FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1433451-000

Total Deleted Page(s) = 52
Page 56 ~ b6; b7C; b7E;
Page 57 ~ b6; b7C; b7E;
Page 58 ~ b6; b7C; b7E;
Page 59 ~ b6; b7C; b7E;
Page 60 ~ b6; b7C; b7E;
Page 61 ~ b6; b7C; b7E;
Page 62 ~ b6; b7C; b7E;
Page 63 ~ b6; b7C; b7E;
Page 64 ~ b6; b7C; b7E;
Page 65 ~ b6; b7C; b7E;
Page 66 ~ b7E;
Page 67 ~ b7E;
Page 68 ~ b6; b7C; b7E;
Page 69 ~ b6; b7C; b7E;
Page 70 ~ b6; b7C; b7E;
Page 71 ~ b6; b7C; b7E;
Page 72 ~ b7E;
Page 73 ~ b7E;
Page 74 ~ b7E;
Page 75 ~ b6; b7C; b7E;
Page 76 ~ b6; b7C; b7E;
Page 77 ~ b7E;
Page 78 ~ b7E;
Page 79 ~ b7E;
Page 80 ~ b7E;
Page 81 ~ b7E;
Page 82 ~ b7E;
Page 83 ~ b7E;
Page 84 ~ b7E;
Page 85 ~ b6; b7C; b7E;
Page 86 ~ b7E;
Page 87 ~ b7E;
Page 88 ~ b7E;
Page 89 ~ b7E;
Page 90 ~ b6; b7C; b7E;
Page 91 ~ b7E;
Page 92 ~ b7E;
Page 93 ~ b7E;
Page 94 ~ b6; b7C; b7E;
Page 95 ~ b6; b7C; b7E;
Page 96 ~ b6; b7C; b7E;
Page 97 ~ b6; b7C; b7E;
Page 98 ~ b6; b7C; b7E;
Page 99 ~ b7E;
Page 100 ~ b7E;
Page 101 ~ b7E;
Page 102 ~ b7E;
Page 103 ~ b7E;
Page 104 ~ b7E;
Page 105 ~ b7E;
Page 106 ~ b7E;
Page 107 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

Memorandum

To : SAC, WMFO (264A-WF-165334) (P*)   Date 9/12/91

From : SA [redacted] (C-14)   b6 b7C

Subject: UNSUB(S);
UNAUTHORIZED ACCESS OF FEDERAL/
FEDERAL INTEREST COMPUTERS;
SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND
HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS;
W.COM "WANK" WORM;
OCTOBER, 1989;
CFA
(OO:WMFO)

Attached are materials received from [redacted] [redacted] manager. They are: b6 b7C b7E

[redacted]

264A-WF-166334-21

1-WMFO (Attachment)
JLK:jk

sending a screen message, "WORMS AGAINST NUCLEAR KILLERS" - "Your System Has Been Officially WANKed" - "You talk of times of peace for all, and then prepare for war." The worm was also performing a more insidious task. Upon successful penetration of a system, it was electronically mailing information regarding the system penetrated, including accounts and passwords, to an account in a computer at NASA's Goddard Space Flight Center (GSFC), Greenbelt, Maryland.

On 10/19/89, [redacted] SPAN security manager, GSFC, advised that to date 68 DECNET systems have been identified as being effected by the worm. The worm's mail is being sent to an account named GEMPAK on a Goddard node (computer) named DIATOM, DECNET #6.59. The account has no system privileges.

b6
b7C
b7D

According to [redacted] the intrusion was first noted at 4:30am on 10/16/89, by the University of Rhode Island and reported to him at about 10:00am that day. The University of Rhode Island did not have its accounting function enabled so there is no record of the location of the intrusion.

[redacted] has checked the accounting records for the GEMPAK account at Goddard and noted that GEMPAK had logon activity from a node in France several hours before the University of Rhode Island intrusion. The [redacted] node name is LPNVAX (#32.121), user CCPN. [redacted] is attempting to check with the system administrator in France to determine this user's identity.

On 10/23/89, [redacted] advised he functions as the HEPNET Manager. According to [redacted] approximately 8 HEPNET nodes have been identified as being effected by the worm, plus 4 or 5 DECNET nodes in Japan not related to HEPNET. He is asking his network users to keep accounting records of intrusion attempts and to send him details of the accounts infected. They will be available should any prosecution be undertaken.

b6
b7C

On 10/23/89, [redacted] Investigative Services, DEC, Maynard, Massachusetts, advised that a similar worm has been detected in DEC's corporate network called EASYNET, a network of approximately 40,000 computers worldwide. The EASYNET worm is sending mail to a node on EASYNET. No source of the intrusion has yet been identified. [redacted] will advise if information is developed which may identify the source of the EASYNET intrusion, since it is most likely the same source as the SPAN/HEPNET intrusions.

WMFO advised NASA, Office of Inspector General (OIG), on 10/16/89, and DOE OIG on 10/18/89, both of which were unaware of the worm intrusions until advised by WMFO. NASA OIG has assigned a Special Agent to insure that material of an evidentiary nature is retained for possible prosecutive use should the source of the intrusions be identified.

It is not known at this time how long the worm has been sending mail containing account and password information to the DIATOM GEMPAK account and if this account has been periodically downloaded and thereafter erased by an intruder based in France or elsewhere. If this has happened, then an unknown number of nodes on SPAN and HEPNET are subject to individual attack and compromise at a later date.

WMFO will follow efforts of the network security managers to identify the source of the intrusions. WMFO will conduct active investigation only if a possible source is identified.

SG-031 (264A-WF-165334) 8 March 1990

[redacted]

b6
b7C

COMPUTER FRAUD -
Unknown Persons
also known as
"WANK WORMS"

On 16 October 1989, the University of Rhode Island first noted an unauthorized intrusion into the "DECNET INTERNET" system, which is a world-wide collection of computer networks based on protocols of Digital Equipment Corporation (DEC). The case networks are: SPAN (Space Physics Analysis Network), European SPAN, HEPNET (High Energy Physics Network) and European HEPNET. The DECNET INTERNET comprises over 17,000 computers throughout the world, mostly in the United States and Western Europe.

The intrusion noted on 16 October 1989 spread to about 100 computers on the DECNET INTERNET. Another intrusion was noted on 30 October 1989 which affected about 500 computers. Called the "WANK WORM", the intrusion may display the following message on the computer screen:

"WORMS AGAINST NUCLEAR KILLERS. - YOUR SYSTEM HAS BEEN OFFICIALLY WANKED" "YOU TALK OF TIMES OF PEACE FOR ALL AND THEN PREPARE FOR WAR".

The "worm" then changes account passwords, runs the authorize utility and attempts to penetrate additional accounts by using a list of over 80 frequently used passwords as well as by using user identification names as passwords. The "worm" also electronically mails information about the penetrated system, including accounts and passwords to an account in a SPAN computer at the National Aeronautics and Space Administration (NASA) Goddard Space Flight Center in Maryland, U.S.A.

NASA security officials have checked accounting records for the computer at the Goddard Space Flight Center and noted unusual activity prior to 16 October 1989, originating from France.

It is not known whether any of the penetrated computer systems have been further subjected to individual attack, but the possibility certainly exists.

The FBI in Washington, D.C. is investigating this matter in coordination with NASA Security officials and Digital Equipment Corporation security personnel.

The above is for your information. If you are aware of any similar activity in Switzerland, please advise.

2 - Addressee
1 - Bern (264A-WF-165334)
RMF/hac
(3)

264A-WF-165334-3

R/S

11/28/89

[redacted]

Per our conversation today, please advise [redacted] as you deem appropriate— b6 b7C

[redacted] Ext. 5594

Thanks!

RECEIVED 12/4/89 AM [redacted]

Received from FBIHQ 12-4-89

264A-WF-165334
-3

[redacted] b6 b7C

b6
b7C

0112 MRI 00815

RR RUEHFB

DE PAR #0003 3260800

ZNY SSSSS

R 220758Z NOV 89

FM LEGAT PARIS (264B-PA-7349) (P)

TO DIRECTOR FBI/ROUTINE/

BT

~~SECRET~~

CITE: //5250:PAR857.325 21 NOV 89//

SUBJECT: UNSUBS, AKA WORMS AGAINST NUCLEAR KILLERS; CF&A; OO: PARIS.

THIS COMMUNICATION IS CLASSIFIED ~~"SECRET"~~ IN ITS ENTIRETY.

