MAY 2023

DETAILED REPORT

Quarterly Adversarial Threat Report

Meta

TABLE OF CONTENTS

PURPOSE OF THIS REPORT

Our public threat reporting began about six years ago when we first shared our findings about coordinated inauthentic behavior (CIB) by a Russian influence operation. Since then, we have expanded our ability to respond to a wider range of adversarial behaviors as global threats have continued to evolve. To provide a more comprehensive view into the risks we tackle, we've also expanded our regular threat reports to include cyber espionage and other emerging threats — all in one place, as part of the quarterly reporting series. In addition to sharing our analysis and threat research, we're also publishing threat indicators to contribute to the efforts by the security community to detect and counter malicious activity elsewhere on the internet (See Appendix).

We expect the make-up of these reports to continue to evolve in response to the changes we see in the threat environment and as we expand to cover new areas of our Trust & Safety work. This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform our community's understanding of the evolving security threats we see. We welcome ideas from our peers across the defender community to help make these reports more informative, and we'll adjust as we learn from feedback.

For a quantitative view into our Community Standards' enforcement, including content-based actions we've taken at scale and our broader integrity work, please visit Meta's Transparency Center here: https://transparency.fb.com/data/.

SUMMARY OF OUR FINDINGS

- Our quarterly threat report provides a view into the risks we see across multiple adversarial behaviors including CIB and cyber espionage.
- **We took action against three cyber espionage operations in South Asia**. One was linked to a group of hackers known in the security industry as Bahamut APT (advanced persistent threat), the other to the group known as Patchwork APT and one to the state-linked actors in Pakistan. Here is what stood out from our threat research (See *Section 1* for details):
    - **Diversifying social engineering efforts:** These APTs relied heavily on social engineering and invested in making some of their fake accounts into more varied and elaborate fictitious personas with backstops across the internet so they can withstand scrutiny by their targets, platforms and researchers. While we saw them continue using traditional lures like women looking for a romantic connection, they also developed personas posing as recruiters, journalists or military personnel.
    - **Continued reliance on low-sophistication malware:** This investment in social engineering to trick people into clicking on malicious links or sharing sensitive information means that threat actors did not have to invest as much on the malware side. In fact, our investigations showed that cheaper, low-sophistication malware can be effective in targeting people when used together with social engineering. For at least two of these operations, we observed a reduction in the malicious capabilities in their apps, likely to ensure they can be published in official app stores.
    - **Impact of public disruptions and threat reporting:** As the security community continued to disrupt these APTs, they have been forced to set up new infrastructure, change tactics, and invest more in hiding and diversifying their operations in order to persist, which likely degraded their operations.
- In our Q1 Adversarial Threat report, we're sharing findings about **six separate covert influence operations** we took down for violating our policy against CIB. They originated in the United States and Venezuela, Iran, China, Georgia, Burkina Faso and Togo. More than half of them targeted audiences outside of their countries. We removed the majority of these networks before they were able to build authentic audiences. Here is what stood out from our CIB threat research (See *Section 2* for details)**:**

- **Creating fictitious entities across the internet**: In an attempt to build credibility, nearly all of these operations invested in creating fictitious entities across the internet, including news media organizations, hacktivist groups, and NGOs. They operated on many platforms, including on Facebook, Twitter, Telegram, YouTube, Medium, TikTok, Blogspot, Reddit, Wordpress, freelancer[.]com, hacking forums and their own websites.

- **Fake hacktivists from Iran**: The operation from Iran posted claims of having hacked organizations in Israel, Bahrain and France, including news media, logistics and transport companies, educational institutions, an airport, a dating service and a government institution. Some of these individual claims have been reported by the press in these countries, but we cannot confirm if any of them are credible. This is not the first time an Iran-origin operation claimed to have hacked government systems; a similar claim was promoted by another CIB network we removed ahead of the US 2020 election.

- **For-hire operations:** As we called out in our past reporting, we continue to see for-hire organizations behind covert influence operations globally, with half of the operations in this report attributed to private entities. This included an IT company in China, a marketing firm in the United States and a political marketing consultancy in the Central African Republic.

- **The evolution of China-origin operations:** Finally, this report brings the total of the China-origin CIB networks we removed since 2017 to six, with half of them reported in the last seven months. These latest takedowns signal a shift in the nature of the China-based CIB activity we've found with new threat actors, novel geographic targeting, and new adversarial tactics. Yet, we continue to find and remove them before they are able to build their audience. These latest networks experimented with a range of tactics we haven't seen in China-based operations before (though we've observed them elsewhere over the years, including in operations linked to troll farms, and marketing and PR firms). The latest behaviors included creating a front media company in the West, hiring freelance writers around the world, offering to recruit protesters, and co-opting an NGO in Africa.

01

Removing three cyber espionage networks from South Asia

Cyber espionage actors typically target people across the internet to collect intelligence, manipulate them into revealing information and compromise their devices and accounts.

As part of these latest disruptions against three networks, we took down accounts, blocked their domain infrastructure from being shared on our services and notified people who we believe were targeted by these malicious groups to help protect their accounts and encourage them to be cautious when interacting with people they don't know online. We also shared information with security researchers and our industry peers so they too can take action to stop this activity. We have included threat indicators, including malware hashes and command and control infrastructure, in the Appendix to this report, to enable further research and detection by the security community.

This report describes our threat research findings into the three cyber espionage networks we took down in South Asia — all long-running advanced persistent threat groups targeting people across the internet. It includes: a group known as a prolific user of the malware family GravityRAT that we attributed to state-linked actors in Pakistan, a threat actor in India known in the security industry as Patchwork APT, and the threat group known as Bahamut APT operating out of South Asia.

