United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
10:00 a.m. EDT
Thursday
July 20, 1989

November 1988 Internet Computer Virus and the Vulnerability of National Telecommunications Networks to Computer Viruses

Statement of
Jack L. Brock, Jr., Director, Government
Information and Financial Management Issues
Information Management and Technology Division

Before the
Subcommittee on Telecommunications and Finance
Committee on Energy and Commerce
House of Representatives

046061/139178

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the November 1988 Internet computer virus incident and issues stemming from the virus--in particular, vulnerabilities of the Internet computer network system to such intrusions and factors affecting the prosecution of computer virus incidents. The virus attack caused thousands of computers on the Internet--an unclassified multi-network system connecting over 60,000 computers nationwide and overseas--to shut down. The virus, embodied in a computer program, entered computers and continually recopied itself, consuming resources and hampering network operations. Much of our testimony today is based on our report, released today, Computer Security: Virus Highlights Need for Improved Internet Management, GAO/IMTEC-89-57. The report contains recommendations aimed at improving Internet security.

BACKGROUND ON THE INTERNET AND THE INTERNET COMPUTER VIRUS

The Internet is an interconnected set of national research networks that provide for communications between computers at universities and governmental and industrial research facilities. The Internet supports a vast community of researchers including physicists, computer scientists, medical researchers, astronomers, and many others. The most frequent use of the Internet is for electronic mail, which provides a way of sending person-to-person messages almost instantaneously. Other uses include file transfers and remote access to computer data banks and supercomputers. Access to supercomputers has had a dramatic impact on scientific endeavors; experiments that took years to complete on an ordinary computer can take weeks on a supercomputer.

The Internet comprises over 500 unclassified local, regional, and national networks, with two of the largest networks sponsored by the National Science Foundation (NSF) and DOD's Defense Advanced Research Projects Agency (DARPA). The Internet connects over half a million users. Federal funding for Internet operations, totalling about $50 million a year, comes from the five agencies[1] involved in operating research networks. In addition, universities, states, and private companies have invested hundreds of millions of dollars in local and regional networks.

Management of the Internet is decentralized, with both the host sites and the individual networks responsible for certain functions. No one agency or organization is responsible for overall Internet management. Rather than having centralized management, the hosts sites, such as the college campuses and federal agencies that own and operate the computers, are responsible for managing and securing their computers. The initial developers of the Internet believed that the host sites were in the best position to determine a level of security appropriate for

[1] The five federal agencies that fund Internet operations are NSF, DARPA, the Departments of Energy and Health and Human Services and the National Aeronautics and Space Administration.

their systems. Individual networks are responsible for operational management. Each network is autonomous and has an operations center that monitors and maintains its portion of the Internet.

The Internet virus, which entered computers and continuously recopied itself, differed from earlier viruses in several key respects. Previous viruses were almost always limited to personal computers whereas the Internet virus infected larger systems, such as minicomputers, work stations, and mainframes. In addition, the Internet virus was the first to spread over a network automatically. The Internet virus spread largely by exploiting certain security flaws (holes) in systems software based on the Berkeley Software Distribution UNIX system and by taking advantage of weaknesses in host site security policies--for example, poor password management.

The onset of the virus was extremely swift. Within hours after it appeared, the virus had reportedly infected up to 6,000 computers, clogging systems and disrupting most of the nation's research centers. After 2 days, the virus was eradicated at most sites, largely through the efforts of university computer experts. The virus apparently caused no permanent damage; its primary impact was lost processing time on infected computers and lost staff time. However, a few changes to the virus could have resulted in widespread damage and compromise. For example, computer experts told us that by modifying the program slightly, the virus could have erased files on infected computers or remained undetected for weeks, surreptitiously changing information on computer files.

VULNERABILITIES HIGHLIGHTED BY THE VIRUS

The virus incident revealed several Internet vulnerabilities that made it easier for the virus to spread and harder for it to be eradicated. The vulnerabilities include:

-- First, the lack of an Internet security focal point to address Internet-wide security problems. The absence of a focal point made it difficult to respond to the virus. For example, many users affected by the virus had no idea how to report the problem or to whom to report it.

