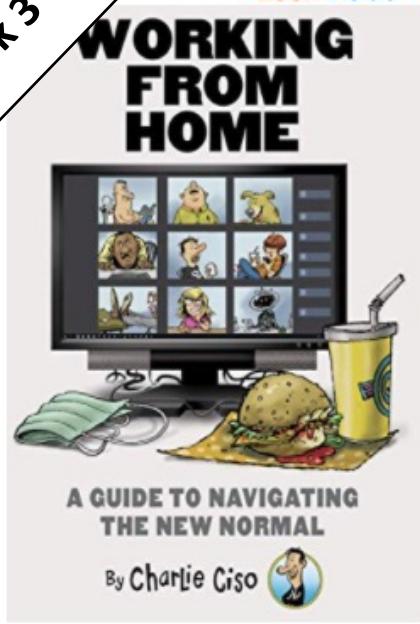




An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
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.



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 ▾ 0 Cart

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"

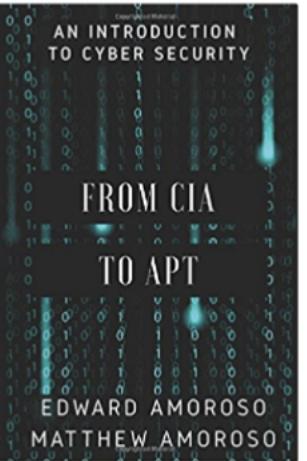
From CIA to APT: An Introduction to Cyber Security and over one million other books are available for Amazon Kindle. Learn more

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

▶ 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

Look inside ↗

Flip to back
See all 2 images

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.

Read more

Report incorrect product information.

Share    

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 ▾

https://tag-cyber.com/advisory/quarterly

TAG CYBER

Research Content Advisory Publications Taxonomy About Climate

Let's Talk

TAG Cyber Quarterly

The TAG Cyber Quarterly includes original works from our analysts, including interviews with icons in the cybersecurity industry. Available for free download, our Quarterly is designed to provide insights through reporting, surveys, analysis, and other original pieces.

Download Latest Quarterly

[Recommended Additional Reading: https://www.tag-cyber.com/](https://www.tag-cyber.com/)

Required Week Three Readings:

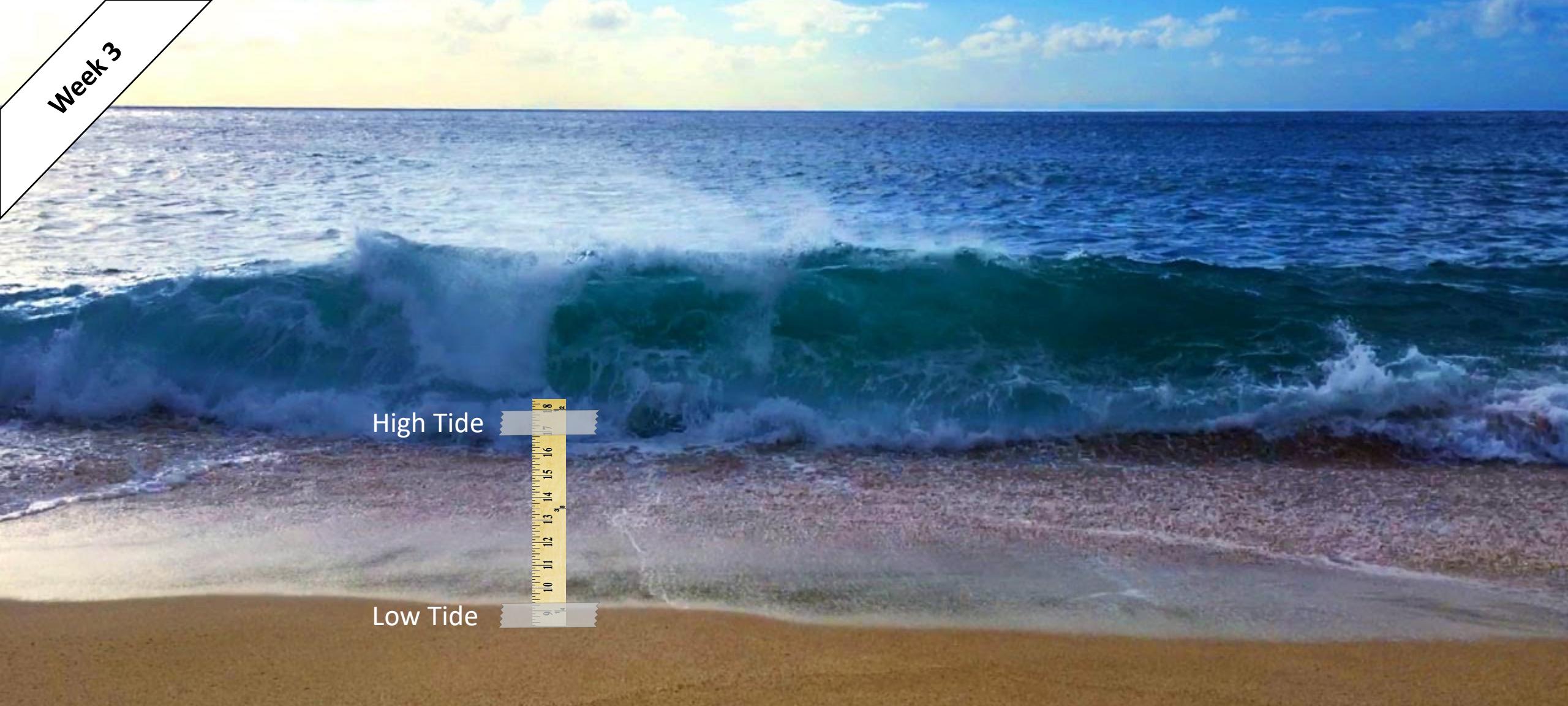
1. “The Birth and Death of the Orange Book,” Steve Lipner

<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"

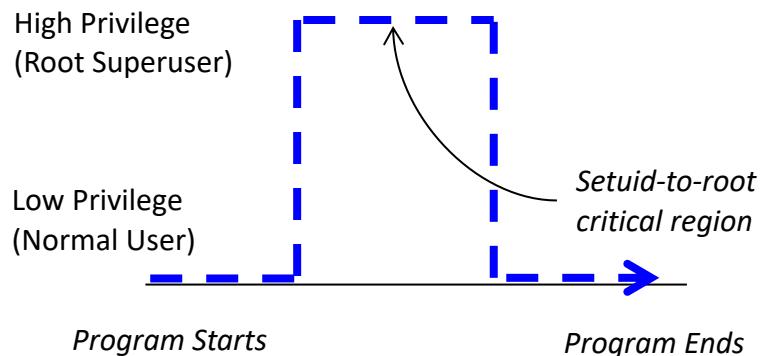
Classic Unix Kernel Attack

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

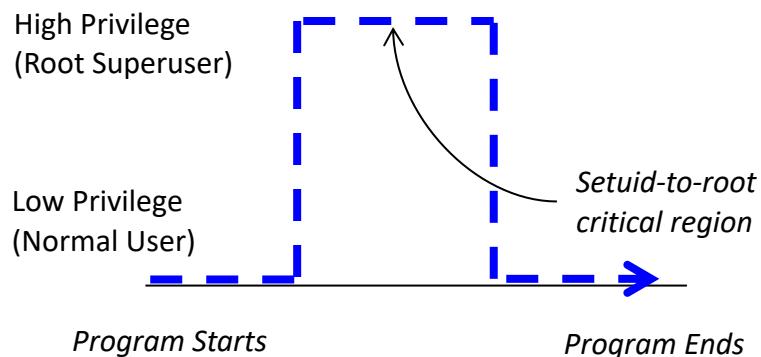
- Set IFS variable to include ‘/’
- “/etc/file” same as “etc file”

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

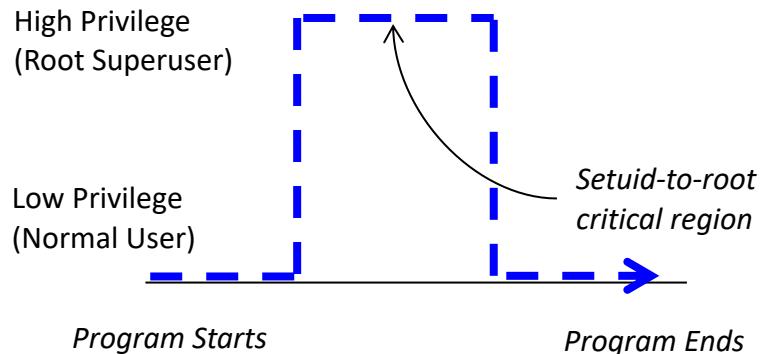
- Allows increase in privilege
- Normal user to Unix “Root”

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 the shell (“cp sh myshell”)
- Copied program inherits privileges



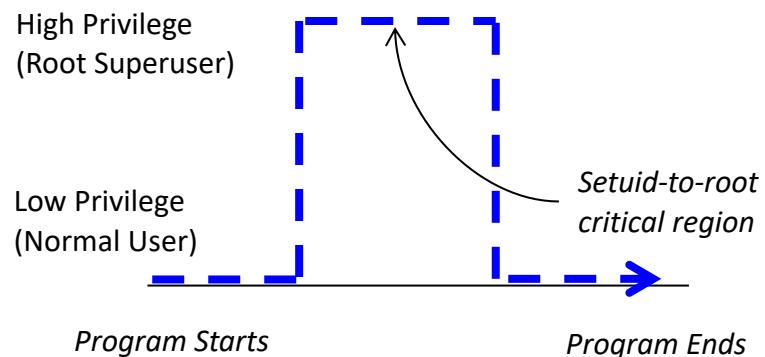
Classic Unix Kernel Attack

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 the shell ("cp sh myshell")
- Copied program inherits privileges

Unix Kernel Attack:

- Step 1: Set IFS variable to include '/'
- Step 2: Create UNIX shell program called "etc" that performs "cp sh myshell"
- Step 3: Run "at" program, which will run "etc"
- Step 4: Now "etc" should copy sh to myshell
- Result: myshell is a root shell owed by me!

Classic Unix Kernel Attack

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

Classic Buffer Overflow Attack Code

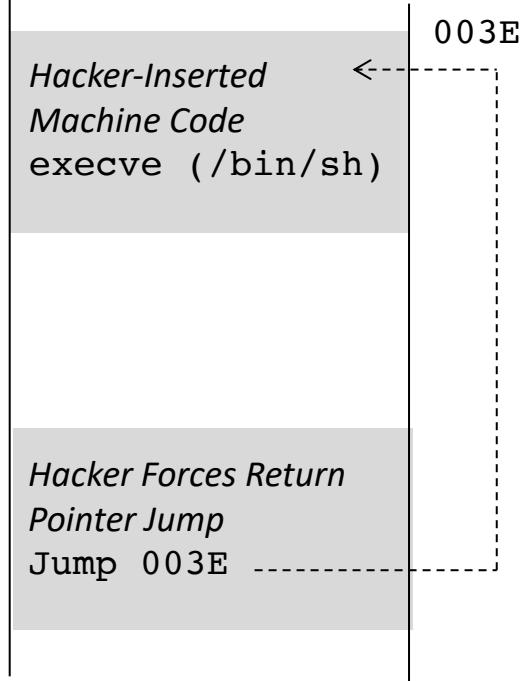
```
void overflow_function(char *string)
{
    char buffer[16];
    strcpy(buffer, string);
    return;
}

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



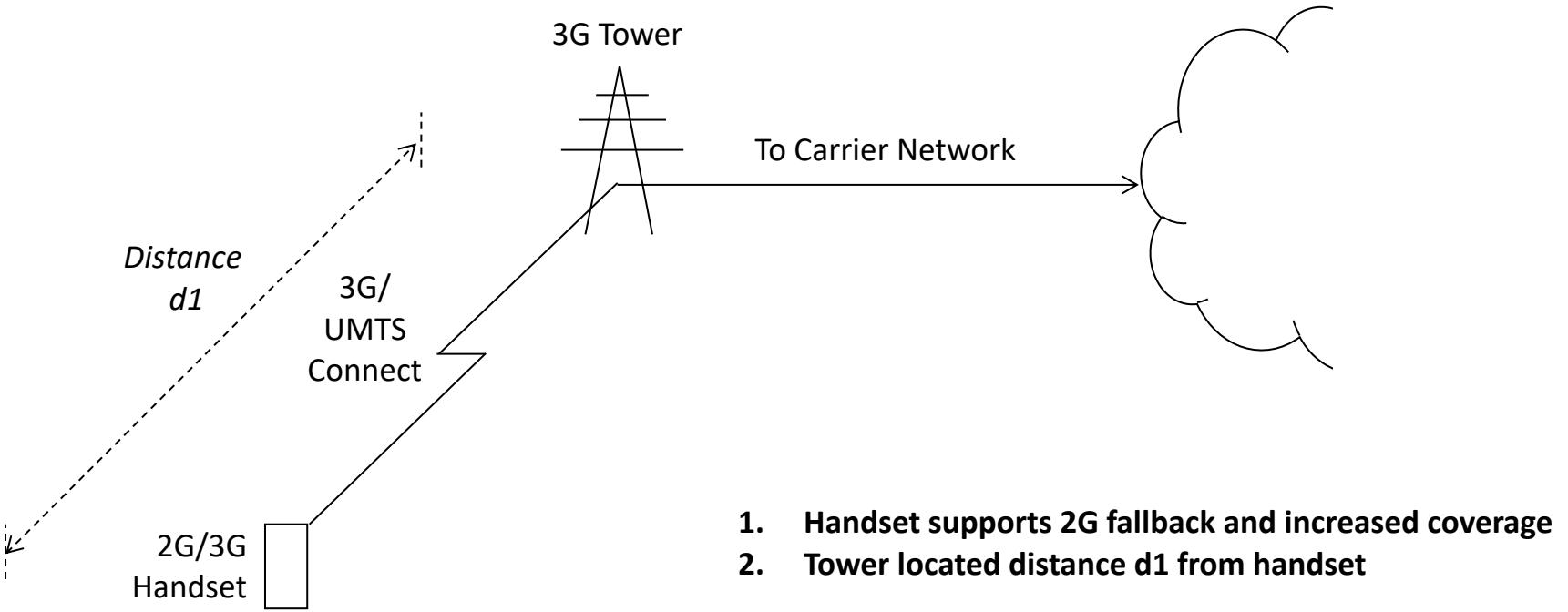
```
void overflow_function(char *string)
{
    char buffer[16];
    strcpy(buffer, string);
    return;
}

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

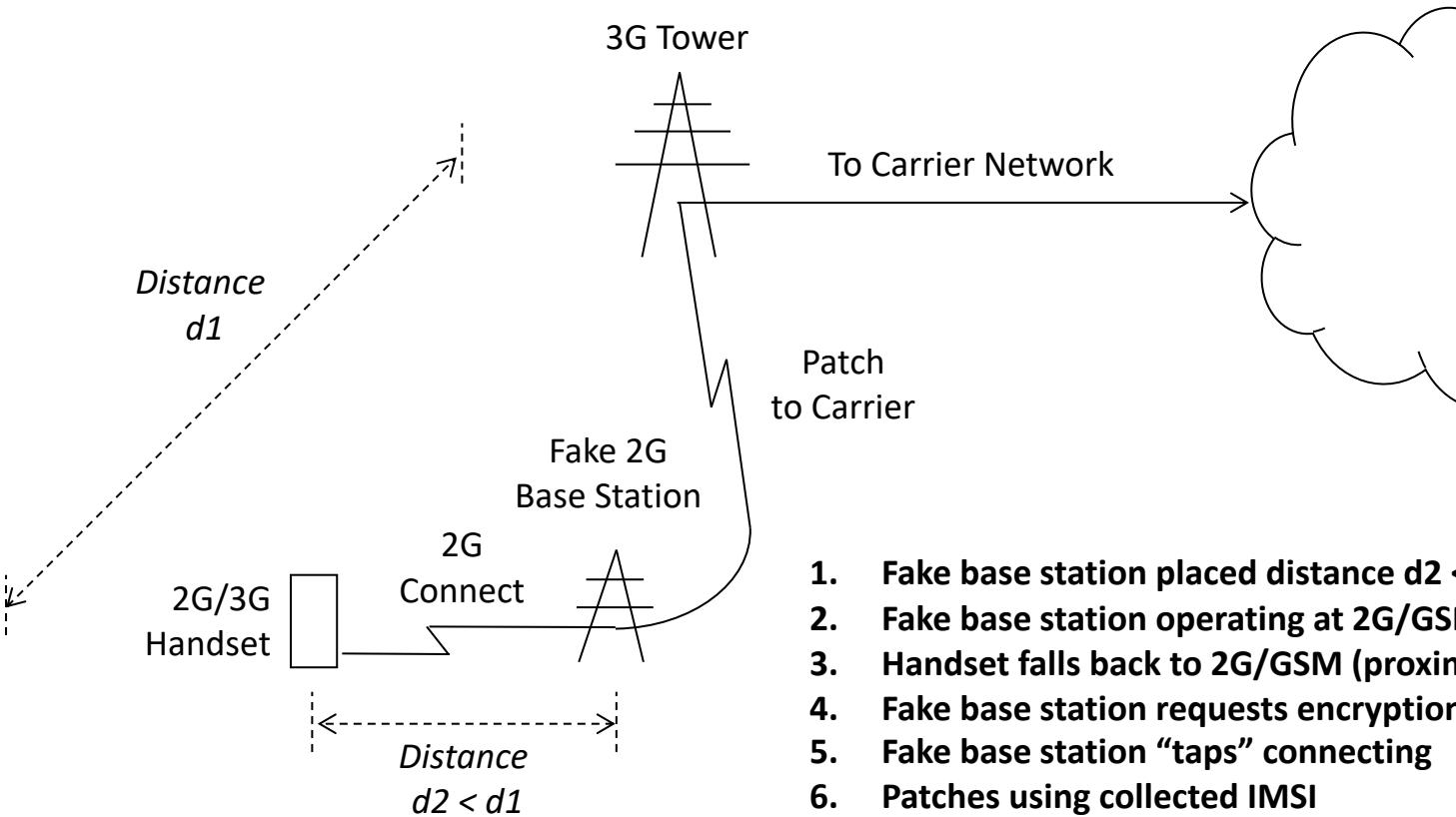
    for(i=0; i<255; i++)
        large_buffer[i]='A';

