REPORT OF COMPUTER VIRUS INCIDENT AT AMES NOVEMBER 2-5, 1988

REPORT BY

D. FISHER, H. FINGER, W. KRAMER, J. STANLEY

EXECUTIVE SUMMARY

On Wednesday, Nov. 2, a network borne Virus was detected in computer systems at Ames Research Center. This report describes the activities at the Center that followed detection including verifying and understanding the Virus, eradication efforts, and installation of protective code to prevent reinfection of Center systems by the virus in the future.

Ames systems were disconnected from the INTERNET at approximately 1 a.m. November 3, 1988. Fixes to the system code were installed in approximately 150 affected minicomputer and workstation systems and after functional testing was completed, the systems were reconnected to the INTERNET at approximately 3 p.m. on Sunday November 5, and normal computer operations resumed.

Primary loss from this event was lost time of the technical staff to deal with the consequences of the invading Virus. No loss of data or software programs was experienced. Overall estimate of lost time at Ames for this event totals $72,500

INTRODUCTION

After experiencing disruptions to Ames computer systems caused by a network borne Virus, and after successfully installing protections against the Virus during the period of Nov. 2 to Nov. 5, a review team was convened by Ames Computer Security Official, David Fisher, to review the Ames' response to the incident, and to develop recommendations for improvements to Ames' future computer security posture. Review team members include in addition to David Fisher; Herb Finger, Chief, Communication Operations Branch, William Kramer, Chief, NAS Computational Services Branch, and Jack Stanley, Chief, Security Operations Office.

THE ENVIRONMENT

Ames Research Center, a field laboratory of the National Aeronautics and Space Administration (NASA), specializes in scientific research, exploration, and applications aimed toward creating new technology for the Nation. The Center's major program responsibilities are concentrated in: Computer Science and Applications, Computational and Experimental Aerodynamics, Flight Simulation, Flight Research, Rotorcraft and Powered Lift Technology, Aeronautical and Space Human Factors, Life Sciences, Space Sciences, Airborne Sciences and Applications, and Infrared Astronomy. To provide support for this broad spectrum of research activity, Ames has developed an advanced supercomputer complex hereafter referred to as the Central Computer Complex (CCF) having a highly flexible Local Area Network (LAN) to make the supercomputer resources directly available to the research scientist. In addition to the CCF, Ames is also the site of a national supercomputer facility, hereafter referred to as NAS (Numerical Aerodynamic Simulation) Facility. The Ames CCF serves the computational research requirements of Ames Research Center while the NAS serves the computational research requirements of a national consistency, which also includes Ames Research Center. These two facilities serve their user base through communication networks that provide required communications between the user's engineering workstations and the supercomputers. Both the minicomputer processors that provide the network functions and the engineering workstations themselves were the target of this Virus. The CCF and NAS networks are in turn connected to a large international consortium of interconnected networks called the INTERNET and this was the distribution vehicle for this Virus.

One of the functions of the INTERNET is to provide an electronic messaging capability between the connected systems. One software implementation of this message capability called "sendmail" (a UNIX based function) was exploited by this worm/virus (hereafter referred to as Virus in this report) as a pathway for attacking a large number of systems. Other UNIX functions were also exploited by the Virus, namely features referred to as "finger" and "remote shell". A detailed technical explanation of the Virus and its attack mechanisms is included in Appendix 1.-NAS WORM/VIRUS ATTACK INCIDENT REPORT. (NOTE: Viruses and worms do not as yet have precise definitions in computer science, but this Virus does not exactly fit most commonly held definitions of either a worm or a virus. It is virus-like in that it replicates over the network and infects a given system multiple times, however unlike typical viruses it does not modify or destroy system programs or data. It is also worm-like in that it looks through data files to find new user names and addresses in order to propagate itself to other systems.) The INTERNET Sendmail feature utilizes the TCP/IP protocol as implemented in Berkeley UNIX 4.3. TCP/IP was first developed at Berkeley as part of the Berkeley distribution of UNIX, and in particular allows interface to networks utilizing TCP/IP protocol such as ARPANET/MILNET, INTERNET and others. A number of system manufacturers have selected the Berkeley UNIX implementation as a basis for their operating systems, in part to take advantage of the Berkeley UNIX TCP/IP network capabilities (e.g.,DEC and SUN) Weaknesses in the implementation of Berkeley UNIX were exploited by this Virus.

FIGURE 1. gives an overview of some of the participants in INTERNET, showing the network environment in which the Virus was launched to infect network connected systems. Although not shown in this diagram, it is important to note that at each INTERNET node, and at Ames in particular, large local area networks exist that connect most local computer resources together. An attack launched over the network therefore has the potential of involving a very large number of systems. Systems on the network, and particularly Ames' systems are provided with security protections against unauthorized access, however, this Virus exploited obscure paths/bugs to circumvent these protections.

(NOTE: detailed technical descriptions of the Virus and its method of attack as well as technical details of eradication activities are included in Appendices 1 and 2 of this report)

INCIDENT DESCRIPTION

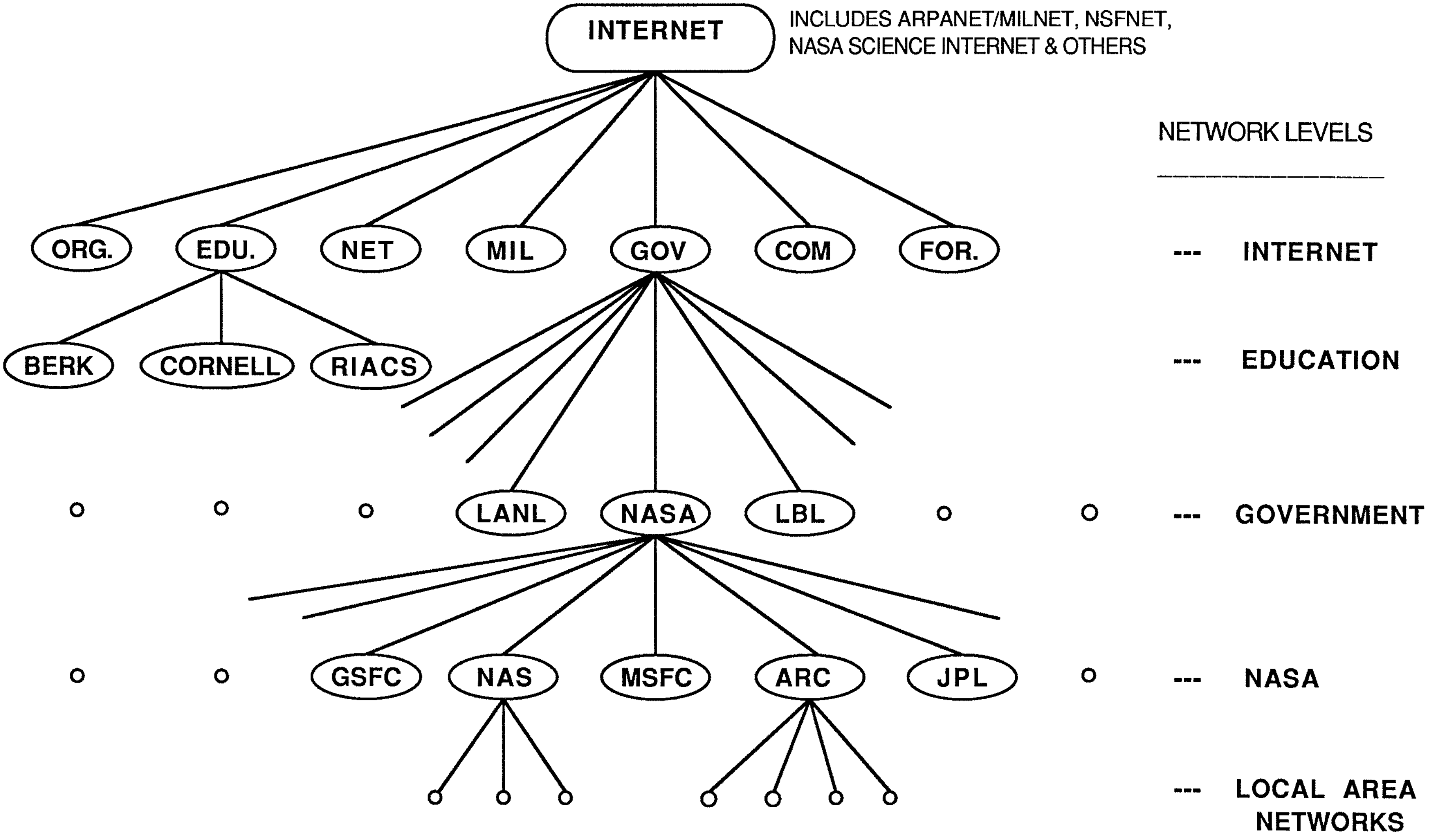
On November 2, 1988, at approximately 9:00 p.m., personnel at Ames Research Center in contact with University Of California at Berkeley (UCB) became aware that a computer virus had affected a number of INTERNET connected systems at both locations. Detailed reports of the sequence of events areincluded in the appendices to this report.

The first evidence that a computer virus was present was the detection by alert operations and development personnel of an overload condition of some of the systems at a

FIGURE 1

INTERNET PARTICIPANTS

(PARTIAL LISTING)



time when system loading would be expected to be quite light. No corruption of system software or loss of data was noted, and later analysis bore out this initial finding. This phenomenon was detected at UCB and at the NAS Facility and was shortly thereafter confirmed to involve systems in the CCF. All three sites, while remaining in close communication, proceeded to take immediate steps to understand the attacking virus, devise a protection mechanism, and provide warning and protection for other nodes and computers on the network. Dedicated personnel worked throughout the night and the next day to accomplish these protection goals. By approximately 11:00 p.m. on Nov. 2, UCB in collaboration with Ames had developed a good understanding of the Virus. This information pointed to the INTERNET "Sendmail" feature as a mode of transmittal for the Virus, and therefore systems at Ames as well as those of JPL, Goddard and Marshall were disconnected (with management approval) from the INTERNET by 1 a.m. on Nov. 3. This quick action prevented the Virus from reaching JPL and limited the impact at other NASA sites. In addition to the disconnect action, UCB provided a set of software fixes that were designed to prevent a system from being reinfected by the Virus, and early on Nov. 3, a management directed and coordinated approach for protecting all systems and for reconnecting to the network was initiated. The approach selected was a conservative one directed at providing high levels of system protection and integrity before reconnecting to the network where the Virus would undoubtedly still exist. The strategic approach for reconnection to the network was a three step process:

1. Put software fixes in all vulnerable systems to prevent infection by the Virus,
2. Create a test environment where a "system with fixes installed" successfully withstands repeated attacks by the Virus as a demonstration of the the effectiveness of the fixes.
3. Reconnect protected systems onto INTERNET while carefully monitoring system integrity.

Task teams were formed within the NAS and the Ames Information and Communications Systems Division to accomplish the above in the shortest possible time. Regular status meetings were held and communication between the two task teams was maintained. By Sunday, November 5, at approximately 2 p.m. Ames' systems were reconnected to INTERNET, and normal operations resumed. DEC minicomputers and Sun workstations running UNIX 4.3 BSD were the systems primarily affected by this Virus at Ames (numbering approximately 150 systems). These systems are utilized for network operations, job preparation, job submittal, results analysis and display and other user directed activities. To the extent that researchers at Ames were dependent on network access to other sites, their work was impacted by disconnecting all Ames systems from the INTERNET. The virus was eradicated from most systems at Ames by Nov. 3, and they became available for operation in a stand-alone mode (still disconnected from INTERNET) and in many cases near normal operations resumed. Other UNIX systems were impacted in a minor way as the Virus attempted to infect them also, but only DEC and Sun systems replicated the virus on a large scale.

OPERATIONAL IMPACT OF VIRUS

Shortly after the Virus was detected on Nov. 2 all connections to the INTERNET were severed at Ames. The local area networks at Ames (Ethernet and DECNET) were not impacted by this Virus and remained fully operational at all times. These local networks were used by Ames researchers to continue local processing and job submittal to the CCF Supercomputers. Researchers who utilized INTERNET to communicate with other sites to accomplish their work were of course affected during the INTERNET disconnect which lasted from 1 a.m. on Nov. 3 until 2 p.m. on Nov. 5. CCF processing remained at normal levels, since the normal access paths used for the CCF were not disrupted. The remote users of NAS were impacted in that they were unable to communicate with the NAS supercomputers during the period of outage of the network. The supercomputers at Ames, both at the Central Computer Facility and at NAS were not directly impacted by the Virus, and near-normal batch workload processing continued on these systems, however, interactive supercomputing services were curtailed during this period for remote users of NAS. Two major system acceptance tests were underway at NAS and these continued without interruption.

COST IMPACT OF THE VIRUS

Since no data or information was lost due to this Virus incident, the cost impact is primarily in the area of lost time of technical staff in dealing with Virus detection, eradication and prevention activities. Supercomputers and mainframes continued to operate. The minicomputers and workstations that were affected required some out-of-service time to install Virus prevention code, however, following this minimal outage the systems became available for stand-alone use. Since in most cases system workload was scheduled around these interruptions, the costs of unscheduled system downtime were assumed to be small and therefore no estimate of the value of these losses was attempted. Therefore, the cost impact experienced at Ames as a result of this Virus incident was primarily in the area of lost labor hours estimated to be approximately 1160 hours at an estimated cost of $72,500.

RECOMMENDATIONS

The following recommendations are proposed by the Virus incident review team as a means of not only preventing reoccurrence of this Virus in Ames systems, but as a means of improving the overall Ames computer security environment so as to reduce the probability of sustaining severe damage from future virus incidents. Implementation of these recommendations is expected to be the responsibility of the individual organizations having computer management responsibility, however, it is recommended that the Ames Computer Security Official provide coordination and integration oversight where activities span organizational boundaries.

1. Complete installation of fixes for this Virus on all network connected systems at Ames. (NOTE: this action is substantially complete). Insure that systems subsequently acquired for use at Ames have installed fixes for this Virus as appropriate.

2. Acquire or develop new fixes for this Virus that reduce the functional loss of system features experienced as a result of the current quick fix.

3. Form a standing computer security incident response management team to provide for management coordination of all activities associated with computer security incidents, such as virus attacks, break-ins etc.

4. Ensure that fixes to all known bugs that compromise system security are installed in a timely fashion on all vulnerable systems.

5. Develop minimum standards for passwords on all network connected systems at Ames. These standards should address password size and content as well as system enforcement policies.

6. Provide for Center-wide network configuration management so that an overall minimum security profile is maintained for network attached systems.

7. Improve overall Center computer security status by timely development of risk assessments, contingency planning and emergency backup procedures for all sensitive systems as defined and required in the Computer Security Act of 1987.

8. Provide funding and qualified technical personnel at the system management level to implement and maintain computer security protections.

9. Require that system program source code be provided with all future systems acquired at ARC (to the greatest extent possible). Lack of system source code complicates the ability to rapidly devise and apply system fixes.

10. Advocate the establishment of a national control center for the INTERNET to act as a coordination clearinghouse for information and activities related to network problems and incidents.

Report prepared and submitted by:

David Fisher

David Fisher, Ames Computer Security Official

11/30/88
Date

Herb Finger

Herb Finger, Chief, Communications Operations Branch

11/30/88
Date

WTKramer

William Kramer, Chief, NAS Computational
Services Branch

11|30|88
Date

Jack D Stanley

Jack Stanley, Chief, Security Operations Office

11-30-88
Date

NAS VIRUS TABLE OF CONTENTS

APPENDICES

NUMERICAL AERODYNAMIC SIMULATION

21 November 1988

To: David Fisher, Ames Computer Security Officer

CC: F. Ron Bailey, Ron Deiss, Bruce Blaylock, Tom Lasinski
Bill Wall

From: William T.C. Kramer, Chief, Computational Service Branch (RNS)

Subject: Report of Computer Virus Incident 11/2/88 to 11/7/88

Attached is a report, prepared by Captain William Wall on the recent computer virus incident at NAS. The report chronicles the incident from when it was first detected until NAS was completely back on-line, essentially from 9 pm on November 2 until 1 pm on November 7, 1988. Along with the report, it is necessary to provide some introduction to the Numerical Aerodynamical Simulation (NAS) System. I would also like to make several conclusions about the report.

