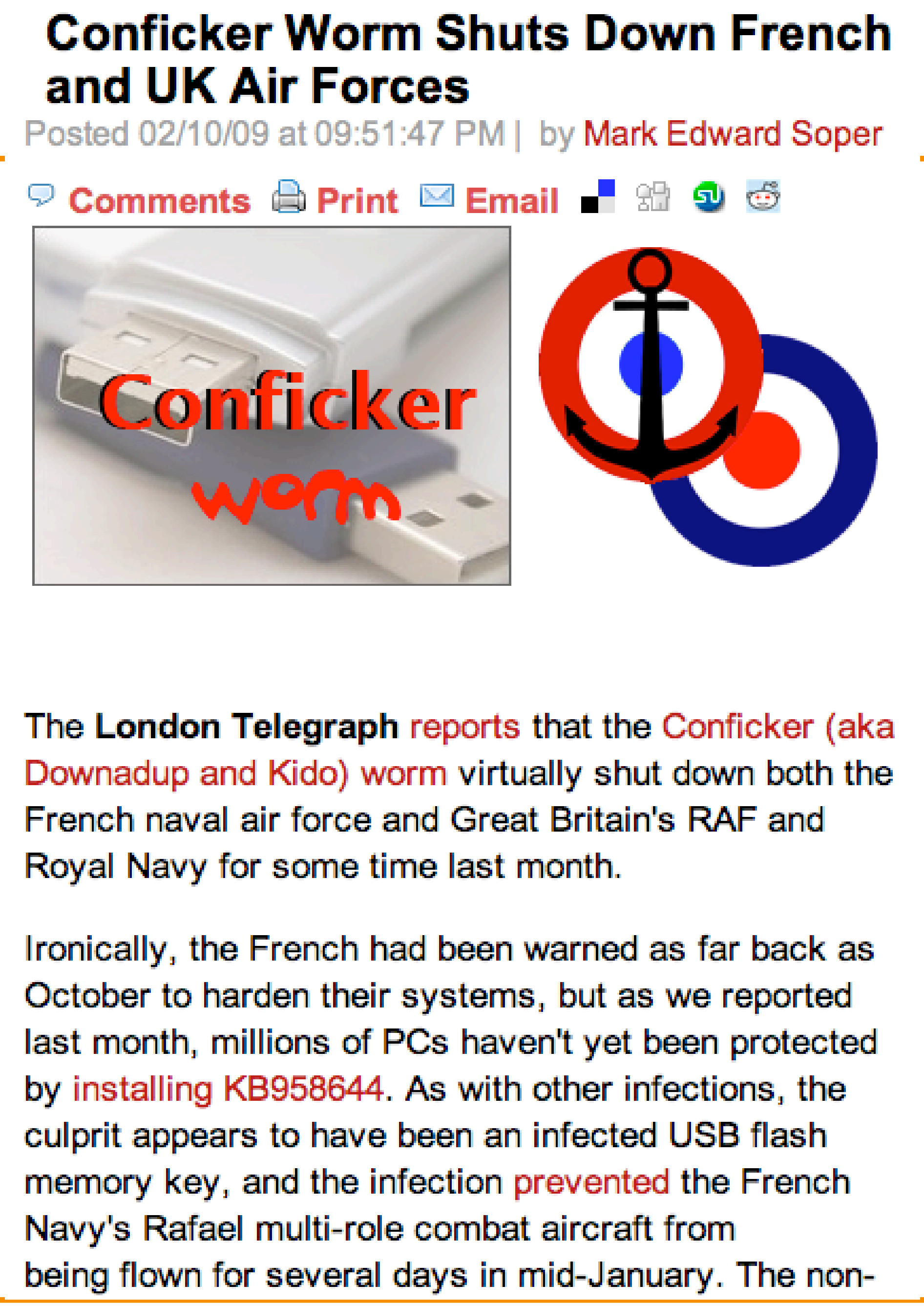


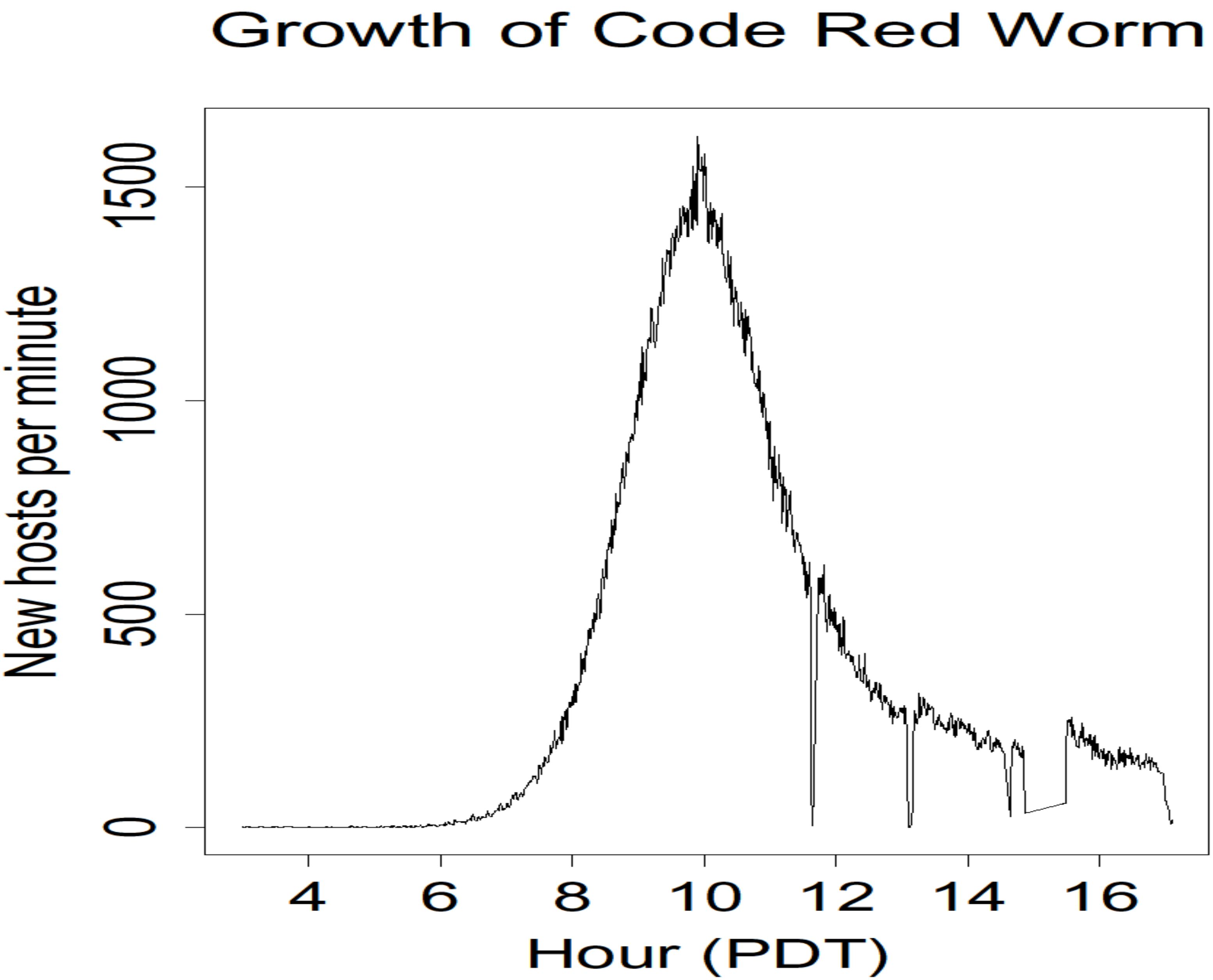
Conficker Worm Shuts Down French and UK Air Forces

