

InfoWorld LEAD WITH KNOWLEDGE

Back To Article

August 09, 2002 02:45 PM

'Network telescopes' spy on net attacks
By Stephen Lawson

SAN FRANCISCO - Researchers looking for more accurate information about Internet threats such as worms and DoS (denial-of-service) attacks are experimenting with a technique that looks at the Internet something like the way astronomers look at the universe.

A "network telescope" operated by the Cooperative Association for Internet Data Analysis (CAIDA), in San Diego, has gathered statistics about DoS attacks and the 2001 Code Red and Code Red 2 worm attacks through monitoring of the traffic that hits one part of the Internet.

That technique may produce more accurate information about those kinds of events than is now available, according to David Moore, a technical manager at CAIDA. Moore discussed the technique and results here Thursday at the Usenix Security Symposium.

More accurate information about the size and timing of Internet attacks could aid in understanding such events and their true cost. It might even help insurance companies determine a customer's risk of being hit by one, so they could sell policies that cover the damage, Moore said.

CAIDA monitors traffic directed toward any one of a large block of IP (Internet protocol) addresses at the University of California at San Diego, a block so big that it makes up about 1/256th, or 0.4 percent, of all the world's addresses. The behavior of typical large-scale DoS attacks and worms is almost bound to involve some of those addresses, he said. It has also monitored two smaller blocks of addresses for comparison.

The network telescope works in the following ways:

-- In most DoS attacks, the source address is faked by software that makes it look as if the attack is coming from another IP address. Those fake source addresses are generated more or less randomly, so they are likely to include at least some from the large block that CAIDA monitors. When DoS attack messages hit their target, the victim machine automatically sends packets back to the "source" address. CAIDA looks for those unsolicited responses, or "backscatter" packets, and records patterns.

-- Worms such as Code Red cause infected systems to forward the worm to more or less randomly chosen IP addresses. A widely spread worm is likely to go out to addresses in that large address block roughly at a rate and a time that reflects how it is spreading across the Internet as a whole. CAIDA detects those packets as they arrive and records the patterns.

So far, tracking the spread of worms and determining the severity of DoS attacks from outside the targeted site have been difficult, according to Moore.

A network telescope has some limitations, Moore cautioned. In most cases, it can't track "reflector" DoS attacks because they cause systems to respond to the target.

The bigger the telescope, the better, he said. Smaller telescopes -- ones that monitor a smaller set of addresses -- tend to both underestimate the peak intensity of an attack and detect it later than a bigger telescope, Moore said.

Would-be Internet astronomers who don't have access to a chunk of the Internet as big as CAIDA's can organize distributed telescopes that scan several smaller blocks of addresses, he added. It's best to use a block of addresses that's not heavily used.

The findings CAIDA has gleaned through its Internet telescope have serious implications for Internet security, Moore said. For one thing, they suggest that home and small-office users on DSL (digital subscriber line) and cable modem connections played a big role in spreading Code Red and also are the targets of many DoS attacks.

Monitoring traffic for the first three weeks of February 2001, CAIDA found more than 12,000 DoS attacks against more than 5,000 targets. It estimates 10 percent to 20 percent of those attacks were against home users, some of them going on regularly for weeks. Moore believes these attacks may be vendettas against individual users for postings they made in Internet chat rooms. The pattern of attacks probably hasn't changed significantly since that period, but may have, Moore cautioned.

In addition, many of the systems that were infected and inadvertently helped to spread Code Red and Code Red 2 were on DSL and cable modem accounts, he said. CAIDA determined this by looking at the owner of the block of addresses from which the traffic came.

"These machines are an important aspect of Internet health. There are a lot of machines out there that are not well maintained that can be broken into," Moore said. Home users and most small businesses don't have full-time network administrators to update software and take other steps to maintain security, he explained.

"We're going to have to find solutions to help (non-professional) people manage the security of their boxes," Moore said. Developers could take three key actions to help this occur, he added:

-- make security products easier to use;

-- make security understandable to non-professional users;

-- automate some aspects of security.

Although CAIDA's charts suggest DoS attacks are more frequent during the workday Monday through Friday in any given time zone, they are now a constant reality, Moore said.

"There's (at least) 20 people under attack at all times," Moore said.

ABOUT INFOWORLD | CONTACT US | EMPLOYMENT | PRIVACY

Copyright 2001 InfoWorld Media Group, Inc.