Introduction

NAS is designed to fulfill the following key goals:

> Provide a national computational capability available to NASA, DoD, Industry, other Government agencies and universities, as a necessary element in ensuring continuing leadership in Computational Fluid Dynamics and related Disciplines
>
> Act as a pathfinder in advanced, large scale computer system capability through systematic incorporation of state-of-the-art improvements in computer hardware and software technologies
>
> Provide a strong research tool for the NASA office of Aeronautic and Space Technology

At the time the virus struck, NAS supported 26 long distance connections at speeds up to 1.5 Megabits per second. This network is called NASnet. In addition, NAS is connected to national and regional networks, including NSFnet (National Science Foundation network), the ARPAnet, MILnet, BARRnet (Bay Area Regional Research network), and the NASA Science internet. In addition, NAS supports dial-in/dial-back access through a micom switch and is connected to the rest of the machines at Ames Research Center through ARClan. These networks allow access for our user community since more than 70% of the supercomputer CPU cycles are used by people who are not physically at Ames.

NAS consisted of 99 major systems, including two Cray-2 supercomputers, the first Cray YMP supercomputer shipped to a customer, and an ETA-10Q system. The two Cray-2s run 24 hours a day, 7 days a week in production operation and have a significant backlog of jobs. The YMP and ETA systems were involved in sensitive acceptance tests during the virus time period. The NAS Processing System Network (NPSN) consists of both ethernet and HYPERchannel hardware. Connected to the network along with the Cray supercomputers and the ETA are the more than 90 systems ranging from Sun workstations to Amdahl 5880. There are 35 Iris workstations, which are the prime tool the local scientists use in conjunction with the Crays, for their work. In addition to the range and uniqueness of the hardware environment, NAS is constantly trying new and untested software technology. NAS typically has three or four beta test projects going on at a time, ranging from new operating systems to new hardware. This work requires flexibility and a constantly changing environment, which at times means sacrificing stability, documentation and other aspects which are valued in more traditional centers.

The combination of the three NAS goals led to a design requiring a single operating system across all user accessible hardware. The only viable candidate at the time of system implementation (and even today) was UNIX^{TM}. The Darpa protocol suite, including TCP/IP, was selected as the primary (and almost exclusive) network protocol due to the connectivity and functionality it provides. This design has allowed significant developments at NAS both for our immediate scientific community and for the supercomputer community as a whole. Some examples of these developments are distributed graphics (PLOT3D, RIP, DPLANE), the Network Queuing System (NQS), distributed system administration tools, and a non-system specific Mass Storage System. Without the flexibility and openness of the network protocol and a single user interface, these would have been much more difficult if not impossible.

It is also necessary to mention that the NAS user community is used to and very much advocates an open environment, much like a typical university. There is much to be gained from the easy exchange of information between peers, and many of our scientists regularly exchange information. No less important is the continued desire to minimize the amount of computer expertise a scientist requires to use the various computers so they can concentrate on the scientific field. The basic tenet of one operating system means the user only need learn one basic set of commands. Other tools and functions which allow ease of use are generally pursued at NAS as well.

Conclusions

The virus impacted the NAS in four ways. First, significant resources were used to diagnose, combat and recover from the virus. These resources consisted primarily of on site contractor and government support personnel. Second, there was disruption of service to our users since full connectivity was disabled for 74 to 98 hours depending on their site. Thirdly, there was the cost of the CPU time and other resources used by the virus that would have been used by useful work otherwise. Lastly, there is the cost in additional security and administrative measures that will be put into place, in part, due to this virus.

Since the prime motivation during the period of diagnosing and fixing the virus was to protect our supercomputers, ensure an uninterrupted acceptance test, and to allow the supercomputers to process with little interruption, we were cautious in our approach. During the time of the virus attack, diagnosis and correction, the acceptance tests were unaffected and there is no evidence the machines in acceptance were even attacked. The two production supercomputers continued to process during the entire time. While the long haul networks were disabled, both Cray-2 systems had sufficient backlog of batch jobs to remain fully utilized. This remained the case even when the internal network was disconnected while the patches to prevent reinfection were being installed. Since the systems were not reachable, system development personnel were able to accomplish much of their backlog of work using stand alone time. This represented several weeks of work under normal conditions.

The machines most affected by the virus were Vaxes and Sun workstations. The Vaxes are used as general support processors for scientists and support staff to do editing, text processing, system administration, and to support remote access. However, they are not critical to accomplishing the scientific work at NAS since most scientific users work with their workstations and the supercomputers. Likewise, the Sun workstations are used for system support primarily by system administration staff. There were two Sun workstations affected which serve as file servers to the scientific workstations, and did have some impact on the scientist's ability to do work, but these were quickly brought into service.

Lastly, NAS started to reconnect the long haul sites on Sunday November 6. When disconnected, NAS personnel told these sites they would not reconnect unless the site also agreed. Since many sites did not have personnel available on Sunday, many connections waited until Monday - delaying return to full service until early Monday afternoon.

As was stated in the report, no permanent damage has been detected. No files were lost nor files damaged and no hardware was disrupted. As the virus was diagnosed and decoded it became apparent that no "trojan horses" or other latent affects were possible. The only possible impact is the decoding of passwords, which is being addressed in several ways.

It is believed, by most of the people at NAS, that the act of releasing this virus was intentional and malicious. It apparently was an attempt to acquire passwords to which the originator had no legitimate claim. The purpose of this attack is open to speculation, but the fact that the program attempted multiple methods of attack, used sophisticated programming and operating system knowledge, and attempted to relay information back to a collection point not associated with the suspected origin of the attack indicates it was well thought out and intentional.

The losses to NAS are significant in the disruption of service and the impact on staff resources.

The actual CPU time used by the virus as it attempted to replicate is also significant, but primarily on systems that play a secondary role. Captain Wall's report lists suggestions, many already being implemented, for providing increased security.

William T.C. Kramer
Chief, Computational Services Branch, RNS

NAS WORM/VIRUS ATTACK INCIDENT REPORT

Captain William D. Wall, USAF
NAS Computer Security Officer

INCIDENT DESCRIPTION

On November 2, 1988 shortly after 21:45, one of our development staff, Eugene Miya, noticed that the load average was high on one of the DEC VAXes at the Numerical Aerodynamic Simulation (NAS) Facility at NASA/Ames Research Center in Mountain View, California. He told the VAX manager and network support manager for the NAS Systems Development Branch (RND), John Lekashman, who diagnosed the problem on Orville (VAX 11/780) within the sendmail program and the finger daemon (fingerd). At 23:05 John notified the control room to disable sendmail on the systems and kill all processes associated with the virus. The high load average was caused by the virus as it searched for other internet devices to attack.

At 23:45 the Branch Chief for the Computational Services Branch (RNS), Bill Kramer, was notified and informed of the problem by the Operations shift supervisor, Toby Harness. Steps were being taken to disable sendmail. All file systems were still intact, but the NAS VAXes were still "under attack."

On November 3 at approximately 00:45 Kramer and Lekashman decided to disconnect NAS from the rest of Ames Research Center and all other outside nets. By this time, John Lekashman had a much better understanding of the program and discovered modes of attack other than sendmail. The virus was using the finger daemon and some password cracking attempts were being made. Milo Medin, a Sterling employee on contract to the Network Development Branch (EDN), was disabling all ARCLAN connections in Building N254.

At 02:45 the University of California at Berkeley developed and distributed an initial fix to either recompile or patch sendmail to disallow the debug option.

At 02:45 all vitalink connections at NAS were disconnected by John Lekashman. At 03:05 all other external internet connections (ARPAnet, NSFnet, ARCLAN, MILnet, and HYPERchannels) were disconnected by Milo Medin.

At 03:20 the workstation lead analyst, Michele Crabb, was informed of the problem and called in to assist stopping the virus on the Sun file servers. The virus had spread from the VAXes to the Sun workstations.

At 04:00 sendmail on all NAS machines were killed and commented out of the startup rc files (/etc/rc, rc.local, netstart, local.rc). Fingerd was commented out in /etc/inet.conf since it was another suspected point of contact.

At 07:00 all NAS network sites were called and informed of the problem. Ron Bailey and Ron Deiss were also informed of the problem.

At 08:30 the NAS Computer Security Officer, Capt. Bill Wall, and Workstation Subsystem Manager, Bob Van Cleef were briefed of the situation. A set of tasks was prepared for lead system analysts and subsystem managers to isolate NAS and install the fixes. All subsystems were checked for infection.

At 09:42 Snoopy (Micro Vax) and Gottfried (VAX 8350) were checked and shown not to be infected. However, their sendmail was killed. The affected machines were Amelia, Wilbur, Fred, Orville, Sun 200-207, Sun 209, and Sun 108.

At 10:00 the Acting Director for Aerophysics, Ron Bailey, was briefed of the problem. It became obvious that this was a national incident. At this time, Milo and John recommended two fixes: recompile sendmail without the debugging option and rename the .rhosts files. Questions from the press or outside sources were referred to Ron Bailey.

At 10:13 Bendix had powered down the dial-back system.

At 10:50 a VAX (Orville) had its sendmail recompiled with debug off and tested okay (done by Lekashman and Keith Thompson). The patch was given to other subsystem managers. The lead system analysts were responsible for the patch. The following is a list of each subsystem and lead system analyst:

VAX 11/780s (Amelia, Orville, Fred, Wilbur)	Rich Mahn
Amdahl 5880 UTS machines (Prandtl, Meyer)	Don Seal
Workstations (Suns, Irises, Engineering wks)	Michele Crabb
Cray-2 Supercomputers (Navier, Stokes)	John Musch
Snoopy (Ultrix)	Steve Storm
ETA-10Q (Piper) and Cray Y-MP	Marty Fouts
Connection Machine and Gottfried	Creon Levit
Convex and Alliant Super Mini Computer	Ken Broll
Stellar Workstation	Jeff Hultquist

We have source files for the Vaxes but not for all the Suns which prevented the virus from spreading. A binary fix was made to the Suns. The virus affected 4 Vaxes and 10 Sun workstations. The problem existed on other machines at NASA/Ames (reported by Milo Medin).

At 11:00, Bill Kramer convened the first of a series of status meetings to discuss the problem and recommend the fixes to some of the technical staff. At this time, all external networks were disabled and assignments were given to implement the fixes on the various machines. The Long Haul group were to talk to their technical contacts at offsite locations. Any questions from the press or outside contacts would be referred to Ron Bailey, Acting Director for Aerophysics. The root passwords for all machines were to be changed. All lead analysts would check their machines and validate any fix.

Lead analysts were asked to look for strange files and strange binaries in /usr/tmp as an indication of attempted infection.

Ron Deiss, acting Division Chief, stated that the primary objective was to get NAS back in service when the system is at an acceptable level of security. Lead analysts would audit their software and compare present software with files from several days ago.

The remote sites contacted included Amtec, Boeing, Center for Turbulence Research, Flow Research, General Dynamics, Grumman, Goddard, Johnson Space Center, Langley Research Center, Lewis Research Center, Lockheed, McDonnell Douglas, Marshall Spaceflight Center, Northrop, Redstone Arsenal, Rocketdyne, Rockwell, United Technologies, Vertol, Computational Mechanics, SAIC, Marquardt, and Allison Gas Turbine.

A Message of the Day (MOTD) went out to all computers stating the following: "An emergency security situation affecting many sites nation-wide has required the disabling of all NAS external communication links, inter-system mail, and some local networks. Resolution of this situation is being given the highest priority. All logins to other systems should be done with telnet. All .rhosts files have been renamed. Please do not replace your .rhosts files until further notice."

At 15:00 another status meeting was held. Sendmail was fixed on all machines and .rhosts were disabled. NAS had contacted 19 of the 26 Long Haul sites. All the VAXes, Prandtl (Amdahl machine), the Cray-2s and the Stellar had the fix installed and validated. There were reported indications of the virus on some IRISes and the engineering workstations. RIACS reported that their computers were under attack at 19:10 on 2 November, the earliest for any NASA/Ames site. It was also decided to disconnect from the Micom switch as well.

The following steps were to be taken by NAS:

1) NAS would disconnect from the external world;

2) the lead analyst would patch and check their machine;

3) analysts would verify their machines clean after patching;

4) each machine would be verified by a second person after patching;

5) internal re-connection would be made with uneffected machines;

6) internal traffic would be monitored with the virus let loose to see if it would re-infect any of the machines;

7) NAS machines would be re-connected to the outside world.

At 16:15 all inet daemons had been removed on the VAXes. At 17:00 the 150 and 190 Micom switches were disconnected to NAS. All interconnectivity between systems were down.

On November 4 at 11:00 another status meeting was held. The FBI was informed and a special agent, inspector Jim Montee, showed up along with the Ames Security Officer, Jack Stanley, and Ames Cognizant Computer Security Officer, Dave Fisher, and briefed. The status of all machines were reviewed with the sendmail fix and the finger daemon disabled. Questions from the press or outside sources were referred to the Public Affairs office.

NAS had contacted 21 of the 22 Long Haul remote sites and sent the fixes in sendmail to each site by fax. Keith Thompson had done some reverse engineering on the code and discovered it opened to a port at U.C. Berkeley. The location of the virus was being sent back to Ernie, a system for UCB computer science graduate students.

The FBI wanted to know if a trap could be set up and how much damage this virus was causing in time and money. Ron Deiss said he could provide a cost estimate. The FBI also wanted to know if malicious damage had been done. No files were altered or deleted, so no damage was done to the system except lost CPU time.

At 13:30 the Cray Y-MP and Wilbur were put on their own HYPERchannel network while work on the virus problem continued. This ensured the acceptance tests of the ETA and Y-MP were not disrupted. MVS dedicated time was cancelled due to the virus problem.

Another status meeting was held at 15:00. NASA Headquarters was very concerned about the NAS computers. The virus did not affect the acceptance test period of the Cray Y-MP nor the ETA-10Q. These systems did not have sendmail invoked. The systems were checked and were clean. Marty Fouts had a backup from before the start and verified the correctness of files on the Cray Y-MP and ETA-10.

A fix to the finger daemon problem was found and would be distributed to the operations room for all system analysts.

It was decided to use a test Sun workstation machine (Bamboo) to test the patches and see if it would become re-infected when the virus was introduced into it. If it was protected, one long haul site would be connected to it to see if the remote network was clean.

By 16:00 copies of the virus fix for the fingerd had been distributed to all lead system analysts. They were to install the fix and test it. Once their system was "virus" proofed, they could connect their networks back and inform the control room. External networks, however, would stay down.

At 17:00 all root passwords on all computer systems were changed.

On November 5 at 10:36 the VAXes were inoculated and passed the verification tests. At 12:37 the Mass Storage Subsystem (MSS) was up without inetd, fingerd, or sendmail.

At 14:00 the ethernet to building N202A was re-connected.

At 14:30 a workstation (Han) was used as a guinea pig and connected to the Long Haul sites to see if it would be infected after being inoculated with the fix. Everything seemed fine. The internet switch and dial-back system were brought back to service.

At 16:40 NAS set loose the virus on the network to test the inoculation. The virus infected the Sun in building N254. The link to N254 was then brought up. All systems were monitored for re-infection.

On November 6 at 12:25 there was no evidence of virus problems. Most remote sites were notified of the virus fix and NAS sent a copy of the patch via fax machine. It took about 24 hours for all remote sites to be contacted and verified that their machines were clean or had the virus fix.

