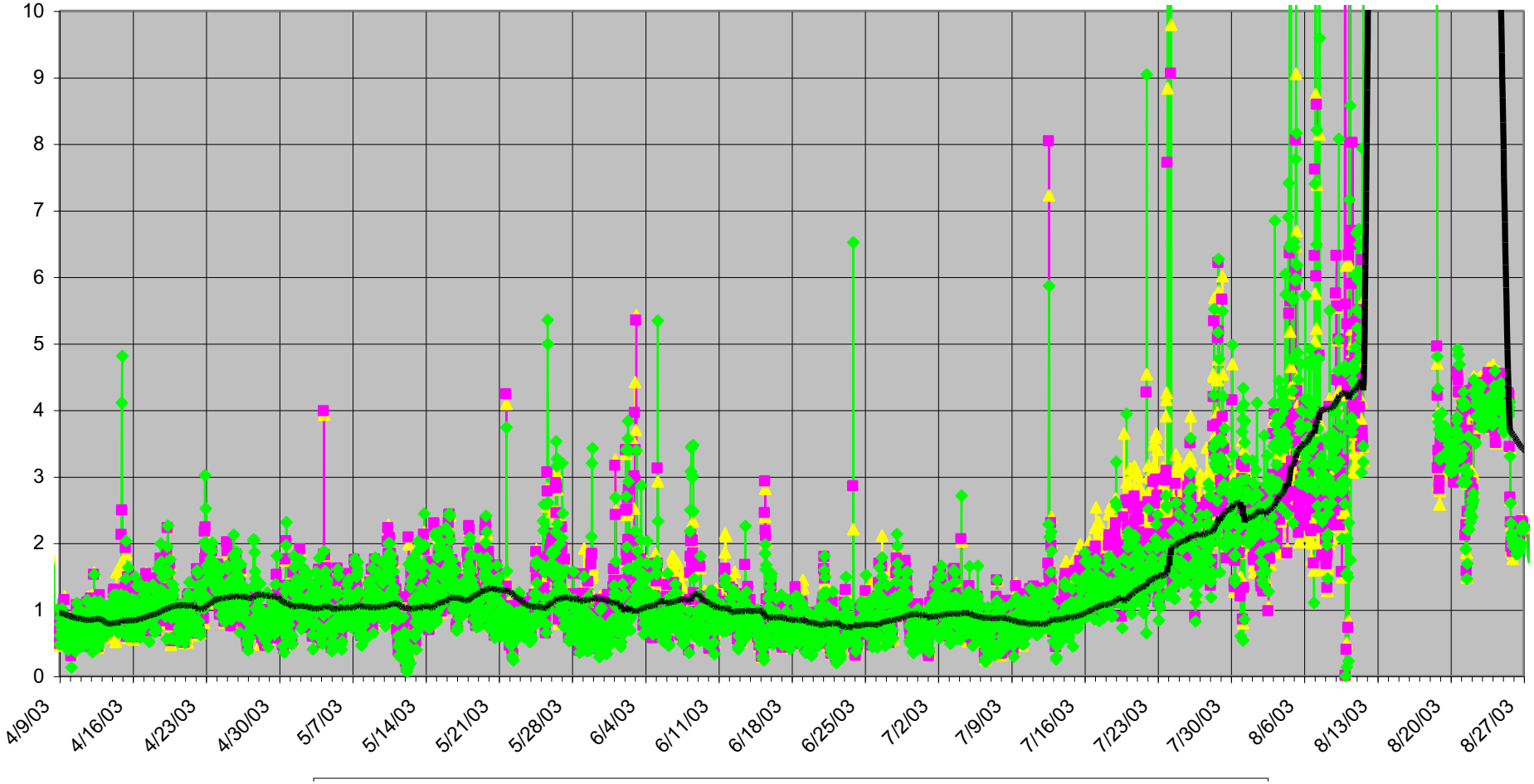
Week 3

Internet View of TCP 135 – Blaster Worm – 2003



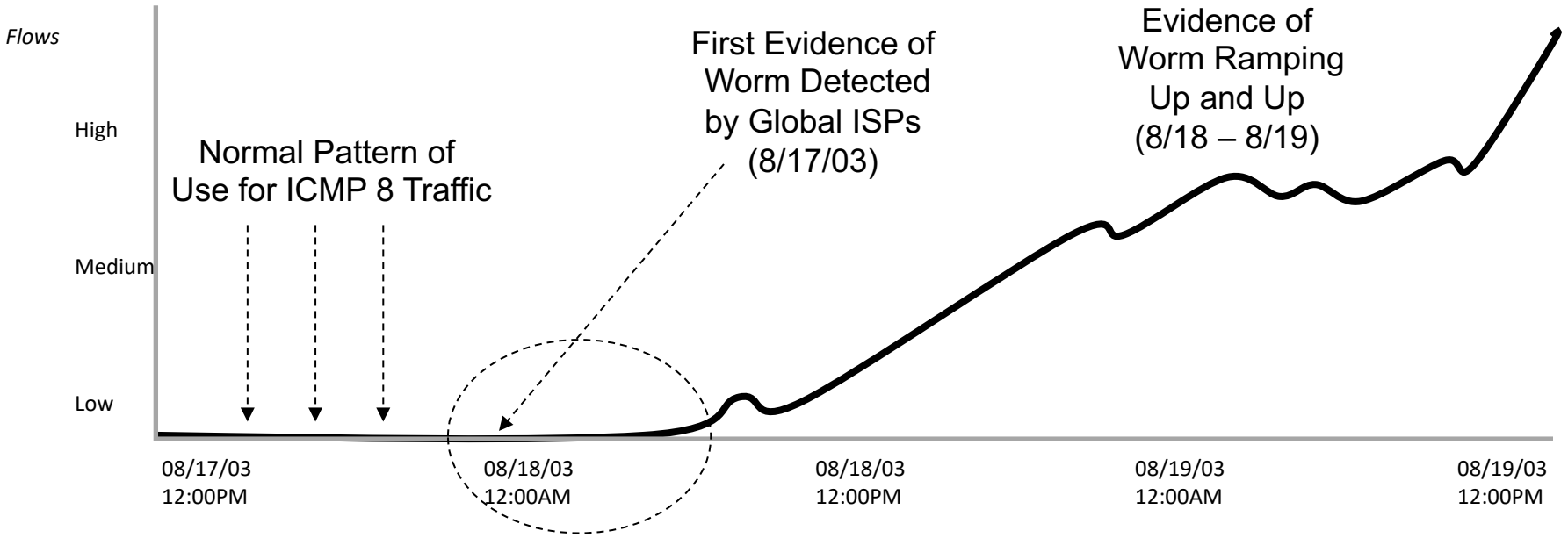
Week 3

Deeper Internet View of TCP 135 Activity – Blaster Worm



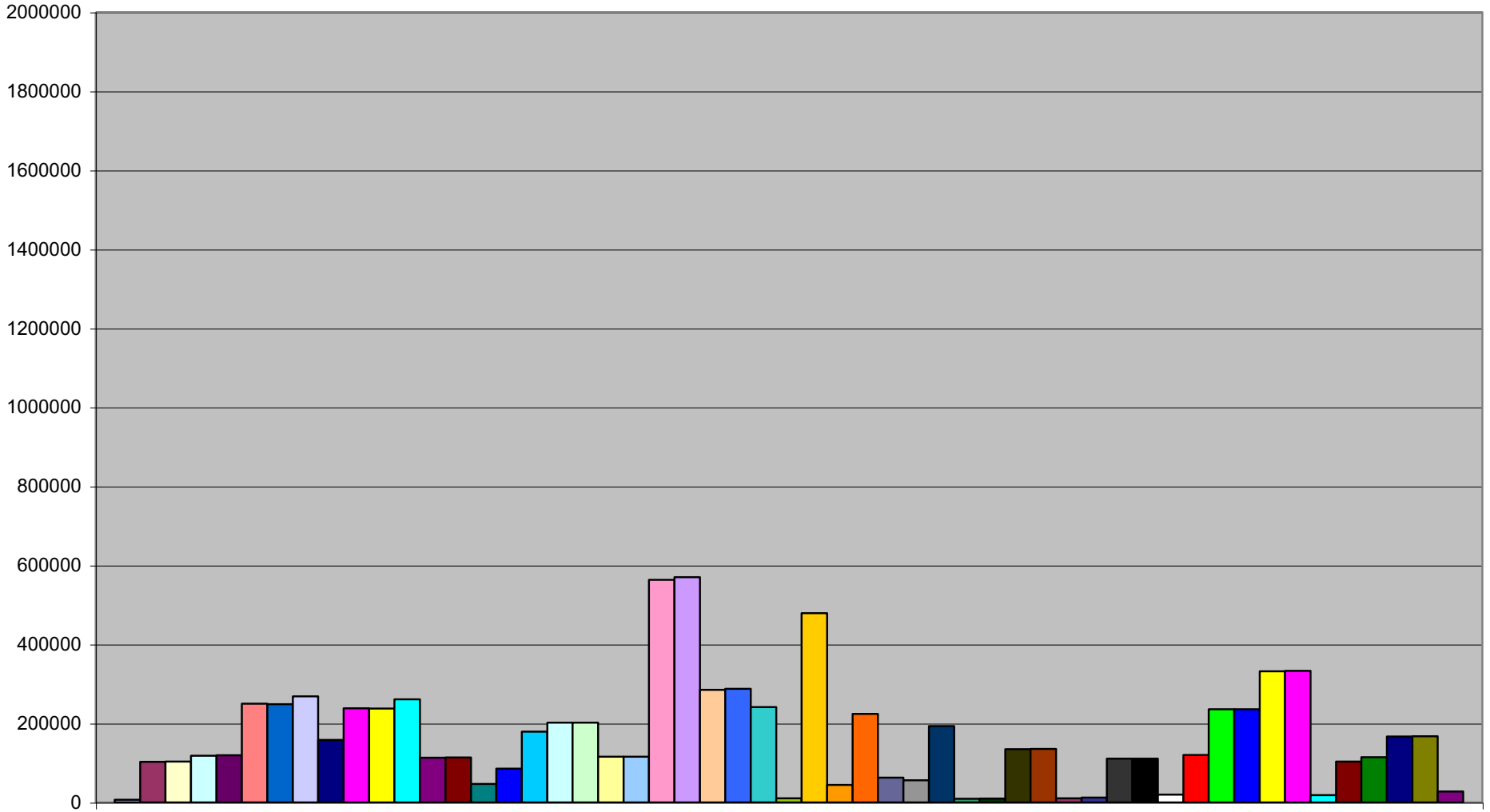
Week 3

Nachi Worm of 2003



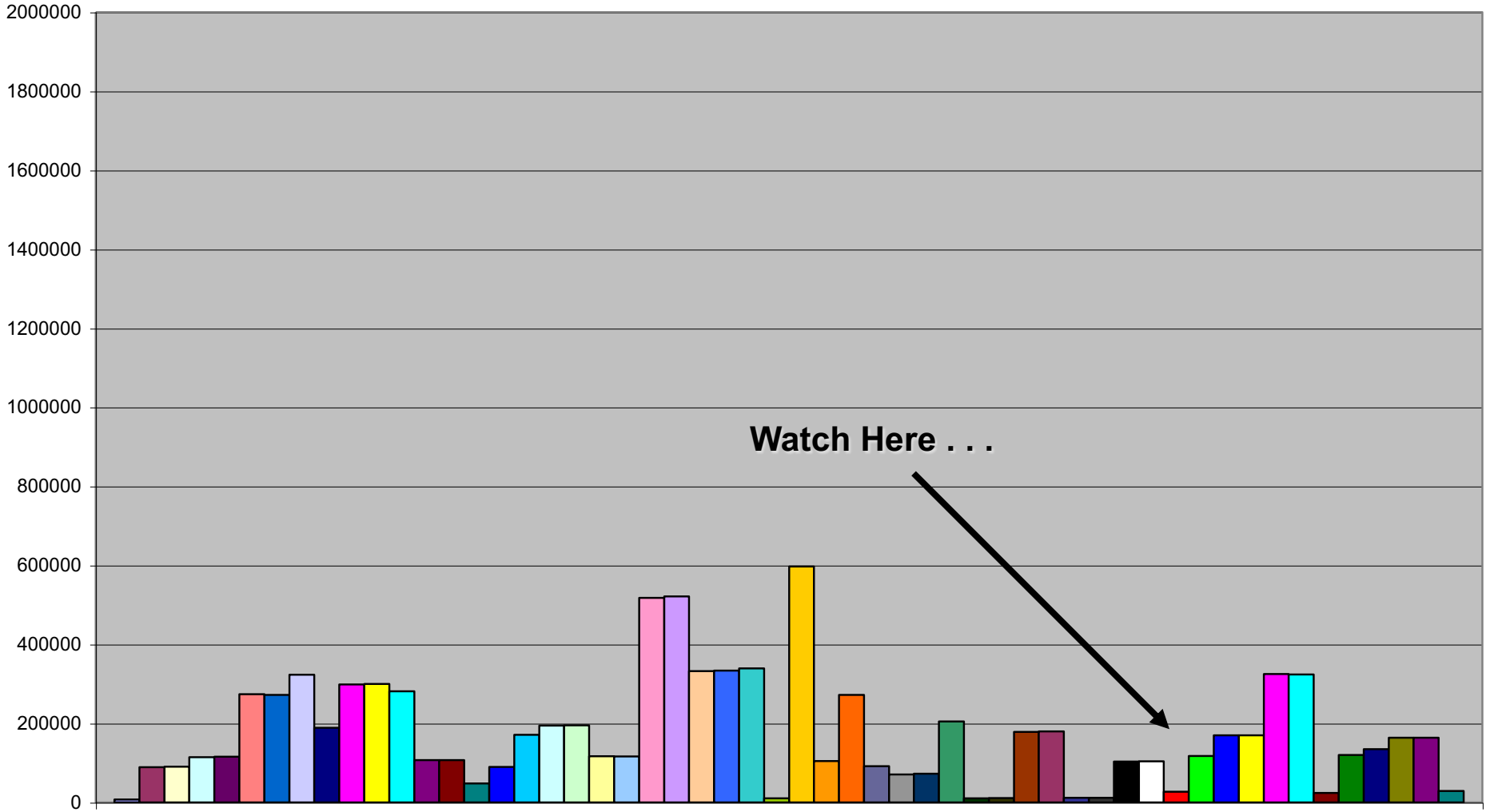
