MyDoom/Novarg Worm (W32.Novarg.A@mm)

Vital information on what the worm does, how to repair infected systems, and how to protect against future attacks

On January 26, 2004, computer security specialists detected a computer worm known as MyDoom or Novarg. This fast-spreading worm propagates primarily via email attachments and infects Windows®-based workstations and servers. It can also impact networks because of the amount of email traffic it generates.

MyDoom gained momentum extremely quickly. Within 24 hours from the time it was first identified, Symantec™ Security Response was receiving more than 500 submissions per hour of MyDoom-infected files from Symantec antivirus solutions that have automatic reporting mechanisms. That number is comparable to past worms such as Blaster and BugBear.B. However, the peak rates for Novarg (on January 27 and 28) set a new high of over 900 submissions per hour.

Because it can masquerade as a harmless file attachment, because it installs a "back door" into a computer that may allow hackers to run spyware or other malicious code, and because network performance can be degraded by its attempt to launch a denial-of-service attack, Novarg is considered particularly dangerous. For these reasons, Symantec Security Response urges all system and network administrators to respond to this threat quickly and effectively.

KEY POINTS

- MyDoom propagates as an email attachment and via Kazaa peer-to-peer sessions.
- It disguises its executable payload with a text file or screen saver icon, greatly increasing the odds that unsuspecting users will consider the attachment harmless and open it.
- Its payload is designed to coordinate a DDoS attack on www.sco.com.
- The payload also creates a "back door" to the infected system that could leave a computer open to information theft and further attacks.
- The worm grabs email addresses from the infected system and spreads itself further by sending email messages to those addresses.
- It is very common to see variants like W32.Mydoom.B@mm after a major worm.

What is MyDoom?

MyDoom is an encrypted mass-mailing worm that arrives as an attachment with a .exe, .scr, .zip, .pif, .cmd, or .bat extension. (The attachment may actually have two suffixes. If it does, the first one will be .doc, .htm, or .txt, making the attachment appear to be a non-executable file and thus distracting users from the real nature of the file.) The message itself will have an innocuous subject line such as "hi" or "Mail Delivery System."

The worm performs the following actions when it infects a computer:

- Creates a "back door" into the system by installing a file (Shimgapi.dll) that acts as a proxy server, and opening a range of TCP ports to listen for activity. This back door potentially allows a hacker to connect to the system and use the proxy to gain access to the computer's network resources. The back door can also download and execute arbitrary files, such as spyware that can collect and report passwords, credit card numbers, and other confidential information.
- Prepares to launch a distributed denial-of-service (DDoS) attack on the Web site of software company SCO (www.sco.com) from February 1 to February 12, 2004.
- Uses email addresses found on the computer to send itself to other systems. It can find addresses not only in email address books, but also in many other types of files, including text and HTML documents. MyDoom can also detect the presence of Kazaa file-sharing software and propagate by placing files in the Kazaa shared-files folder.

Although mass-mailing worms are not a new category, MyDoom has spread faster than others because it uses a more effective social engineering technique. The attached file containing the worm uses a Microsoft® Windows icon that makes it appear to be a harmless text file or screen saver. Thus many users who have previously heeded warnings about opening executable files may be fooled by the benign icon and open the file containing MyDoom.

MyDoom/Novarg is designed to stop spreading as of February 12, 2004. However, any back doors it has opened will remain active even after that date.

On January 28, a MyDoom variant called W32.MyDoom.B@mm was discovered. This worm has the same characteristics, but it has a more extensive payload and is designed to last until March 1, 2004. MyDoom.B contains code to create a DDoS attack not only against SCO, but also against Microsoft (www.microsoft.com). Further, it overwrites the local host file to prevent users from accessing more than 60 Web sites—including www.symantec.com and other sites that are vital for obtaining information and software to fight Novarg/MyDoom infections. (Symantec and other companies are taking steps to ensure that customers will continue to be able to reach their Web sites.)

AFFECTED SYSTEMS

Computers using the following operating systems can be affected by W32.Novarg.A@mm: Windows 2000; Windows 95; Windows 98; Windows Me; Windows NT®; Windows Server™ 2003 Windows XP

It is important to remove the infection and prevent new infections even if you are not currently seeing any symptoms in the systems you manage. Infected systems are vulnerable to future damage because of the back door opened by the Novarg worm.

What to do now

Administrators of the computers listed in the previous section should immediately take measures to block Novarg from reaching those systems and to remove it from computers it has already infected. Enterprise customers should block potentially infected mail at the gateway by filtering attachments and subjects. Administrators should also caution users not to open unexpected attached files, no matter how benign they may appear to be.

HOW TO REMOVE THE WORM

Symantec Security Response has developed a free, easy-to-use tool that checks for and removes W32.Novarg.A@mm. The tool is available from the Symantec Security Response Web site at **www.sarc.com/avcenter/venc/data/w32.novarg.a@mm.removal.tool.html.** You do not need to be a registered Symantec customer to download this removal tool.

If you prefer to remove the infection manually, you will need to perform these actions:

- Disable System Restore (Windows Me/XP)
- Update the virus definitions
- Restart the computer in Safe or VGA mode
- Run a full system scan and delete all the files detected as W32.Novarg.A@mm
- Delete and modify the value that was added to the registry

For more information about manual removal, visit
www.sarc.com/avcenter/venc/data/w32.novarg.a@mm.html

HOW TO PROTECT YOUR COMPUTERS

All systems running Symantec™ antivirus products should immediately be updated with the latest virus definitions via Intelligent Updater™ or LiveUpdate™. Administrators should also ensure that all updates have been installed for other security solutions (including intrusion protection) in use on their networks. Symantec consumer products that support Worm Blocking functionality automatically detect this threat and prevent it from spreading.

