

November 2003

## **NetScaler's Defense Against Web-Based Worm Attacks**

*With the widespread adoption of the Internet for enterprise connectivity and application delivery, there has been an exponentially increasing threat of computer-based virus and worm attacks penetrating enterprise infrastructures, potentially compromising, or crippling corporate resources. This concern is shared by many IT organizations that are now challenged with protecting servers and clients while providing with access to corporate information. In most circumstances, the responsibility falls purely on the IT organization to keep user systems and servers protected from the ever increasing barrage and sophistication of these types of attacks.*

*Worms are a class of attack that spread via web protocols (HTTP and HTTPS) and are particularly harmful to enterprises since they target mission-critical resources. Anti-virus and operating system vendors have provided assistance through incremental software updates and patches for servers and clients, unfortunately these updates can only be supplied after the attack has been introduced and detected. This approach also relies heavily on network and software administrators to stay abreast of newly identifying attacks and vulnerabilities, and keep relevant systems at the right patch level which can include tens or even hundreds of servers. Such updates are time consuming and also disrupt the availability, capacity and performance of the applications since the servers have to be take offline to apply the updates. This can be a never ending, expensive and extremely disruptive cycle for some corporations. Although many IT organizations have been able to somewhat solve the threat of virus attacks, the sophistication of worms have left many solutions virtually useless.*

## OVERVIEW OF VIRUS AND WORMS

Although computer viruses have been in existence for some time, worms are a relatively new phenomenon, but can still be classified as a class of virus. Like viruses, worms spread (propagate) and cause damage or loss of data and or productivity. The purpose of a worm is similar to that of a traditional virus, but unlike viruses worms can spread at greater speeds and are deemed to be self-contained entities—not requiring user intervention to spread or infect. The purpose of this paper is to discuss the ability to provide infrastructure protection against web-based worm attacks. Unlike email-based worms that rely on email applications to propagate, web-based worms rely on network protocols and the ability for most infrastructure systems to forward traffic without inspection.

The following outlines the difference between email-based worms and web-based worms, describing their approach to infection and the proposed attack profile.

- **Payload** - refers to the attack that is contained within the virus or worm. When a system is infected, there can be a number of different types of attacks applied. Some can be minor or nuisance attacks, like displaying a message on the systems monitor or writing a file to disk with pointless messages. Other attack types can be serious or malicious, like crashing a system during operation, or changing/removing the contents of stored data.
  
- **Replication** - refers to how the worm or virus propagates itself to other systems. This is often the distinguishing factor that defines whether an attack is a worm or virus:
  - *Email-based Worms*  
Replication occurs by seeking and utilizing an installed email application on an infected system. Once the worm detects the appropriate application, it will automatically generate emails to every email address contained within the address book for that system. Typically the

email will have simple subject text and an attached file. An unsuspecting recipient will open the attached (infected) file which will in turn infect the recipients system. This process continues using each infected system to start another process of emails and potential infections.

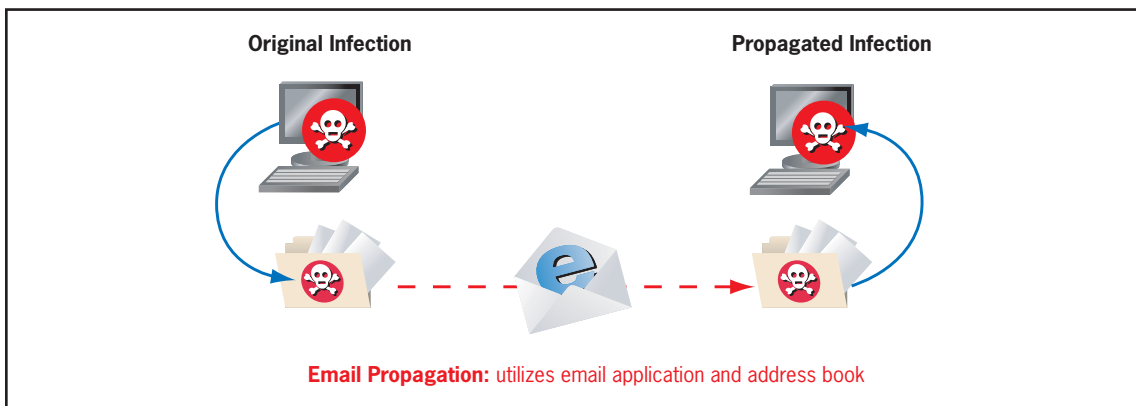
*Example*

Nimda— which is a “mass mailing” worm that utilizes multiple methods for self replication including email applications. When the worm arrives by email, it uses an email (MIME) exploit allowing the threat to be executed by the user reading or previewing the attached file.