    overflow_function(large_buffer);
}
```

Classic Buffer Overflow Attack Code



Classic 3G Mobile Intercept Attack (Fake Base Station)



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](#)

Enter a course name or other keyword



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.

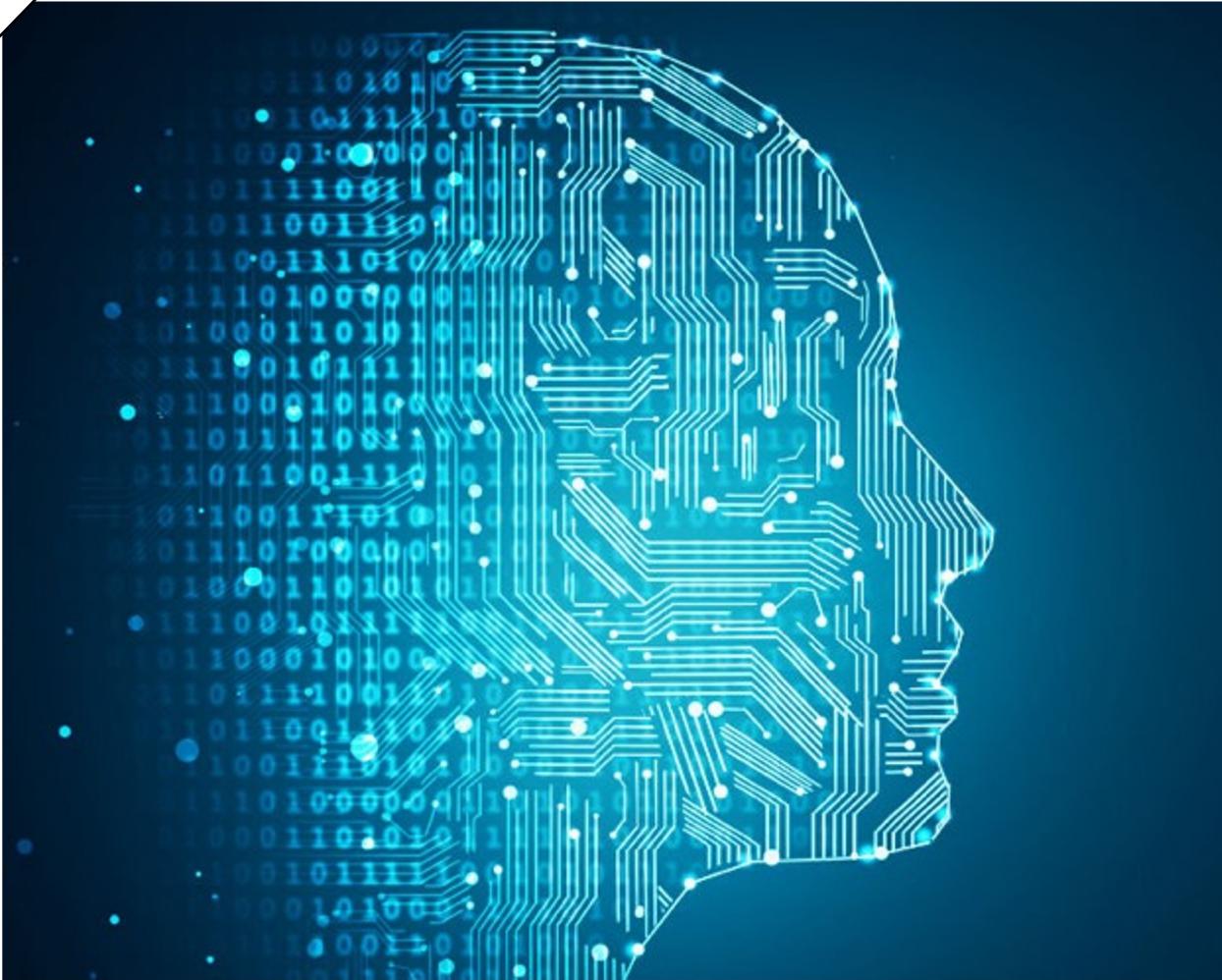
[BOOK YOUR COURSE](#) [VIEW PRICE NOW](#)



InfoSec Institute Ethical Hacker Program

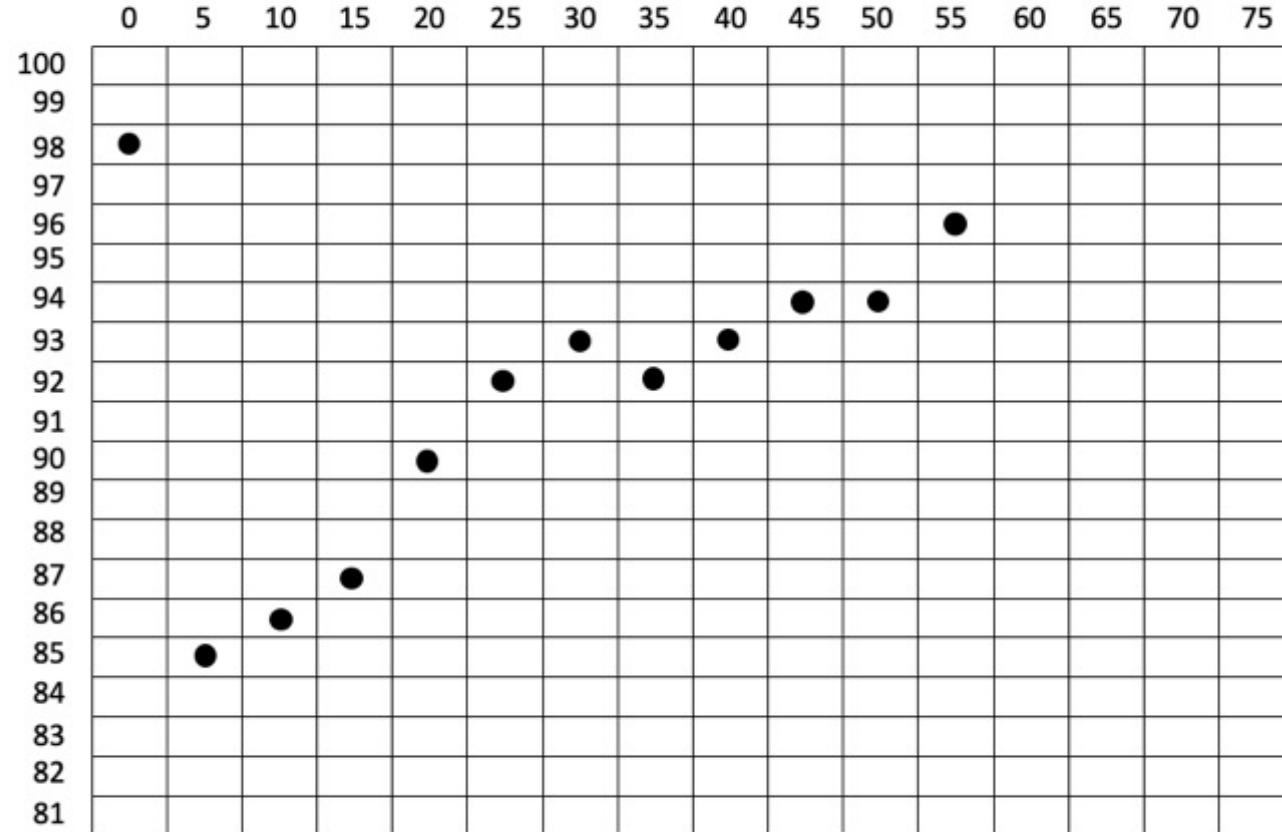
How Can Machine Learning be Used for Network Security?

You Already Understand
Basic Linear Regression



Developing an AI to Predict Student GPA

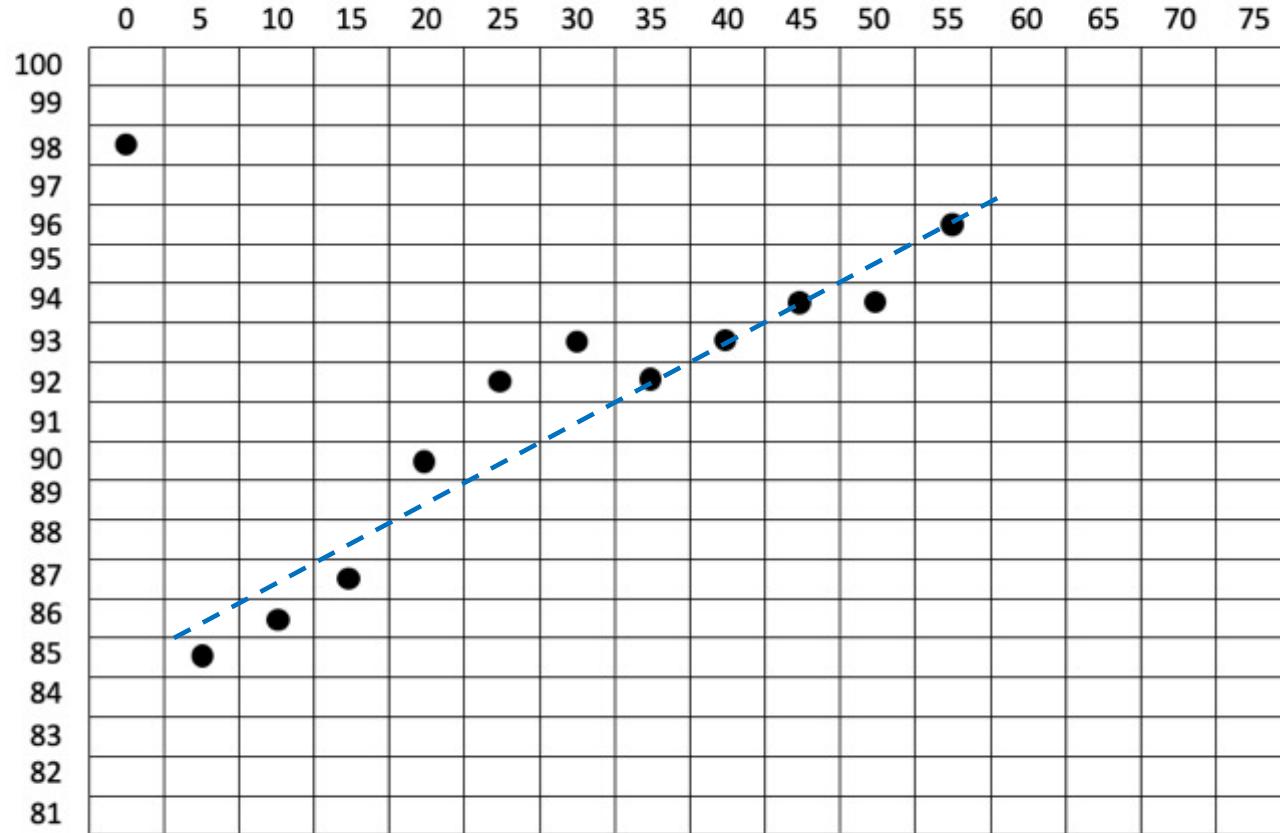
Grade
Point
Average
(GPA)



Minutes Spent Studying	Grade Point Average
0	98
5	85
10	86
15	87
20	90
25	92
30	93
35	92
40	93
45	94
50	94
55	96

Let's Start with Some Training Data

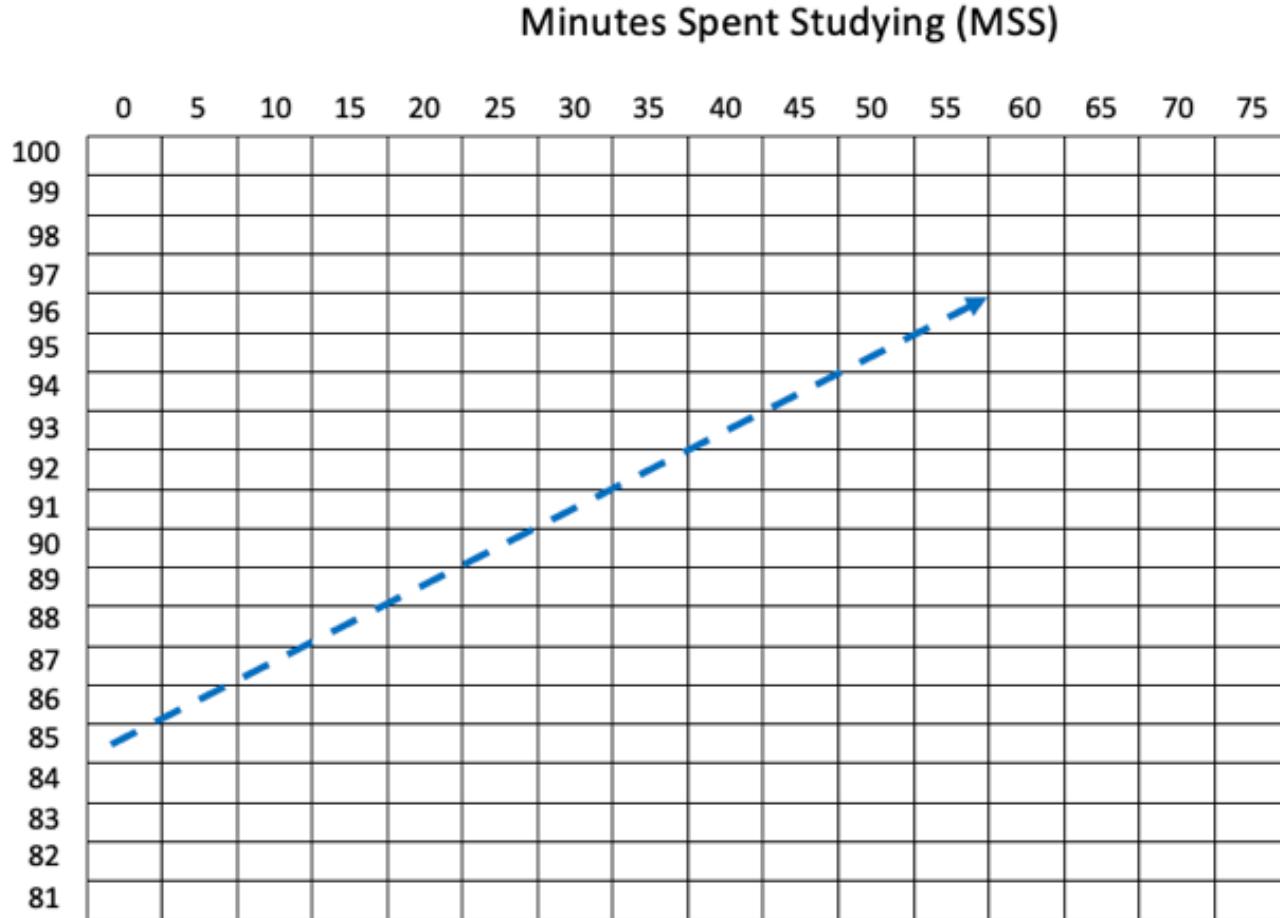
Grade
Point
Average
(GPA)



Minutes Spent Studying	Grade Point Average
