Understanding Mutable Internet Pathogens

Or, How I Learned to Stop Worrying and Love Parasitic Behavior

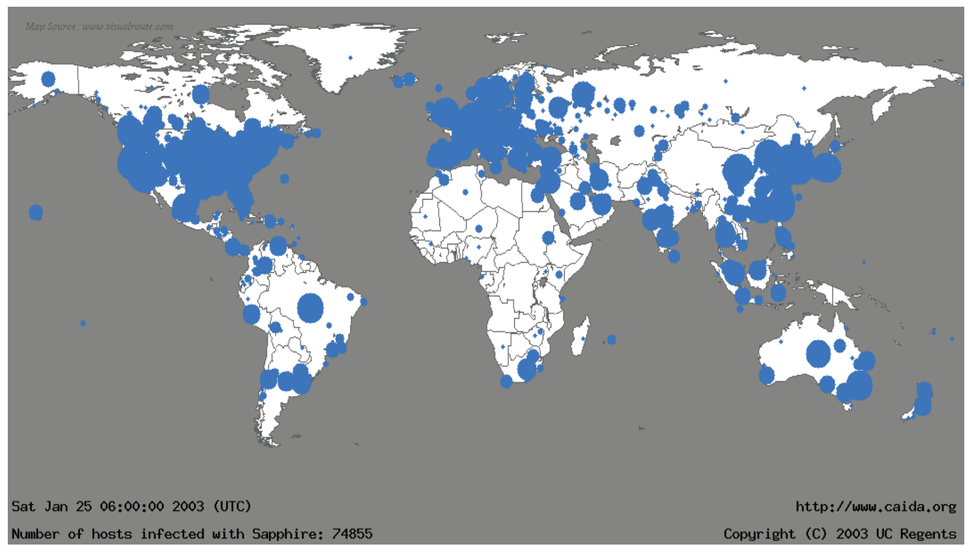
KEVIN BUTLER AND PATRICK MCDANIEL

Internet Worms

The Internet is rife with malware. Malicious worms can spread across the world in a matter of minutes, and their effects are becoming increasingly harmful to national and global infrasctuctures. *Flash worms* can infect huge swaths of machines in minutes or even seconds.

Slammer worm: Hit over 90% of its target systems in under ten minutes, took out Bank of America's ATM system, crashed a 911 system in Bellvue, WA, caused a safety monitoring system at a nuclear plant in Ohio to be disabled by crashing the computer network it relied upon

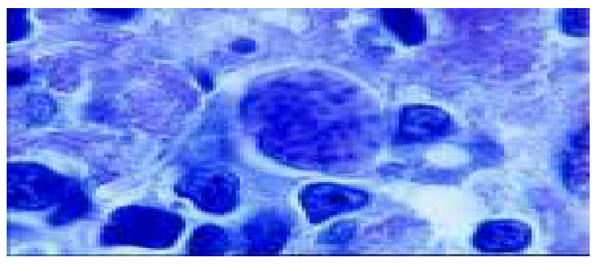
Witty worm: Unlike Slammer which caused problems as a side effect, Witty was designed to be actively malicious, destroying the disk drives of infected systems. Initial targets were systems at US Army bases: a potential cyber-warfare attack.



Within 30 minutes, Slammer had spread completely worldwide.

New Directions in Worm Research

We have seen how damaging flash worms can be, but are they the most dangerous type of Internet pathogen? Consider a *contagion worm*, one that replicates slowly and silently instead. While its immediate impact may not be great, over time it will continue to work undetected by any systems, eventually spreading to take over entire networks and beyond. These worms operate silently, look the same as other traffic, and can learn new methods of transmission. In effect, we have created a new sort of pathogen: the ***Internet parasite.***



Biological parasites can present useful metaphors for thinking about their computer equivalents. Parasites are the most abundant lifeforms on earth, due to their ability to adapt and cloak themselves. T. gondii overrides the behavior of its host for it to do the parasite's bidding, while S. mansoni covers itself with the host's antigens to evade detection.