Week 3

Nachi 8/17/03 10:00PM



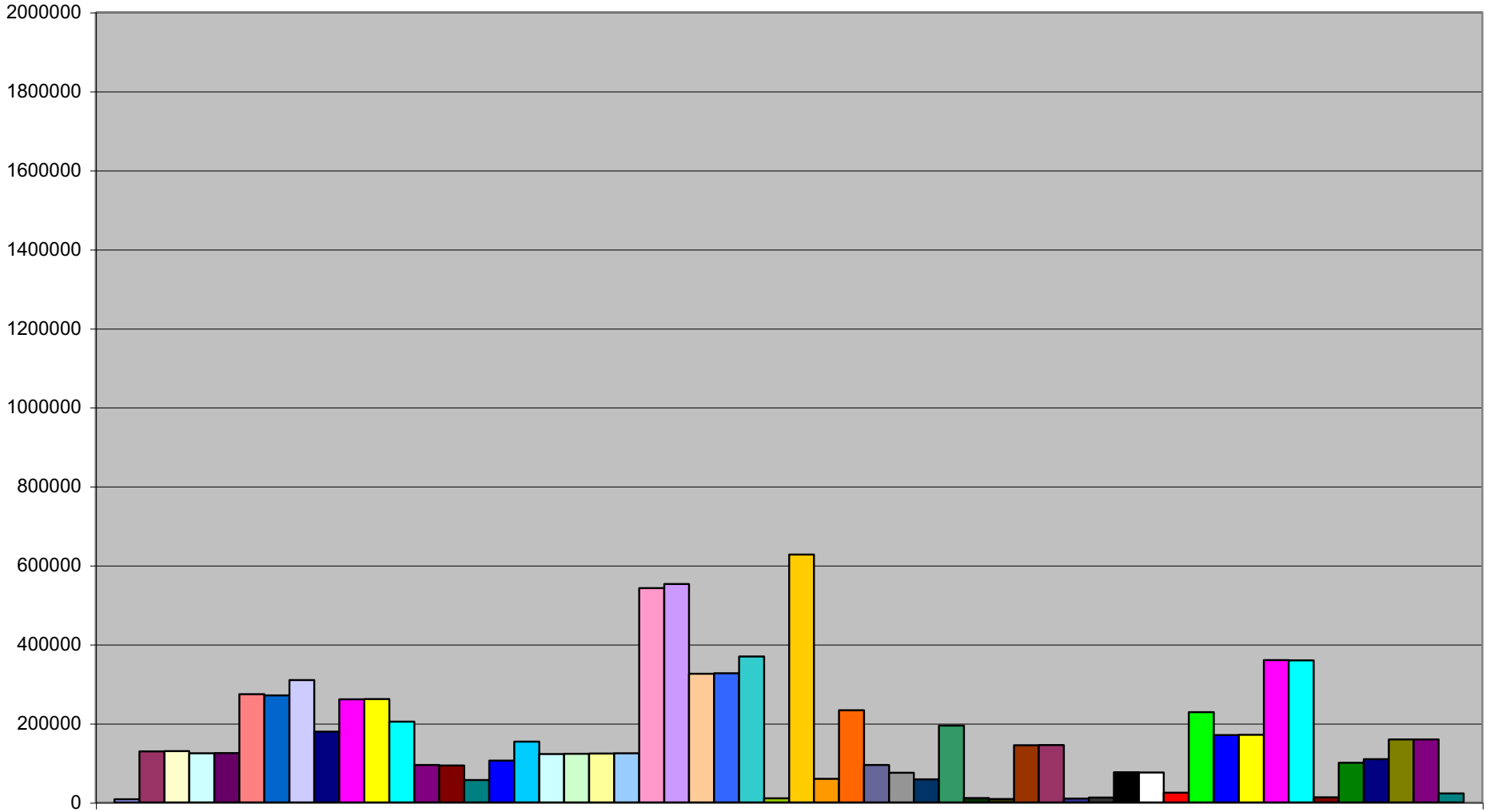
Week 3

Nachi 8/17/03 11:00PM



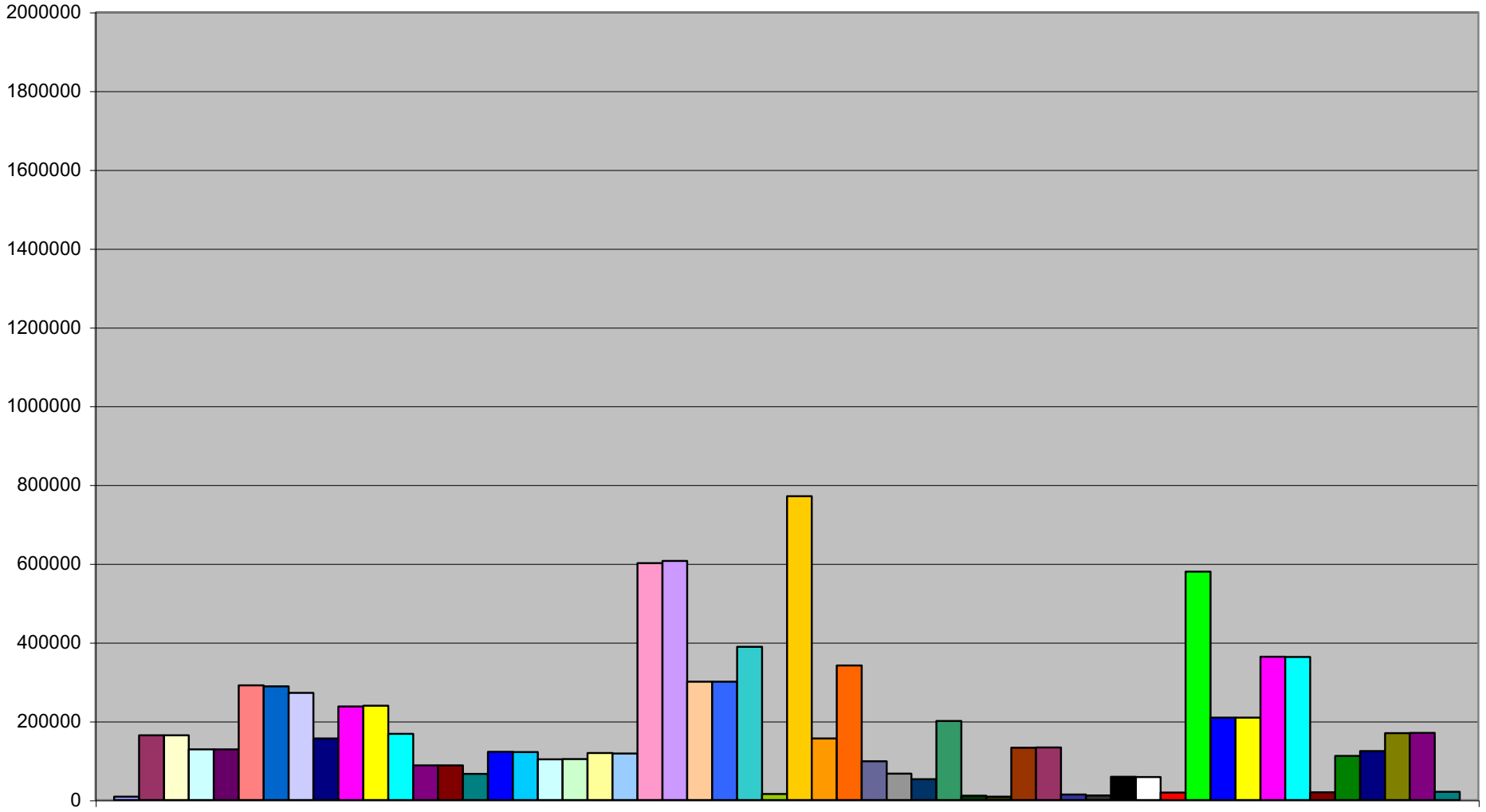
Week 3

Nachi 8/17/03 Midnight



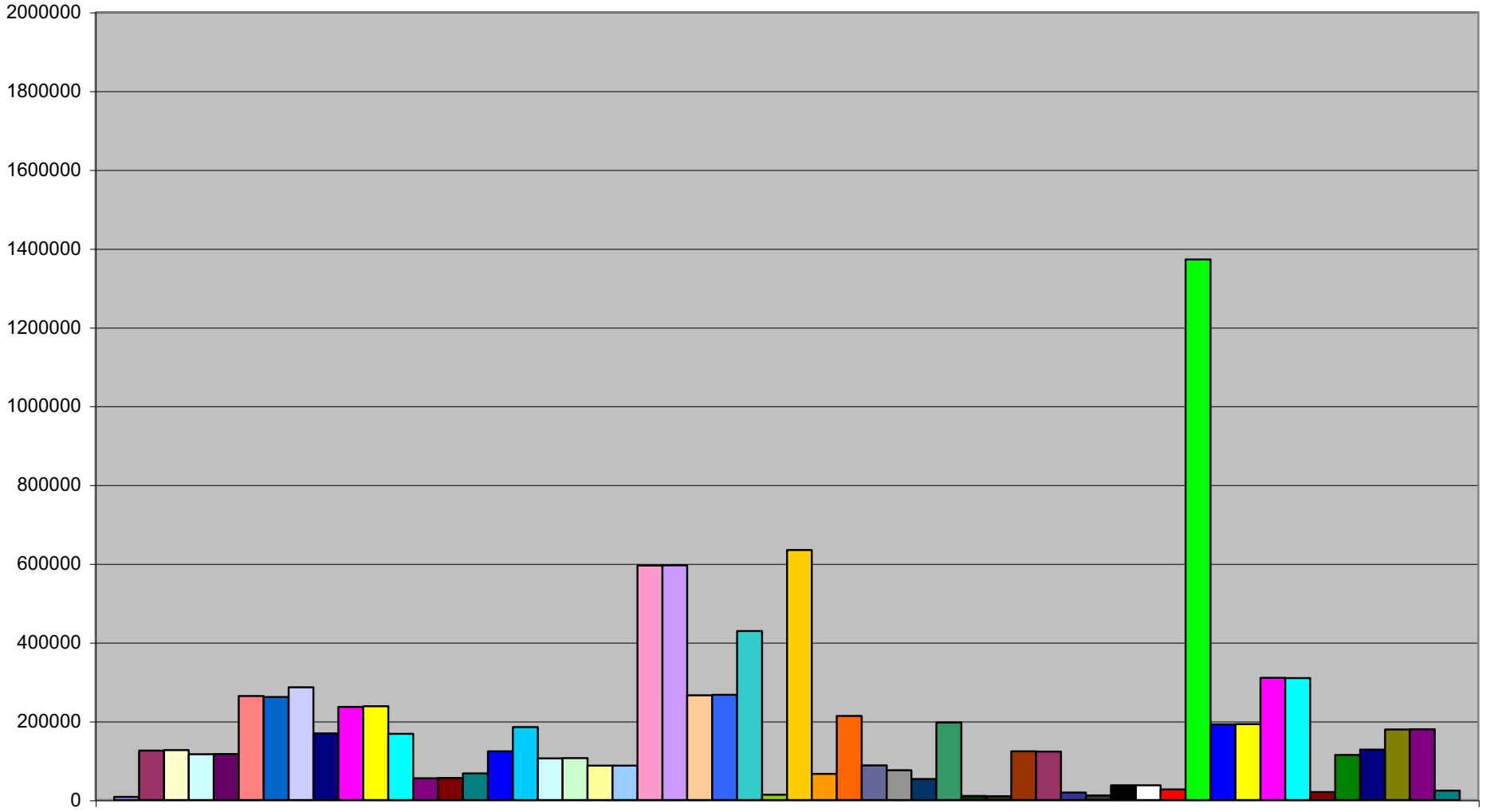
Week 3

Nachi 8/18/03 1:00AM



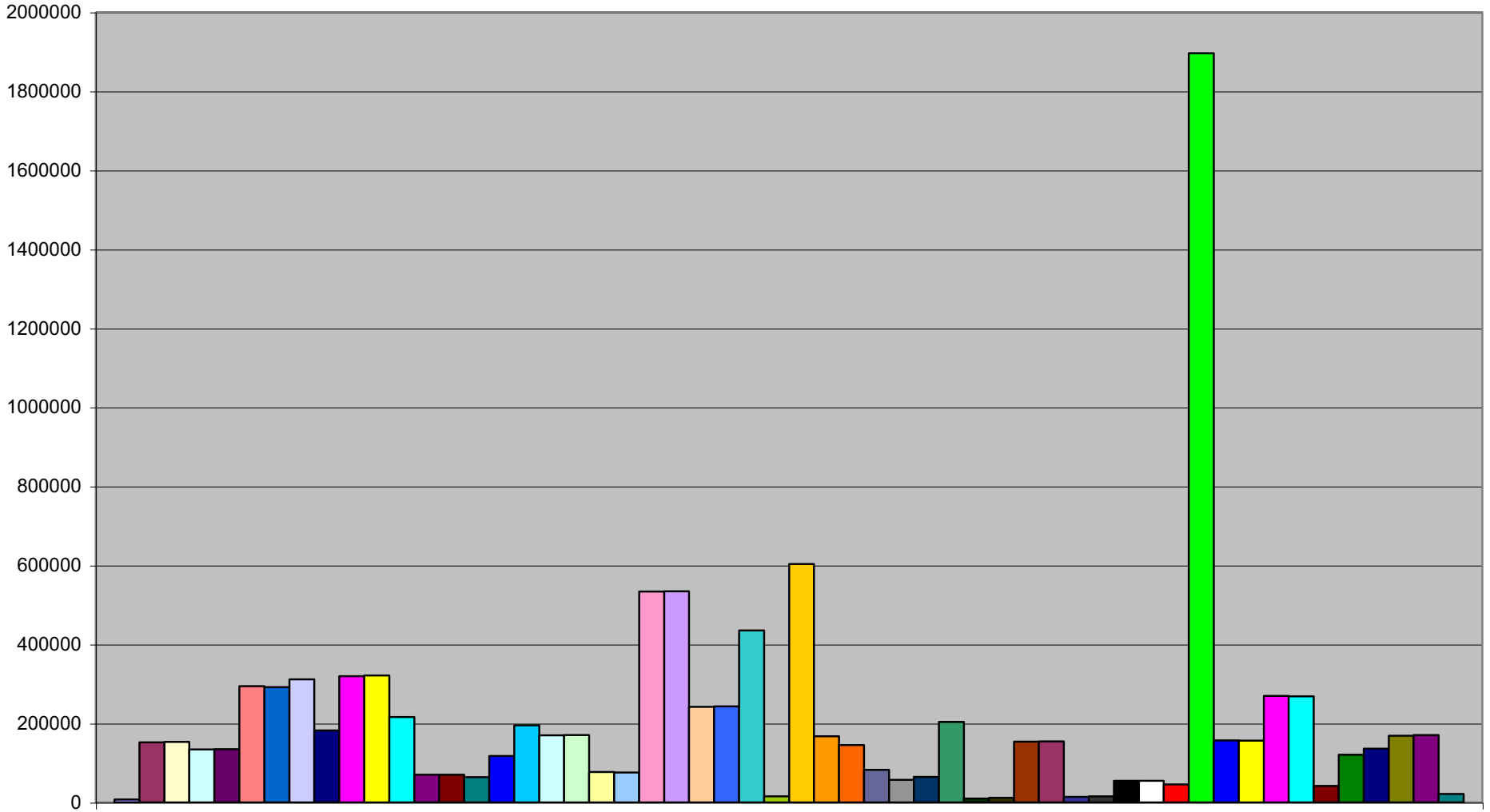
Week 3