Source: Symantec Corporation ([www.symantec.com](http://www.symantec.com))

*Solution*

Solutions are available from many anti virus companies which include products for client, server and gateway systems. These products use both in-memory and file inspection techniques to detect signatures of known worms allowing each system to detect or block active worms prior to infection. Since many worms utilize email to propagate, many organizations deploy email gateway software which can detect and deny a worm before infecting other systems.



**Figure 1: Virus Replication Overview**

- *Web-based Worms*

Web-based worms can replicate in a number of ways. Unlike email-based worms, they do not rely on other applications like email or file sharing to infect systems. Instead, they are designed to be a self-contained entity that seeks out networking system's vulnerabilities using standards-based protocols like HTTP. Once these vulnerabilities are discovered, the worm will automatically exploit them to infect other systems on that network. Unlike email-propagation which relies on other applications to propagate, a worm can infect an entire network almost instantaneously without user or administrator knowledge. This can have catastrophic effects for IT administrators and enterprises that rely on network resources for critical business functions.

*Example*

Code Red — sends its code as an HTTP request. The HTTP request exploits a known buffer-overflow vulnerability, which allows the worm to run on your computer. The malicious code is not saved as a file, but is inserted into and then run directly from memory.

Source: Symantec Corporation ([www.symantec.com](http://www.symantec.com))

### Solution

There are many approaches to solving the threat of worm infection within an organization. Many of the anti-virus companies have capabilities to detect worms that may have already infected a system. Although anti-virus software can provide a defense against these worm attacks, it is important to complement these solutions with infrastructure protection systems.

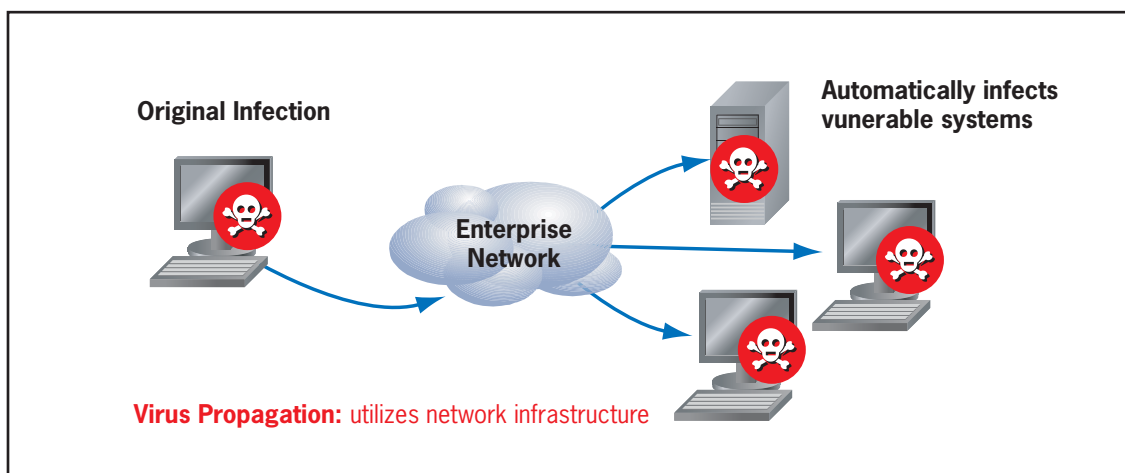


Figure 2: Worm Replication Overview

## COMMON NETWORK DEFENSE SOLUTIONS

Since worms commonly utilize network vulnerabilities for propagation, and although anti-virus software can assist in detecting worms, it may not be able to block its propagation to the rest of the network. To do this, there needs to be complementary infrastructure security products that can inspect active network traffic, seeking potential worm attacks. Common products deployed for infrastructure defense include Firewalls, Intrusion Detection and Intrusion Prevention Systems.

### Firewalls

Firewalls provide an infrastructure solution for filtering common Denial of Service (DoS) and Distributed DoS (DDoS) attacks from entering the corporate infrastructure. These solutions are designed to block these types of attacks, and prevent common intrusion attempts by inspecting traffic at high speeds — often inspecting Layer 2-4 information, with some limited application filtering capabilities. Although some firewalls can be configured with Layer 7 content inspection (required for worm detection), they may provide little or no defense against worms:

- Invoking complex Layer 7 filters (required for worm detection), would cause a dramatic performance decrease.
- Encrypted traffic would mask a worm from being detected, allowing it to enter the network. Once the traffic is decrypted (from a VPN gateway or server inside the network), it will begin infection and replication.

## Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS)

IDS/IPS are specifically designed to protect against unauthorized intrusions and detect network attacks, inspecting traffic that is passed to it. These systems are typically installed in a one-arm configuration, relying on network traffic to be mirrored from a Layer2-3 switch for inspection, comparing incoming traffic to a predetermined set of profiles and rules. If any of the profiles or rules are matched, then an alarm is generated, with some of the more sophisticated systems potentially updating firewall rules to stop the traffic from re-entering the network after detection. Although these systems are useful in helping administrators detect and potentially block unauthorized intrusions or attacks, they may provide little defense against worms:

- A worm may only be detected after it has entered the network and potentially infected some systems. Even if the worm is detected early, the IDS cannot stop the replication process, but only alert an administrator to its presence.
- Encrypted traffic would mask a worm from being detected by either an IDS or IDP, allowing it to enter the network. Once the traffic is decrypted (from a VPN gateway or server inside the network), it will begin infection and replication.

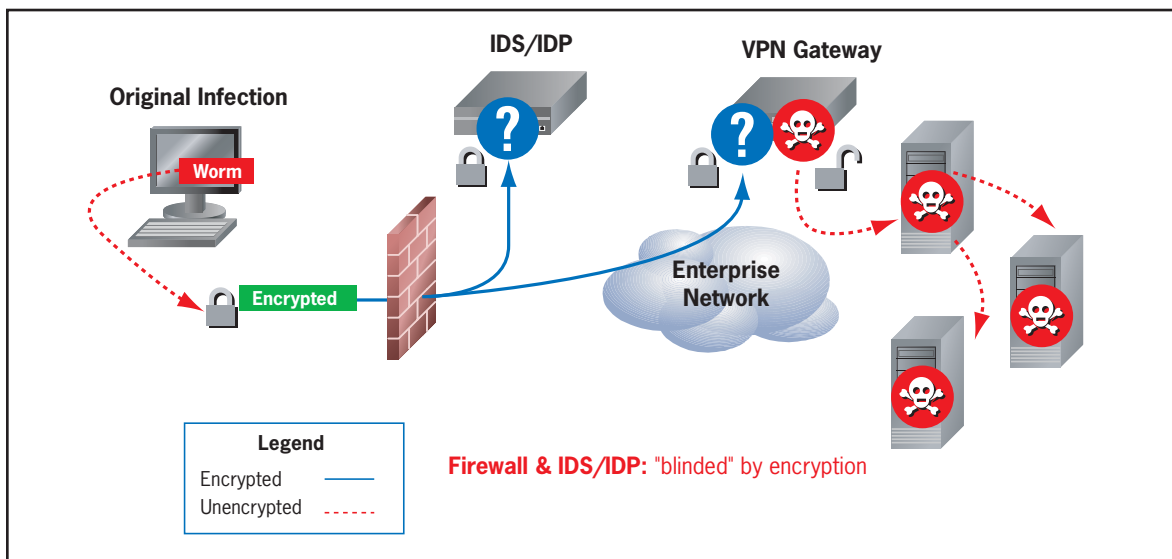


Figure 3: Encryption Cripples IDS/IPS Solutions

## NETSCALER DELIVERS A ROBUST WORM DEFENSE SOLUTION

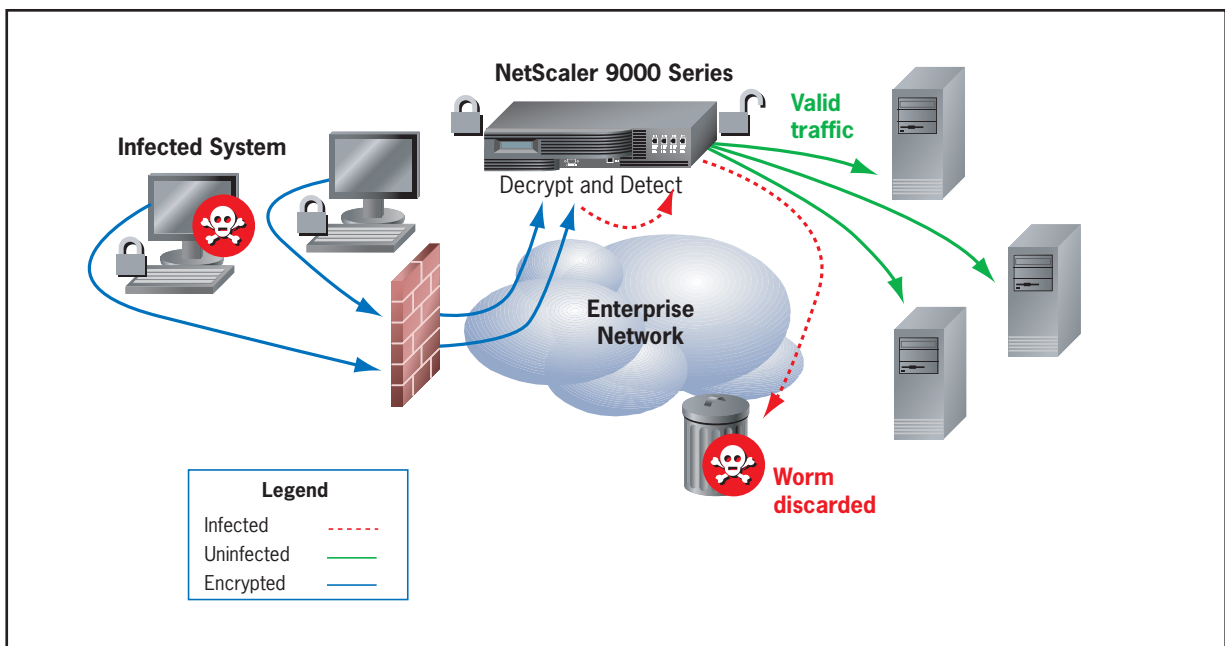
Introducing the NetScaler 9000 Series, a unified platform that combines the fundamentals of security protection with the advantages of application optimization and switching. When investigating a solution for worm protection, it is imperative that it provides the capability to decrypt encrypted traffic and provide Layer 7 inspection capabilities. The NetScaler 9000 Series is based on a multi-patented Request Switching™ architecture that allows traffic to be inspected from the application layer (Layer 7). Coupled with comprehensive content encryption/decryption capabilities, the NetScaler 9000 Series provides the ideal solution for complete security including worm protection.

The NetScaler 9000 Series provides a comprehensive security solution delivering complete DoS/DDoS protection and intrusion filtering capabilities that specifically target and eliminate these types of attacks. When a web worm such as Nimda attempts to propagate through the network by infecting internet application servers through malicious HTTP and HTTPS requests, the only way to detect its presence is to inspect the complete packet header including the application layer information. This inspection requires a high-performance application layer inspection engine, like that which is implemented within the NetScaler 9000 Series. By embedding a highly tuned Layer 7 inspection engine, the NetScaler 9000 can detect and discard application layer attacks including web worm attacks without impacting network performance, but ensuring that the propagation of a worm is denied prior to entering the infrastructure.

