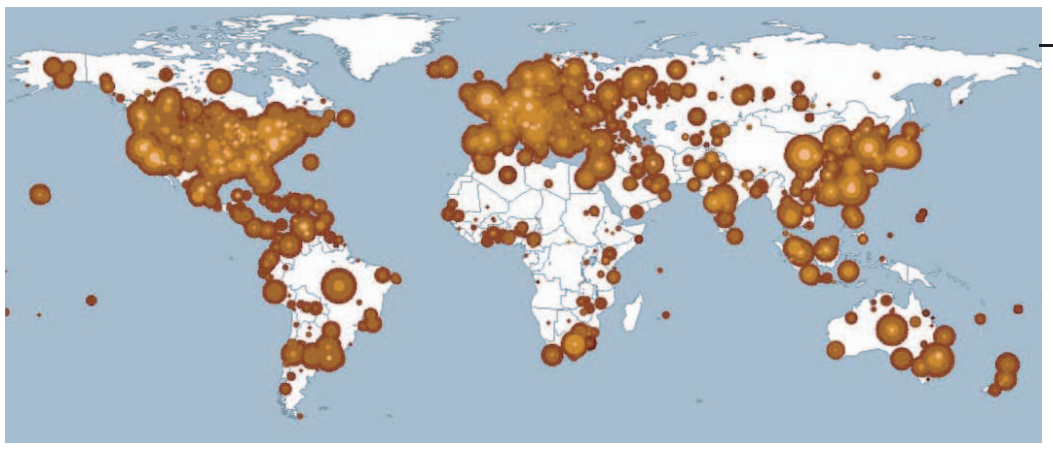
CAIDA Analysis of Malicious Software

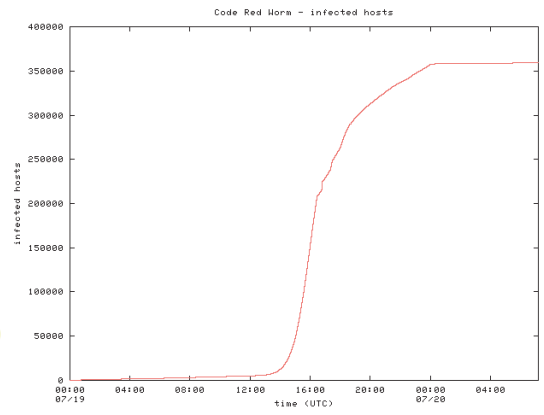
Since 2001, security researchers at CAIDA have measured and analyzed large-scale malicious traffic on the Internet, including distributed denial-of-service (DDOS) attacks and Internet worms. This poster describes the spread and global impact of several variants of malicious software. One of the tools used in these analyses is the UCSD Network Telescope, which consists of a large piece of globally announced IPv4 address space. The telescope contains almost no legitimate hosts, so inbound traffic to nonexistent machines is always anomalous in some way. For more information on CAIDA security research, see http://www.caida.org/research/security/.



Code-Red

http://www.caida.org/analysis/security/code-red/

On July 19, 2001 more than 359,000 computers were infected with the Code-Red (CRv2) Internet worm in less than 14 hours. Code-Red, which infected some versions of Microsoft's IIS webserver, was the first Internet worm in more than a decade to automatically compromise a significant number of computers. A patch to prevent exploit of the IIS vulnerability was available 29 days before Code-Red version 2 began to spread. At the peak of the infection frenzy, more than 2,000 new hosts were infected each minute. 43% of all infected hosts were in the United States, while 11% originated in Korea followed by 5% in China and 4% in Taiwan. The .NET Top Level Domain (TLD) accounted for 19% of all compromised machines, followed by .COM with 14% and .EDU with 2%. We also observed 136 (0.04%) .MIL and 213 (0.05%) .GOV hosts infected by the worm. Summarized data about the spread of the Code-Red worm is available at: http://www.caida.org/data/passive/codered_worms_dataset.xml

