

REPORT 2026

BTMOB-Driven Android Malware: Emerging Risk in Pakistan

Analysis by CTM360

TLP	REPORT DATE	THREAT TYPE	CONFIDENCE
White	April 2026	Android RAT + Miner	High malicious behavior



Overview

CTM360 analyzed an Android application presented as a repackaged notes/IPTV-style app. The sample showed behavior consistent with a multi-component Android threat: a BTMOB-style remote access component and a mining-related communication path. Although this malware has been observed worldwide, this report specifically focuses on its emergence in Pakistan.

The strongest observations are BT-MOB identifiers, device enrollment traffic, installed-application inventory collection, screen and foreground-application telemetry, remote options for keylogging and notification harvesting, and a mining-related endpoint on port 8443.

INDUSTRY	COUNTRY	REGION	CAMPAIGN CONTEXT
Financial / Mobile	Pakistan	South Asia	BTMOB / BeatBanker overlap

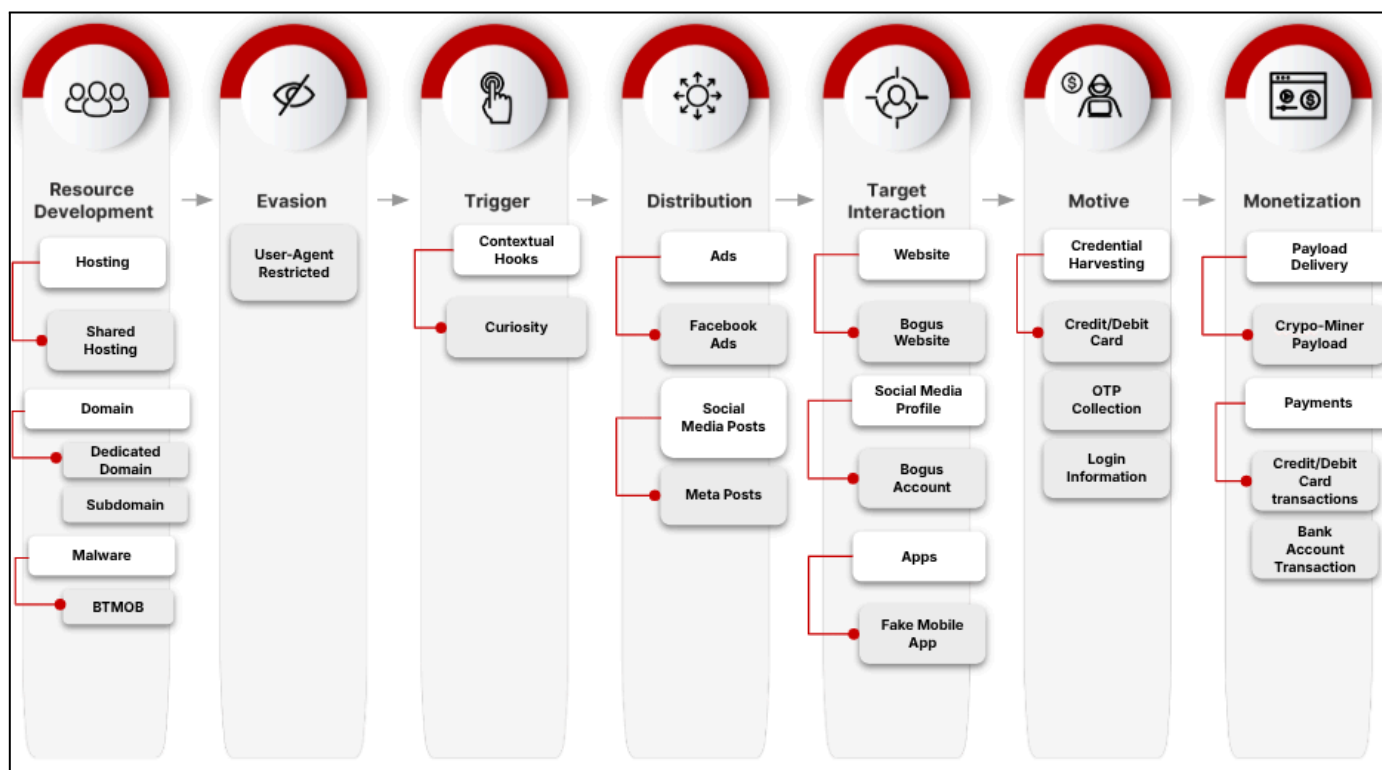
Key takeaway

The sample should be treated as a high-risk Android compromise because it combines surveillance-style RAT behavior with mining-related infrastructure. The mining endpoint `aptabase.jesfeoqrj3.xyz:8443`, resolving to `147.93.153.119:8443`, is a priority indicator for blocking and hunting.

CTM360 Fraud Navigator, inspired by the MITRE framework, is an analysis of the observed scams showing how the scammers navigate through different stages of the scam. Fraud Navigator is a tool that categorizes common scam techniques, providing insights into typical patterns of fraudulent activity. Built on the MITRE model, it identifies six key stages in a scam: resource development, trigger, distribution, target interaction, motive, and monetization.

There are commonly 2 phases in the scam, represented as Phase 1 (in white) & Phase 2 (in grey).

The Fraud Navigator framework has been mapped below to show how it aligns with each stage of the newly identified scam variants. This helps highlight how the scams evolve across both phases.



Distribution

Threat actors heavily exploit social media, particularly Facebook, as their primary distribution channel by creating fake profiles to promote malicious APKs. They also invest in paid advertisements to reach users across Pakistan, which are then used to promote the links to these malware sites.

