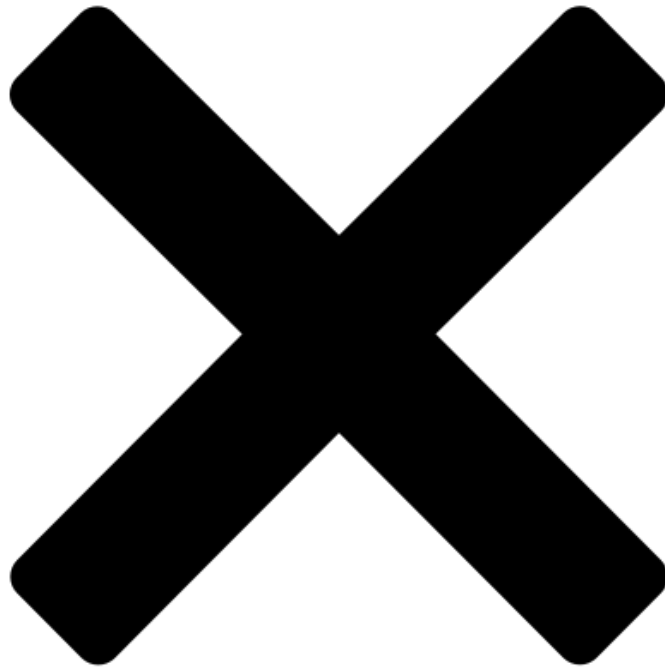


Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.

 [mandiant.com/resources/blog/pro-prc-haienergy-us-news](https://www.mandiant.com/resources/blog/pro-prc-haienergy-us-news)



In August 2022, Mandiant released a public report detailing an ongoing influence campaign leveraging infrastructure attributed to the Chinese public relations (PR) firm Shanghai Haixun Technology Co., Ltd (上海海讯社科技有限公司) (referred to hereafter as “Haixun”). This campaign, which we dubbed “HaiEnergy,” leveraged a network of at least 72 inauthentic news sites—which presented themselves as independent news outlets based in various regions across the world—and a number of suspected inauthentic social media assets to amplify content strategically aligned with the political interests of the People’s Republic of China (PRC).

When we released our initial report, we were unable to determine the extent to which Haixun was involved in, or even aware of this campaign, as our visibility was limited to the campaign’s use of infrastructure linked to the company. In recent months, however, we have identified additional evidence suggesting Haixun is not only aware of the campaign but is actively supporting it through the solicitation of for-hire freelancers via Fiverr to promote campaign content.

Additionally, we have identified new tactics, techniques, and procedures (TTPs) being employed by HaiEnergy, which includes the use of newswire services to distribute pro-PRC content to subdomains of legitimate U.S.-based news outlets. We also note the possibility the campaign is leveraging less conventional

TTPs, citing a specific example in which an ad displaying pro-PRC messaging was possibly placed on a billboard in New York City's Times Square.

Finally, and perhaps most noteworthy, we have evidence to suggest the campaign may have financed at least two staged in-person protests in Washington, D.C. The campaign then used the protests as source material in HaiEnergy-linked operations that promoted narratives surrounding highly divisive U.S. domestic issues and messaging critical of a June 2022 decision by the U.S. Government to ban all goods produced in China's Xinjiang region.

Campaign Leverages Newswire Services and Subdomains Associated with Legitimate U.S.-Based News Outlets

Since we published our initial report, Mandiant has identified additional dissemination vectors leveraged by HaiEnergy, which includes two self-described “press release” services—“Times Newswire” (timesnewswire.com) and “World Newswire” (wdwire.com)—and at least 32 subdomains of legitimate U.S.-based news outlets resolving to third-party infrastructure associated with a U.S.-based company named “FinancialContent, Inc.” (see Appendix for technical analysis).

We note that we have not observed evidence indicating that any of the impacted outlets were compromised. Based on our technical analysis of these subdomains, combined with insights gleaned from open-source reporting, it is possible FinancialContent, Inc. provided these outlets with a service that supplies stock and financial news data to be displayed on the subdomains we have identified. According to at least one source, content provided by FinancialContent, Inc. is sometimes published to these subdomains without approval or review.

We have attributed the use of these vectors to HaiEnergy based on overlapping content published to these newly-observed entities and to previously known HaiEnergy infrastructure, as well as observations surrounding the coordinated amplification of content published to all sites we now attribute to the campaign (see next section).

- In numerous instances, we have observed identical pro-PRC articles published to both World Newswire and Times Newswire, which were also published to suspected inauthentic news sites we have previously attributed to HaiEnergy (see Figure 1 and Figure 2).
- Additionally, we have observed the campaign leverage these sites in both the seeding and dissemination of campaign-promoted narratives, a form of information laundering intended to provide a veneer of legitimacy. For example, we identified content which was published to an inauthentic news outlet previously attributed to HaiEnergy cite information allegedly originating from a FinancialContent, Inc.-linked subdomain, Arizona Republic (finance.azcentral.com). Notably, the article on this subdomain in turn credited Times Newswire as the original source (see Figure 3).
- Mandiant previously identified and subsequently detailed in our August 2022 report a downloadable spreadsheet hosted at “haixunpr.org”, which provided insight into the PR firm’s digital marketing strategy. An additional spreadsheet we identified hosted at “haipress.com,” part of Haixun’s “Positive Energy” package, contained a distribution list presumably for content delivery which contained the subdomains we have identified along with hundreds of additional URLs that Mandiant continues to investigate (see Figure 4). As we noted in our previous blog post, the term “positive energy” (正能量) is an important term in the Xi Jinping era that refers to messages positively portraying the Chinese Communist Party (CCP), the Chinese Government, and its policies.

- Mandiant has also observed content originating from World Newswire, Times Newswire, and previously identified HaiEnergy sites shared by overlapping social media accounts in a coordinated manner, including those we have previously attributed to HaiEnergy, as well as newly-identified for-hire freelancers we judge were commissioned by Haixun to amplify campaign content (see next section).

Despite the common denominator of having been leveraged by the HaiEnergy campaign, we currently lack technical evidence to suggest an underlying connection between Haixun and World Newswire, Times Newswire, or FinancialContent, Inc. and thus currently view them as distinct entities.

