CERT Incident Note IN-99-06: Distributed Network Sniffer

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

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.