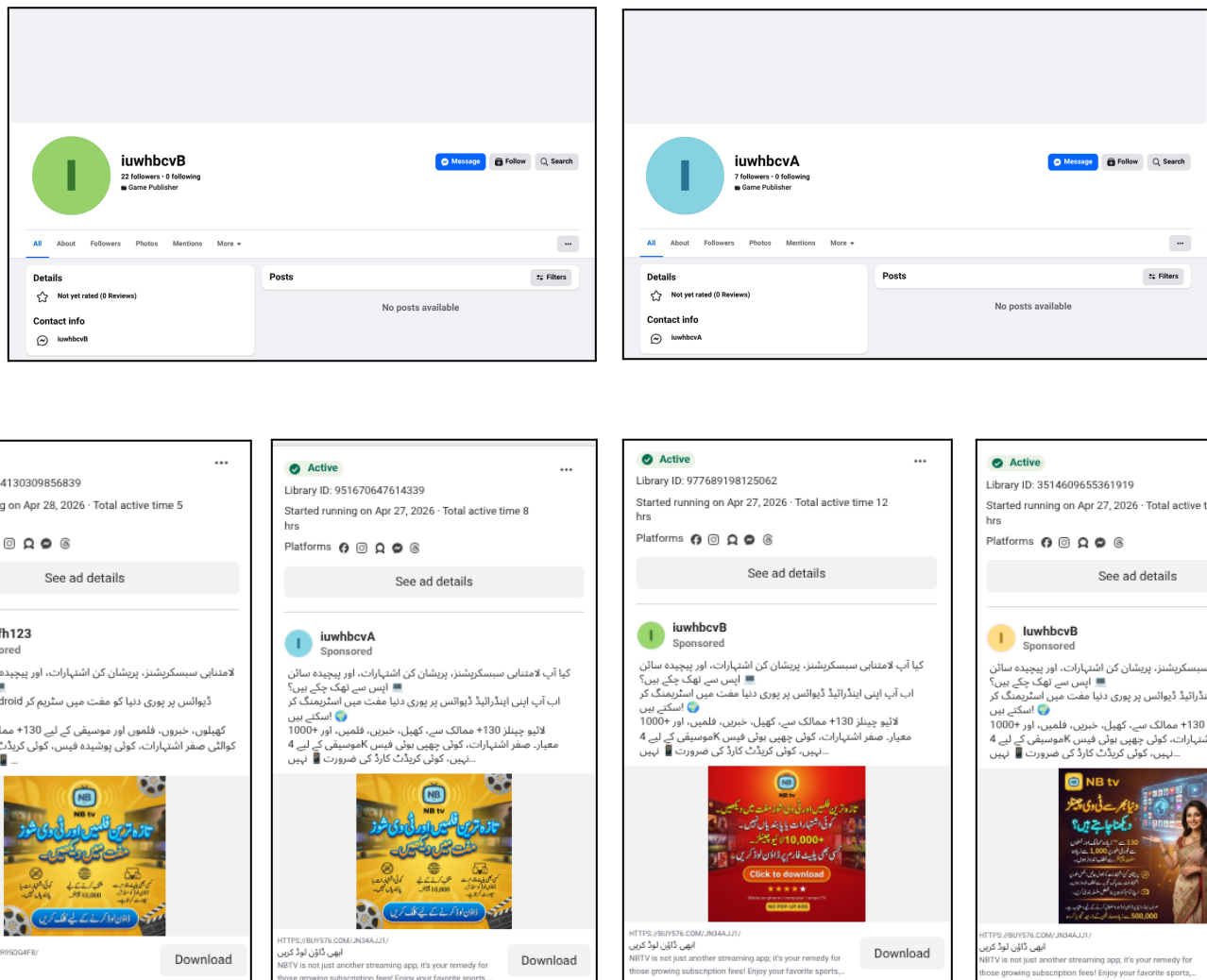


Fig. 1 - Simple apps from facebook ads

On April 29th, **400+ Facebook ads** were seen promoting these sites in Pakistan. Please note that the distribution method is identical to how the Gambling/Casino sites are propagated in Pakistan.

Furthermore, CTM360 has discovered **60+ sites** promoting these APKs over the past 4 months. The sites have been provided in Appendix A.



Observed Attack Chain

The following step-by-step view summarizes what happens in a typical compromise path based on CTM360 lab observations and public BeatBanker/BTMOB context.

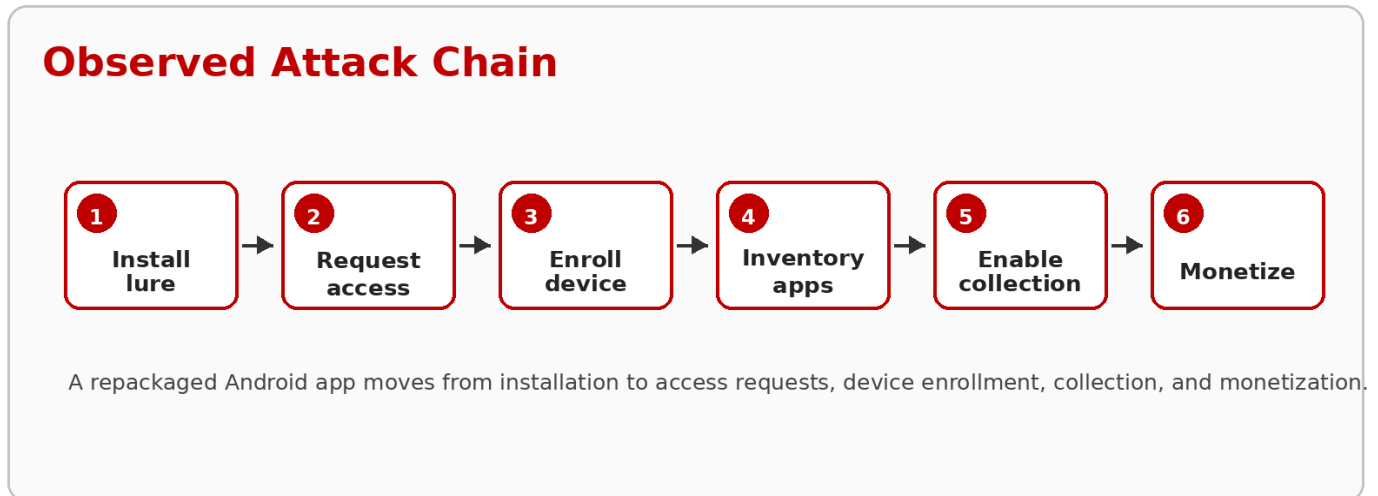


Fig. 2 - Simplified infection and monetization flow.

Step-by-step explanation

1. User installs a repackaged application

The app is presented as a benign notes/IPTV-style utility. This lowers suspicion and increases the chance that the user will grant requested permissions.

2. The app pushes permission and access paths

The screenshots show Android notification, unknown-app installation, and Accessibility/installed-app paths that are important during mobile malware triage.

3. The device enrolls with the remote infrastructure

The sample sends device identifiers and status information that allow the operator to track the victim and manage later activity.

4. Installed applications are collected

The app inventory allows the operator to understand which banking, messaging, security, or crypto applications are present on the device.

5. Remote options enable collection

Observed option messages enabled keystroke and notification collection, creating risk to credentials, chats, OTPs, and MFA prompts.

6. Monetization paths activate

The sample shows both RAT-style surveillance and mining-related communication.

Screenshot Evidence and Meaning

Screenshots captured during the lab run. The images below explain the user-facing steps and why each step matters to defenders.

