



Slammer Worm at-a-glance:

- Infected copies of Microsoft SQL Server and ASDE 2000
- Spread through port 1434
- Infected more than 90 percent of vulnerable computers within 10 minutes
- Available patch could have prevented vulnerability but often wasn't applied

The SQL Slammer Worm "doubled in sized every 8.5 seconds . . . and reached the full rate at which it was scanning for vulnerable computers . . . after about three minutes."

-- From a report by the Cooperative Association for Internet Data Analysis (CAIDA)



How QVISION™ Slammed the SQL Slammer Worm

QVISION helped businesses, academic institutions, and government agencies diminish the effects of the SQL Slammer Worm.

The Situation

Worm attacks spread rapidly over networks of all types by first hitting one vulnerable machine, then using it to scan for and infect other vulnerable systems. As a result, worms can propagate across the Internet on an exponential basis. The magnitude of the vulnerability of global networks became clear in the early morning hours of January 25, 2003, when the SQL Slammer Worm infected more than 90 percent of vulnerable computers within 10 minutes.

The SQL Slammer Worm infected copies of Microsoft SQL Server and MSDE 2000 (Microsoft SQL Server Desktop Engine) on computers that were accessible via the Internet. This worm did not spread through an e-mail attachment, but through Internet port 1434 (the SQL monitor port). The worm exploited vulnerability in the SQL Server indexing service, and caused the execution of arbitrary code on the SQL Server computer.

The worm produced massive amounts of Internet traffic and resulted in dramatic Internet slow-downs. Many small businesses had no access to the Internet. ATM machines were affected at several large banks, 911 service was unavailable in a large US city, and telecommunications on the Asian continent were disrupted for days.

In July 2002, Microsoft released a patch to reconstitute the software vulnerability that the SQL Slammer. But, six months later, many systems were left unpatched.

The Slammer Worm either had a flaw in its design or the developer chose not to include additional code this time which limited the overall damage to the Internet. This variant did not carry a malicious payload. It did not attack more widespread areas of vulnerability, and it did not target a more complete set of system services. If it had, the effects to the Internet would have been even more dramatic and would have severely impacted business globally.

The Solution

As Internet providers around the globe were flooded with traffic from the Slammer Worm, enterprises using QVISION were alerted at a very early stage of the potential threat. As a result, they were able to quickly identify the suspicious activity and were able to respond rapidly with appropriate measures, preventing damage to their networks.

With QVISION, system administrators can set up alerts for activity that is "unusual" to their network. They are notified by phone, e-mail, or pager when any alert threshold has been reached or broken. Since QVISION is web-based, administrators can connect remotely to monitor what's going on.

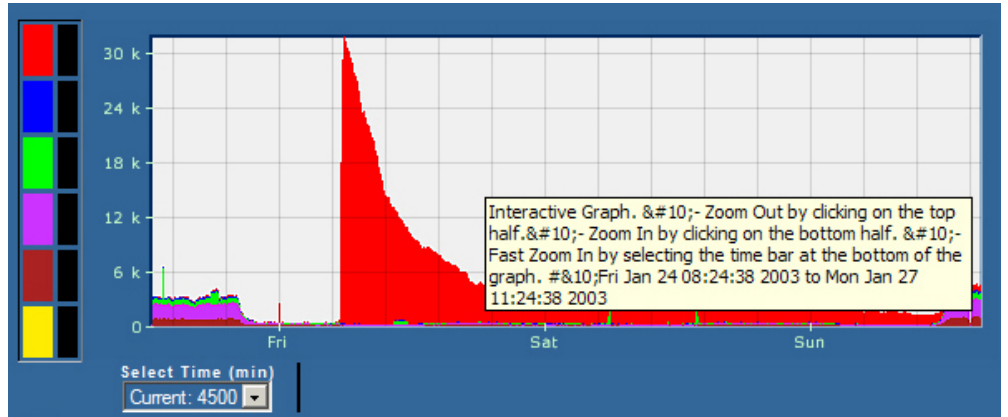
Government Agency

System administrators for a government agency using QVISION set an alert for unusual inbound activity. The inbound flow jumped suddenly to 18,000 communication requests, surpassing the threshold by 800% in a matter of minutes, and then spiked to 30,000. Because of the unusual behavior and volume of the flows, administrators knew that worm-like activity was occurring on a massive scale.



“If someone had taken the Slammer Worm code, changed it to use one of the known web server exploits, and added a hostile payload that deletes content from those infected web servers then a third of the Internet would be adversely impacted in under five minutes.”

