Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment
Version 1.3 (amended December 12, 2001)

This assignment has been submitted by:
Rogan Mallon

"The W32.Klez.E@mm virus, and how it relates to a 'defence in depth' security model."

CONTENTS

ABSTRACT:

This article uses the properties of a recent virus to expand on multiple key issues in the world of Information Security.
The virus is a Windows 32bit Platform mass mailing worm, that also propagates through network drives and shares and is known as the Klez virus.
The article will investigate how the virus can be defeated at several different levels throughout its intended journey from one machine to the next. It will also cover the techniques the virus employed to attempt to circumvent these various defensive strategies. Furthermore the article discusses the role of anti-virus vendors in reacting and reporting new virus threats, and suggests the need for some alternative to the current situation whereby six different ratings were issued for the same virus. Finally the article concludes by suggesting that overall information security has improved dramatically, but also warns on the need to remain vigilant in expectance of the next major threat.

Introduction:

"I Love You". "CodeRed". "Nimda". "Ana Kournikova". "Klez".

If you were asked to pick the 'odd one out' in the list above, assuming one was relatively well versed on computer viruses, it would be safe to venture that your answer would be 'Klez'.
The first four listed, 'I Love You', 'CodeRed', 'Nimda' and 'Ana Kournikova' could all be considered high profile viruses, indeed they all made headlines in the national television news [in this author's country at least].
However it is this last virus that I would like to discuss in this article, for it affords the opportunity to highlight a few points worthy of further investigation. For instance, the Klez virus exploited a known vulnerability. It used methods of propagation that have already been seen in other viruses. It had mechanisms to defeat some 'defence in depth' strategies that may already be deployed in your company. It also had another interesting trait, whereby it tried to disable two of the 'high profile' viruses already mentioned above, namely 'Nimda' and 'CodeRed'.

The Virus:

The Klez virus, also known as; W32.Klez.E@mm, Klez.E, W32/Klez.F, WORM_KLEZ.E, W32/Klez-E, was discovered around the 17th of January 2002.
There are also a couple of other variants of the Klez virus, W32.Klez.A@mm also known as W32.Poverty.A@mm, W32.Klez.gen@mm, and

W32.Klez.D@mm also known as W32.Klez.B@mm.
For the purposes of this article however, the name "Klez" refers to the W32.Klez.E@mm variant.
Interestingly enough, a number of high profile antivirus vendors initially 'rated' the Klez virus as a relatively low risk.

The McAfee web site begins their description with:

> "-- Update 3/4/2002 --
> Due to a slow, but steady, increase in prevalence over the past few weeks, AVERT has raised the risk assessment of this threat to MEDIUM."

Similarly, the Symantec site states:

> "Due to an increased rate of submissions, Symantec Security Response is upgrading the threat level for W32.Klez.E@mm from level 2 to level 3 as of March 6, 2002."

How Does It Work:

So what is the Klez virus's modus operandi?
First and foremost, Klez is a 32bit Windows executable that affects multiple Windows Platforms, and exploits a known vulnerability in Internet Explorer, Outlook and Outlook Express.
Klez is described as a virus - more specifically a 'worm' virus – and a 'mass mailer'. A mass mailer attempts to spread itself via email to as many computers as possible. With a bit of luck the target computer will not only be one of the affected platforms, but will also have in place the necessary conditions required by the virus to continue on its path of replication. In the case of Klez, those conditions included the recipient computer running a 32bit Windows Operating System, and preferably that the computer was part of a network that had 'open' network shares. Ideally the user would be utilizing an un-patched version of Outlook or Outlook Express as their email client application.
A 'Worm' is a virus that attempts to self-replicate. Self-replication simply means that the virus has some built-in mechanism whereby it can propagate itself to other computers generally via email and network shares, without specifically relying on end-user intervention. For Klez the self-propagation mechanism is to farm the Windows Address Book, ICQ Database as well as html and txt files for email addresses it can then use to email itself out to. Klez includes it's own SMTP engine, as well as the intelligence to guess at available SMTP servers to contact. As well as this Klez will try to spread via network shares by placing copies of itself in shared folders and mapped drives on the network where it can obtain 'write' access.
One key caveat for Klez - and other similar viruses - to be able to continue infection is that it still needs to be executed or launched upon arrival to a users' computer as an email attachment..