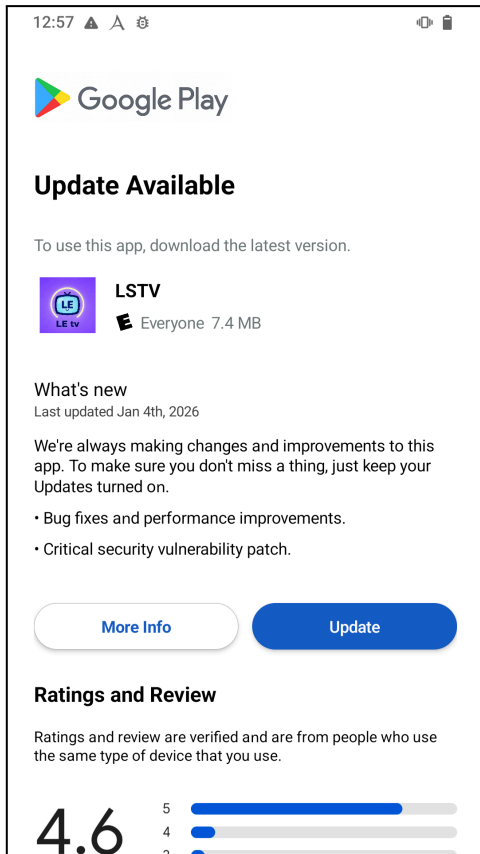


Fig. 3 - Fake update-style screen

The screen resembles a Google Play update page for the LSTV app. This style of prompt can make a sideloaded APK appear legitimate and encourage the user to continue installation.

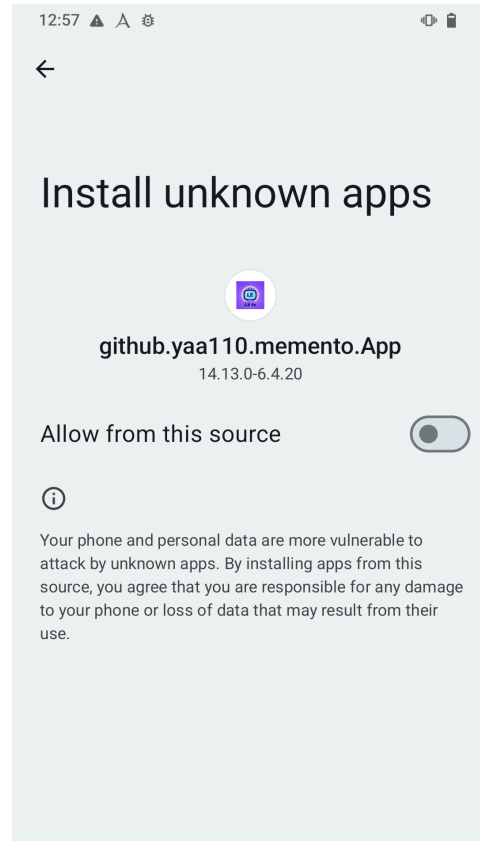


Fig. 4 - Unknown-app installation path

Android shows that github.yaa110.memento.App is allowed or being considered for installation from an unknown source. This is a high-value triage point because sideloading bypasses normal app-store controls.

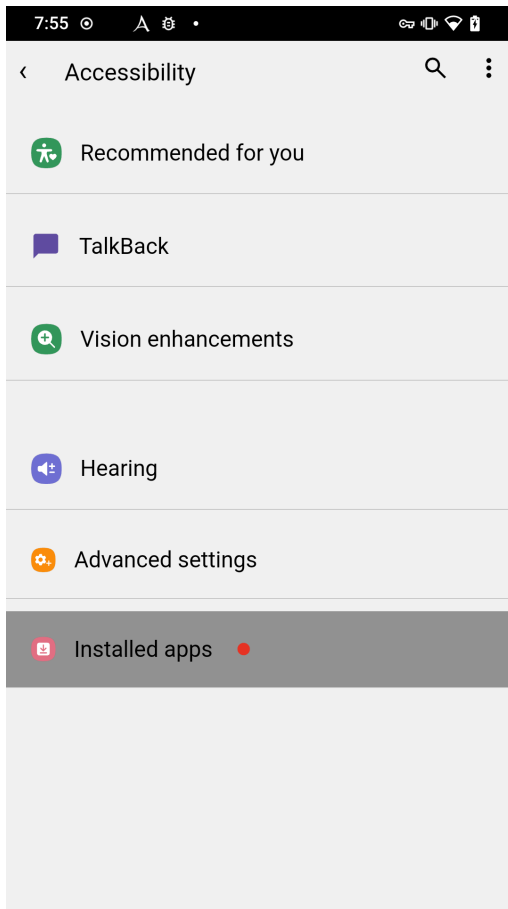


Fig. 5 - Accessibility settings path

The Accessibility menu is a common location to review when investigating Android malware. Abuse of Accessibility can give malware visibility into screen content and user interaction.

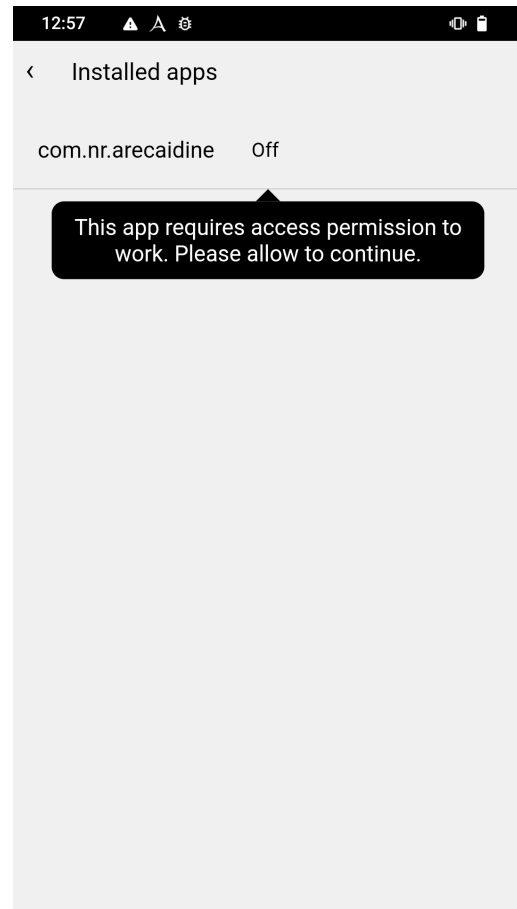


Fig. 6 - Installed-app service prompt

The screenshot shows a service under Installed apps requesting access to work. Permission prompts in this area should be reviewed carefully because they can grant broad device-interaction capabilities.

