The Threats of Internet Worms

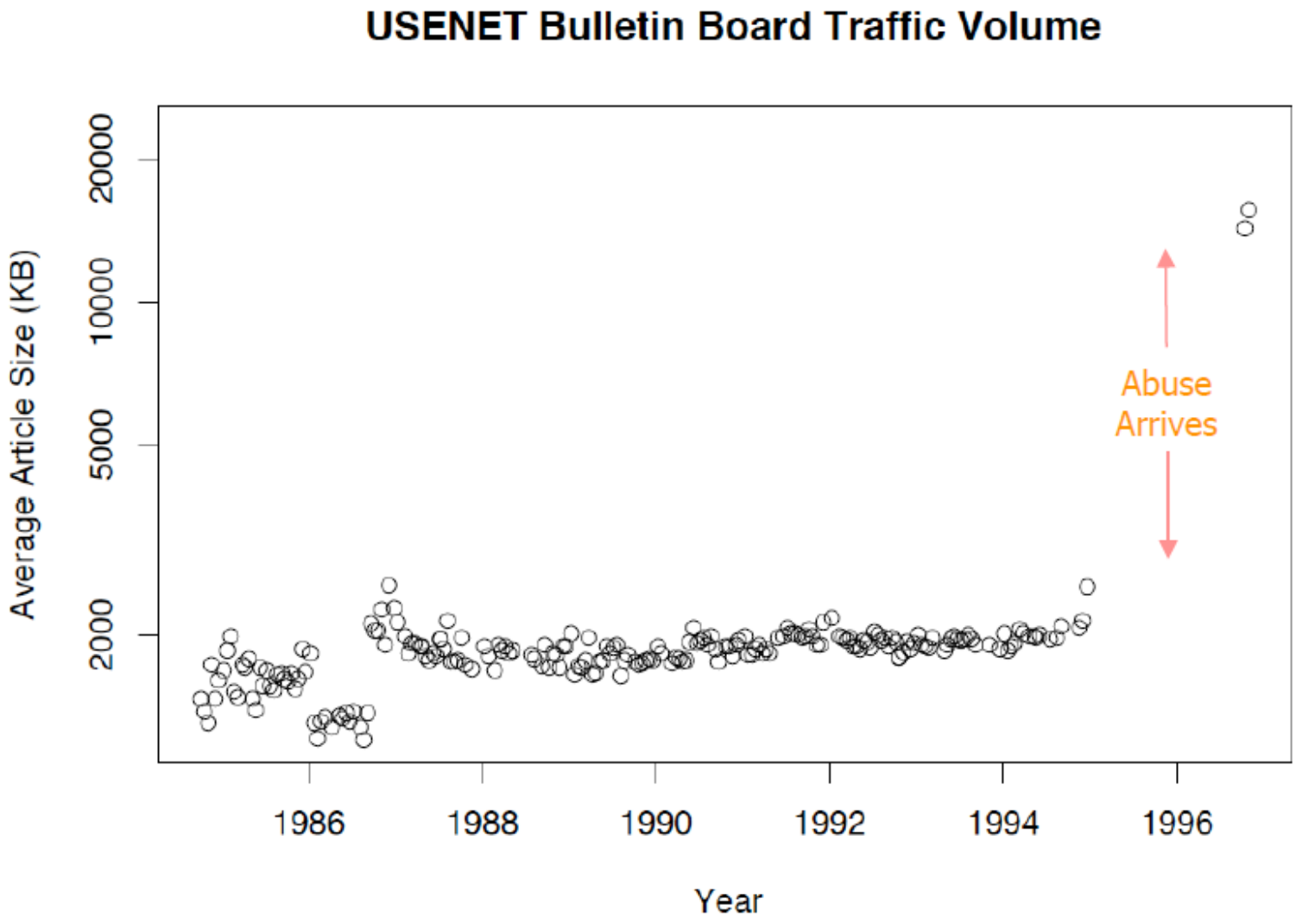
Based on

Addressing the Threat of Internet Worms

Vern Paxson UCB/ICSI

UCLA Jon Postel Distinguished Lecturer Series, 2005

Internet Abuse



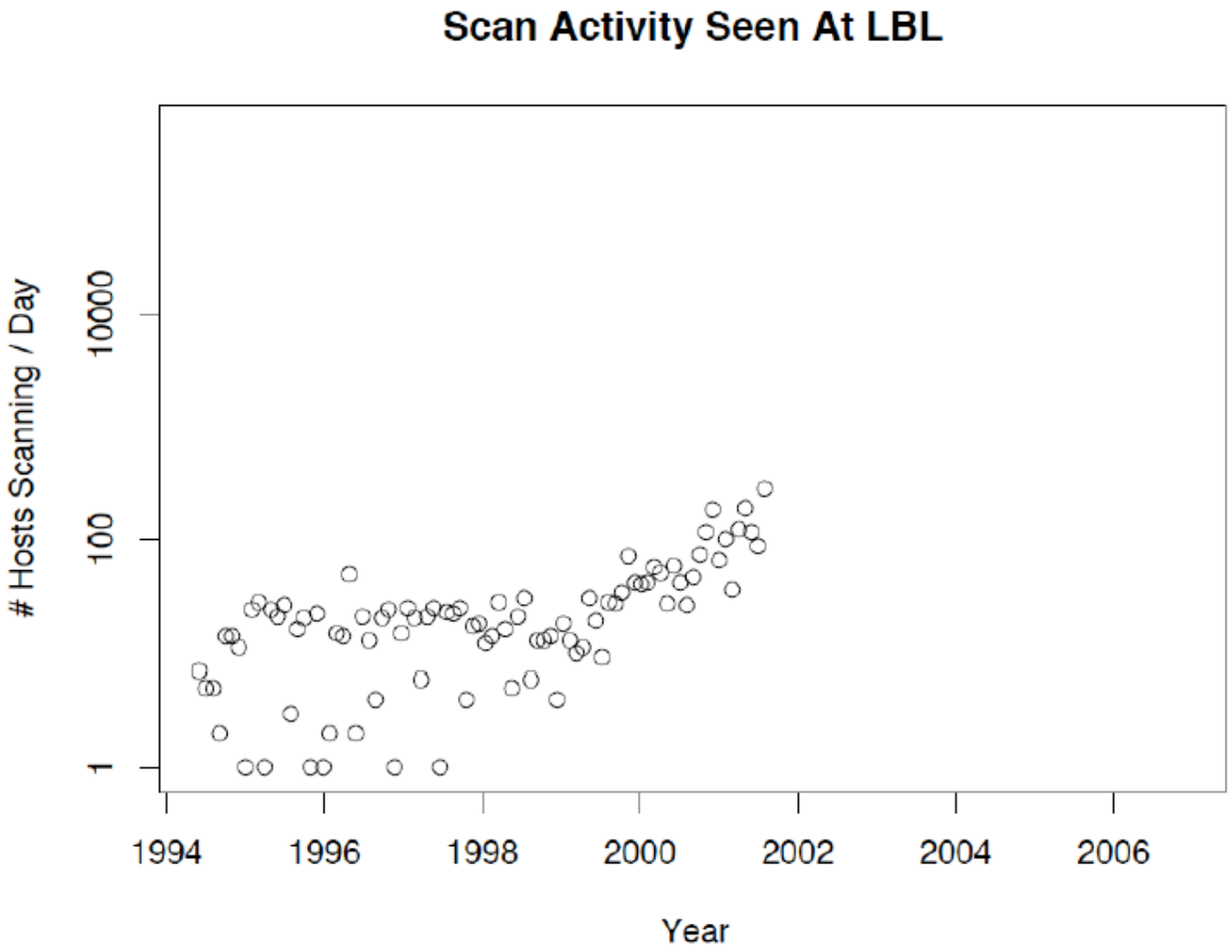
What is a Worm?

