ACQUISITION

THE UNDER SECRETARY OF DEFENSE
WASHINGTON, DC 20301

5 DEC 1988

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: Summary Report of the OASD(C3I) Executive After Action Assessment Team on the Computer Virus of November 1988 -- ACTION MEMORANDUM

An Executive After Action Assessment Team met on November 14 to assess the Internet computer virus attack which was first detected on November 2. The review team was composed of senior representatives from OASD(C3I), DCA, DARPA, NSA and JCS/J6 (Tab H). The team reviewed the events and actions taken after the detection of the virus on ARPANET and MILNET on November 2; reviewed the DARPA report on the technical characteristics of the virus (Tab G); reviewed the report by the National Computer Security Center of the Proceedings of the Virus Post-Mortem Meeting held November 8 (Tab F); and concluded with recommendations for improving the Department's responsiveness to future attacks.

The team generally recognized that due to the extraordinary efforts of a few talented people and the specific nature of this virus, the Department of Defense did not experience a major catastrophe. However, preventive actions should now be taken to reduce the DoD's exposure to future, potentially more destructive viruses. The team concluded that improvements at the national level and within the Department of Defense and other Federal Agencies are advisable and could be grouped in two general categories--response organization and improved awareness.

In order to provide a rapid response capability, there should be a "central coordination center" established as quickly as possible with the following characteristics:

- national level center
- manned 24 hours/day, 7 days/week (could be an extension to an existing center like the NCC under the NCS)
- emergency alerting procedures including key personnel recall (to include key network operations centers and investigative (DoJ/FBI) poc's)
- access to executive level decision makers if necessary

- establish contact to technical experts both in industry and academia
- focal point when major problems (viruses as well as other computer security related vulnerabilities) are identified
- receive problem reports
- coordinate solutions
- able to authenticate source of corrections
- emergency communications capability
- available as the single interface point to press
- archival repository

This central coordination center should be designed under the joint auspices of the National Computer Security Center (NCSC) under NSA and the National Institute of Standards and Technology (NIST, formerly NBS) under Commerce, with technical assistance from DARPA. Its primary focus would be in the unclassified domain, but extensions to the procedures should be developed to deal with classified network/computer events. The Joint Staff is aware of the potential impact on DoD's classified networks and is working that issue in parallel. Current prototype coordination center efforts being initiated by the Software Engineering Institute for DARPA provide conceptual demonstrations and should be the design model for the center.

There is also a need for increased security awareness relating, for example, to passwords and file backups. Lessons learned from this particular virus attack should be documented jointly by the NCSC and NIST and then widely published. Additionally, the Office of Personnel Management (OPM) should be provided with a copy of this report for use in their future training endeavors.

In addition to the general recommendations above, there were events that occurred during the virus that warrant further specific DoD actions. Due to the limited information available and the rapid changes that have occurred in all local and wide area data networks in the past several years, a current vulnerability assessment of all major DoD networked systems should be completed. This action may well uncover additional actions which should be taken to reduce the risk of or the effect of future virus attacks. Consideration should be given to assembling a minimum set of virus analysis tools. The memorandum to NSA (Tab B) includes both of these requirements. The need for intensified research and development in this particular computer security area is also stressed to both NSA and DARPA in the memorandum. Further, responsibilities for the security, management and operation of the Defense Data Network and ARPANET should be more clearly defined, coordinated and documented. The memorandum to DCA and DARPA (also Tab B) includes this requirement.

Recommendations: Because of the joint effort required from Commerce and NSA, recommend that you sign the letter (Tab A) to Mr. Verity, Secretary of Commerce, requesting their collaboration in the development of the response organization and improved awareness.

Recommend you sign the memorandum at Tab B asking NSA, DCA and DARPA to support the findings of the After Action Assessment Team.

Recommend you sign the letter at Tab C to the Department of Justice asking for their support in the development of the central coordinating center.

Recommend you sign the letter at Tab D to OPM forwarding the findings and recommendations to them for their consideration in future computer security training.

Once these actions are complete the press release prepared by OASD (Public Affairs) (Tab E) is recommended for immediate release.

Coordination:

DCA/BGen Bracher *via phone/18 Nov88
DARPA/Dr. Fields *via phone/18 Nov88
NSA/Mr. Gallagher *via phone/18 Nov88
Joint Staff/J6, Dr. Bialick *via phone/18 Nov88

*signature copies will be added as soon as available

Coord: ASD(FM&P) 12/2
Grant S. Green, Jr

Prepared by: DFountaine/IS/57181

Coord: ASD(PA) DEC 15 1988
Fred S. Hoffman
Principal Deputy Assistant Secretary

THE UNDER SECRETARY OF DEFENSE
WASHINGTON, DC 20301

ACQUISITION

5 DEC 1988

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: Summary Report of the OASD(C3I) Executive After Action Assessment Team on the Computer Virus of November 1988 -- ACTION MEMORANDUM

An Executive After Action Assessment Team met on November 14 to assess the Internet computer virus attack which was first detected on November 2. The review team was composed of senior representatives from OASD(C3I), DCA, DARPA, NSA and JCS/J6 (Tab H). The team reviewed the events and actions taken after the detection of the virus on ARPANET and MILNET on November 2; reviewed the DARPA report on the technical characteristics of the virus (Tab G); reviewed the report by the National Computer Security Center of the Proceedings of the Virus Post-Mortem Meeting held November 8 (Tab F); and concluded with recommendations for improving the Department's responsiveness to future attacks.

The team generally recognized that due to the extraordinary efforts of a few talented people and the specific nature of this virus, the Department of Defense did not experience a major catastrophe. However, preventive actions should now be taken to reduce the DoD's exposure to future, potentially more destructive viruses. The team concluded that improvements at the national level and within the Department of Defense and other Federal Agencies are advisable and could be grouped in two general categories--response organization and improved awareness.

In order to provide a rapid response capability, there should be a "central coordination center" established as quickly as possible with the following characteristics:

- national level center
- manned 24 hours/day, 7 days/week (could be an extension to an existing center like the NCC under the NCS)
- emergency alerting procedures including key personnel recall (to include key network operations centers and investigative (DoJ/FBI) poc's)
- access to executive level decision makers if necessary

- establish contact to technical experts both in industry and academia
- focal point when major problems (viruses as well as other computer security related vulnerabilities) are identified
- receive problem reports
- coordinate solutions
- able to authenticate source of corrections
- emergency communications capability
- available as the single interface point to press
- archival repository

This central coordination center should be designed under the joint auspices of the National Computer Security Center (NCSC) under NSA and the National Institute of Standards and Technology (NIST, formerly NBS) under Commerce, with technical assistance from DARPA. Its primary focus would be in the unclassified domain, but extensions to the procedures should be developed to deal with classified network/computer events. The Joint Staff is aware of the potential impact on DoD's classified networks and is working that issue in parallel. Current prototype coordination center efforts being initiated by the Software Engineering Institute for DARPA provide conceptual demonstrations and should be the design model for the center.

There is also a need for increased security awareness relating, for example, to passwords and file backups. Lessons learned from this particular virus attack should be documented jointly by the NCSC and NIST and then widely published. Additionally, the Office of Personnel Management (OPM) should be provided with a copy of this report for use in their future training endeavors.

