



Common Sense Network Security

**Because on the cutting
edge, someone has to bleed!**



viawest



The Problem

- Denial of Service
- Unauthorized Use of Services
- Data Alteration
- Data Loss
- Public Image
- Loss of Trust



viawest



Growing Concerns

New Vulnerabilities Growth

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-Q1 2005

Year	2000	2001	2002	2003	2004	Q1-2005
Vulnerabilities	1090	2437	4129	3784	3780	1220

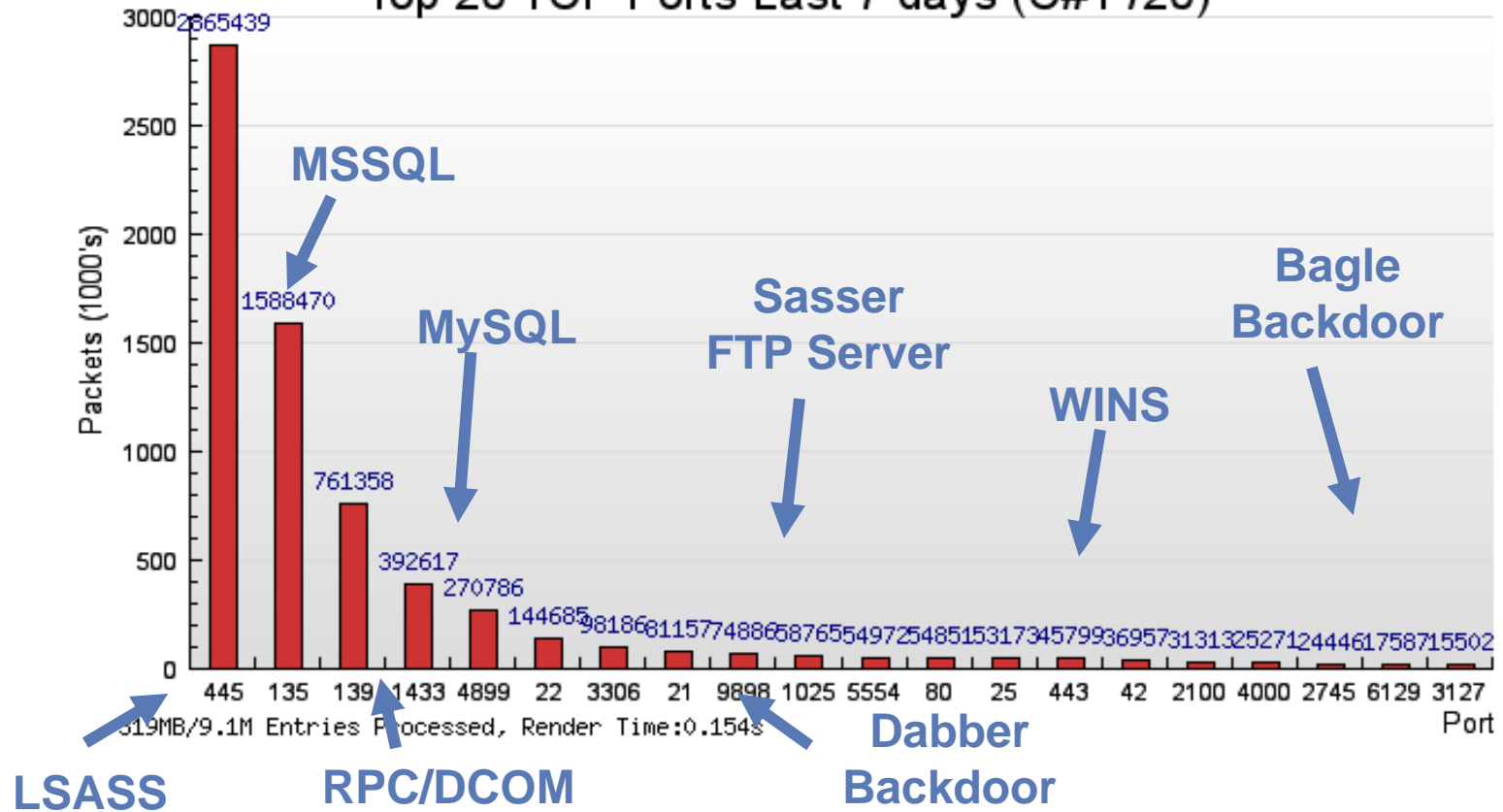


viawest

What ViaWest Sees at One Monitoring Point!

