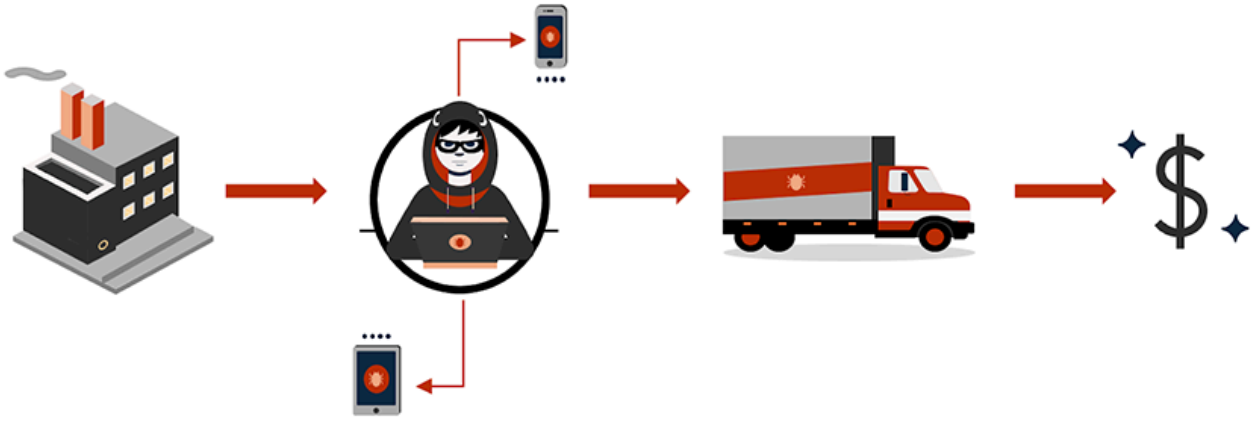
# BADBOX Botnet Is Back

By Pedro Falé

Published: 2024-12-17 · Archived: 2026-04-06 01:02:06 UTC

Imagine this: you're at home, eagerly waiting for the new device you ordered from Amazon. The package arrives, you power it on, and start enjoying all the benefits of 21st century technology—unaware that, as soon as you powered it on, a scheme was unfolding within this device. Welcome to the world of BADBOX.

BADBOX is a large-scale cybercriminal operation selling off-brand Android TV boxes, smartphones, and other Android electronics with preinstalled *malware*. What does this mean? It means the device is infected before it even reaches your hands.



These devices fall victim to a complex criminal scheme, where they are either tampered with during the supply chain or sold by the manufacturer with the ability to install APKs without the user's consent. They are then sold through reputable/popular retailers, such as Amazon, eBay, AliExpress, and others. This supply chain attack makes it extremely difficult for consumers to detect the threat.

At its peak, the BADBOX botnet was thought to consist of about 74,000 compromised Android-based devices. This botnet was presumed dead, after a push to stop its spread. However, not only is it still active, but it also appears to be larger and more versatile than previously anticipated.

- Bitsight TRACE uncovered new BADBOX infrastructure. Telemetry shows over **192,000 BADBOX infected devices** — a number that keeps increasing
- Of the overall infected devices: **160,000 infected devices** belong to unique models not seen before, in particular a **Yandex 4K QLED Smart TV** and a **T963 Hisense Smartphone**
- The top affected countries: Russia, China, India, Belarus, Brazil and Ukraine

This operation came to light in April 2023, when researcher Daniel Milisic became suspicious of a 'T95' Android TV box he purchased, which was performing unusual communications with unknown websites.

At the core of the BADBOX malware lies resemblances to a malware family known as Triada. This malware family emerged around 2016, and it's known for its stealthiness as a firmware backdoor—a secret access someone has to your device. BADBOX malware seems to be an adaptation of that.

A few months after its initial discovery, in October 2023, HUMAN's Satori Threat Intelligence and Research Team's published a comprehensive report on BADBOX and PEACHPIT botnet operations, further corroborating initial findings on the malware and botnet size. We will be focusing on BADBOX devices, which are alarmingly sold to consumers already compromised.

