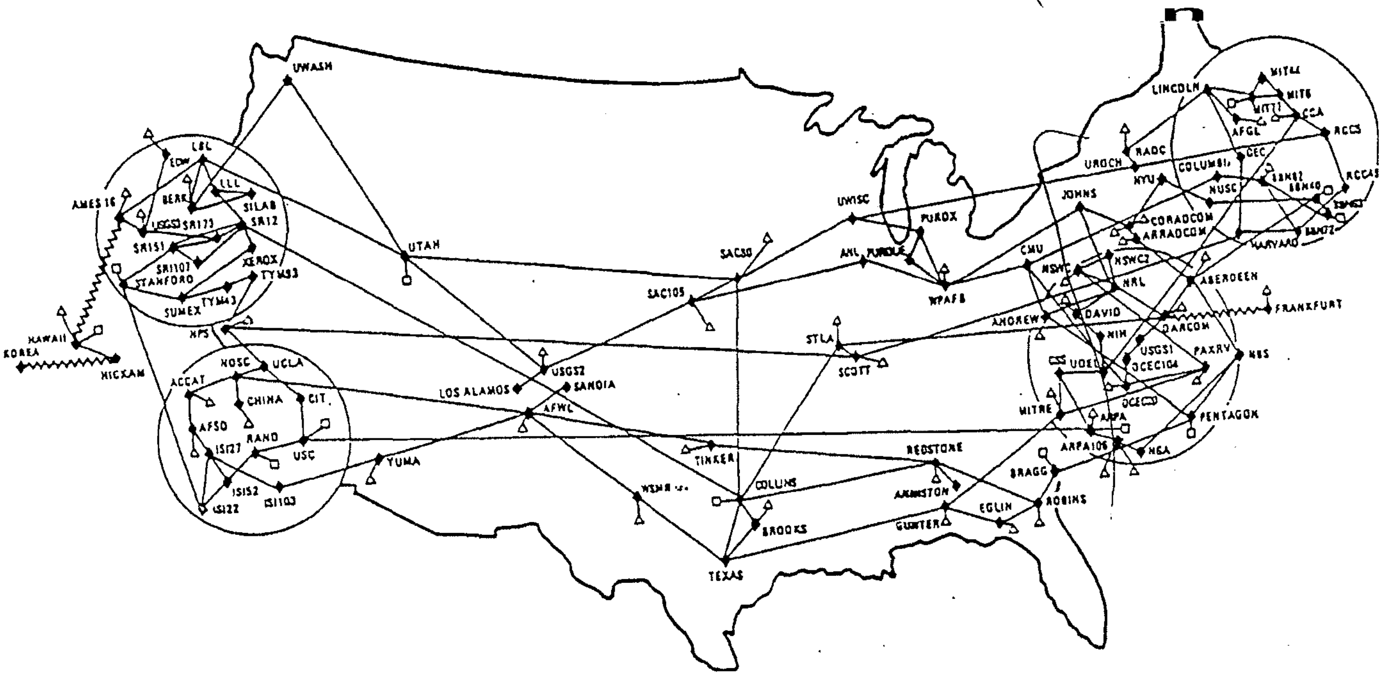
National Computer Security Center
PROCEEDINGS
of the
VIRUS POST–MORTEM MEETING
8 November 1988



ARPANET / MILNET Computer Virus Attack
of
3 November 1988

TABLE OF CONTENTS

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.

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

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

6. Develop etandard procedures for "trusted fixes."
During this recent event, several different fixes or patches to the virus were disseminated to users. There was no method available to determine if the fix was to be trusted (i.e., to authenticate the purported origin of the fix and determine whether the patch itself contained malicious code). A related issue concerns the legal liability of the individual or organization developing and promulgating the fix in the event it causes undesired results. A good samaritan exclusion is desired.

7. Designate a centralized repository for virus infection reports.
The National Computer Security Center (NCSC) has designated a bulletin board on Dockmaster as a central repository for this purpose.

8. Include law enforcement agencies in the planning and implementation phases.
The response and recovery from viral attacks will generate information which may be evidence from the legal perspective. Their input is needed. Participation in response teams should be an option.

9. Training for system operators.
Many system operators lacked the technical ability to understand that a virus had attacked their system. Similarly, those same system operators had difficulty in administering the antidote. It is recommended that standards be established and a training program started. A similar event occurred during the 1986 German hacker penetration of ARPANET/MILNET; i.e., the system operators when informed that their system had been penetrated refused to believe it.