In addition to the general recommendations above, there were events that occurred during the virus that warrant further specific DoD actions. Due to the limited information available and the rapid changes that have occurred in all local and wide area data networks in the past several years, a current vulnerability assessment of all major DoD networked systems should be conducted. This action may well uncover additional actions which should be taken to reduce the risk of or the effect of future virus attacks. Consideration should be given to assembling a minimum set of virus analysis tools. The memorandum to NSA (Tab B) includes both of these requirements. The need for intensified research and development in this particular computer security area is also stressed to both NSA and DARPA in the memorandum. Further, responsibilities for the security, management and operation of the Defense Data Network and ARPANET should be more clearly defined, coordinated and documented. The memorandum to DCA and DARPA (also Tab B) includes this requirement.

Recommendations: Because of the joint effort required from Commerce and NSA, recommend that you sign the letter (Tab A) to Mr. Verity, Secretary of Commerce, requesting their collaboration in the development of the response organization and improved awareness.

Recommend you sign the memorandum at Tab B asking NSA, DCA and DARPA to support the findings of the After Action Assessment Team.

Recommend you sign the letter at Tab C to the Department of Justice asking for their support in the development of the central coordinating center.

Recommend you sign the letter at Tab D to OPM forwarding the findings and recommendations to them for their consideration in future computer security training.

Once these actions are complete the press release prepared by OASD (Public Affairs) (Tab E) is recommended for immediate release.

Coordination:

DCA/BGen Bracher *via phone/18 Nov88
DARPA/Dr. Fields *via phone/18 Nov88
NSA/Mr. Gallagher *via phone/18 Nov88
Joint Staff/J6, Dr. Bialick *via phone/18 Nov88

*signature copies will be added as soon as available

Coord: ASD(FM&P) 12/2
Grant S, Green, Jr

Prepared by: DFountaine/IS/57181

Coord: ASP(FA) DEC 15 1988
Fred S. Hoffman
Principal Deputy Assistant Secretary

MEMORANDUM

OFFICE OF THE DEPUTY SECRETARY

Office of the Deputy Secretary of Defense

December 12, 1988

MEMORANDUM FOR: Assistant Secretary of Defense (PA)

Please see comment on attached from Mr. Taft which reads:

"Dan Howard should look over the press release here. We should probably have a briefer available on it. WHT, IV"

respectfully,

James A. Prout, III

Military Assistant

c: USD(A)

Attachment

OFFICE OF THE SECRETARY OF DEFENSE

MAD 12 Dec 88

MEMO FOR ~~ASD(PA&T)~~ Exec.

1. See note next under for required action.

2. Please return complete package to C&D, 3A948.

VR

B. Whitehead

Beverly C. Whitehead
Staff Assistant
Corres & Directives

cc: USD(A)

W.

OFFICE OF THE SECRETARY OF DEFENSE

The Senior Military Assistant

SECDEF

Principal concern:

We need to incorporate some qualification to this!

e.g.

-No computers associated with our Nuclear War Plans or Release procedures, or any of our sensitive computers within OSD were or could have been affected.

SEC DEF HAS SEEN

DEC 20 1988

V/R Bill

12/20/88

C+D

Note Adm Owens "Sc

2.

Nancy

14 November 1988

The Center would appreciate knowing of any errors in the enclosed Proceedings of the Virus Post-Mortem Meeting. Please provide corrections to:

National Computer Security Center
Attn: C34
9800 Savage Road
FT. George G. Meade, MD 20755-6000

If comments are received before 10 December 1988, we will publish a set of corrections to be mailed by 17 January 1989.

DRAFT PRESS RELEASE

No.
(202) 695-0192 (info.)
(202) 697-3189 (Copies)
(202) 697-5737
(Public/Industry)

IMMEDIATE RELEASE

IMPROVEMENTS IN COMPUTER SECURITY PROCEDURES

Secretary of Defense Frank C. Carlucci has authorized several measures to improve computer security procedures within the Department of Defense (DoD). These steps resulted from an internal assessment of the Internet computer virus attack that vas first detected on November 2, 1988. The preventive measures are designed to reduce DoD's exposure to future, potentially more destructive viruses and to provide fast, effective response should unauthorized intrusions happen again in government computer networks.

Essentially these initiatives call for greater awareness of the dangers of virus attacks and the establishment of a central response organization. Implementation will require cooperation from other Government Agencies; to that end, the Department of Commerce, through its National Institute of Standards and Technology (NIST), the Department of Justice, and the Office of Personnel Management have been asked to join in combatting the problem of computer viruses.

To increase awareness, the National Computer Security Center (NCSC), under the National Security Agency (NSA), and Commerce's NIST will develop a report on the lessons learned from the early November attack. Among the lessons already identified are requirements for frequent backup procedures to prevent loss of data and the need to discourage the use of common passwords, such as proper names or words found in the dictionary. This report will be available to users and training officials throughout the government.

The DoD is proposing the establishment of a 'central, nationally-based coordination center to handle emergency situations involving computers and netvorks. This center would be in operation 24 hours a day, have contact with technical experts both in industry and academia, and be the focal point--for operating and investigative personnel--when major problems are identified. The center vould receive problem reports, coordinate solutions, be able to authenticate sources of corrections, and provide information to the public on the attack.

Secretary Carlucci has also directed NSA to undertake a current vulnerability assessment of all major DoD networked computers. In addition, DoD will be revieving the need for intensified research and development against virus attacks. DARPA is implementing a coordination center at the Softvare Engineering Institute to provide direct support to the Internet community which consists primarily of research institutions. This center will be developed in close coordination vith NCSC and NIST, and will provide a prototype for the operational systems of broader scope that they will be developing.

TAB E

RECOMMENDATIONS FROM THE 8 NOVEHBER 1988
POST MORTEM OF THE ARPANET/MILNET VIRUS PROPAGATION

1. Establish a centralized coordination center.
This center, supported jointly by NIST and NSA, would also function as a clearinghouse and repository. Computer site managers need a place to report problems and to obtain solutions. This center might evolve into a national level command center supporting the government and private sector networks. The center needs to provide 24 hour service, but not necessarily be manned 24 hours a day (i.e., responding via beeper after hours might be acceptable).

2. Establish an emergency broadcast network.
In the ARPANET/MILNET case, the network was used to disseminate the patches (i.e., antidote) at the same time the virus was still actively propagating. If the net had gone down, there would have been no way to coordinate efforts and disseminate patches. It is recommended that a bank of telephone lines be designated as an emergency broadcast network. The phones would be connected to digital tape recorders and operate in a continuous broadcast mode (or a recorded "binary" announcement mode) to disseminate network status, patches, etc.

3. Establish a response team.
The technical skills required to quickly analyze virus code and develop antidotes or system patches are highly specialized. The skills required are system specific (i.e., UNIX 4.3 in this case), and in many cases exist only at vendor development facilities (e.g., the majority of commercial operating systems are proprietary and source code is not provided to users). The concept of a response team would require advance coordination so that personnel with the requisite skills can be quickly mobilized.

4. Maintain technical relationships with the computer science "old boy network".
The ARPANET/MILNET virus was analyzed and eradicated through the services of this old boy network, not by U.S. Government (USG) personnel. This old boy network is willing to participate in supporting USG initiatives; however, their consensus, support, and trust is required.