[redacted] b7D

[redacted] HAS BEGUN INVESTIGATION OF A "VIRUS" WHICH, ON OCTOBER 16 AND 17, 1989, ATTEMPTED AND IN SOME CASES, SUCCEEDED IN PIRATING SEVERAL COMPUTER SITES SPECIALIZING IN SPACE AND NUCLEAR MATTERS. THIS VIRUS CONSISTED OF A PARASITIC WICOM PROGRAM WHICH ALWAYS LEFT THE LOGO, "WORMS AGAINST NUCLEAR KILLERS" IN THE SYSTEMS IT ATTACKED.

[redacted] b6
b7C

264-A-WF-165334
10/24/89 opened.

9C

b6
b7C

PAGE TWO DE PAR 0003 ~~SECRET~~

PROPAGATING ITSELF THROUGH THE SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND HEPNET, WHICH IS THE NETWORK OF THE "PHYSIQUE DES HAUTES ENERGIES" (HIGH ENERGY PHYSICS), THIS VIRUS (WHICH ONLY EFFECTED DEC/VMS SYSTEMS TRANSMITTING ITSELF THROUGH THE DECNET MENU), WAS INTRODUCED TO THE [redacted] SITES FROM COMPUTERS CONNECTED TO THESE TWO NETWORKS IN THE UNITED STATES. b7D

[redacted] HAS REQUESTED ALL INFORMATION THE BUREAU MAY HAVE CONCERNING THIS COMPUTER ATTACK AS WELL AS THE ORIGIN OF THE VIRUS. PURSUANT TO ITS INVESTIGATION OF THE MATTER, [redacted] HAS ALSO REQUESTED A MEETING WITH FBI COMPUTER SPECIALISTS IN ORDER TO EXCHANGE INFORMATION CONCERNING THIS VIRUS. b7D

CLASSIFIED BY [redacted] DECLASSIFY ON OADR.

BT

#0003

NNNN

Embassy of the United States of America

Jubilaumstrasse 93
CH 3005 Bern, Switzerland

Our No. 264A-WF-165334
[redacted]

8 March 1990

b6
b7C

Interpol, Vienna

RE: <u>COMPUTER FRAUD</u> -
Unknown Persons,
also known as
"WANK WORMS"

Dear Sir:

On 16 October 1989, the University of Rhode Island first noted an unauthorized intrusion into the "DECNET INTERNET" system, which is a world-wide collection of computer networks based on protocols of Digital Equipment Corporation (DEC). The case networks are: SPAN (Space Physics Analysis Network), European SPAN, HEPNET (High Energy Physics Network) and European HEPNET. The DECNET INTERNET comprises over 17,000 computers throughout the world, mostly in the United States and Western Europe.

The intrusion noted on 16 October 1989 spread to about 100 computers on the DECNET INTERNET. Another intrusion was noted on 30 October 1989 which affected about 500 computers. Called the "WANK WORM", the intrusion may display the following message on the computer screen:

"WORMS AGAINST NUCLEAR KILLERS. - YOUR SYSTEM HAS BEEN OFFICIALLY WANKED" "YOU TALK OF TIMES OF PEACE FOR ALL AND THEN PREPARE FOR WAR".

The "worm" then changes account passwords, runs the authorize utility and attempts to penetrate additional accounts by using a list of over 80 frequently used passwords as well as by using user identification names as passwords. The "worm" also electronically mails information about the penetrated system, including accounts and passwords to an account in a SPAN computer at the National Aeronautics and Space Administration (NASA) Goddard Space Flight Center in Maryland, U.S.A.

NASA security officials have checked accounting records for the computer at the Goddard Space Flight Center and noted unusual activity prior to 16 October 1989, originating from France.

2 - Addressee
1 - Bern (264A-WF-165334)
RMF/hac
(3)

COMPUTER FRAUD

It is not known whether any of the penetrated computer systems have been further subjected to individual attack, but the possibility certainly exists.

The FBI in Washington, D.C. is investigating this matter in coordination with NASA Security officials and Digital Equipment Corporation security personnel.

The above is for your information. If you are aware of any similar activity in Austria, please advise.

Sincerely yours,

[redacted]
Legal Attache

b6
b7C

ORIGINAL

SPAN
Space Physics Analysis Network

SPAN Network Information Center
SPAN Operations Center
NASA/Goddard Space Flight Center
Code 630.2
Greenbelt, Maryland 20771 USA
FAX #: +1-301-286-9803 or FTS 888-9803

[redacted]

[redacted]

b6
b7C

TO: [redacted]

ORGANIZATION: FBI

OFFICE PHONE NUMBER: [redacted]

FAX PHONE NUMBER: 324-6426

NO. OF PAGES: 2
(including lead page)

COMMENTS:

[redacted]

This is the information you requested.
Let me know if there's anything more
you need.
Regards -
[redacted]

b6
b7C

264A-WF-165334-4

JG
240

The WANK Worm (Virus) was programmed to send mail messages to node 6.59 at NASA's Goddard Space Flight Center. Accounting records from the NASA node 6.59 show interactive network logins originating from node 32.121 in France on 0h-3h EDT on 16-Oct-1989. The earliest report of a worm attack on either HEPnet or SPAN was at approximately 4h30 EDT on 16-Oct-1989.

SPAN Management has obtained accounting files from node 32.121 which indicate that the computer hacker (pirate) appeared to be debugging and testing the worm code on node 32.121 as early as 4-October-1989, 12 days before the world-wide outbreak on 16-Oct-89.

SPAN Management believes that the worm was introduced onto U.S. SPAN computer systems from European HEPnet (High Energy Physics Network) site LPNVAX (32.121). It is anticipated that the account in question, userid CCPN, was probably penetrated by the hacker prior to any of the noted activity.

/FIND/MRI 1648/348

Retrieval completed at 2302
/FIND/MRI 1648/348
Results are: 0001 found

/READ/REF 2
0025 MRI 01648

RR FBIAXTX

DE FBIWMFO #0035 3482303

ZNR UUUUU

R 142236Z DEC 89

FM FBI WMFO (246A-WF-165334) (C-9 NVMRA)

Resent with correct File # on 12-15-89

TO DIRECTOR FBI/ROUTINE/

LEGAT PARIS/ROUTINE/

BT

UNCLAS

CITE: //3920//

SUBJECT: UNSUB(S), UNAUTHORIZED ACCESS OF FEDERAL/FEDERAL INTEREST COMPUTERS; SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS; W. COM "WANK" WORM; OCTOBER, 1989; CFA; OO: WMFO.

RE LEGAT PARIS TELETYPE, DATED NOVEMBER 22, 1989; CAPTIONED, "UNSUBS, AKA WORMS AGAINST NUCLEAR KILLERS; CF&A; OO: PARIS."

REFERENCED TEL ADVISED [redacted] IS CONDUCTING INVESTIGATION AND IS REQUESTING FBI ASSISTANCE. b7D

CONTACT HAS BEEN MADE WITH DIGITAL EQUIPMENT CORPORATION

264A-WF-165334-5

[redacted] b6 b7C

(DEC) AND SPAN SECURITY OFFICIALS. BOTH ARE AGREEABLE TO MEETING WITH [redacted] TO EXCHANGE INFORMATION AND TO COORDINATE RESPECTIVE INVESTIGATIONS. THE FOLLOWING WAS PROVIDED BY SPAN SECURITY: b7D

"THE WANK WORM WAS PROGRAMMED TO SEND MAIL MESSAGES TO NODE 6.59 AT THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION'S (NASA) GODDARD SPACE FLIGHT CENTER. ACCOUNTING RECORDS FROM NASA NODE 6.59 SHOW INTERACTIVE NETWORK LOGINS ORIGINATING FROM NODE 32.121 IN FRANCE DURING ZERO HOURS TO THREE HOURS (12 MIDNIGHT TO 3 AM) U.S. EASTERN DAYLIGHT TIME (EDT), ON OCTOBER 16, 1989. THE EARLIEST REPORT OF A WORM ATTACK ON EITHER HEPNET OR SPAN WAS AT APPROXIMATELY FOUR HOURS 30 MINUTES (4:30 AM) EDT, ON OCTOBER 16, 1989.

"SPAN MANAGEMENT HAS OBTAINED ACCOUNTING FILES FROM NODE 32.121 WHICH INDICATE THE INTRUDER APPEARED TO BE DEBUGGING AND TESTING THE WORM CODE ON NODE 32.121 AS EARLY AS OCTOBER 4, 1989, 12 DAYS BEFORE THE WORLD-WIDE OUTBREAK ON OCTOBER 16, 1989."

