Uncovering Joker's C2 Network: How Hunt's SSL History Exposed Its Infrastructure

Published: 2025-02-27 · Archived: 2026-04-05 14:43:49 UTC

Joker is a mobile malware family that has targeted Android devices since at least 2017. Masquerading as legitimate applications, it is frequently distributed through the Google Play Store, slipping past security controls before being removed. Once installed, it intercepts SMS messages, harvests contact lists and device information, and stealthily subscribes victims to premium services.

The malware's operators deploy their command-and-control (C2) infrastructure across cloud-hosted servers, frequently reusing SSL certificates to encrypt communications and obscure network traffic. Tracking these certificates and their associated IPs can expose connections between seemingly unrelated servers, offering defenders a method to uncover and monitor malicious infrastructure over time.

This post examines the role of SSL intelligence in tracking and identifying Joker-linked C2s, showing how certificate pivots can uncover additional infrastructure and provide insight into the malware's operational patterns.

It All Started With an APK

Our research began with an APK file uploaded to Hatching Triage, an online malware sandbox, named com.hdphoto.wallpaper4k.apk (SHA-256: `7f186746152d9569421a88e506c89844eaf0c2036ab5dbe0edb0775a79d9bb9d`). A search for the file in VirusTotal showed that six out of 47 vendors flagged it as Joker malware.

The APK's name suggests the malware operators lure potential victims under the guise of a 4K wallpaper application. The app is not hosted on the Google Play Store as of this writing.

Network Communication and Additional Infrastructure

Upon execution, the malware initiates an HTTP POST request to `http[:]//hdphoto[.]uno/conf/vcheck`. This domain resolved to `47.236.49[.]195`, and then moved to `47.237.68[.]53` in mid-February.

Both servers belong to the Alibaba Cloud network, hosted in Singapore, and have servers running nginx version 1.18.0 on ports 80 and 443. The below domains also resolve to the IPs:

- `47.236.49[.]195 → gasu[.]pw`
- `47.237.68[.]53 → femk[.]top, tuatol[.]store`

The IP ending in .195 will be our starting point for this post as hdphoto[.] initially resolved to that address.

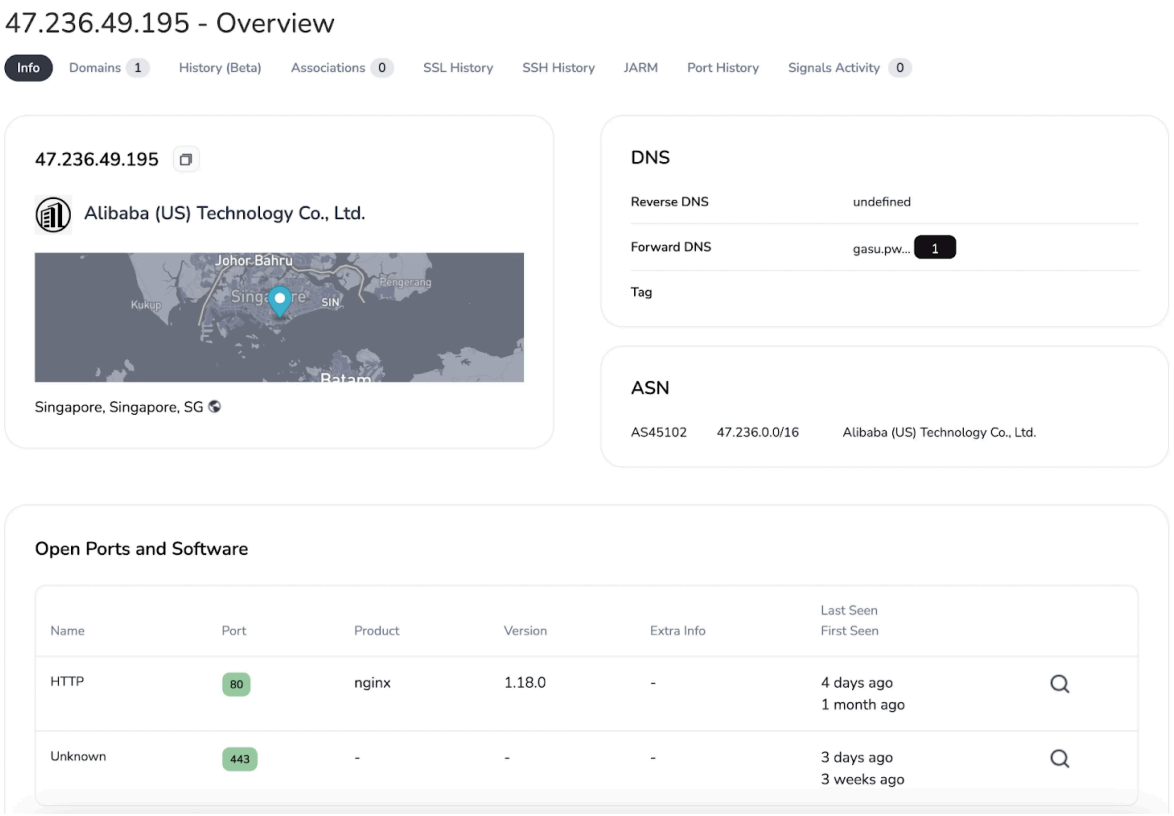

Figure 1: IP overview of 47.236.49[.]195 in Hunt.

