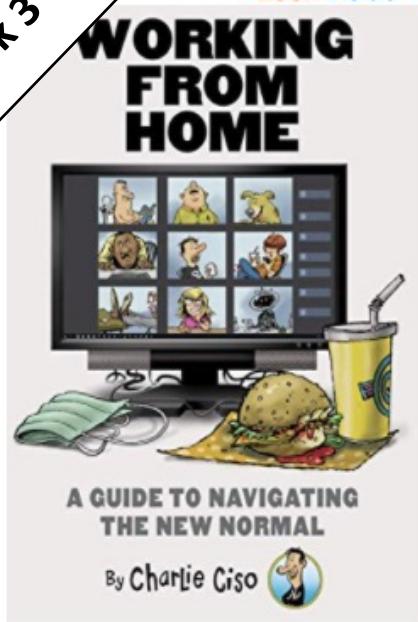




# An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso  
[eamoroso@tag-cyber.com](mailto:eamoroso@tag-cyber.com)

Week 3



Look inside ↓

# 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

# Charlie Ciso

Our VP is three minutes late.  
Should we all click to drop?



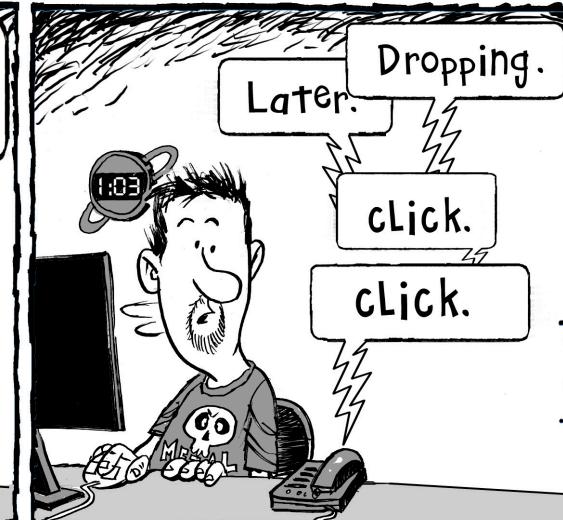
Let's show her the same respect we showed our college professors.



Dropping.  
Later.

Click.  
Click.

Powell/Amoroso



# 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

amazon Try Prime Books ▾ from cia to apt

Departments ▾ Browsing History ▾ Edward's Amazon.com Today's Deals Gift Cards & Registry Sell Help EN Hello, Edward Account & Lists Orders Try Prime Cart 0

Books Advanced Search New Releases NEW! Amazon Charts Best Sellers & More The New York Times® Best Sellers Children's Books Textbooks Textbook Rentals Sell Us Your Books Best Books of the Month

◀ Back to search results for "from cia to apt"

From CIA to APT: An Introduction to Cyber Security and over one million other books are available for Amazon Kindle. Learn more

**From CIA to APT: An Introduction to Cyber Security** Paperback – August 11, 2017  
by Edward G. Amoroso (Author), Matthew E. Amoroso (Author)  
Be the first to review this item

Look inside ↗ See all 2 formats and editions

Kindle \$0.00 kindleunlimited Paperback \$25.00  
This title and over 1 million more available with Kindle Unlimited  
\$9.99 to buy 2 New from \$25.00

Most introductory books on cyber security are either too technical for popular readers, or too casual for professional ones. This book, in contrast, is intended to reside somewhere in the middle. That is, while concepts are explained in a friendly manner for any educated adult, the book also necessarily includes network diagrams with the obligatory references to clouds, servers, and packets. But don't let this scare you. Anyone with an ounce of determination can get through every page of this book, and will come out better informed, not only on cyber security, but also on computing, networking, and software. While it is true that college students will find the material particularly accessible, any adult with the desire to learn will find this book part of an exciting new journey. A great irony is that the dizzying assortment of articles, posts, and books currently available on cyber security makes it difficult to navigate the topic.

Flip to back See all 2 images

Report incorrect product information.

Share Email Facebook Twitter Pinterest

Buy New \$25.00  
Qty: 1 ▾  
FREE Shipping.  
In Stock.  
Ships from and sold by Amazon.com.  
Gift-wrap available.  
 Yes, I want FREE Two-Day Shipping with Amazon Prime  
Add to Cart Turn on 1-Click ordering for this browser  
Want it Wednesday, Aug. 30? Order within 19 hrs 39 mins and choose Two-Day Shipping at checkout. Details  
Ship to:  
Edward Amoroso- Sparta - 07871 ▾

## 2021 TAG CYBER SECURITY QUARTERLY

**A PROPOSED BIDEN DOCTRINE FOR CYBER**  
EDWARD AMOROSO

This article first appeared on the TAG Cyber website in late November 2020 as the results of the 2020 election were becoming clear. The advice and guidance remain 100% relevant today in early 2021.

The first mistake the US federal government has made in cyber security since 2000 has been its misplaced belief in a collective defense or offense. The truth is, however, that the best defense is a good offense. The problem is that preventing attacks is much harder than breaking into systems – hence the twisted emphasis.

It's time to leave cyber offense to US Cyber Command and to refocus 100% of our collective energies on improving our nation's defenses through distribution, virtualization, and simplification. This is best done locally, not nationally. After all, the place that will win our elections to be local and distributed. When it comes to cyber defense – we must think local.

The second mistake we have made in cyber has been our over-reliance on the effectiveness of information sharing. Certainly, good threat intelligence is important – and excellent commercial platforms exist. But this belief that a big-group-hug with our international allies will stop cyber threats is both immature and incorrect.

The third and most serious mistake we have made as a nation in cyber involves our private requests (Obama) and public coping (Trump) that the Russians and Chinese should please stop attacking our infrastructure. Asking your adversary to stop hacking is like calling the clouds to stop raining. This approach does not work.

It amazes me that more experts in our field do not see the folly in this strategy. Imagine the misguided CEO wandering into the board room to explain that the new risk reduction plan is to plead with the bad guys to stop hacking. Any CEO taking this approach would be out of work quickly. And yet, we do this every day on a national level.

My advice instead to the incoming administration would be to create a new strategy – a Biden Doctrine for Cyber, if you will. Such a strategy would boldly establish the following goal: To implement a massively centralized monitoring system that can detect and respond to coordinated teams that is so effective as to render attacks from adversaries obsolete. Here's how to do it:

First, we should immediately refine any new investment in overlay security programs such as Einstein 2. This centralized monitoring system was conceived twenty years ago and has been about as useful as

2021 SECURITY ANNUAL - 1ST QUARTER TAG CYBER

### 2021 TAG Cyber Security Quarterly Report

Insights, Perspectives, and Commentary on Cyber Risks, Security Safeguards, and Technology Innovations

DOWNLOAD REPORT - 1ST QUARTER 2021

Required Additional Reading: <https://www.tag-cyber.com/advisory/quar>terly

## **Required Week Three Readings:**

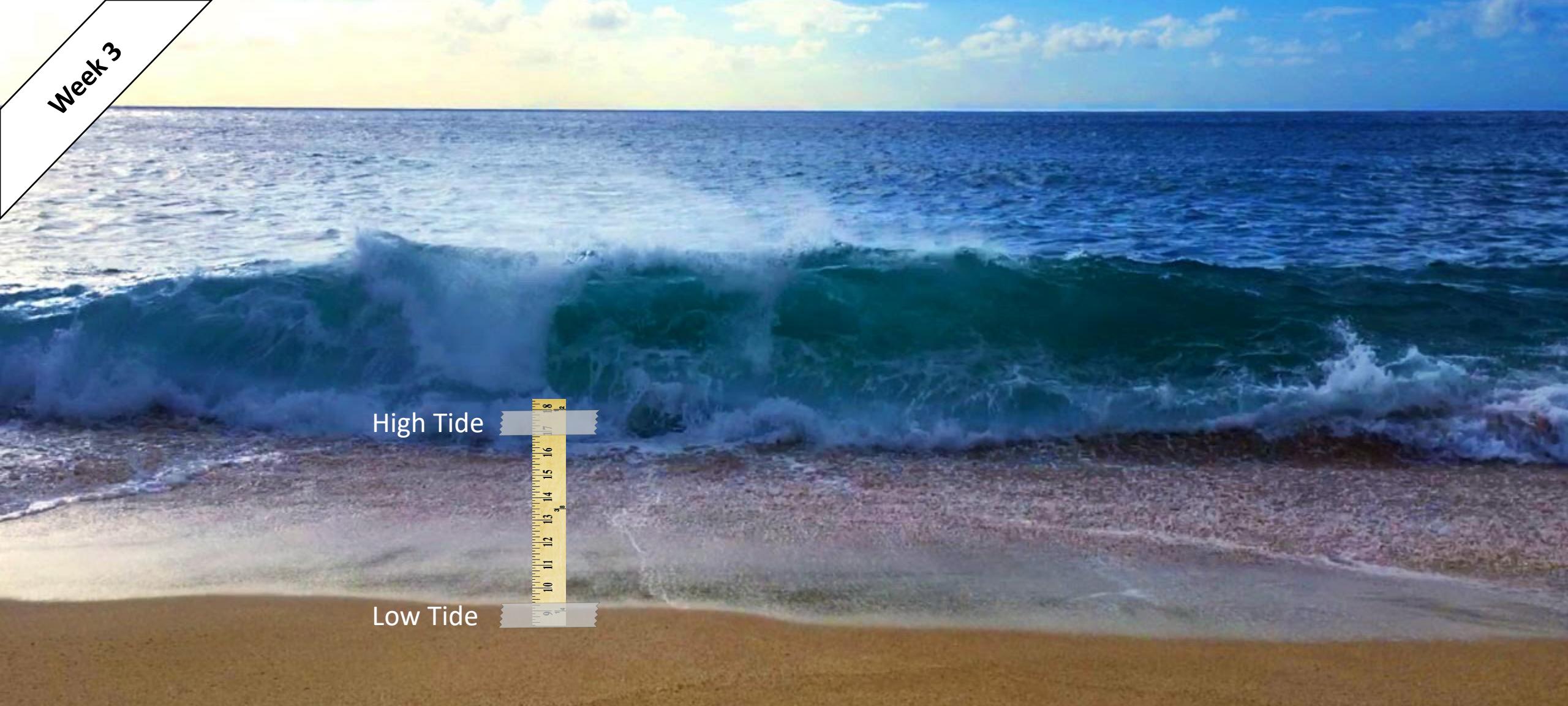
### **1. “The Birth and Death of the Orange Book,” Steve Lipner**

<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



## Week 3: Network Security Threats

# What Are Some Classic Cyber Attack Approaches?

Week 3

# 2600

GET THE  
.PDF

Magazine

Radio



MM/DD/YY	UTC	DISPATCH	
09.20.21	0628	!	LOST AUDIO POSTED FOR
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 ST
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



The Hacker Quarterly

NOW ON STANDS!

Current issue: SUMMER 2021

Digital Editions



res

Events

2600 Store

2

Search 2600



## Original Hacking Journal

### Stage 1: IFS Variable

- Set IFS variable to include '/'
- "/etc/file" same as "etc file"

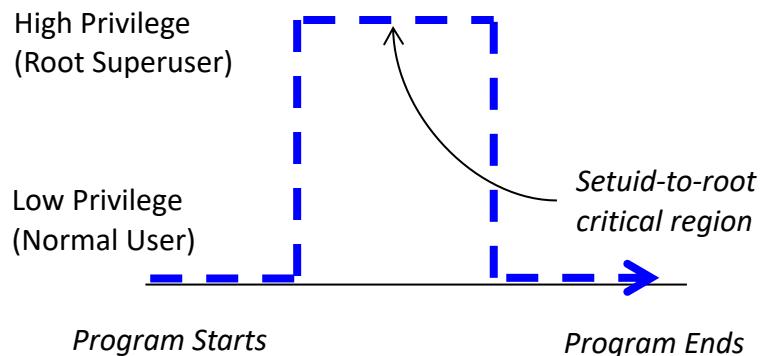
# Classic Unix Kernel Attack

### 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

**Stage 1: IFS Variable**

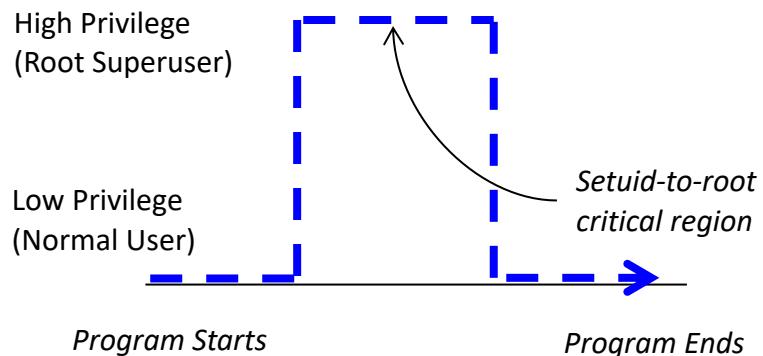
- Set IFS variable to include ‘/’
- “/etc/file” same as “etc file”

**Stage 3: Notice Source Code in “At” Program**

- Program has setuid-to-root critical region
- Region includes “exec /etc/protect/file”

**Stage 2: Find setuid-to-root program**

- Allows increase in privilege
- Normal user to Unix “Root”



# Classic Unix Kernel Attack

**Stage 1: IFS Variable**

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

**Stage 2: Find setuid-to-root program**

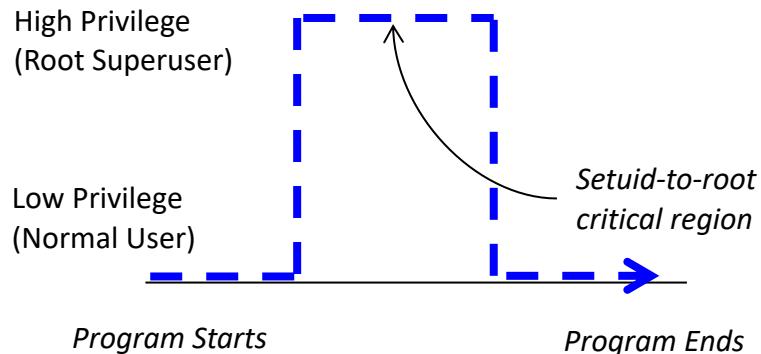
- Allows increase in privilege
- Normal user to Unix “Root”

**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



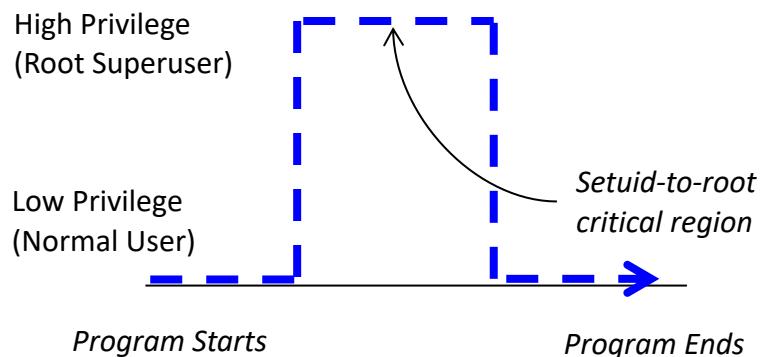
# Classic Unix Kernel Attack

**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”

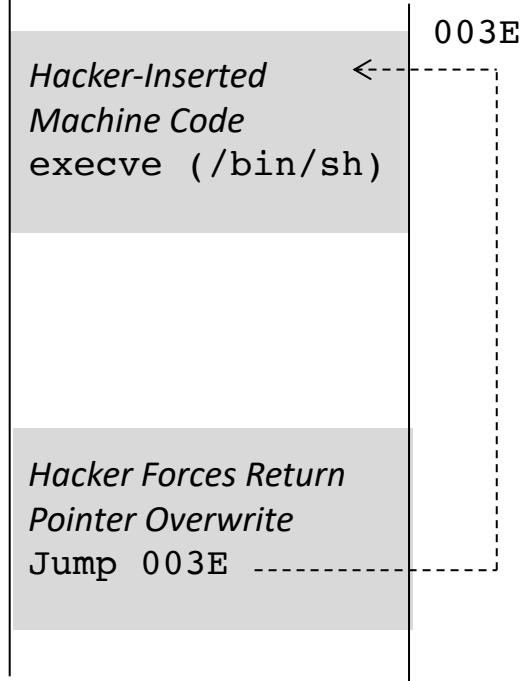
**Stage 4: Unix Shell Program**

- 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 copy /bin/sh to myshell
- Step 3: Run “at” program
- Result: myshell is root shell owed by me!

# Classic Unix Kernel Attack



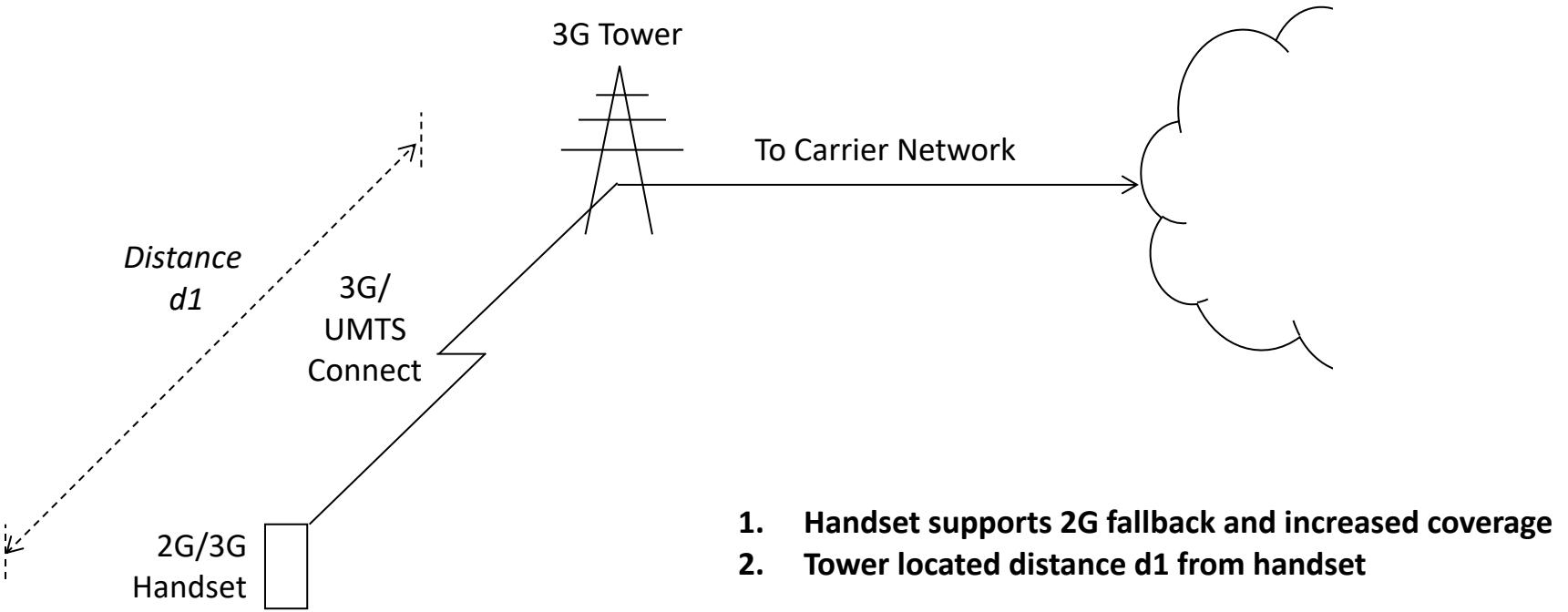
```
void overflow_function(char *string)
{
    char buffer[16];
    strcpy(buffer, string);
    return;
}

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

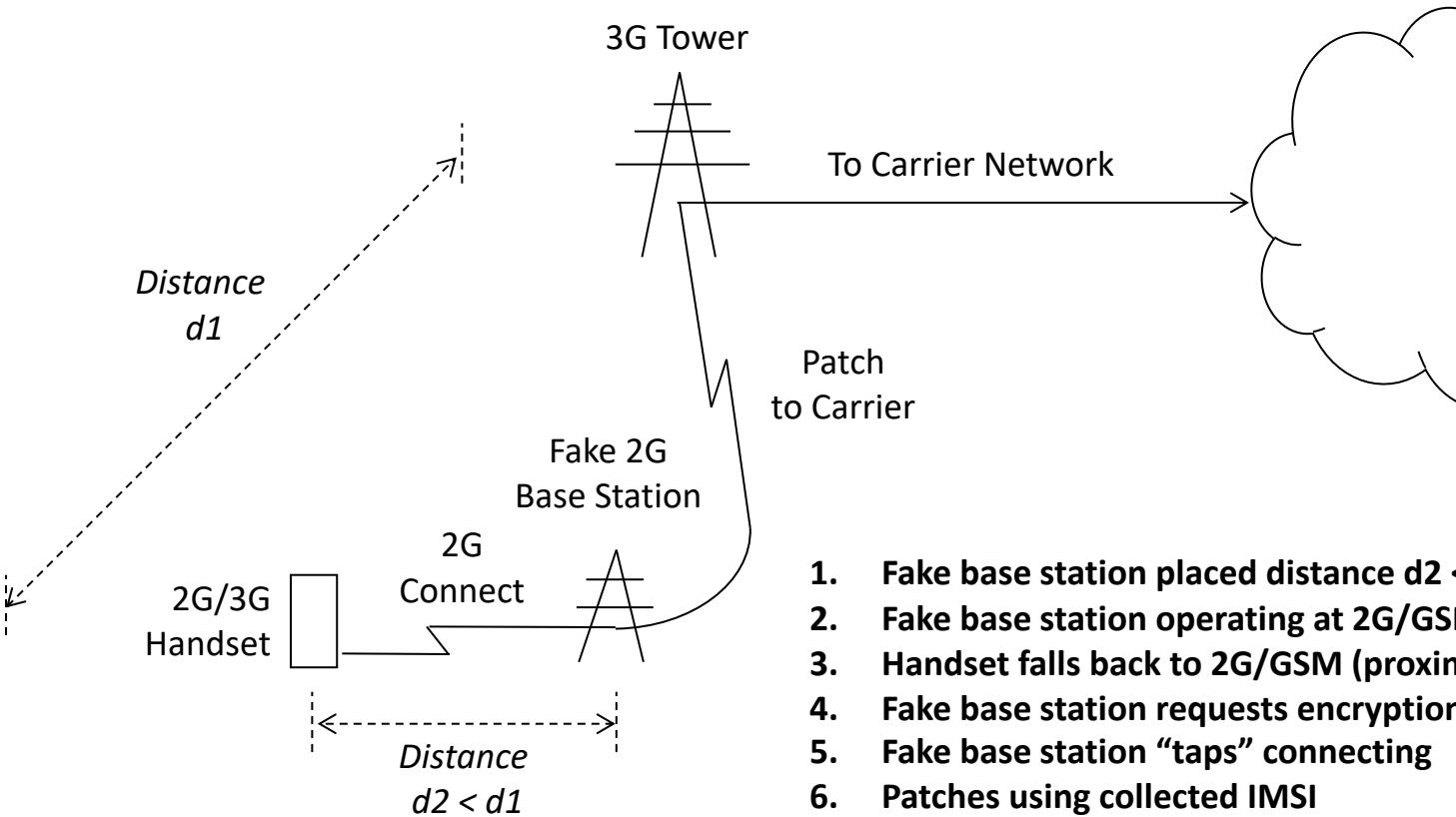
    for(i=0; i<255; i++)
        large_buffer[i]='A';

    overflow_function(large_buffer);
}
```

## Classic Buffer Overflow Attack Code



## Classic 3G Mobile Intercept Attack (Fake Base Station)



1. **Fake base station placed distance  $d_2 < d_1$  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)

## Limited time offer: Buy one month, get one FREE!

Get one month of Cybrary Insider Pro and we'll add another to your account for free. Offer ends September 23rd.