- A worm is self-replicating software designed to spread through the network
  - Typically exploits security flaws in widely used services
  - Spreads across a network by exploiting flaws in open services.
  - Can cause enormous damage
    - Launch DDOS attacks, install Botnets
    - Access sensitive information
    - Cause confusion by corrupting the sensitive information
- Worm vs. Virus vs. Trojan horse
  - A virus is code embedded in a file or program
  - Viruses and Trojan horses rely on human intervention
  - Worms are self-contained

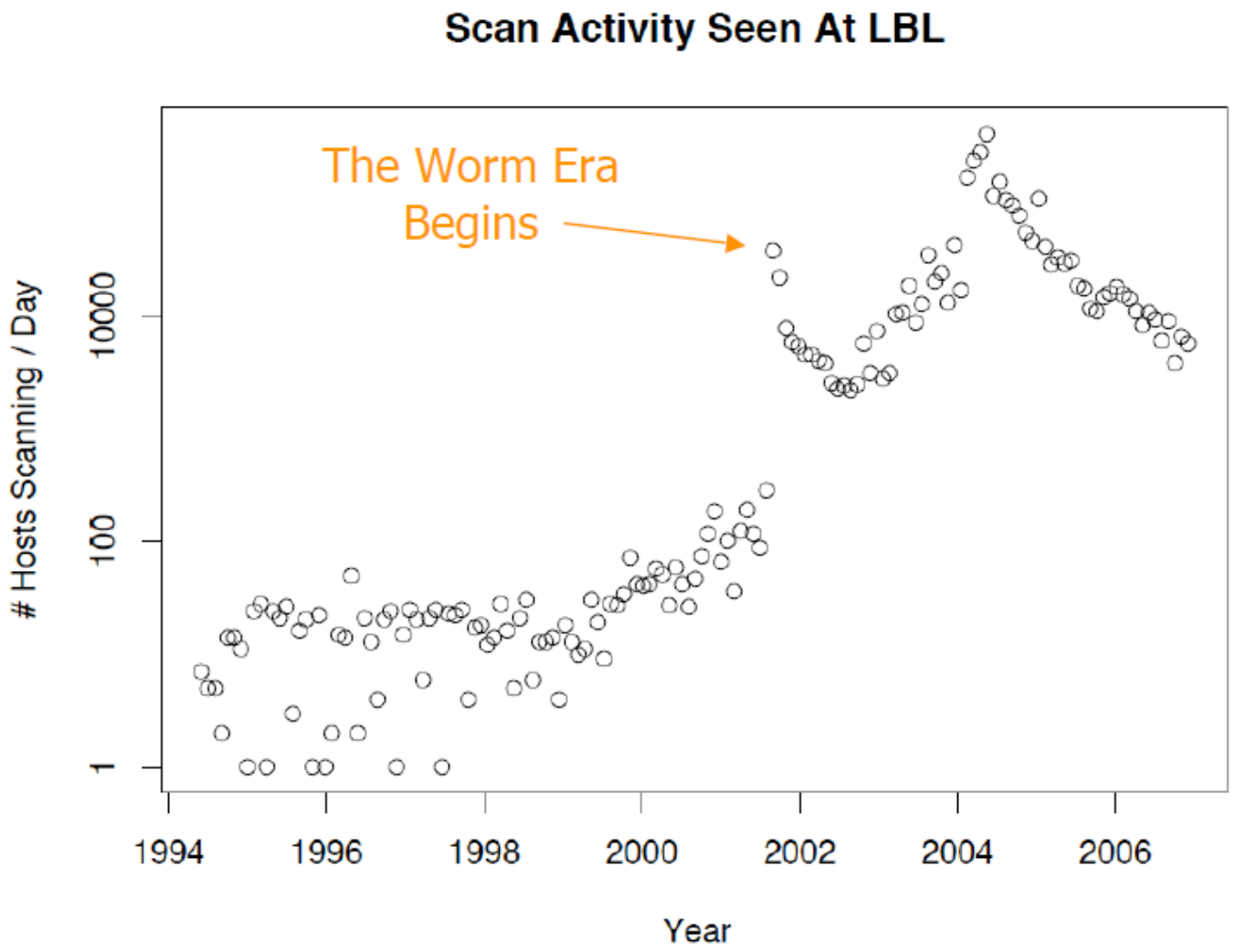
What is a Worm? (2.)

- Not new — Morris Worm, Nov. 1988
  - 6-10% of all Internet hosts infected
  - Infects DEC VAX and Sun machines running BSD UNIX connected to the Internet, and becomes the first worm to spread extensively "in the wild", and one of the first well-known programs exploiting buffer overrun vulnerabilities
- Many more since, but for 13 years none on that scale, until …

Impact of worms on scanning



Impact of worms on scanning



Code Red

- Initial version released July 13, 2001.
- Exploited known bug in Microsoft IIS Web servers.
  - GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090% u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090% u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078% u0000%u00=a HTTP/1.0
- Payload: Web site defacement
  - HELLO! Welcome to http://www.worm.com!
  - Hacked by Chinese!
  - Only done if language setting = English

Code Red of July 13, con't

- 1st through 20th of each month: spread.
- 20th through end of each month: attack.
  - Flooding attack against 198.137.240.91 …
  - … i.e., www.whitehouse.gov
- Spread: via random scanning of 32-bit IP address space.

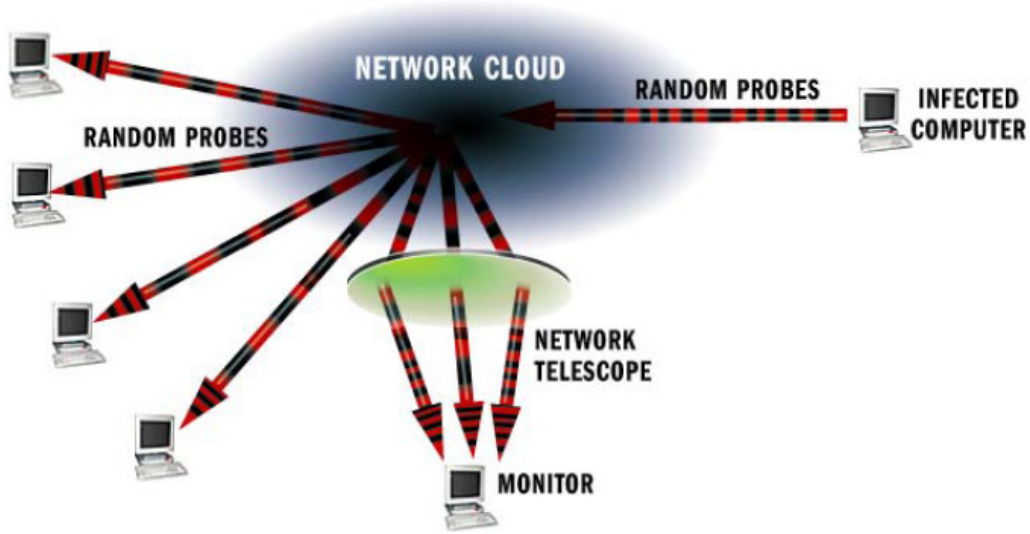
- But: Failure to seed random number generator
  $\Rightarrow$ linear growth.