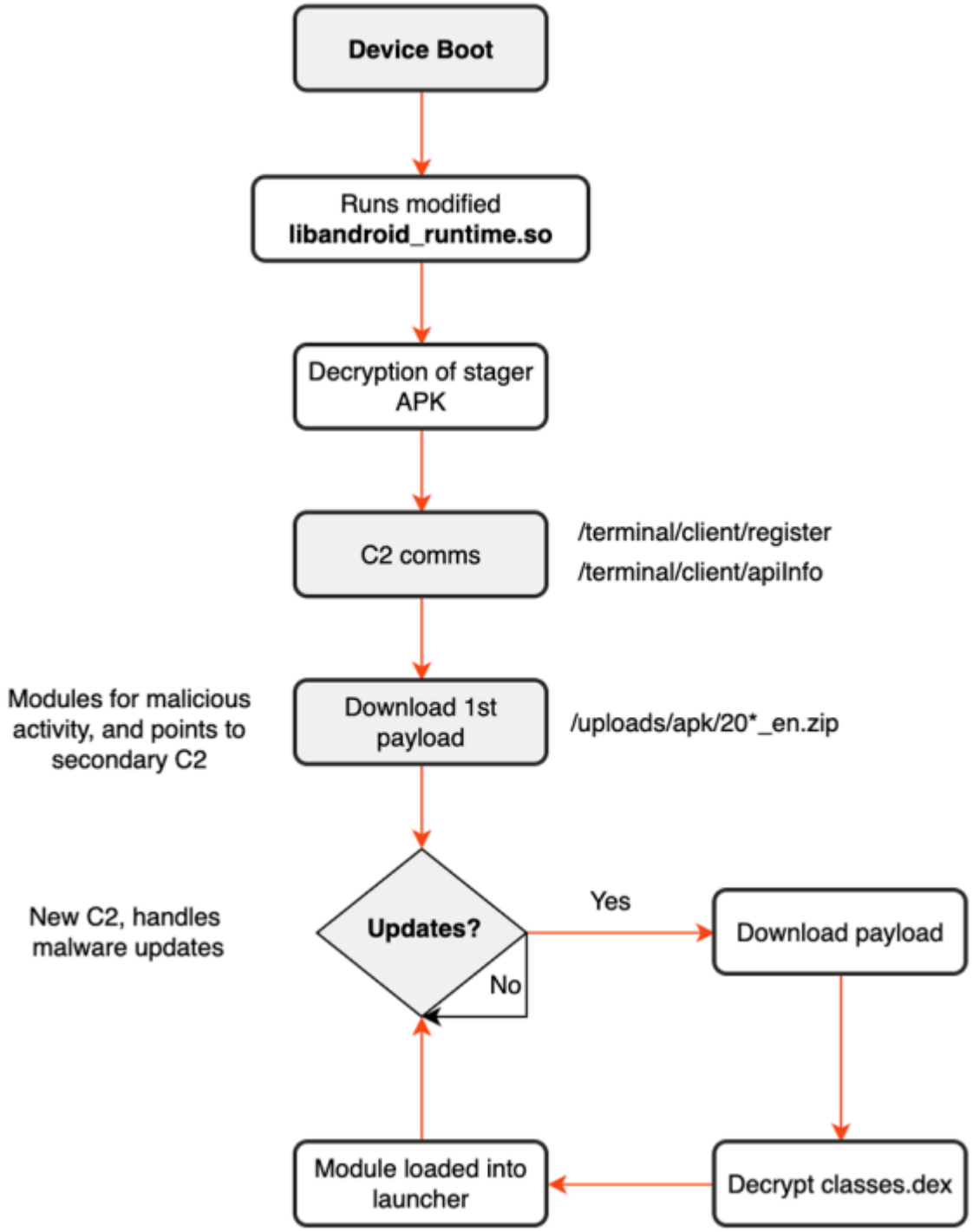
## How does BADBOX work?