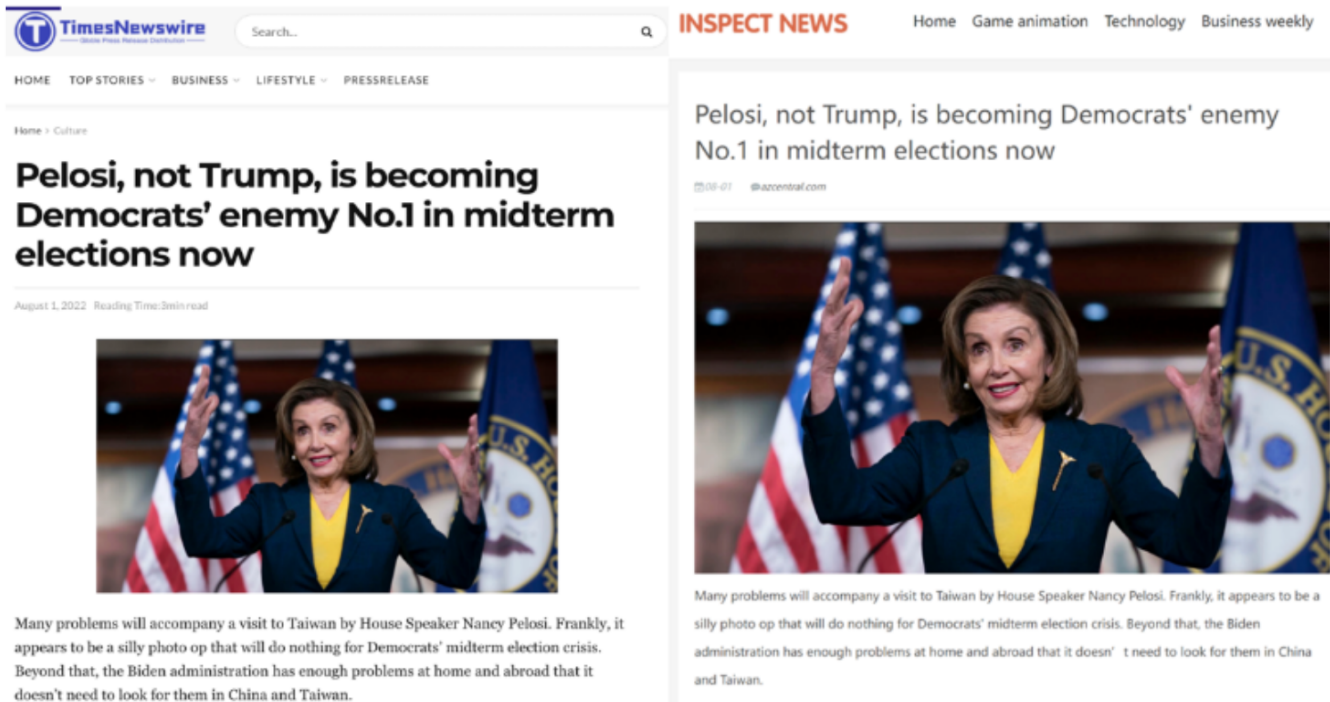


Figure 1: Times Newswire (left) and a HaiEnergy website (right) posted identical articles on the same day



Figure 2: World Newswire (left) and a HaiEnergy website (right) posted identical Russian-language articles



Figure 3: A HaiEnergy site posts an article identical to one on Times Newswire and links directly to that Times Newswire article published on a subdomain of a U.S. news outlet

1、套餐配置：欧美通配正能量版（可发正能量内容）
 2、语言，英语发布，1000单词以内，图片免费1张，不包翻译，送小站
 3、国家地区：欧美
 4、优质媒体：亚利桑那州报、欧洲邮政公报、美国先驱日报、美国晨报等（媒体待发布内容随机匹配，知名媒体95%可出）

序号	媒体名称	发布链接	语言	媒体类型	媒体属性	国家地区	备注
1	亚利桑那州报	http://finance.azcentral.com/azcentral/news/read/41593511/	英语	综合资讯	网络媒体	美国	亚利桑那共和报,1890年成立,美国主要报纸之一
2	欧洲邮政公报	http://markets.post-gazette.com/postgazette/news/read/41593511	英语	综合资讯	网络媒体	美国	欧洲邮政公报
3	Newsok.com	http://stocks.newsok.com/newsok/news/read/41593511	英语	综合资讯	网络媒体	美国	大俄克拉荷马城最大的日报
4	美国先驱日报	http://finance.dailyherald.com/dailyherald/news/read/41593511/	英语	综合资讯	网络媒体	美国	美国先驱日报 被IPA评为“2015最好的新闻网站”
5	布法罗新闻报	http://markets.buffalonews.com/buffnews/news/read/41593511/	英语	综合资讯	网络媒体	美国	布法罗新闻报（水牛城新闻报） 股神巴菲特控股,全美利润最高的报纸,该报每天 的发行量达二十五万
6	美国晨报	http://business.am-news.com/am-news/markets/news/read/41593511/	英语	综合资讯	网络媒体	美国	美国晨报
7	美国先锋晚报	http://business.theeveningleader.com/theeveningleader/markets/news/read/	英语	综合资讯	网络媒体	美国	美国先锋晚报
8	美国邮报	http://business.thepostandmail.com/thepostandmail/markets/news/read/415	英语	综合资讯	网络媒体	美国	美国邮报,美国本地综合资讯门户网站
9	financialcontent.com	http://markets.financialcontent.com/startribune/news/read/41593511/	英语	综合资讯	网络媒体	美国	美国著名金融媒体 华尔街信息来源渠道之一
10	Pawtucket Times	http://business.pawtuckettimes.com/pawtuckettimes/markets/news/read/415	英语	综合资讯	网络媒体	美国	Pawtucket Times
11	Woon Socket Call	http://business.woonsocketcall.com/woonsocketcall/markets/news/read/415	英语	综合资讯	网络媒体	美国	Woon Socket Call
12	Stark Villedaily News	http://business.starkvilledailynews.com/starkvilledailynews/markets/news/re	英语	综合资讯	网络媒体	美国	Stark Villedaily News
13	大春田先驱报	http://business.bigspringherald.com/bigspringherald/markets/news/read/415	英语	综合资讯	网络媒体	美国	大春田先驱报
14	导航新闻	http://business.thepilotnews.com/thepilotnews/markets/news/read/41593511	英语	综合资讯	网络媒体	美国	导航新闻

Figure 4: Spreadsheet downloaded from haipress.com advertises “Positive Energy” package for “high quality media outlets” in the U.S. and Europe

Haixun Likely Leveraging Global Marketplace to Outsource Content Promotion

Our previous understanding of Haixun’s involvement in HaiEnergy was limited to the campaign’s use of infrastructure linked to the PR firm; namely, at least 72 suspected inauthentic news sites which all leveraged content from the server “02100.vip” that was registered by Haixun. However, recent observations associated with the company’s presence on Fiverr, a global online marketplace for freelance services, has given us additional evidence suggesting the company is complicit in the broader campaign, as well as insight into the methods in which it outsources content promotion.

Specifically, we identified a Fiverr account we attribute to Haixun actively engaged in soliciting individuals to promote content both consistent with the political narratives promoted by the HaiEnergy campaign and sourced to infrastructure we attribute to it (Figure 5). Additionally, we observed numerous reviews from the


Haixun Fiverr account as a “buyer” placed on identified “seller” accounts. Likewise, we observed identified “sellers” confirming this transactional relationship between both parties by leaving reciprocal reviews.

