Mydoom, Doomjuice, Win32/Doomjuice

by: Hang Chau, 09/18/2004

http://www.securitydocs.com/library/2562

Abstract

On February 1, 2004, the Web site of the SCO Group on that weekend was hit by a massive Distributed Denial of Service (DDoS) attack generated by the Mydoom.A worm. Between February 9 to 12, 2004, Mydoom.B worm launches a Denial of Services (DoS) attack against www.microsoft.com. Mydoom.A and Mydoom.B worms have caused more than $850 million worth economic damages worldwide in just the first 24 hours, according to mi2g, a security analyst company based in London.

Both Microsoft and SCO Group have offered $250,000 rewards for information leading to the arrest and conviction of the people who wrote the worms, but I see little chance the money will lead to an arrest. A expert on network security said: "If virus writers know there is a strong cash incentive for someone to grass them up, they may think twice about unleashing a virus."

In this research paper, I will introduce and discuss:

1. *Mydoom worms, a mass-mailing worms that attempts to spread via email and by copying itself to any available shared directories used by Web sites;*
2. *Doomjuice worms, which not infect via e-mail, but it scans random Internet addresses for computers that have had backdoors installed by Mydoom.A;*
3. *W32/Doomjuice worms, they spread and attack the Microsoft's Windows systems. '*

After thinking and discussing with some members of a group on network security and searching online, I think that both Mydoom.A and Mydoom.B have a programming error that limits the number of infected machines that will conduct the DoS attacks at the same time. Only about 7% of the Mydoom.B-compromised computers actually attack Microsoft.com simultaneously, but about 25% of the infected machines are able to attack the SCO's web site.

I also provide some solutions for protecting the W32/Doomjuice worms.

1. Introduction

On February 1, 2004, the Web site of the SCO Group (a UNIX vendor based in Lindon, Utah) on that weekend was hit by a massive Distributed Denial of Service (DDoS) attack generated by the Mydoom.A worms. From February 9 to 12, 2004, the variant of Mydoom.A worm, Mydoom.B worm launches a Denial of Services (DoS) attack against www.microsoft.com.

Mydoom worms have caused more than $850 million worth economic damages worldwide in just the first 24 hours, according to mi2g, a security analyst company based in London. Both Microsoft and SCO Group have offered $250,000 rewards for information leading to the arrest and conviction of the people who wrote the worms, but most experts see little chance the money will lead to an arrest. A expert on network security said: "If virus writers know there is a strong cash incentive for someone to grass them up, they may think twice about unleashing a virus."