In addition, because MyDoom/Novarg installs a back door program that opens ports 3127 to 3198 in order to listen for TCP traffic, administrators should block those ports on all systems.

How to guard against future threats

Because of the increasing prevalence and virulence of viruses, worms, and other computer attacks, it's important for every organization to proactively protect its networks, servers, and workstations. Symantec Security Response recommends that you combine best practices with best-of-breed products and services.

IMPLEMENT BEST PRACTICES

Symantec Security Response encourages all users and administrators to adhere to the following basic security best practices:

- Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, Telnet, and a Web server. These services are potential avenues of attack, so if they are removed, blended threats have fewer avenues of attack and there are fewer services to maintain through patch updates.
- If a blended threat exploits one or more network services, disable or block access to those services until a patch is applied.
- Always keep patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers and help prevent or limit damage when a computer is compromised.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.
- Isolate infected computers quickly to prevent compromising your organization further. Perform a forensic analysis and restore the computers using trusted media.
- Instruct employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

DEPLOY EFFECTIVE SOFTWARE AND SERVICES

Symantec solutions—either singly or in combination—have been instrumental in protecting customers' systems and networks from becoming infected with high-profile viruses and worms.* The integrated, state-of-the-art firewall, intrusion protection, antivirus, and alert and response capabilities of Symantec solutions are expressly designed to protect against today's blended threats. Please contact Symantec for assistance to determine which of these products and services best meet your organization's needs.

- SYMANTEC DEEPSIGHT SOLUTIONS provide early warning of new vulnerabilities and threats. The Symantec DeepSight™ Threat Management System tracks Internet activities globally, providing early warning of active attacks to help protect critical information assets. With Symantec DeepSight™ Alert Services, administrators receive personalized vulnerability and malicious code alerts, providing actionable information to help them mitigate vulnerabilities before they can be exploited.
- SYMANTEC ANTIVIRUS™ ENTERPRISE EDITION is a comprehensive suite that delivers multi-tiered protection for Internet and email gateways, network servers, and workstations. It combines award-winning technology and Symantec's global response infrastructure to deliver high-performance, scalable protection that stops virus threats before they enter the network. In addition, it enables administrators to block unwanted email (such as spam) by content. By incorporating industry-leading technologies and protection for all network tiers, Symantec AntiVirus Enterprise Edition eliminates the complexity of a multi-vendor security solution.
- SYMANTEC™ CLIENT SECURITY protects remote users and networked desktop clients by integrating virus protection, firewall, and intrusion detection technologies. Laptops outside the corporate firewall are protected from being used by hackers to gain unauthorized enterprise network access during an ISP connection. Symantec Client Security can automatically scan files for known and unknown viruses, block suspicious inbound and outbound traffic, and prevent unauthorized intrusions and port scans. It can also audit the network to identify unprotected nodes that are vulnerable to attack.
- SYMANTEC™ GATEWAY SECURITY provides protection against even the most malicious Internet security threats while reducing the complexity of security management. It integrates a full inspection firewall, protocol anomaly and signature-based intrusion prevention and intrusion detection engines, award-winning virus protection, URL-based content filtering, antispam and IPsec-compliant virtual private networking technology with hardware-assisted high-speed encryption.
- SYMANTEC MANHUNT™ protects enterprise networks against intrusions and DoS attacks through high-speed network intrusion detection, real-time analysis and correlation, and proactive prevention and response. Because Symantec ManHunt can detect both known and unknown threats, it helps eliminate network exposure and the vulnerability inherent in traditional signature-based IDS products.

*Some solutions may be more or less effective depending upon specific characteristics of a threat.

- SYMANTEC™ HOST IDS is a scalable intrusion detection and prevention solution for critical servers. It provides enterprises with a sophisticated combination of intrusion protection and management capabilities. In addition to simply detecting security events, Symantec Host IDS can actually stop known and unknown attacks before system damage occurs. It uses an organization's unique security policies and configurations to determine when to alert administrators to changes to the file system, Registry, audit logs, and processes.
- SYMANTEC INTRUDER ALERT™ is a host-based, real-time intrusion monitoring system that detects unauthorized activity and security breaches, then responds automatically according to pre-established security policies to prevent information loss or theft. As a complement to firewalls and other access controls, Symantec Intruder Alert enables the development of precautionary security policies that prevent expert hackers or authorized users with malicious intent from misusing systems, applications, and data.
- SYMANTEC™ MANAGED SECURITY SERVICES protect enterprise networks and business information from emerging security threats with real-time analysis and immediate notification of hostile activity. Through the use of global intelligence resources, Symantec Managed Security Services deliver around-the clock security monitoring, management, and response. Fully audited processes and procedures that have been validated through certifications such as BS7799 and SAS70 Type II, enable customers to focus on core business issues and be assured of world-class security protection for their enterprise network.

For more information

The following resources can help you protect your systems against Novarg worm infections, remove infections that have already occurred, and safeguard against future blended threats.

- **Symantec Security Response home page:** http://securityresponse.symantec.com
- **Symantec Security Response MyDoom/Novarg incident pages:**
  - www.sarc.com/avcenter/venc/data/w32.novarg.a@mm.html
  - www.sarc.com/avcenter/venc/data/w32.mydoom.b@mm.html
- **Symantec Enterprise Solutions MyDoom/Novarg Resource Center:** http://enterprisesecurity.symantec.com/article.cfm?articleid=2420
- **Microsoft MyDoom incident page:** www.microsoft.com/security/antivirus/mydoom.asp

SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934

www.symantec.com

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

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.