ViaWest
/20

Top 20 TCP Ports Last 7 days (C#1 /20)





A Holistic Approach

- There is no single device that will save you
 - You have to have a layered approach
- Get a good lay of the land
 - Know what your most valued assets are and work to best protect those
- Take it in chunks
 - There is no reason to allow protocols that you do not run to have access to your establishment



viawest



A Holistic Approach Continued

- Don't just throw money at it
 - Now that you have a good overview of your asset risk, determine a plan to mitigate those risks
 - Plan your work and work your plan
 - If you aim at nothing – you will hit it



viawest

It's Common Sense

- If you have the wrong people – nothing will help!
 - Smart equipment cannot protect you from stupid people
 - You need a well-rounded security geek
- If you don't know what you expect to find, expect what you don't want to find
 - Figure out what you should be running on your network in order to isolate what should not be running on your network
- Eventually it will get in
 - A worm, virus, Command and Control hack – it will happen
 - This can come from employee laptops, websites, downloads, chat clients...
 - Keep it from getting out (while you track it down)



viawest



Routers and Switches

- Hidden management addresses
 - Loop-back addresses for management access
 - Loop-back addresses for protocol communication
- Encrypted protocols
 - Management through SSH
 - Inter-device communication if possible
- Accounting - Access and Command
 - Know who and what is going on with management of your devices
- Periodical code reviews
 - If no issues are identified in the current code tree, there is a review of existing code for non-critical issues
 - Look to improve stability and limit vulnerabilities
 - IOS Security Template
 - <http://www.cymru.com/Documents/secure-ios-template.html>
 - IOS Secure BGP Template
 - <http://www.cymru.com/Documents/secure-bgp-template.html>



Routers and Switches Continued

- Limit Device access
 - Much of what is occurring today are “command and control” hacks. By limiting the addresses that are allowed to control routers and switches we can minimize this threat.
 - “Need to know” access
 - Limit access to certain devices to appropriate personnel
- Reverse Path Forwarding principles are used on all customer facing ports (this could be ACL’s or RPF in the routing table)
 - Many DOS attacks and viruses “spoof” the source address. On ViaWest’s network, customers can only send traffic from “their” address space. This limits the spread of many viruses while quelling some DOS attacks.