0	98
5	85
10	86
15	87
20	90
25	92
30	93
35	92
40	93
45	94
50	94
55	96

Now Let's Graph a Learning Model (From Sixth Grade Math)

Grade
Point
Average
(GPA)



$$y = mx + b$$

$$\text{GPA} = m (\text{MSS}) + b$$

(where $(\text{MSS} > 0)$)

$$\text{GPA} = 0.2 (\text{MSS}) + 85$$

Now We Have a Predictive Model (2 Dimensions)

ChatGPA



Examples

"Explain quantum computing in simple terms" →



Capabilities

"Got any creative ideas for a 10 year old's birthday?" →



Limitations

"How do I make an HTTP request in Javascript?" →

May occasionally generate incorrect information

Allows user to provide follow-up corrections

May occasionally produce harmful instructions or biased content

Trained to decline inappropriate requests

Limited knowledge of world and events after 2021

If I spend 30 minutes studying, what will be my GPA?



Let's Use
Natural Language
to Support GPA
Queries

EA

If I spend 30 minutes studying, what will be my GPA?



Based on our linear regression model, if you spend 30 minutes studying, then it is likely that your GPA will be 91.0. Of course, all linear regression models are only as accurate as the factors used as input. Our model uses only one input factor to predict your GPA, so students should be careful interpreting our results.

Here is a
Simulated
AI-Generated
Response



ChatGPA Uses
1 Factor
to Predict Output



ChatGPT Uses
175 Billion Factors
to Predict Output

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



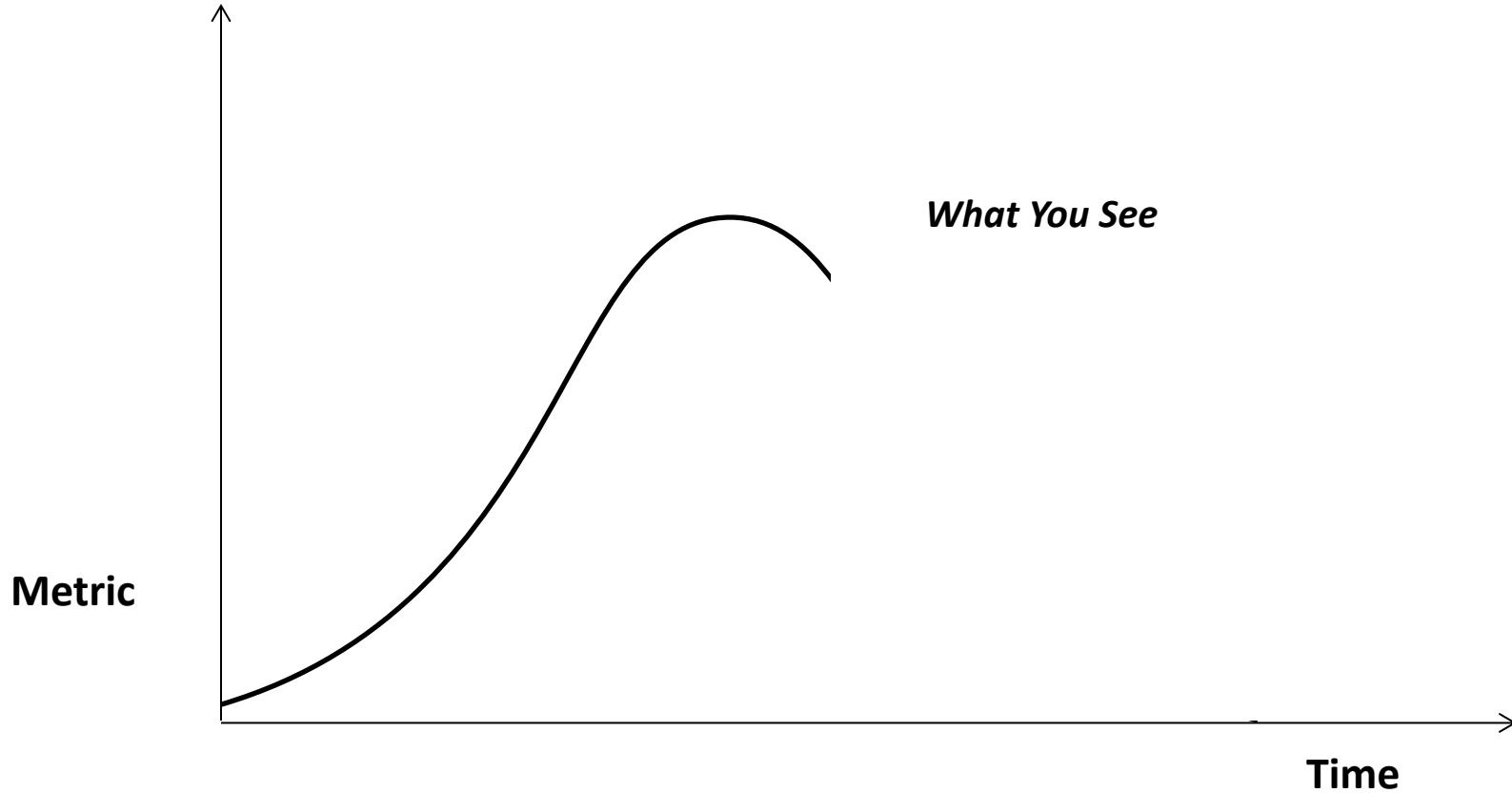
Training Data for App Security (Two Factors)

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

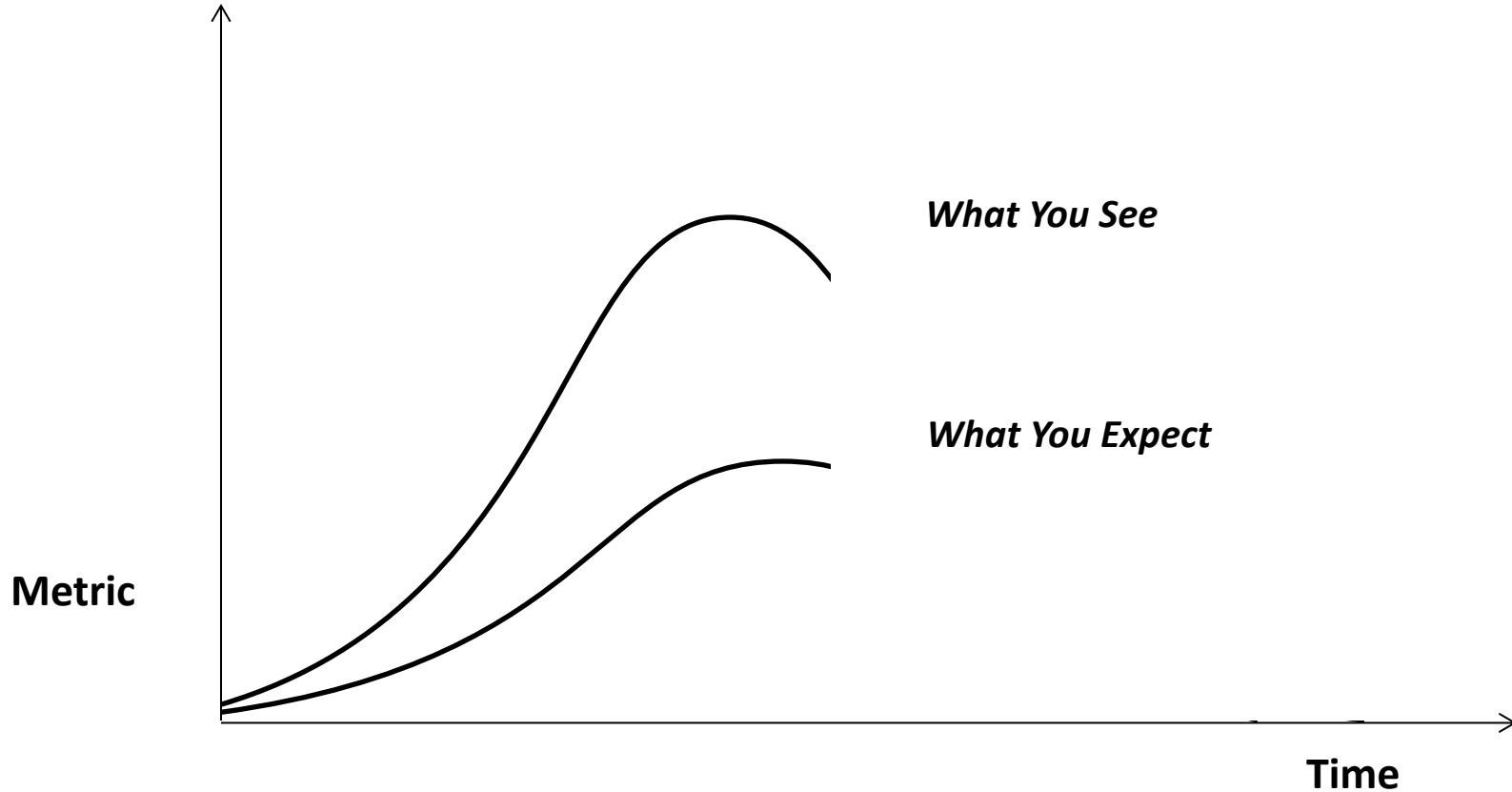
Linear Regression Strategy: Graph the Data and Use to Predict Number of Vulnerabilities from Two Input factors

How Can Network Security Attacks Be Visualized?

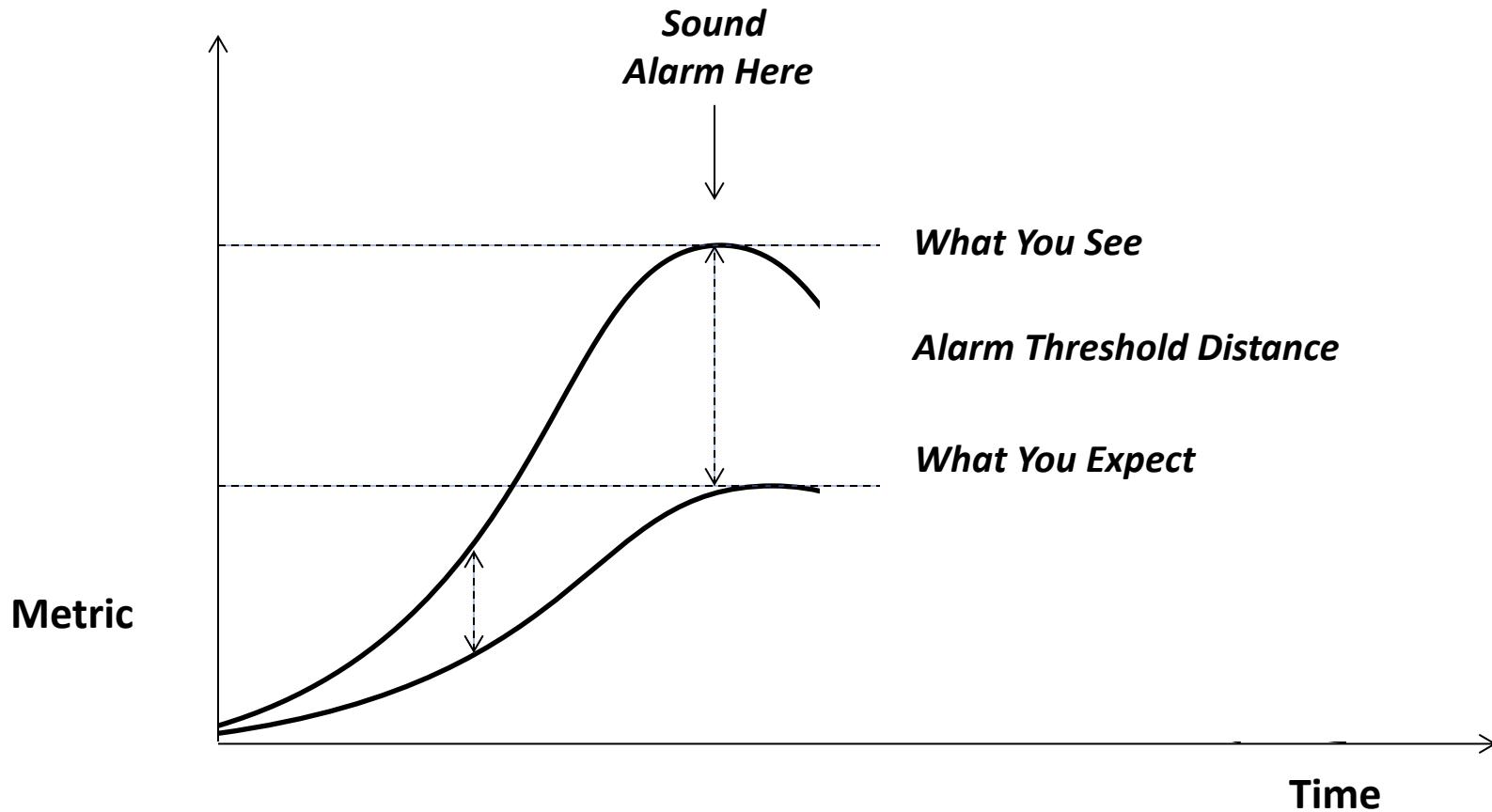
