Software Engineering Institute
Carnegie Mellon University

1999 CERT Incident Notes

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 IN-99-01: "sscan" Scanning Tool

Thursday, January 28, 1999

Recently a new scanning tool named "sscan" was announced on various public mailing lists. This tool is a derivative of the "mscan" tool that was widely used against a large number of sites in the second half of 1998. For more information about mscan, please read our earlier Incident Note IN-98.02: http://www.cert.org/incident_notes/IN-98.02.html

The sscan tool performs probes against victim hosts to identify services which may potentially be vulnerable to exploitation. Though sscan itself does not attempt to exploit vulnerabilities, it can be configured to automatically execute scripts of commands that can be maliciously crafted to exploit vulnerabilities. Thus, it is possible for an unpredictable set of attacks to be mounted against a victim site in conjunction with the sscan probes.

The documentation distributed with sscan includes an example set of scripted commands illustrating how a self-replicating attack might be crafted using well known vulnerabilities detected by sscan. We encourage you to familiarize yourself with the actions sscan performs and to insure that your site is not vulnerable to attack.

The current version of sscan has been written specifically to execute on a UNIX platform. Because the tool crafts packets with custom attributes, privileged access to the source host is required to run sscan. We encourage you to be mindful of the potential for intruder control of the source host when responding to an incident involving sscan probes.

To determine whether the sscan tool is possibly being used against your site, look for the following activity:

1. Initial probes to selected services to determine the availability of the target host. TCP ACK packets are sent to the target host with the source and destination ports set as follows:
    - source and destination TCP port 23 (telnet)
    - source and destination TCP port 25 (smtp)
    - source and destination TCP port 110 (pop3)
    - source and destination TCP port 143 (imap)
    - source and destination TCP port 80 (www)

    As currently configured, the sscan tool will not attempt to probe a host further if no response is received from these initial probes.

2. If any of the above probes receives a response, further probes are made to the target host in an attempt to identify potential vulnerabilities. Connection probes to the following TCP ports are user optional and may or may not appear in additional sscan activity. The TCP ports are listed in the order in which they currently would be probed by sscan.
    - 80 (www)
    - 23 (telnet), 143 (imap), 110 (pop3) [all three, or none, are probed]

- 111 (sunrpc)
- 6000 (x11)
- 79 (finger)
- 53 (domain)
- 31337 (unassigned by IANA)
- 2766 (Solaris listen/nlps_server)

Connection probes to the following TCP ports are always attempted and are not user optional. The TCP ports are listed in the order in which they are probed by sscan.

- 139 (netbios-ssn)
- 25 (smtp)
- 21 (ftp)
- 22 (ssh)
- 1114 (Linux mSQL)
- 1 (tcpmux)

Ports responding to the probes in this section are considered by sscan to be "open" ports.

3. Two types of probes are made in an attempt to identify the target host's operating system.
   - TCP connection probe to port 23 (telnet) to obtain the login banner
   - Probes attempting to identify system and network architecture similar to those discussed in CERT Incident Note IN-98.04:

     http://www.cert.org/incident_notes/IN-98.04.html

     In this case, five packets are sent to the target host on the first TCP port identified as being "open" in the previous scanning (section 2). The five packets have the following characteristics:
     - Packet #1 - SYN ACK packet from source TCP port 1
     - Packet #2 - FIN packet from source TCP port 2
     - Packet #3 - FIN ACK packet from source TCP port 3
     - Packet #4 - SYN FIN packet from source TCP port 4
     - Packet #5 - PUSH packet from source TCP port 5
4. Using information gathered from the probes, sscan attempts to determine if the target host may potentially have any of the following accessible information services or known vulnerabilities:
   - qpopper - see
     http://www.cert.org/advisories/CA-98.08.qpopper_vul.html
     ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-98.01.qpopper.buffer.overflow.vul
   - imapd - see
     http://www.cert.org/advisories/CA-98.09.imapd.html
     http://www.cert.org/advisories/CA-97.09.imap_pop.html
   - SMTP EXPN command
   - Solaris listen/nlps_server (port 2766)
   - Linux mSQL (port 1114)