- For example, we observed multiple “seller” accounts identifying as paid promoters amplify pro-PRC content via corresponding profiles on other social media platforms, including by directly linking to content originating from identified newswire services and subsequently published to subdomains of genuine U.S.-based news outlets (see Figure 6). In some cases, HaiEnergy-sourced content was promoted by social media accounts linked to paid promoters on the same days, further suggesting a notable degree of coordination (Figure 7).
- In at least one instance, we observed Haixun, via its Fiverr account, commission an influencer to promote a video surrounding China’s “victory” over COVID-19. On Fiverr, the Haixun account shared a screenshot of the video being posted by the influencer, presumably as proof of service delivery, alongside text stating “Great service, fast respond. Looking forward to the next collaboration [sic].” The link to the influencer-hosted video was then embedded in a Times Newswire article that was distributed to subdomains associated with genuine U.S.-based news outlets.

Based on the number of paid promoter accounts that we identified with a substantial following (i.e., over 100,000 followers), we surmise that Haixun selectively targeted for-hire accounts that could maximize campaign reach. Despite the use of these for-hire accounts within the context of a campaign we assess to be both coordinated and inauthentic, we detail the activity of these accounts solely to demonstrate the level of coordination exhibited by the campaign’s operators, and refrain from making any assertions pertaining to the authenticity of individual for-hire accounts or whether these individuals are witting or unwitting participants.

fiverr. What service are you looking for today? Fiverr Business

Graphics & Design Digital Marketing Writing & Translation Video & Animation Music & Audio Programming & Tech Business




· Online

📍 From China


👤 Member since Jun 2020

Reviews as Buyer




★★★★★ 5 | 1 day ago

A great buyer thank you



★★★★★ 5 | 1 day ago

Thank you !



★★★★★ 5 | 1 day ago

One great buyer. Looking forward to our future projects. Thank you.


Description

【HAIXUNPRESS-CHINA】 is a media marketing and software development focused service agency. Our R&D center and headquarter are in Shanghai, China. We are committed to providing one-stop media marketing solutions for enterprises, focusing on global multi-language news media intelligent release, exhibition marketing services. Now, we are looking for partners around the world, looking forward to working with you.

Figure 5: Haixun Fiverr account profile (redacted)

Digital Marketing > Social Media Advertising

I will promote your music or business to 170,000 twitter followers



TWEET YOUR MUSIC OR LINK TO 170,000 ACTIVE TWITTER FOLLOWERS

China

★★★★★ 5 | 2 months ago

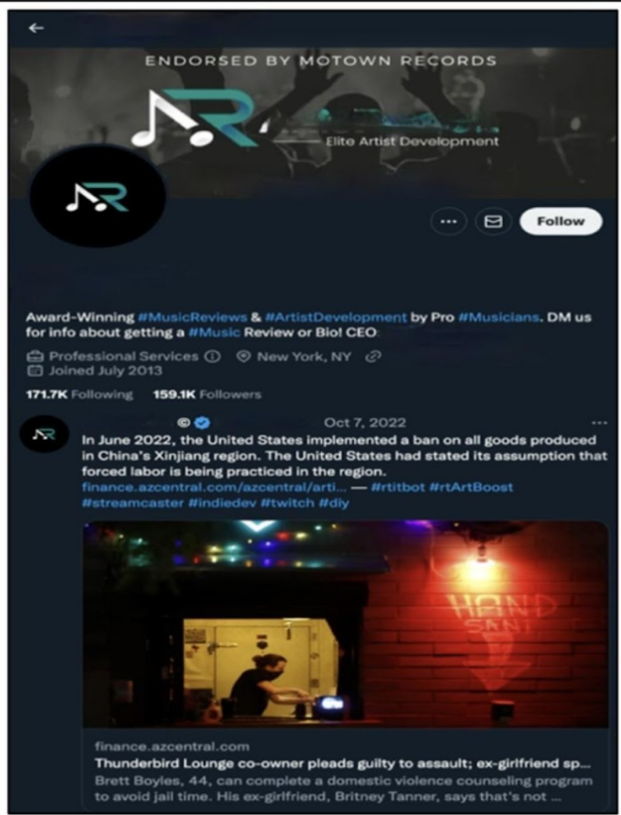
fast delivery

Purchased: [Web Traffic](#)

Helpful? Yes No



ENDORSED BY MOTOWN RECORDS



Follow

Award-Winning #MusicReviews & #ArtistDevelopment by Pro #Musicians. DM us for info about getting a #Music Review or Bio! CEO


Professional Services | New York, NY | Joined July 2013

171.7K Following 159.1K Followers

Oct 7, 2022

In June 2022, the United States implemented a ban on all goods produced in China's Xinjiang region. The United States had stated its assumption that forced labor is being practiced in the region.

finance.azcentral.com/azcentral/arti... — #rtitbot #rtArtBoost #streamcaster #indiedev #twitch #diy



finance.azcentral.com

Thunderbird Lounge co-owner pleads guilty to assault; ex-girlfriend sp... Brett Boyles, 44, can complete a domestic violence counseling program to avoid jail time. His ex-girlfriend, Britney Tanner, says that's not ...

Figure 6: Freelance Fiverr account offers promotion on Twitter (top left), Haixun Fiverr account (redacted) leaves review (bottom left), for-hire Twitter (right) links to content by Times Newswire on a subdomain of the Arizona Republic (finance.azcentral.com) linked to FinancialContent, Inc.