Worms traditionally originate from malicious users within public networks (Internet). Since these worms are generated by unauthorized users, they are commonly generated in the “clear” (without encryption). This type of attack may be detected and blocked by traditional network infrastructure security devices as described above.

With the introduction of HTTPS (SSL encrypted web protocol) applications for extranets, as well as VPN technology for employee remote access, the threat of authorized users being a source of worm origination is a reality. The introduction of wireless LANs and the use of application layer encryption to secure the local access by employees has made this problem even more acute. These users are often unaware that they may be infected with a worm, but when connected to the network infrastructure via a VPN connection, they become a launching pad for the worm to propagate throughout the infrastructure. The fact that the traffic is encrypted will mask the threat from traditional infrastructure protection devices.

By integrating comprehensive, high-throughput HTTPS and VPN support with the Layer 7 filtering, the NetScaler 9000 Series provides the ability to decrypt all encrypted traffic prior to inspection, ensuring that worm attacks will not be “hidden” by application encryption.



**Figure 4: Protecting Against Encrypted Attacks**



## CONCLUSION

For comprehensive application security and worm protection, the NetScaler 9000 Series is the only product in the industry that combines robust application security, application optimization and application switching into a single unified platform. These capabilities combined with Anti-virus systems that protect against SMTP-born worm attacks provide IT organizations with a complete solution to defend against attacks, whether the traffic originates from a public internet source, a protected encrypted VPN or even an encrypted wireless LAN. The NetScaler 9000 Series is an ideal complement to existing anti-virus systems and network infrastructure protection systems preventing worm attacks for both encrypted and unencrypted application traffic.

*NetScaler, the NetScaler logo and Request Switching are trademarks of NetScaler, Inc. All other products are trademarks of their respective holders and should be treated as such.*