Melissa Virus Creates a New Type of Threat

Lee Garber

The Melissa virus, which tore through computer networks at an astonishing speed in late March, sent a shiver down the 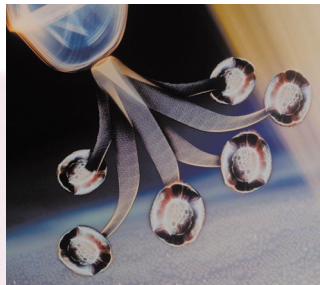spine of the computer industry. There was concern because Melissa spread quickly via infected e-mail attachments that, when opened, sent the virus to people in unsuspecting victims' address books. This meant that Melissa spread very fast throughout the world, overwhelming e-mail servers, before it could be stopped.

Melissa could also send out sensitive documents to people in address books without the user's knowledge. Melissa's approach was particularly insidious because the virus made infected e-mail attachments appear to come from people the recipients knew.

But perhaps the greatest concern about Melissa is what it could mean for the future.

Melissa was relatively easy to create and attacked weaknesses in important and popular technologies that could be exploited again with even more serious results.

For example, Melissa exploited users' widespread and often careless opening of e-mail attachments, which can contain macro viruses.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org

Melissa could be the forerunner of malicious viruses that can spread incredibly fast.

Melissa also took advantage of a potential security threat created by macro languages, in this case Microsoft's Visual Basic for Applications (VBA), which let users program executable functionality into documents. In the case of Melissa, the author programmed malicious functionality into a document used as an e-mail attachment. (See the sidebar "Viruses and Visual Basic for Applications.")

Because of this, the Melissa virus represents a major new development in virus technology, said Peter Tippett, chair and chief technologist at the International Computer Security Association (ICSA), a security consultancy.

Similar viruses in the future could be much more malicious than Melissa, noted Jeff Carpenter, incident response team leader for Carnegie Mellon University's Computer Emergency Response Team.

This could have serious ramifications because many organizations depend on e-mail for mission-critical tasks and because Internet-based commerce is becoming an important economic factor.

At its worst, this type of problem could disrupt Internet-based business operations and cause tens of billions of dollars in losses, said Michael A. Vatis, director of the National Infrastructure Protection Center (NIPC).

MELISSA'S RAMPAGE

Melissa debuted on Friday, 26 March.

Melissa's effects

Users began receiving e-mail messages with

- a subject line that read, "Important Message From …" followed by the name of the previous victim, who had the recipient's name in an e-mail address book and thus probably knew him or her;
- a text message that said, "Here is that document you asked for … don't show anyone else ;-)"; and
- an attachment, called list.doc, with a purported list of user names and passwords for pornographic Web sites taken from the alt.sex newsgroup.

Because the message appeared to come from an acquaintance, it encouraged recipients to open the attachment, said Dan Schrader, business manager for security in the Portal Division at Trend Micro, an antivirus software vendor.

If a victim used the Microsoft Outlook e-mail client and either Word 97 or Word 2000, the macro virus' instructions would send the message and infected attachment to the first 50 contacts in each of the victims' e-mail address books. Because a contact could represent a group of people, not just an individual, the virus could be sent to many more than 50 recipients at one time.

The virus also infected Word's normal.dot template, generally used to create documents. New documents would then become infected with Melissa. If users subsequently e-mailed infected documents as attachments, recipients with

Microsoft Outlook would activate the virus upon opening the attachment, thereby sending copies of the infected document to the first 50 contacts in their address books. If the document contained sensitive material, this would cause security problems. Some companies shut down their e-mail servers to keep this from happening.

For Melissa recipients using e-mail clients other than Outlook, the virus infected their Word 97 or Word 2000 normal.dot template and documents subsequently created using the template. However, the virus would not automatically transmit infected documents to people in the victims' address book. Nonetheless, victims could inadvertently send infected documents to other people via e-mail or floppy disk.