BADBOX exploits devices for activities such as **residential proxying** (using backdoored devices as exit points), **remote code installation**, **account abuse, and ad fraud**. One of its most dangerous features is the ability to install additional code/modules without the user's consent, enabling threat actors to deploy new schemes.

Researchers' discovery of BADBOX infections out-of-the-box suggests either a manufacturing intention, where customizable system images allow remote code installation by malicious actors, or a supply chain attack where malware is embedded sometime during the development, manufacturing, shipping, and/or sales processes. We cannot determine if these vectors are mutually exclusive in the case of BADBOX.

As explained in a previous post about OEM infection, "The peril of neglecting mobile apps", infection at this level is exceptionally difficult to remove. These methods share similarities with past attacks like *Triada* and *Guerrilla*, which compromised Android libraries or system firmware. For now, we're moving on to how the BADBOX backdoor operates, before diving into Bitsight's findings.

Below you can see a high-level overview of the activity flow behind the process of BADBOX deployment:




The compromised firmware on the device ensures that, upon booting, it will immediately try to connect to the malicious infrastructure in an attempt to load its backdoor. The backdoor itself is capable of downloading secondary payloads that allow further remote module installation without permissions.

Meaning that entirely new payloads could be constructed by the threat actors, downloaded and executed, to perform new schemes beyond what we have visibility as of now.

If you wish to further understand the underlying technical aspects of the backdoor, take a look at HUMAN's Technical Report, as it provides a more extensive view of this process.

This was the last update on BADBOX at the time of writing. Now, let's examine currently active BADBOX operations in 2024.

## Is BADBOX Dangerous in 2024?

Very much so. Countries should proactively pursue efforts to disrupt the botnet, such as German authorities have recently, in the operation that affected 30,000 devices. Despite such efforts, it did not affect our telemetry, due to the action being contained to Germany. The reality is that BADBOX still seems to be very much alive and spreading. This was evident when Bitsight managed to sinkhole a BADBOX domain, registering more than **160,000 unique IPs in a 24 hour period**. A number that has been steadily growing.

Until now, most research on the topic covers off-brand devices, on the principle that "low-cost devices come at a different cost". What if that wasn't always the case? Bitsight saw **over 100,000 unique IPs from Yandex 4K QLED Smart TVs** in 24 hours, and these devices aren't necessarily cheap. Yandex is a well established brand in Russia—think of it as their own Google enterprise.

How and why so many of these high-end devices became infected is still unknown to us. What we do know, is that the devices are compromised, as evidenced in the findings detailed below.

## BADBOX Infections: Yandex

An investigation on the domain **coslogdydy[.]in** revealed the following:

BADBOX infected devices upon booting and would immediately POST telemetry to try and contact a C2 server, awaiting further instructions. The **coslogdydy[.]in** url received several communications matching that of BADBOX:

```
POST /terminal/client/apiInfo
```

(i.e: The Yandex TV model: YNDX-00091 and Instawall_T963)

```
Model: YNDX-00091
Manufacturer: yandex
Content-Length: 0
Connection: Keep-Alive
Channel: T10801
Vcode: 1
Content-Type: text/xml
Imei: [redacted]
Uuid: [redacted]
Androidid: [redacted]
Accept-Encoding: gzip
Launchername: com.yandex.tv.home
Sdk: 30
Brand: yandex
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; YNDX-00091 Build/RD2A.211001.002)
```

```
coslogdydy.in

POST

/terminal/client/apiInfo
```

```
Model: Instwall_T963
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; Instwall_T963 Build/PPR1.180610.011)
Accept-Encoding: gzip
Connection: Keep-Alive
Channel: T10801
Brand: Droidlogic
Uuid: [redacted]
Content-Length: 0
Content-Type: text/xml
Imei: [redacted]
Launchername: com.instwall.launch
Sdk: 28
Vcode: 1
Androidid: [redacted]
Manufacturer: Droidlogic
```

```
coslogdydy.in

POST

/terminal/client/apiInfo
```

```
POST /terminal/client/register
```

```
POST /terminal/client/apiInfo HTTP/1.1
Connection: Keep-Alive
Content-Type: text/xml
channel: T10901
imei: xx:xx:xx:xx:xx:xx
launchername: com.swe.dgbluancher
model: MBOX
sdk: 29
brand: google
uuid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
vcode: 1
androidId: xxxxxxxxxxxxxxxx
manufacturer: Google
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; MBOX Build/QP1A.191105.004)
Host: cbphe.com
Accept-Encoding: gzip
Content-Length: 0
```