The request to /conf/vcheck returns the following response:

```
https[:]//hdphotouno.oss-me-east-1[.]aliyuncs[.]com/dex1_v16.txt
```

A VirusTotal search of the resolving IP, `47.91.99[.]31`, hosted on the Alibaba network, reveals multiple APK files communicating with the server, many of which are detected as malicious.

Testing different HTTP requests to check for unique responses is essential when tracking adversary infrastructure. The malware sends a POST request, so we'll send a GET request in a lab environment to assess any changes.

The server responds with a Django REST framework webpage, suggesting the server is configured to handle API-based communications for managing malware-related requests. Django is an open-source web framework written in Python, and the REST framework is an extension specifically for building Web APIs.

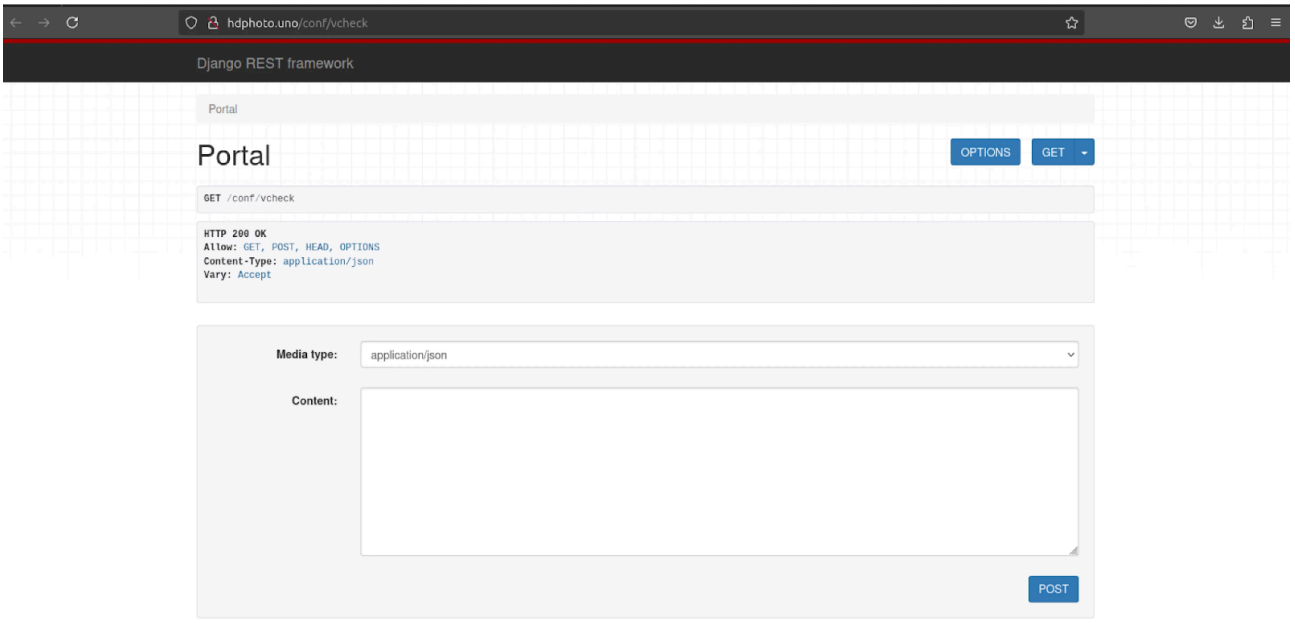

Figure 2: Screenshot of the API endpoint page at hdphoto[.]uno/conf/vcheck.

dex1_v16.txt (SHA-256: `2766ce69097ccb0cd9b4a7f3cf6eac19d76db2acf7d1b6844cc10d5460528138`) contains base64-encoded text, which we can easily decode with CyberChef. The result is an executable DEX file containing the Joker payload. The filename suggests versioning, with 'v16' likely indicating an iteration of the trojan. Of note, the malware authors made no effort to obfuscate the document's name to conceal its purpose.

Figure 3: Result of running the contents of dex1_v16.txt in CyberChef.

Next, a request to the same domain is made for another text file, encoded2.txt (SHA-256: `4000d8110f92d5622a19a75d85c7af38fef810cecfe054e02779da9c1e218e5d`). This file follows a similar path as the previously described and is likely the second stage of the attack.

Finally, the malware makes repeated POST requests to `https[:]//hdphoto[.]uno/1VybiUSr`. Once again, sending a different HTTP request results in a different API page titled 'Aes Api.'

