What will be the Coming Super Worms and Viruses

By

Alan S H Lam

Outlines

- Review
- Prediction
- Threat
- Worst case scenario
- What can we do

The Coming Super Worms and Viruses

What will be the coming super computer worms and viruses?

What can we do?

Review

Worms and Viruses

- Malicious code
- Exploit weaknesses
- Replicate themselves and/or attach themselves to other programs
- Spread from system to system

Review (2)

Worms

- Spread with no human intervention once started

Viruses

- Require action from user before spreading

Review (3)

- Some have both worm and viruse properties, e.g. Nimda
- Some may even work with spammers hand in hand, e.g. SoBig

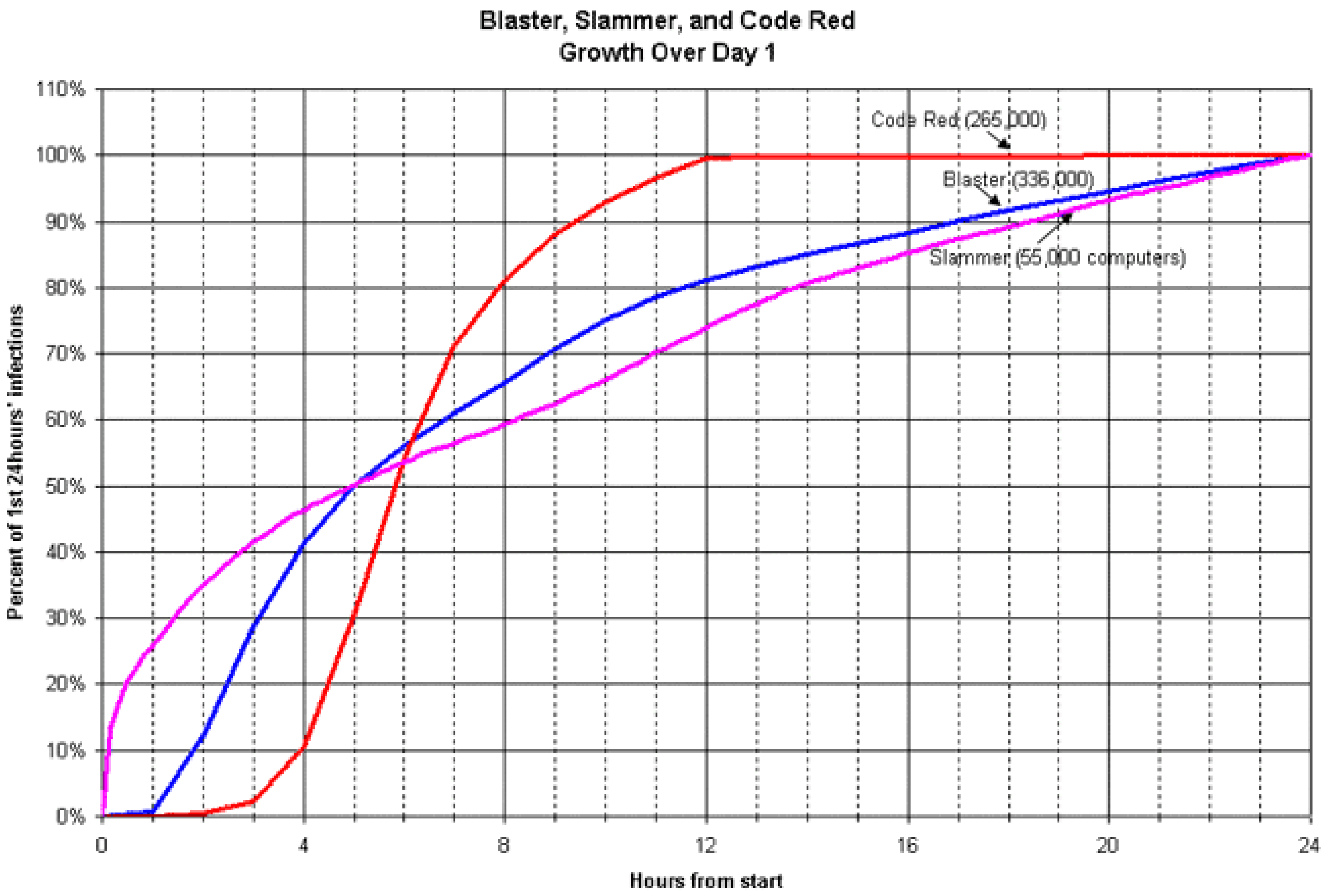
Review (4)