This quickly indicated two things:

First, the models ranging from YNDX-00091 to YNDX-000102 are 4K Smart TVs from a well-known brand, not cheap Android TV boxes. It’s the first time a major brand Smart TV is seen directly communicating at such volume with a BADBOX command and control (C2) domain, broadening the scope of affected devices beyond Android TV boxes, tablets, and smartphones.

These YNDX Smart TV models weren't the only ones compromised. We saw communications from the following devices:

| Device Model | Launcher APK |
| --- | --- |
| YNDX-00102<br>YNDX-00101<br>YNDX-00092<br>YNDX-00091<br>YNDX-00077<br>YNDX-00076<br>YNDX-00075<br>YNDX-00074 | com.yandex.tv.home |
| Instwall_T963 | com.instwall.launch |
| t963_ak301 | com.mk.ifpd.digitalsignage |
| t963_ak301 | com.mk.ifpd.setup.guide |
| Car Entertainment shenzhen | com.android.launcher3 |

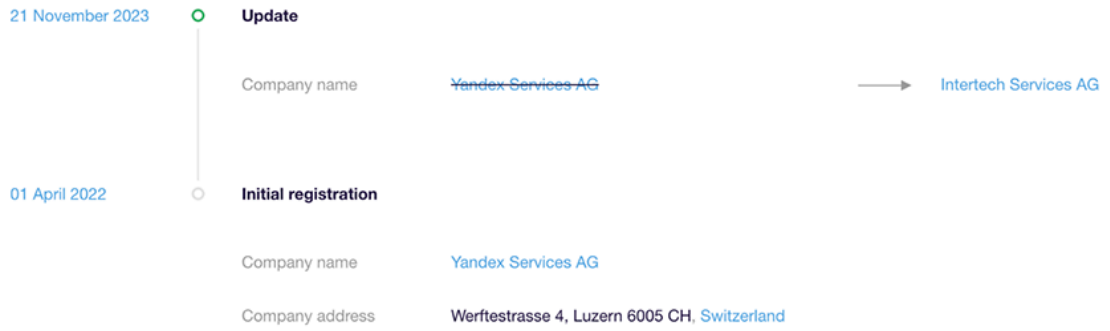
OS: Android

Over 98% of traffic comes from both the YNDX Smart TV models and the T963 smartphone:

| Yandex Smart TV (64%) | Hisense T963 (34%) |
| --- | --- |
| YNDX-00092 (29%) | |
| YNDX-00091 (20%) | Instwall_T963 (29%) |
| YNDX-00101 (10%) | t963_ak301 (5%) |
| YNDX-00102 (6%) | |