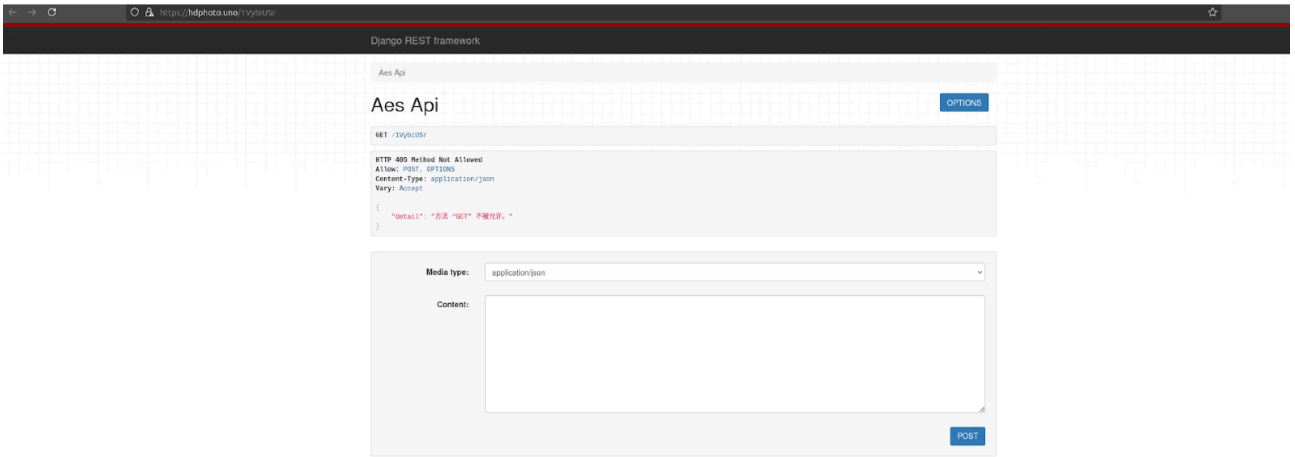

Figure 4: Screenshot of the API endpoint page at hdphoto[.]uno/1VybiUSr.

Tracking Joker's Infrastructure via Hunt SSL History

SSL certificate analysis is a powerful tool for uncovering malicious infrastructure, tracking adversary movement, and identifying attack staging before operations go live. Building on previous research into SSL intelligence, we applied the same methodology to analyze `47.236.49[.]195` using the SSL History tab in Hunt.

SSL Certificate Observations

According to our scan data, this IP only began using SSL certificates in early February 2025. Both certificates were issued through **Let's Encrypt**, a free certificate authority that automates issuance and renewal. While widely used for legitimate services, Let's Encrypt is frequently leveraged by threat actors due to its ease of acquisition and lack of strict identity validation.

Additionally, both certificates use uncommon top-level domains (TLDs) in the subject common name, similar to the .fit, .top, and .store domains observed in the previous section. While TLDs alone aren't necessarily a strong indicator of malicious activity, the reuse of infrastructure across different certificates indicates the operators are maintaining control over their servers rather than fully abandoning them.

Rotation of certificates is a common threat actor tactic used to refresh encryption keys, evade detections on specific certificate fingerprints, or extend the lifespan of malicious infrastructure.

By pivoting on **Certificate IPs**, we can quickly uncover additional servers that have used these certificates---whether actively in use or historically linked. This approach helps reconstruct attack timelines and track infrastructure reuse, which is particularly relevant in long-running malware operations.

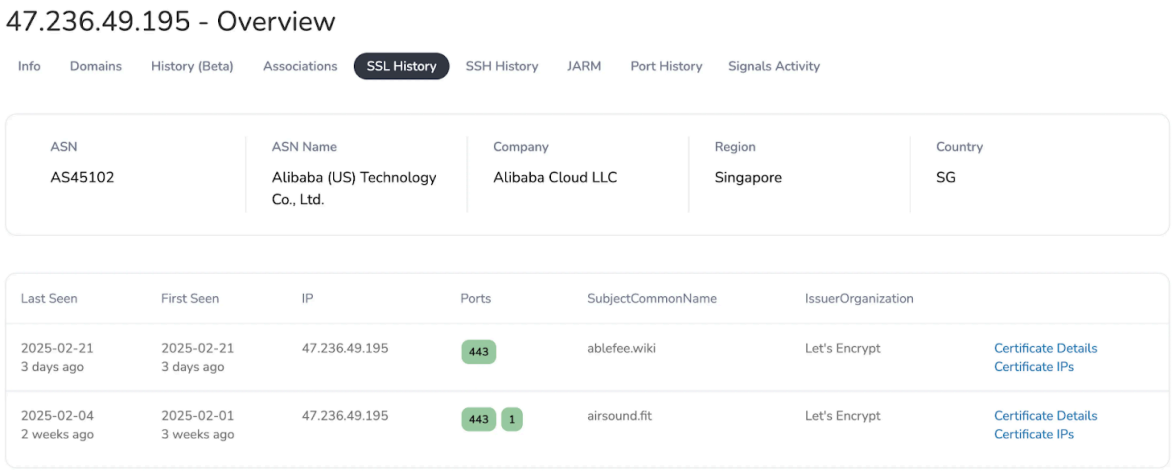

Figure 5: Screenshot of SSL History of IP address 47.236.49[.]195 in Hunt.

Infrastructure Shifts Between Certificates

The older certificate, SHA-256: `95F845F390269A3805657C9F544719C937FD458966818FADCBAD7D4CC05B69FF`, issued for `airsound[.]fit` was observed from February 1 to February 4, 2025, and is associated with 71 IPs, all hosted within Alibaba Cloud infrastructure.