viawest

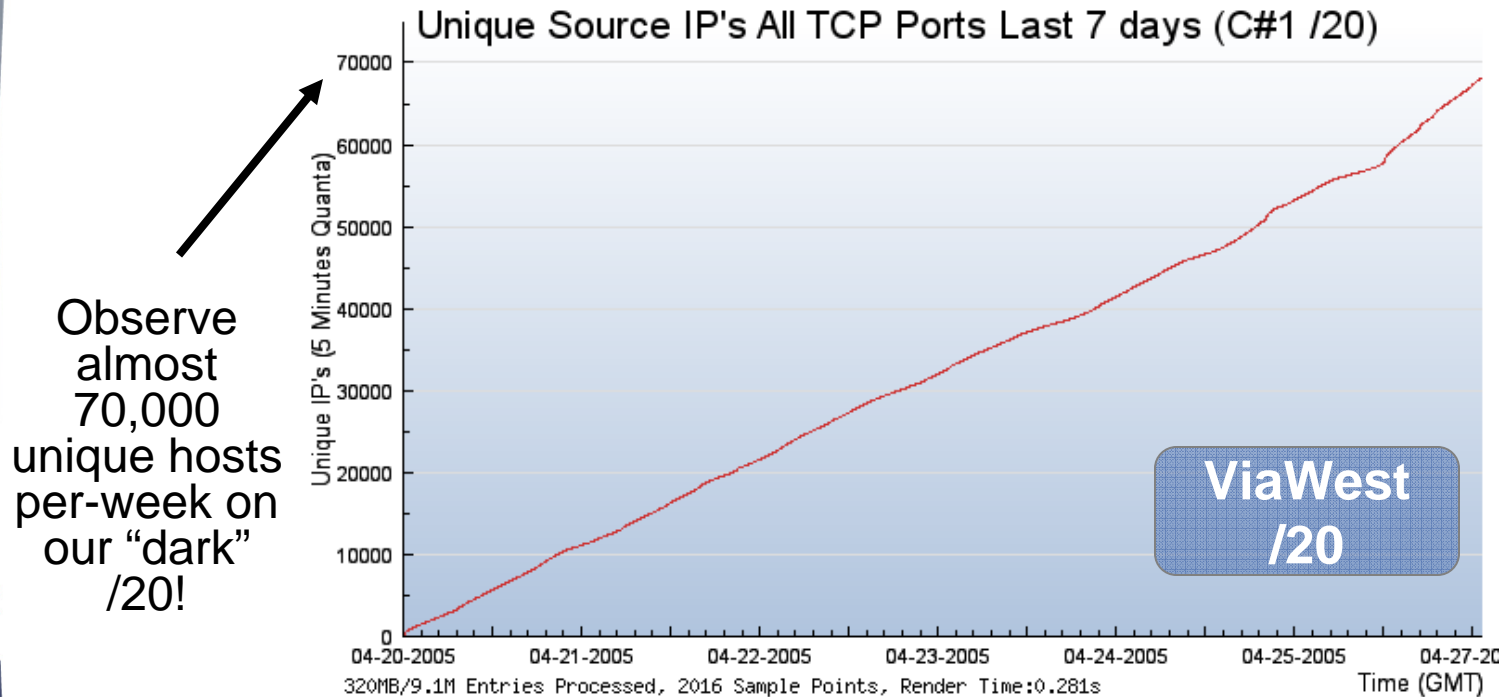
Monitoring

- Define what is “normal” for your network
 - Then you can tell what is abnormal
- It’s not “fire and forget”
 - Someone actually has to look at the data
- Bandwidth
 - Just watch for abnormal bandwidth changes on **your** network.
 - Is a 5 minute spike from 20Mbps to 100Mbps normal behavior on your network?
 - Do at multiple layers- Borders, Cores, Switches, Offices...
- Watch the Flow
 - IP flow monitoring can be very useful
 - Watch for anomalies and known issues
- Communicate with the community
 - Use mailing lists and websites for information
 - Bugtraq
 - CERT
 - seclist.org
 - IMS
 - iDEFENSE



What You Can Find

- Deployed an IMS sensor in May 2004 - One of the *first* IMS participants
- Currently Monitoring: /20, /21, /22