Real Time Network Security Behavioral Analytics



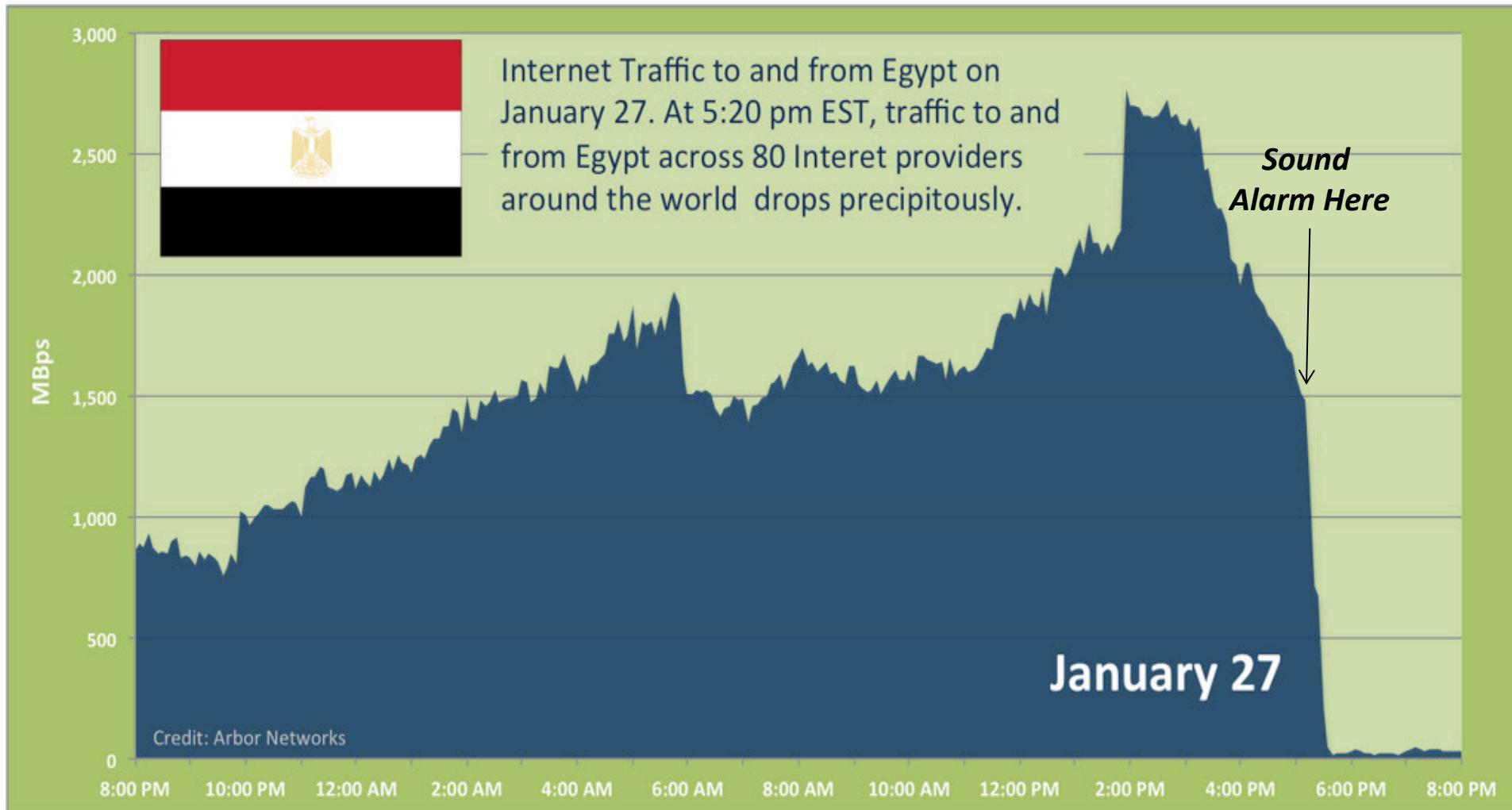
Real Time Network Security Behavioral Analytics



Real Time Network Security Behavioral Analytics

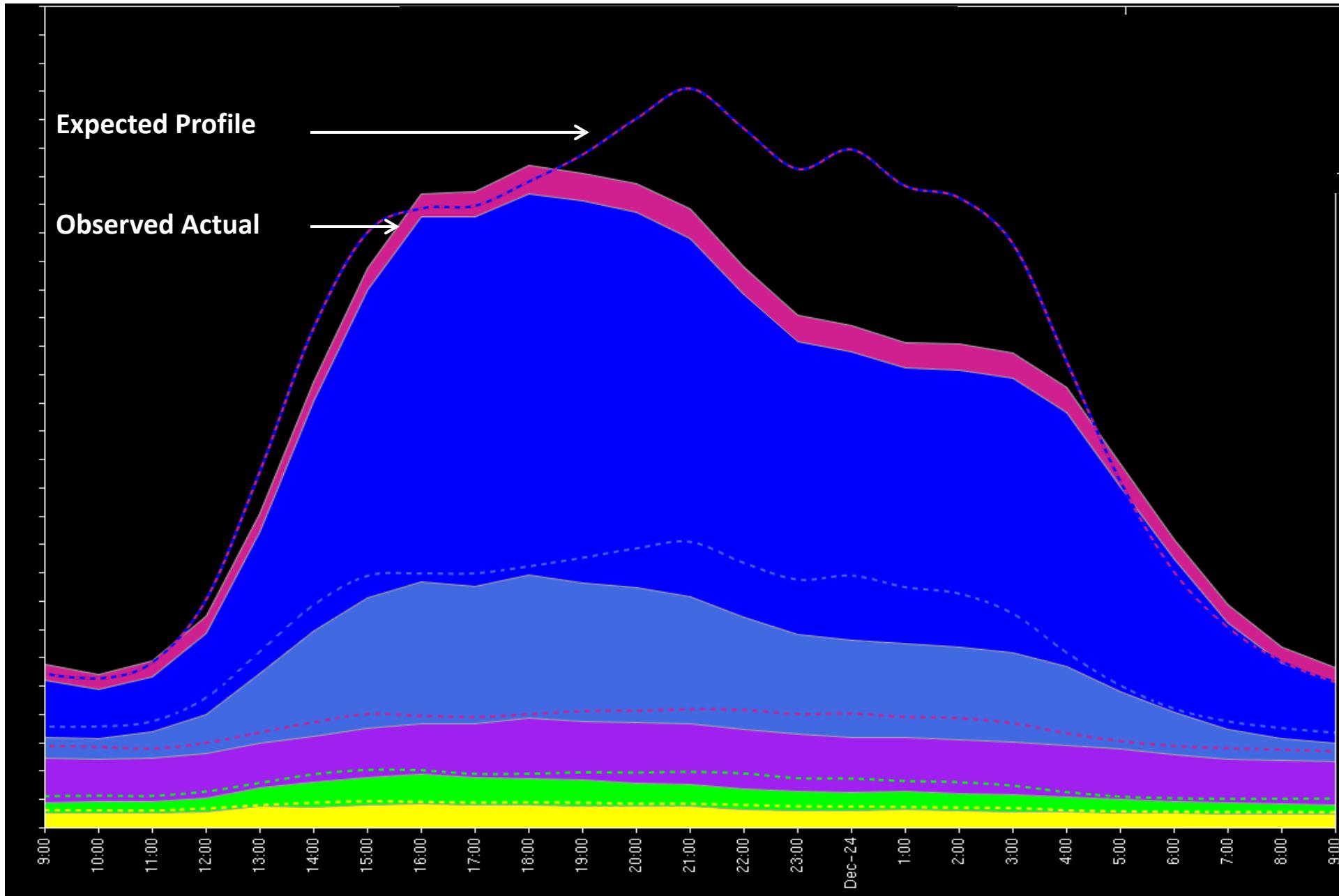


Internet Blackout in Egypt – 01/27/11



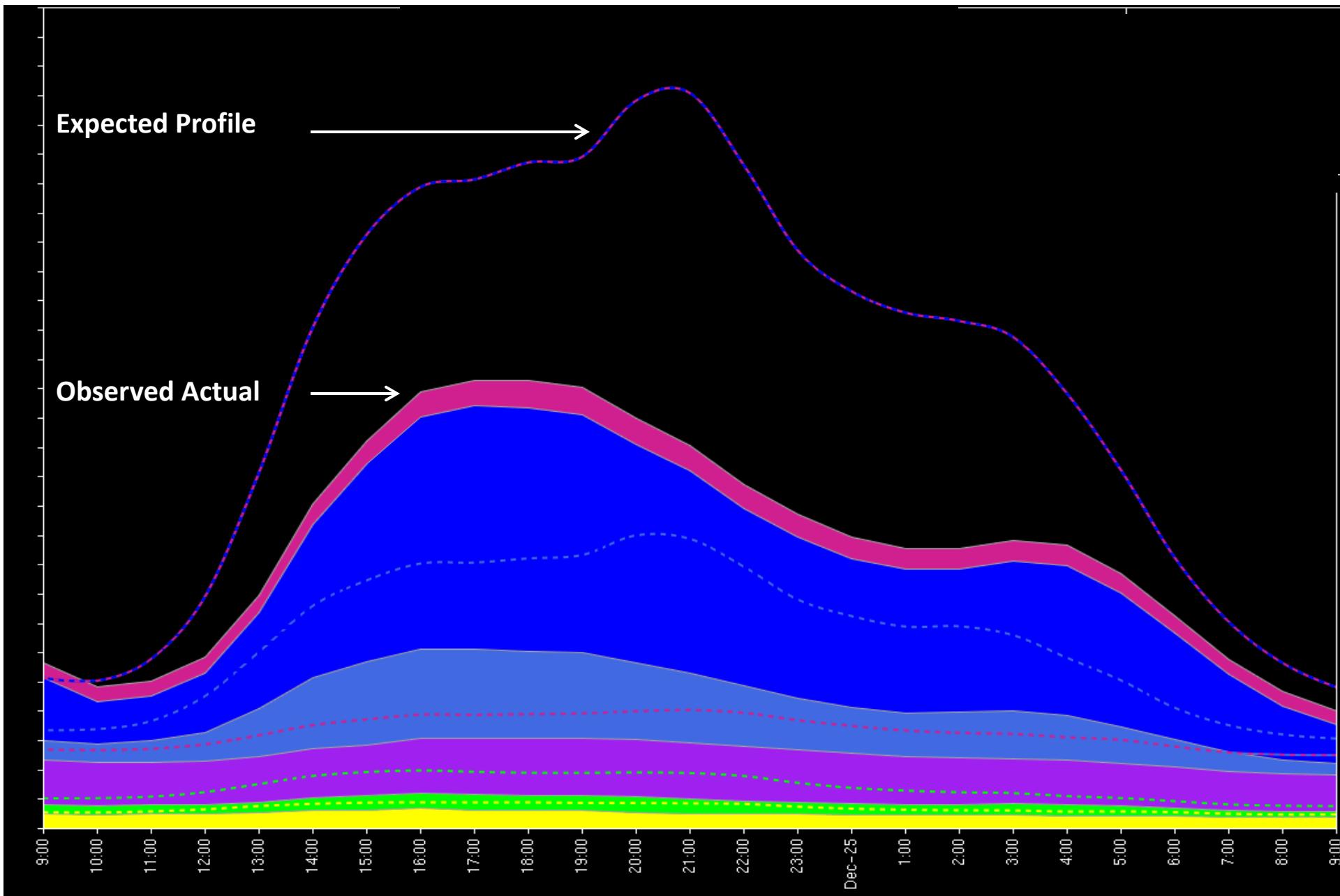
Week 3

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



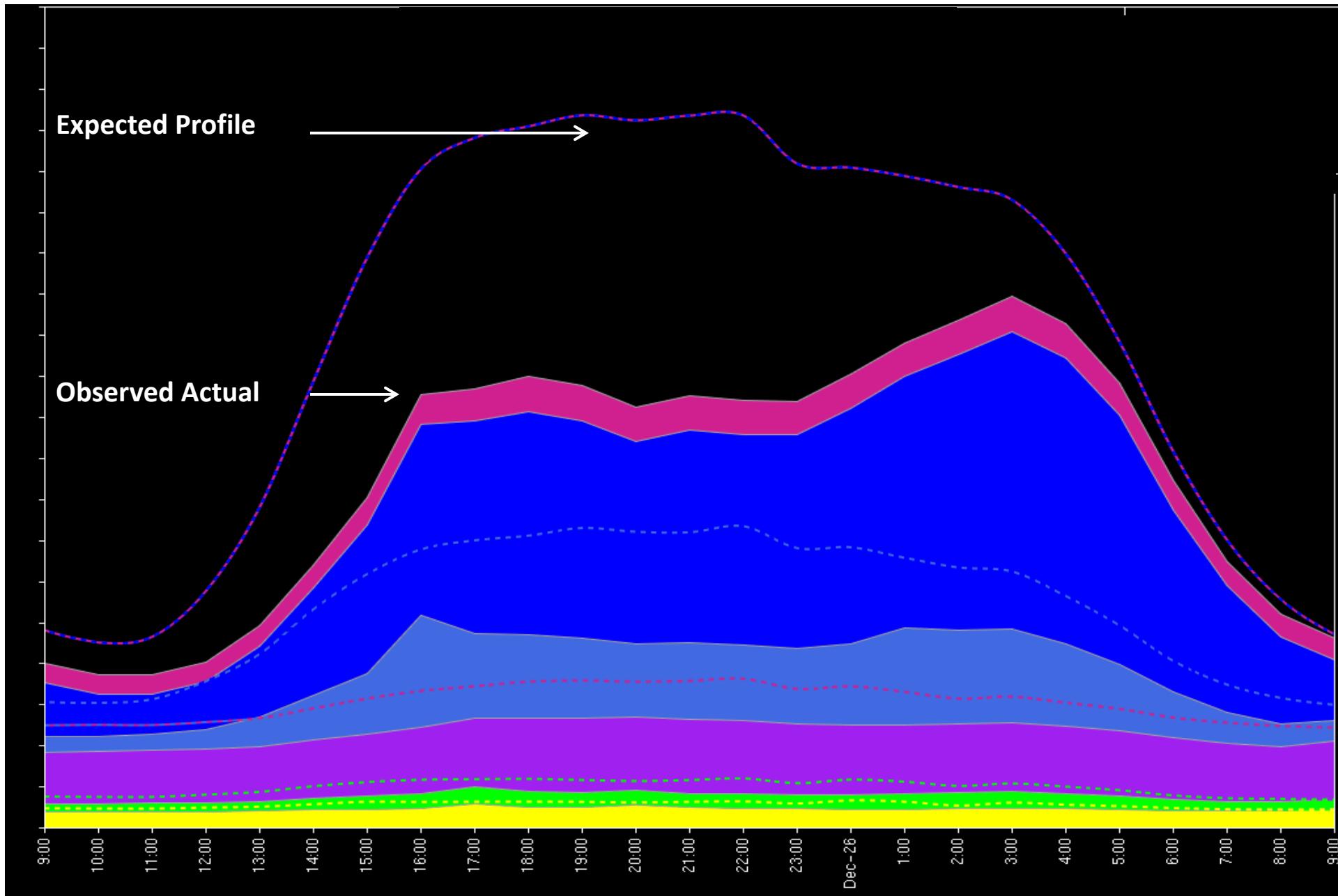
Week 3

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

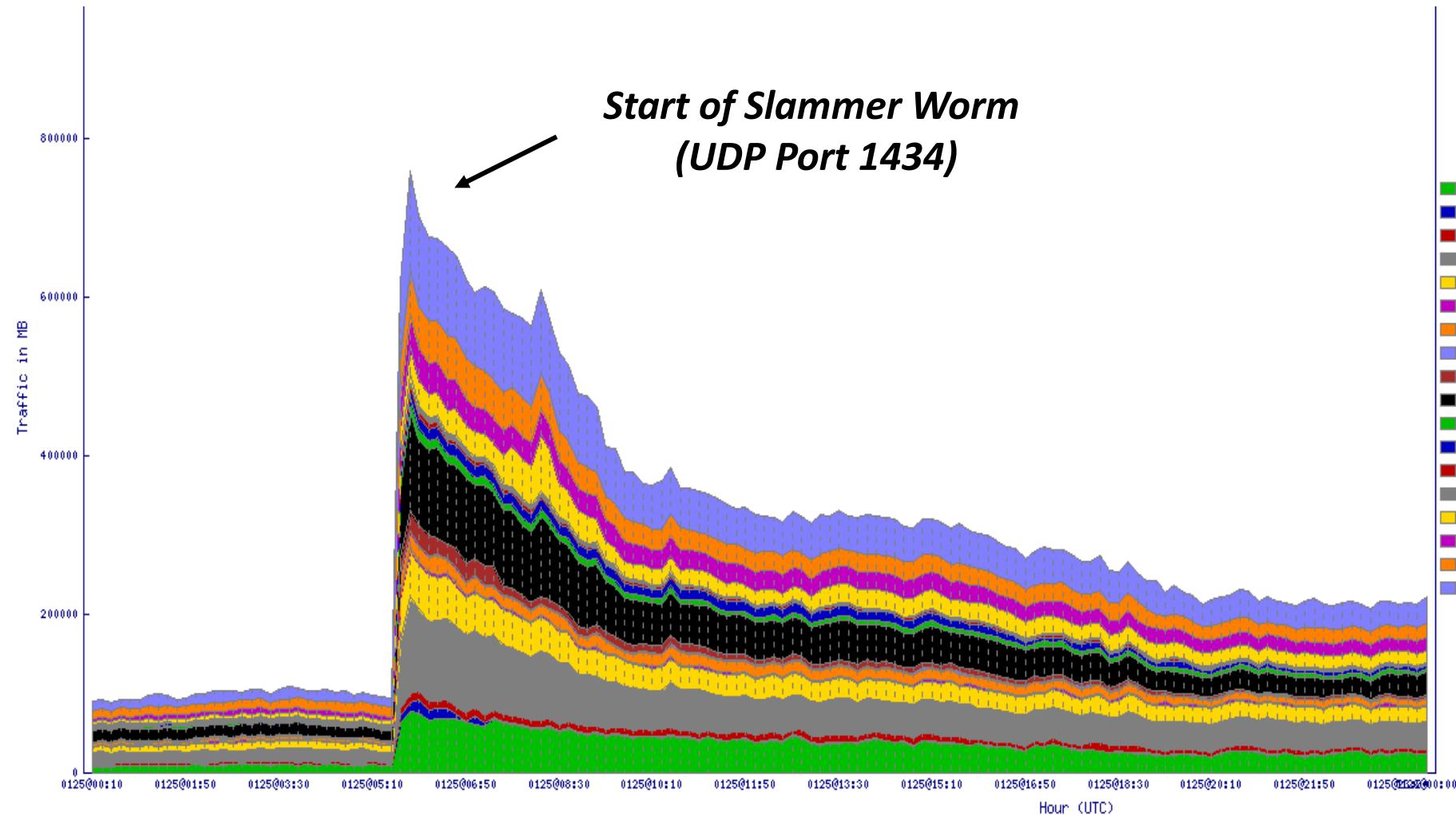


Week 3

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

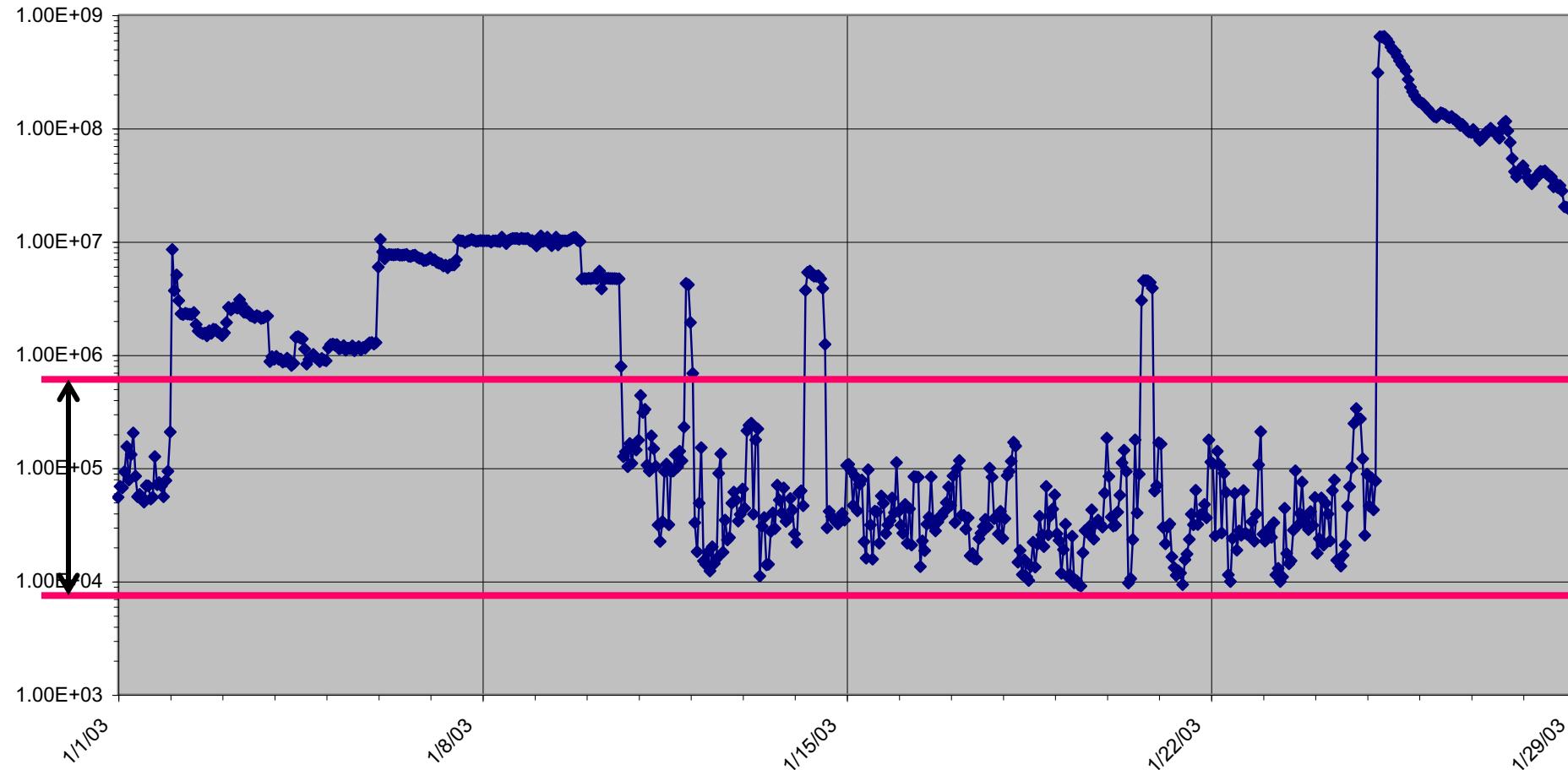


Internet View of Slammer Worm – UDP Port 1434: 01/25/03



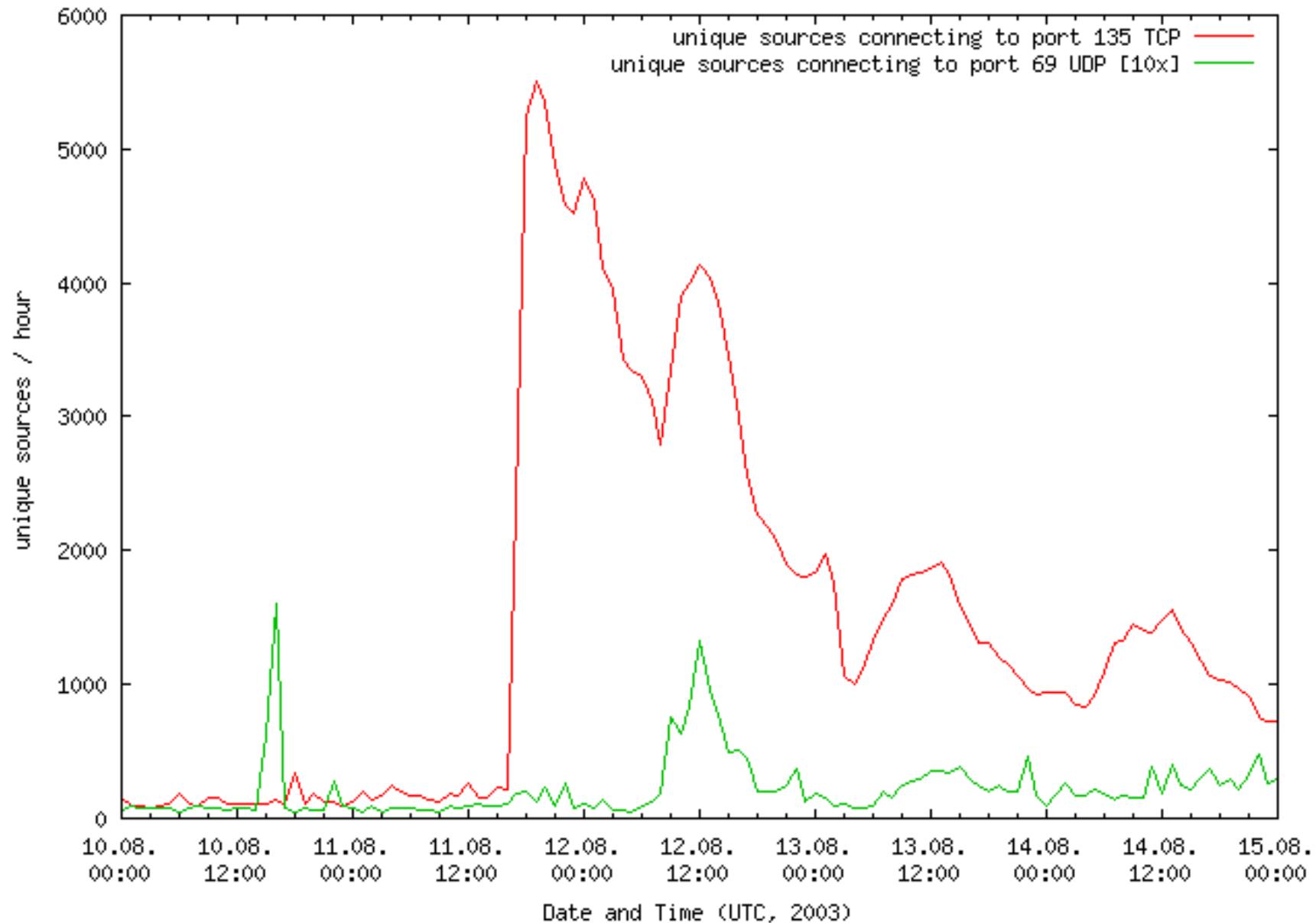
Week 3

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

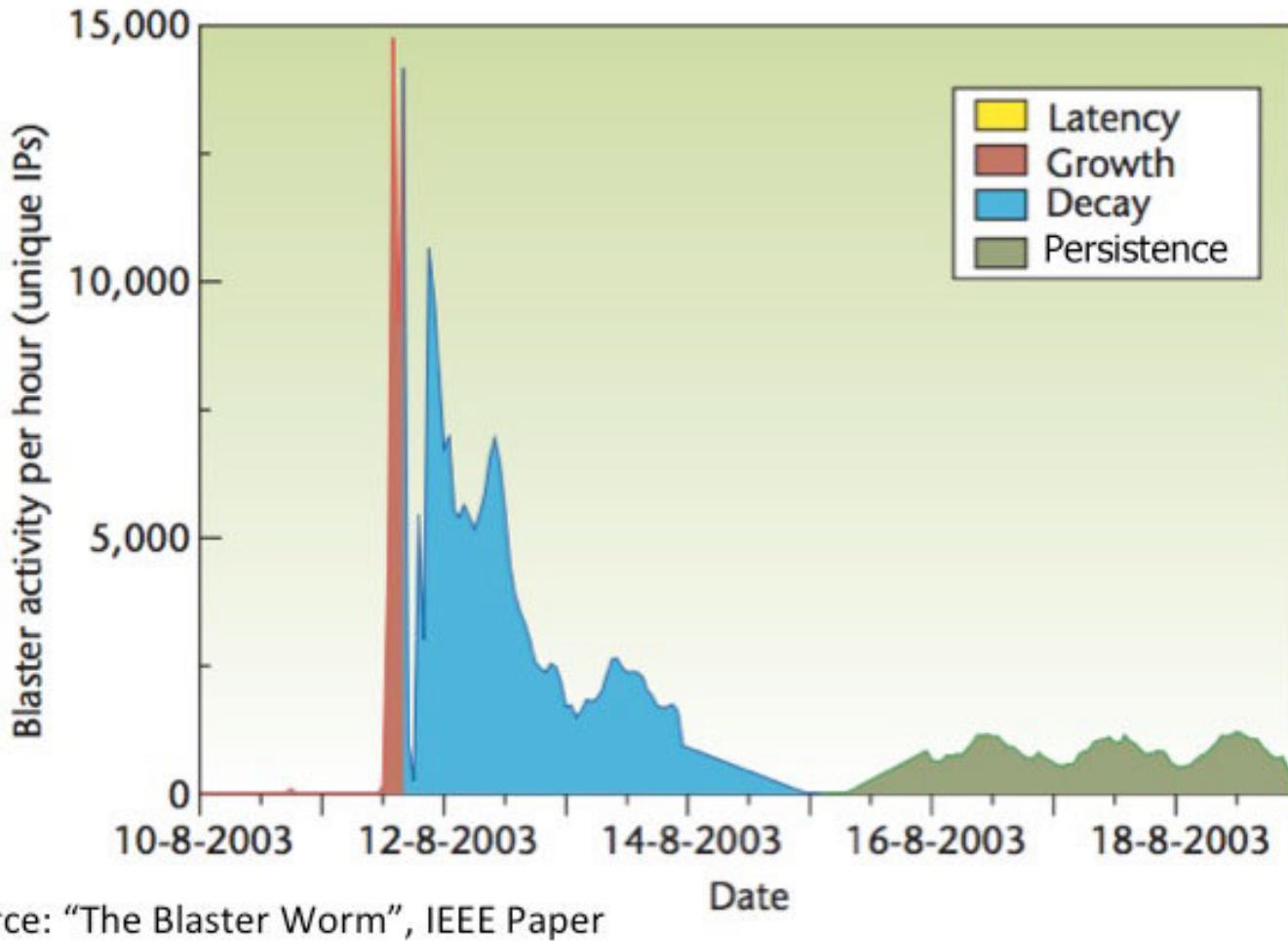


Week 3

Sharp Spike from Blaster Worm – 8/11/03



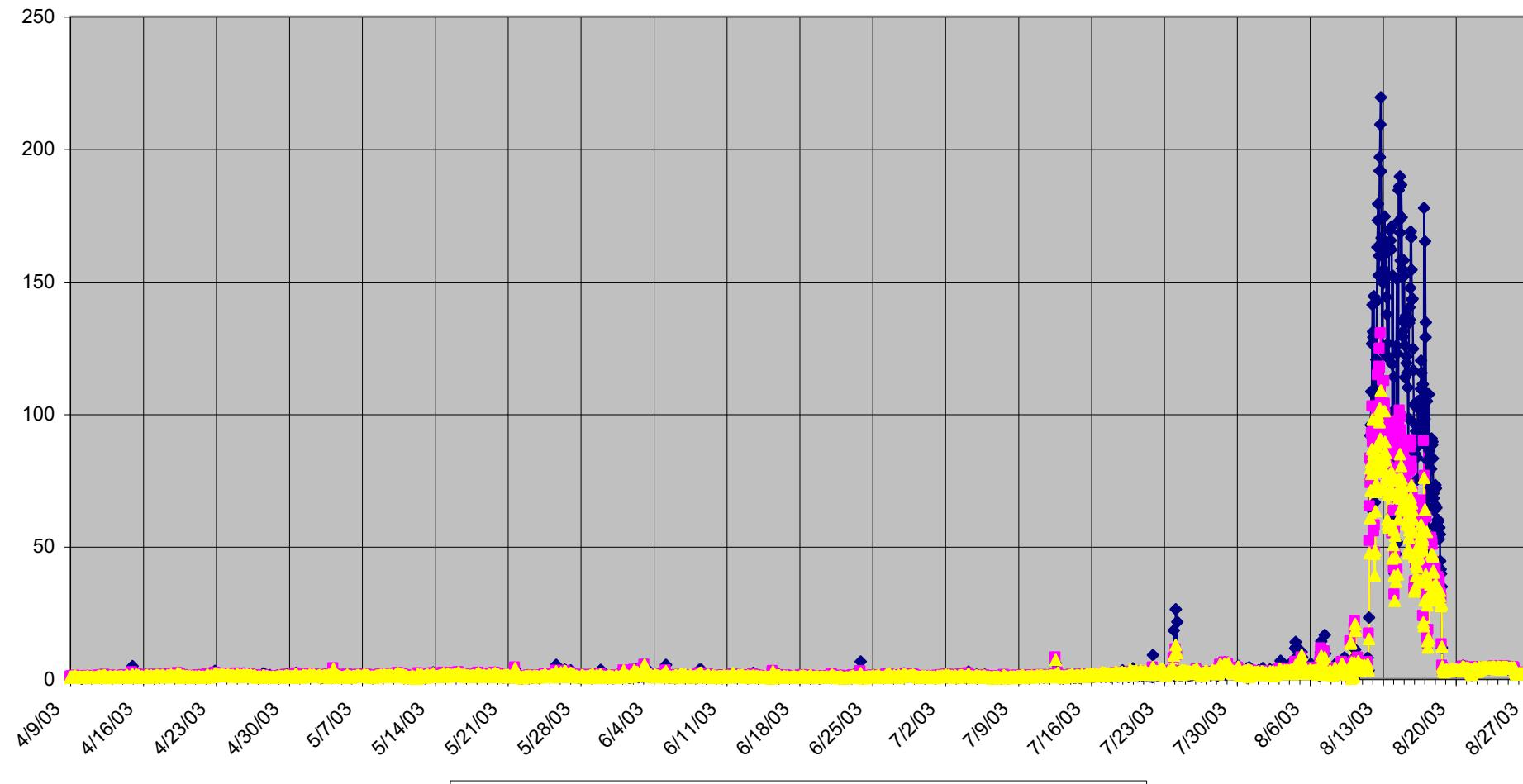
