Owner of an Android TV box? May want to check if it's an active botnet member...

By DesktopECHO

Published: 2022-11-16 · Archived: 2026-04-05 20:44:51 UTC

- Thread starter DesktopECHO
- Start date Nov 16, 2022

-
- #1

I installed Pi-hole on my Android device and pointed DNS at 127.0.0.1
Saw a bunch of funky domains in the query log and blocked them.

2022-11-15 22:17:14	AAAA	adc.flyermobi.com	localhost	Blocked (gravity)	IP (0.3ms)	Whitelist
2022-11-15 22:17:14	AAAA	ipinfo.io	localhost	Blocked (exact blacklist)	IP (1.0ms)	Whitelist
2022-11-15 22:13:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:13:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:13:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (0.3ms)	Whitelist
2022-11-15 22:12:09	AAAA	7.zxczj.top	localhost	Blocked (exact blacklist)	IP (0.4ms)	Whitelist
2022-11-15 22:11:19	AAAA	sdk-event-sg.ap-southeast-1.log.aliyuncs.com	localhost	Blocked (exact blacklist)	IP (0.5ms)	Whitelist
2022-11-15 22:11:19	AAAA	sdk.navnow.xyz	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 22:08:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (0.3ms)	Whitelist
2022-11-15 22:08:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:08:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:07:14	AAAA	adc.flyermobi.com	localhost	Blocked (gravity)	IP (1.3ms)	Whitelist
2022-11-15 22:07:14	AAAA	ipinfo.io	localhost	Blocked (exact blacklist)	IP (1.2ms)	Whitelist
2022-11-15 22:05:29	AAAA	7.zxczj.top	localhost	Blocked (exact blacklist)	IP (1.1ms)	Whitelist
2022-11-15 22:03:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (1.1ms)	Whitelist
2022-11-15 22:03:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 22:03:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (1.3ms)	Whitelist
2022-11-15 22:01:24	AAAA	mirror.us.leaseweb.net	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:59:54	AAAA	googleads.g.doubleclick.net	localhost	Blocked (gravity)	IP (0.7ms)	Whitelist
2022-11-15 21:58:51	AAAA	www.dgddh.xyz	localhost	Blocked (exact blacklist)	IP (1.0ms)	Whitelist
2022-11-15 21:58:49	AAAA	7.zxczj.top	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:58:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:58:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:58:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (1.0ms)	Whitelist

But what was causing it?

```
 root@walleye:~# tcpflow -p -c -i wlan0  port 80 | grep -oE '(GET|POST|HEAD) .* HTTP/1.[01]|Host: .*'
reportfilename: ./report.xml
tcpflow: listening on wlan0
GET /logs/log.info?package=com.swe.dgbluancher&osv=10&gaid=ff9300dd-f771-40ff-84d7-42184fc40d95&get_ip_info=ff9
Host: 128.199.97.77
GET /logs/log.active?package=com.swe.dgbluancher&osv=10&gaid=ff9300dd-f771-40ff-84d7-42184fc40d95&model=MBOX&mak
Host: 128.199.97.77
```

```
GET /logs/log.info?package=com.swe.dgbluancher&osv=10&gaid=ff9300dd-f771-40ff-84d7-42184fc40d95&get_ip_info=ff9
Host: 128.199.97.77
GET /?timestamp=1668566687503&version=1&biz=10016&os=2&id=3e2dfd4c426e38721ac0bcc09612aa96&sign=d59dab281300157
Host: www.forfor123.com
GET /get_endpoint?timestamp=1668566687493&version=1&biz=10016&os=2&id=3e2dfd4c426e38721ac0bcc09612aa96&sign=135
Host: qweqwe135.top
POST /u.php?id=30018&m=cTUJPWA&s=d1,u3&p=cY29tLnN3ZS5kZ2JsdWFuY2hlcg&aid=df53b410ca1fd8a6&am=2 HTTP/1.0
Host: v.sustat.com
GET /stg?channel=hzsdk_05&sdk=js_club HTTP/1.1
Host: sdk2.appclicking.com
GET /logs/log.info?package=com.swe.dgbluancher&osv=10&gaid=ff9300dd-f771-40ff-84d7-42184fc40d95&get_ip_info=ff9
Host: 128.199.97.77
GET /logs/log.info?package=com.swe.dgbluancher&osv=10&gaid=ff9300dd-f771-40ff-84d7-42184fc40d95&get_ip_info=ff9
Host: 128.199.97.77
GET /d/bcc/v2/o/ffeca781ecfd6067e5e56b04d67edc7e HTTP/1.1
Host: dct.g1ee.com
```

D

Deleted member 11959327

Guest

-
- #3

Is your device roughly the same as this?

```
https://www.amazon.com/gp/product/B08CRV62C4
```

I have that one. It still has the shipped build. I haven't had it hooked up much because it is kind of a piece of crap. I'll check and see what it has.

