OFFICE OF THE
SECRETARY OF DEFENSE

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000 88 NOV -9 PM 12: 46

Serial: J-1005-88
7 November 1988

(b)(3) - P.L. 86-36

MEMORANDUM FOR THE SECRETARY OF DEFENSE

SUBJECT: Synopsis of the 3 November Computer Virus ARPANET Propagation - INFORMATION MEMORANDUM

The National Computer Security Center learned of the virus attack shortly after the first reports on Wednesday evening and has been in nearly continuous contact with the major members of the network ever since. The Center obtained a copy of the offending software on Thursday morning, 3 November, and is examining the sizeable and sophisticated software line by line to determine exactly how it works and what specific system vulnerabilities it exploits.

The major impact on those systems operating within the network was loss of computer time. To the best of our knowledge no computers containing classified information were affected. The virus managed to replicate and place into execution enough copies of itself to consume all or nearly all of the available computer time. The effects of the ARPANET/MILNET virus attack can be described, in terms of the Department of Defense Trusted Computer Criteria as a "denial of service." Certain ARPANET and MILNET subscribers simply disconnected their computers from the net; DDN operations shut down the ARPANET-MILNET mail gateways once they were aware of the attack. Packet-switches, terminal access controllers, and monitoring centers were not affected because the attack took advantage of vulnerabilities of the Berkeley UNIX 4.3 operating system which is only used on host computers.

A meeting of representatives from DCA, NIST, DOE, FBI, and Lawrence Livermore Labs, among others, will be convened on Tuesday, 8 November, to exchange information on the nature of the attack and what can be done to preclude further attacks.

When it became known that the son of an NSA employee, [redacted] might be involved in the computer virus, my General Counsel contacted both the Office of the DoD General Counsel and the Department of Justice in order to provide any information which might be relevant to investigations of this incident. On November 5, 1988 representatives of the FBI met with our employee [redacted] in the presence of members of the Office of the NSA General Counsel to discuss his personal knowledge of the situation.

44454

~~FOR OFFICIAL USE ONLY~~

413.51

1 NOV 88

(b)(3) - P.L. 86-36

(b)(6)

Serial: J-1005-88

I will continue to keep you advised as this matter develops.

GERALD R. YOUNG
Deputy Director

Copy Furnished:
D/SECDEF
DIR IC Staff
DIR DARPA
ASD (C^3I)

PREPARED BY: [redacted] 859-4485 secure

NATIONAL SECURITY AGENCY
FORT GEORGE G MEADE MARYLAND 20755-6000

OFFICE OF THE SECRETARY OF DEFENSE
89 FEB 15 PM 2:00

Serial: J-054-89
13 February 1989

DEF SEC DEF HAS SEEN
FEB 17 1989

MEMORANDUM FOR THE DEPUTY SECRETARY OF DEFENSE

SUBJECT: Computer Security Virus After Actions Assessment - INFORMATION MEMORANDUM

Please refer to the Secretary of Defense memorandum of 20 December 1988 and our initial response of 11 January 1989 (Serial: J-013-89). Our detailed course of action in response to the tasking in the Secretary's memorandum is attached. I believe it represents a comprehensive set of initiatives, growing out of our computer security (COMPUSEC) program, that will help the Department better deal with the problems posed by computer viruses and related computer security vulnerabilities.

We believe the most important strategic directions continue to be the development, evaluation, and effective use of trusted computer security products coupled with a management commitment to sound computer system management and administrative practices. The establishment of a broadly based research and development program in the area of malicious software, of which viruses are but one manifestation, is also crucial for the long term. Lastly, a continuing information system security assessment process is essential in maintaining the security of the nation's telecommunications and automated information systems.

The following paragraphs highlight the major points of our response with respect to the four specific tasks outlined in the Secretary's memorandum. Details are included in the attachment.

We are working with NIST, DARPA, DCA, the FBI and others to improve the DoD's and the country's ability to respond to computer security attacks. All parties now agree that a distributed confederation of coordination facilities, rather than a single national response center, is the best approach. This strategy, founded on the principle that individual system and network managers are the first line of defense, features community response centers to assist system managers in identifying and responding to COMPUSEC problems. The national-level organizations identified above will mainly be involved with top-level planning, providing guidance to the community centers, and assisting individual communities when requested. NSA will make available to all participants the communications and information exchange facilities of our unclassified

Approved for release by NSA on 05-[illegible] pursuant to E.O. [illegible]

48931

(b)(3) - P.L. 86-36

DOCKMASTER system, and will establish links with U.S. computer vendors to help identify and correct COMPUSEC vulnerabilities.