5. Centrally orchestrate press relations.
An inordinate amount of time at virtually every site was spent responding to the news media. Multiple press reporting from geographically dispersed sites has the potential for circular reporting of incorrect and misleading data. A single USG focal point at the national level to interact with the press is recommended.

ENCLOSURE

POST MORTEM OF 3 NOVEMBER ARPANET/MILNET ATTACK

Tuesday, 8 November, 0900

AGENDA

WELCOME	L. Castro
KICKOFF	P. Gallagher
INTRODUCTION	D. Vaurio
SITE EXPERIENCES	
HARVARD	C. Stoll
LAWRENCE LIVERMORE	C. Cole
BERKELEY	P. Lapsley
MIT	D. Alvarez M. Eichin J. Rochlis
LOS ALAMOS NATIONAL LABS	A. Baker
DCA/DDN	G. Mundy
ARMY BALLISTICS RESEARCH LAB	M. Muuss
SRI	D. Edwards
HOW THE ATTACK WORKS	
INTRODUCTION	G. Meyers
CONTRAST WITH OTHER VIRUSES	J. Beckman
RECOMMENDATIONS	R. Brand

DISCUSSION: A GOVERNMENT MALICIOUS CODE INFORMATION NETWORK

D. Vaurio	P. Fonash
S. Katzke	W. Scherlis
C. Stoll	L. Wheeler

INTRODUCTION

On Wednesday, 2 November 1988, a sophisticated virus attacked host computers throughout the MILNET and the ARPANET computer network communication systems and significantly reduced computer operations at many facilities. Host managers and software experts responded effectively to this challenge. They identified the virus attack routes, analyzed the virus software, developed antidotes, and communicated information about both the attacks and antidotes to other sites. Defensive software was in place and the virus largely purged from the network within 48 hours.

The National Computer Security Center (NCSC) hosted a meeting on Tuesday, 8 November 1988, to review and document the virus attack and its subsequent solution. Over 75 researchers and administrators from government, industry, and university computer facilities recounted their experiences and shared their approaches to stopping the propagation of the virus and purging the virus from their computer systems. This document is a summary of their reports. We would appreciate comments concerning errors or omissions; please contact Dr. C. Terrence Ireland at the NCSC on 301-859-4485.

THE VIRUS

Once introduced into a host computer the virus can automatically propagate itself to other hosts using several different mechanisms. The virus can use a documented feature in the sendmail program that was intended for use during program development. Sendmail is UNIX user interface to the network mail system. A debugging feature in sendmail allows a user to send a program to a host which then goes directly into execution bypassing the standard loain procedure.

The virus can use a program error in the finaerd program. Finaerd allows a UNIX user to query a remote host about its current activity or the profile of a specific user. The error occurs when specific (and improper) data is passed into the program. When finaerd quits, a rogue program contained in the passed data goes into execution.

The virus can masquerade as a legitimate user by discovering a user's password that was not carefully constructed, logging on as that user and starting the entire infection process over. The virus uses host tables maintained by the system and by its legitimate users to select other hosts and gateways to attack. It takes advantage of high levels of trust between remote hosts frequently accessed by users who can connect to trusting hosts without manually having to go through the loain procedure.

CHRONOLOGY OF EVENTS

The following chronology is compiled from presentations at the 8 November 1988 Post Mortem review. As in any historical analysis, it is difficult to determine the exact sequence of events.

The format gives the Eastern Standard Time (EST) of the event in the left-hand column, followed by the reported time of the event in parentheses if the report came from a different time zone, then a short description of the event followed by a parenthesized list of the people reporting it. The following list of abbreviations is used extensively.

BRL	Army Ballistic Research Laboratory
DCA	Defense Communications Agency
DOE	Department of Energy
LANL	Los Alamos National Laboratory
LLL	Lawrence Livennore Laboratory
NASA	National Aeronautic and Space Administration
UCB	University of California, Berkeley
UCD	University of California, DavisUCSD University of California, San Diego

Wednesday, 2 November 1988

1700		Cornell detects virus (Stoll, Myers)
1830		University of Pittsburgh infects RAND (Myers)
2100	(1800 PST)	Stanford and RAND detect virus (Stoll)
2100	(1800 PST)	BRL hears of virus (Muuss)
2200	(1900 PST)	UCB detects virus (Muuss)
2300		Virus spreads from MIT AI Labs (Stoll)
2328	(2028 PST)	Peter Yee sends first notice that UCB, UCSD, LLL, Stanford and NASA Ames have been attacked by a virus (Rochlis)
2345		Virus enters VGR.BRL.MIL at BRL (Muuss)

Thursday, 3 November 1988

0000	(2100 PST)	UCB shuts off sendmail, finaerd, etc. (Muuss)
0100		More than 15 ARPANET hosts infected (Stoll)
0105	(2205 PST)	Virus attacks LLL (Cole)
0200		Harvard detects virus (Stoll)
0300		Virus spreads from VGR.BRL.MIL (Muuss)
0300		Virus spreads into most subnets (Stoll)
0310		MIT detects virus (Rochlis)
0330	(0030 PST)	LLL begins virus analysis (Cole)

0334		Virus threat posting from Harvard to TCP-IP with sendmail, finserd, and rexecd warnings; requires 26 hours to reach MIT
0400		Network overloading slows spread of virus; Approximately 1000 hosts infected (Stoll)
0400	(0100 PST)	UCB fixes sendmail problem (Lapsley)
0400	(0100 PST)	LLL believes problem serious enough to consider disconnecting from network (Cole)
0400		MIT Athena Project detects virus (Schiller)
0448	(0148 PST)	LLL disconnects from network (Cole)
0500		Stoll alerts MILNET and ARPANET operations centers (Stoll)
0515		MILNET monitoring center notified of virus by University of Pittsburgh(Mundy)
0530	(0230 PST)	LLL notifies DOE Headquarters (Cole)
0600	(0300 PST)	UCB posts sendmail antidote on TCP-IP, USENET bulletin boards (Lapsley)
0600	(0300 PST)	UCB contacts UCD (Cole)
0630	(0330 PST)	LLL installs sendmail antidote on VAX host but it does not prevent reinfection (Cole)
0645		Stoll calls NCSC (Stoll)
0800		Smithsonian Astrophysical Center detects virus (Stoll)
0800		UCB identifies finserd problem (Lapsley)
0806		UCB sendmail fix forwarded to nntp-managers@ucbvax.berkeley.edu (Rochlis)
0900	(0700 MST)	DOE Headquarters notifies Los Alamos (Baker)
1000		DOE Headquarters advises its 7 ARPANET hosts to leave the net (Vaurio)
1000	(0700 PST)	LLL holds first press conference (Cole)
1000		BRL disconnects from MILNET, DISNET, NSI (Muuss)
1007		MIT receives UCB sendmail fix to MIT Project Athena (Rochlis)
1015		MIT Math department detects virus and shuts down gateway to their Suns (Rochlis)
1028	(0728 PST)	NCSC requests copy of virus from LLL (Cole)
1100		MIT begins work on virus (Rochlis)
1130		DCA inhibits mail bridges between ARPANET and MILNET (Mundy)
1130	(0830 PST)	LLL tells Lab Directors to remove their hosts from the network (Cole)
1200		BRLNET completes internal checking for virus, concludes virus no longer present (Muuss)
1500	(1300 MST)	LANL first receives antidotes (Baker)
1500	(1200 PST)	LLL installs antidote and restarts internal networks (Cole)
1500		Antidote published (Stoll)
1800	(1600 MST)	LANL receives antidotes (Baker)

