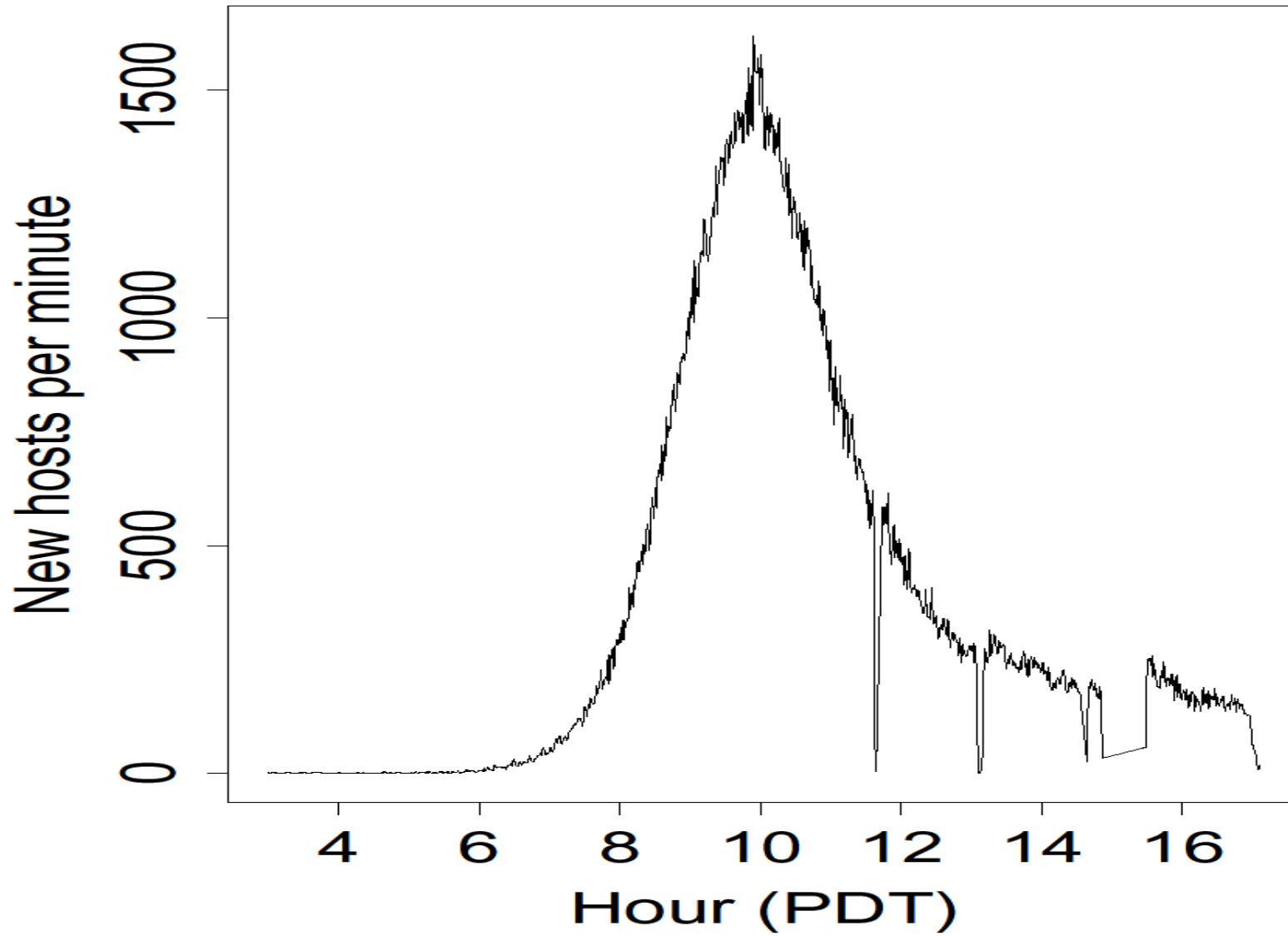