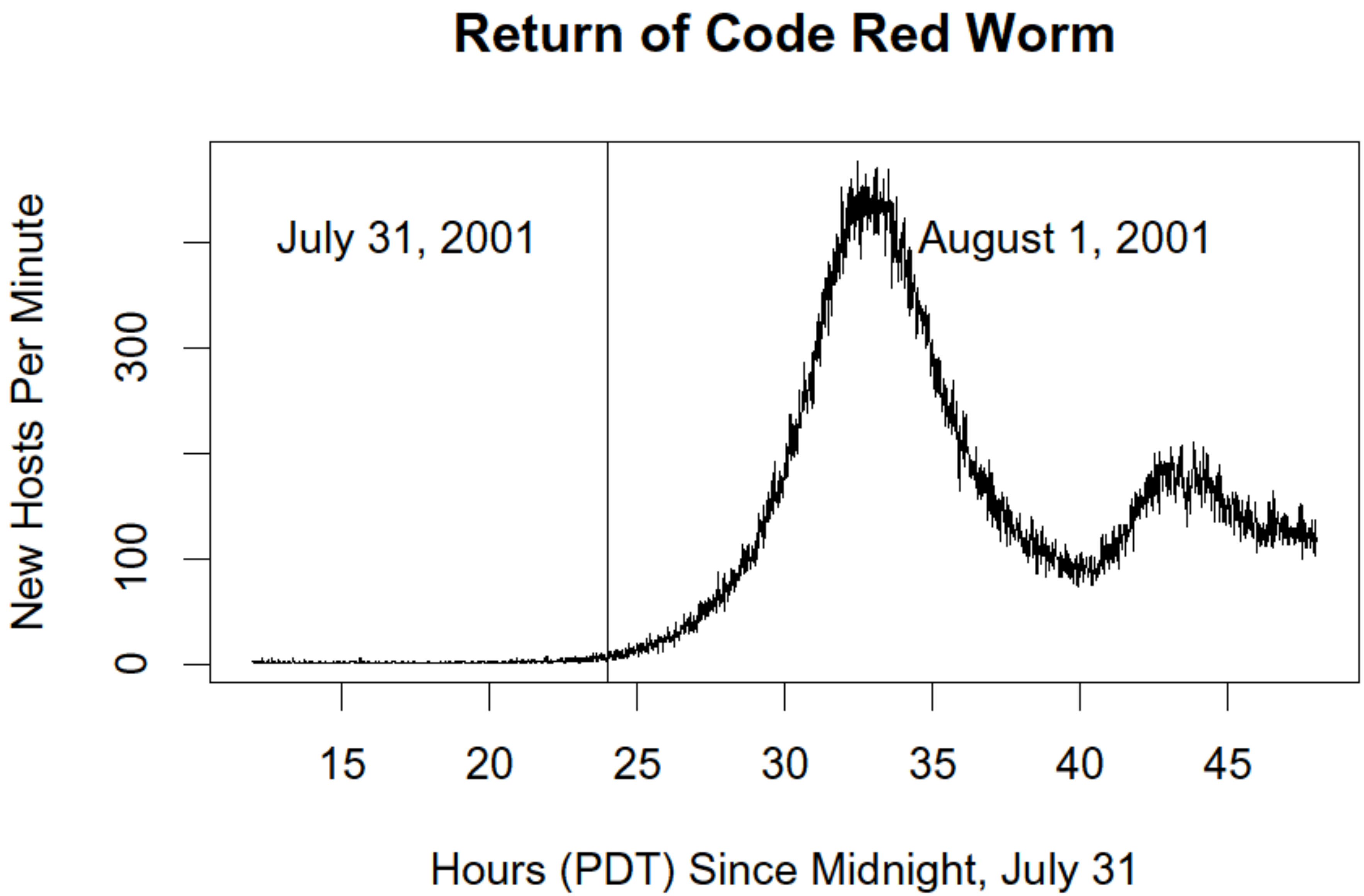
Posted 02/10/09 at 09:51:47 PM | by Mark Edward Soper

Comments Print Email

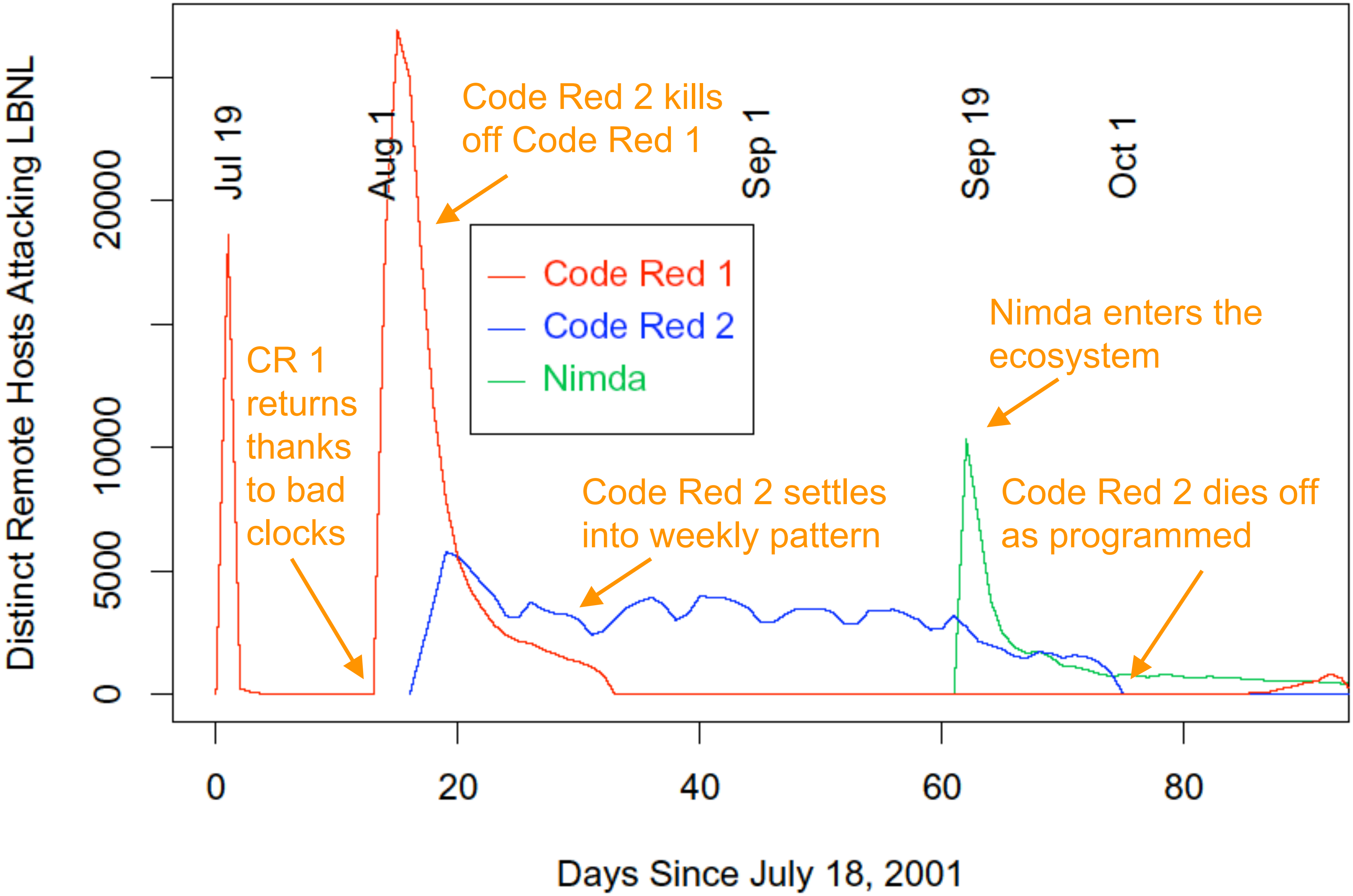
The **London Telegraph** reports that the Conficker (aka Downadup and Kido) worm virtually shut down both the French naval air force and Great Britain's RAF and Royal Navy for some time last month.

