Why Code Red Changed the Face of Network Security

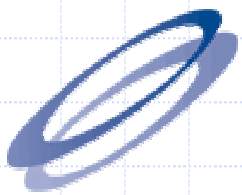
Simon Baker and Tom Meyer,
JANET-CERT

History of Internet Worms...

- The Shockwave Rider

...science fiction story by John Brunner in 1975

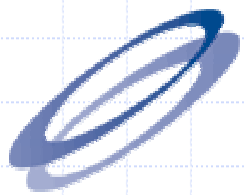
- The Morris Worm



History of Internet Worms...

- *There may be a virus loose on the internet.*

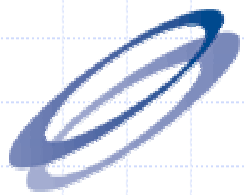
Andy Sudduth of Harvard, 34 minutes after midnight, Nov. 3, 1988



The Morris Worm

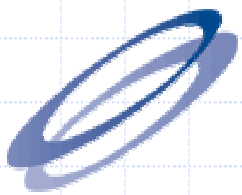
- *"Could an incident like this occur today? If so, how much damage could it cause?"* *SANS, Larry Boettger December 24, 2000*

Clearly it could!!!



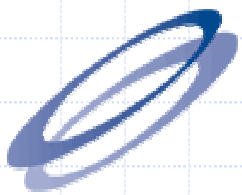
Morris Worm

- Exploited sendmail
- Exploited fingerd
- Nothing overly clever, was in fact not designed to be a `real' worm!

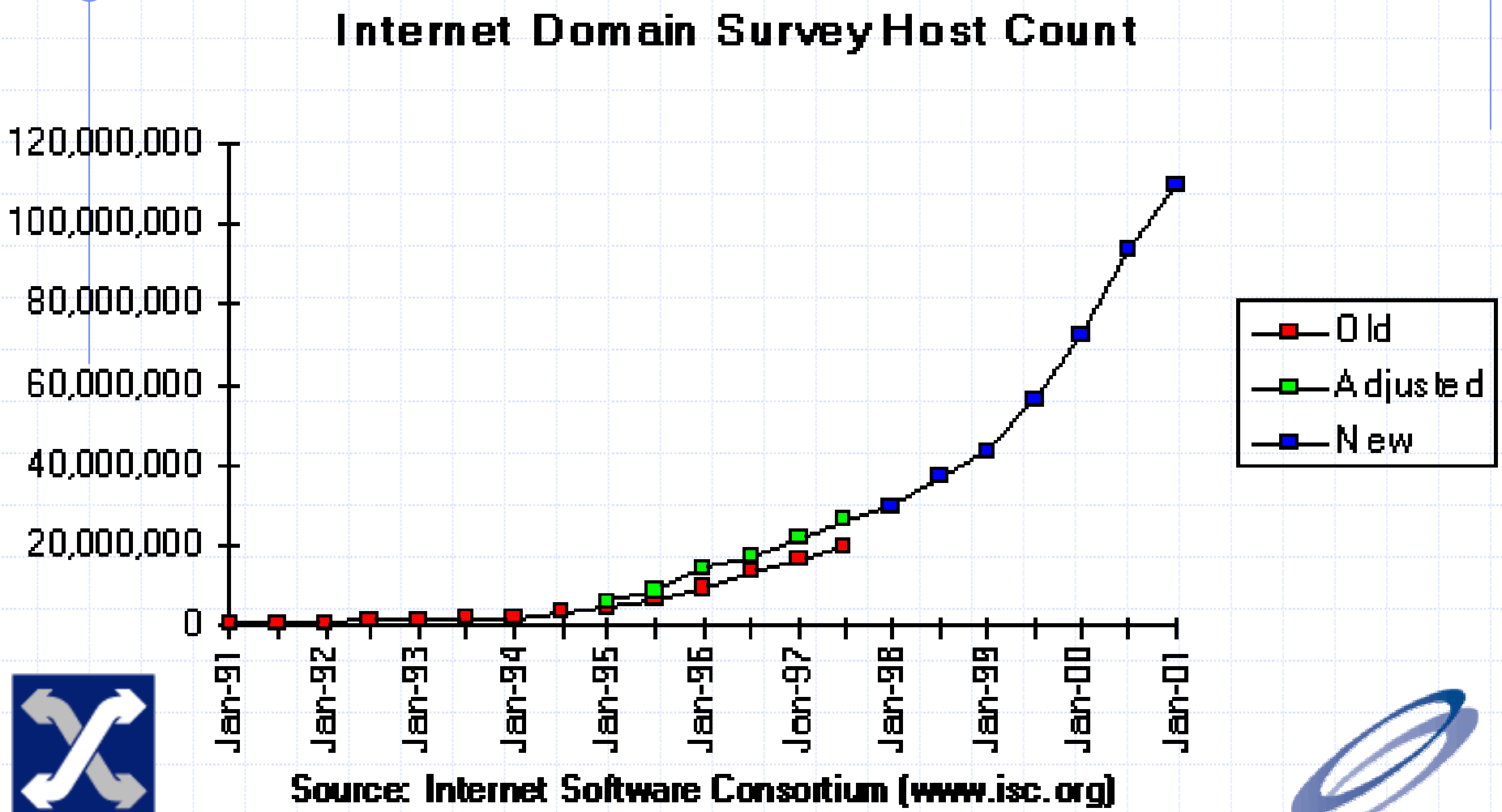


Punishment!