"SPAN MANAGEMENT BELIEVES THE WORM WAS INTRODUCED IN THE U.S. SPAN COMPUTER SYSTEMS FROM EUROPEAN HEPNET SITE "LPNVAX" (32.121) IT ANTICIPATED THE ACCOUNT IN QUESTION. USER IDENTIFICATION [redacted] WAS PROBABLY PENETRATED BY THE INTRUDER PRIOR TO ANY OF THE NOTED ACTIVITY."

b6
b7C

LEADS. LEGAT PARIS: AT PARIS, FRANCE.

(1) PASS ABOVE INFORMATION TO THE [redacted] AND REPORT RESPONSE. b7D

(2) DETERMINE THE BEST COURSE TO PROCEED IN ESTABLISHING DIRECT CONTACT BETWEEN FBI, EEC, AND SPAN TECHNICAL PERSONNEL AND THE [redacted]

BT

#0035

NNNN

Memorandum

To : Director, FBI (Date 3/8/90

From : Legal Attache, Bern   (264A-WF-165334)(P)

Subject: UNSUBS; UNAUTHORIZED ACCESS OF FEDERAL INTEREST COMPUTERS; SPAN AND HEPNET - VICTIMS: W. COM "WANK" WORM; 10/89; CFA; OO: WMFO.

Reference: WMFO teletype 1/30/90.

Dissemination, as outlined below, was made on dates indicated.

□ ____________ copies of

☒ Pertinent information from referenced communication.

Name and Location of Agency	Date Furnished
[redacted]	3/8/90
[redacted]	3/8/90

b7D

2 - Bureau
    (1-OLIA)
2 - Bern (1-264A-WF-165334)(66-120)
hac
(4)

264A-WF-165334-5
SEARCHED ____
SERIALIZED ____
INDEXED ____
FILED ____

264A-WF-165334-5

[redacted]

b6
b7C

/READ/REF 1
0005 MRI 02659

RR RUEHFB AFO ALO FBIWMFO

DE FBIWMFO #0016 0301932

ZNR UUUUU

R 301929Z JAN 90

FM FBI WMFO (264A-WF-165334) (P) (C-9)

TO ~~DIRECTOR~~ FBI/ROUTINE/

ALL FBI FIELD OFFICES/ROUTINE/

ALL LEGATS/ROUTINE/

BT

UNCLAS

CITE: //3920//

SUBJECT: UNSUB(S); UNAUTHORIZED ACCESS OF FEDERAL/FEDERAL INTEREST COMPUTERS; SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND HIGH ENERGY PHYSICS NETWORK (HEPNET)-VICTIMS; W. COM "WANK" WORM; OCTOBER, 1989; CFA; OO: WMFO.

RE TELEPHONE CONVERSATION BETWEEN FBIHQ SSA [redacted] AND WMFO SA [redacted] ON JANUARY 30, 1990.

b6
b7C

DURING REFERENCED TELEPHONE CONVERSATION, SSA [redacted] REQUESTED THAT WMFO ADVISE ALL FIELD DIVISIONS AND LEGATS OF THIS

DUE [redacted] BXD

264-WF-165334-6

93

CASE TO PREVENT DUPLICATION OF EFFORTS.

THE WANK WORM INTRUSION AFFECTS THE DECNET INTERNET WHICH IS A WORLD-WIDE COLLECTION OF NETWORKS BASED ON DIGITAL EQUIPMENT CORPORATICN (DEC) PROTOCOLS. THE CORE NETWORKS ARE SPAN, EUROPEAN SPAN, HEPNET, AND EUROPEAN HEPNET. THE DECNET INTERNET TOTALS OVER 17,000 COMPUTERS.

THE WANK WORM WAS FIRST NOTED ON OCTOBER 16, 1989, BY THE UNIVERSITY OF RHODE ISLAND. IT LATER SPREAD TO APPROXIMATELY 100 COMPUTERS ON THE DECNET INTERNET. ANOTHER ATTACK ON OCTOBER 30, 1989, AFFECTED APPROXIMATELY 500 COMPUTERS. UPON SUCCESSFUL PENETRATION OF A COMPUTER, THE WORM MAY DISPLAY THE SCREEN MESSAGE, "WORMS AGAINST NUCLEAR KILLERS" - "YOUR SYSTEM HAS BEEN OFFICIALLY WANKED" - "YOU TALK OF TIMES OF PEACE FOR ALL, AND THEN PREPARE FOR WAR." THE WORM ALSO PERFORMS A MORE INSIDIOUS TASK. IT CHANGES ACCOUNT PASSWORDS, RUNS THE AUTHORIZE UTILITY, AND ATTEMPTS TO PENETRATE ADDITIONAL ACCOUNTS BY USING A CANNED LIST OF OVER 80 PASSWORDS, AS WELL AS BY USING USER IDENTIFICATION NAMES AS PASSWORDS. THE WORM ELECTRONICALLY MAILS INFORMATION REGARDING THE SYSTEM PENETRATED, INCLUDING ACCOUNTS AND PASSWORDS, TO AN ACCOUNT IN A SPAN COMPUTER AT THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION'S (NASA) GODDARD SPACE

MARYLAND.

NASA SPAN SECURITY OFFICIALS CHECKED ACCOUNTING RECORDS FOR THE GODDARD COMPUTER AND NOTED UNUSUAL ACTIVITY BEFORE OCTOBER 16, 1989, ORIGINATING FROM FRANCE. IT IS NOT KNOWN IF COMPROMISED COMPUTERS HAVE BEEN SUBJECTED TO INDIVIDUAL DIRECT ATTACK, ALTHOUGH THE POSSIBILITY CERTAINLY EXISTS.

WMFO IS CONDUCTING AN INVESTIGATION IN COORDINATION WITH THE NASA OFFICE OF INSPECTOR GENERAL, WASHINGTON D.C., AND SPAN SECURITY PERSONNEL. INITIAL CONTACT HAS BEEN MADE BY LEGAT PARIS WITH [redacted] b7D

[redacted] REGARDING THIS MATTER. [redacted] MAY PROVIDE INFORMATION WHICH WILL HELP TO IDENTIFY THOSE RESPONSIBLE FOR THIS WORM. WMFO IS ALSO IN CONTACT WITH DEC SECURITY PERSONNEL WHO ARE CONDUCTING THEIR OWN INVESTIGATION.

SINCE THESE ARE EXTENSIVE WORLD-WIDE NETWORKS, MULTIPLE COMPLAINTS MAY HAVE BEEN RECEIVED BY DIFFERENT FIELD DIVISIONS AND LEGATS. IF YOUR OFFICE HAS OPENED A CASE BASED ON SUCH COMPLAINTS, PLEASE ADVISE FBIHQ AND WMFO AND PROVIDE DETAILS.

BT

#0016

NNNN

[redacted]

P
C-9

[redacted]

b6
b7C

UCFN ☒ Pos □ Neg VDH

GENERAL INDICES:

□ Automated Search

WF: □ Pos □ Neg AX: □ Pos □ Neg

□ Manual Search

WF: □ Pos □ Neg AX: □ Pos □ Neg

```
/REAT:
0021  MRI 00490

RR RUEHFB FBIWMFO

DE BER #0004 0361635

ZNR UUUUU

R 051452Z FEB 90

FM LEGAT BERN (264A-WF-165334) (P)

TO DIRECTOR FBI/ROUTINE/

FBI WMFO (264A-WF-165334) (C-9)/ROUTINE/

BT

UNCLAS

CITE:  //3550:BER047.036  05 FEB 90//
```

[redacted]

b7D per DOS

REWMFOTEL DATED 1/30/90.

LEGAT, BERN IS NOT AWARE OF ANY INVESTIGATIONS OF SUBJECT MATTER, HOWEVER, IT IS POSSIBLE THAT SWISS OR AUSTRIAN AUTHORITIES ARE INVOLVED. UNLESS ADVISED TO THE CONTRARY BY WMFO OR FBIHQ BY FEBRUARY 16, 1990, LEGAT, BERN WILL DISSEMINATE THE

264A-WF-165334-7

[redacted]

b6
b7C

PAGE TWO DE PER 0004 UNCLAS

BASIC FACTS OF THIS MATTER TO APPROPRIATE [redacted] [redacted] FOR INFORMATION AND TO DETERMINE IF EITHER HAVE ANY INVESTIGATION OR COMPLAINTS CONCERNING CAPTIONED MATTER.

b7D per FBI, DOS

BT

#0004

NNNN

C-9

/READ/REF 1
0013 MRI 00543

RR RUEHFB FBIWMFO

DE BER #0001 0961502

ZNR UUUUU

R 060803Z APR 90

FM LEGAT BERN (264A-WF-165334) (RUC)

TO DIRECTOR FBI/ROUTINE/

FBI WMFO (264A-WF-165334) (C-9)/ROUTINE/

BT

UNCLAS

CITE: //5550:BER152,096 06 APR 90//

[redacted]

b7D per DOS

REWMFOTEL DATED JANUARY 30, 1990; AND BERTEL DATED FEBRUARY 5, 1990.