Code Red, con't

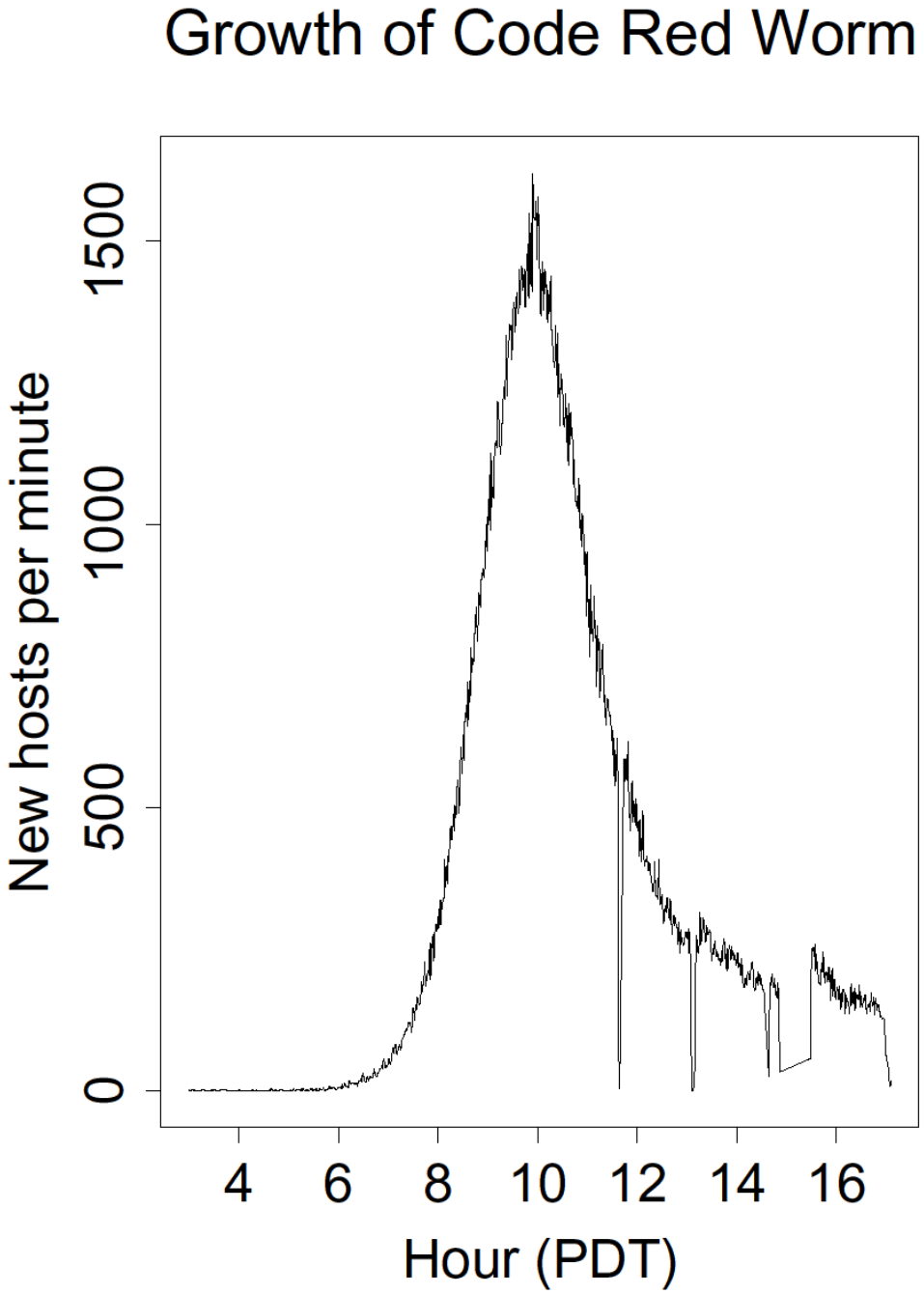
- Revision released July 19, 2001.
- White House responds to threat of flooding attack by changing the address of www.whitehouse.gov
- Causes Code Red to die for date ≥ 20th of the month.

- But: This time random number generator correctly seeded. Bingo!

Measuring activity: Network telescope



- Monitor cross-section of Internet address space, measure traffic
  - "Backscatter" from DOS floods
  - Attackers probing blindly
  - Random scanning from worms
- LBNL's cross-section: 1/32,768 of Internet
- UCSD, UWisc's cross-section: 1/256.


Growth of Code Red Worm
New hosts per minute
0
500
1000
1500
4
6
8
10
12
14
16
Hour (PDT)

Measuring Internet-Scale Activity: Network Telescopes

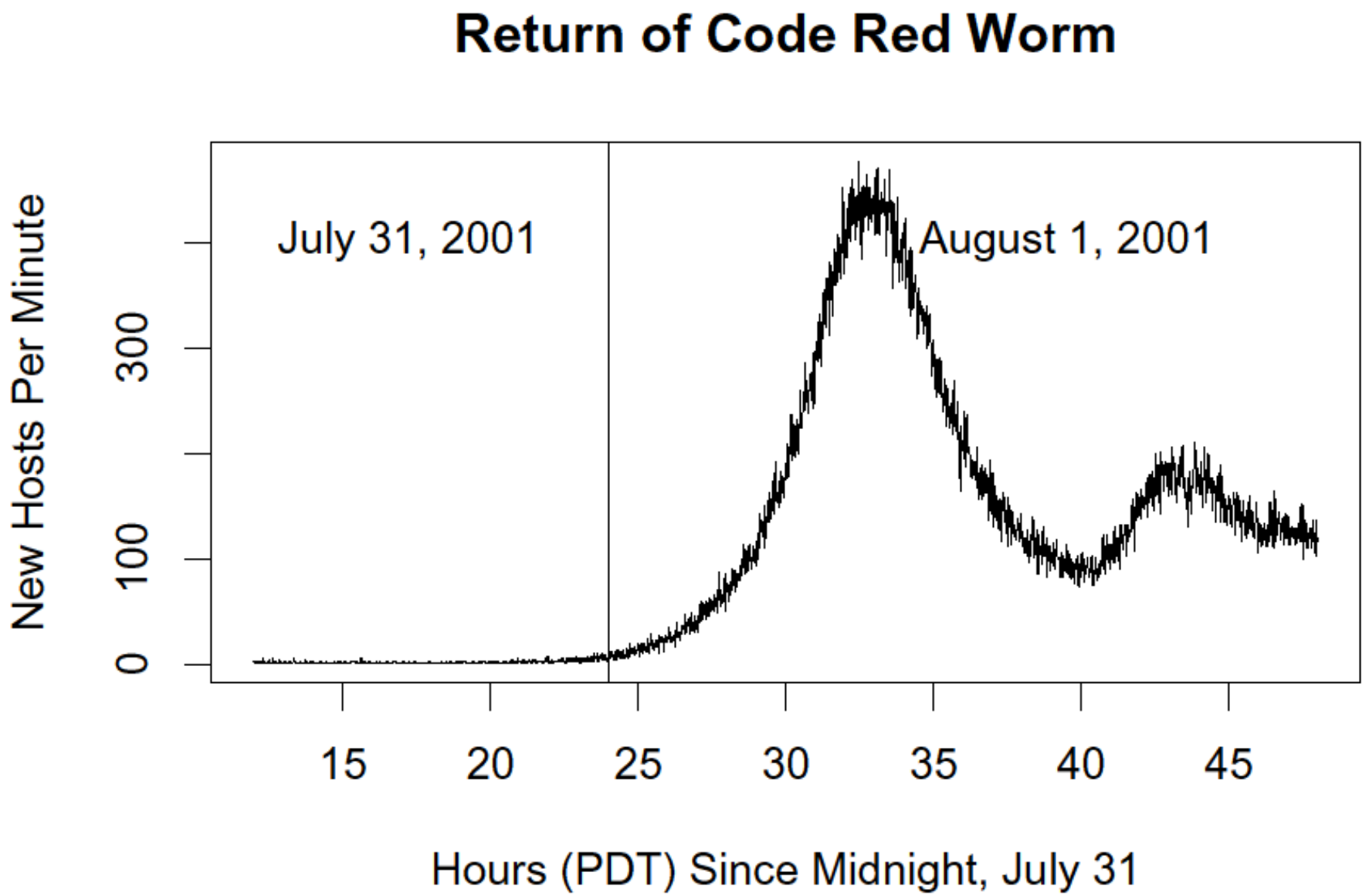
- Idea: Monitor a cross-section of Internet address space to measure network traffic involving wide range of addresses
  - "Backscatter" from DOS floods
  - Attackers probing blindly
  - Random scanning from worms

Spread of Code Red

- Network telescopes estimate of # infected hosts: 360K.
- Note: The larger the vulnerable population, the faster the worm spreads.

- That night ($\Rightarrow$ 20th), worm dies …

  … except for hosts with inaccurate clocks!
- It just takes one of these to restart the worm on August 1st …


Return of Code Red Worm
July 31, 2001
August 1, 2001
New Hosts Per Minute
0
100
300
15
20
25
30
35
40
45
Hours (PDT) Since Midnight, July 31