Nachi 8/18/03 2:00AM



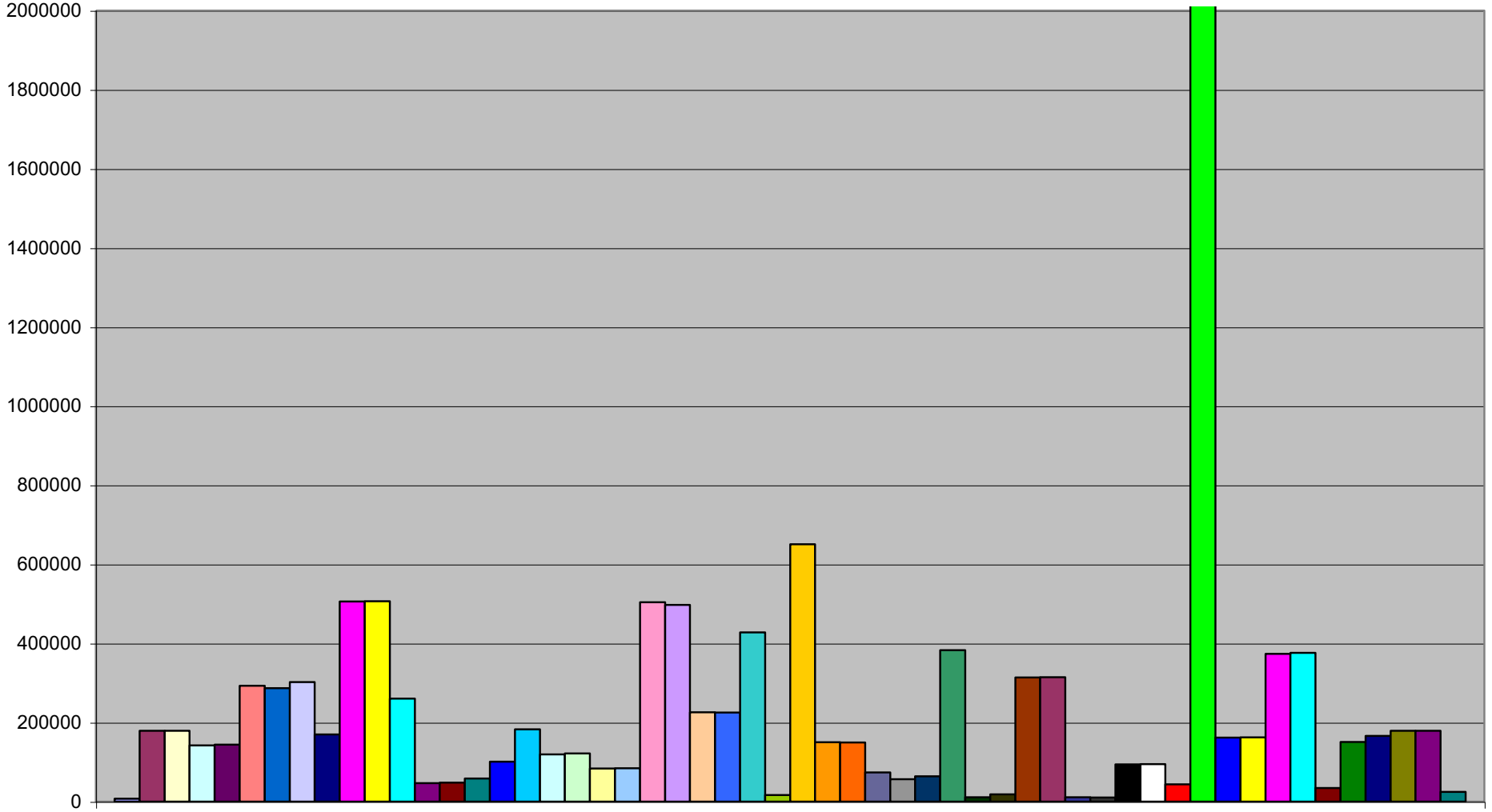
Week 3

Nachi 8/18/03 3:00AM



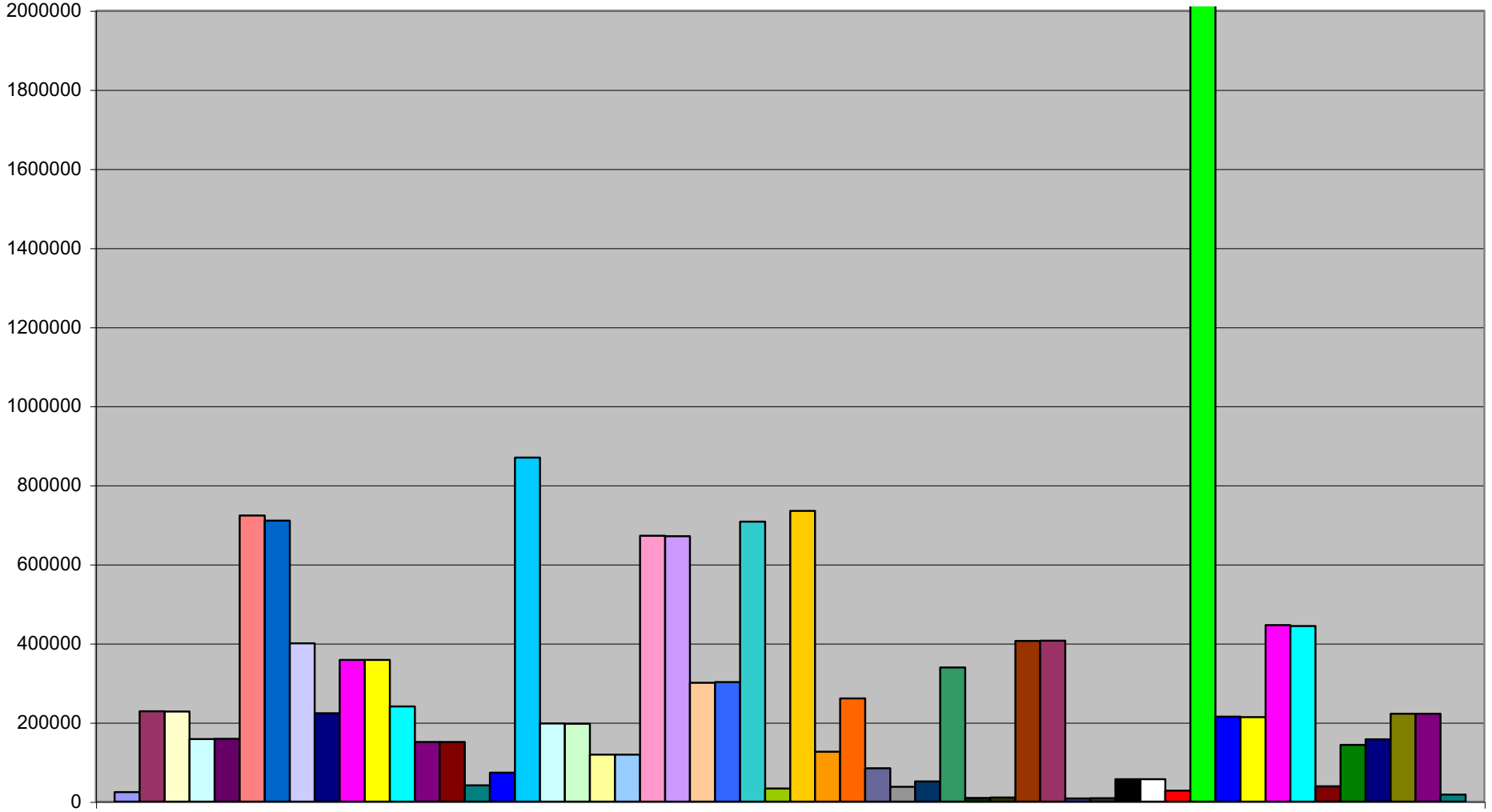
Week 3

Nachi 8/18/03 4:00AM



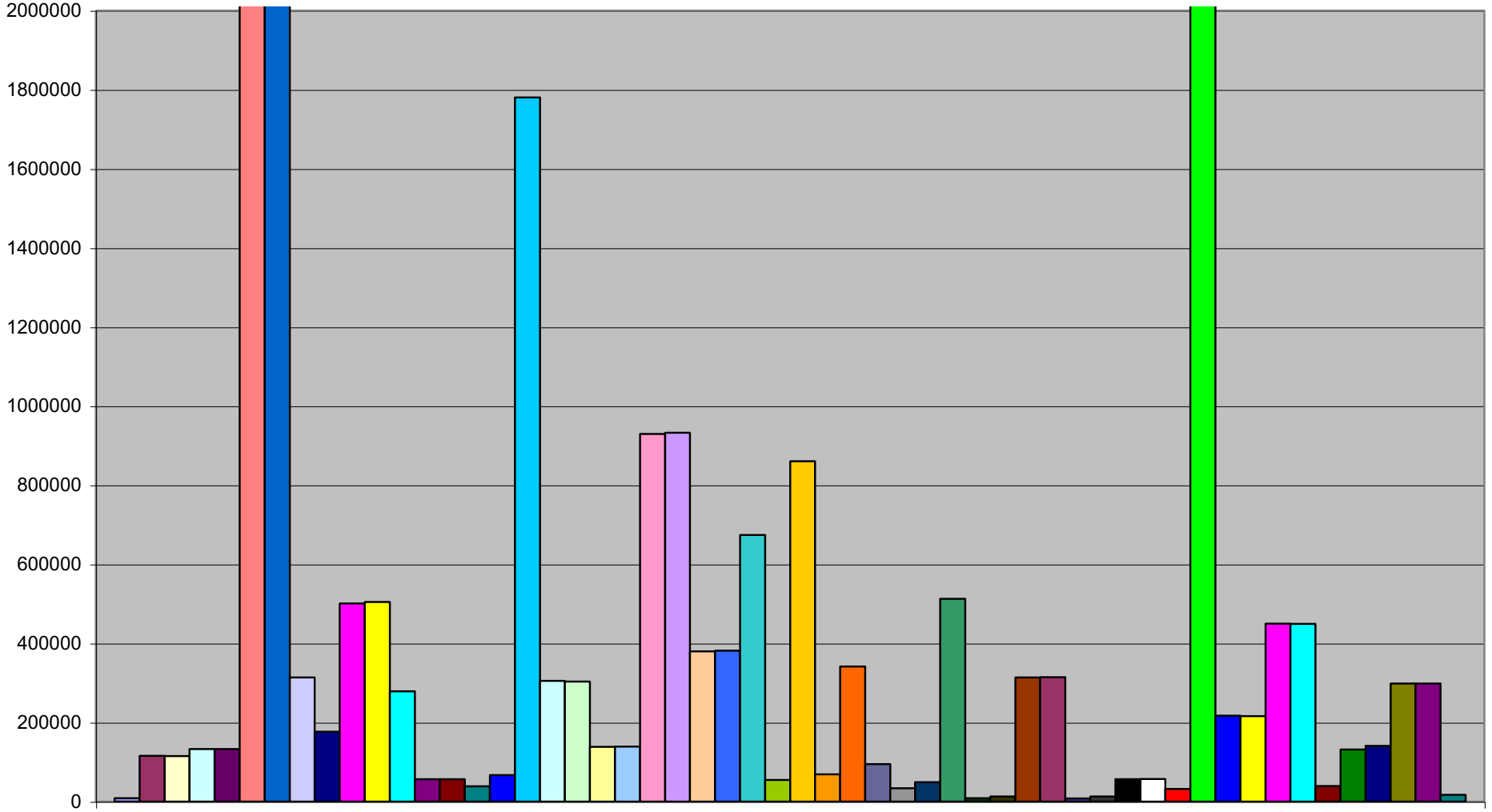
Week 3

Nachi 8/18/03 5:00AM



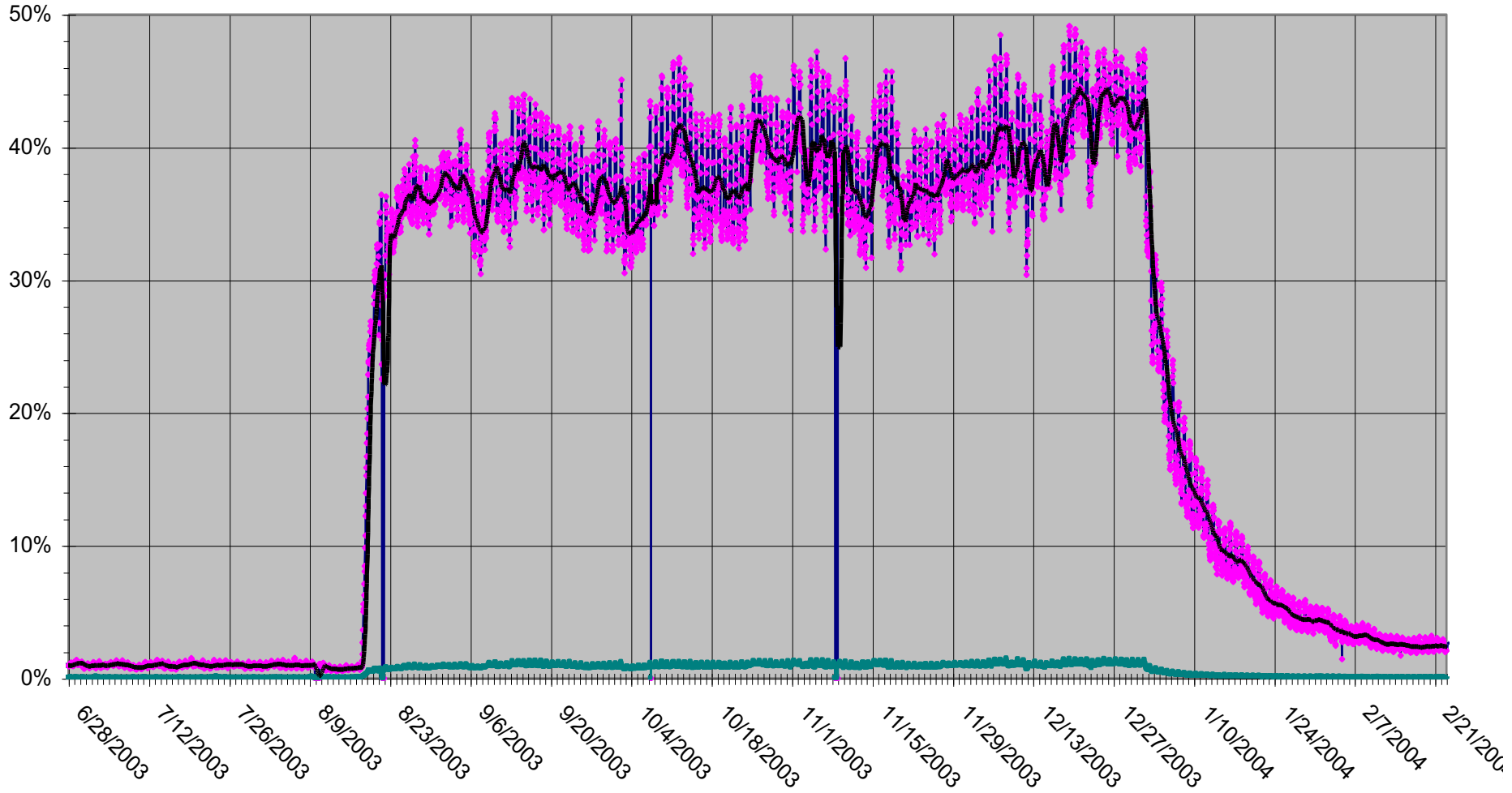
Week 3

Nachi 8/18/03 6:00AM