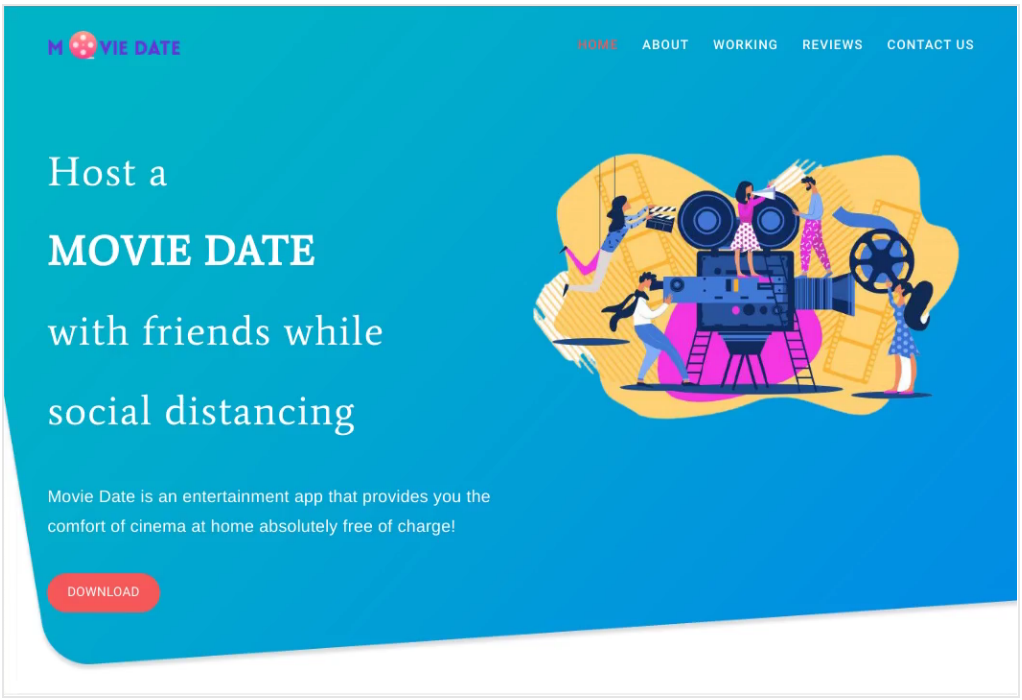
Pakistan-based APT

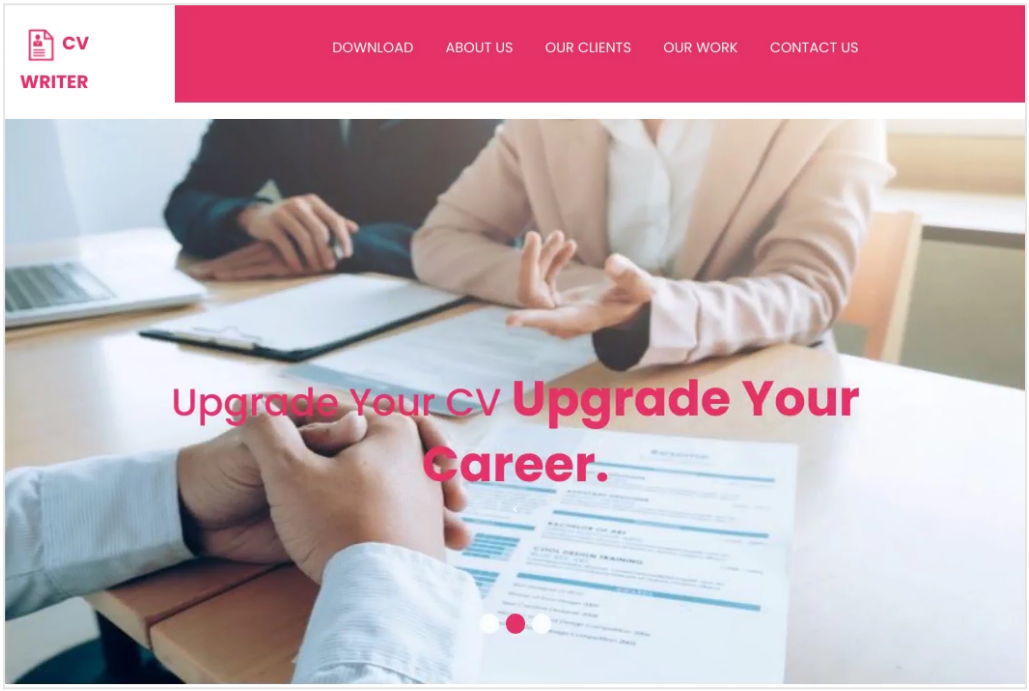
We took action against about 120 accounts on Facebook and Instagram linked to a hacking group in Pakistan that predominantly targeted people in India and Pakistan, including military personnel in India and among the Pakistan Air Force. Our investigation connected it to state-linked actors in Pakistan.

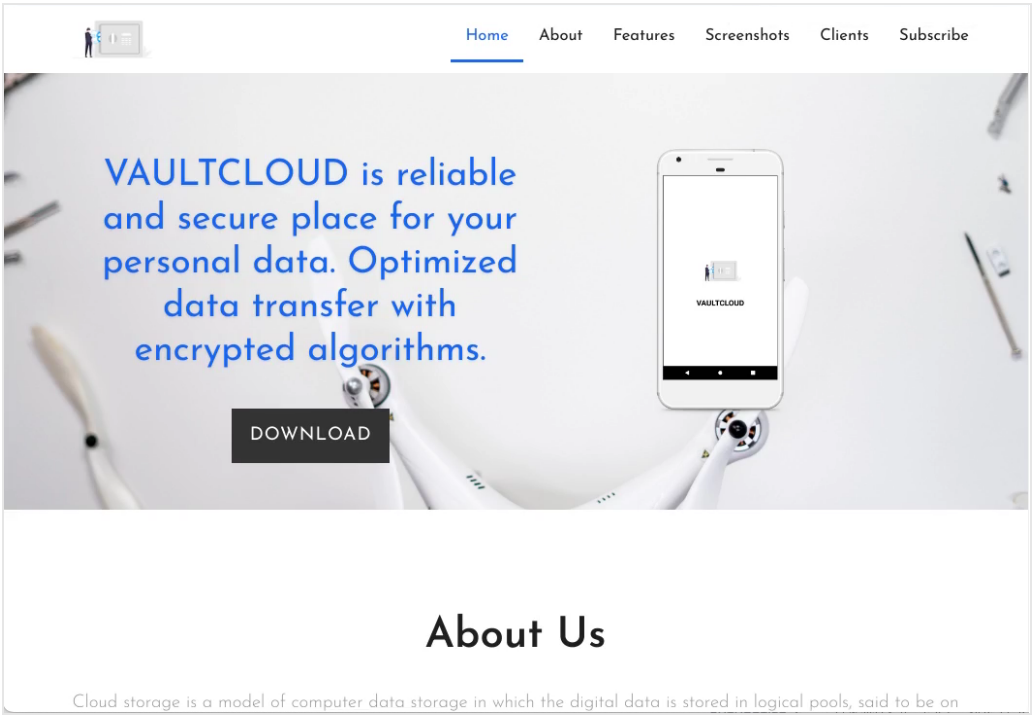
While this group's activity was relatively low in sophistication, it was persistent and targeted many services across the internet. They relied heavily on a web of attacker-controlled websites to distribute malware through highly targeted campaigns aimed to trick targets into clicking on malicious links and downloading Android or Windows malware.

