VIRUS ANALYSIS 1

HOW DUMARU?

Peter Ferrie
Symantec Security Response, USA

Take the SMTP client engine from W32/Mimail (see *VB*, September 2003, p.4), add some primitive social engineering in the email and some alternative-stream support from W2K/Stream (see *VB*, October 2000, p.6). Share the code freely so that others can add some backdoor capabilities and disable and/or remove other features. The resulting mess could be the W32/Dumaru family.

While Dumaru is classified as a virus family, the only variants that infect files are .A, .B, .D, .J, .Q and .T. Variants .F, .O, .S, .U and .AA do not even replicate, since their email replication code is disabled; these are simply backdoor programs.

AND I RAN …

Dumaru variants .A, .D, .J and .T begin by attempting to run the host code stored in an alternative stream called 'STR'. The alternative stream exists only on the Windows NT File System (NTFS). Interestingly, Dumaru.B and .Q also infect files, yet neither runs the host. Perhaps the author(s) of those variants considered the action to be unnecessary. This causes little trouble, though, owing to a bug in the infection code (described below).

After running the host, if applicable, all known Dumaru variants check for the existence of an atom, in order to prevent multiple copies of the virus running at the same time. The name of the atom is 'Program12345' in Dumaru.A, .D, .J and .T. The name changed to 'Program12345678' in variants .B–.V (excluding .D, .J and .T), to 'Program123' in Dumaru.W, 'Stamm-4' in variants .Y and .AB, and 'Stamm-2' in the .Z variant. The virus exits if the atom exists already, otherwise the virus creates it.

All known variants of Dumaru copy themselves to a number of locations, using several filenames, and alter the system in several ways in order to ensure that at least one copy is executed whenever *Windows* is restarted. All known variants copy themselves to the '%system%' directory and create a value named 'load32' under the 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run' key in the registry, to point to the copied file.

Dumaru variants .A–.X copy themselves as 'load32.exe'; variants .Y, .Z and .AB copy themselves as 'l32x.exe'. Variants .A–.V copy themselves to the '%windir%' directory as 'dllreg.exe', then create a value named 'run=', in the 'Windows' section of the '%windir%\win.ini' file, to point to the copied file. Under W*indows NT/2000/XP/2003*, this action is usually redirected to the 'Run' value under the 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' in the registry, however this behaviour is controlled by the values in the 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping' registry key.

All known variants of Dumaru copy themselves to the '%system%' directory, and create a value named 'shell=', in the 'Boot' section of the '%windir%\system.ini' file, to point to the copied file. Under W*indows NT/2000/XP/2003*, this action is usually redirected to the 'Shell' value under the 'HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' key in the registry. Variants .A–.X copy themselves as 'vxdmgr32.exe'; variants .Y, .Z and the .AB variant copy themselves as 'vxd32v.exe'.

All known variants of the virus except for .A, .D, .J and .T query the 'Startup' value under the 'HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders' key in the registry, and copy themselves to the directory listed there. All of those variants prior to Dumaru.Y copy themselves as 'rundllw.exe'; variants .Y, .Z and Dumaru.AB copy themselves as 'dllxw.exe'.

DROP AND GIVE ME TEN

At this point, Dumaru.A, .D, .J and .T create a file called 'windrv.exe' (if it did not exist already) in the '%windir%' directory, then run the file. This file is an IRC Trojan of limited capabilities (and not of sufficient interest to be described in detail here). All other known variants of Dumaru, except .L, .V, .Y, .Z and .AB, also carry this Trojan, though these variants will place it in a file called 'windrive.exe', and drop it at a later stage in their execution.

After dropping the 'windrv.exe' file, Dumaru.A, .D, .J and .T enumerate all drives from C: to Z:, looking for drives that are not CD-ROMs. For each such drive that is found, the virus changes to the root directory of that drive, and searches recursively for files whose suffix is 'exe'.