Many Security Professionals and Network Administrators will tell you that one of the key "Anti-Virus Education" messages they try to convey to their end users is "Don't run attachments without being absolutely certain of who sent it or what their contents are!"

Vulnerability Exploit:

Klez however, is one step ahead of the user in this respect. Klez uses a 'vulnerability' in the recipients email application whereby simply opening or even just previewing a message an attachment is able to *automatically* execute. The following article details this vulnerability:

"Incorrect MIME Header Can Cause IE to Execute E-mail Attachment"

Surely then one could be excused for becoming infected by Klez, as the user has no way to know before opening or previewing a message that there is any malicious content.
As it turns out, further investigation reveals that the vulnerability is not one that has only just been uncovered with the advent of the Klez virus.
In fact the article was "Originally posted: March 29, 2001" and includes links allowing anyone to download patches to fix the problem.
Herein lies a major issue in today's world of computing – it is vitally important that computer users make a habit of keeping up to date with patches and fixes.

The Analogy:

Furthermore it raises an interesting question. Is it reasonable to hold software vendors responsible for flaws that leave one vulnerable to attack?
Consider for a moment a scenario where one purchases a product of any sort – let's say it's a new car. Now it turns out that this car is susceptible to [possibly irreparable] engine failure due to a particular part the car manufacturer chose to use, or even left out altogether. Would one now be expected to become semi-mechanically savvy, pinpoint the issue, track down the solution, then finally to repair it themself? On top of all of this, would they also be expected to cover all the costs involved?
Often times people try to draw analogies between the computing world and other everyday business, something that is not an easy task. In fact if we place this car analogy under closer examination, we see it has many debatable points, but I would like to reiterate the central theme. In almost any other industry it would be completely unacceptable for a company to release a product that, due to a manufacturing fault, puts a large percentage of their customers at risk of product damage or even failure. Yet we seem to accept this as an everyday risk of owning or using a computer and or computer software.
To continue the analogy a little further, one could say that at least in the case of the car, an individual is free to dismantle it to try to find the issue and fix it

themself. This is largely impossible with computer software.
Conversely though, we are seeing today a lot more open source software in the market. The debate rages over the relative merits of open source versus proprietary software, but one thing that open source has in it's favour is that at least it is possible now to 'get under the hood' so to speak, albeit that the average computer 'motorist' still has to take the software to their programmer-mechanic. At least however, they are no longer necessarily forced to rely on the manufacturer releasing a patch or version upgrade.

The Partner:

We can see then that Klez *exploited a known vulnerability*. Investigating further we discover some more interesting traits. For instance Klez included another virus in its payload namely the Elkern virus.

According to the Symantec Security Response Site, Elkern

> "…is a virus that infects files over open shares, mapped drives; it also tries to infect all executable files in the \Windows\System folder.
> If it is activated under Windows NT/2000, then this virus will crash when first activated.
> If it is activated under Windows 9x and you have a mapped network share that is write-protected, then this virus will crash your computer after a short period. Some files that become infected with this virus will not change in size.
> This virus has a payload that will destroy all files on locally connected drives (including mapped drives).
> This payload becomes active on:
> - March 13
> - September 13
>
> When executed, the virus also has a very small chance of randomly activating this payload."

The Origin:

The relationship between these two viruses is an interesting one. Did they originate from the same source? Are the closely related variants of each also from the same source? Do we know or can we find the source?
According to an article on the ZDNet website http://www.zdnet.com, the original Klez variant may have originated as a job application from a programmer situated in China, who's simple wish was to be able to support his or her parents.