LEGAT, BERN HAS SUBMITTED BACKGROUND INFORMATION AS SET FORTH IN REFERENCED WMFO TELETYPE TO APPROPRIATE [redacted] [redacted] IT SHOULD BE NOTED THAT NEITHER

b7D per FBI, DOS

264A-WF-165334-8

[redacted] K

b6
b7C

PAGE TWO DE BER 0001 UNCLAS

[redacted] HAS ANY LAW AS SUCH THAT IS COMPARABLE TO THE COMPUTER FRAUD ACT IN THE U.S. ANY ATTEMPTS TO OBTAIN SOMETHING OF VALUE WOULD BE INVESTIGATED/PROSECUTED UNDER NORMAL FRAUD AND/OR THEFT STATUTES, BUT NORMALLY ONLY AFTER SOMETHING OF VALUE HAS BEEN SHOWN TO HAVE BEEN OBTAINED BY A PERPETRATOR. UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS AS SUCH IS NOT PUNISHABLE AND THEREFORE THERE ARE NO POLICE OR OTHER INSTITUTIONS [redacted] THAT ROUTINELY HANDLE SUCH MATTERS AS UNAUTHORIZED ENTRY TO COMPUTER SYSTEMS.

b7D per FBI, DOS

b7D per FBI, DOS

LEGAT HAS REQUESTED TO BE ADVISED OF ANY INFORMATION THAT MAY BECOME AVAILABLE CONCERNING CAPTIONED MATTER, BUT DOES NOT EXPECT A RESPONSE AS NO SPECIFIC LEADS/REQUESTS WERE MADE.

BERN CONSIDERING THIS MATTER RUC.

BT

#0001

NNNN

C-9

/READ/REF 1
0003 MRI 00217

RR RUEHFB FBIWMFO

DE PAR #0003 0991542

ZNR UUUUU

R 090839Z APR 90

FM LEGAT PARIS (264B-PA-7349) (P)

TO DIRECTOR FBI/ROUTINE/

FBI WMFO/ROUTINE/

BT

UNCLAS

CITE: //5250:PAR567.095 5 APRIL 1990//

PASS: FBIHQ, SSA [redacted]

b6 per FBI, DOS
b7C per FBI, DOS

[redacted]

b7D per DOS

REFERENCE WMFO TELETYPE CAPTIONED AS ABOVE DATED 1/30/90.

THE [redacted] HAS ADVISED THAT [redacted]

b7D per FBI, DOS

264A-WF-165384-9

[redacted] 9K

b6
b7C

[redacted]

[redacted] ADVISES THAT THEY ARE WAITING FOR THE RESULT OF THE INVESTIGATIONS TO BE CONDUCTED IN FRANCE WHICH SHOULD BE FORTHCOMING BEFORE ASKING FOR AN OFFICIAL MEETING WITH THE FBI ON CAPTIONED MATTER. IT IS [redacted] OPINION THAT THERE ARE NUMEROUS ELEMENTS OF IMPORTANCE IN THIS INVESTIGATION WHICH CAN ONLY BE OBTAINED IN THE UNITED STATES.

b7D per FBI, DOS

AS [redacted] PROVIDES ADDITIONAL INFORMATION, FBIHQ AND WMFO WILL BE ADVISED.

BT

#0003

NNNN

C-9

/READ/REF 1

0032 MRI 00609

RR RUEHFB FBIPG FBIWMFO

DE PAR #0003 1231402

ZNR UUUUU

R 030938Z MAY 90

FM LEGAT PARIS (264A-PG-51364) (264B-PA-7349) (P)

TO DIRECTOR FBI/ROUTINE/

FBI PITTSBURGH (264A-PG-51364)/ROUTINE/

FBI WMFO (264A-WF-165334)/ROUTINE/

BT

UNCLAS

CITE: //3250:PAR709.122 2 MAY 1990//

[redacted]

b6 Per DOS
b7D Per DOS

[redacted] ADVISED THAT AN ASSOCIATED PRESS RELEASE OF APRIL

b7D per FBI, DOS

b6
b7C

2, 1990, MENTIONS THE ARREST OF THREE YOUNG COMPUTER PIRATES IN AUSTRALIA THAT HAD PENETRATED VARIOUS AMERICAN UNIVERSITY SYSTEMS AND AUSTRALIAN GOVERNMENT SITES.

THE ARREST FOLLOWED A MORE THAN SIX MONTH JOINT INVESTIGATION BY THE FBI AND THE [redacted]

b7D per FBI, DOS

[redacted] DUE TO THEIR ONGOING INVESTIGATION OF WORMS AGAINST NUCLEAR KILLERS (WANK) WOULD LIKE TO KNOW IF THE INVESTIGATION WHICH PRODUCED THIS ARREST HAD ANY CONNECTION WITH THE WESTINGHOUSE MATTER OR THE WANK MATTER.

FBIHQ, WMFO AND PITTSBURGH ARE REQUESTED TO ADVISE IF THE ARREST IN AUSTRALIA IS RELATED TO THE WESTINGHOUSE OR WANK MATTERS.

BT

#0003

NNNN

FM FBI WMFO (264A-WF-165334) (P) (C-14)

TO DIRECTOR FBI/ROUTINE

LEGAT PARIS (264A-PG-51364) (264B-PA-7349)/ROUTINE/ C-14

FBI PITTSBURGH (264A-PG-51364)/ROUTINE/

BT

UNCLAS

CITE: //3920//

SUBJECT: UNSUB(S); THEFT OF INFORMATION AND UNAUTHORIZED AFFECT OF COMPUTER SYSTEMS, WESTINGHOUSE ELECTRIC CORPORATION (WEC) - VICTIM; MATRA DATAVISION - VICTIM; CFA; OO: PG; (PG FILE 264A-PA-7490); UNSUB(S); UNAUTHORIZED ACCESS OF FEDERAL/FEDERAL INTEREST COMPUTERS; SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS; W. COM "WANK" WORM; OCTOBER 1989; CFA; OO: WMFO (WMFO FILE 264A-WF-165334).

RE WMFO TEL DATED DECEMBER 15, 1989, AND LEGAT PARIS TEL

[redacted]

b6
b7C

264A-WF-165334-12

673/134
11 25 A

^PAGE TWO DE WMFO (264A-WF-165334) (UNCLAS)

DATED MAY 2, 1990.

REFERENCED WMFO TELETYPE PROVIDED INFORMATION RE EUROPEAN
HEPNET SITE "LPNVAX" (32.121) AND USER ACCOUNT [redacted] WHICH WAS b6 b7C
PROBABLY PENETRATED PRIOR TO THE RELEASE OF THE WANK WORM.

RE PARIS TEL ADVISED [redacted] REQUESTING INFORMATION RE b7D
POSSIBILITY SUBJECTS RECENTLY ARRESTED IN AUSTRALIA ARE CONNECTED
WITH CAPTIONED MATTERS.

WMFO HAS NO INFORMATION DIRECTLY LINKING AUSTRALIAN SUBJECTS
WITH THE WANK WORM. HOWEVER, IT IS A POSSIBILITY CAPTIONED
MATTERS ARE CONNECTED, SINCE THE WANK WORM WAS RELEASED JUST
AFTER THE WESTINGHOUSE INTRUSIONS ENDED.

WMFO IS STILL INTERESTED IN OBTAINING A RESPONSE FROM [redacted]
[redacted] RE OUR REQUEST PER REFERENCED WMFO TELETYPE. WMFO HAS NO
INFORMATION THE WANK WORM ORIGINATED IN THE UNITED STATES, AS MAY b7D
BE SUSPECTED BY [redacted] IF AVAILABLE, LEGAT PARIS IS REQUESTED
TO REPORT THE DETAILS OF SUCH [redacted] INFORMATION.

BT

Memorandum

To : SAC, WMFO (264A-WF-165334) (P*) Date 1/16/91

From : SA [redacted] (C-14)

b6
b7C

Subject: UNSUB(S);
UNAUTHORIZED ACCESS OF FEDERAL/
FEDERAL INTEREST COMPUTERS;
SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND
HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS;
W.COM "WANK" WORM;
OCTOBER, 1989;
CFA
(OO:WMFO)

The purpose of this memorandum is have this case placed into a pending inactive status, due to circumstances beyond the control of WMFO.

This case was opened on 10/24/89, and all logical leads have been covered to date. Serial 1, this file, describes the facts surrounding the captioned attack. It should be noted that SPAN officials claim the damage, including labor costs to secure systems, easily exceeds $500,000.

