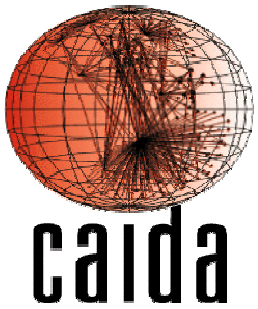
Security Data Collection at CAIDA

Colleen Shannon (CAIDA)
David Moore (CAIDA/UCSD-CSE)

cshannon @ caida.org
dmoore @ caida.org
www.caida.org



Outline

- Data Collection at CAIDA
- CAIDA Security Research:
  - What is a Network Telescope?
  - Denial-of-Service Attacks
    - SCO DoS Attack
  - Internet Worms
    - Code-Red
    - SQL Slammer

Current Project Areas

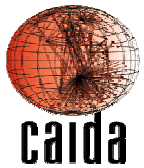
- Routing topology and behavior
- Passive monitoring and workload characterization
- Internet Measurement Data Catalog
- Bandwidth estimation
- Flow collection and efficient aggregation
- Security: DoS and Internet worms
- DNS performance and anomalies
- Visualization

Current Project Areas

- Routing topology and behavior
  - Skitter, scamper; monitors around the world
- Internet Measurement Data Catalog
- Trace Collection and Storage
  - Maintaining remote monitors
  - Transferring files back to SDSC
  - Sanitizing data
  - Managing data access
- Security: DoS and Internet worms

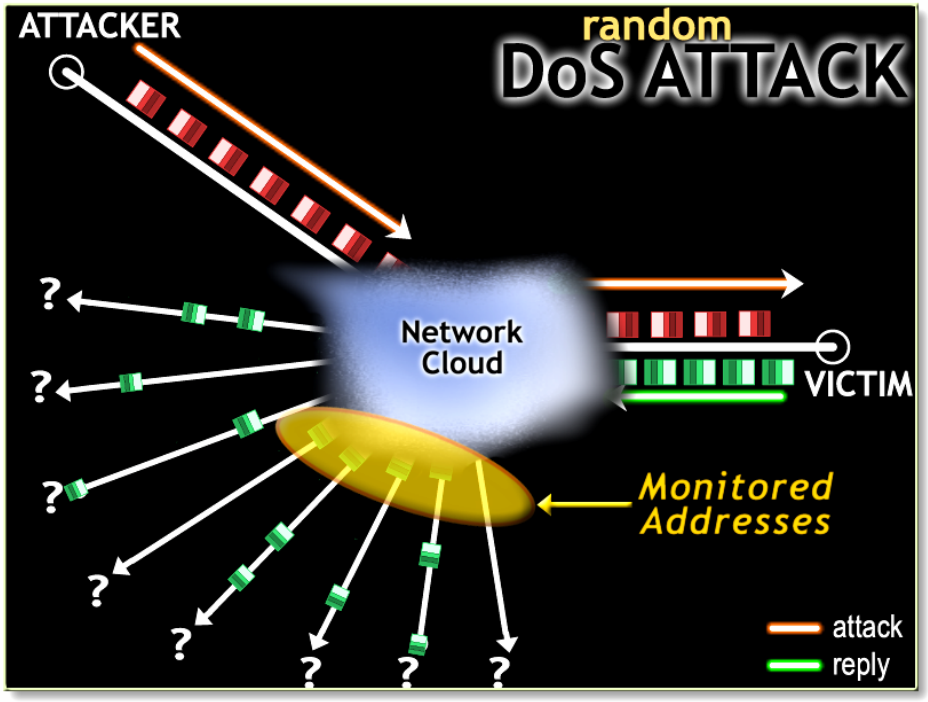
Network Telescope

- Chunk of (globally) routed IP address space
  - 16 million IP addresses
- Little or no legitimate traffic (or easily filtered)
- Unexpected traffic arriving at the network telescope can imply remote network/security events
- Generally good for seeing explosions, not small events
- Depends on random component in spread

