VIRUS ANALYSIS 2

Raised Hacklez

Peter Ferrie
Symantec Security Response, Australia

When W32/Klez first appeared, it seemed like just another mass mailer of little note, but its later variants have spread so widely and rapidly that the Klez family has generated more interest. At the time of writing, there are 12 known variants of Klez. Despite the speed with which anti-virus developers released detection updates, despite the fact that some anti-virus products detected the later variants even before they were released, and despite its destructive payload, Klez remains a problem that shows no sign of being resolved in the near future.

The Buck Stops Here

All known variants of Klez begin with a call to a function in a dll that does not exist in *Windows 95* (*Windows 95* does not support Winsock 2.0), and import a function that does not exist in another dll in *Windows NT* (*Windows NT* does not support the Toolhelp interface). Therefore, Klez cannot replicate under either of these platforms. However, this has clearly proved to be not much of a limiting factor.

Copy Me, I want to Travel!

Klez creates several threads in order to perform a number of functions simultaneously. The first thread terminates certain applications – anti-virus and firewall programs – based on application name. Later variants also search for strings in process memory, and will terminate processes and delete files that contain them. Initially, this search was restricted to viruses, such as Nimda and SirCam, but the feature was extended later to include searching for anti-virus programs and the deletion of Registry keys.

Under *Windows 98*/*ME*, Klez writes itself to the Registry key 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run'. Early variants use 'krn132' as the value name and data, while the later ones use a name that begins with 'Wink' followed by two to four random letters. The result is that *Windows* launches the Klez file whenever the computer is booted. The thread is set to execute ten times per second, making it impossible to run on-demand anti-virus software for long enough to remove the virus. Later variants of Klez also run this routine (thousands of times) as part of the payload, but in such a way that processes will be terminated and files deleted, regardless of their content.

Dropping your Bundle

The second thread drops and runs the W32/Elkern virus, which is carried as a compressed file within the body of Klez. Klez decompresses this file and drops it using a random filename in the %temp% directory. Once execution of the file is complete, Klez will delete it.

When Elkern is run, it copies itself to the %system% directory, using a filename whose suffix depends on the platform upon which it is executed. Under *Windows 98*/*ME*, the filename is 'wqk.exe', and under *Windows 2000*/*XP* it is 'wqk.dll'. Klez is aware of this behaviour and under *Windows 98*/*ME* it will run wqk.exe; under *Windows 2000*/*XP*, it will load wqk.dll into its own process memory. This action will prevent the wqk file from being deleted, unless the Klez process is terminated first.

At this point, Klez copies itself to the %system% directory, using the same name as it used in the Registry. Under *Windows 98*/*ME*, Klez will then write itself to the Registry again, as above. If the RegisterServiceProcess() API exists, Klez will use this to register itself as a service, which removes it from the Task List. If the copied file is not running already, Klez will run it now.

Under *Windows 2000*/*XP*, Klez determines whether it is running as a service, using a rather complicated-looking method involving tokens and security IDs. If it is not running as a service, Klez will create a service, using the same name as it used in the Registry. If the copied file is not running, Klez will run it now, as a service. The most recent variants assign random values for the copied file's date and time, in an attempt to conceal its presence within sorted directory lists that would otherwise show the Klez file as the file created or modified most recently. Those variants that infect files will decompress and run the host file at this time.

Little Black Book

The third thread is used to send email. Klez uses the *Windows* Address Book as a source of email addresses, and assumes that the address book can be located from the Registry key 'HKCU\Software\Microsoft\WAB\WAB4\Wab File Name'.

This key is created by email products such as *Outlook* and *Outlook Express*, although others, such as *Exchange* and *Windows Messaging*, store the location of the address book using a different Registry key. Later variants of Klez also search for *ICQ* data files, which begin with 'db' or are called 'user.db'.

If it finds either the address book or an *ICQ* data file, Klez reads from there as many addresses as will fit into its 4 Kb buffer. Klez has two routines for reading email addresses. One supports the ANSI character encoding for addresses, as used on *Windows 98*/*ME* by *Outlook Express*, *ICQ*, and *Outlook* prior to *Outlook 2002*. The other routine supports

the Unicode character encoding for addresses, as used by all versions of *Outlook* and *Outlook Express* on *Windows 2000/XP*, and *Outlook 2002* on all platforms. However, Klez stores the Unicode addresses in ANSI format. Klez considers an email address valid if it contains one '@', followed by at least two characters, then a dot ('.'). Later variants of Klez check that there are additional characters following the dot.

If early variants find fewer than ten email addresses, Klez generates a random number of addresses (between 20 and 29), each containing three to nine letters, with the domain selected randomly from yahoo.com, hotmail.com and sina.com.

For each email address in the list, all known variants will select another address at random and use this as the 'From:' address. Klez prepends 'smtp' to the domain name in the 'From:' address, and attempts to connect to this server. If the connection is unsuccessful, Klez will enumerate the entries in 'HKCU\Software\Microsoft\Internet Account Manager\Accounts\' to find SMTP information and attempt to connect to the server that is found. If the connection is successful, Klez will attempt to send itself to the chosen email address. Thus, person A's computer will be used to send an email to person B, but the email will appear to have come from person C.