Striving for Greater Virulence: Code Red 2

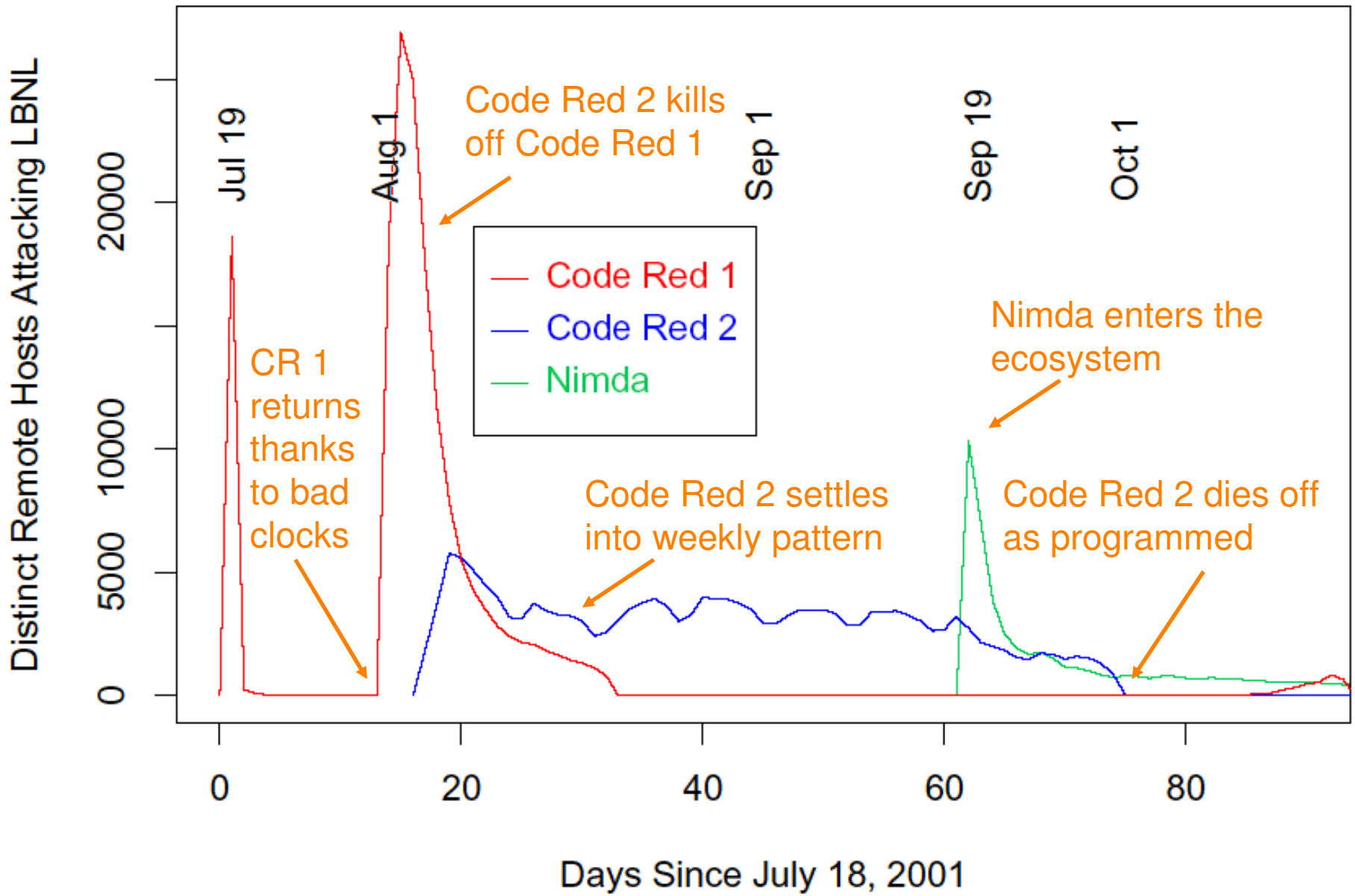
- Released August 4, 2001.
- Comment in code: "Code Red 2."
  - But in fact completely different code base.
- Payload: A root backdoor, resilient to reboots.
- Bug: Crashes NT, only works on Windows 2000.

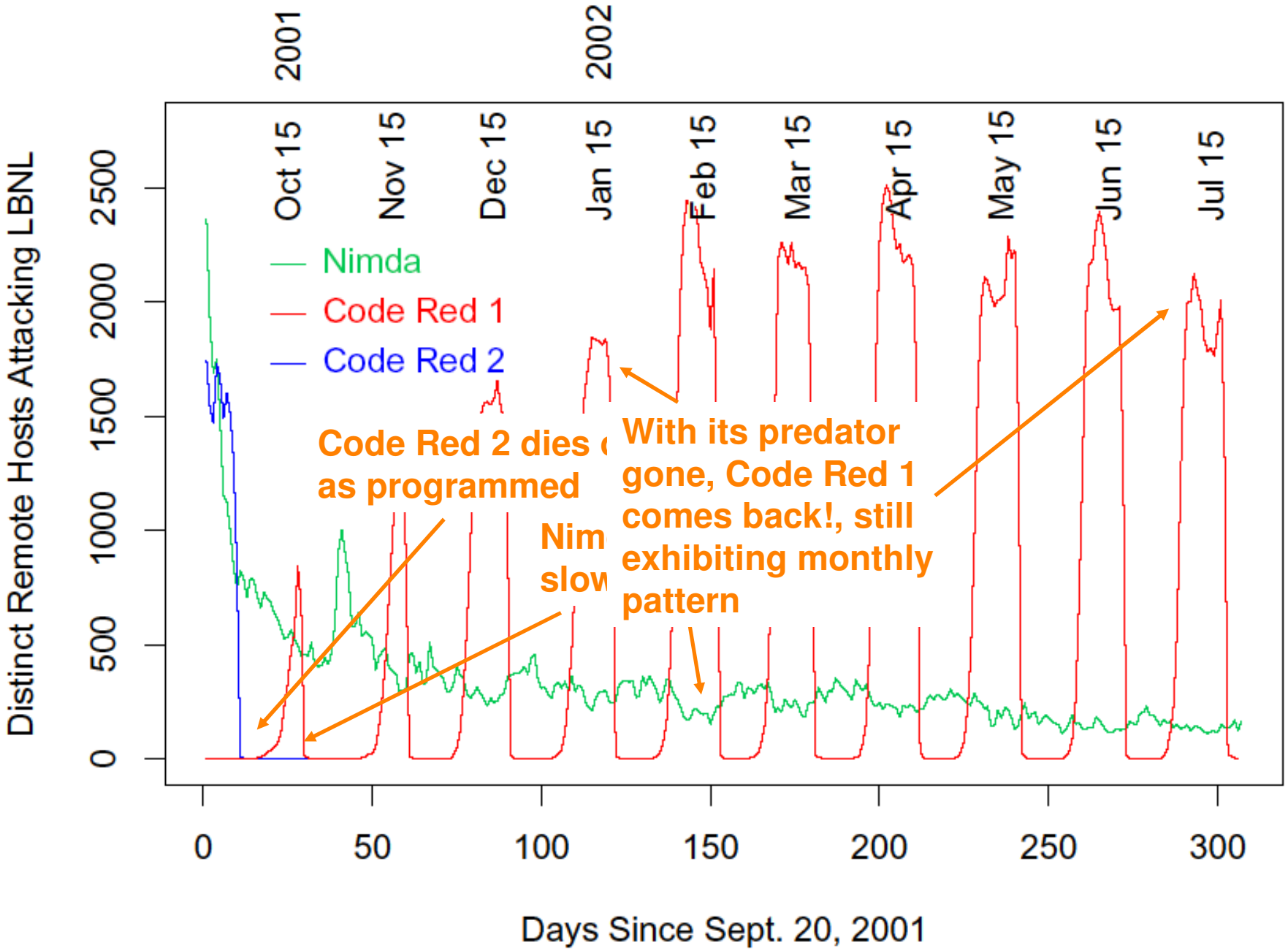
- Kills Code Red 1.

- Safety valve: Programmed to die Oct 1, 2001.

