

supplied by Phoenix Datacom  
01296 397711  
info@phoenixdatacom.com  
www.phoenixdatacom.com



## Worms & Viruses: Flow-Based Network Security

APP NOTE

HOW DO YOU DEFEND THE NETWORK AGAINST A NEW WORM OR VIRUS? HOW CAN YOU RAPIDLY IDENTIFY ANOMALOUS BEHAVIOR THAT INDICATES A NETWORK SECURITY BREACH? HOW DO YOU IDENTIFY AND ISOLATE INFECTED SYSTEMS? WHICH USERS, APPLICATIONS, OR SERVERS ARE AFFECTED? WHAT IS THE IMPACT ON YOUR BUSINESS OF AN INFECTION?

### Dealing with Intruders

For the enterprise network manager, preventing network infection by malicious programs is a never-ending job. And sometimes, despite your best efforts, something gets through.

The problem is, when prevention fails, traditional network management systems don't offer any help in dealing with the consequences, or even seeing what's happening. Utilization is skyrocketing on a router port—which servers, applications, or users are affected? Application response time is slow—who's connected? Which servers are affected? Which subnets are infected users on? Device-oriented systems can only see the details, and what you need when a worm or virus is bringing your network down is a top-to-bottom, end-to-end view: where the infection is raging, who's infected, how it's progressing, and how it's affecting your network and its support of business services.

*"Not only did the Network Physics Problem Management Dashboard alert us to the anomalous behavior caused by the Blaster worm—without any pre-programming; but the comprehensive, real-time view the product gave us of what was happening allowed us to quickly zero in on infected servers and subnets and rapidly corral the worm."*

*Global Network Architect, Big Five Consulting Firm*

### Go with the Flow

The Network Physics appliance gives you just that view, rapidly detecting anomalous behavior that can indicate a security breach and enabling you to quickly zero in on affected devices to control the infection.



### Customer Problem:

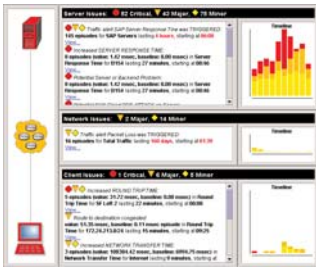
- > Unable to quickly spot virus or worm infections
- > Difficulty identifying infected servers and clients
- > No way to measure impact on business

### Network Physics Solution:

- > Flow-based non-invasive monitoring of all traffic, all the time, in real time
- > Automatic detection of anomalous behavior without programming or signature updates
- > Business-centered view of network performance and utilization

### Customer Benefits:

- > Quick detection and identification of infection
- > Rapid localization and isolation of infected servers and clients
- > Improved ability to prevent re-infection
- > Clear indication of impact on business services

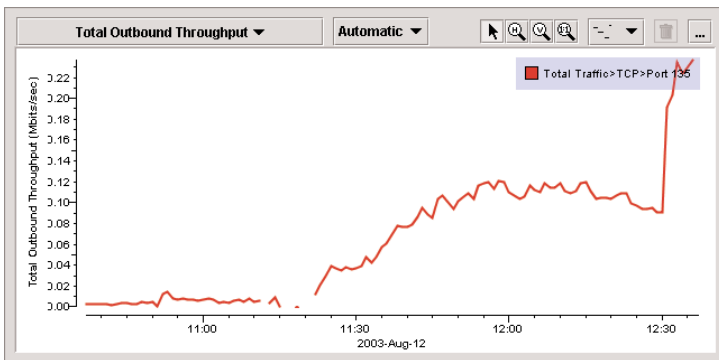
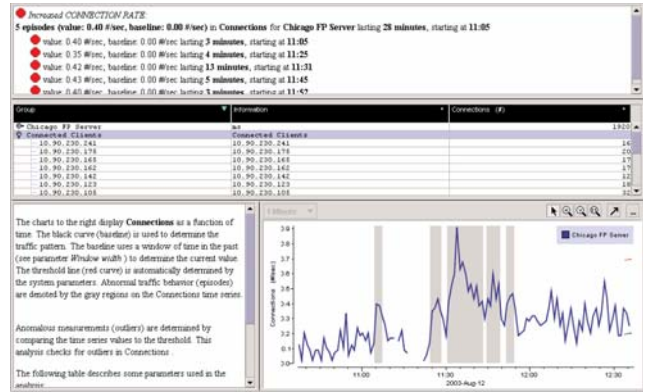


The Problem Management Dashboard applies a number of advanced statistical and correlative techniques to automatically flag anomalous behavior, enabling it to detect the activity of rogue programs without programming or the need for signature information.