We identified the following new and noteworthy tactics, techniques and procedures (TTPs) used by this threat actor across the internet:

- **Social engineering and fake personas:** This group used fictitious personas — posing as recruiters for both legitimate and fake defense companies and governments, military personnel, journalists and women looking to make a romantic connection — in an attempt to build trust with the people they targeted.
- **Fake apps and websites delivering malware:** This group deployed a wide range of tactics, including the use of custom applications and infrastructure, to host and deliver their malware. To distribute it, some of these domains masqueraded as file storing and sharing services or recruiting-related websites. File sharing sites like Dropbox and Google Drive were used to host malware. This group also ran non-malicious custom desktop apps for Windows that were likely used to send malware directly to targets.


MOVIE DATE
HOME
ABOUT
WORKING
REVIEWS
CONTACT US
Host a
MOVIE DATE
with friends while
social distancing
Movie Date is an entertainment app that provides you the comfort of cinema at home absolutely free of charge!
DOWNLOAD


CV
WRITER
DOWNLOAD
ABOUT US
OUR CLIENTS
OUR WORK
CONTACT US
Upgrade Your CV Upgrade Your Career.



Screenshots of some of the websites run by this group

- **Malware:** This group has been known in the security industry as a prolific user of GravityRAT, a low-sophistication malware family capable of gathering sensitive user data. Related campaigns have been reported every couple of years, which speaks to the persistence of this APT's activity that we assess goes as far back as 2015. Since GravityRAT's creation,

we've seen them add new malicious capabilities to their malware and release versions for a range of operating systems, including Android, Windows and MacOS. They also added some resilience to their command-and-control infrastructure so that their malware can continue to operate when existing infrastructure goes down or gets exposed. In response to the security community continuing disruption of this group's activity, they were forced to set up new infrastructure following each threat report, likely degrading their operations .

We shared the most recent threat indicators with industry peers and security researchers to help provide insights into the personas this APT used and the groups they targeted, so we can collectively continue to further reduce their ability to run offensive cyber operations.

Bahamut APT

We took action against about 110 accounts on Facebook and Instagram linked to a hacking group known in the security community as Bahamut. It targeted people in Pakistan, India, including the Kashmir region, including military personnel, government employees, activists and others.

Our investigation found this group to be a persistent threat actor that ran campaigns across the internet, including link-shortening services, compromised or attacker-controlled websites, official and spoofed app stores, and third party hosting providers. They maintained a range of fictitious personas in an attempt to socially engineer people throughout South Asia into providing information or compromising their mobile devices. This group primarily used Android malware.

We identified the following new and noteworthy TTPs used by this threat actor across the internet:

- **Social engineering and fake personas:** Bahamut relied on social engineering to trick people into sharing sensitive information or installing malware on their devices. They relied on fictitious personas pretending to be tech recruiters at large tech companies, journalists, students and activists.
- **Android malware:** While Bahamut's Android malware continues to be of low sophistication, at times they've managed to publish their Android malware in the Play Store. Typically, it was included in apps posing as VPN providers or secure chat applications. We reported these apps and, as of this report, they are no longer available in the app store. In one instance, Bahamut distributed links to a trojanized Android word-processing application with support for various languages including Urdu — a language predominantly spoken in Pakistan, India and other regions in South Asia.
- **Fake and spoofed websites**: Bahamut used a range of tactics to host and distribute malware, including running a network of malicious domains purporting to offer secure chat, file-sharing, connectivity services, or news applications. Some of them spoofed the domains of regional media outlets, political organizations, or legitimate app stores, likely to make their links appear more legitimate. This group periodically made use of third-party hosting providers like MediaFire[.]com, file[.]io and link-shortening services like bit[.]ly and Grabify.

Patchwork APT

We took action against around 50 accounts on Facebook and Instagram linked to a hacking group in India known in the security industry as Patchwork. It targeted people in Pakistan, India, Bangladesh, Sri Lanka, the Tibet region, and China, including military personnel, activists, and minority groups.

We identified the following new and noteworthy TTPs used by this threat actor across the internet:

- **Social engineering and fake personas:** Patchwork relied on a range of elaborate fictitious personas to socially engineer people into clicking on malicious links and downloading malicious apps. Some of them posed as journalists in the United Kingdom (UK) or United Arab Emirates working for both legitimate and fake media outlets, military personnel or defense intelligence consultants.
- **Persistent malware distribution:** This group ran malicious apps, often posing as communications applications, available in Google Play Store. We reported these apps and, as of this report, they are no longer available in the app store. These apps contained relatively basic malicious functionality with the access to user data solely reliant on legitimate app permissions granted by the end user. Notably, Patchwork created a fake review website for chat apps where they listed the top five communication apps, putting their own, attacker-controlled app at the top of the list.
- **Adversary adaptation:** In response to continual detection and blocking of Patchwork's domains over the years by our security teams, the attackers attempted to change their tactics to enable persistence. For example, we've seen them turn to sending images of malicious links instead of the links themselves or sharing broken links that would require their targets to correct URLs manually. This adversarial adaptation has likely increased overhead and reduced the effectiveness of Patchwork's operations.

02

Coordinated inauthentic behavior (CIB)

We view CIB as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. In each case, people coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. When we investigate and remove these operations, we focus on behavior rather than content — no matter who's behind them, what they post or whether they're foreign or domestic.

Continuous CIB enforcement: We monitor for efforts to come back by the networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past.

Iran

We removed 40 Facebook accounts, eight Pages and one Group for violating our policy against coordinated inauthentic behavior. This network originated in Iran and targeted primarily Israel, and also Bahrain and France.