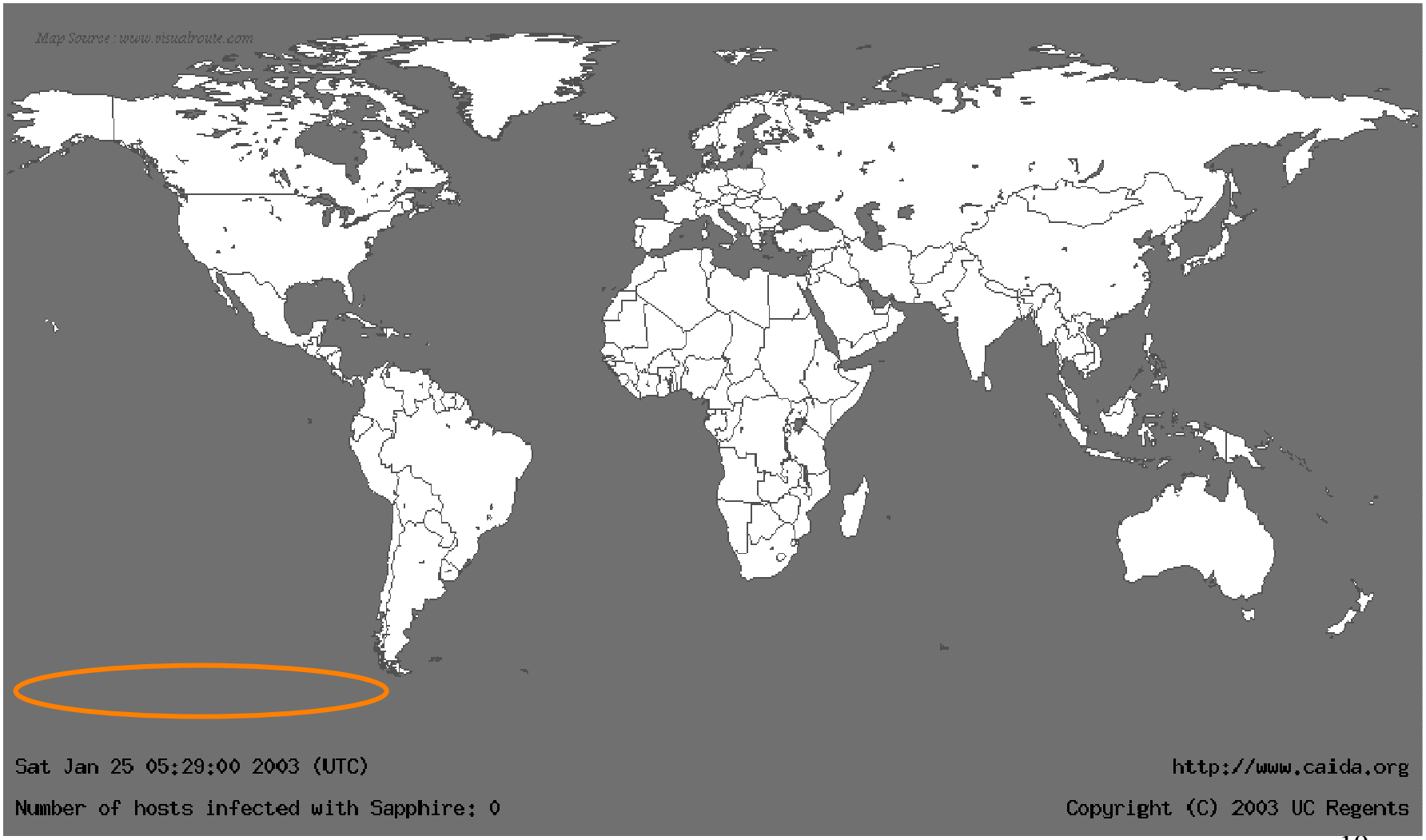
Striving for Greater Virulence: Nimda

- Released September 18, 2001.
- Multi-mode spreading:
  - Attack IIS servers via infected clients
  - Email itself to address book as a virus
  - Copy itself across open network shares
  - Modifying Web pages on infected servers w/ client exploit
  - Scanning for Code Red II backdoors (!)
- Worms form an ecosystem!
- Leaped across firewalls.

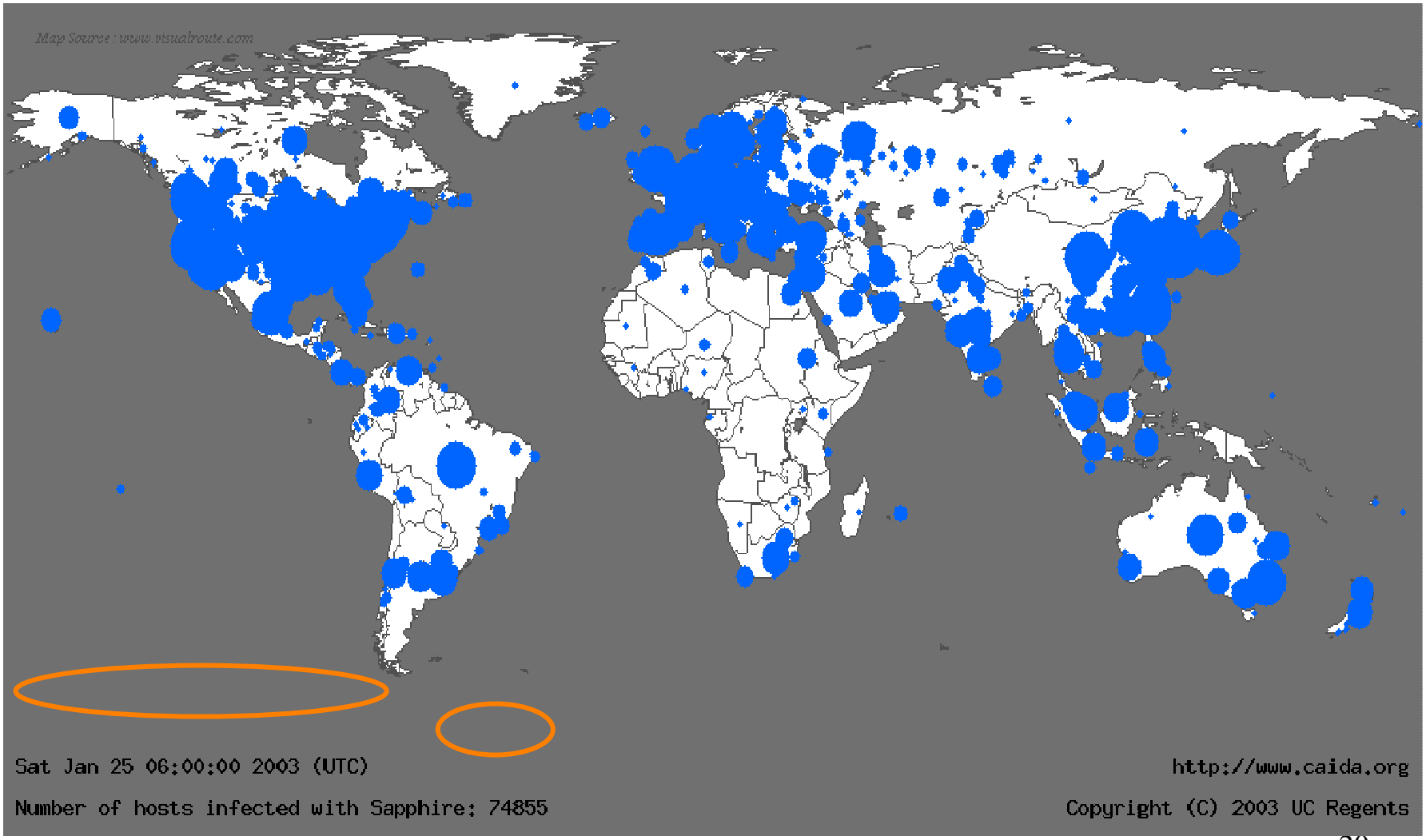

Distinct Remote Hosts Attacking LBNL
0
5000
10000
20000
Jul 19
Aug 1
Sep 1
Sep 19
Oct 1
Code Red 2 kills
off Code Red 1
Code Red 1
Code Red 2
Nimda
CR 1
returns
thanks
to bad
clocks
Nimda enters the
ecosystem
Code Red 2 settles
into weekly pattern
Code Red 2 dies off
as programmed
0
20
40
60
80
Days Since July 18, 2001


2001
2002
Oct 15
Nov 15
Dec 15
Jan 15
Feb 15
Mar 15
Apr 15
May 15
Jun 15
Jul 15
Nimda
Code Red 1
Code Red 2
Code Red 2 dies
as programmed
With its predator
gone, Code Red 1
comes back!, still
exhibiting monthly
pattern
Distinct Remote Hosts Attacking LBNL
0
500
1000
1500
2000
2500
0
50
100
150
200
250
300
Days Since Sept. 20, 2001

