VIRUS ANALYSIS 2

WE'RE ALL DOOMED

Gabor Szappanos
VirusBuster, Hungary

'The crisis in Hungarian soccer deepens at almost the same rate as the Mydoom worm destroys computer systems.' This quote is from a Hungarian daily sports newspaper. Nothing I have come across illustrates the impact of this virus better – and the extent to which it has infiltrated everyday life.

The first identified sample of Mydoom came from Russia, which is the suspected origin of this virus. According to *MessageLabs*, about 1.2 million samples were detected during the first 24 hours of the virus spread – which overtook the previous record holder, Sobig.F, by a narrow margin. During the peak, 1 in 12 emails were infected with Mydoom.A – also a new record.

The first alerts on Mydoom arrived on Monday 26 January 2004, at around 10pm local time. Having spent a busy weekend fighting the Dumaru.Y outbreak (see p.4), I felt the name of this virus was completely justified.

OVERVIEW

The virus usually spreads via email, but it can also spread using the *Kazaa* file exchange network. Mydoom.A is a 22,528-byte UPX compressed program. It uses a simple ROT13 algorithm to encode the most sensitive string variables in the virus code. The username and server name pool is not encrypted, but the registry locations, SMTP command and the message bodies are.

Upon execution the virus checks for the existence of the 'SwebSipcSmtxS0' mutex to ensure that only one instance of the virus runs at any one time. To indicate that a system is already infected, the virus creates the registry entry:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\
0Explorer\ComDlg32\Version
```

If this key is not present the virus launches a separate thread that creates a file with the name 'Message' in the %Temp% directory. The file contains nonsensical text (using characters between 16 and 255 ASCII code) and displays in the *Notepad* text editor. The virus generates 4096 characters for the file, but the actual size of the file is larger and varies, because line breaks are inserted (CRLF) randomly within the text.

After the editor window has been closed, the virus deletes this file.

The virus drops its backdoor component SHIMGAPI.DLL into the *Windows* system folder, and loads this library immediately.

At this point the worm checks the system date. If it is later than 12 February 2004, 02 hours 28 minutes 57 seconds UTC, no more of the virus's actions will be executed: it will not spread or run the DoS attack. However, it is only at this point that the date is checked, so if the worm instance was started before the drop-dead date, it will not stop working when the time passes this limit – the change will take effect only on the next startup.

Next the virus copies itself into the *Windows* system folder as TASKMON.EXE. The worm creates the key 'TaskMon=%System%\taskmon.exe' under the registry location:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

to ensure that it will execute automatically on *Windows* startup.

If the virus cannot create the key here (because of a lack of user privileges), it creates the key under the location

HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run

MAILING

In order to spread via email the virus gathers addresses from the *Windows* Address Book and from files with the extensions .htm, .sht, .php, .asp, .dbx, .tbb, .adb, .pl, .wab and .txt. The files are searched in the web browser cache and on all local hard drives. The addresses are stored in memory, rather than being saved to a local file.

The address gathering and the mail sender routines run in separate threads, with several memory variables synchronizing between them.

The subject line of the outgoing messages may be one of the following:

test	Mail Transaction Failed
hi	Server Report
hello	Status
Mail Delivery System	Error

The message body is one of the following (or, depending on the value of a random variable, random characters):

- Mail transaction failed. Partial message is available.
- The message contains Unicode characters and has been sent as a binary attachment.
- The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.

This is a clever twist of social engineering: the virus doesn't even attempt to make itself look interesting. Instead, it camouflages itself as an error message, with the main content of the message attached. As the virus executable has the same icon as *Notepad* text documents, the unsuspecting recipient may think it is safe to open the attachment. In fact, the attachment is the virus with extension .bat, .exe, .pif, .cmd or .scr.