Ironically, the French had been warned as far back as October to harden their systems, but as we reported last month, millions of PCs haven't yet been protected by installing KB958644. As with other infections, the culprit appears to have been an infected USB flash memory key, and the infection prevented the French Navy's Rafael multi-role combat aircraft from being flown for several days in mid-January. The non-


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



Return of Code Red Worm



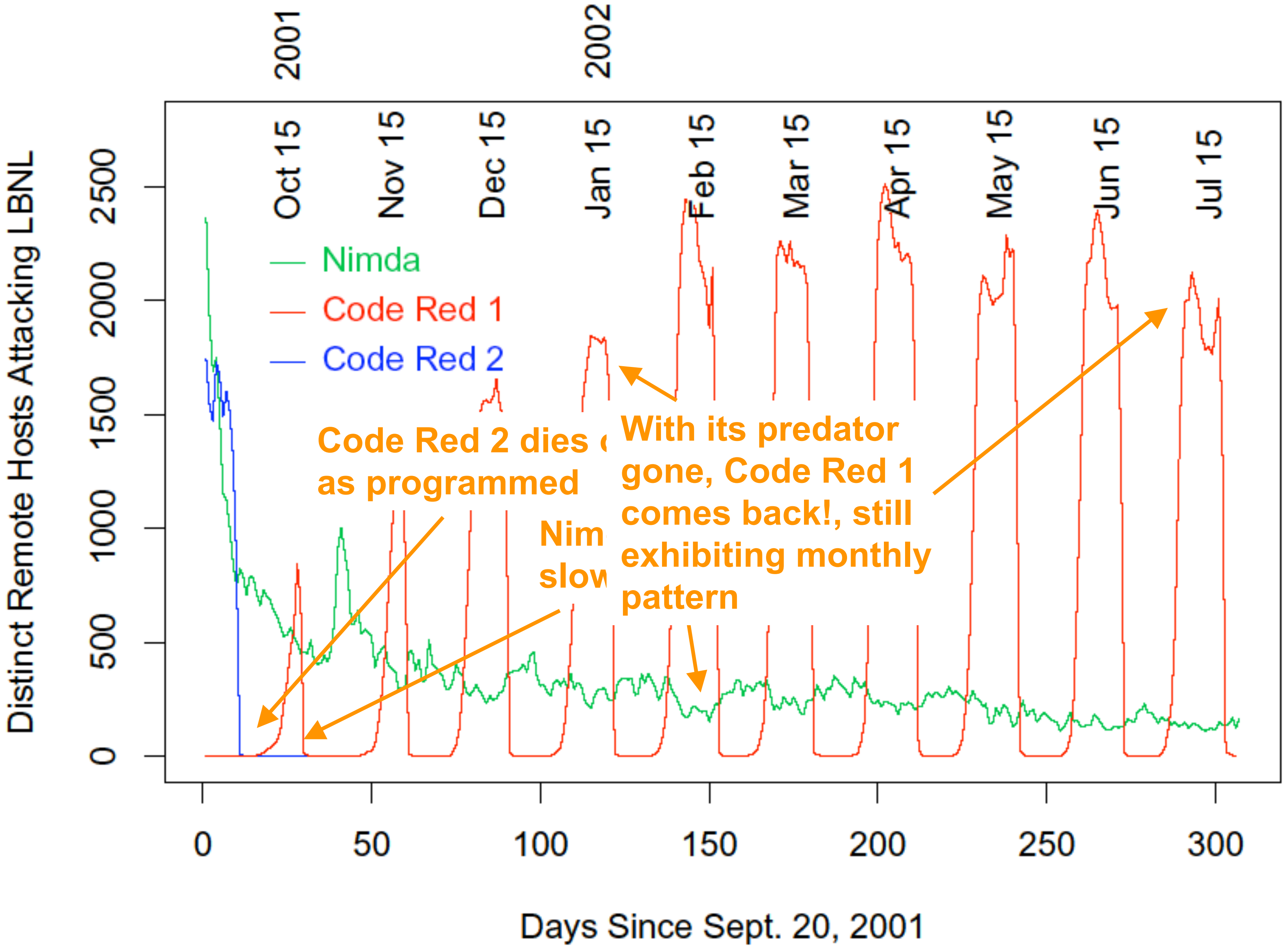
Code Red 2 kills off Code Red 1

CR 1 returns thanks to bad clocks

Code Red 2 settles into weekly pattern

Nimda enters the ecosystem

Code Red 2 dies off as programmed



Code Red 2 dies
as programmed

Nim
slow

With its predator
gone, Code Red 1
comes back!, still
exhibiting monthly
pattern

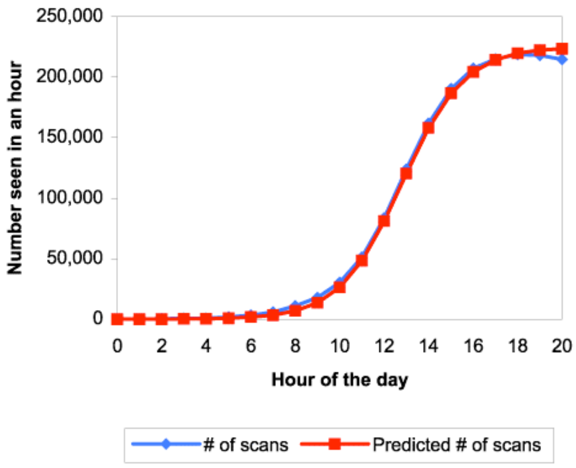
Modeling Worm Spread

- Often well described as *infectious epidemics*
  - Simplest model: homogeneous random contacts