1800		MIT observes virus using the finaerd attack (Rochlis)
1852		Risks digest seen at MIT. Includes Stoll message describing spread and other messages describing sendmail propagation mechanism (Rochlis)
2000	(1700 PST)	UCB begins decompilation of finaerd component (Lapsley)
2100		MIT decodes most of virus strings; sees the net address ernie.berkeley.edu to whom the virus was supposed to send messages (Rochlis)
2100		First press interviews at MIT (Rochlis)
2300		BRL connects protected host to MILNET in effort to capture virus (Muuss)

Friday, 4 November 1988

0000	(2100 PST)	UCB posts finaerd antidote on TCP-IP, USENET bulletin boards (Lapsley)
0500		MIT finishes decompilation (Rochlis)
0900	(0600 PST)	UCB finishes virus decompilation (Lapsley)
1100		Mailbridges returned to service (Mundy)
1200	(0900 PST)	LLL back on network (Cole)
1800		Virus pretty much eliminated (Stoll)

Saturday, 5 November 1988

0030	BRL captures virus in protected host (it's still out there) (Muuss)

Monday, 7 November 1988

0600	Analysis completed by BRL on 2 virus modules (Muuss)
1200	BRL "Vulnerability Sweep" programs operating (Muuss)
1600	Antidotes installed at BRL (Muuss)

Tuesday, 8 November 1988

0900	Post Mortem Review at NCSC

SITE EXPERIENCES

Researchers directly involved with analyzing and stopping the virus attack shared their experiences during a Post Mortem Review at the National Computer Security Center. The following is a summary of their accounts presented at the 8 November 1988 Review.

HARVARD-SMITHSONIAN CENTER FOR ASTROPHYSICS

Personnel were alerted to the situation during the early morning hours on Thursday, 3 November 1988 when the virus was first seen at Harvard. Researchers who responded to the call soon realized that there had been continual network reinfection suggesting that the virus was being spread by the sendmail utility in the UNIX BSD 4.3 and related operating systems.

Five hours later that day the virus reinfected this site. Personnel spent the rest of the day trying to eradicate the virus using the antidote that had been sent our over the network, and dealing with press media inquiries.

Harvard researchers were frustrated in combatting the virus by the lack of coordination with other sites experiencing the same problem; the lack of communication with sites that had been disconnected from the network; the slow network response caused by the saturation of the network by virus packets passing between hosts; and the variety of tactics used by the virus to spread among the hosts.

Harvard researchers provided much-needed assistance to the community by suggesting methods for host cleanup and urging users to change their passwords.

LAWRENCE LIVERMORE LABORATORIES (LLL) OF THE DEPARTMENT OF ENERGY

The LLL security force called the appropriate Laboratory officials just before midnight on Wednesday, 2 November 1988, to report a serious problem with the Laboratory's computer systems. After arriving on the scene the LLL officials assembled a six-person virus team as soon as possible and set up a response center to deal with the situation. The six-person team began exploring LLL computer facilities, all the while maintaining close contact with their University of California, Berkeley (UCB) counterparts.

When officials were convinced that the problem was serious enough to sever network connections to prevent internal spreading of the virus, the people responsible for the various interface connections were instructed to disconnect them. At that point UCB researchers informed LLL by phone that they were working on a

fix for the sendmail problem. A fix was later installed on a VAX which was then reconnected to the network to determine if the fix would prevent reinfection -- it did not. LLL officials then notified DOE headquarters and the University of California, Davis.

A memo was distributed to LLL employees as they arrived for work at the laboratory's three entrance gates. The memo advised everyone to turn on their machines. As the workday began, press inquiries multiplied and the LLL community received an update on the virus situation. LLL laboratory directors were told to disconnect from the network: fixes were described at a meeting with 300 people. By noon Thursday the fixes had been installed on all of the LLL computers and they were brought back on line. Later that day a final press conference was held. Not long after the press conference, LLL's DOE headquarters was again called and again headquarters reported that it had not been hit by the virus.

LLL reported that a test fix had been created and was running. LLL expected to know whether the fix worked by late in the day on 8 November 1988. Because the virus probes a password file, all LLL users are in the process of changing their passwords on all systems.

UNIVERSITY OF CALIFORNIA, BERXELEY

Researchers first noticed that their machines had been attacked shortly after dusk (PST) on Wednesday, 2 November 1988. Within a few hours they had determined that the systems involved included, among others, sendmail and telnet. They were able to determine what the virus was doing through a network message from NASA Ames and phone contacts with LLL. UCB researchers were able to work out an initial fix to disable the debug option in the sendmail system. They later sent out a second fix.

Very early Thursday morning, UCB researchers had observed a second virus attack using the fincrerd system and by early evening began decompiling that virus component. The decompiling process lasted into the early morning hours on Friday. Three UCB terminals were still decompiling as of Monday.

The UCB spokesman was quick to acknowledge that he and his colleagues had received expert assistance in the decompiling effort from members of the Berkeley UNIX workshop attendees who, luckily, happened to be in town.

LOS ALAMOS NATIONAL LABORATORY (LANL) OF THE DEPARTMENT OF ENERGY

The DOE Center for Computer Security received the first word on the virus on Thursday, 3 November 1988. When they learned of

the virus, LANL researchers gathered information from DOE headquarters and LLL, then devoted their efforts to analyzing the virus. By the time LANL had learned of the virus attack, others in the computer security community already had been working on virus fixes.

The LANL effort was hampered by a lack of timely information. Most of the information they received was inaccurate and they seldom received followup information. LANL researchers received conflicting information on the fixes; they did not receive a copy of the first patch until Thursday evening. Since LANL does not have a UNIX expert on site, it was difficult to figure out which fixes would work and which would not, whether the fix was reliable, and who had originated the patch. LANL had difficulty dealing with information being passed from on nontechnical person to another and the technical people had problems interpreting this information effectively.

DEFENSE COMMUNICATIONS AGENCY (DCA)

The MILNET monitoring center, housed at DCA, was notified of the virus attack early Thursday morning. Just before noon on Thursday, the ports on both sides of the mail bridges were looped back to prevent any traffic flow between the ARPANET and the MILNET. DCA received phone calls from the Army Ballistic Research Laboratory (BRL) about once every 3 hours. The MILNET was looped back at 1130 a.m. on Thursday and opened early on Friday morning at BRL's request. The rest of the machines were turned back on later on Friday.

The Network Operations Center was not able to identify this virus attack: monitoring the system usage did not yield the necessary information. It is not unusual for a host (or several hosts) to go down on the MILNET or ARPANET. If DCA receives a call about an ARPANET problem, they take it seriously. In this instance they received no calls until early Thursday morning and saw no indication of a virus. The MILNET and ARPANET monitoring centers do receive constant information on network status, but the propagation of the virus appeared to be routine host activity.

DCA is in the process of evaluating the impact of the virus attack and has instructed personnel to set up a mailbox to collect information. The INTERNET address of the infected machines should be useful. DCA researchers are particularly interested in the impact of the virus on the MILNET.

Operations personnel on the MILNET and the ARPANET are concerned about the lack of administrative reporting.