While performing the search, the virus skips the first entry in every directory. Although this is usually the '.' directory, this is not always the case (never for the root directory itself, and depending on the sorting order that is in use for subdirectories). Another bug exists in this code – since the search code in the virus does not change the current directory, a full path is required to access the file. In fact, the virus constructs the full path as required, but then passes only the filename to the infection routine. The result is that only files in the root directory can be infected.

The infection marker used by the virus is the presence of the read-only attribute on the file, with no other attributes set. The virus does not infect files that have only this attribute set. However, this causes a number of problems for the

virus. The virus is interested only in *Windows* Portable Executable (PE) files, but compares only the first three bytes of the four bytes in the PE signature. While this is generally sufficient, it is not always so. If the file is of the PE format, the virus enables filesystem compression for that file, if it is supported, using the DeviceIoControl() API that has been part of NTFS since *Windows NT 3.51*. This is the infection marker for W2K/Stream.

The virus creates a temporary file in the current directory, whose name begins with 'str', copies the found file to this temporary file, and attempts to copy itself over the file it found. This action fails if the file was read-only with other attributes set.

In the event that the copy was successful, the virus creates a stream called 'STR' in the copied file, and writes the temporary file to there, then attempts to delete the temporary file. This action fails if the file was read-only with other attributes set. The entire infection code (apart from the infection marker) is based on code from the W2K/Stream virus.

THE-MAIL

After infecting the files in the root directory, Dumaru.A, .D, .J, .T, .Y, .Z and .AB attempt to delete a file called 'winload.log' in the '%windir%' directory, then enumerate all drives from C: to Z: once again, looking for drives that are not CD-ROMs. For each such drive that is found, the virus searches recursively for files whose suffix is 'htm', 'wab', 'html', 'dbx', 'tbb' or 'abd'. The virus searches within these files for text that resembles email addresses. The code used to perform this search is identical to that used by the W32/Mimail family.

The virus stores each unique email address in the 'winload.log' file. Once the search has been completed, the virus waits for an active Internet connection. When one is found, the virus determines the email server name for each email address in the 'winload.log' file by performing a Mail eXchange (MX) lookup on the domain name, using the first DNS server known to the local machine, if available – otherwise the virus will use 199.166.6.2 (ns.execulink.com) for the DNS.

The code to perform this task is clearly written by someone else, in the style of the virus writer Zombie (see *VB*, March 2001, p.6). The code searches in memory for the address of certain APIs that are already freely available to the virus. There is additional code that is unused by all known variants of Dumaru, which would load ADVAPI32.DLL and NTDLL.DLL.

If the email server can be determined, the virus will send an email. For all known variants of Dumaru prior to .Y, the email appears to come from 'security@microsoft.com'; for Dumaru.Y, .Z and .AB, the mail appears to come from a *Hotmail* user.

The subject is usually 'Use this patch immediately !', except in variants .L, .O and .P, which have no subject, and Dumaru.Y, .Z and .AB, in which the subject is 'Important information for you. Read it immediately !'.

For all known variants of Dumaru, prior to .Y, the message body is:

```
Dear friend , use this Internet Explorer patch now!
There are dangerous virus in the Internet now!
More than 500.000 already infected!
```

For Dumaru.Y, .Z and .AB, the message body is:

```
Hi !
Here is my photo, that you asked for yesterday.
```

The boundary is always 'xxxx'. For all known variants of the virus prior to Dumaru.Y, the attachment name is 'patch.exe'; for Dumaru.Y, .Z and .AB, it is 'myphoto.zip', a Zip file that contains a stored copy of the virus, whose name is 'myphoto.jpg[57 spaces].exe'.

Variants .L, .O and .P also encode another copy of the exe file into a script that will execute using HTML format email. While sending mail, the virus writes mail server return codes to the console, however since the application uses the GUI subsystem, the texts are not displayed. Dumaru.A, .D, .J and .T exit after sending the emails.