Week 3

Nachi Worm (08/03 – 01/04)



How are Botnets Used for DDOS Attacks?

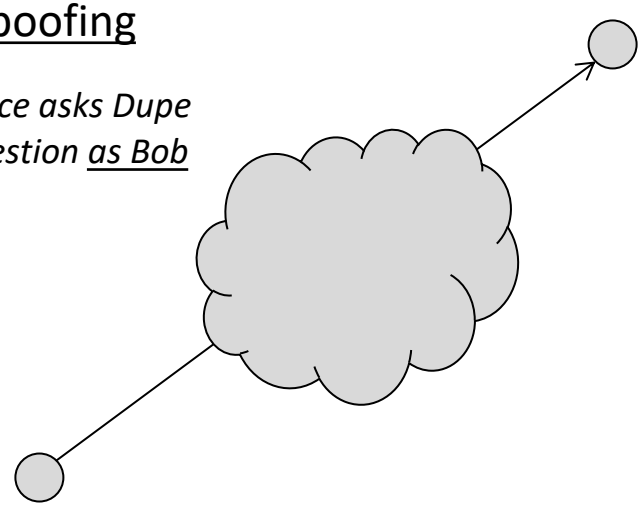
Week 3

Spoofing and Reflection

Typically just change source IP address to Bob

Spoofing

1. Alice asks Dupe a question as Bob



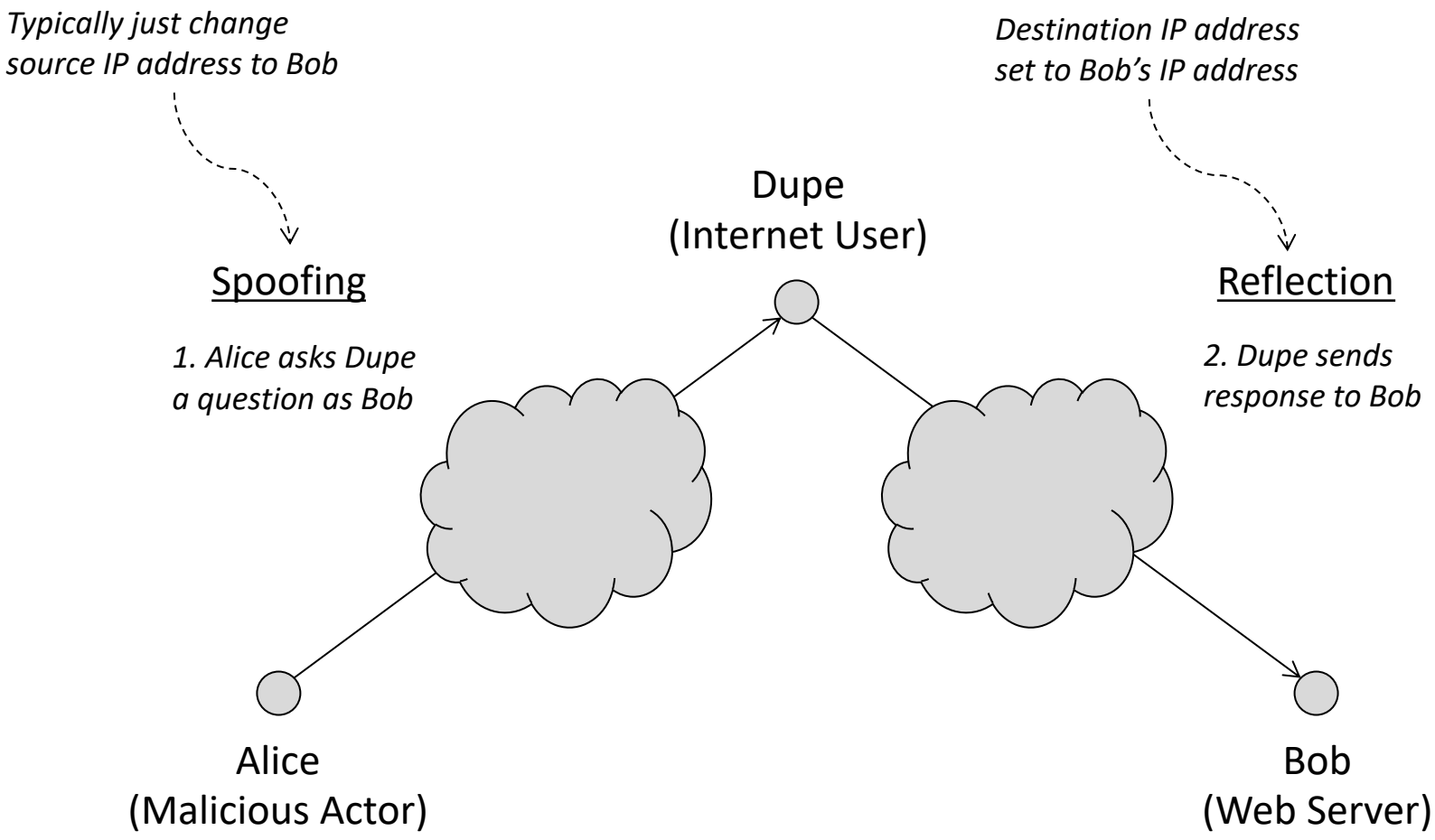
Dupe
(Internet User)

