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

Emotional Issues Are the 1988 Battleground
Return of Code Red Worm

July 31, 2001

August 1, 2001

New Hosts Per Minute

0 100 300

Hours (PDT) Since Midnight, July 31

0 15 20 25 30 35 40 45
Code Red 2 kills off Code Red 1
Code Red 2 settles into weekly pattern
Nimda enters the ecosystem
Code Red 2 dies off as programmed
CR 1 returns thanks to bad clocks
Code Red 2 settles into weekly pattern
Code Red 2 dies off as programmed.

Nimda hums along, slowly cleaned up.

With its predator gone, Code Red 1 comes back, still exhibiting monthly pattern.
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 $t$
  - $\beta$: contact rate
  - $i(t)$: $I(t)/N$, $s(t)$: $S(t)/N$

\[
\begin{align*}
\frac{dI}{dt} &= \beta \frac{IS}{N} \quad \Rightarrow \quad \frac{di}{dt} = \beta i(1 - i) \\
\frac{dS}{dt} &= -\beta \frac{IS}{N} \\
\end{align*}
\]

\[
i(t) = \frac{e^{\beta(t-T)}}{1 + e^{\beta(t-T)}}
\]
The Usual Logistic Growth

Probes Recorded During Code Red's Reoutbreak

Number Seen in an hour

Hour of the day

- # of scans
- Predicted # of scans
Slammer’s *Bandwidth-Limited* Growth

**DSHIELD Probe Data**

- **Probes in 2 second bucket**
- **Seconds after 5am UTC**

- **DSHIELD Data**
- **K=6.7/m, T=1808.7s, Peak=2050, Const. 28**