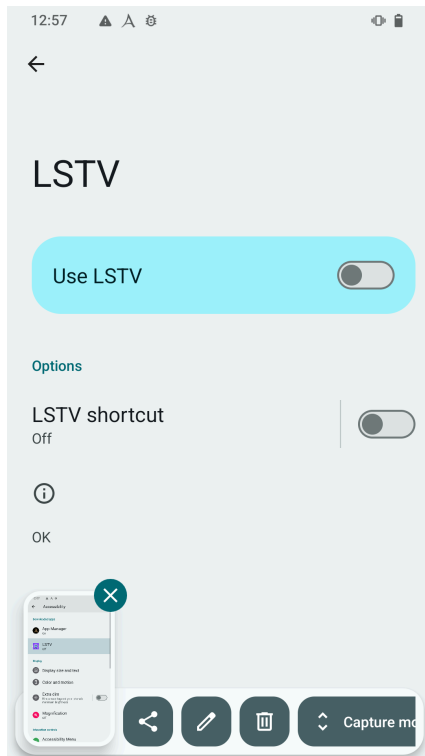


Fig. 7 - App permission toggle view

This screen shows the LSTV-related setting page. For Accessibility Permission

CTM360 Observations

Resource Development

The application was presented as a benign notes/IPTV-style app, while background behavior indicated RAT and mining-related capability. The primary package observed in the lab was com.jhp.shivah, with a secondary or protected package observed as com.nr.arecaidine.

Protected or staged execution patterns were observed, including mining-related logic referenced as MinerCommunicator and repeated attempts to interact with a foreground connector service named com.vuku.cleaners/com.components.ExternalForegroundConnectorService.

Motive and Monetization

The likely motive is financial gain through device access, sensitive-data collection, and mining-related activity. Keylogging and notification collection create exposure for credentials and OTPs. Mining-related traffic creates a resource-hijacking path that can drain battery, increase device heat, and generate revenue for the operator.

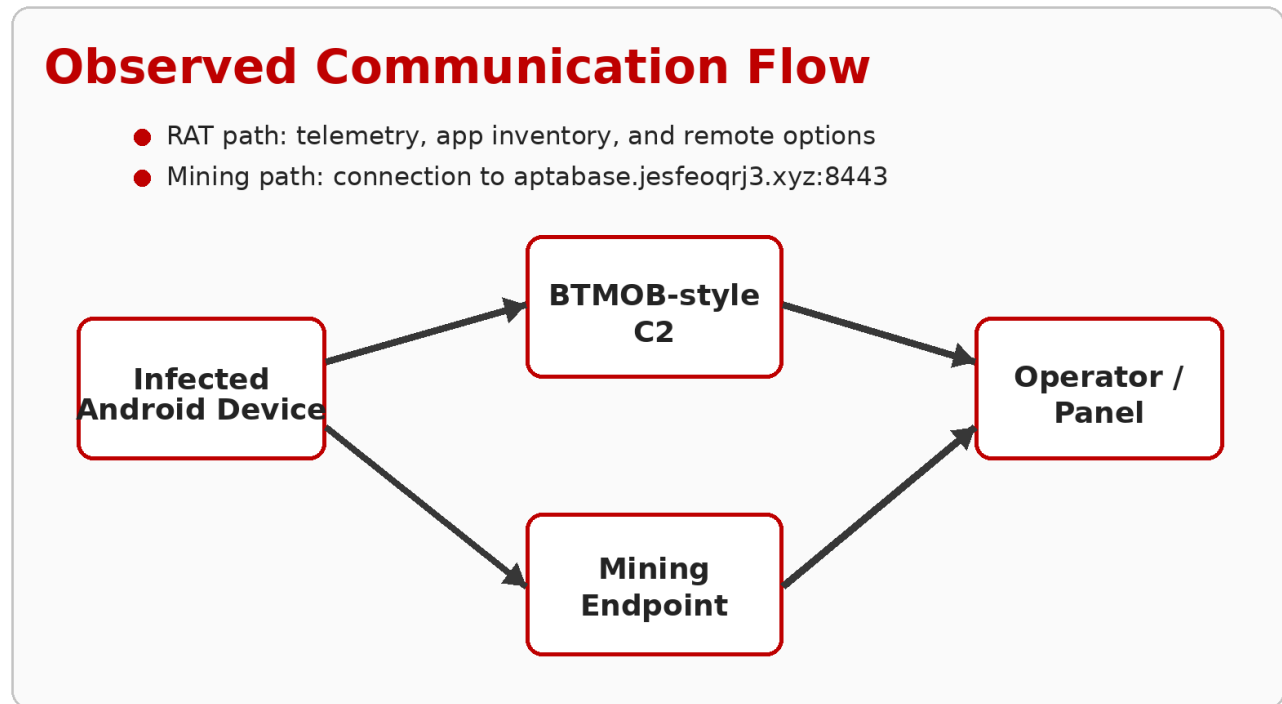


Fig. 9 - High-level observed communication flow without packet-level assumptions.

Impact on Banking Users and Mobile Banking Apps

This malware can create serious risk for banking users because it is designed to monitor activity on the infected Android device. If a victim opens a mobile banking app, the malware may be able to observe the active application, capture typed information, collect notifications, and potentially expose one-time password or authentication messages. This can help attackers steal login credentials, bypass account verification steps, and perform unauthorized access attempts.

Analysis

BTMOB-style RAT Behavior

The RAT-style component collected device and activity information and accepted remote configuration. This is not normal analytics behavior because it includes operator-style controls and collection options that expose credentials, app usage, and notifications.

Observed behavior	Security impact
Device enrollment and status telemetry	Creates a unique victim profile and allows operator-side tracking.
Installed-app inventory collection	Helps identify banking, messaging, security, and crypto apps on the device.
Foreground-app tracking	Reveals what the victim is using in near-real time.
Keylogging option enabled	Creates risk of credential, search, and private-message exposure.
Notification capture enabled	Creates risk of OTP, MFA, password-reset, and private-message exposure.
Screen / PNG telemetry markers	Supports screen-monitoring or screenshot-related activity.