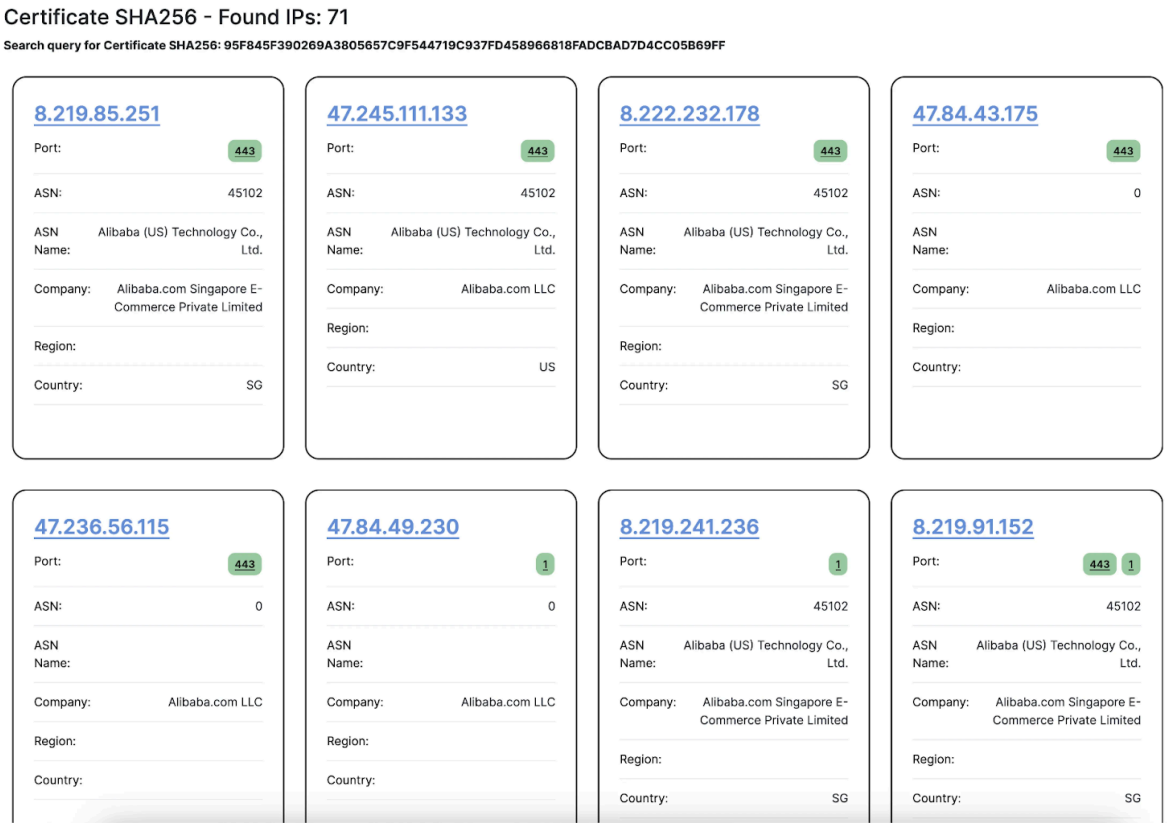

Figure 6: Snippet of IPs related to the airsound[.]fit certificate in Hunt.

The more recent certificate, SHA-256: `5848152508ACC864869500C0DFFF20723A087019EB717131DC6D7DF51FBD75E6`, issued for `ablefee[.]wiki`, was observed for a single day on February 21, 2025. Despite this short-lived presence, it appeared on 77 IPs, which completely overlapped with the older certificate but included a handful of additional servers.