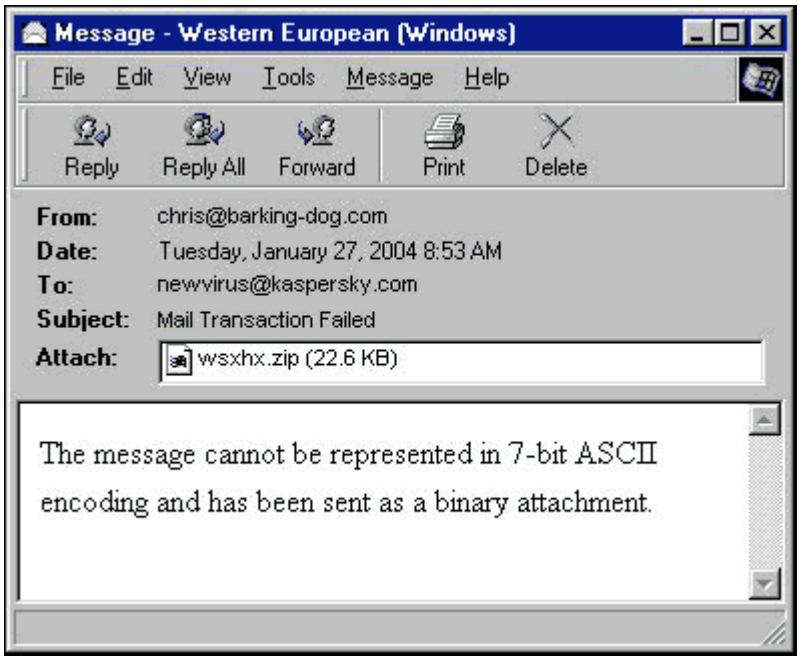
2. Mydoom.A and Mydoom.B

2.1 Mydoom.A/Mydoom

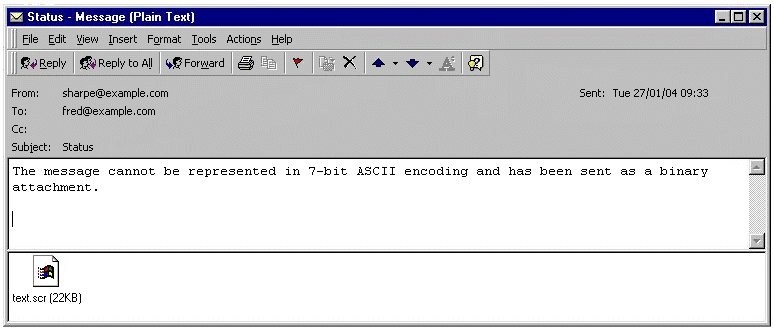
Mydoom.A is a mass-mailing worm that attempts to spread via email and by copying itself to any available shared directories used by Web sites. Mydoom.A selects from a list of email subjects, message bodies, and attachment file names for its email messages. It spoofs the sender name of its messages so that they appear to have been sent by different users instead of the actual users on infected machines. Mydoom.A can also propagate through the Kazaa peer-to-peer (P2) file-sharing network (KaZaA is a completely distributed peer-to-peer file sharing service).

The Mydoom worms harvest addresses from infected machines and targets files with the following extensions: **.wab, .adb, .tbb, .dbx, .asp, .php, .sht, .htm and .txt**. and generally uses the words “test”, “hi” and “hello” in the subject line. The message in Mydoom is sent as a binary attachment. It often arrives in a zip archive of 22,528 bytes and is represented by a text icon even though it is an executable file, which are renowned for carrying viruses.

While the body of the email varies, it usually includes what appears to be an error message, such as:



or:



(Enlarge Picture)

Analysts say Mydoom is spreading so quickly because it fools successfully users to open the email files

then open the attachment. The email often disguises itself as an email that the user sent that has bounced back. The user, wanting to know why the email failed, opens it up and then sees a text file icon, instead of the icon for an executable. A text file icon leads people to believe it is innocuous. So for the email users, the best thing to do stop the spread of the Mydoom, experts said, was not to open the suspicious attachments in unexpected emails, and delete the emails as soon as possible.

Mydoom also sets up a backdoor Trojan in the infected computers, allowing the virus writer or anyone else capable of sending commands to an infected machine to upload code or send Spam. The worm also is geared to launch a denial-of-service (DoS) attack against SCO.com starting on Feb. 1, 2004.

Mydoom can slow internet performance significantly. Mydoom is contained in emails with random sender's addresses and subject lines. When loaded, some versions of the Mydoom launch Notepad and show random characters. At the same time it replicates itself, opens a backdoor that could allow hackers to break in and, in some instance, installs a "keystroke" program that records everything being typed, including passwords, and credit numbers.

2.2 Mydoom.B

Another variant of the Mydoom.A worm, Mydoom.B, is similar to the Mydoom.A, but Mydoom.B contain an added DoS attack against Microsoft's web site and a feature that blocks access to anti-virus web sites on infected machines.

Mydoom.B started a similar attack as the Mydoom.A on February 1, 2004, on both SCO's and Microsoft's Web sites, but that attack won't likely be an issue. While Mydoom.A has infected hundreds of thousands of systems, only a slight fraction of that were hit by Mydoom.B.

So the Mydoom.B worm is generally considered by leading anti-virus software companies and e-mail security firms to be less effective than Mydoom.A at propagating itself and causing widespread damage to computer systems.

Microsoft has classified the Mydoom.B as a moderate threat. The small number of reports of Mydoom.B suggested that the attacks on Microsoft have failed.

2.3 Mydoom.A vs. Mydoom.B

Both Mydoom.A and Mydoom.B used infected machines to conduct DoS attacks against sites. The worms forced compromised systems to bombard the home pages of SCO and Microsoft in the hopes of overloading their servers and making the URLs inaccessible.

After thinking and discussing with some members of a group on network security and searching online, I think that both Mydoom.A and Mydoom.B have a programming error that limits the number of infected machines that will conduct the DoS attacks at the same time. Only about 7% of the Mydoom.B-compromised computers actually attack Microsoft.com simultaneously, but about 25% of the Mydoom.A-compromised computers are able to attack the SCO's web site.