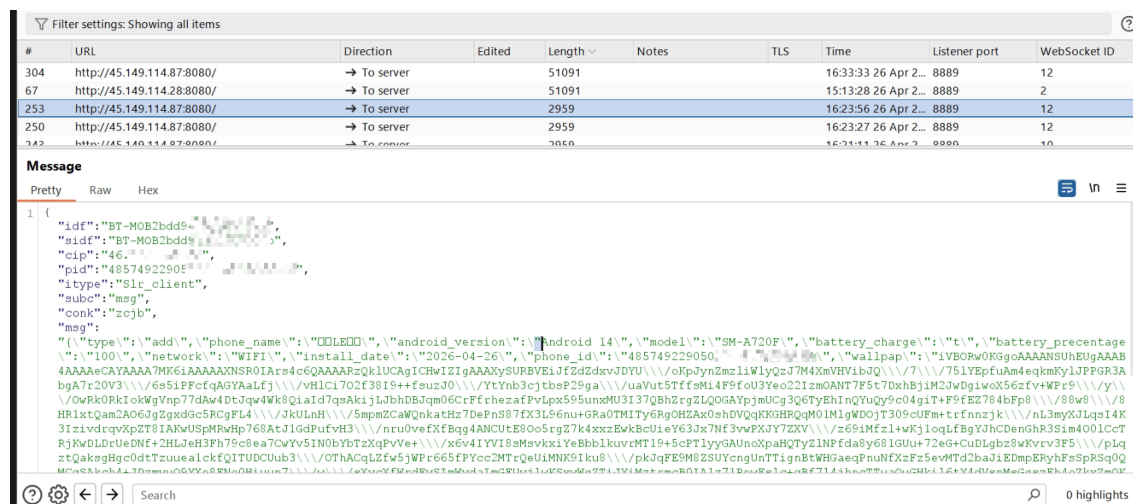


Fig. 10 - Burp view showing device enrollment-style telemetry containing BT-MOB identifiers and device details.

This screenshot shows the device enrolling with the remote infrastructure. The presence of BT-MOB-style identifiers, device model, Android version, battery state, and app-generated telemetry indicates a managed victim profile rather than ordinary app statistics.

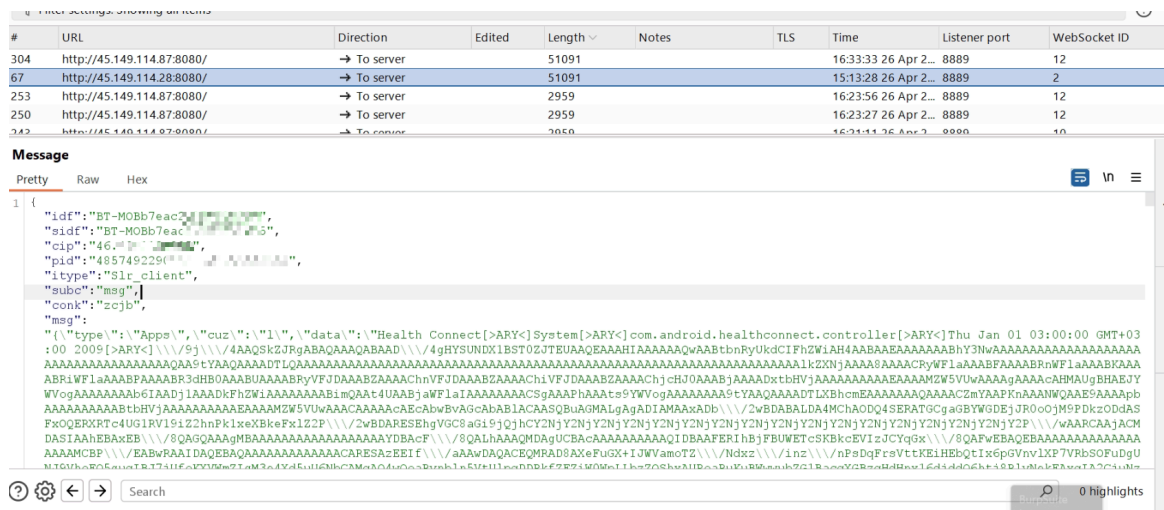


Fig. 11 - Installed-application inventory message observed in the traffic capture.

The installed-app inventory gives the operator a view of applications present on the device. This is valuable for identifying financial apps, messaging tools, security software, browsers, and other targets of interest.

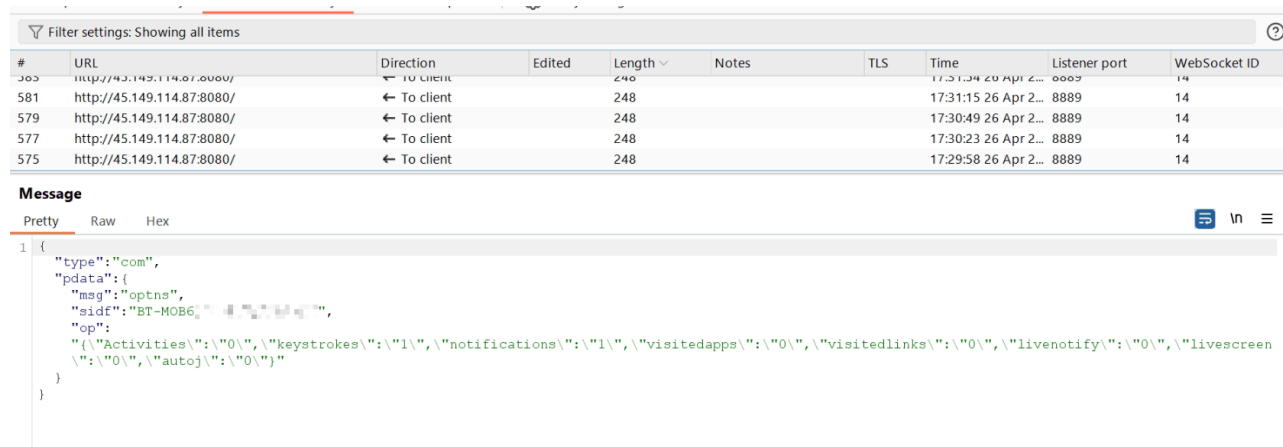


Fig. 12 - Remote option message enabling sensitive collection features

The options message showed keystroke and notification collection enabled. This materially increases risk because notifications often contain OTPs, account recovery messages, private communications, and transaction alerts.

Mining-Related Activity

CTM360 identified a mining-related endpoint and mining-related code paths. The report intentionally avoids packet-size or protocol-marker claims and focuses on the reliable defensive evidence: destination, port, app behavior, and security impact.