We have taken several steps to heighten computer security awareness in the aftermath of the 2 November incident. The proceedings of the 8 November post mortem were issued on 20 November and given wide distribution. In cooperation with NIST and a major national user organization, we conducted a forum for UNIX vendors on 2 December 1988, laying the basis for wider government/industry cooperation to address computer security problems. We have also reviewed our publication plans, and will issue three publications that respond to the Secretary's call for increased COMPUSEC awareness. In March we will distribute a report that discusses viruses and some of the available software techniques for detecting them. In June we will issue two publications, one addressing the role of trust technology in combating malicious software, the other helping system managers and security officers better use available security mechanisms and features.

In March the National Information Security Assessment Center (NISAC), in conjunction with DCA, will begin an INFOSEC assessment of the Defense Data Network (DDN) as requested in the Secretary's memorandum. After completion of a one-month preassessment, we will provide a detailed schedule and completion date. My goal is for the assessment to be completed within four to six months.

Lastly, we will expand our current COMPUSEC R&D program to allow DoD components to better prevent, detect, and contain the effects of viruses and other forms of malicious software. In close cooperation with the Services, DCA, and DIA, and with input from DARPA, we are developing initiatives in four fundamental research areas: software engineering of trusted computer systems, formal system development methods, secure operating systems, and malicious software analysis tools. By focusing more intensely on malicious software, we intend to develop more general techniques to replace the ad hoc approaches we rely on today.

If you or your staff have additional questions, please contact me directly or my action officer on this issue, [redacted], the Director of the National Computer Security Center on [redacted]

[redacted]

(b)(6)

GERALD R. YOUNG
Deputy Director

Encl:
a/s

PREPARED BY: [redacted]

NSA/CSS RESPONSE TO DOD TASKING ON COMPUTER SECURITY VIRUS AFTER ACTION ASSESSMENT

10 February 1989

NSA/CSS RESPONSE TO DOD TASKING ON COMPUTER SECURITY VIRUS AFTER ACTION ASSESSMENT

BACKGROUND

Computer viruses are part of that technical subset of computer security technology known as malicious software. Malicious software is not new; examples of its use were noted as long ago as the 1950s and 60s. Until recently, however, these were mainly of academic interest. In the last few years, public awareness of and interest in computer viruses has increased, kindled by the publication of articles in the popular press that pointed out the potential damage that malicious software can cause.

Until November of last year the virus problem had been largely confined to personal computers (PCs). The Internet virus attack of 2 November, however, altered the nation's perception of the problem. What had formerly been viewed as a PC problem was now shown to be capable of shutting down a large number of major host computer systems connected to one of the largest computer networks in the world. In response to the Internet virus incident, a group of senior DoD officials met on 14 November as an Executive After Action Assessment Team to review the events of 2 November and develop recommendations for improving the Department's ability to respond to future incidents. As a result of that meeting, NSA was tasked by the Secretary of Defense to develop a course of action that responded to four specific tasks. These tasks requested the Agency to:

- work with NIST and DARPA to address quickly the establishment of a central coordination center;
- publicize computer security lessons learned from this incident;
- reassess the major defense data networks on a "priority basis to determine current vulnerabilities"; and
- pursue intensive research and development in the area of computer security against viruses.

The remainder of this plan constitutes the NSA response to this SECDEF tasking.

TRUST TECHNOLOGY AND EFFECTIVE SYSTEM MANAGEMENT

Before discussing our response to the four specific tasks, we believe it would be useful to discuss the role that our basic

program--the promotion of the development and use of trusted products--can play in combating the effects of malicious software attacks and other computer security vulnerabilities.

Although there are no known solutions that can guarantee protection of a system against malicious software, we believe the introduction and proper use of trusted products, coupled with sound system security management, offer the best hope for preventing, detecting, and containing such attacks. Consequently, we will continue to promote the development of trust technology by U.S. computer manufacturers and the acquisition and proper use of such products by customer organizations in the DoD and intelligence community. For example, we are cooperating with DARPA in an effort to implement a high assurance trusted system of the type that was exploited in the 2 November attack.

Even when there is widespread availability and use of trusted products, diligent system and network management will continue to be the principal means that the DoD can rely on to reduce the risk of attack. Such "common sense" operational procedures as effective password management, proper software configuration management, and aggressive user security awareness programs go a long way toward minimizing risk. Fortunately, many DoD operational systems have already taken steps in this direction, some as a direct result of the Internet virus incident. We encourage system managers and accrediting authorities to continue to insist that such procedures are adopted and followed because the responsibility for security is ultimately theirs. We will publish, in June 1989, a guide for system managers and security officers to inform them on system security mechanisms, how to use them properly, and the potential harm of poor implementation. We have assisted OPM in developing courses to foster increased computer security awareness among users and managers. These will be available to all government agencies by the end of this month.