Get the Message

The early variants of Klez choose the subject of the email randomly from the following:

Hi
Hello
How are you?
Can you help me?
We want peace
Where will you go?
Congratulations!!!
Don't cry
Look at the pretty
Some advice on your shortcoming
Free XXX Pictures
A free hot porn site
Why don't you reply to me?
How about have dinner with me together?
Never kiss a stranger

Later variants use more complex subject generation. With a one in three chance, the current date will be checked against a list of specific dates. If the dates match, then the subject will begin with 'Happy' or 'Have a'. With another one in three chance (or always if the subject begins with 'Have a'), these variants will select one of the following words: new, funny, nice, humour, excite, good, powful [*sic*], followed by the name which relates to the date. The dates and names are as follows:

1 January: New year
6 January: Epiphany
2 February: Candlemas
14 February: Saint Valentine's Day
25 March: Lady Day
1 April: April Fools' Day
15 August: Assumption
31 October: Allhallowmas
2 November: All Souls'Day
25 December: Christmas

So the result may be, for example, 'Have a powful Candelmas', 'Happy Christmas', or 'Happy excite Lady Day'.

If no subject has been chosen yet, it may be left completely blank or begin with one of the following texts:

Undeliverable mail–
Returned mail–
Hi,
Hello,
Re:
Fw:

followed by any one of:

how are you
let's be friends
darling
don't drink too much
so cool a flash,enjoy it
your password
honey
some questions
please try again
welcome to my hometown
the Garden of Eden
introduction on ADSL
meeting notice
questionnaire
congratulations
sos!
japanese girl VS playboy
look,my beautiful girl friend
eager to see you
spice girls' vocal concert
japanese lass' sexy pictures

Alternatively, the subject may be a random string from a data file, or chosen from this list:

a %s %s game

a %s %s tool

a %s %s website

Each %s is replaced by a word from the adjective list described previously (new, funny, etc.).

Other subjects include 'a %s %s patch', where the first %s is replaced by an adjective, and the second by 'WinXP' or 'IE 6.0', and '%s removal tools', where %s is replaced by 'W32.Elkern' or 'W32.Klez'. The most recent variants of Klez may use the subject 'Worm Klez.E immunity'.

The email body of early variants contains a message which appears to be from the virus author, describing his financial situation. However, this message is not visible if the email is viewed in HTML format.

The message body in later variants remains empty unless the subject is one of those that contains a %s, the subject refers to Klez.E immunity,
or the subject begins with 'Undeliverable mail–' or 'Returned mail–'.

If the subject refers to an undeliverable or returned mail, the message body will read 'The following mail can't be sent to %s:', where %s is the random 'From:' email address, followed by 'The %s is the original mail', where %s is 'attachment' or 'file'.

If the subject refers to a removal tool, the message body will contain one of the following names: Symantec, Mcafee, F-Secure, Sophos, Trendmicro, or Kaspersky, followed by 'give you the %s removal tools', where %s is 'W32.Elkern' or 'W32.Klez'. The following line is either 'W32.Elkern is a %s dangerous virus that can infect on Win98/Me/2000/XP' or 'W32.Klez is a %s dangerous virus that can spread through email', where %s is 'very' or 'special'. This is followed by 'For more information,please visit http://www.%s.com', where %s is the name of the anti-virus vendor from the list above. The filename of the attachment is 'setup.exe' or 'install.exe'.

For emails whose subjects refer to a game, tool, or website, the message body will begin 'This is', then repeat the subject, followed by 'I %s you would %s it.', where the first %s is replaced by 'wish', 'hope' or 'expect', and the second is replaced by 'enjoy' or 'like'. The message may begin with 'Hi' or 'Hello'.

If the subject refers to a game, the message will continue with 'This game is my first work. You're the first player' and the name of the attachment will be one of the following: 'setup', 'install', 'demo', 'snoopy', 'picacu', 'kitty', 'play', 'rock'.

If the subject refers to Klez.E immunity, then the message body will read:

```
'Klez.E is the most common world-wide
spreading worm.It's very dangerous by
corrupting your files.

Because of its very smart stealth and
anti-anti-virus technic,most common AV
software can't detect or clean it.

We developed this free immunity tool to
defeat the malicious virus.

You only need to run this tool once,and
then Klez will never come into your PC.

NOTE: Because this tool acts as a fake
Klez to fool the real worm,some AV moni-
tor maybe cry when you run it.

If so,Ignore the warning,and select 'con-
tinue'

If you have any question,please
<a href=mailto:%s>mail to me</a>.'
```

where %s is replaced by the random 'From:' address.

If the subject does not refer to a removal tool, the suffix of the attachment will be .exe, .scr, .pif, or .bat.