- Convicted of violating the computer Fraud and Abuse Act (Title 18)
- Three years of probation
- 400 hours of community service
- A fine of $10,050
- ...and the costs of his supervision

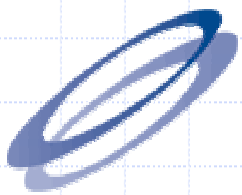


Internet population



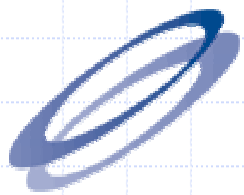
Why Code Red???

- It was called ‘Code Red’ by eEye.
- ...because it defaced pages with the words “Hacked by Chinese”
- ...and “’Code Red’ Mountain Dew was the only thing that kept us awake while we disassembled this exploit…”



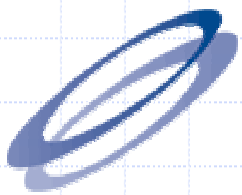
Key Points of Code Red

- Exploited the '.ida' bug in IIS web servers...
- Spread *very* rapidly, estimated that it could infect "roughly half a million IP addresses a day. "



IDS Signature

- GET default.ida?…multiple N's in the original, X's later on…



Code Red Infestations...

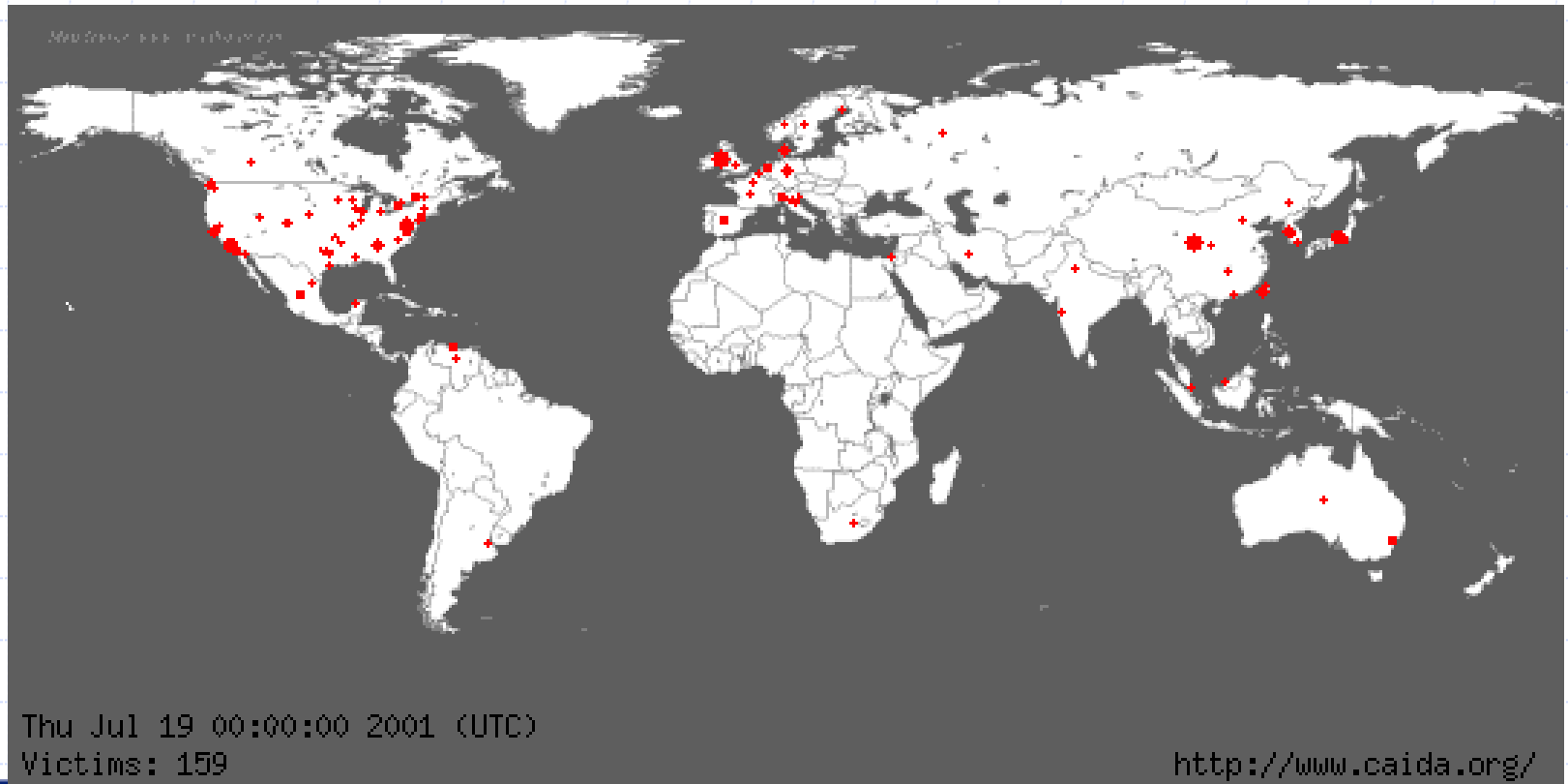
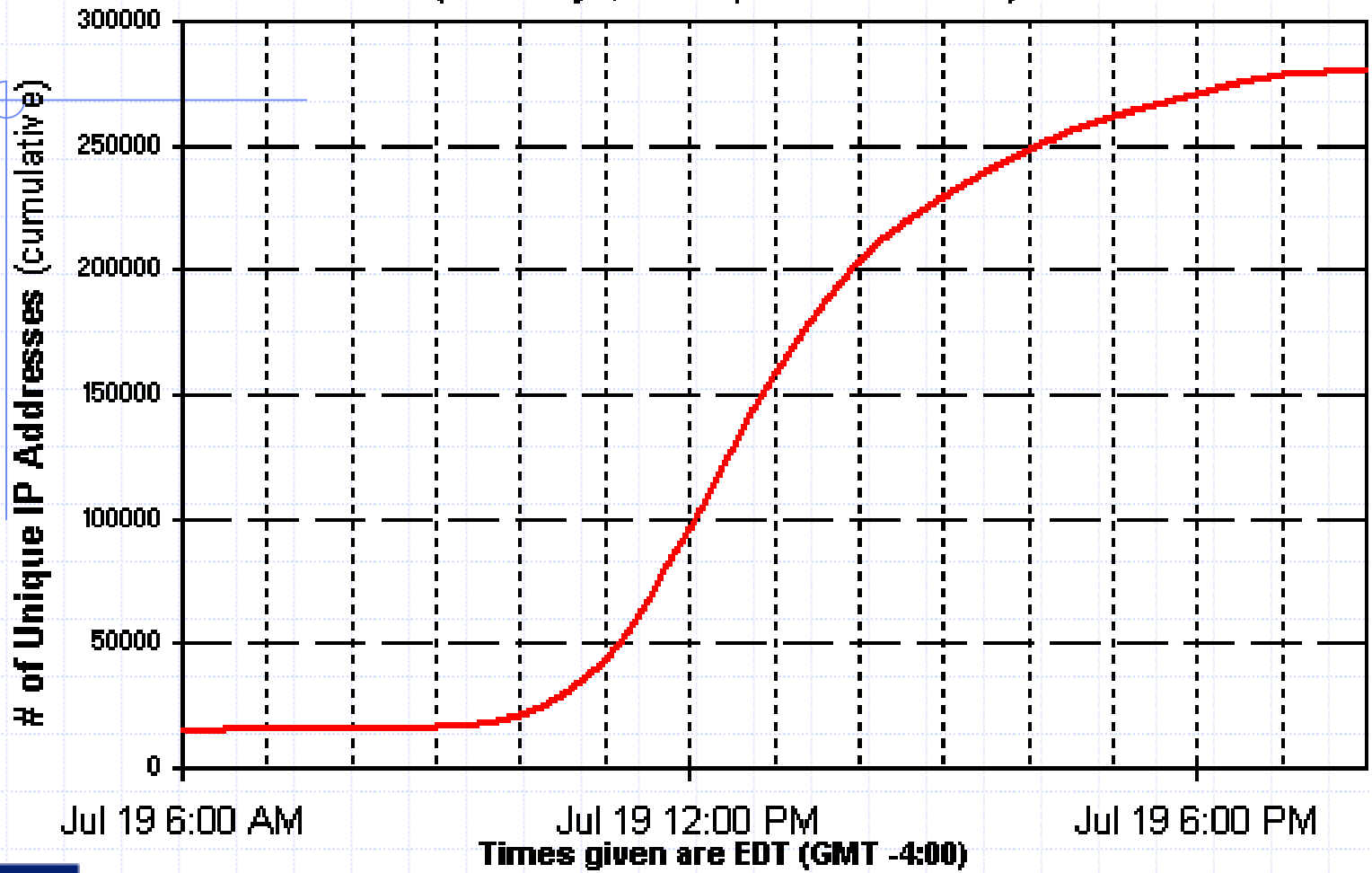