-- Second, security weaknesses at host sites. Our report cites inadequate attention paid to security, such as poor password management and systems managers who lacked the technical expertise to deal with security problems, such as the Internet virus. One study demonstrated the relative ease with which passwords can be guessed. It found that out of over 100 password files, up to 30 percent were guessed using just the account name and a few variations.

-- The third problem involves problems in developing, distributing, and installing corrections to identified software holes. This can be a two-sided dilemma. For example, vendors are not always timely in repairing software holes that may create security vulnerabilities, and even when corrections are available, sites may not install them, through either neglect or lack of expertise. The intrusions which occurred after the virus in November and December 1988 at multiple sites, including Lawrence Livermore National Laboratory and Mitre Corporation provided good examples of this dilemma. In these instances, intruders entered several computer systems by exploiting a known software hole. In one case, the vendor had not supplied the fix for the hole, and in the other, the fix was supplied but not installed.

FACTORS HINDERING PROSECUTION OF COMPUTER VIRUS INCIDENTS

There are some factors that may hinder prosecution of virus-type incidents. For example, federal laws are not specifically directed at computer virus-type issues. The law most relevant to such incidents--the Computer Fraud and Abuse Act of 1986 (18 U.S.C. 1030)--is untested with regard to virus-type offenses and contains terms that are not defined. The act defines "exceeds authorized access" as access to a computer with authorization and use of such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter. However, the act does not define "access" or "information." Because some of the terminology has not been defined, it is not clear whether all virus-type cases would fit within the act's scope. Further, the evidence in such cases tends to be highly technical, which may hinder prosecution.

To date, no federal computer virus-type cases have been tried. As of July 17, 1989, there have been no indictments in the Internet incident. Legislation directed at computer virus-type incidents could eliminate the uncertainty regarding the applicability of current laws.

CONCLUSIONS

Discussions of computer security frequently cite the trade-offs between increased security and the sacrifices, in terms of convenience, system function, flexibility, and performance, often associated with security measures. According to Internet users, systems managers at research sites have traditionally not been very concerned with security. Since the Internet virus occurred, various steps have been taken to address some of the vulnerabilities stemming from the incident, from creating computer security response centers to issuing ethics statements to raise the moral awareness of Internet users.

We support these actions and believe they are an important part of the concerted effort required to upgrade Internet security. In addition, host sites may need to take additional actions to heighten security awareness among users and to improve identified host level weaknesses, such as lax password management. However, we believe that many of the vulnerabilities highlighted by the virus require actions beyond those of individual agencies or host sites. For this reason, we believe that a security focal point should be established to fill a void in the Internet's management structure and provide the focused oversight, policy-making, and coordination necessary at this point in Internet's development. These concerns will take on even greater importance since the Internet is evolving into a high-speed, enhanced network system, which will be faster, more accessible, and have more international connections than the present Internet.[2]

We believe the Office of Science and Technology Policy, which has been given a leadership role in planning for an enhanced research network, is the most appropriate body to coordinate the establishment of a security focal point. As such we recommended in our report that the President's Science Advisor, within that

[2] A bill, the National High-Performance Computer Technology Act of 1989, has been introduced before the Senate to fund the enhanced network, to be called the National Research and Education Network. The bill calls for the Federal Coordinating Council for Science, Engineering, and Technology within the Office of Science and Technology Policy to establish a National Network Advisory Committee comprising representatives from all parties involved in the network program. The committee is to provide technical and policy advice to the enhanced network.

office, coordinate the establishment of an interagency group to serve as an Internet security focal point. This group should include representatives from the federal agencies that fund Internet research networks. As part of its agenda, we have recommended that the group

-- Provide Internet-wide policy, direction, and coordination in security-related areas.

-- Support efforts already underway to enhance Internet security.

-- Develop mechanisms for obtaining the involvement of Internet users, vendors, industry and technical groups, and federal agencies regarding security issues.

-- Become a part of the structure that emerges to manage the enhanced research network.

*****

That concludes my statement. I would be glad to respond to your questions.