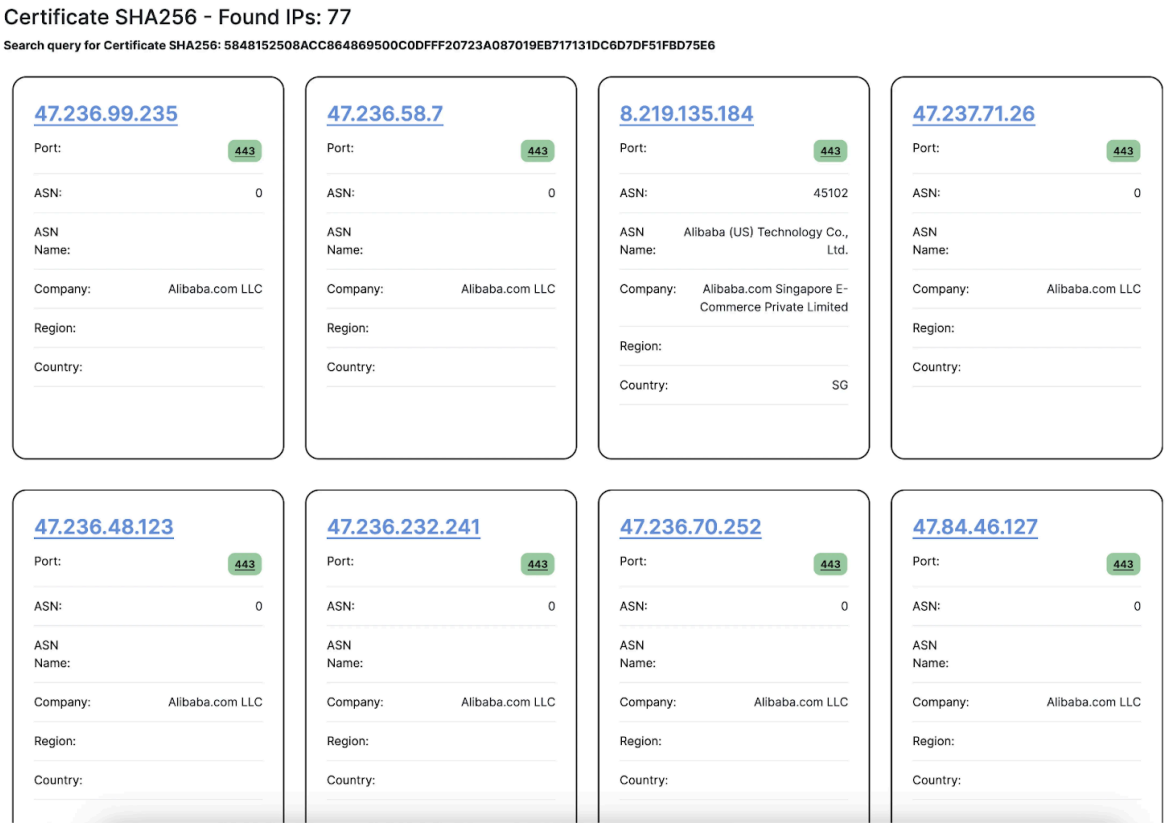

Figure 7: Screenshot of 'Certificate IPs' results for ablefee[.]wiki certificate in Hunt.

Infrastructure Analysis

The 77 IPs associated with the `ablefee[.]wiki` certificate are spread across two autonomous systems (ASNs):

- Alibaba.com LLC
- Alibaba.com Singapore E-Commerce Private Limited

The majority of these servers are hosted in Singapore, with a smaller subset located in the United States. All use the standard port associated with TLS-encrypted communications, 443.

The domains linked to this infrastructure continue to follow the pattern of uncommon TLDs, which the threat actor(s) seem to rely heavily on. Some domains suggest potential themes designed to lure victims, such as:

- `securemsg[.]store`
- `screenlocker[.]art`
- `timestampmark[.]me`

These domains were registered through one of two providers:

- NameSilo
- Alibaba Cloud Computing Ltd. d/b/a HiChina (www[.]net[.]cn)

Active Servers and Observed Payloads

Many IPs and their associated domains have been flagged as malicious in VirusTotal, with several APKs identified as Joker malware. Given the ongoing activity, we focused on two servers whose certificates were still observed in Hunt's scans as of February 26, 2025.

Server 1: `8.222.246[.]250`

- Resolves to: `cgan[.]info`
- Likely Target: Camera app users
- APK Info:
  - Filename: `com.defabook.camera_1.5.apk`
  - SHA-256: `a5aa7e18aa8e0473d37661830eaf9ccd0401ee4c44de426e53e39fe47fa06ed4`