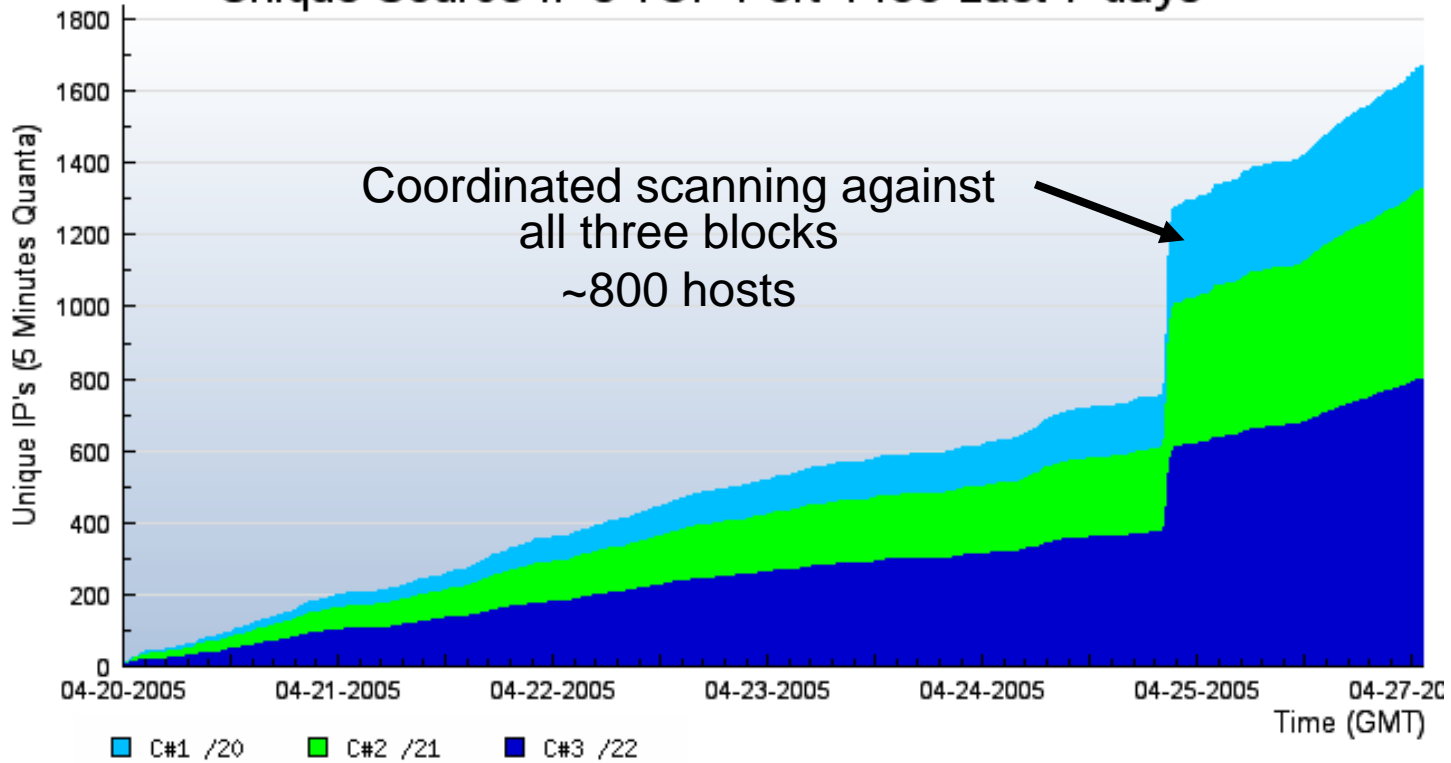


What Can You Find

- Targeted attacks are common (A botnet?)

