at the Phoenix PI meeting, it was clear that the DARPA sponsor wanted a single metric for comparing systems and approaches.

The New York Times

U.S.

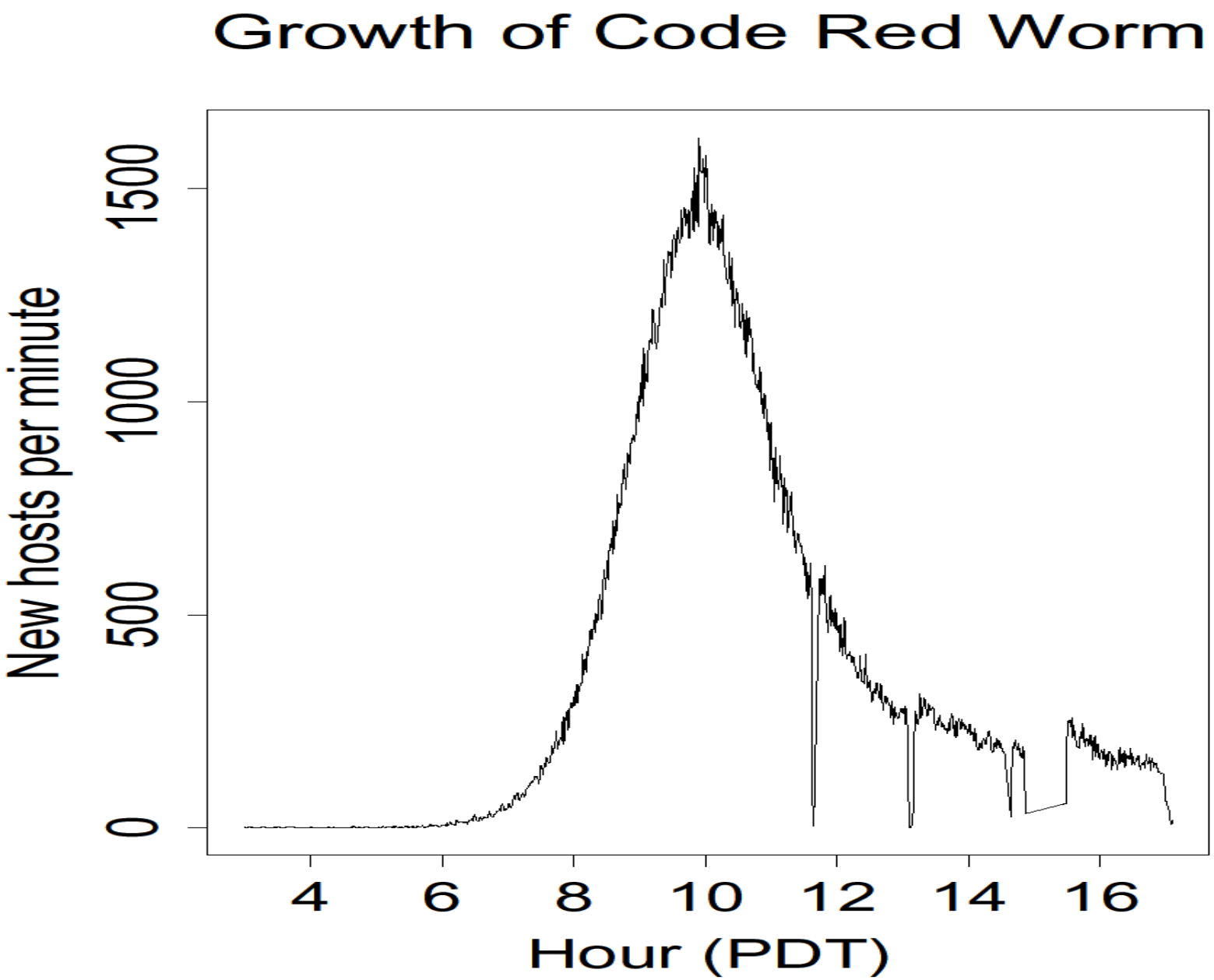
'Virus' in Military Computers Disrupts Systems Nationwide