Discount automatically applied at checkout

CYBRARY STUDY GUIDE

# Prepare Yourself to Pass the Certified Ethical Hacker Exam

Ready to ace your ethical hacking certification exam? You've come to the right place. This comprehensive, 300+ question study guide will equip you with all of the required knowledge to be successful on the certification exam. You'll review important topics such as the elements of security, testing methodologies and various attacks. Begin reviewing with this free resource today. Want more depth? Take Cybrary's [ethical hacking training](#).

## Cybrary Ethical Hacker Program

[Train and Certify](#)[Manage Your Team](#)[Resources](#)[Focus Areas](#)[Get Involved](#)[About](#)[Home > Courses](#)

# Cybersecurity Courses & Certifications

Not sure where to start?

[View the Training Roadmap](#)

## SANS Ethical Hacker Program

**INFOSEC  
INSTITUTE**

COURSES ▾ LIVE ONLINE IT TEAM TRAINING ▾ SECURITYIQ ▾ COMPANY ▾ **MY INFOSEC**

# Ethical Hacking Boot Camp - CEH v9 Training

Our most popular information security and hacking training goes in-depth into the techniques used by malicious, black hat hackers with attention getting lectures and hands-on lab exercises.

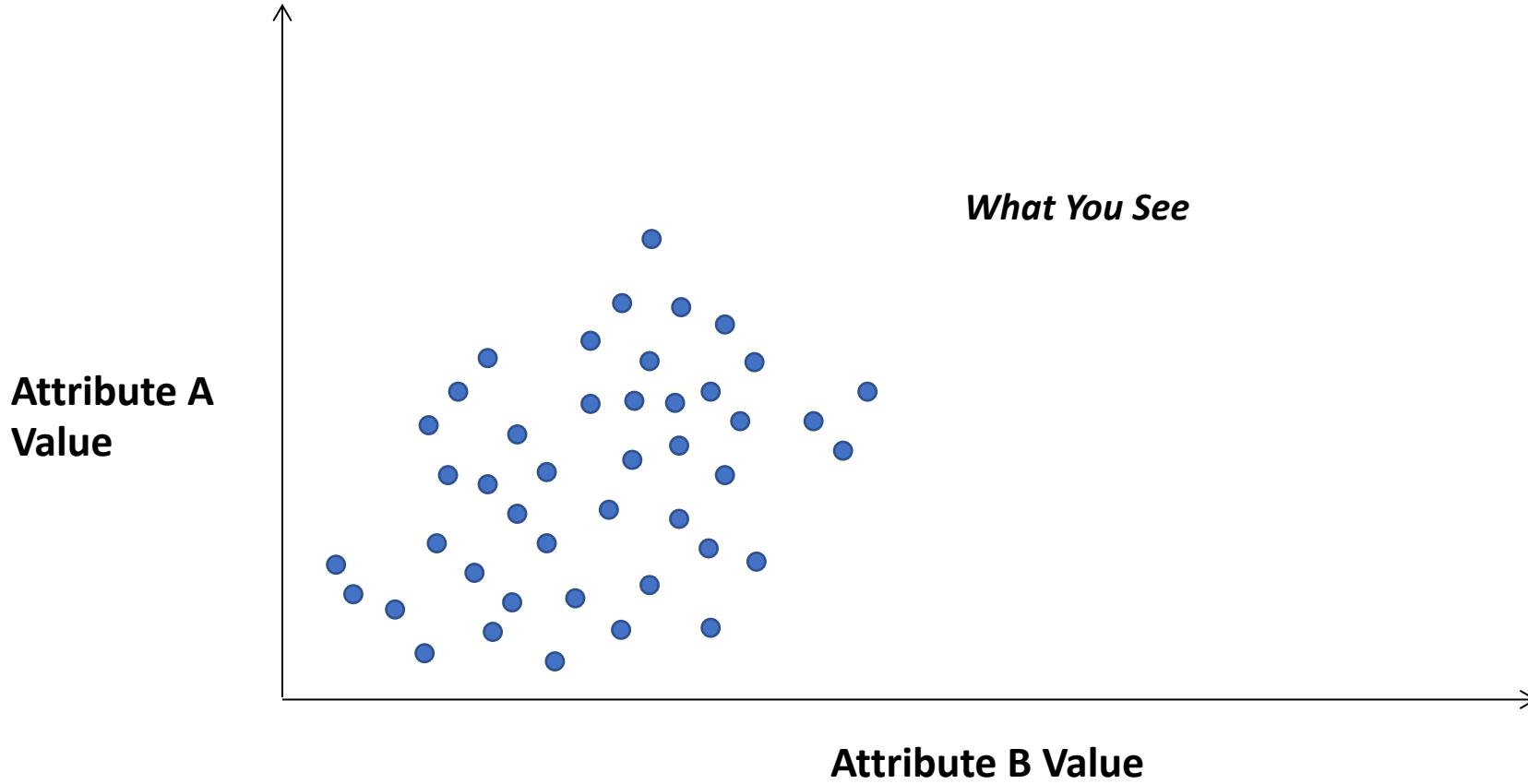
[BOOK YOUR COURSE](#) [VIEW PRICE NOW](#)



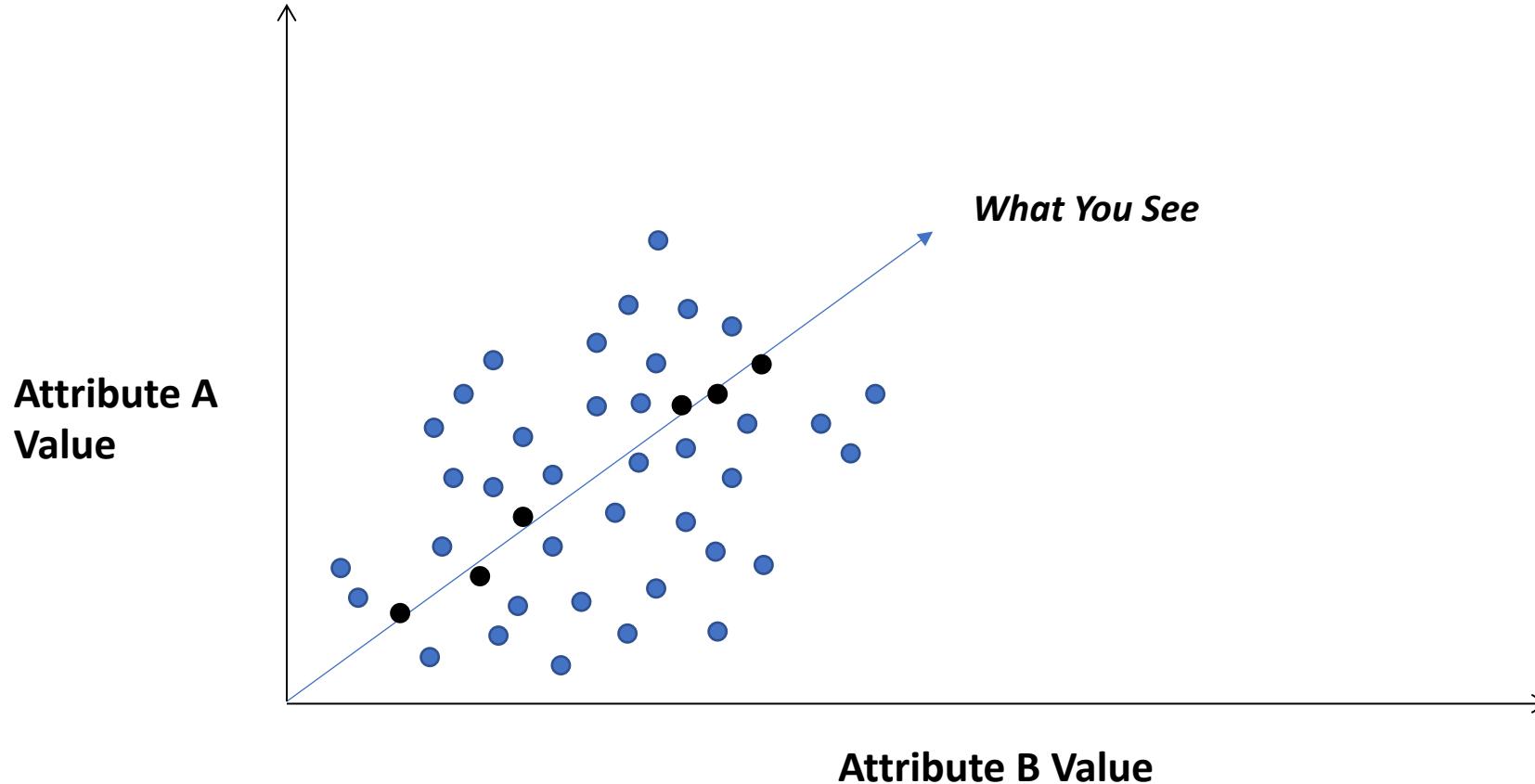
## InfoSec Institute Ethical Hacker Program

# How Can Machine Learning be Used for Network Security?

# Supervised Machine Learning

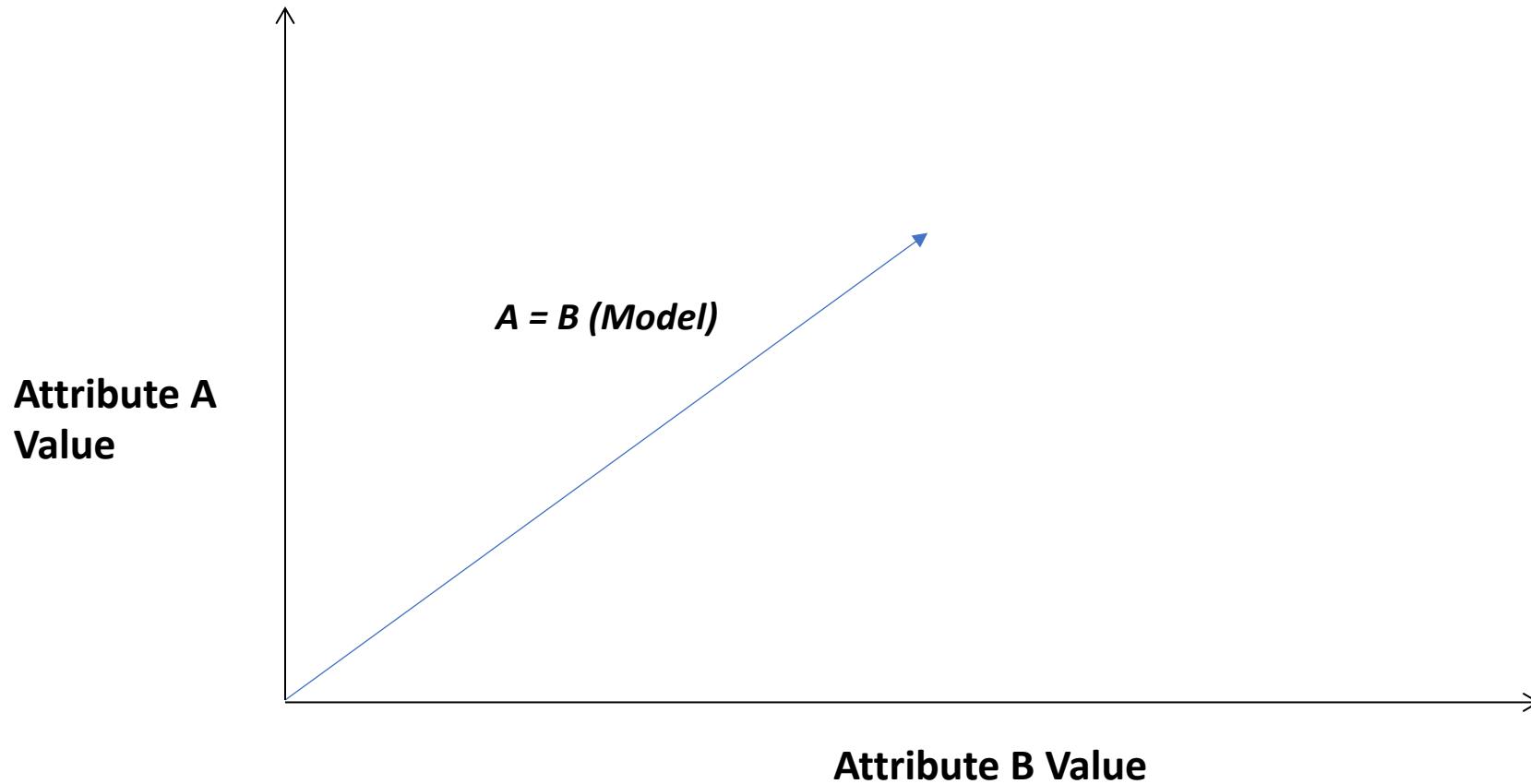


# Supervised Machine Learning



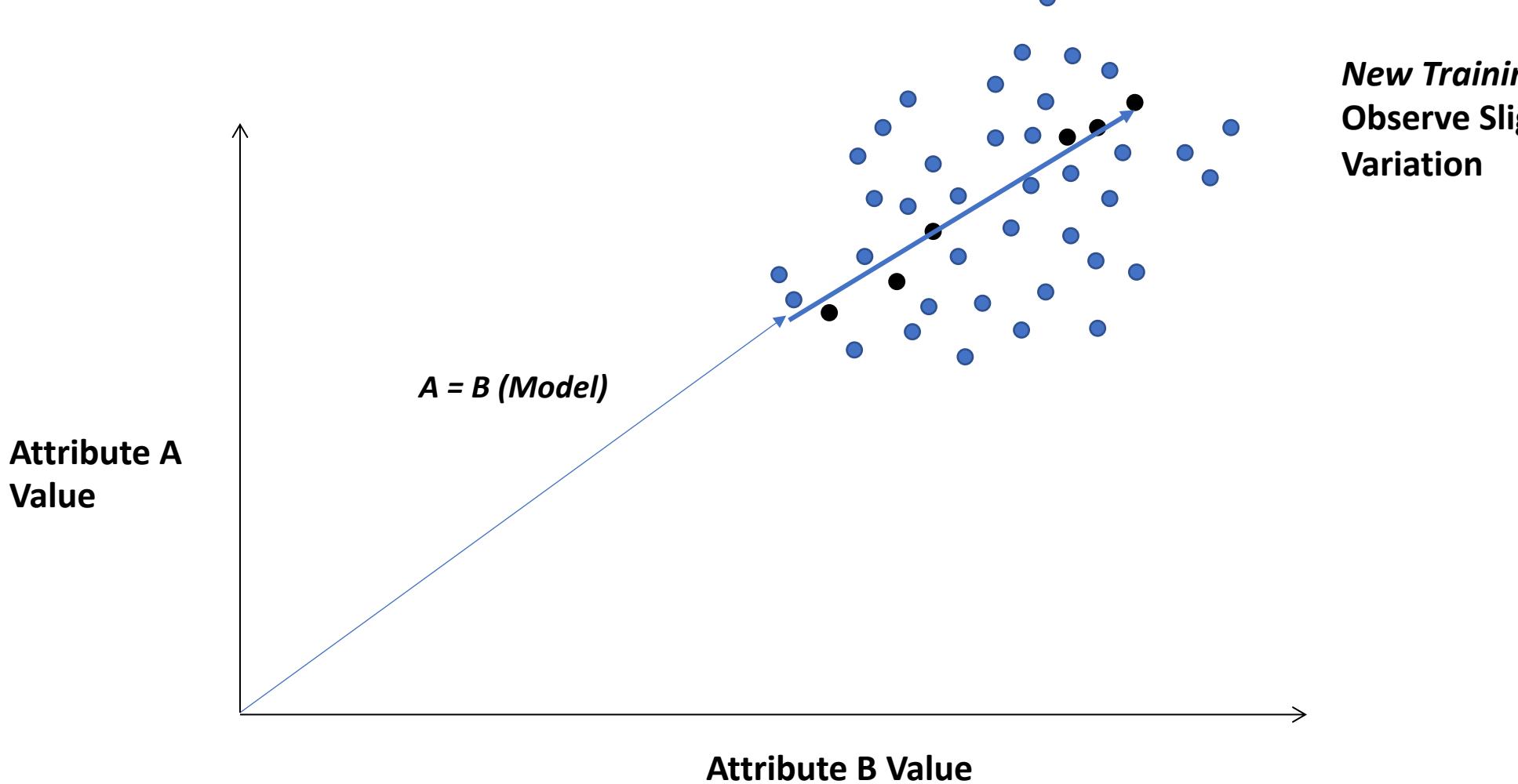
*Initial Training:*  
Attribute A Value =  
Attribute B Value  
Implies Some Desired  
Condition