Occasionally it can create a ZIP package containing the virus (stored without compression) and send it as an attachment. In this case, the ZIP header contains the name of the executable in the archive, therefore the length of the header – and consequently the length of the archive – varies, despite the fact that the executable inside the archive is the same in all cases.

The filename of the attachment may be one of the following:

document	text	test
readme	file	message
doc	data	body

The worm avoids sending itself to email addresses that contain the following strings (these domains are annotated in the virus source as being friendly domains):

"berkeley"	"kernel"	"ripe."
"unix"	"linux"	"isi.e"
"math"	"fido"	"isc.o"
"bsd"	"usenet"	"secur"
"mit.e"	"iana"	"acketst"
"gnu"	"ietf"	"pgp"
"fsf."	"rfc-ed"	"tanford.e"
"ibm.com"	"sendmail"	"utgers.ed"
"google	"arin."	"mozilla"

Another set of domains is also avoided, but these are not likely to be considered friendly, these are more likely to be domains that are better avoided:

"avp"	"sopho"	"ruslis"
"syma"	"borlan"	".gov"
"icrosof"	"inpris"	"gov."
"msn."	"example"	".mil"
"hotmail"	"mydomai"	"foo."
"panda"	"nodomai"	

The worm also avoids sending itself if the username contains the following strings (thus avoiding mailboxes with owners who may be more careful than the average):

www	someone	service	ntivi
secur	your	help	unix
abuse	you	not	bsd
root	me	submit	linux
info	bugs	feste	listserv

samples	rating	ca	certific
postmaster	site	gold-certs	google
webmaster	contact	the.bat	accoun
noone	soft	page	
nobody	no	admin	
nothing	somebody	icrosoft	

Despite these limitations, the virus obviously found enough targets to enable its global epidemic. This is probably because it relies on sending itself to general users who tend to click on attachments without consideration, while the addresses it avoids are likely to belong to sysadmins, who may be more careful.

Depending on the value of a random variable, the worm may not use the harvested email address. Instead it combines the domain part of the address with one of the usernames in the following list:

sandra	adam	jane	jose
linda	ted	bob	andrew
julie	fred	robert	sam
jimmy	jack	peter	george
jerry	bill	tom	david
helen	stan	ray	kevin
debby	smith	mary	mike
claudia	steve	serg	james
brenda	matt	brian	michael
anna	dave	jim	john
alice	dan	maria	alex
brent	joe	leo	

Finally, the virus sends itself via SMTP, constructing messages using its own SMTP engine. The worm attempts to guess the recipient email server. First it probes the domain part of the email address then, if it fails, it prepends the following strings and issues a DNS query of that server for each:

mx.	smtp.	mxs.	relay.
mail.	mx1.	mail1.	ns.

If none of the queries is successful, or the virus fails to connect to the target SMTP server, it will use the locally defined SMTP server read from the registry.

The sender of the message is spoofed by the virus. One of the collected email addresses may be used for this purpose or, with a two per cent chance, the sender name will be a three- to five-character string with one of the following domain names:

aol.com	msn.com	yahoo.com	hotmail.com

This leads to all the usual problems caused by a virus outbreak. Not only did the virus generate an enormous number of infected messages, but even more were generated by misconfigured mail servers. First, many of the recipients were invalid addresses, either because they were generated randomly, or because the email address collecting routine of the worm is faulty (the routine only checks the '@' character – so, for example, the worm attempted to send itself to the address 'w32.zaushka@mm.zip' – without much success of course).

Some servers throw the message back to the spoofed sender, and another problem comes in the form of infection notification messages. Despite the fact that many of the most prolific mass mailers spoof the sender address, the majority of email gateways send infection notifications to the spoofed sender when an infected message is encountered.

Another advanced feature of email protection programs is to purge the messages that are known to be generated by mass mailers. Otherwise, if only the attachment is deleted, the message still comes through, increasing the number of useless messages; but without the attachment, it is not easy to filter them out.

KAZAA SPREADING

