



Responding to the Nimda worm: Recommendations for addressing blended threats

INSIDE

- › Case study of blended threats
- › Countermeasure practices and solutions

Contents

Executive summary	3
Nimda: Case study of blended threats	4
Alternate methods of propagation	4
Need for integrated countermeasures	5
Best practices	5
Comprehensive and complementary solutions	5
Symantec Norton AntiVirus – Finds and removes the threat	6
Symantec Enterprise Firewall/VelociRaptor – Defends against Nimda scans	6
Symantec Enterprise Security Manager (ESM) – Identifies patch levels	6
Symantec NetRecon – Scans networks for improper activity	7
Symantec NetProwler – Provides real-time alerts and identifies victimized systems	7
Symantec Intruder Alert – Detects unauthorized actions and accesses	7
Symantec Security Response	7
Conclusion	7

> **Executive summary**

Life is no longer simple. The pressure of working and reacting in Internet time is rapidly increasing. An unfortunate side effect of Internet maturity and progress is that adversaries can enjoy equal success. The Nimda worm is the latest example of how the Old World strategy of “one threat, one cure” has become outdated. The purpose of this paper is to explore the nature of blended threats using the Nimda and CodeRed worms as examples of these new dangers. Both of these worms have shown that today’s adversaries are employing new combinations of offenses against IT infrastructures. They also graphically point out that mere single point solutions will no longer be adequate to address them. It is now necessary to protect all parts of the network and to respond on the Gateway, Server, and Client levels. Subsequent to analyzing the threat we will explain the need for a comprehensive response to these threats and show how Symantec has maintained its position as the world’s leading Internet Security company by providing our customers with a broad array of products and complementary services that address today’s and tomorrow’s threats.

Nimda is a worm. What makes it different from other Internet worms is that it requires no human interaction to spread, instead using known software vulnerabilities and multiple vectors of infection. The nature of a worm’s propagation and the speed with which it is able to infect victims is a hallmark of its prevalence. Nimda, also known as W32.Nimda.A@mm, W32/Nimda@mm, PE_NIMDA.A, I-Worm.Nimda, W32/Nimda-A, and W32.Nimda.A, was discovered on September 18, 2001. Computer Economics (Carlsbad, CA) estimates that Nimda infected over 2.2 million servers and PCs in a 24-hour period, between 2:30 PM EDT on September 20 and 2:30 PM, September 21. The firm notes that 65% (1.43 million) of the worm’s targets during its initial attack were servers and the remaining 35% (770,000) were PCs. Computer Economics estimates the economic costs of downtime and subsequent clean-up for Nimda at \$531 million (as of September 19, 2001).

As of August 31, 2001, Computer Economics projects virus- and worm- attack costs of \$10.7 billion.

The calculated global cost of the CodeRed worm alone is \$2.6 billion. This includes \$1.1 billion for clean-up of over 1 million infected servers, as well as inspection of over 8 million other servers; with inspection including the necessary actions to install, test, and certify these systems fit for service. Another \$1.5 billion can be attributed to “negative impact on productivity of system users, support staff, helpdesk staff, and other staff responsible for assisting internal end users, IT staff, and customers worldwide.”

These significant figures represent more than a growing dependence on the Internet and Internet technology. They illustrate the increased sophistication of threats and the escalating costs needed to recover from them. The threats embodied by Nimda and CodeRed are blended threats: that is, they are multi-faceted in their operating methods and effects. Blended threats require comprehensive security solutions that provide multiple layers of defense and response; with triggers to pre-determined responses when threats are encountered. Comprehensive includes the ability to secure all levels within the IT infrastructure: Gateway, Server, and Client as well as the ability to synergistically apply complementary security functions. Symantec offers the most comprehensive arsenal of solutions to deal with these threats. The combination of Symantec security products or Managed Security Services for Virus Protection, Vulnerability Assessment, Firewall, and Intrusion Detection Systems offer the best protection for today and tomorrow’s threats.

> **Nimda: Case study of blended threats**

The Nimda creator appears to have learned from the characteristics of preceding worms and viruses, as evidenced by the following:

ALTERNATE METHODS OF PROPAGATION

Nimda has four alternate methods of propagation.