ViaWest
/20,/21,/22

Unique Source IP's TCP Port 1433 Last 7 days

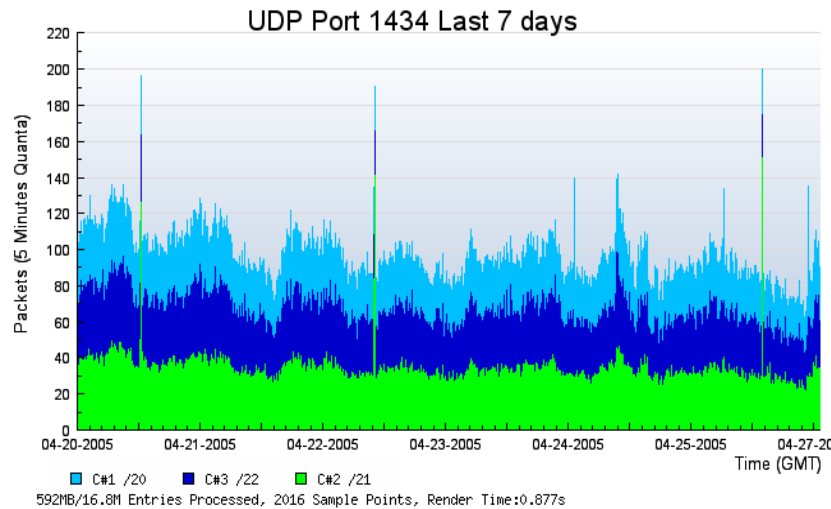


590MB/16.7M Entries Processed, 2016 Sample Points, Render Time:0.842s

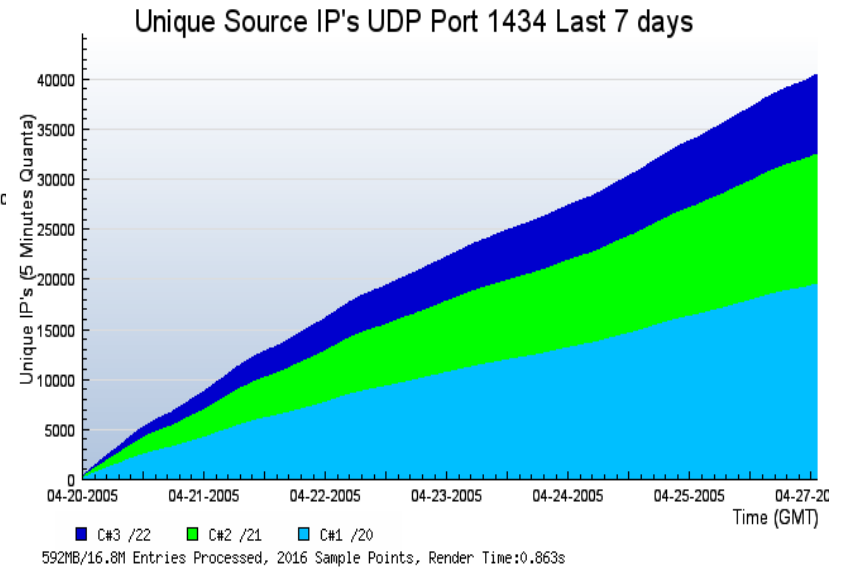


What Can You Find

- Similar port mix: TCP 135/445 still dominate
- Many more multi-vector threats. Single IP address can try more than 6 exploits
- Old worms still haunt us: **SQL Slammer (2003)**