- BIND - see http://www.cert.org/advisories/CA-98.05.bind_problems.html
- Various CGI-BIN vulnerabilities - see http://www.cert.org/tech_tips/cgi_meta-characters.html
  - phf - also see http://www.cert.org/advisories/CA-96.06.cgi_example_code.html
  - handler - also see ftp://ftp.cert.org/pub/cert_bulletins/VB-97.07.sgi
  - Count.cgi - also see http://www.cert.org/advisories/CA-97.24.Count_cgi.html
  - test-cgi - also see http://www.cert.org/advisories/CA-97.07.nph-test-cgi_script.html
  - php.cgi - also see ftp://ftp.auscert.org.au/pub/auscert/ESB/ESB-97.047
  - webgais
  - websendmail
  - webdist.cgi - also see ftp://ftp.cert.org/pub/cert_bulletins/VB-97.07.sgi
  - faxsurvey
  - htmlscript
  - pfdisplay.cgi
  - perl.exe (Windows platforms)
  - wwwboard.pl (Windows platforms)
- NFS filesystems exported to everyone - see http://www.cert.org/advisories/CA-94.15.NFS.Vulnerabilities.html
- mountd - see http://www.cert.org/advisories/CA-98.12.mountd.html
- rstatd - see http://www.cert.org/advisories/CA-97.26.statd.html
- nlockmgr
- rpc.nisd - see http://www.cert.org/advisories/CA-98.06.nisd.html
- X11 (open X servers)
- Wingate - see http://www.cert.org/vul_notes/VN-98.03.WinGate.html
- Finger (optional) - The default behavior is to perform finger on 'root' and 'guest' accounts. Target accounts are configurable and may differ from the defaults mentioned here.

5. At this point, there may be additional, unpredictable activity if sscan is configured to execute user crafted scripts of commands.

If any machines in your network use any of the above services, we encourage you to make sure that all patches are up to date and your machines are properly secured.

We also urge you to filter all traffic at your firewall except that which you explicitly decide to allow. Please read our packet filtering tech tip for more information: http://www.cert.org/tech_tips/packet_filtering.html.

Sites using UNIX systems may also wish to consult the following documents:

http://www.cert.org/tech_tips/unix_configuration_guidelines.html
ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist

CERT/CC wishes to thank AusCERT for their assistance in developing this Incident Note.

This document is available from: http://www.cert.org/incident_notes/IN-99-01.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

2 IN-99-02: Happy 99 Trojan Horse

Monday, March 29, 1999

Overview

Around January 20, 1999, we began receiving reports of a Trojan horse program named Happy99.exe. Anti-virus vendors have given this program the following names: SKA, WSOCK32.SKA, SKA.EXE, I-Worm.Happy, PE_SKA, Trojan.Happy99, Win32/SKA, and Happy99.Worm.

Description

The first time Happy99.exe is executed, a fireworks display saying "Happy 99" appears on the computer screen and, at the same time, modifies system files. The executable affects Microsoft Windows 95/98 and NT machines by

- copying the WSOCK32.DLL file to WSOCK32.SKA
- modifying the WSOCK32.DLL file, which is used for Internet connectivity
- creating files called SKA.EXE and SKA.DLL in the system directory
- creating an entry in the registry to start SKA.EXE

Once Happy99 is installed, every email and Usenet posting sent by an affected user triggers Happy99 to send a followup message containing Happy99.exe as a uuencoded attachment. Happy99 keeps track of who received the Trojan horse message in a file called LISTE.SKA in the system folder. Note that messages containing the Trojan horse will generally appear to come from someone you know.

Solutions

You can prevent the spread of the Happy99 by setting the WSOCK32.DLL file attributes to "read only".