This operation ran across multiple internet services — including Facebook, Twitter, Telegram, YouTube and hacking forums — where it claimed to have hacked entities in the countries they targeted, including news media, logistics and transport companies, educational institutions, an airport, a dating service, and a government institution. The individuals behind this network alleged to have stolen these organizations' data or defaced their websites. We cannot confirm if any of the claimed attacks against these entities have, in fact, occurred. We removed this network before it was able to gain a following among authentic communities on our platforms.

We found multiple distinct clusters that posed as separate hacktivist teams, with each only active for a few days to a few weeks. Three separate clusters focused on Israel, where they offered to sell hacked data that allegedly belonged to commercial companies, educational institutions and a dating app. Another cluster that targeted Bahrain claimed to have hacked government websites before the country's elections. It was removed last year by both automation and our investigative team. The final cluster focused on France and claimed to have hacked the Charlie Hebdo newspaper. The news media reported some of these individual claims in Israel, Bahrain and France.

The people behind this network used fake accounts to post, like and share their own content to make it appear more popular than it was, as well as to manage Pages and Groups posing as hacktivist teams. They also liked and shared other people's posts about cyber security topics, likely to make fake accounts look more credible. Some of these accounts used profile photos likely generated using machine learning techniques like generative adversarial networks (GAN). We found the full scope of this activity after reviewing information shared with us by our peers at Microsoft.

- *Presence on Facebook and Instagram:* 40 Facebook accounts, eight Pages and one Group.
- *Followers:* Around 750 accounts followed one or more of these Pages; around 80 accounts joined one or more of these Groups.

China

We removed 50 Facebook accounts, 46 Pages, 31 Groups and 10 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This activity originated in China and targeted India and the Tibet region.

This operation ran across multiple internet services including Facebook, Twitter and YouTube, where they operated a number of fictitious brands focused on the regions they each targeted. These brands posed as independent media outlets, cultural associations or human-rights groups dedicated to issues related to Tibet or particular states on the border between China and India. We removed this network before it was able to build an audience on our apps.

The people behind this network used fake accounts — some of which were detected and removed by our automated systems — to manage Pages and Groups, comment on other people's posts and share their content in other people's Groups. Some of the accounts used profile photos likely generated using machine learning techniques like GAN. This network posted in English and Tibetan about news and current events in India and Tibet, including articles and memes that criticized the Indian government and military, questioned claims of human-rights abuses in Tibet raised by Western journalists, and accused Western countries of human-rights abuses. The operation also posted news articles by legitimate news outlets from the region, likely to make its fake brands appear more authentic.

We found this network as a result of our internal investigation into suspected coordinated inauthentic behavior in the region. Although the people behind it attempted to conceal their identities and coordination, our investigation found some links between the latest activity and the network we disrupted in September 2022. Just like the earlier operation, this latest campaign ran on a shift schedule — nine-to-five, Monday-to-Friday during working hours in China — with a dip in activity for lunch, and much less activity on weekends.

- *Presence on Facebook and Instagram:* 50 Facebook accounts, 46 Pages, 31 Groups and 10 Instagram accounts.
- *Followers:* About 5,800 accounts followed one or more of these Pages, around 19,600 accounts joined one or more of these Groups and about 200 accounts followed one or more of these Instagram accounts.
- *Advertising:* About $74,000 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.

China

We removed 107 Facebook accounts, 36 Pages, six Groups and 35 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in China and targeted many regions around the world, including Taiwan, Sub-Saharan Africa, Japan, Central Asia and the Uyghur community around the world. We took down this activity before the network was able to build an audience on our services.

This operation targeted multiple internet services including Facebook, Instagram, YouTube, Twitter, Telegram, PayPal, cryptocurrency, Blogspot, Reddit, Wordpress and freelancer[.]com. They also ran a front entity called London New Europe Media Ltd — a media representation service registered in the UK — which attempted to recruit content creators and translators around the world. For example, they tried to engage individuals to record English-language videos scripted by the network. In at least one case, recorded videos were posted on a YouTube channel criticizing the United States.

The people behind this media firm operated fictitious employee personas across the internet, and maintained a Wordpress blog and a website, likely to appear more legitimate and withstand scrutiny by the security community and the public. On the organization's website, they copy-pasted authentic articles taken from legitimate news media to post under fictitious bylines, in an apparent attempt to create the impression of a functioning news outlet. One of the network's fictitious personas partnered with an NGO in Uganda that featured the persona's logo at an event run by the NGO.

On our platforms, this network used fake accounts — some of which were detected and removed by our automated systems — to manage Pages and post content. Some of the Pages impersonated companies and institutions, including public offices in Europe, a US think tank, and a US technology company. In each case, these Pages made a few posts that mimicked the entity they pretended to be, and then switched to posting negative commentary about Uyghur activists and critics of the Chinese state. They also liked and commented on their own content. This activity only lasted a few days, and none of the Pages were able to build a substantial audience. Some of these accounts posed as Uyghur supporters and some used profile photos likely generated using machine learning techniques like GAN.

The individuals behind this network posted mainly in English, Russian, Uyghur and Chinese about news and current events in the regions they targeted. It included content about geopolitics in Central Asia; the impact of the Collective Security Treaty Organization (CSTO), the Organization of

Turkic States, and anti-Russia sanctions on Central Asia; warnings against boycotting the 2022 Beijing Olympics; allegations of US foreign policy in Africa; abuses against migrants in Europe, particularly Muslim refugees; calls for protests in Budapest against George Soros, including a public offer on Twitter to hire “part-timers” as protesters; alleged discharge of nuclear waste from Fukushima in Japan; claims of comfortable living conditions for Uyghurs in China; and criticism of politicians in Taiwan.

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the Asia-Pacific region. Although the people behind it attempted to conceal their identities and coordination, our investigation found links to individuals in China associated with Xi'an Tianwendian Network Technology, an information technology company.

- *Presence on Facebook and Instagram:* 107 Facebook accounts, 36 Pages, 6 Groups and 35 Instagram accounts.
- *Followers:* Around 15,500 accounts followed one or more of these Pages, around 200 accounts joined one or more of these Groups and about 200 accounts followed one or more of these Instagram accounts.

Venezuela and the United States

We removed 24 Facebook accounts, 54 Pages and four accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Venezuela and the United States and targeted Guatemala and Honduras.

This operation ran across multiple internet services including Facebook, Twitter, Medium, and websites associated with fictitious "news media" brands. None of their activity appeared to have gained engagement from authentic communities on our services.