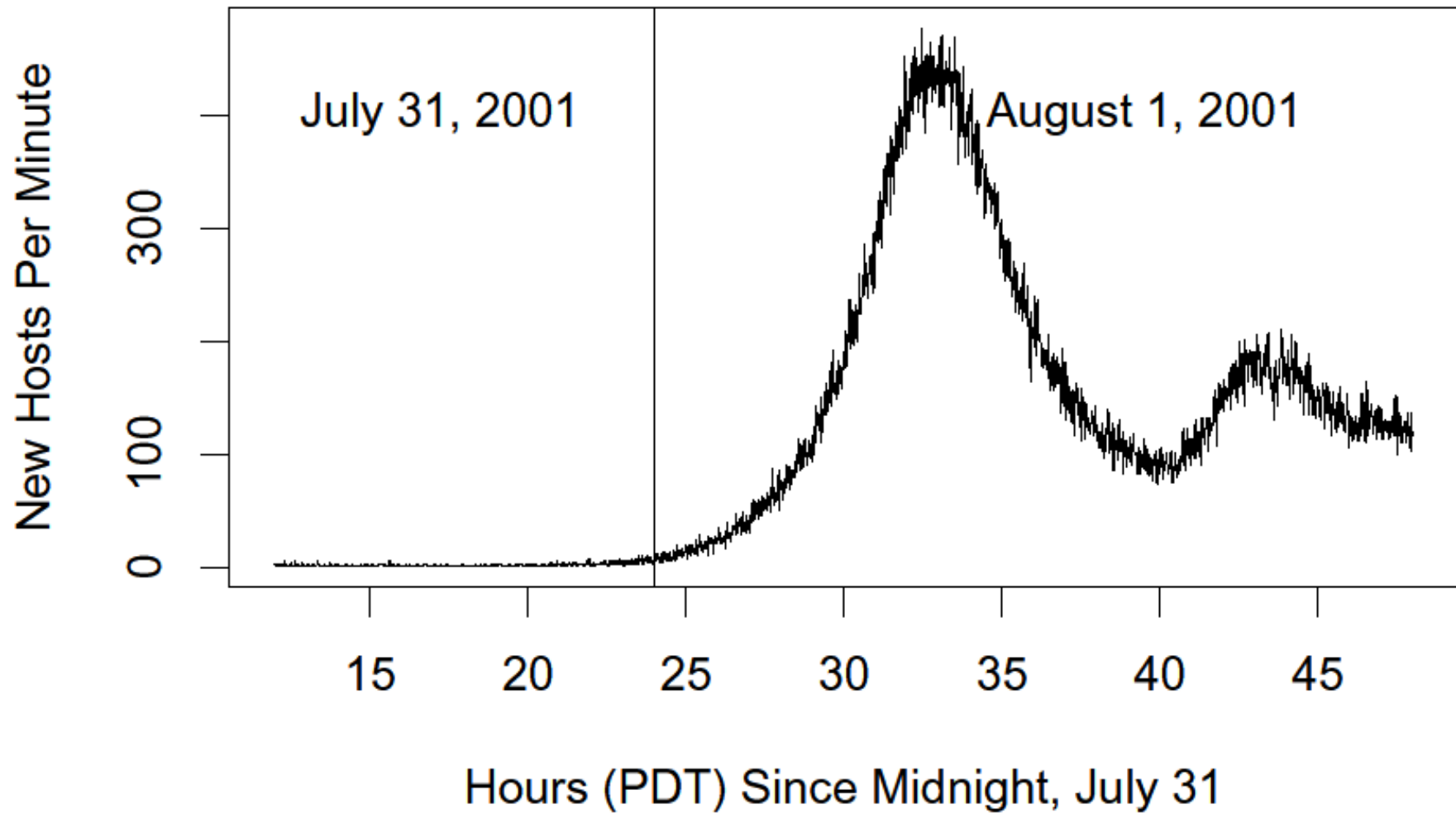