To understand how Network Physics can improve your response to security breaches, consider the Blaster worm attack of August, 2003. A major consulting firm had the Network Physics appliance installed on their network when the worm hit.

### Automatic Detection of Anomalous Behavior

IT staff first became aware of the worm infection when the Network Physics Problem Management Dashboard flagged several anomalous behaviors, including skyrocketing connection rates and an unusual level of activity on TCP port 135.



### Quick Diagnosis and Localization

A drill-down link from the Dashboard immediately identified the affected server farm, and, equally important, the connected clients that might be infected from it.

Further investigation confirmed the signature of the worm by the abrupt increase of traffic on TCP port 135, as noted in the CERT alert.

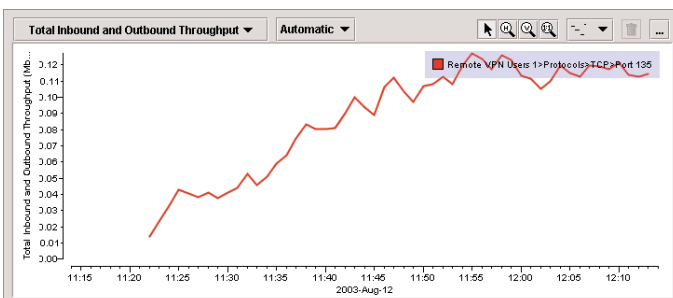
### Isolation, Mitigation, and Follow-Up

Using the Client Prefix/24 table, managers quickly identified all infected subnets and took

Group	Connections (#)	Connection Rate (#/sec)	Outbound TCP Throughput (Mbits/sec)	Inbound TCP Throughput (Mbits/sec)	Network Transfer Time (msec)	Round Trip Time (msec)	Connection Setup Time (msec)
531122	147.534	0.341	2.356	4053.497	721.175	749.259	
1858	0.516	0.882	4967.773	12.880	179.159		
461	0.128	0.005	3154.843	155.753	318.176		
270	0.075	98.32E-6	125.98E-6	469.226	10.196	64.668	
234	0.065	0.002	390.607	151.079	129.004		
108	0.030	0.009	154.835	67.689	59.070		
103	0.029	0.002	476.58E-6	7927.424	27.404	34.894	
99	0.028	0.001	636.474	64.390	64.930		
92	0.026	0.014	332.570	103.877	124.421		
88	0.024	58.72E-6	50.08E-6	40790.988	163.846	288.416	
85	0.024	93.34E-6	159.38E-6	46496.994	136.356	215.416	
83	0.023	79.89E-6	179.48E-6	277995.506	191.674	207.147	
78	0.022	395.78E-6	0.001	274.968	134.246	138.406	
63	0.018	61.73E-6	111.38E-6	736913.025	283.008	273.646	
63	0.018	0.002	0.064	0.000	1.318	0.000	
62	0.017	471.38E-6	0.007	534.691	119.728	91.620	
60	0.017	0.001	463.78E-6	670.233	212.068	160.329	
59	0.016	0.001	80.126	0.633	0.293		
58	0.016	145.88E-6	89.65E-6	0.147	0.101	31.692	
56	0.016	33.83E-6	40.64E-6	0.000	198.372	85.800	

appropriate action to isolate and disinfect them.

Re-infection by remote users on the VPN remains a possibility until everyone has updated their virus protection. The signature of such re-infection can be easily identified via port 135 traffic on a VPN.



### In-Depth Visibility, Immediately

The Network Physics appliance delivers unprecedented power to track, contain, and control security breaches without relying on agents, SNMP, or pre-programmed signatures and updates. It monitors all your traffic non-intrusively via spanning port or tap, and gives you in-depth visibility and end-to-end network coverage immediately. Fill the holes in your defense, and speed your response to business-crippling attacks with Network Physics.



491 Fairchild Drive, Mountain View, CA 94043 USA  
 1.650.230.0900 (main) 1.650.230.0909 (fax)  
 info@networkphysics.com www.networkphysics.com



supplied by Phoenix Datacom  
 01296 397711  
 info@phoenixdatacom.com  
 www.phoenixdatacom.com