ARMY BALLISTICS RESEARCH LABORATORY (BRL)

BRL researchers first learned of the virus from the attack on RAND on Wednesday. Early on Thursday BRL received phone calls notifying them that the virus had infected other sites, and later that day they began a coordinated effort with various sites. BRL researchers said that their contribution was fairly modest. The virus attacked only one or two BRL hosts. BRL personnel responsible for installing computer systems must adhere to a U.S. Army regulation which states that each host must defend its own host-to-network interface. Every host is set up to defend itself. The mechanisms to block improper entry attempts and to log all entry attempts are built into every host. Since most weapons systems for the year 2000 are being designed at BRL, researchers are forced to take a very conservative approach to computer security.

BRL was able to develop a protected or "test cell" host which they placed back on the network in an effort to capture the virus for analysis. The protected host was placed on the network very late on Thursday evening, but did not capture the virus until early Saturday morning. By noon on Monday they had created vulnerability sweeping modules to check their machines for infestations of the virus. They will reconnect all of their machines to the network once they believe their machines to be clean and protected (most likely, around noon on Tuesday, 8 November 1988).

The effort expended at BRL was estimated to be 500 work-hours. Six four-line telephones were in active use throughout the entire effort. BRL was especially concerned about the virus attack to recover user passwords. They suggested that Berkeley do a code review of this problem.

SRI INTERNATIONAL (SRI)

SRI became aware of the virus late Wednesday night via information received from other infected sites. The SRI Computer Science Laboratory gateway was down for about 2 hours on Thursday morning with several other gateways down until Friday morning. The Computer Science Laboratory remained largely unaffected due to the lack of host table entries. However, the virus had been detected because of unusual command usage and excessive audit entries. Personnel were able to examine finaerd and to determine how they had been infected. The virus problem consumed an estimated 3 workhours to shut down the gateway, correct the mailers, clean up the system and return to service.

Since the virus attacked only a small Sun network, SRI researchers feel lucky. Personnel are in the process of downloading to the Suns and hope to use the Sun audit data to

detect the virus path. If the virus had entered the main server, SRI feel that could have done considerable damage.

SRI researchers are working on a real time intrusion-detection expert system called IDES sponsored by a DoD computer security program. The IDES team feels that an IDES-enhanced prototype would have detected the sendmail attack as it would have noted the compiler and command usage by finaerd, the excessive audit records, and the input-output and CPU usage. Sendmail connects to standard network ports only. The virus was using nonstandard ports to download its binary images. A system such as IDES could have detected the usage of nonstandard ports.

The communication and coordination problem existed at SRI as it did at other sites. System managers needed more instruction. Suggested actions included establishing a better notification and coordination system and general procedures to follow for the INTERNET hosts.

Serial:

The attendees developed the 11 attached recommendations to reduce the vulnerability of U.S. Government and private networks to virus attack. All unanimously agreed with the recommendations and concluded that the computer security community faces an urgent responsibility to develop the capability to rapidly respond to subsequent attacks. In response to this charge the NCSC in conjunction with the NIST is developing a detailed implementation plan for these recommendations.

Sincerely,

LAWRENCE CASTRO
Chief
Research and Development

Encl:
a/s

NATIONAL COMPUTER SECURITY CENTER

FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: C3-0021-88
14 November 1988

MEMORANDUM FOR DISTRIBUTION

SUBJECT: 8 November Post-Mortem Meeting on the ARPANET/MILNET Virus Propagation - INFORMATION MEMORANDUM

The National Computer Security Center (NCSC) hosted a meeting on 8 November 1988 of highly respected researchers from government and university research facilities for the purpose of documenting their unique contribution in categorizing and resolving the recent virus attack. Representatives from Air Force, Army, ASD (C^3I), CIA, DARPA, DCA, DOE, FBI, NIST, NCSC, NSA, and their colleagues from academia, recounted their site experiences and shared their respective approaches to thwarting the propagation and purging the virus from their systems. The sharing of information that took place at this meeting was unprecedented and reflected very positively on all participants. The high degree of professionalism and dedication by those involved, particularly in the university research community, was the key to rapidly understanding and ending the propagation of this virus. In the pages that follow, our editors have captured the essence and record of the meeting's presentations and discussions. Some of the material is obviously in "early draft" form; however, we believe that the value of these proceedings will be in its timely dissemination as opposed to its format quality.

This virus attack was the first occurrence of a virus propagating autonomously via a network and affecting host computers throughout the United States. The goal of the post-mortem was to examine this virus incident in depth and develop an assessment of U.S. capability to react and recover from future attacks of this nature. While the DoD ARPANET/MILNET was the focus in this incident, the lessons learned are generic and applicable to all networks or distributed computing systems processing classified or unclassified data.

TABLE OF CONTENTS

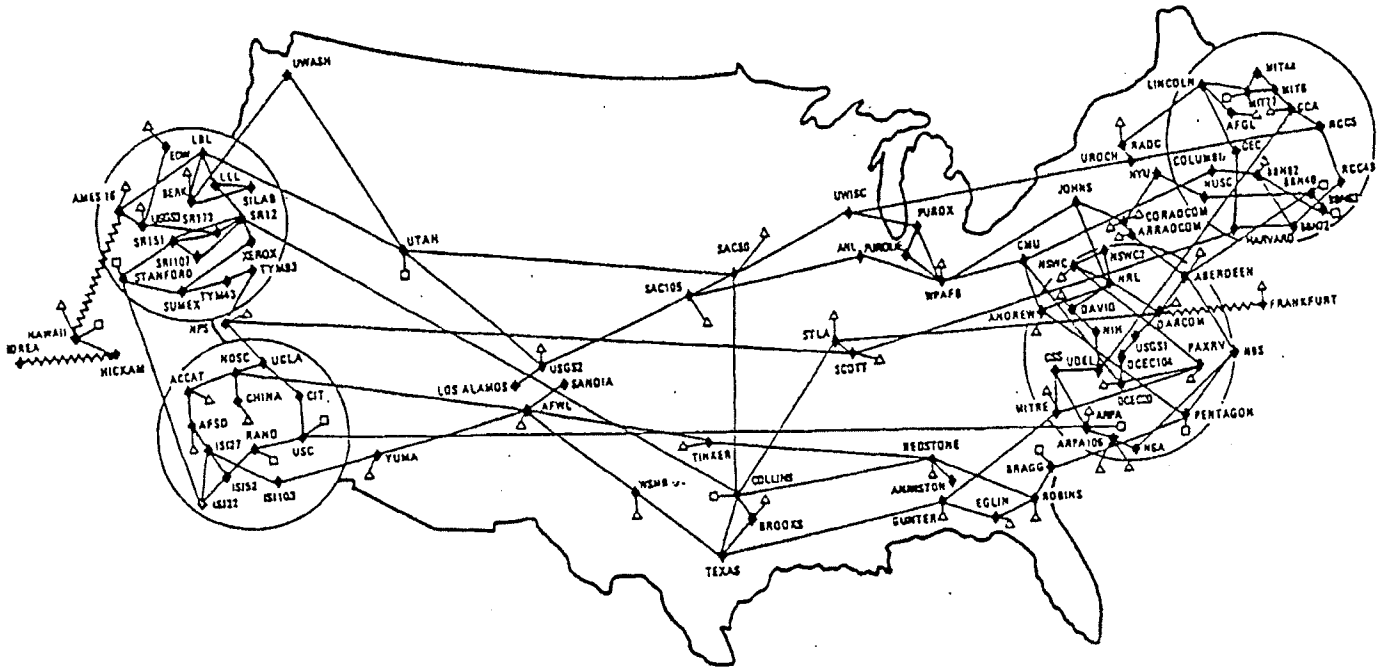
National Computer Security Center

PROCEEDINGS

of the

VIRUS POST-MORTEM MEETING

8 November 1988



ARPANET / MILNET Computer Virus Attack

of

3 November 1988

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
1400 WILSON BOULEVARD
ARLINGTON, VA 22209-2308

8 November 1988

MEMORANDUM FOR THE DIRECTOR

SUBJECT: Account of the 2 November 1988 internet virus **(updated)**

The swiftness of onset and scale of infection of the recent Internet virus reinforce the need to make more aggressive steps in developing appropriate technology and policy for computer security.