At 13:20 the local networks at NASA/Ames were re-connected. All of the NAS machines had been disconnected from the rest of the world for 74 hours. At 13:30 the wide area networks and ARCLAN were started.

On November 7 at 12:30 all connections were back in place with full access to all our systems.

On November 8 the Computer Security Working Group met to discuss the virus and make recommendations. These recommendations would be taken to the Management Interface Group (MIG) for approval. Issues such as password aging, having source code for all systems, developing an emergency response team, developing security benchmarks, and changing the password algorithms were all discussed.

HOW THE VIRUS WORKS

There are several ways this virus can transmit itself from one machine to another:

1) use sendmail (via the "debug" command);

2) use finger (via a bug in /etc/fingerd);

3) use rsh (remote shell) to create itself on the remote machine through trusted accounts (due to .rhosts or hosts.equiv files);

SENDMAIL ATTACK

The virus uses the debug option in sendmail as one of the first attempts to gain entry. From a distant host, a message is sent to sendmail (i.e., telnet target.machine 25). The virus running on an infected machine opens a TCP connection to another machine's sendmail (the SMTP port), invokes the debug mode, and sends a RCPT TO that requests its data be piped through a shell.

A binary program then searches for Internet addresses to attack. It builds and compiles a program to see if a remote machine would respond. The program then tries to load and execute them by running a /bin/sh shell on the remote machine. The shell script creates a temporary file in the world-writable /usr/tmp directory named x$$,l1.c (where the $$ gets replaced by the current process id) and copies code for a "listener" and "helper" program. This is a 40-line C program. The shell compiles this helper program using the "cc" command local to the system. The helper is invoked with arguments pointing back at the infecting virus, giving hostid/socket/password as arguments.

The compiled C program sucks over two object files, x$$,vax.o and x$$,sun3.o from the attacking host. It has an array for 20 file names (for 20 different machines), but only two (vax and sun) were compiled into this code. It then figures out whether it is running BSD or Sun OS and links the appropriate file against the C library to produce an executable program called /usr/tmp/sh.

FINGERD ATTACK

The virus knows how to penetrate systems via a bug in "fingerd," the finger daemon. This method is where most of the sucess was in penetrating the VAXes

On the Sun workstations the attempt results in a core dump. Fingerd is a remote user information server that provides an interface to the "name" and "finger" programs. It listens for TCP requests. The bug allows a different program other than finger to be run. When fingerd is connected, it reads its arguments from a pipe, but does not limit how much it reads. If it reads more than what the 512-byte buffer allows, it writes past the end of its stack. After the stack is a command to be executed (/usr/ucb/finger). The virus replaces the finger command with the /bin/sh command. This command creates a bourne shell which is started with no arguments. Since this is run in the context of the finger daemon, standard inputs and outputs (stdin and stdout) are connected to the network socket. This sucks over all the files just like the shell that sendmail provided.

RSH ATTACK

Another way the virus tried to get into systems was via the .rhosts and /etc/hosts.equiv files. The program collects information from the /etc/hosts files, the etc/hosts.equiv file, and other files containing host names and host IP addresses to determine trusted hosts. It then repeats the attempt to connect to these sites. The virus uses individual .rhosts files (which it found using the password file) and any other remote hosts it could locate which it had a chance of connecting to.

The virus was running as daemon, not as root. So, to use the their idividual accounts. To do this, it went through the /etc/passwd files, trying to guess passwords. The virus uses a combination of usernames (last, first, last + first, and nicknames).

The virus also contains a set of over 400 built-in words, contents of /usr/dict, and words from system files to crack user passwords. It uses the initial account that it acquired and any others whose passwords it decoded to gain entry to other systems through the use of trusted hosts. A trusted host is one whose name is contained in the system file "hosts.equiv" or a user file ".rhosts." Once a trusted host is set up, the remote host does not require a password for a connection. Since this trust is generally symmetrical, the virus reasonably assumes the systems trusted by the infected system will also trust the infected systems.

The virus uses a brute force attempt at discovering easy passwords. The spawned processes attack the encrypted password file to enable ftps in case the .rhosts attack would not work. If the program succeeds in breaking a local password, it looks for a .rhosts file and does an 'rsh' and/or 'rexec' to another host. It then sucks over the necessary files into /usr/tmp, forks a child process to use telnet to break into that account and copy itself, and runs /usr/tmp/sh to start over again.

If the virus does not break into any accounts or systems for awhile, it enters a mode where it tries to break the root password via brute force searching.

The virus program is designed to replicate itself on other machines. When the virus successfully connects to one host, it forks a child to continue the infection while the parent keeps on trying new hosts. The virus forks repeats copies of itself as it tries to spread itself. This uses up all the CPU on a machine in the process. The load averages on infected machines skyrocket. Some machines can run out of swap space and kernel table entries, preventing login to even see what is going on. This was the major tipoff that the machines were under attack.

Except for the helper source file, the program does not copy around source files. It copies around pre-compiled binaries that are linked on the local machine and then run. These binaries are for VAX 7xx and 8800 machines as well as 68020-based Sun workstations.

The helper then connects to the "server" and copies a number of files to the /usr/tmp directory. After the files are copied, it executes a shell with standard input coming from the infecting virus program on the other end of the socket. The newly executed shell attempts to compile itself from the files copied over to the target machine. The virus has several "sleep" calls to slow itself down before collecting more user names and probing with "rsh."

The child requests and initializes a new socket, then builds and invokes a listener with a new socket number and hostid as arguments. Everytime the virus connects to the telnet port, it immediately closes the port. Messages such as "telnetd: ttloop: peer died" in /usr/adm/messages means the virus attempted an attack on that particular system.

The virus tries to clean up after itself so as to leave no evidence. For example, it called itself "sh" and destroyed its argument list to make it appear in the process table as some random shell script. When it starts up, the virus clobbers its argv array so a "ps" (process status) will not show its name. Files are copied into /tmp which is cleaned up after reboot. Other incriminating files are unlinked (deleted) by the virus itself so they can't be found (since it has them open, however, it can still access the contents). However, sendmail log files show mail coming in from user /dev/null for user /bin/sed (it uses the SED editor to strip off headers), which is a tipoff that the virus entered a system.

It also tries to disguise itself and its origins. A monitoring mechanism built into the program broadcasts the location of the virus back to a computer named Ernie at U.C. Berkeley. Each time the virus is started, there is a one in 15 chance that it sends a single byte to ernie.berkeley.edu on some magic port.

The virus had another signaling mechanism. It would signal a new computer to learn whether it had been invaded. If not, the program would copy itself into that computer. However, once every 7 times it sent the query signal it would copy itself into the new machine regardless of the answer. The choice of 1 in 7 was too frequent, allowing the program to echo back and forth through the network in minutes, copying and recopying itself thousands of times on each machine, eventually stalling the computers.

The virus uses the "netstat -r -n" command to get the local routing information for its use in figuring out what networks the machine is attached to.

This information is used to attempt to penetrate sendmail on those machines. It also uses the system call "ioctl" to get the list of network interfaces attached to the machine, the "netmask" of each interface and the names assigned to each interface. It uses the yellow pages (YP) in the Sun workstations to see what distributed hosts files are available.

The program appears to be able to directly install the regeneration part of itself on VAXes and Sun workstations. It executes large numbers of remote shell programs from VAXes and Suns to other machines, using up their CPU resource. The program appears to create and compile programs in /usr/tmp only.

THE VIRUS FIX AT NAS

The repair to version 5.59 of sendmail was to disallow execution of the debug command to be executed. This was done by commenting out or deleting "debug" in srvrsmtp.c or commenting out the #define DEBUG 1 in conf.h.

For the fingerd daemon, the library routine "gets" was replaced with "fgets" so that the stack could not be overwritten.

In addition, .rhosts files and /etc/hosts.equiv were made inactive.

For machines that did not have source code, kill off the mailer and make the fingerd program inaccessible were the main implementations. For the 3.5 Sun workstations a binary patch replaced the "debug" command with another "showq" command.

For the 4.0 Sun workstations, sendmail was temporarily disabled. The 4.3 BSD sendmail with source patches was then ported to these Suns. The Suns do not run fingerd.

For the IRIS workstations the source patch was made to the 3.6 version of the source tree. The source tree was then placed on a 3.5 machine to build a 3.5 version. Because the IRISes are not BSD based, the changes to the necessary module, rcmd.c, were not made in libc.a. The changes were made to libsun.a. There were two calls to "_invaliduser" added. The code for "_invaliduser" was also added at the end. With that library rebuilt, the daemons rexecd, rshd, and rlogind were rebuilt. The new versions were then copied to their appropriate places. The binary image of login was also rebuilt. The IRISes do not run fingerd.

SUMMARY OF SECURITY HOLES

The Unix 4.3 BSD version of sendmail has a debug option which exists if sendmail is compiled with "debug" enabled. It was distributed with this debug option enabled in the binary BSD distribution. By giving a specific option to the "debug" command in sendmail, you can cause it to execute a command. As sendmail runs setuid to root, the command also has root privileges. This option should not have been compiled into the program when it was built for installation in a production mode. Programs should not have debugging options that execute an arbitrary command.

The security bug in the Unix finger daemon permits its invoker to obtain a shell with super-user privileges. The C standard I/O library routine "gets" in fingerd with a buffer on the stack. It is then possible to send a long string of data to a program such that upon return from "gets" the next thing the program executes is "execl." A machine that executes in the data space can give an intruder full access. "Gets" is unable to check that the input line fits within the buffer, so a suitable-constructed line of input to the finger daemon steps on other variables.

Standard I/O contains an alternative to "gets", called "fgets," which takes three parameters: an input buffer, its size in bytes, and the stream to be read.

The offset needed to break the BSD fingerd was known, but the correct offset for the Sun's fingerd was not known. This caused the core dump in the Suns.

RECOMMENDATIONS FROM NAS SECURITY TEAM

(1) Compile sendmail with the debug option turned off or deleted.

(2) Do not run fingerd as root.

(3) Source code should be available for all production machines.

(4) Encourage all users to change their passwords.

(5) Examine all daemons for other potential loopholes.

(6) Develop an emergency response team and list of contacts to handle virus attacks in the future.

(7) All system source code should be backed up and stored off site.

(8) Develop a method for timely installations of security modifications.

(9) Periodically verify that security modifications are still in place.

(10) Change the current password algorithm with a pure DES.

(11) The .rhosts files should contain as few entries outside of NAS as practical.

(12) Develop security benchmarks for all software on NAS machines.

(13) Determine a clearinghouse for information (NIC or NASA/Ames - Code ED) and 24-hour trouble desk.

(14) Develop better configuration management tools for software (effective source control).

(15) Hire computer security specialist full time to look at potential computer security loopholes, implement fixes, and audit the system.

(16) Task a NAS employee to do computer security work such as audits, fixes Add a security checklist in the RFP for software vendors.

CONCLUSION

This virus attack was the largest assault ever on the nation's computers. The virus program was alleged to be the result of an experiment by 23-year-old Robert T. Morris, Jr., a Cornell University graduate student. The virus was planted in the Arpanet/Milnet computer network, which is used by NASA, DoD, universities, and many government agencies. A programming mistake caused the virus to multiply hundreds of times faster than had been planned.

Besides NASA/Ames, the virus hit such places as MIT, Harvard, Dartmouth, the Naval Research Laboratory in Maryland, University of Maryland, Lawrence Livermore, Stanford, SRI, University of California Berkeley and San Diego, Naval Ocean Systems Command (NOSC) in San Diego. The virus slowed over 6,000 computers throughout the nation by replicating itself and taking up memory space. It did not destroy any data that we know of.

This virus is not unique to the UNIX operating system. The bug is part of the mailer program, sendmail. It takes advantage of security holes that were deliberately left open to make debugging operations more convenient when dealing with other trusted machines.

This incident illustrates the vulnerability of computer network systems and the lack of adequate security measures. A similar attack that could cause more damage is always possible. This case is being pursued by federal authorities under the Computer Fraud and Abuse Act of 1986. This statute makes it a federal crime to penetrate a computer owned by or run on the behalf of the U.S. Government.

Much remains to be learned from this incident to better protect our computer systems in the future and establish a precedent of prosecution if this case ends up in court. Although no files or data was lost, a lot of valuable CPU time was lost at NAS in the 74 hours of disconnect time from remote users. A lot of hours was also invested by many people in understanding the nature of this virus and protecting the computer systems from attack. In addition, NAS was disconnected from its 900 researchers with over 300 projects at 100 universities, aerospace firms, laboratories, and other U.S. agencies.

ACKNOWLEDGEMENTS

Some of this report's information was obtained from the following people: Henry Alubowicz, Matt Bishop, Bruce Blaylock, Mike Bridges, Bohden Cmaylo, Michele Crabb, Jim Craw, Ron Deiss, Art Edmonds, Dave Fisher, Mary Fouts, Richard Fox, Jonathan Hahn, Toby Harness, Jordan Hays, Jeff Hultquist, Dan King, William Kramer, John Lekashman, Rich Mahn, Milo Medin, Eugene Miya, Tony Quintana, Julian Richards, Don Seal, Steve Storm, Keith Thompson, Dave Tweten, Robert Van Cleef, Gary Veum, and Howard Walter.

