QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ January 28, 2004

Multiple Variants of the MyDoom Email Worm

ADVISORY OVERVIEW

January 28, 2004 – Qualys™ Vulnerability R&D Lab today released an update to a vulnerability signature in the QualysGuard® Web Service to protect enterprises against the variants of the MyDoom email worm that is rapidly propagating across the Internet. Customers can immediately audit their networks for hosts infected with this worm by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

The MyDoom worm (also known as Novarg or Shimg) is a mass-mailing and peer-to-peer file sharing worm that affects Microsoft® Windows™ computers and is spread by both email and the KaZaa peer-to-peer file sharing application.

Both variants of MyDoom frequently arrive in an email message as a .zip file or executable attachment. When the end-user opens the attached file, the worm installs itself into the system directory and then modifies the registry to ensure it runs at system startup. The MyDoom.A variant performs three actions:

- Sends emails to users in the infected computer's address book
- Leaves a backdoor that can allow the computer to be accessed by a remote attacker. The backdoor runs on TCP port 3127.
- Sends continuous page requests to SCO.com as part of a distributed denial of service attack (DDoS)

The later variant of the worm, MyDoom.B, also performs these additional actions:

- Overwrites the local host file to prevent the infected computer from accessing Microsoft and anti-virus vendor update sites
- Opens TCP ports 1080, 3128, 80, 8080, and 10080 for future backdoor access. The backdoor program has the ability to relay TCP packets, which provides IP spoofing capabilities and can facilitate future distribution of Spam emails.
- Sends continuous page requests to microsoft.com as part of a distributed denial of service attack (DDoS)

For additional information concerning the MyDoom worm, please visit the Carnegie Mellon CERT® Coordination Center incident knowledge base at:
http://www.cert.org/incident_notes/IN-2004-01.html

HOW TO PROTECT YOUR NETWORK

A check for the MyDoom variants is already available in the QualysGuard vulnerability management platform. A default scan will detect computers infected by this worm. In addition, QualysGuard users can perform a selective scan for infected computers using the following check:

- "MyDoom.a and MyDoom.b"
  - Qualys ID: 1125
  - Limit the scan to TCP ports 139, 445, 3127, 1080, 3128, 80, 8080, and 10080.
  - A Windows login is not required, but using one will provide an added level of detection.
  - Additionally, enable the “Windows Host Name” check with Qualys ID 82044 if you want to report on infected hosts by Windows (NetBIOS) machine name.

Infected systems can be remedied using the following procedures.

MyDoom.A

1. Kill the process `readme.txt`
2. Remove the files `taskmon.exe` and `shimgapi.dll` in the system directory.
3. Remove the registry entry HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "TaskMon"
4. Restore the registry entry HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 "(Default)" to it's original value of %SystemRoot%\System32\webcheck.dll

MyDoom.B

1. Kill the process `readme.txt`
2. Remove the files `Explorer.exe` and `ctfmon.dll` in the system directory.
3. Remove the registry entry HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Explorer.exe"
4. Restore the registry entry HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 "(Default)" to its original value of %SystemRoot%\System32\webcheck.dll
5. Remove all the suspicious entries in you host file.

Please note that this procedure does not protect against infection or re-infection. End user education is critical to protecting your network against email worms such as MyDoom. End-users need to frequently update their anti-virus signatures and to exercise caution when opening emails with attachments that include filename extensions such as .exe, .scr, .bat, or .zip.

For information about protecting Microsoft Outlook users from MyDoom and other mass mailer worms, please visit the Microsoft Privacy and Security Center at:
http://www.microsoft.com/security/antivirus/mydoom.asp

TECHNICAL SUPPORT

For more information, customers can contact Qualys Technical Support directly at support@qualys.com or 1-866-801-6161.

ABOUT QUALYSGUARD

QualysGuard is an on-demand security audit service delivered over the web that enables organizations to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues. By continuously and proactively monitoring all network access points, QualysGuard dramatically reduces security managers' time researching, scanning and fixing network exposures and enables companies to eliminate network vulnerabilities before they can be exploited.

Access for QualysGuard customers: https://qualysguard.qualys.com

Free trial of QualysGuard service: http://www.qualys.com/forms/maintrial.html