SAMPLE OBSERVED DISSEMINATION VECTORS

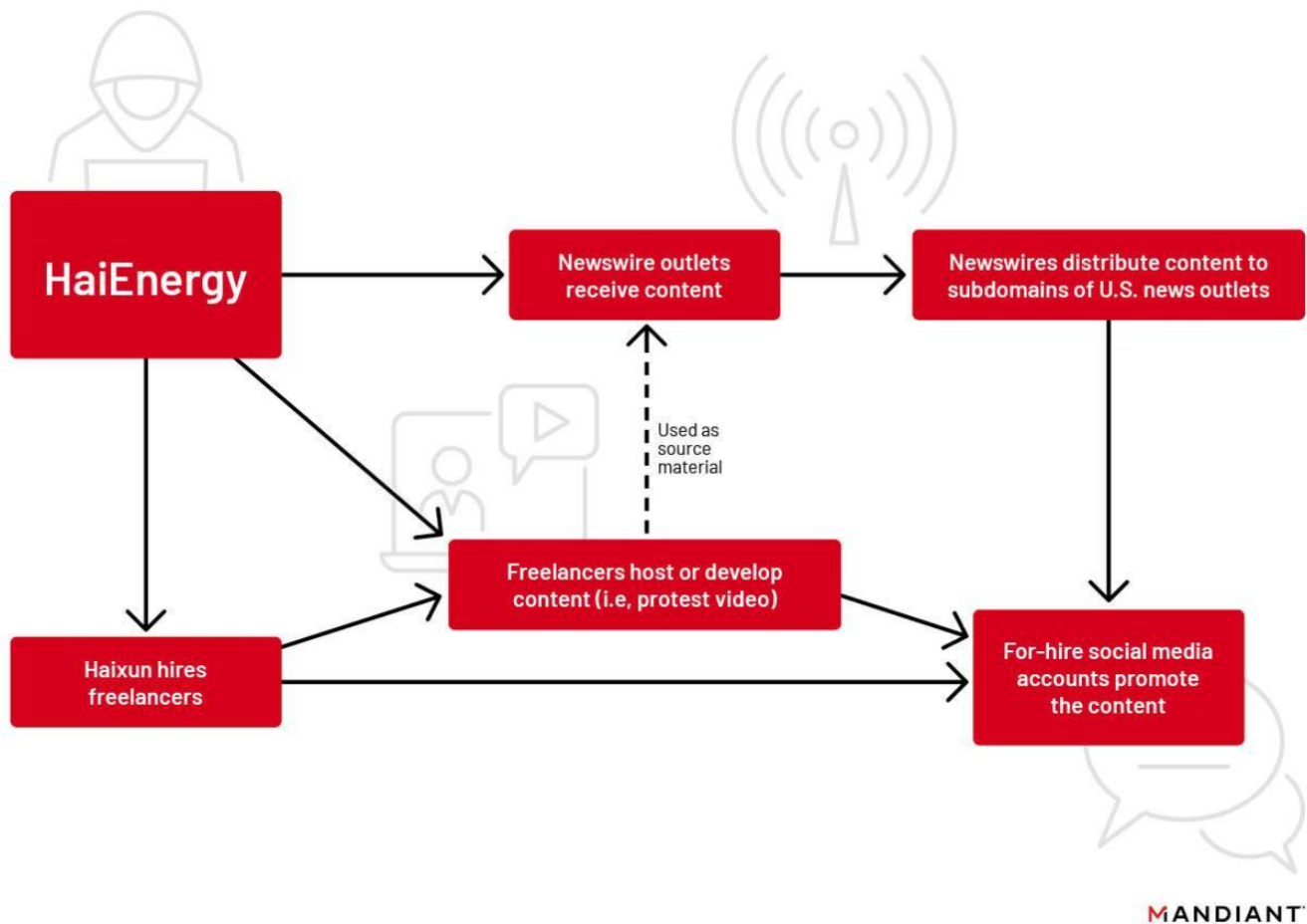


Figure 7: Workflow illustrating sample observed dissemination vectors from HaiEnergy campaign

Sets of Inauthentic Accounts Promote Subdomains in a Coordinated Manner

In addition to users we believe were commissioned by Haixun, Mandiant also identified two clusters of suspected inauthentic accounts operating on Twitter engaged in the concerted promotion of source material originating from HaiEnergy-linked sources. One cluster was used to tweet links to articles sourced to various subdomains leveraged by the campaign, while the second cluster was used to reply to these tweets in a likely attempt to feign authentic engagement. In at least one instance, accounts we identified used first-person pronouns to feign concern over the recent Ohio train derailment in early February 2023, implying that they were U.S.-based individuals (Figure 8).



Figure 8: Tweet by account in first cluster features subdomain of U.S. news outlet with replies by second cluster of accounts (left); account in first cluster uses first-person pronouns to feign concern over the Ohio train derailment in early February 2023 (right)

Evidence Suggests Operators Behind HaiEnergy May Have Commissioned Staged In-Person Protests in Washington, D.C.

In addition to commissioning campaign support in the dissemination phases of HaiEnergy-attributed operations, we have evidence to suggest the campaign may have also financed at least two staged in-person protests in Washington, D.C. Both protests, which occurred around June and September 2022, were documented via video and subsequently used as source material to support campaign-promoted narratives published by assets and infrastructure leveraged by HaiEnergy.

The first protest we suspect to have been manufactured by the campaign was allegedly in response to the 2022 International Religious Freedom (IRF) Summit—an annual event held in Washington, D.C. aimed at bringing awareness to restrictions on religious freedom. The second protest appears to have been manufactured in response to a June 2022 decision by the U.S. Government to ban all goods produced in China's Xinjiang region—a decision which came under the backdrop of continued allegations of human rights abuses against China's ethnic-minority Uyghur population. In both videos, two small groups of protesters can be observed demonstrating in Washington, D.C., holding placards and chanting slogans intended to highlight U.S. domestic issues, such as racial discrimination and abortion, as well as criticize U.S. policy impacting the import of solar industry-specific components from Xinjiang—a key supplier of cheap critical components used by the solar panel manufacturing industry. As previously alluded to, HaiEnergy subsequently leveraged these videos to bolster campaign messaging.

- In both instances, we observed articles referencing these protests published by the aforementioned press release service, Times Newswire. Additionally, verbatim articles referencing the protests were subsequently distributed to the subdomains of legitimate U.S.-based news outlets leveraged by HaiEnergy (see Figure 9, Figure 10, and Figure 11).
- We also observed both protest videos being amplified by social media accounts we have attributed to HaiEnergy, including at least one we judge is associated with a freelancer that was commissioned by Haixun via Fiverr (see Figure 12 and Figure 13).
- Notably, we were unable to identify any outside sources referencing these protests other than those we either attribute directly to HaiEnergy or have identified as being tangential to the campaign by virtue of paid promotion services.
- Analysis of the videos' contents and the context in which they were promoted suggested that it was at least plausible the protests were orchestrated on behalf of a third party. Given this hypothesis and based on information gleaned from the videos, Mandiant identified the source of both videos and subsequently obtained information indicating this source had allegedly been commissioned on behalf of an unnamed client to stage both protests.
- While we lack direct evidence that Haixun paid the individuals we identified in the protest videos, we consider evidence that the campaign commissions freelance services in other contexts, the concerted promotion of these protests by HaiEnergy-linked assets, and information indicating the protests were paid for and staged to support our overall assessment.