GOSSAMER THREADS

All other known variants of Dumaru are multi-threaded. Dumaru.B and .Q create seven threads (ftp, tcp, mail, infect, proxy, clip, kwm) at this time. Other known variants of the virus have the mail and/or the infect threads removed. Dumaru.P contains only the mail, clip and kwm threads; Dumaru.Z contains only the mail, clip and mouse threads (perhaps because it downloads a variant of W32/Spybot, which contains far more functionality).

The most likely reason for the removal of the infect thread from other variants of Dumaru is the fatal bug that exists, which causes the virus to terminate entirely.

If the virus has not crashed, and is not Dumaru.V, .X, .Y, .Z or .AB, it enumerates the running processes and terminates any process whose filename matches any in the list that the virus carries. The list is identical in all known variants of the virus that contain this code, with the exception of Dumaru.P, in which one name is not present on the list, and Dumaru.AA, in which several names are not present on the list.

After creating the threads, all known variants of the virus prior to .Y create a file called 'guid32.dll' in the

'%windir%' directory. This file is a key-logging DLL. In Dumaru.H, .L, .M, .N, .O and .P, the DLL has been 'processed' in a manner similar to one of the infection methods that is present in W95/ZMist (see *VB*, March 2001, p.6). In Dumaru.Y, .Z and .AB, the key-logging functionality remains inside the virus itself. It functions similarly to the mouse thread that exists in the .W variant.

If the virus dropped the key-logging DLL, then it attempts to change the log filename in the DLL from 'SilentLog.txt' to '%windir%\vxdload.log' – however, doing so results in the corruption of the filename, with the degree of corruption depending on the length of the *Windows* directory name. In any case, the virus loads this file and uses it to install a system-wide keyboard hook, allowing logging to continue to run even after the virus exits. It is at this point that the remaining variants of Dumaru wait for an active Internet connection, then drop and run the 'windrive.exe' file.

HOW TYPE-ICAL

The virus enables keylogging now. The code contains placeholders for up to five words (11 in Dumaru.W, 18 in Dumaru.Y and .AB, and 8 in Dumaru.Z) for which to search in window titles. The presence of any of these words enables the key logging automatically. If no words are specified, then the virus logs keys for all windows.

Currently, only variants .H, .O, .P, .W, .Y, .Z and .AB check for specific words:

Dumaru.H checks for 'Bank', 'Banking', 'Logon', 'Westpac', 'gold'.

Dumaru.O checks for 'gold', 'bank', 'Logon', 'Bank', 'Money'.

Dumaru.P checks for 'e-gold', 'PayPal', 'eBay', 'Sign', 'Evocash'.

Dumaru.W checks for 'gold', 'WebMoney', 'WM Keeper', 'Fethard', 'fethard', 'bull', 'mull', 'PayPal', 'Bank', 'bank', 'cash'.

Dumaru.Y and .AB contain the same list as Dumaru.W, with the addition of 'Storm', 'e-metal', 'Keeper', 'Bull', 'ebay', 'localhost', 'Winamp'.

Dumaru.Z checks for 'e-gold Account Access', 'e-metal', 'bull', 'Bull', 'mull', 'PayPal', 'Bank', 'bank'.

For all known variants of Dumaru except .W, .Y and .Z, if the title of a window is the Russian equivalent of 'The entrance to WM Keeper', then the virus searches recursively on the A: drive for '.kwm' files, and writes the contents of each found file to a file called 'rundlln.sys' in the '%windir%' directory. Dumaru.W appears to be of German origin, so perhaps something specific to Russia is of no interest to the author of that variant. The .Y, .Z and .AB variants are all based on Dumaru.W, so the code is probably missing for the same reason.

Periodically, the virus constructs an email to send to certain email addresses. The content of the email varies between different variants of Dumaru, but always contains sensitive information, such as: the local machine's IP address; a list of passwords for the 'Far Manager' software retrieved from the 'HKCU\Software\Far\Plugins\FTP\Hosts' registry key; a WebMoney ID list retrieved from the 'HKCU\Software\WebMoney\Options' registry key; the 'vxdload.log' keylogger data file (although this will be empty because of the filename bug described above); the clipboard log file (see below), and the kwm log file (see below).