X
JK

The source of this attack may have been in France. Serial 2, this file, is a teletype to Legat Paris, dated 12/15/89, requesting assistance from [redacted] [redacted]. Serial 12, this file, dated 5/14/90, is a follow up request to Legat Paris for information from [redacted] Legat Paris, to date, has not obtained a direct response from [redacted]

b7D

[redacted] however, has requested a meeting in Washington, D.C., with FBI personnel to discuss this and other cases of mutual interest. Serial 3, this file, is a teletype, dated 11/22/89, requesting such a meeting.

1-WMFO
JLK:jk

~~5~~ 6 months review of [redacted] in 264-165334

9/12/91

1/16/91

264-WF-165334-15

b6
b7C

No such meeting has been arranged by FBIHQ. The Computer Fraud and Abuse control file (264-WF-C164574) has numerous serials (some classified) regarding FBIHQ lack of progress in arranging such a meeting.

I recommend this case be placed in a pending inactive status pending a meeting with [redacted] I also recommend the inactive status be reviewed in 6 months. b7D

DECLASSIFICATION AUTHORITY DERIVED FROM:
FBI AUTOMATIC DECLASSIFICATION GUIDE
DATE 06-11-2024 BY: [redacted]

C-14

b6
b7C

[illegible]

RR RUCNFB F3IPG FBIWMFO

DE PAR #0009 1751227

ZNY SSSSS

R 240733Z JUN 91

FM LEGAT PARIS (264A-WF-165334) (P)

~~SECRET~~

TO DIRECTOR FBI/ROUTINE/

FBI PITTSBURGH/ROUTINE/

FBI WMFO/ROUTINE/

BT

~~S E C R E T~~

CITE: //5250:PAR901.172 21 JUNE 1991//

PASS: HQ FOR [redacted]

b6 per FBI, DOS
b7C per FBI, DOS

[redacted]

b6 per DOS
b7D per DOS

THIS COMMUNICATION IS CLASSIFIED ~~SECRET~~ IN ITS ENTIRETY.

RETELCALL, 6/20/91, LEGAT PARIS WITH WMFO SA [redacted] AND

b6 per FBI, DOS
b7C per FBI, DOS

264A-WF-165334-16

~~SECRET~~

CONFERENCE 5/29-30/91.

IN RE CONFERENCE IT WAS CONCLUDED THAT FURTHER INVESTIGATIVE INITIATIVES INVOLVING [redacted] COOPERATION IN THE "WANK WORM" MATTER WOULD BE PURSUED UNDER CAPTIONED WMFO CASE. IN RETELCALL SA [redacted] ADVISED THAT CAPTIONED PITTSBURGH CASE WAS NOW CLOSED.

b6 per FBI, DOS
b7C per FBI, DOS
b7D per FBI, DOS

ACCORDINGLY, LEGAT PARIS IS PLACING IN RUC STATUS 264A-PG-51364 AND WILL OPEN 264A-WF-165334 FOR FUTURE CORRESPONDENCE.

LEGAT PARIS RECEIVED A NOTE FROM [redacted] EXPRESSING THEIR PROFOUND APPRECIATION FOR THE CONFERENCES OF 5/29-30/91 IN WASHINGTON. THEY SPECIFICALLY CONGRATULATED SECTION CHIEF WILLIAM J. ESPOSITO AND SSA [redacted] FOR THE QUALITY OF THE ORGANIZATION AS WELL AS THE WILLINGNESS AND KEEN INTEREST OF THE WMFO AND PITTSBURGH AGENTS AND SUPERVISORS WHICH CONTRIBUTED TO WHAT THEY DESCRIBE AS A SOLID BASE FOR [redacted] [redacted] IN THE AREA OF COMPUTER FRAUD.

b6 per FBI, DOS
b7C per FBI, DOS
b7D per FBI, DOS

[redacted] RE-EMPHASIZED THEIR LIVELY INTEREST IN THE "WANK WORM" MATTER AND INQUIRED ANEW AS TO WHEN THE COMPREHENSIVE UPDATED REPORT AND REQUESTS PROMISED BY WMFO WOULD BE FORTHCOMING.

WMFO IS REQUESTED TO EXPEDITE TRANSMISSION OF REPORT IN THIS MATTER BY EXPRESS MAIL.

CLASSIFIED BY [redacted] DECLASSIFY ON OADR

~~SECRET~~

'PFF DE PAR 0009 ~~S E C R E T~~

BT

#0009

~~SECRET~~

NNNN

CI-4
RUCG

[redacted]

b6
b7C

0002 MRI 00241

RR RUCNFB FBIWMFO

DE PAR #0010 2241208

ZNY SSSSS

R 120828Z AUG 91 0

~~SECRET~~

FM LEGAT PARIS (264A-WF-165334) (P)

TO DIRECTOR FBI/ROUTINE/

FBI WMFO/ROUTINE/

BT

~~SECRET~~

CITE: //5250:PAR189.221 9 AUGUST 1991//

PASS: HQ FOR [redacted] WMFO FOR [redacted]

b6 per FBI, DOS
b7C per FBI, DOS

[redacted]

b6 per FBI, DOS
b7C per FBI, DOS

THIS COMMUNICATION IS CLASSIFIED ~~SECRET~~ IN ITS ENTIRETY.

RE LEGAT PARIS TELETYPE DATED JUNE 21, 1991.

WMFO IS REMINDED THAT A COMPREHENSIVE UPDATED REPORT ON

UCFN ☑ Pos ☐ Neg

GENERAL INDICES:

☐ Automated Search

WF: ☐ Pos ☐ Neg AX: ☐ Pos ☐ Neg

☒ Manual Search

WF: ☐ Pos ☐ Neg AX: ☐ Pos ☐ Neg

264A-WF-165334-17

b6
b7C

EITHER MATTER WAS PROMISED TO [redacted] ON 5/20/91.

LEGAT PARIS REQUESTS THIS REPORT BE EXPEDITED FOR DISSEMINATION TO [redacted]

b6 per FBI, DOS
b7C per FBI, DOS
b7D per FBI, DOS

CLASSIFIED BY [redacted] DECLASSIFY ON OADR

BT

#0010

NNNN

[redacted] b6
b7C

C-14

FD-36 (Rev. 8-29-85)

FBI

TRANSMIT VIA:
☒ Teletype
☐ Facsimile
☐ AIRTEL

PRECEDENCE:
☐ Immediate
☐ Priority
☒ Routine

CLASSIFICATION:
☐ TOP SECRET
☐ SECRET
☐ CONFIDENTIAL
☐ UNCLAS E F T O
☒ UNCLAS

Date 8/18/91

FM FBI WMFO (264A-WF-165334) (P*)

TO DIRECTOR FBI/ROUTINE/

LEGAT PARIS/ROUTINE/

BT

UNCLAS

CITE: //3920//

PASS: FBIHQ CID, ECU - SSA [redacted] b6 b7C

SUBJECT: UNSUBS; UNAUTHORIZED ACCESS OF FEDERAL/FEDERAL INTEREST COMPUTERS; SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS; W.COM "WANK" WORM; OCTOBER, 1989; CFA; OO:WMFO.

RE LEGAT PARIS TELETYPES JUNE 21, 1991, AND AUGUST 12, 1991.

FOR INFORMATION OF FBIHQ AND LEGAT PARIS THIS CASE REMAINS IN A PENDING INACTIVE STATUS. WMFO HAS ONE AGENT ASSIGNED TO CFA CASES, AND HE HAS BEEN ASSIGNED TO HANDLE

264A-WF-165334-18

Approved: RMB/HJH Original filename: SUB 00/W.231

Time Received: ______ Telprep filename: SUB 00/80231

MRI/JULIAN DATE: 1928/231 ISN: 039

FOX DATE & TIME OF ACCEPTANCE: 8.19.91 6:56 pm

OTHER CFA MATTERS. REQUESTS FOR ADDITIONAL MANPOWER ARE PENDING AT FBIHQ.

LEGAT PARIS IS REQUESTED TO ADVISE [redacted] OF WMFO'S SITUATION. ALSO, PLEASE ADVISE THESE OFFICIALS THAT WMFO CONSIDERS THE WANK WORM INCIDENT TO BE A SIGNIFICANT CRIMINAL ACT, AND THAT APPROPRIATE INVESTIGATION WILL BE CONDUCTED WHEN SUFFICIENT STAFFING IS AVAILABLE.

b7D

BT

[illegible] MRI 01928

RR RUCNFE PAR

DE FBIWMFO #0039 2312356

ZNR UUUUU

R 192355Z AUG 91

FM FBI WMFO (264A-WF-165334) (P*)

TO DIRECTOR FBI/ROUTINE/

LEGAT PARIS/ROUTINE/

BT

UNCLAS

CITE: //3920//

PASS: FBIHQ CID, ECU - SSA SETTLE.