Life Just Before Slammer



Life Just After Slammer

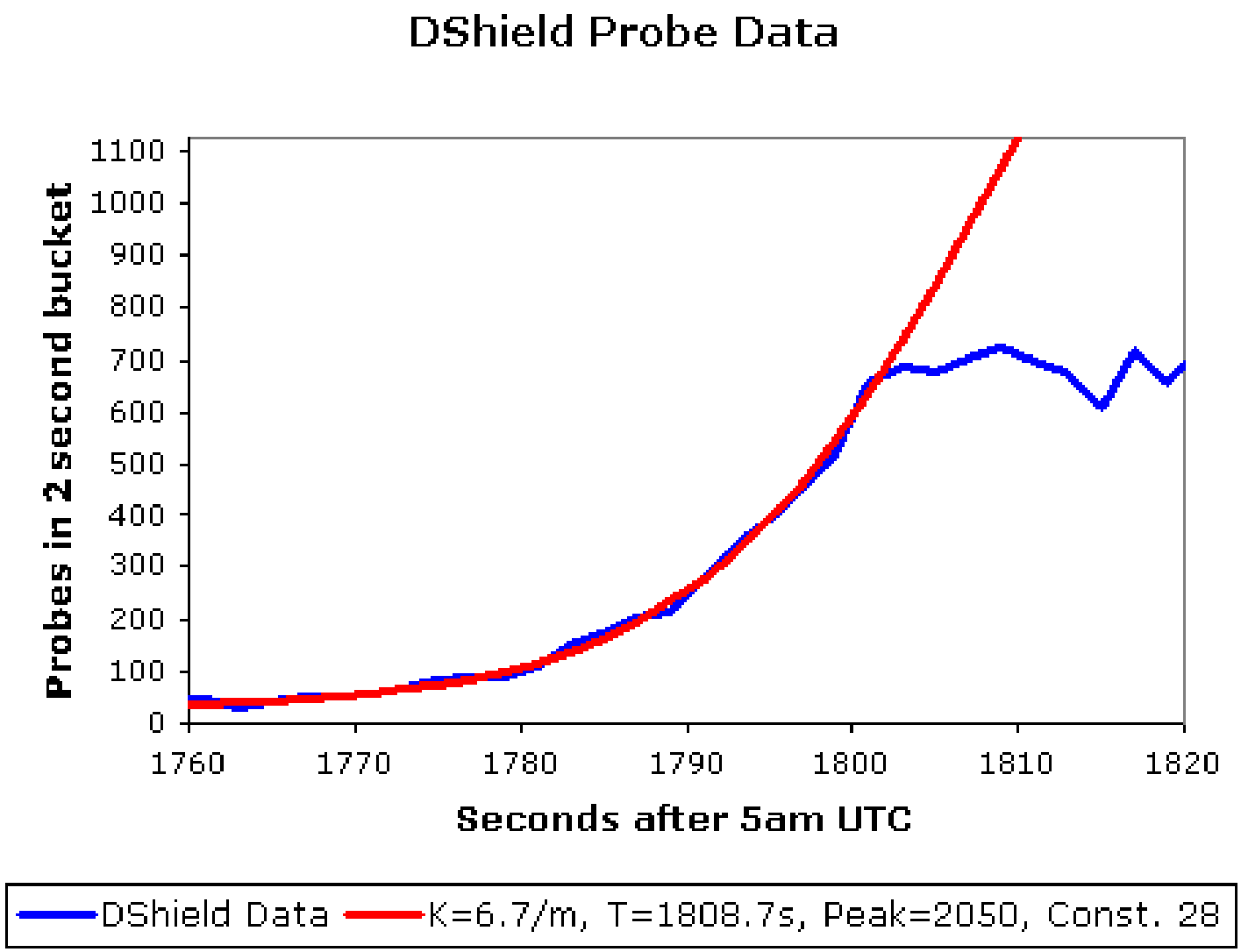


A Lesson in Economy

- Slammer exploited a connectionless UDP service, rather than connection-oriented TCP.
- Entire worm fit in a single packet!
- When scanning, worm could "fire and forget".

- Worm infected 75,000+ hosts in 10 minutes (despite broken random number generator).
  - At its peak, doubled every 8.5 seconds
- Progress limited by the Internet's bandwidth capacity!

Slammer's *Bandwidth-Limited* Growth



Blaster

- Released August 11, 2003.
- Exploits flaw in RPC service ubiquitous across Windows.
- Payload: Attack Microsoft Windows Update.
- Despite flawed scanning and secondary infection strategy, rapidly propagates to (at least) 100K's of hosts.
- Actually, bulk of infections are really Nachia, a Blaster counter-worm.
- Key paradigm shift: Firewalls don't help.

Cost of worms

- Morris worm, 1988
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - Cost ~ $10 million in downtime and cleanup
- Code Red worm, July 16 2001
  - Direct descendant of Morris' worm
  - Infected more than 500,000 servers
    - Programmed to go into infinite sleep mode July 28
  - Caused ~ $2.6 Billion in damages,
- Love Bug worm: $8.75 billion

Statistics: Computer Economics Inc., Carlsbad, California

Cost of worms (2.)

Financial Impact of Virus Attacks 1995—2005

	Worldwide Impact (US $)
2005	$14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion
1996	1.8 Billion
1995	500 Million

Source: Computer Economics, 2006

Figure 1

What if Spreading were Well-Designed?

- Observation:

  Much of a worm's scanning is redundant.
- Ideas:
  - Accelerate later phase: Coordinated scanning
  - Accelerate initial phase: Use precomputed hit-list
- Greatly accelerates worm.

How do worms propagate?

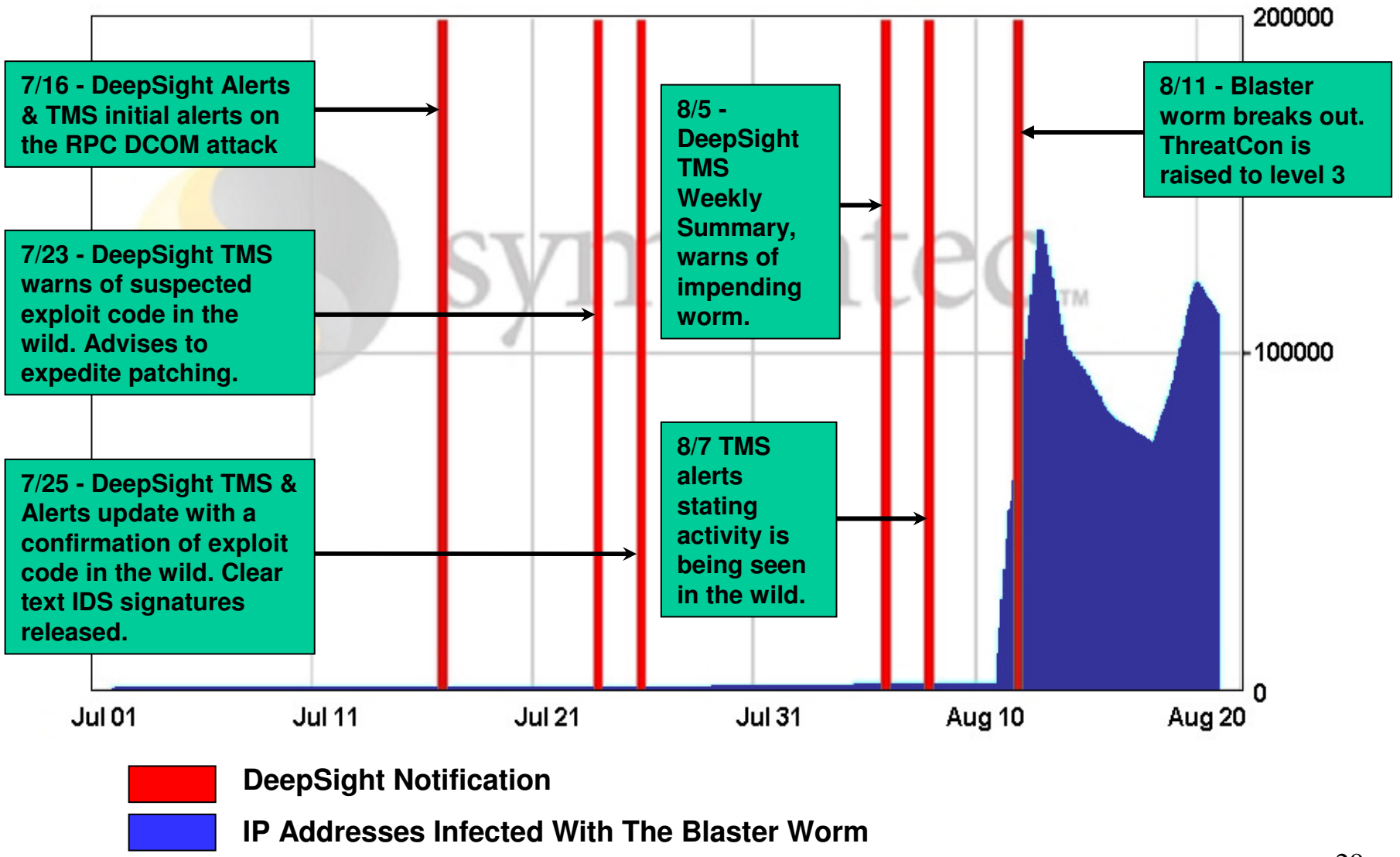
- Scanning worms
  - Worm chooses "random" address
- Coordinated scanning
  - Different worm instances scan different addresses
- Flash worms
  - Preassemble tree of vulnerable hosts, propagate along tree
    - Not observed in the wild, yet
    - Potential for 106 hosts in < 2 sec ! [Staniford]
- Meta-server worm
  - Contact server for hosts list (e.g., Google for "powered by phpbb")
- Topological worm
  - Use information from infected hosts (web server logs, email address books, config files, SSH "known hosts")
- Contagion worm
  - Propagate parasitically along with normal communication

