Who Is This Melissa Anyway?

Chengi Jimmy Kuo
Director, AntiVirus Research, Network Associates Inc.

The presentation will go over the details of the Melissa virus, including lesser known side-effects and ramifications resulting from the virus. It will also detail the sequence of events which led to the capture of the person who is alleged to have distributed the virus. There will be discussion about the viruses which followed Melissa, such as CIH (Chernobyl), Papa, and ExploreZip. Finally, as events continue to unfold in this arena, as time permits, we will cover anything else occurring in the antivirus arena which may be more pressing at the time of the presentation.

Chengi Jimmy Kuo is an NAI Fellow at Network Associates (formerly McAfee) where he has been for over 4 years and serves as the Director of AntiVirus Research. He has spoken and published at numerous industry conferences and been quoted in newspapers around the world on the subject of computer viruses. He was a panelist at last year's NISS Conference to offer Free Macro AntiVirus Techniques. He is a graduate of the California Institute of Technology, BS 1982.

Who's watching your network

Who Is This Melissa Anyway?

Network Associates, Inc.

Jimmy Kuo

Director, AV Research

jkuo@nai.com

Agenda

- Description of virus
- The effects
- What are we to learn?
- Who done it?
- ExploreZip
- What else?

W97M/Melissa

All the time, every time

- Word macro virus
  - Infects Word97 and Word2000
  - Resets Word macro protection

```
PrivateProfileString("",
    "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
    "Level") = 1&
Else
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):
    Options.SaveNormalPrompt = (1 - 1)
End If
```

network ASSOCIATES

W97M/Melissa

```
UngaDasOutlook = CreateObject("Outlook.Application")
DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
```

Been there, done that?

```
If PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "...
    by Kwyjibo" Then
```

If Outlook98 or Outlook2000 installed

```
If UngaDasOutlook = "Outlook" Then
```

- For each address book

```
For y <= 1 To DasMapiName.AddressLists.Count
    AddyBook = DasMapiName.AddressLists(y)
```

- Grab up to 50 mail addresses

```
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
```

W97M/Melissa

Set up the mail message

Subject: Important Message From <your name here>

Message text:

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

- **Most of the first 50 are mailing lists.**

Set registry

PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"

W97M/Melissa

One last thing

'WORD/Melissa written by Kwyjibo

'Works in both Word 2000 and Word 97

'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

The Simpsons tie-in

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

It's the Mailing Lists

50 to 50 to 50?

- It's the same entries in everyone's address books.
  - Except for the personal address book.
- Means the same people are going to get many copies of the same LIST.DOC.
- In order to get 60,000 mails in the server, you need a LOT of stupid people.

It's the mailing lists!

- Each time someone double-clicks, thousands of emails are generated.

Lesser Known Melissa Effects

The name of the file is LIST.DOC.

- Melissa mails the active document, which remains the same document every time.

LISTn.DOC

- Eudora
  - Same named files get numeric suffix

Lesser Known Melissa Effects

Later, infected users will send infected documents to someone who hasn't been affected by Melissa before.

This second person, if not protected, will divulge to the world your hard work.

Lesser Known Melissa Effects

On certain (my assessment: unlikely) conditions, Melissa will end up sending uninfected documents:

- **"Melissa?" registry setting is not "inoculated"**
- **User site (normal.dot) infected.**

Result:

Widely infected sites must also use Exchange's feature of subject line filtering.

network ASSOCIATES

Psychological Effects

Previously:

"Know who you're dealing with."

Now:

"Trust noone!"

Desired Psychological Effect

Virus cases get law enforcement attention.

We need some global companies to file suit in other countries against the person who released Melissa. Just the news that other countries will seek to prosecute will make virus writers more aware that they are affected by the law worldwide.

Lessons

Expect to work weekends!

Establish corporate policy against people cruising sex related newsgroups, especially on Fridays.

Lessons

Lock out those mailing lists!

How many times have you seen a message to "All" that you thought was meaningful?

How many times have you seen "goodbye" messages sent to "All?"

Lessons

Upgrade to Office 2000.

Set all security settings to High!

- If someone says they need the setting to be something different, let them set it themselves.
- Doing so, they will at least be aware that they changed it.
- Expose them to some of the Free Macro AntiVirus Techniques.

Lessons

Mail server antivirus scanners are more than just "nice to have."

Protecting against Melissa using a mail server takes hours if not minutes.

Protection via desktop products will never have full confidence that the problem is resolved.

Who Done It?