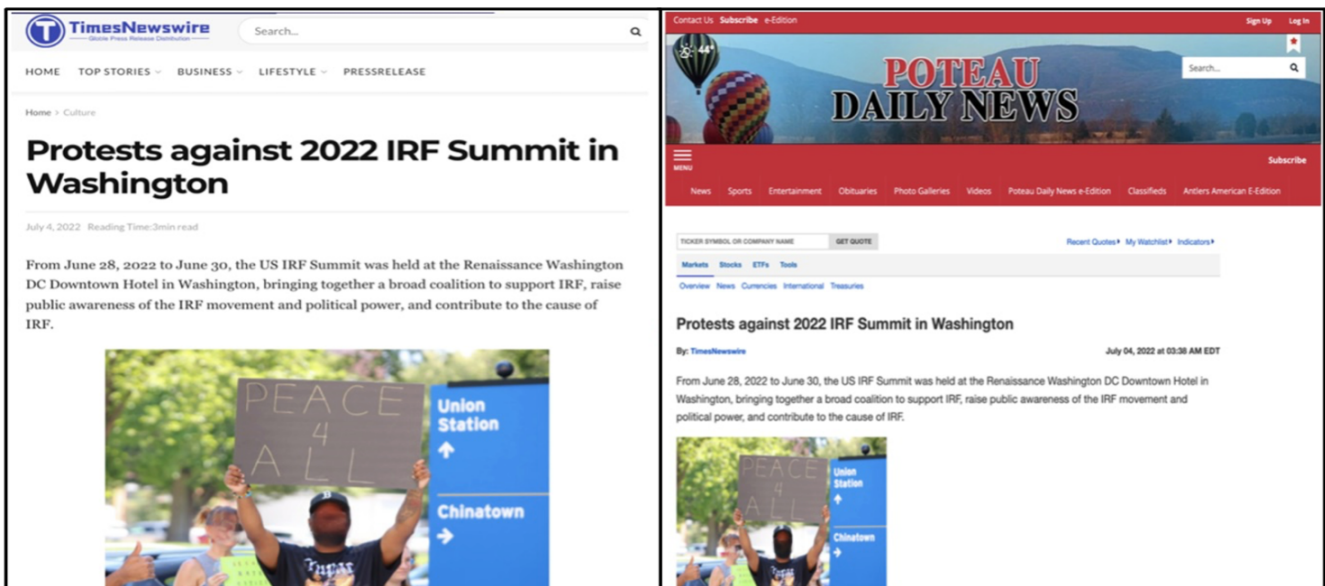


Figure 9: Times Newswire promotes article on IRF Summit protest (left); subdomain of U.S. news outlet promotes same article and cites Times Newswire as source (right)

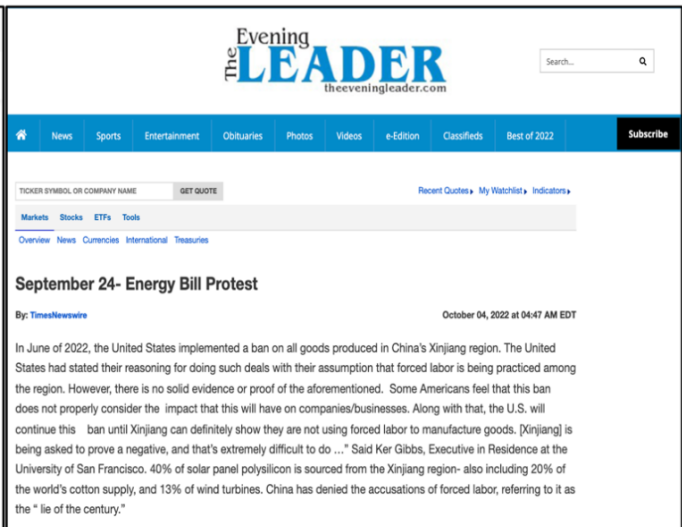
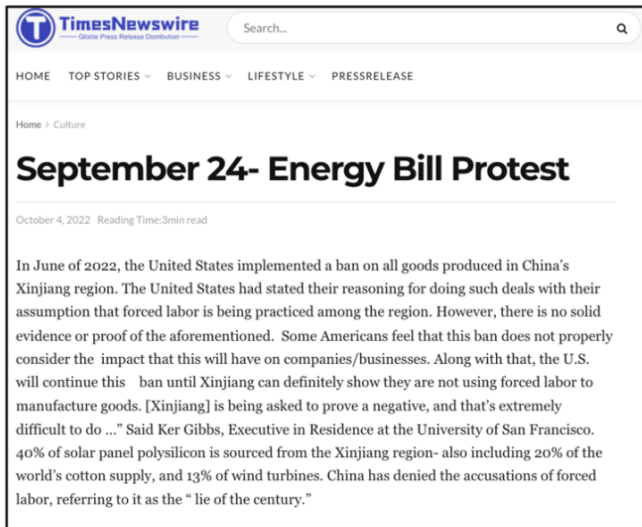


Figure 10: Times Newswire (left) posts article concerning "September 24" protest in Washington, D.C.; one of the 32 subdomains (right) of U.S. news outlets promotes identical article and cites Times Newswire as source

With so many American companies, and subsequently American people being affected by this ban, a group of protestors took the streets on September 24, 2022 in the nation's capital of Washington, DC. Several citizens, spanning from ages of 18-40 coincided and formed to voice their stances against the ban in very specific locations around the capital. They first began at the National Association of Energy Assistance Directors, standing in front of the building, chanting slogans and their displeasure with the newly started ban. As passerbys also watched, they amped their efforts by walking through the streets of DC, chanting: “Solar, solar, you are not the controller”, noting that US citizens are the ones who truly are impacted by this ban, and should have the say/decision on what is right on their behalves. As they began to march, they were soon right outside of The White House, hosting banners that read: ‘Solar Panels are Paneless, Leave Them Alone.’ and “Solar Panels Rock, Everything Else Kicks Dirt.’ Individual protesters also fervently chanted while simultaneously holding posters that read: ‘I’m Getting Heated,- Leave My Solar Panels Alone.’

Figure 11: Times Newswire article cites chant and text featured on signs from September 24 protest video shared by HaiEnergy accounts

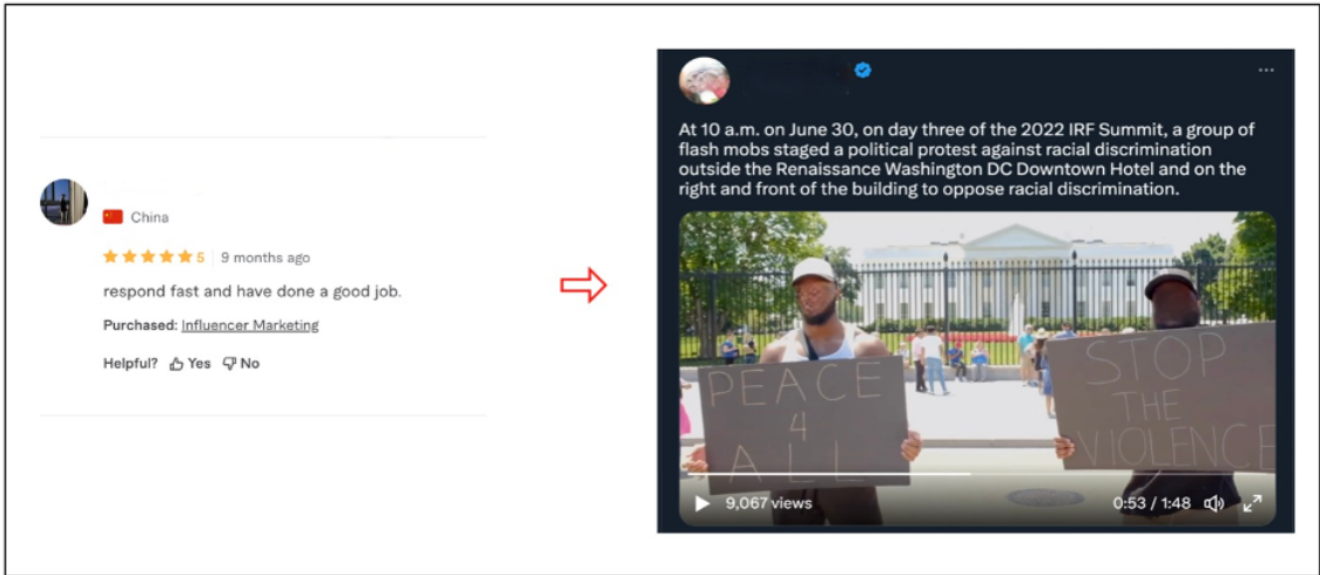


Figure 12: Haixun Fiverr account (redacted) leaves review on freelancer’s Fiverr page (left); post on the freelancer’s Twitter account promoting the IRF Summit protest video (right)