Alice
(Malicious Actor)

Bob
(Web Server)

Week 3

Spoofing and Reflection

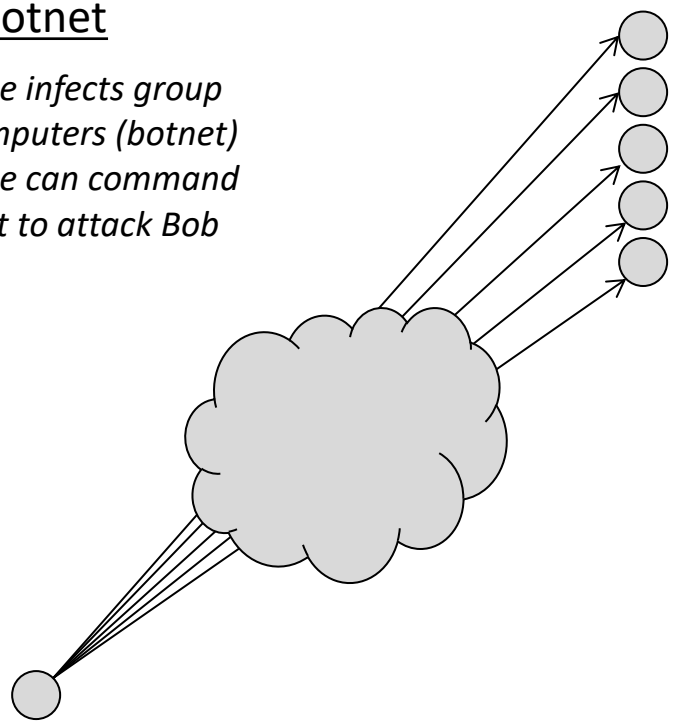


Week 3

Distribution and Amplification

Botnet

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



Alice
(Malicious Actor)

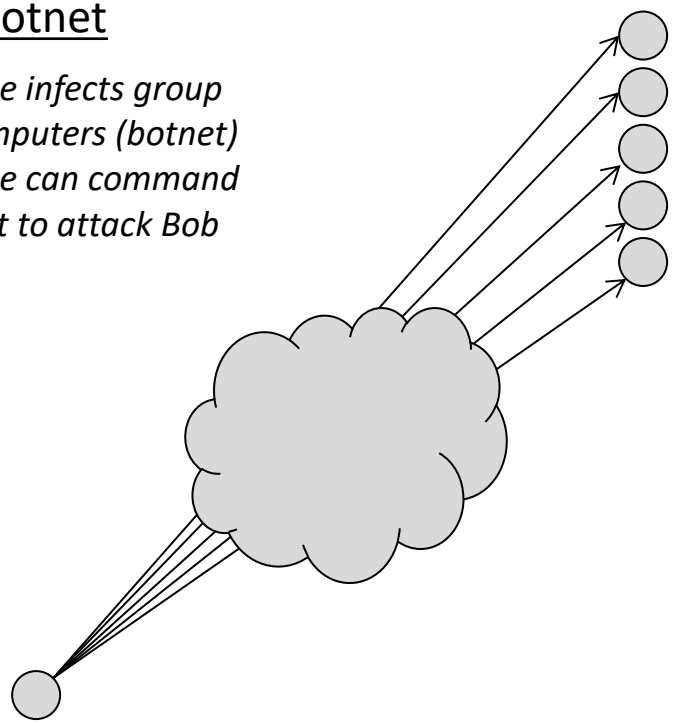
Bob
(Web Server)

Week 3

Distribution and Amplification

Botnet

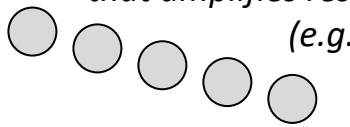
1. Alice infects group of computers (botnet)
2. Alice can command botnet to attack Bob

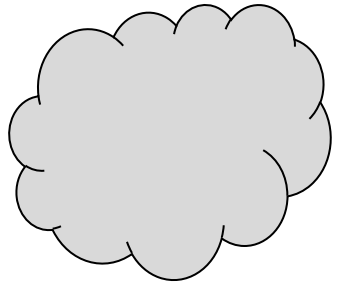


Alice
(Malicious Actor)

Amplifying Service

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

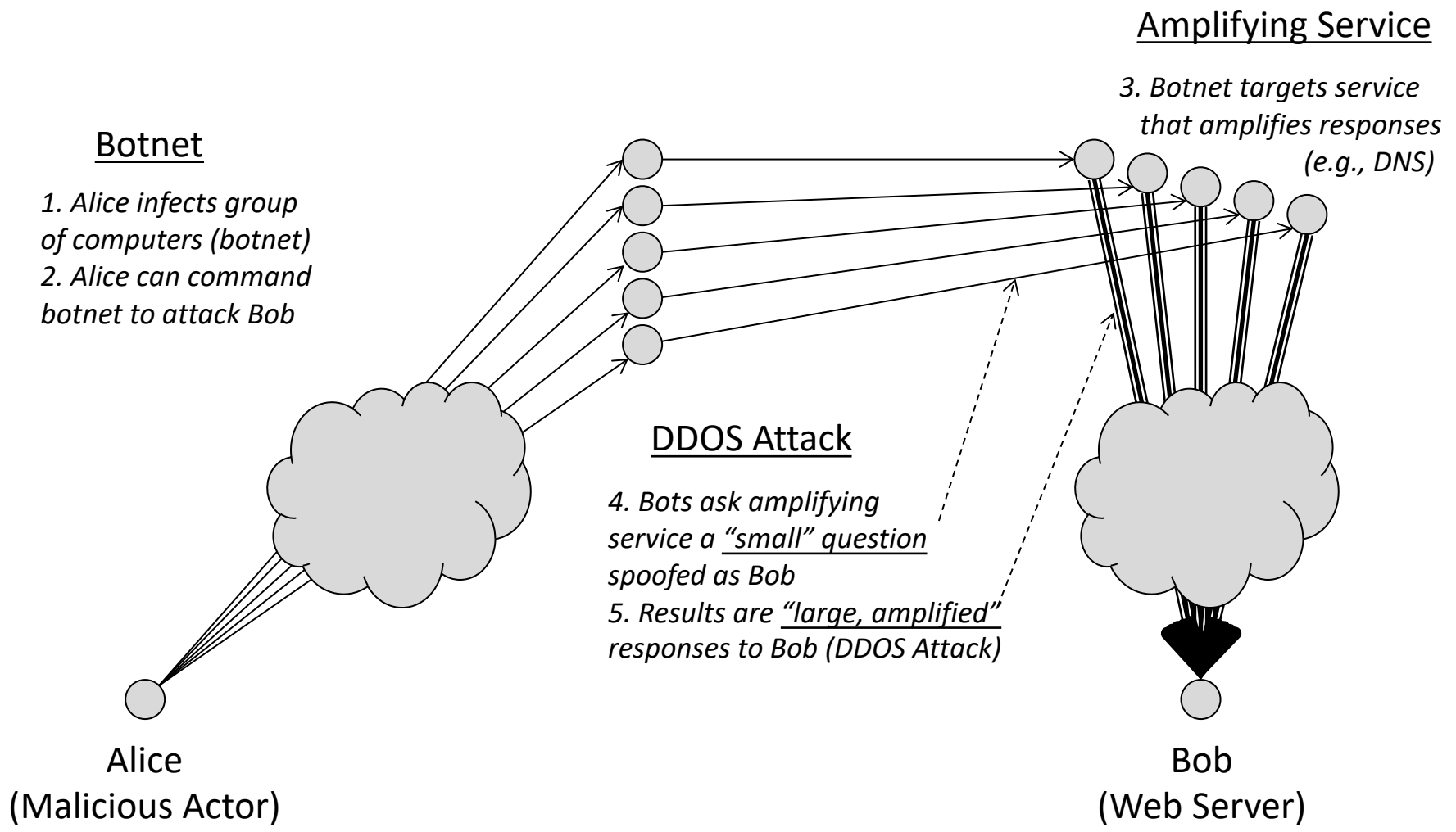




Bob
(Web Server)

