Void captures over a million Android TV boxes

Published: 2024-09-12 · Archived: 2026-04-05 15:16:55 UTC

12.09.2024

Real-time threat news | Hot news | All the news | Virus alerts

September 12, 2024

Doctor Web experts have uncovered yet another case of an Android-based TV box infection. The malware, dubbed Android.Vo1d, has infected nearly 1.3 million devices belonging to users in 197 countries. It is a backdoor that puts its components in the system storage area and, when commanded by attackers, is capable of secretly downloading and installing third-party software.

In August 2024, Doctor Web was contacted by several users whose Dr.Web antivirus had detected changes in their device's system file area. The problem occurred with these models:

TV box model	Declared firmware version
R4	Android 7.1.2; R4 Build/NHG47K
TV BOX	Android 12.1; TV BOX Build/NHG47K
KJ-SMART4KVIP	Android 10.1; KJ-SMART4KVIP Build/NHG47K

All these cases involved similar signs of infection, so we will describe them using one of the first requests we received as an example. The following objects were changed on the affected TV box:

- install-recovery.sh
- daemonsu

In addition, 4 new files emerged in its file system:

- /system/xbin/vo1d
- /system/xbin/wd
- /system/bin/debuggerd
- /system/bin/debuggerd_real

The vo1d and wd files are the components of the **Android.Vo1d** trojan that we discovered.

> The trojan's authors probably tried to disguise one if its components as the system program /system/bin/vold, having called it by the similar-looking name "vo1d" (substituting the lowercase letter "l" with the number "1"). The malicious program's name comes from the name of this file. Moreover, this spelling is consonant with the English word "void".

The install-recovery.sh file is a script that is present on most Android devices. It runs when the operating system is launched and contains data for autorunning the elements specified in it. If any malware has root access and the ability to write to the /system system directory, it can anchor itself in the infected device by adding itself to this script (or by creating it from scratch if it is not present in the system). **Android.Vo1d** has registered the autostart for the wd component in this file.

```
#!/system/bin/sh
func_start_kr() {
    /system/xbin/wd &
}

KR_TMP_FNAME=boxdaemon2
LOG_FILE_TMP=/data/local/tmp/$KR_TMP_FNAME.txt.tmp
LOG_FILE=/data/local/tmp/$KR_TMP_FNAME.txt
rm -f $LOG_FILE_TMP
rm -f $LOG_FILE
echo "[$0] begin ..." > $LOG_FILE_TMP
chmod 0777 $LOG_FILE_TMP
id >> $LOG_FILE_TMP  2>&1
func_start_kr >> $LOG_FILE_TMP 2>&1
echo "[$0] end!" >> $LOG_FILE_TMP
chcon u:object_r:shell_data_file:s0 $LOG_FILE_TMP
chown shell.shell $LOG_FILE_TMP
chmod 00644 $LOG_FILE_TMP
mv $LOG_FILE_TMP $LOG_FILE
```

The modified install-recovery.sh file

The daemonsu file is present on many Android devices with root access. It is launched by the operating system when it starts and is responsible for providing root privileges to the user. **Android.Vo1d** registered itself in this file, too, having also set up autostart for the wd module.

The debuggerd file is a daemon that is typically used to create reports on occurred errors. But when the TV box was infected, this file was replaced by the script that launches the wd component.

The debuggerd_real file in the case we are reviewing is a copy of the script that was used to substitute the real debuggerd file. Doctor Web experts believe that the trojan's authors intended the original debuggerd to be moved into debuggerd_real to maintain its functionality. However, because the infection probably occurred twice, the trojan moved the already substituted file (i.e., the script). As a result, the device had two scripts from the trojan and not a single real debuggerd program file.

At the same time, other users who contacted us had a slightly different list of files on their infected devices:

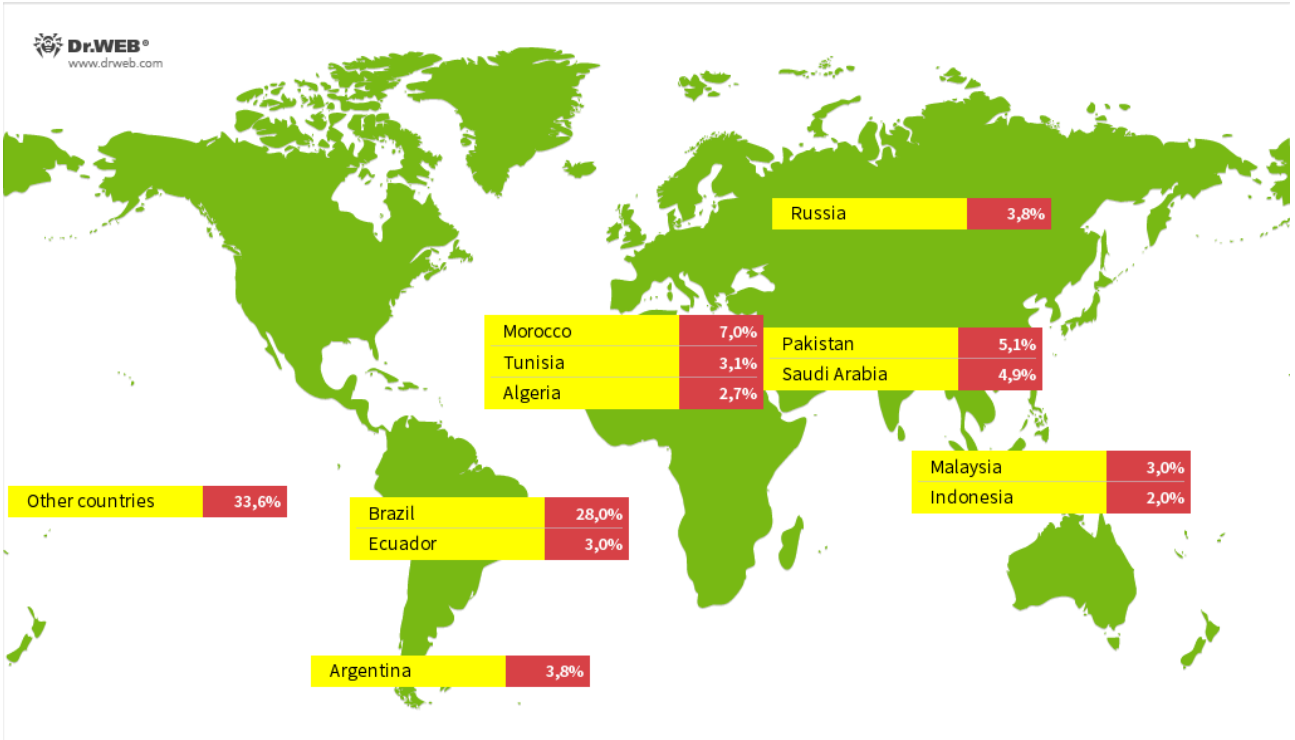
- daemonsu (the vo1d file analogue — **Android.Vo1d.1**);
- wd (**Android.Vo1d.3**);
- debuggerd (the same script as described above);

- debuggerd_real (the original file of the debuggerd tool);
- install-recovery.sh (a script that loads objects specified in it).

An analysis of all the aforementioned files showed that in order to anchor **Android.Vo1d in the** system, its authors used at least three different methods: modification of the install-recovery.sh and daemonsu files and substitution of the debuggerd program. They probably expected that at least one of the target files would be present in the infected system, since manipulating even one of them would ensure the trojan's successful auto launch during subsequent device reboots.

Android.Vo1d's main functionality is concealed in its vo1d (**Android.Vo1d.1**) and wd (**Android.Vo1d.3**) components, which operate in tandem. The **Android.Vo1d.1** module is responsible for **Android.Vo1d.3**'s launch and controls its activity, restarting its process if necessary. In addition, it can download and run executables when commanded to do so by the C&C server. In turn, the **Android.Vo1d.3** module installs and launches the **Android.Vo1d.5** daemon that is encrypted and stored in its body. This module can also download and run executables. Moreover, it monitors specified directories and installs the APK files that it finds in them.

A study conducted by Doctor Web malware analysts showed that the **Android.Vo1d** backdoor has infected around 1.3 million devices, while its geographical distribution included almost 200 countries. The largest number of infections were detected in Brazil, Morocco, Pakistan, Saudi Arabia, Russia, Argentina, Ecuador, Tunisia, Malaysia, Algeria, and Indonesia.



Countries with the highest number of infected devices detected

One possible reason why the attackers distributing **Android.Vo1d** specifically chose TV boxes is that such devices often run on outdated Android versions, which have unpatched vulnerabilities and are no longer supported with updates. For example, the users who contacted us have models that are based on Android 7.1, despite the fact that for some of them the configuration indicates much newer versions, such as Android 10 and Android 12.

Unfortunately, it is not uncommon for budget device manufacturers to utilize older OS versions and pass them off as more up-to-date ones to make them more attractive.

In addition, users themselves may mistakenly perceive TV boxes to be better protected devices, compared to smartphones. As a result, they may install anti-virus software on these less often and risk encountering malware when downloading third-party apps or installing unofficial firmware.

At the moment, the source of the TV boxes' backdoor infection remains unknown. One possible infection vector could be an attack by an intermediate malware that exploits operating system vulnerabilities to gain root privileges. Another possible vector could be the use of unofficial firmware versions with built-in root access.

Dr.Web anti-virus for Android successfully detects all known **Android.Vo1d** trojan variants, and, if root access is available, cures the infected devices.

Indicators of compromise

More details on **Android.Vo1d.1**

More details on **Android.Vo1d.3**

More details on **Android.Vo1d.5**