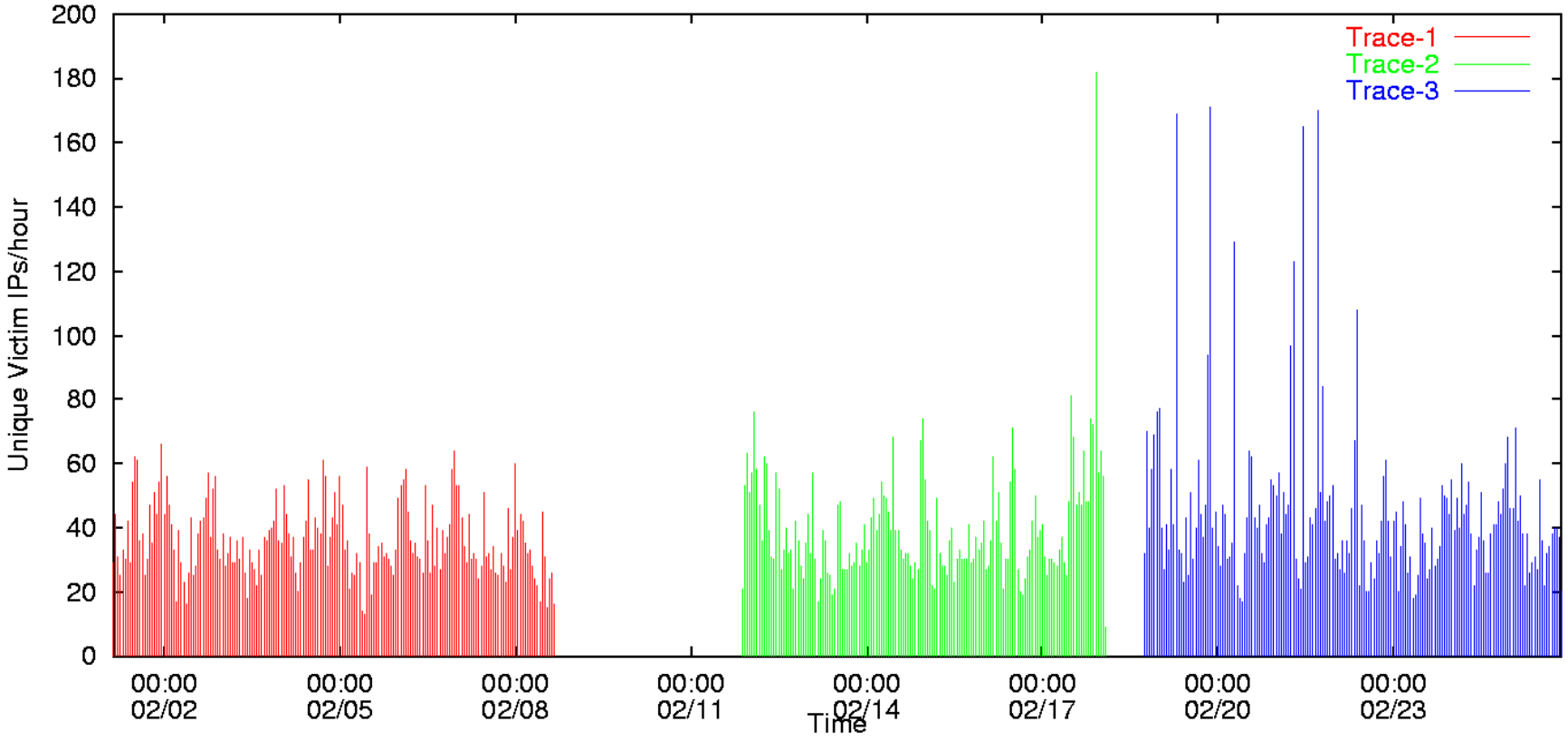


Network Telescope: Denial-of-Service Attacks

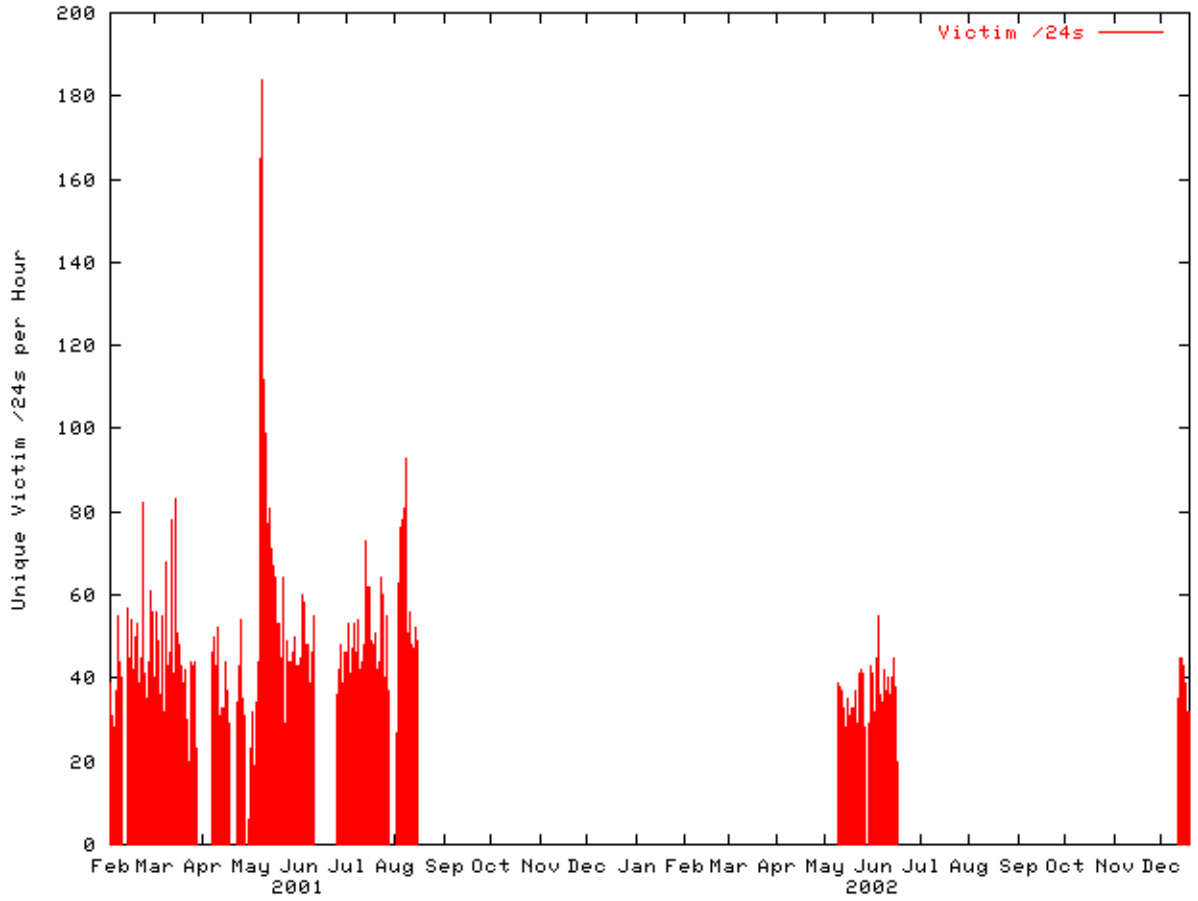
- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- We observe 1/256th of all *victim responses* to spoofed addresses [MSV01]



Denial-of-Service Attacks



DoS Attacks over time



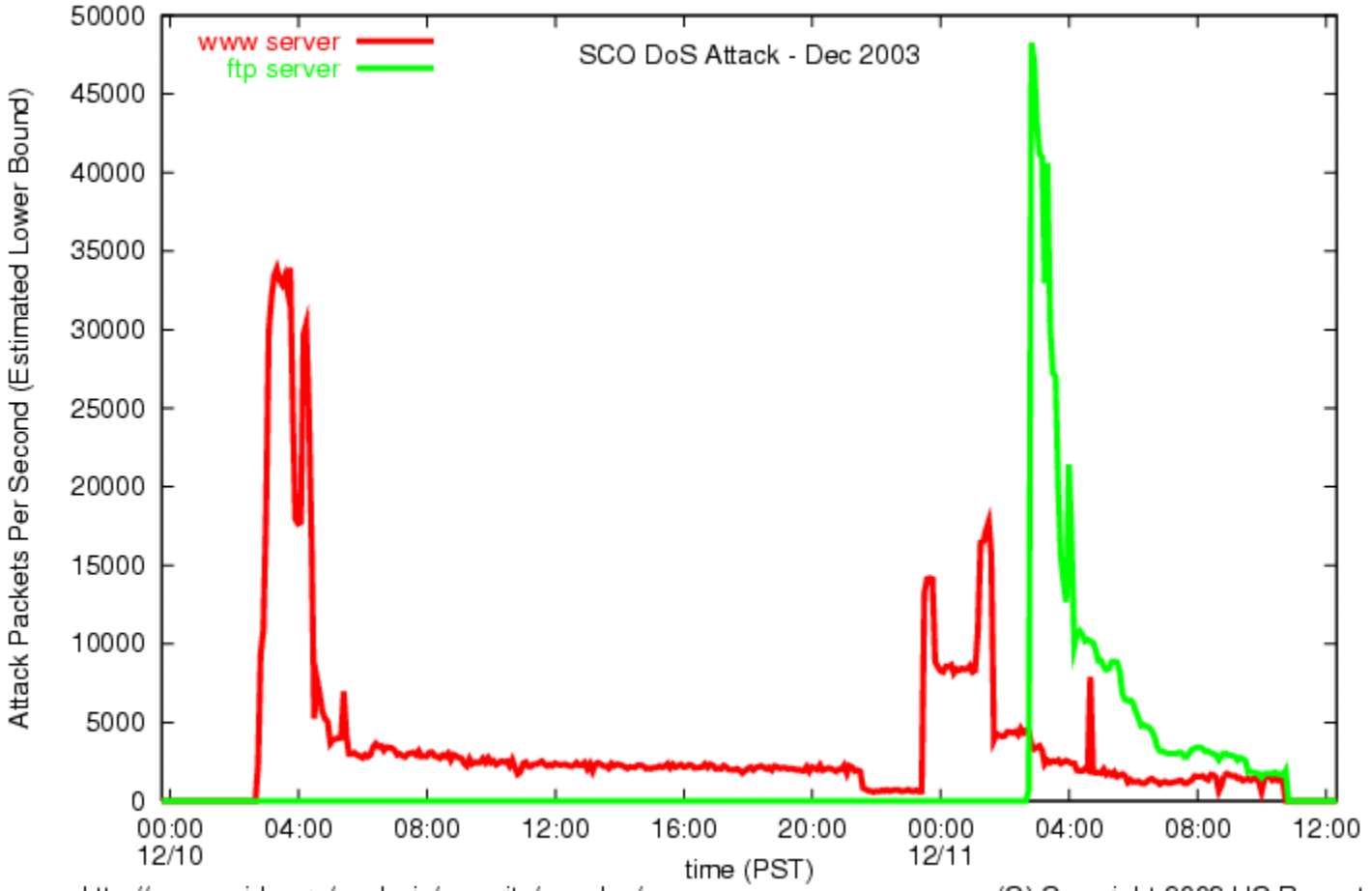
SCO Denial-of-Service Attack

- Who is SCO?
  - UNIX (linux) software company
  - Originally Santa Cruz Operations
  - Caldera bought Unix Server Division from Santa Cruz Operations in August of 2000
  - Caldera changed its name to "The SCO Group" in Aigist 2002
  - Sued IBM in March 2003 claiming that IBM misappropriated its UNIX operating system intellectual property (acquired from Novell)
  - Threatened lawsuits against many others