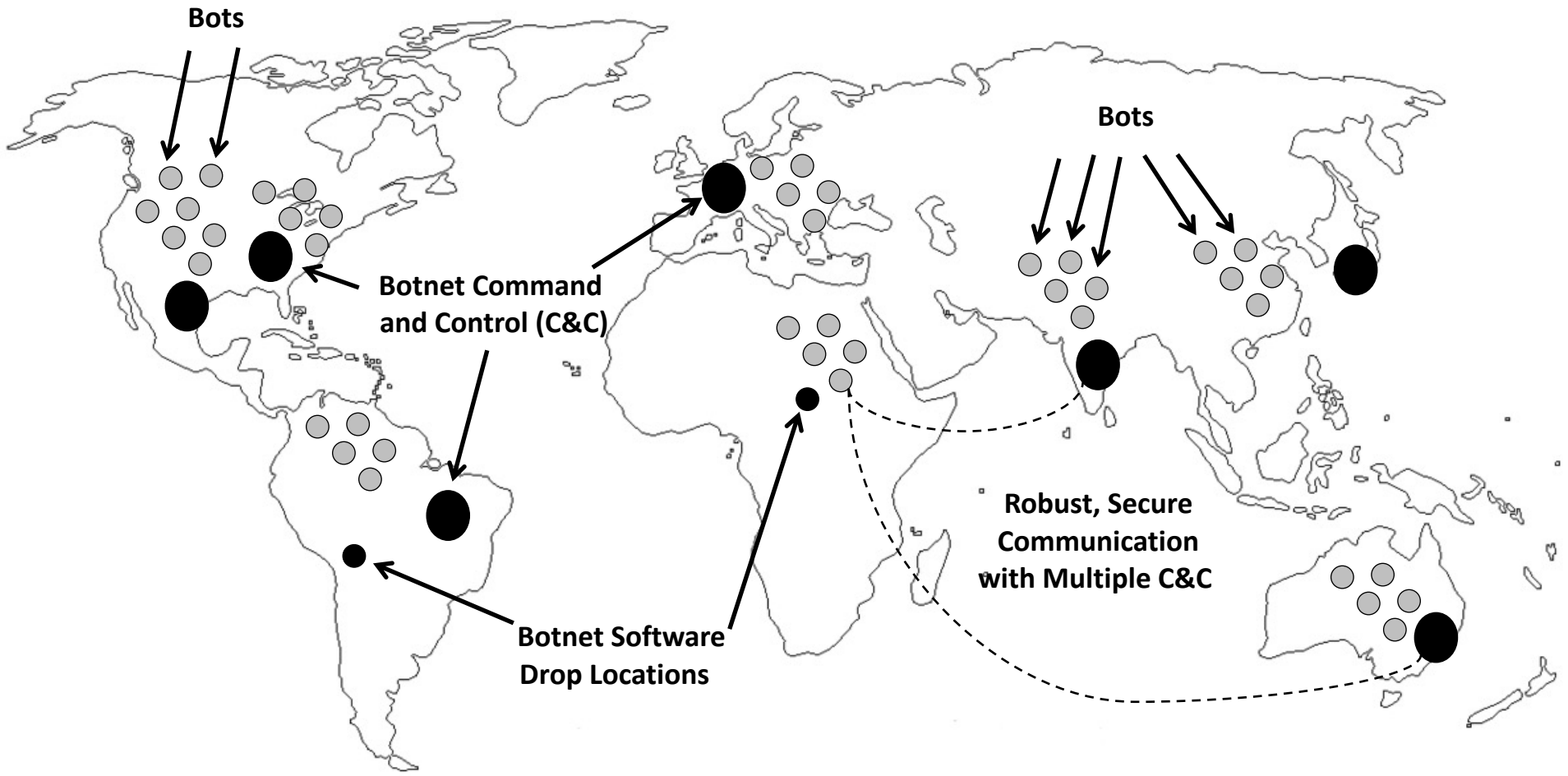
Week 3

Distribution and Amplification



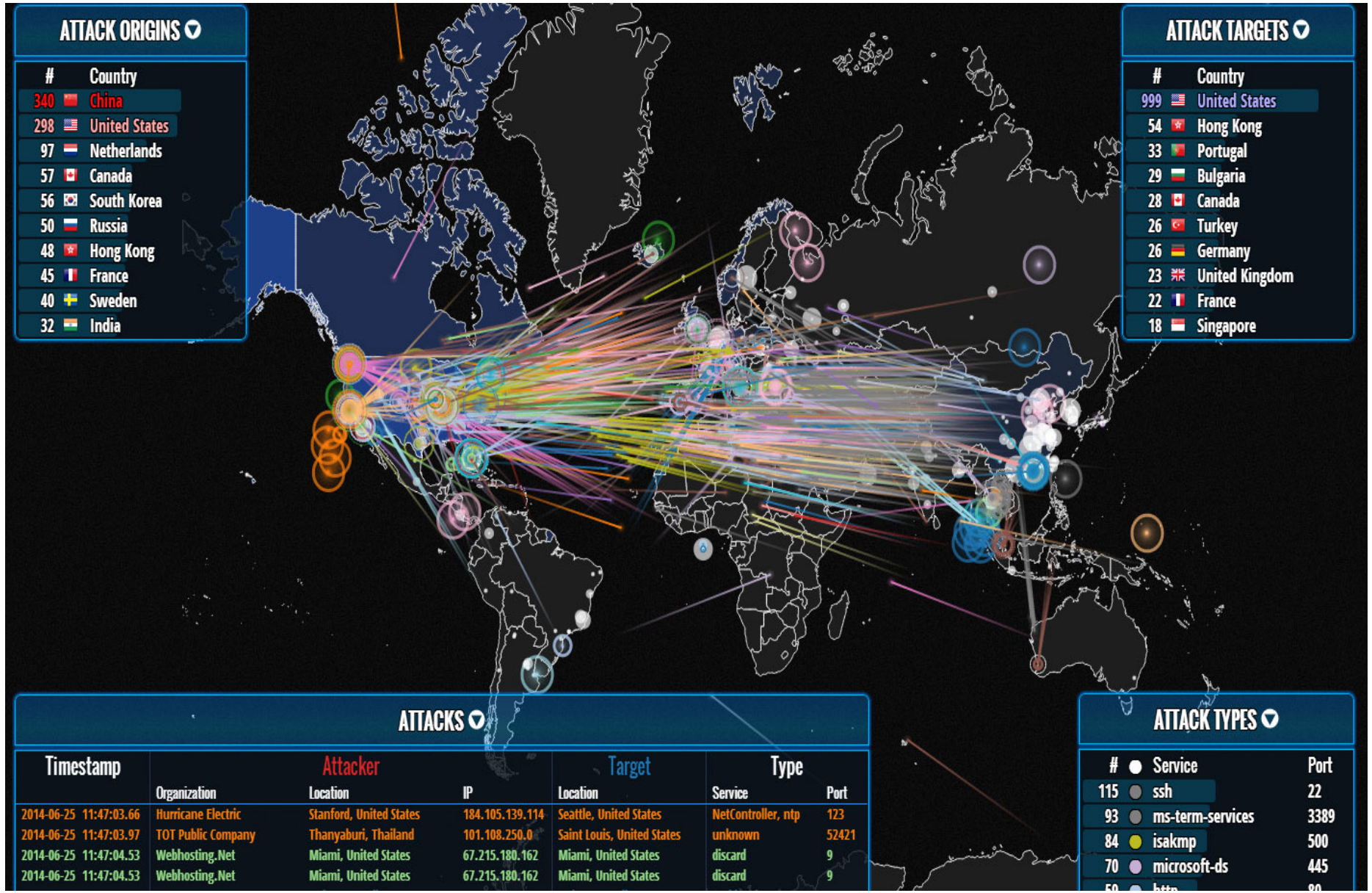
Week 3

Botnets



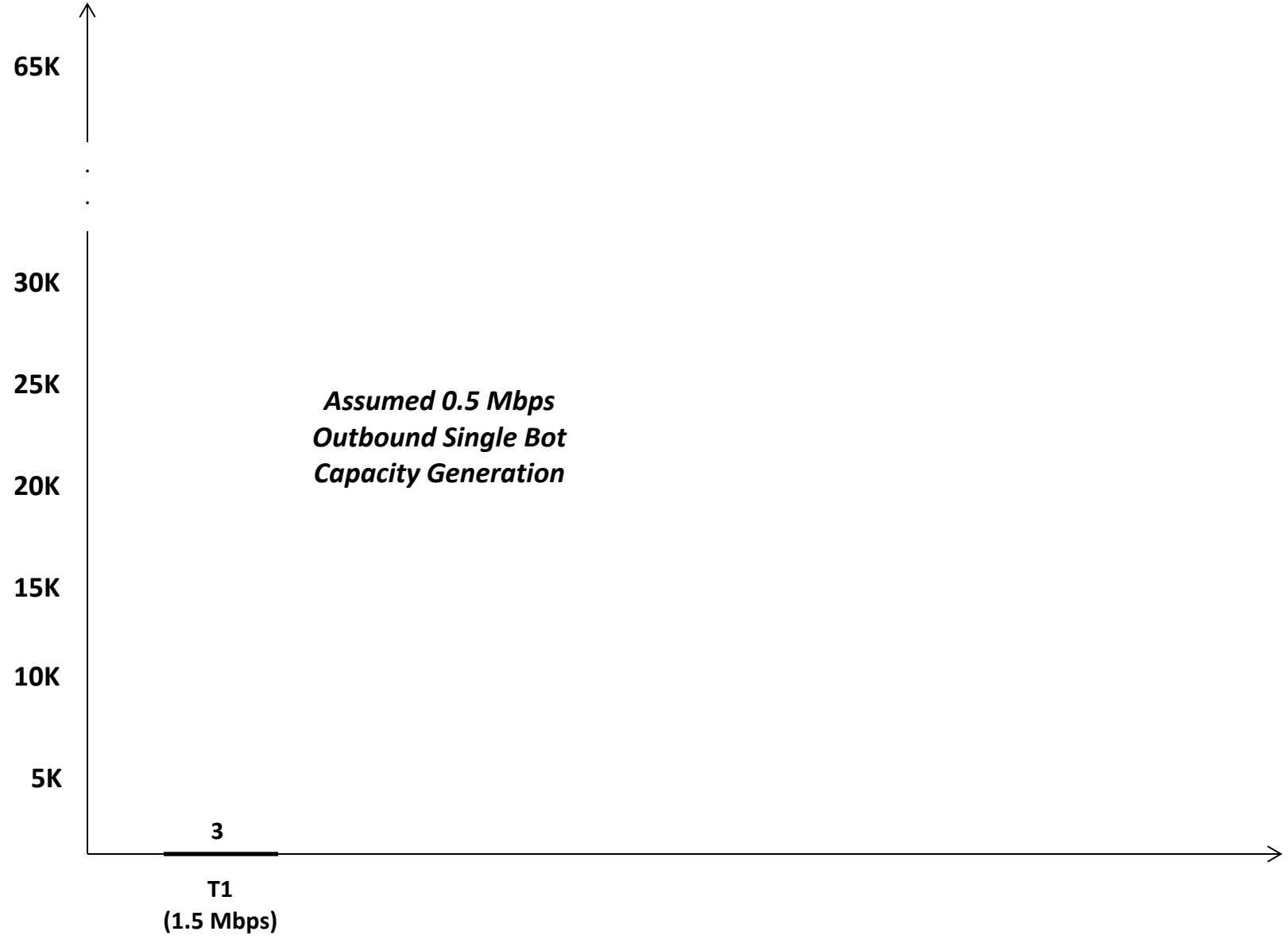
Week 3

Typical Botnet Visualization



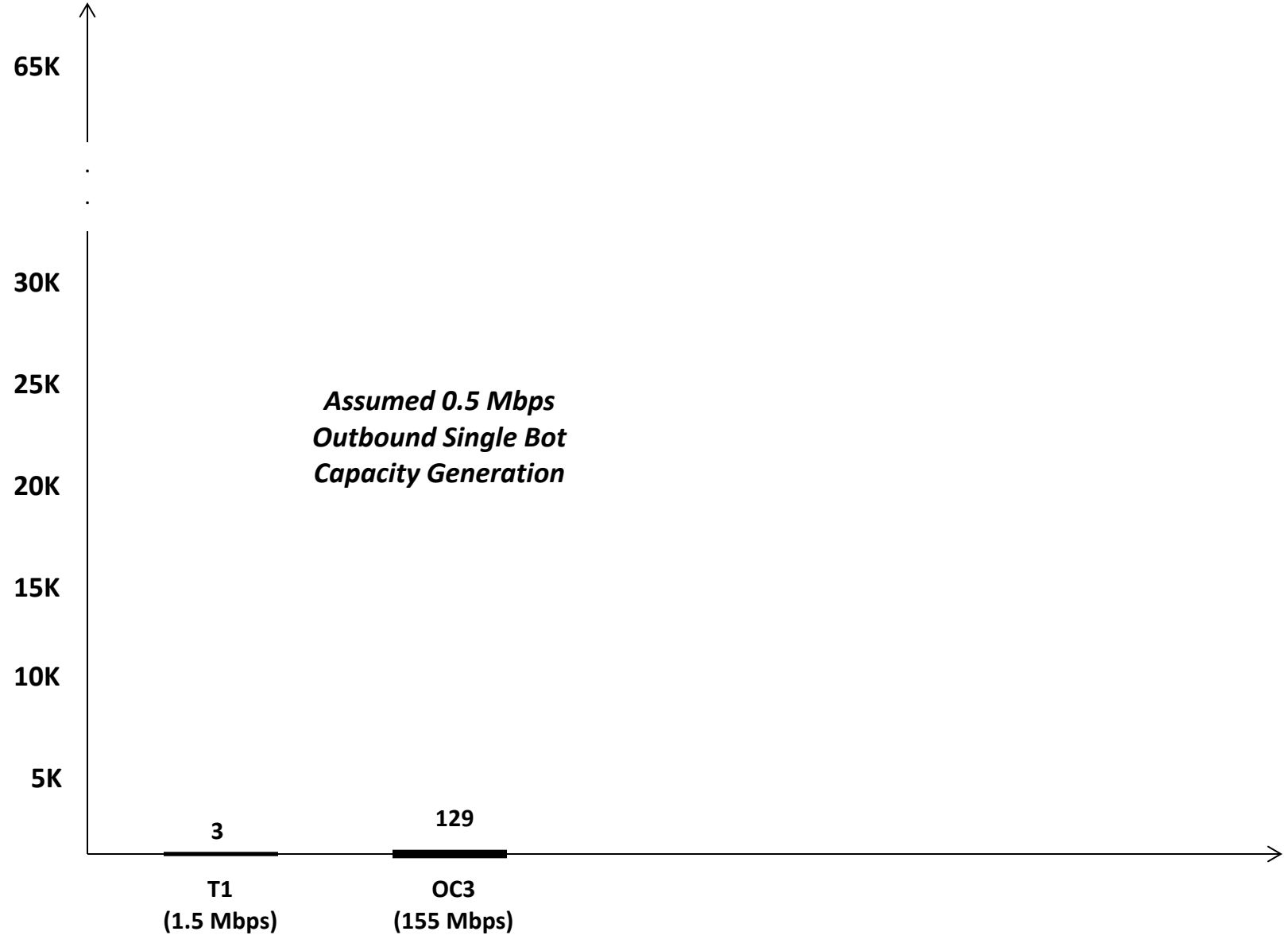
Week 3

Bot Capacity Generation (500Kbps)