The attached memorandum provides details concerning the technical characteristics of the virus, **and it** makes **preliminary** recommendations concerning associated policy issues and areas for accelerated research.

William L. Scherlis
Information Science and Technology Office

Stephen L. Shires
Information Science and Technology Office

1. THE **VIRUS.**

1.1. ONSET. The virus appeared on computers interconnnected by the **ARPANET,** MILNET, and associated regional and local networks. These are unclassified networks linking tens of thousands of users and supporting a wide range of research and military applications.

The onset of the virus was extremely rapid. There was an initial report from Cornell at 1700 EST Wednesday 2 November 1988, but the first reports outside Cornell occurred four hours later at approsimately 2100 EST, when the virus appeared at more than a dozen major sites. Sites affected include UC Berkeley, University of Maryland, Cornell, Carnegie Mellon, **NASA** Ames, MIT, University of Southern California, UCLA, Livermore Laboratories, BRL, and many others. By midnight, the virus had spread through more than a thousand computers (workstations, minis, and mainframes) on both the **ARPANET** and MILNET and on connected local networks. The virus first appeared on DARPA/ISTO computers just before midnight.

1.2. SYMPTOMS AND BEHAVIOR. The principal ***symptoms*** of the virus, as perceived by computer users, are degradation of system response and loss of available space in the file system. These are benign symptoms in the sense that (1) the virus does not delete or alter existing files, and (2) it does not compromise files by transmitting them to remote sites or by altering protections.

The principal activity of the virus is to replicate itself and spread to other machines. The virus runs as a background process on its host, so its presence is not immediately obvious to a user. In many cases, large numbers of multiple independent instances of the virus appear on single machines, with resultant degradation of performance.

1.3. METHODS OF ATTACK. The virus attempts to propagate itself using four methods of attack. Two of the four methods **(SENDMAIL** and FINGERD) relied on implementation errors (now fixed and distributed to most major Sites) in network protocol server programs. **A** third method (PASSWORD) is a "brute force" method. The last method (RSH) exploits security assumptions in local networks that are violated as **a** result of successful attack on the external local net security perimeter using one of the other three propagation methods.

It must be emphasized that the implementation errors that permit spread of this particular kind **of** virus are NOT in the network protocols themselves, or in the host operating system designs or their implementations, or in the computer or network hardware. They are in specific implementations of programs running on hosts that provide specific network services.

SENDMAIL ATTACK. In most cases, the virus propagates itself to a remote machine by exploiting an error in a server program called SENDMAIL that handles the sending and receiving of computer mail. The program implements **a** network mail protocol called SMTP. 'There is nothing wrong with the protocol in this case. The error was that the program that uses this protocol adds a new feature. Ordinarily, the program

receives a block of text along with header information indicating which user is the recipient of the message. The block of text is inserted at the end of the user's mail file and a record is added to a log file. Erroneous messages are logged and returned to the sender and possibly a postmaster mailbox as well.

The developer of the **SENDMAIL** program had included a special feature, however, to facilitate his debugging. Mail messages whose headers contain a special DEBUG flag are interpreted not as text but as programs to be executed. It must be emphasized that this feature is not part of the protocol, but was included by the developer for his own convenience. It transpired that when the program went into formal distribution the feature was not disabled.

The virus propagates itself by exploiting this feature to create a running process on a remote machine with whatever access and privileges were available to the SENDMAIL process. In most cases, because **of** file protections and operating system safeguards, these privileges are sufficient to do moderate damage at most. In some cases (usually involving poor systems configuration), the potential for damage is much greater.

But, as indicated above, the virus does not remove files even when it is possible for it to do so. In this sense, it is benign.

PASSWORD ATTACK. The virus tries to establish itself **as a** legitimate user (rather than remaining a system process wih few privileges) on the **infected host** and other local machines by guessing passwords. It does this by trying **as passwords** (1) the words in the standard online spelling dictionary, (2) various transformations **on** the users name, and (3) words in a special list of possible passwords included **in** the virus itself. Ordinary login attempts cannot use this technique because time delays are generally inserted on all password failures. In this case, the virus uses its own implementation of the DES algorithm to generate the encoded password representation used in Unix password files. (This could imply that the virus is subject to export control in the same way that Unix **with DES is currently** subject to export **control.)**

There were cases in which this guessing of passwords by the virus was successful, and the virus often appeared running as if it were a legitimate user. The attacking program contained no indication of any intent to exploit special access it might acquire as a result of this attack.

RSH ATTACK. Once established on a local network, the virus could propagate itself by exploiting a feature, called RSH, that enables local machines to authenticate users for each other. This feature is convenient when a local network is itself well protected, and when users on that network must interact frequently. If the feature is enabled in a local network, and if the virus had succeeded as masquerading as a legitimate user, then it could spread quickly in a local net since the machines in the net would assume that the virus had already been authenticated.

FINGERD ATTACK. **A** fourth method of entry was to exploit an error in a different protocol server program, for locating users on remote machines. This program error is exploited by the virus to establish a running process on the remote machine.

1.4. ESTABLISHING THE INFECTION. After a successful attack, the first stage of infection is the infiltration of a small "bootstrap" program onto the remote machine. The bootstrap program then retrieves from the previous point of infection a much larger main program. Both the bootstrap program and the main program were designed to evade detection by masquerading as system or user processes and by removing the programs from the disk once they are running in memory.

The bootstrap program is transmitted in source form, and it compiles and loads itself on the remote machine. Its main function is to retrieve the main program. As the virus propagates, the bootstrap program is adapted (by the main program that propagates it), so that it refers only to the most immediate infected source.

The main program, which contains the actual code for assaulting remote machines (using the four methods detailed above), is transmitted in object form. Actually, two versions of the program are transmitted for two different instruction set architectures. A portion of the data of the main program is encrypted (using a simple XOR code). When the program starts, it decrypts most of its data area that is the main memory of the newly infected host. The disk version remains in encrypted form, and is eventually deleted as the virus covers its tracks.

Once the main program is running, the machine is in an infectious state. In many cases, multiple instances of the program were running simultaneously, each attempting to infect other machines on the network. Randomization techniqes are used to ensure that the multiple instances did not overly interfere with each other. The virus would also occasionally spawn a clone of itself and then terminate, with the effect that no large accumulations of CPU time would be evident on casual browsing of process status information.

