THE "FATHER CHRISTMAS WORM"

by

James L. Green
National Space Science Data Center
Goddard Space Flight Center
Greenbelt, MD 20771

and

Patricia L. Sisson
SPAN Security Manager
Science Applications Research
Lanham, Maryland 20706

June 1989
Published in the 12th National Computer Security Conference Proceedings

ABSTRACT

Three days before Christmas 1988, a computer worm was released on a very large international DECnet network. The worm reproduced itself and was received on an estimated 6,000 computer nodes worldwide. However, only a small percentage of these nodes actually executed the program. The computers that successfully ran the program would try to propagate the worm to other computer nodes.

The worm was released onto the DECnet Internet from a computer at a university in Switzerland. Within 10 minutes after it was released, the worm was detected on the Space Physics Analysis Network, or SPAN, which is NASA's largest space and Earth science network. Once the source program for the worm was captured, a procedural cure, using existing functionality of the computer operating systems, was quickly devised and distributed. A combination of existing computer security measures, the quick and accurate procedures devised to stop copies of the worm from executing, and the network itself, were used to rapidly provide the cure. These were the main reasons why the worm executed on such a small percentage of nodes.

The purpose behind the worm was to send an electronic mail message to all users on the computer system running the worm. The message was a Christmas greeting and was signed "Father Christmas." This paper presents an overview of the analysis of the events concerning the worm based on an investigation that was made by the SPAN Security Team and provides some insight into future security measures that will be taken to handle computer worms and viruses that may hit similar networks in the future.

INTRODUCTION

The Space Physics Analysis Network, or SPAN [1], has been an extremely reliable international scientific computer network that has become a major element in NASA's quick reaction capability for supporting many major NASA missions over an eight-year period [2]. Major features of SPAN are its ease of use, efficiency, and availability to scientists conducting research in scientific disciplines such as astronomy, astrophysics, climate, Earth, ocean, planetary, life, and solar terrestrial science.

Currently, SPAN ties together well over 2,800 computers at NASA centers, other government agencies, private companies, and universities in the United States, with extensions to the European Space Agency's E-SPAN network. SPAN utilizes computer-to-computer communications (DECnet protocol) allowing mail, binary file transfer, and remote log-on capability. The majority of the computers connected to the network are VAX machines running the VMS operating system. SPAN is managed by the National Space Science Data Center (NSSDC), located at NASA's Goddard Space Fight Center (GSFC).

SPAN has interconnections with several national and international wide area networks such as HEPNET, INFN, THEnet, DAN, GEONET, UARSnet, and ASTRONET. All these networks cooperatively manage unique computer DECnet addresses. The nodes from all these networks then form one transparent worldwide network called the DECnet Internet. The combined total number of computers reachable over the DECnet Internet is about 12,000. To the user, the DECnet Internet operates like one "easy-to-use" network. The DECnet Internet, on one hand, has solved the problem of transparency between computers regardless of what DECnet network they are connected to. On the other hand, the DECnet Internet provides the connectivity to make one network's security problem everyone's concern.

On December 22, 1988, at approximately 17:00 EST (eastern standard time), a computer worm was discovered on SPAN. This worm has been affectionately called the "Father Christmas Worm." A computer worm is a program that is self-contained and has the ability to propagate itself across a computer network to any idle machine. Unlike a virus, a worm does not modify another program. In the case of the Father Christmas Worm, virtually any computer on the DECnet Internet could have received a copy of the program. However, an individual computer may not have the system software configuration that would enable it to execute the program (because of the implementation of certain security precautions).

The purpose of this paper is to provide an overview analysis of the events concerning the Father Christmas Worm, based on an investigation made by the SPAN Security Team. From this investigation it has been determined that the worm was released from a computer (node number 20597::) at a university in Switzerland. Much of this analysis would not have been possible without the extensive help and assistance of the system manager of node 20597::.

The Father Christmas Worm was designed to travel quickly. Estimates are that it was copied to over 6,000 computer nodes. However, it is believed to have executed on only a fraction of those computers.