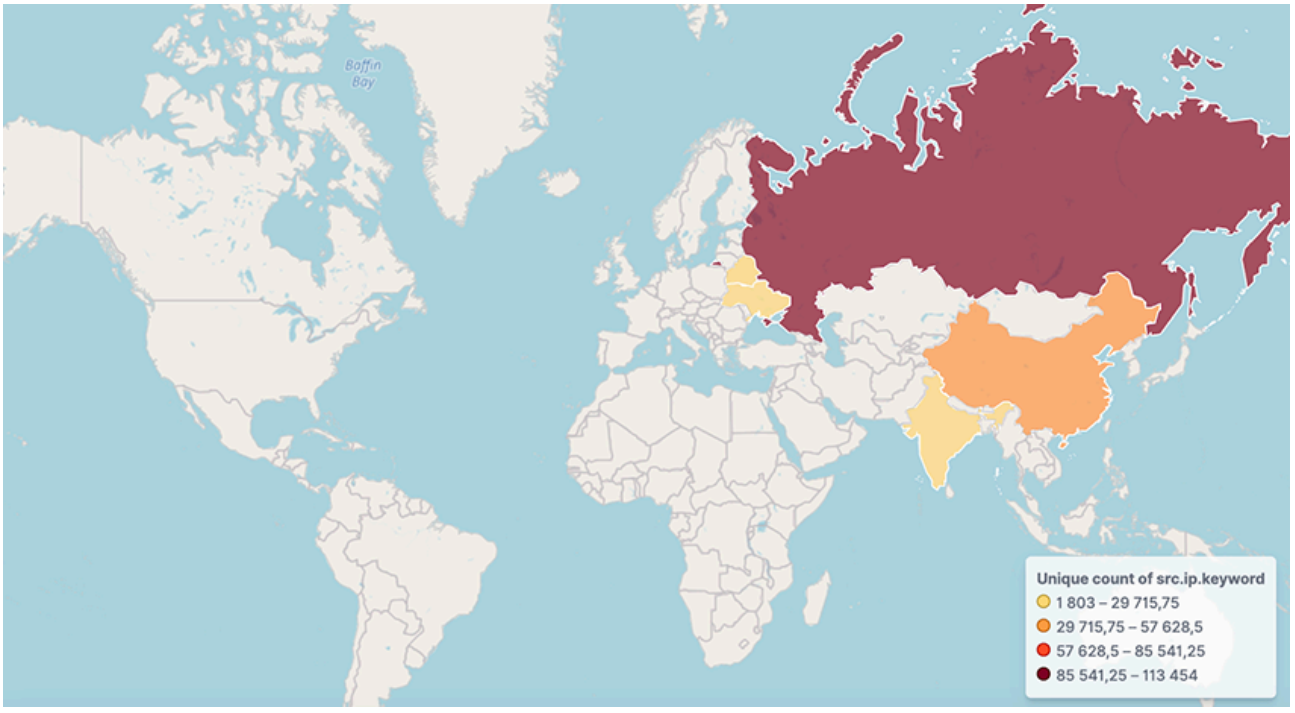
Traffic distribution of the 85% (~160,000 IPs in 24h)

Looking at the Yandex models, they are registered to a Yandex branch in Switzerland registered in 2022. That name changed on November 21, 2023.




Models are disclosed here and here via mac address.

Second, let's talk volume. Telemetry collected indicates that more than **160,000 unique IPs** communicate daily, a number that has been steadily growing.




The majority of communications originate from Russia with the YNDX Smart TV model, followed by China with its Hisense Instwall_T963 smartphone model. Less popular locations include India, Ukraine, and Belarus. Residual traffic (<1300 daily IPs) was also seen from Saudi Arabia, Kazakhstan, Czech Republic, United States, France, and Netherlands.

According to the official website of alice yandex, the manufacturer of the YNDX Smart TVs is actually “LLC Alice Laboratory” with the production site of “Higher Industry Rus LLC” and not the Swiss branch “Intertech Services AG”, this discrepancy is curious. On the same website, the users can buy directly to Russia, Belarus, and Kazakhstan or through **market.yandex[.]ru** and other official partner Russian vendor markets. This and brand popularity alone could explain the lower visibility in other countries including Yandex recent split.

## Hunting of BADBOX Domains

Before packing our bags, we decided to see if we could uncover more BADBOX infrastructure actively communicating, as this would be a strong indication that the botnet is very much alive.

There were several pivot points here: previous IP assignment, URI paths, SSL certificates. The latter produced more results but, nonetheless, we will go through the results of each phase.