CHRONOLOGY OF WORM/VIRUS AT NAS

11/02	21:45	LEKASHMAN NOTICED HIGH LOAD AVERAGE (> 20) ON THE VAXES
11/02	23:06	LEKASHMAN CALLED OPERATIONS - SECURITY BREACH THROUGH MAILER
11/03	23:45	OPS CALLED KRAMER ABOUT VIRUS; KILL SENDMAIL, FINGERD
11/03	00:30	CALLED HENRY ALUBOWICZ ABOUT VIRUS
11/03	00:45	DECISION TO DISCONNECT NAS FROM THE REST OF AMES
11/03	00:50	PASSWORD CRACKING GOING ON BY THE VIRUS PROGRAM
11/03	02:45	VITALINKS DISCONNECTED AT NAS
11/03	03:20	CRABB CALLED TO AID IN SHUTTING DOWN VIRUS ON SUN FILE SERVERS
11/03	07:00	CALLED NAS NET SITES TO INFORM THEM OF VIRUS PROBLEM
11/03	08:23	ARCLAN, MILNET, ARPANET, NSFNET, HYPERCHANNEL DISCONNECTED
11/03	09:05	MOTD STATING INTERNET MAIL IS DOWN
11/03	09:42	SNOOPY, GOTTFRIED (CM-2) NOT AFFECTED, BUT SENDMAIL KILLED
11/03	09:42	SUNS, AMELIA, WILBUR, FRED, ORVILLE (ALL VAXES) AFFECTED
11/03	10:00	MEETING WITH RON BAILEY, KRAMER, DEISS TO ASSESS THE SITUATION
11/03	10:13	BENDIX POWERED DOWN THE DIAL-BACK SYSTEM
11/03	10:54	RECOMPILED SENDMAIL WITH DEBUG OFF; INSTALLED ON CRAYS; TEST OK
11/03	11:00	RESPONSE TEAM MEETING TO GIVE ASSIGNMENTS FOR FIXES, AUDITS
11/03	11:00	VIRUS AFFECTED ALL 4 VAXES AND 10 SUN WORKSTATIONS
11/03	15:00	STATUS MEETING; SENDMAIL FIXED; .RHOST DISABLED
		BINARY PATCH TO SUNS BECAUSE WE DO NOT HAVE SOURCE CODE
11/03	14:00	AMELIA & FRED TO BE SHUT DOWN FOR REBOOT TO RESTORE COMMUNICATIONS
11/03	14:26	FRED AND AMELIA BACK UP
11/03	16:10	ALL INETD NEEDS TO BE KILLED; DOWN FOR THE NIGHT
11/03	16:15	INET DAEMONS HAVE BEEN REMOVED AND TAKEN OUT OF FRED & AME
11/03	17:00	MICOM SWITCHES DISCONNECTED TO NAS
11/03	17:20	INETD ON HAN BROUGHT UP AFTER REMOVING FROM MAIN ETHERNET
11/03	18:15	INETD, SENDMAIL DISABLED ON ALL WORKSTATIONS
11/04	07:00	NO MORE FREE TAPES FOR AMELIA; NEED LEVEL 0 BACKUP
11/04	08:00	VIRUS ALSO ATTACKING THROUGH FINGERD; FINDERD DISABLED
11/04	08:43	EARTH IS OFF THE MICOM
11/04	10:05	BEGAN FULL BACKUP OF STOKES
11/04	11:48	FINISHED FULL BACKUP OF STOKES
11/04	13:30	YMP & WILBUR PUT ON THEIR OWN HYPERCHANNEL NETWORK
11/04	13:30	MVS DEDICATED TIME CANCELED DUE TO VIRUS PROBLEM
11/04	16:00	LEKASHMAN HAS COPIES OF VIRUS FIX FOR DISTRIBUTION IN CONTROL RM
11/04	21:00	VIRUS FIX ON THE VAXES COMPLETE AND TESTED
11/05	00:10	ROOT PASSWORDS CHANGED ON ALL NAS COMPUTERS
11/05	10:36	AMELIA INOCULATED AND VERIFICATION TEST HAVE PASSED
11/05	10:36	WILBUR & ORVILLE ARE UP AND RUNNING WITH NO PROBLEMS
11/05	11:03	FRED RUNNING, INNOCULATED AND PASSED VERIFICATION
11/05	11:26	SNOOPY TESTED FOR SENDMAIL AND PASSED AS OKAY. NO HOST.EQUIV
11/05	12:37	MEYER UP WITHOUT INET, FINGERD, OR SENDMAIL
11/05	13:35	LINK TO N233 AND N202A RESTORED
11/05	14:00	ETHERNET TO N-202A RECONNECTED
11/05	14:00	MOTD MESSAGE TO NOTIFY USERS OF THE VIRUS PROBLEM
11/05	14:09	NAVIER & STOKES CLEAN, BRINGING UP A HYPERCHANNEL
11/05	14:30	HAN TO BE USED AS GUINEA PIG FOR CONNECTION TO LONG HAUL SITES
11/05	14:48	INTERNET SWITCH AND DIAL-BACK SYSTEM BACK UP
11/05	14:57	SANDBOX, TUTS, NEWTUTS CLEAN AND VERIFIED
11/05	16:40	VIRUS SET LOOSE ON THE NETWORK TO TEST INNOCULATION
11/06	12:25	NO EVIDENCE OF VIRUS PROBLEMS
11/06	13:00	ALL REMOTE SITES NOTIFIED AND SENT VIRUS FIX
11/06	13:20	LOCAL NETS STARTED BY MILO MEDIN
11/06	13:30	WIDE AREA NETS & ARCLAN STARTED
11/06	13:33	FTP ANONYMOUS DISABLED ON AMELIA
11/06	13:45	RIACS SUBNET NOW ON
11/06	14:15	ALL IRISES, SUNS, 4D/60S ARE UP & ON NETWORK
11/06	16:30	NAME DAEMON NOT RUNNING ON ORVILLE DUE TO SENDMAIL QUEUE GROWING
11/06	23:30	BROUGHT HSX UP BETWEEN NAVIER & STOKES
11/07	06:45	LARC RECONNECTED
11/07	11:00	14 OF THE 26 SITES ARE CONNECTED
11/07	11:30	BLDG N256 STILL ISOLATED
11/07	12:30	ALL LONG HAUL SITES NOW CONNECTED TO NAS

Att[illegible] 1

From: bostic@OKEEFFE.BERKELEY.EDU (Keith Bostic)
Subject: V1.67 (Virus posting)
Message-ID: <8811031054.AA22156@okeeffe.Berkeley.EDU>
Date: 3 Nov 88 10:54:57 GMT
Sender: daemon@ucbvax.BERKELEY.EDU
Organization: University of California at Berkeley
Lines: 107

Subject: Fixes for the virus
Index: usr.lib/sendmail/src/srvrsmtp.c 4BSD

Description:

There's a virus running around; the salient facts. A bug in sendmail has been used to introduce a virus into a lot of Internet UNIX systems. It has not been observed to damage the host system, however, it's incredibly virulent, attempting to introduce itself to every system it can find. It appears to use rsh, broken passwords, and sendmail to introduce itself into the target systems. It affects only VAXen and Suns, as far as we know.

There are three changes that we believe will immunize your system. They are attached.

Thanks to the Experimental Computing Facility, Center for Disease Control for their assistance. (It's pretty late, and they certainly deserved some thanks, somewhere!)

Fix:

First, either recompile or patch sendmail to disallow the `debug' option. If you have source, recompile sendmail after first applying the following patch to the module svrsmtp.c:

```
*** /tmp/d22039 Thu Nov  3 02:26:20 1988
--- srvrsmtp.c  Thu Nov  3 01:21:04 1988
***************
*** 85,92 ****
        "onex",         CMDONEX,
  # ifdef DEBUG
        "showq",        CMDDBGQSHOW,
-       "debug",        CMDDBGDEBUG,
  # endif DEBUG
  # ifdef WIZ
        "kill",         CMDDBGKILL,
  # endif WIZ
--- 85,94 ----
        "onex",         CMDONEX,
  # ifdef DEBUG
        "showq",        CMDDBGQSHOW,
  # endif DEBUG
+ # ifdef notdef
+       "debug",        CMDDBGDEBUG,
+ # endif notdef
  # ifdef WIZ
        "kill",         CMDDBGKILL,
  # endif WIZ
```

Then, reinstall sendmail, refreeze the configuration file,

Attach 2

using the command "/usr/lib/sendmail -bz", kill any running sendmail's, using the ps(1) command and the kill(1) command, and restart your sendmail. To find out how sendmail is execed on your system, use grep(1) to find the sendmail start line in either the files /etc/rc or /etc/rc.local

If you don't have source, apply the following patch to your sendmail binary. SAVE A COPY OF IT FIRST, IN CASE YOU MESS UP! This is mildly tricky -- note, some versions of strings(1), which we're going to use to find the offset of the string "debug" in the binary print out the offsets in octal, not decimal. Run the following shell line to decide how your version of strings(1) works:

```
        /bin/echo 'abcd' | /usr/ucb/strings -o
```

Note, make sure the eight control 'G's are preserved in this line. If this command results in something like:

```
        0000008 abcd
```

your strings(1) command prints out locations in decimal, else it's octal.

The patch script for sendmail. NOTE, YOUR OFFSETS MAY VARY!! This script assumes that your strings(1) command prints out the offsets in decimal.

```
        Script started on Thu Nov  3 02:08:14 1988
        okeeffe:tmp {2} strings -o -a /usr/lib/sendmail | egrep debug
        0096972 debug
        okeeffe:tmp {3} adb -w /usr/lib/sendmail
        ?m 0 0xffffffff 0
        0t10$d
        radix=10 base ten
        96972?s
        96972:          debug
        96972?w 0
        96972:          25701   =       0
        okeeffe:tmp {4} ^D
        script done on Thu Nov  3 02:09:31 1988
```

If your strings(1) command prints out the offsets in octal, change the line "0t10$d" to "0t8$d".

After you've fixed sendmail, move both /bin/cc and /bin/ld to something else. (The virus uses the cc and the ld commands to rebuild itself to run on your system.)

Finally, kill any processes on your system that don't belong there. Suspicious ones have "(sh)" or "xNNNNNNN" where the N's are random digits, as the command name on the ps(1) output line.

One more thing, if you find files in /tmp or /usr/tmp that have names like "xNNNNNN,l1.c", or "xNNNNNN,sun3.o", or "xNNNNNNN,vax.o" where the N's are random digits, you've been infected.

End of article 67 (of 67)--what next? [npq]

There was this gaping security breach on Nov 2. I first noted it at about 9:45 pm. I talked with Bill about it, and I will show up at 10:00am tomorrow to talk more about it.

What occurred:
1. At some point in time on Nov. 2, large parts of the TCP/IP Internet was 'attacked' by a program designed to replicate itself on other machines, and use up all the CPU on a machine in the process.

2. The detected methodology is in several parts. Some of these are:

A mail message comes in, with a particular pattern that causes the mailer to execute a program. The program is a simple one, which pulls in a binary image and source files from the attacking host.

The binary is then executed. It has several functions.

a. It searches for Internet addresses to attack. This search is done in a CPU intensive way. It builds and compiles a program to see if a remote machine will respond. If so, it then sends off a copy of this program.

b. There is some of password cracking that goes on. When it finds a likely candidate, it searches through .rhosts files, looking for machines that are accessible, and then cloning itself. It has been noted to be running as root, although not on NAS machines.

c. Much of the basic function appears to be to eat all of the CPU on a machine. Load average climbs to at least 20. The compiler is run a great deal. The network routing tables are examined for some reason.

3. So far, this only appears to be able to directly install the the regeneration part of itself on vaxes and suns. The crays were not affected so far. All four NAS vaxes were hit. Icase, sun200, sun205, crayon, were known to have been hit. It does seem to be able to execute large numbers of remote shell programs from vaxes and suns to other machines, using up their CPU.

4. Complete file systems have been checked on some machines (not at NAS.) So far, no parts of the existing file system appear to have been touched. The program appears to create and compile programs in /usr/tmp, only.

5. I have made the repair to the mailer, on orville, and brought it back up. We shall see if it gets re-attacked.
The repair to version 5.59 of sendmail is to comment out the #define DEBUG 1 in conf.h.
In addition, .rhosts files and /etc/hosts.equiv cannot be active, while this exists, or that path will be used.

6. The external networks to Ames have been shut off at this time, while everyone is cleaning up. All the gateways in N254 are disabled. The vitalinks in 258-133 are currently unplugged, as I didn't see the power switches. We will probably

Attach 3

to contact all users sites to see if any got attacked.

I'll be in, probably at 10:00, for more questions. I did save a bunch of running state on orville while this was going on, so we can look at it some more.
her folks around the country have done other debugging and tection.

john

Here are the things that need to be done to a machine to sanitize it against this virus, and some similar things. This is online on orville in ~lekash/repairs

1. Sendmail - The sendmail source must be repaired to no allow debug commands to be executed. This is done in the file srvrsmtp.c
The change is to find the line

```
   "debug",         CMDDBGDEBUG,
```

and either delete it entirely,
or change it to be like:

```
#ifdef notdef
   "debug",         CMDDBGDEBUG,
#endif
```

so that one can know of its existence for possible use during debugging.

One could also edit conf.h to comment out the #define DEBUG 1

2. fingerd - This requires a gets be replaced with an fgets, so that the stack cannot be overwritten.

```
diff -c fingerd.c fingerd.c~
*** fingerd.c       Fri Nov  4 18:39:57 1988
--- fingerd.c~      Mon Sep 22 10:32:23 1986
***************
*** 27,33
   char *argv[];
  {
   register char *sp;
!  char line[BUFSIZ];
   struct sockaddr_in sin;
   int i, p[2], pid, status;
   FILE *fp;

--- 27,33 -----
   char *argv[];
  {
   register char *sp;
!  char line[512];
   struct sockaddr_in sin;
   int i, p[2], pid, status;
   FILE *fp;
***************
*** 37,43
   if (getpeername(0, &sin, &i) < 0)
           fatal(argv[0], "getpeername");
   line[0] = '\0';
!  fgets(line, BUFSIZ, stdin);
   sp = line;
   av[0] = "finger";
   i = 1;

--- 37,43 -----
   if (getpeername(0, &sin, &i) < 0)
           fatal(argv[0], "getpeername");
```

Attach 4

```
+ {
+   FILE *fd;
+   char buf[BUFSIZ], *index();
+   if ((fd = fopen ("/etc/users.unequiv","r")) == NULL) return (0);
+   while (fgets(buf, BUFSIZ, fd)) {
+     if (index(buf, '\n')) *index(buf, '\n') = 0;
+     if (!(strcmp(ch, buf))) {
+       fclose (fd);
+       return (-1);
+     }
+   }
+   fclose (fd);
+   return (0);
  }

  _validuser(hostf, rhost, luser, ruser, baselen)
```

The following is what to do for machines which do not have source code. This list is not a final solution, as all it does is disable the things which had holes in them. The end result is to go repair the source code.

1. kill off the mailer.
   see that it is not able to be started in the boot file.
   This is typically /etc/rc.local on a sun workstation.
   See to a new mailer being made, from source code, with the above repair.

   For example:

```
diff -c /tmp/bogons /etc/rc.local
*** /tmp/bogons Fri Nov  4 19:11:05 1988
--- /etc/rc.local       Fri Nov  4 13:43:29 1988
***************
*** 61,71 ****
  if [ -f /dev/gpone0a ]; then
        /usr/etc/gpconfig gpone0 -f -b cgtwo0                 >/dev/console
  fi
 (echo -n 'local daemons:')                                   >/dev/console
! if [ -f /usr/lib/sendmail -a -f /usr/lib/sendmail.cf ]; then
!       (cd /usr/spool/mqueue; rm -f nf* lf*)
!       /usr/lib/sendmail -bd -q1h & (echo -n ' sendmail') >/dev/console
! fi
  if [ -f /etc/nd.local -a -f /dev/rndl0 ]; then
        (echo -n ' nd'; /etc/nd - </etc/nd.local)             >/dev/console
        (echo -n ' rarpd'; \
--- 61,71 ----
  if [ -f /dev/gpone0a ]; then
        /usr/etc/gpconfig gpone0 -f -b cgtwo0                 >/dev/console
  fi
  (echo -n 'local daemons:')                                  >/dev/console
! #if [ -f /usr/lib/sendmail -a -f /usr/lib/sendmail.cf ]; then
! #     (cd /usr/spool/mqueue; rm -f nf* lf*)
! #     /usr/lib/sendmail -bd -q1h & (echo -n ' sendmail') >/dev/console
! #fi
  if [ -f /etc/nd.local -a -f /dev/rndl0 ]; then
        (echo -n ' nd'; /etc/nd - </etc/nd.local)             >/dev/console
        (echo -n ' rarpd'; \
```

2. See to the fingerd program not being accesible. This is done by

```
     line[0] = '\0';
!    gets(line);
     sp = line;
     av[0] = "finger";
     i = 1;
```

3. The following change prohibits certain well known usernames
which are frequently used as ids by executing programs
from being used in rsh and rlogin. This needs to be changed
in the c-library. This is done by:

  a. make the following change to rcmd.c
  b. rebuild libc.a
  c. install libc.a
  d. make rshd rlogind rexecd login
  e. install rshd rlogind rexecd login
  f. create a file /etc/users.unequiv and put

nobody
daemon
     in it.

```
*** typescript     Fri Nov  4 18:29:01 1988
*** typescript     Fri Nov  4 18:29:01 1988
--- /usr/src/lib/libc/net/rcmd.c   Fri Nov  4 18:57:30 1988
***************
*** 201,206
     }
     *p = '\0';
     hostf = superuser ? (FILE *)0 : fopen("/etc/hosts.equiv", "r");
   again:
     if (hostf) {
             if (!_validuser(hostf, fhost, luser, ruser, baselen)) {

--- 201,210 -----
     }
     *p = '\0';
     hostf = superuser ? (FILE *)0 : fopen("/etc/hosts.equiv", "r");
+    if (hostf && _invaliduser(luser)) {
+            fclose(hostf);
+            return(-1);
+    }
   again:
     if (hostf) {
             if (!_validuser(hostf, fhost, luser, ruser, baselen)) {
***************
*** 229,234
             goto again;
     }
     return (-1);
   }

   _validuser(hostf, rhost, luser, ruser, baselen)

--- 233,255 -----
             goto again;
     }
     return (-1);
+  }
+
+  _invaliduser(ch)
+  char *ch;
```

The following tests can be done to verify that a machine is now repaired. This file is on-line on orville in ~lekash/checklist

1. Mailer problem.
A program has been written which tests for vulnerability to the mailer attack. This is on orville.
The program is named "testmailer".
After a machine is successfully repaired, and the networks on it are brought back up, run the testmailer program from orville.
For example:

Be sure that sendmail is running in server mode on the machine to be tested. If you get "connection refused" it is not up.

```
cd /usr/local/bin
./testmailer prandtl
rsh prandtl ls -l /usr/tmp/insecure
```

If the bug still exists, then a file will be created on the remote system (prandtl in this example) called /usr/tmp/insecure.
If this file does not exist, then the bug is fixed.