SCO Denial-of-Service Attack Timeline

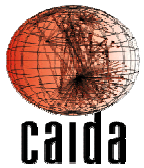
- May 2003: SCO gets hit by its first major DoS Attack
- August 2003: SCO gets hit by its second major DoS Attack
  - random rumors that an internal network problem was publicized as a DoS attack
- December 10, 2003 3:20 AM: an ~340,000 MB/s SYN flood incapacitates SCO's web servers
- December 10, 2003 1:37 PM: groklaw.net blog "reports" on rumors that SCO is not being attacked; they are faking the whole thing to implicate the open source community
- December 11, 2003 2:50 AM: the SYN flood is expanded to target SCO's ftp server in addition to their webservers
- December 11, 3003 noon: SCO takes themselves off the 'net while pursuing upstream filters to block the attack

SCO Denial-of-Service Attack



Now it gets interesting…

- Rabid open source folks attack CAIDA -- did you know:
  - all of our work is funded by SCO
  - CAIDA isn't actually a research organization at all; it didn't exist before December 10th
- CAIDA webserver gets a DoS attack of its own
  - 11pm-1am PST
  - Some attack characteristics point to the same perpetrator (or simply same attack tool) but no conclusive evidence

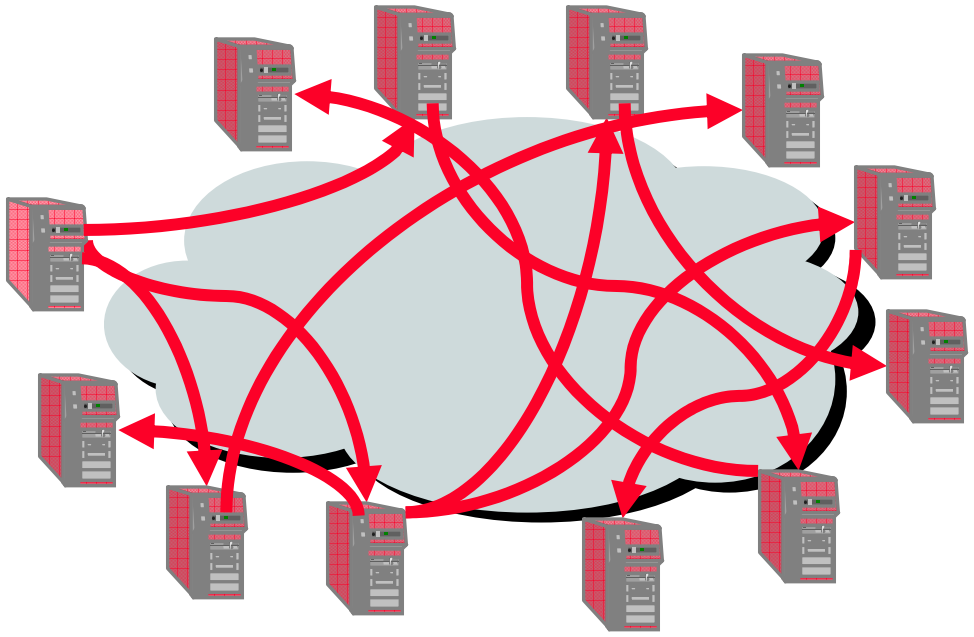


SCO DoS Attack "Results"

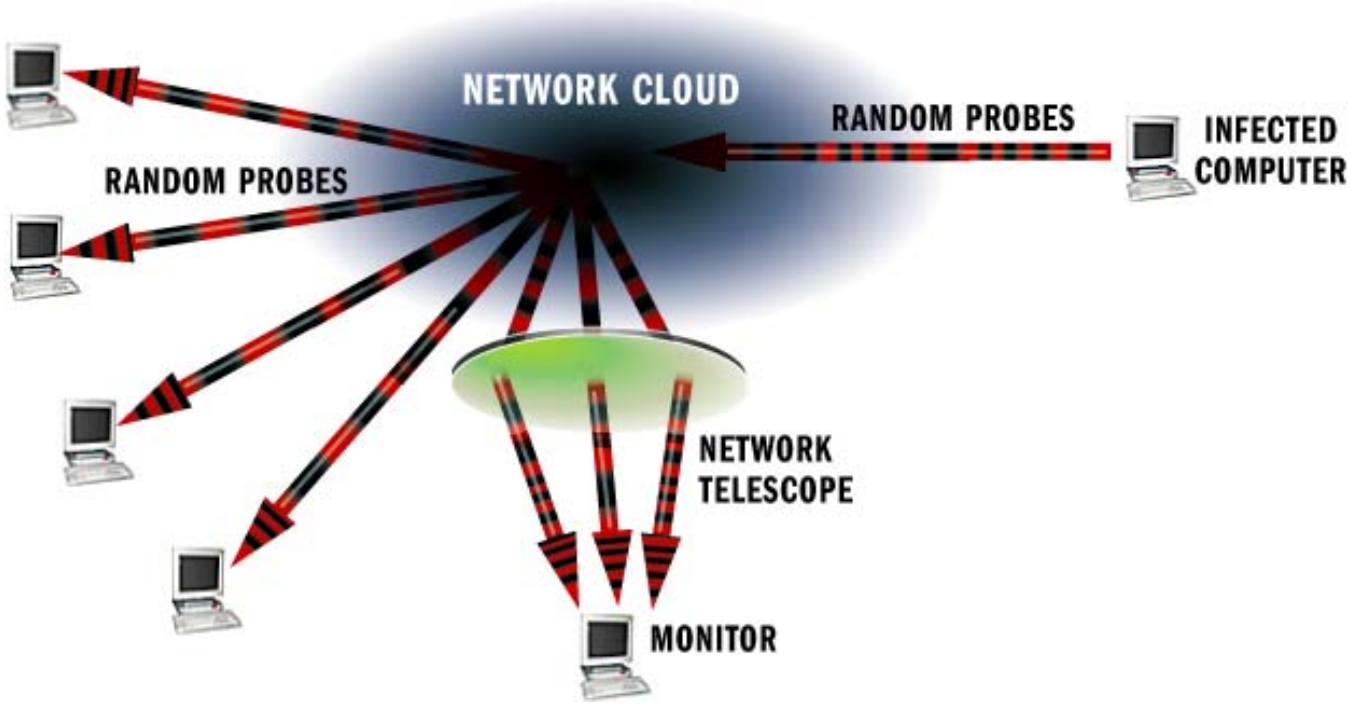
- Security experts (us included) need to be careful what they say in the absence of details
  - Sure, technology exists to thwart SYN floods, but not at 340 MB/s inbound coming to a DS3
- It's no fun to be a SCO network admin
  - your own ISP won't admit they give you connectivity, let alone corroborate the attack reports
  - your CEO is quoting the aforementioned security experts who say any 5 year old could stop the attack
  - your only hope is upstream ISPs helping you, but your company is not popular with NOC employees
- Why did folks believe SCO was faking the attack?

What is a Network Worm?