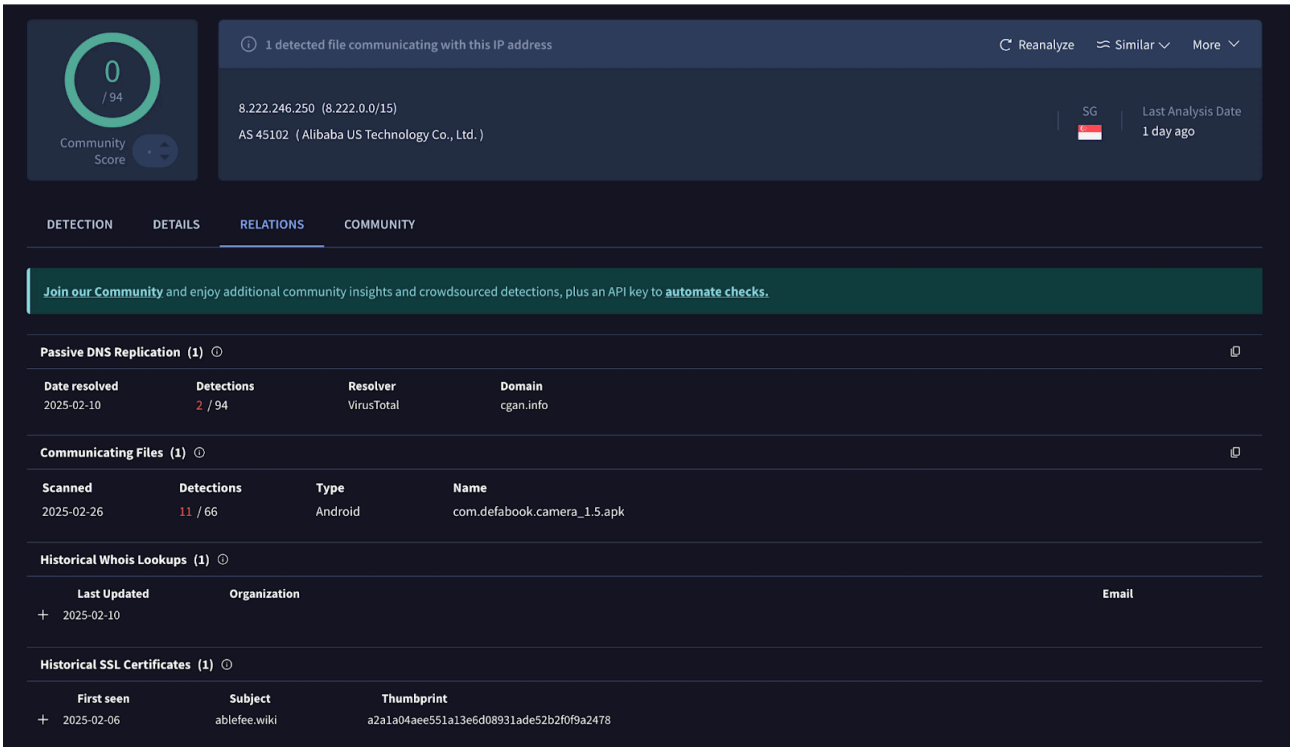

Figure 8: Screenshot of VirusTotal analysis of Joker payload and domain.

Server 2: `8.222.195[.]150`

- Resolves to: `kuen[.]work`
- Likely Target: Users tracking water consumption
- APK Info:
  - Filename: `Drinking Water_2.3.apk`

- SHA-256: `2c0845ff2ef220b6fcdd57c30471ee854bcd886b5c7d78c468bef47436197f36`

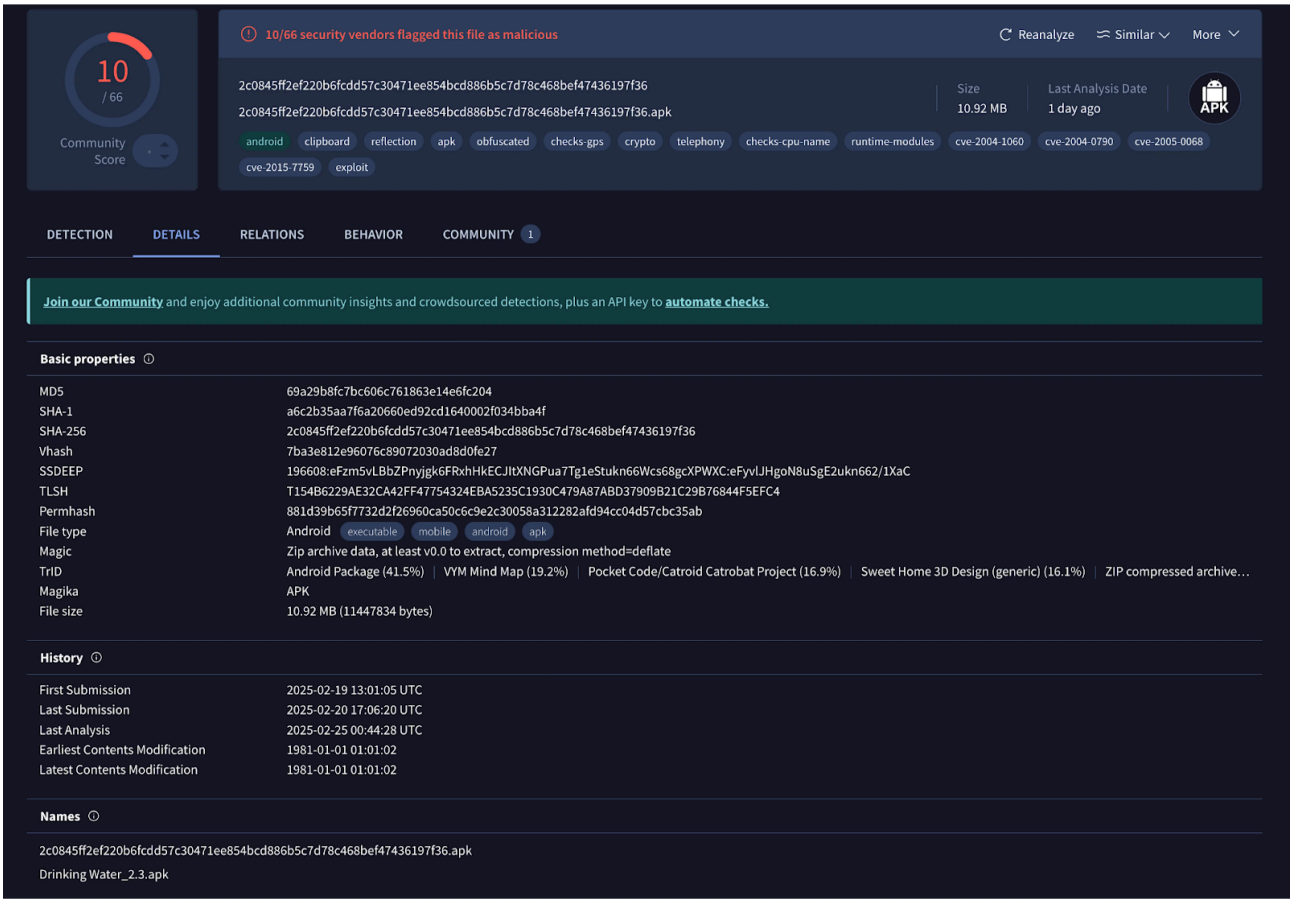

Figure 9: VirusTotal analysis of Joker detected APK.