2. Finger problem.
No program has been written for this, yet. However, the program is sufficiently small, and the change sufficiently explicit, that if it is done and installed, confidence is vey high that it will work.
For those uncomfortable with this, the fingerd program can be left disabled as described in the problem resolution for machines without source until a program is written to test this out.

3. rsh problem.
Install /etc/hosts.equiv
On some system that is up and functioning on the network, perform the following commands. This verifys that the users nobody and daemon cannot execute remote commands.

```
su
Password: xxxxxxxx
su nobody

rsh prandtl date
rlogin prandtl

exit
su daemon
rsh prandtl date
rlogin prandtl
```

All 'r' commands should return permission denied.

At this point, the machine under test is protected against the known attacks.

john

Attach 5

commenting out the line in the inetd configuration file which enables it. Once again, see to the appropriate source code repair. For example, on the sun workstation:

```
diff -c /etc/bogons /etc/servers
*** /etc/bogons        Tue Aug  2 11:09:04 1988
--- /tmp/servers Fri Nov  4 19:18:24 1988
***************
*** 12,18 ****
  time  tcp     /usr/etc/in.timed
  time  udp     /usr/etc/in.timed
  name  udp     /usr/etc/in.tnamed
! finger        tcp     /usr/etc/in.fingerd
  rpc   udp     /usr/etc/rpc.rstatd      100001  1-3
  rpc   udp     /usr/etc/rpc.rusersd     100002  1-2
  rpc   udp     /usr/etc/rpc.rwalld      100008  1
--- 12,18 ----
  time  tcp     /usr/etc/in.timed
  time  udp     /usr/etc/in.timed
  name  udp     /usr/etc/in.tnamed
! #finger       tcp     /usr/etc/in.fingerd
  rpc   udp     /usr/etc/rpc.rstatd      100001  1-3
  rpc   udp     /usr/etc/rpc.rusersd     100002  1-2
  rpc   udp     /usr/etc/rpc.rwalld      100008  1
```

3. To prevent the rsh spread, move /etc/hosts.equiv to another name, saving it until the appropriate source can be repaired.

After these changes have been done, the system should be fairly safe against this sort of attack. Things are probably ready to be brought back up.

john

DATE 11-2

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
2306	All		Per J. Lekashman, security breach through mailer on our systems, he suggests killing mailer and ifinger daemons, related to sendmail bug being worked on at Berkeley, Lekashman working on orville; in addition comment out sendmail mailer in .rc file and reboot mach.	vJ
2341	NSS	↑	after backups	JL

Attach C

DATE 11-3

page 1 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
0010	YMP	↓	CRI called	TH
0030	YMP		Bobt have	TH
0036	YMP	↑	after crash	TH
0113	Stokes	↑	with new kernel	TH
0021	Fred	↓	crash	TH
0051	Fred	↑	after auto boot	TH
206	YMP	↓	Bobt still have – took it down	
			to clear excessive Single bit errors	TH
300	YMP	↑		TH
0320			Michelle Crabb called to aid in	
			shutting down virus on sun file	
			servers	TH
0425	Prandtl		killed runaway ftp (79 mins)	TH
0030	all		Called Henry Alubowicz about virus	TH
0040	all		Called Bill Kramer about virus. will	
			kill sendmail on all NAS machines and	
			comment it out of the startup rc	
			files (one of /etc/rc, rc.local, netstart,	
			local.rc, NETSTART). Also commenting	
			out fingerd in /etc/inet.conf – this	
			is another susspected point of attack	

DATE 11/3/88

page 3 of 7

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
0730	YMP	↓	YMP IS DOWN, NOT RESPONDING TO PING (4K)	JS
0731	YMP		ADVISED B. TURMAN OF CONDITION	JS
0747	VITALINK		ART EDWARDS DISCOVERED VITALINKS DICONNECTED, ADVISED	
			HIM TALK TO B. KRAMER, WANTS TO BE NOTIFIED WHEN RECONNECTED	
0743	YMP	↑	YMP IS UP, PER CRAY FE	JS
0823	ACRLAN		ARCLAN, MILNET, ARPANEN, NSFnet,	
	Hyperchannel		to Bld 202 Hyperchannel to bldg 254, 233A	
	+ RIACs		+ 202A	
	"CNS"		CNS (A222-53) is still up.	SH
0905	motd		The motd that stated the internet	SH
			mail is down temporarily has	
			been removed.	
0924	motd		Putting the internet mail global	SC
			motd message back in.	
0928	NAS		Deleted "COHEN 25665.STRKES	
			" ECHTERIN 24944.STRKES	
			" LOPEZ 24976 STRKES	
			" SPERR 24995 STRKES' from [illegible]	JS
0942	SNOOPY		SNOOPY IS NOT INFECTED (USER/TRIP), BUT SENDMAIL KILLED	TH
	GOTTFRIED		GOTTFRED NOT INFECTED	TH
0942	LIST		LIST OF AFFECTED MACHINES:	
			SUN 200-204 + 209, SUN 108, AMES, WIL, FRED, ORV	TH
			(SUN 92-96 ARE OK, SUN 101, 102, 104, 105, 107 are OK)	

(SUN 205, 210 OK, SUN 103, 106 OK)

DATE 11/3/88

page 3 of 7

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1012	doors		Bob Fuller said that the outside doors will be open for painting. The computer room door will be painted during second shift	Sc
1013	Dialback	↓	Bendix has powered down the dial back system	KH
1016			Moffet field fire dept & Scott marse looking at fire abort button	
1014	DBIU		Reset from 911	TH
10:54	Cray2		recompiled sendmail with Debug off and installed it on navier & stokes. Tested OK	Ed
11:05	Perfmon		Perfmon Account was moved from /u1/pA to /u1/pa ~~from~~ on prandtl as per Don Seal. An attempt was made to contact V. Lee but to no avail.	
1137	YMP	↓	YMP IS DOWN, ADVISED CRI	
1153	ymp	↑	Ymp 's up; NO PROB FOUND	
1215	YMP	↓	YMP IS DOWN NOT RESPONDING TO PING (1X)	
1216	YMP	↑	YMP IS UP, RESPONDING	

DATE 11/3/88

page 4 of 7

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1400			Ame + Fred to be shut down for quick	Ja
			reboot in 5 minutes to restore communications	
1405	Fred	↓	taken down	Ja
	Ame	↓	taken down	Ja
1412	Fred	↑	back up and accessible	Ja
1426	Amelia	↑	Back up	
1540	Networks		System still disable due to	
	NAS		virus problem. NAS is still disconnected	
			from the rest of the world.	
			No estimated update.	
1605	VM2		A. Poston cancelled dedicated time.	
1610	All NAS systems		All inetd need to be killed per	
			Bob Van Cleef (from NSD Meeting)	
			leave the inetd down for	
			tonight.	
1610	Gott		GOTTFRIED checked for virus by R. MAHN. CAME	RF
			out clear. No inetd or sendmail running	
1616	VMF	↓	not responding to any - notified	
			CRI analyst + FE	TO
16:15	Fred Ame		R Mahn said inetdaemons have	
			been removed & taken out on Fred & Ame	LW
16:20	ETA	↓	Shutdown for reboot for security problems	LR

DATE 11-3 88

page 5 of 7

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1620	Alliant Convex		Karen is still looking at Alliant	
			and Convex	[illegible]
1620	Micom Switch		Doug Sending is disconnecting	
			micom switch from the world,	
			will let me know when done	[illegible]
16:22	YMP	↑	YMP up & running. It was rebooted	
			for security reasons	LK
1630	Alliant Convex		Joe Scott - Ken Keller - working [illegible]	
			on Alliant & Convex	VJ
16:35	Alliant		Ken Brell said Alliant was "clean" - no virus	LK
			He is checking "Convex now.	LK
1640	NAVIER		R. Peiss has authorized	
	STOKES		unlimited dedicated time	
			on Cray 2s, in lieu of all the	
			Networks being down.	[illegible]
1700	150		150 + 190 Micom switches disconnected	
	190		to NAS. ~~No~~ All interconnection	
			between system are down.	[illegible]
17:20	Nav	↓	Shutdown for CRI ~~P.M.~~ dedicated time until	
			further notice.	LK
17:20	Stokes	↓	Shutdown for CRI P.M. until	
			further notice.	LK
1700	Ame	↓	for dedicated time	

DATE 11/3/88

page 6 of 7

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
17:20	Han		Rfox brought up inetd on Han after removing it from main ethernet in order to connect Han to Bamboo via Delni box. OK. Per Henry A.	LR
18:03	YMP	↓	YMP down for P.M.	MM
1815	WORK-STATIONS		Michele Crabb called to say she has completed her tasks on the workstations, ie. No: inetd, sendmail, . . .	JE
1930	ETA	↑	Bob from Eta called + said A was up	P
			Dirk is working on AHU-2 "just ack" any more alarms	
2004			on that AHU	PC
2024	ETA	↓	down for testing per analyst	VJ
2035	HAN		Restored connection to Ethernet, Inetd killed per R.Fox	JE
2104	ETA	↑	up after testing per analyst	KJ
2111	AME	↑	BACK FROM DEDICATED TIME. Do level 0 on /USR don't do ~~te~~ /u/ah	RM
2140	ETA		Bob Is taking ETA for more testing	PR
2200	ETA	↑	Bob called It is up	PR
2250	YMP	↑	Up & running.	LR

DATE 11-03

page 1 of 1

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT DESCRIPTION	IN
2345			At approximately 2345, a fire alarm sounded.	
			checked the panel and it showed that	
			12 was red. Called Duty Office, they	
			informed us to evacuate the building.	SP.
0				

DATE 11-04

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
0000			The Fireman said it was a sensor located in the Computer room underneath the floor one row behind Orville. Fireman said that he does not know what set it off.	SP.
0010	Navier		CRI said they are finished with Navier	SP.
0015			Fire alarm 12 sounded off again. Duty Office notified. Fireman on their way.	SP.
0025			Fire Dept. arrived.	SP.
0035			called Scott Morse → said to acknowledge alarms → enable us ~~to~~ reset Doomsday box	Dt
0115	Navier		NQS is up and running. All network interfaces are Still disabled per John Musch	SP.
	Notes		Several Users have called with concern on their /scr files. Knowing if they are not moved by a certain time they will lose them. Maybe some sort of message should be put out to let users know about these files if systems are not to be restored today. Thanks.	SP
0450	Stokes		NQS is also up and running. All network interfaces are disabled, per John Musch.	

He said a FE is on his way in to work on

DATE 11/4/88 page 2 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	I
0538	Piper	↓	ETA paged, Piper II down	[illegible]
0539			ETA responded (Prescott)	[illegible]
0600	Piper	↑	rebooted by Prescott	[illegible]
0625		.	erep completed	[illegible]
0700	Ame		There are no more (free) ~~scratch~~ tapes for Ame.	
			We need to do level Ø backups tonight	
			and need some tapes	SP
0841	YMP	↓	Not responding to Ping. YMP down	[illegible]
			Ray Park will tell [illegible]	
0843	Milnet		Gary from Bendix says "[illegible] is now	[illegible]
			off the [illegible]"	
0854	YMP	↑	[illegible]	
1031	ALL CRAYS		SHIFT TEAMS ARE NOT TO ALLOW THE	RF
			PAINTING OF DOORS FOR THE CRAYS IN	
stokes			THE HSP ROOMS. PAINT MOLECULES IN AIR	
			CAUSE HEADS TO CRASH. HAPPENED ONCE	
			ALREADY — HAVE PAINTERS GO ELSEWHERE	
			PER RICH BRULET + FACILITIES	
1200	VIRUS		Direct "Press" questions to NASA	
	Status		Public Affairs 694-5091.	
	.		Networks will still be down until 1530 PST	[illegible]

DATE 11/04/88

page 3 of 6

NAS/GE OPERATIONS LOG

	TIME	EQUIP	RS	EVENT DESCRIPTION	IN
	1005	STOKES		Began "full" backup	JD
	1148	STOKES		finished "full" backup	JD
↑ at 1241 →	12.20	Fred	↓	A Quick reboot on Fred by R Hinkin	DI
	12.20	Piper		Piper is not responding to ping EAA Flagged	DI
	12.22	Piper		Murray returned the call	DI
↑ at 13.07	12.30	Amelia	↓	R [illegible] will reboot Amelia	DI
	12.45			CE WILL BE OFF FOR THE WEEKEND	DI
	1330	YMP		YMP & WILBUR are being put on	
		WILBUR		their own HYPERchannel network	
				while work on the "virus" continues	[illegible]
	1330	NAV		Has dedicated time tonight,	
				1900-0200 PST for 4.3 networking	
				work by John Musch & CRI.	[illegible]
	1330	MVS		MVS dedicated time canceled	
				tonight due to "virus" problem	[illegible]
	1323	EAA	(Piper)	Backup at 1322 per Murray Goggins	[illegible]
	1410	Piper	↓	Bob Ciotti has taken piper down	[illegible]
	1435	Paul R.		PAUL R IS ON PAGER FOR REMAINDER OF THE DAY	KF
	1515	PIPER	↑	back up per BOB CIOTTI	KF
	1452	12.[illegible]		Bendix called to look in 12 problem [illegible]	[illegible]
		Brandt		Pete Lansdale sees mail problem of NE [illegible]	[illegible]

in the [illegible] due to bad disk nodes. The problem should be fixed

DATE 11/04/88 page 4 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1540	Piper	↓	Not responding to ping (3 times). Piper	
			is down. Paged Marisa	FL
1544	Piper		Marisa returned paged.	FL
1600	Bendx	.	If Bendix is needed please call	
			(415) 447-4121 (Cathy) until Sunday	
			at 10 AM; she is on duty and can be	
			reached directly	
1600	ETA	↑	Piper is up	
1600	YMP		YMP is up; the net connection is	
			temporarily closed	
1600	"VIRUS	"	J. Lekashani will have copies for	
	PROBLEM		"virus" fix for Seal, King, Reü,	
			Mahn, Veurn, Mahn, Storm,	
			Fouts + Thompson in the Control	
			Room. Please distribute.	
			As these people install the fix	
			+ test it. When their system is	
			"virus" proofed, they will	
			connect their networks back	
			+ inform the Control Room.	
	.		Log when systems are backup	

on the Network.