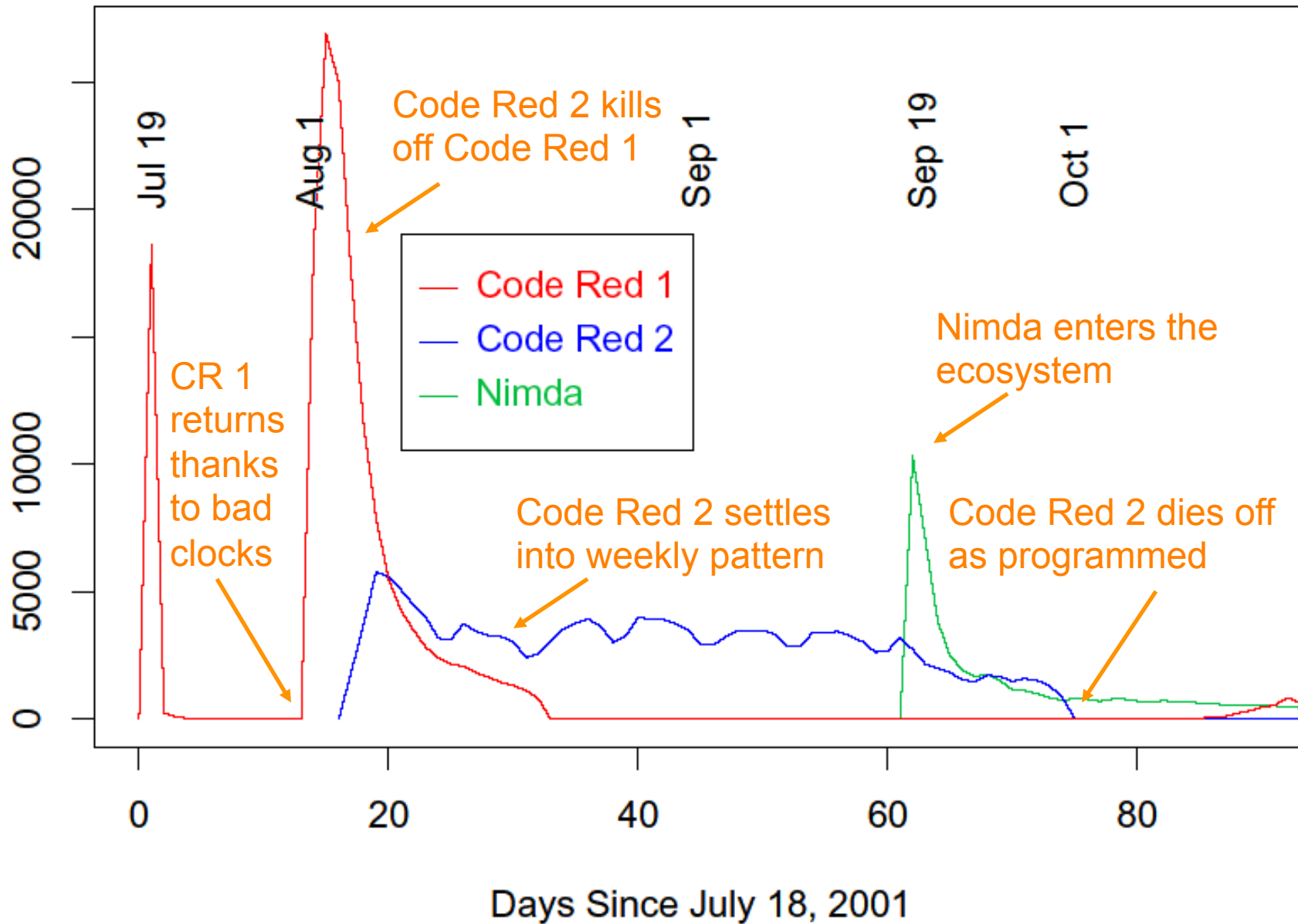
Growth of Code Red Worm



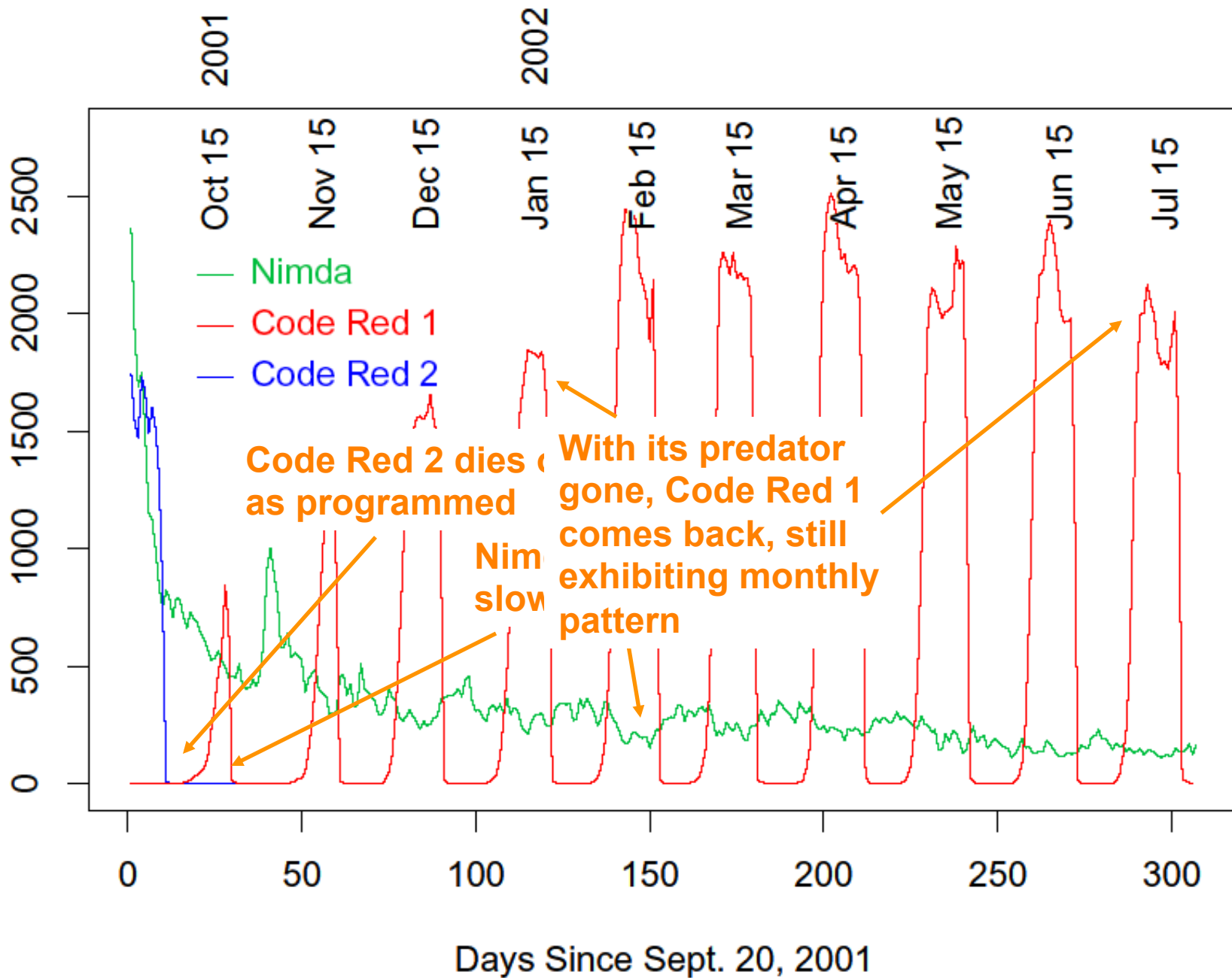
Return of Code Red Worm



Distinct Remote Hosts Attacking LBNL



Distinct Remote Hosts Attacking LBNL



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 propagation 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

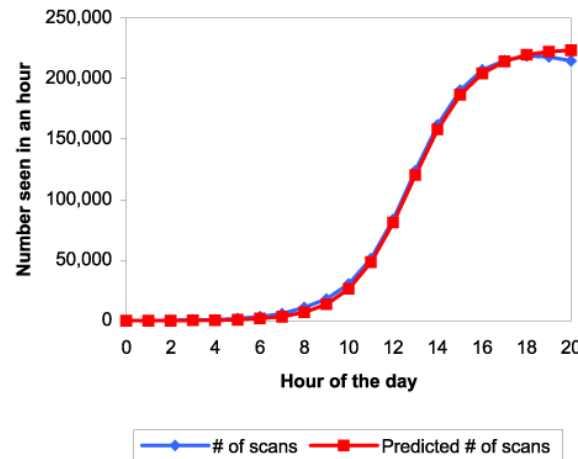
- Often well described as *infectious epidemics*
 - Simplest model: homogeneous random contacts