COORDINATION CAPABILITY

In the Secretary's memorandum, NSA was asked to work with NIST and DARPA to address the establishment of a central coordination center. While the idea of a single national center seemed attractive in the immediate aftermath of the 2 November virus incident, all parties now agree that such a single center is neither practical nor necessary. Rather, because the main function of such a coordination facility is to serve as an information clearinghouse, a distributed confederation of coordination facilities seems the better approach. It provides multiple contact points, adding robustness to the overall system. Moreover, it allows the system to effectively use diverse talents of the different organizations. NSA, NIST, and DARPA agree on the basic principles of this strategy.

The strategy encompasses three conceptual layers as depicted in the attached diagram. At its foundation, the system is composed of individual Automated Information Systems (AIS) or networks. A host computer or a local area network connected to the Internet are examples. A fundamental principle underlying the strategy is that the responsibility for controlling and operating an AIS or network rests with the management of the individual system. These managers understand the operational requirements of their systems, have access to in-house or contracting assets to fix problems, and, thus, form the first line of defense against attack.

Groups of these individual systems can organize themselves into a larger community or constituency that facilitates exchange of information to help members operate the individual systems more securely. These communities form the second layer in the confederation. The ARPANET research community has established the first community coordination facility, referred to as the Computer Emergency Response Team (CERT), at the Software Engineering Institute (SEI). This element serves as the prototype for other community coordination centers across the country. Communities are largely self-defining and self-organizing, so they may take different forms depending on the particular environment. The MILNET, for example, operates under different guidelines and constraints from those of the more open ARPANET. In addition to ARPANET and MILNET, other communities that have been suggested include a community representing Department of Energy (DOE) laboratories and communities representing the Services and other DoD components.

The third layer in the confederation is formed by national-level organizations, whose degree of involvement will vary depending on need and interest. NIST, consistent with its responsibilities defined in the Computer Security Act of 1987 (PL100-235), will play a major role. NIST is setting up a center to provide encouragement and guidance for the establishment of other centers, procedures and mechanisms for effective emergency communications among centers, and an ongoing resource clearinghouse function. NSA, in keeping with its role under PL100-235, will concentrate on our R&D effort against malicious software and will exchange information with the computer security community. Because of the ties we have established with U.S. computer vendors, NSA, in cooperation with NIST, will establish vendor contact points and use them as needed, e.g., if an individual CERT is unable to establish contact with a vendor on a particular problem and requests our assistance. We will also ensure that lessons learned in the unclassified world are made available to classified system managers as appropriate. In the event of unauthorized disclosure of classified information, NSA involvement will obviously increase.

DARPA, which manages the ARPANET and is the main DoD link with the research community, will also be a key player. DCA,