Who's watching your network

Virus Patrol

WARNING! A virus has been found in a binary file posted to the following newsgroup(s):

alt.sex

Message header follows:

>Message-Id: <19990326071553.24526.00000525@ng-cg1.aol.com>
>From: skyroket@aol.com (Sky Roket)
>Subject: Passcode List 3-26-99
>Date: 26 Mar 1999 20:15:53

Dr Solomon's FindVirus/VirusScan report follows:

Dr Solomon's FindVirus IN-HOUSE version. Copyright (c) 1999 Network Associates Inc.
Drivers : 26 Mar 1999
Scanning for 42254 viruses, trojans and variants.

list.zip\LIST.DOC ... Found the W97M/Melissa virus !!!

network ASSOCIATES

Skyroket@aol.com

Screen name Sky Roket is Scott Steinmetz-

from Lynnwood WA-

born 2-25-62

Male

Married

Hobbies: Historical Gamming, Miniature Gamming, and of coarse computers

Computers: AST Premium

Occupation: Civil engineer

Personal Quote: Be happy in all you do

Search for Scott Steinmetz

How Jimmy Kuo spent his Saturday:

- Search the internet: Internet white pages (lycos.com, altavista.net, yahoo.com, excite.com)
- Only Scott Steinmetz in Washington is in a different part of WA.
- Only 2 Steinmetz in Lynnwood, not him.
- Contact Seattle Times (Wired magazine also investigating)
- Both reporters able to find unlisted telephone number and talk to Mr. Steinmetz.
- Both report: "He can't be the one!"

AOL

- Scott Steinmetz says his login id was compromised (stolen).
- AOL searches for "Who logged into that account and posted to the newsgroup at the time specified?"

Message-Id: <19990326071553.24526.00000525@ng-cg1.aol.com**>**
From: skyroket@aol.com (Sky Roket)
Date: 26 Mar 1999 20:15:53

- IP address of user found.
- IP belongs to Monmouth ISP.

network ASSOCIATES

Got Him

- Search warrant presented to Monmouth ISP.
- IP is issued to dialups. Phone number which connected to that ISP is located.
- FBI and police go to house. No one home.
- Neighbors tell of brother.
- Go to brother's house.
- Arrest David L. Smith.

GUID

- Unique machine identifier stored in each Office document.
- GUID in List.doc was the same as other viruses written by VicodinES and ALT-F11.
- GUID remains with file, even after editing.
- GUID not involved in the capture of Smith.

Is He VicodinES?

- **Melissa is named after a topless dancer from Florida.**
- **Message post by VicodinES:**

Re: INDUSTRIAL MUSIC FOR SALE #1 - #4
Author VicodinES <vicodines@aol.com>
Date: 1995/04/16
Forum: rec.music.industrial

Anyone interested in buying any of these disks 1st punch yourself in the face for even considering paying those OUTRAGOUS prices 2nd check around - D.U. or I.T. or even Blockbuster could beat these prices - hell I've seen some of those cd's in the used stores for $8.00 and I live in the Bass heavy - Industrial scarce state of Florida!

More Messages By VicodinES

Look for these characteristics:

- **Use of "-" (dash) to separate thoughts, not commas.**
- **Signoff.**
- **Very long sentences.**
- **Always one space between sentences.**
- **Use of quoted words to highlight meanings.**

Some Messages By DLSmith

You Decide!

What Could Be Worse

From: Dmitry Gryaznov <grdo@dial.pipex.com> (dgryazno@nai.com)

Date: Sunday, March 28, 1999 5:50 PM

Chengi Jimmy Kuo wrote:

> > Variants will appear shortly, that won't be detectable through subject line scanning.

> Like not having a subject. Just as effective. It comes from someone you know already. There's no need for a subject. In fact, it will work better that way.

As I said, there is a still better way. A virus can browse through the existing messages in one's Inbox and pick up a subject from one of them. It could also pick up recepients from there too. So that the virus' mail would look like a valid reply to another message.

> > Variants that don't depend on Outlook will appear, probably later than variants with variable subject lines but who knows.

> Maybe, maybe not. I think they will depend on a specific email package. And if that's the case, then "not depend on Outlook" is actually a restriction on its likelihood to spread.

Using MAPI.Session instead of Oulook.Application is more universal and still covers Outlook as well.

W32/ExploreZip

From an infected user, you get a reply to a message you just sent, with the following text:

I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.

Attached is zipped_files.exe (210,432 bytes) which produces the following error message when opened:

Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help.

How ExploreZip Spread So Fast

Infected system then:

- Searches all drives D: through Z: for win.ini.
  - If found, adds run=_setup.exe and copies itself to that directory.
  - When machine sharing that drive next boots up, it will be infected.
- Searches all networked drives.
  - Does same.

How ExploreZip Spread So Fast

Every 5 minutes, it would re-scan the D: through Z: drives.

If a machine is being cleaned but still its drives were shared to a machine which was infected, it would just be re-infected.

A Couple Other Viruses

Chernobyl

CIH 1.2 (Chernobyl), April 26

- US: home users
- Europe: some companies, lots of home users
- Asia: Lots of sad people.

Papa.B: Friday to Monday

[Sitenames removed for Security]

Will History Repeat?

CHRISTMA EXEC

- 1987?
- Christmas card, re-mailed itself to everyone in your personal mailing list.
- IBM's and global VNET system shutdown from too much traffic.

Questions & Answers

Your Partner
Against the Virus Problem