"**Klez worm may be a job request from a Chinese programmer**"

Anti-virus and Content Filters:

Furthermore, Klez disabled real time virus scan mechanisms and crippled many different versions of Anti-virus software. The fact that Klez was able to do this seems at first sight to be almost laughable. Is it not after all the job of Anti-virus products to protect a computer from these very same viruses? This is true, but it is also true that no matter how good an Anti-virus vendor is, or how fast their response time may be, the ability to immediately detect and protect a user from a virus that has not yet been 'seen' or discovered is virtually impossible.
Anti-virus technology is still for the most part a re-active technology.
A person can after all take any number of vaccines to protect them from known diseases and viruses, but if you want to protect yourself from unknown risks then you need to minimise your risk factors. This is also the case in terms of computers.
There are a number of products on the market that will allow one to 'minimise' their risk of infection.
Firstly, firewalls do a good job of minimizing risk in a corporate environment. Like the security guard in your office, they will stop all unwanted traffic at the door before they get inside to do anything malicious. Unfortunately, just like the security guard, your firewall will still let your mail come through, normally without question.
Content filters can then be our next line of defence for mass mailing viruses. The job of the mail content filter is to inspect the 'envelopes', check the sender and even to open up the message and have a look inside.
In the instance of a virus such as 'the love bug' a content filtering product was a major benefit. It allowed network administrators to block the virus by not allowing any messages that had "I Love You" as their subject. This had the added benefit of protecting a network from a dangerous threat simply by not allowing the virus entry to the mailboxes in the first place. All this can happen even before the various Anti-virus vendors are able to issue updates to their virus signatures.
Furthermore, even though your workstations may all have their respective virus products updated, you cannot be certain that everyone in the outside world has done likewise. Therefore the content filter maintains its effectiveness by continuing to block the incoming virus.
In the case of Klez however, the 'blocking by subject line' technique loses its effectiveness, as Klez is able to generate semi-random subject lines.

Below are examples of subject lines observed by McAfee technicians:

> "In our experiments we have, for example, observed the following Subject lines (more common at the top):
>
> Subject: Document End
> Subject: Happy Lady Day
> Subject: From
> Subject: Eager to see you
> Subject: Returned mail--"Document End "
> Subject: HEIGHT
> Subject: A WinXP patch

Subject: Hi,spice girls' vocal concert
Subject: Happy nice Lady Day
Subject: Have a humour Lady Day
Subject: Happy good Lady Day
Subject: ALIGN
Subject: Have a good Lady Day
Subject: Undeliverable mail--"IIS services with this Web administration tool."
(The virus can also send mails with empty Subject and/or body)"

This is where the attachment-blocking feature of a content filtering product will serve well. In terms of the Klez virus, the attachment was known to have certain file extensions:

"**Attached file:** Randomly named with extension .PIF, .SCR, .EXE or .BAT."
http://www.sophos.com/virusinfo/analyses/w32kleze.html

Now you have your content filter pro-actively protecting your email gateway. The trade off however is that by blocking these extensions you may well be hindering legitimate day-to-day business if the file extensions being blocked are the same as those used in the course of conducting ordinary non-malicious communications.
This is where it is beneficial to have already developed and documented a policy with respect to the types of attachments that can be sent and received by users of the network, and a documented emergency response procedure for temporarily or permanently adding or removing file-types from the content filtering 'blacklist'.

Network Shares:

The next layer of defence for Klez is at the file sharing level. Information garnered from the Symantec Security Response site informs that:

"The [Klez] worm copies itself to local, mapped, and network drives as:

- A random file name with a double extension. For example, filename.txt.exe.
- A .rar archive with a double extension. For example, filename.txt.rar.

There are several tools to help in identifying insecure shares on your network. Legion, from PacketStorm is but one example. There is also a useful article on the threat of network shares available at:
http://rr.sans.org/threats/file_shares.php

Removal:

So what happens if this virus finally does make it's way to one of the machines in your network?
Firstly, one of the best things to consider doing with any machine infected with a virus that propagates on a network, is to disconnect that machine physically from the network. Often times it can be as simple updating an already installed Anti-virus product, and scanning the infected machine for the new virus. Unfortunately this is not always practicable, especially with the Klez virus, as it disabled on-access virus scanners by stopping certain services from running and deleted other essential working files for these products– oddly enough it also attempted to stop some other worms such as Nimda and CodeRed from running in memory.
In the instance of the Klez virus, it also employed a now common virus technique of inserting itself into one of several areas that will allow it to initiate during machine start-up.