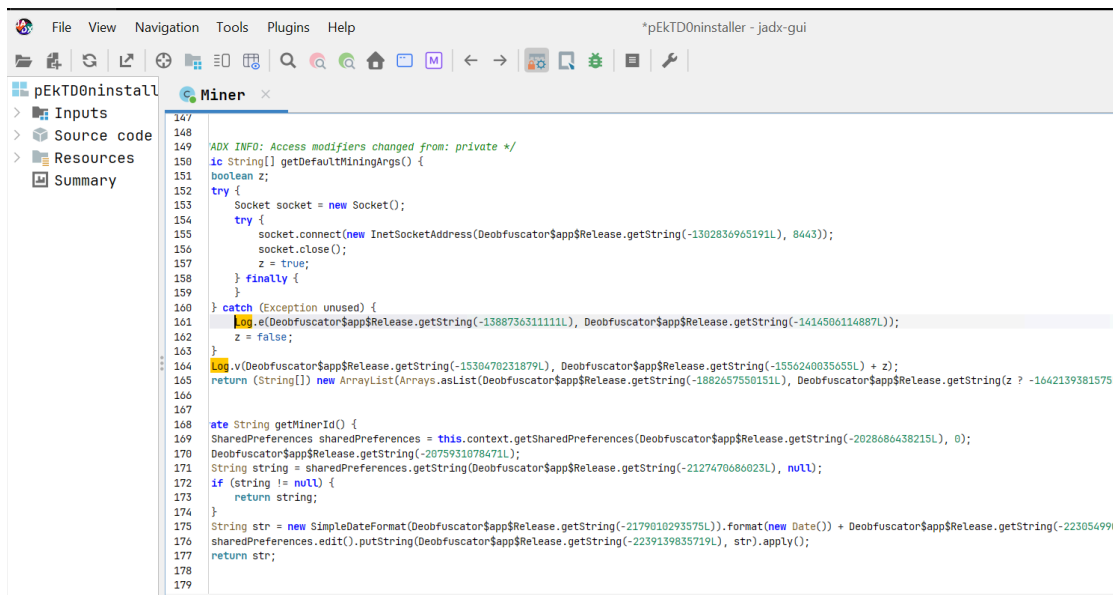


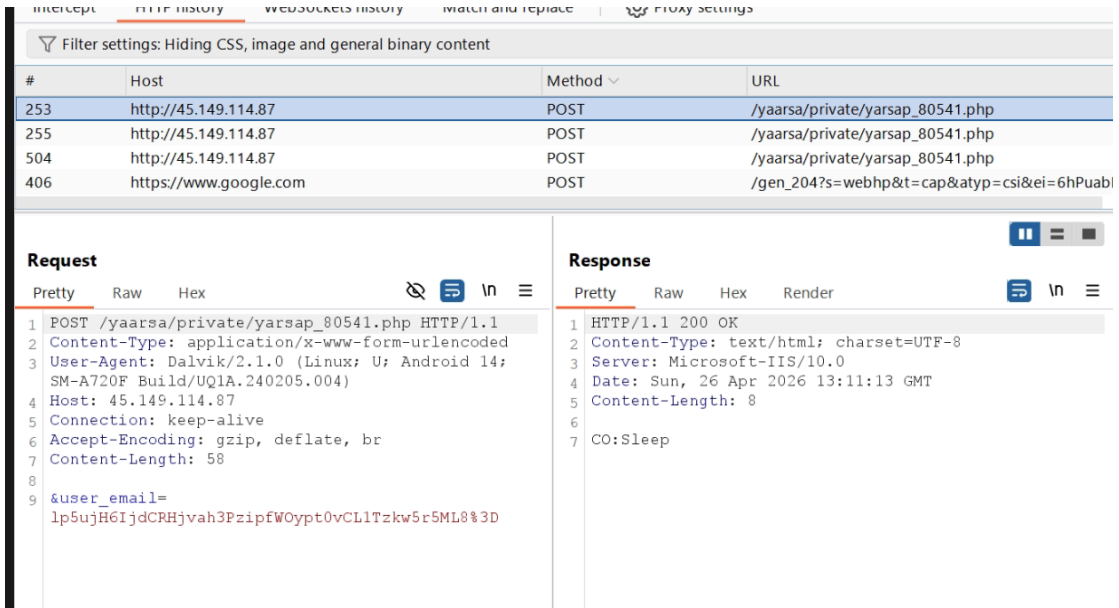
Fig. 13 - Decompilation view showing mining-related logic and a connection attempt to port 8443.

The decompilation screenshot shows a mining-related class view and a connection to port 8443. In combination with lab notes identifying aptabase.jesfeorj3.xyz, this supports the assessment that the sample included a mining-related communication path.

Indicator type	Value	Assessment
Domain	aptabase.jesfeorj3.xyz	Mining-related endpoint identified in CTM360 lab notes.
IP / Port	147.93.153.119:8443	Resolved endpoint associated with the mining-related channel.
Related endpoint	famelack.com:443	Secondary endpoint noted in lab context;
Mining proof level	Endpoint and code-path evidence	The report does not claim wallet address, revenue, or accepted shares were recovered.

Network Evidence

Network captures show C2-style HTTP/WebSocket traffic and device registration messages. These artifacts are useful for building blocklists, detection rules, and incident-response timelines.



Wireshark network capture showing an HTTP POST request to `/yaarsa/private/yarsap_80541.php`. The request includes a `user_email` parameter encoded in the body. The response is a 200 OK status.

#	Host	Method	URL
253	http://45.149.114.87	POST	/yaarsa/private/yarsap_80541.php
255	http://45.149.114.87	POST	/yaarsa/private/yarsap_80541.php
504	http://45.149.114.87	POST	/yaarsa/private/yarsap_80541.php
406	https://www.google.com	POST	/gen_204?s=webhp&t=cap&atyp=csi&ei=6hPuabl

Request

Pretty Raw Hex

```
1 POST /yaarsa/private/yarsap_80541.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 User-Agent: Dalvik/2.1.0 (Linux; U; Android 14;
  SM-A720F Build/UQ1A.240205.004)
4 Host: 45.149.114.87
5 Connection: keep-alive
6 Accept-Encoding: gzip, deflate, br
7 Content-Length: 58
8
9 &user_email=
  lp5ujH6IjdCRHjvvh3PzipfWOypt0vCL1Tzkw5r5ML8%3D
```