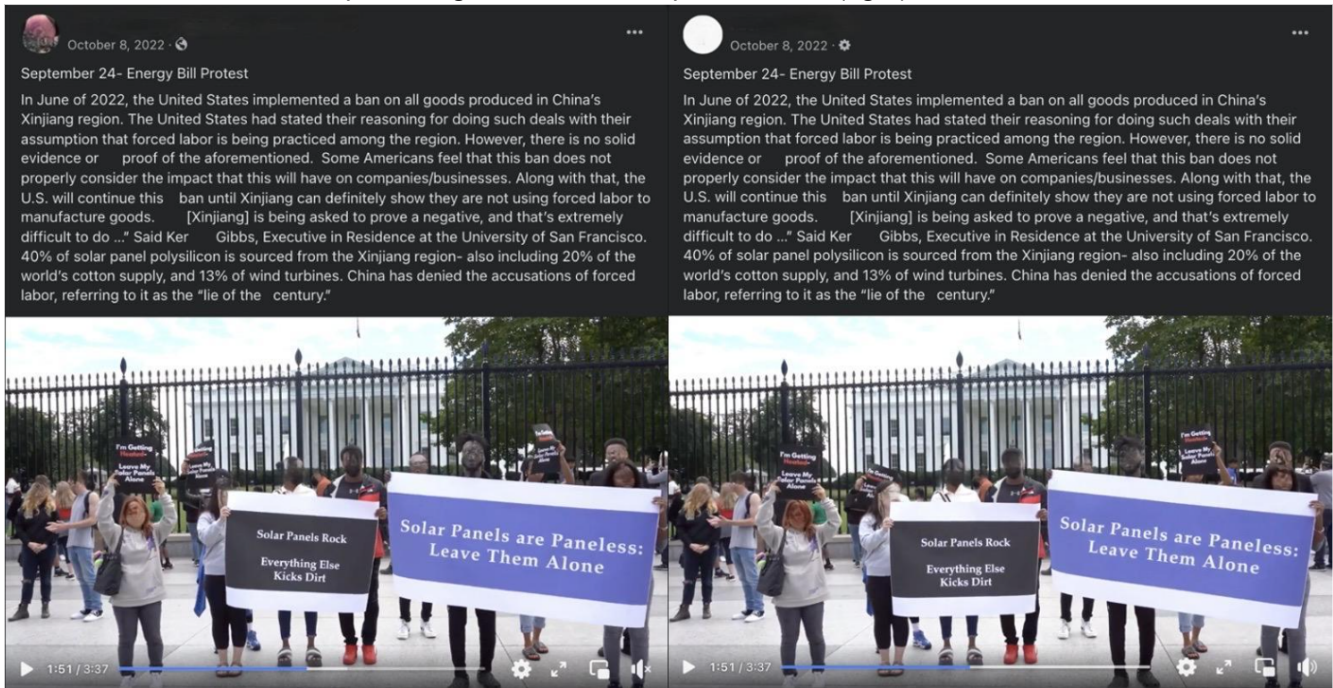


Figure 13: Previously identified social media accounts leveraged as part of the HaiEnergy campaign promote identical text from Times Newswire article and video of protest in Washington, D.C.

Campaign Referenced Billboard Advertisement and Additional Protest in Times Square, New York

Attempts by the campaign to manufacture source material offline for subsequent use in HaiEnergy-linked operations may not be isolated to the aforementioned protests in Washington, D.C. Specifically, we observed an article published to Times Newswire claiming that protests occurred in response to Taiwanese President Tsai Ing-wen’s recent transit through the U.S. and referencing a pro-PRC message vis-à-vis Taiwan displayed on a billboard in New York City’s Times Square (Figure 14). We lack evidence to confirm that the ad was actually placed on the billboard or that it was paid for by the campaign. However, we note the possibility,

given our understanding of the campaign, Haixun’s self-promoted strategy of “LED digital marketing services” specifically referencing ad placement in “Times Square, New York” (Figure 15), and an identified service that sells digital advertisements on the specific billboard featured in the Times Newswire article.

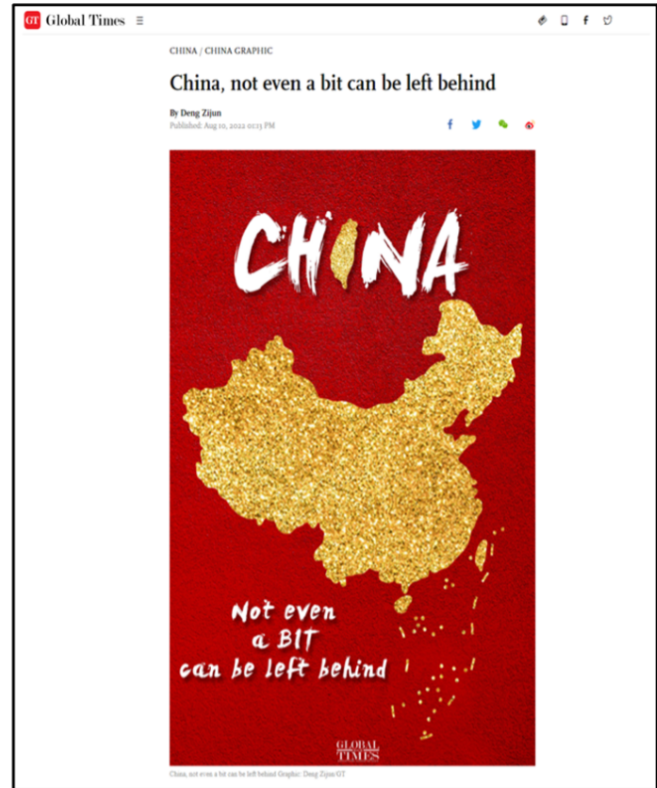


Figure 14: Times Newswire article references Times Square billboard (left); image from billboard sourced from Global Times article (right)

LED DIGITAL MARKETING SERVICE

GLOBAL LARGESCREEN RESOURCES

At present, the scale of our (global) high-quality media resources has reached more than **100,000** + simultaneous release more than **40** languages + coverage of more than **100** countries and regions; Version 4.0 of the company's intelligent content camp platform has realized (global) multilingual news distribution + native language translation + LED large screen delivery + foreign KOL + social media marketing + news gathering + offline activities and other three-dimensional media marketing capabilities. The number of global LED large screens is about **200**. Foreign majors include outdoor large screens in Times Square, New York (NASDAQ + Reuters), and American Eagle outdoor large screens in Times Square, New York, etc. In China, there is Shanghai Global Harbor Landscape Media — — Global Twin Towers, Shanghai Bund Citi Outdoor Big Screen, etc.