For the Klez virus, it attempted to do this in the following manner:

> "When executed, the worm copies itself to %System%\Wink[random characters].exe
> NOTE: %System% is a variable. The worm locates the Windows System folder (by default this is C:\Windows\System or C:\Winnt\System32) and copies itself to that location.
>
> It adds the value:
> Wink[random characters] %System%\Wink[random characters].exe
>
> to the registry key:
>
> HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
>
> or it creates the registry key:
>
> HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Wink[random characters]
> and inserts a value in that subkey so that the worm is executed when you start Windows."
>
> http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.klez.e@mm.html

It is for this very reason that it is not always prudent to shut down or restart a computer you suspect has an infection. It may have altered the machine in some way so as to activate or trigger some mechanism only upon re-starting the system. It is certainly worthwhile interrogating the machine before shutting down or restarting. With the Klez virus, if you were to inspect the registry and find the key above had already been created, it would not necessarily do you any good to simply delete it, as the virus also had the ability to recreate the registry key immediately.
Indeed if your Windows machine was already infected then it was necessary

to restart in “safe mode”. Starting the machine in safe mode meant the virus was not allowed to load into memory first, and it was possible to delete both the registry key it created, and the virus file itself.

The Vendors:

Consulting various Anti-virus vendors’ websites will provide detailed instructions for removal of the Klez virus from the different Windows platforms, and this is generally the case for all viruses.
In fact it is common for the Anti-virus vendors to continually update their information as they learn more and more about a virus.
Hence it would be deemed good practice for any Security Professional to consult multiple sources when trying to handle any new threat:

> “"When attempting to put a finger on the real risk of a virus, it is important to review at least three major vendors' Web sites," said analyst David Bass at PricewaterhouseCoopers in New York. "A user or administrator should not jump to conclusions based on information on any one vendor's site."
> http://www.nwfusion.com/news/2002/0311virus.html

Even two months after the discovery of the Klez virus, it is possible to find information on some vendor’s sites that is not included in others. Fortunately none of the information provided by any given Anti-virus vendor seems to be in direct conflict with any other vendor, but rather most of it is complimentary. For example, Canada's Sensible Security Solutions site informs that the Klez virus has a payload:

> **Payload**
>
> Large scale e-mailing: Emails all addresses in the Windows Address Book (WAB).
> Capable of spreading itself across network drives via shared folders with read/write access.
> Deletes files: Deletes some anti-virus related files.
> Disables common antivirus products.

The above site doesn’t mention however, as on the Sophos site that:

> “On the 6th of March, May, September and November the worm will overwrite files on all drives which have one of the following extensions. TXT, HTM, HTML, WAB, DOC, XLS, JPG, C, PAS, MPG, MPEG, BAK, MP3”

Or, as reported by Symantec

> “If the month is January or July, this payload attempts to overwrite *all files* with zeroes, not just those with the aforementioned extensions.”

Something that does differ from one vendor to another is their actual 'rating' of a virus. The author of the article "Virus alerts lack standards" sums up this issue:

> "The lack of consensus and standard threat-rating procedures for virus outbreaks was highlighted last week, when six of the major antivirus vendors issued six different threat levels for the Klez.E worm. All six vendors that issued warnings acknowledged the need for a standard warning system."
> http://www.nwfusion.com/news/2002/0311virus.html

In fact at least two vendors proceeded to upgrade their threat ratings several weeks after the initial discovery of the Klez virus.
On top of all of this, because these particular vendors rated the virus as a 'low' threat, the new signatures were not readily available until nearly a week after the discovery. It is understandable when one considers the logistics of testing and releasing new signatures for every single virus that appears, that vendors may only release signature updates at regular intervals – each update encompassing more than a single new virus signature. Following this rationale however, and assuming the vendors will make 'special signature releases' when a high threat virus appears 'in the wild', it is vitally important that the vendors get it exactly right when attempting to ascertain the potential threat of a new virus.
It would certainly be in the consumers' best interests if the anti-virus vendors could also agree on a standard for determining the threat imposed by a newly discovered virus.
Alternatively, it may be an option to do away with grading altogether, and treat all viruses as a threat.
Having said all this though, it is also important for the consumers to realise the importance of the role they play in the bigger 'security' picture by providing this data for the vendors. It is not acceptable to continually sit back and solely rely on the vendors to "get it right". Everybody has to be prepared to step up and play his or her part. Build that relationship with you vendor, and make it a habit to report back your findings. Only by pooling collective experiences and knowledge will it be possible to report useful and meaningful information back to the general public.

