The Spinning Cube of Potential Doom

Stephen Lau - slau@lbl.gov
Lawrence Berkeley National Labs / NERSC
May 27, 2015

Code Red, Nimda, Blaster, Slammer. It's rare to have not heard of these names regardless of your familiarity with computers. Their presence in the media is an example of how the field of computer security has changed over the past few years. The former image of an attacker sitting in the dark attempting to hack into a computer has been replaced by the image of waves of attacks with media friendly names. This month it's Slammer, next month it's Blaster. Sometimes it appears as though the entire Internet has unwittingly received a subscription to a "Worm of the Month" club.

Unfortunately, these media darlings of computer security hide a disturbing reality of today's Internet. Unbeknownst to most people, the majority of systems attached to the Internet are being scanned for vulnerabilities *all* the time and these attacks are increasing in number and becoming more numerous. If you think you only need to worry about computer security whenever the Worm of the Month starts to make its rounds on the airwaves and news websites, you're a computer security incident waiting to happen.

So what is this malicious traffic on the Internet and what are they trying to do? The majority of this traffic consists of vulnerability scans. They are the network equivalent of car thieves walking through parking lots searching for unlocked cars. But unlike the Hollywood image of a lone attacker launching directed attacks, many of these attempts are automated and are not directly targeted at any particular system. It's not a new phenomenon either. As the Internet has evolved so has the underlying level and type of continual malicious traffic.

The majority of these scans are used for reconnaissance for subsequent directed attacks. Others will automatically attempt an exploit against a system once a potential vulnerability is discovered. Some will use previously compromised systems to perform their dirty deeds; others will hijack a system specifically to search for other vulnerable systems.

The "Spinning Cube of Potential Doom" [1] was developed in an effort to increase awareness of the level of malicious traffic on the Internet. The Cube is a visual display of network traffic collected using the Bro Intrusion Detection System (IDS) [2]. Bro, developed by Vern Paxson of Lawrence Berkeley National Labs and ICIR, monitors network links, searching for traffic that potentially violates a site's access and usage policies.

Although there are many tools available for displaying network traffic and potential security incidents, the vast majority of these tools are developed by network and security professionals for network and security professionals. The Cube attempts to display the overall level of malicious traffic in a fashion that can be easily understood by those without a computer security or networking background.

The Cube leverages Bro's capability to log all instances of completed and attempted TCP connections, displaying this information within a three dimensional cube. Each axis represents a different component of a TCP connection. The 'X' axis represents the local IP address space. The 'Z' axis represents the global IP addresses space. The 'Y' axis represents the port number. Port numbers are used in connections to locate services and coordinate communication (i.e. 22 for ssh and 80 for http).

TCP connections, both attempted and successful, are displayed as single points for each connection. The successful connections (SYN/FIN) are shown as white dots. Incomplete TCP connections are displayed as colored dots. Incomplete connections are either attempts to communicate with non existent systems or systems that are not listening on that particular port number, i.e. SYN/RST or SYN with no response. The incomplete connections are colored using a rainbow colormap with the color varying by port number. This color mapping was used to assist the viewer in locating the point in 3-space.

The vast majority of colored dots can be considered to be malicious traffic searching for potentially vulnerable systems. A high number of connection attempts can be seen at the low end of the port range (0-1024), representing attempts to locate enabled well-known services (i.e. http, ssh, etc). Although some of these attempted connections can be explained by misconfigured applications or hosts that have inadvertently crashed and are no longer listening for connections, the patterns that emerge from the data shows that these "false positives" are most likely in the minority.

Further evidence that these false positives are low in number can be 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, even surprising to those with backgrounds in computer security, are the visual patterns that emerge from the data. Various distinct patterns are easily discernable. *Port scans* appear as linear lines where vertical lines represent scans directed at a particular host searching for any listening port and horizontal lines being scans directed at the entire local address space on a particular port. Aside from these linear scans, other forms emerge from the data that are somewhat unexpected.

A prevalent scan pattern was dubbed "*Barber pole*" because its appearance is similar to the striping on barber poles. These scans vary their port number and IP addresses in an attempt to elude detectors. Although they may be capable of evading detectors, they stand out when visualized in this way. A notable feature of these scans is that the slopes of the lines vary. This implies that some of these tools either skip addresses and port numbers or scan more than one port on a particular address.

Another type of scan that was detected was dubbed a "*Lawnmower*" scan. These scans are quite noisy in that they scan a wide range of contiguous ports while simultaneously marching across the entire local address space. Some of these scans are quite rapid,

occurring within a few seconds. Others take a more leisurely time, ranging on the order of minutes.

The Cube was initially displayed at the SC03 conference, an annual conference on high performance computing and networking.. The Cube displayed network traffic captured using a Bro system monitoring SCinet, the conference high performance network.

The Cube received much interest from attendees with the most prevalent comment being surprise at the amount of potentially malicious traffic on the Internet. Overall, most people enjoyed watching the display and were mesmerized by the continual amount of traffic detected. Many attendees were curious as to what portion of the data represented attempts against their systems and expressed surprised that they had not noticed it themselves.

Although the Cube is still a work in progress, I believe that its main goal of raising awareness has been achieved. The most promising comments have occurred from those who have stated that they are going to make sure their systems are kept up to date with the latest security patches after seeing the Cube.

The field of computer security has been likened to an arms race, with each side developing new defenses as rapidly as the other is developing new attacks. Computer users need to be computer security aware all the time not just when media grabbing attacks are present. Hopefully the Cube will raise the awareness that the Internet has truly become a hostile place.

References

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