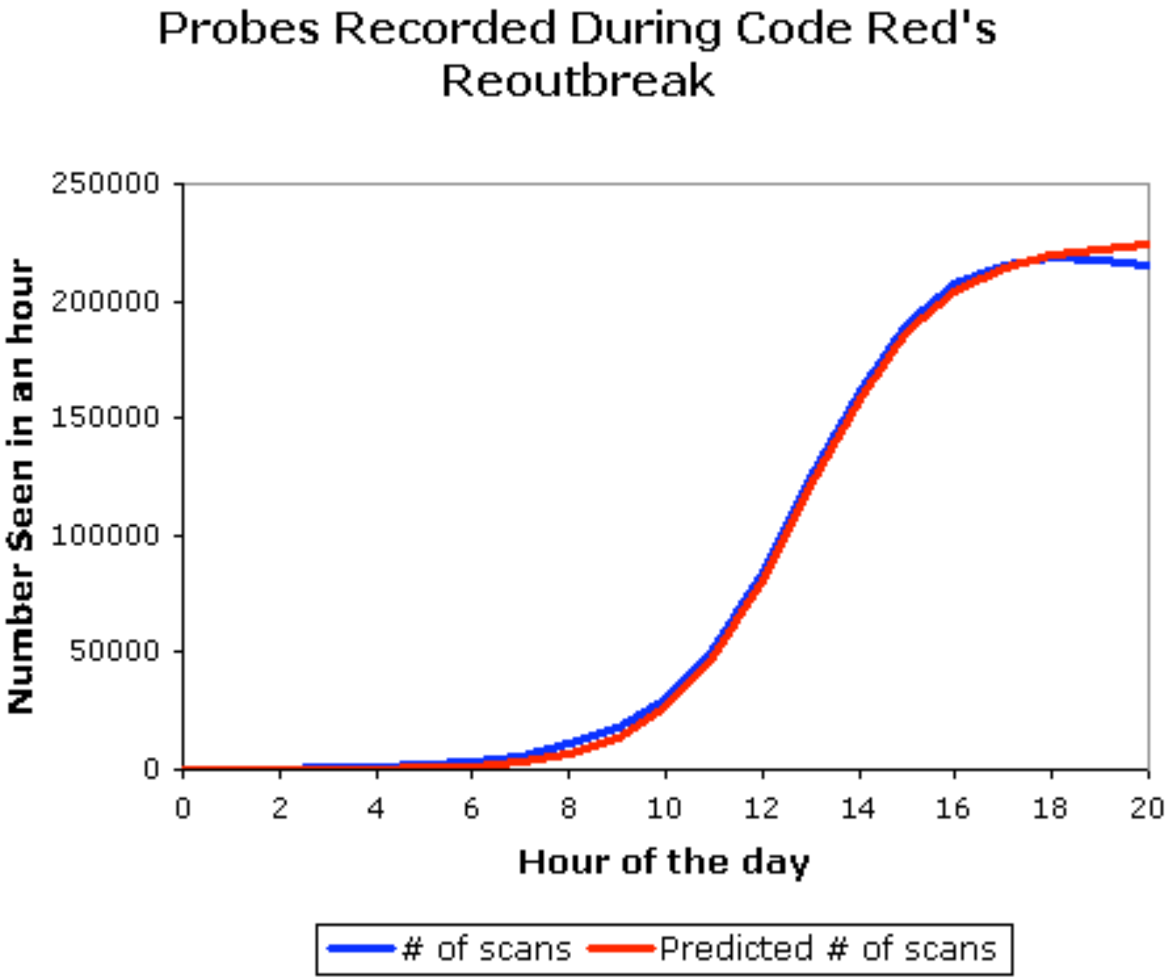
- Classic SI model
  - N: population size
  - S(t): susceptible hosts at time t
  - I(t): infected hosts at time t
  - β: contact rate
  - i(t): I(t)/N, s(t): S(t)/N

$$\begin{aligned} \frac{dI}{dt} &= \beta \frac{IS}{N} \\ \frac{dS}{dt} &= -\beta \frac{IS}{N} \end{aligned} \quad \Rightarrow \quad \frac{di}{dt} = \beta i(1-i)$$

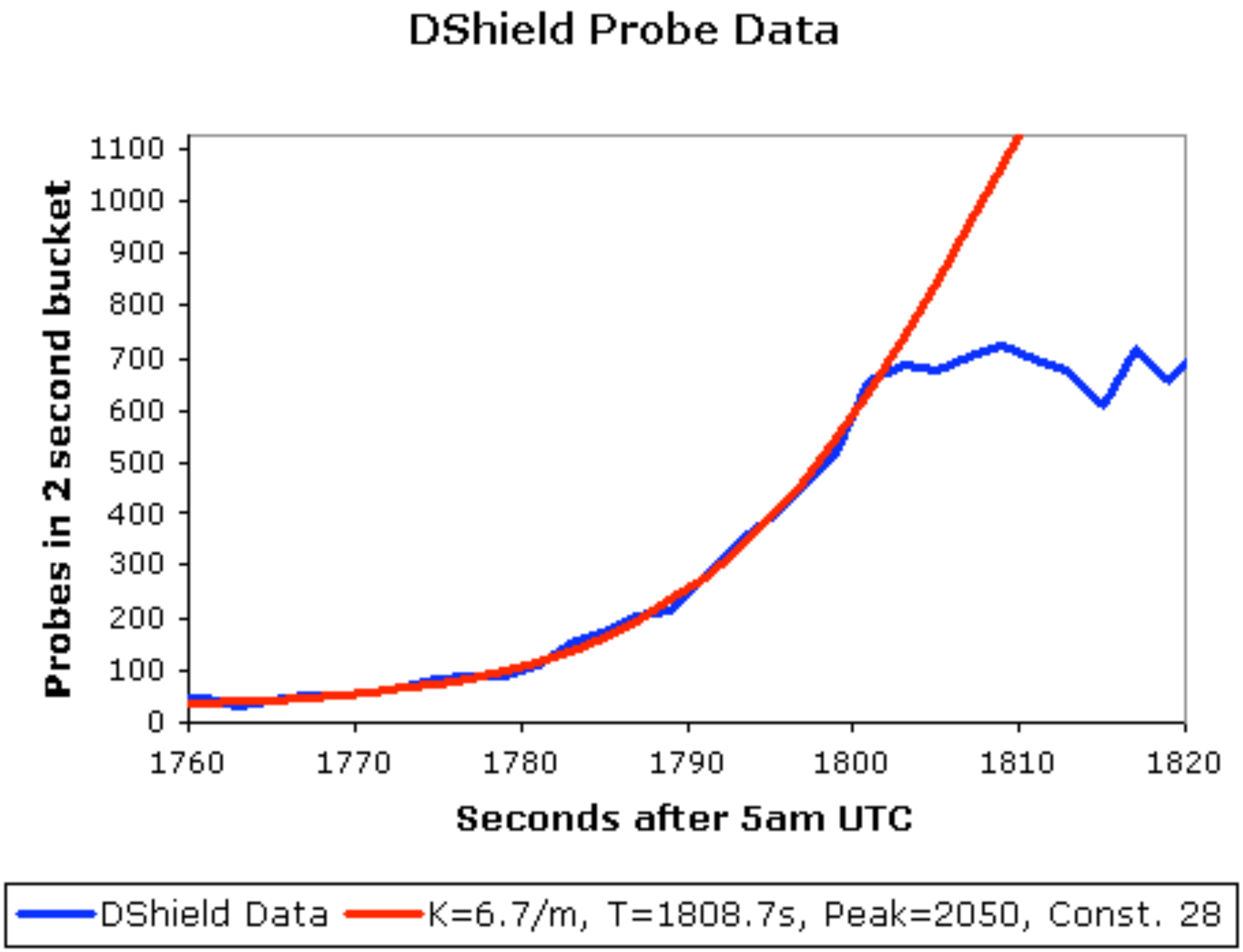
$$i(t) = \frac{e^{\beta(t-T)}}{1+e^{\beta(t-T)}}$$