Defenses

- Detect via honeyfarms: Collections of "honeypots" fed by a network telescope.
  - Any outbound connection from honeyfarm = worm.
  - Distill signature from inbound/outbound traffic.

- Thwart via scan suppressors: Network elements that block traffic from hosts that make failed connection attempts to too many other hosts.
  - 5 minutes to several weeks to write a signature
  - Several hours or more for testing

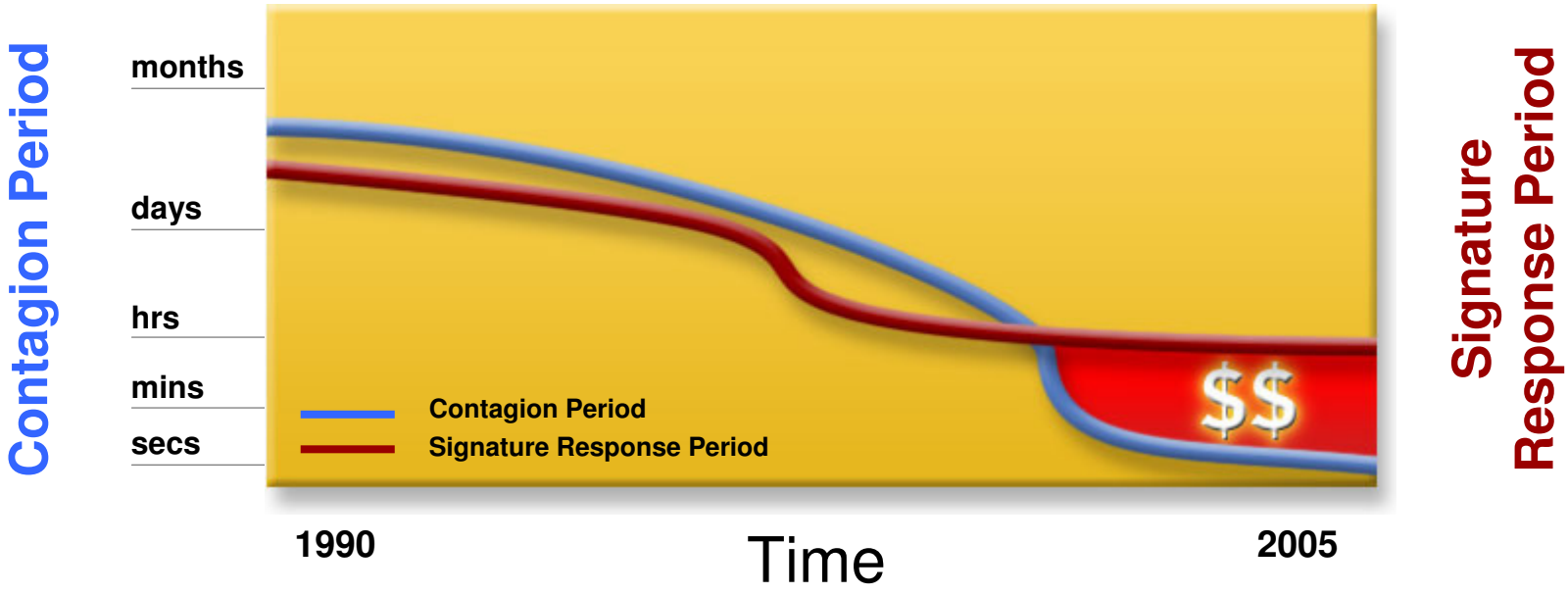
Early Warning: Blaster Worm



Slide: Carey Nachenberg, Symantec

Need for automation

- Current threats can spread faster than defenses can reaction
- Manual capture/analyze/signature/rollout model too slow



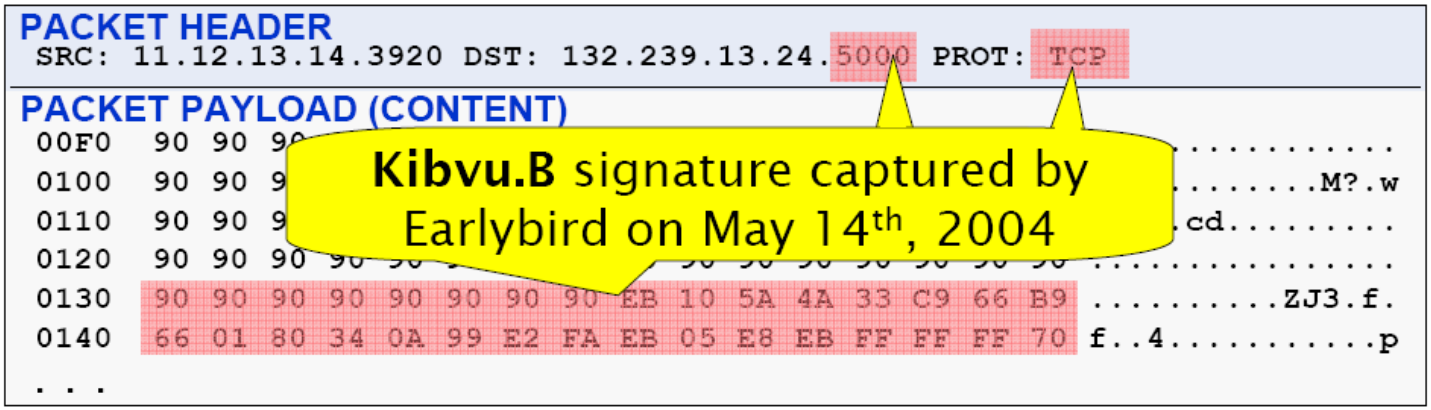
Slide: Carey Nachenberg, Symantec

Signature inference

- Challenge
  - Need to automatically learn a content "signature" for each new worm – potentially in less than a second!
- Some proposed solutions
  - Singh et al, Automated Worm Fingerprinting, OSDI '04
  - Kim et al, Autograph: Toward Automated, Distributed Worm Signature Detection, USENIX Sec '04

Signature inference

- Monitor network and look for strings common to traffic with worm-like behavior
  - Signatures can then be used for content filtering



Slide: S Savage

Defenses?

- Observation:

  Worms don't need to randomly scan

- Meta-server worm: Ask server for hosts to infect (e.g., Google for "powered by phpbb")
- Topological worm: Fuel the spread with local information from infected hosts (web server logs, email address books, config files, SSH "known hosts")
- No scanning signature; With rich inter-connection topology, potentially very fast.

Defenses??

- Contagion worm: Propagate parasitically along with normally initiated communication.