HOW THE WORM WORKED

The worm program was named HI.COM. The COM file type in VAX/VMS signifies a command file and is usually written in the DEC command language (DCL). DCL provides a user with access to operating- and network-level system functions on a local or a remote host.

Figure 1 provides a graphic overview of how the worm propagated and executed on other nodes. During execution of the worm, Node A transferred the worm file (HI.COM) to Node B. Node B was determined by a section of code in the worm program that randomly generated node numbers and then checked to see if the node was reachable. Once the transfer of the program was complete and Node B had the worm, Node A then would try to direct Node B to execute the HI.COM program.

So long as the worm was executing, it would continue to search out randomly reachable computers and try to propagate itself. On the DECnet Internet, separate blocks of DECnet addresses are allocated to individual wide area networks that are not confined to geographic regions. The use of randomly generated node numbers by the worm program would ensure a worldwide distribution across many networks, which would increase its survivability.

Node A would try to execute the worm on Node B by one of the following two methods:

- TASK Object 0 - If a system level program, called TASK Object 0, is installed in a VAX/VMS computer, it will accept and execute commands from another computer. In other words, TASK Object 0 allows task-to-task jobs to be run between two computer systems. In the case of the Father Christmas Worm, nodes that were following the SPAN security guidelines had TASK Object 0 disabled and were not able to execute the HI.COM file. In addition, nodes that had disabled TASK Object 0 would also not propagate the worm.

- Username/Password Combination - Another way to direct a remote node to execute a program (in this case HI.COM) is by providing a legitimate username/password combination for verification by the remote node. The Father Christmas Worm also tried a username/password combination of DECNET/DECNET. This combination of username/password has strongly been discouraged from use in documentation by the Digital Equipment Corporation (DEC) and in the SPAN Security Policy and Guidelines document [3].

In the example shown in Figure 1, Node B had TASK Object 0 installed. Node A then directed Node B to load HI.COM in memory and, disguising it under the process name MAIL_178DC, begin execution. The renaming of the process from HI to MAIL_178DC was done to hide the fact that a foreign program was executing. Mail processes execute quite frequently on these computer nodes and are easily missed by a system manager monitoring the system. Once executing on Node B, the worm deleted the file HI.COM that was stored on the disk, once again covering its tracks. Next, the worm mailed Node B's welcome banner to the remote node/account 20597::PHSOLIDE in Switzerland. This action provided the initiator of the worm a record of the nodes that were able to execute the worm program. However, there is no accurate record of the nodes that received a copy of the worm but did not execute it.

The MAIL_178DC program also went through a series of time checks looking for 1988-12-24-00:00 on the computer clock. If the actual time did not match the Christmas Eve time, the worm randomly generated a new computer node number (Node C in Figure 1). If Node C was operationally available over the network, then the Node B worm networked the HI.COM file from its memory to the new Node C and asked Node C to execute the program. The cycle then started all over again.

If the system clock time on Node B (or any node executing the worm) was greater than 1988-12-24-00:00, the worm created a listing of all the authorized users on that system and sent a Christmas greeting to all those users. The Christmas greeting message is shown Figure 2. It is signed by "Father Christmas." After sending out the Christmas mail message, the worm then deleted the user list it created and stopped execution.

WORM EVENT TIMELINE

On December 22, 1988, at 16:52 EST, the Father Christmas Worm was released from node 20597:: onto the worldwide DECnet Internet. The worm was first noticed at GSFC by John McMahon, systems manager of SPAN node CSDR, at approximately 17:00 EST, some 10 minutes after it had been released. After notifying SPAN management and the NASA Science Internet Project Office (NSIPO), John also contacted GSFC security to register the unauthorized access to U.S. Government computers. The worm command procedure HI.COM was captured at GSFC, as it had been at several other locations throughout the network, and the task of analyzing it began.