The people behind this network used fake accounts — some of which were detected and removed by our automated systems — to manage Pages and profiles posing as independent media outlets, general lifestyle brands, independent journalists and local citizens in countries they targeted. They often reposted other people's content with long-form commentary, in addition to sharing original posts by the operation's fictitious media brands. Some of these accounts had Cyrillic names and were likely acquired from account farms in Eastern Europe, and some Pages displayed Twitter handles in their cover images on Facebook.

The individuals behind this effort shared memes and long- and short-form text posts in Spanish. They ran two targeted efforts focused on mayoral politics in Guatemala and national politics in Honduras. In Guatemala, this network focused on criticizing the current mayor of San Juan Sacatepéquez. In Honduras, they focused on political corruption and criticism of the president of the Honduran Congress, while posting supportive commentary about the Liberal Party.

We found this activity after receiving a tip from journalists at Reuters. Although the people behind the operation attempted to conceal their identities and coordination, our investigation found links to Predictvia, a Florida-registered firm, operating from both Venezuela and the United States. We banned this company from our services and issued a Cease and Desist letter.

- *Presence on Facebook and Instagram:* 24 Facebook accounts, 54 Pages and 4 Instagram accounts.
- *Followers:* Around 6,700 accounts followed one or more of these Pages and about 400 accounts followed one or more of these Instagram accounts.
- *Advertising:* About $1,650 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.

Togo and Burkina Faso

We removed 134 Facebook accounts, 142 Pages and 20 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated primarily in Togo and also in Burkina Faso, and targeted Burkina Faso.

This operation ran a network of websites posing as independent news media outlets in Burkina Faso. On our services, they used fake accounts — some of which were detected and removed by our automated systems — to drive people to their fictitious news websites, manage Pages, like and share each other's posts to make them appear more popular than they were. Some of these Pages represented the firm's fake news outlets. Others posed as grassroots groups in Burkina Faso and shared other people's content, likely to seem more authentic.

The people behind this activity posted primarily in French about news and current events in Burkina Faso, including positive commentary about the military ruler Captain Ibrahim Traoré, the military forces more broadly and the Patriotic Movement for Safeguarding and Restoration (MPSR).

We began looking into this operation after reviewing public reporting about a portion of this activity. Although the people behind it attempted to conceal their identities, our investigation found links to a political marketing consultancy in Togo called the Groupe Panafricain pour le Commerce et l'Investissement (GPCI). We assess this to be a comeback attempt by a network we took down in April 2021, which we linked to Aimons Notre Afrique, an NGO in the Central African Republic.

- *Presence on Facebook and Instagram:* 134 Facebook accounts, 142 Pages and 20 Instagram accounts.
- *Followers:* About 65,500 accounts followed one or more of these Pages and around 500 accounts followed one or more of these Instagram accounts.
- *Advertising:* About $500 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.

Georgia

We removed 80 Facebook accounts, 26 Pages, nine Groups and two accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network targeted multiple apps, including Facebook, Instagram and TikTok, originated in Georgia and focused on domestic audiences in that country.

The people behind this activity relied on fake accounts to run fictitious personas, manage Groups and Pages, post, comment, and like their own content to make it appear more popular than it was. These Pages and Groups purported to be local, independent, pro-government grassroots groups. The network operated around the clock to amplify content in support of the current Georgian government, including resharing posts by the official government Pages and pro-government media reports. They also shared criticisms of the opposition, particularly during the most recent public protests related to the now-retracted legislative proposal on the so-called "foreign agents" law in Georgia. In fact, this operation responded to protest developments in real time, including posting in the middle of the night. The individuals behind this network posted memes, text articles, and comments, primarily in Georgian.

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region. Although the people behind this operation attempted to conceal their identities and coordination, our investigation found links to the Strategic Communications Department of the Government Administration of Georgia.

- *Presence on Facebook and Instagram:* 80 Facebook accounts, 26 Pages, 9 Groups and 2 Instagram accounts.
- *Followers:* Around 138,000 accounts followed one or more of these Pages, around 238,000 accounts joined one or more of these Groups and about 400 accounts followed one or more of these Instagram accounts.
- *Advertising:* About $33,500 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.

Appendix: Threat indicators

The following section details unique threat indicators, such as apps, domains and email addresses, that we assess to be associated with each network. For the first time, to help the broader research community to study and protect people across different services, we've organized these indicators according to the Online Operations Kill Chain framework, which we use at Meta to analyze many sorts of malicious online operations, identify the earliest opportunities to disrupt them, and share information across investigative teams. The kill chain describes the sequence of steps threat actors go through to establish a presence across internet services, disguise their operations, engage with potential audiences, and respond to takedowns.

We're sharing these threat indicators to enable further research by the open-source research community into any related activity across the internet. This section includes the latest threat indicators and is not meant to provide a full cross-internet, historic view into the activities by these persistent threat actors. It's important to note that, in our assessment, the mere sharing of these links or engaging with them by online users would be insufficient to attribute accounts to a given operation without corroborating evidence.

1. PAKISTAN-BASED APT

Tactic	Threat indicator
Acquiring assets	
Acquiring online accounts	About 120 accounts on Facebook and Instagram
Acquiring domains hosting GravityRAT malware	bingechat[.]net
	cloudinfinity[.]co[.]uk
	vaultcloud[.]net
	cloudstore[.]net[.]in
	chatico[.]co[.]uk

Acquiring domain likely used to host cross-compiled Gravity RAT malware for MacOS	textra360[.]com
Acquiring domains to host, deploy, and support malware campaigns	moviedate[.]co[.]uk
	sexyber[.]net
	webbucket[.]co[.]uk
	cvscout[.]uk
	cvwriter[.]co[.]in
	androidwebkit[.]com
	comicum[.]co[.]uk
	craftwithme[.]uk
	recoverbin[.]co[.]uk
	crypted[.]co[.]in
	hookups4u[.]com
Developing custom malware	**BingeChat (Gravity RAT) hash:** 3f827039964a09f1179f66d6b2f9fe31
	CloudStore (Gravity RAT) hash: 7d6a6edc28579ac632d666d0dae86d0b
	Chatico (Gravity RAT) hash: dc00d22c2c04c49a40cb7cbd81080a7a
	WebBucket (attacker controlled-application) hash: de54f9b71f957808ea84fbda7895e329
	Textra360 application (attacker-controlled application) hash: f3c868403b3d468a2ab013a4d79613b0
	CVScout (attacker-controlled application) hash:

	de47f3525c4de36096f2888ac0947deb
	Sexyber (attacker-controlled application) hash: 321817f1f1d1a78b89682a79fdda0485
Disguising assets	
Creating fictitious personas	Posing as recruiters for defense companies (real or fictitious)
	Posing as government recruiters
	Posing as military personnel
	Posing as journalists
Creating romance lures	Posing as women seeking romance
Disguising malware sites	Disguising malware sites as dating sites
	Disguising malware sites as CV / resumé advice sites / apps
	Disguising malware sites as cloud storage providers or file sharing services
	Disguising malware site as entertainment site
Coordinating and planning	
Using domains and subdomains for command and control (C2)	dev.jdklibraries[.]com
	jre.jdklibraries[.]com
	androidadbserver[.]com
	api2.androidsdkstream[.]com
	api4.androidsdkstream[.]com
	adb.androidadbserver[.]com
	ping.androidadbserver[.]com

	cld.androidadbserver[.]com
	jupiter.playstoreapi[.]net
	moon.playstoreapi[.]net
	mars.playstoreapi[.]net
	venus.playstoreapi[.]net
Evading detection	
Publicly-available privacy protecting website registrations	Registering domains with Tucows Domains
	Registering domains with Internet Domain Services BS Corp t/a Internet.bs
	Registering domains with Ionos SE
	Registering domains with TLD Registrar Solutions Ltd.
	Registering domains with Namecheap Inc
Using third party infrastructure	Using third party file hosting providers to host and distribute malware
Compromising assets	
Sharing malicious files & links	Sharing malicious links & files via non-malicious custom applications (inferred behavior)
Socially engineering targets to deliver malware	Socially engineering targets to visit sites hosting malware
	Socially engineering targets to download Windows, Android, or MacOS malware
Enabling longevity	

Adding malware capabilities	Releasing Gravity RAT for Windows
	Releasing Gravity RAT for Android
	Releasing Gravity RAT for MacOS
Replacing infrastructure	Adding resilience to command-and-control infrastructure in response to disruptions and exposures
	Creating new domains to host malware after older ones were exposed
	Creating new fake social media accounts to replace disabled ones

2. BAHAMUT APT

Tactic	Threat indicator
Acquiring assets	
Acquiring online assets	About 110 accounts on Facebook and Instagram
Acquiring domains to host malware	usmimedia[.]com
	khalsaforum[.]com
	play-store-secure-safechat[.]usmimedia[.]com
	mamoonchat[.]com
	punjab-news18media-tribuneindia-mail[.]usmimedia[.]com
Creating apps	https://play.google[.]com/store/apps/details?id=com.secure safe
	InPage Android APK (part of Bahamut's malware family) hash: 35552112fcf0190c882e35de55f4b9c11e30e8144c39571c620da75fe5c70135
	PikaShow app (part of Bahamut's malware family) hash: 672d56b13708752b9d5287a8ac5e063174aa0af0c616a3ce8dd0dfbaff13386a
	MamoonChat app (part of Bahamut's malware family) hash: 1c914443afca5dbcf65ddb1b87ae4b9e9b7360f3f1ed1bfbce25fa027f1eb889
	Khalsa app (part of Bahamut's malware family) hash: 18982da2c181f9d4551b019e260284e0b20281f2cb2af538bf3c1a38c1369199
	InPage viewer (part of Bahamut's malware family) hash:

	4d73de1b6853955c61a096d224a2686b0fa9aed84cd51e018ec52da4639e03c8
	Secure Chat app (part of Bahamut's malware family) hash: 11ce6d6d2a8f98bebfb45d1d65cd07be5276187949112966f7e2046a7376300d
	Secure Chat app (part of Bahamut's malware family) hash: c80d8b7bd9759a9264f6504ffc58ee859a2434f8d258b05bf4f384f3fe3a7abc
	Secure Chat app (part of Bahamut's malware family) hash: bd52386932b071ba56b9f9941f79723df4cfc58f3c966fc1e8ca9e5cc06c1d7b
Disguising assets	
Creating fictitious personas	Posing as recruiters and developers at tech companies
	Posing as activists
	Posing as journalists
	Posing as students
Disguising malicious apps	Disguising apps as chat apps
	Disguising apps as VPN providers
	Disguising app as document reader
Impersonating news website	Disguising site hosting malware as news site
Coordinating and planning	
Acquiring domains and subdomains for command and control (C2)	5iw68rugwfcir37uj8z3r6rfaxwd8g8cdcfcqw62[.]de
	hbx5adg6vk[.]de

	rwzj2nntc3[.]de
Evading detection	
Privacy protecting website registrations	Registering domains with Vautron Rechenzentrum AG
Using link shortening services	Using bit[.]ly to hide the ultimate destination of malicious links
	Using grabify[.]link to hide the ultimate destination of malicious links
Using third-party hosting providers	Using MediaFire[.]com
	Using file[.]io
Using non-malicious apps	Some of the APT's apps for Android avoided explicit malicious functionality, relying on user granted permissions and capabilities one would expect to find in the attacker controlled apps (e.g., a chat application accessing contact information).
Compromising assets	
Socially engineering targets to deliver malware	Socially engineering targets into clicking on links to sites hosting malware
	Socially engineering targets to install trojanized apps
Enabling longevity	
Adding malware capabilities	Updating malware for Android
Replacing infrastructure	Creating new fake social media accounts to replace disabled ones

3. PATCHWORK APT

Tactic	Threat indicator
Acquiring assets	
Acquiring online assets	About 50 accounts on Facebook and Instagram
Creating apps	**JustPing hash**: 9481f10c51e9ad5b36846978587b4374
	Howdee hash: c11ed89d2584564fdb99d6ba1b42bd7d
	Click hash: a626a32a17bc49d2858798dcae3f36ee
Acquiring blog account	securemessagingapps[.]blogspot[.]com
Disguising assets	
Creating fictitious personas	Posing as journalists for news media outlets
	Posing as journalists for fictional outlets
	Posing as military personnel
	Posing as defense intelligence consultants
Disguising malicious apps as chat / communication apps	**JustPing hash**: 9481f10c51e9ad5b36846978587b4374
	Howdee hash: c11ed89d2584564fdb99d6ba1b42bd7d
	Click hash: a626a32a17bc49d2858798dcae3f36ee
Evading detection	
Using link shortening services	Using tinyurl[.]com to hide the ultimate destination of malicious links
	Using rebrand[.]ly to hide the ultimate destination of malicious links
	Using bit[.]ly to hide the ultimate destination of malicious links