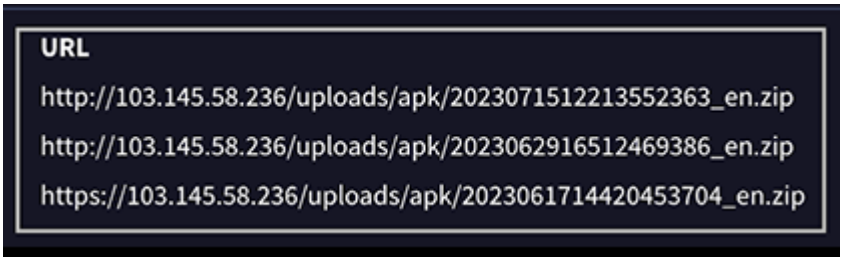
### IP and URI Pathing

Looking into the IPs pointing to `coslogdydy[.]in` (e.g., `170.187.159[.]173` and `103.145.58[.]236`), and pivoting on the URI path of previously known BADBOX C2 domains such as `yxcrl[.]com` led to the discovery of the following domains:

- `cxlcyy[.]com`
- `cxzyr[.]com`
- `goologer[.]com`
- `huuww[.]com`
- `logcer[.]com`
- `pccyy[.]com`
- `pcxrl[.]com`
- `pcxrlback[.]com`
- `soyatea[.]online`
- `ycxad[.]com`
- `yydsmr[.]com`

We can see some indicators: domains are added around the same day, they share naming similarities to previous BADBOX domains. Domains contain ‘log’ wording and variants of the known C2 domain ‘ycxrl[.]com’ named with a one letter difference.

Both mentioned IPs, also show direct communications with the files ”/uploads/apk/20*_en.zip”, a path known as the C2 backdoor payload:




This further confirms its employment in the BADBOX operation.

### SSL Thumbprint

Lastly the ssl thumbprinting creates a fingerprint for a ssl certificate, through a hash function. This is great, because it enables us to easily query any domains that use this certificate, especially relevant when the certificate is self-signed. Which is the case.

The ssl_thumbprint generated from the certificate used by the domain **coslogdydy[.]in** allows us to pivot: 5b3aa659cb8dece5c9a14d605c68a432b773969c (saae)

| First seen | Subject | Thumbprint |
| --- | --- | --- |
| 2023-05-31 | saee | 5b3aa659cb8dece5c9a14d605c68a432b773969c |

```
Data:
   Version: V1
   Serial Number: 90452e0ba6bccfa
   Thumbprint: 5b3aa659cb8dece5c9a14d605c68a432b773969c
Signature Algorithm:
   Issuer: C=65 , CN=saee , L=singapore , O=singapre , ST=singapore , OU=sall
   Validity
      Not Before: 2020-12-12 09:11:34
      Not After: 2030-12-10 09:11:34
```

**36 domains share this self-signed ssl**: Domain list here

Most of these domains seem to be missing A record IP, meaning we are unable to communicate with those domains for further confirmation. This does mean that operations could resume whenever by assigning an IP back to it.

However **2 domains were active: yydsmr[.]com** and **logcer[.]com** by making a http request to the known paths of BADBOX, we confirm their involvement. Both domains responded with an encrypted string.

```
http://yydsmr.com/terminal/client/apiInfo:  200
9uosv0nLR9rfew6AB4QLKz0X9CdRTvceCdGZxrhFO5X5CukgsmYLGsx
```

```
http://logcer.com/terminal/client/apiInfo:  200
gz5kD6+9Z/j8X9ZzOerrHx5M6xS4ANXA2BaLHZ2D/gNAbgfthnBl
```

Perhaps the most shocking factor was the domain `yydsmr[.]com` having over **2 Million pDNS requests** resolved in less than 3 months between **12-2023** and **03-2024**. With another **620,000** between **03-2024** and **10-2024**. This is a clear indication of the large volume of this botnet.