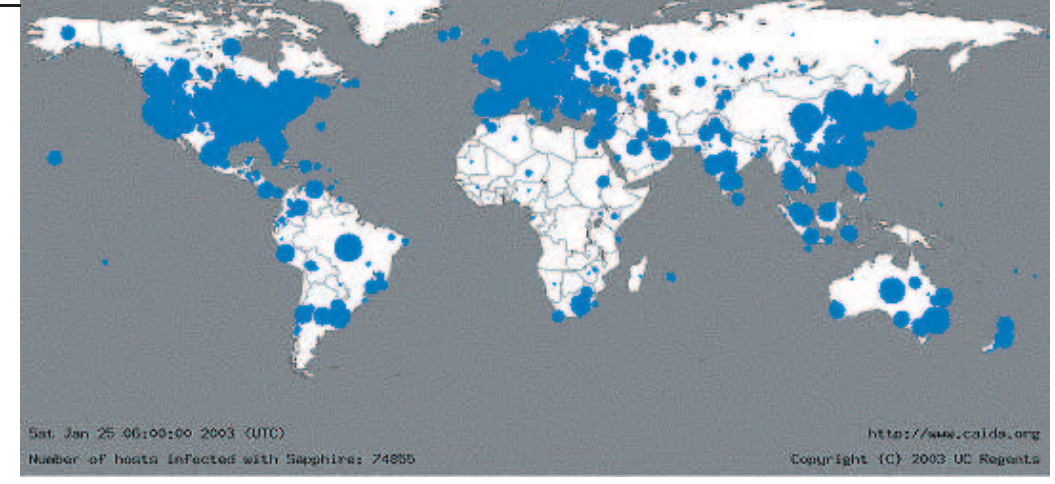


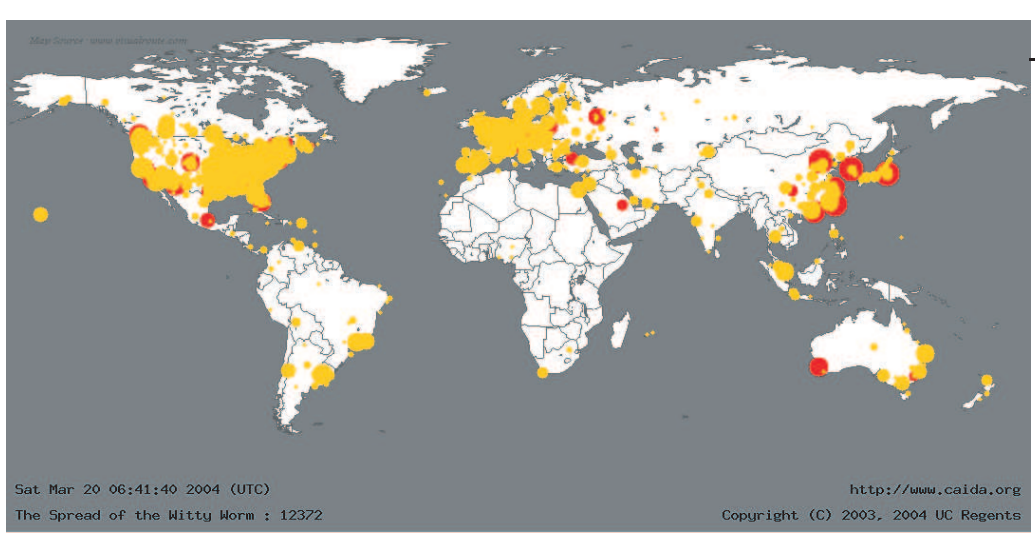
Slammer

http://www.caida.org/analysis/security/sapphire/

Joint work with: Vern Paxson (ICIR & LBNL), Stefan Savage (UCSD CSE), Stuart Staniford (Silicon Defense), and Nicholas Weaver (Silicon Defense & UC Berkeley EECS).

The Slammer worm began to infect hosts slightly before 05:30 UTC on Saturday, January 25. Propagation speed was Slammer's novel feature: in the first minute, the infected population doubled in size every 8.5 (±1) seconds. The worm achieved its full scanning rate (over 55 million scans per second) after approximately three minutes, after which the rate of growth slowed down somewhat because significant portions of the network did not have enough bandwidth to allow it to operate unhindered. Most vulnerable machines were infected within 10-minutes of the worm's release, with at least 74,856 computers infected in the first 30 minutes of worm spread. As with Code-Red, 43% of all infected hosts were in the United States, while 12% originated in South Korea, 6% in china, and 4% in Taiwan. The .NET Top Level Domain (TLD) accounted for 14% of infected hosts, followed by .COM with 11%, .EDU with 3%, and .TW with 1%.





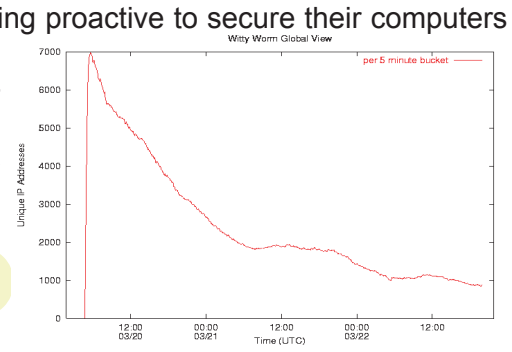
Witty Worm

http://www.caida.org/analysis/security/witty/

On Friday March 19, 2004 at approximately 8:45pm PST the Witty worm began to spread, targeting a buffer overflow vulnerability in several Internet Security Systems (ISS) products. Once the Witty worm infects a computer, it periodically deletes a randomly chosen section of the hard drive, over time rendering the machine unusable.

While the Witty worm is only the latest in a string of self-propagating remote exploits, it distinguishes itself through several interesting features: 1) Witty was the first widely propagated Internet worm to carry a destructive payload. 2) Witty was started in an organized manner with an order of magnitude more ground-zero hosts than any previous worm. 3) Witty represents the shortest known interval between vulnerability disclosure and worm release -- it began to spread the day after the ISS vulnerability was publicized. 4) Witty spread through a host population in which every compromised host was doing something proactive to secure their computers and networks. 5) Witty spread through a population almost an order of magnitude smaller than that of previous worms, demonstrating the viability of worms as an automated mechanism to rapidly compromise machines on the Internet, even in niches without a software monopoly.