The SPAN Security Team sent messages to all SPAN NASA center managers warning them about the worm and what action to take to stop it. The SPAN NASA center managers are responsible for distributing warnings to the remote SPAN sites that are directly connected to them. Notice was also sent to HEPNET and THEnet representatives.

NASA personnel at the Jet Propulsion Laboratory sent out a warning mail message to 20597::SYSTEM on December 22, 1988, at 23:30 EST. The warning stated that the running of an automated command procedure, like HI.COM, was not permitted on SPAN. This message was received but not read, since it was very early in the morning in Switzerland and 20597:: was running unattended, which is quite common.

The PHSOLIDE account (where the worm started) was again logged into on December 23, 1988, from 1:58-2:23 EST. During this time, all the mail messages containing the system banners from the systems which successfully executed the worm were read and deleted.

The DECnet Internet line linking 20597:: to the rest of the world was disconnected on December 23, 1988, at approximately 03:41 EST. This link was scheduled to go down for an upgrade to the circuit. The action had nothing to do with the worm, but it did isolate an active worm on the large local area network at the university in Switzerland, where it continued to propagate to the local university nodes (see next section).

During the early course of trying to stop the worm, several network systems personnel, on their own initiative, issued procedural patches or cures for the worm. It is important to note that, unlike some virus situations, no vaccine software was necessary; a tightening up of existing computer systems security features is all that was needed to prevent a node from executing the Father Christmas Worm. The patches distributed were easy to describe and were issued by, for example, SPAN, HEPNET, DCA, and the San Diego Supercomputer Center personnel. The basic elements of all the procedural patches were:

a) Delete/Disable TASK Object 0
b) Stop Process MAIL_178DC
c) Delete all copies of HI.COM

Many of these patches went out on mailing distribution lists, such as VIRUS-L over ARPANET (a TCP/IP network). The Father Christmas Worm itself was also distributed to everyone on the VIRUS-L mailing list (by person or persons unknown to us). By the end of December 23, the Father Christmas Worm was virtually stopped on the DECnet Internet. In general, procedural patches were reasonably good and provided necessary protection against the Father Christmas Worm.

Within several days after the worm incident, the SPAN Security Team received full cooperation from the systems manager of node 20597::. The systems manager supplied the team with detailed logs and accounting records from his system. In February, a detailed report about the Father Christmas Worm was completed by the SPAN Security Team and was turned over to the appropriate authorities.

RESULTS OF THE INVESTIGATION

After carefully reviewing all of the log-in records to the PHSOLIDE account in conjunction with the system manager of 20597::, it was concluded that a user coming through a particular terminal server released the worm program. The terminal server accesses could have come from one building on the campus or from existing dial-in modems. The director of the university where node 20597:: is located has had every authorized user of the PHSOLIDE account (15 such users) sign a non-involvement statement. This affidavit stated that these users were not responsible for the creation of HI.COM nor were they responsible for the propagation of the worm onto the network. This action leads the SPAN Security Team to the conclusion that the account had been compromised by an unknown individual. This conclusion is not too difficult to realize, since the password on the account was the same as the username.

The accounting records also show that on December 23, from 1:58-2:23 EST, the PHSOLIDE account was logged into again via the terminal server. Once logged on, this user read and deleted all the computer system banners from the nodes that returned this information to the 20957::PHSOLIDE account over the eight-hour period after the worm was released. Even though the actual banners had been deleted, the network transaction files revealed that 79 nodes sent their banners to the Switzerland computer. Of the 79, only 27 of these nodes were on SPAN.

Within an hour after the intruder collected the banners, then deleted them to cover his tracks, the DECnet line linking this computer to the rest of the DECnet Internet was disconnected for a scheduled maintenance. At this time the worm was still running on node 20957:: and continued to randomly select new nodes to propagate to. However, the only nodes available to this active worm were connected to the local area network at the university. During the next eight hours, of the 610 nodes on the local university network, the worm executed on 46 computers 90 times, with 15 computer nodes executing multiple versions of the program.