1. Systems infected with Nimda will scan the network looking for unpatched Microsoft® Internet Information Server (IIS). It then attempts to use the a specific exploit, called Unicode Web Traversal exploit, to gain control of the target server.
2. Nimda can also propagate via email. It does this by harvesting email addresses from any MAPI compliant email program's mailboxes. It can also extract email addresses from .html and .htm files. The worm uses these email address for the To: and the From: addresses. Thus, the From: addresses will not be from the infected user. The worm uses its own SMTP server to send out emails. When the worm arrives by email, the worm uses a MIME exploit allowing the virus to be executed just by reading or previewing the file.
3. Users visiting compromised Web servers will be prompted to download an .eml (Outlook Express) email file, which contains the worm as an attachment (readme.eml).
4. Nimda attacks hard disks of systems that have enabled file sharing over the network. It will also create open network shares on the infected computer, allowing access to the system. During this process the worm creates the guest account with Administrator privileges.

This variety of propagation methods underscores the complexity of the threat and was partially responsible for the speed of its infection rate.

One of the major side effects of Nimda is that it also causes localized bandwidth DoS conditions on networks with infected machines. This is due to a combination of the infected systems' network scanning and the additional email traffic generated by the worm.

From a coverage perspective, Nimda demonstrated a follow-the-sun pattern, appearing first in the United States and then migrating to Asia and Europe.

CodeRed is another example of a blended threat, as it was able to launch a DoS attack at a designated IP address (target), deface Web servers, and then, with CodeRed II, leave Trojan viruses behind for later execution. The nature of CodeRed—processing in memory rather than on a hard disk—allowed it to slip by detection of some anti-virus products. Its discovery was further hampered by the fact it presented no outward indications of its presence on the IIS server.

> **Need for complementary and comprehensive countermeasures**

BEST PRACTICES

Security experts agree that implementing best practices in a consistent, on-going, manner is the best defense against infection—and the best way to minimize harm. In addition to best practices, a variety of information security products or services are required to defend against a blended threat, optimize the chance for early detection and containment, and facilitate recovery.

Remove unneeded services

Organizations need to determine which services they truly require and remove any that are unnecessary. For services that are needed, software patches should be installed as soon as possible after discovery of a vulnerability. Recognizing that services are an exposure because they are listening on a TCP port is important, and elimination of unneeded services can dramatically reduce system vulnerability. For example, is there is no reason to run a Windows NT Server with IIS Web Server on a company's desktops; removal of IIS from those desktops will preemptively defeat attacks on that particular target.

Implement strong passwords

Another key area for attention to security is password use and discipline. The use of strong passwords enforced through consistent and frequent vulnerability assessment can help mitigate some threats.

Keep patches up to date

Most blended threats are based on known vulnerabilities. Keeping your operating systems and applications up to date with the latest security patches, protects your systems from many of the attacks and can help stop the propagation of certain worms.

Data forensics

Employment of best practices should include policies, procedures, and standards for such functions as logging, reporting, and auditing. And tools should be put in place that help enhance the effectiveness of event analysis through after-the-fact data forensics.

COMPREHENSIVE AND COMPLEMENTARY SOLUTIONS

Successful defense against this new generation of blended threats requires a combination of steps and security functions. The threat must be identified and removed as early on as possible as with an effective anti-virus product such as Norton AntiVirus™. Potential Nimda incursions should be blocked employing a state of the art hybrid firewall based on highly secure Application Inspection technology, such as Symantec Enterprise Firewall™ or VelociRaptor™ firewall appliance. The network and hosts must be monitored for improper activity, and unauthorized actions and access by complementary host and network intrusion detection and vulnerability assessment products such as Symantec NetRecon™, Symantec NetProwler™, and Symantec Intruder Alert™. It is also necessary to insure that all patches have been properly implemented. This requires a comprehensive vulnerability assessment tool such as Symantec Enterprise Security Manager™. Symantec offers leading products in each of these areas. Their use in the blended threat scenario is discussed below.

› **Symantec Norton AntiVirus™ – Finds and removes the threat**

Symantec Norton AntiVirus is the world's most trusted anti-virus solution. It repairs common virus infections without user intervention. It can be updated automatically with the latest virus definitions over the Internet employing Symantec's state-of-the-art LiveUpdate™ support system.

Symantec offers antivirus solutions at all levels of the network, including the gateway, email server, and client levels. This tiered approach of virus protection is especially important when faced with a worm like Nimda, with multiple methods of propagation.

Symantec also provides specialized removal tools online to help remove remnants of the threats and purify clients' systems. These unique tools dramatically reduce the time and effort it takes to recover from the effects of a blended threat by automating many of the manual processes required to recover from an infection.