This might be kind of a good argument to use certified builds on certified devices. But the amount of data collection done by those would make your head spin. And it is all outsourced to the factory. Servers to sdmc, sei, skyworth, and the like. Sdmc even advertises these features as "big data" features.

-
- #4

> Is your device roughly the same as this?
>
> ```
> https://www.amazon.com/gp/product/B08CRV62C4
> ```
>
> I have that one. It still has the shipped build. I haven't had it hooked up much because it is kind of a piece of crap. I'll check and see what it has.
>
> This might be kind of a good argument to use certified builds on certified devices. But the amount of data collection done by those would make your head spin. And it is all outsourced to the factory. Servers to sdmc, sei, skyworth, and the like. Sdmc even advertises these features as "big data" features.

That's the one! I'm about to pull the trigger on a second one to see how deep the rot goes. If this is how they come from Amazon it'd be a pretty big deal.

Jul 11, 2012

18

11

-
- #6

That's... horrifying.

Just to confirm, you're using a stock device, unflashed box?
Did you see the да folder in:

```
/data/data/com.swe.dgbluancher/files
```

How did you discover your device was infected? If possible, can you name where you bought the device, like an Amazon link or similar?

Jul 11, 2012

18

11

-
- #7

yes, stock. I bought four of these:

They were being blown out for ~ $14 each. Wonder why.....

I can't claim credit, found your threads here. I was looking for options to flash linux to them in order to run klipper or kodi. Had taken a look around the stock android, and being paranoid that included preinstalled apps. I was actually thinking it was fairly clean compared to say an ATT motorola prepaid android phone or something. But that "luancher" was there, for sure. WIthout uninstall or disable options


-
- #9

It seems to be a popular Android box over there. Here is the link to a megathread dedicated to that deivce:
{Mod edit: Link removed. Oswald Boelcke}

It might be helpful to ask in that forum if anyone with one of these devices sees the folder:

```
/data/data/com.swe.dgbluancher/files/да
```

...and if so, let them know their device is compromised.

The firmware links being shared here and elsewhere have the malware built-in. Actually, I have yet to see a 'clean' downloadable firmware for this box, *anywhere* on the Internet.

-
- #10

> yes, stock. I bought four of these:
>
> They were being blown out for ~ $14 each. Wonder why.....
>
> I can't claim credit, found your threads here. I was looking for options to flash linux to them in order to run klipper or kodi. Had taken a look around the stock android, and being paranoid that included preinstalled apps. I was actually thinking it was fairly clean compared to say an ATT motorola prepaid

> android phone or something. But that "luancher" was there, for sure. WIthout uninstall or disable options

Thanks for the info. Really hard to believe these devices can be built for $14 with the reseller making a dollar or two per unit.

Does the foler ***/data/data/com.swe.dgbluancher/files/∂a*** exist on your device?

-
- #11

To be clear, ***com.swe.dgbluancher*** appears to be a simple open-source launcher that was rebuilt with the malware and packaged in the ROM. the presence of the launcher is not an indication of malware, but the "**/да"** folder *definitely* is.

The Universal Android Debloater will get rid of this easily, but I'm not sure that is enough to clean the device. There may be more nasty stuff in the ROM I haven't yet found. For a safe replacement, I'm using Microsoft Launcher because it includes an entry point to the device's settings menu.

-
- #12

One last bit of traffic I can't account for:

```
ycxrl.com / li1470-135.members.linode.com (139.162.57.135)
```

Every few minutes the T95 wants to send "something" to **ycxrl.com**

```
 |ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1
|ycxrl.com|POST /terminal/client/apiInfo HTTP/1.1
```

How many of these things sold on Amazon and AliExpress?!

-
- #13

Update -- The malware injects the *system_server* process. Looks to be deeply baked-into the ROM.

If I can't remove this malware, find a clean ROM, or get 'regular' Linux running, this T95 box is worse than useless.

Pretty sophisticated malware, resembling CopyCat in how it works.

Sep 27, 2006

223

111

-
- #14

This was actually an interesting topic. Part of me isn't surprised because I've heard of a lot of these types of boxes and mobile devices used for stuff like botnets. I have a Xiaomi Mi box and am curious if they are also similar.