CLEANUP ACTIVITIES

A follow-up investigation by the SPAN Security Team several days after the worm was released revealed that over three-quarters of the known nodes (79) that previously executed the worm still had TASK Object 0 accessible as before. If needed, TASK Object 0 performs an important function by easily allowing the sharing of peripherals in a local environment. It was obvious that the deletion of TASK Object 0 from the operating system was not a permanent solution to a potential security problem. Since then, the SPAN Security Team has provided these nodes with several alternatives from which to chose. These procedures are outlined in a new release of the SPAN Security Policy, Standards, and Guidelines [3] document.

At the university in Switzerland where the worm was initially released, a report was written and distributed campus-wide to alert the systems managers of the security problems they needed to address. Below is a list of the things the systems manager of node 20597:: insisted would be done campus-wide in addition to their existing security procedures.

a) There would be no multi-user accounts
b) Passwords would be required for dial-in access (through modems)
c) There would be a restricted user list for dial-in access
d) Additional accounting information would be required for terminal server access
e) Certain Username/Password combinations would not be allowed
f) A secure solution for providing TASK Object 0 program functionality would be implemented

It is important to point out that, in addition to the above, the first and most important practice in providing a rudimentary level of computer security rests with users, by their choice of passwords. Strict password control should be of prime importance for everyone on a computer system and its associated networks. For SPAN nodes, a new software audit system is available that will provide the system manager with tools to rapidly identify many other security weaknesses in the system in addition to the ones described above (send mail to NCF::Sisson for further details).

CONCLUSIONS

The Father Christmas Worm has over 150 lines of non-trivial control language code demonstrating a reasonable understanding of VAX/VMS and the DECnet protocol implementation on DECnet networks. It is obvious from the analysis of this event that the individual who released the Father Christmas Worm realized what he or she was doing and carefully returned again to the compromised node to collect information (system banners) indicating the extent of the worm on the DECnet Internet. It is also obvious that the perpetrator expected a large number of computers to receive and execute the worm, since the worm was released during the Christmas holiday season when there would have been the best chance of a worm executing on unattended VAX machines. In addition, it is typically held by computer hacker groups who make a habit of compromising the integrity of computer systems that computer systems managers, in general, do not implement appropriate security procedures and, therefore, are asking for unauthorized access to occur.

It is estimated that half of the 12,000 DECnet Internet nodes received the worm, but much less than 2 percent of those computers executed HI.COM within the first eight hours after the release of the worm. Within minutes after the worm was released, a very quick user reaction across the DECnet internet occurred, and the situation was immediately taken seriously. Once the source program for the worm was captured, a procedural cure, using existing functionality of the computer operating systems, was quickly devised and distributed by several organizations that use the network. A combination of existing computer security measures, the quick and accurate procedures devised to stop the worm from executing, and the network itself were the main reasons the worm executed on such a small percentage of nodes.

On Friday, January 13, 1989, a worm nearly identical to the Father Christmas Worm entered the DEC internal network, called Easynet. The private Easynet network contains more nodes than the DECnet Internet. However, as discussed in a recent issue of *Digital News* [4], according to DEC the worm was spotted as it entered the network, and the system manager "was able to segregate the infected system before the worm could spread." It is believed that this incident was quickly controlled because of the widespread exposure and experience gained the previous month with the Father Christmas Worm.

Overall, the impact of the Father Christmas Worm was minimal in an operational sense but extensive in the area of strengthening computer system security (an ongoing activity). A process has been started to formalize procedures that will deal with worms, viruses, and other violations that threaten the DECnet Internet in the future. Key security personnel have been identified from each of the major networks in the DECnet Internet, and their responsibilities are being delineated.

Whatever may be the intention of the authors of computer worms and viruses, if these threats are not met head on and dealt with rapidly, the ultimate result may be that they destroy the productive working environment that an open network provides.

REFERENCES

[1] J. L. Green, V. L. Thomas, B. Lopez-Swafford, and L.Z. Porter, Introduction to the Space Physics Analysis Network (SPAN), Second Edition, NSSDC Technical Report, January 1987.