SUBJECT: UNSUBS; UNAUTHORIZED ACCESS OF FEDERAL/FEDERAL INTEREST COMPUTERS; SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS; W.COM "WANK" WORM; OCTOBER, 1989; CFA; OO:WMFO.

RE LEGAT PARIS TELETYPES JUNE 21, 1991, AND AUGUST 12, 1991.

FOR INFORMATION OF FBIHQ AND LEGAT PARIS THIS CASE REMAINS IN A PENDING INACTIVE STATUS. WMFO HAS ONE AGENT

264-WF-165334-18

PAGE TWO DE FBIWMFO 0039 UNCLAS

ASSIGNED TO CFA CASES. AND HE HAS BEEN ASSIGNED TO HANDLE OTHER CFA MATTERS. REQUESTS FOR ADDITIONAL MANPOWER ARE PENDING AT FBIHQ.

LEGAT PARIS IS REQUESTED TO ADVISE [redacted] b7D
[redacted] ALSO. PLEASE ADVISE THESE OFFICIALS THAT WMFO CONSIDERS THE WANK WORM INCIDENT TO BE A SIGNIFICANT CRIMINAL ACT. AND THAT APPROPRIATE INVESTIGATION WILL BE CONDUCTED WHEN SUFFICIENT STAFFING IS AVAILABLE.

BT

#0039

NNNN

Memorandum

To : SAC, WMFO (264A-WF-165334) (P*)   Date 9/12/91

From : SA [redacted] (C-14)

b6
b7C

Subject: UNSUB(S);
UNAUTHORIZED ACCESS OF FEDERAL/
FEDERAL INTEREST COMPUTERS;
SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND
HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS;
W.COM "WANK" WORM;
OCTOBER, 1989;
CFA
(OO:WMFO)

Attached is a paper entitled, "Beyond Preliminary Analysis of the WANK and OILZ Worms: A Case Study of Malicious Code." This paper was presented at the Workshop on Computer Security Incident Handling, August 6-8, 1991, in Herndon, VA. This workshop was jointly sponsored by the Computer Emergency Response Team (CERT), Software Engineering Institute, Carnegie Mellon University (funded by the Defense Advanced Research Projects Agency), and the Computer Incident Advisory Capability (CIAC) Team, University of California, Lawrence Livermore National Laboratory (funded by the Department of Energy).

264A-WF-165334-19

1-WMFO (Attachment)
JLK:jk

Beyond Preliminary Analysis of the WANK and OILZ Worms: A Case Study of Malicious Code

Thomas A. Longstaff and E. Eugene Schultz

University of California
Lawrence Livermore National Laboratory
L-303, PO Box 808
Livermore, CA 94550

e-mail: longstaf@llnl.gov/schultz3@llnl.gov
phone: 415-423-4416/415-422-7781

Abstract

In October, 1989 a DECnet worm attacked the NASA Space Physics Analysis Network (SPAN) and the DOE's High Energy Physics (HEP) and Energy Science (ES) Networks. Approximately two weeks later a second worm, a modification of the first, attacked additional systems. These worms (written in DCL) used several methods of propagation, including guessing accounts with an identical username and password and entering through system accounts and unpassworded accounts. The original version of the worm, WANK (Worms against Nuclear Killers), contained bugs preventing, among other things, penetration into unpassworded accounts. In the second version, OILZ, some of the problems of the first worm were corrected. OILZ intruded into user accounts probed from remote systems already breeched by this worm. OILZ masqueraded its presence and its method of discovering user accounts and privileged access helped circumvent standard VMS alarm settings. The style of each worm code indicated that the worm evolved over time and was not written by a single individual. This paper focuses on selected procedures from both variations of the worm and analyzes the authorship and history of the development of this worm. This information may be useful not only in determining the origin of this malicious code, but also in studying the evolution of malicious code.

This paper also presents some lessons learned from studying this attack and applies these lessons to recommendations for network policy. More than anything else, the WANK and OILZ worms demonstrate the need for effective password management and proper system and network configuration. Determining the source and style of malicious code can assist in developing policy and procedures for effectively detecting and preventing attacks of this type.

1. Introduction

The period from October to November, 1989 was an event-filled time for those of us on the Department of Energy's (DOE's) Computer Incident Advisory Capability (CIAC). The World Series was in town, with the Oakland A's fighting the San Francisco Giants in a Bay Area battle. This was interrupted by the 1989 San Francisco earthquake (at the time, the only reprieve for the overmatched Giants). Half of the CIAC team members were on travel, presenting a workshop on handling major computer security incidents, while back at home, a worm identified as WANK (Worms against Nuclear Killers) was attacking hundreds of VMS systems around the European SPAN, NASA SPAN, and HEPNET networks.

The worm attacks, lasting for a total of five weeks, grabbed the attention of incident response teams, system administrators, users, the media, and others, as each reacted to this threat. Whenever a system was infected with WANK or OILZ, the damage ranged from worm spread quickly throughout the U.S. due to the pervasive nature of the vulnerabilities exploited by the worm. Since this worm would infect an individual host repeatedly, the code quickly used up a large number of computing resources across the US. The amount of media attention brought the term "worm" to the public's vocabulary. In the aftermath of this worm attack, many response teams (including the CIAC team) were formed to coordinate responding to this type of incident, as well as related threats.

1.2. The Response Process during the Attack

We are not aware of any prescribed process for responding to malicious code. Intuitively, the first step is to detect the presence of the malicious code. In the case of the WANK/ OILZ attack, detection was trivial. Users of systems successfully attacked by the worm quickly noticed symptoms such as unusual screen writes and frequently reported these and other observations to their system administrators. Similarly, system managers of such systems rapidly noticed an unusual process as well as other systems and often contacted a variety of people at the particular site/institution and/or called an incident response team.

Another step in responding to malicous code is to determine the results (e.g., damage) of executing this code. This does not necessarily require a complete reverse engineering effort; confirmation of reported systems may be sufficient to form workable hypotheses. In the case of the WANK/OILZ incident, however, this step was arduous, because it was difficult to determine whether there was one or more than one worm. Computers at a wide variety of sites and organizations were attacked. Consequently, computer scientists obtained copies of the worm within the same approximate time window and started to analyze the worm and its effects independently. Small errors in different individuals' analysis made it difficult to determine whether one or more than one worm had attacked DECnet systems, thereby hindering analysis of the worm's effects. Ultimately, obtaining multiple instances of the worm (which proved to be a slow process), then comparing each instance led to the conclusion that there was initially one version of the worm. By that time, reverse engineering efforts were well underway. Had there been a mechanism for rapidly sharing the various instances of WANK that were discovered among trusted individuals and for coordinating efforts of the various people responding to this incident, this step would have required considerably less time.

The next step in responding to malicous code such as a worm is determining how the code is transmitted and how execution on a remote system is initiated. This step is useful in containing the spread of the code in that it may lead to blocking future infections or otherwise protecting an attacked system by early detection of a worm's attempts to penetrate a that system. As stated previously, the reverse engineering efforts were well underway by the time it was determined that there was one version of the worm. The proliferation routine (as discussed below) was reverse engineered with little subsequent delay.

Once transmission/proliferation mechanisms are understood, immunization scripts can be written to prevent penetration of additional systems and eradication scripts can be developed to destroy the malicious code and clean any successfully attacked systems from the results of the attack. This step was a critical step in responding to the worm because an important decision had to be made--was it more important to concentrate on eradicating the worm from systems already penetrated, or was it better to focus on immunizing other systems from the attack? At this point, three individuals, one from Fermi National Laboratories, one from NASA Goddard Space Center, and one from Lawrence Livermore National Laboratory, emerged as leaders in the development effort. They determined that it was more important to produce immunization scripts to contain the rapid spread of the worm. If the worm had systematically destroyed each system it attacked, and if the worm evolution, style, and authorship of the two versions of this worm. The code maintained all of the original variable names, capitalization and other coding style clues that allow at least some level of reconstruction of the history of this code to be attempted.

In this section, the WANK/OILZ worm incident will be described, with an overview description of the worms themselves. The sequence of events was critical during the analysis process and the amount of detail available at any point in time during the event changed the perception and actions associated with handling the event.

2.1. Timeline

The following unfolds some of the events surrounding the WANK/OILZ incident as it was handled by the CIAC team.