Most virus scanning tools will detect and clean Happy99 from a system. Happy99 can be manually removed from affected systems. You can find the steps for this procedure at the following site: http://www.symantec.com/avcenter/venc/data/happy99.worm.html.

To detect and remove current viruses, you must update your scanning tools with the latest virus signatures or definitions. We also recommend you contact all of the people listed in the LISTE.SKA file. This file lists of other people that may have received the Happy99 Trojan horse from you.

It is important to take great caution with any email or Usenet attachments that contain executable content. If attachments are in a message, we recommend that you save the file to the local drive and scan the file with a virus scanning product before you open or run the file. Be aware that this

is not a guarantee that the contents of the file are safe, but it will check for viruses and Trojan horses that your scanning software can detect.

Not the Same as Melissa

Happy99 is not a macro virus and should not be confused with the Melissa Word macro virus. Further information about the Melissa Word macro virus can be found at the following site: http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html.

Happy99 vs. Melissa Word Macro Virus

	Happy 99	Melissa
How does it propagate?	email or Usenet attachment	email or Usenet attachment
Where does it reside?	Modified WSOCK32.DLL	Macro in Microsoft Word documents
Who is it sent to?	The recipients of the last message you sent out that are not in the LISTE.SKA file	First 50 entries in each address book

This document is available from: http://www.cert.org/incident_notes/IN-99-02.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/..

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

3 IN-99-03: CIH/Chernobyl Virus

Thursday, April 22, 1999

Friday, April 23, 1999 -- Updated vendor information

Monday, April 26, 1999 -- Updated vendor information, added FAQ

Overview

We have received a number of information requests about a computer virus named CIH. Anti-virus vendors have given this virus the following names: CIH, Win95.CIH, PE_CIH, Win32.CIH, and W95/CIH.1003. The virus has also been called the Chernobyl virus. Some versions of the CIH virus become active on April 26, 1999 which is the 13th anniversary of the Chernobyl disaster.

In addition to this Incident Note please see the CIH FAQ (Frequently Asked Questions) document: http://www.cert.com/tech_tips/CIH_FAQ.html.

Description

The CIH virus infects executable files and is spread by executing an infected file. Since many files are executed during normal use of a computer, the CIH virus can infect many files quickly.

There are several variants of the CIH virus. Some activate every month on the 26th, while other variants activate just on April 26th or June 26th. Once the CIH virus activates, the virus attempts to erase the entire hard drive and to overwrite the system BIOS. Some machines may require a new BIOS chip to recover if overwritten by the CIH virus. CIH only affects Win95/98 machines.

More technical details about the CIH virus can be found at the following site: http://www.virusbtn.com/VirusInformation/cih.html.

Solutions

The following items will help to prevent the CIH virus from deleting your data or writing to the BIOS, but if your computer has already been damaged by the CIH virus the following will not help to recover. If your computer has been damaged by the CIH virus we recommend you contact your computer vendor or motherboard vendor to find out how to recover the system BIOS. The data on the hard drive might not be recoverable, but a data recovery service might be able to retore some portion of the data.

Many motherboards have a "jumper" that will enable or disable the ability to write to the BIOS. To prevent the CIH virus or any other program from writing to your computer BIOS, we recommend that you set the motherboard jumpers so that the BIOS can not be modified. Some motherboards vendors may ship with the jumper set in the writable/programmable mode for the BIOS.

This is a known virus and anti-virus vendors are able to detect the CIH virus. To detect and remove current viruses, you must update your scanning tools and anti-virus software with the latest virus signatures or definitions. To properly clean the CIH virus we recommend booting an infected computer from a clean floppy diskette (one that is not infected) and then run anti-virus software.

Vendor Information

Below is a list of anti-virus vendors that have futher infomation and tools relating to the CIH virus.