If an infection occurred when the number of minutes past the hour of the current time matched the date (for example, at 9:27 a.m. on 27 March), the virus would insert a Bart Simpson quotation from *The Simpsons* television show, "Twenty-two points, plus triple word score, plus 50 points for using all my letters. Game's over. I'm outta here," into a victim's active document.

In Word 97, Melissa disabled the command that would let users receive notification if a document contained a macro and open the document without enabling the macro.

And Melissa set Word 2000 to the lowest macro-virus security level and blocked settings that would let users raise security levels.

As Melissa propagated, it quickly began to overwhelm and force the closure of e-mail servers. This represented a particular hardship for many small organizations that use a single server for e-mail and other important applications.

Millions in losses

Melissa caused serious disruptions at such big organizations as E.I. du Pont de Nemours and Co., Honeywell, Intel, Lockheed-Martin, Lucent Technologies, Microsoft, and the US Marine Corps.

Trend Micro's Schrader said, "Melissa was clearly the fastest spreading virus I've seen, without a doubt."

The ICSA's Tippett estimated that

Viruses and Visual Basic for Applications

The growing popularity of macro languages has fueled concern that macro viruses will become more popular and more dangerous, particularly since the Melissa outbreak.

Macro languages can be used to embed various types of functionality within documents. For example, users could embed a pop-up calendar in an expense report, so they could keep track of travel dates as they fill out the document, noted Neil Charney, Microsoft's group product manager for Office 2000 Developer and Visual Basic for Applications (VBA).

However, virus writers, like the one who wrote Melissa, can use macro languages to embed malicious functionality within documents.

Various application vendors offer macro languages for their products. VBA, first released in 1993, is used with Microsoft's Office, the biggest application platform, so it is the most widely used macro language.

Despite their name, Charney said, macro languages can be used for more than creating macros to automate tasks. He said VBA can serve as a development environment. For example, he said, VBA can be used to customize Microsoft applications, adding features that the vendor did not include.

In addition, VBA can be used to integrate multiple applications' functionality. For example, Charney said, instead of manually entering information from a database into a spreadsheet, VBA could be used to have the spreadsheet automatically pull the appropriate data from the database.

Dan Schrader, business manager for security in the Portal Division at Trend Micro, an antivirus software vendor, agreed that many power users want these capabilities. However, he said, the computer industry must be careful because macro languages can turn documents into executables. Users who open a document just to read its contents can unknowingly activate an embedded program, which could be malicious.

As is generally the case, more functionality leads to less security, noted Roger Thompson, technical director of malicious code research for the International Computer Security Association, a security consultancy. Features like VBA make it easier to do good things and easier to do bad things, he said.

Nonetheless, Schrader said, macro languages are the type of convenient feature that won't go away, so the computer industry must find a way to live safely with them.

Melissa infected about 1.2 million computers and 53,000 servers at 7,800 North American companies that had at least 200 PCs, and it cost between $249 million and $561 million to fix.

ICSA spokesperson Barbara Rose said that of 300 corporations surveyed, the median cost for combating Melissa was $1,750, although some respondents reported costs as high as $100,000.

On 1 April, law enforcement agencies arrested a suspect in the case. (See the sidebar "Melissa Suspect Arrested.")

The fixes

Over the weekend following the Melissa outbreak, IT workers in infected organizations began learning about the virus, shutting down their e-mail servers in many cases, and eliminating the virus from their systems. For example, administrators filtered out all e-mail with Melissa's signature subject line.

Meanwhile, antivirus vendors began their work. "This was a simple virus," said Schrader. "The solution was easy. It took us 20 minutes to develop a pattern to recognize this virus."

Organizations with centralized security-management systems scanned their entire network to get rid of Melissa infections. Other organizations had to scan each desktop.

The variants

In the days following the outbreak,

Melissa Suspect Arrested

As Melissa began spreading through networks on 26 March, law enforcement agencies, including the FBI, began looking for the virus' creator. They eventually tracked the source of the virus to New Jersey.