1.5. DETECTION AND DIAGNOSIS. The presence of a large scale virus infection is readily detectable by casual users due to its effect on machine performance. Small scale infections are not as easily noticed (and, indeed, it is easy to imagine that the virus could have been tuned to be less readily detectable by decreasing the extent of denied service). Expert users generally could spot the spurious running processes and remove them as they appeared. This provides fast symptomatic relief, but not immunization.

When detection first occured Wednesday night, many sites disconnected themselves from the network and powered down critical machines. Both Livermore Labs and NASA Ames disconnected themselves from the network. Bridges between MILNET and ARPANET were closed, but only after the infection had already spread to MILNET. Many sites left one or two machines running in order to enable communication with other sites and to permit study of the virus activity. In the DARPA/ISTO local network, for example. infection occured around midnight Wednesday. (The other DARPA offices were unaffected because the); are not on the network.) The network connections were disabled during the night, and machines were powered down Thursday morning.

As die virus spread; systems programmers at the various network sites established close communication and were able to share observations and results on an hourly

basis. By continually killing spurious processes as they appeared on computers, most of the systems programmers were able to stay online and share results using network mail and bulletin boards. The virus did, however, have the effect of slowing communications on the network as it spread Wednesday night and Thursday morning. Becuase of the close working relationship DARPA has with the research community affected, it was able to facilitate communication among groups, track the situation, and keep appropriate people advised. Many of the procedures followed at **DARPA** were based-on a prior experience with the 13 May 1988 virus hoax.

Monitoring of the virus process activities revealed the various methods of attack that were used, which led to the development of immunization techniques and implementation of preventive measures.

1.6. IMMUNIZATION **AND PREVENTION.** For each of the four methods of attack, immunization and/or prevention measures were developed. Many major sites had already eradicated the virus and were immunized by Thursday evening or early Friday morning. **DARPA** machines were running and connected to the network within 18 hours of appearance of the virus at **DARPA.**

SENDMAIL -- IMMUNIZATION. This method of attack was permitted due to an error in a widely distributed mail protocol server program. Within hours of discovery of the virus, fixes were in general distribution. The first posting was made at 0600 EST Thursday, with corrections that followed. The fixes were sufficiently simple that they could be carried out by instructions given over the telephone. These fixes generally prevented infection of a site, if it was not infected already.

PASSWORD -- PREVENTION. This method of attack works only in cases where users fail to follow conventional password guidance, which is not to use dictionary words or their own names. Affected users and potentially affected users were instructed ***to*** change their passwords.

RSH -- PREVENTION. This method of attack works only because of a failure of the external security perimeter of a local network. In most cases, the level of trust among machines in local networks was temporarily reduced (i.e., by disabling RSH) pending full eradication and immunization.

FINGERD -- IMMUNIZATION. A day after discovery of the virus, fixes for FINGERD were in general circulation. The error was a common programming error. Input to FINGERD that was too long resulted in certain unrelated internal data areas being overwritten by portions of the input. The virus exploited this by using overlong input values that overwrote the unrelated data areas with data that resulted in the virus being able to start a new process. The fix to FINGERD is to insert a check for incorrect input.

1.7. ASSESSMENT AND RECOVERY. Other than denial of service and lost time, no specific unrecoverable damage was caused by the virus. As indicated above, no files are known to be lost, and no information is known to be compromised.

Once eradication and immunization were underway, the systems programmers at Berkeley and MIT embarked on a project to analyze the 60000 bytes of encrypted object code and data for the main program. A special program was written to decrypt the data for the main program. The dictionary of common passwords stored in the virus was extracted and distributed to many sites.

The major challenge of the analysis project was reverse-engineering the object code into source programs. A preliminary version was completed on Saturday 5 November. MIT has released a prelim-inary document describing the actions of the object code.

The derived source code itself is not being released, however,since many systems are not yet fully immunized, and the code exposes specific vulnerabilities. The program is sophisticated and was written by someone with considerable systems expertise.

The smaller "bootstrap" program used upon initial penetration is propagated in source form. Copies of the messages were obtained when mail to remote sites not running the bad SENDMAIL program returned the message **.back** to the Postmaster mailbox of the originating (previously infected) site. These intercepted mail messages contain the source text.

2. PRELIMINARI' OBSERVATIONS.

2.1. RISKS. The **ARPANET** is a dual-use network. It serves as a laboratory for performing experiments in large scale networking while providing services for the research community. Because of the leverage it provides, this dual-use approach is common in the computing research community, and applies to other large scale technologies such as operating systems, parallel computers, user interaction systems, experimental expert systems shells, and the like.

Historically, the research community has been willing to sustain the additional risk in order to obtain functionalty beyond the state *of the art*

Policy requires that no classified data be accessible on the **ARPANET,** MILNET, and interconnected networks, except through **NSA** certified private line interfaces. Messages encrypted using approved devices are unclassified..The Internet community consists of 300 or more sites, some of which have hundreds (and in some cases thousands) of computers attached to local networks. A common set of protocols, called TCP/IP, enables communication in the net despite the wide range of computers and operating systems employed.

A key issue is the extent to which improved security safeguards are required by the Internet community.

2.2. COSTS. Current systems that have **high** security requirements generally achieve this through (1) physical isolation of the network or computing installation (an exception is the use of **NSA** approved private line interfaces), (2) provision of access only to cleared personnel, and (3) use of design and engineering principles including

redundancy, tagging, and precise specifications. Satisfying these requirements generally means making sacrifices in functionality, performance, and cost. Interoperability and open interfaces are also often sacrificed, making it difficult to incrementally improve the capabilities of the systems after deployment.

In research systems, on the other hand, security is often sacrificed in order to maximize functionality, performance, and flexibility. In general, however, there are tradeoffs among these characteristics, with security currently exacting a very high cost.

2.3. VULNERABILITIES. The virus exploited errors in the implementation of two protocol server programs. Installation of correct versions of the programs, as was done as part of the response to this virus, resulted in immunization.

The virus exploited implementation errors. The vulnerabilities exploited by the virus are NOT in the network protocol design, the operating system design, or the underlying hardware design.

(This is in distinction with the PC community, in which viruses are able to propagate and cause damage as a result of specific shortcomings of design of the PC operating systems. In the PC community, virus detection and eradication are often quite difficult, and immunization is often impossible.)

It should be noted that if the author of this virus had chosen to be destructive, wanton destruction of user files would nonetheless have been prevented by a properly implemented and configured operating system. Errors in implementation can result in vulnerabilities, of course.

For this reason, formal security guidelines such as those articulated in the Orange Book emphasize good implementation practice. B1 secure implementations of Unix now exist, and implementations at higher levels of security are being developed for Unix/POSIX (B3 level) and for Mach (A level and beyond). Confidence in security in these cases is achieved through a social process involving attention to design principles and inspection of code. Higher confidence can be obtained using the formal methods approaches that now being developed.

It is probably fair to conjecture, however, that even if the operating system kernel was trusted at B3 or A level, a virus would still be able to propagate itself by exploiting server errors (in cases where servers are outside the kernel). Of course, this hypothetical virus would not be able to damage or compromise protected data.