Computer Associates InoculateIT

http://www.cai.com/virusinfo/melissa_virus.htm#cih

Current Virus Signature Versions that Detect and Cure the CIH virus are as follows:

- Any version of InoculateIT signature file later than 4.15 will detect and cure CIH.
- Current version of InoculateIT signature file is 4.20.

Any of the above virus signatures files can be downloaded at www.support.cai.com

Data Fellows F-Secure Anti-Virus

http://www.datafellows.com/cih/

Network Associates/McAfee

http://www.avertlabs.com/public/datafiles/valerts/vinfo/spacefiller411.asp

ProLand Software

http://www.pspl.com/faqs/cihfaq.htm

http://www.pspl.com/download/cleancih.htm

Sophos

http://www.sophos.de/companyinfo/pressrel/uk/19990310chernobyl.html

Symantec/Norton AntiVirus

http://www.symantec.com/avcenter/venc/data/cih.html

http://www.symantec.com/avcenter/kill_cih.html

TrendMicro

http://216.33.21.51/vinfo/virusencyclo/default3.asp?VCode=EN001344

This document is available from: http://www.cert.org/incident_notes/IN-99-03.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

4 IN-99-04: Similar Attacks Using Various RPC Services

Updated: December 9, 1999 (added information about IN-99-07)
Updated: October 15, 1999 (added information about statd exploit)
Thursday, July 22, 1999

Overview

We have received reports that intruders are using similar methods to compromise systems. We have seen intruders exploit three different RPC service vulnerabilities; however, similar artifacts have been found on compromised systems.

Vulnerabilities we have seen exploited as a part of these attacks include:

- CA-99-08 - Buffer Overflow Vulnerability in rpc.cmsd
  http://www.cert.org/advisories/CA-99-08-cmsd.html
- CA-99-05 - Vulnerability in statd exposes vulnerability in automountd
  http://www.cert.org/advisories/CA-99-05-statd-automountd.html
- CA-98.11 - Vulnerability in ToolTalk RPC Service
  http://www.cert.org/advisories/CA-98.11.tooltalk.html

Description

Reports involving these vulnerabilities have involved very similar intruder activity. The level of activity and the scope of the incidents suggests that intruders are using scripts to automate attacks. These attacks appear to attempt multiple exploitations but produce similar results. We have received reports of the following types of activity associated with these attacks:

- Core files for rpc.ttdbserverd located in the root "/" directory, left by an exploitation attempt against rpc.ttdbserverd
- Files named callog.* located in the cmsd spool directory, left by an exploitation attempt against rpc.cmsd
- Exploitations that execute similar commands to create a privileged back door into a compromised host. Typically, a second instance of the inetd daemon is started using an intruder-supplied configuration file. The configuration file commonly contains an entry that provides the intruder a privileged back door into the compromised host. The most common example we have seen looks like this:

  ```
  /bin/sh -c echo 'ingreslock stream tcp wait root /bin/sh -i' >>

  /tmp/bob;/usr/sbin/inetd -s /tmp/bob
  ```

  If successfully installed and executed, this back door may be used by an intruder to gain privileged (e.g., root) access to a compromised host by connecting to the port associated with the ingreslock service, which is typically TCP port 1524. The file names and service names are arbitrary; they may be changed to create an inetd configuration file in a different location or a back door on a different port.

The /tmp/bob directory has also been evident in exploits against the statd vulnerability. The most common example we have seen for statd looks like this:

```
/var/statmon/sm/; echo "pcserver stream tcp nowait root /bin/sh sh -i" >>
  /tmp/bob ; /usr/sbin/inetd -s /tmp/bob
```

- In many cases, scripts have been used to automate intruder exploitation of back doors installed on compromised hosts. This method has been used to install and execute various intruder tools and tool archives, initiate attacks on other hosts, and collect output from intruder tools such as packet sniffers.