10. Establish etandard backup policies.
The conventional methodology of routinely performing a system backup by saving a "mirror" image on disk, would have been disastrous in the case of this particular virus because the virus would have unwittingly been included on the backup. New standards and criteria for backup should be developed and promulgated by NIST or the NCSC.

11. Develop a common set of virus analysis tools.
The analysis of a virus is initiated by reverse engineering the virus code. The reverse engineering of software is complicated, tedious, and computer specific. A common set of virus analysis tools needs to be developed and available for use by the quick response team.

Caveat: All of the recommendations must be implemented within the constraints of PL 100-235. PL 100-235 assigns responsibilities in computer security to NIST for unclassified systems and the National Security Agency for classified systems. These recommendations clearly fall into both areas.

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
S. Katzke
C. Stoll
P. Fonash
W. Scherlis
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 login procedure.

The virus can use a program error in the fingerd program. Fingerd 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 fingerd 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 login 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 Livermore 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, finserd, 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 *finserd* 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 *finserd* 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, BERKELEY

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 fingerd 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 finserd 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.

ATTENDEES

Title	FirstName	LastName	Organization	Address	Phone
Mr.	Don	Alvarez	MIT-Center for Space Research **37-618**	77 Massachusetts Ave. Cambridge, MA **02139** Boomer@space.mit.edu	**617-253-7457**
CPT	**Bill**	Arbaugh	HQDA, OCSA	Attn : CSDS-AI Washington, D.C. **20310** Arbaugh@pentagon-ai.army.mil	**202-694-6912**
Ms.	Beth	Babyak	FBI-HQ	10th & Pennsylvania Ave., NW Rm **8391, TL245** Washington. D.C. **20535**	
Mr.	Dave	Bailey	DOE	Production Operations Division P.O. Box **5400** Albaquerque, NM **87115** DB@a.lanl.gov	**505-846-4600**
Ms.	Alice	Baker	DOE	**P.O Box 1663** MS **E541** **Los** Alamos, **NM 87545** Alb@lanl.gov	**505-665-2577**
Mr.	Joseph	Beckman	NCSC Attn : **C31**	**9800** Savage Road Ft. Meade, MD **20755-6000** Beckman@dockmaster.arpa	**301-859-4489**
SA	Paul	Boedges	HQ AFOSI/IVSC	Bolling AFB Washington. D.C. **20332-6001**	**202-767-5847**
Dr	Russell **L.**	Brand	Lawrence Livermore National Labs	**1862** Euclid Ave., Suite **136** Berkeley, CA **94709** Brand@lll-crg.llnl.gov	**415-548-136L**
Dr	Leon	Breault	DOE	Washington, D.C. **20545**	**301-353-4255**
Mr.	Brute	Calkins	NCSC Attn: C31	**9800** Savage Road Ft. Meade, MD **20755-6000** **BCalkins@dockmaster.arpa**	**301-859-4488**

Title	FirstName	LastName	Organization	Address	Phone
Mr.	Larry	Castro	NCSC Attn : C3	9800 Savage Road Ft. Meade, MD 20755-6000	301-859-4485
SA	Jim	Christy	HQ AFOSI/IVSC	Bolling AFB Washington, D.C. 20332	202-767-5847
Mrs.	Judi	Citrenbaum	NCSC Attn: C34	9800 Savage Road Ft. Meade. MD 20755-6000	301-859-4486
Mr.	Chuck	Cole	Lawrence Livermore National Labs	P.O. Box 808 Livermore, CA 94550 Cole@lll-crg.llnl.gov	
Mr.	William	Collins	NCSC Attn: C34	9800 Savage Road Ft. Meade, MD 20755-6000	301-859-4486
Mr.	Jared	Dreicer	DOE	P.O. Box 1663 M/S E541 Los Alamos, NM 87545 Jzzd@lanl.gov	505-667-0005
Mr.	Dave	Eastep	Attn: T33	9800 Savage Road Ft. Meade. MD 20755-6000	301-688-5456
Mr.	David	Edwards	DCA	Code B602 McLean Washington, D.C. 20305-2000 DLE@csl.sri.com	703-285-5206
Dr.	Mark	Eichin	MIT Project Athena	4 Ames Street, Nichols 201 Cambridge, MA 02139 Eichin@athena.mit.edu	617-253-7788
Mr.	Paul	Esposito	Attn : T44	9800 Savage Road Ft. Meade, MD 20755-6000	
Mr.	Steven D.	Fleshman	Attn: X21	9800 Savage Road Ft. Meade, MD 20755-6000 Fleshman.xeva/@dockmaster.arpa	301-688-5726