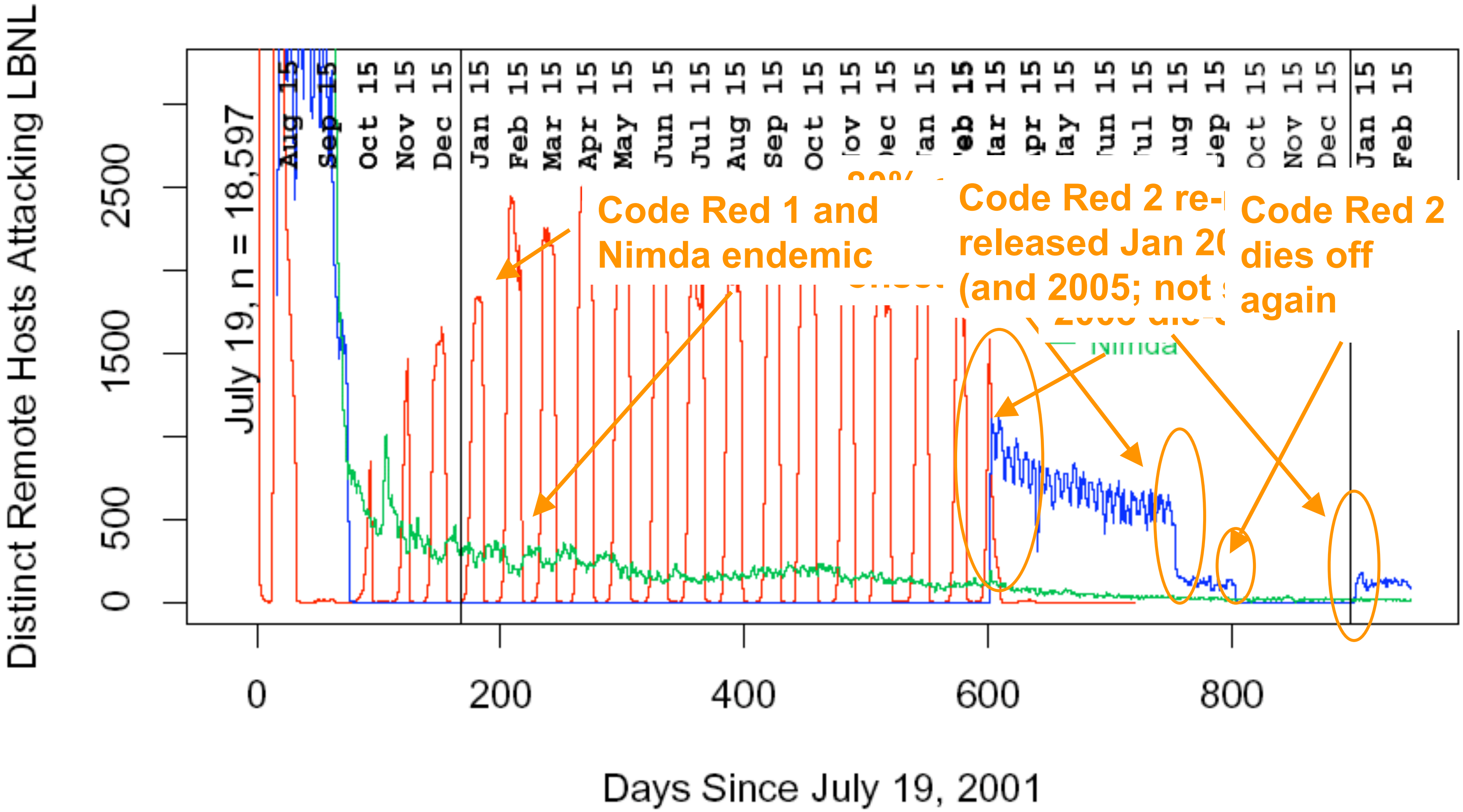


The Usual Logistic Growth



Slammer's *Bandwidth-Limited* Growth



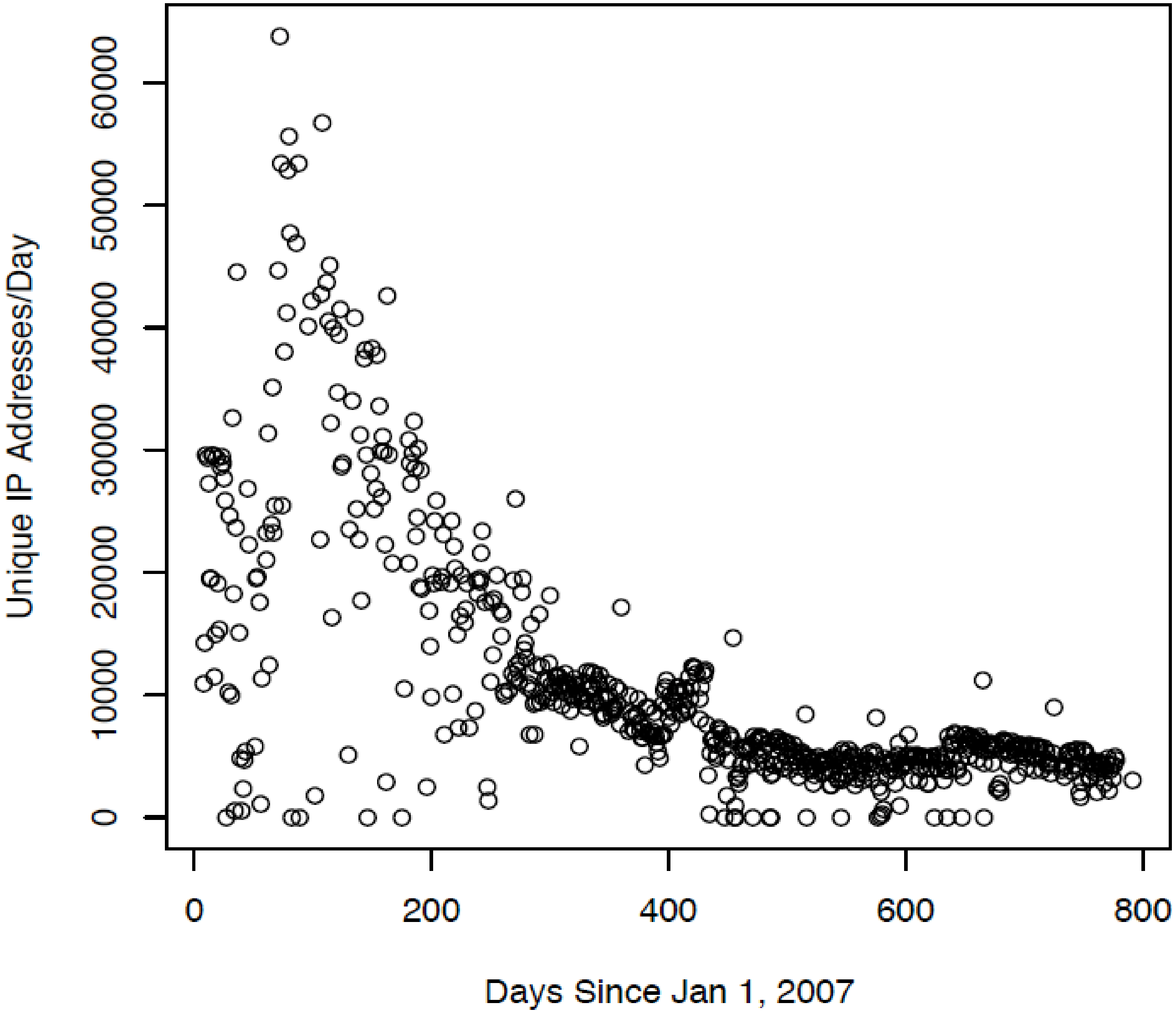


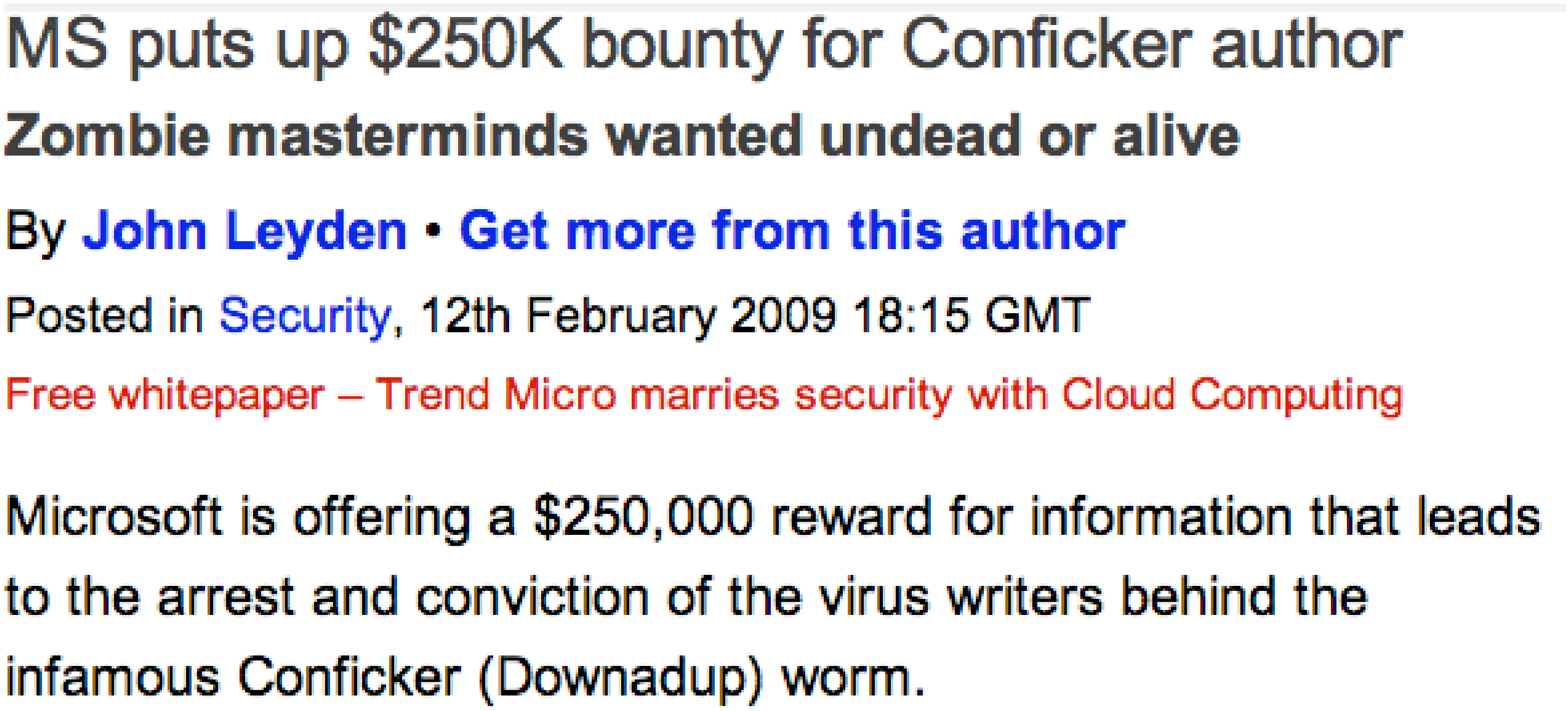
Code Red 1 and