  One common set of intruder tools we have seen is included in an archive file called neet.tar, which includes several intruder tools:

  - A packet sniffer named update or update.hme that produces an output file named output or output.hme
  - A back door program named doc that is installed as a replacement to /usr/sbin/inetd. The back door is activated when a connection is received from a particular source port and a special string is provided. We have seen the source port of 53982 commonly used.
  - A replacement ps program to hide intruder processes. We have seen a configuration file installed at /tmp/ps_data on compromised hosts.

  Another common set of intruder tools we have seen is included in an archive file called leaf.tar, which includes serveral intruder tools:

  - A replacement in.fingerd program with a back door for intruder access to the compromised host
  - eggdrop, an IRC tool commonly installed on compromised hosts by intruders. In this activity, we've seen the binary installed as /usr/sbin/nfds
  - Various files and scripts associated with eggdrop, many of which are installed in the directory /usr/lib/rel.so.1
  - A replacement root crontab entry used to start eggdrop

  It is possible that other tools and tool archives could be involved in similar activity.

- Installation of distributed denial of service tools. For more information, see

  IN-99-07, Distributed Denial of Service Tools

- In some cases, we have seen intruder scripts remove or destroy system binaries and configuration files.

Solutions

If you believe a host has been compromised, we encourage you to disconnect the host from the network and review our steps for recovering from a root compromise:
http://www.cert.org/tech_tips/root_compromise.html

In many cases intruders have installed packet sniffers on compromised hosts and have used scripts to automate collection of the output logs. It may be the case that usernames and passwords used in network transactions with a compromised host, or on the same network segment as a compromised host, may have fallen into intruder hands and are no longer secure. We encourage you to address password security issues after any compromised hosts at your site have been secured.

You should also review the state of security on other hosts on your network. If usernames and passwords have been compromised, an intruder may be able to gain unauthorized access to other hosts on your network. Also, an intruder may be able to use trust relationships between hosts to gain unauthorized access from a compromised host. Our intruder detection checklist can help you to evaluate a host's state of security:
http://www.cert.org/tech_tips/intruder_detection_checklist.html.

We encourage you to ensure that your hosts are current with security patches or work-arounds for well-known vulnerabilities. In particular, you may wish to review the following CERT advisories for suggested solutions:

- CA-99-08 - Buffer Overflow Vulnerability in rpc.cmsd
  http://www.cert.org/advisories/CA-99-08-cmsd.html
- CA-99-05 - Vulnerability in statd exposes vulnerability in automountd
  http://www.cert.org/advisories/CA-99-05-statd-automountd.html
- CA-98.11 - Vulnerability in ToolTalk RPC Service
  http://www.cert.org/advisories/CA-98.11.tooltalk.html

We also encourage you to regularly review security related patches released by your vendors.

This document is available from: http://www.cert.org/incident_notes/IN-99-04.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

5 IN-99-05: Systems Compromised Through a Vulnerability in am-utils

Updated: December 9, 1999 (Added information about IN-99-07)
Friday, September 17, 1999

Overview

We have received reports of intruder activity involving the am-utils package. Reports submitted to the CERT/CC indicate that intruders are actively exploiting a vulnerability in *amd* that is resulting in remote users gaining root access to victim machines.

The vulnerability we have seen exploited as a part of these attacks is:

- CA-99-12, Buffer Overflow in amd
  http://www.cert.org/advisories/CA-99-12-amd.html

Description

Reports of successful exploitations of the vulnerability in *amd* have included some or all of the following attack characteristics:

- Generation of a syslog message as a result of the vulnerability in amd being exploited, similar to

```
xxx xx xx:xx:xx xxxxx amd[xxxx]: amq requested mount of
^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
```

```
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P
xxx xx xx:xx:xx xxxxx amd[xxxx]: AMQ request from
xxx.xxx.xxx.xxx DENIED
```

- Addition of user accounts to /etc/passwd. Reports indicate the usernames bionic and foom are commonly added
- Creation of a backdoor on port 1337/tcp using the file /tmp/bob as a configuration file for a second instance of /usr/sbin/inetd
- Remote retrieval and installation of additional intruder tools, including root kits that contain replacements for various system binaries
- Replacement versions of ssh and sshd installed and used by the intruder to gain access to compromised systems
- Packet sniffer installed in "/dev/sda69/. /" (note the extra space)

In some cases, we have seen distributed denial of service tools installed on compromised machines. For more information, see IN-99-07, Distributed Denial of Service Tools.