- Self-propagating self-replicating network program
  - Exploits some vulnerability to infect remote machines
    - No human intervention necessary
  - Infected machines continue propagating infection



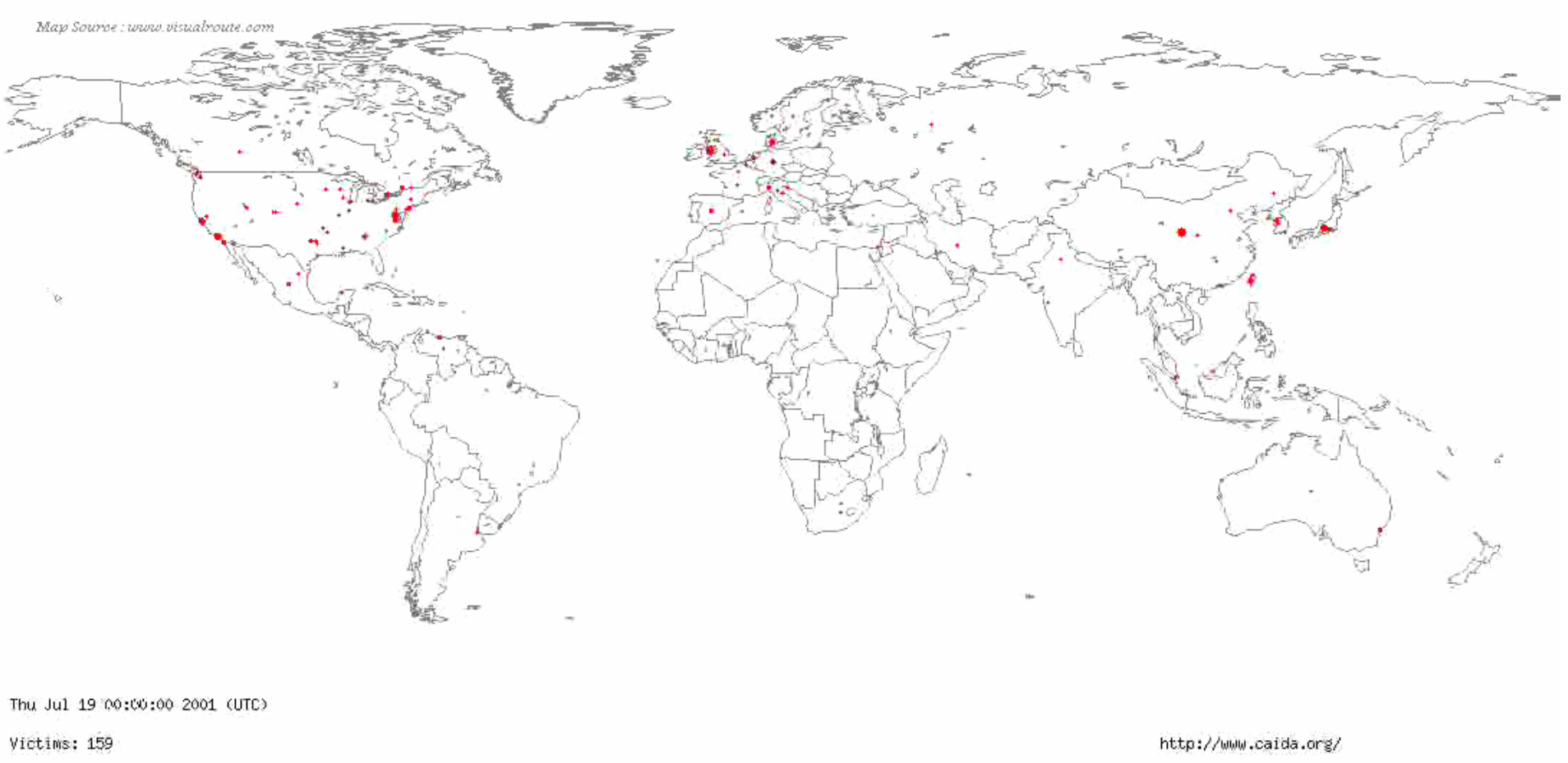
Network Telescope: Worm Attacks



- Infected host scans for other vulnerable hosts by randomly generating IP addresses
- We monitor 1/256th of all IPv4 addresses
- We see 1/256th of all worm traffic of worms with no bias and no bugs

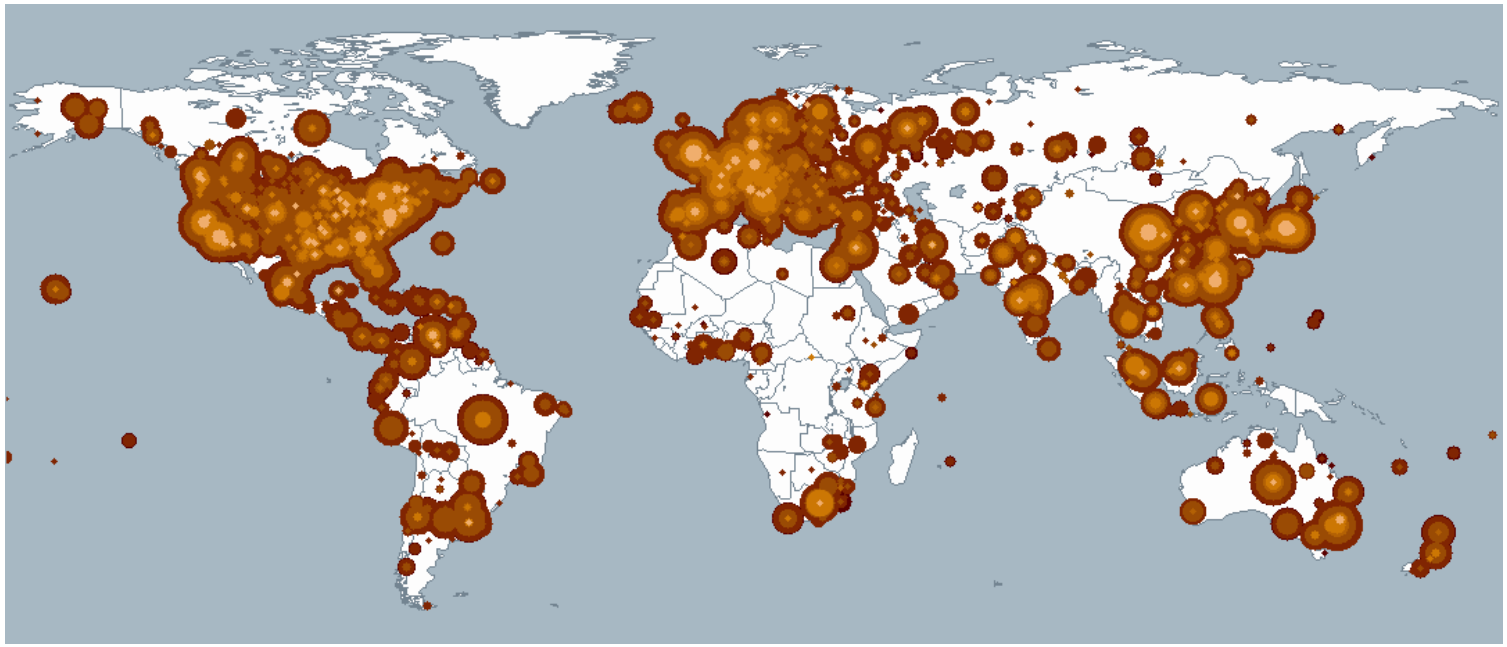
Internet Worm Attacks: Code-Red

(July 19, 2001)



Internet Worm Attacks: Code-Red

(July 19, 2001)



- 360,000 hosts infected in *ten hours*
- No effective patching response
- More than $1.2 billion in economic damage in the first ten days
- Collateral damage: printers, routers, network traffic

