Tablet MediaTek BJ68

/etc/udev/rules.d/bj68.rules

```
SUBSYSTEM!="usb|usb_device", ACTION!="add", GOTO="tablet_bj68_rules_end"

# MediaTek BJ68
ATTRS{idVendor}=="0e8d", ATTRS{idProduct}=="201d", SYMLINK+="tablet-%k", MODE="660",
GROUP="adbusers"

LABEL="tablet_bj68_rules_end"
```

Hardware

CPU

- MediaTek MT6737
- 4x1.3 GHz ARM Cortex-A53
- 2016
- Mali-T720 MP2
- Mem max: 3 GB

```
BJ68:/ $ cat /proc/cpuinfo
Processor□: ARMv7 Processor rev 4 (v7l)
processor□: 0
model name□: ARMv7 Processor rev 4 (v7l)
BogoMIPS□: 35.29
Features□: half thumb fastmult vfp edsp neon vfpv3 tls vfpv4 idiva idivt vfpd32 lpae evtstrm
aes pmull sha1 sha2 crc32
CPU implementer□: 0x41
CPU architecture: 7
CPU variant□: 0x0
CPU part□: 0xd03
CPU revision□: 4
```

```
Hardware□: MT6737
Revision□: 0000
Serial□□: 0000000000000000
```

Memory

- 2GB

```
BJ68:/ $ free -m
□□total        used        free      shared     buffers
Mem:             1939        1869          70          16           0
-/+ buffers/cache:           1868          71
Swap:            1454          29        1424
```

Storage

- 8.9 GB usable / ~16 GB total

```
BJ68:/ $ df -h
Filesystem            Size  Used Avail Use% Mounted on
tmpfs                 970M  652K  969M   1% /dev
/dev/block/mmcblk0p23 2.5G  0.9G  1.5G  39% /system
/dev/block/mmcblk0p22 2.7G  2.5G  113M  96% /vendor
tmpfs                 970M     0  970M   0% /mnt
/dev/block/mmcblk0p24 106M   56K  104M   1% /cache
/dev/block/mmcblk0p3  5.6M   48K  5.3M   1% /vendor/protect_f
/dev/block/mmcblk0p4  5.6M   44K  5.3M   1% /vendor/protect_s
/dev/block/mmcblk0p19  27M  2.2M   24M   9% /vendor/nvdata
/dev/block/dm-0       8.9G  2.8G  5.6G  34% /data
/data/media           8.9G  2.8G  5.6G  34% /storage/emulated
```

Software

Virus

- `/system/app/Rsota/Rsota.apk`

- https://www.virustotal.com/gui/file/500acc4e80a4dd5b41b505b840c0373e3929e178a1a88410040609258b0bc235
- `Android:DwPhon-A`, `TrojanDownloader:Android/Dwphon.8d63ab63`...
- https://www.malwarebytes.com/blog/news/2021/04/pre-installed-auto-installer-threat-found-on-android-mobile-devices-in-germany
- https://forums.malwarebytes.com/topic/216616-removal-instructions-for-adups/

Looks like it is OTA updater.

```
 <!-- □□□URL -->
<string name="test_ota_serverl_url">http://fota.mwhtml5.com:6100/service/request</string>
<string name="test_ota_report_url">http://fota.mwhtml5.com:6100/service/report</string>
<string name="ota_serverl_url">http://fota.redstone.net.cn:6100/service/request</string>
<string name="ota_report_url">http://fota.redstone.net.cn:6100/service/report</string>
<!-- □□□HTTPS URL -->
<string
name="test_ota_serverl_https_url">https://fota.mwhtml5.com:6200/service/request</string>
<string name="test_ota_report_https_url">https://fota.mwhtml5.com:6200/service/report</string>
<string
name="ota_serverl_https_url">https://fota.redstone.net.cn:7100/service/request</string>
<string name="ota_report_https_url">https://fota.redstone.net.cn:7100/service/report</string>
```

Lists as: `adb shell pm list packages -f -u`

```
package:/system/app/Rsota/Rsota.apk=com.abfota.systemUpdate
```

Uninstall for user:

```
adb shell pm uninstall -k --user 0 com.abfota.systemUpdate
```

Revision #10
Created 2024-12-30 15:26:49 GMT by hxd
Updated 2024-12-30 20:31:45 GMT by hxd