

## Ensuring Business Continuity And Mitigating Risk From Sophisticated Threats and Exploits

### Introduction

Every company has experienced it — somehow, some way, the network becomes infected with the latest worm or virus, disrupting business operations and threatening the integrity of sensitive information. From Code Red and Slammer to Blaster and Sasser, the rising onslaught of malicious traffic is showing no signs of abating. As the frequency and intensity of malicious attacks increase, enterprises find themselves hustling to build stronger defenses. However, those defenses are in need of constant reassessment. Like an arms race, the escalating sophistication of malicious attacks is causing businesses to increase their efforts and stay a step ahead of the pace. What was impenetrable last month may not be today. It's not surprising that in today's frenetic environment, business organizations often fall short. The pressing need to ward off threats to IT investments, let alone business performance, is heightening the urgency around maintaining business continuity and minimizing damage.

### Infection Entry Points

Most IT professionals typically consider the problem confined to perimeter security. If the network was more secure, the problem would just go away. Unfortunately, this philosophy does not represent reality. No matter how strict or secure the network, infections still occur. Some common examples of how a "secured" network becomes infected include:

- Employees infecting their laptops at home and bringing them back to the office
- Business partners and contractors bringing laptops into the network
- Employees downloading Trojan programs from the Web or using peer-to-peer applications
- Email worms spreading before the signatures have been defined and patches distributed
- Employees transferring files via Instant Messenger services
- Malicious attackers sending sophisticated viruses that masquerade as legitimate traffic

It doesn't really matter how the infection occurs, only that it does occur. Considerable effort should be spent blocking infections, but assuming that efforts will be 100 percent successful is unrealistic. Prepare for the inevitable — it will pay off handsomely when it counts most.

### The Typical Progression

When an infection strikes the network, proliferation is often swift. This is especially the case with worms, which can propagate quickly without human involvement. Most infections typically search for other prey to infect. This process usually occurs unabated, because security measures are employed at the perimeter. Once inside, the rest of the network and hosts are wide open to invasion.

Propagation can occur via any mechanism or protocol. In the early stages of an attack, many users don't even know that their machines are infected because regular services are still functioning. But each infected host is sending many connection probes, each of which consumes a small amount of bandwidth.

When enough machines become infected, the amount of traffic that is generated causes congestion at bandwidth-constrained WAN links. Often, IT's first sign that a problem exists emerges in the form of vague reports that indicate slow application performance on the WAN. As a virus or worm continues to spread, the resulting surge in traffic can completely shut down network services to individual sites or servers, and in extreme cases, the entire wide-area network.

At this point, IT realizes that it is facing a full-fledged security breach. Plenty of questions emerge: "Is this a known virus or a blended threat that uses multiple modes of infection? Is there a signature or patch posted? Which machines are infected? Can I shut down the source of the traffic? How do I get my network back until I can get the infected hosts inoculated?"

### **The Cost of Infections**

The time between when an attack is launched and a patch or virus signature is made available is called "Zero Day". During this window of vulnerability, IT is at the mercy of the outbreak because the tools to prevent its propagation and eliminate it from the network are unavailable. The financial and productivity costs that are incurred during Zero Day are the most significant. The initial costs involve IT's time spent tracking down infected hosts and inoculating machines. Without the proper tools, this task can be daunting and painstakingly long.

More costly is the overall loss of productivity that the entire company experiences during outbreaks. If access to an application is slow or non-existent, and that application is part of a critical business process, then user productivity suffers. In extreme cases, network outages from worms and viruses translate directly into lost revenue. If customer service representatives can't access their ordering application, then that revenue may go to a competitor.

## Surviving "Zero Day" Attacks: The Need for Application Traffic Management

Ensuring business continuity and mitigating risk requires:

- Early identification that an event is occurring on the network
- Automated control of the malicious traffic that is being generating
- Real-time protection of business-critical applications during an attack

Packeteer's Application Traffic Management solutions excel in accomplishing these tasks.

### **Early Identification**

Understanding how a virus or worm might manifest itself on the network is difficult because so many possibilities exist. Some use email, some ping for hosts, some use Microsoft protocols, and some do port scanning. The next virus might look completely different than any previous virus, making it difficult to identify. Despite differences, there is one trait that most viruses have in common: Most viruses feature an abnormal jump in connections and attempted connections. Each newly infected machine attempts to find new hosts to infect. Whether this search process is conducted through a barrage of pings, SQL queries, or emails, the amount of connections emanating from that specific host skyrockets.

Having a tool that automatically identifies abnormal connection rates and traffic loads and notifies the appropriate party is critical to preventing a full-scale outbreak.