Nimda endemic

Code Red 2 re-
released Jan 20
(and 2005; not

Code Red 2
dies off
again

Bagle Infectee Contacts at Monitor





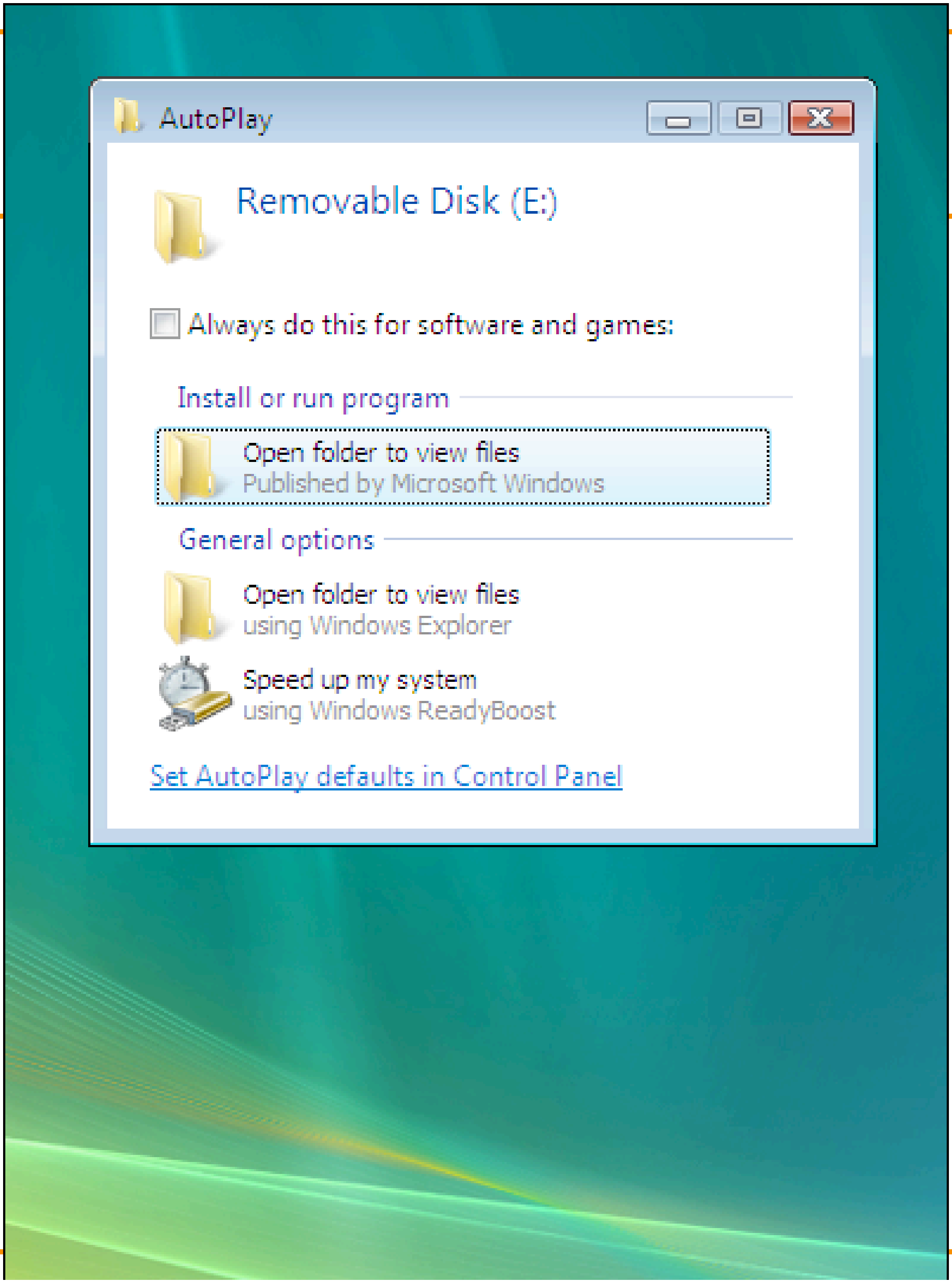
MS puts up $250K bounty for Conficker author