# Supervised Machine Learning

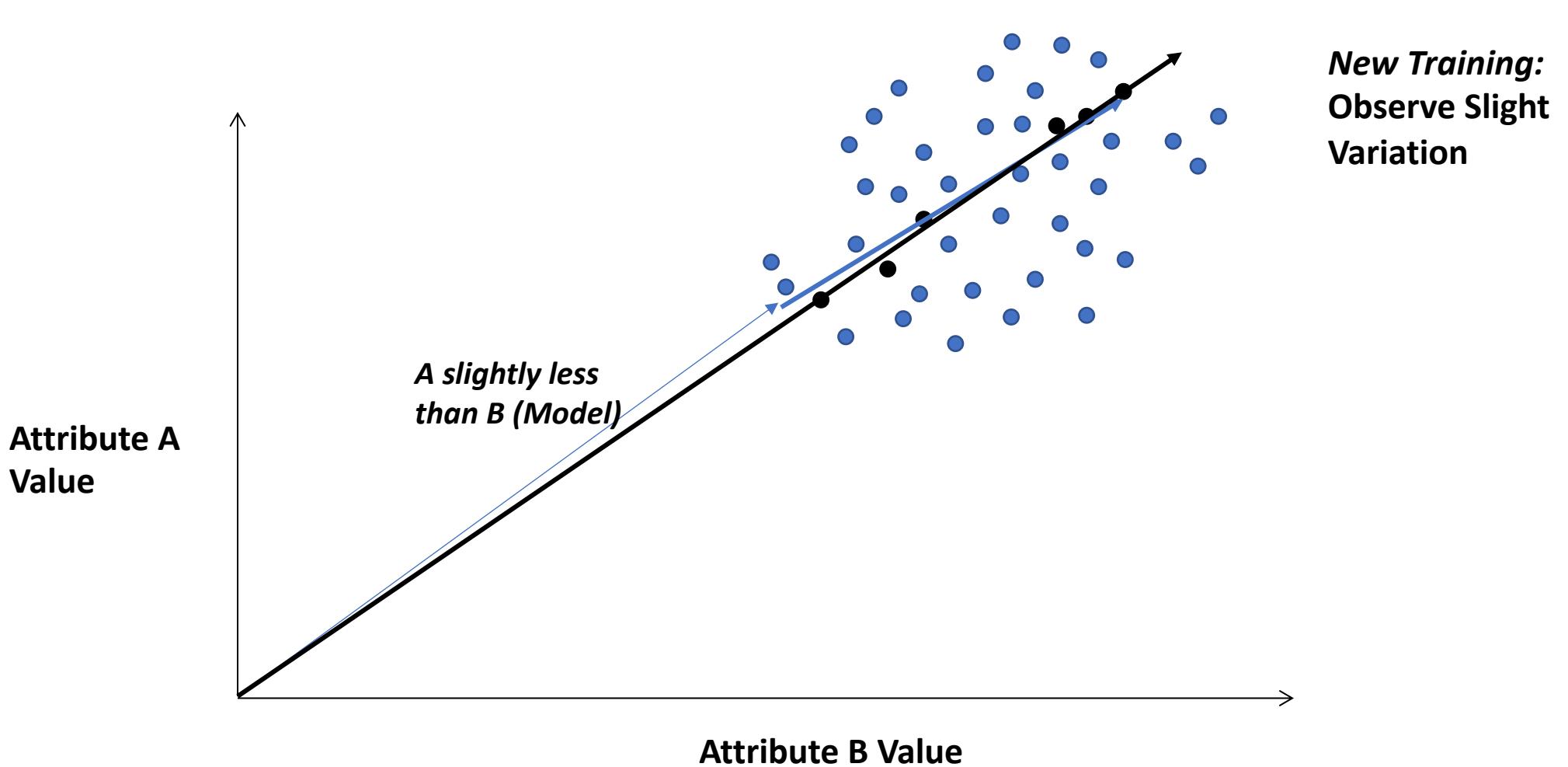


***New Training:***  
Observe Slight  
Variation

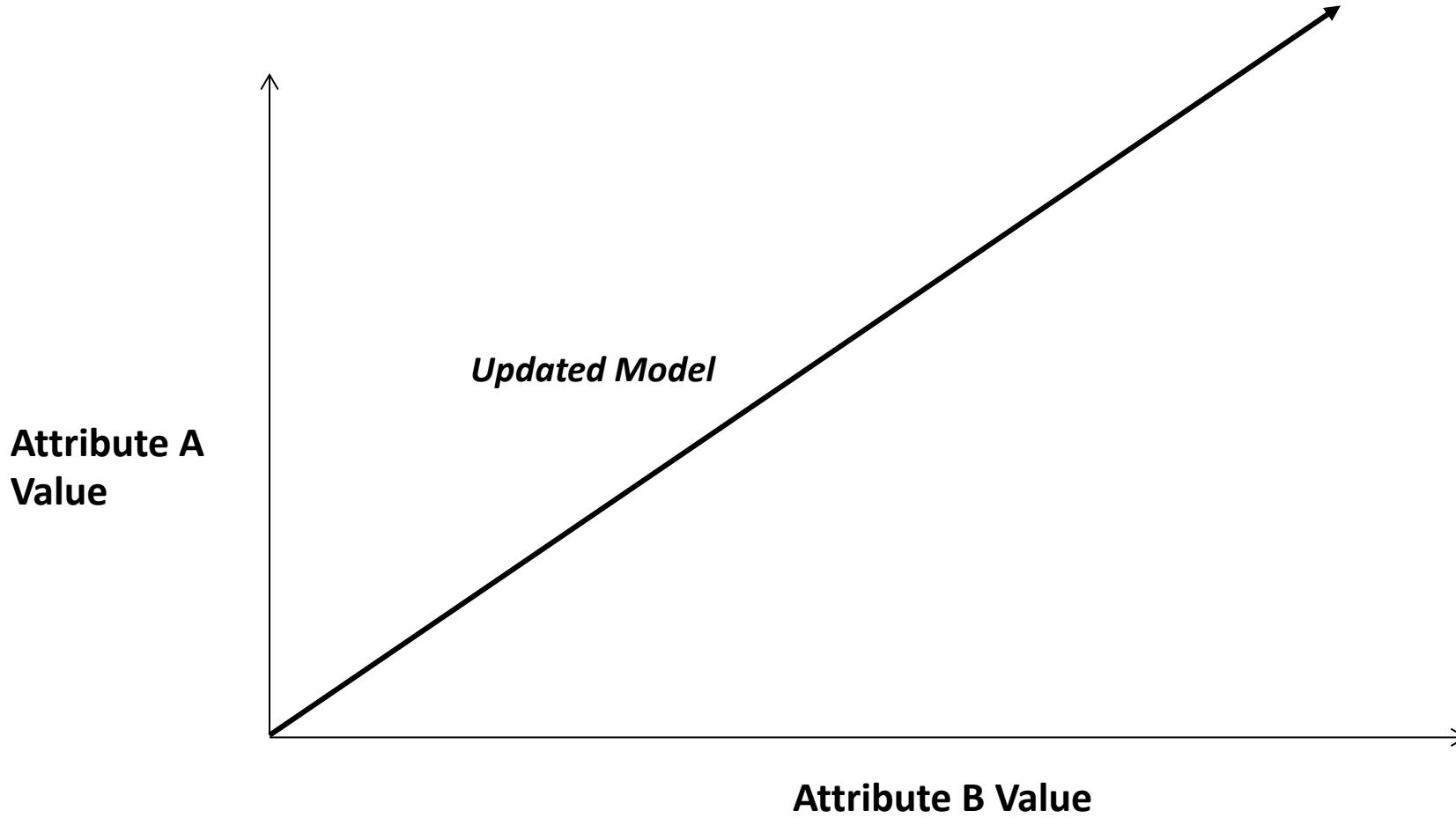
# Supervised Machine Learning



# Supervised Machine Learning



# Supervised Machine Learning



# Supervised Machine Learning for Security – Concepts



# 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

# 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

# Supervised Machine Learning for Security – Concepts



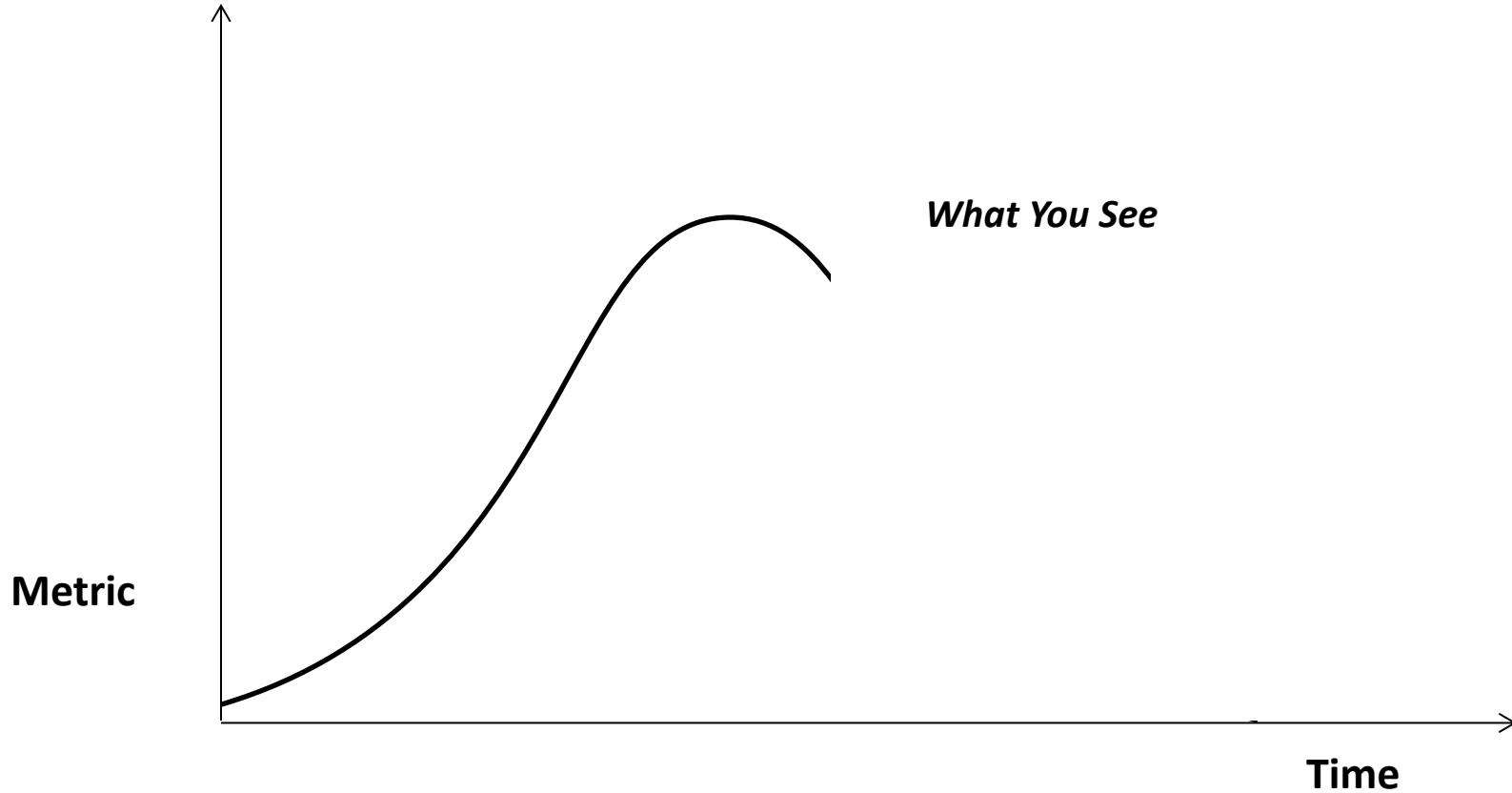
## Training Data for App Security (Two Factors)

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

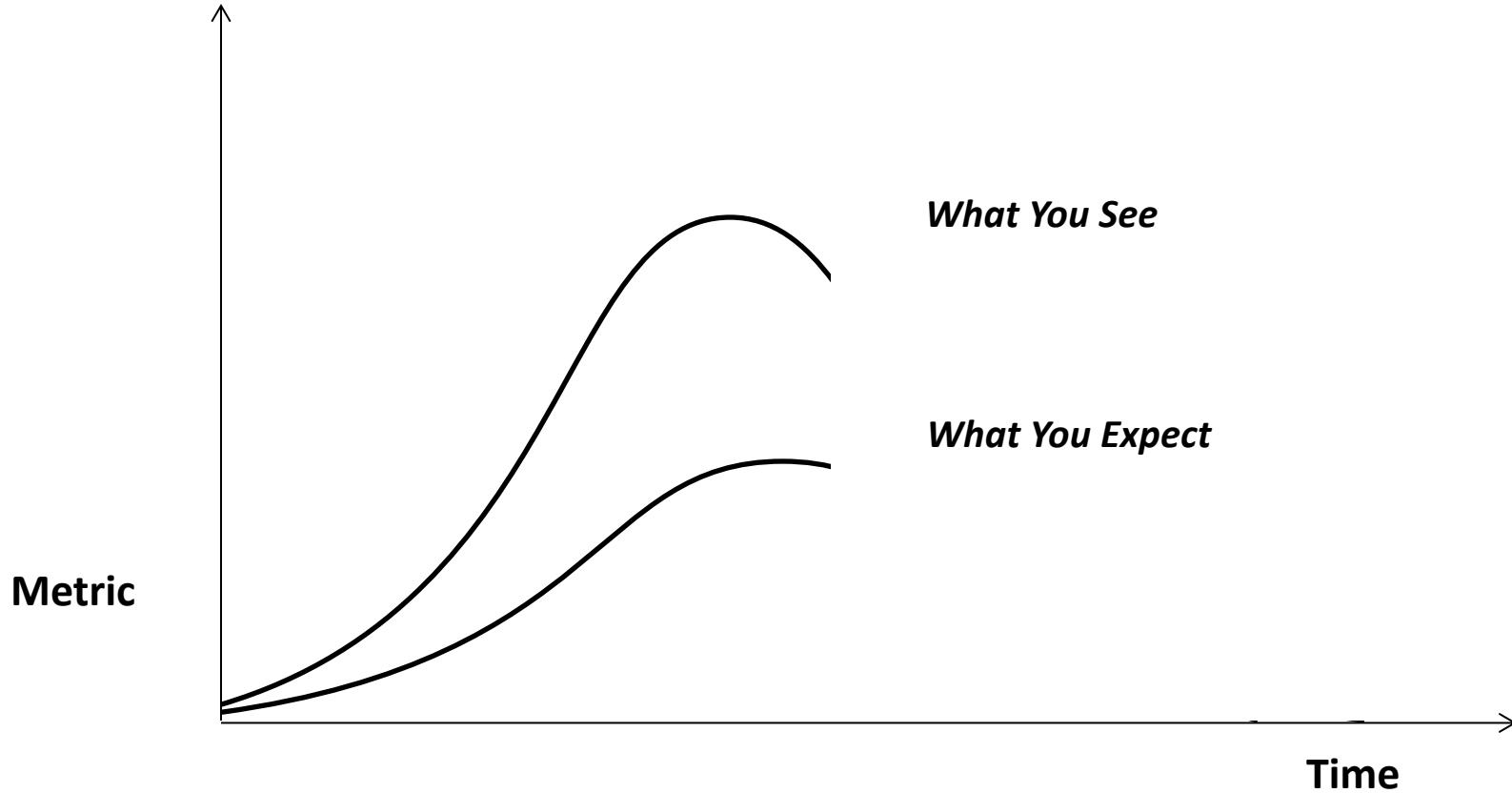
**Linear Regression Strategy:** Graph the Data and Use to Predict Number of Vulnerabilities from Two Input factors

# How Can Network Security Attacks Be Visualized?

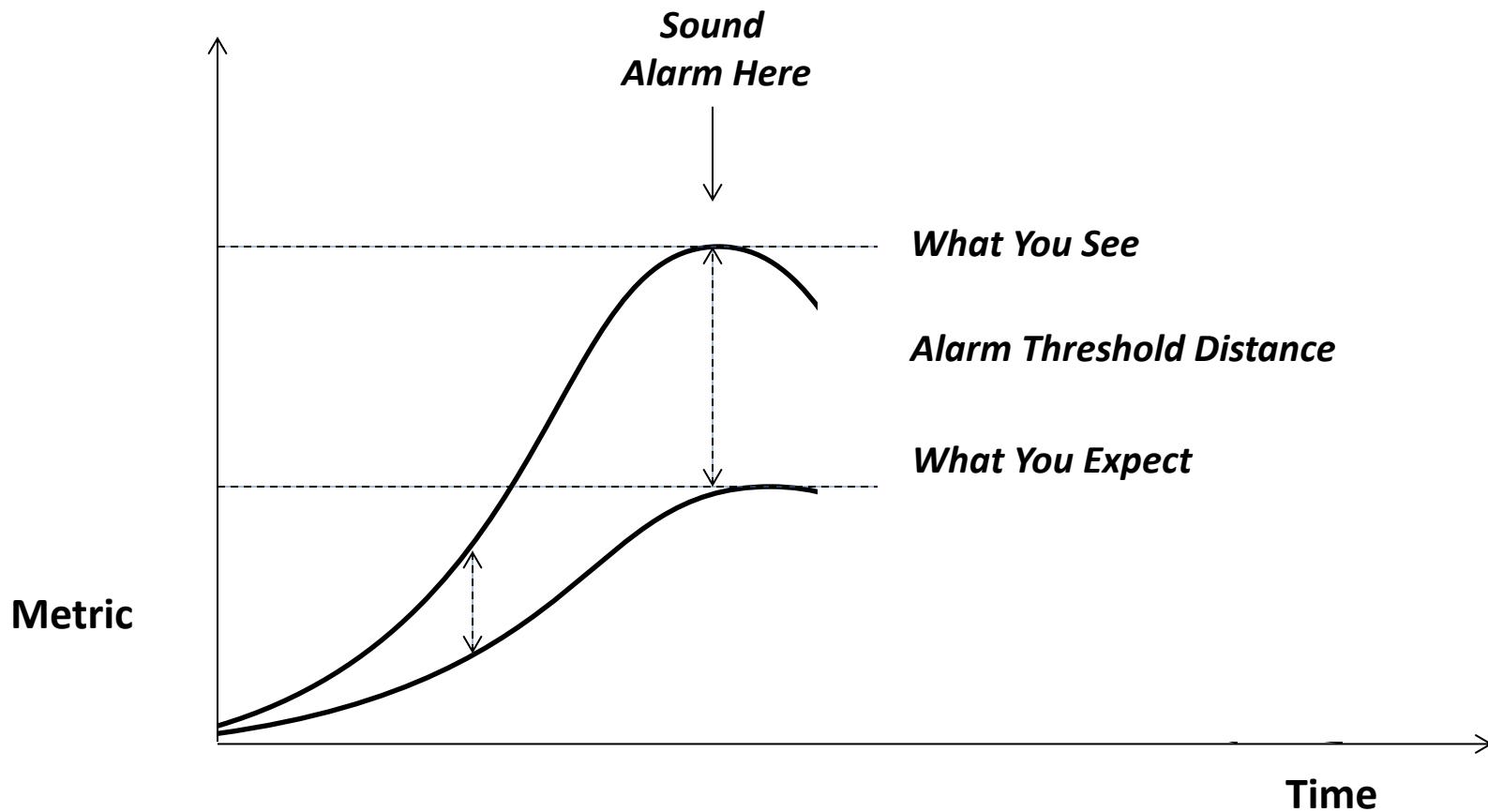
# Real Time Network Security Behavioral Analytics



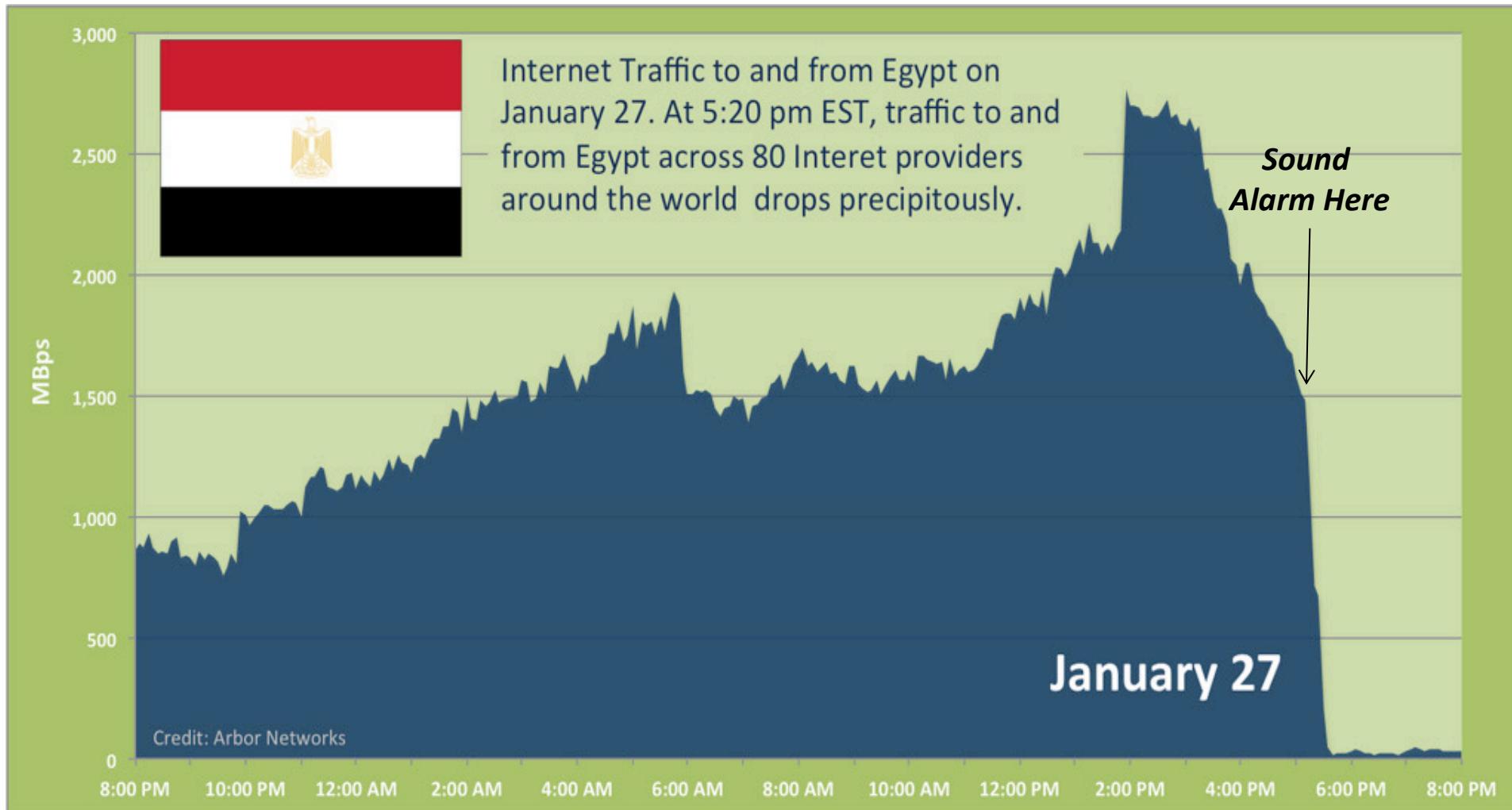
# Real Time Network Security Behavioral Analytics