Response to August 1st CodeRed

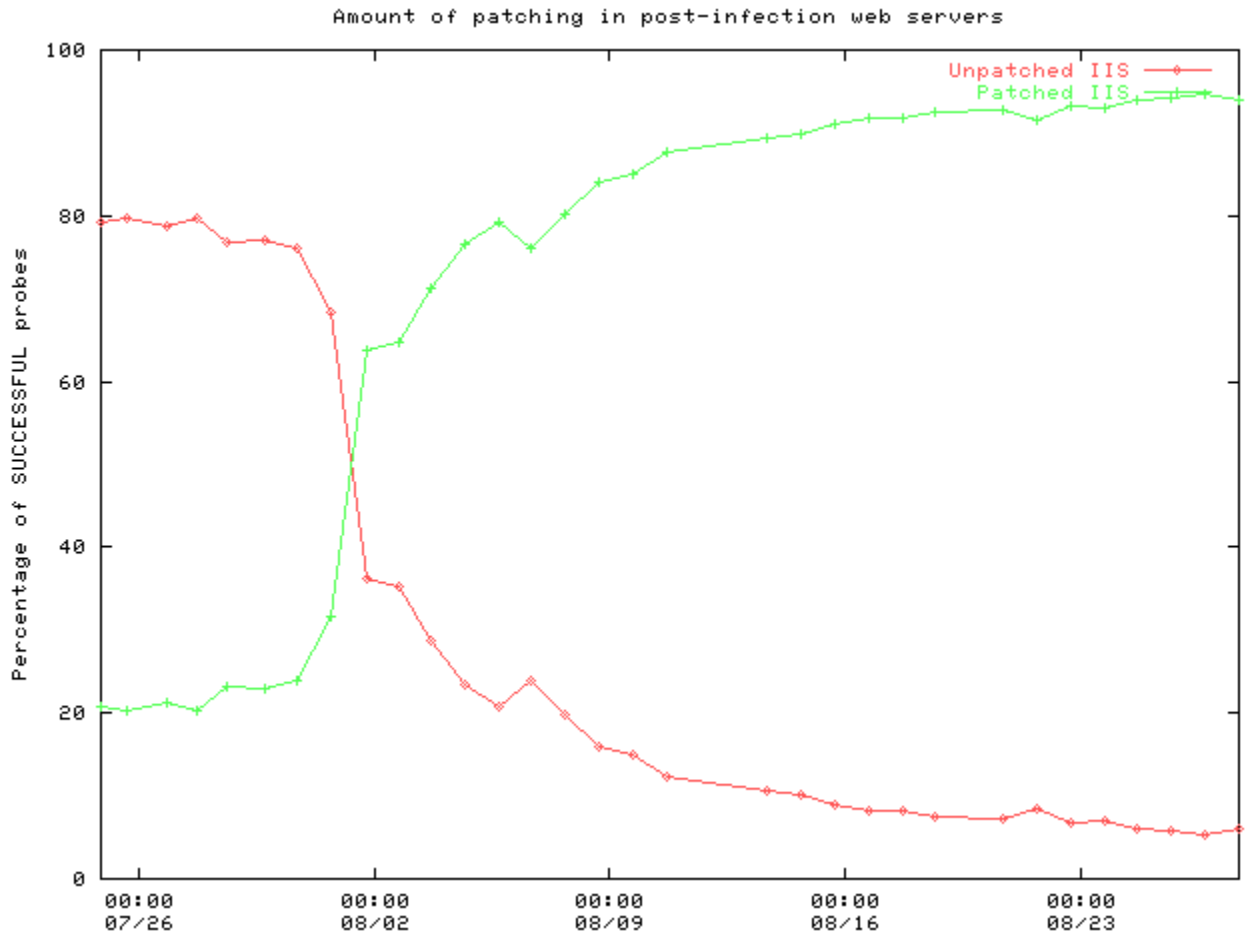
- CodeRed was programmed to deactivate on July 20th and begin spreading again on August 1st
- By July 30th and 31st, more news coverage than you can shake a stick at:
  - FBI/NIPC press release
  - Local ABC, CBS, NBC, FOX, WB, UPN coverage in many areas
  - National coverage on ABC, CBS, NBC, CNN
  - Printed/online news had been covering it since the 19th
- "Everyone" knew it was coming back on the 1st

- Best case for human response: known exploit with a viable patch and a known start date

Patching Survey

- How well did we respond to a best case scenario?
- Idea: randomly test subset of previously infected IP addresses to see if they have been patched or are still vulnerable
- 360,000 IP addresses in pool from initial July 19th infection
- 10,000 chosen randomly each day and surveyed between 9am and 5pm PDT