- 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

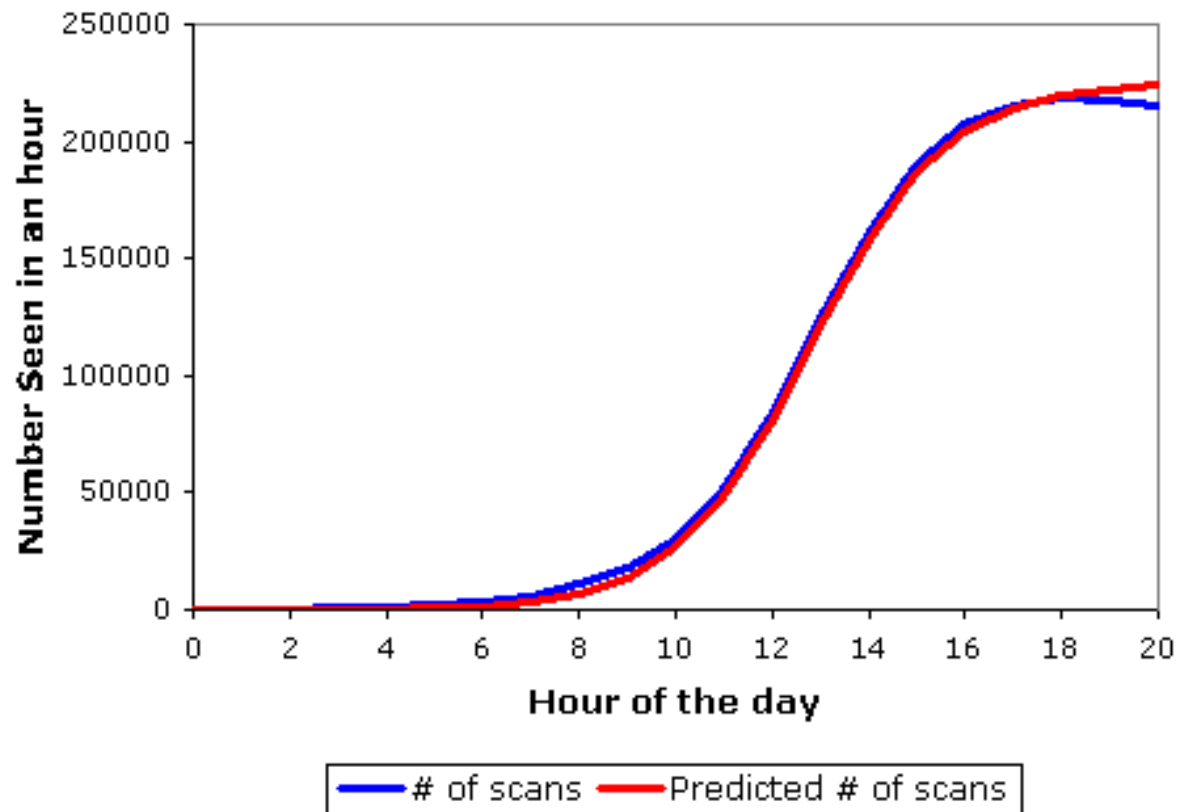
$$\begin{aligned} \frac{dI}{dt} &= \beta \frac{IS}{N} \\ \frac{dS}{dt} &= -\beta \frac{IS}{N} \end{aligned} \rightarrow \frac{di}{dt} = \beta i(1-i)$$