# Real Time Network Security Behavioral Analytics

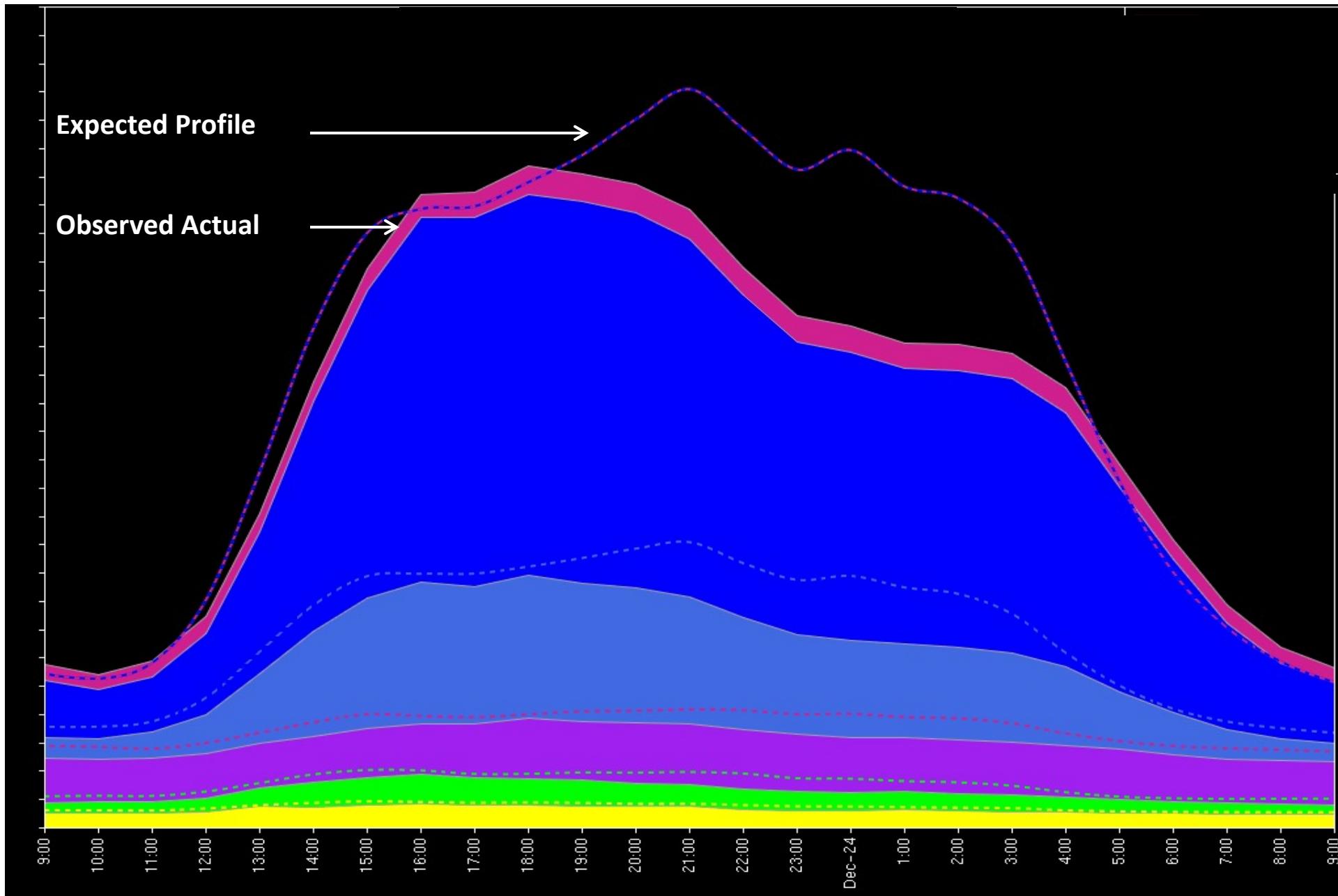


# Internet Blackout in Egypt – 01/27/11



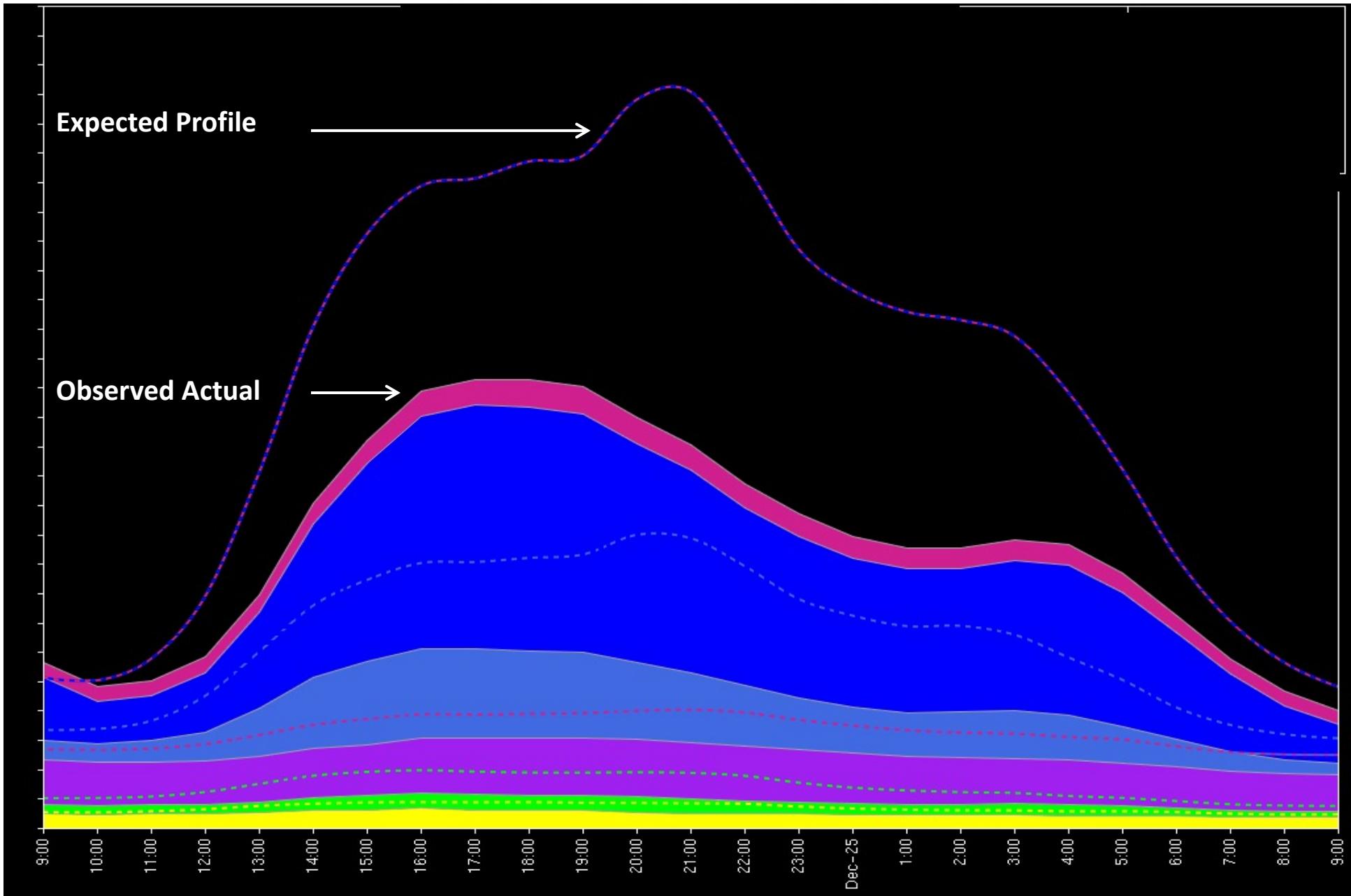
Week 3

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



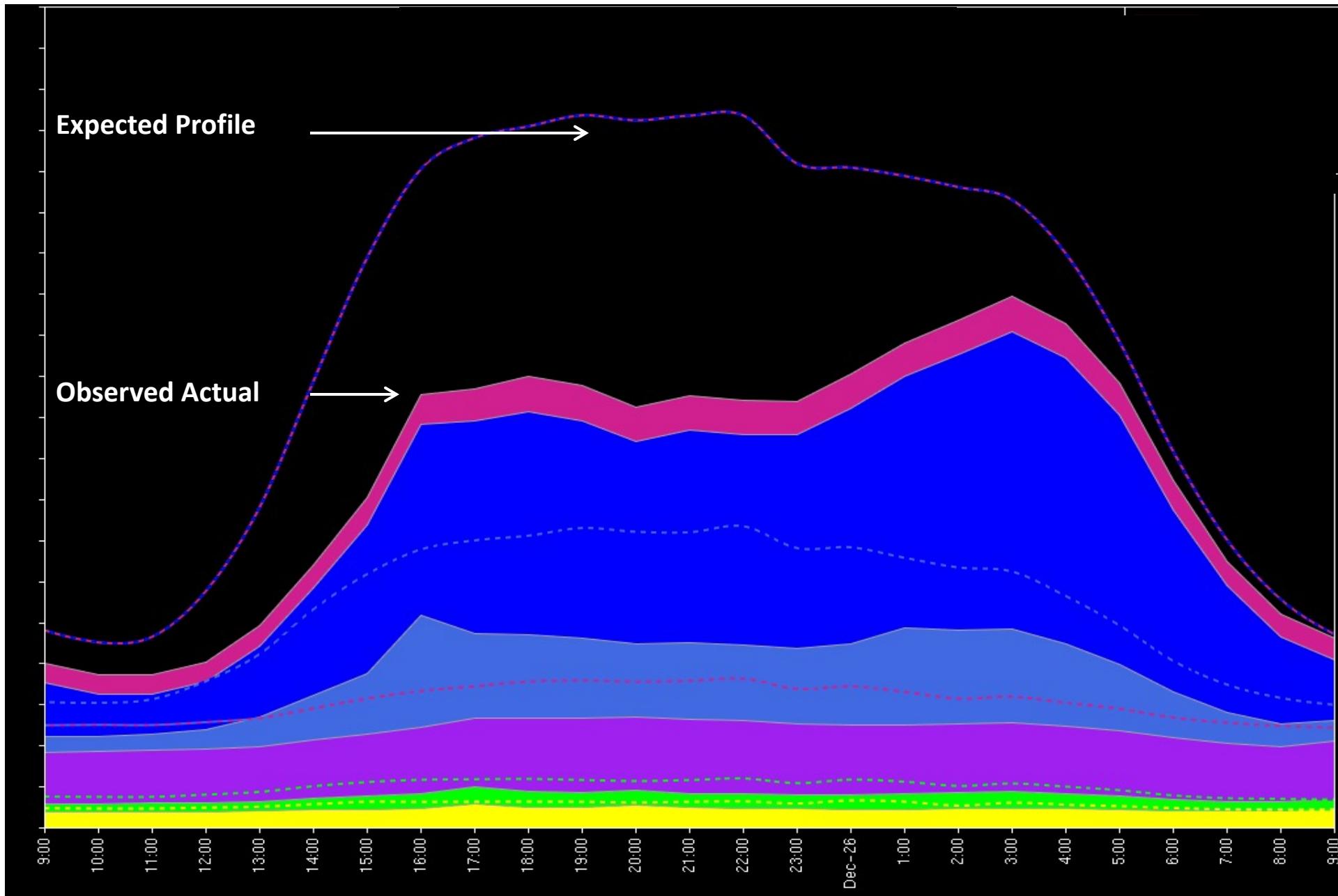
Week 3

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

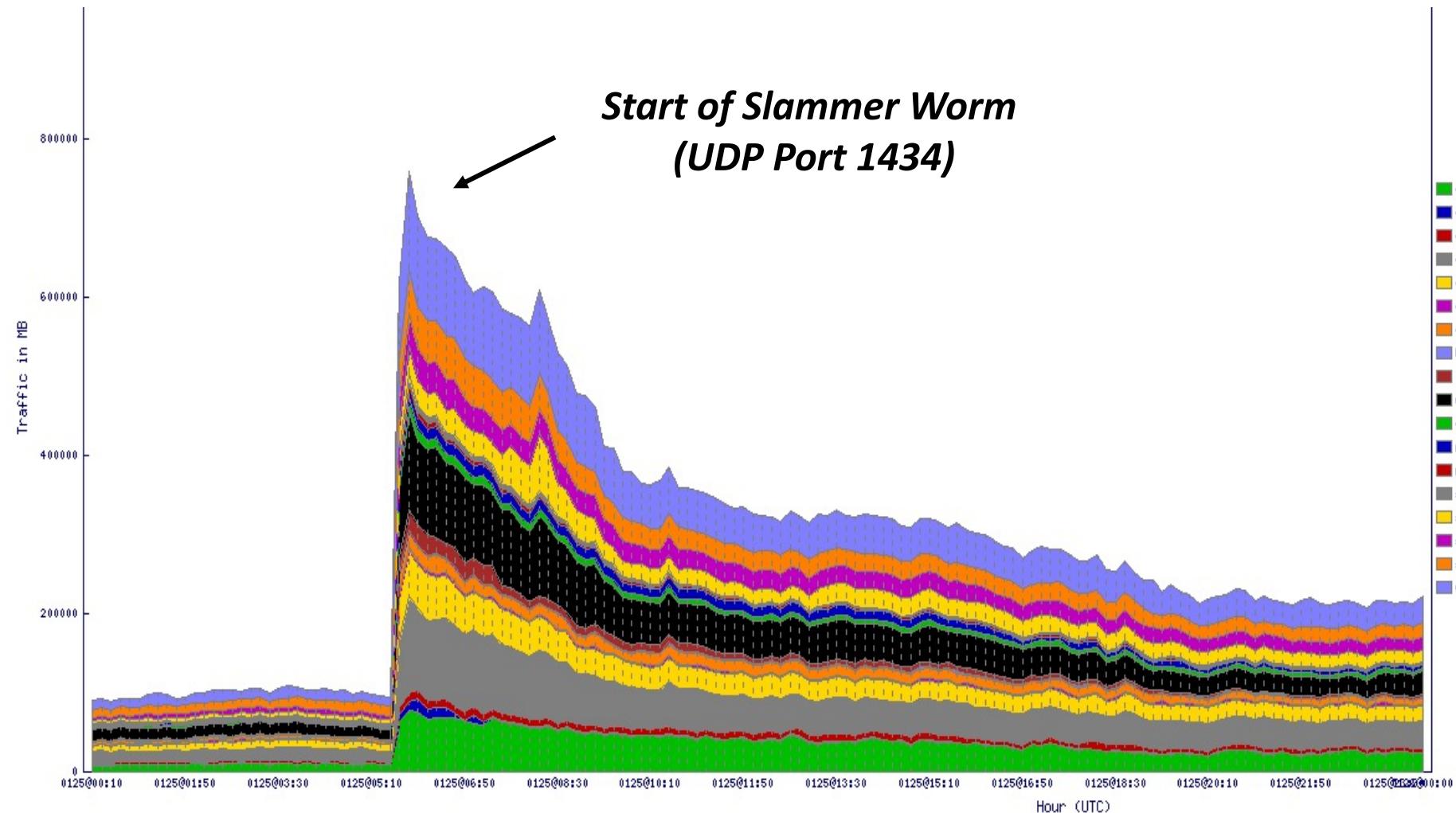


Week 3

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

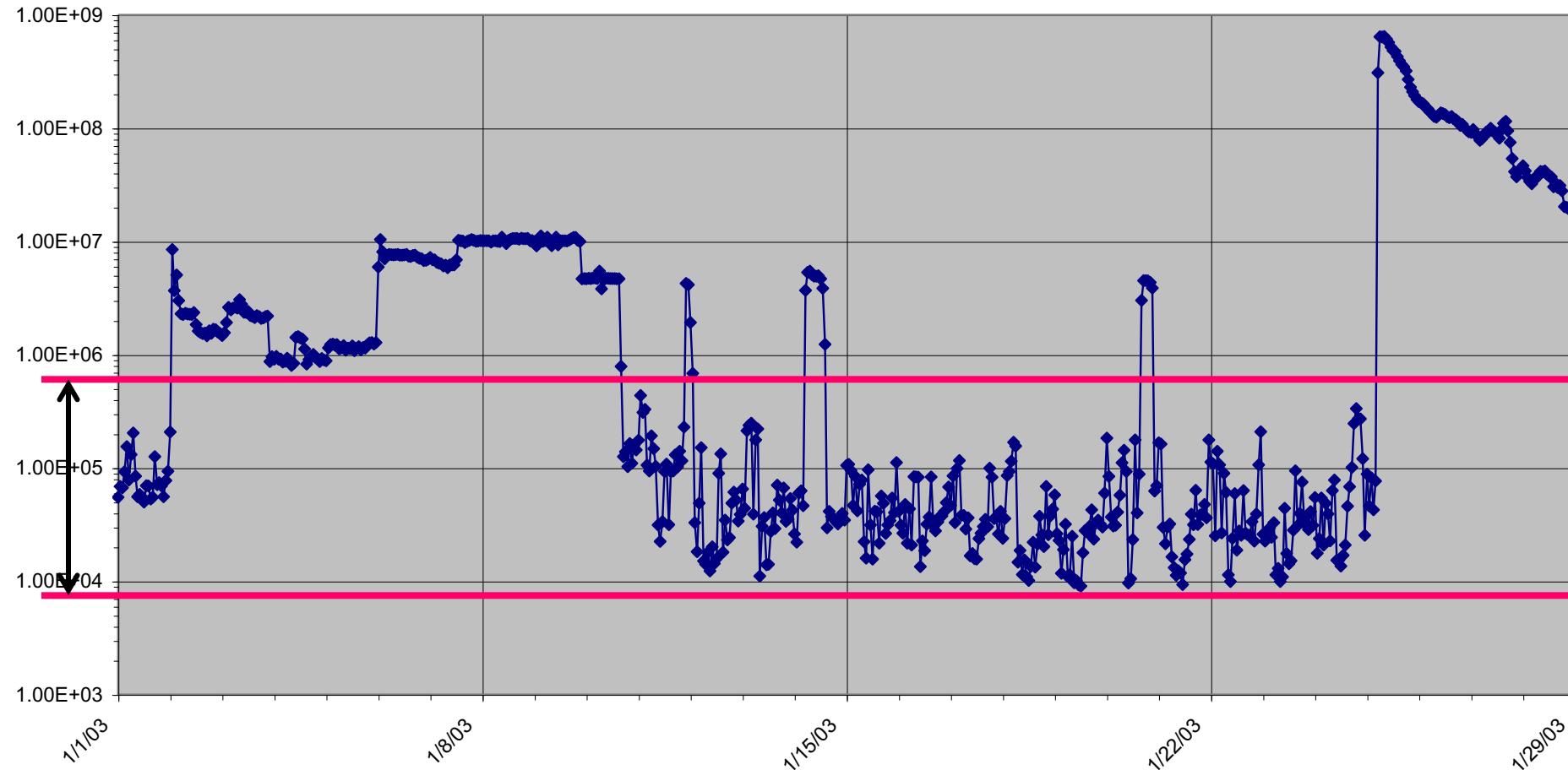


# Internet View of Slammer Worm – UDP Port 1434: 01/25/03



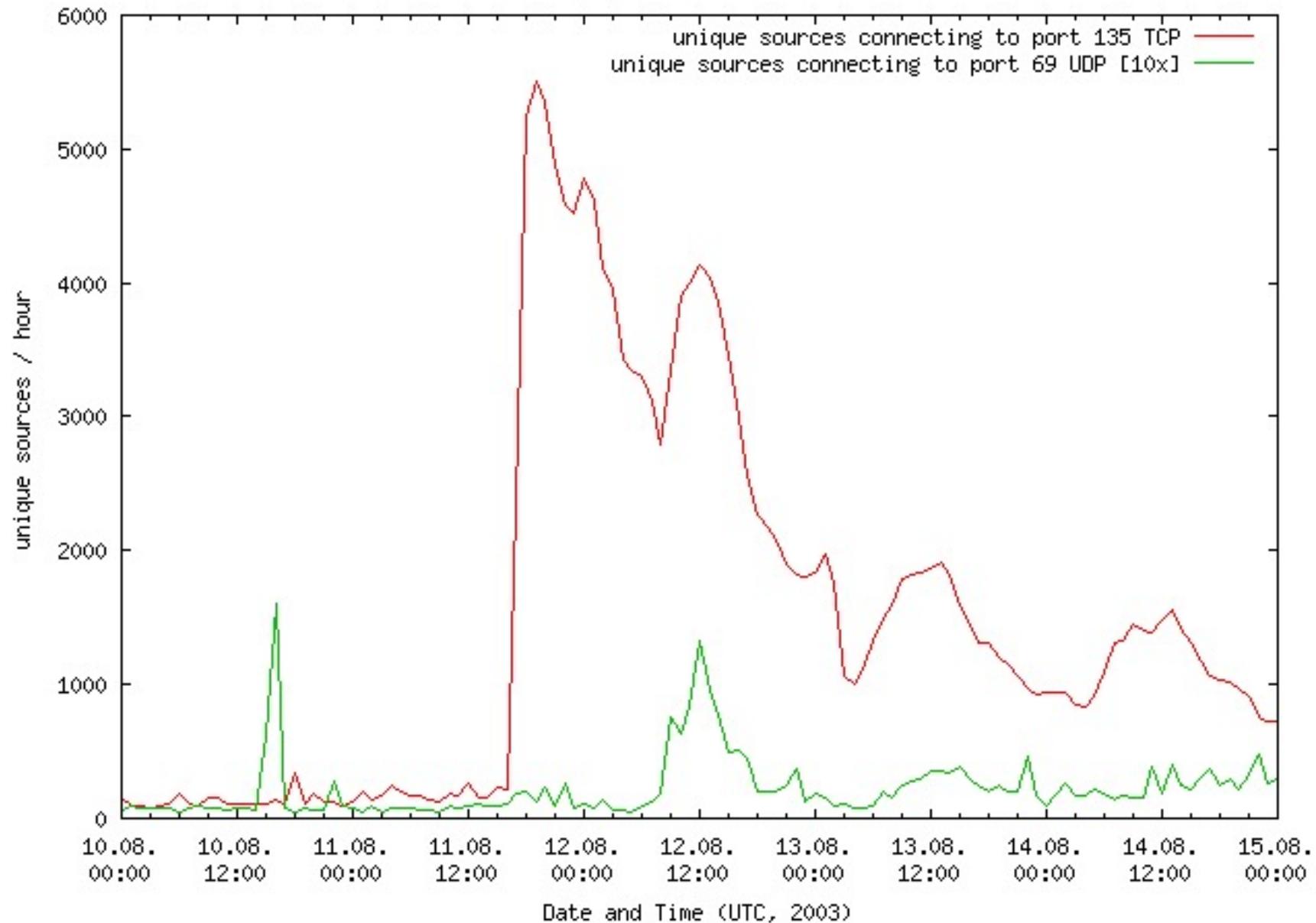
Week 3

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