Solutions

If you believe a host has been compromised, we encourage you to disconnect the host from the network and review our steps for recovering from a root compromise: http://www.cert.org/tech_tips/root_compromise.html.

We encourage you to ensure that your hosts are current with security patches or work-arounds for well-known vulnerabilities. In particular, you may wish to review the following CERT advisory for suggested solutions:

- CA-99-12, Buffer Overflow in and http://www.cert.org/advisories/CA-99-12-amd.html

We also encourage you to regularly review security related patches released by your vendors.

This document is available from: http://www.cert.org/incident_notes/IN-99-05.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University

Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

6 IN-99-06: Distributed Network Sniffer

Monday, October 25, 1999

Overview

We have received reports of intruders using distributed network sniffers to capture usernames and passwords. The distributed sniffer consists of a client and a server portion. The sniffer clients have been found exclusively on compromised Linux hosts.

Description

The following characteristics may be present on compromised hosts running the sniffer client:

- The sniffer clients have been found exclusively on compromised Linux hosts. Some reports indicate a vulnerability in the cron daemon may be used to leverage privileged access. We suspect user accounts with compromised passwords may be used to gain initial access.
- The executing sniffer binary may appear in the process list using a deceptive name, such as in.telnetd. Here is an example of the client as found in a process list of a compromised host:

  ```
  in.telnetd ARGS=/sbin/init 59300 NO_MOD_PARMS=install
  ARGS=/USR/SBIN/CRON EMB= ARG=/tmp/passwd LOGHOST=xxx.xxx.xxx.xxx
  ```

  The value of LOGHOST appears to be one or more IP addresses for remote sniffer servers.
- The binary /sbin/init may be replaced with an intruder-supplied binary, with the original moved to /dev/init. The malicious /sbin/init binary makes use of kernel modules to conceal system changes. An existing /dev/init copy may be visible to stat() if it's full path is given (e.g., "ls -l /dev/init").
- UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.

The characteristics of the sniffer server include these:

- Appears to listen for incoming UDP packets from sniffer clients on port 21845/udp.
- May run as an ordinary user without privileges.

Solutions

If you believe a host has been compromised, we encourage you to disconnect the host from the network and review our steps for recovering from a root compromise: http://www.cert.org/tech_tips/root_compromise.html.

We encourage you to ensure that your hosts are current with security patches or work-arounds for well-known vulnerabilities.

This document is available from: http://www.cert.org/incident_notes/IN-99-06.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

---

7 IN-99-07: Distributed Denial of Service Tools

Updated: January 15, 2001 (changed RFC 2267 to RFC 2827/BCP 38)
Updated: December 8, 1999 (added DSIT Workshop paper and IN-99-05)
Thursday, November 18, 1999

Overview

We have received reports of intruders installing distributed denial of service tools. Tools we have encountered utilize distributed technology to create large networks of hosts capable of launching large coordinated packet flooding denial of service attacks.

We have seen distributed tools installed on hosts that have been compromised due to exploitation of known vulnerabilities. In particular, we have seen vulnerabilities in various RPC services exploited. For more information see the following CERT Incident Notes:

IN-99-04, Similar Attacks Using Various RPC Services

IN-99-05, Systems Compromised Through a Vulnerability in am-utils

Two of the tools we have seen are known as ***trinoo*** (or trin00) and ***tribe flood network (or TFN)***. These tools appear to be undergoing active development, testing, and deployment on the Internet.