Repeat as Required

In addition to the message body, there is HTML code that exploits a vulnerability in unpatched *Outlook* and *Outlook Express*. There are two parts to this vulnerability. The first is that applications can be launched automatically from an IFrame, without any prompt. The second part is that the MIME content type is trusted explicitly, without reference to the filename (and thus the file content), yet the launching of the application is performed by a part of *Windows* that does examine the filename. The result is that certain multimedia content types can be used to launch *Windows* executable files.

Klez uses this vulnerability to launch itself automatically. In addition to the viral attachment, if a data file is found (see below), there is a 50 to 100 per cent chance (depending on the variant) that Klez will attach this file to the email as well.

Once the email has been sent, the recipient's address is added to a master list. If the email connection proved unsuccessful, Klez will try five other addresses, selected at random from the email list. If the connection is still unsuccessful, Klez will try five addresses chosen randomly from its master list. Later variants of Klez also carry a list of open relays and will attempt to connect to one chosen at random from this list.

Regardless of whether the email has been sent successfully, the master list is updated each time, by removing the first entry and shifting the others up. This thread is executed repeatedly, at intervals of between 10 minutes and five hours, depending on the variant.

Share and Enjoy

The fourth thread that is created searches for open shares on the local area network. Klez will copy itself once to each shared directory. If a data file is found (see below), then Klez will use its filename without extension as its base filename, otherwise it will generate a random name, consisting of two to five letters followed by a number. To this will be attached two suffixes. The first is chosen randomly from txt, htm, doc, jpg, bmp and xls. The second is always '.exe'.

Later variants of Klez can also drop RAR archives, containing only the Klez file, into these directories. Under *Windows 2000/XP*, Klez will launch the file as a service on the remote computer. The more recent variants will also connect to the remote Registry and add an entry to the 'HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce' key to run the copied .exe file when the remote computer is rebooted. The danger of this action is clear: not only can Klez send an executable to another computer, but it can cause the file to execute, too. This thread is run repeatedly, at intervals of between 30 minutes and eight hours, depending on the variant.

Here's One I Made Earlier

Klez searches for data files to use as filenames on remote computers and as decoy attachments in emails. Later variants of Klez also look in these files for email addresses. Klez searches for files by creating 26 threads, one for each possible drive letter. On hard drives and network drives, Klez searches for files whose extension is in the following list: txt, htm, html, wab, doc, xls, jpg, cpp, c, pas, mpg, mpeg, bak, mp3.

Although only one filename is saved, the use of threads raises the possibility that the email and network routines will see different filenames. Later variants of Klez also delete anti-virus integrity database files whenever they are found, and replace RAR archives with new archives containing only the Klez file. Early variants of Klez execute these threads only once, but later variants execute them repeatedly, at intervals of between 30 minutes and eight hours, depending on the variant.

We're the Infectious Grooves

Later variants of Klez infect files. Klez enumerates the entries in the 'HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths' key, then searches all directories whose name contains the string 'Program'.

A file is a candidate for infection if it is not infected already, is not protected by the System File Protection that exists in *Windows 98/ME/2000/XP*, is between 67 Kb and 3 Mb in size, and its filename does not contain EXPLORER, CMMGR, msimn, icwconn, or winzip.

Klez infects by copying the original file to a random filename and replacing the original contents with itself. The size of the infected file is not altered, which is why infectable files must be at least as large as Klez itself. The copied file is then compressed using a Run-Length Encoding algorithm, and the file attributes are set to Hidden, System, and Read-Only, to hide it from the default directory listings. This thread is executed once every hour.

The Wait is Over

It is at this point that Klez checks whether its payload should trigger. The payload activates during odd-numbered months (January, March, May, July, September and November). The early variants of Klez activate on the 13th of those months, while later variants activate on the 6th of those months.

When the payload activates, Klez creates 26 threads, one for each possible drive letter. If the drive is a hard drive or a network drive, Klez will search for files in all directories, and overwrite the files entirely with data from memory.

For early variants of Klez under *Windows 98/ME*, the data will be random, and under *Windows 2000/XP*, the data will be the characters 'BA AD F0 0D' (a *Windows* default value); for later variants of Klez, the data will be zeroes for all platforms.

Early variants affect all files in this way, but later variants of Klez affect all files only during January and July. At other times, only files with extensions that are included in the data file list above are affected. Early variants of Klez execute this thread every 30 minutes, but later variants execute it only once.

Conclusion

What conclusions can be drawn from Klez? It seems that the combination of an old exploit with social engineering can convince an enormous number of people to open attachments from people they don't know.

Klez does not present new ways to replicate, only new words to entice people to help it replicate. Some computers experience symptoms and their owners seek a cure, while others do nothing and allow the replication to continue.

It will take a change in people's behaviour to halt the spread of viruses like Klez... Klez: the new social disease.

W32/Klez	
Type:	Memory-resident, direct-action companion infector.
Infects:	*Windows* Portable Executable files.
Payload:	Date-triggered file deletion.
Removal:	Delete infected files and restore them from backup.