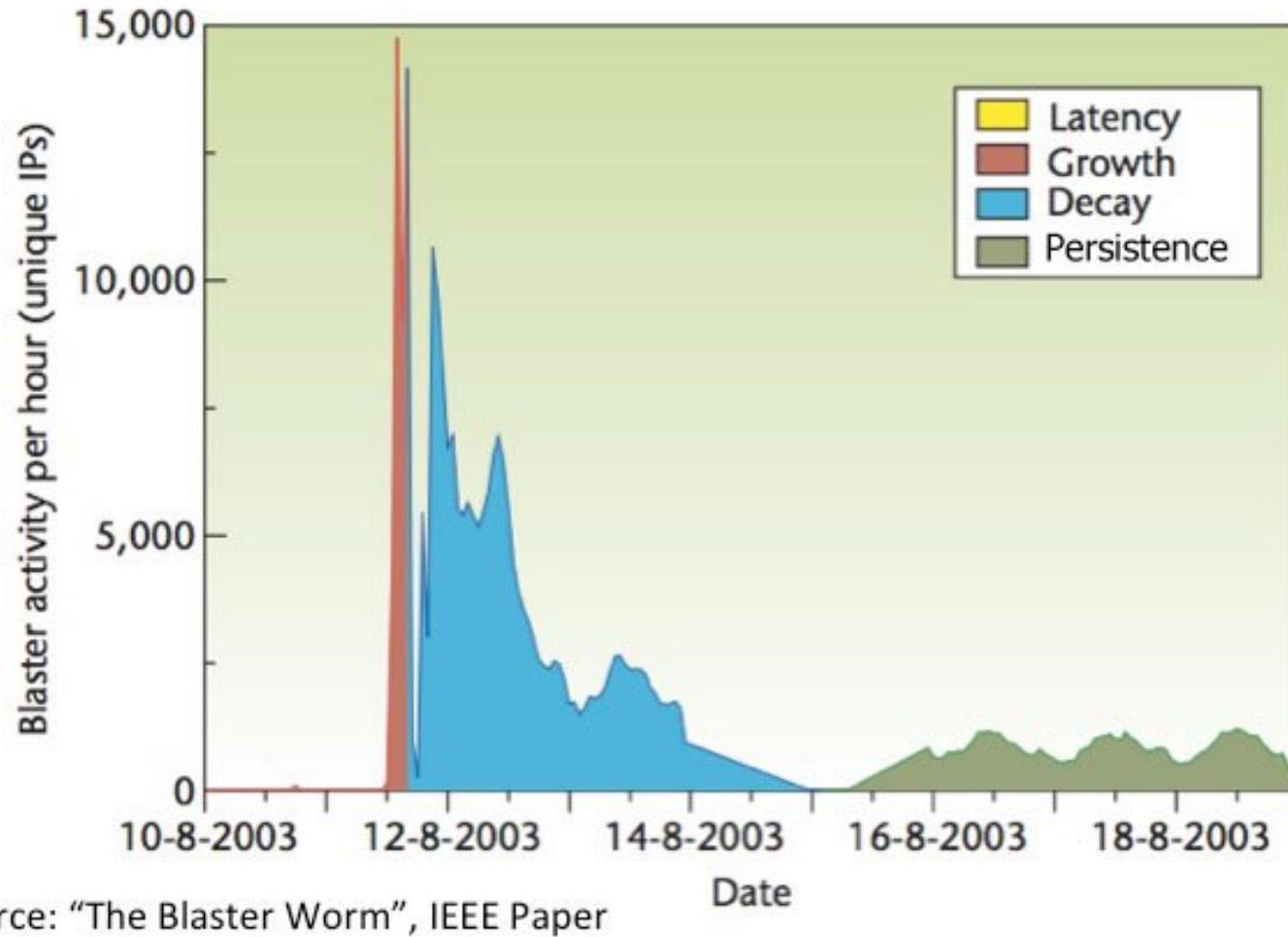


Week 3

# Sharp Spike from Blaster Worm – 8/11/03

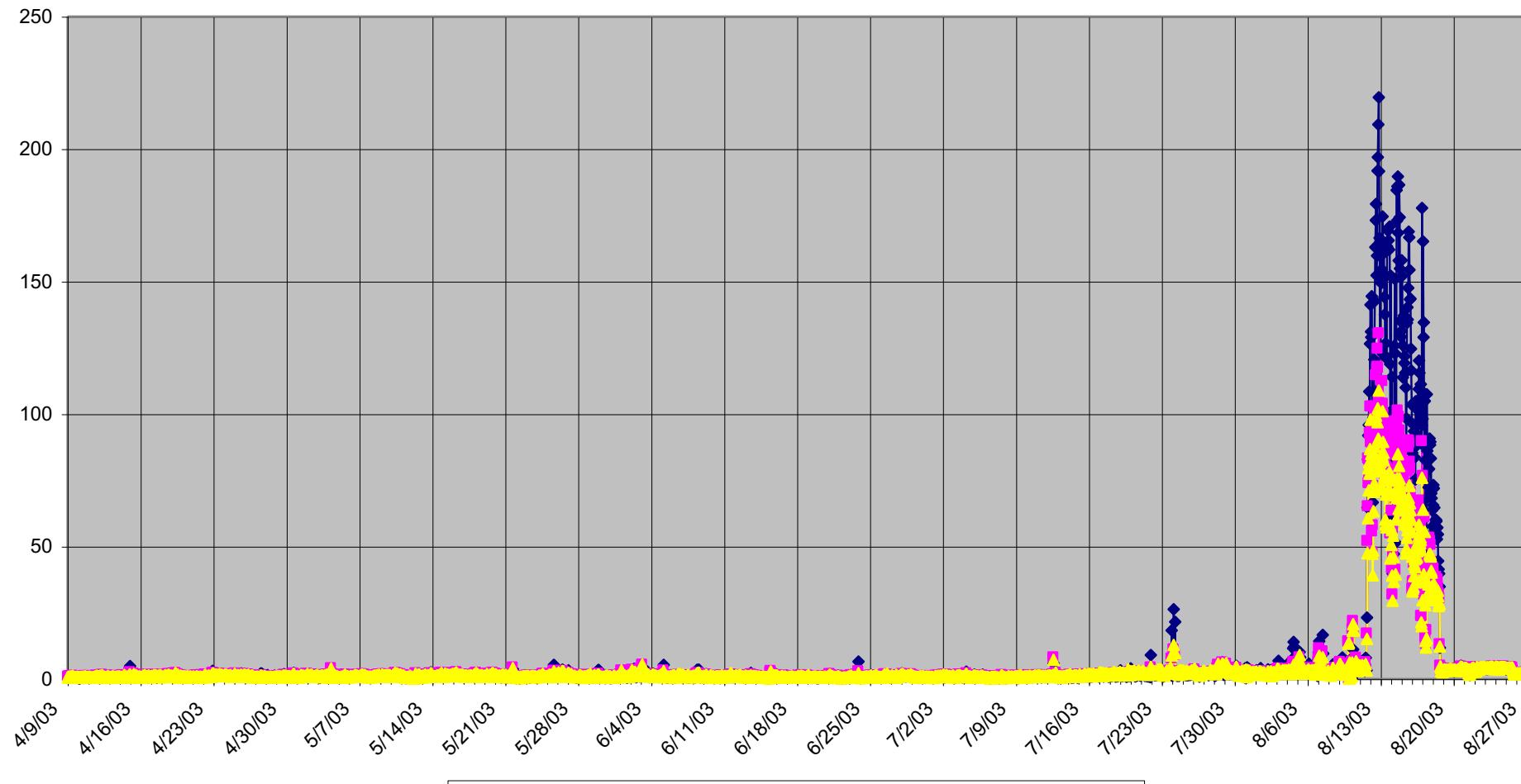


# Sharp Spike from Blaster Worm – 8/11/03



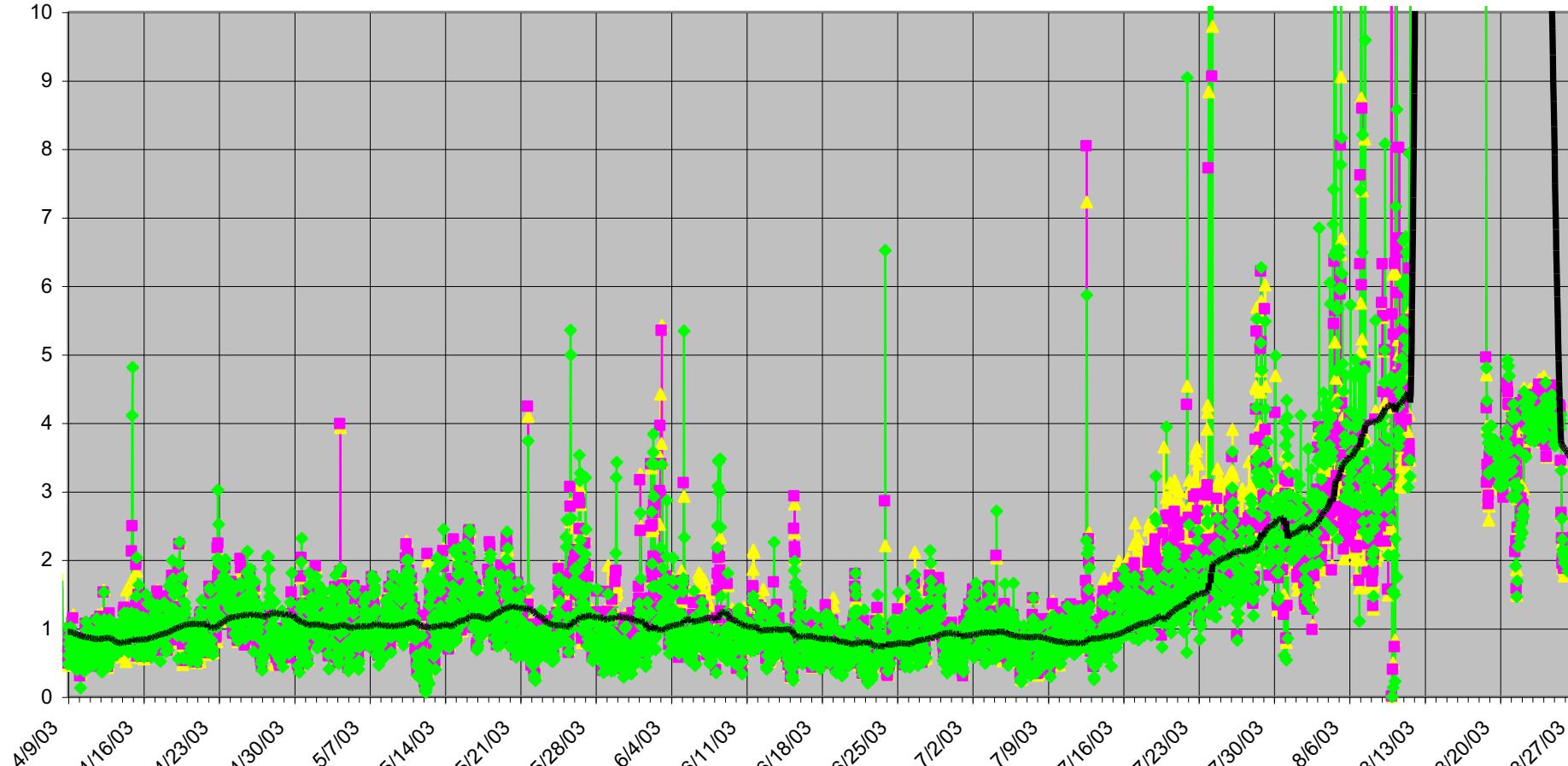
Week 3

# Internet View of TCP 135 – Blaster Worm – 2003

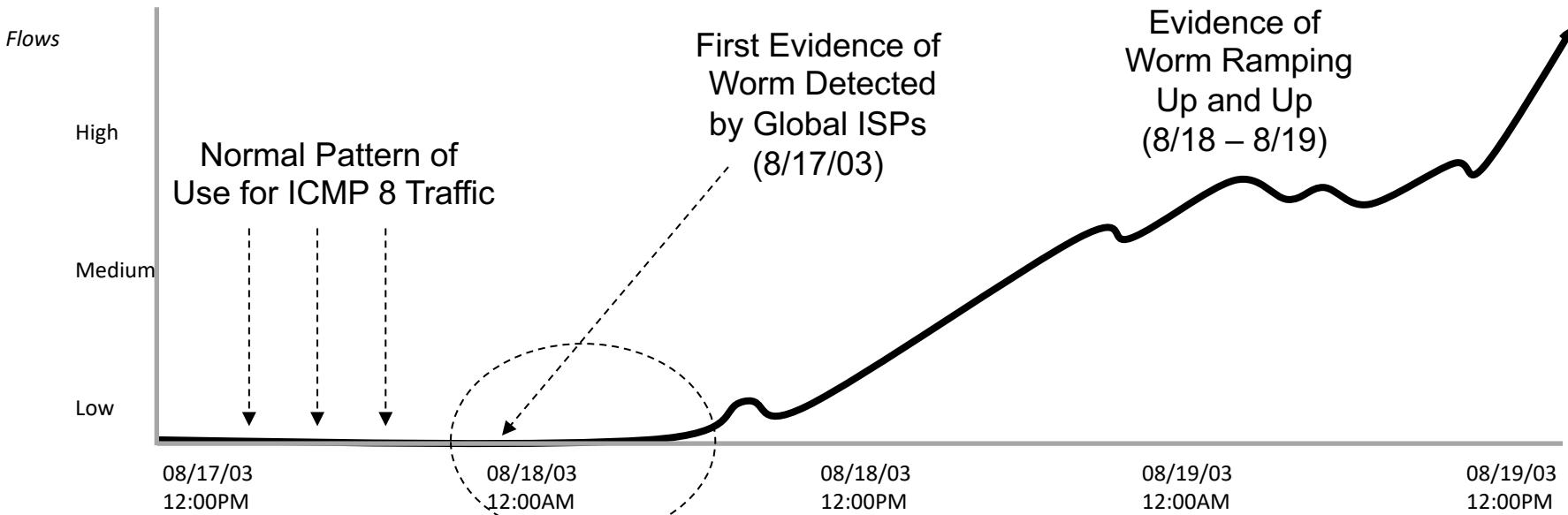


Week 3

# Deeper Internet View of TCP 135 Activity – Blaster Worm

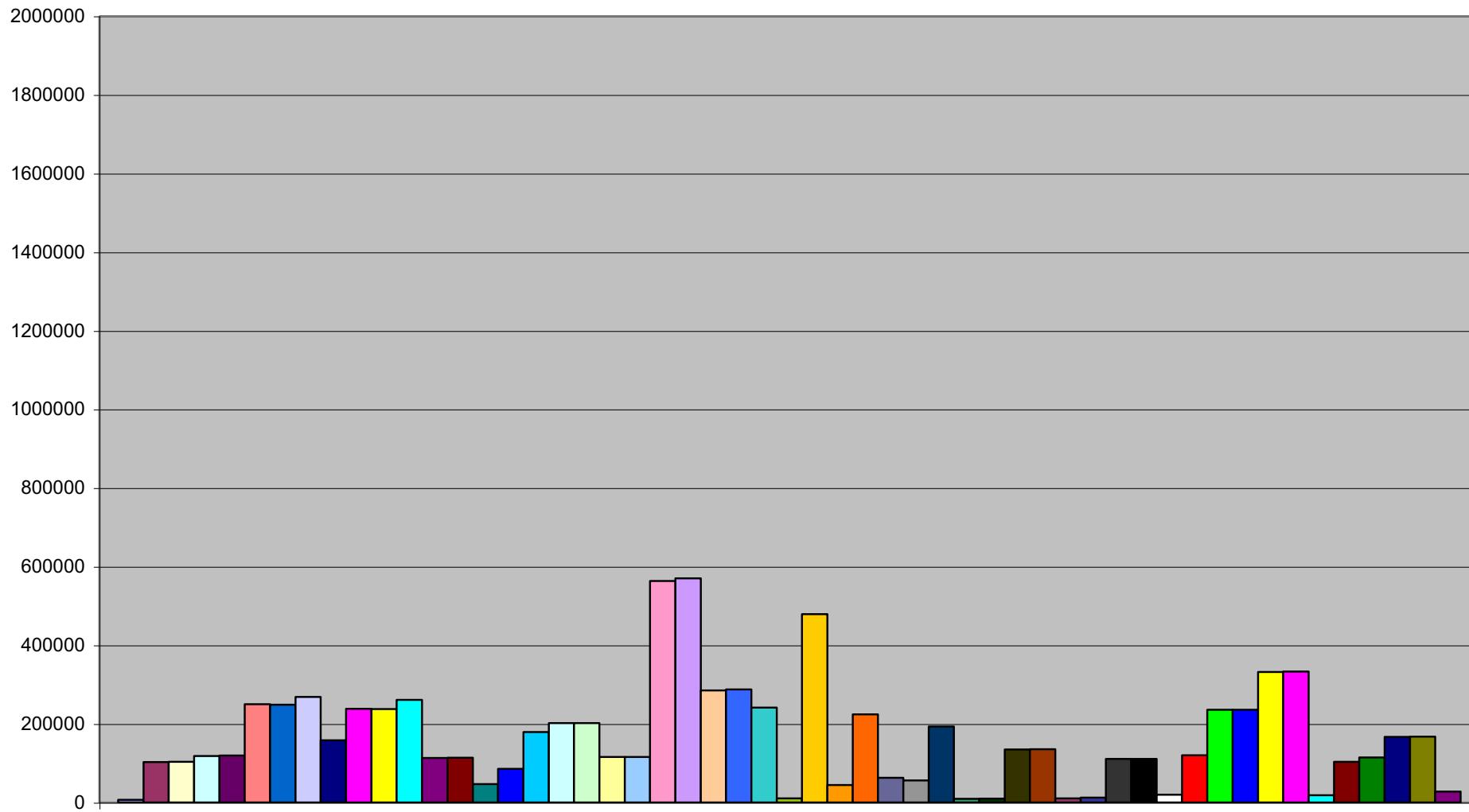


# Nachi Worm of 2003



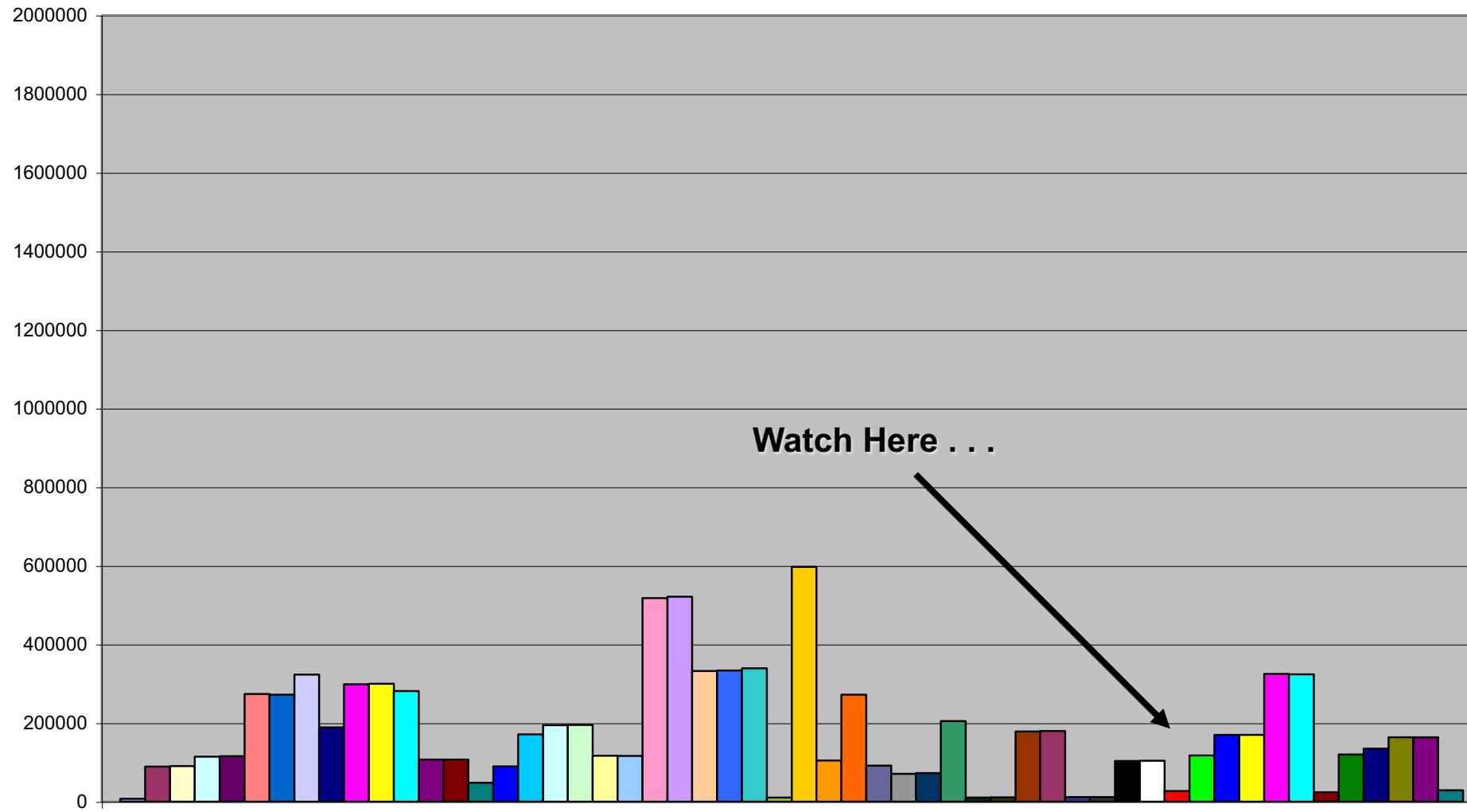
Week 3

Nachi 8/17/03 10:00PM



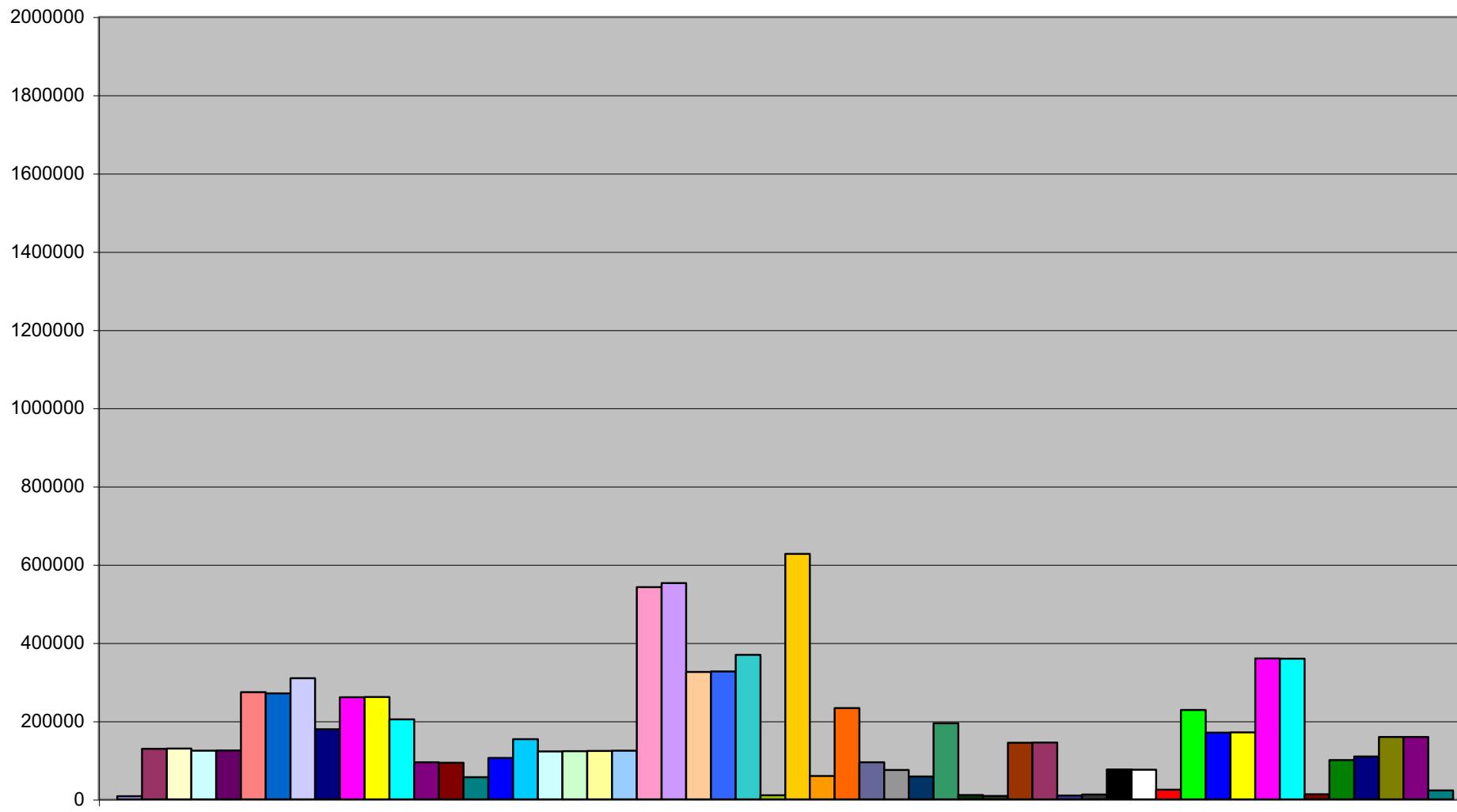
Week 3

Nachi 8/17/03 11:00PM



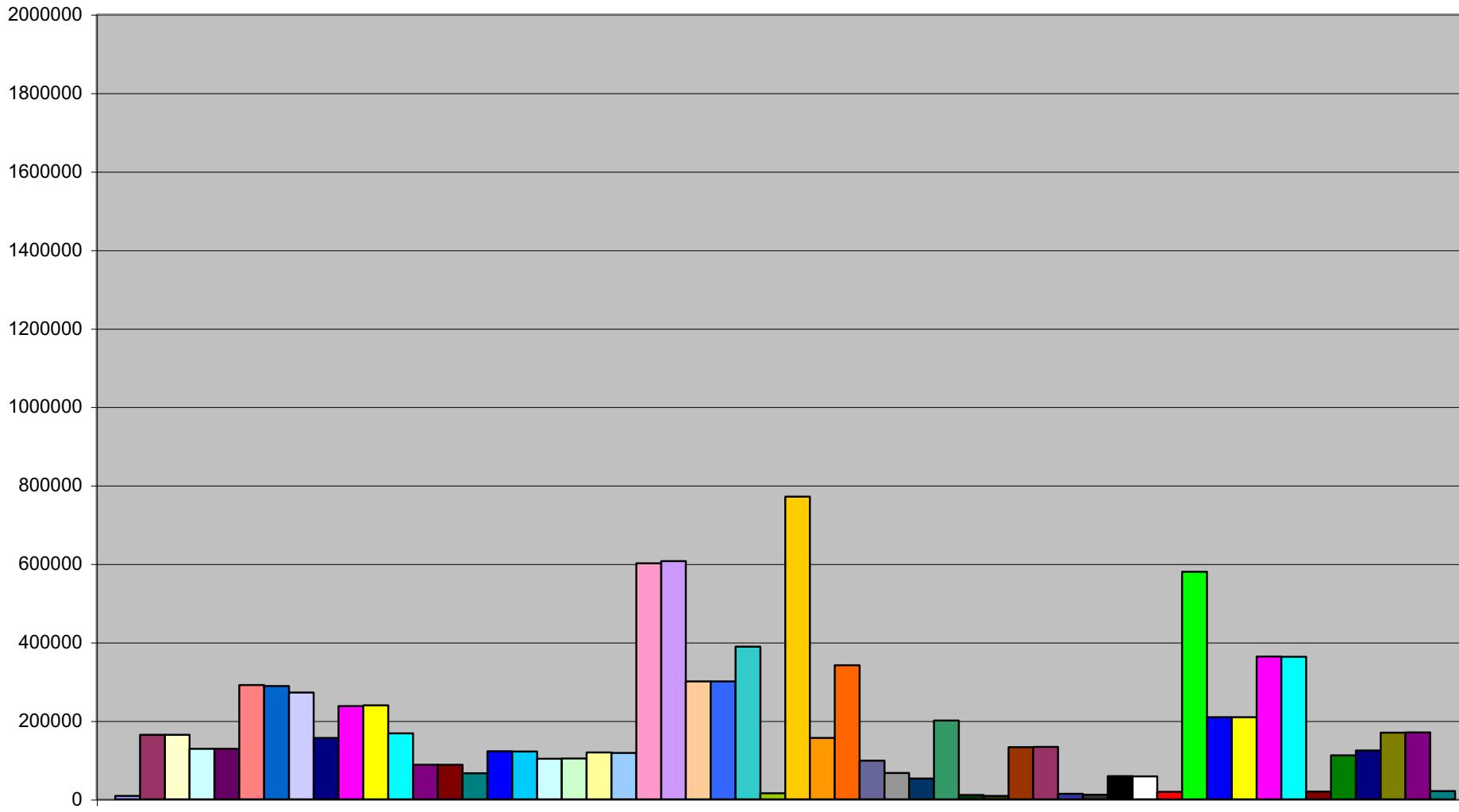
Week 3