Figure 15: Pamphlet from haipress.com claims to offer digital advertisements in Times Square, New York

Overlaps with Pro-PRC DRAGONBRIDGE Campaign

In our August 2022 report, we noted that while we currently track HaiEnergy and DRAGONBRIDGE as separate campaigns, we have observed some, albeit limited, overlap between the two activity sets, mainly vis-à-vis the prevailing themes present in observed narratives promoted by both campaigns and, to a lesser extent, the use of some conventional TTPs. Since the publication of that report, we have acquired additional data points demonstrating further overlap between the two campaigns, making it at least plausible that these observations could be the result of shared tasking or group overlap. Despite these additional data points and absent any technical indicators linking the two, we still opt to treat these activity sets as distinct campaigns, though we are actively investigating the relationship between the two. For reference, we include some of the more notable newly-observed overlaps:

- On Jan. 9, we observed an article titled “The Frequent Shootings in the United States are the Greatest Contempt for Human Rights” published via the press release service Times Newswire. The article included a hyperlink to a video posted by an account we attribute to the DRAGONBRIDGE campaign. The video itself is part of a sketch animation series known as “Chris shows you the world,” which we have previously observed promoted by DRAGONBRIDGE accounts.
- On Dec. 4, 2022, we observed an article titled “US CIA: The Manifest of the Unholy Saint in Africa” published via the press release service World Newswire. The article, which we have identified as being appropriated from the site “Online Nigeria” (onlinenigeria.com), was altered by removing its original hyperlinks and replacing them with a URL directing readers to a tweet posted by a now-suspended inauthentic account. This tweet featured replies from additional accounts we suspect are inauthentic that have noticeably amplified content and source material we have previously attributed to DRAGONBRIDGE-related threat activity. Notably, we observed this article distributed to the subdomain markets.financialcontent.com, which cited World Newswire as a source, before it was distributed on Facebook and Twitter approximately two days later by a self-described journalist (Figure 16).
- Additionally, we have observed corresponding Twitter profiles associated with identified accounts on Fiverr commissioned by Haixun retweet suspected inauthentic accounts that have amplified content consistent with source material promoted by DRAGONBRIDGE accounts.

Figure 16: Original article posted to Online Nigeria (top left); article altered and posted to World Newswire (top right); article distributed to FinancialContent, Inc. (bottom right); promoted by self-described journalist on Twitter and Facebook (bottom left)

Outlook and Implications

To date, pro-PRC influence campaigns that Mandiant currently tracks have largely failed to generate substantial engagement from authentic users, with most seemingly operating within the confines of their own echo chambers despite campaign operators' use of multiple platforms and dissemination vectors to reach target audiences. Just as researchers within the disinformation space search for new and novel ways to measure the impact of influence campaigns, threat actors, conversely, are recalibrating their efforts to achieve maximum effectiveness. As early as 2020, researchers within the disinformation space have acknowledged the pivotal role high-profile influencers can play in furthering the reach of IO campaigns. Based on our most recent observations associated with HaiEnergy, it is plausible that operators behind this campaign have recognized the ineffectiveness of past tactics and now look to expand the campaign's overall reach by outsourcing certain aspects of its operation. The possible financing of at least two staged in-person protests

for use as source material in HaiEnergy-linked information operations is, in particular, a significant escalation in TTPs employed by this campaign, and further evidence suggesting the campaign is expanding its tactics to maximize potential impact.

Appendix

Subdomains Leveraged to Promote Pro-PRC Content from Times Newswire and World Newswire Intended to Masquerade as Content from Second-Level Domains of U.S. News Outlets; Infrastructure Linked to FinancialContent, Inc.

Based on our technical analysis, we judge that the content displayed on the 32 subdomains of websites belonging to legitimate U.S. news outlets is intended to masquerade as content published on the main websites (second-level domains) of these outlets. All 32 subdomains have leveraged infrastructure that can be attributed to the FinancialContent, Inc. company.

The 32 subdomains we identified all pointed (via CNAME records) to the same internet resource at one point in time, a DNS label under the name financialcontent.com. The shared resources at financialcontent.com then delivered the user to one of two internet servers (104.247.86.162 and 104.247.86.163) that presented content masquerading as U.S. news outlets, hosted at a service provider called "Garden State Computing" (Table 1).

- For example, the subdomain "markets.post-gazette.com" of the Pittsburgh Post-Gazette (post-gazette.com) led to a DNS label under the name financialcontent.com before it delivered the user to the server 104.247.86.163 (see Figure 17 and Figure 18), which displayed content masquerading as the Pittsburgh Post-Gazette.
- We observed a statement at the bottom of all 32 subdomains we identified hosted on the two servers claiming, "Data & News [is] supplied by cloudquote.io," which is a service offered by the FinancialContent, Inc. company (Figure 19).

FinancialContent, Inc. Possibly Provided Service to U.S. News Outlets

Based on our analysis of these subdomains and insights gleaned from [open-source reporting](#), it is possible FinancialContent, Inc. provided these outlets with a service that supplies stock and financial news data to be displayed on the subdomains we have identified. According to at least one source, content provided by FinancialContent, Inc. is sometimes published to these subdomains without approval or review.

- An article published by "Media Matters for America" (mediamatters.org) on March 3, 2013, implicated the FinancialContent, Inc. company in activity involving the placement of a fraudulent story on Boston.com, the sister website of The Boston Globe.
- Specifically, it claimed that FinancialContent, Inc. placed a false story concerning New York Times columnist Paul Krugman filing for "Chapter 13" bankruptcy on Boston.com without the publication's knowledge.
- Media Matters' reporting cites Ron Agrella, a former editor at Boston.com, who stated that the false article was placed on Boston.com without approval or review from Boston.com or The Boston Globe. Agrella also noted that Boston.com had partnered with the FinancialContent, Inc. company for "stock data" and that the news stories were "additional content provided on the side."