Zombie masterminds wanted undead or alive

By John Leyden • Get more from this author

Posted in Security, 12th February 2009 18:15 GMT

Microsoft is offering a $250,000 reward for information that leads to the arrest and conviction of the virus writers behind the infamous Conficker (Downadup) worm.



AutoPlay

Removable Disk (E:)

□ Always do this for software and games:

Install or run program

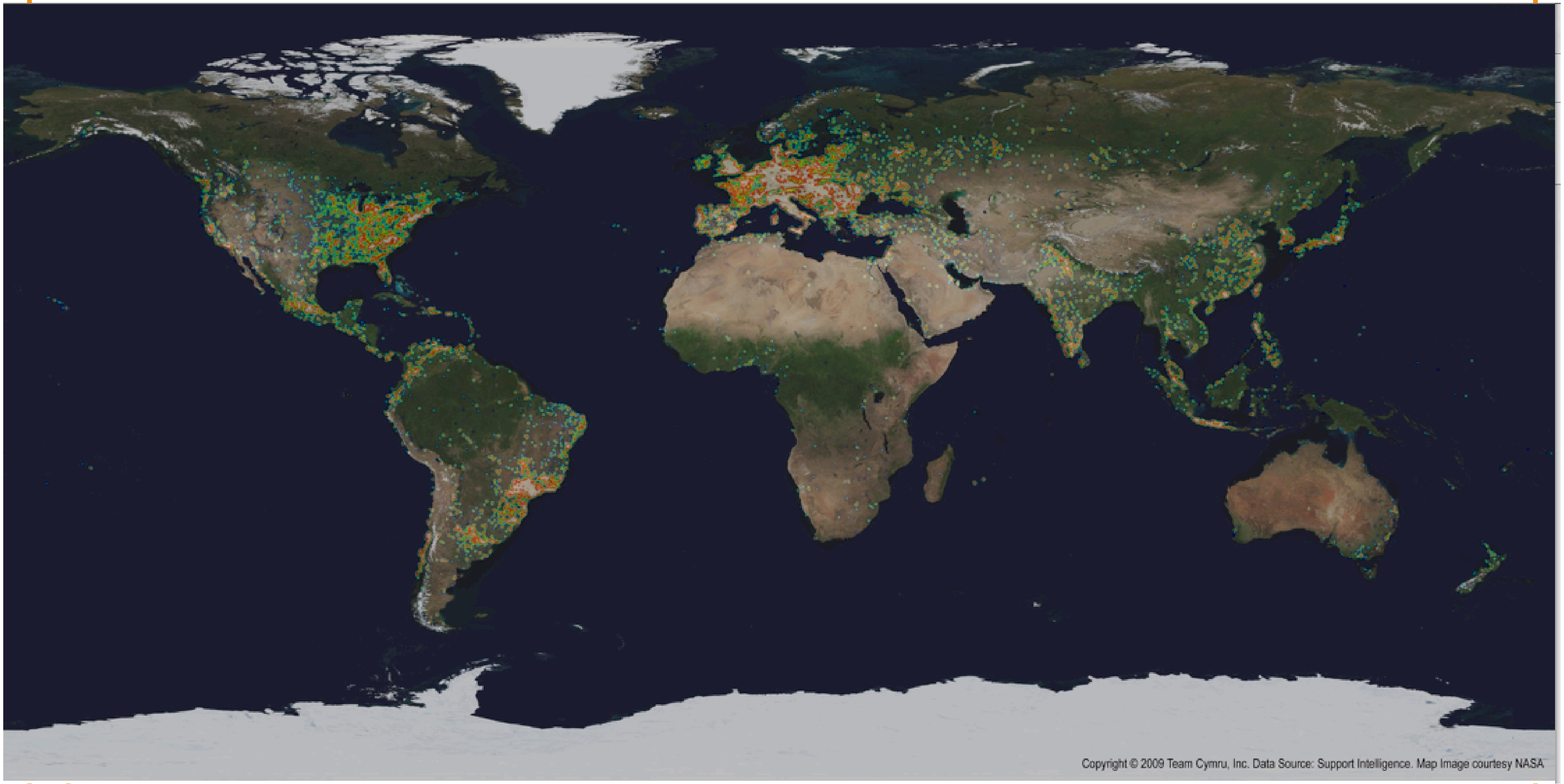
Open folder to view files
Published by Microsoft Windows