It makes me curious what a good modern android box is these days.

-
- #15

Xiaomi maybe not so much, but these vendors on Amazon operating with names like BLAÜMTRON could be up to anything apparently.

If other T95 owners can check their devices for DNS traffic to ***ycxrl.com*** it'd be a huge help to determine the extent of this problem.

-
- #16

> It seems to be a popular Android box over there. Here is the link to a megathread dedicated to that deivce:
> ***{Mod edit: Link removed. Oswald Boelcke}***
>
> It might be helpful to ask in that forum if anyone with one of these devices sees the folder:

> ```
> /data/data/com.swe.dgbluancher/files/да
> ```
>
> ...and if so, let them know their device is compromised.
>
> The firmware links being shared here and elsewhere have the malware built-in. Actually, I have yet to see a 'clean' downloadable firmware for this box, *anywhere* on the Internet.

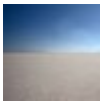
@DesktopECHO

I've removed the link to 4pda from your above post! 4pda is not only another phone related website (and not at all affiliated with xda-developers) but also well known for the distribution of malware and warez. **Links or references to 4pda are not accepted on XDA.**
XDA Forum Rules (excerpt):

> ...
> **6. Do not post or request warez.**
>
> If a piece of software requires you to pay to use it, then pay for it. We do not accept warez nor do we permit members to request, post, promote or describe ways in which warez, cracks, serial codes or other means of avoiding payment, can be obtained or used. This is a site of developers, i.e. the sort of people who create such software. When you cheat a software developer, you cheat us as a community.
>
> (...)
>
> **11. Don’t post with the intention of selling something.**
>
> - Don’t use XDA to advertise your product or service. Proprietors of for-pay products or services, may use XDA to get feedback, provide beta access, or a free version of their product for XDA users and to offer support, but not to post with the intention of selling. This includes promoting sites similar / substantially similar to XDA-Developers.com.
> - Do not post press releases, announcements, links to trial software or commercial services, unless you’re posting an exclusive release for XDA-Developers.com.
> - Encouraging members to participate in forum activities on other phone related sites is prohibited.
> - Off-site downloads are permitted if the site is non-commercial and does not require registration.
> - Off-site downloads from sites requiring registration are NOT encouraged but may be permitted if both of the following conditions are met:
>   **A)** The site belongs to a member of XDA-Developers with at least 1500 posts and 2 years membership, who actively maintains an XDA-Developers support thread(s) / posts, related to the download.
>   **B)** The site is a relatively small, personal website without commercial advertising / links (i.e. not a competitor forum-based site with purposes and aims similar to those of XDA-Developers.com.)
>
> ...

Please refrain from sharing of such links in future! Thanks for your cooperation.

Regards
Oswald Boelcke
Senior Moderator

Dec 2, 2022

77

21

-
- #19

> Xiaomi maybe not so much, but these vendors on Amazon operating with names like BLAÜMTRON could be up to anything apparently.
>
> If other T95 owners can check their devices for DNS traffic to ***ycxrl.com*** it'd be a huge help to determine the extent of this problem.

I would love to check for this, what do I need..??

Mar 13, 2010

442

117

-
- #20

So, I just bought a H96 MAX with RK3528 CPU, 4G+64GB Storage and Android 13 and was curious if these are infected, too.

This is a list how I tested the device:

- Connected the Device to a empty and isolated vLAN
- Did a Network Package analysis for traffic coming from that vLAN, no suspicious traffic detected

- Scanned the device with a forensics tool called MVT. Root Binary "su" together with "busybox" detected. Means the device is rooted. None Malware / Virus detected.
- Dumped all user apks and uploaded them to VirusTotal. No detections, everything is clean.
- Gained root access via su binary, dumped all system apks and uploaded them to VirusTotal. 2 minor detections, analyzed the behavior of these deeper, false positive in my opinion. Everything else is clean.
- Checked if known malware / virus folder /data/system/Corejava or file /data/system/shared_prefs/open_preference.xml exists in filesystem. They do not exits.
- ADB has no confirmation, if enabled in Android Settings, every device can connect
- SU has no confirmation nor any notification on screen

Conclusion:

- The Device looks clean, beside 2 minor false positives there was no suspicious activity or malware / virus detected.
- The Device is rooted by default with su. This is dangerous because any app can request root and the user wouldn't notice. I recommend to replace the binary with some solution that gives feedback to the user.
- Anyone in the same network can connect to the device via ADB without any confirmation. Keep that in mind and may disable ADB if not needed.