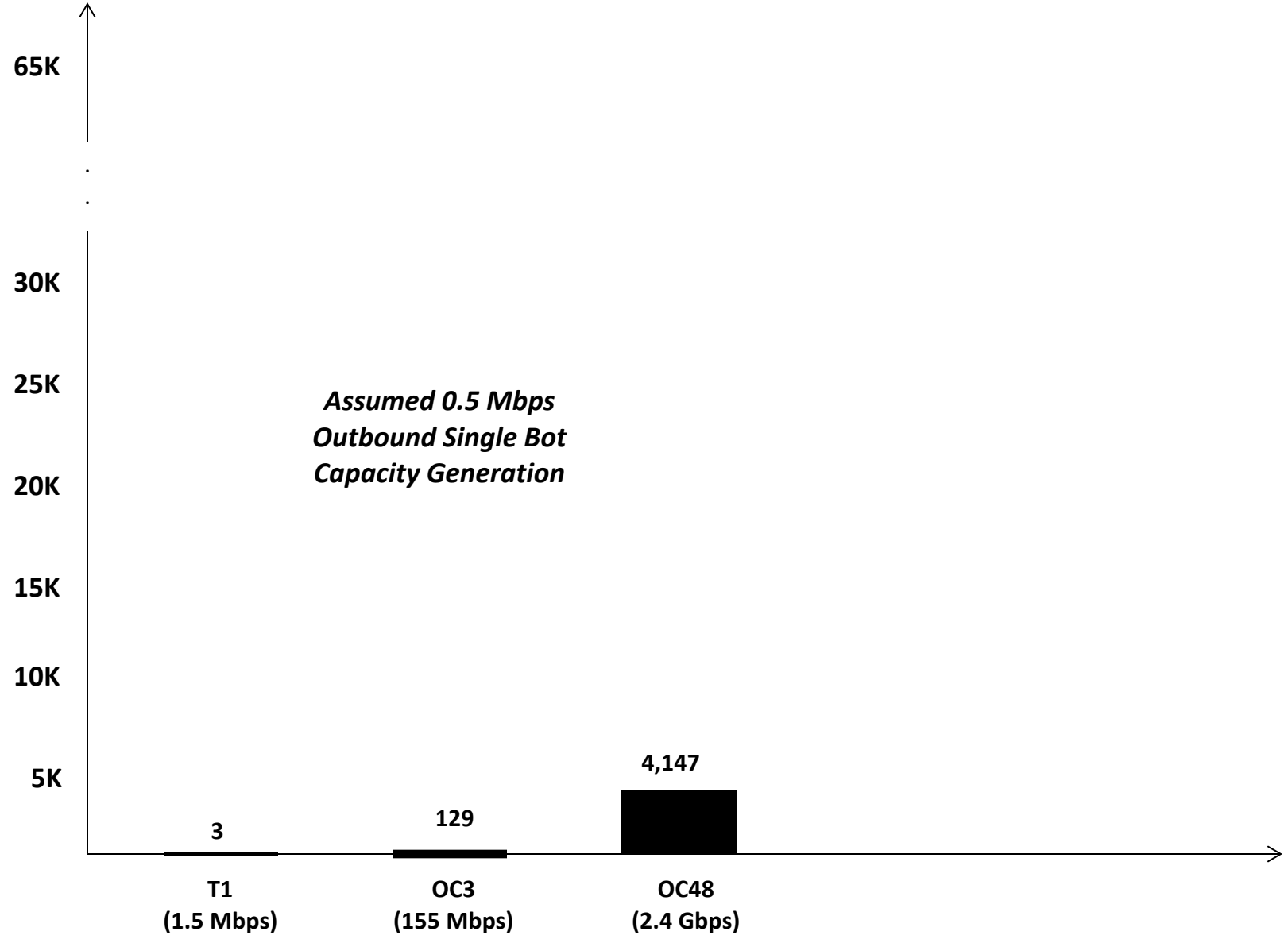
Week 3

Bot Capacity Generation (500Kbps)



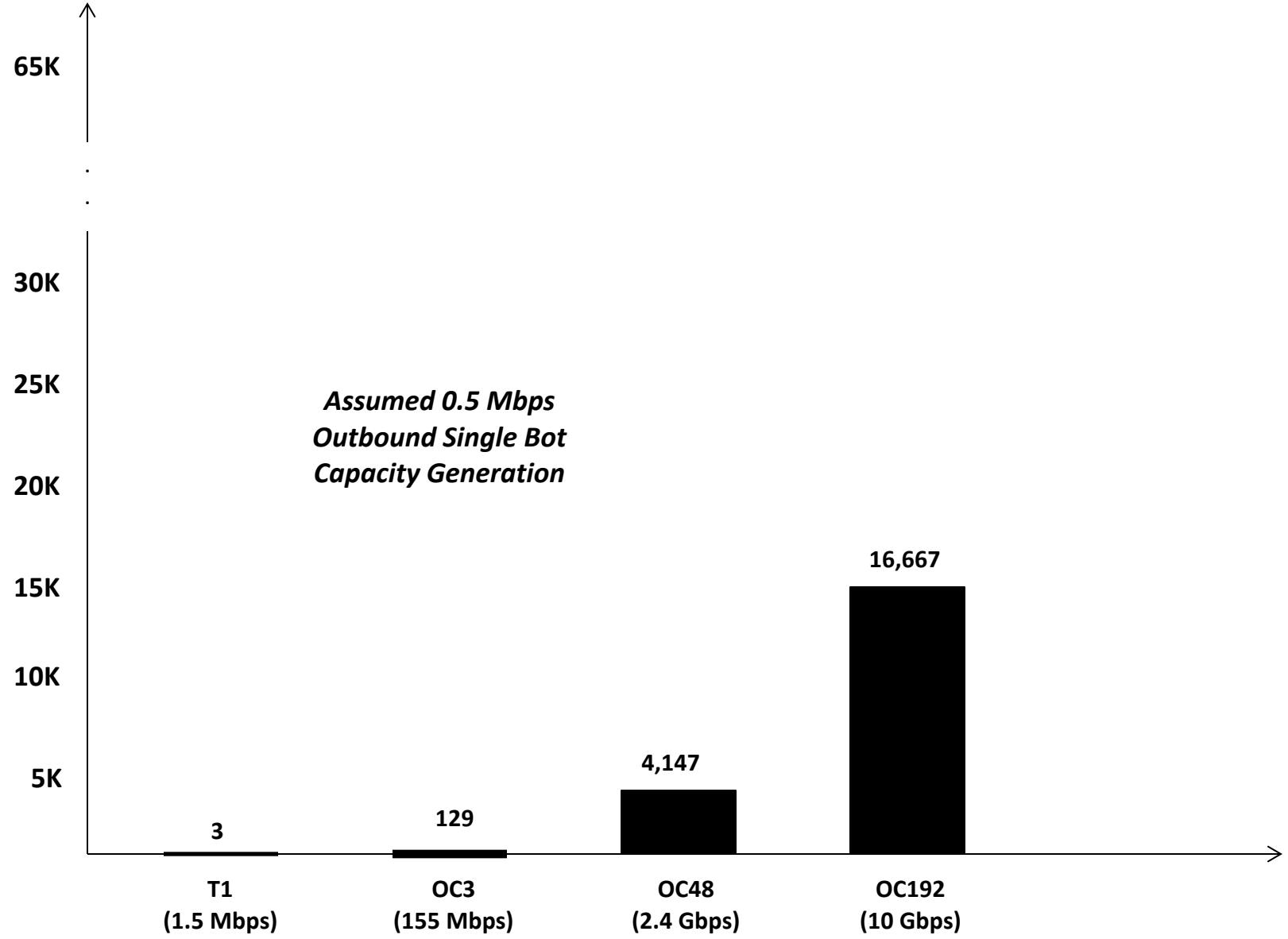
Week 3

Bot Capacity Generation (500Kbps)



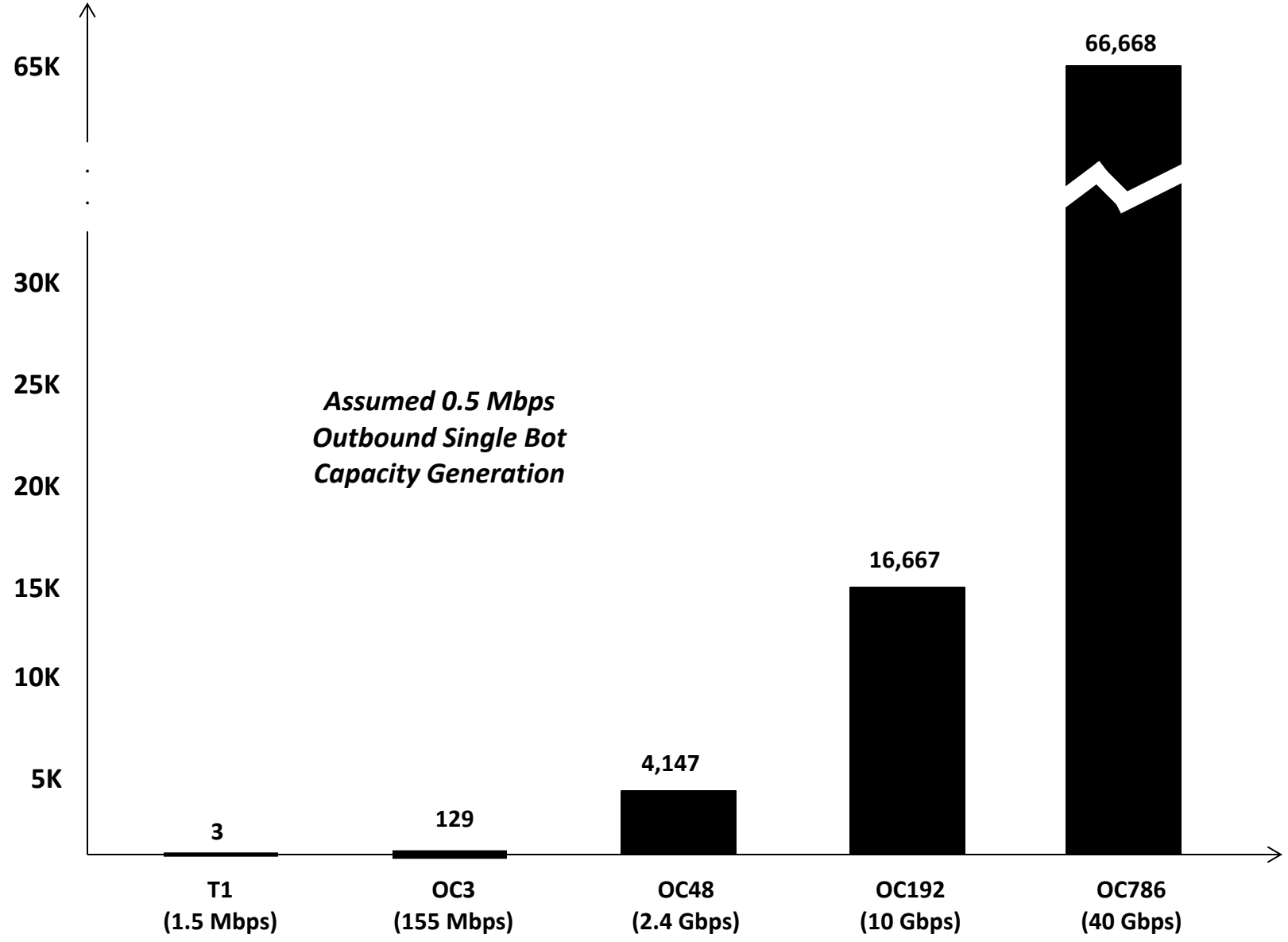
Week 3

Bot Capacity Generation (500Kbps)



Week 3

Bot Capacity Generation (500Kbps)



Week 3

Botnet Capacity Generation (750 Kbps – 1.0 Mbps)

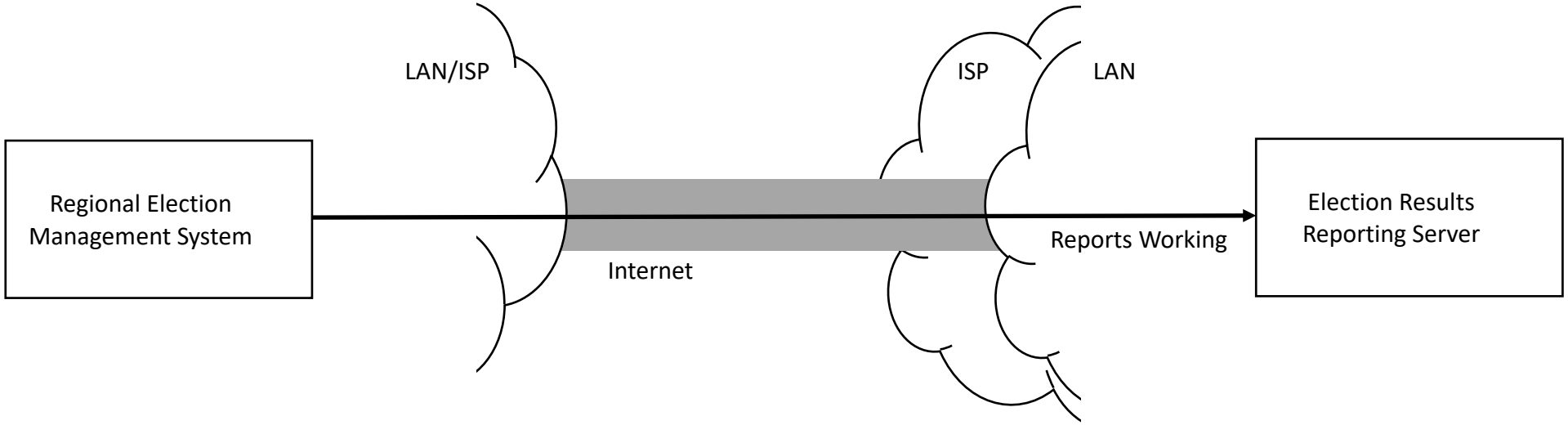
Number of Bots	Outbound Capacity	Size of Attack	Network Size
2	750 Kbps	1.5 Mbps	T1
1,200	1.0 Mbps	1.2 Gbps	OC-24
2,400	1.0 Mbps	2.4 Gbps	OC-48
10,000	1.0 Mbps	10.0 Gbps	OC-192
40,000	1.0 Mbps	40.0 Gbps	OC-768
80,000	1.0 Mbps	80.0 Gbps	
100,000	1.0 Mbps	100 Gbps	*Starts to fill typical ISP backbone*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

Week 3

Can You Stop DDOS Attacks?