Unsuccessful:

Overall the Klez virus seems to have all the traits of another potential "Love Bug" or "Ana Kournikova". It targets a platform widely in use. It has the ability, given the right conditions, to activate without user intervention. It has multiple methods of propagation. It even disables some Anti-virus products. Why then, has it not made as big of an impact as some of the other better-known viruses?
Perhaps it is because the computing community as a whole have learned

from their past mistakes. More people have some form of anti-virus protection on their personal machines than even just a couple of years ago. These same people are maybe more diligent in keeping their virus signatures up to date. Maybe they are more suspicious when it comes to opening emails and their attachments than in the past. In the corporate space it could be due to more companies adopting a much more in depth, multi-tiered security model. It could be due to more and better firewall technology, content filtering products and their intelligent deployment. Perhaps even, we are seeing quicker responses on all fronts during times of potential crisis. Not only from the software vendors protecting their customers from the threats, but also from the security professionals in the field who are actually implementing these technologies and monitoring the environment on a day-to-day basis.
Maybe even it is possible that the Internet community as a whole is slowly but surely winning the battle against malicious attacks on several different fronts.
Is the next Love Bug, Nimda, CodeRed or Ana Kournikova just around the corner, or is there something even more spectacular in scale, some 'sleeping giant' just waiting to be woken from its slumber?

Conclusion:

In conclusion, although the Klez virus was relatively innocuous in the greater sense of the virus world, it still served to remind everyone how vital it is to stay awake. The mass mailing characteristics, which by their very nature meant a user would most likely receive the virus from someone who was known to them, reminded everyone to stay vigilant when it comes to receiving email attachments if they are not necessarily expecting them. The vulnerability exploit served to remind users and administrators they must ensure that they stay up to date with the very latest patches and fixes. The use of certain file extension types reminded companies of the virtues of filtering their email as it arrives on their cyber-doorstep. The network propagation reiterated the need to be more prudent when sharing files folders and drives with everyone on the network. The potential to destroy vital data was a timely reminder of how important it is to keep backups of information. The fact that it received six different ratings from six different Anti-virus vendors, was a reminder of how important it is, not only to collate information from as many different sources as possible when considering a course of action for whatever the latest threat may be, but also reminding security professionals everywhere of the key part they have to play by providing feedback for the vendors to utilize in their decision making.
The need for 'defence in depth' has been reinforced. Perimeter firewalls, gateway anti-virus, mail content filters, desktop anti-virus, desktop firewalls, intrusion detection, and regular vulnerability assessment all have their part to play in the overall safe keeping of essential business and personal resources.

References:

Klez Worm Attempts to Overwrite Files
Dennis Fisher
January 18, 2002
http://www.eweek.com/article/0,3658,s%253D701%2526a%253D21462,00.asp

McAfee – AVERT
http://vil.nai.com/vil/content/v_99367.htm

Norman - the antivirus company
http://www.norman.com/virus_info/w32_klez_f_mm.shtml

Open File Shares: An Unexpected Business Risk
Jaime Carpenter
June 21, 2001
http://rr.sans.org/threats/file_shares.php

Sensible Security Solutions - W32.Klez.E@mm Virus Information
http://www.canada-av.com/sensible/home.nsf/adaa5c5ed383cbbd85256894005ff0dc/95cb83d918f36ad185256b45004e8abd?OpenDocument

Sophos virus analysis: W32/Klez-E
http://www.sophos.com/virusinfo/analyses/w32kleze.html

Symantec Security Response - W32.Klez.E@mm
http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.klez.e@mm.html

Trends glossary of terms:
http://www.antivirus.com/vinfo/virusencyclo/glossary.asp#virus_types

Virus alerts lack standards
Dan Verton
March 11, 2002
http://www.nwfusion.com/news/2002/0311virus.html

ZDNet: Klez worm may be a job request from a Chinese programmer
Robert Vamosi
October 26, 2001
http://www.nwfusion.com/news/2002/0311virus.html

NB: Any sources directly quoted in the body of the article have been indented, and where the URL has not been explicitly stated, it has been used

as an obvious hyperlink. Those references also appear above.