[2] V. L. Thomas and J. L. Green, "SPAN - A revolutionary tool for scientific research," Journal of the National Technical Association, p. 45, Winter 1989.

[3] P. Sisson, T. Butler, D. Peters, V. Thomas, and J. Green, SPAN Security Policy, Standards, and Guidelines, NSSDC Technical Report, July 1989.

[4] S. Lawson, "Catching the worm," News Briefs, Digital News, January 23, 1989.

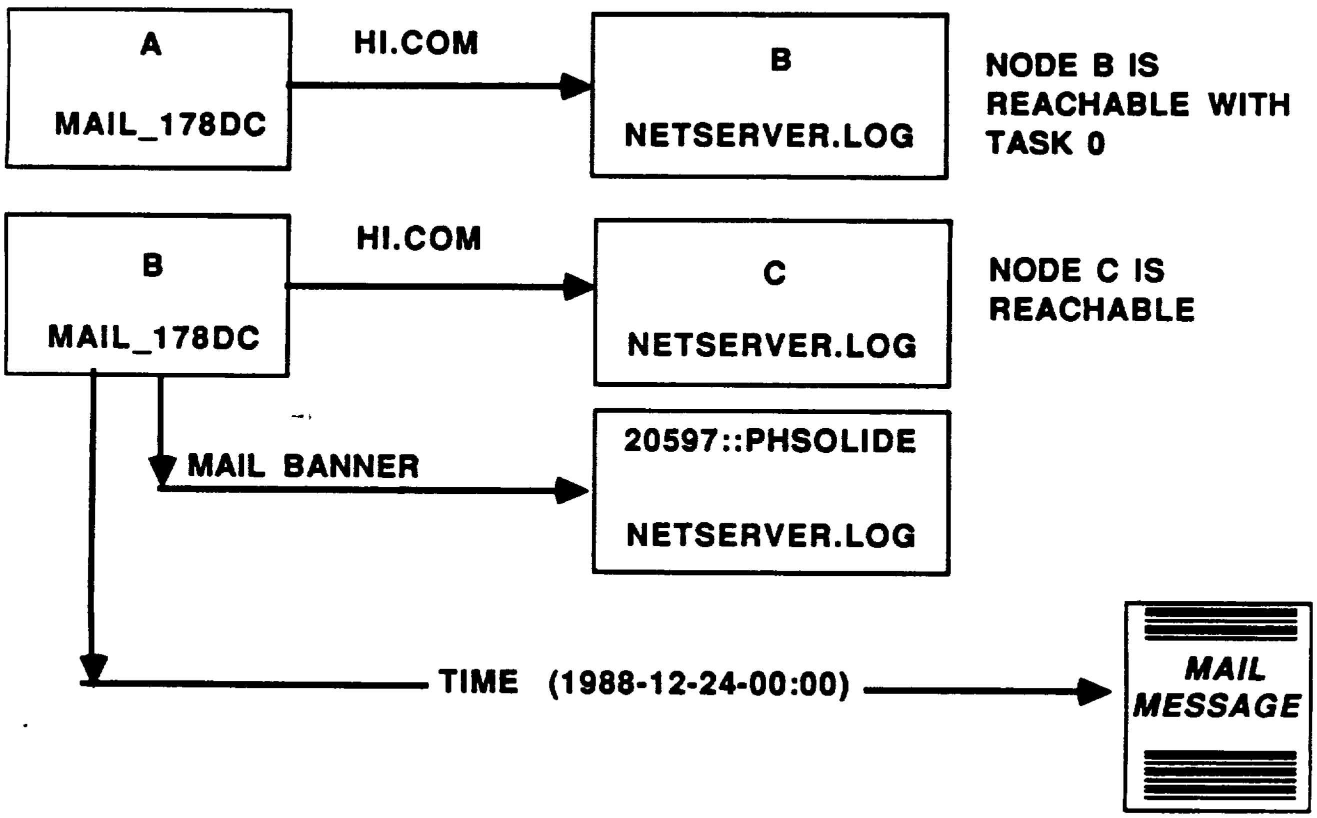
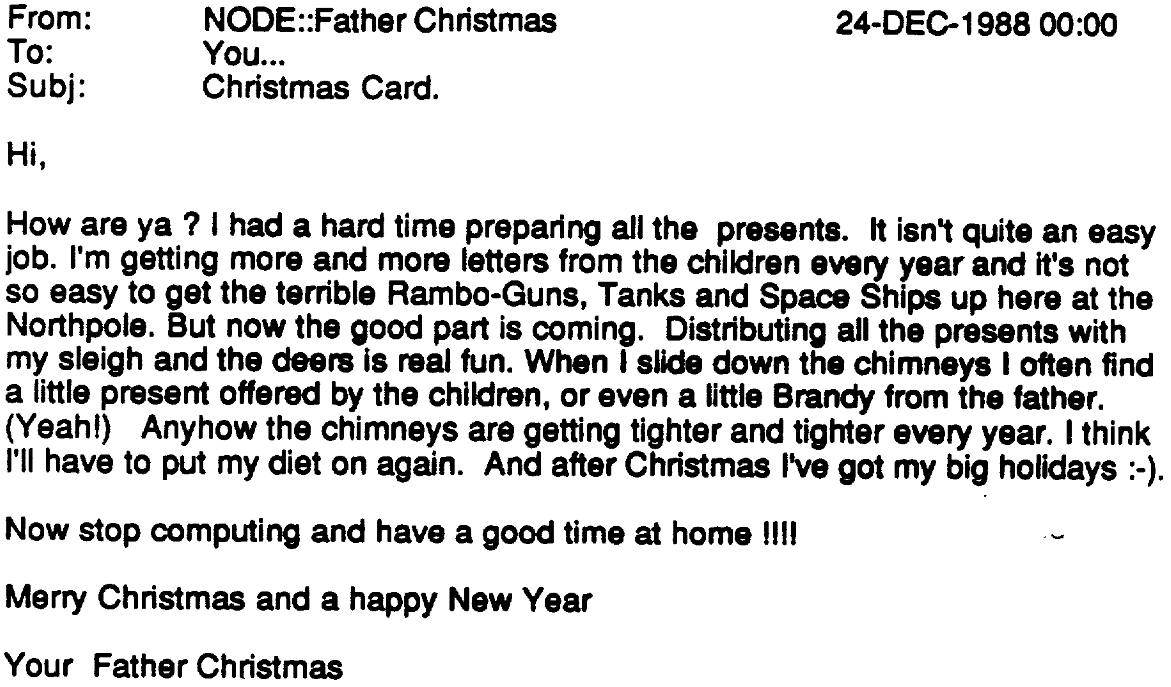


Figure 1: An overview of the major processes of the "Father Christmas Worm." In this example, Nodes A and B are executing the worm program HI.COM. Although Node C has a copy of the worm, it does not execute the program nor does it participate in the propagation of the worm because it has implemented certain security measures.



From: NODE::Father Christmas 24-DEC-1988 00:00
To: You...
Subj: Christmas Card.

Hi,

How are ya ? I had a hard time preparing all the presents. It isn't quite an easy job. I'm getting more and more letters from the children every year and it's not so easy to get the terrible Rambo-Guns, Tanks and Space Ships up here at the Northpole. But now the good part is coming. Distributing all the presents with my sleigh and the deers is real fun. When I slide down the chimneys I often find a little present offered by the children, or even a little Brandy from the father. (Yeah!) Anyhow the chimneys are getting tighter and tighter every year. I think I'll have to put my diet on again. And after Christmas I've got my big holidays :-).

Now stop computing and have a good time at home !!!!

Merry Christmas and a happy New Year

Your Father Christmas

Figure 2: The "Father Christmas Worm" electronic mail greeting. This message would only be sent to the users on a system executing the worm if it remained undetected until December 24, Christmas eve. After this mail message was sent, the worm program would stop executing.