Descriptions

- Trinoo
- Tribe Flood Network

Trinoo

Trinoo is a distributed tool used to launch coordinated UDP flood denial of service attacks from many sources. For more information about various UDP flood attacks, please see CERT Advisory CA-96.01. A trinoo network consists of a small number of servers, or *masters*, and a large number of clients, or *daemons*.

A denial of service attack utilizing a trinoo network is carried out by an intruder connecting to a trinoo master and instructing that master to launch a denial of service attack against one or more IP addresses. The trinoo master then communicates with the daemons giving instructions to attack one or more IP addresses for a specified period of time.

1. intruder -------> master; destination port 27665/tcp
2. master --------> daemons; destination port 27444/udp
3. daemons -------> UDP flood to target with randomized destination ports

The binary for the trinoo daemon contains IP addresses for one or more trinoo master. When the trinoo daemon is executed, the daemon announces it's availability by sending a UDP packet containing the string "*HELLO*" to it's programmed trinoo master IP addresses.

1. daemon -------> masters; destination port 31335/udp

The trinoo master stores a list of known daemons in an encrypted file named "..." in the same directory as the master binary. The trinoo master can be instructed to send a broadcast request to all known daemons to confirm availability. Daemons receiving the broadcast respond to the master with a UDP packet containing the string "PONG".

1. intruder -------> master; destination port 27665/tcp
2. master -------> daemons; destination port 27444/udp
3. daemons -------> master; destination port 31335/udp

All communications to the master on port 27665/tcp require a password, which is stored in the daemon binary in encrypted form. All communications with the daemon on port 27444/udp require the UDP packet to contain the string "l44" (that's a lowercase L, not a one).

The source IP addresses of the packets in a trinoo-generated UDP flood attack are not spoofed in versions of the tool we have seen. Future versions of the tool could implement IP source address spoofing. Regardless, a trinoo-generated denial of service attack will most likely appear to come from a large number of different source addresses.

We have seen trinoo daemons installed under a variety of different names, but most commonly as

- ns
- http
- rpc.trinoo
- rpc.listen
- trinix
- rpc.irix
- irix

Running *strings* against the daemon and master binaries produces output similar to this (we have replaced master IP address references in the daemon binary with X.X.X.X)

trinoo daemon	trinoo master
socket bind recvfrom %s %s %s aIf3YWfOhw.V. PONG *HELLO* X.X.X.X X.X.X.X X.X.X.X	---v v1.07d2+f3+c trinoo %s l44adsl sock 0nm1VNMXqRMyM 15:08:41 Aug 16 1999 trinoo %s [%s:%s] bind read *HELLO* ... rest omitted ...

Tribe Flood Network

TFN, much like Trinoo, is a distributed tool used to launch coordinated denial of service attacks from many sources against one or more targets. In additional to being able to generate UDP flood attacks, a TFN network can also generate TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast (e.g., smurf) denial of service attacks. TFN has the capability to generate packets with spoofed source IP addresses. Please see the following CERT Advisories for more information about these types of denial of service attacks.

CA-96.01, TCP SYN Flooding and IP Spoofing Attacks

CA-98.01, "smurf" IP Denial of Service Attacks

A denial of service attack utilizing a TFN network is carried out by an intruder instructing a client, or *master*, program to send attack instructions to a list of TFN servers, or *daemons*. The daemons then generate the specified type of denial of service attack against one or more target IP addresses. Source IP addresses and source ports can be randomized, and packet sizes can be altered.

A TFN master is executed from the command line to send commands to TFN daemons. The master communicates with the daemons using ICMP echo reply packets with 16 bit binary values embedded in the ID field, and any arguments embedded in the data portion of packet. The binary values, which are definable at compile time, represent the various instructions sent between TFN masters and daemons.

Use of the TFN master requires an intruder-supplied list of IP addresses for the daemons. Some reports indicate recent versions of TFN master may use blowfish encryption to conceal the list of daemon IP addresses. Reports also indicate that TFN may have remote file copy (e.g., rcp) functionality, perhaps for use for automated deployment of new TFN daemons and/or software version updating in existing TFN networks.