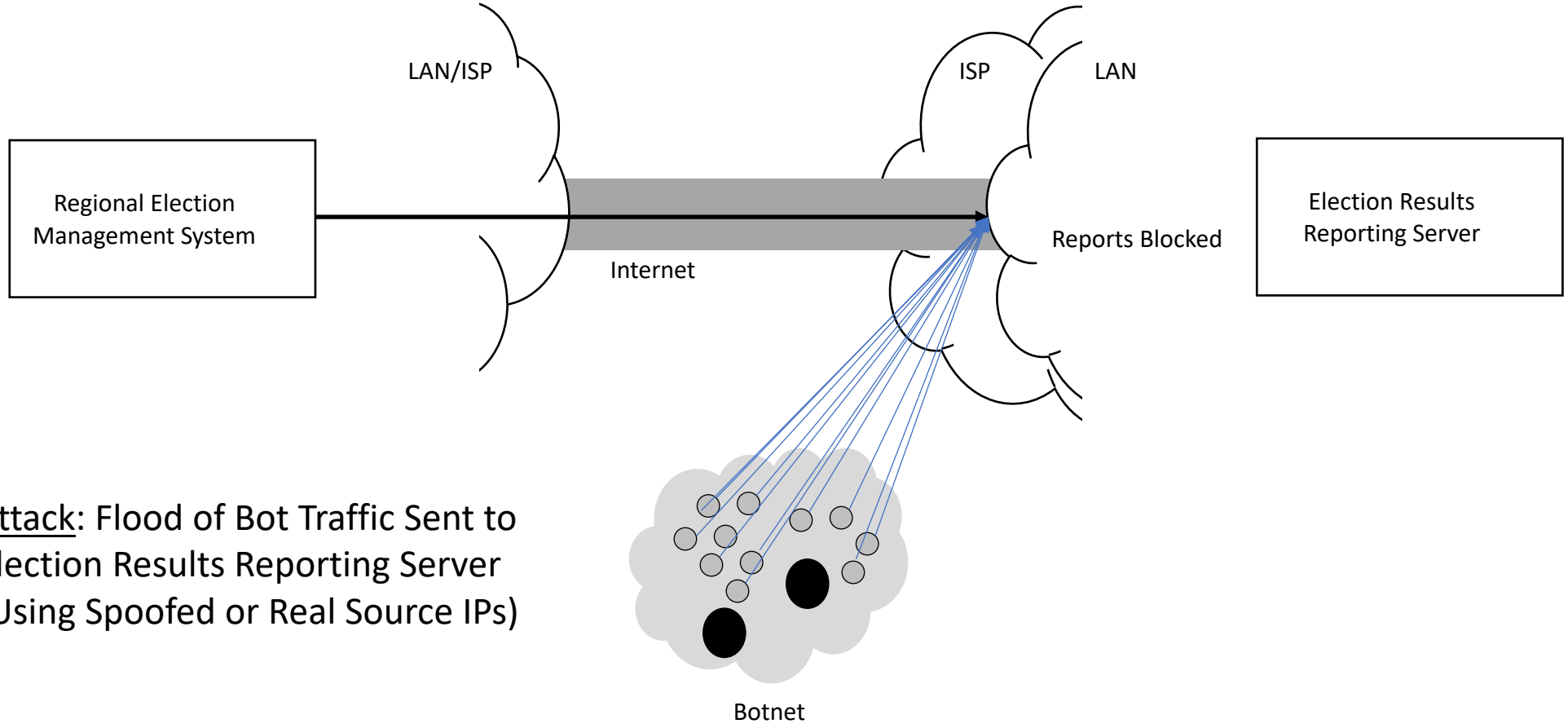
Week 3

Case Study: Mitigating Inbound Election Reporting DDOS



Week 3

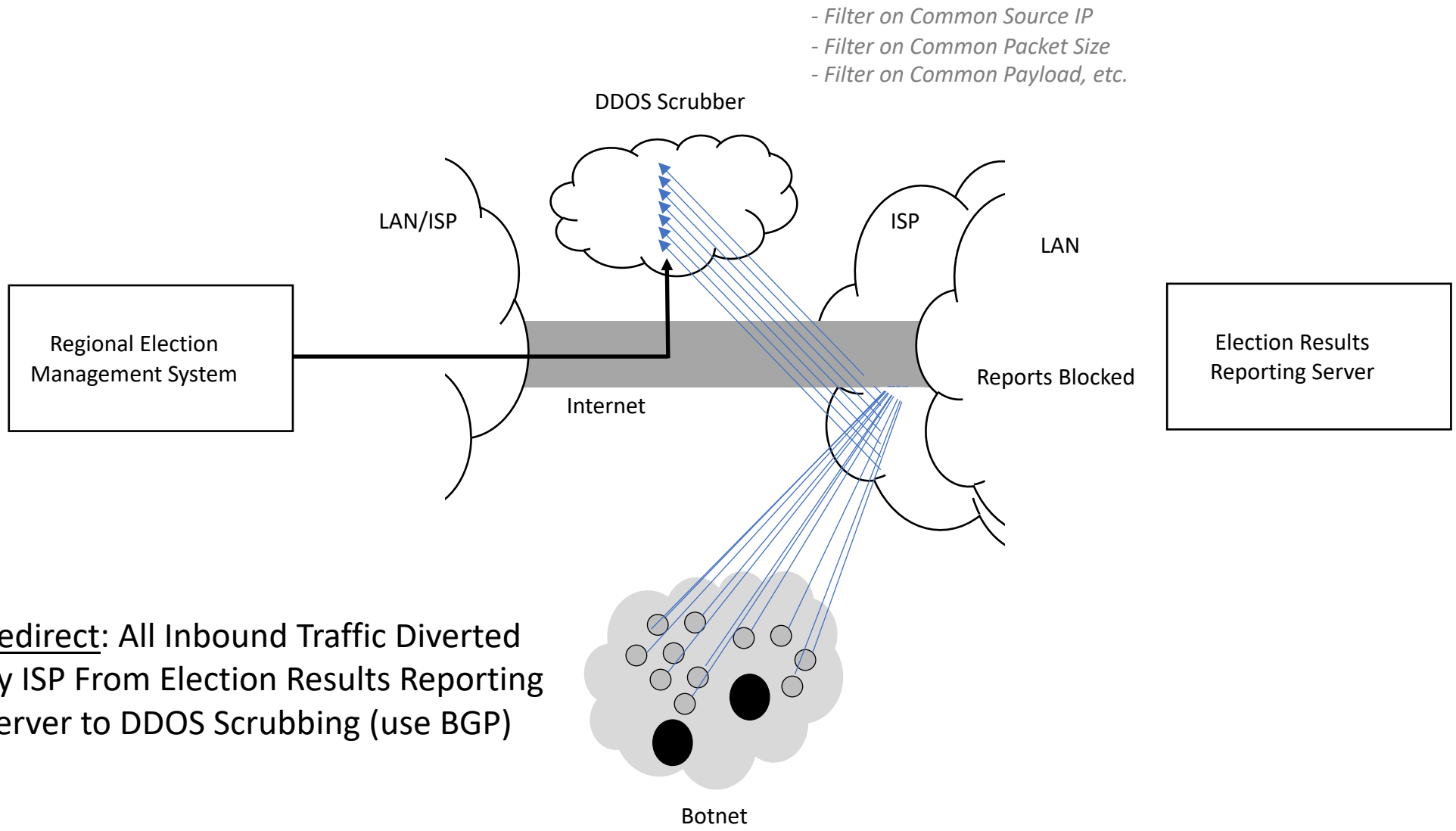
Case Study: Mitigating Inbound Election Reporting DDOS



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

Week 3

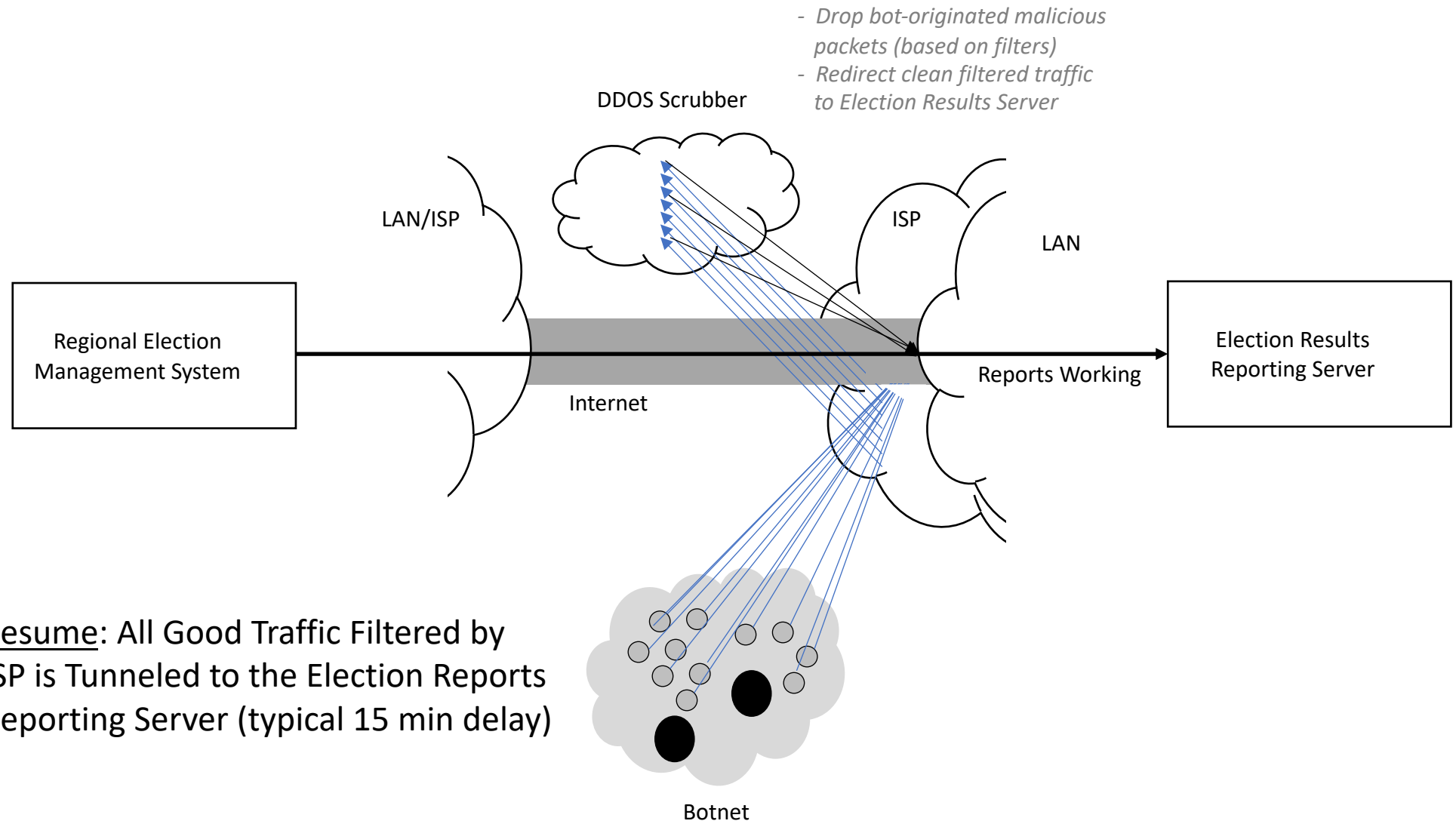
Case Study: Mitigating Inbound Election Reporting DDOS



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)