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



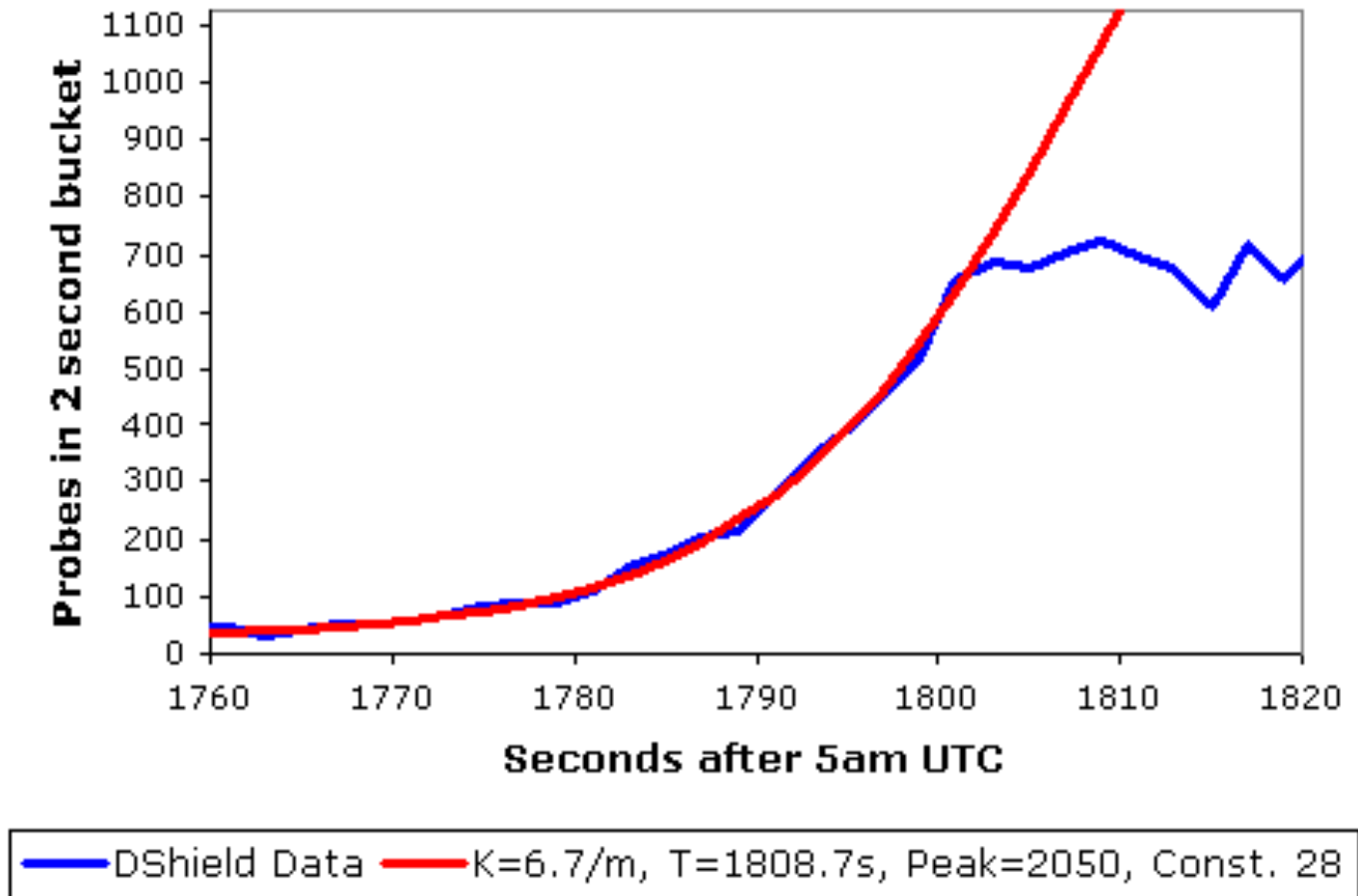
The Usual Logistic Growth

Probes Recorded During Code Red's Reoutbreak

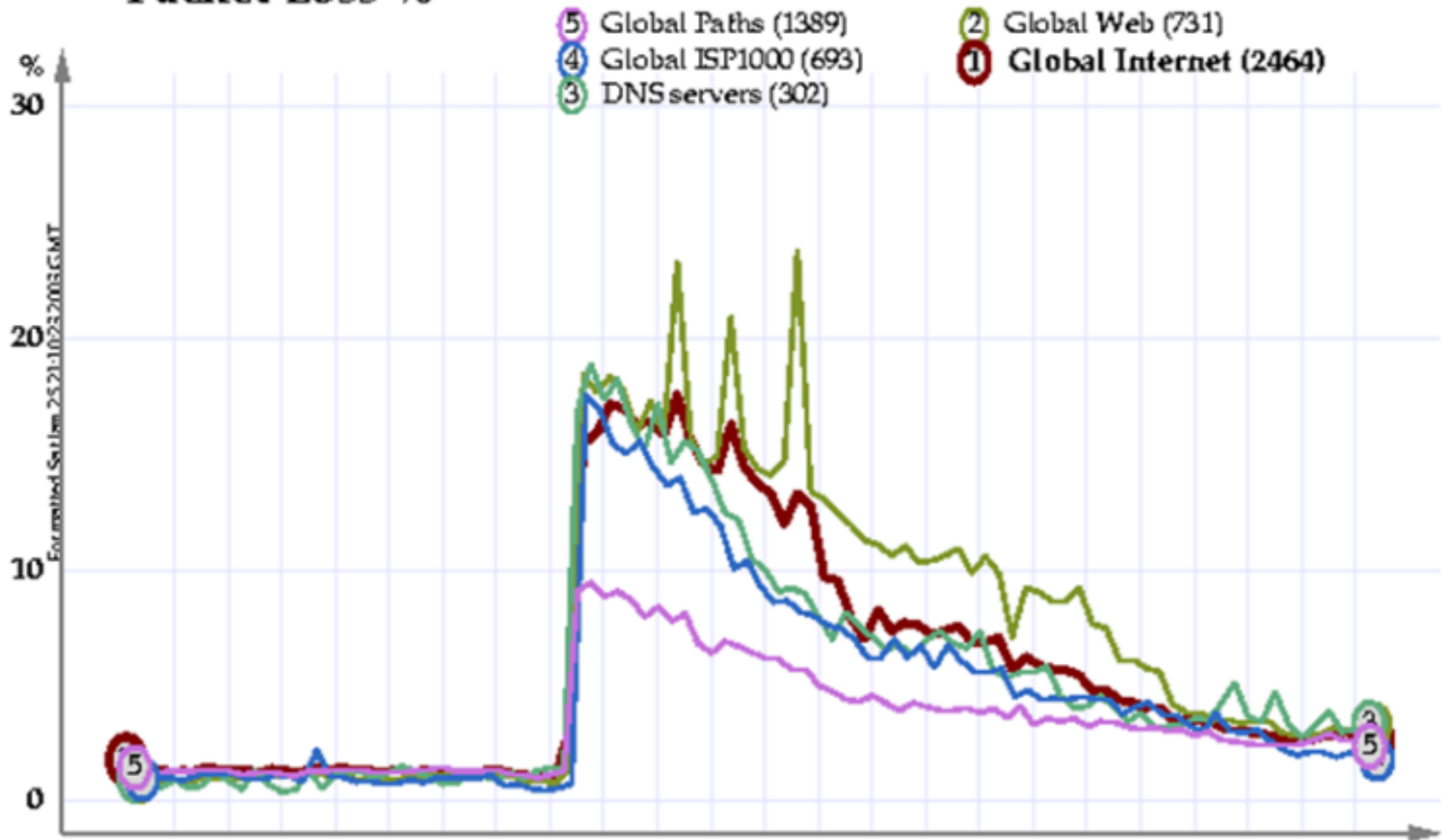


Slammer's *Bandwidth-Limited* Growth

DShield Probe Data



Packet Loss %



Timezone () (c) Copyright 2003 Matrix NetSystems, Inc. www.matrixnetsystems.com

GMT	Jan 24	Jan	02:00	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00
EST	Jan 24	7 PM	9 PM	11 PM	Jan 25	3 AM	5 AM	7 AM	9 AM	11 AM	1 PM	3 PM