(continue next page)

DATE 11/04/88 page 5 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
			(from dayshift)	
			Note external Network will be	
			down at least through 11/05/88	
			1300 PST & probably longer.	
			150 & 190 Micom switch is still down.	
1630			LARRY RUNCIMAN IS SICK WILL NOT BE IN	FL
1644	YMP		Back monitoring the YMP VIA Wilbur.	FL
1700	Navier		Ivan Chiung will have dedicated	
			Sometime this evening or	
			tomorrow morning. He will be done	
			before 12:00 NOON Sat morning per.	
			Howard Walter	Mm
1900	Stokes		Another disk has been temporarily	Mm
			added to /scr2 31Ø75Ø	
1930	CNS		Noticed that someone outside the	
			control room reset CNS.	FL
2025	YMP & piper		John Barton said Eugene Miya is working	
			on the acceptance tests for both the	
			YMP & piper. Eugene will need access	
			into the Cray 2 room and computer room.	
			Please let him in.	FL

1900 NAV ded

DATE 11/4/88 page 6 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
2054	Piper	↓	Bob Ciotti is taking Piper down for	
			testing	FL
2100			Contacted or left (by J. Lekashman) message re: virus fix	[illegible]
			with the following Seal, King, Pew,	
			Mahn, + Stone, e-mail on Wilbur for	
			Fants; no # for Veum or Thompson	
2220	Navier		Per J. Barton Eugene Muze	
			needs access to Cray 2 room to	
			run some tests on navier, he	
			will be in about 2AM tonite	VJ
2205	Piper	↑	Per Bob Ciotti "Piper is back up	FL
~~9:30~~			~~AAPtek 10 will be down for 1 hr.~~	

DATE 11/5/88

page 1 of 5

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
200	Nav		E. Mayo here to run tests on Nav	D
300	Nav	↑	J. Musch installed 4.3 networking code NOT TRUE	LD
630	VM2		Erep completed on VM2	HM
0735	Wilbur	.	APPEARS "CHECKED OUT" PER M. FOUTS	JS
08:45	Navier	↓	Bring down Navier to change the ~~to~~ FSTAB table by Ivan Chung.	DI
09:30	Hyperchannel		Adapter 10 given to NSC for approx 1 hour	SS
10:05	CRAY		let a delivery person in the building to see Scott	DI
10:36	AMELIA	↑	AMELIA IS INNOCULATED + VERIFICATION	
			TEST HAVE PASSED.	SS
10:36	ORV + WILBUR		APPARENTLY ~~THESE~~ WILBUR + ORVILLE ARE	
			UP + RUNNING; HAVING BEEN VERIFIED	
			BY J. LEKASHMAN + M. FOUTS.	SS
11:03	FRED	↑	FRED RUNNING, VERIFIED PER MANN	JS
11:05	FRED	↑	INNOCULATED + PASSED VERIFICATION	RW
1109	PIPER	↓	PIPER IS DOWN, NOT RESPONDING (1X)	JS
1112	BOTTFRKS		TESTED FOR SEND MAIL - O.K., HOST. EQUIV IS OFF	EM
1114	PIPER	↑	PIPER IS UP, RESPONDING	
1126	SNOOPY	↑	Tested for Sendmail, passed. No hosts.equiv	EM
11:[illegible]	Navier	↑	FSTAB has been brought back as normal. (Ivan Chu) Done with the dedicated time.	IC
1200	Navier		J Musch has system for dedicated time	JS
1216	YMP	↓	YMP IS DOWN, NOT RESPONDING TO PING (1X)	JS

DATE 11/5 page 2 of 5

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	I
1217	YMP	↑	YMP IS UP, RESPONDING	
1225	MSS-Meyer	↓	Brought down meyer to verify comes up okay	
1237	MSS Meyer	↑	Up without inetd, findcd or sendml	
1245	YMP	↓	not responding to ping. Called CRI	D
1253	YMP	↑	RESPONDING TO PING	5
1400	LZ		lz 2 + lz 4 now working ok from Prandtl reboot	RI
1400	N202A		ETHERNET TO N202A RE-CONNECTED	SS
1300	PAM		Up to net, clean	Se
1409	CRAY2		Navier + Stokes clean, bringing up on HYPCHAN	MF
1432	PIPER	↓	NOT RESPONDING TO PING ETA WAS PAGED	J D
1435	PIPER		ETA. RETURNED CALL	DL
1436	PIPER	↑	PIPER IS UP	Di
1448	BENDIX	↑	GARY JUST BROUGHT UP THE INTER SWITCH and THE DIAL BACK SYSTEM	Di
1450	NAVIER		J. MUSCH WILL HAVE DEDICATED FROM 1900 ONWARD UNTIL FURTHER NOTICE	
1440	VM2		Meyer, SSCDEV, SSSTST1 and SSCTST2 check out okay	
1457	VM2		Sandbox, tuts, newtuts clean and verified	

DATE 11/5

page 3 of 5

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1335	Hyperchannel		LINK TO N233 + N202A RESTORED.	SS
1415	CRAYS		NOTE: AS OF 11:00 ON SUN 11/6 THE	RF
			"UNLIMITED" CRAY DEDICATED TIME WILL CEASE.	
			NO MORE CRAY TIME CAN BE HAD UNLESS	
			SCHEDULED IN ADVANCE. ALSO, STARTING AT TODAY	
			14:00, ONLY ONE CRAY CAN BE USED FOR	
			DEDICATED TIME AT A TIME. (NOT BOTH)	
			IVAN CHUNG HAS DEDICATED TIME ON NAVIER	
			FROM 1600-1900, AND JOHN MUSCH HAS DEDICATED	
			TIME FROM 1900 - ? (ABOUT 0200 ON 11/6)	
			OTHERS CAN HAVE 'EM UNTIL 11:00 11/6.	
			UNTIL FULL CONNECTIVITY IS RESTORED, DON'T	
			KILL DEFERQ ABUSERS. (PER H. WALTER)	
1430	POLICY		SEE FOLLOWING SHEETS FOR OFFICIAL RELEASE	RF
			PUT IN MOTD WHEN NETMOTD WORKS + NOTE	
			NAS USER CALL INFO RESPONSE	RF
1430	MICOM		150, 190, dial back + all ports to MICOM turned	RF
			back on at 1330	
	LHC		We are going to be used as a guinea pig for	
			connection to LHC sites temporarily to see if	
			virus attacks occur	

DATE 11/5

page 4 of 5

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1430	LAN		SUN IN BLDG 254 being used as guinea pig for local net connection. If no attacks, local nets will be connected in a few hours. Rest of ARCLAN on Monday.	RF
1430	test		virus will be set loose at ≈1400 to see it propagates locally. If no affects seen in 2 hours, nets will be started on other internal links (202, 233)	
1430			NAS net + other external links will be up by ≈0600 on Monday 11/7 unless "mutant" virus appears (changed versions of original)	RF
1640			Virus set loose on the network. This was done by J. Kekashman infecting the Sun in N254 and our link to N254 being brought up. Prior to this all external links to N254 were disconnected by M. Medin	SS
19:00	NAV	✓	Navier turned over to J. Musch from I. Chung in single user mode	JM

DATE 11/5

page 5 of 5

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1930	Piper	↓	EOF encountered reading socket. Piper not	
			responding to ping. Piper is down.	
			Paged ETA.	FL
2000			Virus active on network until	
			told otherwise by John Lekashman	AG
1933	Piper		Steve Prescott returned paged. He had me	
			check console. Piper is up. But did	
			~~got n~~ see messages:	
			NOTICE: ptalloc: Insufficient memory	
			to allocate 1 page - systems call failed.	FL
20:21	Piper	↑	Rebooted Piper per instructions from	
			Steve Prescott. Piper is responding to ping	FL
21:29	Piper	↓	Not responding to ping. Down.	
21:30	Piper		Paged ETA.	LK
21:32	Piper	↑	Piper responding to ping.	LK

DATE 11-06-88

page 1 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
0312	MSS	↑	after backups	[illegible]
0325			motd changed on Sto, Pra, Ame, Fred, Orv, uk27, HAN; unable to change others	[illegible]
0421	PIPER	↓	Timed Out on ping ETA paged	HY
0423	PIPER	↑	Came back up on ping.	H
0430	DBIU		Reset from 3:08	TH
0510	Navier	↑	after ded time	TH
0548	PIPER	↓	Timed out. ETA Paged	TH
0550	PIPER	↑	Back up	TH
1050	STOKES		Users experincing "memory" problems, "not enough space", "CPU limit exceeded	Ja
1055	STOKES		paged C. Burke, C. Burke responded suspects global CPU limit not corret, reboot STOKES, should reset limit	Ja
1058	STOKES	↓	Stokes rebooted to clear possible memory, CPU problems	[illegible]
1114	STOKES	↑	Stokes back up.	[illegible]
1120	Stokes		The reboot did not correct memory problem J. Branam paged	[illegible]
1125	Stokes	↓	Stokes rebooted once again to reinitialize quotas	[illegible]

DATE 11-06-88

page 2 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1155	Stokes	↑	Called J. Musch and	
			Bob Thurman About the	
			problem with memory. The	
			two reboots did not clear	
			the problem. A message was	
			left on Thurmans machine.	
			Musch said he would look	
			@ the problem from home	
			Branaum knows About the	
			problem NQS is not up	SK
12:20	Stokes		Bob Thurman & Jo Musch	
1225			J Lekashman called - he found no evidence	fo
			of virus problems	
1245	Stokes NQS		per Jim Branaum, NQS started	
12:55	Stokes		Musch called and said A work	
			Around for the limit problem	
			is to remove (move) the	
			/usr/local/etc/grplmt file. This	
			will give All users "nolimit"	
13:05	Stokes		moved the "/usr/local/etc/grplmt" file	
			to "/usr/local/etc/grplmt.copy" Stokes	

Continue ↓

DATE 1/6

page 3 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1305	Stokes		will be rebooted to initialize	
			quotas. All per J. Branam AS BY JOHNMUSH	SA
1312	LAN/LHC		LHC sites ~~that~~ need verification will be	
			done at 0800 by TONY Q on Monday.	
			Contact should be made by Storm or Quintaro	
			first to see if remote site is clean. Local	
			test with HAN will verify cleanliness. LHC	
			sites will then be connected to NAS	
1320			Local nets being started by Milo in 251.	RF
			Amelia will probably be busy sending	
			mail. Most workstations have sendmail	
			disabled. Forward files to WKS should be changed	
1330	WAN		Wide area nets & ArcLAN now on (MILO)	RF
1330	STOKES	↓	down to get CPU limits up	
1345	STOKES	↑	back up; CPU limits for all users of	
			"no limit"! Probable accounting failure;	
			leave note for Victor Lee	
1345	Navier		no kdld running; red on Snoopy; will	RF
			start after PASSWD changes	
1345	LAN		Riacs subnet now on.	SS
1333	Ame		ftp anonymous account disabled on Amelia per V Cheff	Ja

DATE 11/6

page 4 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1345	NAV		STARTED HDLD J. Branum	
1445	WKS		CURRENT WKS STATUS: ALL IRIS's, SUNS + 4D/60's are up + on network except: WA01-WA05 SUN210, SUN205, SUN105, FS05, WK01, WKD5, + EW01. FS06 IS DOWN W/ HARDWARE PROBS (WK00 WILL BE THE ONLY TRUSTED HOST FOR NOW). REST WILL BE BROUGHT UP BY 11:00 AM 11/	RF
1510	Snoopy		Disabled testing of HDLD For NAV-0 & NAV-2 Deamons do not appear to be up!	SM
1550	Amdahl		Don Phan will be a little late.	FL
1555	Adapter 70s		Per Dennis McKey - do~~e~~ not reset any hyperchannel ~~70~~ Adapter 70's series (70, 71, 72, 73). Please Notify Dennis Via the answering service (408) 947-5757.	FL
16:30	Meyer	↓	Meyer Down for dedicated time	Jm
1630	ORVILLE		Slow because name daemon not running therefore send-mail queue is growing. per Keith Thompson. Tried calling John Lekashman - NO answer.	FL
16:41	MUS	↓	MUS down for dedicated time	MW

DATE 11/6

page 5 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1730			Victor Lee called. Returning call from Steve Robinson. Told Victor Steve's call was probably related to Stokes "no limit" ~~gor~~ for Stokes Cpu limit	FL
1800	Navier	↓	Started 10-min shutdown for PM.	FL
1720	STOKES HSX	↓	Dont. Cant ping	GE
1723	STOKES HSX		Trying to bring up, Got error " WARNING: hsx.c: hsx 03051: device protocol error on open: dev = 1 proto = 1 ifconfig: ioctl (SIOCSIFADDR): Device busy." returned "HSX up", but could not ping it	GE
1725	STOKES HSX	↑	retried ~~bringing~~ HSX up. successful. can ping it	GE
1842	Meyer	↑	Up ~~aft~~ after Amdahl PM. Dien Phan installed new BUS & TAGG cables.	FL/GE
1843	MVS	↑	Up after Amdahl PM	
1843	MSS	↑	Up on ~~meyer &~~ MVS	FL
1853	MSS	↑	Up on meyer. Channel-to-Channel (CTC) ports e51-e53 & f51-f53 were attached to ssctst2. Had to Detach them & re-attached to meyer before MSS/meyer would come up	FL/GE

DATE 11/6 page 6 of 6

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
2015	A222-20	↓	After several attempts to reset, paged	
			Dennis McKey	GK
2020	A222 20		Dennis McKey return of page. Dennis	
			said Adapter 20 needs to be vary on VM2	
2045	VM2		Called George Navas. George said to	
	meyer	↓	"vary on bØØ-b3f" on VM2. Then bring	
	Mss	↓	meyer down and back up.	FL
2115	MEYER	↑	Back up Also Adapter 20 now works	GK
2118	MSS	↑	Restart on both MEYER and MVS sides	GK
2155	Navier	↑	Up after PM	FL
22:30	TAPE DRIVES		Cant vary on "900-906 to eithe VM1or2	Tm
			Paged Amdahl dispatch for Dien Phan	
2230			D. FUNG WILL BE ~ 1/2 hr late	FL
2330	Navier Stokes HSX.		Brought HSX up between navier	
			& Stokes by taking it down on	
			both sides, ifconfig ing the HSX	
			channels off, rerunning hyroute to them,	
			and bringing it back up on both	
			sides	TH
2340	TAPE DRIVES		BILL NUNN, AMDAHL FE, RETURNED CALL	
			-will send Dien out at 0800	TH

DATE 11/7

page 1 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
0030	900-90B		Re-initl'ed tape controlers -	
			Controler for 900-903 had error	
			light on. will now vary on	
			(and load tapes) on vm1, vm2 &	
			MVS. ~~Trouble call.~~ Amdahl	
			dispatch called to cancel trouble	
			call, but will leave a note for	
			Dien in morning	TH
0100	Meyer	↓	Not talking on hyper channel -	
			get 'network unreachable'	
			errors. Netshut / Netstart had	
			no effect. routing tables look	
			ok, but changed default routes -	
			no effect. ~~to~~ no one logged on	TH
0105	Meyer	↑	after reboot - still cannot access	
			hyperchannel	TH
0130	YMP	↓	Not responding to ping	TH
0132	YMP	↑	back	TH
0230	Nairev		Not talking to amelia, pam, etc - get	
			'no buffer space' took down HSX on	
			both sides and brought back up - ok now	TH

DATE 11/7/88

page 2 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT DESCRIPTION	IN
0300	Ame		lulah/news/lib is full; sent mail to R. Malm	
0300	hyp0-63		master cleared	TH
0530			Ever Completed	HT
0642			S. Clew will be in at 0745	
0638	Piper	↓	Piper is down, not seen	
0639	Piper		ETA paged	
0643	Piper		Murray returned call	
0647	Piper	↑	rebooted	
0645			LARC is reconnected per T. Quintana	
0745	Amdahl		Dein called in about tape drives	
			— told him they were init'ed	
			and are ok now	TH
0730	Meyer		Paged D. King about meyer's	
			continuing hyperchannel adapters	TH
0830	NQS		deleted "EKATERIN 32184.NAVIER	
			" EKATERIN 32165.NAVIER	
			" EKATERIN 25654.STOKES	
			" SINGH 32133.NAVIER(X) from [illegible]	JS
0925	LZ4		Problems staying enabled Jobs from 0800	
0930	VMIC		per Ernie VTFV1, PIE all, fixed up VMIC	
			needs IPL; will notify + start ~~shutdown~~	