Conclusion

Joker malware remains an active threat, relying on a few SSL certificates shared across multiple IP addresses to maintain its infrastructure. Our analysis led to 77 Joker-linked servers across the Alibaba network, highlighting the operator's preference for certificate reuse. This approach could suggest automation is used to streamline server setup, reducing the effort usually required to manage certificates across an extensive C2 network.

Certificate tracking is crucial for identifying adversary activity, offering defenders a way to uncover infrastructure connections that might otherwise go unnoticed. When combined, using Let's Encrypt certificates, Alibaba-hosted IPs, and unique TLDs creates a strong foundation for hunting this campaign, enabling proactive detection of related activity.

In addition to only downloading apps from official stores, users can reduce their risk of infection by reviewing app permissions, checking for inflated reviews, and conducting searches of web presence for apps with large download counts.

Joker Network Observables and Indicators of Compromise (IOCs)

IP Address	ASN	Domain(s)/Hostnames
47.236.49[.]195	Alibaba (US) Technology Co., Ltd.	gasu[.]pw hdphoto[.]uno
47.91.99[.]31	Alibaba (US) Technology Co., Ltd.	me-east-1.oss.aliyuncs.com
47.237.68[.]53	Alibaba (US) Technology Co., Ltd.	femk[.]top tuatol[.]store hdphoto[.]uno
47.236.99[.]235	Alibaba.com LLC	N/A
47.236.58[.]7	Alibaba.com LLC	lushere[.]host
8.219.135[.]184	Alibaba.com Singapore E-Commerce Private Limited	bsjk-jp.82021819[.]com paltric[.]xin
47.237.71[.]26	Alibaba.com LLC	ryowzs[.]fit hoful[.]homes
47.236.48[.]123	Alibaba.com LLC	soundbutton[.]art
47.236.232[.]241	Alibaba.com LLC	effeai[.]me
47.236.70[.]252	Alibaba.com LLC	colamati[.]fun
47.84.46[.]127	Alibaba.com LLC	atck[.]wang photy[.]top
47.236.60[.]207	Alibaba.com LLC	yamibox[.]store
47.236.89[.]240	Alibaba.com LLC	mablefam[.]art
47.236.66[.]130	Alibaba.com LLC	kxnwf[.]fun
47.236.254[.]202	Alibaba.com LLC	politan[.]site vokepru[.]art
47.236.64[.]124	Alibaba.com LLC	eureca[.]fit easdr[.]cyou
47.237.165[.]56	Alibaba.com LLC	umerz[.]info wetanra[.]fit
47.237.132[.]7	Alibaba.com LLC	N/A
47.236.56[.]63	Alibaba.com LLC	N/A

IP Address	ASN	Domain(s)/Hostnames
47.237.23[.]24	Alibaba.com LLC	goldseek[.]cc pnidh[.]fun monitor-hospot.rinjanihost[.]com
47.245.106[.]232	Alibaba.com LLC	amazingcam[.]xyz
47.245.112[.]50	Alibaba.com LLC	feltwod[.]fun
47.236.140[.]108	Alibaba.com LLC	cirlate[.]work
47.236.142[.]61	Alibaba.com LLC	graffity[.]fun shpum[.]work polar[.]info
47.84.42[.]161	Alibaba.com LLC	pallet[.]top rok[.]quest bhc[.]beauty neatsu[.]ink mukit[.]fun fusionworks[.]me
47.236.43[.]172	Alibaba.com LLC	wrenoby[.]work tokyojihen[.]store
47.236.43[.]141	Alibaba.com LLC	rocketbox[.]cc
47.236.86[.]187	Alibaba.com LLC	N/A
8.222.167[.]209	Alibaba.com Singapore E-Commerce Private Limited	ooouni[.]com goodivew[.]store
47.84.49[.]230	Alibaba.com LLC	pojys[.]vip artistchoice[.]fit
47.236.52[.]163	Alibaba.com LLC	gordid[.]work
47.236.132[.]59	Alibaba.com LLC	cetalpre[.]me
8.222.164[.]8	Alibaba.com Singapore E-Commerce Private Limited	colorfulmsg[.]store
8.219.0[.]154	Alibaba.com Singapore E-Commerce Private Limited	N/A
47.241.220[.]222	Alibaba (US) Technology Co., Ltd.	richus[.]top