Spread faster and faster

Outbreak date	Name	Hosts infected in the first 24 hours
Aug 2001	Code Red	265,000
Jan 2003	Slammer	55,000
Aug 2003	Blaster	336,000

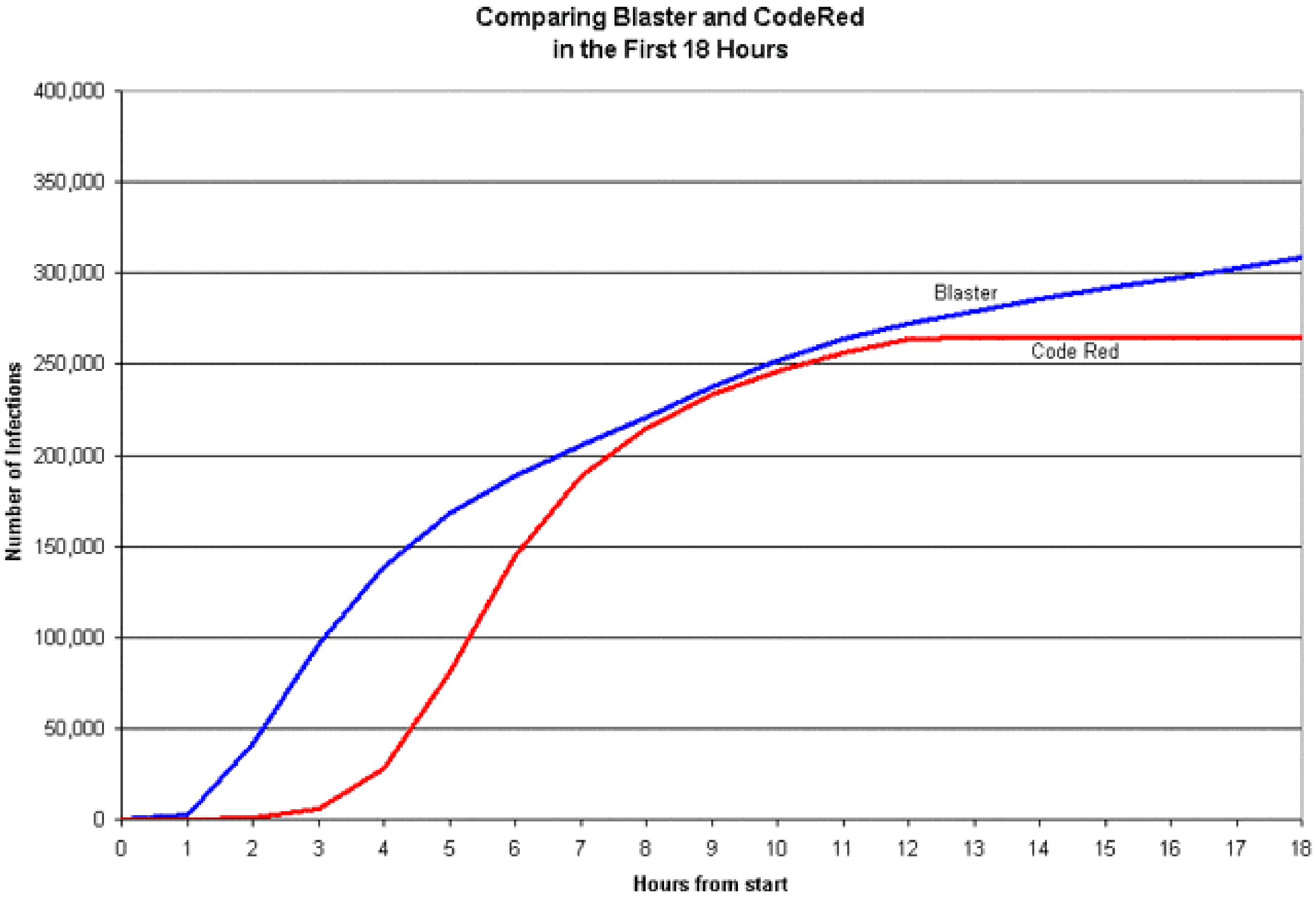
Source: CERT

Review(5)



Source: CERT

Review (6)



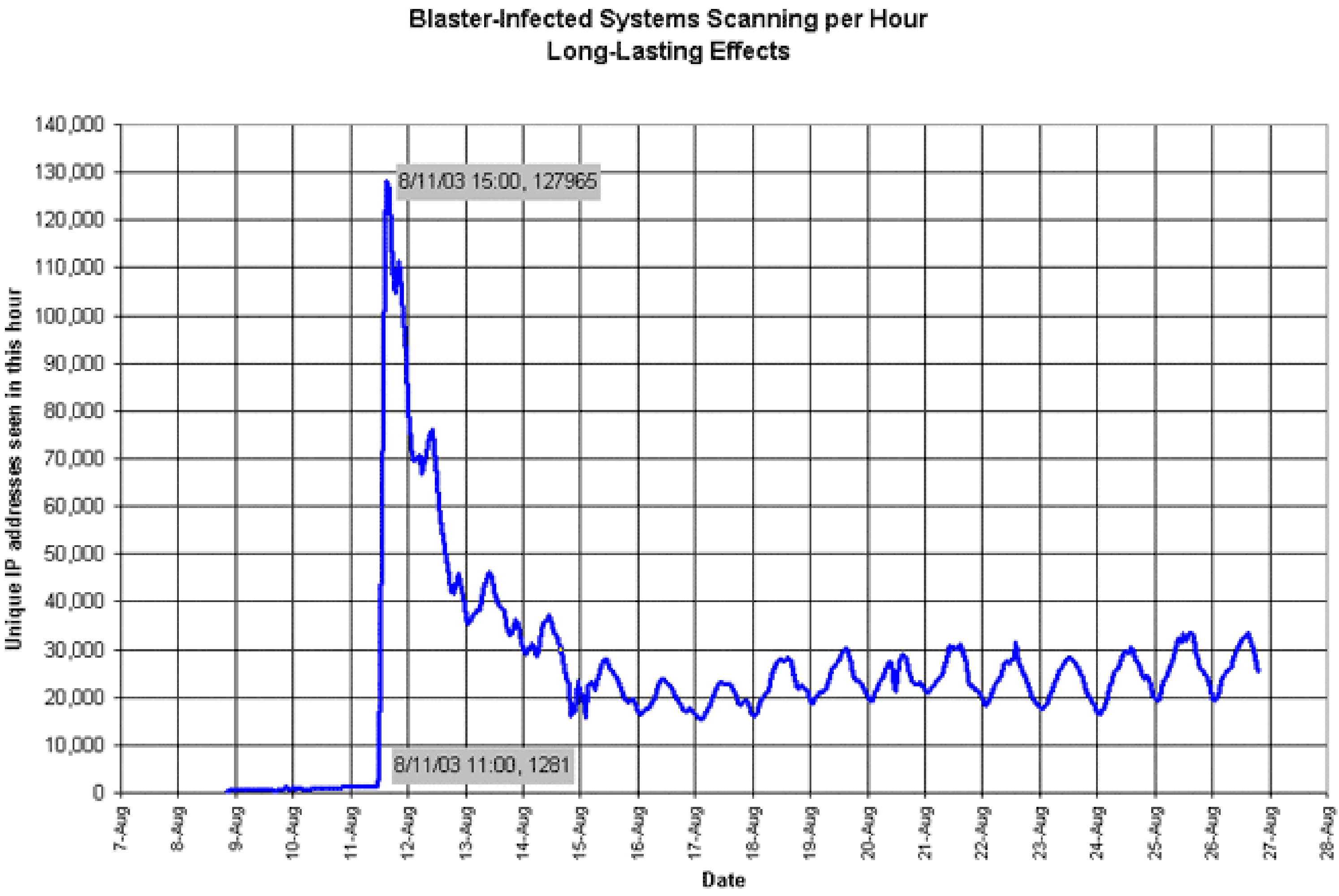
Source: CERT

Review(7)