# Nachi 8/17/03 Midnight



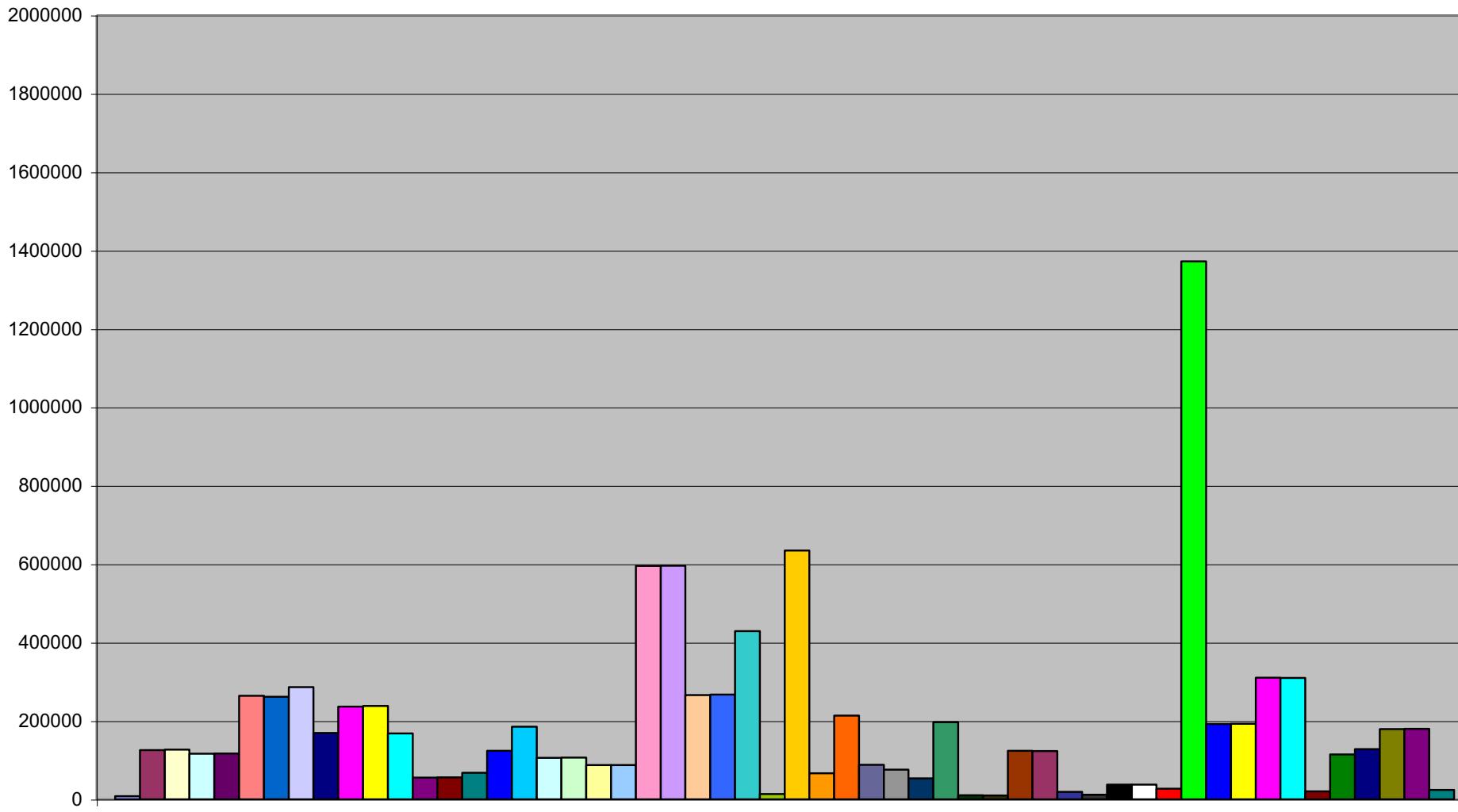
Week 3

# Nachi 8/18/03 1:00AM



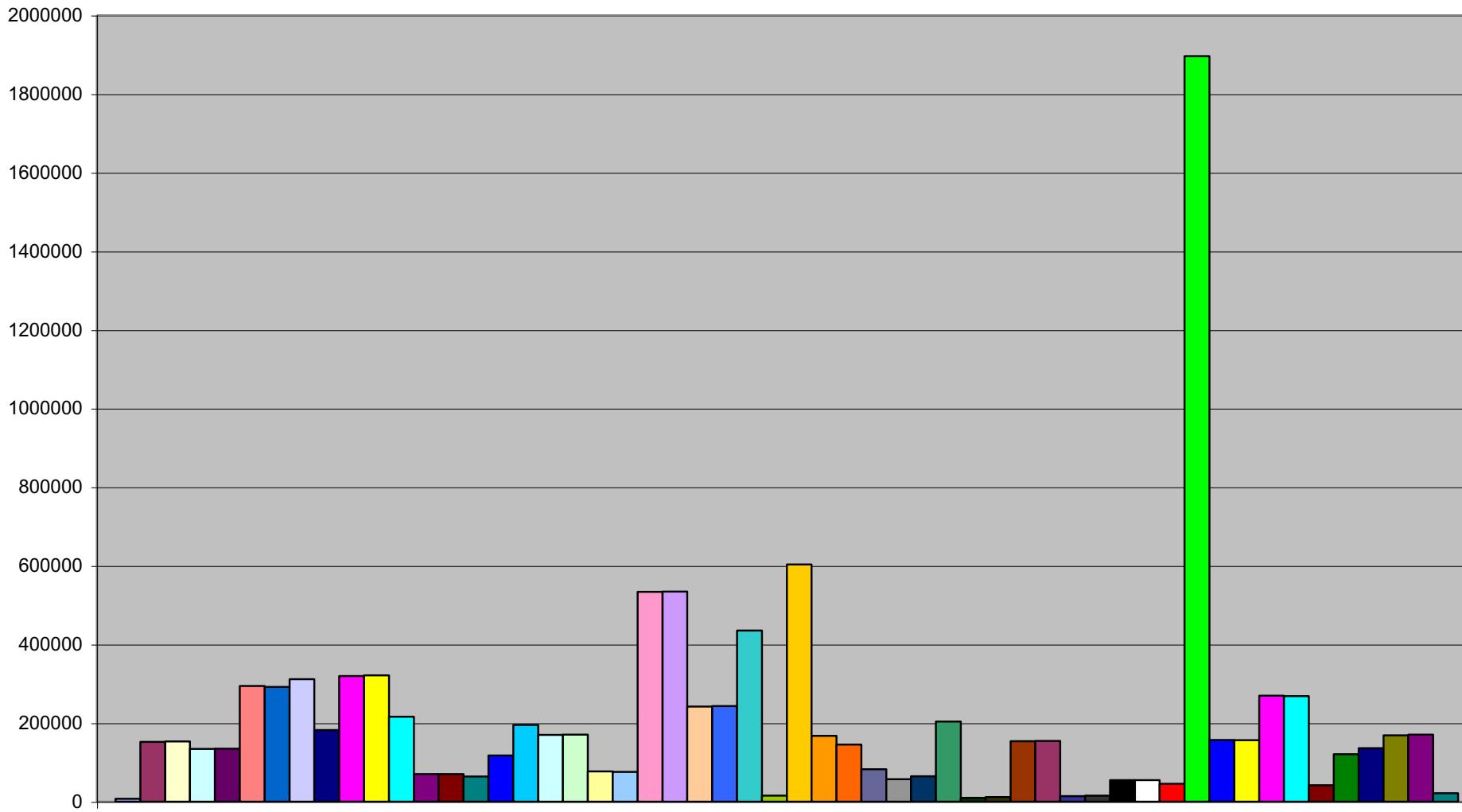
Week 3

# Nachi 8/18/03 2:00AM



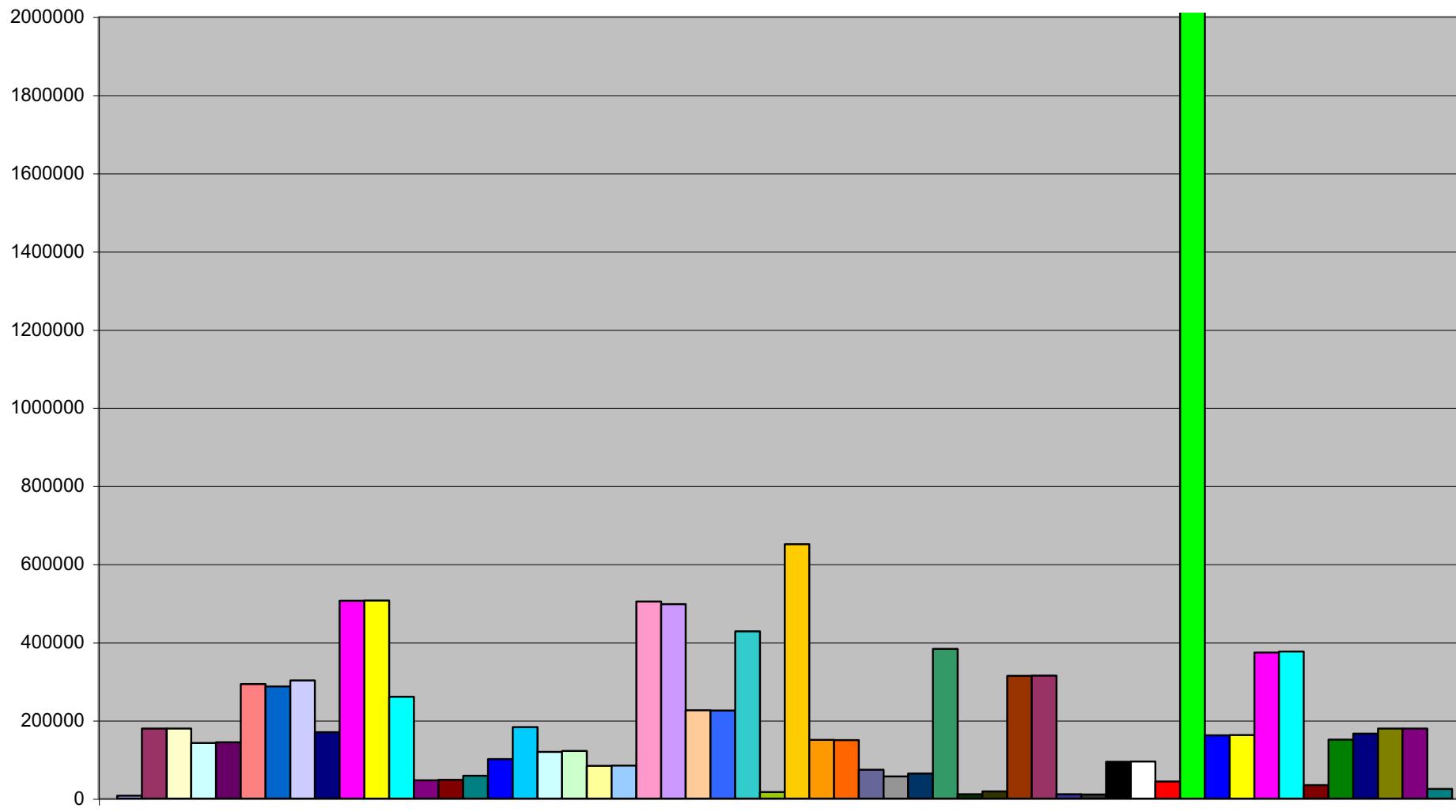
Week 3

# Nachi 8/18/03 3:00AM



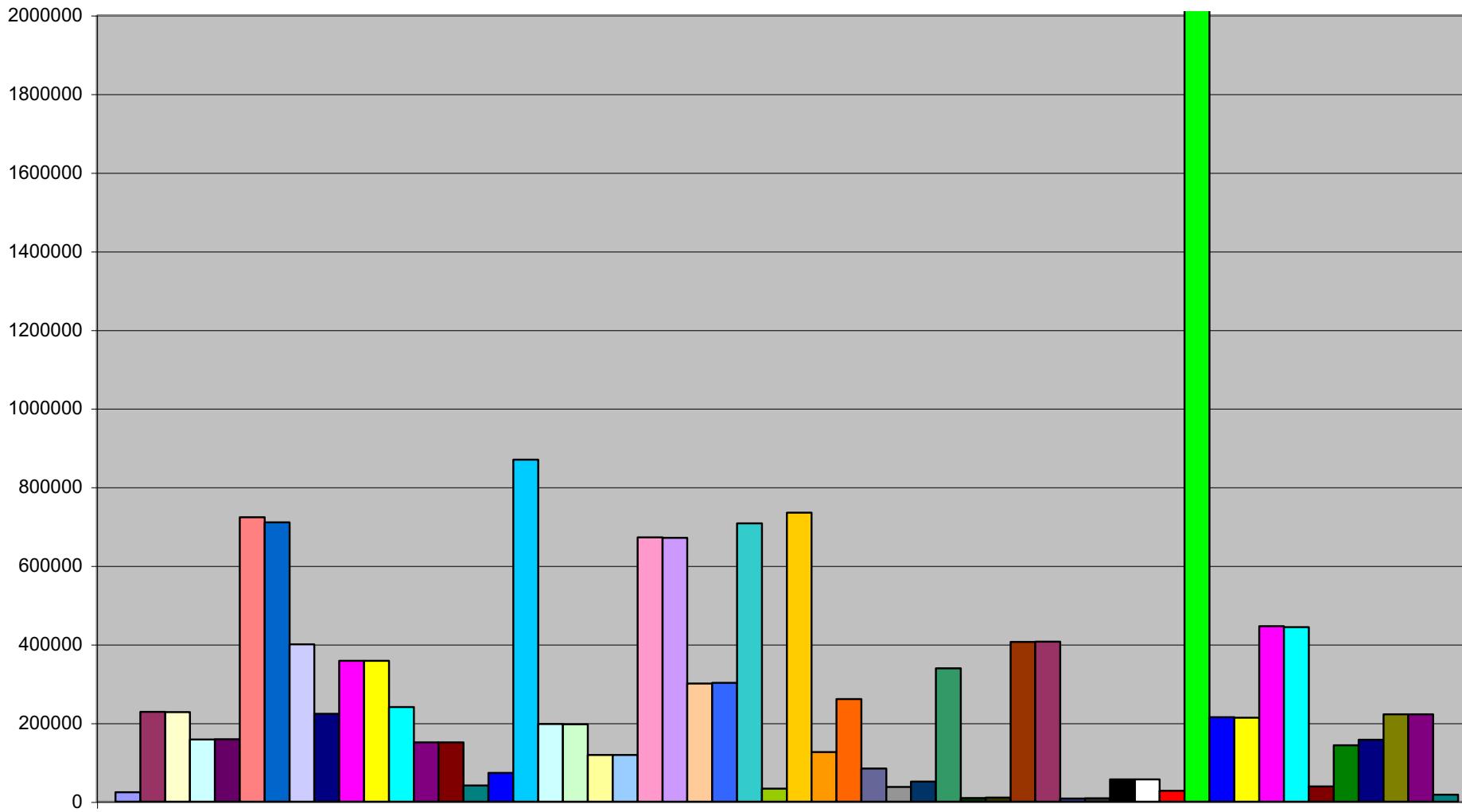
Week 3

# Nachi 8/18/03 4:00AM



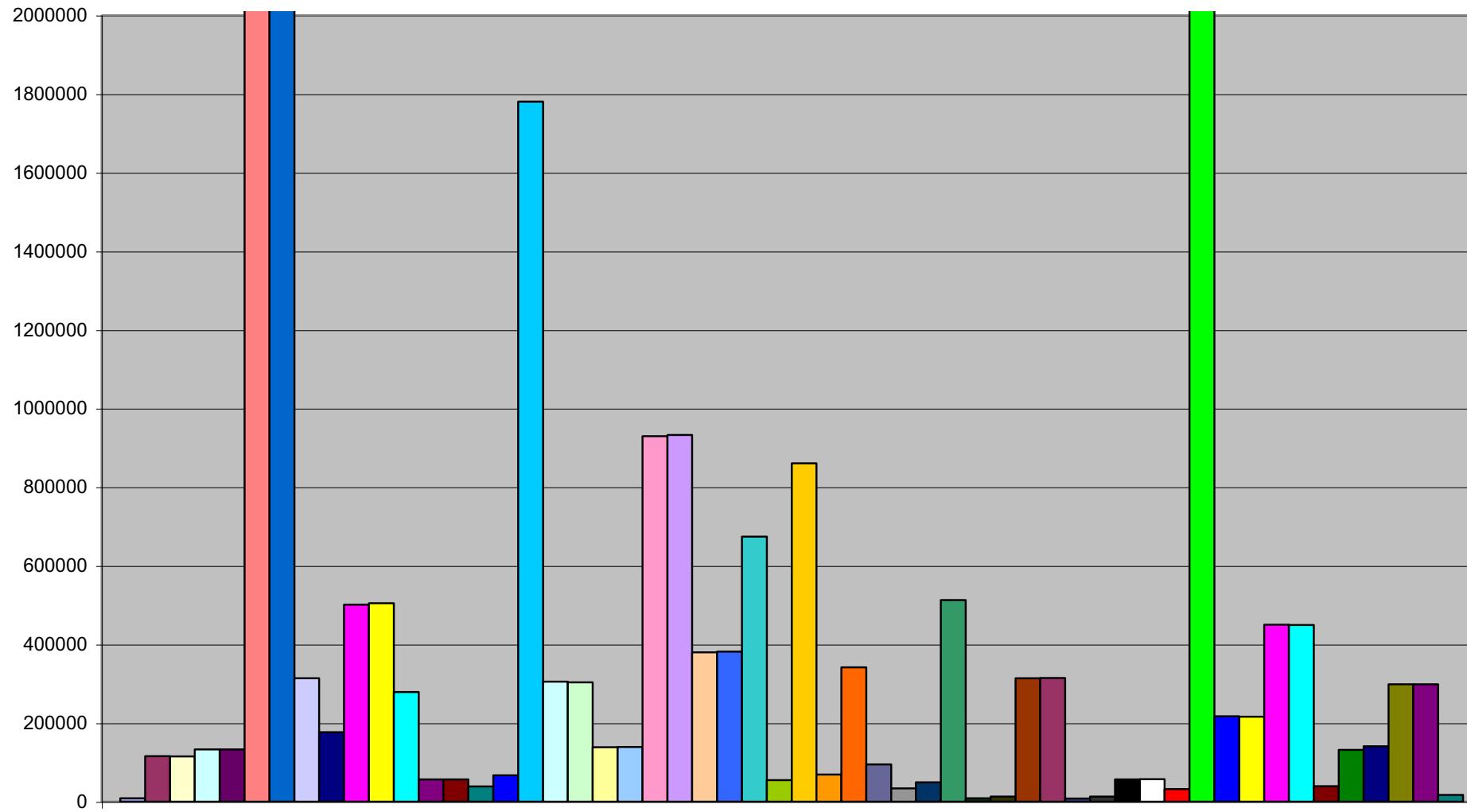
Week 3

# Nachi 8/18/03 5:00AM



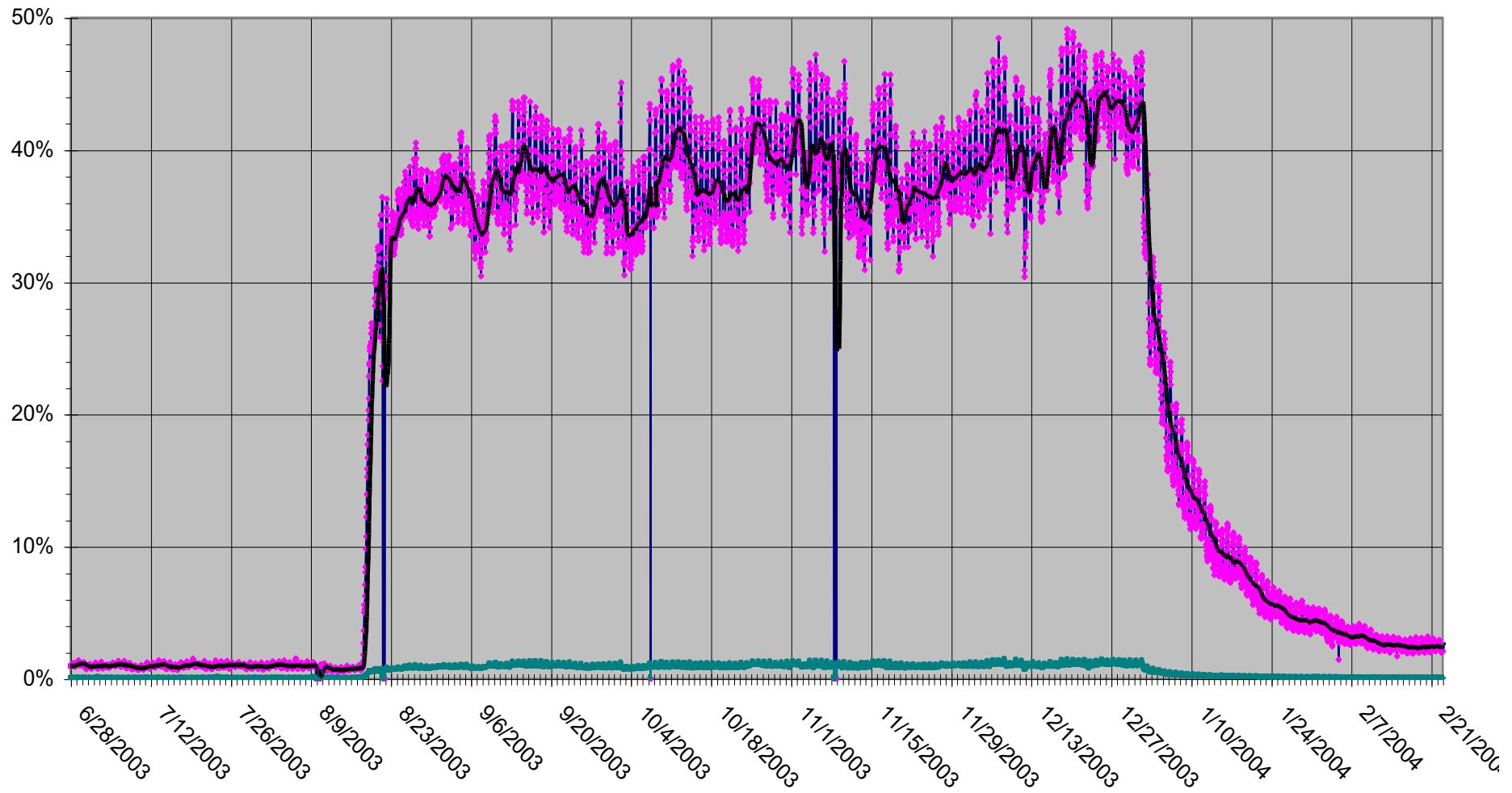
Week 3

# Nachi 8/18/03 6:00AM



Week 3

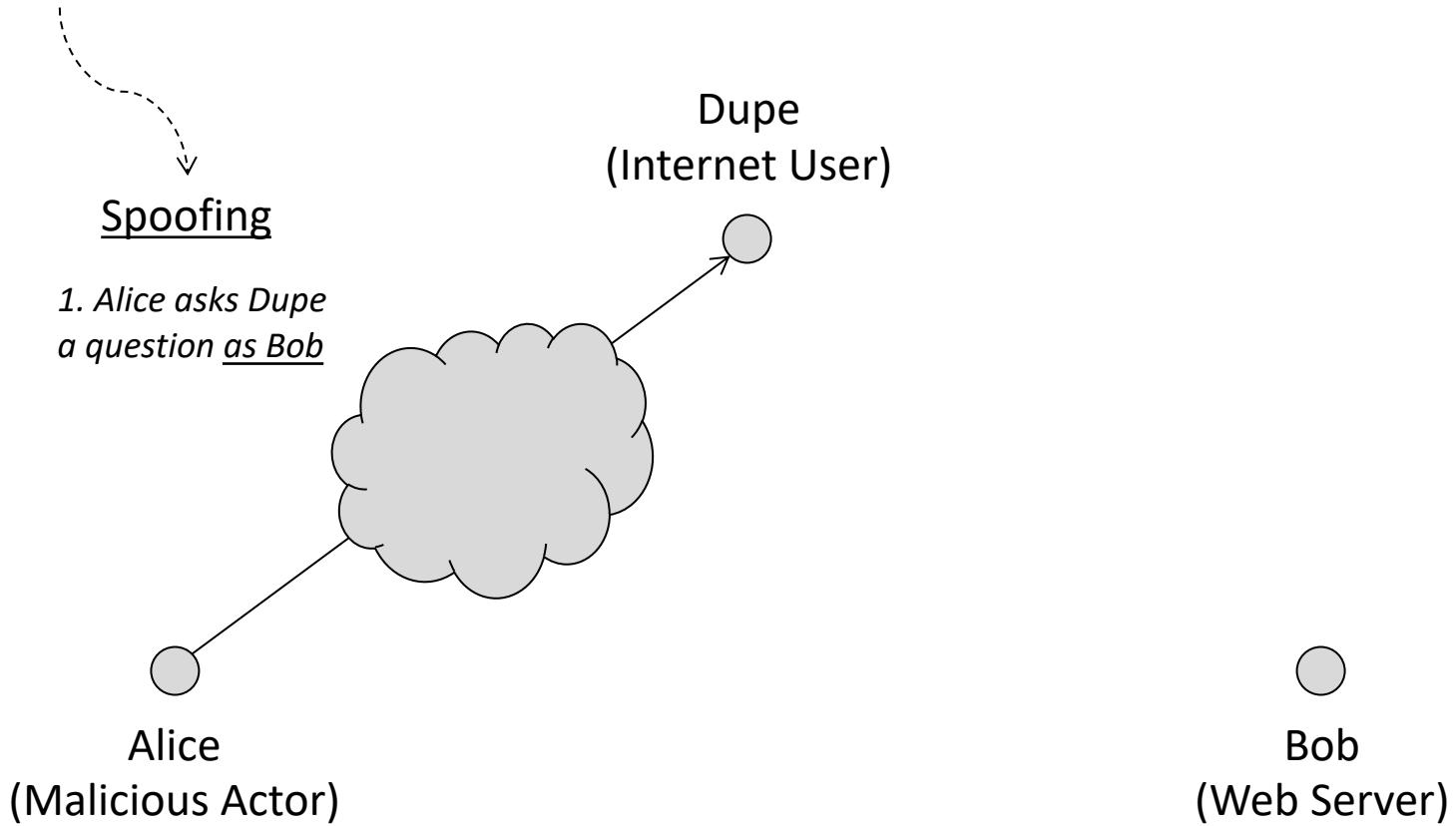
# Nachi Worm (08/03 – 01/04)



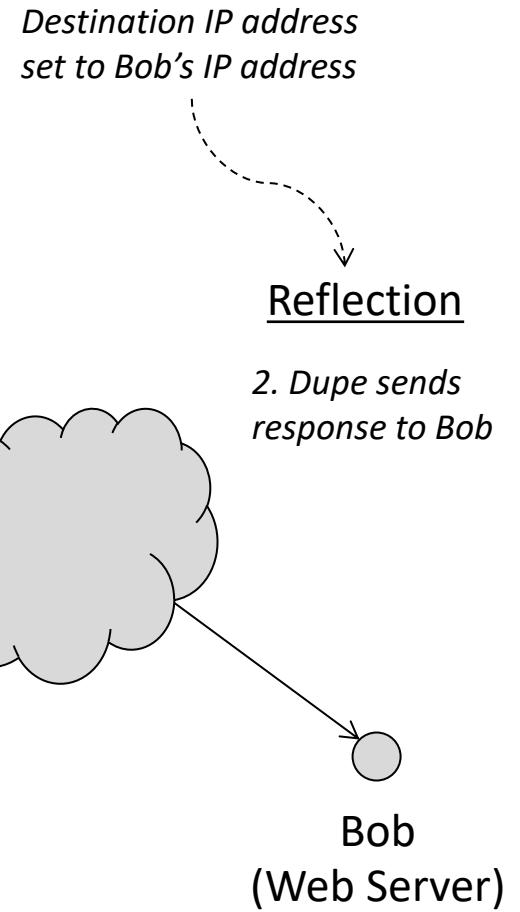
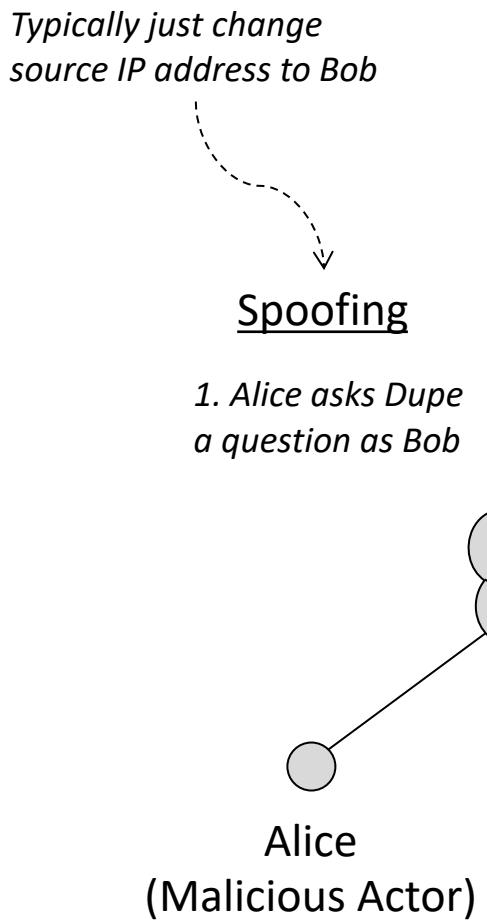
# How are Botnets Used for DDOS Attacks?