Title	FirstName	LastName	Organization	Address	Phone
Mr.	Pete	Fonash	DCA	Code H102 **8th &** Courthouse Road Arlington, VA Fonash@edn-vax.dca.mil	202-746-3642
Mr.	Paul	Franceus	NCSC Attn: C321	9800 Savage Road Ft. Meade, MD 20755-6000 Franceus@tvcho.arpa	301-859-4491
S.A.	J. Michael	Gibbons	FBI-WMFO	300 N. Lee Street, Suite 500 Alexandria. VA 22314	703-683-2680
Mr.	Bill	Gordon	**DoD**	Washington, D.C. 20505	703-482-5493
Mrs.	Kimberly	**Hebda**	NCSC Attn: C311	9800 Savage Road Ft. Meade, MD 20755-6000	301-859-**4488**
Mr.	Gericks	Hendricks	NISAC/S2	9800 Savage Road Ft. Meade, MD 20755-6000	
LT	Alan	Hensley	NCSC Attn: C34	9800 Savage Road Ft. Meade, MD 20755-6000 Hensley@dockmaster.arpa	301-859-4494
Mr.	George	Hoover	Attn: V45	9800 Savage Road Ft. Meade, MD 20755-6000 Hoover@dockmaster.arpa	301-859-4374
Mr.	Douglas	Hunt	National Inst. of Standards & Tech.	Computer Security Division - Bldg 225 Gaithersburg, MD 20899 DHunt@ecf.icst.nbs.gov	301-975-5140
Dr.	David J.	Icove	**FBI**	FBI Academy Quantico, VA	703-640-1176
Dr.	Terry	Ireland	NCSC Attn: C	9800 Savage Road Ft. Meade, MD 20755-6000 **Ire**land@dockmaster.arpa	301-859-4371
Mr.	John	Jackson	NCSC Attn: C321	9800 Savage Road Ft. Meade, MD 20755-6000 Jackson@tvcho.arpa	301-859-4491

Title	FirstName	LastName	Organization	Address	Phone
Dr.	Mike	Karels	University of California	CSRG Computer Science Div., EECS Berkeley, CA 94720 **Karels@ucbarpa.Berkeley.** EDU	415-642-4948
Dr.	Stu	Katzke	National Inst: of Standards & Tech.	Technology Bldg; A2 16 Gaithersburg, MD 20899 Katzke@ecf.icst.nbs.gov	975-2929
Mr.	Stephen J.	Kougoures	Attn: S81	9800 Savage Road Ft. Meade. MD 20755-6000	301-688-6026
Mr	Timothy W.	Kremann	NCSC Attn: C31	9800 Savage Road Ft. Meade. MD 20755-6000	301-859-4488
Dr.	Phil	Lapsley	University of California	Experimental Computing Facility 199B Cory Hall Berkeley, CA 94720 Phil@ucbarpa.Berkeley.EDU	415-642-7447
Mr.	Peter	Loscocco	NCSC Attn: C321	9800 Savage Road Ft. Meade, MD 20755-6000 Loscocco@tycho.arpa	301-859-4491
SSA	R. Stephen	Mardigian	FBI	FBI Academy Quantico, VA	704-640-6131
Capt	John	McCumber	NCSC Attn: C	9800 Savage Road Ft. Meade. MD 20755-6000	
Mr.	Jack	Moskowitz	NCSC Attn: C2	9800 Savage Road Ft. Meade, MD 20755-6000 JJMoskowitz@dockmaster	301-859-4465
Lt Col	George R.	Mundy	DCA	Code B602 Washington, D.C. 20305-2000 Mundy@beast.ddn.mil	703-285-5481