On 1 April, computer-crime investigators with New Jersey's State Police and Department of Law and Public Safety arrested David L. Smith, 31, a programmer who lived in Aberdeen Township, New Jersey.

David L. Smith (center) attends a court hearing in New Jersey on charges that he created the Melissa virus. He is accompanied by his attorney, Edward F. Borden Jr. (left). AP/Wide World Photo.

Authorities charged Smith, who was released after posting $100,000 bail, with second-degree interruption of public communication, conspiracy to interrupt public communication, and attempted interruption of public communication; and third-degree theft of computer service and damage or wrongful access to computer systems.

Smith's attorney, Edward F. Borden Jr. of Princeton, New Jersey, said his client has pleaded not guilty to all charges.

Smith faces maximum penalties of $480,000 in fines and 40 years in prison, according to Paul Loriquet, spokesperson for the New Jersey Attorney General's Office.

When the ongoing investigation is completed, Loriquet said, the Attorney General's Office can send the case to a state grand jury, which could then decide whether to indict Smith.

virus writers released several Melissa variants, with names like Papa, Mad Cow, Marauder, and Syndicate.

For example, Papa affected Microsoft Excel, which, like Word, supports VBA. When a victim using Microsoft Outlook opened an Excel-based attachment to an e-mail note, the virus would send the note and attachment to the first 60 contacts in the victim's address book.

Roger Thompson, ICSA's technical director of malicious code research, noted that writers may have based their variations on Melissa's code, which was posted on several newsgroups shortly after the virus' outbreak.

However, many antivirus companies expected variants and produced software updates that would recognize them. For example, Schrader said, Trend Micro developed software that catches any macro that, like Melissa, tries to use the Mail API (MAPI) to open Outlook.

Probably because so many users downloaded antivirus updates in the wake of Melissa, he said, comparatively few users were affected by variants.

POTENTIAL FUTURE PROBLEMS

According to Schrader, Melissa represents a significant new type of viral threat, not because its elements were new but because of the way it combined and used its elements.

Also, Melissa was relatively easy to write using VBA. This means that even virus creators with limited programming skills could author similar, more harmful viruses that might not be detected even by current antivirus products.

Such a virus could inflict damage like that caused by the CIH virus, which struck in late April. Although it affected far fewer PCs than Melissa, CIH was more harmful. It could wipe out parts of a hard drive and destroy the flash BIOS, leaving users unable to reboot their computers.

It's not clear that a micro virus alone could cause such problems. However, the ICSA's Thompson said Microsoft's OLE (object linking and embedded) framework for compound documents permits users to embed a binary object within a document. Thus, he said, an author could write a macro virus that, when opened, would call a binary object that causes CIH-like problems.

"The potential effects could be devastating," CERT's Carpenter said.

A Melissa-like virus could also be written to subtly change data in documents or databases. Antivirus software vendors could find ways to detect and block these viruses but couldn't restore the altered data.

Meanwhile, Schrader noted, an author could create an even more infectious version of Melissa by enabling it to strike multiple MAPI-compliant e-mail clients, not just Outlook.

RECOMMENDATIONS

Documents used to be safe to open because they were not executables, but macro languages have changed that, as Melissa shows.

The ICSA's Thompson said macro lan-

guages give "the power of programming to people who aren't programmers, including virus writers."

Other word processing programs, such as WordPerfect, have their own macro languages, but VBA is more significant because of Microsoft Word's popularity.

Because of their functionality, Schrader said, macro languages are here to stay. So, he said, "We need to figure out how to deal with it."

Macro safety settings

In past Microsoft Office versions, users who are about to open a document that contains a macro are shown a dialog box that lets them choose whether to enable or disable the macro.