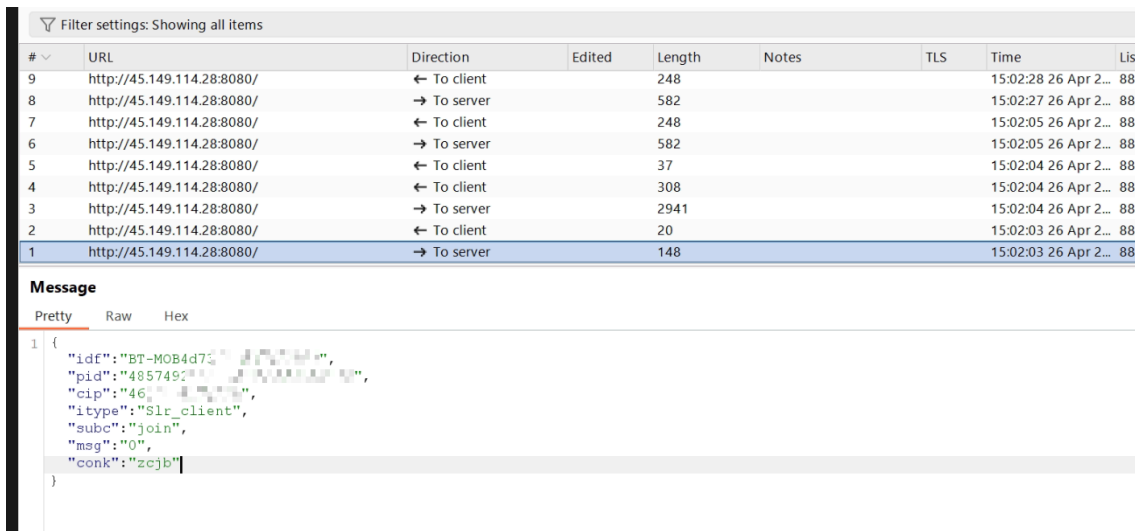
Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=UTF-8
3 Server: Microsoft-IIS/10.0
4 Date: Sun, 26 Apr 2026 13:11:13 GMT
5 Content-Length: 8
6
7 C0:Sleep
```

Fig. 14 - HTTP request to an observed staging path with encoded user identifier parameter.

The request to `/yaarsa/private/yarsap_80541.php` shows an encoded user-related parameter and a server response.



Wireshark network capture showing a join-style message containing BT-MOB identifier fields. The message is a JSON object with fields like `idf`, `pid`, `cid`, `itype`, `subc`, `msg`, and `conk`.

#	URL	Direction	Edited	Length	Notes	TLS	Time	Lis
9	http://45.149.114.28:8080/	← To client		248			15:02:28 26 Apr 2...	88
8	http://45.149.114.28:8080/	→ To server		582			15:02:27 26 Apr 2...	88
7	http://45.149.114.28:8080/	← To client		248			15:02:05 26 Apr 2...	88
6	http://45.149.114.28:8080/	→ To server		582			15:02:05 26 Apr 2...	88
5	http://45.149.114.28:8080/	← To client		37			15:02:04 26 Apr 2...	88
4	http://45.149.114.28:8080/	← To client		308			15:02:04 26 Apr 2...	88
3	http://45.149.114.28:8080/	→ To server		2941			15:02:04 26 Apr 2...	88
2	http://45.149.114.28:8080/	← To client		20			15:02:03 26 Apr 2...	88
1	http://45.149.114.28:8080/	→ To server		148			15:02:03 26 Apr 2...	88

Message

Pretty Raw Hex