- E.g., using 2 exploits – Web browser & Web server – infect any vulnerable servers visited by browser, then any vulnerable browsers that come to those servers.
- E.g., using 1 BitTorrent exploit, glide along immense peer-to-peer network in days/hours.
- No unusual connection activity at all! :-(

Some Cheery Thoughts

(Stefan Savage, UCSD/CCIED)

- Imagine the following species:
  - Poor genetic diversity; heavily inbred
  - Lives in "hot zone"; thriving ecosystem of infectious pathogens
  - Instantaneous transmission of disease
  - Immune response 10–1M times slower
  - Poor hygiene practices
- What would its long-term prognosis be?
- What if diseases were designed …
  - Trivial to create a new disease
  - Highly profitable to do so

Broader View of Defenses

- Prevention – make the monoculture hardier
  - Get the darn code right in the first place …
    - … or figure out what's wrong with it and fix it
  - Lots of active research (static & dynamic methods)
  - Security reviews now taken seriously by industry
    - E.g., ~$200M just to review Windows Server 2003
  - But very expensive
  - And very large Installed Base problem

- Prevention – diversify the monoculture
  - Via exploiting existing heterogeneity
  - Via creating artificial heterogeneity

Broader View of Defenses, con't

- Prevention – keep vulnerabilities inaccessible
  - Cisco's Network Admission Control
    - Frisk hosts that try to connect, block if vulnerable
  - Microsoft's Shield ("Band-Aid")
    - Shim-layer blocks network traffic that fits known vulnerability (rather than known exploit)
- Detection – look for unusual repeated content
  - Can work on non-scanning worms
  - Key off many-to-many communication to avoid confusion w/ non-worm sources
  - EarlyBird, Autograph – distill signature
  - But: What about polymorphic worms?

Once You Have A Live Worm, Then What?

- Containment
  - Use distilled signature to prevent further spread
- Would like to leverage detections by others
  - But how can you trust these?
  - What if it's an attacker lying to you to provoke a self-damaging response? (Or to hide a later actual attack)

Once You Have A Live Worm, Then What?, con't

- Proof of infection
  - Idea: Alerts come with a verifiable audit trail that demonstrates the exploit, ala' proof-carrying code
- Auto-patching
  - Techniques to derive (and test!) patches to fix vulnerabilities in real-time
    - (Excerpt from a review: "Not as crazy as it sounds")
- Auto-antiworm
  - Techniques to automatically derive a new worm from a propagating one, but with disinfectant payload
    - (This one, on the other hand, is as crazy as it sounds)

Incidental Damage … Today

- Today's worms have significant real-world impact:
  - Code Red disrupted routing
  - Slammer disrupted elections, ATMs, airline schedules, operations at an off-line nuclear power plant …
  - Blaster possibly contributed to Great Blackout of Aug. 2003 … ?
  - Plus major clean-up costs
- But today's worms are amateurish
  - Unimaginative payloads

Where are the Nastier Worms??

- Botched propagation the norm
- Doesn't anyone read the literature?

  e.g., permutation scanning, flash worms, metaserver worms, topological, contagion
- Botched payloads the norm

  e.g., Flooding-attack fizzles
- Current worm authors are in it for kicks …

  (… or testing) No arms race yet.

Next-Generation Worm Authors

- Military.
- Crooks:
  - Denial-of-service, spamming for hire
  - "Access worms"
  - Very worrisome onset of blended threats
    - Worms + viruses + spamming + phishing + DOS-for-hire + botnets + spyware
- Money on the table $\Rightarrow$ Arms race
  - (market price for spam proxies: 3-10¢/host/week)

"Better" Payloads

- Wiping a disk costs $550/$2550*
- "A well-designed version of Blaster could have infected 10M machines." (8M+ for sure!)
- The same service exploited by Blaster has other vulnerabilities …
- Potentially a lot more $$$: flashing BIOS, corrupting databases, spreadsheets …
- Lower-bound estimate: $50B if well-designed

Attacks on Passive Monitoring

- Exploits for bugs in read-only analyzers!
- Suppose protocol analyzer has an error parsing unusual type of packet
  - E.g., tcpdump and malformed options
- Adversary crafts such a packet, overruns buffer, causes analyzer to execute arbitrary code

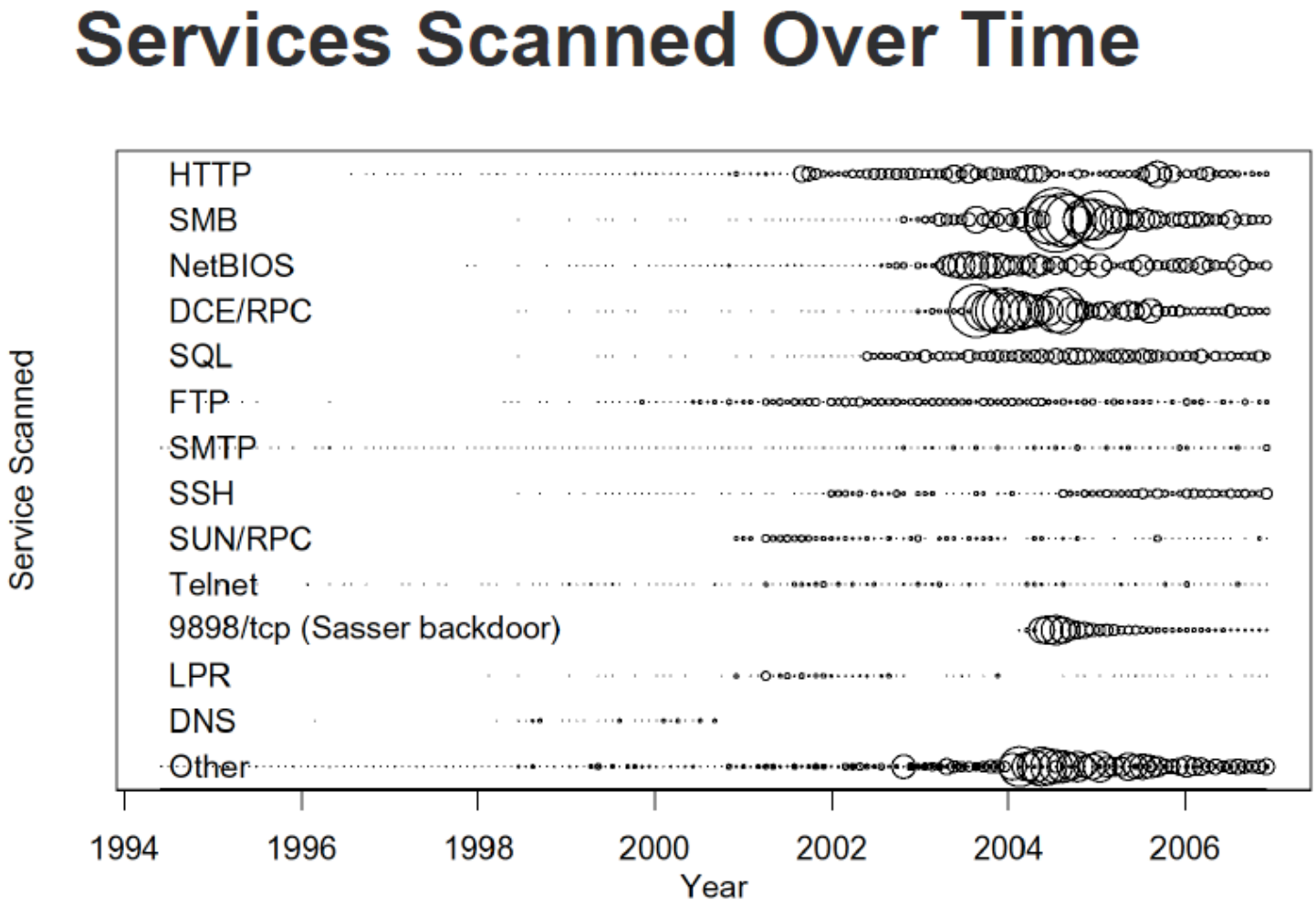
Witty

- Released March 19, 2004.
- Single UDP packet exploits flaw in the passive analysis of Internet Security Systems products.
- "Bandwidth-limited" UDP worm à la Slammer.
- Distribution:
  - Used a pre-populated list of ground-zero hosts.
  - Vulnerable pop. (12K) attained in 75 minutes.
- Payload:
  - First Internet worm to carry a destructive payload
  - Slowly corrupt random disk blocks.

Witty, con't

- Flaw had been announced the previous day.
- Telescope analysis reveals:
  - Initial spread seeded via a hit-list.
  - In fact, targeted a U.S. military base.
  - Analysis also reveals "Patient Zero", a European retail ISP.
- Written by a Pro.

What kind of services are targeted



More information

- Timeline of virus and worms
  - http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms
- Early worms:
  - Eugene H. Spafford, The Internet Worm: Crisis and Aftermath, CACM 32(6) 678-687, June 1989
  - Page, Bob, "A Report on the Internet Worm", http://www.ee.ryerson.ca:8080/~elf/hack/iworm.html
- Summaries:
  - http://www.icir.org/vern/talks.html