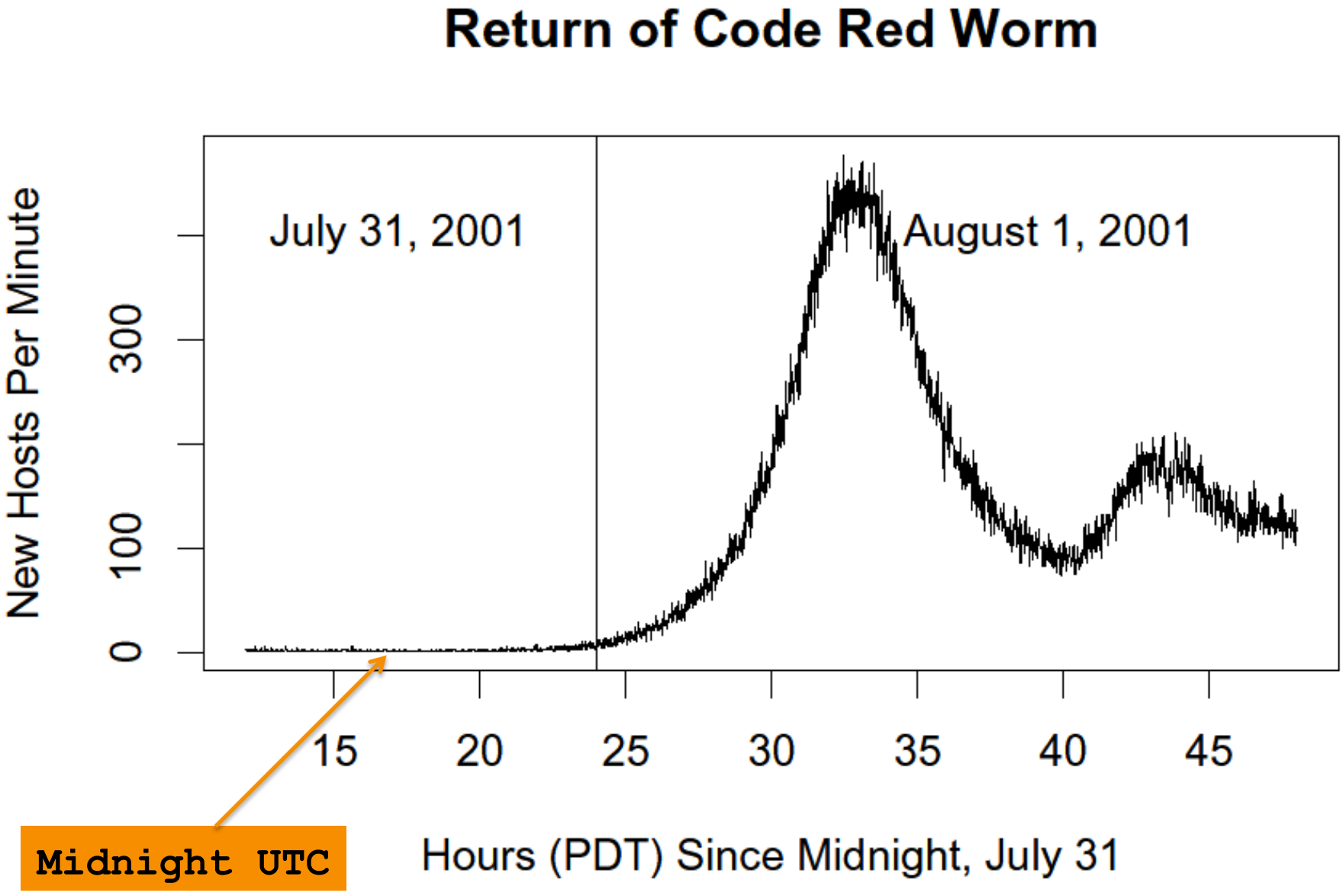
By JOHN MARKOFF
Published: November 4, 1988