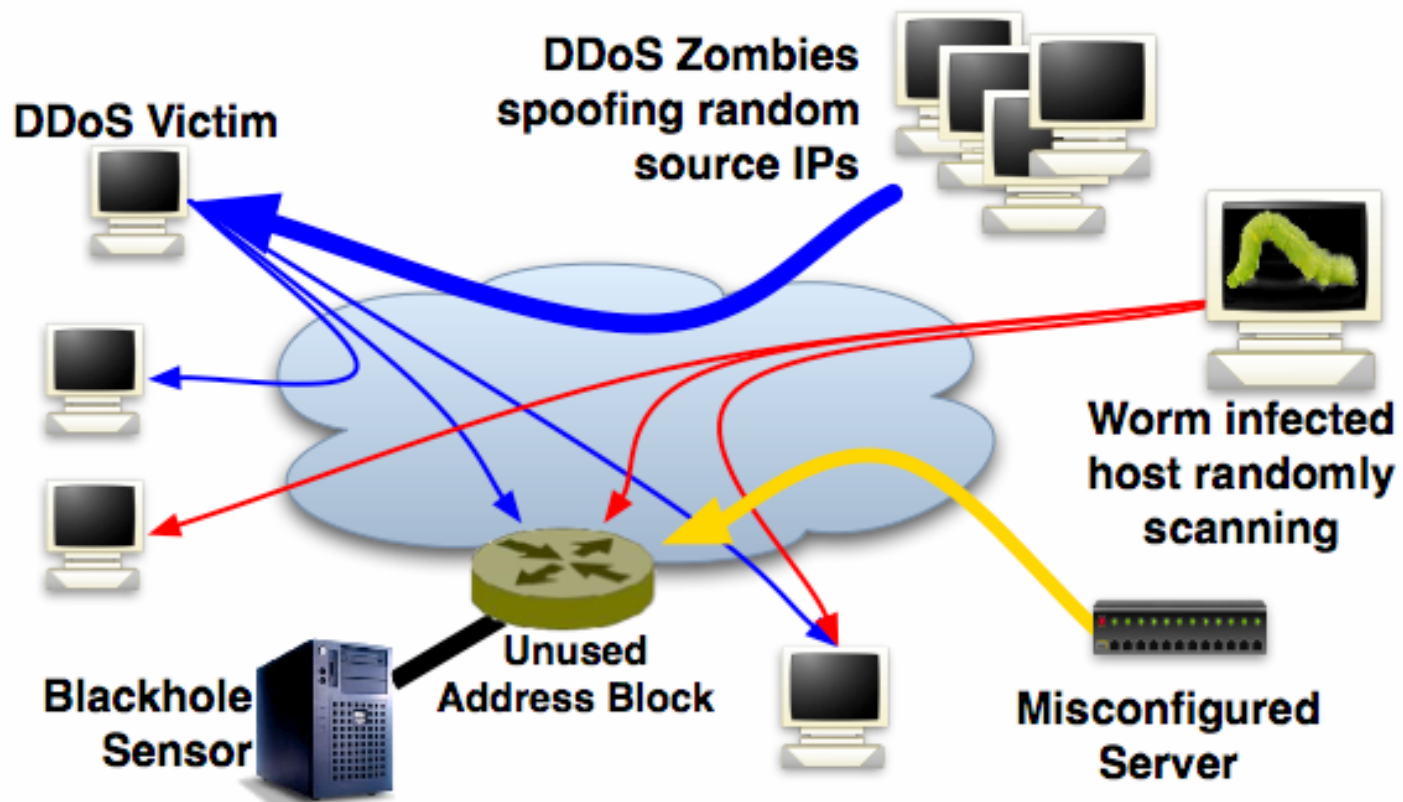
ViaWest
/20,/21,/22



Yup, that's 20K
Slammer hosts at
one sensor!



How a Blackhole Monitor Works



The Internet Motion Sensor: A Distributed Blackhole Monitoring System



Infrastructure Protection

- Face it – you are a target!
 - As you can see, if you are on the Internet – you are a participant
- Segmentation
 - If everything is in the same LAN and same IP network, it's going to be very hard to control
- Firewalls
 - DMZ
 - Departments
- IDS
 - Appliances
 - Host based



viawest

Infrastructure Protection Continued

- DNS
 - Split
 - Run a hidden master or a true split setup
 - Controlled access
 - Not everyone needs to do a zone transfer
- Regular systems patching
 - Patch when they are available and able
 - They may have fixed a hole that they are about to announce!
 - Automated is nice
- Virus protection
 - You have to protect your employees from their regular work
 - If they use email – it's just a matter of time
- Enforced termination procedures
 - When someone leaves, does access get revoked quickly and immediately?



Pre-planned Corrective Action

- Don't run on the edge of resources
 - There is no overhead left to deal with the attack
- Sinkhole routing – IGP oriented
 - Once trouble addresses are determined, we can send them to our sinkhole router to minimize their ability to infect others
- Blackhole routing – BGP oriented
 - We allow our customers to send blackhole and preference communities to us
 - we have agreements with our upstream providers to accept certain BGP community strings to blackhole suspect traffic *before* it hits our network
- IDP products
 - Stop small attacks in progress



viawest



Policy

- Define your policy in writing
 - It's hard to refer to speeches
- Define enforcement procedures
 - What happens when someone keeps bringing viruses from home?



viawest



Summary

- It IS going to happen to you
- Be holistic in your approach
 - There is no silver bullet
 - Protection through layers
- Know what is normal
 - So that abnormal is obvious
- Keep code up to date
 - If you are running 10 series IOS on your Cisco you have problems
- Plan for failure
 - Eventually something will occur, have a plan of action
- Write it all down
 - Documentation is critical for consistency



Questions?

- Contact information
 - Barry Dykes
 - bdykes@viawest.net
 - Danny McPherson
 - Internet Motion Sensor/Arbor Networks
 - Brady Ranum
 - branum@viawest.net



viawest



Thank You



viawest