Figure 1: IP Addresses Compromised by the "CodeRed" worm

(data for July 19, 2001 as reported to the CERT/CC)



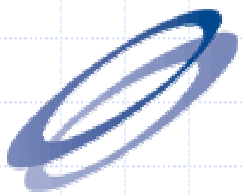
http://www.cert.org/advisories/CA-2001-23.html

Source: incident data for CERT#36881

UKERNA

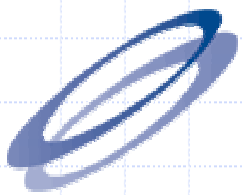
Code Red II

- Uses the same injection vector (the .ida vulnerability)
- Only exploits Windows 2000 web servers because it overwrites EIP with a jmp that is only correct under Windows 2000.



Win32/Nimda.A worm

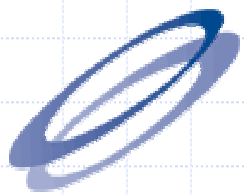
- Mass mailing email worm
- Will infect Windows systems as well as computers installed with IIS servers
- Nimda also spreads over network shares



Nimda

Infection routes

- From client to client via email
- From client to client via network shares
- From web server to client by browsing an infected site
- From client to web server by scanning for vulnerable versions of IIS
- From client to web server by scanning for backdoors left by CodeRed II

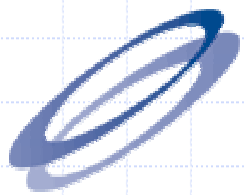


Impact

Opens machine to further compromise

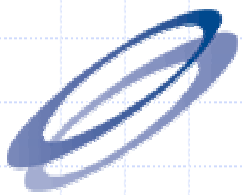
- Enables sharing of network drives
- Creates guest account with administrator privileges
- Adds itself to files on the system
- Scanning can cause local denial of service

Recovery requires reinstall and patch



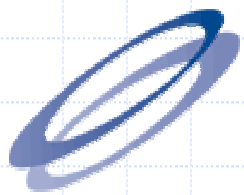
The Future...

- These are only Guestimations but...
- ...if *we* can make them, so can they!
- It ain't over!



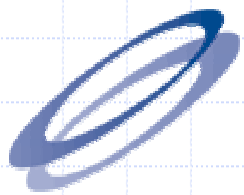
Distribute Passwd Cracking?

- A ‘la Distributed.net...
- JANET sites are already having big Solaris servers hacked in order to steal cpu cycles for this...
- A distributed worm that does this could have amazing results!



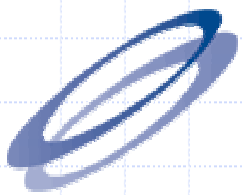
Distributed Passwd Sniffing?

- Passwords can be sniffed of the wire.
- People don't understand the lax security in POP3, IMAP, Telnet, HTAuth, etc.
- SSL encrypted sessions can be attacked (Dsniff!)



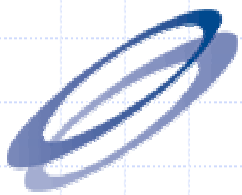
Distributed DoS?

- Already happened!
- ...but not as yet fully automated!
- If it was well hidden enough, could never be discovered until it was too late...
- JANET is a particular target.



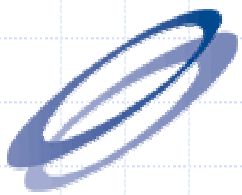
P2P Networking?

- Multiple machines could set up their own P2P network
- Distribute DivX movies, pr0n, warez
- Encrypted channels
- IPSec?
- IPv6?



Has it Happened?

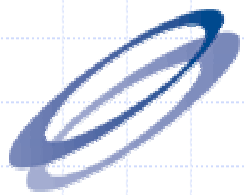
- Maybe it's already happened!
- Every worm so far has had severe flaws
- Someone *will* get it right
- DDoS Agents? Still lots of infected machines on the Internet!
- MIRKForce?



How to prevent 99.9% of Infestations...

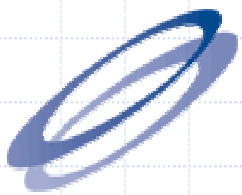
- PATCH! PATCH! PATCH! PATCH!
  PATCH! PATCH! PATCH! PATCH!
  PATCH! PATCH! PATCH! PATCH!
  PATCH! PATCH! PATCH! PATCH!

PATCH!



You were expecting more?

- Patching a system is imperative!
- Worms rely on unpatched, vulnerable, sloppily administered systems
- Patching will fix this!
- Seriously! We have not had a **single** report of a properly **patched, compromised system!**



Further Reading...

- RFC 1135
- http://www.eeye.com/html/Research/
- Google Searches!!!