The worm copies itself into the download directory of the *Kazaa* peer-to-peer file exchange program. The location is read from the value of the registry key 'HKCU\Software\Kazaa\Transfer\DlDir0'. It uses one of the following file names:

winamp5	strip-girl-2.0bdcom_patches
icq2004-final	office_crack
activation_crack	nuke2004
rootkitXP	

The extension is .PIF, .BAT, .SCR or .EXE.

DENIAL OF SERVICE ATTACK

Between 1 February 2004 and 12 February 2004, Mydoom.A performs a denial-of-service (D0S) attack against the website www.sco.com.

Since the virus only checks the system date on startup, this action will not take place until the next startup of the infected computer within this time frame. Also, the attack will continue after the end date until the computer is rebooted (or the virus process is stopped, for that matter). The DoS attack takes place if the virus is started after 16:09:18 UTC.

The worm sends a GET request every millisecond to port 80 of the site being attacked. However, due to a bug in the virus code the attack will not begin on all infected computers after the start date. While checking the current date against the start date, the virus compares the two dwords separately, requiring each to be above the specified start date. Thus, even if the qword representing the current date is higher than the qword of the start date, the attack only starts if the low dword is higher as well. As the stored low dword of the attack is 0xbe9ecb00, the attack occurs on only about 25 per cent of the infected computers.

The same does not apply to the end-of-life date check, because if the high dword is later than the end date, the worm exits without checking the lower dword.

THE BACKDOOR

The virus drops SHIMGAPI.DLL, which is a backdoor component listening on the first available TCP ports between 3127 and 3198.

The DLL itself is stored in encoded form within the virus body. It is used for two purposes:

1. To establish a path to download and execute file to the infected computer.
2. To establish a proxy.

The DLL registers itself via the registry key:

HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 "(Default)" = %SysDir%\shimgapi.dll

The default value of this key is 'Webcheck.dll', which is a COM interface for web monitoring. With this modification the worm makes sure that the shimgapi.dll file is loaded into the address space of explorer.exe upon the next startup. On the first execution on an infected computer, the virus itself loads this library.

While searching for a free port, the backdoor starts from port 3127. If the port is not free, it waits for 400 ms and skips to the next port. If none of the ports up to 3198 are free, it waits another 800 ms and goes back to port 3127 to start the process all over again.

When an available port is found, the backdoor creates three threads that listen on that port. A counter increments on incoming connections. If only one free listener thread is available, the backdoor will open two more listener threads.

On incoming data the first byte serves as an ID. Only two values of this ID are supported in Mydoom.A. If anything else is sent, or an error occurs, an error status message is sent back.

If the ID is 85h, then four bytes are skipped, the next four bytes must match the magic dword 133C9EA2h. If this condition is true, the rest of the stream is saved into a temporary file and executed. An attempt was made to use this feature in Mydoom.B to update the systems infected with the original version of the worm.

If the ID is 4h, the rest of the stream is read, then the target IP address is extracted from the stream. If the backdoor can connect to the IP address, it acts as a proxy.

The first function enables an attacker to install a program of his will to the infected computer. All that needs to be done is to scan for these open ports, and then the computer is wide open for the attacker. Only a couple of days after the appearance of the virus there were already signs of port scans within this port region. Some of the scans were coming from sysadmins trying to find infected systems, but the volume of traffic seen was more than could be attributed to this source.

While the worm will not spread or perform the DoS attack if executed after the drop date, it will still create and execute the backdoor after its time has expired.

TAKE TWO

A couple of days after the original, a modified variant of Mydoom appeared. Its functionality was similar to that of the .A variant, with slight modifications. Mydoom.B infests itself as EXPLORER.EXE.

The subject lines are:

```
Returned mail       Mail Transaction Failed
Delivery Error      Mail Delivery System
Status              hello
Server Report       hi
```

And the message bodies:

- `sendmail daemon reported:`
- `Error #804 occured during SMTP session. Partial message has been received.`
- `Mail transaction failed. Partial message is available.`
- `The message contains Unicode characters and has been sent as a binary attachment.`
- `The message contains MIME-encoded graphics and has been sent as a binary attachment.`
- `The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.`

The filename of the attachment may be one of the following:

document	text	message
readme	data	body
doc	test	file

The worm copies itself into the download directory of the *Kazaa* peer-to-peer file exchange program. It uses one of the following file names:

- icq2004-final
- Winamp5
- Xsharez_scanner
- AttackXP-1.26
- ZapSetup_40_148
- NessusScan_pro
- MS04-01_hotfix
- BlackIce_Firewall_Enterpriseactivation_crack

Starting on 1 February 2004, Mydoom.B performs a denial of service attack against the website www.microsoft.com, and from 3 February 2004 against the website www.sco.com. The virus stops its activities upon the first system boot after 1 March 2004.

The virus modifies the hosts file to redirect the following websites to 0.0.0.0, thereby disabling access to them:

- ad.doubleclick.net
- ad.fastclick.net
- ads.fastclick.net
- ar.atwola.com
- atdmt.com
- avp.ch
- avp.com
- avp.ru
- awaps.net
- banner.fastclick.net
- banners.fastclick.net
- ca.com
- click.atdmt.com
- clicks.atdmt.com
- dispatch.mcafee.com
- download.mcafee.com
- download.microsoft.com
- downloads.microsoft.com
- engine.awaps.net
- fastclick.net
- f-secure.com
- ftp.f-secure.com
- ftp.sophos.com
- go.microsoft.com
- liveupdate.symantec.com
- mast.mcafee.com
- mcafee.com
- media.fastclick.net
- msdn.microsoft.com
- my-etrust.com
- nai.com
- networkassociates.com
- office.microsoft.com
- phx.corporate-ir.net
- secure.nai.com
- securityresponse.symantec.com
- service1.symantec.com
- sophos.com
- spd.atdmt.com
- support.microsoft.com
- symantec.com
- update.symantec.com
- updates.symantec.com
- us.mcafee.com
- vil.nai.com
- viruslist.ru
- windowsupdate.microsoft.com
- www.avp.ch
- www.avp.com
- www.avp.ru
- www.awaps.net
- www.ca.com
- www.fastclick.net
- www.f-secure.com
- www.kaspersky.ru
- www.mcafee.com
- www.microsoft.com
- www.my-etrust.com
- www.nai.com
- www.networkassociates.com
- www.sophos.com
- www.symantec.com
- www.trendmicro.com
- www.viruslist.ru
- www3.ca.com

One particular feature of Mydoom.B is worth mentioning. Using the file upload and execute feature of the backdoor component, the virus attempted to upgrade existing Mydoom.A infections with the new version. After activation it generated random IP addresses and attempted to upload itself to port 3127 of those systems. Fortunately and surprisingly, the .B variant did not spread well. While *MessageLabs* stopped over one million samples of the first variant on the first day, only eight samples of the second variant were found – which were most likely seeding samples.

There was also a bug in the DoS routine of the second variant. Due to a programming error (the same comparing error, coupled with another check), the attack against www.microsoft.com never occurs.

AFTERMATH

The sheer number of infected computers with the backdoor installed was too tempting an opportunity to let pass. Around 1 million computers were waiting for someone to send them just about any code to execute. The author of Mydoom.A couldn't resist this temptation, and wrote a new worm, Doomjuice.A. This had only one propagation method, the 'Mydoom backdoor' method. It attempted to connect to port 3127 of random IP addresses then sent itself for execution. On infected computers it dropped an archive containing the (almost) complete source code for Mydoom.A. This worm also had a fixed date check in the DoS procedure, for attacking www.microsoft.com.

CONCLUSION

Once again, a simple email worm hit the world. Mydoom did not use clever tricks or new exploits (in fact, not even old exploits) to launch its attachment automatically. It relied on the old click-and-run routine. It has been possible to configure *Outlook* and *Outlook Express* to block access to files with executable extensions for years. However, the majority of users do not bother to install the latest patches for these email clients and the vast majority of users have not learned the lesson of not clicking on attachments. We are bound to be doomed again in the future.

[In next month's VB Gabor Szappanos will look at the worms that use the backdoor component of Mydoom to spread in 'Life after Mydoom'.]