General options

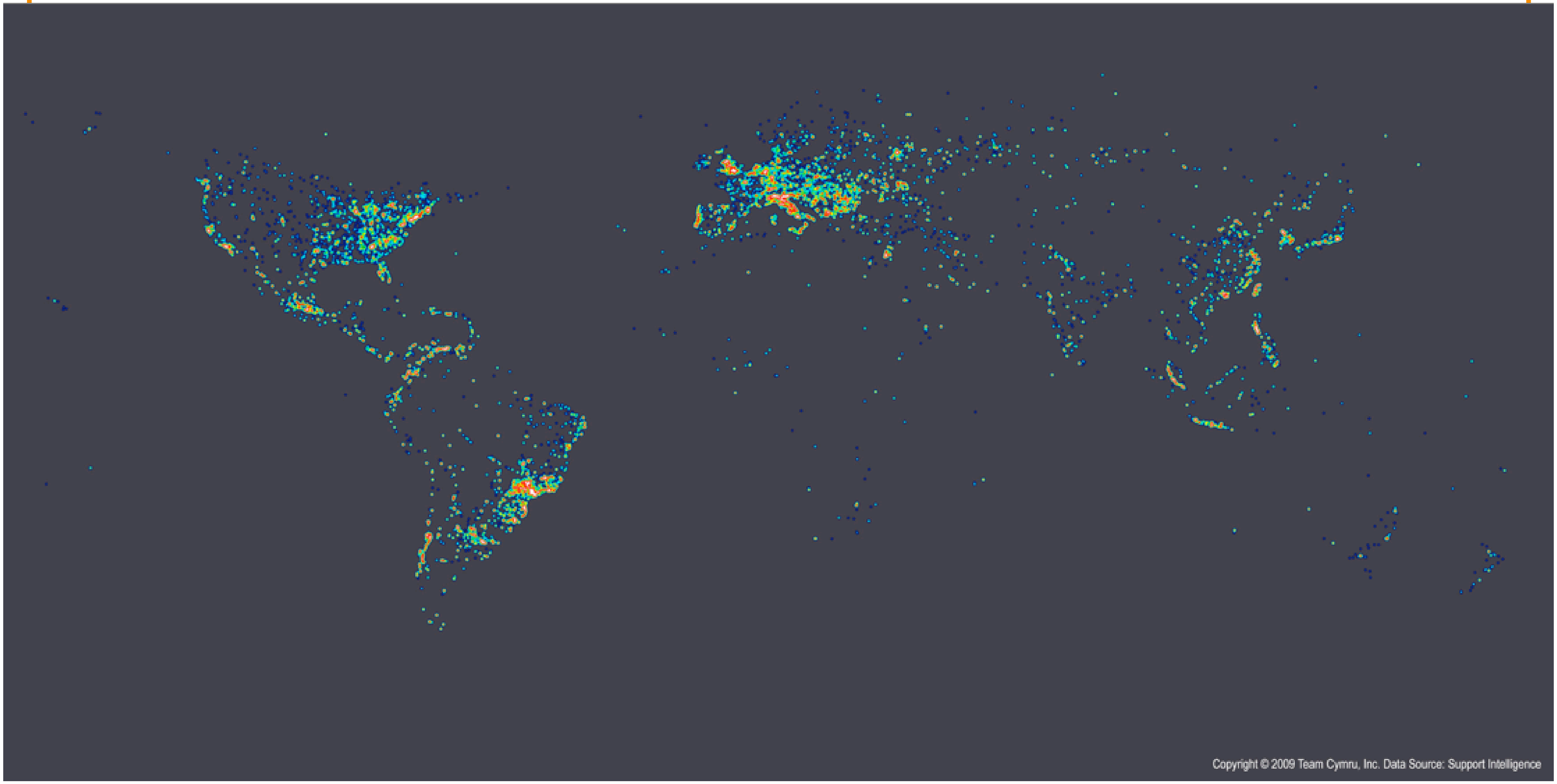
Open folder to view files
using Windows Explorer

Speed up my system
using Windows ReadyBoost

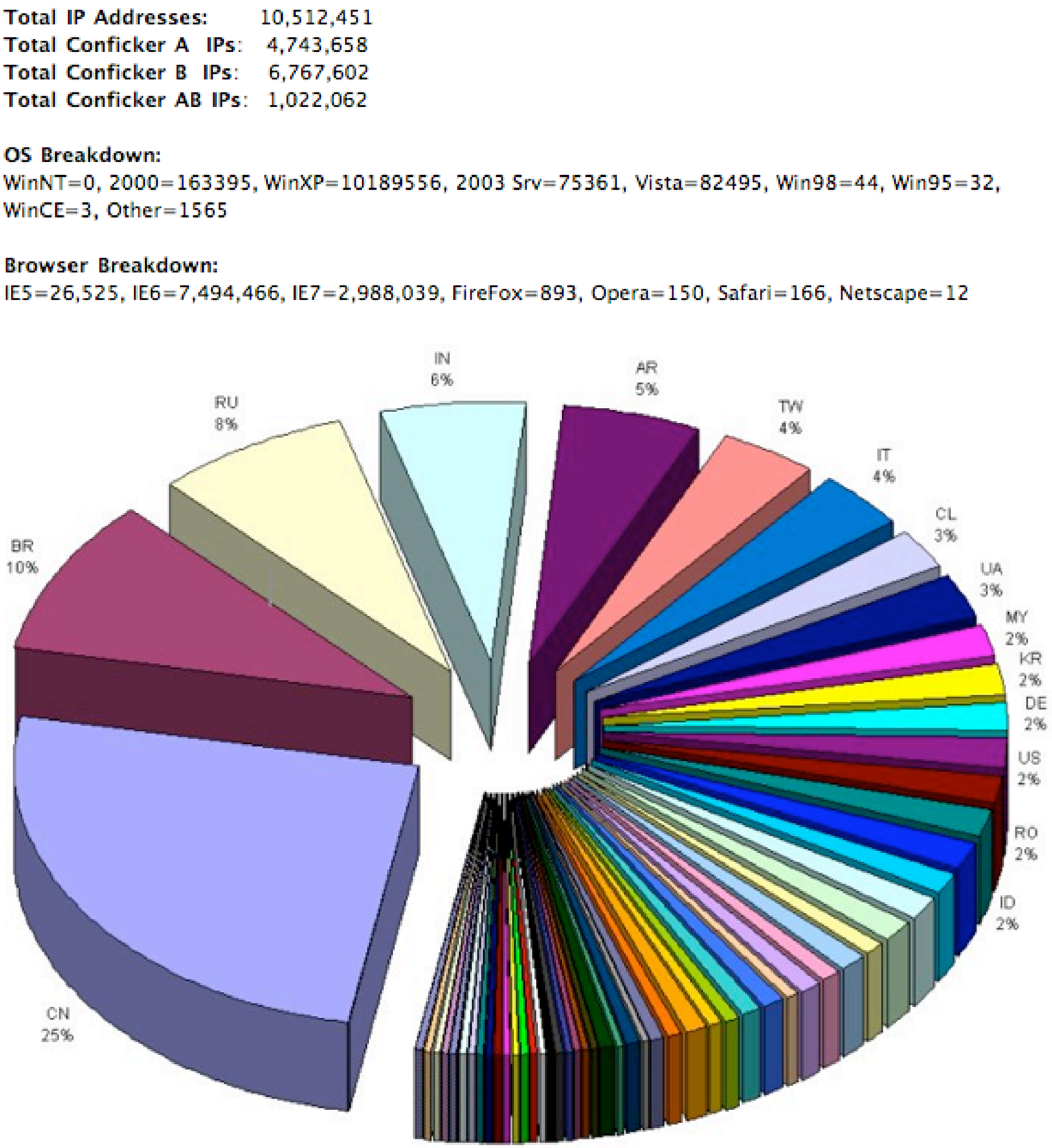
Set AutoPlay defaults in Control Panel



Copyright © 2009 Team Cymru, Inc. Data Source: Support Intelligence. Map Image courtesy NASA



Copyright © 2009 Team Cymru, Inc. Data Source: Support Intelligence



Total IP Addresses: 10,512,451
Total Conficker A IPs: 4,743,658
Total Conficker B IPs: 6,767,602
Total Conficker AB IPs: 1,022,062

OS Breakdown:
WinNT=0, 2000=163395, WinXP=10189556, 2003 Srv=75361, Vista=82495, Win98=44, Win95=32, WinCE=3, Other=1565

Browser Breakdown:
IE5=26,525, IE6=7,494,466, IE7=2,988,039, FireFox=893, Opera=150, Safari=166, Netscape=12