Alan Paller, director of research with the SANS (System Administration, Networking, and Security) Institute, said this is not good enough because most users are not sophisticated or "scared" enough to use such preventive measures properly. Instead, he said, software vendors should send their applications with the capability to receive macros disabled. Users who want the capability can then turn it on, perhaps during the installation process, he explained.

"After all," he said, "shouldn't the guys selling medications put a safety cap on so kids can't get into them?"

The ICSA's Thompson agreed, saying macros present too much of a risk and many users don't need to run them.

The problem is that software vendors like to market products based on a high level of functionality and thus don't want to disable their capabilities, Paller said.

However, Thompson noted, "Security and functionality exist in an inverse relationship."

Neil Charney, Microsoft's group product manager for Office 2000 Developer and VBA, said Office products should not come with macro capabilities disabled. He said many people want to create and use macros and thus don't want to have to spend time and effort enabling those capabilities.

Authentication

Charney said security capabilities that Microsoft has added to its Office 2000 products should protect users.

Microsoft has included an antivirus API that lets antivirus firms integrate their software into Office 2000 products to scan documents before users open them.

> **Some experts say current default security settings in many applications are not good enough to stop macro viruses.**

In addition, Office 2000 users who write VBA 6.0 macros could digitally sign them, certifying the code has come from a trusted source. Users can then configure products or set Word 2000's default setting so the applications will run only macros digitally signed by trusted sources. The default settings for other Office 2000 applications will continue to call the current macro-notification dialog box.

CERT's Carpenter said authentication is a good idea because it verifies that the sender is a trusted source. However, he said, if a trusted source unknowingly passes on a virally infected document, authentication won't help the recipient.

Improved virus protection

Schrader said Melissa's main lesson is the need for antivirus products that scan entire networks, not just individual desktops, as is traditionally the case.

"The antivirus community hasn't owned up to this problem," he said. "The battle has to shift from the desktop to the entry point to your environment."

This could keep viruses like Melissa from getting into a network in the first place. If security is left on the desktop, Schrader said, users may turn it off or use it incorrectly.

Meanwhile, viruses could be cleaned up more easily with centralized antivirus management programs.

The most important place for corporate virus protection is the Internet e-mail gateway, and the second most important is the internal e-mail server, Schrader said.

Currently, though, he said, "We esti-

mate that only about 45 percent of corporations have rolled out virus protection on their e-mail servers."

The ICSA's Thompson cautioned that many organizations don't want to rely solely on network-scanning antivirus software because it won't catch, for example, boot viruses and viruses introduced by floppy disks.

Meanwhile, Schrader said, organizations should use antivirus programs that look for the type of behaviors that a virus causes, even those that appear innocuous, rather than programs that look for specific byte strings from known viruses.

However, Thompson said, the former approach has not been very successful in the marketplace because it has not been supported by corporate help desks. Help desks don't want to respond to the false alarms that occur with the behavior-based approach when legitimate activities cause virus-like behaviors.

Other concerns

Melissa emphasizes that perhaps organizations should stop encrypting all e-mail, Schrader said. When messages are encrypted, antivirus software cannot read their contents and thus cannot determine if they contain e-mail-borne viruses, such as Melissa.

"People need to be more sophisticated," Schrader said. "Is it necessary to encrypt all e-mail? Perhaps they should encrypt only the most critical."

Of course, virus experts also said users should be more careful by, for example, using and regularly updating antivirus software.

C ERT's Carpenter said, "While security gets a lot of press attention, I think there are still a lot of people who don't give it the priority they should. Users don't understand the extent of the problem. They don't understand the worth of the assets that need protection."

Schrader agreed and said, "Many people have ignored viruses in the past. But I think Melissa has raised their profile." ❖

Lee Garber is Computer's *news editor. Contact him at l.garber@computer.org.*

Authorized licensed use limited to: Concordia University Library. Downloaded on August 14,2022 at 23:26:27 UTC from IEEE Xplore. Restrictions apply.