Long lasting capacity

- Far-reaching
- Steady-state after initial surge

Review (8)



Source: CERT

Review (9)

Tendency to Zero-Day Exploit

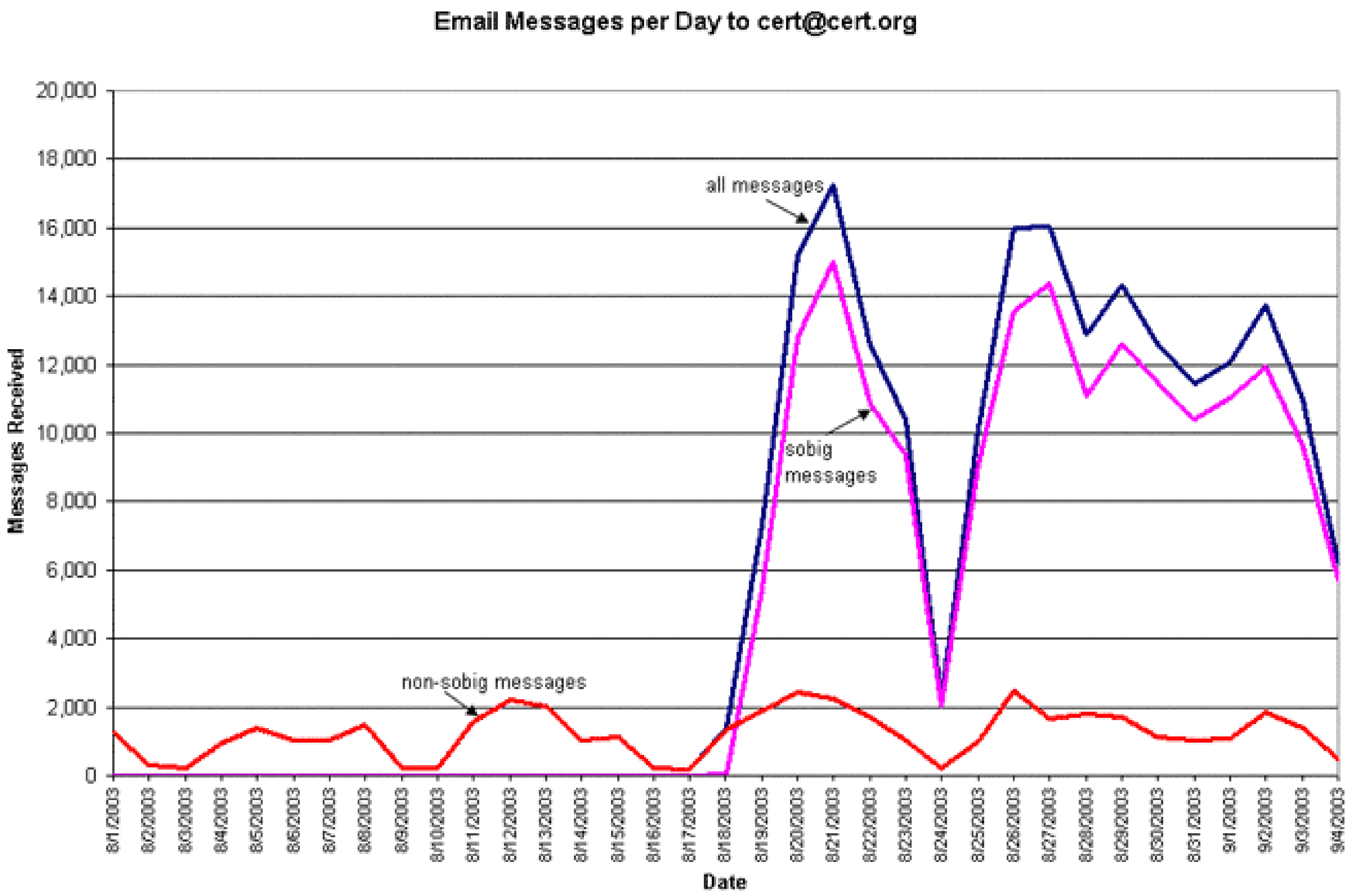
Code Name	**Worm/virus released**	**Vulnerability discovered and patch released**
Code Red	July 2001	June 2001
Slammer	Jan 2003	July 2002
Blaster	Aug 2003	July 2003
aim.exe	Nov 2003	No information from anti-virus vendor when discovered. ☹
WinTcpIp.exe	Nov 2003	No information from anti-virus vendor when discovered ☹