# Spoofing and Reflection

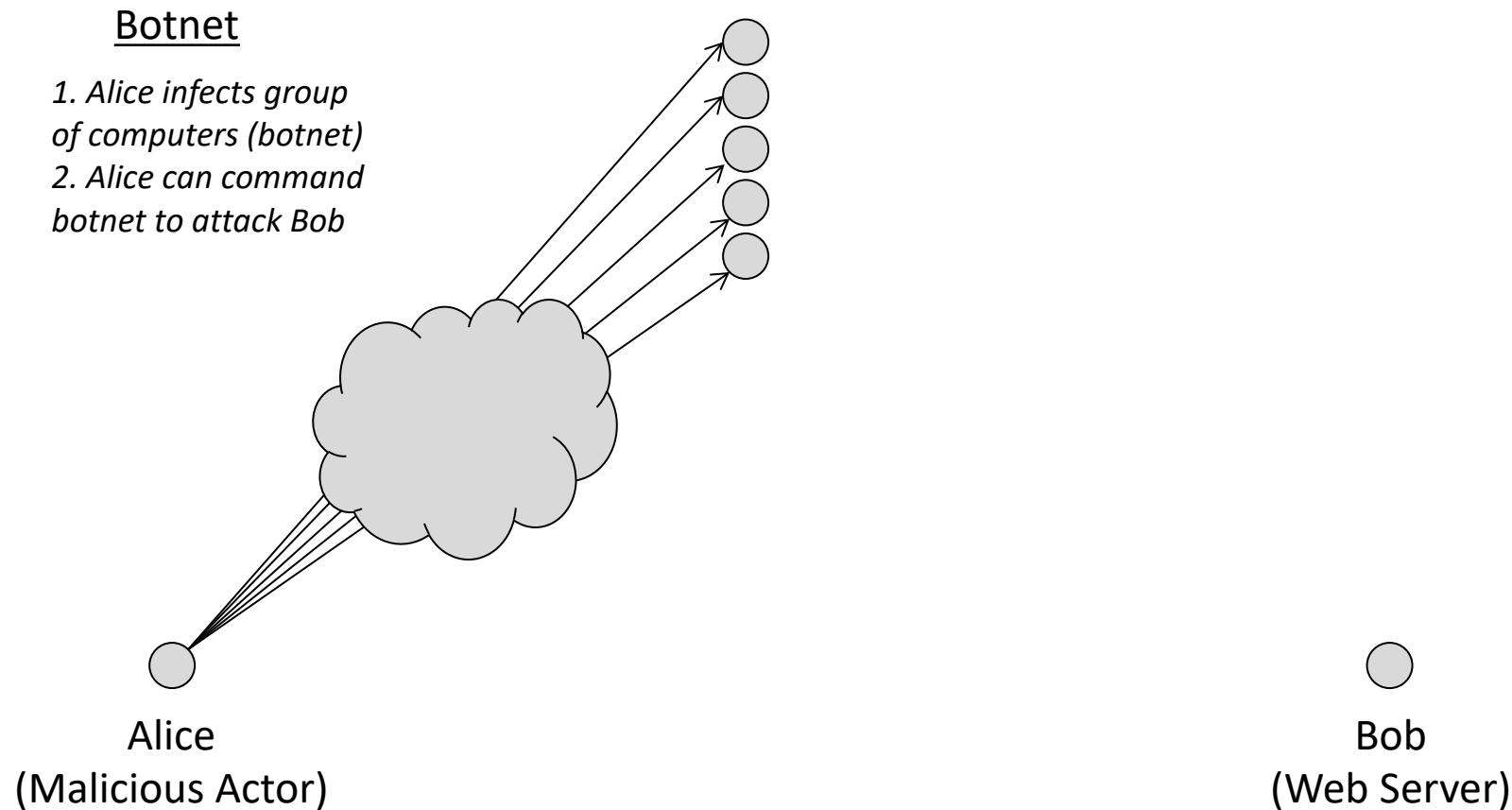
*Typically just change  
source IP address to Bob*



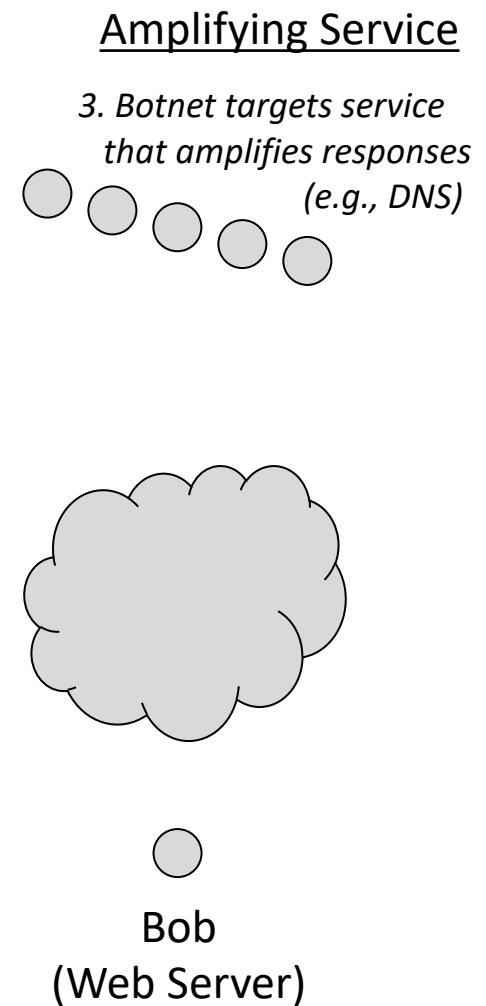
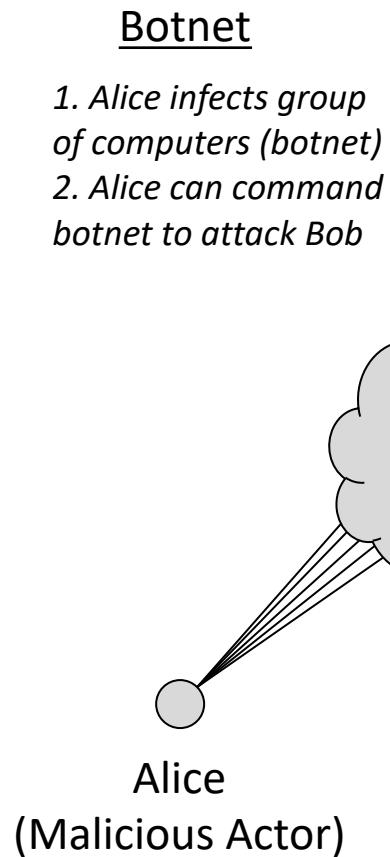
# Spoofing and Reflection