Chris Newton
Chief Architect,
Q1 Labs



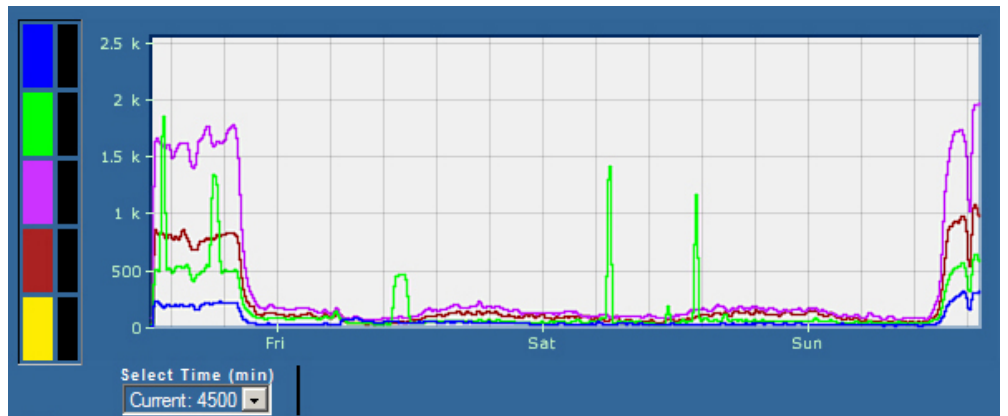
The graph shows a huge spike in inbound only flows. Shows the number of inbound communication requests that go unanswered (the red spike).

The next step was to drill down through the different views associated with the same traffic available within QVISION and determine where the activity was coming from, where it was going, and what machines were being targeted.

When the administrators viewed the Local and Remote Hosts, and the Geographic View, they quickly identified that the majority of the traffic was coming from North America and Asia.

An experienced administrator quickly concluded that it was a worm and that the overall potential impact was significant. From the spike on the network view, they determined that it was targeting every machine on their local network in an attempt to find a vulnerable system.

When the administrator adjusted the view to focus on outbound traffic, he discovered that the systems were not responding to the inbound threat. The lack of activity, as shown by the absence of spikes in the blue line, determines that there is minimal to normal outbound traffic. The network has not been compromised, and the firewall is working.



By observing the spike in outbound-only flows (blue), the user can quickly see that no local systems have been compromised

Because they were alerted of the potential threat so quickly, the system administrators were able to identify the source of the problem and immediately implement corrective measures. In addition, they verified that their firewall was protecting their network as it needed to. Using QVISION they are able to collect valuable data from the firewall and routers on perimeter activity.

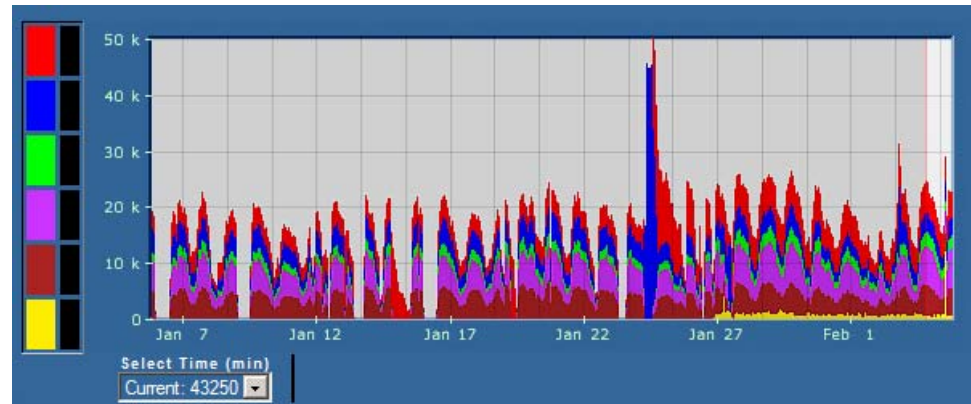




Academic Institution

The University of New Brunswick (UNB), with its large network of thousands of users, also received an alert on unusual activity. Though the university had no primary servers running SQL Server software, a researcher had installed SQL Server on his machine for his own purposes and did not install the patch.

The university's system administrators drilled down to find and quickly pinpoint systems that had been compromised.



The blue on the graph represents outbound traffic, and in this case, the activity indicates compromised outbound traffic. Where the spike stops, the system was shut down.

It was discovered that four machines at UNB were infected with the worm, and they were spewing data across the LAN and across internal connections. The administrators used QVISION to discover the IP addresses of the infected machines. They worked their way through the network to disrupt the connections to the infected machines.

They remotely disabled the ports on these infected machines, restoring the network to smooth and efficient function. To prevent re-infection by the SQL Slammer worm, the administrators set up blocks against the worm in routers, gateways and firewalls. The action the system administrators took in routing out the SQL Slammer worm on the UNB network required just under an hour of their time.

The Result

The Slammer Worm set a precedent in that its impact was more obvious to the public – ATMs weren't working, planes weren't flying on schedule, communications were down. The lessons learned: Internet security affects everyone. You can't prevent all threats or attacks, and no network is completely impenetrable.

The best defense against worms like the SQL Slammer is early detection, intelligent alert, rapid analysis, and immediate, corrective action preventing the threat from being successful. While many system administrators were frantically scanning logs from firewall and Intrusion Detection systems or the voluminous data gathered by sniffers, QVISION customers were able to quickly pinpoint the source of the traffic and resolve the situation with minimal to no down time on their system.