Sharp Spike from Blaster Worm – 8/11/03



Source: "The Blaster Worm", IEEE Paper

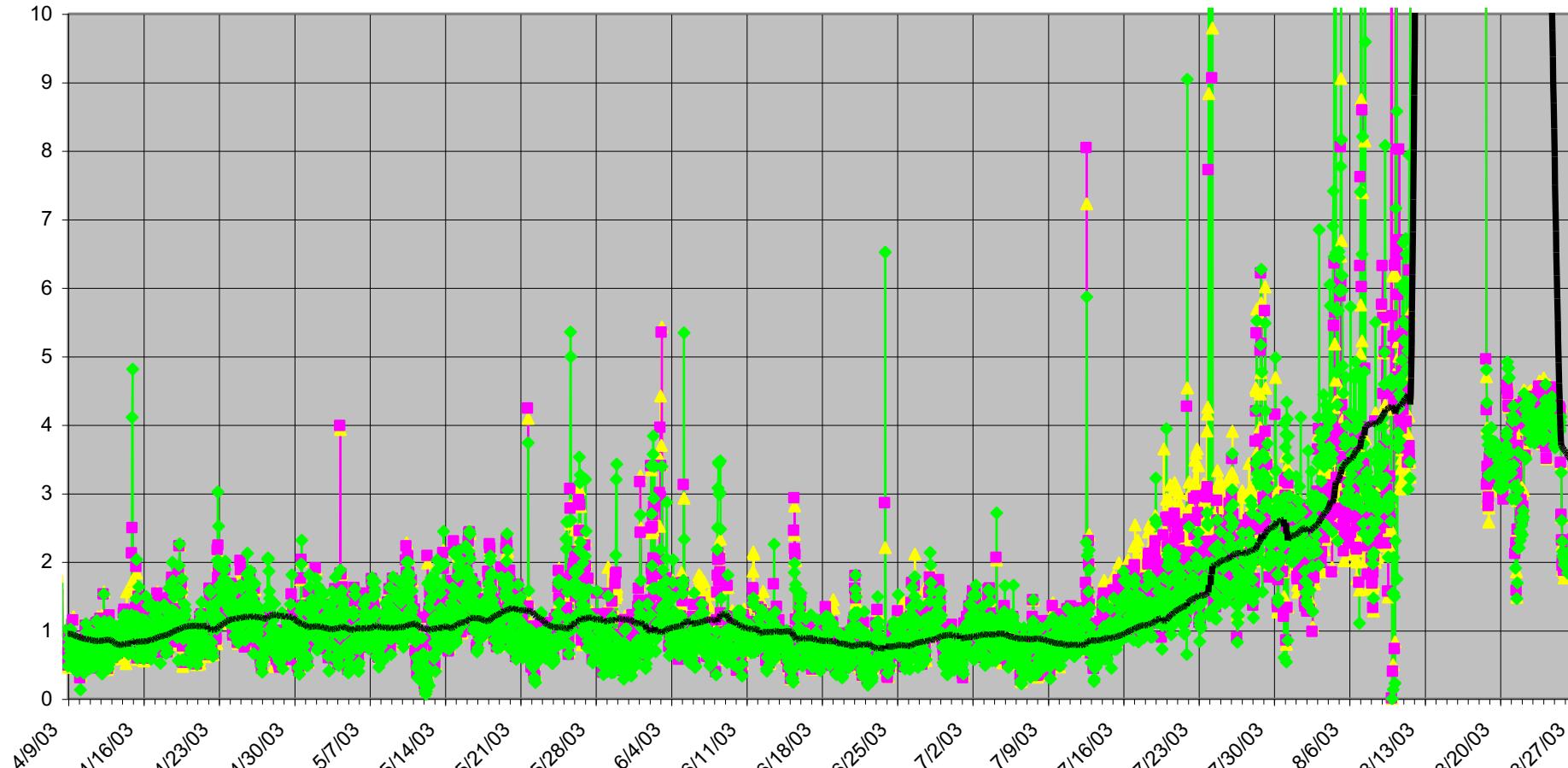
Week 3

Internet View of TCP 135 – Blaster Worm – 2003

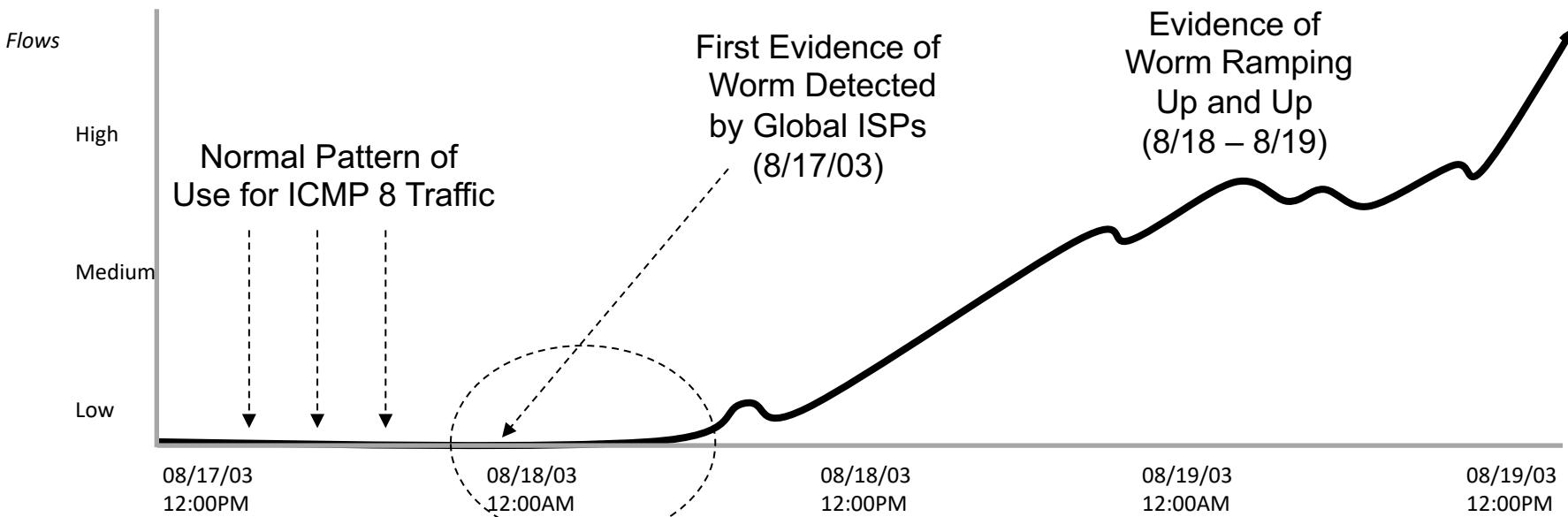


Week 3

Deeper Internet View of TCP 135 Activity – Blaster Worm



Nachi Worm of 2003

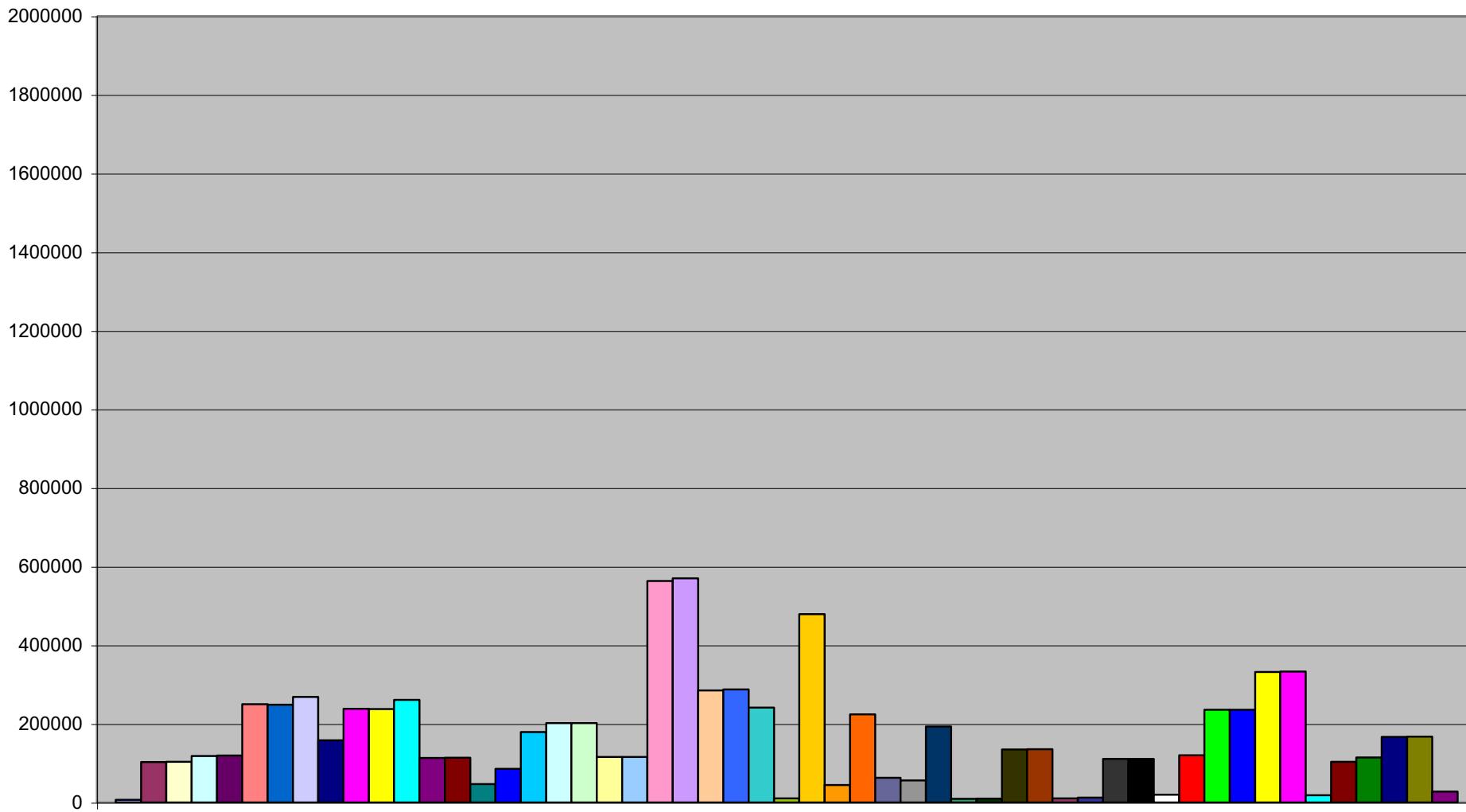


Week 3



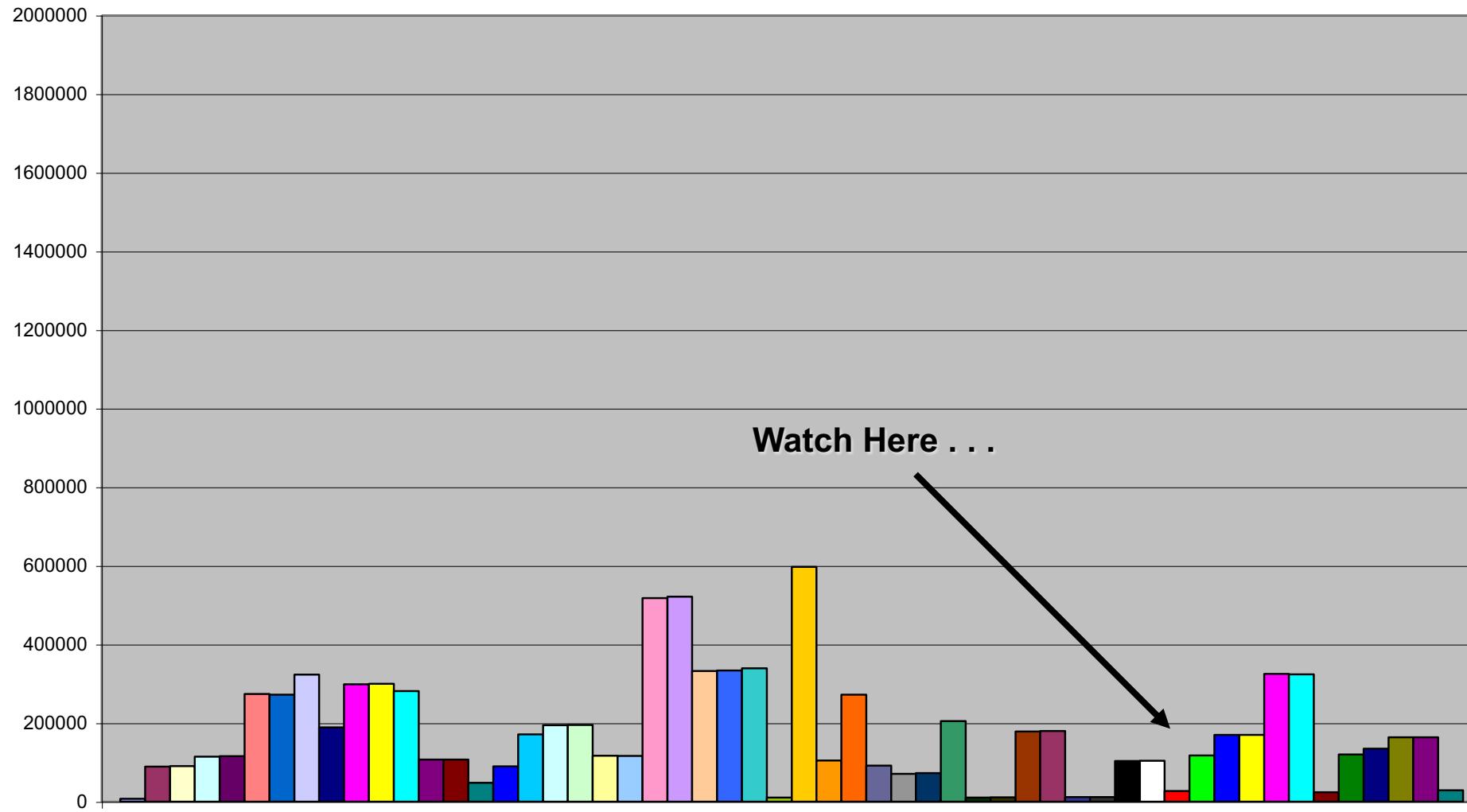
Week 3

Nachi 8/17/03 10:00PM



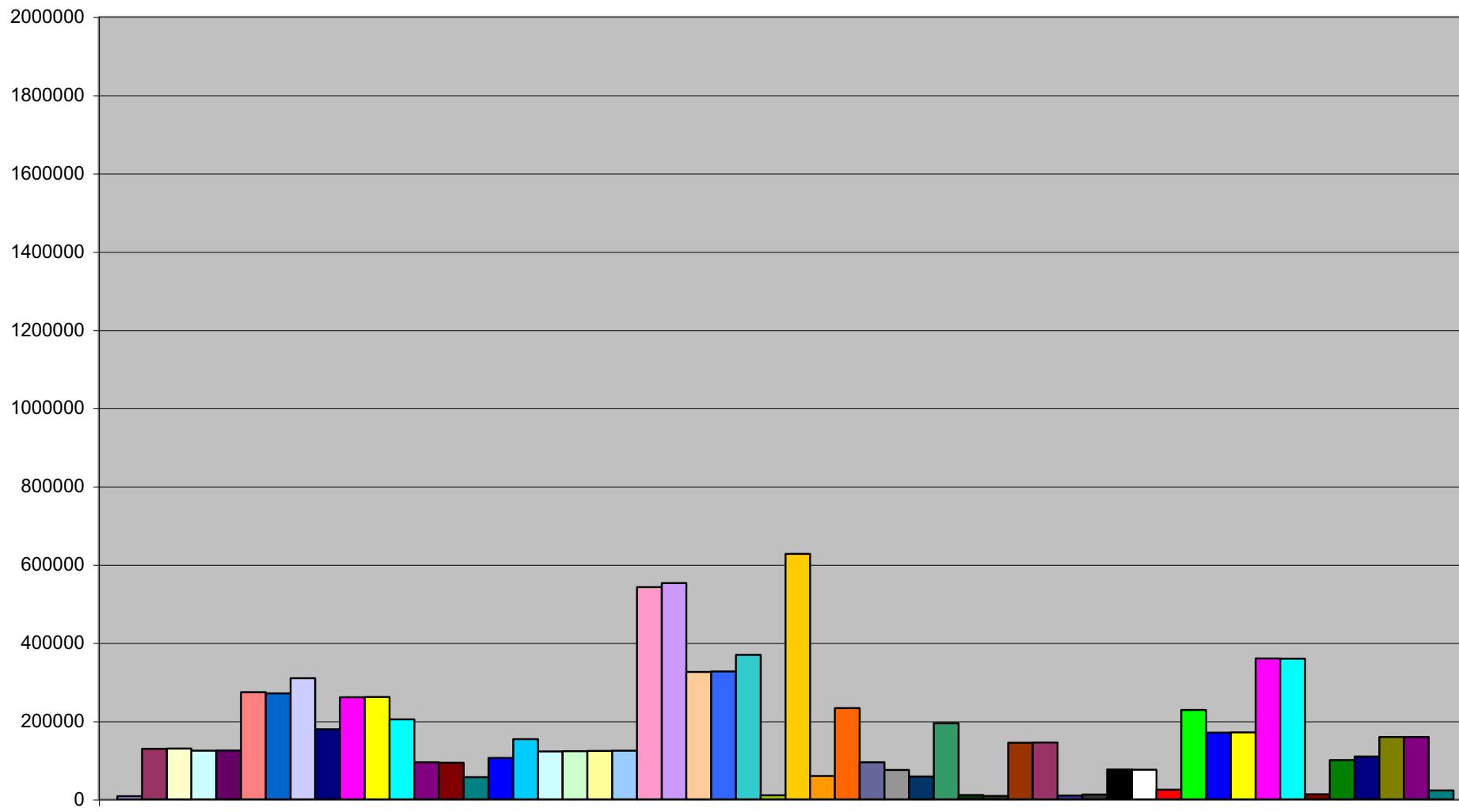
Week 3

Nachi 8/17/03 11:00PM



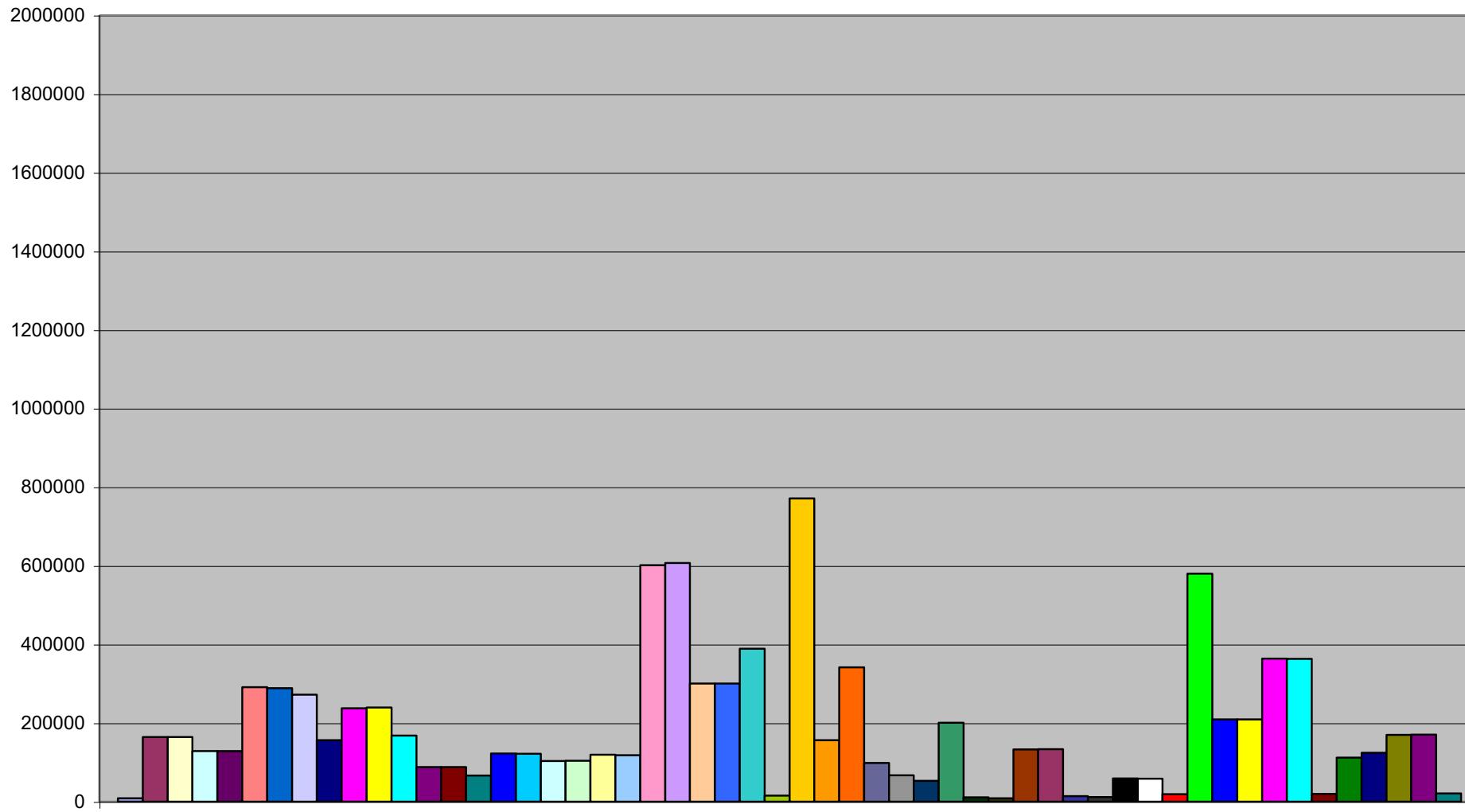
Week 3

Nachi 8/17/03 Midnight



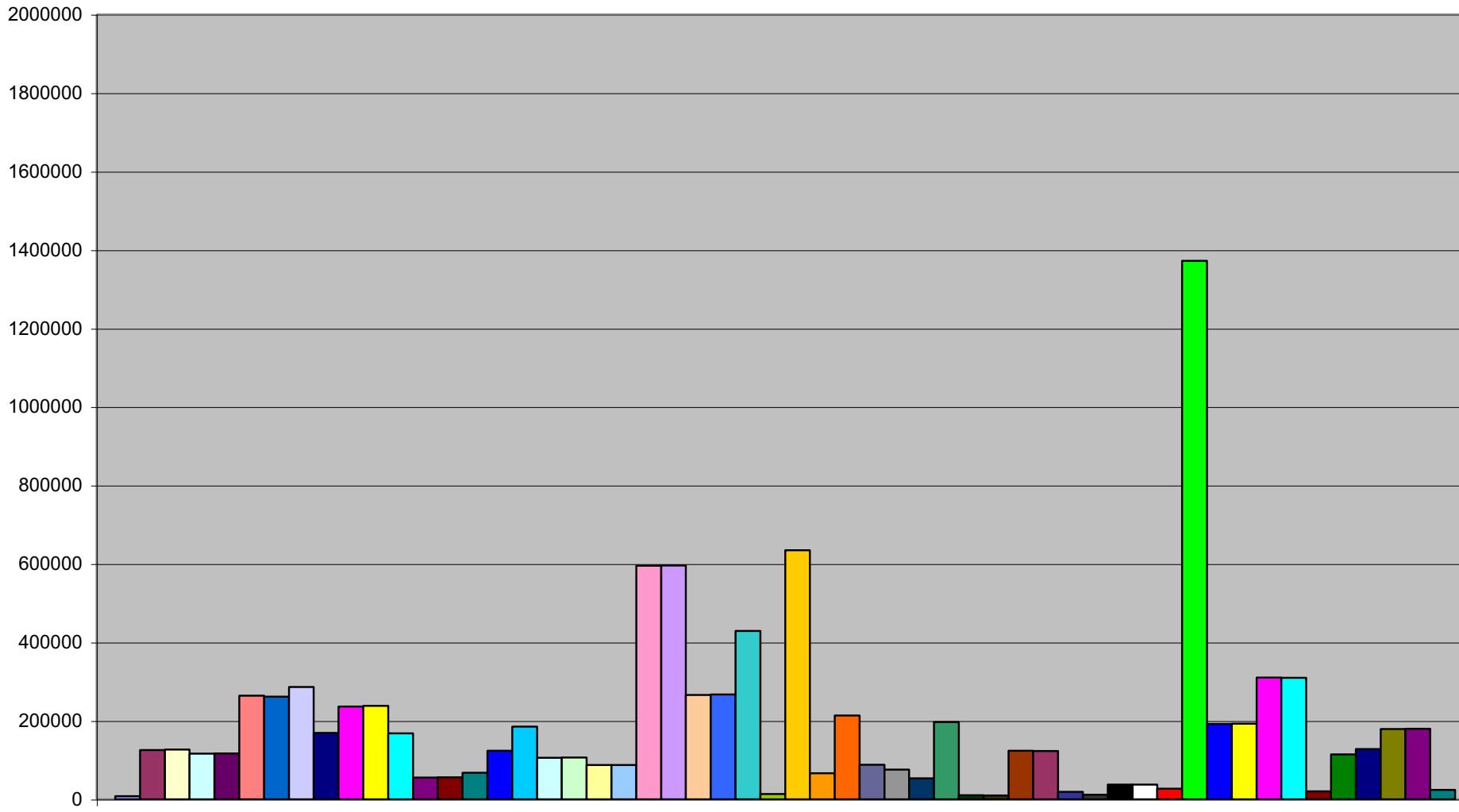
Week 3

Nachi 8/18/03 1:00AM



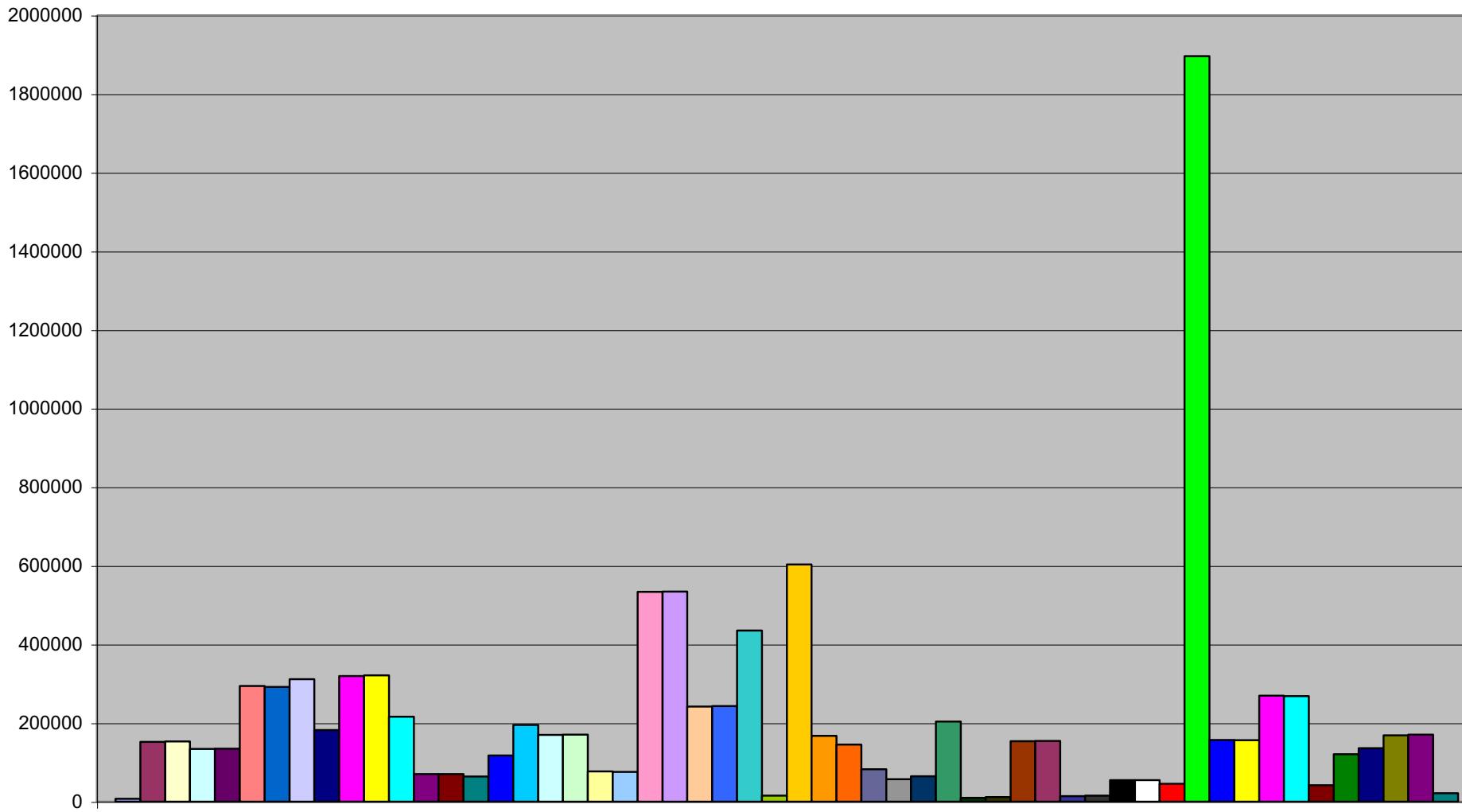
Week 3

Nachi 8/18/03 2:00AM



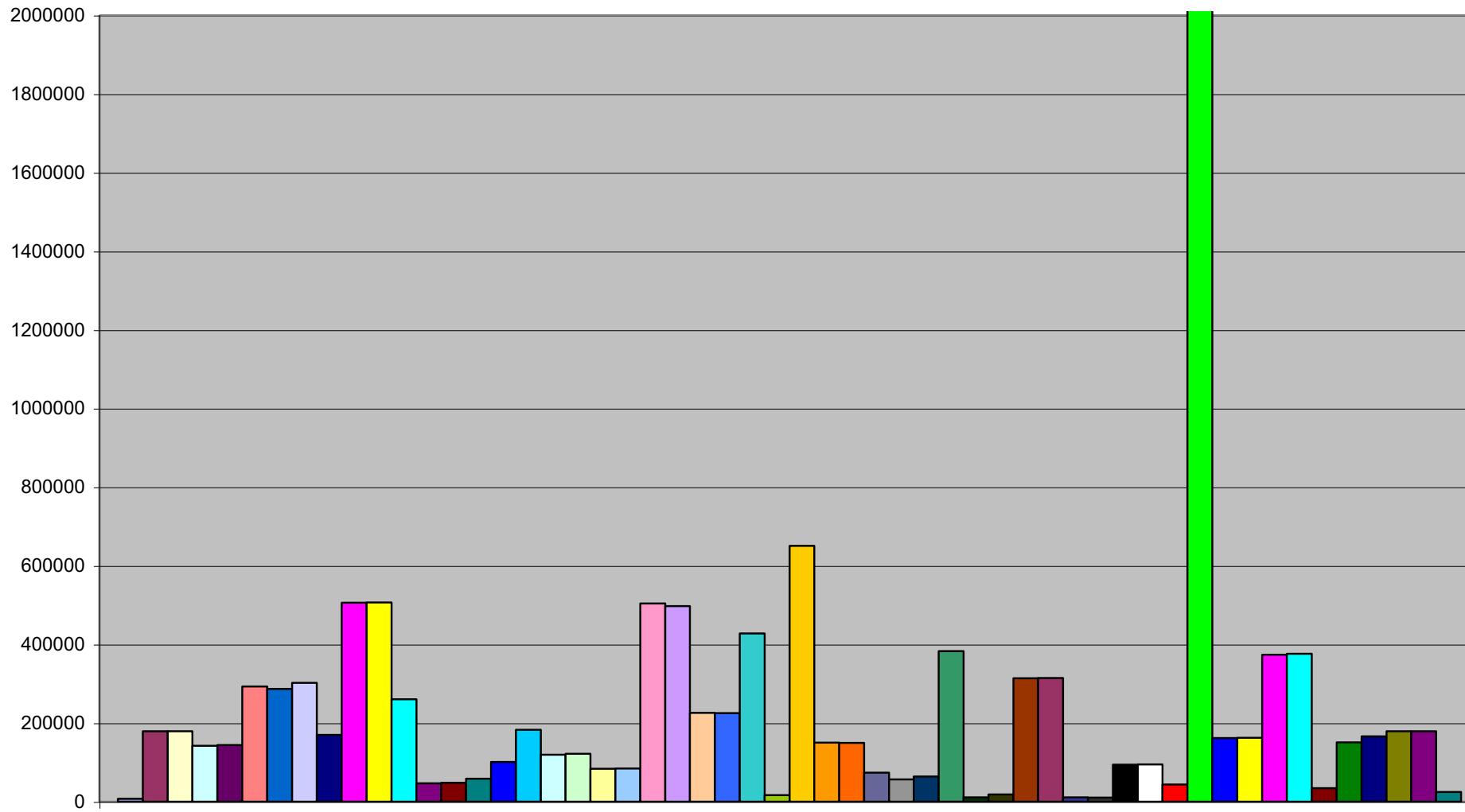
Week 3

Nachi 8/18/03 3:00AM



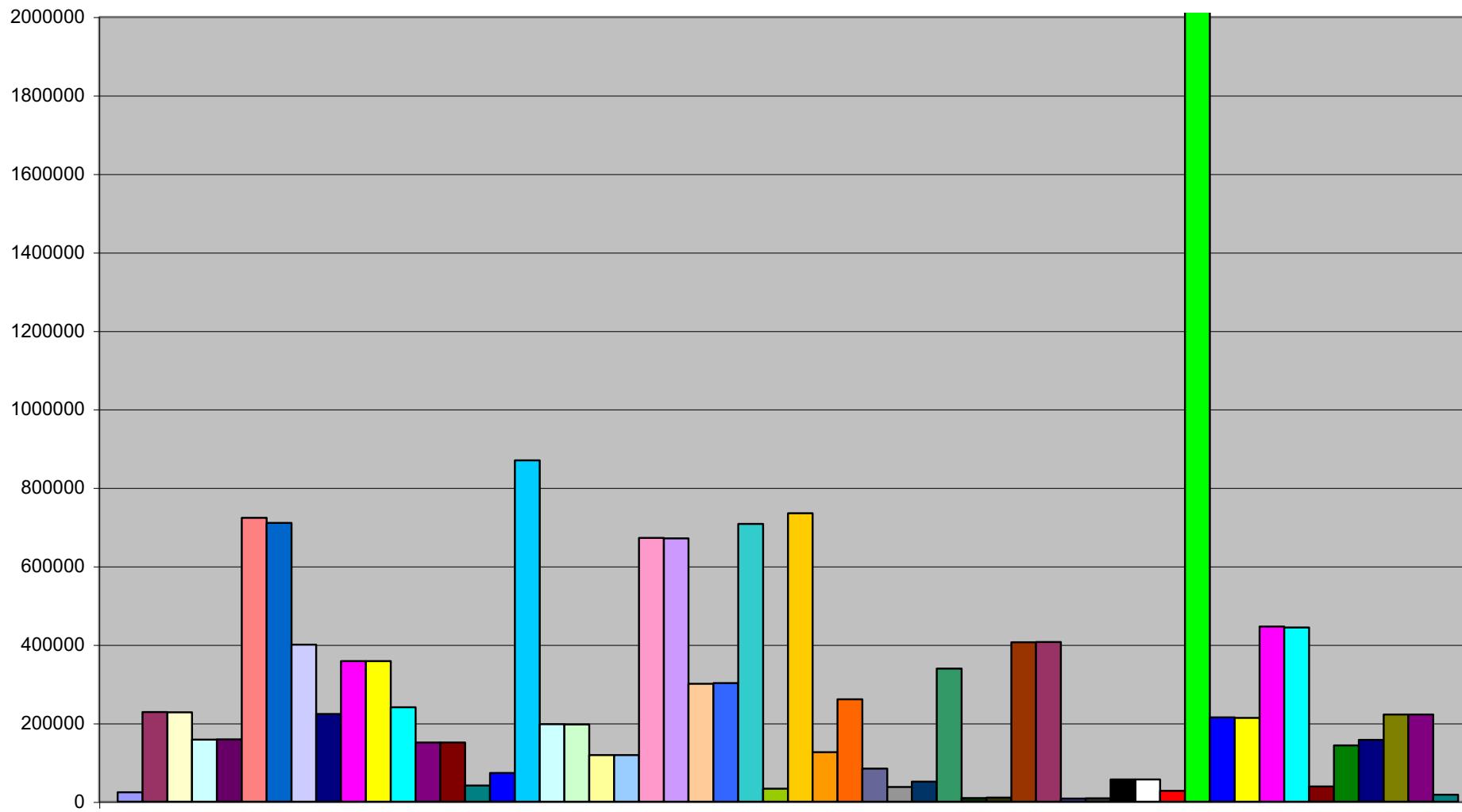
Week 3

Nachi 8/18/03 4:00AM



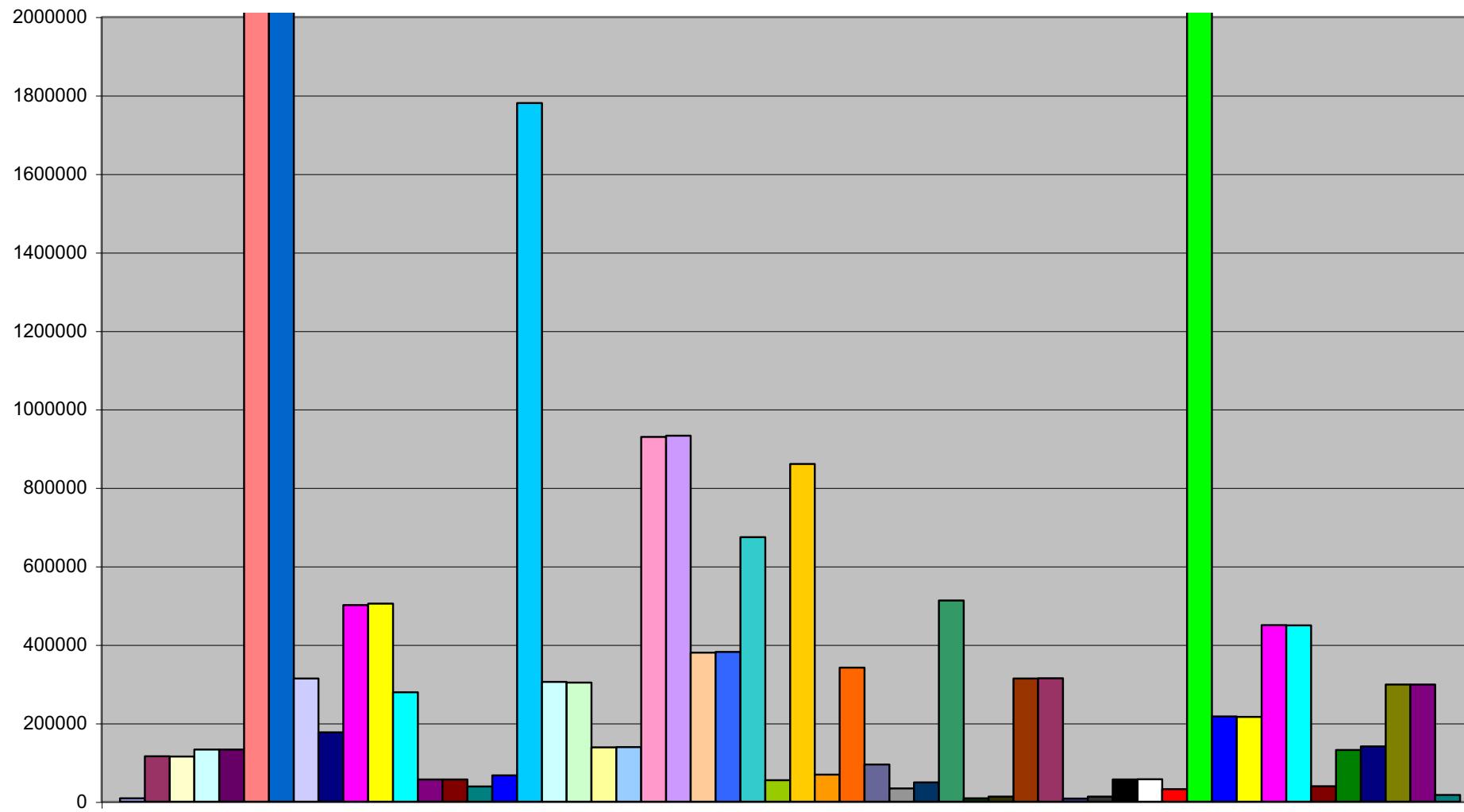
Week 3

Nachi 8/18/03 5:00AM



