United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
April 15, 1999

INFORMATION SECURITY

The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data

Statement of Keith A. Rhodes
Technical Director for Computers and Telecommunications
Accounting and Information Management Division

GAO/T-AIMD-99-146

Madam Chairwoman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the "Melissa" computer virus. Although it did disrupt the operations of thousands of companies and some government agencies, this virus did not reportedly permanently damage systems and did not compromise sensitive government data. Nevertheless, it has shown us just how quickly computer viruses can spread and just how vulnerable federal information systems are to computer attacks. Moreover, Melissa has clearly highlighted the urgent and serious need for stronger agency and governmentwide protection over sensitive data. Today, I will discuss the immediate effects of the Melissa virus and variations of it as well as its broader implications. I will also discuss some critical measures that should be taken to help ensure that federal departments and agencies are better prepared for future viruses and other forms of attack.

The Melissa Virus and Its Immediate Impact

Melissa is a "macro virus" that can affect users of Microsoft's Word [1] 97 or Word 2000. Macro viruses are computer viruses that use an application's own macro programming language[2] to reproduce themselves. Macro viruses can inflict damage to the document or to other computer software.

Melissa itself is delivered in a Word document. Once the Word document is opened, and the virus is allowed to run, Melissa:

- Checks to see if Word 97 or Word 2000 is installed.
- Disables certain features of the software, which makes it difficult to detect the virus in action.
- Generally sends copies of the infected document to up to 50 other addresses using compatible versions of Microsoft's Outlook electronic mail program.[3]

[1]Word processing software. The virus can also infect Word 98 for Macintosh and documents created by this application. However, in the Macintosh environment, the virus will not automatically send the infected document to others.

[2]Macros are tools for customizing computer applications so that often-used commands can be automatically executed.

[3]Outlook is a desktop information manager that also provides e-mail support. If any of the first 50 addresses in Outlook's address book represents a mailing list, then everyone on that list also receives a copy of the virus. In addition, if the user has more than one address book, the first 50 addresses in each book are used.

- Modifies the Word software so that the virus infects any document that the user may open and close. If these documents are shared, the virus is spread.

Under some circumstances, Melissa could cause confidential documents to be disclosed without the user knowing it.

If addresses in an electronic mail address book are within the same organization, Melissa can quickly overload electronic mail servers and result in a denial of service. According to Carnegie Mellon University's CERT Coordination Center,[4] for example, one site reported receiving 32,000 copies of mail messages containing Melissa on its systems within 45 minutes.

In fact, what made Melissa different from other macro viruses was its ability to take advantage of the Microsoft e-mail application and the speed at which it spread. According to the CERT Coordination Center, the first confirmed reports of the virus were received on Friday, March 26, 1999. By Monday, March 29, it had reached more than 100,000 computers at more than 300 organizations.

In the course of spreading, variations of the Melissa virus also surfaced, including the "Papa" virus—a Microsoft Excel 97[5] or Excel 2000 macro virus that can also be delivered by e-mail. According to the Microsoft Corporation, this virus could generate commands that result in significant network traffic congestion without the user's knowledge.

Fortunately, aside from shutting down e-mail systems, Melissa did not reportedly permanently damage government and private sector information systems and did not compromise sensitive government data. However, because the federal government does not have a process for reporting and analyzing the effects of such attacks, quantitative analysis is difficult.

[4]Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with and respond to incidents and building awareness of security issues across the Internet community.

[5]Spreadsheet software.

In its information bulletin on the virus, the Department of Energy (DOE) reported that Melissa had been detected at multiple DOE sites and had spread widely within the department. According to DOE, the risk of damage was low because most users did not have macros in files and would be alerted by Word's macro detector.[6] However, at the time it issued its advisory, DOE believed the risk of lost productivity and lost mail messages was high as mail servers might need to be shut down and purged of infected messages.

Broader Implications of the Melissa Virus

Although the Melissa virus reportedly did not compromise sensitive government data or damage systems, it demonstrated the formidable challenge the federal government faces in protecting its information technology assets and sensitive data.

First, Melissa showed just how quickly viruses can proliferate due to the intricate and extensive connectivity of today's networks—in just days after the virus was unleashed, there were widespread reports of infections across the country. Worse yet, as the virus made its way through the Internet, variations appeared that were able to bypass security software designed to detect Melissa. These two factors alone made it extremely difficult to launch countermeasures for the infection.