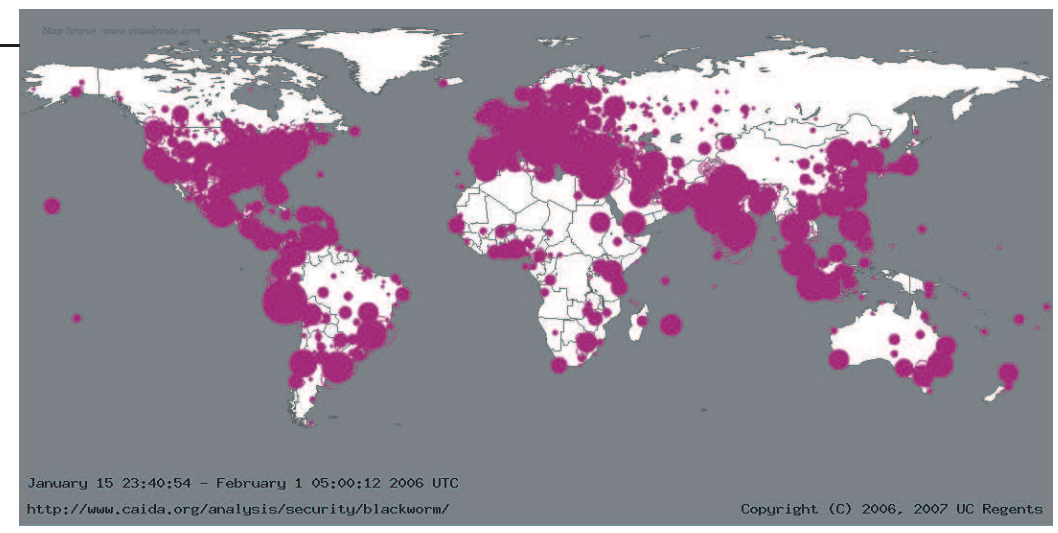
The Witty worm infected a total of approximately 12,000 computers in approximately 45 minutes. 26% of infected hosts were located in the United States, with 7% in the UK, 3% each in Canada, China, and France, and 2% each in Japan, Australia, and Germany. The .NET domain hosted 33% of the infected computers with 20% in .COM, 3% in .FR, and 2% each in .CA, .JP, and .AU. Summarized data about the spread of the Witty Worm is available for general research use. A dataset including trace data is available for academic/non-profit use. For more information, see: http://www.caida.org/data/passive/witty_worm_dataset.xml

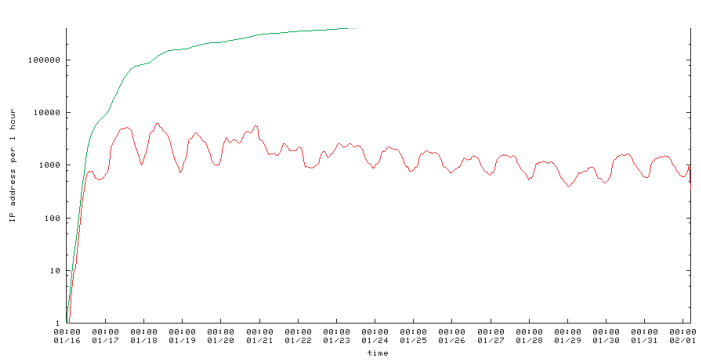


Blackworm/Nyxem

http://www.caida.org/analysis/security/blackworm/

The Nyxem/Blackworm/Blackmal/Kama Sutra/MyWife email virus began to spread approximately Sunday January 15 23:40:54 UTC 2006. The virus contained a malicious payload designed to overwrite files with certain extensions on the 3rd of every month (beginning February 3, 2006). While destructive email viruses are a ubiquitous part of the online environment, Nyxem was relatively rare in that newly infected hosts connect once to a single website, providing a single source of information about the infected population. We analyzed logs from this website to eliminate connections from non-infected computers to achieve a data set containing computers believed to be infected with the virus. We estimate that between 469,507 and 946,835 computers in more than 200 countries were infected by the Nyxem virus between January 15 23:40:54 UTC 2006 and Wednesday February 1 05:00:12 UTC. At least 45,401 of the infected computers were also compromised by other forms of spyware or bot software. Approximately 32% of infected computers were located in India, with 18% in Peru, 8% in Italy, and 6% each in Turkey and the United States. 16% of infected computers were hosted in the .NET domain, with 15% in .PE, 7% in .IT, 5% in .IN, and 4% in .COM.





Research by: Colleen Shannon and David Moore
Cooperative Association for Internet Data Analysis

Poster design: Lisa Hecht

Copyright © 2001 - 2007 UC Regents. All rights reserved.

caida · CCIED · CISCO · LIMELIGHT NETWORKS · U.S. Department of Homeland Security · NSF · DARPA · SDSC San Diego Supercomputer Center · UCSDCSE Computer Science and Engineering · UCSD