Dumaru.F, .S, .U and .AA send a list of ICQ numbers retrieved from the 'HKCU\Mirabilis\ICQ\Owners' registry key, and all files whose suffix is 'pwl' that were found by searching recursively in the '%windir%' directory.

Additionally, variants prior to Dumaru.Y drop and run a file called 'winimg.exe' in the '%windir%' directory. This file is a protected-storage password viewer. The file is run with the '/stext %windir%\rundllz.sys' parameter to force saving of the information to '%windir%\rundllz.sys'. The resulting file is sent, too. In Dumaru.Y, .Z and .AB, the protected-storage password viewing code exists in the virus itself, and the results are written directly into the email to send.

The delay before the virus sends the sensitive mail is variant-specific. The list follows:

Dumaru.B, .F, .H, .M–.O, .S:	every 30 minutes
Dumaru.C, .G, .K, .L:	every 5 minutes
Dumaru.E, .U:	every 2.5 minutes
Dumaru.I:	every 3.3 minutes
Dumaru.P:	every 23.3 minutes
Dumaru.Q:	every 50 seconds
Dumaru.R:	every 30 seconds
Dumaru.V:	every 15 minutes
Dumaru.W:	every ~21 minutes (*[1])
Dumaru.X–.Z, .AB:	every 20 minutes (*[2])
Dumaru.AA:	every 3 minutes

([1]) Dumaru.W also sends the keylog file whenever the file size exceeds 300 bytes.*
([2])Dumaru.Z also sends the keylog file whenever the file size exceeds 100 bytes.*

Dumaru.Z also checks for the existence of a value called 'mailsended' [sic] in the 'HKLM\Software\SARS' registry key, and sends the mail immediately if it is not present. After sending the mail, Dumaru.Z creates that registry value.

The recipients of the email are variant-specific. Additionally, most variants support the use of a file called

'email.dat' which contains a user-defined email address. In the absence of this file, the default address is used. The list of default addresses follows:

Dumaru.B:	x1234512345@centrum.cz
Dumaru.C, .G, .I, .L:	shogunn@world-banking.org
Dumaru.E, .Q, .R:	spbstels@rol.ru
Dumaru.F:	kollektinfo@mail.ru
Dumaru.H:	davailave@yandex.ru
Dumaru.K:	test799@altern.org
Dumaru.M, .O:	bank_acc@oligarh.ru
Dumaru.N:	bank-acc@yandex.ru
Dumaru.P:	trojan@e-e-mail.com
Dumaru.S:	kollekt-info@mail.ru
Dumaru.U:	info@domenov.net
Dumaru.V:	collector100@mail.ru
Dumaru.W:	geomir@centrum.cz
Dumaru.X:	pizdatiy_email1@list.ru
Dumaru.Y, .Z, .AB:	anyname@btw.egold-hosting.com
Dumaru.AA:	7653345@list.ru

Most variants of Dumaru will perform the MX lookup on the recipient's email address for the sensitive mail, too. However, variants .F, .U and .AA carry a list of servers (mxs.mail.ru, mx1.yandex.ru, mxd.rambler.ru, relay.hotbox.ru, mail.xaker.ru and mail.xakep.ru) and Dumaru.Y and .Z carry a single server (pop.btw.egold-hosting.com) to contact.

Additionally, variants .F, .U and .AA log in to POP3 servers before contacting another server. Those variants connect to 'pop3.rambler.ru' as user 'x1234512345' before sending through that server. Dumaru.F logs in to 'pop.mail.ru' as user 'pere-ssilka' before sending through 'smtp.mail.ru'; Dumaru.U logs in to 'pop.domenov.net' as user 'support@domenov.net' before sending through 'smtp.domenov.net'; Dumaru.AA logs in to 'pop.mail.ru' as user '5567' before sending through 'smtp.mail.ru'. [*The passwords used to access the sites are not given here, since some of the sites are still running - Ed*]. Those variants also retrieve the SMTP Server name from the 'Internet Account Manager' hive in the registry, and attempt to send the mail using that server.