DATE 11/7/88 page 3 of

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT DESCRIPTION	IN
0945	MSS	↓	for VM2 install	SS
0945	MEYER	↓	for VM2 install	SS
0950	SANDBOX	↓	Sandbox brought down by R. Henderson	KF
1000	3480	.	IBM came to install autoloaders; due to	SS
			previous outages + needed drives, postponed install	
			to at least Wednesday	
1005	VM2	↓	as above	
1009	VM2	↑	as above	
1015	VTAM		sync up being done by Bonnie	
	VTAM		still having probs, Bonnie checking it out	KF
1026	YMP	↓	not responding, can't rlogin/telnet called	~~[illegible]~~
			R Park who will notify B Thurman. YMP	
			presumed down	
1026	MEYER	↑	back up	KF
	MVS	↑	" " ; chan E50-E53 + F50-F53 were	KF
			attached to SSCTE2 instead of [illegible] for [illegible]	
1033	YMP	↑	back up per R. Popelka MVS	~~ETC~~
1035	VTAM	↑	back up per Bonnie Ballinger	KF
1045			NASJA is the old JA on	
			the CRAYS the new JA	
			is the standard 4.0 unicos JA AS PER	

Victor Lee. SR

DATE 11/7 page 4 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1045	MEYER/MFS		[illegible] hyperchannel still not working.	K
			Ethernet is OK. [illegible] looking w/ client to	
			determine problem range	
1130	CS/100	.	Note CS/100 can't status any	
			NASnet site, configuration problem	
			from 11/04/88. See list for	
			NASnet site that are up.	[illegible]
1130	Virus Status		Expect most distributed processing	
			to be back up in next 24 hrs.	
			Ames is still working on some of	
			their own systems Bldg 256 still	
			isolated.	[illegible]
1200	MEYER		UTS side looks OK; hardware prob suspected.	RF
	MFS		Joe M. tested port 20 + 27 (A222) + [illegible] that	
			data loss occurs on A222-20 (NAVAS + McKEY WILL	CH
1200	PIPER	⇓	missed pings (5X), called place to ETN; ETH reported	SC
1210	MEYER	↓	down by Joe, reboot to see if A222-20	RF
	MFS	↓	is OK	
1210	DBIU		reset from 1008	[illegible]
1220	MEYER	↑	back up	RF
	MFS	↑	" "	RF

DATE 11/7

page 5 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1210	ETA	↑	back up for [illegible]	JA
1226	MEYER	↓	hung on MSS start up; multiple boots	RF
	MSS	↓		
1230	LHC	.	all LHC sites now connected to NAS	AQ
1245	MEYER	↑	back up again; still no hyp chan	
1250	HSP B		Let workman into HSPB to put in cables	Ja
1300	MSS	↑	MSS back up + running	RF
	MEYER		altered /etc/NETSTART to start up hyp	RF
			chan properly. HY-CHAN OK TO MEYER NOW ON PING	
1320	A400-48		NSC has A400-48 to tighten cables	
			+ check internal cables (30 min).	Om
1330	MSS		MSS commands from Cray 2 timing out.	RF
			still can't reach meyer over HY-CHAN	
1405	meyer		Started inetd to clear [illegible]	
			problems; NETSTART did not start it up	
1440	PIPER		"NASOPS" will be installed on PIPER	
			tonight. New procedures, if PIPER	
			fails a ping, try rlogining or telneting	
			in. If this fails log it & call ETA.	
			If not log it as up + rlogin worked.	

DATE 11/07/88 page 6 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
1447	Wilbur		M. Foots will crash/reboot Wilbur at 1700	
			to set "root" password correctly	JS
1445	Prandtl	↓	~~Wilbur~~ crashed, reason unknown	JS
1500	Prandtl	↑	Prandtl is back up	SE
1506	WILBUR		ROOT PW set correctly - passwd rolled	RF
1516	PIPER	↓	PIPER IS DOWN, NOT SEEN (4X)	
			PAGED ETA	JS
1517	PIPER		CHANCELLOR RETURNED CALL	JS
1518	Prandtl	↓	Brought down by Don Seal because some	SE
			disk drives weren't attached	
1527	Prandtl	↑	Prandtl is back up	SE
1533	Piper	↑	Piper is back up.	
1530	PRINTING		IRIS WORKSTATIONS SHOULD BE ABLE TO	RF
			REMOTELY PRINT. SUN WORKSTATION WILL NOT	GL
			AS OF NOW DUE TO ~~H~~ S/W, EQUIP NOT INSTALLED	
1630	Piper		We now have nascps on Piper. Password	
			is not the same as regular nascps; it will	
			be put in find.pw on Prandtl.	SE
1802	YMP	↓	down for ded Time PM	
1845	DBW		Reset DBW - ~~from~~ Down since 15:47	FL

DATE 11/07/88 page 7 of ____

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	IN
19:10	MEYER	↓	Down for dedicated time per G. Nuvns	[illegible]
19:13	PRANDTL VM1	↓	Down for ded. time	GA
19:14	VM2	↓	Down for ded. time	GA
2140	CONVEX	.	CONVEX TAPE DRIVE IS BAD - NOT TOO MUCH	
			VACUUM.	FL
2258	YMP	↑	up after ded time	[illegible]
2315	NVS	↑	up after ded	HY
2320	VM1 Prandtl	↑	up from dedicated time	SP
2328	VM2 Meyer	↑	up " " "	SP

DATE 11/8/88

page 1 of

NAS/GE OPERATIONS LOG

TIME	EQUIP	RS	EVENT_DESCRIPTION	I
0300	MSS	↑	After running backups and dedicated time.	S
0710	Convex		Unable to do backup; drive broken	K
0610	WKS		Bendix called open pin on cable (No Horz.	DL
			movement on mouse) D. Lindstedt	
			Bendix was called last week on this!	
0130			Toby Harness left early, feeling	HY
			ill.	
0615	EREP		completed	HY
0700			Prandtl IBR's delayed until 5:25	SP
			due to Restores.	

NAS REMOTE SITES

SITE NAME	LOCATION
Allison Gas Turbine	Indianapolis, Indiana
Amtec	Bellevue, Washington
Boeing Airplane Company	Seattle, Washington
Center For Turbulence Research	Stanford, California
Computational Mechanics	Knoxville, Tennessee
Flow Research	Kent, Washington
General Dynamics	Fort Worth, Texas
Grumman	Bethpage, New York
Goddard Spaceflight Center	Greenbelt, Maryland
Johnson Space Center	Houston, Texas
Langley Research Center	Hampton, Virginia
Lewis Research Center	Cleveland, Ohio
Lockheed, California	Burbank, California
Lockheed, Georgia	Marietta, Georgia
Lockheed, Palo Alto	Palo Alto, California
Marquardt	Van Nuys, California
Marshall Spaceflight Center	Huntsville, Alabama
McDonnell Douglas, California	Long Beach, California
McDonnell Douglas, Missouri	Berkeley, Missouri
Northrop	Hawthorne, California
Redstone Arsenal	Huntsville, Alabama
Rocketdyne	Canoga Park, California
Rockwell	Thousand Oaks, California
Science Applications International	Wayne, Pennsylvania
United Technologies	East Harford, Connecticut
Vertol (Boeing)	Eddystone, Pennsylvania

Attach 7

STATUS OF NAS REMOTE SITES
6 November 1988, 13:00

SITE NAME	STATUS
Allison Gas Turbine	Clean
Amtec	Clean
Boeing Airplane Company	Notified
Center For Turbulence Research	Notified
Computational Mechanics	Clean
Flow Research	Clean
General Dynamics	Notified
Grumman	Notified
Goddard Spaceflight Center	Notified
Johnson Space Center	Notified
Langley Research Center	Notified
Lewis Research Center	Notified
Lockheed, California	Notified
Lockheed, Georgia	Clean
Lockheed, Palo Alto	No answer
Marquardt	Notified
Marshall Spaceflight Center	Notified
McDonnell Douglas, California	Clean
McDonnell Douglas, Missouri	Notified
Northrop	Clean
Redstone Arsenal	Notified
Rocketdyne	Notified
Rockwell	Notified
Science Applications International	Clean
United Technologies	Notified
Vertol (Boeing)	Notified

Hack 8

STATUS OF NAS REMOTE SITES
7 November 1988, 11:00

SITE NAME	STATUS
Allison Gas Turbine	Clean
Amtec	Connected at 09:50
Boeing Airplane Company	Connected at 10:10
Center For Turbulence Research	Notified
Computational Mechanics	Connected at 06:10
Flow Research	Connected at 10:05
General Dynamics	Connected at 09:30
Grumman	Notified
Goddard Spaceflight Center	Clean
Johnson Space Center	Notified
Langley Research Center	Connected at 06:45
Lewis Research Center	Connected at 10:35
Lockheed, California	Connected at 09:10
Lockheed, Georgia	Clean
Lockheed, Palo Alto	Notified
Marquardt	Connected at 10:00
Marshall Spaceflight Center	Notified
McDonnell Douglas, California	Connected at 08:30
McDonnell Douglas, Missouri	Connected at 06:35
Northrop	Connected at 08:50
Redstone Arsenal	Notified
Rocketdyne	Notified
Rockwell	Notified
Science Applications International	Connected at 06:20
United Technologies	Connected at 07:15
Vertol (Boeing)	Notified

NAS COMPUTER SYSTEMS

SYSTEM	DESCRIPTION
Cray Y-MP 8/32 (1 SSD, 2 IOSes)	8 processors, 32 MW, 1 Gflop
Cray-2 Supercomputer (Navier)	4 processors, 256 MW, 250 Mflop
Cray-2 Supercomputer (Stokes)	4 processors, 256 MW, 250 Mflop
Amdahl 5880 VM machine (Prandtl/Meyer)	2 processors, 48 MB, 280 Mips
Vax 11/780 (Amelia)	1 processor, 1 Mip
Vax 11/780 (Orville)	1 processor, 1 Mip
Vax 11/780 (Wilbur)	1 processor, 1 Mip
Vax 11/780 (Fred)	1 processor, 1 Mip
Convex C-1/XP Super Mini	1 processor
Alliant FX-8 Super Mini	4 processors
Connection Machine	32,000 processors
Vax 8350 (Gottfried)	front end to Connection Machine
Lisp machine	connected to Connection Machine
ETA-10Q (Piper)	1 processor, 64 MW
DN 3000 (Apollo)	front end for ETA
microVax II (Snoopy)	Network control
Stellar Wks	Superworkstation
SGI IRIS 2500 T	25 IRIS workstations
SGI IRIS 3030	17 IRIS workstations
SGI 4D/60	16 IRIS engineering workstations
Sun 3/260	6 Sun workstations
Sun 3/50	11 Sun workstations
Sun 3/60	1 Sun workstation
NSC Adaptors	HYPERchannel connections
Vitalinks	10 long distance connections
Ethernet	119 Ethernet connections

			IRIS Workstations		
System	Type	Ser #	Location (CPU/Console)	Contact	Phone
wk00 chewbaka	3030	1767	RNS 258, Rm 107/125	Van Cleef, Bob	x44366
wk01	2500T	330	RFT 202A, Rm 118/111	Keefe, Lawrence	x45361
wk02	2500T	426	RFA 258, Rm 107/120	Gundy-Burlet, Karen	x44475
wk03	2500T	427	RFT 202A, Rm 118/113	Wray, Allen	x46066
wk04	2500T	428	RFT 202A, Rm 118/215	Maksymiuk, Catherine	x44737
● wk05 dogstar	2500T	998	RFT 202A, Rm 118/211C	Pulliam, Tom	x46417
wk06	2500T	367	RFA 258, Rm 107/117	Lawrence, Scott	x44050
wk07	2500T	451	RFT 202A, Rm 118/216B	Mehta, Unmeel	x45548
wk08	2500T	361	RFT 202A, Rm 118/109	Moser, Bob	x44733
wk09	2500T	449	RFA 258, Rm 107/118	Chaderjian, Neal	x44472
wk10	2500T	453	RFT 202A, Rm 118/216C	Barth, Tim	x46740
wk11 reptile	2500T	421	RFA 258, Rm 107/124-8	Cordova, J.	x44484
wk12	2500T	448	RFA 258, Rm 107/124-4	Rogers, Stewart	x44481
wk13	2500T	450	RFA 258, Rm 107/105	Guruswamy, P.	x46329
wk14	2500T	452	RFT 202A, Rm 118/114A	Kim, Jon	x45867
wk15	2500T	366	RFA 258, Rm 107/102	Edwards, T.	x44465
wk16	2500T	429	RFA 258, Rm 107/124-2	Srinivasan, G.	x44478
wk17	2500T	331	RFT 202A, Rm 118/215	Merriam, Marshall	x44737
● wk18	2500T	328	RFT 202A, Rm 118/209	Jespersen, Dennis	x46742
wk19 rotor	3030	2045	RFW 258, Rm 143/134-18	Kelaita, P.	x44453
wk20 igors	3030	2106	RFA 258, Rm 107/119	Baeder, Jim	x44473
wk21 perseus	3030	2165	RFA 258, Rm 107/115	Van Dalsem, Bill	x44469
wk22 jls	3030	2164	RFA 258, Rm 107/124-14	Schiff, Lew	x44467
wk23	3030	2447	RFW 258, Rm 107/126	Smith, Merritt	x45194
wk24	3030	2810	RFA 258, Rm 143/134-14	Jettmar, Uwe	x44493
wk25	3130	3157	RFA 258, Rm 143/134-22	Meakin, Bob	x44456
● wk26	3130	3156	RNS 258, Rm 143/134-11	Veum, Gary	x44373
wk27 lando	3130	3155	RFA 258, Rm 257/247	Van Cleef, Bob	x44366
wk28	3130	4337	RFA 258, Rm 107/124-3	Schiff/Steger	
wk29	3130	4345	RFA 258, Rm 143/134-15	Green, Mike	x46447
wk30	3130	4335	RFA 202A, Rm 118/	Rogers, Mike	4732
● wk31 ect	2500T	332	RCR 258, Rm 205/	Hultquist, Jeff	x44970
● wk32 pegasus	2500T		RIACS 258, rm 257/	Kirble, Phil	x46363

● – Modified – Application Development (MAD)

wk00–wk32 – Production systems

NAS Workstations

10/1/88

IRIS Development Workstations

	System	Type	Ser #	Location (CPU/Console)	Contact	Phone
●	wkd0 garuda	3130	2952	RND 258, Rm 205/219	Swisshelm, Julie	x44430
●	wkd1 annie	2500T	368	RND 258, Rm 205/208	Choi, Diana	x44406
*	wkd2 igor	2500T	1047	RND 258, Rm 205/201	Kehoe, Bill	x44318
●	wkd3 rodan	2500T	329	RND 258, Rm 205/200	Levit, Creon	x44403
*	wkd4 han solo	2500T	333	RNS 258, Rm 230/227	Van Cleef, Bob	x44366
*	wkd5 darth	4D60/GT	11265	RND 258 Rm 200/200	Tristram, Dave	x44404
1	wkd6 stellar			RND 258, Rm 125	Vaziri, Arsi	x44799
2	wkd7 eclipse			RND 258, Rm 204	Lasinski, Tom	x44405