3. TECHNOLOGY AND POLICY ISSUES

3.1. GOALS. In the near term, effective procedures must be developed that can provide suitable response to viruses that can spread to thousands of computers across the country in a matter of hours, as this one did. In the longer term, policies and technology solutions must be developed to reduce vulnerability of both classified and unclassified networks and systems while not sacrificing functionality and Performance.

3.2. RESPONSE PROCEDURES. We recommend the formation of a National Computer Infection Action Team (NCIAT) to work in the Defense and national research communities.

FUNCTION. The NCIAT would have three functions: (1) It would provide a mechanism for coordinating response in acute situations. As the recent virus episode demonstrates, extremely rapid mobilization and coordination with the community is essential. (2) It would provide a coordination point for rumors of viruses. In the recent virus episode there was no advance warning; the virus simply appeared. Several months earlier, however, there was a case in which there were rumors of a virus about to strike, with tremendous resulting defensive activity in the community. The virus was a hoax. (3) It would provide a focal point for discussion of prevention, coordination, and awareness in the community, perhaps through publications.

ORGANIZATION. The NCIAT would operate at three organizational levels. (1) The top level would consist of an "Executive Group" at the level of flag officers who would empower the group and have sufficient authority and access to permit fast response when required. (2) The middle level "Action Group" would provide working level support in the government. (3) The operating level "Associates Group" would include elite systems programmers from industry, government, and the research community. This group is the heart of the NCIAT. These positions would be assigned in such a way that appointment as an Associate is a mark of significant recognition and accomplishment as a senior systems programmer. Rotating terms of appointment would enable a new set of Associates to be designated each year after a formal selection process. This would ensure effective community representation. Retired Associates remain a source of expertise, though they are not expected to provide the same rapid response as Associates. Associates would become a primary means of access for the community to NCIAT both for routine and emergency operations.

Membership in NCIAT Executive and Action groups would include Services and Agencies in DoD, NSA, NCSC, NIST, NSF, the FBI, and other appropriate organizations. Close coordination contacts would be developed with industry and with major research laboratories, including the National Labs. A database of key experts and industry and government contacts would be maintained. NCIAT would have a small core staff to support routine operations, data collection and dissemination, and, in acute situations, communications with NCIAT group members and others. The NCIAT would focus its initial efforts in the Internet community.

NCIAT would have a well-known network mailbox, an 800 number, and a computer facility to provide database service and to enable emergency data and authentication communications. The computer facility would consist of a primary system that is connected to the Internet and a secondary system that is not connected to the network, but only to the first system, and through a protected interface. The primary system would serve as a database platform and would supprt routine operations. The second system, through provision of dial-up or other special access support. would provide

NCIAT members and others in the community with a known communications point to be used in an emergency, even if the Internet should become damaged or unavailable.

Community support for NCIAT is essential, since discussion of local viruses and vulnerabilities can require a high level of trust and respect for privacy. It is anticipated that much coordination with the user and systems support community would occur at the Associates level.

3.3. TECHNOLOGY CHALLENGES. We recommend that security assessments should be done for existing nonclassified systems in order to determine (1) what are appropriate natural levels of security that can be achieved with reasonable impact (e.g., cryptographic checksums for configuration management, validation viruses, server and gateways audits, audit trails, authentication service), and (2) what mid-term technology steps can be made that will provide significant improvements.

For the longer term, we recommend acceleration of investment in technology for the development of trusted and secure systems. The challenges are (1) to increase the absolute level of security attainable and (2) to reduce drastically the functionality and performance premium for security and trust. The first challenge must be met if we are to build systems that provide the very high levels of security assurance and trust that are required in highly sensitive applications and in life-critical systems.

A basic technology in this area is formal methods, which also has applications to parallel programming and program optimization. The European defense community is already moving towards use of formal methods for systems acquisitions in which safety and security are critical. A verified microprocessor chip design has already been produced by RSRE.

Major areas for development with more immediate payoff include (1) operating systems security, particularly for parallel operating systems, (2) secure network technology, (3) trusted servers, including authentication service and network file service, and (4) trusted hardware designs, such as for embedded 32 bit RISC processors.

3.4. POLICY AND BALANCE. We recommend that closer working relationships be developed among the various organizations involved in computer security and trust. At a minimum this includes NSA (as a user), NCSC (as a policy and certification organization), MST (as a policy and certification organization), DARPA (as a technology developer), DCA (as a network operator), and Service agencies.

In the recent episode, an informal open process in the community led to fast eradication and immunization. It is obvious that any formalized response mechanism must be at least as efficient as the current process. This requires clear channels of communication, trust and cooperation among the parties involved, effective two-way information flow, and, most importantly, the empowerment of the best technical people available in the community to work together to detect, diagnose, and resolve acute problems when they occur.

Executive **After** Action Assessment Team
"DoD Computer Viruses"

OASD(C3I)
D. Diane Fountaine, Chairperson
Director, Information Systems

DCA
Brigadier General Phillip Bracher
Director, Defense Communications System Organization

DARPA
Dr. Craig Fields
Deputy Director for Research

NSA
Mr. Patrick R. Gallagher Jr.
Director, National Computer Security Center

JCS/J6
Dr. Irving Bialick
Deputy Director for C3 Systems Integration

EXECUTIVE SECRETARY
Lt Col Larry Wheeler
OASD/C3I/Information Systems

TAB H

OSD

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
FOR COMMAND, CONTROL, COMMUNICATIONS
AND INTELLIGENCE

Date November 21,1988

Memo for: Administrative Information

Subject: Assembly and Mailing of the TABS on the OASD(C3I) Computer Virus Report

Due to the voluminous nature of the attachments to each of the TABS in the computer virus report, recommend the complete package be returned to **OASD(C3I)-IS** for assembly and mailing, after signature by SECDEF.

D. Diane Fountaine
Director
Information Systems

Prepared by: Lt Col Wheeler/IS/57181/lw

* U.S.G.P.O.: 1984-454-380/18738

AO 3946

THE SECRETARY OF DEFENSE

WASHINGTON, THE DISTRICT OF COLUMBIA

FIXES

Honorable William Verity
Secretary of Commerce
Washington, D.C. 20230

Dear Bill:

Shortly after the Internet computer virus attack, which was first detected on November 2, we formed an Executive After Action Assessment Team within the Department of Defense. The team met on November 14 and reviewed the events and actions taken after detection of the virus on ARPANET and MILNET; reviewed the report by the National Computer Security Center of the Proceedings of the Virus Post-Mortem Meeting held November 8 1988 (Enclosure 1); reviewed the DARPA report on the "technical characteristics of the virus (Enclosure 2); and concluded with recommendations for improving the Department's responsiveness to future attacks.

As you will see from the team's report to me (Enclosure 3), the two areas on which we need to focus are the development of a central, national level coordination center, and increased computer security awareness. It became quickly evident during their analysis that the actions which need to be taken in the unclassified domain should be addressed by the National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC), with technical coordination from the Defense Advanced Research Projects Agency.

I have requested that each of the Defense Components involved in the after action assessment support the recommendations on a priority basis. In tasking the National Security Agency, I have asked that the NCSC be ready to work with the staff of NIST to quickly address the establishment of a central coordination center and the publication and wide distribution of computer security lessons learned from this incident. I solicit your perscnal support for this effort and ask that we move rapidly to improve our national posture to deal with potential computer security problems in the future.

Sincerely,

Enclosures:
As Stated

355