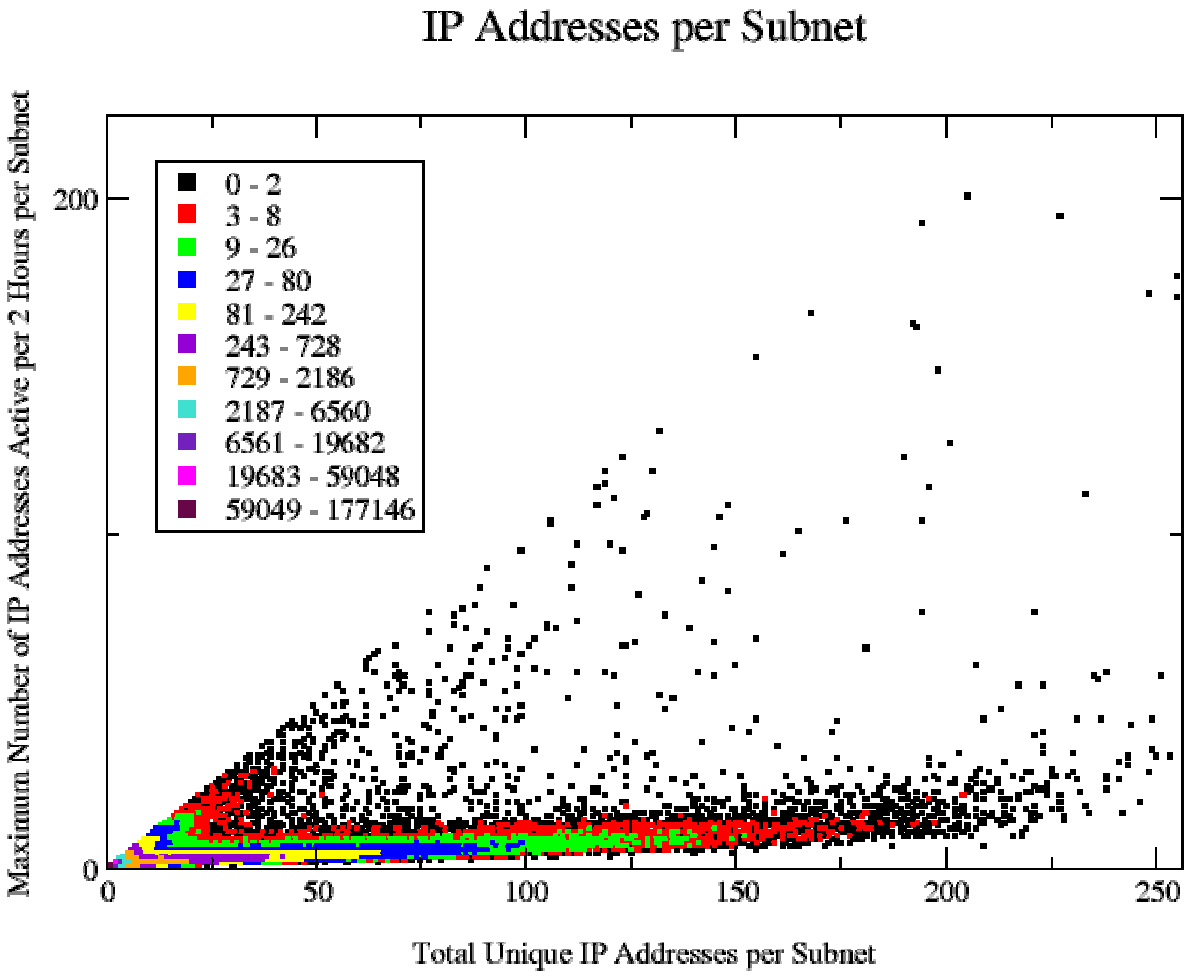
Patching Rate



Dynamic IP Addresses

- How can we tell how when an IP address represents an infected **computer**?
- Resurgence of CodeRed: Max of ~180,000 unique IPs seen in any 2 hour period, but more than 2 million across ~a week.
- This ***DHCP effect*** can produce skewed statistics for certain measures, especially over long time periods

DHCP Effect seen in /24s



Summary of Recent Events

- **CodeRed** worm released in Summer 2001
  - Exploited buffer overflow in IIS
  - Uniform random target selection (after fixed bug in CRv1)
  - Infects 360,000 hosts in 10 hours (CRv2)
  - Still going…
- Starts **renaissance** in worm development
  - CodeRed II
  - Nimda
  - Scalper, Slapper, Cheese, etc.
- **Sapphire/Slammer** worm (Winter 2003)
- **Witty** worm (March 19, 2004)

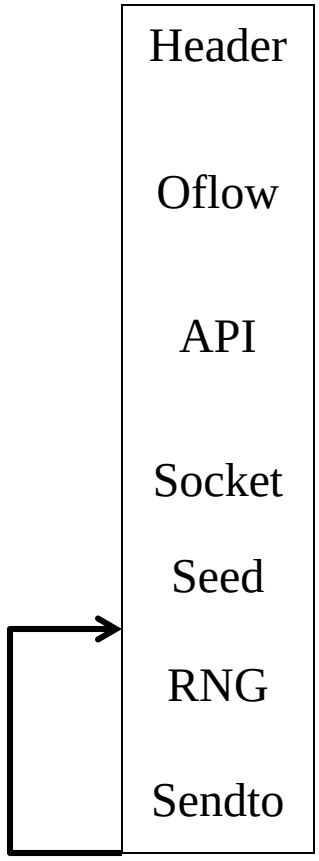
Inside the Sapphire/Slammer Worm

- Exploited bug in MSSQL 2000 and MSDE 2000
- Worm fit in a single UDP packet (404 bytes)

- Simple code structure
  - Cleanup from buffer overflow
  - Get API pointers

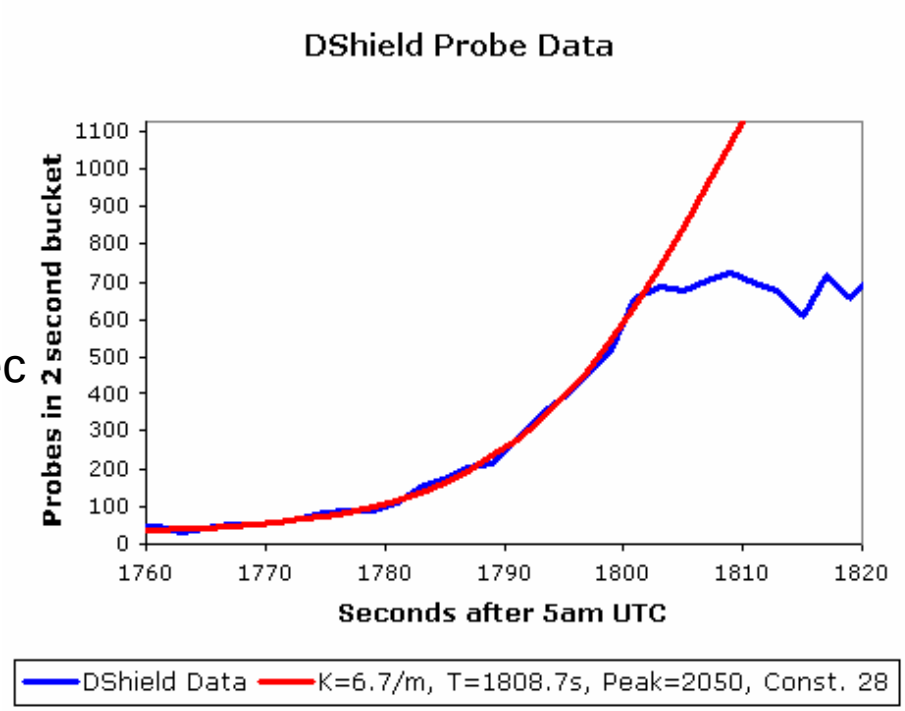
  } Code borrowed from published exploit

  - Create socket & packet
  - Seed RNG with `getTickCount()`
  - While (TRUE)
    - Increment RNG (mildly buggy)
    - Send packet to RNG address
- Key insight: non-blocking & stateless scanning (adaptable to TCP-based worms)