Lessons learned from biological parasites:

- polymorphic forms
- mutiple attack vectors
- transforming size and shape
- methods of host detection

Evolution

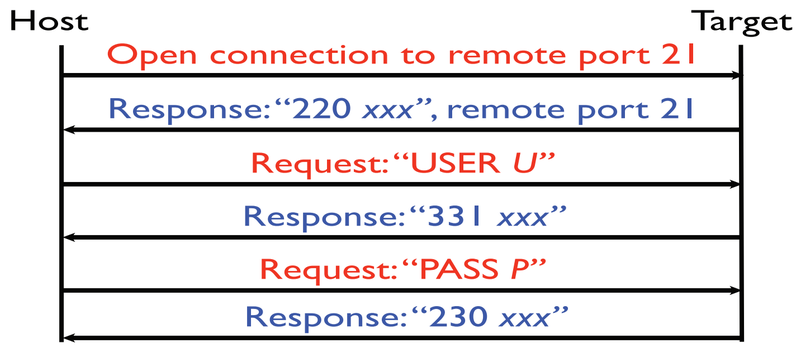
Parasites do not have complex thought patterns to reason how to attack their hosts; their successes are based on evolving mutations across many generations.

Complexity evolves through time!

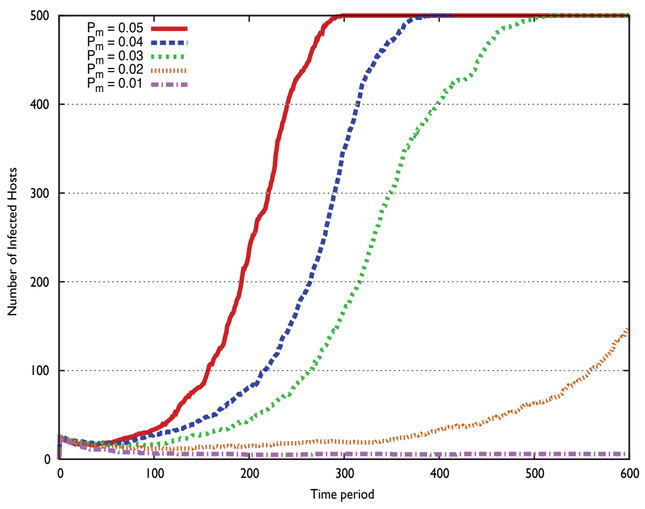
Modeling Computer Parasites

✸ Evade host detection through listening to incoming/outgoing traffic and determine open ports this way.
✸ Infer protocols using a finite state machinebased on observed traffic flows.
✸ Dynamically discoverattack vulnerabilities through automated methods.
✸ Innocuously transmit by using the vulnerabilities to aid transmission to the victom.

This flow diagram shows how FTP can be inferred. An FSM can be created by the parasite based on inference of these flows, and vulnerabilities tested based on fault-injection methods.



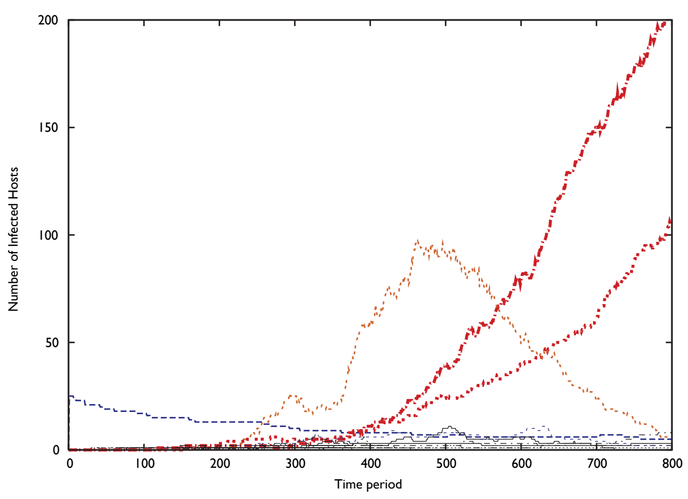
Simulating Propagation



We simulated a 500 node fully connected network using parameters from classical epidemiological work, and varied infection, mutation and innoculation rates.

As the graph on the left shows, the number of infected hosts greatly increases as the mutation rate increases; there is a point of criticality (0.03 in this case) at which point the infections saturate the network.

The graph on the right shows individual mutation strains. Most die out, but a small number survive and infect the entire network.



RESEARCH SUPPORTED BY NSF