3. Doomjuice.A (W32/Doomjuice.A), Doomjuice.B (W32/Doomjuice.B)

3.1 Doomjuice.A (W32/Doomjuice.A)

Doomjuice.A (or W32/Doomjuice.A) worm, known as the variant of the Mydoom worm, first appeared on February 9th, 2004. Doomjuice.A worm is programmed to execute a DDoS attack against Microsoft's web site www.Microsoft.com with the systems/computers that already infected by Mydoom worms. Doomjuice.A is approximately 35 KB in size, compressed using UPX (Ultimate Packer for

eXecutables). The size of the decompressed file is approximately 43 KB. Doomjuice.A does not have a pre-programmed expiration date, the computers which have successfully removed Mydoom are not at risk for infection by Doomjuice.A.

Doomjuice.A does not infect via e-mail, but it scans random Internet addresses for computers that have had backdoors created by Mydoom.A (the virus writers or attackers can access freely your computers through the backdoors). Doomjuice.A searches for computers on which TCP ports 3127 is open and sends itself to these computers, copying itself to the Windows directory as ***intrenat.exe.***

Except copy itself as intrenat.exe, Doomjuice.A also creates a backup of Mydoom source code and copies it as **sync-src-1.00.tbz** to the following locations:

- root directory
- Windows directory
- Windows system directory

The worm also creates a Mutex **sync-Z-mtx_133** to ensure a single copy is running in the memory, the unique identifier sync-Z-mtx_133 shows the worm's presence in memory. It alters the Windows registry at the following location to load itself during next startup:

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

To propagate, the Doomjuice.A makes use of infected computers. The worm connects to TCP port 3127, which has been opened by **shimgapi.dll**, the backdoor component of Mydoom, to receive commands. If the infected computer answers the command, Doomjuice establishes a connection and sends a copy of itself. The backdoor component of Mydoom accepts the file and executes it.

In order to choose IP addresses to attack, the worm uses the following formula: (A.B.C.D). The first value in the address (A) is selected from the following list:

3,4,6,8-9,11-22,24-26,28-30,32-35,38,40,43-57,61-68,80-81,128-191,193-196,198-220,225-239.

The second (B) and third (C) values are randomly generated by the worm. The final value (D) will be a number between 0 and 254, with values being selected in sequence.

The connection between Doomjuice.A and the Mydoom in the weeks (from the end of January to middle of February, 2004) is, however, not limited to the exploitation of these infected computer's vulnerabilities. Doomjuice.A contains the source code of Mydoom and drops Mydoom on the hard drives of infected computers. It has been speculated that the inclusion of this payload in Doomjuice.A is an attempt by the writers/attackers to spread the evidence, so to speak, since the possession of the original source code of Mydoom.A now less convincing evidence of responsibility for the recent Mydoom attacks than otherwise.

DoS (Denial of Service) Attack
The Doomjuice.A worm determines the system date, and if the date is between 1st and the 11th of the month, the worm carries out a modified DoS attack on the site www.Microsoft.com. One GET command will be sent to port 80, and then repeated at random intervals. If the date is the 12th of the month or later, the commands will be sent without a break.

3.2 Doomjuice.B (W32/Doomjuice.B)
A new version of the Doomjuice worm, Doomjuice.B, sought to launch a more effective Denial of

Service (DoS) attack on Microsoft's web site on February 16, 2004. Doomjuice.B is compressed via UPX utility in 5120 bytes in file size. After decompression, its size increases to 6656 bytes. Unlike the Doomjuice.A, the Doomjuice.B does not carry the source code of the Mydoom worm.

Doomjuice.B sets random HTTP headers to make it more difficult to filter the attack traffic, seeking to work around a defensive measure used by Microsoft earlier that week, when www.Microsoft.com dropped requests without User-Agent headers to differentiate between Web browsers and the DDoS attack agents. The Doomjuice.B DDoS also initiates twice as many requests as its predecessor, launching 32-192 parallel threads instead of the 16-96 of Doomjuice.A.