Oct. 16
- 4:30am, first report from University of Rhode Island
- Preliminary WANK analysis (in sections)
- Span Notice on WANK
- Many mail gateways closed down
- Commands to kill WANK
- Dummy program to block WANK
- Found at least two versions
- Report on WANK (minor errors)
- CIAC notice A-2 describing the worm

Oct. 17
- Many reports on systems hit
- CERT Advisory
- California Earthquake 1700 PDT
- Correction to Oct. 16 notice (passwords sent to GEMPAK rather than GEMTOP account)
- Script created and distributed to kill worm and monitor systems (Terminate.com)
- Press involvement

Oct. 18
- SPAN and CIAC fixes - netupdate.com
- Still recording hits
- Info from worm retrieved in Saclay France
- More scripts to kill the worm available (Check_System.com)

Oct 19
- More detailed reports of worm action and prevention
- Anti-worm scripts
- Very few hits
- New York Times and Wall Street Journal (stated that it was an internet worm)

Oct 20
- Fewer hits
- Password checkers become available
- Analysis interest in worm drops off
- CIAC Notice A-3 - available scripts for WANK

Oct 23 - 24
- No real hits - CIAC considers putting out an All-Clear
- Federal Computer Week article

Oct 29
- Probes on HEPNET - possible second worm

Oct. 30
- Span Notice on OILZ

```
          \                                                   /
           \    Your System Has Been Officically WANKed      /
            \_____________________________________________/

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

The next step was to check for SYSPRV (SYStem PRiVileges), and, if found, to disable mail to the system account. This would prevent the system manager, operating under the system account, from receiving mail about this worm attack. No other mail access was affected.

The worm would then check again for SYSPRV access, and if found, would change the startup file executed by users on login. This change would redefine the DIR command to simply print a string representing no files found. The startup file would also print "OOPS!" and show output that appeared to delete all files in the users account. This code would not actually delete files, but would make it appear as if it had. The redefinition of the DIR command was designed to further convince the user that all files had been deleted.

Once these mildly irritating steps were complete, WANK then attempted to modify all .COM files on the system[2]. This had the effect of creating a trojan horse in all writable .COM files that would activate when a privileged user executed the command file. This back door could later be used by the creator of the worm to gain privileged access through the FIELD account on the system. The trojan horse checked for privilege, and, if found, the trojan code would add or modify the FIELD account on the system. The modification would change the password of the FIELD account to FIELD (this is commonly referred to as a "JOE" account) and change the privilege to SETPRV (set any privilege).

At this point, the worm began an infinite loop to spread itself to other systems. This loop consisted of the following steps:

1. Select a DECNET node number at random (the victim node) from all possible node numbers.
2. Attempt to use the PHONE object to find all users logged into the system.
3. Pick a user at random from (2), and send a random message to that user through the PHONE object.
4. Attempt to do a default copy of the RIGHTSLIST.DAT file from the victim node.
5. If the copy was successful, use all the usernames in the file and determine whether the password of that account is null or equal to the username. If the copy failed, goto step 8
6. If step 5 returns true, determine if the account has access to modify the SYSUAF.DAT file (the password file on a VMS machine). Add the successful username to the built-in list of usernames stored in the WANK worm (to be used in step 8)
7. If a privileged account is found, use that account to copy the worm to that remote location and start the execution of the remote worm and begin from step 1 again.
8. For each username saved in the worm, attempt to connect to the victim node using passwords equal to the username and to null (a bug in the code prevented this from working properly in all cases. See the OILZ description below).

[2] A .COM file on a VMS system represents a DCL script file. This is a plain text file containing a sequence of DCL commands to be executed by the system.

3.1.1. The Proliferation Section

The core of the worm consists of a proliferation section of code. This code starts with a very careful check for access to the current directory (using a subroutine FIXPROT) and a resetting of all commands it will be using. The code to spread the worm is written in an assembler style that uses self-modifying techniques to expand a list of usernames successfully attacked. This self-modification would occui when the system penetrated an account which had not been penetrated by any of that worm's ancestors. The account name would be added to the list to be tried on other hosts. This actually had the effect of making the worm's length variable depending on how many accounts had been penetrated in the past by the direct ancestors of the worm.

Taken out of the context of the rest of the WANK/OILZ worms, the proliferation sections were a well-written algorithm that would use quiet, careful steps to spread and begin execution on other systems. The proliferation section would prefer privileged accounts (which would support other modifications to the system). The privilege of an account would be determined by attempting a default open to the SYSUAF.DAT file, the password file on a VMS system. If the default open was successful, the worm would mark that this account had sufficient privilege to add or modify existing accounts.

The WANK worm was designed to try three forms of attack. First, the worm would attempt to copy the remote RIGHTSLIST.DAT file from the remote host, to provide a complete list of account names to attempt. If this attempt failed, the system would use the built-in list of usernames that was accumulated over time based on previously penetrated accounts.

Once a list of accounts was taken, the worm would try to copy a short, executable file to each account using: 1) an identical username - password combination (a "joe" account), or 2) a null password. Only these two attempts were made on each account. If this copy was successful, the file copied would be the FIXPROT routine mentioned above. The worm would then attempt to execute the FIXPROT code remotely, assuring that the worm could spread to that account. If successful, the worm would store that username as a possible attack vector on the victim system. If unsuccessful, the worm would continue with the next username in RIGHTSLIST.DAT.

The other form of attempted entry into systems was using the default DECNET account and the FAL object to copy and start the worm code. This code was not exercised in the WANK worm, but the OILZ worm corrected a bug in the logic that allowed this code to be activated.

The code was written as a series of short segments that were connected together by if statements and gotos. As an example, consider the following segment:

```
$getnextnode:
$on error then continue
$range=64512
$gosub random
$nodenum=value
$checknode=nodenum
$gosub checknode
$if .not. up then goto getnextnode
$reploop:
$on error then continue
$mustfind:
$on error then continue
$ gosub finduser
$ if .not. gotl then goto mfind
```

Each of these routines caused different levels of damage. The "announce" routine modified the system login banner, replacing it with the "Worms against nuclear killers" banner, but did not modify or delete any other system or user file. Other routines were not so benign.

The fixmail routine checked for system access and then disabled mail to the system account. The apparent purpose of this code was to prevent eradication scripts or other information from reaching the node, but, in fact, it did cause damage in that the system account could not receive mail of any kind. On VMS systems where the system account was used extensively, the damage caused by this was for the system to be off the network until the mail facility was repaired.

The code then checked for SYSPRV once again, and, if found, would proceed to install a trojan horse program in every user's startup file. The code would print "OOPS!" to the user and then proceed to appear to delete the user's files. It would then redefine the directory command to display a string indicating "no files found". When a user logged in and saw what looked like a complete deletion of the files, the first command executed was usually the directory command (to be sure the files were gone). The damage caused by this particular "joke" was to cause frightened users to restore files in the account from a backup, completely erasing the current files in the directory.

The last action taken by the worm was to scan the entire file system for DCL scripts that the program could modify. Whenever one was found, the system would add a trojan horse that would check for privilege, then add or modify the FIELD account on the system to have full privileges and a password of FIELD. On many systems, this segment of the code did the most damage, since every writable DCL script on the system was modified to add a "backdoor" to the system.

3.1.3. Putting it all together

The remaining portions of the code were designed to connect all the above parts of the code together. Mostly this was in the form of gosub statements and initialization statements to start and setup the execution of the worm. This portion of the worm had several coding errors in its first release, which were repaired in the release of the OILZ worm. Because of the nature of the looping and gotos based on variable settings, tracing the execution of this worm was not trivial. Numerous bugs in the initial release of WANK suggest that this task was also not trivial for the person putting the worm together for release!

3.2. Determining Authorship

There were many clues in the code to determine which portions were written by distinct authors. These clues were stylistic in nature, depending on the choice of variable names, capitalization, and flow control. An analysis of the code seems to produce at least three distinct authors, the characteristics of each will be listed below.

3.2.1. Proliferation Author

The above section of code (lines 84-118) show the style of the author of the proliferation sections. These sections make up the main body of the worm, and are the framework on which the rest of the functionality depends. The code has the following characteristics:

1. Variable names are descriptive and in lower case.
2. The flow control is based on variables and goto statements, with some dependence on subroutines.
3. Use of remote access requires a high level of understanding on VMS, networking, and DCL commands.
4. The flow of execution is convoluted and complex.

1. Mixed upper and lower case for commands and variable names.
2. Use of non-descriptive letters for variables.
3. Simple, BASIC style coding.
4. Attempts to repair other bugs in the code.

It is likely that this author used the WANK attack to determine bugs in the code which were repaired in the OILZ version of the code.

4. Conclusions and Lessons Learned

4.1 The Cause

The vulnerabilities exploited by the WANK/OILZ worms were not new, exotic software bugs. Instead, these vulnerabilities have been well known in VMS systems for some time. Most notably, accounts with a null or easily guessed password provided an easy route into these systems. The WANK worm checked only for passwords identical to the username of a given account, yet this worm was quite successful on a large number of systems. OILZ added only the ability to use the default file and execution access (default DECnet and FAL object) of the VMS system, and was even more successful, even though the vulnerabilities exploited by the WANK worm were well understood. This demonstrates that at the time of the WANK/OILZ attack, there were many system maintenance-level problems involving password maintenance and pre-shipped accounts. Recent releases of VMS (5.4) have made the task of password maintenance easier, but there are still many older releases on the network. Furthermore, even these newer releases must have these password maintenance features activated to be effective. It is likely that many systems connected to DECnet would still be at risk if a worm similar to WANK/OILZ were released today.

4.2 The Response

There was a high level of communication between individuals responding to the WANK/OILZ incident. In comparison, during the Morris Worm incident of 1988, the Internet was so clogged with packets that electronic communications about handling the worm could not be distributed between experts and system administrators. The WANK/OILZ incident did not involve such a reduction in network access, and, correspondingly, the speed at which information about the worm and how to eradicate it was quickly spread to the affected systems. This level of communications occurred despite that fact that much of the communication about this incident took place over the same network used to propagate the worm. If a major incident were to occur today, a major concern would be how communications between experts and system administrators would occur if the Internet were not available. We fear that there is currently too little planning for backup communications during incidents.

Coordination between involved parties in handling the WANK/OILZ worms was fairly good overall. The information shared between experts and system administrators was mostly clear and useful. For example, several effective immunization/ eradication scripts became available shortly after the worm was discovered on the networks; these scripts saved a large number of systems from attack and eradicated the worm from many others. However, not all the coordination and information exchange was beneficial. As stated previously, small analysis errors in an early report on the worm caused considerable confusion as the number of versions of the worm attacking the network was drawn into possibility of penetrating systems, WANK/OILZ added a simple password cracking mechanism. In this way, WANK/OILZ was more sophisticated, and was able to penetrate a greater number of systems.

Another reason for the greater success of the WANK/OILZ compared to Father Christmas was the increased connectivity of the DECnet community one year later. As DECnet Phase IV is installed, more of the local DECnet networks are becoming vulnerable to attacks such as those attempted by WANK/OILZ. The use of "Poor Man's Routing[3]," while more inconvenient to the user of a DECnet system, provides some isolation to a worm attack. This is because the worm must first penetrate the gateway machine of a local network before any of the other systems on that network become visible. This suggests that one protection mechanism that could be used is the concept of a *firewall* system to isolate a local network from the rest of the world at large. This would require a worm or other attack to first penetrate the firewall machine, which could be more thoroughly protected then the other individual nodes on the network. Services required by the users of the network can be configured to pass through the gateway without additional effort on the part of the user (Longstaff, in press).

As was shown above, the WANK/OILZ worms were written by different authors and each apparently had a different purpose. The author of the proliferation sections seemed to be interested in experimentation with proliferation mechanisms and could have had a possible political motivation for this attack. The WANK banner installed suggests that any political motivation involved opposition to government laboratories and networks that support nuclear weapon design or construction, or possibly to a then impending NASA rocket launch involving nuclear materials.

The author of the sections containing the malicious alterations of accounts and system files seemed demonstrated sexist inclinations (as suggested by some of the PHONE messages delivered to random users). This author also appeared to be motivated by hostility (as suggested by the tone of the messages as well as the destructive nature of trojan horse programs installed in users' startup files and DCL files). Some of these goals appeared to be shared by the assembler author who combined the various parts of the worm for release. This author appeared to be interested in installing back doors into penetrated systems and sending that information to a node for later collection. Also attributed to these authors is the code to modify and add the FIELD account and the code to assure that the trojan horse modifying this account was distributed as widely as possible through the penetrated system. The nature of this segment of the WANK/OILZ worms reinforces the speculation concerning the possible motivation of these authors.

As mentioned previously, the WANK worm contained a routine to notify an identified node of the penetrated system name. This notification code was removed in the OILZ version of the worm, suggesting perhaps that the authors of this worm realized that this notification would aid in the trace of WANK to its source. The also points out that the authors were aware of the progress and analysis of the WANK worm attack and used this information to modify WANK to create OILZ. This is an extremely important aspect of handling a worm attack; individuals responding to the attack should consider that information about the course of the attack is probably being received by the author(s) of the attacking code itself. Wider distribution of information from response teams, vendors, etc. in the future assures that this will be a problem of greater magnitude.

[3] Poor-Man's Routing is a method of addressing a node through the specification of the path to that node. All intermediate systems used to bridge to that node must be specified.

Longstaff, T .A., "DOE Site Computer Security Criteria," University of California Technical Report, in press.

McLean, J., "The Specification and Modeling of Computer Security." *IEEE Computert*, V23:1, 1990.

Schultz, E. E., Brown, D.S., & Longstaff, T.A., "Responding to Computer Security Incidents: Guidelines for Incident Handling." University of California Technical Report UCID-ID-104689, Livermore, CA, 1990.

Memorandum

To : SAC, WMFO (264A-WF-165334) (P*) Date 9/12/91

From : SA [redacted] (C-14)

b6
b7C

Subject: UNSUB(S);
UNAUTHORIZED ACCESS OF FEDERAL/
FEDERAL INTEREST COMPUTERS;
SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND
HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS;
W.COM "WANK" WORM;
OCTOBER, 1989;
CFA
(OO:WMFO)

Attached is a listing provided by [redacted] [redacted] during a meeting at WMFO, NVMRA on 5/30/91. [redacted] [redacted] believes the worm may have in fact been developed outside of France and provided the attached listing as an indication of the possible sources. It should be noted [redacted] has other source addresses in Australia and elsewhere, the exact details of which were not disclosed.

b6
b7C
b7D
b7E

264A-WF-166334-20

1-WMFO (Attachment)
JLK:jk

Date	Heure	NR
11.08.89	13.46	3110305003380000
11.08.89	15.18	3110 "
11.08.89	15.34	3110 "
11.08.89	15.58	"
11.08.89	16.4	"
11.08.89	17.33	"
26.08.89	05.36	3110612000720000
23.10.89	21.32	3110321070350000
23.10.89	21.34	"
28.10.89	12.48	3110208000700000
28.10.89	12.49	"

Numéro français appelé : 2080691101062

heures françaises

FD-36 (Rev. 8-29-85)

FBI

TRANSMIT VIA:
□ Teletype
□ Facsimile
☒ AIRTEL

PRECEDENCE:
□ Immediate
□ Priority
□ Routine

CLASSIFICATION:
□ TOP SECRET
□ SECRET
□ CONFIDENTIAL
□ UNCLAS E F T O
□ UNCLAS

Date 10/23/89

TO : DIRECTOR, FBI

FROM : SAC, WMFO (264A-WF-) (P) (C-9, NVMRA)

UNSUB(S);
UNAUTHORIZED ACCESS OF FEDERAL/
FEDERAL INTEREST COMPUTERS;
SPACE PHYSICS ANALYSIS NETWORK (SPAN) AND
HIGH ENERGY PHYSICS NETWORK (HEPNET) - VICTIMS;
W.COM "WANK" WORM;
OCTOBER, 1989;
CFA
(OO:WMFO)

On 10/16/89, WMFO SA [redacted] was advised by [redacted], Network Security Officer, MILNET (Defense Communications Agency Military Network), that a worm (a form of malicious software code that moves by itself from computer to computer on a network) was on DECNET (a commercial network run by the Digital Equipment Corporation). It was effecting the National Aeronautics and Space Administration's (NASA) Space Physics Analysis Network (SPAN) and the Department of Energy's (DOE) High Energy Physics Network (HEPNET).

b6
b7C

The following is a summary of selected additional telephonic conversations:

On 10/16/89, [redacted] Computer Emergency Response Team (CERT), Software Engineering Institute (funded by the Defense Advanced Research Projects Agency), Pittsburgh, Pennsylvania, advised the worm (W.COM) was entering DEC VAX/VMS hosts on DECNET. Upon successful penetration, it was

DUE(INFO) BKD
FRAIN(INFO) JRL

2-FBIHQ
2-WMFO
JLK:jk
(4)

264A-WF-165334 -1

264A-1024

[redacted]

10-23-

93

b6
b7C

Approved: ______ Transmitted ______ (Number) (Time) Per [redacted]