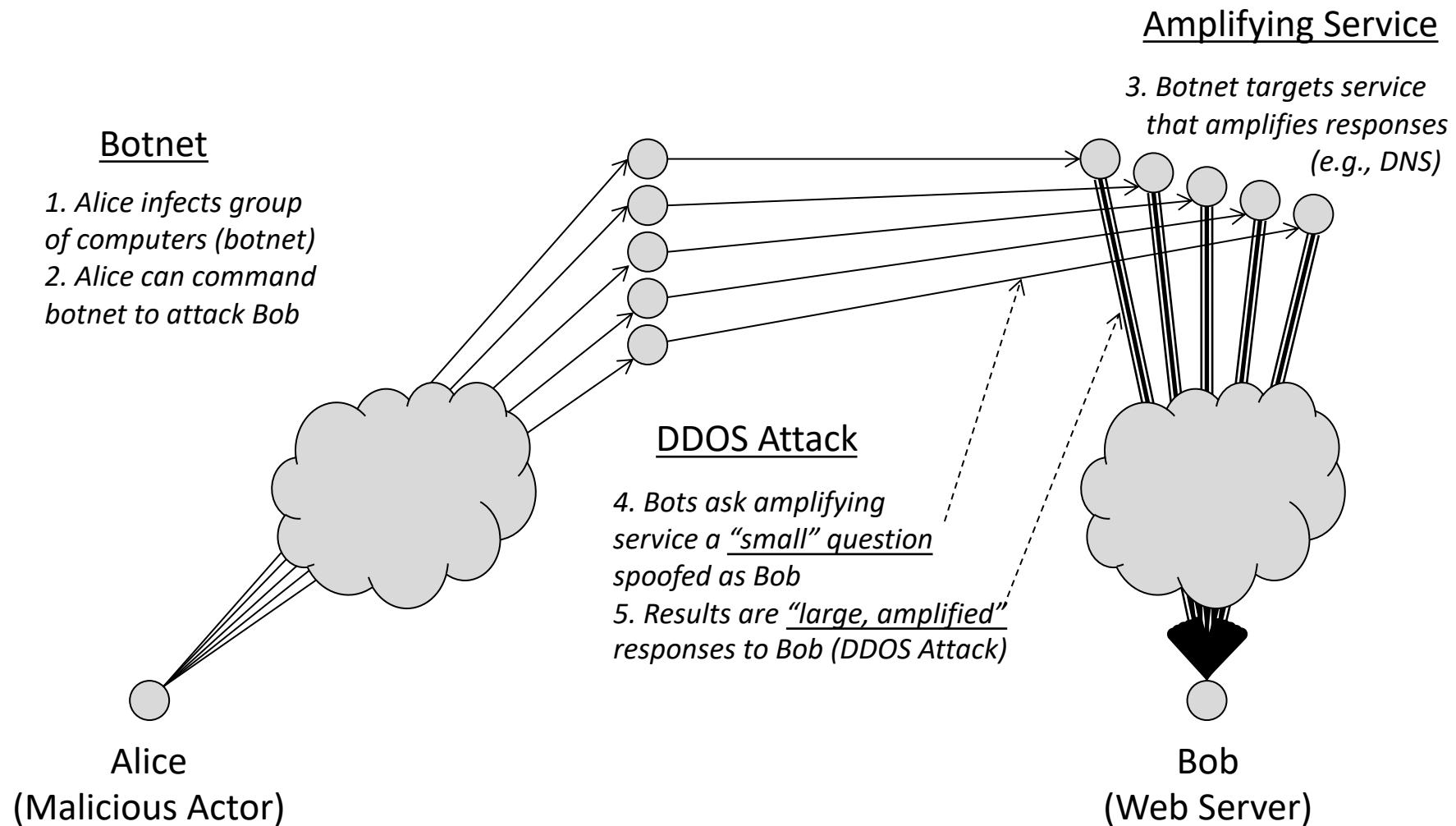
# Distribution and Amplification



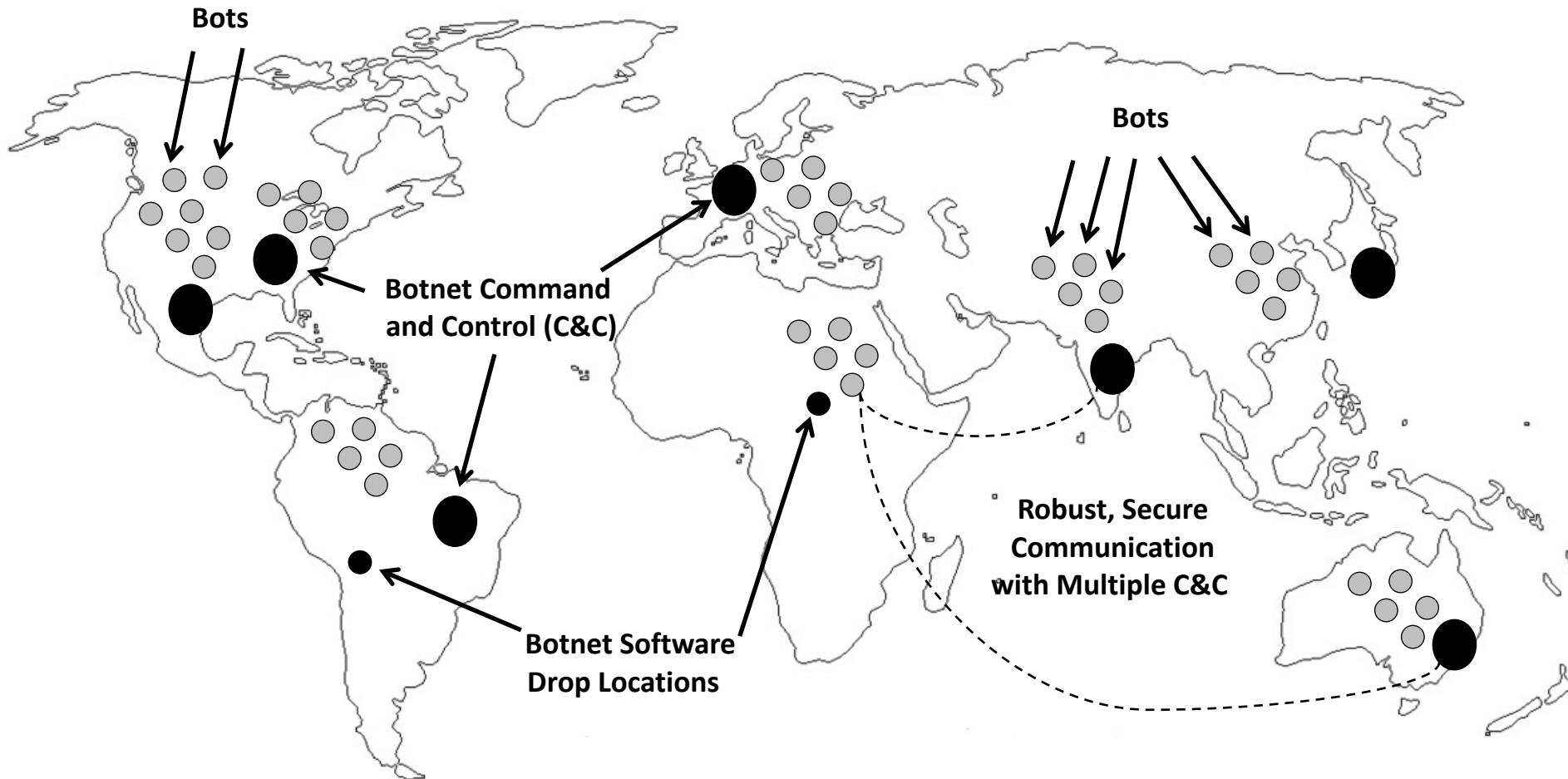
# Distribution and Amplification



# Distribution and Amplification



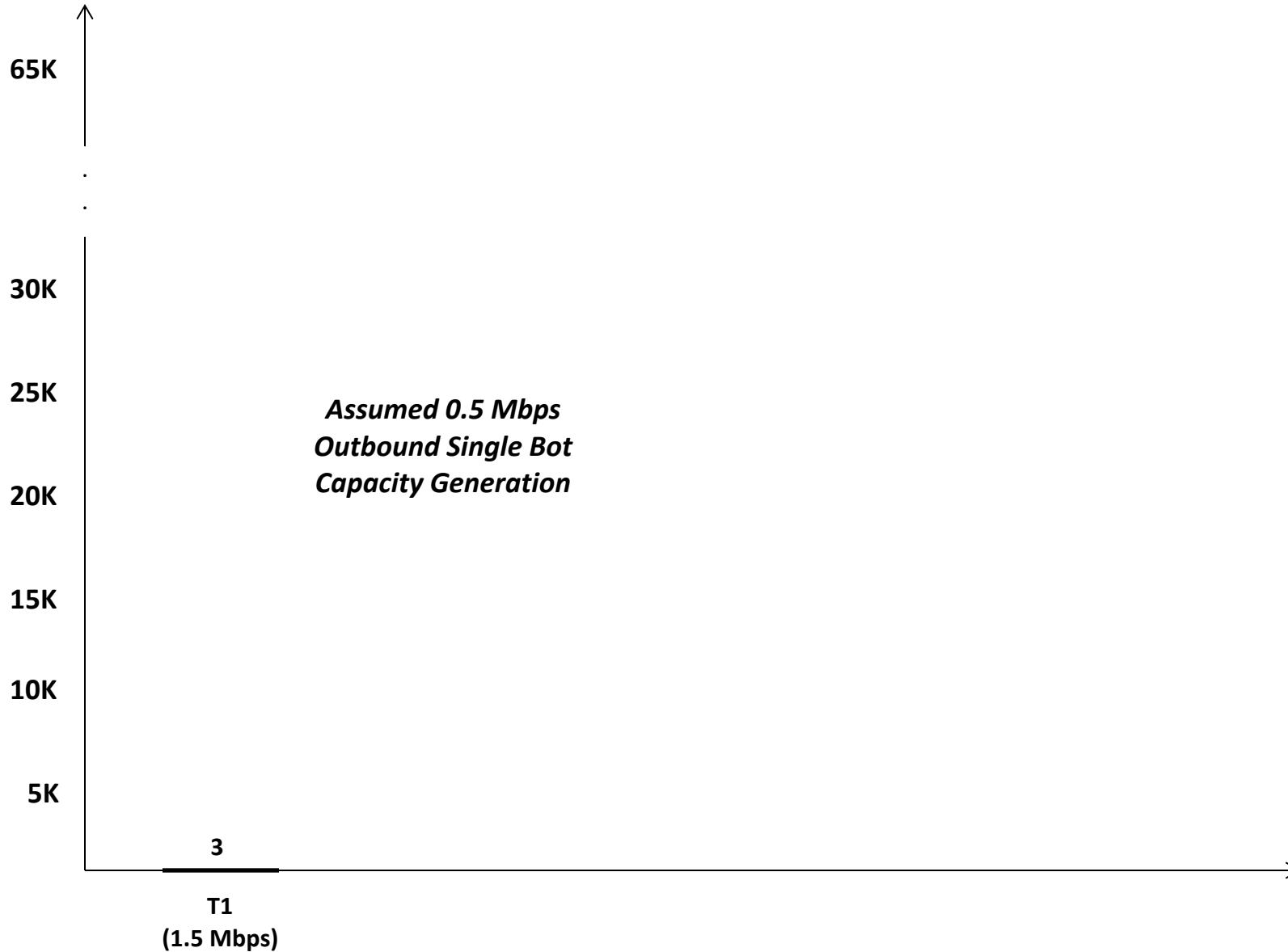
# Botnets



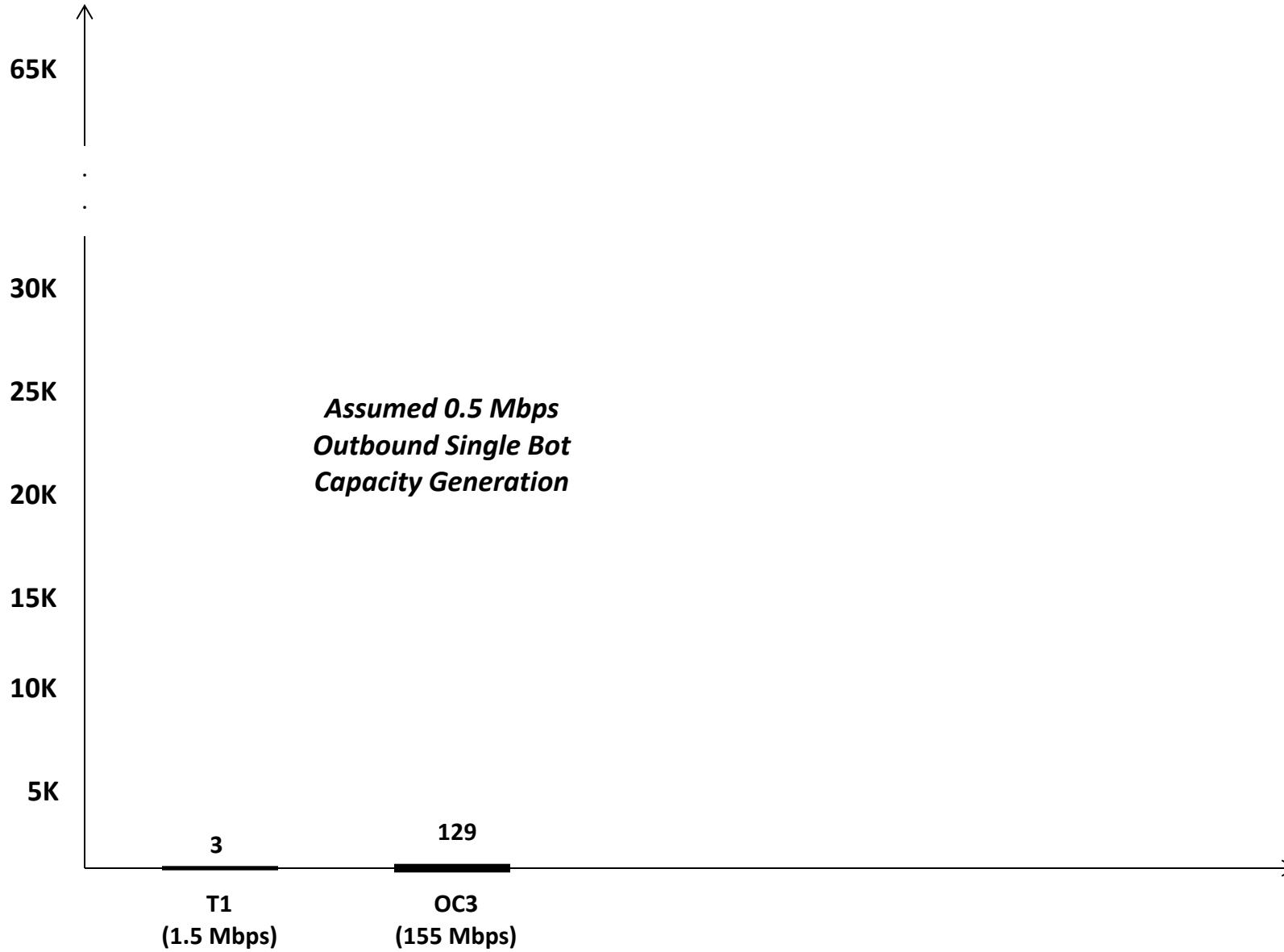
# Typical Botnet Visualization



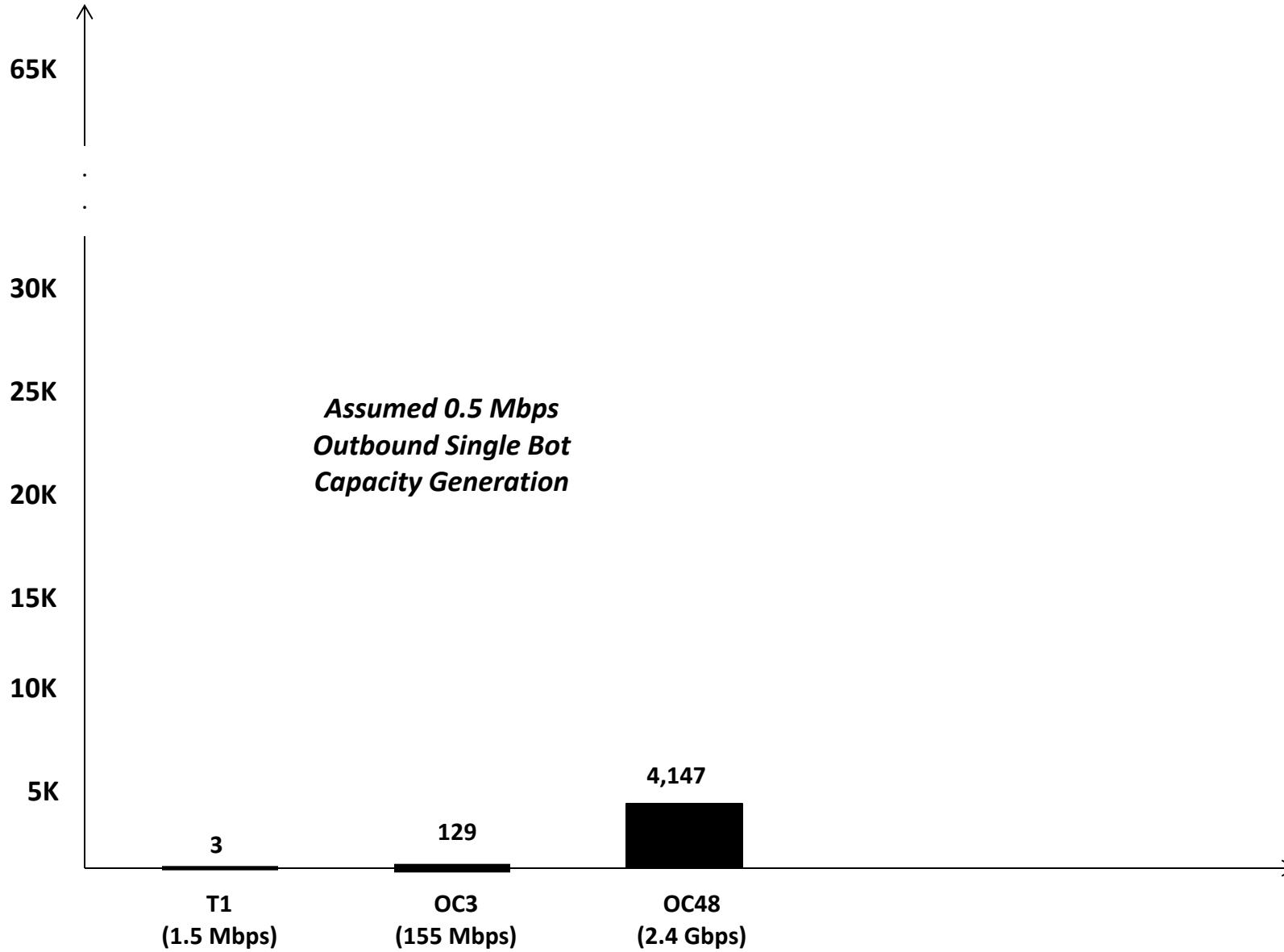
# Bot Capacity Generation (500Kbps)



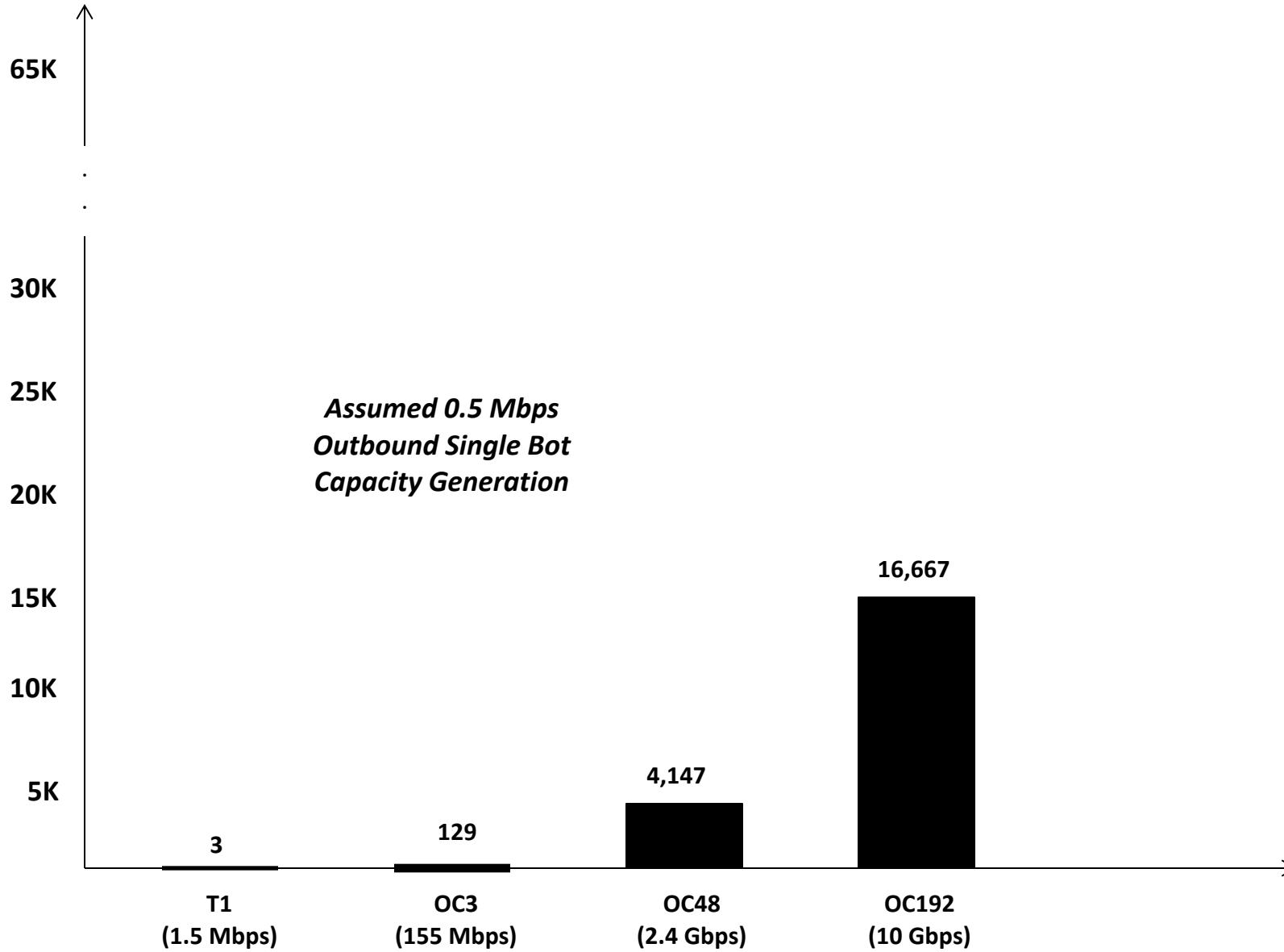
# Bot Capacity Generation (500Kbps)



# Bot Capacity Generation (500Kbps)

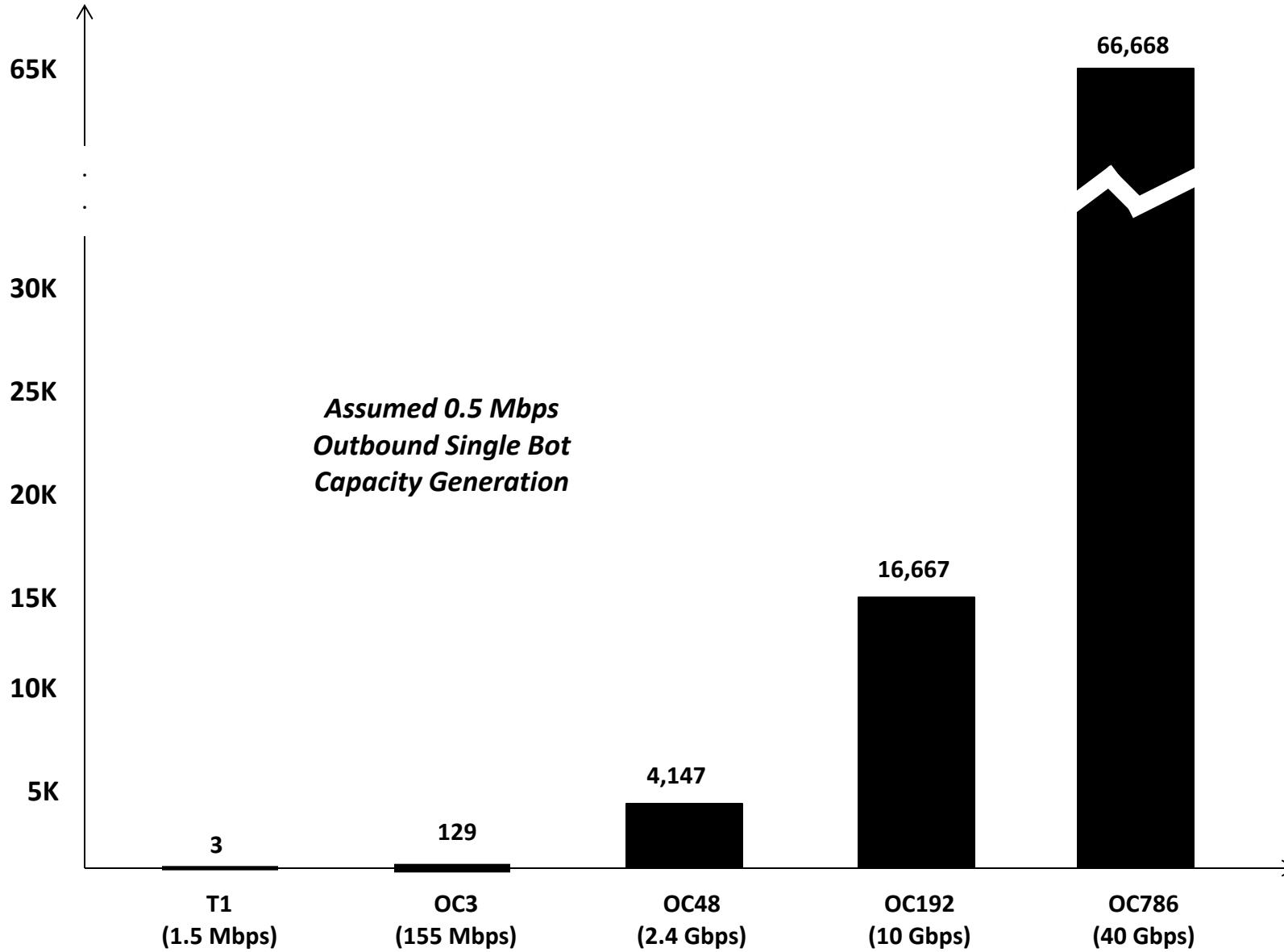


# Bot Capacity Generation (500Kbps)



Week 3

# Bot Capacity Generation (500Kbps)



# Botnet Capacity Generation (750 Kbps – 1.0 Mbps)

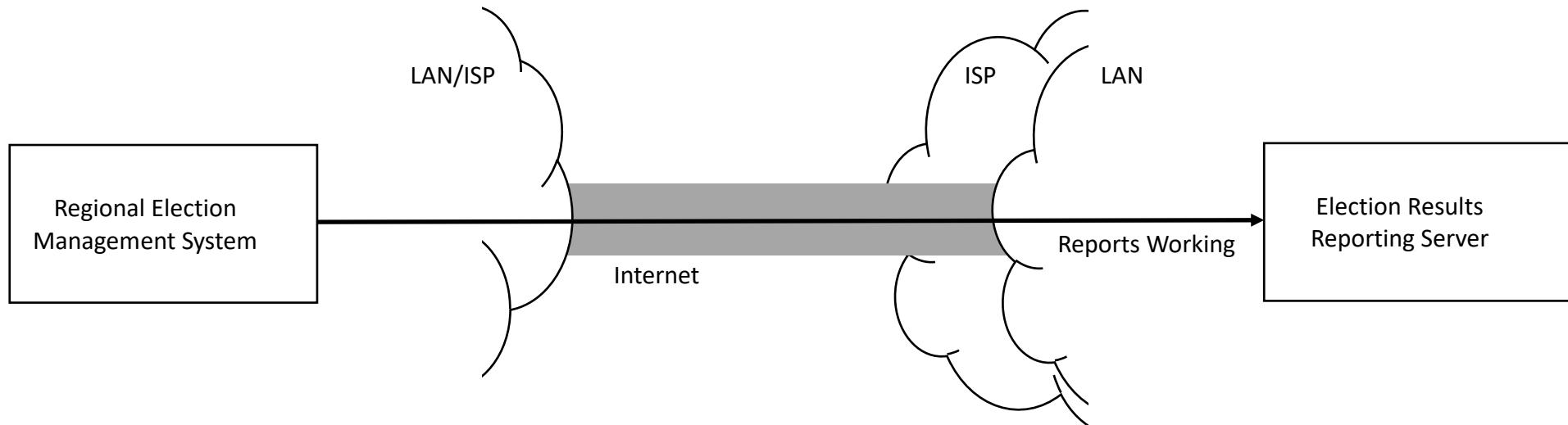
Number of Bots	Outbound Capacity	Size of Attack	Network Size
2	750 Kbps	1.5 Mbps	T1
1,200	1.0 Mbps	1.2 Gbps	OC-24
2,400	1.0 Mbps	2.4 Gbps	OC-48
10,000	1.0 Mbps	10.0 Gbps	OC-192
40,000	1.0 Mbps	40.0 Gbps	OC-768
80,000	1.0 Mbps	80.0 Gbps	<i>Starts to fill typical ISP backbone</i>
100,000	1.0 Mbps	100 Gbps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

Week 3

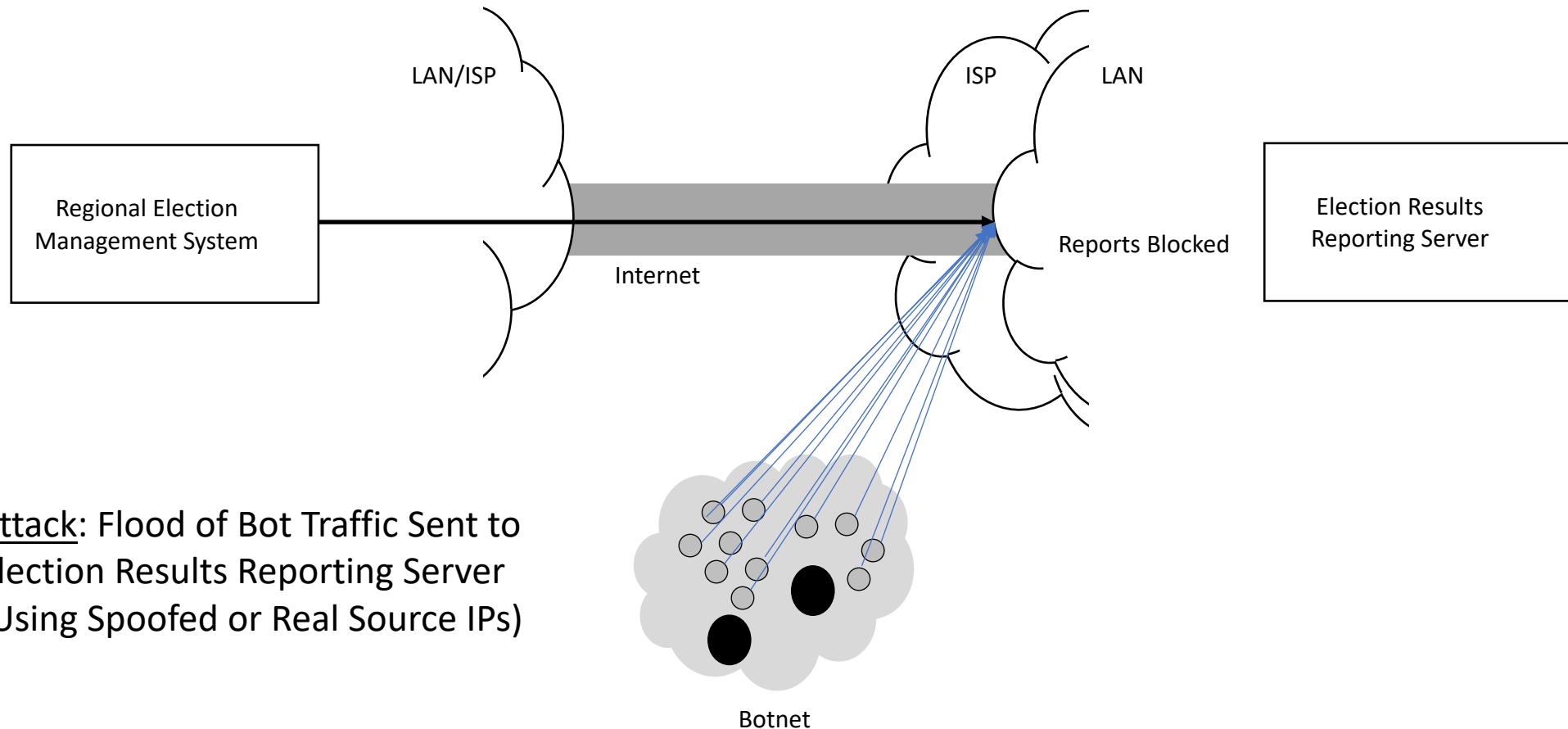


# Can You Stop DDOS Attacks?

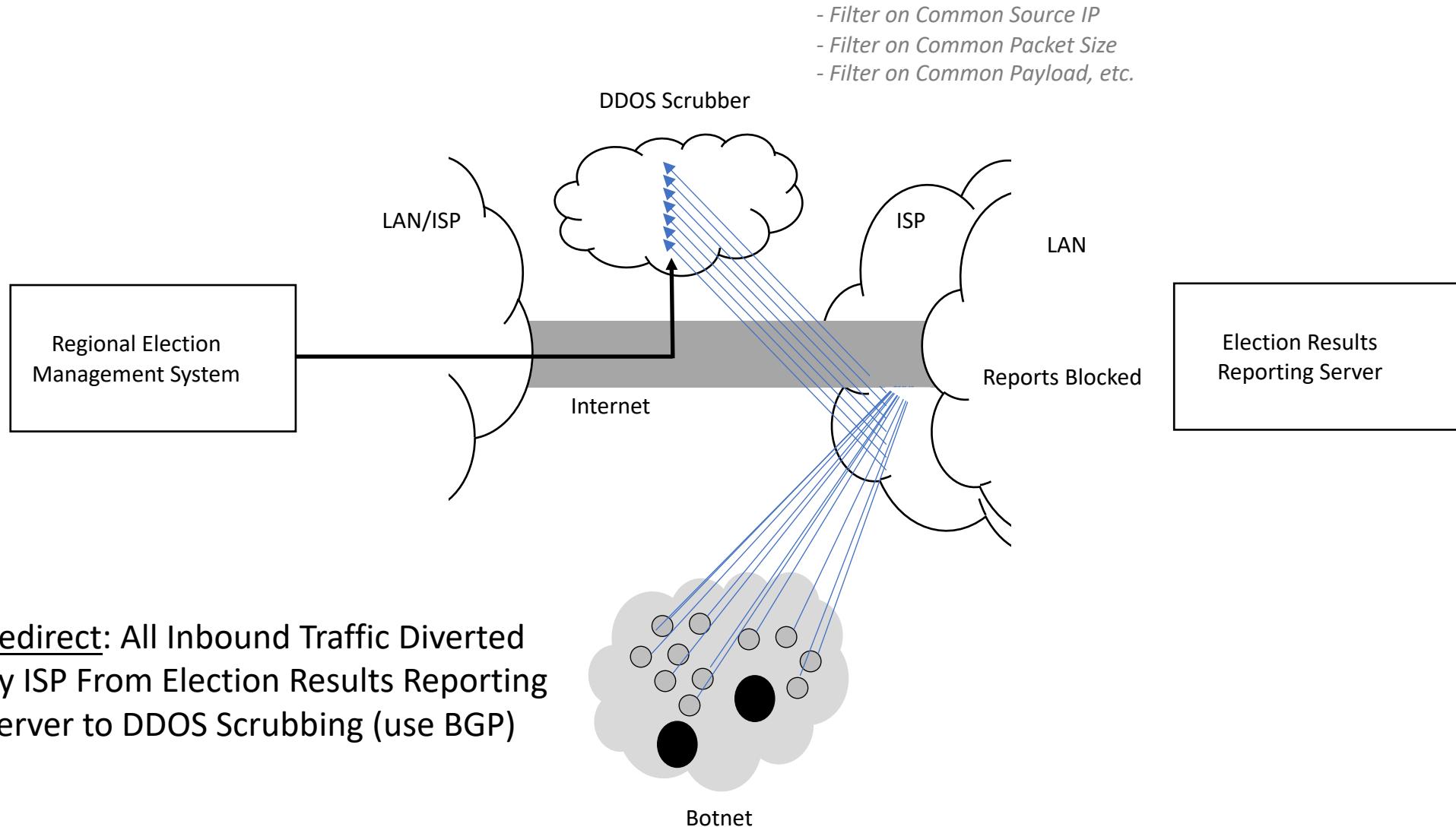
# Case Study: Mitigating Inbound Election Reporting DDOS



# Case Study: Mitigating Inbound Election Reporting DDOS



# Case Study: Mitigating Inbound Election Reporting DDOS



# Case Study: Mitigating Inbound Election Reporting DDOS