In case the email sending is unsuccessful, there exists the option to send the data via FTP. Only a few of the variants support this option, and the FTP site, username, and password, are variant-specific. The list follows [*again, passwords removed to protect the innocent - Ed*]:

Variant	FTP site	Username
Dumaru.C:	ftp.calkopt.narod.ru	calkopt
Dumaru.G:	ftp.world-banking.org	cybercrime
Dumaru.M:	ftp.pcihotup.com	pcihotup
Dumaru.N:	fixletterop.com	fixlette
Dumaru.P:	mail-technic.com	ftp1475
Dumaru.U:	207.150.192.12	domenov0

FTP THREAD

The FTP thread listens on port 10000 for incoming connections and accepts commands from a remote machine. It behaves like an FTP server, sending appropriate messages, such as '220' (Service ready for new user) on connection. It accepts the following commands:

user	list	rmd	quit
pass	cwd	rnfr	type
stor	retr	rnto	rest
port	stor [again]	dele	cdup
pwd	mkd	syst	

The 'user' command simply returns '331' (User name okay, need password). The 'pass' command simply returns '230' (User logged in, proceed). The 'stor' command creates the specified file on the local machine, sends '150' (File status okay, about to open data connection), accepts files up to 1,000,000 bytes long, then sends '226' (Closing data connection. Requested file action successful).

The 'port' command accepts a port number (used by the 'list' and 'retr' commands below), then sends '200' (Command okay). The 'pwd' command sends the name of the current directory on the local machine.

The 'list' command connects to the remote machine on the port specified by the 'port' command, sends '150' (File status okay, about to open data connection), sends tree under current directory on the local machine, then sends '226' (Closing data connection. Requested file action successful).

The 'cwd' command sets the current directory on the local machine, then sends '250' (Requested file action okay, completed). The 'retr' command connects to the remote machine on the port specified by the 'port' command, sends '150' (File status okay, about to open data connection), sends specified file from the local machine, then sends '226' (Closing data connection. Requested file action successful).

The 'stor' command would behave as the first 'stor' command does, but with a file size limit of 512 bytes. However, the command is not accessible because of the duplicated name.

The 'mkd' command creates the specified directory on the local machine, then sends '257' (<PATHNAME> created). The 'rmd' command removes the specified directory from the local machine, then sends '250' (Requested file action okay, completed).

The 'rnfr' command assigns the destination filename for the file copy that is performed by the 'rnto' command below, then sends '350' (Requested file action pending further information).

The 'rnto' command renames the specified file on the local machine to the name specified by the 'rnfr' command above, then sends '250' (Requested file action okay, completed).

The 'dele' command deletes the specified file from the local machine, then sends '250' (Requested file action okay, completed). The 'syst' command sends 'system' information (always '220 111 Windows').

The 'quit' command sends '221' (Service closing control connection. Logged out if appropriate), and disconnects from the network, but the virus continues to run.

The 'type' command simply sends '200' (Command okay). The 'rest' command simply sends '350' (Requested file action pending further information).

The 'cdup' command changes to the parent directory on the local machine, then sends '200' (Command okay).

TCP THREAD

The TCP thread listens on port 1001 for incoming connections and accepts the following commands from a remote machine:

!exec	!cdopen	!sndplay	!screen
!quit	!cdclose	!msgbox	

The '!exec' command runs the specified file on the local machine. The '!quit' command disconnects from the network, but the virus continues to run.

The '!cdopen' command opens the CD-ROM drive door on the local machine. The '!cdclose' command closes the CD-ROM drive door on the local machine.

The '!sndplay' command plays the specified sound on the local machine. The '!msgbox' command displays a messagebox with the title 'THIS MACHINE IS CRACKED' and the specified message body. The '!screen' command saves the screen display to the specified file on the local machine.

Most variants of Dumaru support an additional command called '!email'. The '!email' command writes the specified address to 'email.dat' file in the '%windir%' directory.