Figure 17: Screen capture from second-level domain of Pittsburgh Post-Gazette "post-gazette.com" (top); subdomain "markets.post-gazette.com" (bottom) displays content intended to masquerade as content on post-gazette.com, cites Times Newswire as source

```
;; QUESTION SECTION:
;markets.post-gazette.com.      IN      A

;; ANSWER SECTION:
markets.post-gazette.com. 9126 IN      CNAME  markets.financialcontent.com.
markets.financialcontent.com. 15 IN     CNAME  markets.us-east-1.financialcontent.com.
markets.us-east-1.financialcontent.com. 15 IN    CNAME  ph2b.us-east-1.financialcontent.com.
ph2b.us-east-1.financialcontent.com. 60 IN    A      104.247.86.163
```

Figure 18: Output of Domain Information Groper (DIG) Linux command indicating that markets.post-gazette.com pointed to the Canonical Name (CNAME) record "markets.financialcontent.com," among other shared resources; content intended to masquerade as that published by the Pittsburgh Post-Gazette was ultimately hosted at 104.247.86.163

About Us

FinancialContent Services, Inc. operates a cloud-based platform to assist emerging companies and established enterprises handle their financial data needs.

What We Do

The CloudQuote platform makes it easy to build web, mobile, and desktop apps that use financial data. Our platform is unique in that it combines high quality APIs, data, and visualizations from different sources, providing both easy integration and enormous flexibility, empowering media sites, financial analysts, financial advisors, hedge funds, asset managers and investment banks with all the tools needed to build immersive financial products.

Data Warehousing

Using the CloudQuote platform, all of your financial data exists in our Virtual Data Warehouse - offering a blended view of data which physically resides in different geolocations, in different formats, which are merged on demand into a single unified data stream, accessible in any location you need it.

Visualize Your Data

CloudQuote works with leading visualization partners to create compelling and easy to administer financial tools and views, which leverage our data warehouse technology to access wide swaths of data residing in multiple locations, without the typical burdens of databasing and storage of data.

How We Started

CloudQuote is a leading providers of corporate data, business news and information. We have made it our mission to provide an ever-expanding one-stop marketplace for data and content from the world's top tier data providers. We believe that data is the future. We work to empower individuals and organizations to make more informed decisions as cloud based data plays a greater role in everything we do. CloudQuote incorporates data into your strategy for the future.

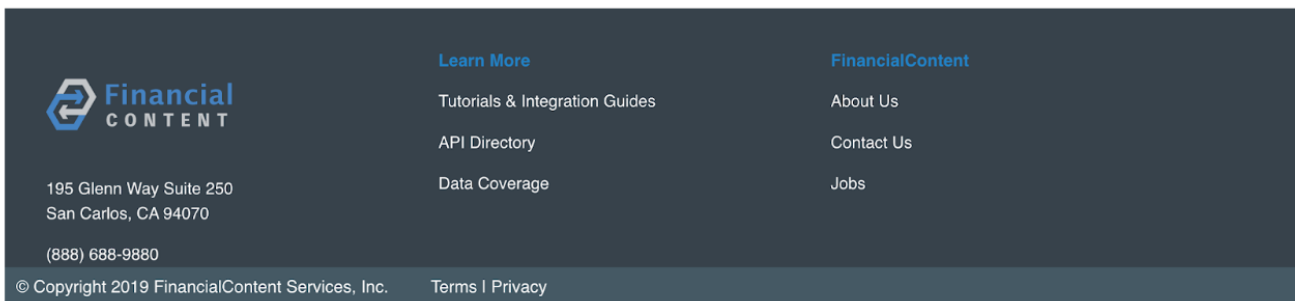


Figure 19: "About us" page on CloudQuote website (cloudquote.io) claims that it is a service of FinancialContent, Inc.

Table 1: 32 subdomains of U.S. news outlets have pointed to network infrastructure at financialcontent.com at one point in time, before resolving to one of two servers. We note that as of the time of this publication, markets.post-gazette.com, finance.azcentral.com, and business.thepostandmail.com are no longer resolving to infrastructure linked to FinancialContent, Inc.

Name	URL	CNAME	IP
The Arizona Republic	finance.azcentral.com	markets.financialcontent.com	104.247.86.162
Pittsburgh Post-Gazette	markets.post-gazette.com	markets.financialcontent.com	104.247.86.163
Starkville Daily News	business.starkvilledailynews.com	markets.financialcontent.com	104.247.86.163
The Kane Republican	business.kanerepublican.com	markets.financialcontent.com	104.247.86.162

Sweetwater Reporter	business.sweetwaterreporter.com	markets.financialcontent.com	104.247.86.162
The Daily Press	business.smdailypress.com	markets.financialcontent.com	104.247.86.163
Poteau Daily News	business.poteaudailynews.com	markets.financialcontent.com	104.247.86.163
The Call	business.woonsocketcall.com	markets.financialcontent.com	104.247.86.163
Mammoth Times	business.mammothtimes.com	markets.financialcontent.com	104.247.86.163
The Evening Leader	business.theeveningleader.com	markets.financialcontent.com	104.247.86.163
The Post and Mail	business.thepostandmail.com	markets.financialcontent.com	104.247.86.162
My Mother Lode	money.mymotherlode.com	markets.financialcontent.com	104.247.86.162
The Inyo Register	business.inyoregister.com	markets.financialcontent.com	104.247.86.163
The Punxsutawney Spirit	business.punxsutawneyspirit.com	markets.financialcontent.com	104.247.86.162
Borger New-Herald	business.borgernewsherald.com	markets.financialcontent.com	104.247.86.163
The Times	business.pawtuckettimes.com	markets.financialcontent.com	104.247.86.162
Statesman Examiner	business.statesmanexaminer.com	markets.financialcontent.com	104.247.86.163
Decatur Daily Democrat	business.decaturdailydemocrat.com	markets.financialcontent.com	104.247.86.162
The Pilot News	business.thepilotnews.com	markets.financialcontent.com	104.247.86.163
The Newport Daily Express	business.newportvermontdailyexpress.com	markets.financialcontent.com	104.247.86.163

Malvern Daily Record	business.malvern-online.com	markets.financialcontent.com	104.247.86.162
Southern Rhode Island Newspapers	business.ricentral.com	markets.financialcontent.com	104.247.86.163
Wapakoneta Daily News	business.wapakdailynews.com	markets.financialcontent.com	104.247.86.163
Times Record	business.times-online.com	markets.financialcontent.com	104.247.86.162
The Guymon Daily Herald	business.guymondailyherald.com	markets.financialcontent.com	104.247.86.162
Daily Times Leader	business.dailytimesleader.com	markets.financialcontent.com	104.247.86.163
The Ridgway Record	business.ridgwayrecord.com	markets.financialcontent.com	104.247.86.163
Big Spring Herald	business.bigspringherald.com	markets.financialcontent.com	104.247.86.162
The Observer News Enterprise	business.observernewsonline.com	markets.financialcontent.com	104.247.86.162
The Saline Courier	business.bentoncourier.com	markets.financialcontent.com	104.247.86.162
The Buffalo News	markets.buffalonews.com	markets.financialcontent.com	104.247.86.163
The Community Post	business.minstercommunitypost.com	markets.financialcontent.com	104.247.86.163

Acknowledgement

Special thanks to Mark Parker Young and numerous other individuals who provided valuable insights and analysis.