```
1 {
  "idf": "BT-MOB4d7...",
  "pid": "485749...",
  "cid": "46...",
  "itype": "Slr_client",
  "subc": "join",
  "msg": "0",
  "conk": "zcjb"
}
```

Fig. 15 - Join-style message containing BT-MOB identifier fields.

This traffic shows client and device identifiers being sent to the server. Such messages are used to register or track an infected device in an operator panel.

Indicators of Compromise

The indicators below are separated into CTM360-observed items and public-context items. Public indicators can support broader hunting, but they should not be assumed present in every related sample without local confirmation.

Type	Indicator	Notes
SHA-256	28FE36653BAB1AC0C16437B794 55AAB1B5A2EF428BF2A67F7815 E61651AB2FEA	APK hash observed in lab.
Package	com.jhp.shivah	Repackaged notes/IPTV-style app.
Package	com.nr.arecaidine	Secondary/protected package observed.
Domain	aptabase.jesfeoqrj3.xyz	Mining-related endpoint.
IP / Port	147.93.153.119:8443	Resolved mining-related endpoint.
Domain / Port	famelack.com:443	Secondary endpoint in lab notes; purpose not fully proven.
IP / Port	45.149.114.87:8080	Observed C2 infrastructure
IP / Port	45.149.114.28:8080	Observed C2 infrastructure
Identifier pattern	BT-MOB*	BTMOB-style victim/client identifier pattern.

Recommendations

- To reduce the risk of infection from Android malware and similar mobile threats, CTM360 recommends the following security practices:
- Download applications only from trusted sources, such as the official Google Play Store or Apple App Store.
- Avoid installing APK files shared through SMS, messaging apps, emails, advertisements, or unofficial websites.
- Use a reputable security solution on mobile devices, laptops, and other connected endpoints.
- Enable Google Play Protect on Android devices and keep it active.
- Use strong, unique passwords and enable multi-factor authentication wherever possible.
- Enable biometric protection, such as fingerprint or facial recognition, to secure mobile device access.
- Be cautious when opening links received through SMS, email, or messaging platforms, especially when they claim to offer urgent updates, rewards, refunds, or account verification.
- Review application permissions carefully before granting access, especially Accessibility, notification access, SMS, overlay, camera, microphone, and file permissions.
- Keep mobile devices, operating systems, browsers, and applications updated with the latest security patches.

References

- Kaspersky Securelist, "BeatBanker: both banker and miner for Android," 10 March 2026.
<https://securelist.com/beatbanker-miner-and-banker/119121/>
- Kaspersky Press Release, "Kaspersky uncovers a new Android malware campaign disguised as Starlink application," 10 March 2026.
<https://www.kaspersky.com/about/press-releases/kaspersky-uncovers-a-new-android-malware-campaign-disguised-as-starlink-application>

Disclaimer

The information contained in this document is intended to provide general threat intelligence and guidance to the intended recipient. It is provided as-is without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Under no condition shall CTM360, its related partners, directors, principals, agents, or employees be liable for damages or claims arising out of or in connection with this advisory.

Appendix A: Websites observed

Active Sites

- [https://jootix\[.\]mom/](https://jootix[.]mom/)
- [https://jccaakt\[.\]cfd/](https://jccaakt[.]cfd/)
- [https://jppyyyi\[.\]mom/](https://jppyyyi[.]mom/)
- [https://jwwaatn\[.\]cfd/](https://jwwaatn[.]cfd/)
- [https://jbcealfoul\[.\]top/](https://jbcealfoul[.]top/)
- [https://jyyccui\[.\]lat/](https://jyyccui[.]lat/)
- [https://jwatchchantva4\[.\]cfd/](https://jwatchchantva4[.]cfd/)
- [https://jwatchchantv20\[.\]cfd/](https://jwatchchantv20[.]cfd/)
- [https://jwatchedxmfreelive04\[.\]cfd/](https://jwatchedxmfreelive04[.]cfd/)
- [https://jwatchedxmfreelive03\[.\]cfd/](https://jwatchedxmfreelive03[.]cfd/)
- [https://jwatchaachantvlive01\[.\]cfd/](https://jwatchaachantvlive01[.]cfd/)
- [https://jwatchchantv17\[.\]cfd/](https://jwatchchantv17[.]cfd/)
- [https://jwatchtvchantnew01\[.\]cfd/](https://jwatchtvchantnew01[.]cfd/)
- [https://jwatchtvchantnew04\[.\]cfd/](https://jwatchtvchantnew04[.]cfd/)
- [https://jwatchtvchantnew03\[.\]cfd/](https://jwatchtvchantnew03[.]cfd/)
- [https://jwatchchanel95\[.\]shop/](https://jwatchchanel95[.]shop/)
- [https://jwatchchantv42\[.\]cfd/](https://jwatchchantv42[.]cfd/)
- [https://jwatchchantv45\[.\]cfd/](https://jwatchchantv45[.]cfd/)
- [https://jwatchchantv44\[.\]cfd/](https://jwatchchantv44[.]cfd/)
- [https://jwatchchantv43\[.\]cfd/](https://jwatchchantv43[.]cfd/)
- [https://jwatchchantv26\[.\]cfd/](https://jwatchchantv26[.]cfd/)
- [https://jwatchchanel91\[.\]shop/](https://jwatchchanel91[.]shop/)
- [https://jwatchchantv27\[.\]cfd/](https://jwatchchantv27[.]cfd/)
- [https://jchannelstv01\[.\]cfd/](https://jchannelstv01[.]cfd/)
- [https://jbobojitv02\[.\]cfd/](https://jbobojitv02[.]cfd/)
- [https://jtvngarden\[.\]net/](https://jtvngarden[.]net/)

Inactive Sites

- [https://jwatchchanytbb15\[.\]cfd/](https://jwatchchanytbb15[.]cfd/)
- [https://jwatchchanytbb13\[.\]cfd/](https://jwatchchanytbb13[.]cfd/)
- [https://jwatchchanytbb05\[.\]cfd/](https://jwatchchanytbb05[.]cfd/)
- [https://jwatchchantv37\[.\]cfd/](https://jwatchchantv37[.]cfd/)
- [https://jwatchchantv15\[.\]cfd/](https://jwatchchantv15[.]cfd/)
- [https://jwatchchanytbb02\[.\]cfd/](https://jwatchchanytbb02[.]cfd/)
- [https://jwatchqxd08\[.\]cfd/](https://jwatchqxd08[.]cfd/)
- [https://jwatchchantv38\[.\]cfd/](https://jwatchchantv38[.]cfd/)
- [https://jwatchchantv41\[.\]cfd/](https://jwatchchantv41[.]cfd/)
- [https://jwatchchantv14\[.\]cfd/](https://jwatchchantv14[.]cfd/)
- [https://jwatchchantv13\[.\]cfd/](https://jwatchchantv13[.]cfd/)
- [https://jhzgongfreetv03\[.\]cfd/](https://jhzgongfreetv03[.]cfd/)
- [https://jwatchchantv11\[.\]cfd/](https://jwatchchantv11[.]cfd/)
- [https://jtvshowdownload02\[.\]cfd/](https://jtvshowdownload02[.]cfd/)

-
- [https://tv-garden-s\[.\]online/](https://tv-garden-s[.]online/)
 - [https://tv-8868\[.\]com/](https://tv-8868[.]com/)
 - [https://watchchantv05\[.\]net/](https://watchchantv05[.]net/)
 - [https://watchchantv34\[.\]cfd/](https://watchchantv34[.]cfd/)
 - [https://watchchantv25\[.\]cfd/](https://watchchantv25[.]cfd/)
 - [https://watchchantv24\[.\]cfd/](https://watchchantv24[.]cfd/)
 - [https://watchchantv21\[.\]cfd/](https://watchchantv21[.]cfd/)
 - [https://watchchantv33\[.\]cfd/](https://watchchantv33[.]cfd/)
 - [https://watchqxd04\[.\]cfd/](https://watchqxd04[.]cfd/)
 - [https://watchchantv06\[.\]cfd/](https://watchchantv06[.]cfd/)
 - [https://watchchantv03\[.\]cfd/](https://watchchantv03[.]cfd/)
 - [https://jazlanhost\[.\]online/](https://jazlanhost[.]online/)
 - [https://dqldwqsdwq-dqwdqoldwq-sd1qdsdlwq-qwdlqqldwqdwq-qwdqw\[.\]cam/](https://dqldwqsdwq-dqwdqoldwq-sd1qdsdlwq-qwdlqqldwqdwq-qwdqw[.]cam/)
 - [https://watchchantv01\[.\]cfd/](https://watchchantv01[.]cfd/)
 - [https://watchchantv02\[.\]cfd/](https://watchchantv02[.]cfd/)
 - [https://watchchanel20\[.\]com/](https://watchchanel20[.]com/)
 - [https://chanelwatch1\[.\]com/](https://chanelwatch1[.]com/)
 - [https://watchchanel10\[.\]com/](https://watchchanel10[.]com/)
 - [https://watchchanel1\[.\]com/](https://watchchanel1[.]com/)
 - [https://watchchanel2\[.\]com/](https://watchchanel2[.]com/)
 - [https://watchchanel3\[.\]com/](https://watchchanel3[.]com/)
 - [https://watchchanel\[.\]com/](https://watchchanel[.]com/)

About us

CTM360 enables organizations to protect themselves and their supply chain against external risks and threats.

CTM360 provides a consolidated platform that includes External Attack Surface Management, Digital Risk Protection, Brand Protection and Anti-Phishing, Data Leakage Protection, Unlimited Managed Takedowns, Security Ratings, Third Party Risk Management, Email Intelligence (DMARC), and Cyber Threat Intelligence.

Contact us

- +973 77 360 360
- info@ctm360.com
- www.ctm360.com
- 21st Floor, East Tower, Bahrain Financial Harbour, Kingdom of Bahrain