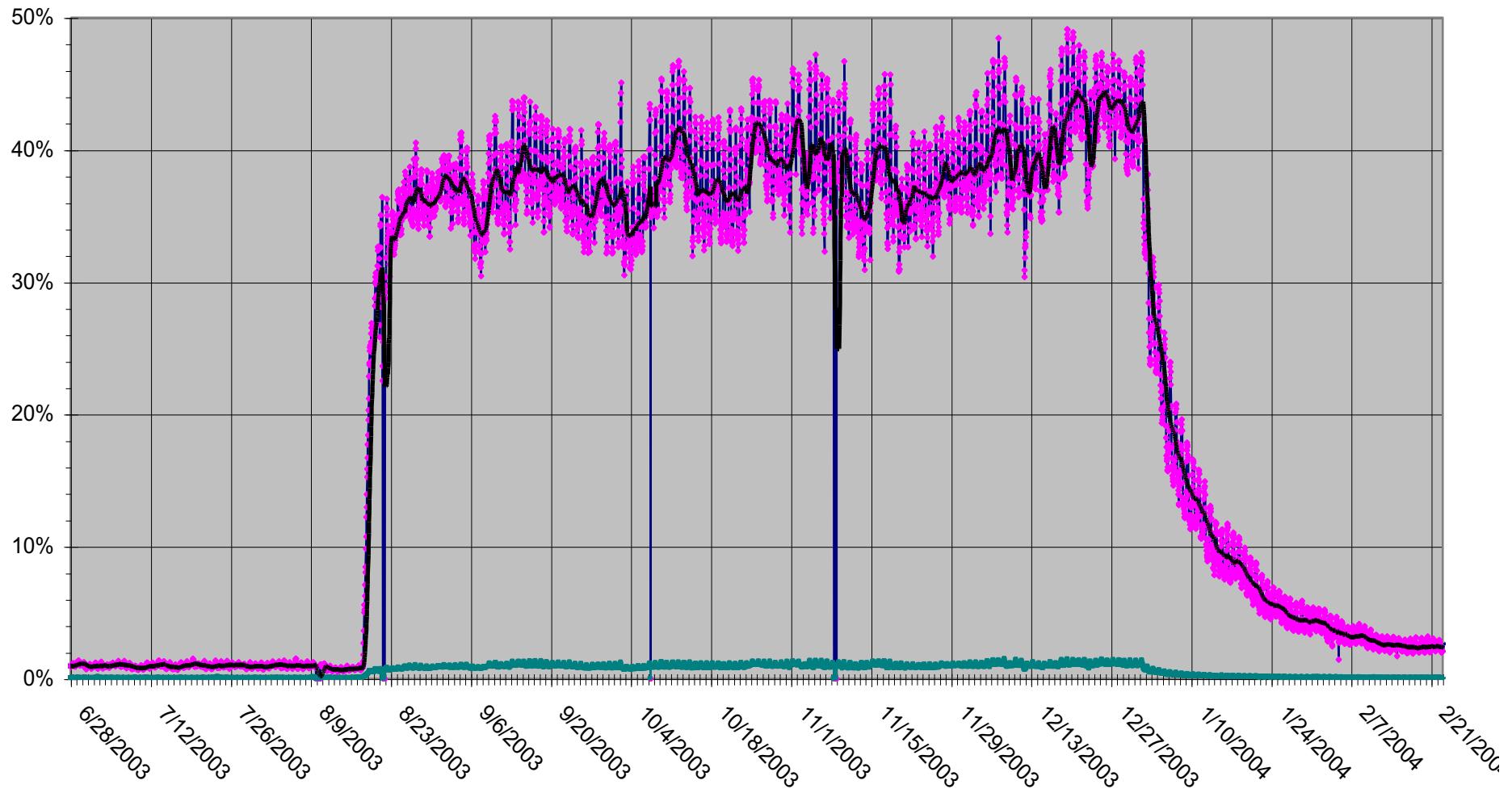
Week 3

Nachi 8/18/03 6:00AM



Week 3

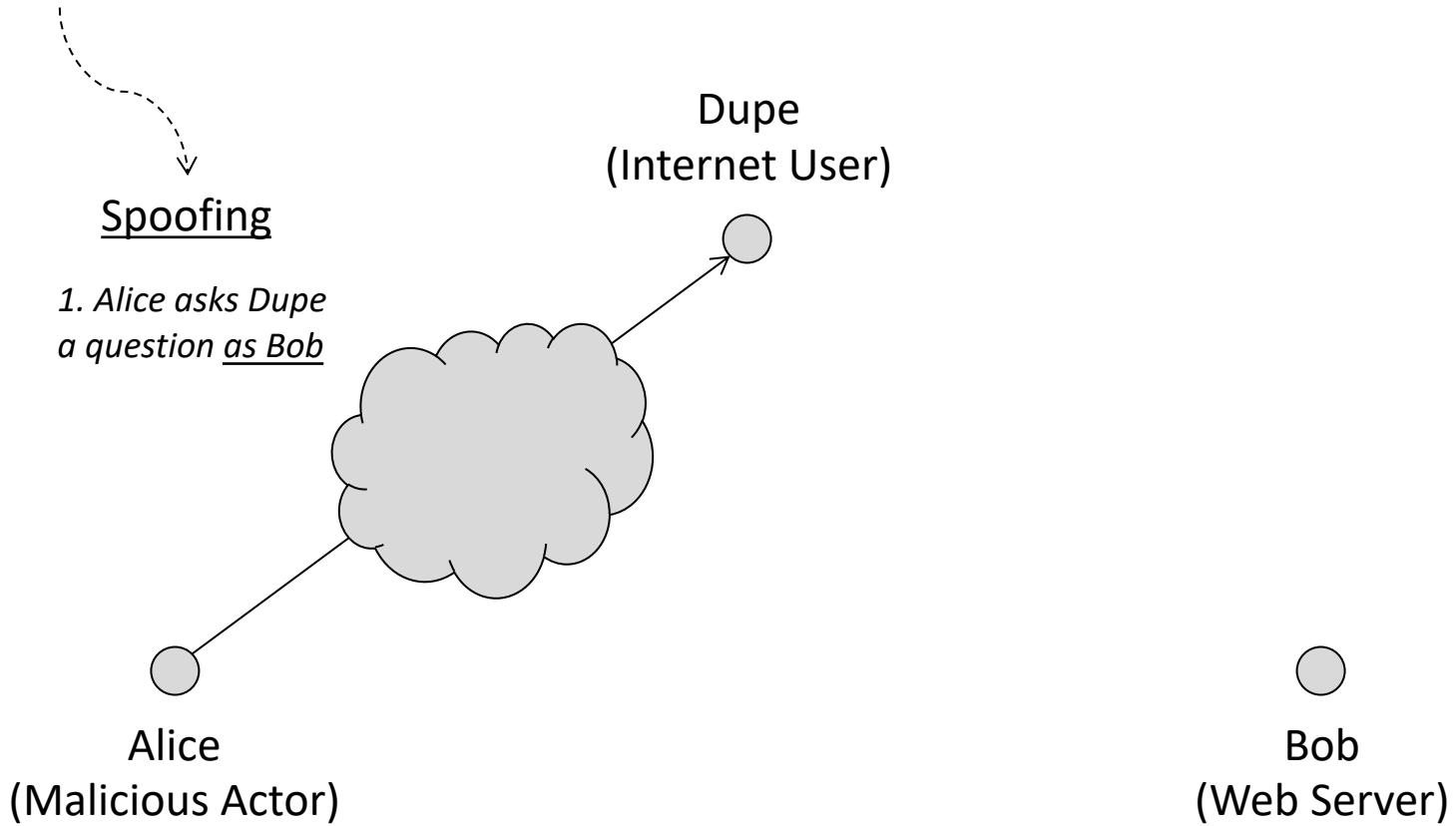
Nachi Worm (08/03 – 01/04)



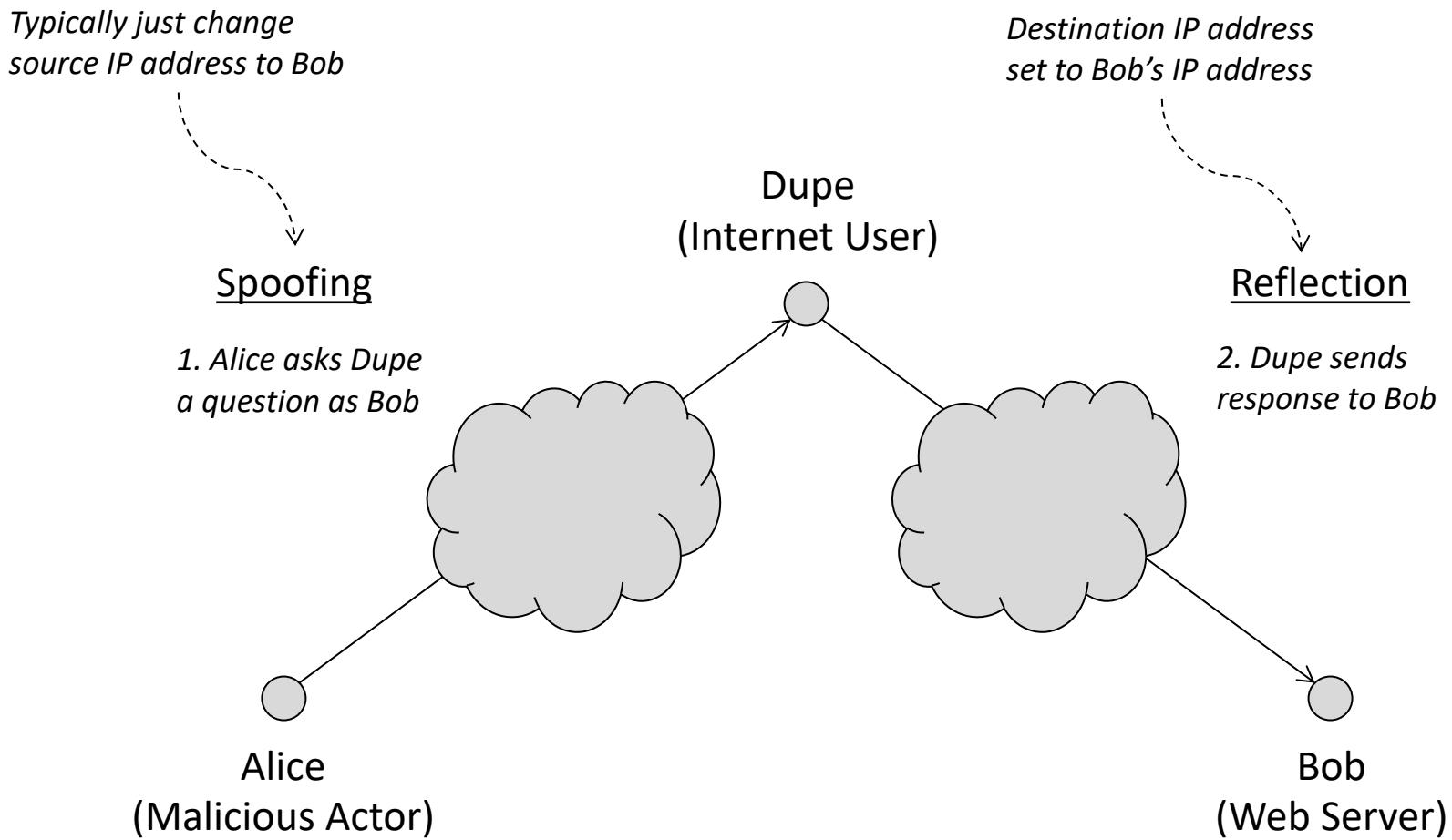
How are Botnets Used for DDOS Attacks?

Spoofing and Reflection

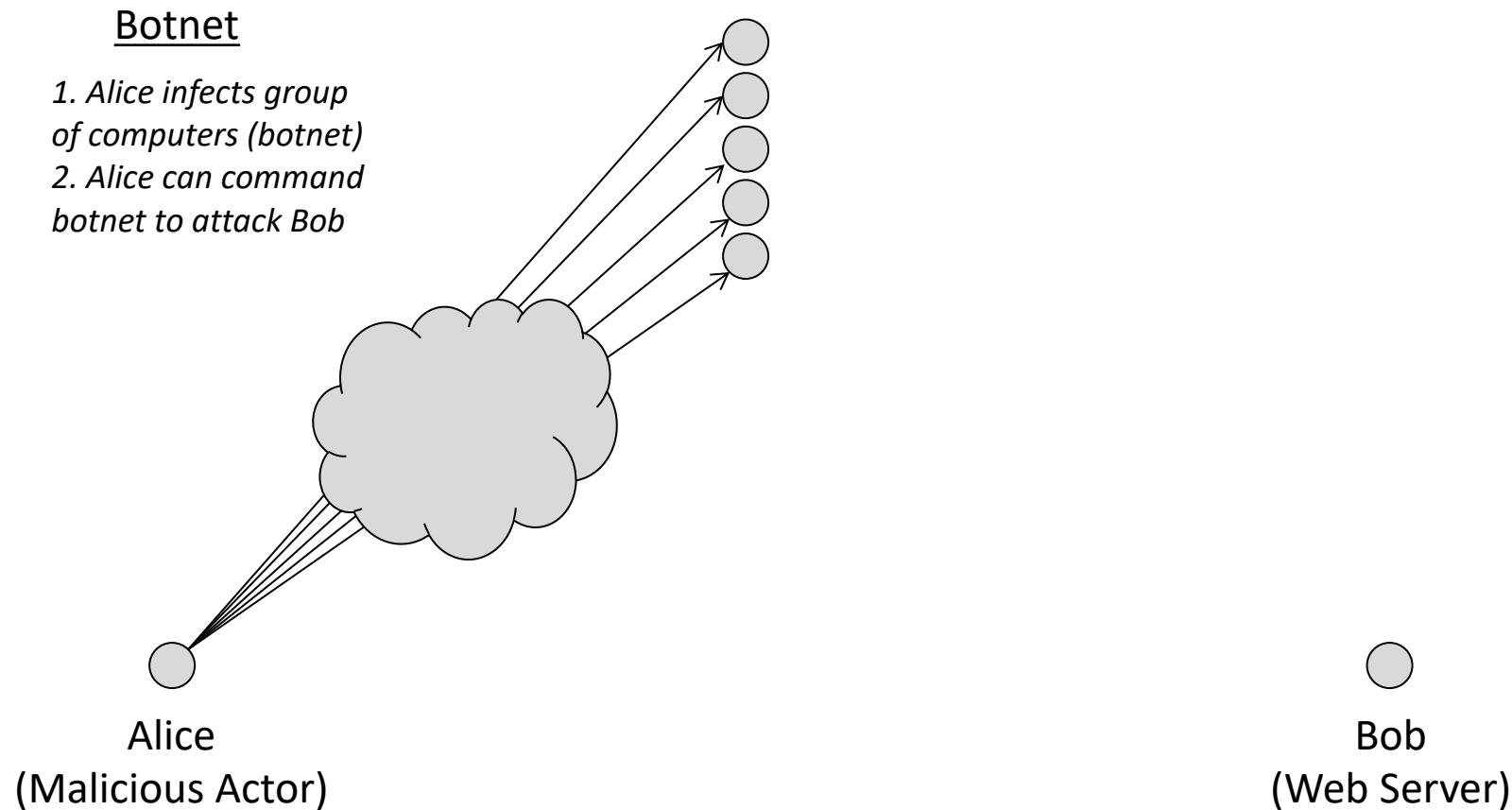
*Typically just change
source IP address to Bob*



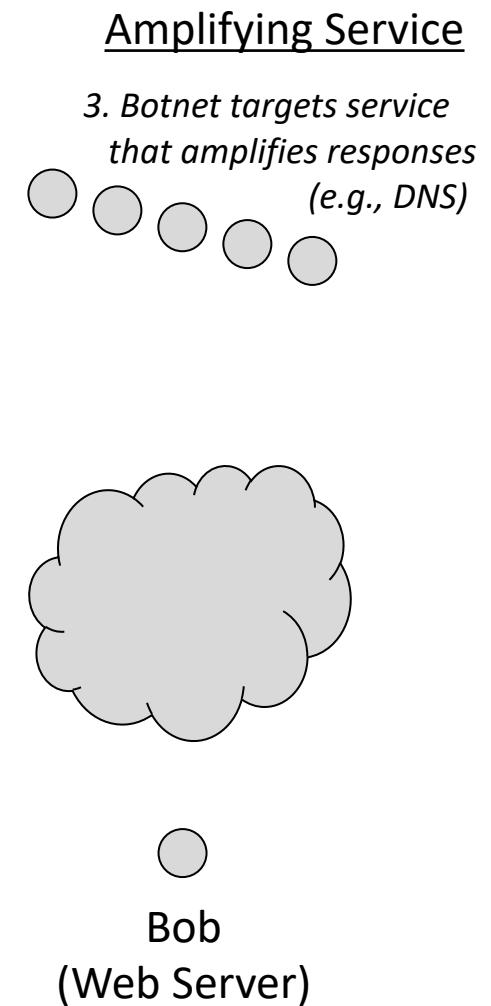
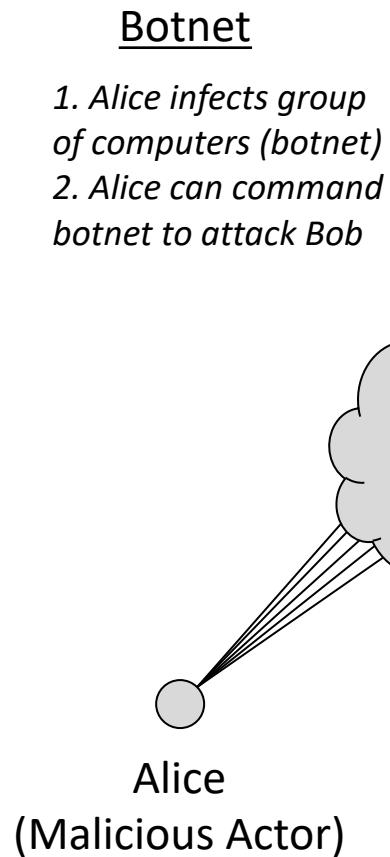
Spoofing and Reflection



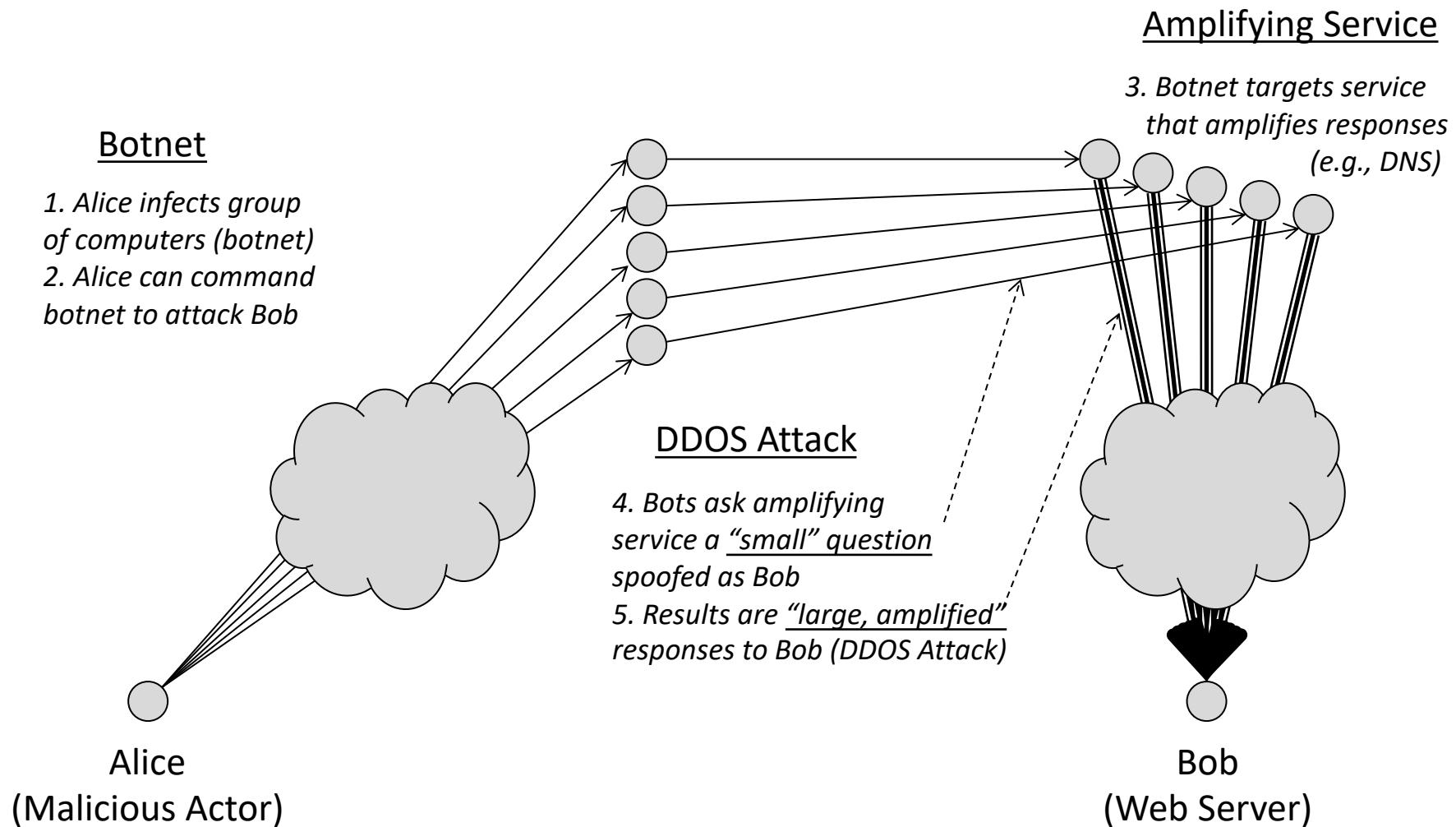
Distribution and Amplification



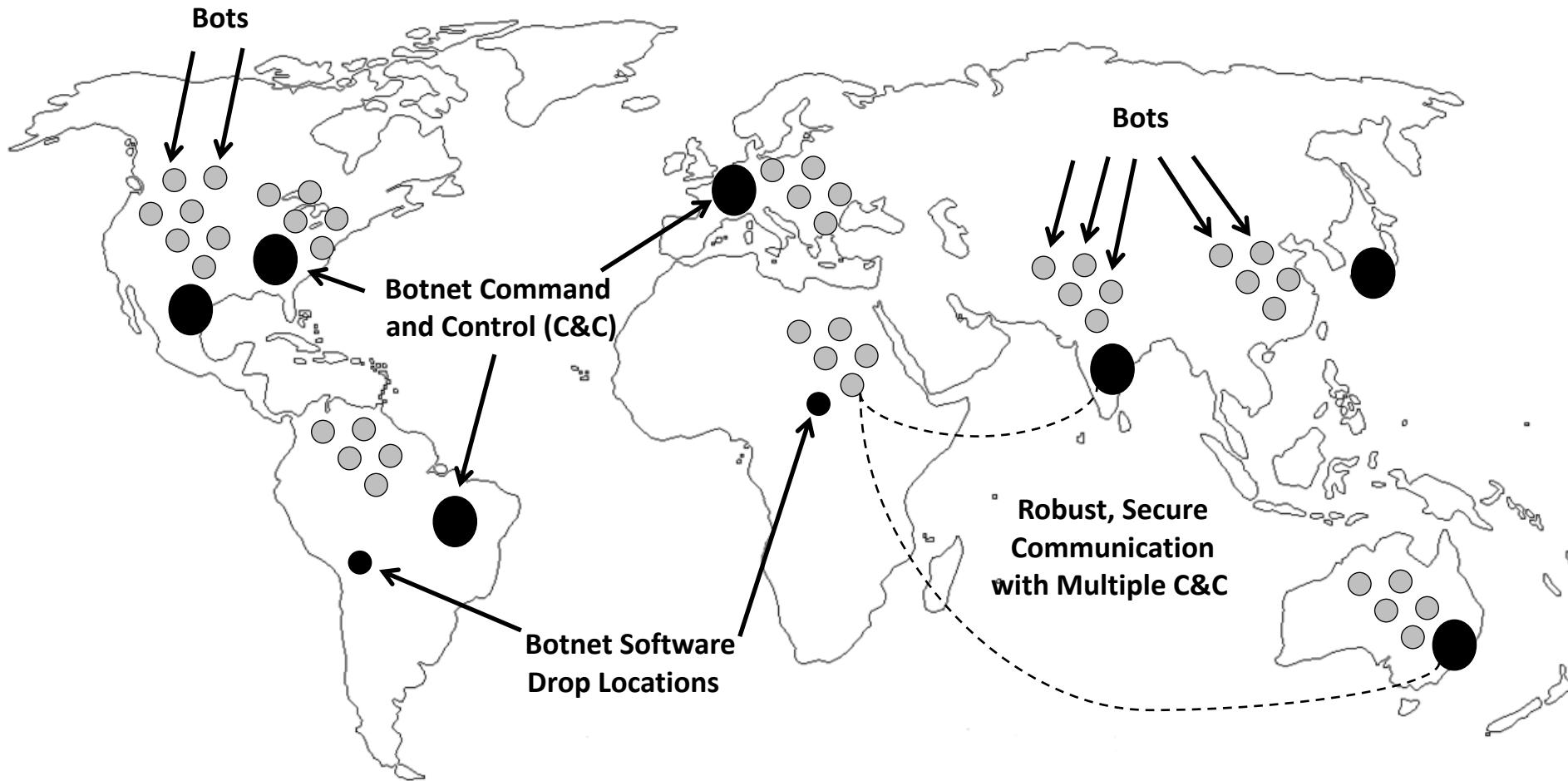
Distribution and Amplification



Distribution and Amplification



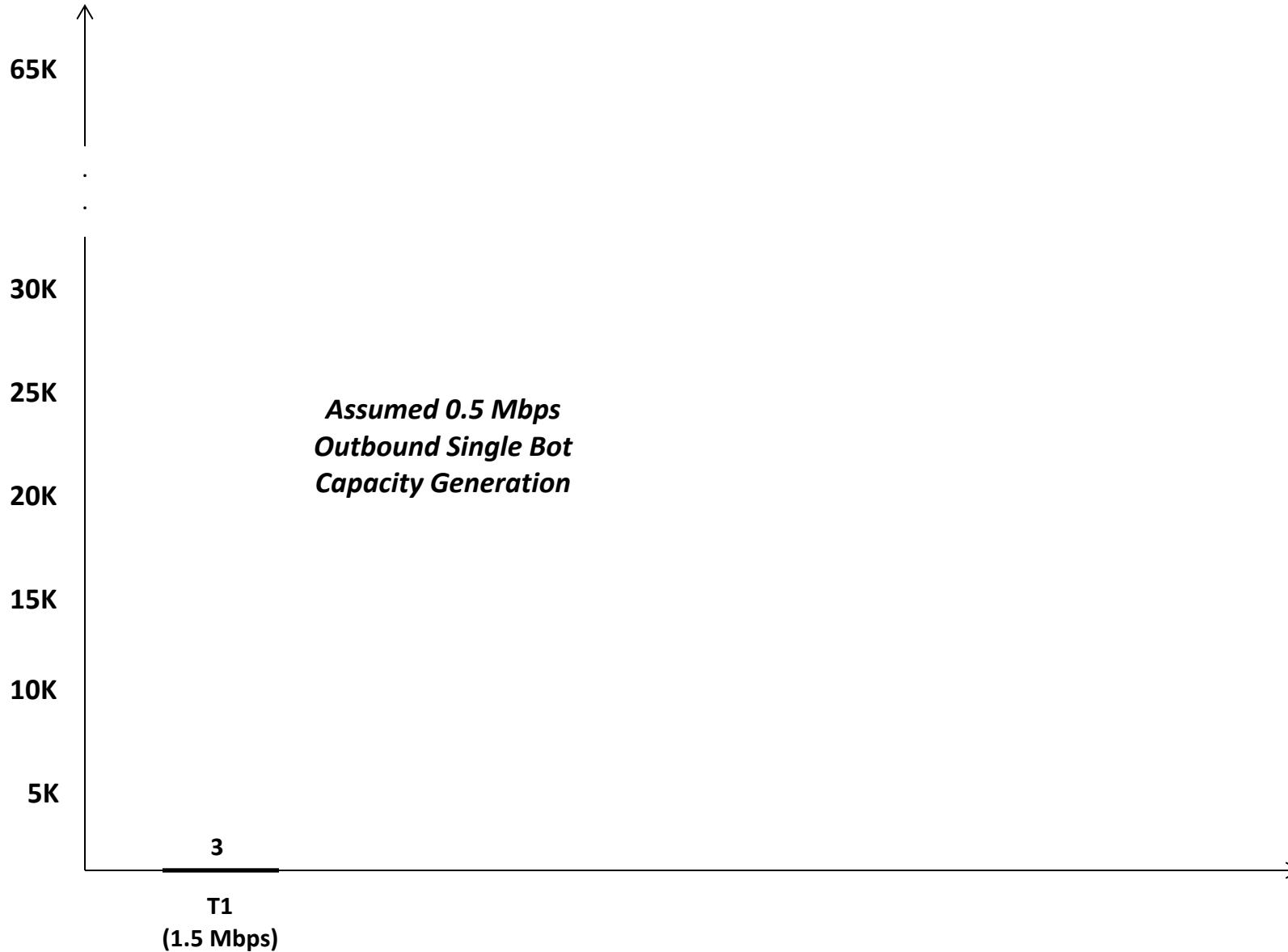
Botnets



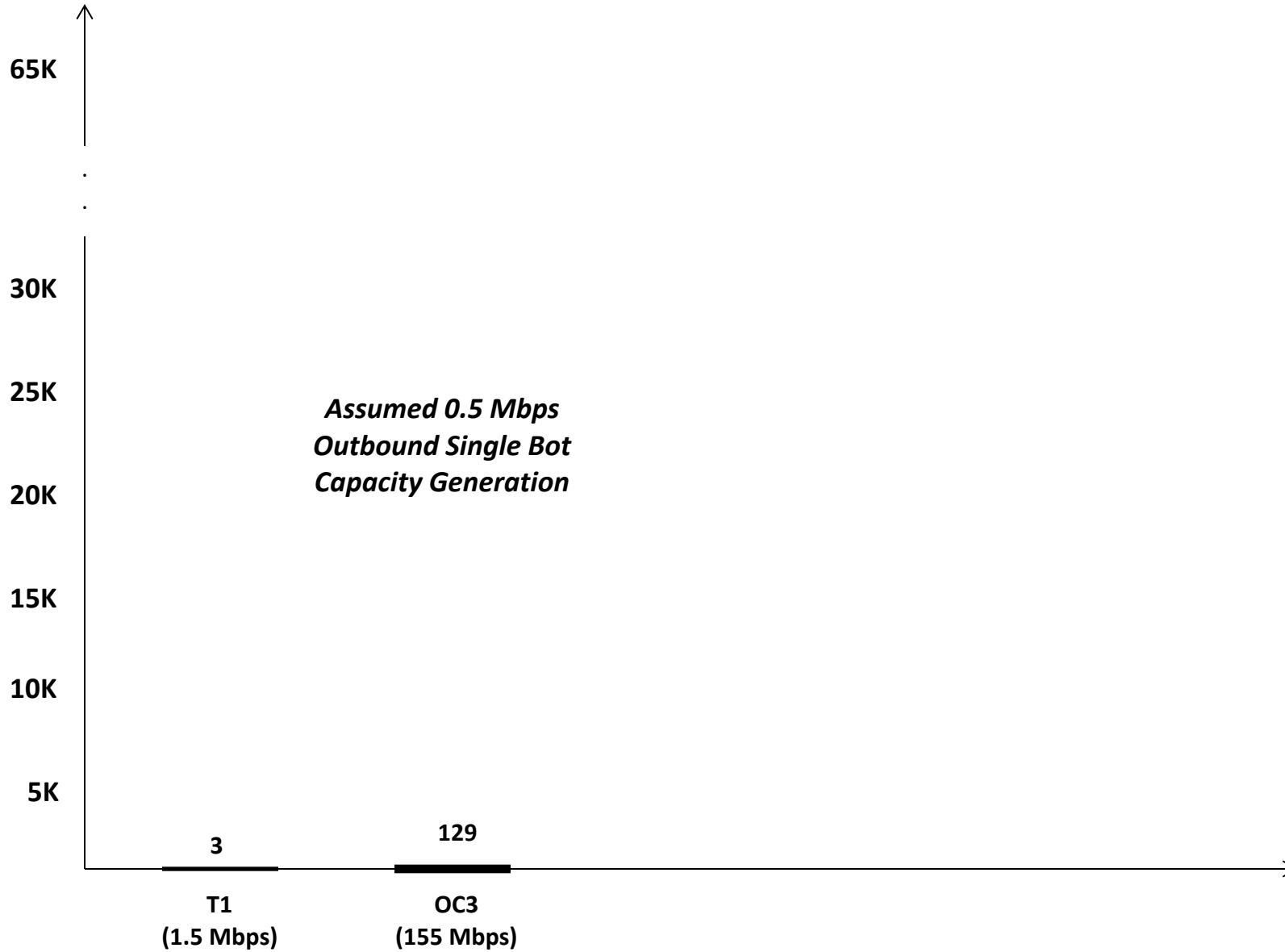
Typical Botnet Visualization



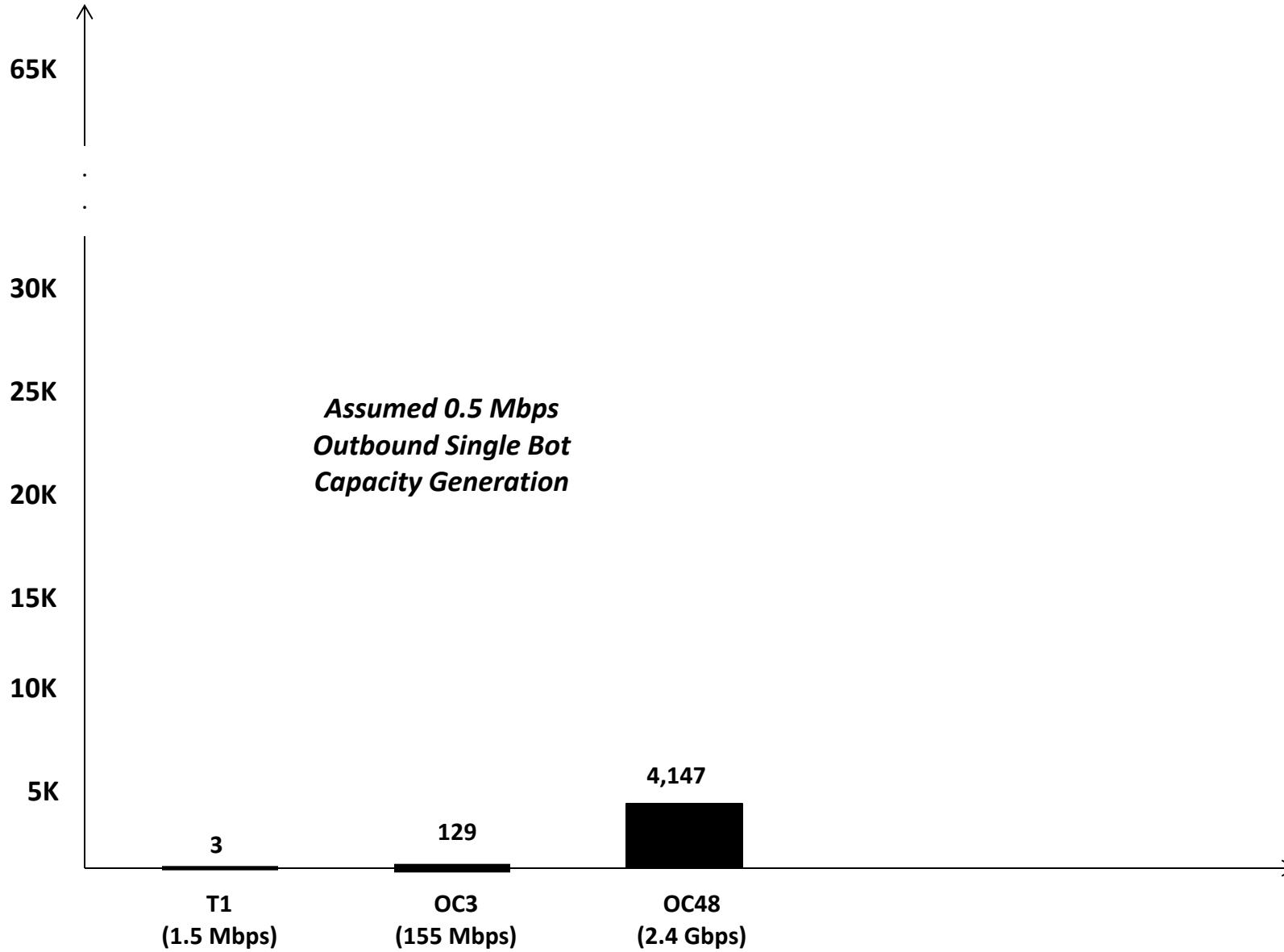
Bot Capacity Generation (500Kbps)



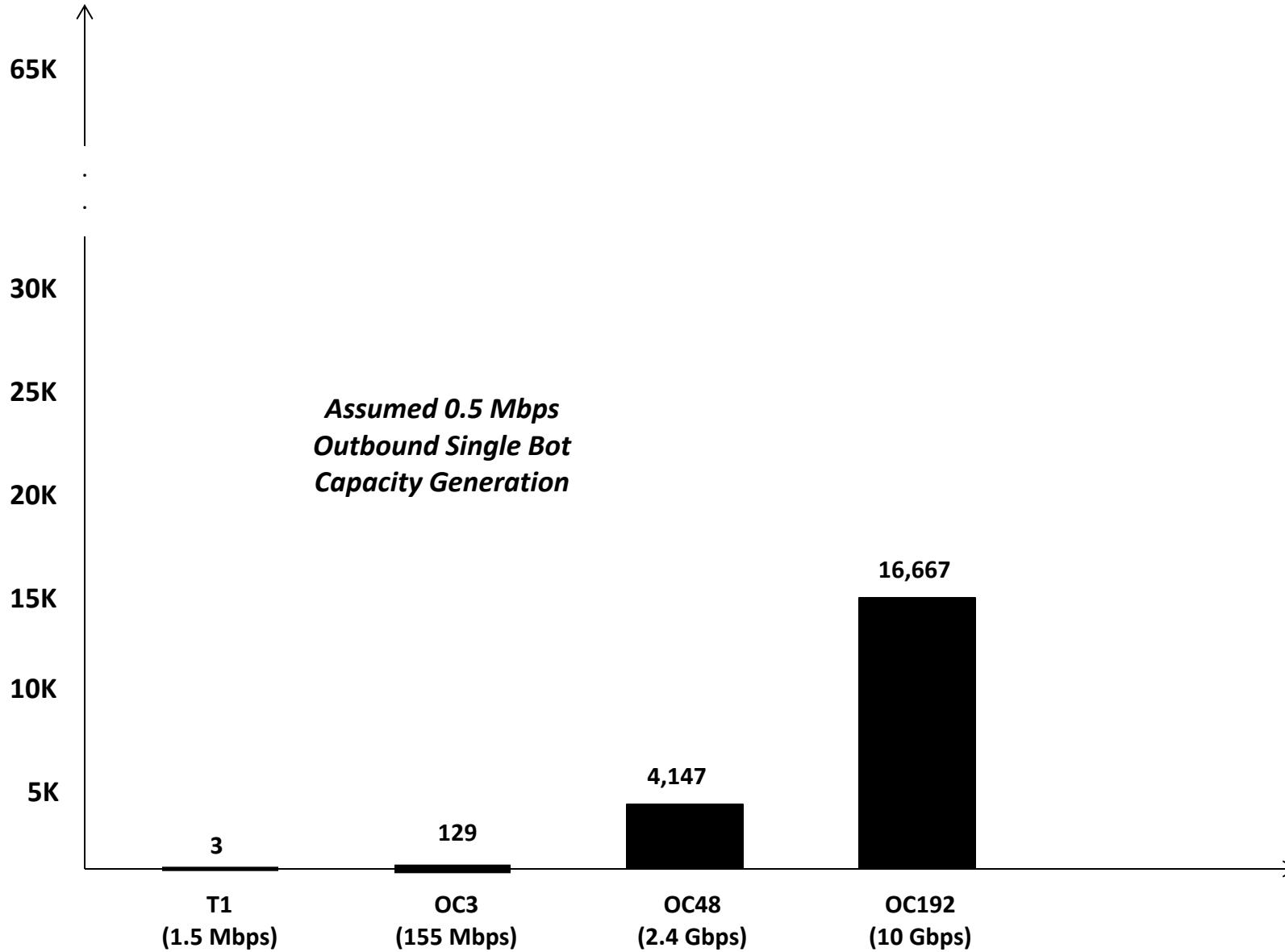
Bot Capacity Generation (500Kbps)



Bot Capacity Generation (500Kbps)