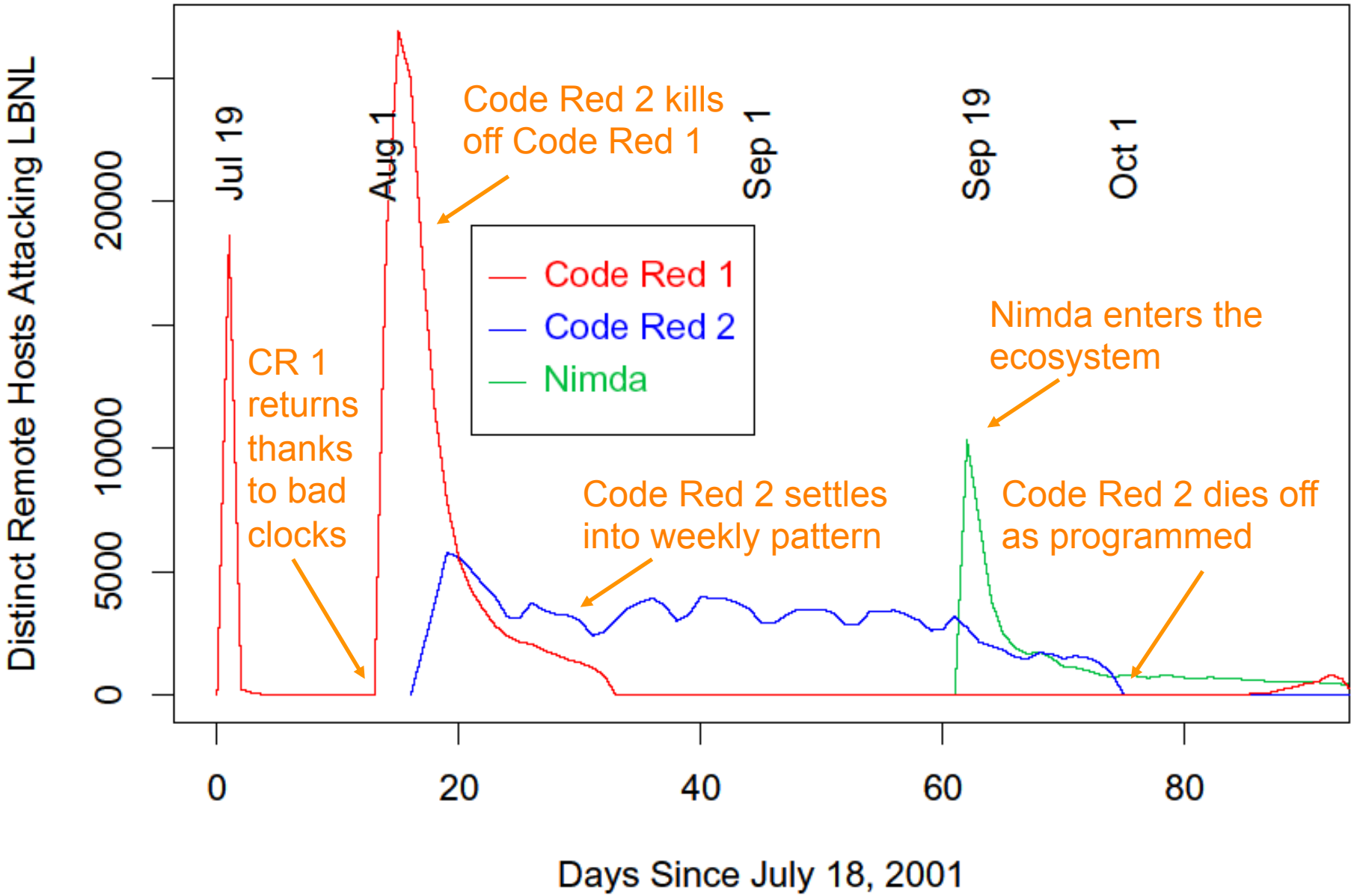
In an intrusion that raises questions about the vulnerability of the nation's computers, a Department of Defense network has been disrupted since Wednesday by a rapidly spreading "virus" program apparently introduced by a computer science student.