Second, Melissa showed how hard it is to trace any virus back to its source. At first, it was widely assumed that Melissa was created by a writer, known by the computer handle "VicodinES," who was distributing the virus from an America Online account known as "Sky Roket." But later, after receiving a tip from America Online, investigators discovered that this account was allegedly stolen by the suspect arrested for creating the virus. Without this level of cooperation, the suspect might not have ever been identified.

Third, Melissa demonstrated that vulnerabilities in widely adopted commercial-off-the-shelf (COTS) products can be easily exploited to attack all their users. This is alarming because agencies are increasingly turning to COTS products to support critical federal operations. Because they are built to appeal to a broad market and not to satisfy a particular

[6]As noted elsewhere, Melissa is a macro virus and requires the host program, such as Word 97, to allow it to execute. By taking advantage of Word's ability to notify the user whenever a macro is going to be executed, a user can prevent the virus from executing in the first place.

organization's unique functional and security requirements, agencies must thoroughly analyze the vulnerabilities and threats associated with COTS products before acquiring them. It is estimated that Microsoft's Office suite, which includes Word and Excel, represented 89 percent of the revenues for this market in 1997.

Fourth, Melissa illustrated that there are no effective agency and governmentwide processes for reporting and analyzing the effects of computer attacks. There is not complete information readily available on what agencies were hit and only partial data on the Department of Defense and DOE. Moreover, there are no data available at this time that quantify the impact of the virus, for example, productivity lost or the value of data lost.

Fifth, Melissa proved that computer users can do a good job of protecting their systems when they know the risks and dangers of computing and when they are alerted to attacks. Reports from the media revealed that organizations that trained their employees and warned them of the attack fared much better than those that did not.

More important, Melissa is a symptom of broader information security concerns across government. Over the past several years, we and inspectors general have identified significant information security weaknesses in each of the largest 24 federal agencies.[7] These include inability to detect, protect against, and recover from viruses such as Melissa; inadequately segregated duties which increase the risk that people can take unauthorized actions without detection; and weak configuration management processes, which cannot prevent unauthorized software from being implemented. Examples of significant security lapses that have been reported follow.

- In November 1997, the Social Security Administration Inspector General reported that security weaknesses subjected sensitive information to potential unauthorized access, modification, or disclosure. The Inspector General reported that 29 convictions involving agency employees were obtained during fiscal year 1997, most of which

[7] Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998); Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets (GAO/T-AIMD-98-312, September 23, 1998); and Financial Audit: 1998 Consolidated Financial Statements of the United States Government (GAO/AIMD-99-130, March 31, 1999).

involved creating fictitious identities, fraudulently selling social security cards, misappropriating funds, or abusing access to confidential information.

- In May 1998, we reported that (1) the Department of State's information systems and the sensitive data they maintain were vulnerable to access, change, disclosure, and disruption by unauthorized individuals [8] and (2) weak computer security practices at the Federal Aviation Administration jeopardized flight safety. [9]
- In October 1998, we reported that weaknesses at Treasury's Financial Management Service placed billions of dollars of payments and collections at risk of fraud. [10]
- Over the past 7 years, the U.S. Department of Agriculture's (USDA) Inspector General reported that USDA's National Finance Center, which annually makes over $21 billion in payroll disbursements to about 434,000 employees, had not ensured that (1) systems security adequately prevented misuse or unauthorized modifications, (2) access to data was needed or appropriate, and (3) modifications made to software programs were properly authorized and tested.
- In September 1998, we reported that general computer control weaknesses placed critical Department of Veterans Affairs (VA) operations, such as financial management, health care delivery, benefit payments, and life insurance services, at risk of misuse and disruption. In addition, sensitive information contained in VA systems, including financial transaction data and personal information on veteran medical records and benefit payments were vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction—possibly occurring without detection. [11]

In view of these and other pervasive security weaknesses, we designated information security as a new governmentwide high-risk area in February 1997. In performing audits at selected individual agencies, we and the inspectors general have also developed hundreds of specific

[8] Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations (GAO/AIMD-98-145, May 18, 1998).