Using non-malicious apps	Some of the APT's apps for Android avoided explicit malicious functionality, relying on user permissions to acquire information
Targeted engagement	
Planting false review to draw attention to malicious app	https://securemessagingapps.blogspot[.]com/2020/03/best-apps-for-secret-texting-to-try-in.html
Uploading apps to Google Playstore	https://play.google[.]com/store/apps/details?id=com.pinglabs.justping
	https://play.google[.]com/store/apps/details?id=com.click.chatapp
	https://play.google[.]com/store/apps/details?id=com.how.chatapp
Distributing malicious links	https://tinyurl[.]com/DeM-bayanat-download **redirects to**: http://file-downloader[.]ga/bayanat_au.apk
	https://bit[.]ly/39roCMd **redirects to**: https://apzshare[.]club/poahbcyskdh/cable.apk
	https://rebrand[.]ly/14d3hxt **redirects to**: https://faridun[.]com/jlkjlkjkl/ZangiV2[.]apk
	https://rebrand[.]ly/wmkzuxc **redirects to**: https://faridun[.]com/wqwqwqwq/ZangiV4[.]apk
	https://rebrand[.]ly/prv163 **redirects to**: https://stockapp-fresh[.]com/yhnlcxwzf/Pry1.63.apk
	https://tinyurl[.]com/invitation-join-nahida **redirects to**: https://www.webmails-authentication[.]tk/google_user_authentication/
	http://bayanat[.]co[.]nf/Bayanat.apk

	http://beautifullimages[.]co[.]nf/Image.apk
	http://newice[.]hopto[.]org/psiphon3.exe
	https://kashmirundergroundnews[.]ml:4040/rapeinkashmir/
Distributing malicious links disguised as downloads for chat / communication apps	https://tinyurl[.]com/Cucu-chatv2 **redirects to**: http://www.drive-sharefiles-downloads[.]ga/cucu2/CucuChat.apk
	https://rebrand[.]ly/YoTalk **redirects to**: https://appplace[.]life/vdfogrglj/YoTalk.apk
	https://rebrand[.]ly/crazytalk **redirects to**: https://appplace[.]shop/aoedfhhs/Crazytalk.apk
	https://bit[.]ly/3c5e9sx **redirects to**: https://chirrups-download[.]ml/chirrups/images/chirrups.apk
	https://bit[.]ly/3aPM6fU **redirects to**: https://file-star[.]buzz/gdgtgdt1245435/chirrups.apk
	https://tinyurl[.]com/cucuchat-download-2019 **redirects to**: https://drive-sharefiles-downloads[.]gq/CucuChat.apk
	https://tinyurl[.]com/fruitchat19 **redirects to**: https://fileshares[.]online/Fruitchat.apk
	https://tinyurl[.]com/Fruitchatv4 **redirects to**: https://fileshares[.]online/Fruitchatv4.apk
	https://tinyurl[.]com/Just-You-apk **redirects to**: https://fileshares[.]online/Just-You.apk
	https://bit[.]ly/37AktWN

	redirects to: https://fun.socialyte[.]site/BABBLEv3.apk
	http://rebrand[.]ly/ptalkk
	http://videvideocaller[.]ml/video/vide_videocall.apk
Distributing malicious links disguised as downloads for VPN service	https://tinyurl[.]com/Google-VPN-apk **redirects to**: http://file-downloader[.]ga/vpn_oa.apk
	https://tinyurl[.]com/google-vpn-download **redirects to**: http://thenewsnation[.]ml:9371/vpn_au.apk
	https://tinyurl[.]com/latest-vpn-downloads **redirects to**: http://vpndownloads.ddns[.]net:2808/vpn_ag.apk
	http://bit[.]do/VPN_latest_secure-apk
	http://downloader-file[.]cf/vpn_hh.apk
	http://downloadvpn[.]comli[.]com/VPN.apk
	http://vpndl[.]co[.]nf/VPN.apk
	http://vpndownload[.]co[.]nf/VPN.apk
	http://vpndownload[.]webutu[.]com/hh/f/n/VPN.apk
	http://vpndownloads[.]co[.]nf/VPN.apk
	http://vpndownloads[.]ddns[.]net:2808/vpn_hh.apk
Distributing malicious links disguised as downloads for news / update services	https://tinyurl[.]com/Dukhtaran-e-Millat-Updates **redirects to**: http://islamicbayanat.ddns[.]net:2808/app_bb.apk
	https://tinyurl[.]com/APHC-updates-live **redirects to**: http://185.82.216[.]57:2125/google_user_authentication/
Compromising assets	

Socially engineering targets to deliver malware	Using fake personas to persuade targets to visit sites hosting malware
	Persuading targets to install malicious apps
Enabling longevity	
Increasing disguise of malicious links	Distributing images of malicious links
	Distributing broken malicious links

4. IRAN-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	67 accounts
Acquiring Facebook Pages	14 Pages
Acquiring Facebook Groups	1 Group
Acquiring Instagram accounts	18 Instagram accounts
Registering domains	amc239[.]com
	holysouls[.]cc
Registering emails on own domains	info[at]amc239[.]com, hosted with Titan.email service
	info[at]holysouls[.]cc
Acquiring Twitter accounts	https://twitter[.]com/GenerousThief1
	https://twitter[.]com/altoufanteam
	https://twitter[.]com/AMC239
	https://twitter[.]com/BlackMagic2511
Acquiring Telegram channels	https://t[.]me/generousthief
	https://t[.]me/generousthief1
	https://t[.]me/ALTOUFANTEAM
	https://t[.]me/SANGKANCIL_LEAK_ISRAEL_CITY4U
	https://t[.]me/BlackMagic2511
Acquiring YouTube channels	https://www.youtube[.]com/@blackmagic7533
	https://www.youtube[.]com/@holy_souls