› **Symantec Enterprise Firewall™/VelociRaptor™ firewall appliance – Defends against Nimda scans**

Symantec Enterprise Firewall (formerly known as Raptor® Firewall) and VelociRaptor firewall appliance have both been used effectively to repel the recent blended threat attacks such as CodeRed, CodeRed II and Nimda. The unique combination of features in these hybrid firewalls provides the best protection against known and unknown attacks. The full application inspection technology ensures users of the Symantec Enterprise Firewall and VelociRaptor firewall products are provided with maximum security against attacks. Symantec's firewall products are layer 7, full inspection firewall and were able to block Nimda and CodeRed scans of Web servers, while, layer 4, stateful inspection firewalls did not. In addition, these firewalls protect by default right "out of the box" ensuring better protection by decreasing the likelihood of vulnerabilities due to configuration errors. By default, these products analyze HTTP, and other protocols' requests and responses to ensure they adhere to the RFC standards defining these protocols behavior. Another feature of Symantec Enterprise Firewall version 6.5 and VelociRaptor 1.1 is the ability to use URL pattern matching on rules to block against identified threats on specific Web server platforms. This feature allows an administrator to implement new, targeted security checks when a new attack arises.

› **Symantec Enterprise Security Manager (ESM)™ – Identifies patch levels**

Symantec Enterprise Security Manager is a scalable security policy compliance and host-based vulnerability assessment tool. It enables corporations to detect systems running IIS server; detect systems that have the Web Directory Traversal Vulnerability, which is used by Nimda; and detect modified files, new files, and deleted files through snapshot technology. It can also detect other modifications in the registry, which is useful in data forensic analysis.

If you have not already deployed ESM within your enterprise, it is of limited use in recovering from a widespread attack such as Nimda. However, once installed, it has tremendous strength in mitigating the risk of the next blended-threat-type worm since it enforces best practices: identifying inadequate patch levels, finding unneeded services, and discovering weak passwords.

Typically O/S and other vendors come out with security patches simultaneously or quickly after the announcement of a security-related bug. Symantec quickly updates our security templates to reflect the new patch levels allowing customers to discover and update systems proactively prior to hackers launching attacks that exploit those bugs.

› **Symantec NetRecon™ – Scans networks for improper activity**

Symantec NetRecon is a network vulnerability assessment scanner with root-cause-analysis capabilities. It detects systems that are running Web services—specifically Microsoft IIS—and also detects systems that have the Web Directory Traversal Vulnerability.

› **Symantec NetProwler™ – Provides real-time alerts and identifies victimized systems**

NetProwler is Symantec's network-based intrusion detection tool that constantly and transparently monitors the enterprise's network for patterns of misuse or abuse. With Security Update 8 installed, NetProwler can detect the CodeRed worm and variants operating on a network, and NetProwler logs will identify each system compromised by the Nimda worm. NetProwler can also assist in forensic analysis by reviewing log entries to provide clues on which network host(s) were first compromised by the worm.

› **Symantec Intruder Alert™ – Detects unauthorized actions and accesses**

Symantec Intruder Alert is a host-based intrusion detection tool that finds unauthorized and malicious activity, keeping systems, applications, and data secure from misuse and abuse. The FileWatch function in Symantec Intruder Alert can monitor and detect mission-critical files for any changes, deletions, or movements resulting from unauthorized access after compromise by Nimda. Symantec Intruder Alert provides utilities to develop custom rules to restore compromised/changed files to their original state. Intruder Alert also monitors a system for suspicious behavior such as rootkit or DDoS agent installation, account creation, or modification. Symantec Intruder Alert can centrally manage log file events from across the network to assist in forensic analysis of compromised systems.

› **Symantec Security Response**

Through global technical support and international research centers, Symantec Security Response ensures customers that their security systems are optimized while providing them up-to-the-minute information and advice regarding emerging security threats. Symantec Security Response combats blended Internet security threats with a unique combination of solutions, services and response capabilities, providing customers with comprehensive, global, 24X7 Internet security expertise.

When a new threat or vulnerability is discovered, Symantec Security Response experts provide rapid emergency response, focusing on communication with customers and delivery of security updates for Symantec security products. Symantec Security Response provides time-sensitive security advisories using Web updates, alerting services, technical support, and media alerts.

› **Conclusion**

Blended threats are expected to appear with increased regularity and growing complexity. The best defense against today's threats consists of adopting best practices and applying them in concert with comprehensive security solutions. Symantec is the only Internet Security firm that offers proven tools and the dynamic support required to maintain them and respond to tomorrow's challenges.

SYMANTEC, A WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 37 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide
operations in 37 countries.
For specific country
offices and contact numbers
please visit our Web site.