Title	FirstName	LastName	Organization	Address	Phone
Mr.	Mike	**Muuss**	US. Army Ballistic Research Lab	Leader, Advanced Computer Systems Team APG, MD 21005-5066 Mike@brl.mil	301-278-6678
Mr.	Eugene	Myers	NCSC Attn: C311 Secure Architectures	9800 Savage Road Ft. Meade, MD 20755-6000 EDMyers@dockmaster.arpa	301-859-4488
Mr.	Gordon R.	Parry	CIA	Washington, D.C. 20505	703-482-6204
Mr.	George	Prettyman	Asst. General Counsel	9800 Savage Road Ft. Meade. MD 20755-6000	301-688-6017
Ms.	Harriet	Roberts	NCSC Attn: C34	9800 Savage Road Ft. Meade. MD 20755-6000	301-859-4486
Mr.	Jon	Rochlis	MIT E40-311	1 Amherst St. Cambridge, MA 02139 Jon@athena.mit.edu	617-253-4222
Mr.	Shawn	Rovansek	NCSC Attn: C12	9800 Savage Road Ft. Meade, MD 20755-6000 **Rovansek@dockmaster.arpa**	301-859-4458
Mr.	Kenneth	Rowe	NCSC Attn: C333	9800 Savage Road Ft. Meade, MD 20755-6000 Rowe@tycho.arpa	301-859-4491
Dr.	William	Scherlis	DARPA	1400 Wilson Blvd. Arlington, VA 22209 Scherlis@vax.darDa.mil	202-694-5800
LTC	James	Sells	NCSC Attn: C33	9800 Savage Road Ft. Meade, MD 20755-6000 JSells@dockmaster.arpa	301-859-4494
Cpt	Richard	Severson	NCSC Attn: C333	9800 Savage Road Ft. Meade, MD 20755-6000 Severson@dockmaster. arpa	301-859-4491
Mr.	Philip L	Sibert	DOE	MA-24 F-315GTN Washington, D.C. 20545	301-353-3307

Title	FirstName	LastName	Organization	Address	Phone
SSA	Karen E.	Spangenberg	FBI-HQ	10th & Pennsylvania NW Washinston, D.C. 20535	202-325-5594
Mr.	K. H.	Speieriman	NSA Senior Scientist	9800 Savage Road Ft. Meade. MD 20755-6000	301-688-6434
Dr.	Stephen L.	Squires	DARPA	Information Science and Technology Office Director, Strategic Computing 1400 Wilson Blvd. Arlington, VA 22209 Squires@vax.darpa.mil	202-694-5800
Capt	Michael	St. Johns	DCA	DCA Code 6612 Washington, D.C. 20305-2000 StJohns@beast.ddn.mil	703-285-5133
Dr.	Howard	Stainer	NCSC Attn: C32	9800 Savage Road Ft. Meade. MD 20755-6000	301-859-4491
Dr.	Dennis D.	Steinauer	National Inst. of Standards and Tech.	A-2 16 Technology Gaithersburg, MD 20899 Steinauer@ecf.icst.nbs.gov	301-975-3357
Mr.	Jim	Steinmeier	NCSC Attn: C2	9800 Savage Road Ft. Meade, MD 20755-6000	301-859-4467
Mr.	Cliff	Stoll	Harvard-Smithsonian Center for Astrophysics	60 Garden Street M.S. 6 Cambridge, MA 02138 Cliff@cfa200.harvard.edu	
Mr.	Jeff	Sweet	Attn: X21	9800 Savage Road Ft. Meade, MD 20755-6000	301-688-5724
Maj	Hugh **H.**	**Thomas**	NCSC Attn: C25	9800 Savage Road Ft. Meade, MD 20755-6000 Thomas@dockmaster.arpa	301-859-4474
Mr.	Mario	Tinto	NCSC Attn: C1	9800 Savage Road Ft. Meade, MD 20755-6000 Tinto@dockmaster.arpa	301-859-4450

Title	FirstName	LastName	Organization	Address	Phone
CDR	David	Vaurio	NCSC Attn: C3	9800 Savage Road Ft. Meade, MD 20755-6000	301-859-4485
Mr.	Wayne J.	Weingaertner	NCSC Attn : C31 Secure Computer Systems	9800 Savage Road Ft. Meade, MD 20755-6000 WWeingaertner@ dockmaster.arpa	301-859-4488
Mr.	Howard	Weiss	NCSC Attn: C32	9800 Savage Road Ft. Meade, MD 20755-6000 HWeiss@dockmaster.arpa	301-859-4491
Lt Col	Larry E.	Wheeler	OSD (C3I)	Pentagon-Room 3E187 Washinaton. D.C. 20301	202-695-7181
Mr.	Mark	**Woodcock**	NCSC Attn: C331	9800 Savage Road Ft. Meade, MD 20755-6000 Woodcock@tycho.arpa	301-859-4494
Mr.	Tom	Zmudzinski	DCA	Code 8602 McLean Washington, D.C. 20305-2000 TomZ@ddn1.arpa	703-285-5206