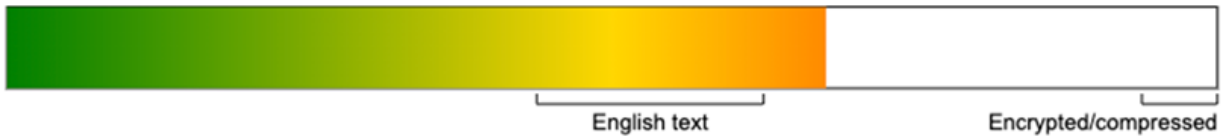
Other interesting domains utilizing this self-signed certificate ( `saae` ) are domains such as `yydsmd[.]com` . Not similar at all to `yydsmr[.]com` . From this list, some shared the same IP (e.g., `172.105.119[.]17` and `139.162.40[.]221` ). The interesting aspect is that they mostly communicate via the following type of request:

```
yydsmd.com/ota/api/conf/v1?m=bd6cb71c8046af6d0851276af7120e50&n=WIFI(1)&syn=1&t=1726327696455
yydsmd.com/ota/api/tasks/v2?m=bd6cb71c8046af6d0851276af7120e50&n=WIFI(1)&syn=1&t=172632771700
```

This definitely looks like a malware check-in, and the response to this request is an encrypted string. With somewhat similar entropy levels between the known BADBOX domains that utilize the `/terminal/client/` path.

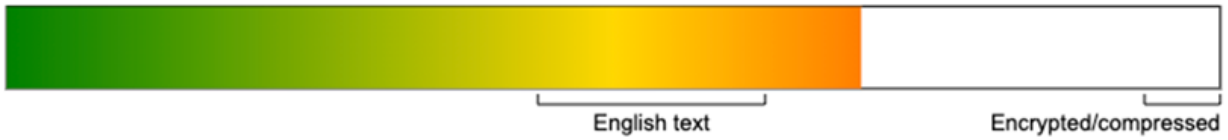
**/terminal/client/** path

```
Shannon entropy: 5.413051110470972
```




And the new domains with the **/ota/api/** path

```
Shannon entropy: 5.633322529690563
```




We also know that BADBOX utilizes different custom encryption schemes depending on the endpoint/uri path.

Currently active domains (respond with an encrypted string to the URI request) are:

- `swiftcode[.]work`
- `home[.]1ztop[.]work`
- `veezy[.]sitev`
- `bluefish[.]work`
- `cast[.]jutux[.]work`
- `echojoy[.]xyz`
- `giddy[.]cc`
- `jolted[.]vip`
- `jutux[.]work`
- `msohu[.]shop`
- `mtcpmpm[.]com`
- `old[.]1ztop[.]work`
- `pixelscast[.]com`
- `pixlo[.]cc`
- `tvsnapp[.]com`
- `www[.]jolted[.]vip`
- `ztword[.]com`

This could be a new adaptation from the BADBOX threat actors, or a new avenue for their schemes—an entirely new investigation is required to explore this further. For now, we will classify the following domains as unconfirmed to be BADBOX malware, but nonetheless, malicious and somewhat related.

The BADBOX operation showcases how cyber criminals are further mastering the art of using global supply chains to spread their malware far and wide. While this blog post focused on infected devices with higher density in Russia and China, BADBOX malware is an epidemic affecting all countries and most types of android devices. Nevertheless, it's crucial to expose how threat actors are slowly creeping their scope to not only off-brand bargain devices, but also diversifying its victim ecosystem to some well-known brands, such as Yandex and Hisense. Choosing trusted vendors becomes increasingly important for the consumer. Likewise, choosing trusted partners becomes a priority for enterprises. Not only is your data at risk, you might also be used for profit and cover of malicious operations. While the crackdown on cyber crime intensifies, selling cover to other cyber criminal groups via ‘compromised’ proxies also gains appeal.

| **C2 Domains** |
| --- |
| coslogdydy[.]in |
| yydsmr[.]com |
| logcer[.]com |
| **SSL Certificate** |
| 5b3aa659cb8dece5c9a14d605c68a432b773969c |
| **APKs** |
| com.yandex.tv.home |
| com.instwall.launch |
| com.mk.ifpd.digitalsignage |
| com.mk.ifpd.setup.guide |
| com.android.launcher3 |

---

Source: https://www.bitsight.com/blog/badbox-botnet-back