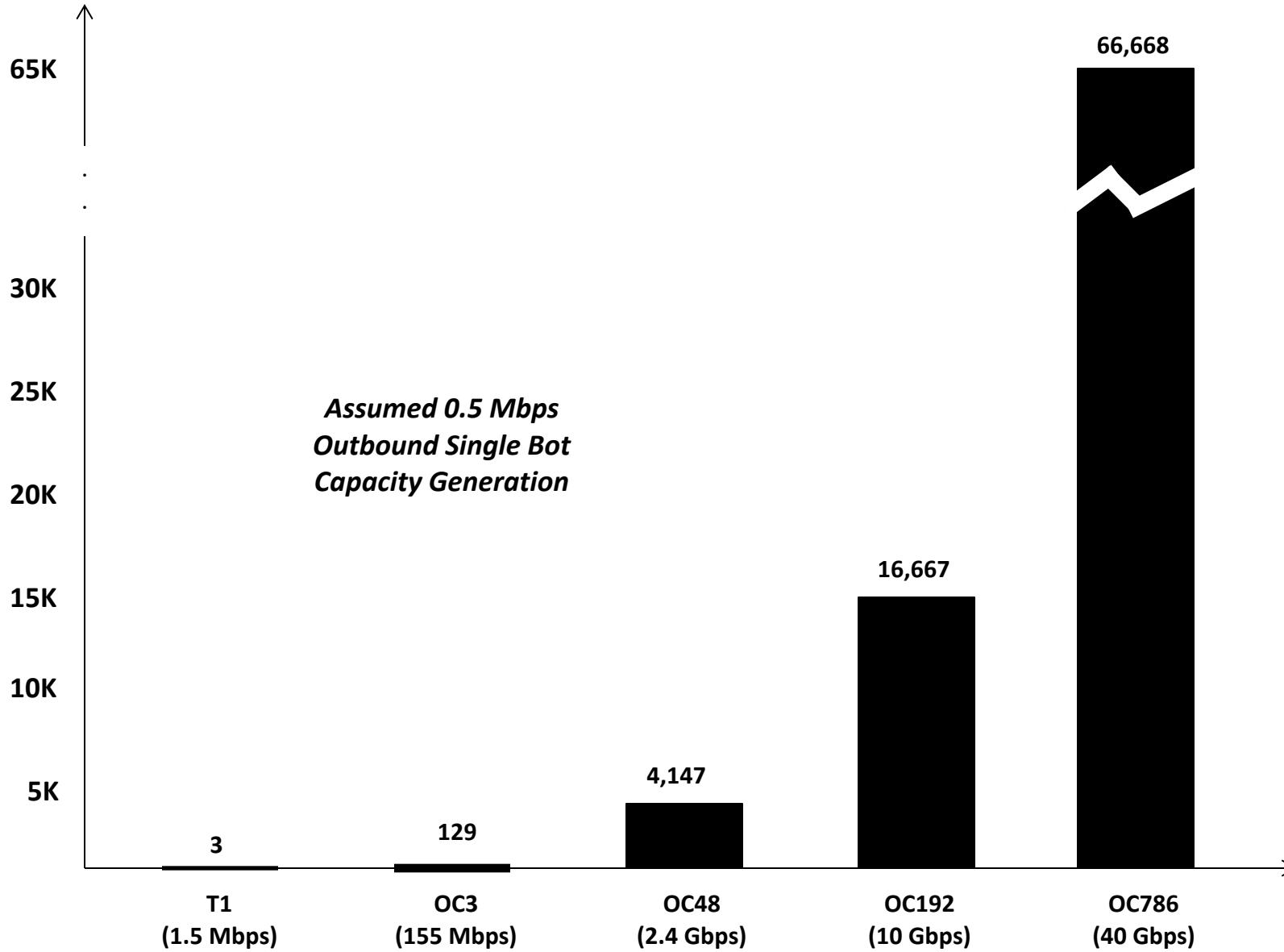


Bot Capacity Generation (500Kbps)



Week 3

Bot Capacity Generation (500Kbps)



Botnet Capacity Generation (750 Kbps – 1.0 Mbps)

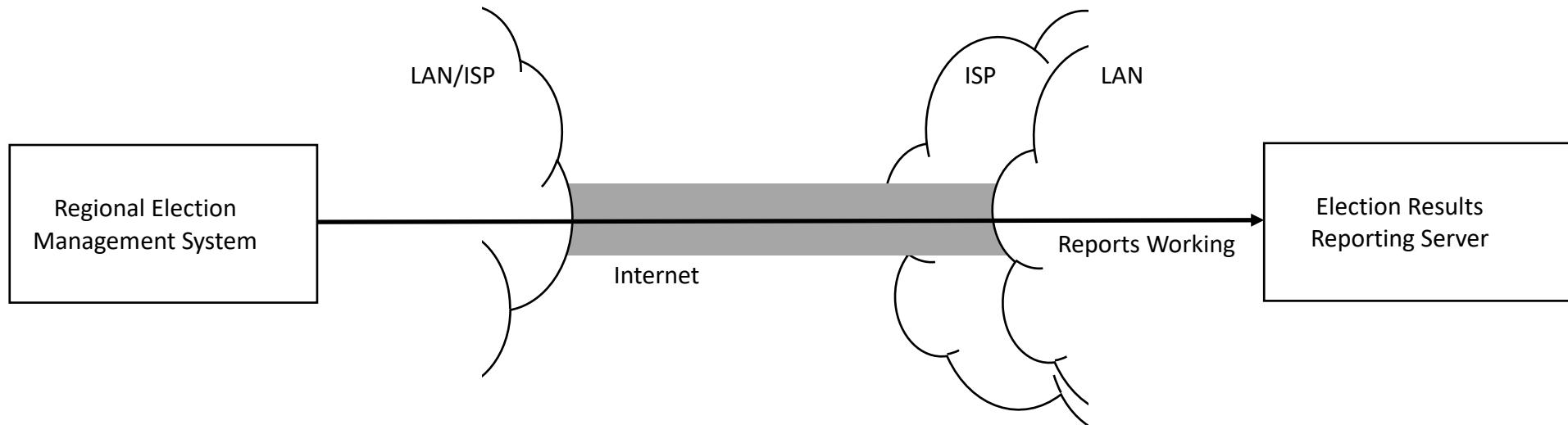
Number of Bots	Outbound Capacity	Size of Attack	Network Size
2	750 Kbps	1.5 Mbps	T1
1,200	1.0 Mbps	1.2 Gbps	OC-24
2,400	1.0 Mbps	2.4 Gbps	OC-48
10,000	1.0 Mbps	10.0 Gbps	OC-192
40,000	1.0 Mbps	40.0 Gbps	OC-768
80,000	1.0 Mbps	80.0 Gbps	<i>Starts to fill typical ISP backbone</i>
100,000	1.0 Mbps	100 Gbps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

Week 3

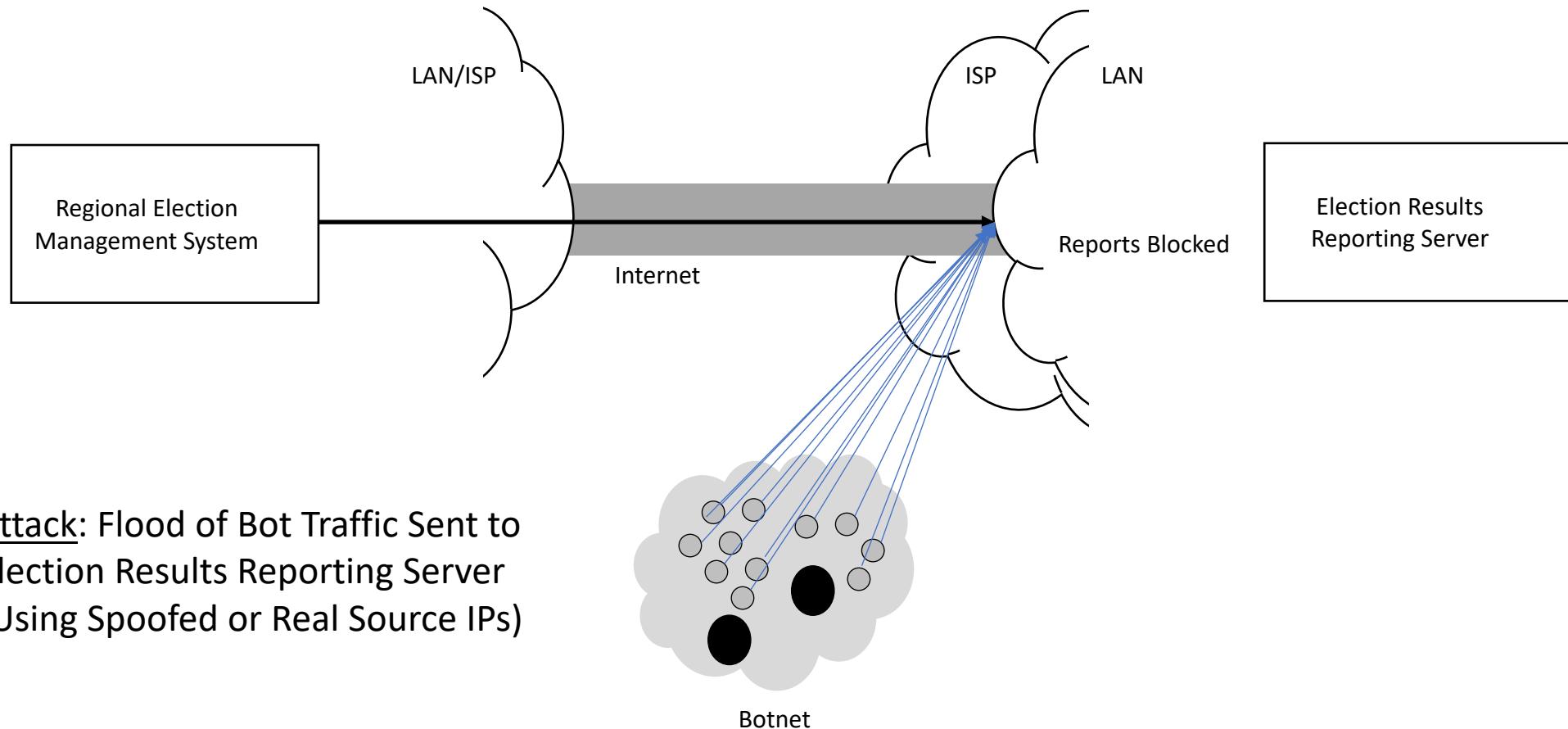


Can You Stop DDOS Attacks?

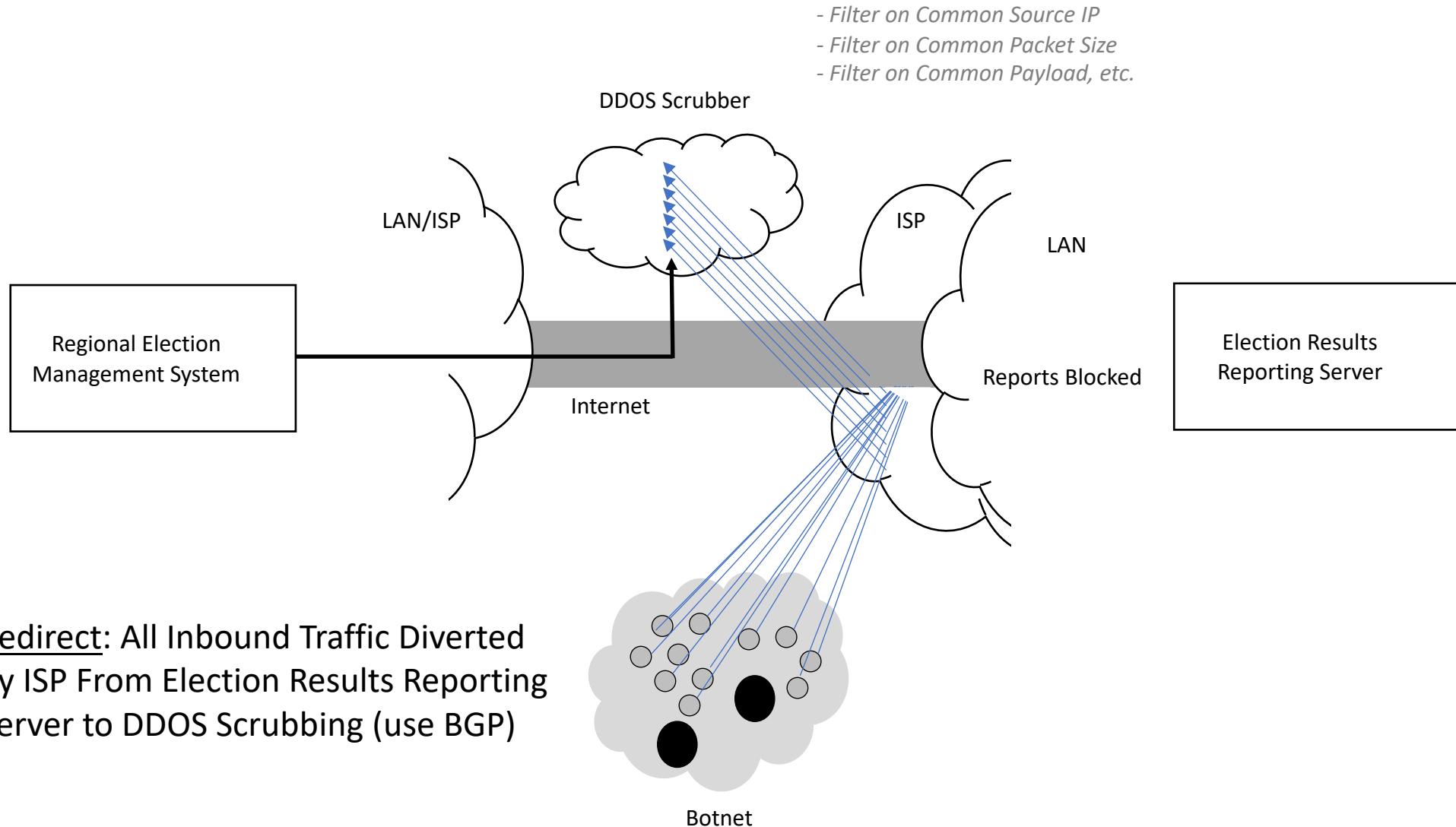
Case Study: Mitigating Inbound Election Reporting DDOS



Case Study: Mitigating Inbound Election Reporting DDOS



Case Study: Mitigating Inbound Election Reporting DDOS



Case Study: Mitigating Inbound Election Reporting DDOS