### **Packeteer's Identification Capabilities**

Packeteer's Application Traffic Management solution provides the necessary tools to quickly identify threats and the hosts that are being affected. Specifically, Packeteer® monitors connections on a per-host basis. Exceeding configurable connection thresholds can generate an event via SNMP, email, or syslog entry that can alert network administrators that an anomaly has occurred. Therefore, any host that becomes infected and starts flooding the network will be flagged automatically.

Tools in the Web User Interface, as well as the centralized reporting application ReportCenter™, readily identify hosts with excessive connections. In addition, they identify hosts with significant failed connections, which often occur while scanning for more victims. Once a suspicious host has been identified, additional tools such as top talkers/listeners, and packet capture can be enabled to collect further details about the event.

### **Automate Control of Malicious Traffic**

Just seeing an infection and notifying IT are not enough to prevent the network from being flooded with unwanted traffic. The next logical step is to limit the connections coming off a particular host. Keeping new connections to a reasonable level will slow the rate of propagation as well as limit the amount of excess traffic traversing the network.

### **Packeteer's Containment Capabilities**

The Packeteer system maintains network integrity and business continuity as outbreaks unfold. In many ways, a virus or worm attack isn't much different than other, less malicious Zero Day events that frequently occur on enterprise networks. For example, this may include a user becoming a super node in a peer-to-peer network, a large email attachment sent across the network to many end users, or a major news or sports story causing everyone to browse the Web at the same time. Packeteer has been dealing with these issues for many years, and worms and viruses are just extreme cases of significant non-business traffic consuming too much WAN bandwidth or overloading resources.

Packeteer also has some specific features designed to detect and react to abnormal circumstances automatically. As previously mentioned, Packeteer monitors connections and sends alerts when they are exceeded, but it also goes a step further. Additional connections above a configurable threshold can be dropped. This automatically prevents a single host from flooding the network.

In addition, Packeteer limits total connections when many hosts try to flood the network simultaneously. In effect, Packeteer recognizes abnormal conditions automatically and lowers the connection thresholds for each host during extreme conditions. This allows individual, non-infected hosts to maintain connections successfully, while excess connections from infected hosts are dropped automatically.

And finally, once Packeteer has diagnosed the profile of an attack, malicious traffic can be eliminated easily. Attacks normally appear as a specific application (e.g. SQL, ICMP, email, etc.), and a simple containment policy can easily be pushed out from the centralized configuration application, PolicyCenter®, to throttle back or block the infection traffic completely. Using Packeteer's bandwidth management tools to contain the "bad" traffic has long been a strategy for ensuring overall network efficiency and stability.



## Real-time Protection of Business-Critical Applications

Even limiting connections from an infected host won't necessarily prevent the network from being flooded if too many machines have been infected. This is where protecting business-critical applications becomes essential. Once protected, an application will continue to function effectively, no matter what threat emerges.

### Packeteer's Protection Capabilities

Packeteer has built its business protecting and enhancing the performance of applications that matter most to an enterprise organization. Because so many unforeseen events can occur on the network, enterprises have no choice but to protect their business applications. Packeteer invented the application traffic management space and has patented the critical technologies required to ensure that applications perform efficiently and reliably.

If each important application has appropriate controls assigned to ensure its effective — and safe — performance, then even if a virus or worm strikes, Packeteer will ensure that critical applications access bandwidth first, leaving whatever's left to the virus. In other words, when applications are protected, a full-scale virus storm could be unfolding without end users ever noticing a slowdown in performance.

## Traffic Management – An Integral Part of Worm/Virus Security

Most enterprises spend a good deal of time keeping worms and viruses out of their network — just as they should. But those same enterprises often do not spend enough time thinking about how to properly prepare when something malicious does gain access to the network. Maintaining network integrity during an attack is critical to reducing the amount of time IT spends fighting outbreaks, and even more important, limiting downtime associated with each event.

Packeteer's application traffic management system provides the keys to surviving an outbreak — identifying early that an outbreak is occurring, controlling the rogue traffic, and protecting critical applications at all times. When deployed properly, the effects of network congestion events of all kinds, including virus and worm attacks, are cleansed more quickly and prevented from impacting business operations. Every well-prepared enterprise should deploy an application traffic management solution to ensure that its critical applications perform efficiently and reliably, particularly under adverse conditions.

The same Packeteer products that identify and mitigate the impacts of worms and viruses also provide extensive network monitoring, industry-leading bandwidth management, and important acceleration capabilities. Having a combined solution enables organizations to distribute security tools to the edge of the network without breaking the security budget.

[www.packeteer.com](http://www.packeteer.com)

10201 N. De Anza Blvd  
Cupertino CA USA 95014  
T +1 408.873.4400 F +1 408.873.4410