[9] Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

[10] Financial Management Service: Areas for Improvement in Computer Controls (GAO/AIMD-99-10, October 20, 1998).

[11] VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

recommendations aimed at improving the effectiveness of information security programs.

Since our 1997 High-Risk Report, the recognition of the importance of addressing information security problems has greatly increased and led to significant actions. In late 1997, for example, in response to our recommendations, the Chief Information Officers (CIO) Council designated information security a priority area and established a Security Committee. During 1998, the committee sponsored a security awareness seminar and developed plans for improving incident response services.

Also, in May 1998, Presidential Decision Directive 63 (PDD 63) was issued. This established entities within the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation to address critical infrastructure issues. It required each major department and agency to develop a plan for protecting its own critical infrastructure. Other provisions include (1) enhanced analysis of information on threats, (2) assessments of government systems' susceptibility to exploitation, and (3) incorporation of infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

Melissa and other recent incidents demonstrate, however, that still much more needs to be done to ensure that systems and data supporting critical federal operations are adequately protected.

Measures That Can Help Ensure Agencies Are Better Prepared for Future Viruses and Computer Attacks

To help strengthen computer security practices, we issued an executive guide in May 1998 entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). It describes a framework for managing risks through an ongoing cycle of activity coordinated by a central focal point. The guide, which is based on the best practices of organizations noted for superior information security programs, has been endorsed by the CIO Council, and distributed to all major agency heads, CIOs, and inspectors general. By adopting the following 16 practices recommended by the guide, agencies can be better prepared to *protect* their systems, *detect* attacks and *react* to security breaches.

Principles	Practices
Assess risk and determine needs	1. Recognize information resources as essential organizational assets 2. Develop practical risk assessment procedures that link security to business needs 3. Hold program and business managers accountable 4. Manage risk on a continuing basis
Establish a central management focal point	5. Designate a central group to carry out key activities 6. Provide the central group ready and independent access to senior executives 7. Designate dedicated funding and staff 8. Enhance staff professionalism and technical skills
Implement appropriate policies and related controls	9. Link policies to business risks 10. Distinguish between policies and guidelines 11. Support policies through a central security group
Promote awareness	12. Continually educate users and others on risks and related policies 13. Use attention-getting and user-friendly techniques
Monitor and evaluate policy and control effectiveness	14. Monitor factors that affect risk and indicate security effectiveness 15. Use results to direct future efforts and hold managers accountable 16. Be alert to new monitoring tools and techniques

Just as it is important for agencies to implement comprehensive security programs, it is important that a comprehensive governmentwide strategy emerge from current efforts to implement PDD 63 and strengthen the CIO Council's focus on security. As we recently recommended to the Director of the Office of Management and Budget (OMB) and the Assistant to the President for National Security Affairs, such a strategy should: [12]

- Clearly delineate the roles of federal organizations with responsibilities for information security.
- Rank the greatest risks.
- Promote the use of proven security tools and best practices.
- Ensure the adequacy of workforce skills.
- Provide for evaluating systems on a regular basis.
- Identify long-term goals, as well as time frames, priorities, and annual performance goals.

[12] Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 23, 1998).

OMB, the CIO Council, and the National Security Council agree that such a strategy should be implemented and are working collaboratively on a plan to (1) assess agencies' security postures, (2) implement best practices, and (3) establish a process of continued maintenance.

Conclusions

Federal agencies were fortunate that the worst damage done by Melissa was to shut down e-mail systems and temporarily disrupt operations. Because of the increasing reliance on the Internet and standard COTS products as well as the increasing improvements in computer attacker tools and techniques, (as evidenced in the additional capability and techniques employed in the Melissa attack), it is likely that the next virus will propagate faster, do more damage, and be more difficult to detect and to counter. It is imperative, therefore, that federal agencies and the government as whole swiftly implement long-term solutions to protect systems and sensitive data. It is also critical that the federal government establish reporting mechanisms that facilitate analyses of viruses and other forms of computer attacks and their impact. Our Information Security Best Practice guide offers a good framework for agencies to follow, but sustained governmentwide leadership is needed to ensure that executives understand their risks, monitor agency performance, and resolve issues affecting multiple agencies.

Madam Chairwoman, this concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Mail
Postage & Fees Paid
GAO
Permit No. GI00