Stephen Lau

The Spinning Cube of Potential Doom

Practically every computer linked to the Internet is constantly being scanned for security vulnerabilities and targeted for attack by viruses, worms, and worse.

Code Red, Nimda, Blaster, Slammer, Netsky, Bagle. Who hasn't heard these names? Their prominence attests to how the field of computer security has changed over the past few years. An image of a lone attacker trying to hack into someone else's computer has been replaced by one of waves of attacks with media-friendly names. This month it's Slammer; next month it's Blaster. Sometimes it seems the entire Internet has unwittingly received a free subscription to the Worm of the Month club.

These media darlings hide a disturbing aspect of today's Internet. Unbeknownst to some of us, practically all systems attached to the Internet are constantly being scanned for vulnerabilities, while the number of attacks keeps increasing. If you think you need to worry about computer security only when the Worm of the Month makes its rounds, consider yourself a security incident waiting to happen.

What is this malicious traffic, and what are its human and software perpetrators trying to do? Most consists of vulnerability scans—the network equivalent of car thieves walking through a parking lot searching for unlocked cars. But unlike the Hollywood image of a loner launching directed attacks, many of these attempts are automated, not targeting any particular system. It's not a new phenomenon either. As the Internet has evolved, so has the volume and sophistication of its malicious traffic.

Most of these scans are reconnaissance for subsequent directed attacks. Others automatically attempt to exploit a system once they discover a potential vulnerability. Some use previously compromised systems to perform their deeds. Still others hijack systems specifically to search for yet other vulnerable systems.

The Spinning Cube of Potential Doom (see the figure here)[1] is an animated visual display of network traffic collected through the Bro Intrusion Detection System.[2] Bro was developed by Vern Paxson of Lawrence Berkeley National Laboratories and the International Computer Science Institute's Center for Internet Research in Berkeley, CA. It monitors network links, searching for traffic that potentially violates a site's access and usage policies.

Although many tools are available for detecting and displaying network traffic and potential security incidents, practically all were developed by network and security professionals for use by other network and security professionals. The Cube displays the overall level of malicious traffic in a fashion that is easily understood, even by those lacking expertise in computer security and networking technology.

The Cube leverages Bro's ability to log all instances of completed and attempted TCP connections, displaying the information within a visually appealing 3D cube a user spins at will. Each axis represents a different component of a TCP connection: X is the local IP address space; Z is the global IP addresses space; and Y is the port numbers used in connections to locate services and coordinate communication (such as 22 for SSH and 80 for HTTP).

TCP connections, both attempted and successful, are displayed as single points for each connection. Successful TCP connections are shown as white dots. Incomplete TCP connections are shown as colored dots. Incomplete connections are attempts to communicate with nonexistent systems or systems no longer

[1] www.nersc.gov/security/TheSpinningCube.html
[2] www-nrg.ee.lbl.gov/bro.html

LISA HANEY

Viewpoint

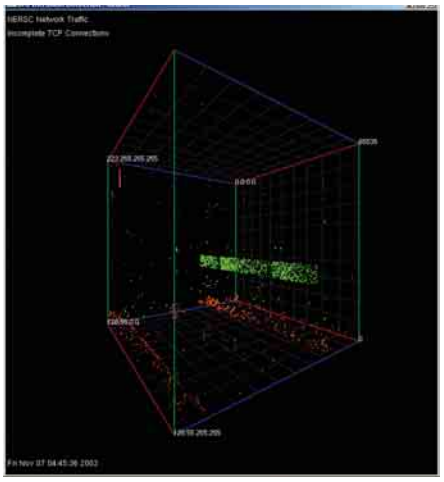
listening on that particular port number. The Cube colors incomplete connections using a rainbow color map with color varying by port number; color mapping assists viewers in locating the point in 3D space.

Practically all of the colored dots can be considered malicious traffic searching for potentially vulnerable systems. A large number seen at the low end of the port range (0 to 1,024) represents efforts to locate well-known services (such as HTTP and SSH). Although some of these attempted connections are explained by misconfigured applications or hosts that have inadvertently crashed and no longer listen for connections, the patterns emerging from the data collected by Bro shows there are few false positives. Further evidence that false positives are minimal is seen in data collected from sparsely allocated networks. Regardless of the number of hosts on a network, similar types and levels of potentially malicious traffic are present.

One of the more interesting findings as revealed by Bro and displayed by the Cube, surprising even to those with expertise in computer security, is the visual patterns emerging from the data that are readily discernable just by glancing at the Cube. Port scans appear as linear lines; the vertical ones represent scans directed at a particular host searching for a listening port; and the horizontal ones are directed at the entire local address space on a particular port.

Aside from these linear scans, other forms emerging from the data are somewhat unexpected. We dubbed one the "barber pole" because its appearance is so much like the helical striping on traditional barber poles. They vary their port number and IP addresses in an attempt to elude detectors. Though they may evade detectors, they stand out when visualized this way. A notable feature is the variation in the slopes of the lines in the patterns, implying that some malicious scans either skip addresses and port numbers or scan more than one port on a particular address.

We dubbed another type of scan the "lawn mower"; blatant and thorough, it covers a range of contiguous ports while simultaneously marching across the entire local address space. Some lawn mowers are quick, occurring in a few seconds; others play out over the course of minutes.



The Cube displays network traffic entering and leaving a site, revealing graphical patterns of potentially malicious traffic.

The Cube was publicly shown for the first time at SC03 in Phoenix in 2003, an annual conference on high-performance computing and networking. The Cube showed network traffic captured through a Bro system monitoring SCinet, the conference's own high-performance network with available bandwidth of more than 30Gbps, or the equivalent of being able to transfer six full DVDs per second.

Attendees expressed surprise at the volume of potentially malicious traffic revealed to be coursing through the Internet. Most enjoyed watching the display, often mesmerized by the amount of traffic being detected. Many were curious as to what portion of the data represented attempts against their own systems and wondered why they had never noticed it themselves.

Though the Cube is a work in progress, its main goal of raising awareness has already been achieved. The most promising comments came from those conference attendees, who, after pondering the Cube, declared that they would now make sure their systems were kept up to date with the latest security patches.

The field of computer security has been likened to an arms race, with each side developing new defenses as quickly as the other develops new attacks. Computer users need to be computer-security aware all the time, not just during media-grabbing attacks. Hopefully, the Cube will help teach the unwary and the clueless, as well as the experts, that the Internet has become a hostile place indeed. C

Stephen Lau (slau@lbl.gov) is a computer security analyst at the National Energy Research Scientific Computing Center at Lawrence Berkeley National Laboratories in Berkeley, CA.