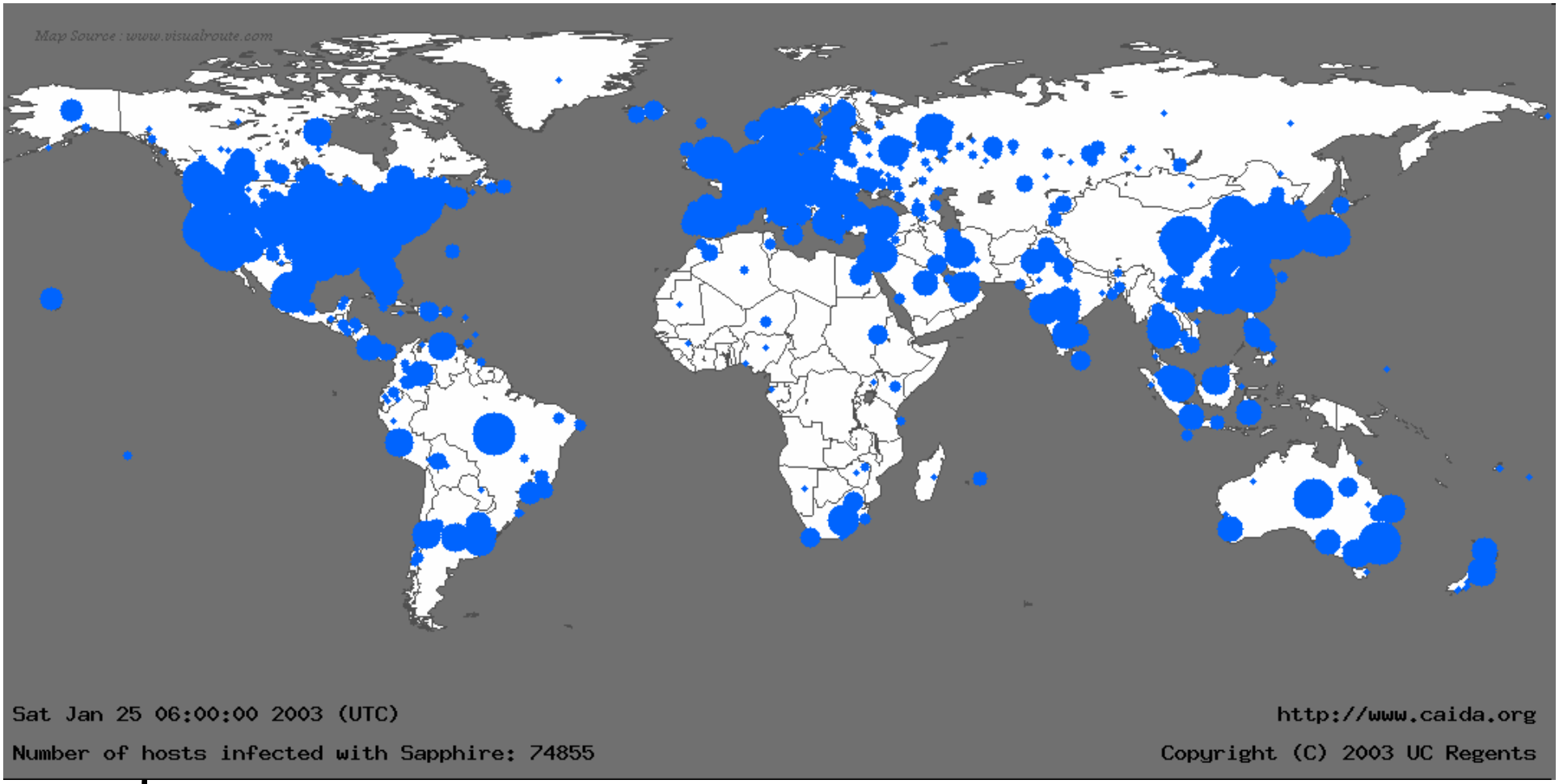


Sapphire growth

- First ~1min behaves like classic random scanning worm
  - Doubling time of ~8.5 seconds
  - Code Red doubled every 40mins
- >1min worm starts to saturate access bandwidth
  - Some hosts issue >20,000 scans/sec
  - Self-interfering
- Peaks at ~3min
  - 55million IP scans/sec
- 90% of Internet scanned in <10mins
  - Infected ~100k hosts (conservative due to PRNG errors)

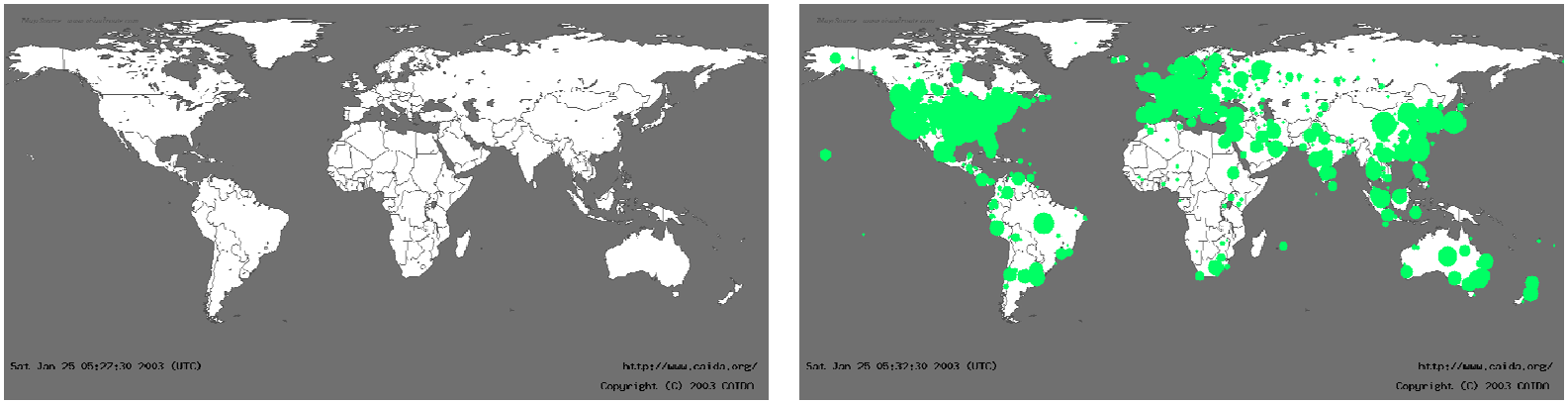


Sapphire Animation



Internet Worm Attacks: Sapphire

(aka SQL Slammer) – Jan 24, 2003



Before 9:30PM (PST) After 9:40PM (PST)

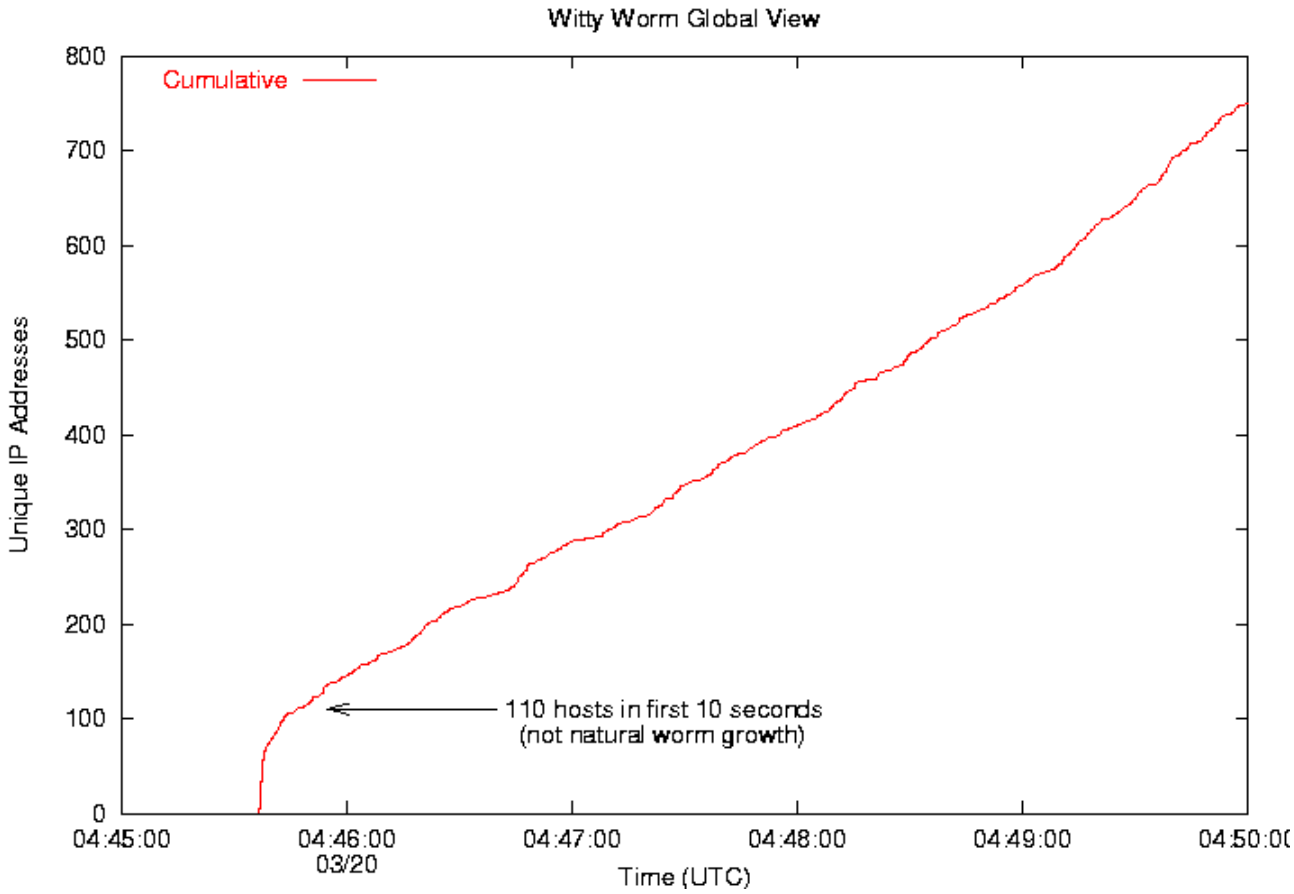
- ~100,000 hosts infected in *ten **minutes***
- Sent more than 55 million probes per second world wide
- Collateral damage: Bank of America ATMs, 911 disruptions, Continental Airlines cancelled flights
- Unstoppable; relatively benign to hosts