The Doomjuice.B worm creates a Mutex consisting of the name of the infected computer and the string "_sncZZmtx_133", the unique identifier _sncZZmtx133 show the worm's presence in memory, same as the Doomjuice.A. The worm copies itself into the %system% directories using the name **regedit.exe**. The worm creates an entry named NeroCheck in one of the following keys:

1. HKLMSoftwareMicrosoftCurrentVersionRunGremlin
2. HKCUSoftwareMicrosoftCurrentVersionRunGremlin

The worm's spreading algorithm mimics that of its predecessor Doomjuice.A. It takes advantage of the backdoor created by the Mydoom worm. Its random IP address generator attempts to find possible victims and tries to connect to the port number 3127. The port number 3127 has been opened by **shimgapi.dll**, the backdoor component of Mydoom, to receive commands. If the infected computer answers the command, then Doomjuice.B establishes a connection and sends a copy of itself. The backdoor component of Mydoom accepts the file and executes it. To determine which IP address to attack, the worm uses following formula: (A.B.C.D).

The first value in the address (A) is selected from the following list:

3,4,6,8,9,11-22,24-26,28-30,32-35,38,40,43-57,61-69,80-81,128-191,193-196,198-220,225-239.

The second (B) and third (C) values are randomly generated by the worm. The final value (D) will be a number between 0 and 254, with values being selected in sequence.

DoS (Denial of Service)
The worm checks the system date, and if the current date is between the 8th and the 12th of the month, the DoS attack function will not be launched. The worm will not launch any DoS attack in January. However, in all other months and on all other dates the worm will launch a DoS attack on www.Microsoft.com site. To carry out the DoS attack, the worm sends multiple GET commands with the following parameters.

GET / HTTP/1.1
*ACCEPT: */**

Accept-Language: en-us or Accept-Language: en

Accept-Encoding: gzip, deflate or blank

User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.0) or
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) or
User-Agent: Mozilla/4.0

Host: www.microsoft.com:80

The worm uses a modified trigger to launch a DoS attack on the www.Microsoft.com site. The attack is launched outside January and between 8th and 12th each month.

4. Solution

1. From Proland Software, download a 30 day Evaluation Copy of Protector Plus for your operating system: http://www.pspl.com/virus_info/worms/doomjuicea.htm

2. According to F-Prot's methods, step-by-step: http://www.f-prot.com/virusinfo/descriptions/doomjuice_a.html

3. According to McAfee's methods, step-by-step: http://mcafee.com/virusInfo/default.asp?id=mydoom

4. According to Trend Micro's methods, step-by-step: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOOMJUICE.A

5. Reference

http://www.viruslist.com/eng/viruslist.html?id=841769

http://www.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci947481,00.html?track=NL-102

http://www.microsoft.com/security/antivirus/mydoom.asp

http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html

http://www.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/

http://www.sophos.com/virusinfo/analyses/w32mydooma.html

http://www.esecurityplanet.com/trends/article.php/3304451

http://us.mcafee.com/virusInfo/default.asp?id=mydoom

http://weblog.cemper.com/a/200401/31-what-you-should-know-about-the-mydoom-worm-variants-mydooma-and-mydoomb.php

http://www.pspl.com/virus_info/worms/doomjuicea.htm

http://washingtontimes.com/business/20040201-105103-4504r.htm

http://www.linuxworld.com/story/43537.htm

http://www.sophos.com/virusinfo/analyses/w32doomjuicea.html

http://www.f-prot.com/virusinfo/descriptions/doomjuice_a.html

==========

Hang Chau
Senior Network/System Administrator, Ming Plaza Development
hcdanny@yahoo.com
(909)864-9456
28925 Clear Spring Lane, Highland, CA 92346, U.S.A.

Degree and IT Certifications:

- M.S. on Computer Science, California State University, Fresno, California, USA;
- CCIE, CCNP, CCNA (Cisco/CCIE: passed the Qualification Exam);
- SCSA, SCNA (Sun/Solaris 8: Certified System and Network Administrators);
- SCJP, SCWCD (Sun/Java 2: Certified Programmer and Web Component Developer);
- MCSE, MCSA (Microsoft 2000 Certified System Engineer and System Administrator).

Also research on Network Attacks and Network Security:

- Cisco IDS/Secure PIX (Intrusion Detection Systems and Firewall);
- DoS/DDoS (Denial of Service/Distributed Denial of Service);
- Mydoom/Doomjuice Worms and DoS/DDoS attacks.