● – Modified – Application Development (MAD)
* – System Applications Development (SAD)
1 – Stellar workstation
2 – SGI Eclipse *beta* test unit – on loan from SGI

wkd0—wkd9 – Development systems

Engineering Workstations

	System	Type	Ser #	Loc. (CPU/Console)	Contact	Phone
	ew00	4D60	12482	RNS 258, Rm 257/257	Crabb, Michele	x44365
	ew01	4D60	12690	RNS 258, Rm 143/134-1	Nonomura, Ken	x44429
●	ew02	4D60G	12686	RND 258, Rm 257/236	Yamasaki, Mike	x44412
●	ew03 gigantor	4D60	12682	RND 258, Rm 257/232-27	Hahn, Jonathan	x44360
●	ew04 lemming	4D60	12689	RND 258, Rm 205/219	Fouts, Marty	x44408
●	ew05 bryan	4D60	12687	RND 258, Rm 257/232-28	Henderson, Bob	x44361
●	ew06	4D60	12684	RND 258, Rm 257/232-26	Poston, Lloyd	x44307
●	ew07	4D60	12691	RND 258, Rm 257/232-24	Pew, John	x44312
●	ew08 rene	4D60	12681	RND 258, Rm 257/232-23	Bierbaum, Neal	x44356
●	ew09	4D60G	12680	RND 258, Rm 205/203	Raible, Eric	x44320
*	ew10	4D60	12688	RND 258, Rm 205/201	Thompson, Keith	x44319
●	ew11	4D60	12679	RND 258, Rm 205/215	Bailey, David	x44410
●	ew12	4D60	12685	RND 258, Rm 205/208	Miya, Eugene	44407

● – Modified – Application Development (MAD)
* – System Applications Development (SAD)

ew00 – File Server
ew01– ew99 – Engineering Workstations

NAS Workstations

10/1/88

Sun Workstations

	System	Type	Ser # (hw/sw)	Location (CPU)	Contact	Phone
°	sun100 **wiley**	1/150	C181	RND 258, Rm 235	Ticknor, Paul	x44354
°	sun101 **lotus**	3/260	742E0178	RND 205, Rm 203	Lekashman, John	x44359
°	sun102 **bamboo**	3/260	742E0355	RND 258, Rm 235	Lekashman, John	x44359
°	sun103 **luke**	3/60C/G	740F7515	RNS 258, Rm 154	Bridges, Mike	x44306
°	sun104 **panda**	3/50M	742F3732	RNS 258, Rm 134-10	Marshall, Tony	x44372
	sun105 **bmw**	3/50M	744F1175	RNS 258, Rm 134-12	Veum, Gary	x44373
	sun106 **audrie**	3/260	824E0800	RNS 258, Rm 231	Musch, John	x44328
	sun107 **chymp**	3/260	824E0802	RNS 258, Rm 231	Thurman, Bob	x44330
	sun108 **seymour**	3/260	824E0828	RNS 258, Rm 230B	Thurman, Bob	x44330
	sun201 **crayon**	3/260C	744E0986	RNS 258, Rm 230	Stutes, Earl	x44305
	sun202 **garg**	3/50M	744F1114	RNS 258, Rm 156	Van Cleef, Bob	x44366
	sun203 **zhan**	3/50M	742F6603	RNS 258, Rm 134-2	Crabb, Michele	x44365
	sun204 **leo**	3/50M	744F1115	RF 258, Rm 100	Steger, Joe	x46459
	sun205	3/50M	815F1056	RNS 258, Rm 134-4	Lee, Victor	x44367
	sun206 **lindberg**	3/50M	815F1057	RNS 258, Rm 141	Branaum, Jim	x44311
	sun207 **corrigan**	3/50M	815F1052	RNS 258, Rm 141	Stutes, Earl	x44305
	sun208	3/50M	815F1051	RNS 258, Rm 141	Simonzi, Ralph	x44357
	sun209 **smaug**	3/50M	815F1049	RNS 258, Rm 232-1	Storm, Steve	x44334
	sun210 **aspin**	3/50M	815F0966	RNS 258, Rm 134-5	Anaya, Maria	x44429
	fs01 **sun200**	3/280S	745E0085	RNS 258, Rm143	Crabb, Michele	x44365
	fs02	3/280S	829E0888	RNS 258, Rm 107	Crabb, Michele	x44365
	fs03	3/280S	829E0885	RNS 258, Rm 257	Crabb, Michele	x44365
	fs04	3/280S	829E0879	RNS 258, Rm 205	Crabb, Michele	x44365
	fs05	3/280S	831E0871	RNS 202A, Rm 118A	Crabb, Michele	x44365
	fs06	3/280S	829E0882	RNS 258, Rm 230	Crabb, Michele	x44365

● – Modified – Application Development (MAD)
* – System Applications Development (SAD)
° – Hardware Only Supported, Engineering Development (HOSED)

sun100–199 – Development systems
sun200–299 – Production systems

Auxiliary Processing Center Workstations

System	Type	Ser.No.	Location (CPU/Console)	Contact	Phone
apc1	4D60G	12683	RND 258, Rm 131/131	Mahon, George	x44325
apc2	4D60G	12719	RND 258, Rm 131/131	Mahon, George	x44325
apc3	3/260HM	818E0202	RND 258, Rm 131/131	Mahon, George	x44325

apc1—apc3 — Auxiliary Procession Center

Non-NAS Workstations that are supported

	System	Type	Ser.No.	Location (CPU/Console)	Contact	Phone
°	ra-iris	2500T	365	RAO 227, Rm 118	Hermstad, Dexter	x45857
●	**wao1 ronnie**	2400T	1039	RFW 258, Rm 125/125	Merritt, Fergus	x44451
1	**wao2 nancy**	3030	1854	RFW 258, Rm 143/142	Merritt, Fergus	x44451
●	**wao3 bonzo**	3130	3261	RFW 258, Rm 143/138	Merritt, Fergus	x44451
●	**wao4 lucky**	3130	3940	RFW 258, Rm 125/125	Merritt, Fergus	x44451

● — Modified — Application Development (MAD)

° — Hardware Only Supported, Engineering Development (HOSED)

1 — Geometry Partners System — Owned by SGI

wao1—wao4 — Workstation Applications Office

Non-NAS Workstations that are NOT supported
Listed for reference only

System	Type	Ser.No.	Location (CPU/Console)	Contact	Phone
cat	3030	1549	RFT 230, Rm 135	Borja, Adrian	x44284
orac	3030		RFT 230, Rm 135	Borja, Adrian	x44284
cyclops	3030	2814	FFF 247, Rm 113	Ross, Jim	x46722
				Bennett, Mark	x45037
	3030	2820	YF 215, Rm 215	Purcell, Tim	x46062
	3030		RFE 229, Rm 134	Pegot, Eva	x46254
	2500T		FFR 221	Stremel, Paul	x46714

ACRONYMS AND TERMINOLOGY

ARCLAN	Ames Research Center Local Area Network (Ethernet)
ARPAnet	Advanced Research Projects Agency Network
BSD	Berkeley Standard Derivitive (A version of Unix)
CPU	central processing unit
daemon	server process that emerges to do a process when it is needed, and then disappears.
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
EDN	Network Development Branch
fgets	gets a string from a stream
finger	user information lookup program
fingerd	finger daemon - remote user information server
ftps	file transfer protocol server
gets(s)	gets reads a string s from the standard input stream
hosts.equiv	contains a list of remote hosts to share account names
I/O	input/output
inet	Internet protocol family
inetd	internet "superserver"
iotcl	input/output control device
IP	internet protocol
IRIS	Integrated Raster Imaging System
LHCS	Long Haul Communications Subsystem
MIG	Managers' Interface Group
MILnet	military portion of ARPAnet
motd	message of the day
MSS	Mass Storage Subsystem
NAS	Numerical Aerodynamic Simulation
netstat	show network status
NIC	Network Information Center
NOSC	Naval Ocean Systems Center
NSFnet	National Science Foundation network
rc	command script for auto-reboot and daemons
RFP	request for proposal
.rhosts	file of remote hosts with which a computer shares its accounts
RIACS	Research Institute for Advanced Computer Science
RND	Development Branch at NAS
RNS	Computational Services Branch at NAS
rsh	remote shell
rshd	remote shell server
sendmail	internetwork mail router
setuid	set user id
sh	shell files
TCP	Transmission Control Protocol (ARPAnet)
Trojan Horse	an illegal program hidden in a legal program in order to attack systems and applications software from within.
UTS	Universal Timesharing System
VAX	Virtual Address Extension (DEC 32-bit computer)
virus	program designed to "infect" other programs by modifying them to include a copy of itself.
worm	program that can run by itself and propogate itself to other machines

INFORMATION AND COMMUNICATIONS SYSTEMS DIVISION

REPORT

ON

INTERNET SENDMAIL VIRUS

EVENTS RELATED TO DETECTION, ERADICATION, AND PREVENTION

November 28, 1988

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
AMES RESEARCH CENTER
MOFFETT FIELD, CALIFORNIA 94035

Executive Summary

On Wednesday November 2 the well publicized Internet Virus was discovered at the Ames Research Center. This report catalogs the events that took place at the Center to verify the existence of the virus, to eradicate it, and to protect the systems at the Center from further attacks.

Ames was disconnected from the Internet at approximately 1 a.m. November 3, 1988. Fixes to the approximately 150 affected systems were completed and re-connection to the Internet was accomplished at approximately 2 p.m. on Sunday November 6.

INTRODUCTION

Over the past several years an extensive nationwide computer network has been developed, connecting government, education, and commercial facilities into a universally accessible address space. The network, known as Internet, is a logic connection of several networks such as NASA Science Internet (NSI), National Science Foundation Network (NSFNet), BITNET, etc. Each of these physical networks are "bridged" enabling users on each of these networks to communicate with systems on any of the other networks. In more recent years international networks have been connected to the Internet system.

Ames' involvement in the Internet network has been extensive. Ames has developed, operates, and maintains the NASA Science Internet (NSI); is a host on the MILNET/APRANET network; and operates the NASA "name server", the computer system which maintains the detailed computer addresses of Internet for NASA.

Ames' contacts with network managers include sites at universities, governmental agencies, and industry throughout the country.

DETECTION AND ISOLATION ACTIVITIES

On November 2, 1988 at approximately 9 p.m., Milo Medin, a Sterling Software employee assigned to support the Ames' Network Development Branch (Code EDN), was contacted by Peter Yee of the University of California at Berkeley (UCB) and advised that a computer virus had been detected on several machines attached to the Internet System. At approximately the same time, John Lekashman of the NAS Systems Development Branch (Code RND) was also informed that something was amiss with one of the NAS machines.

Both gentlemen, in concert with each other, immediately proceeded to determine which and to what extent machines at the Center were affected. John interrogated the machines under control of the NAS Systems Division, while Milo attempted to investigate the state of the remaining machines at the Center.

The virus was detected to be active on several machines at the Center including Aurora in Building N239 and the NORAD name server in N254 and present, though dormant, on other machines such as Orion in Building N233. At 11 p.m., UCB provided a more detailed description of the virus and how it entered and effected the machines. With that information Milo and John began repairing code on the machines under their control. Milo contacted (both electronically and by phone where possible) system managers at Ames as well as those JPL, Goddard, and Marshall and proceeded to disconnect NASA sites from the national network by command from Ames. At 1 a.m. on November 3, John and Milo, with the concurrence of NAS management, completed the isolation of Ames from the Internet system.

DETERMINATION OF THE EXTENT OF THE PROBLEM

At 9:30 a.m. the following morning (11/3), Ron Bailey, Acting Director of Aerophysics, called a meeting with representatives of Code RC, Code RN, and Code ED as well as Security and Public Affairs to discuss the goings-on of the previous 12 hours and to develop an action plan to assess the damage and return the Center to a healthy and normally functioning condition. John and Milo related the events of the past day and the following actions were assigned.

1. Code RN would install the final patches provided by UCB on all systems at the NAS facility. They would then open up one test system and to determine if it would be infected without the patch and remain clean after the virus was again removed and the patch was installed. (In the final analysis this was not done in exactly this manner, but rather the NASA name server, NORAD, was reconnected to the Internet and reinfected, the link to Internet was then again disconnected, and the link from NORAD to NAS was made to confirm that the NAS machines were, in fact, properly protected.

2. ED would attempt to notify over the network all system managers at Ames. This would include advising all known users on the Ames TCP/IP network and attempting to locate other "unknown" users to advise them of the problem

and the patches which should be installed to prevent the problem from reoccurring.

There was also discussion regarding the shutting down of ARCLAN, but this was dismissed as not having any benefit.

A report back to Ron Bailey on the plans was due by the end of the day and was provided by both organizations.

ED conducted several internal meetings to identify tasks and responsibilities. Milo then sent out over the network a message notifying the system managers of the virus's presence and of the necessary fixes to be put into place. The managers were asked to call Network Control Center (NCC), Bendix's Trouble Desk, to advise the division that the fixes had been put into place, which systems had been infected, and who were the system managers, their mail stop, and phone numbers which could be used in the future for notification.

The notice was sent onto the network Thursday afternoon (11/3) and Bendix manned the trouble desk until 9 p.m. to provide extended coverage for system manager responses. Two calls were received that evening. An additional six calls were received the following morning covering approximately 30 systems at the Center. At a Friday noon meeting, a three-pronged effort was set to determine the current state of systems at Ames.

A calling campaign was begun by the NCC to known system managers who had not yet responded. Secondly, a small program had been developed by Steve Schoch (Code EDN) to query each known system on the Ames network to determine if the patch to the SENDMAIL program had been made. This would not check the clearing of the .rhost table which was also recommended. Finally, Warren Van Camp set into place a monitoring program which would look for communication on the network for systems whose Ethernet address was not known to the division. If found, these systems would be added to the list that Steve Schoch was querying. All parties were to report back at day's end to determine what actions should take place over the weekend.

At 3:30 p.m. the parties reconvened and decided that if NAS were ready to reattach to the rest of the country, ED would connect the entire Center to the Internet. It was felt that the virus was still alive in the network but that systems at Ames which could be infected were and those that had received the patch were immune. Further, while some systems at Ames might still be spreading the virus, other systems which might be infected would be attacked whether or not the Ames systems were attached or not.

At approximately 2 p.m. Sunday afternoon, NAS advised Milo that they were ready to reestablish communication with the outside world and the connection to the national network was reopened.

The other NASA site managers were contacted and the networks reconnected to the Internet when properly protected.

COST IMPACT

It is estimated that approximately 200 man-hours of ED time was spent dealing with the virus and its eradication. These included both Government and contractor efforts. Approximately two-thirds of this time was spent by Milo and his associates in Sterling. Burdened these costs are estimated at $50 per hour.

In addition to these costs, an indeterminate cost was incurred as a result of the loss of computer availability due to the virus, and the loss incurred by the inability of personnel to communicate electronically to other sites and systems. These costs can not be calculated.

MID-RANGE ACTION ITEMS AND RECOMMENDATIONS

Two actions are seen as vital for maintaining the integrity of systems at Ames and yet providing the functionality required by the user.

First, a known bug in the FTP module should be repaired on all systems as soon as feasible. While this bug has absolutely nothing to do with the SENDMAIL virus, it is yet another known path for entry into the network which must be closed. Milo has made this change on the NSI machines as well as the NORAD name server. No formal action other than this has taken place to our knowledge.

Second, a more "usable" fix for .rhost must be developed and implemented. The current fix disables most of the .rhost capabilities which enable easy file sharing and access by the users. If a solution, which enables controlled access for authorized users and yet provides the necessary protections, is not implemented, there is a feeling that the clamor from users will force system managers to re-enable this facility.

No authority for these actions has yet been given and thus they remain incomplete at this time.

LONG RANGE ACTION ITEMS AND RECOMMENDATIONS

The primary long range action and recommendation is to establish a structure within Ames to deal with future events such as these. In particular, some authority for managing the Centerwide network must be given so that configuration management of the network is clearly defined and assigned, and that system managers are made aware and accountable as they attach to the network. This will enable the "network manager" to ensure that systems are kept current, that managers are notified when viruses are detected, and that there is a coherent approach to managing systems which are on the network. The most likely candidate for this authority is Code ED, as they are responsible for the operation of the networks and typically (though not exclusively) are the organization which install new systems onto the networks.