We have seen TFN daemons installed on systems using the filename ***td***. Running strings on the TFN daemon binary produces output similar to this.

```
%d.%d.%d.%d
ICMP
Error sending syn packet.
tc: unknown host
3.3.3.3
mservers
randomsucks
skillz
rm -rf %s
ttymon
rcp %s@%s:sol.bin %s
nohup ./%s
X.X.X.X
X.X.X.X
lpsched
sicken
in.telne
```

Solutions

Distributed attack tools leverage bandwidth from multiple systems on diverse networks to produce very potent denial of service attacks. To a victim, an attack may appear to come from many different source addresses, whether or not IP source address spoofing is employed by the attacker. Responding to a distributed attack requires a high degree of communication between Internet sites. Prevention is not straight forward because of the interdependency of site security on the Internet; the tools are typically installed on compromised systems that are outside of the administrative control of eventual denial of service attack targets.

There are some basic suggestions we can make regarding distributed denial of service attacks:

- Prevent installation of distributed attack tools on your systems

  Remain current with security-related patches to operating systems and applications software. Follow security best-practices when administrating networks and systems.

- Prevent origination of IP packets with spoofed source addresses

  For a discussion of network ingress filtering, refer to

  RFC 2827/BCP 38, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

- Monitor your network for signatures of distributed attack tools

  Sites using intrusion detection systems (e.g., IDS) may wish to establish patterns to look for that might indicate trinoo or TFN activity based on the communications between master and daemon portions of the tools. Sites who use pro-active network scanning may wish to include tests for installed daemons and/or masters when scanning systems on your network.

- If you find a distributed attack tool on your systems

  It is important to determine the role of the tools installed on your system. The piece you find may provide information that is useful in locating and disabling other parts of distributed attack networks. We encourage you to identify and contact other sites involved.

- If you are involved in a denial of service attack

  Due to the potential magnitude of denial of service attacks generated by distributed networks of tools, the target of an attack may be unable to rely on Internet connectivity for communications during an attack. Be sure your security policy includes emergency out-of-band communications procedures with upstream network operators or emergency response teams in the event of a debilitating attack.

In November 1999, experts addressed issues surrounding distributed-systems intruder tools. The DSIT Workshop produced a paper where workshop participants examine the use of distributed-system intruder tools and provide information about protecting systems from attack by the tools, detecting the use of the tools, and responding to attacks.

Results of the Distributed-Systems Intruder Tools Workshop

Acknowledgments

The CERT/CC would like to acknowledge and thank our constituency and our peers for important contributions to the information used in this Incident Note.

This document is available from: http://www.cert.org/incident_notes/IN-99-07.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

8 IN-99-08: Attacks against IIS web servers involving MDAC

Friday, December 10, 1999

We have received reports of IIS web servers compromised via a vulnerability in MS Data Access Components (MDAC). This vulnerability has been widely discussed as early as April 22, 1998. Here are some pointers to information about this vulnerability:

http://support.microsoft.com/support/kb/articles/q184/3/75.asp

http://www.microsoft.com/security/bulletins/ms98-004.asp

http://www.microsoft.com/security/bulletins/ms99-025.asp

In incidents reported to us so far, attacks can be identified by looking through the IIS log files for POST access to the file "/msadc/msadcs.dll". For example:

```
1999-10-24 20:38:12  - WWW  POST /msadc/msadcs.dll 200 1409
664 782 ACTIVEDATA - -
```

If you use Microsoft Remote Data Services (RDS) these POST operations may be legitimate.

We encourage all sites using IIS to carefully follow the steps listed in Microsoft Advisory MS99-025, referenced above, to secure or disable RDS.

This document is available from: http://www.cert.org/incident_notes/IN-99-08.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.