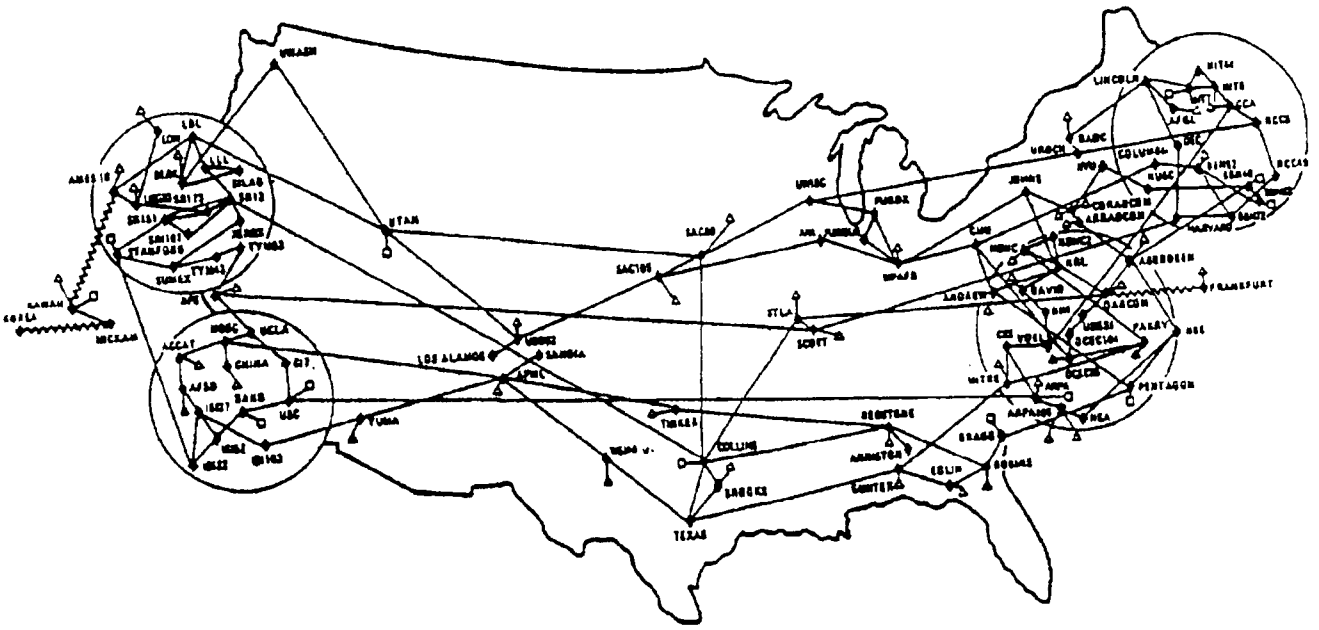
National Computer Security Center

PROCEEDINGS

of the

VIRUS POST-MORTEM MEETING

8 November 1988



ARPANET / MILNET Computer Virus Attack

of

3 November 1988

the manager of the DDN, has participated in the early planning and will continue to play a key role for the DoD. The FBI, in carrying out its responsibility for both criminal and foreign counterintelligence investigations, will also be a participant.

Members of the confederation will communicate in a variety of ways. The primary means will be via electronic mail over the Internet. As one backup, the participants may directly access DOCKMASTER, the trusted computer system of the NCSC, and use its electronic mail and other services. They may also use the telephone, voice mail, and facsimile. If requirements dictate, more elaborate communications schemes can be implemented. DARPA, for example, is working on a low-bandwidth backup data network that uses modems and the public phone network to provide data communications if the Internet is unavailable. Implementation details will be published as part of an overall plan developed by participating agencies. A plan detailing the role of and services to be provided by NSA will be completed by April.

PUBLICIZING LESSONS LEARNED

The events of 2 November and the lessons to be learned from them have already been well-documented and publicized. The proceedings of the 8 November Post Mortem were issued on 20 November and given wide distribution. As a follow-up to the 8 November meeting, the NCSC and NIST, in cooperation with a national UNIX user organization, hosted a special forum for UNIX vendors on 2 December 1988. At this session, we presented a briefing on viruses in general and on the details of the Internet attack in particular. We also discussed a range of possible actions that might help prevent or solve future problems. More effective password management and usage, consistent with guidance issued in FIPS Publication 112, could help significantly in thwarting some of the less sophisticated attacks. Use of trusted products, even at the C2 level of trust, also helps. The UNIX vendor community is reviewing the ideas presented at the 2 December forum as a foundation for more active vendor involvement to address computer security vulnerabilities.

We will also issue a series of publications that deal with malicious software and methods for combating its effects. In June we will publish a report that spells out in more detail the role of trust technology in this area. Also in June we will issue a publication that will describe the fundamental principles of sound system security administration and management and provide useful information to help system managers and information system security officers protect their systems against malicious software and other threats to computer security. Moreover, in March we will issue a report that discusses the nature of virus software, gives specific examples (drawn largely from PC experiences), and reviews some of the software techniques to test for the presence of viruses and protect against attacks. Also, the call for papers for the

12th National Computer Security Conference singled out the topic of computer viruses to encourage papers on this subject.

INFOSEC ASSESSMENT OF DOD DATA NETWORKS

The network "reassessment" called for in the SECDEF memorandum will be a National Information Security Assessment Center (NISAC)-directed INFOSEC assessment focused on the general purpose data networks that make up the Defense Data Network (DDN), to include critical network and end-user components as appropriate. Beginning in March 1989, a one-month preassessment review will determine the exact scope and detailed schedule for the assessment. Although we cannot predict an exact completion date until the preassessment review is completed, we estimate that the entire effort will take from four to six months.

We have formed a multi-disciplinary team of INFOSEC experts to perform the preassessment review, conduct the assessment, and report the results to the DoD. We believe that DCA participation in this effort is essential, and thus are requesting that they provide a representative to serve as a member of the assessment team.

INTENSIFIED RESEARCH AND DEVELOPMENT PROGRAM

A broadly based and well-focused R&D program is an essential part of the DoD's efforts to help prevent, detect, and contain the effects of viruses and other forms of malicious software. We have initiatives in four fundamental research areas: software engineering of trusted computer systems, formal system development methods, secure operating systems, and malicious software analysis tools. The first three areas focus on prevention of attack; the last on recovery.

The NCSC has ongoing R&D activities in all four areas. To date, activity on malicious software analysis has been comparatively limited. The current knowledge base of malicious software attacks is small and confined largely to simple examples, primarily drawn from experiences with PC attacks, and only recently extended toward large host and network examples. Given the possibility that malicious software attacks could be extended to mission critical systems in the DoD or intelligence community, we must develop and implement an expanded program aimed specifically at malicious software that will provide general solutions to replace the ad hoc approaches we use today. Our program, to be executed in cooperation with the Services, DCA, and DIA, with input and assistance from DARPA, is aimed at developing these solutions.