



## QVISION™ Helps Customers Prevent Downtime from MSBlaster Worm

*Through early detection QVISION alerted its users to MSBlaster and helped prevent significant downtime.*

### Blaster at-a-glance:

- Most serious worm since Slammer Worm in January 2003
- Exploits a flaw in most current versions of Microsoft's Windows operating system
- Spread through port 135
- Subsequent coordinated attack on MS update site
- Many users had failed to download available MS patch

*“QVISION users realized the problem immediately. They were first alerted by a rapid increase of inbound connections to port 135. If machines in the client's network were infected, a secondary alert triggered as the infected machines attempted to infect new hosts. A quick drill down using QVISION allowed the clients to find the infected machines and take appropriate actions.”*

Chris Newton, Chief Architect for Q1 Labs



### The Situation

A new study shows that one in every three people in the United States has been affected by a virus or hacker within the last two years. The most recent with a wide-spread impact has been the MSBlaster worm. The virus-like infection, dubbed *Blaster*, or *Lovsan* worm, first appeared on the Internet early in the afternoon Eastern time August 11 and quickly gained momentum. Officials at the CERT Coordination Center estimated that the number of infected machines quickly reached hundreds of thousands making it the most serious since the appearance of the SQL Slammer worm in January, 2003.

The worm exploits the RPC DCOM (Distributed Component Object Model) vulnerability in all of the current versions of Windows, except ME. The worm scans the Internet and attempts to connect to TCP port 135. After establishing a connection, Blaster spawns a remote shell on port 4444 and then uses TFTP (Trivial File Transfer Protocol) to download the actual binary containing the worm. The worm is self-extracting and immediately begins scanning for other machines to infect.

Although Microsoft posted a software patch to fix the flaw July 16, many users failed to download it, leaving them vulnerable. Security experts expressed concern because vulnerable systems can be compromised without any interaction from a user. A large number of the compromised machines were those of home users who weren't even aware of it. And in this case it wasn't as easy as downloading a patch, because once infected users couldn't get enough bandwidth to get online and get the patch.

Experts were also concerned about a denial of service attack that the worm was programmed to launch against Microsoft's automated Windows update Website starting August 16. Microsoft, however, thwarted the worm by making drastic changes in their Internet set-up, changing the operations of their main servers, and by surrendering windowsupdate.com. So in this sense, the worm accomplished what it wanted. Windowsupdate.com will probably never return. This probably was an easy decision for Microsoft, as windowsupdate.com was not used much. The official address for Microsoft's Windows Update Service is windowsupdate.microsoft.com.

### The Solution

A flaw in the worm's code caused machines running Windows XP to crash and reboot, temporarily taking the host offline and tipping off the machine's owner. The resulting slowdown was widespread and especially noticeable to those attempting to use the Internet from a large business network.

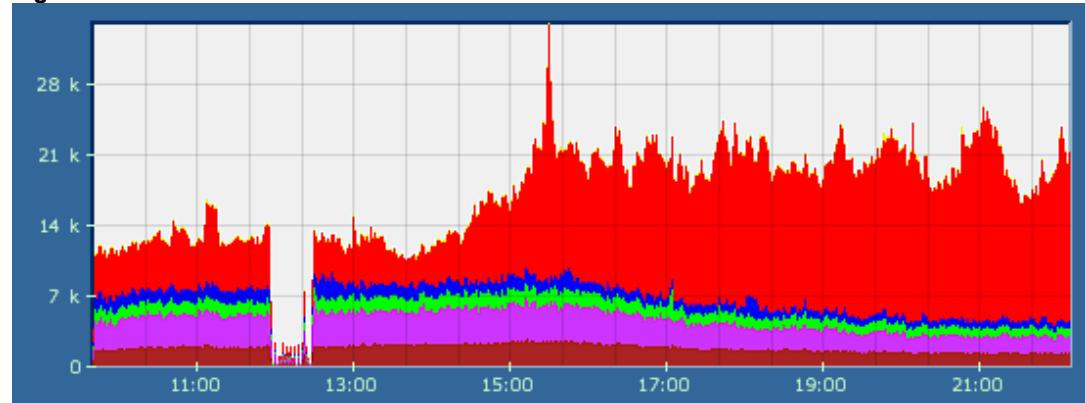
Administrators running QVISION noticed a significant increase in the numbers of hosts talking on the network, indicating they'd been infected by the Blaster. “QVISION users realized the problem immediately,” said Sandy Bird, Chief Technology Officer of Q1 Labs “They were first alerted by a rapid increase of inbound connections to port 135. If machines in the client's network were then infected, a secondary alert triggered as the infected machines attempted to infect new hosts. A



1.877.471.5227  
 info@q1labs.com  
 www.q1labs.com

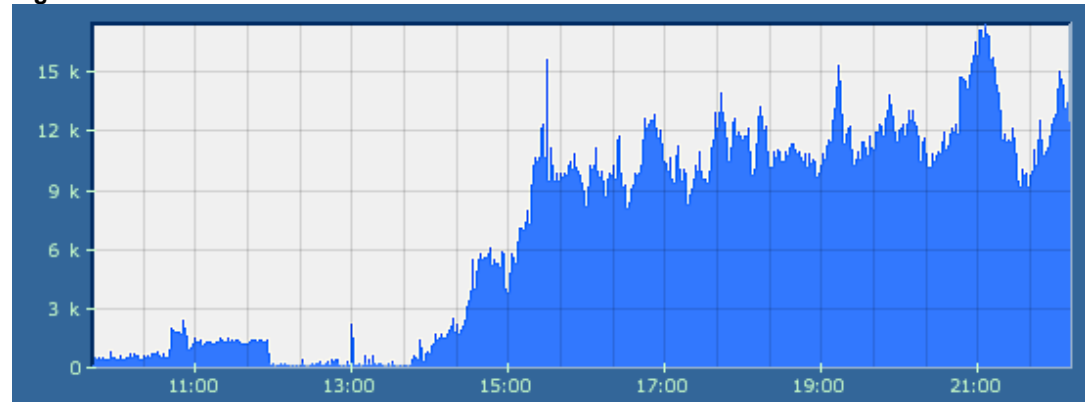
quick drill down using QVISION allowed the clients to find the infected machines and take appropriate actions. Administrators must load the Microsoft patch and prevent immediate re-infection by blocking the known ports.”

Figure 1



From a network running QVISION, these screen shots display the evolution of the “Blaster” virus. Figure 1 displays: 12 hours of Server Message Blocking of Microsoft RPC port 135, counted by the number of local hosts being talked to, a couple hundred every 30 seconds. It is now over 10,000 hosts every 30 seconds and has hit peaks higher than 16,000 hosts per 30 seconds.

Figure 2



Showing: 12 hours in flows increasing significantly

As network administrators know, it’s difficult to monitor where the patch has been applied in a network. QVISION provides an encompassing view of the network. It’s a tool that quickly locates areas of concern.

The Blaster code is small and can be quickly removed using tools from antivirus vendors. Manual removal instructions are available as a link from the ISS Web page at [www.iss.net](http://www.iss.net). For users who are unable to download the patch from Microsoft, CERT recommends an alternative. Physically disconnect the infected machine from the Internet or network. Then, delete the running copy of *msblast.exe* in the Task Manager utility. Users should then disable DCOM and reconnect to the Internet and download the patch. Instructions for disabling DCOM are available at Microsoft’s [Knowledge Base Web site](#)

Users should patch their systems before removing Blaster to prevent re-infection from the worm, and security experts also recommend installing firewall, antivirus, and QVISION for a defense in depth solution to prevent future attacks.

