# CERT Advisory CA-1989-04 WANK Worm On SPAN Network

Original issue date: October 17, 1989
Last revised: September 17, 1997
Attached copyright statement

A complete revision history is at the end of this file.

On 16 October, the CERT received word from SPAN network control that a worm was attacking SPAN VAX/VMS systems. This worm affects only DEC VMS systems and is propagated via DECnet protocols, not TCP/IP protocols. If a VMS system had other network connections, the worm was not programmed to take advantage of those connections. The worm is very similar to last year's HI.COM (or Father Christmas) worm.

This is NOT A PRANK. Serious security holes are left open by this worm. The worm takes advantage of poor password management, modifies .com files, creates a new account, and spreads to other systems via DECnet.

It is also important to understand that someone in the future could launch this worm on any DECnet based network. Many copies of the virus have been mailed around. Anyone running a DECnet network should be warned.

R. Kevin Oberman from Lawrence Livermore National Labs reports: "This is a mean bug to kill and could have done a lot of damage. Since it notifies (by mail) someone of each successful penetration and leaves a trapdoor (the FIELD account), just killing the bug is not adequate. You must go in an make sure all accounts have passwords and that the passwords are not the same as the account name."

The CERT/CC also suggests checking every .com file on the system. The worm appends code to .com files which will reopen a security hole everytime the program is executed.

An analysis of the worm appears below and is provided by R. Kevin Oberman of Lawrence Livermore National Laboratory. Included with the analysis is a DCL program that will block the current version of the worm. At least two versions of this worm exist and more may be created. This program should give you enough time to close up obvious security holes.

If you have any technical questions or have an infected system, please call the CERT/CC:

---

## Report on the W.COM worm.

R. Kevin Oberman
Engineering Department
Lawrence Livermore National Laboratory
October 16, 1989

The following describes the action of the W.COM worm (currently based on the examination of the first two incarnations). The replication technique causes the code to be modified slightly which indicates the source of the attack and learned information.

All analysis was done with more haste than I care for, but I believe I have all of the basic facts correct.

### First a description of the program:

1. The program assures that it is working in a directory to which the owner (itself) has full access (Read, Write,Execute, and Delete).

1. The program checks to see if another copy is still running. It looks for a process with the first 5 characters of "NETW_".
   If such is found, it deletes itself (the file) and stops its process.

   NOTE: A quick check for infection is to look for a process name starting with "NETW_". This may be done with a SHOW PROCESS command.

1. The program then changes the default DECNET account password to a random string of at least 12 characters.

1. Information on the password used to access the system is mailed to the user GEMPAK on SPAN node 6.59. Some versions may have a different address.

1. The process changes its name to "NETW_" followed by a random number.

1. It then checks to see if it has SYSNAM priv.
   If so, it defines the system announcement message to be the banner in the program:

```
W O R M S A G A I N S T N U C L E A R K I L L E R S
_______________________________________________________________
\__ ____________ _____ ________ ____ ____ __ _____/
\ \ \ /\ / / / /\ \ | \ \ | | | | / / /
\ \ \ / \ / / / /__\ \ | |\ \ | | | |/ / /
\ \ \/ /\ \/ / / ______ \ | | \ \| | | |\ \ /
\_\ /__\ /____/ /______\ \____| |__\ | |____| |_\ \_/
\___________________________________________________/
\ /
\ Your System Has Been Officically WANKed /
\_____________________________________________/

You talk of times of peace for all, and then prepare for war.
```

1. If it has SYSPRV, it disables mail to the SYSTEM account.

1. If it has SYSPRV, it modifies the system login command procedure to APPEAR to delete all of a user's file. (It really does nothing.)

1. The program then scans the accounts logical name table for command procedures and tries to modify the FIELD account to a known password with login form any source and all privs.
   This is a primitive virus, but very effective IF it should get into a privileged account.

1. It proceeds to attempt to access other systems by picking node numbers at random.
   It then used PHONE to get a list of active users on the remote system. It proceeds to irritate them by using PHONE to ring them.

1. The program then tries to access the RIGHTSLIST file and attempts to access some remote system using the users found and a list of "standard" users included with the worm.
   It looks for passwords which are the same as that of the account or are blank. It records all such accounts.

1. It looks for an account that has access to SYSUAF.DAT.

1. If a priv. account is found, the program is copied to that account and started. If no priv account was found, it is copied to other accounts found on the random system.

1. As soon as it finishes with a system, it picks another random system and repeats (forever).

## Response:

1. The following program will block the worm. Extract the following code and execute it. It will use minimal resources.
   It create a process named NETW_BLOCK which will prevent the worm from running.

   Editors note: This fix will work only with this version of the worm. Mutated worms will require modification of this code; however, this program should prevent the worm from running long enough to secure your system from the worms attacks.

   ```
   $ Set Default SYS$MANAGER
   $ Create BLOCK_WORM.COM
   $ DECK/DOLLAR=END_BLOCK
   $LOOP:
   $ Set Process/Name=NETW_BLOCK
   $ Wait 12:0
   $ GoTo loop
   END_BLOCK
   $ Run/Input=SYS$MANAGER:BLOCK_WORM.COM/Error=NL:/Output=NL:/UIC=[1,4] -
   SYS$SYSTEM:LOGINOUT
   ```

   Editors note: This fix might only work if the worm is running as SYSTEM. An earlier post made by the CERT/CC suggested the following:

   ```
   $ Run SYS$SYSTEM:NCP
   Clear Object Task All
   ^Z
   ```

   You must then edit the file SYS$MANAGER:STARTNET.COM, and add the line

   ```
   CLEAR OBJECT TASK ALL
   ```

   AFTER the line which says

   ```
   SET KNOWN OBJECTS ALL
   ```

   This has the side-effect of disabling users from executing any command procedure via DECnet that the system manager has not defined in the DECnet permanent database.

1. Enable security auditing.
   The following command turns on the MINIMUM alarms. The log is very useful in detecting the effects of the virus left by the worm. It will catch the viruses modification of the UAF. $ Set Audit/Alarm/Enable=(ACL,Authorization,Breakin=All,Logfailure=All)

1. Check for any account with NETWORK access available for blank passwords or passwords that are the same as the username. Change them!

1. If you are running VMS V5.x, get a copy of SYS$UPDATE:NETCONFIG_UPDATE.COM from any V5.2 system and run it.
   If you are running V4.x, change the username and password for the network object "FAL".

1. If you have been infected, it will be VERY obvious.
   Start checking the system for modifications to the FIELD account. Also, start scanning the system for the virus. Any file modified will contain the following line:
   $ oldsyso=f$trnlnm("SYS$OUTPUT")

   It may be in LOTS of command procedures. Until all copies of the virus are eliminated, the FIELD account may be changed again.

1. Once you are sure all of the holes are plugged, you might kill off NETW_BLOCK. (And then again, maybe not.)

Revision History

September 17,1997 Attached Copyright Statement