Review (10): Impact

Date	Code Name	Worldwide Economic Impact (USD)
8-9/2003	Blaster	$500 million
2003	Slammer	$1.00 billion
2001	Nimda	$635 million
2001	Code Red	$2.62 billion
2001	SirCam	$1.15 billion
2000	Love Bug	$8.75 billion
1999	Melissa	$1.10 billion
1999	ExploreZip	$1.02 billion
2001	9/11 attack to WTC	$15.8 billion (to restore IT and communication capabilities

Source: Computer Economics

Review (11): Sobig.F



Source: CERT

Prediction

Characteristic of the super worms and viruses

- High efficiency spreading
  - High penetration
  - Far reaching
  - Across different platforms
  - Infect via numerous vectors and vulnerabilities
- Highly stealth and anti-forensics
  - Stay silently for long time
  - Cover up activities
  - Difficult to decrypt or reverse engineering

Prediction (2)

- Highly distributed and coordinated
  - Exchange information with master and peers periodically
  - Coordinate attack, propagation or mutation
- Ability to launch attacks and cause serious impact to Internet Infrastructure
  - Deny of Service (DoS) attack to top level DNS servers and major IX core routers
  - Sending spam or forged mails
  - Release confidential information to the public
  - Spoof web page to release Trojan horse program

Prediction (3)

- Highly intelligent, automatic, and self-decisive
  - Self-adjust or mutate according to current condition
  - Decide how to carry out its mission when loses contact with its master or peers
  - Elect new district leader

Threat

- Over 171 million computers connected
- Grow at rapid pace
- Users with different knowledge and background
- Computer system become more and more sophisticated and complicated
- Bandwidth and machine capability keep rising
- Vendor turn off security features in default setting
- Put product to market without fully tested
- End-users disable/bypass security functions deliberately

Worst case scenario

- Zero-day exploit
- Attack preparation
- Complete blackout
- Recurrence
- Chaos

What can we do

- What
- How

We need co-operation from all sectors

What can we do (2)

- High management level
  - Security is no longer “add-on feature” or “option”
  - Resource for security should be in high priority
- System Administrators
  - Follow the best practice: risk assessment; security policy and security audit
  - Keep up with current security knowledge and skill
  - Educate users to raise their security awareness

What can we do (3)

- Vendors
  - Products should be fully tested
  - Do not assume user has certain security knowledge or awareness
  - Do not lower the security level in default setting
- Government
  - Encourage high quality security product
  - Allocate resource to support security researches in Universities
  - Cooperate with non-profit organization to offer security training to the public

What can we do (4)

- Institutes house Internet Infrastructure
  - Have contingency and backup plan in case under serve attack
  - Keep monitoring of any unusual activities
- End users
  - Protect their systems well no matter how trivial and unimportant they are
  - Use consumer power to choose product with high quality security feature
  - Raise security awareness from time to time

Will they come?

When will the super worms and viruses come?

I don’t know but we better prepare for that.

Thank You