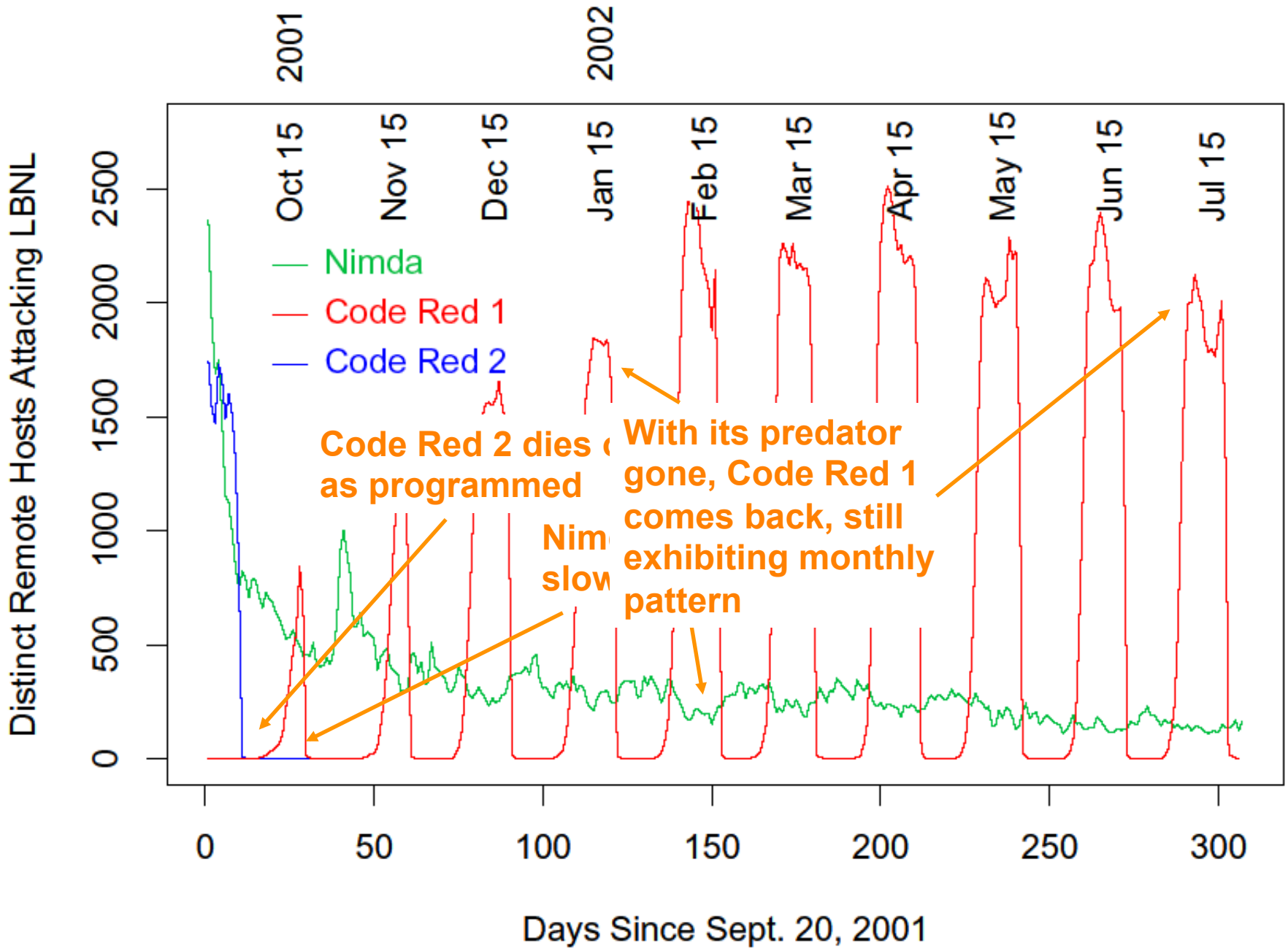
The program reproduced itself through the computer network, making hundreds of copies in each machine it reached, effectively clogging systems linking thousands of military, corporate and university computers around the nation and preventing them from doing additional work. The virus is thought not to have destroyed any files.

By late yesterday afternoon computer experts were calling the virus the largest assault ever


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


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
Code Red 2 settles
into weekly pattern
Nimda enters the
ecosystem
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

i was getting bored by the time I was introduced to the whole 'CDC' proposition.

i'm certainly no expert, and these guys clearly have a decent understanding of their subject, but i'm convinced that the whole thing amounts to a childish attempt to establish a geeky gang of hilariously earnest cyber-heroes.

I would find it very difficult to believe that the top dogs in the network security industries haven't spent a lot more time and money contemplating future exploits (obviously with the somewhat more realistic goal of stiffing businesses for as much money as they can) than this bunch.

I just can't get away from the image of a drooling, pizza-faced ghoul with a cultivated disdain for anyone who can't build a linux kernel, managing to whine nasally over IRC about how no-one really understands how incredibly inevitable a full-scale internet MELT-DOWN is, considering that he's the only man on the planet to have considered the possibility that a Worm could be programmable... uh-huh.

Nothing in the article has any real substance - the 'mathematical models' seem smugly self-serving, the anticipated propogation of a 'Wharhol Worm' being the most indulgent. Who came up with THAT one? It's all approximated, estimated and assumed.
[....]
In a word: unimpressed.

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

$$\frac{dI}{dt} = \beta \frac{IS}{N}$$

$$\frac{dS}{dt} = -\beta \frac{IS}{N}$$

$$\rightarrow \quad \frac{di}{dt} = \beta i(1-i)$$

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