Spread of the Witty Worm

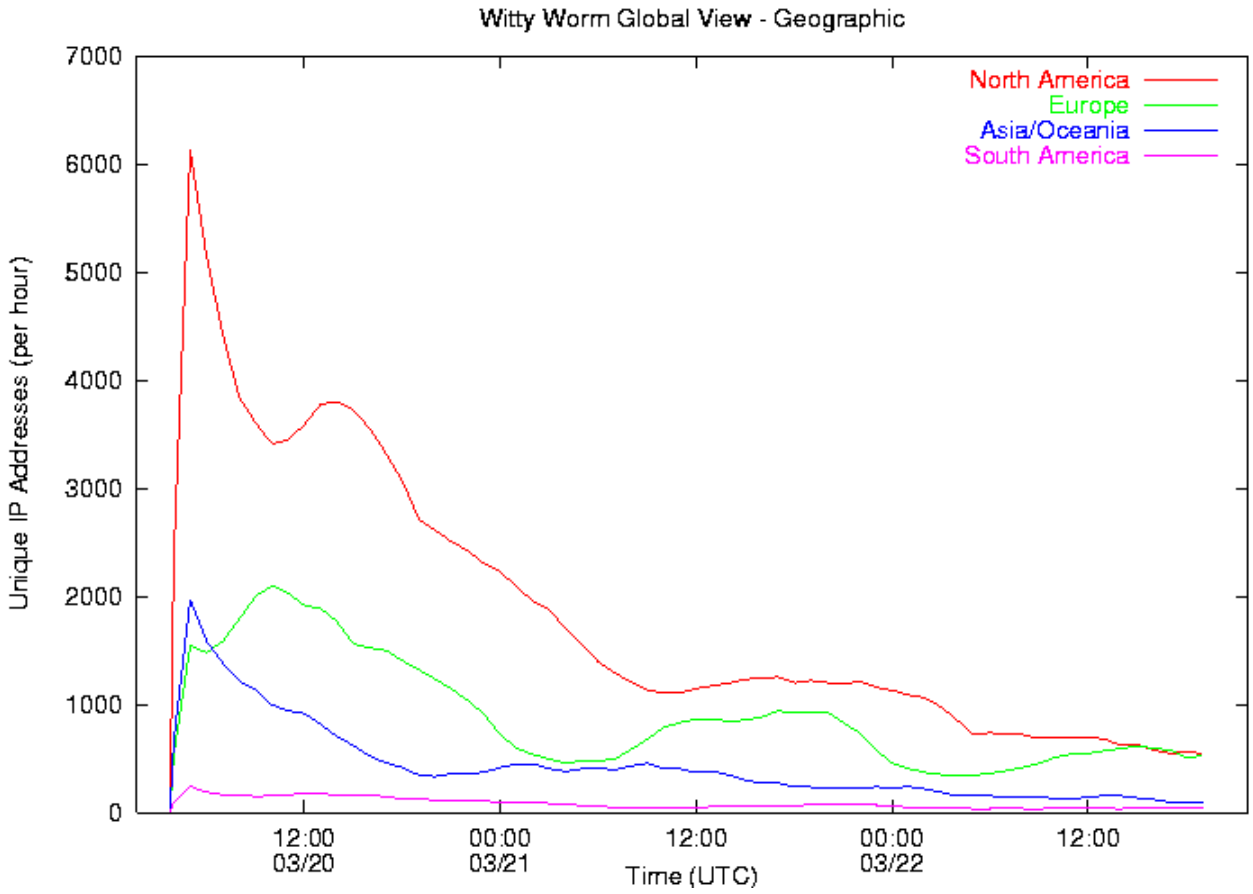
March 19, 2004

- First wide-spread Internet worm with destructive payload
  - writes 64k blocks to disk at random location, repeatedly
- Launched from a large set of ground-zero hosts
  - >100 hosts
- Shortest interval from vulnerability disclosure to worm release
  - 1 day
- Witty infected firewall/security software
  - i.e. proactive user base
- Spread quickly even with a small population
  - ~12,000 total hosts, 45 minutes to peak of infection

Early Growth of Witty



Geographic Spread of Witty



The Sky is Falling…

- **Worms are the worst Internet threat today**
  - Many *millions* of susceptible hosts
  - *Easy* to write worms
    - Worm payload separate from vulnerability exploit
    - Significant code reuse in practice
  - Possible to cause major damage
    - Wipe disk; flash bios; modify data; reveal data; Internet DoS
- **We have no operational defense**
  - Good evidence that humans don't react fast enough
  - Defensive technology is nascent at best

What can we do?

- **Measurement**
  - What are worms doing?
  - What types of hosts are infected?
  - Are new defense mechanisms working?
- **Develop operational defense**
  - Can we build an automated system to stop worms?

Open Research Questions for Measurement

- Denial-of-Service Attacks:
  - how much actual damage to victim
  - overall trends
- Internet Worms:
  - victim classification
  - early detection, automated filters
- Telescope Design:
  - distributed telescopes
  - making monitors which are robust under attack situations (millions of flows per second)

Acknowledgements

- Collaborators:
  - UCSD-CSE: Geoff Voelker, Stefan Savage, Jeffrey Brown
  - ICSI/LBNL: Vern Paxson
  - Silicon Defense: Stuart Staniford, Nicholas Weaver
  - UCB-EECS: Nicholas Weaver
- Data Providers:
  - UCSD: Brian Kantor, Pat Wilson
  - UCB/LBNL: Vern Paxson
  - UWISC: Dave Plonka
  - Dshield: Johannes Ullrich
  - Compaq/WRL: Jeff Mogul
  - DOD CERT: Donald LaDieu, Matthew Swaar
- Funding:
  - Cisco University Research Program (URP)
  - DARPA
  - NSF
  - CAIDA Members

Related Papers

- Inferring Internet Denial-of-Service Activity [MSV01]
  - David Moore, Stefan Savage, Geoff Voelker
  - http://www.caida.org/outreach/papers/2001/BackScatter/
- Code-Red: A Case Study on the spread and victims of an Internet Worm [MSB02]
  - David Moore, Colleen Shannon, Jeffrey Brown
  - http://www.caida.org/outreach/papers/2002/codered/
- Internet Quarantine: Requirements for Containing Self-Propagating Code [MSVS03]
  - David Moore, Colleen Shannon, Geoff Voelker, Stefan Savage
  - http://www.caida.org/outreach/papers/2003/quarantine/
- The Spread of the Sapphire/Slammer Worm [MPS03]
  - David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver
  - http://www.caida.org/outreach/papers/2003/sapphire/

Additional Information

- Code-Red v1, Code-Red v2, CodeRedII, Nimda
  - http://www.caida.org/analysis/security/code-red/
- Code-Red v2 In-depth analysis
  - http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml
- Spread of the Sapphire/SQL Slammer Worm
  - http://www.caida.org/analysis/security/sapphire/
- Network telescopes
  - http://www.caida.org/analysis/security/telescope/