PROXY THREAD

The proxy thread listens on port 2283 for incoming connections. If a received packet begins with the number '4' then the number '1', the virus connects to the specified IP address on the specified port and acts as a proxy for the remote machine.

CLIP THREAD

The clip thread copies small clipboard data (anything that is smaller than 32 bytes in length) to a file called 'rundllx.sys' in the '%windir%' directory.

KWM THREAD

The kwm thread begins by checking for the existence of a file called 'rundlln.sys' in the '%windir%' directory. If the file does not exist, the virus enumerates all drives from C: to Z:, looking for drives that are not CD-ROMs. For each such drive that is found, the virus searches recursively for files whose suffix is 'kwm'. Dumaru.W also searches for files whose name is 'fethard_keyfile' or 'account.cfg'. The virus writes the contents of each found file to the 'rundlln.sys' file.

On completion of the search, the virus creates a key under the 'HKLM\Software' registry key, then writes a value called 'kwmfound', containing '0' if no files were found, otherwise it writes '1'. For most known variants of Dumaru, this key is called 'SARS', however it is called 'AAAA' in Dumaru.O, and 'MSDRV' in Dumaru.P.

IRC THREAD

Dumaru.O and Dumaru.X contain an additional thread that connects on port 6667 (the default for IRC) to a certain channel on an IRC server. For Dumaru.O, the server is 64.191.107.10 (secure.timebase.us) and the channel is 'sars'; for Dumaru.X, the server is 'irc.wonka.net' and the channel is 'cooldman'. In either case, the virus joins the channel using a random nickname. The virus accepts the following commands via 'PRIVMSG':

download	email	stopdos
whois	dos	sendlogs

The 'download' command downloads and runs a file from the specified URL. The 'whois' command sends the local machine's IP address to the channel.

The 'email' command writes the specified address to 'email.dat' file. The 'dos' command connects to the specified site, then sends empty 4kb packets as quickly as possible, until told to stop by using the 'stopdos' command. The 'stopdos' command stops the denial-of-service (DoS) attack started by the 'dos' command above. The 'sendlogs' command sends the sensitive mail as a file to the specified FTP site.

MOUSE THREAD

Dumaru variants .W, .Y and .AB contain an additional thread that watches mouse events. When the left mouse button is pressed, the virus checks the window title of the current window. If the title matches 'C:\DATA\SRK.HTA' for Dumaru.W, or 'https://www.e-gold.com/srk.asp - Microsoft Internet Explorer' for Dumaru.Y and .AB, then the virus will capture the screen to a file whose name is a sequential number that begins at zero.

CONCLUSION

It was interesting to see the variants of Dumaru evolve over time, from a mass-mailing virus to 'simply' a backdoor program (albeit quite a complex one).

Despite the apparent number of different authors among the variants, the basic functionality of the virus did not change significantly. Apparently, not one of them seems to know about the existence of the strcat() function to concatenate strings. Just how dumarthey?

W32/Dumaru

Type:	Win32 SMTP mass-mailer worm.	
Size:	9,216 bytes (A)	34,818 bytes (O)
	34,304 bytes (B)	32,283 bytes (P)
	36,354 bytes (C)	34,308 bytes (Q)
	9,220 bytes (D)	36,352 bytes (R)
	36,352 bytes (E)	31,744 bytes (S)
	31,744 bytes (F)	9,240 bytes (T)
	36,352 bytes (G)	31,800 bytes (U)
	34,304 bytes (H)	31,232 bytes (V)
	36,354 bytes (I)	53,248 bytes (W)
	9,220 bytes (J)	34,304 bytes (X)
	36,354 bytes (K)	17,370 bytes (Y)
	32,768 bytes (L)	14,450 bytes (Z)
	34,305 bytes (M)	31,744 bytes (AA)
	34,305 bytes (N)	47,616 bytes (AB)
Payload:	Steals information, denial of service.	
Removal:	Fix registry, delete worm copies and its data files.	