IP Address	ASN	Domain(s)/Hostnames
8.222.232[.]224	Alibaba.com Singapore E-Commerce Private Limited	inspd[.]club
8.219.145[.]123	Alibaba.com Singapore E-Commerce Private Limited	micap[.]top
8.219.126[.]140	Alibaba.com Singapore E-Commerce Private Limited	oneyipose[.]vip enchan[.]cloud
47.236.31[.]185	Alibaba.com LLC	tamf[.]top youngerpiano[.]xyz
8.222.204[.]79	Alibaba.com Singapore E-Commerce Private Limited	nowaute[.]top
47.236.185[.]226	Alibaba.com LLC	ngxs[.]work petiver[.]art pranfun[.]cc diycont[.]art
8.222.176[.]193	Alibaba.com Singapore E-Commerce Private Limited	intoxit[.]club
8.222.227[.]247	Alibaba.com Singapore E-Commerce Private Limited	edcious[.]shop
8.219.132[.]122	Alibaba.com Singapore E-Commerce Private Limited	mannada[.]cc
8.219.116[.]53	Alibaba.com Singapore E-Commerce Private Limited	rumblesc[.]fun teyvata[.]com
47.236.241[.]158	Alibaba.com LLC	denlaje[.]art mer[.]college
47.84.37[.]53	Alibaba.com LLC	pugoy[.]vip
47.236.136[.]254	Alibaba.com LLC	panel[.]goepos[.]id wanis[.]cc mojifu3d[.]wiki
47.236.13[.]64	Alibaba.com LLC	photopal[.]art
47.245.126[.]152	Alibaba.com LLC	toniben[.]space
47.236.42[.]182	Alibaba.com LLC	ablefee[.]wiki

IP Address	ASN	Domain(s)/Hostnames
47.236.70[.]132	Alibaba.com LLC	qidakan[.]com tmvp[.]xin
47.245.123[.]233	Alibaba.com LLC	passroad[.]beauty timestampmark[.]me
47.236.50[.]129	Alibaba.com LLC	fartsounds[.]xyz
8.219.208[.]157	Alibaba.com Singapore E-Commerce Private Limited	gumblerumble[.]art vocall[.]club
8.222.237[.]93	Alibaba.com Singapore E-Commerce Private Limited	jueo[.]quest tomomsg[.]xyz
8.219.71[.]57	Alibaba.com Singapore E-Commerce Private Limited	helljni[.]com eqim[.]club
8.219.85[.]251	Alibaba.com Singapore E-Commerce Private Limited	N/A
8.222.161[.]7	Alibaba.com Singapore E-Commerce Private Limited	pianomaster[.]store
8.219.77[.]97	Alibaba.com Singapore E-Commerce Private Limited	jkicker[.]art
8.222.246[.]250	Alibaba.com Singapore E-Commerce Private Limited	cgan[.]info
8.219.221[.]185	Alibaba.com Singapore E-Commerce Private Limited	easytexting[.]art
8.222.203[.]59	Alibaba.com Singapore E-Commerce Private Limited	screenlocker[.]art
47.236.184[.]154	Alibaba.com LLC	rophatic[.]website jevq[.]art
47.236.48[.]202	Alibaba.com LLC	timeschord[.]co
47.237.106[.]43	Alibaba.com LLC	lads[.]cc
8.222.195[.]150	Alibaba.com Singapore E-Commerce Private Limited	kuen[.]work
47.237.14[.]161	Alibaba.com LLC	kefu[.]esgxiehui[.]com valenstickers[.]me

IP Address	ASN	Domain(s)/Hostnames
47.236.152[.]0	Alibaba.com LLC	qigu[.]black
47.237.14[.]179	Alibaba.com LLC	ytky[.]tech
47.84.44[.]76	Alibaba.com LLC	N/A
47.236.63[.]223	Alibaba.com LLC	N/A
47.237.68[.]12	Alibaba.com LLC	senspom[.]info
8.222.238[.]142	Alibaba.com Singapore E-Commerce Private Limited	kdo[.]monster
8.219.246[.]210	Alibaba.com Singapore E-Commerce Private Limited	likeand[.]cloud
8.219.124[.]253	Alibaba.com Singapore E-Commerce Private Limited	plusonepic[.]cloud
8.219.230[.]140	Alibaba.com Singapore E-Commerce Private Limited	securemsg[.]store
8.219.92[.]109	Alibaba.com Singapore E-Commerce Private Limited	gbclm[.]info
8.219.63[.]9	Alibaba.com Singapore E-Commerce Private Limited	ynur[.]online appapi[.]cepatcairc[.]cc

Joker Host Observables and Indicators of Compromise (IOCs)

Filename	SHA-256
com.hdphoto.wallpaper4k.apk	7f186746152d9569421a88e506c89844eaf0c2036ab5dbe0edb0775a79d9bb9d
dex1_v16.txt	2766ce69097ccb0cd9b4a7f3cf6eac19d76db2acf7d1b6844cc10d5460528138
encoded2.txt	4000d8110f92d5622a19a75d85c7af38fef810cecfe054e02779da9c1e218e5d
com.defabook.camera_1.5.apk	a5aa7e18aa8e0473d37661830eaf9ccd0401ee4c44de426e53e39fe47fa06ed4
Drinking Water_2.3.apk	2c0845ff2ef220b6fcdd57c30471ee854bcd886b5c7d78c468bef47436197f36