Registering accounts on hacking-themed forums	https://leakzone[.]net/User-holysouls
	https://breached[.]vc/User-holysouls
	https://cracked[.]io/holysouls
	https://www.nulled[.]to/user/5533554-holysouls
Disguising assets	
Creating fictitious "hacktivist" personas	Sangkancil
	Generous Thief
	Altoufan Team
	AMC239
	Black Magic
	Holy Souls
Evading detection	
Privacy protecting website registrations	Registering domains with Namecheap which uses withheldforprivacy[.]com
Using link shortener to disguise URL	https://cutt[.]ly/LZ8iEIt
Copying content from authentic sources	Reusing other people's posts about cybersecurity
Indiscriminate engagement	
Amplifying with fake accounts	Share on Facebook
	Share on Instagram
	Share on Twitter
Targeted engagement	
Posting to reach selected	Posting into cybersecurity-related Groups

audience	
Directing audience off-platform	Directing audience towards Telegram channels
Offering to sell allegedly hacked materials	https://leakzone[.]net/Thread-Selling-the-50Gb-data-of-Israeli-transportation-companies-by-black-magic-group
Direct outreach to news organizations	According to Microsoft's Digital Threat Analysis Center, this network contacted news organizations to publicize its hacks.
Compromising assets	
Defacing websites	According to public reports, the network claimed to have defaced websites linked to the following institutions:
	Bahrain News Agency
	Bahrain Airport
	Bahrain Chamber of Commerce
	Akhbar Al Khaleej newspaper
	Bahrain House of Representatives
	Tehillim-center[.]co[.]il
Stealing data	According to public reports, the network claimed to have stolen data from the following institutions:
	CITY4U, Israel
	Logistics companies in Israel
	7brachot[.]co[.]il
	Center for Educational Technology, Israel
	Charlie Hebdo, France
Enabling longevity	
Changing personas	The network shifted to a new fake persona after each alleged hack and leak, in the following sequence:

	Sangkancil
	AMC239
	Generous Thief
	Black Magic
	Altoufan Team
	Holy Souls

5. CHINA-BASED CIB NETWORK ONE

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	63 accounts
Acquiring Facebook Pages	44 Pages
Acquiring Facebook Groups	28 Groups
Acquiring Twitter accounts	https://twitter[.]com/SaraSil39636921
Acquiring YouTube channels	https://www.youtube[.]com/@user-xf2zm5jj9h
	https://www.youtube[.]com/@knowindia303
	https://www.youtube[.]com/@northeastunion7212
Disguising assets	
Using visual disguises	Using profile pictures likely generated using machine learning techniques like GAN
Creating fake "news outlet" personas	The network ran a number of cross-platform "news outlets", including one called Northeast Union (see YouTube link above)
Coordinating and planning	
Working to a regular shift pattern	Working a 9-5, Monday-to-Friday shift pattern appropriate for the GMT +8 time zone, with much lower activity at lunchtime and the weekends
Evading detection	
Copying content from authentic sources	Between its own posts, the network posted content copied from authentic news outlets focused on the regions it targeted

Indiscriminate engagement	
Amplifying with fake accounts	Sharing on Facebook
	Sharing on Twitter
Targeted engagement	
Posting to reach selected audience	Posting in Groups focused on topics of interest to the network
Directing audience to off-platform content	Directing people towards network's YouTube channels
Using audience-specific hashtags	The network's Twitter account used hashtags appropriate to the region and audience it was targeting
Tagging media, institutions and influencers	The network's Twitter account tagged media and institutions including the UN Human Rights office and BBC World. There is no indication that they engaged in return.
Advertising to promote posts	About $73,600 in spending for ads on Facebook and Instagram, paid for mostly in US Dollars.

6. CHINA-BASED CIB NETWORK TWO

Tactic	Threat indicator
Acquiring assets	
Registering company	London New Europe Media Ltd
Creating website	https://neweurope[.]online
Acquiring Facebook accounts	117 accounts
Acquiring Facebook Pages	38 Pages
Acquiring Facebook Groups	6 Groups
Acquiring Instagram accounts	38 accounts
Acquiring Twitter accounts	https://twitter[.]com/new_observation
	https://twitter[.]com/Dream_andFuture
Acquiring YouTube channel	https://www.youtube[.]com/@Durban_Declaration
Creating Telegram account	http://t[.]me/new_europe
Acquiring safechat[.]com accounts	https://safechat[.]com/u/new_observation
	https://safechat[.]com/u/dreams_and_future
Acquiring WordPress blog	https://org162532576[.]wordpress[.]com/
Acquiring Blogspot accounts	http://89ijlop.blogspot[.]com

	http://hkjluhol.blogspot[.]com
Acquiring Reddit account	https://www.reddit[.]com/user/New-Europe-1993
Creating blog posts	https://org162532576[.]wordpress[.]com/2021/12/06/why-boycott-beijing-winter-olympics%ef%bf%bc/
	http://89ijlop.blogspot[.]com/2021/12/why-boycott-beijing-winter-olympics_5.html
	http://hkjluhol.blogspot[.]com/2021/12/why-boycott-beijing-winter-olympics_21.html
Disguising assets	
Using visual disguises	Using profile pictures likely generated using machine learning techniques like GAN
	Copying profile pictures from publicly available online sources
Impersonating real institutions and companies	The network impersonated public offices in Europe, a US think tank, and a US technology company
Creating fake "news outlet" persona	The network created the New Europe Observation brand across multiple internet services
Creating fake "activist" personas	Fake accounts posed as supporters of the Uyghur community
Creating fake employees	Some of the network's fake accounts posed as employees of New Europe Observation
Gathering information	
Publicly soliciting information	The network advertised for freelance analysts to write on geopolitical subjects, particularly in Central Asia
Coordinating and planning	
Coordinating by email	The network solicited for freelance writers to contact it by email at neweuropeobservation[at]outlook.com

Evading detection	
Copying content from authentic sources	The New Europe Observation website appears to have copied its content from authentic sources, including Euractiv and Foreign Policy
Editing copied content	The website sometimes altered the headlines of its copied articles, and routinely replaced the genuine byline with a fictitious one
Privacy protecting website registrations	Registering domain with privacyprotect[.]org
Indiscriminate engagement	
Amplifying with fake accounts	Sharing on Facebook
	Sharing on Instagram
	Sharing on Twitter
	Sharing on Reddit
	Sharing on safechat[.]com
Targeted engagement	
Advertising for freelance writers	https://www[.]freelancer[.]com/projects/articles/Writing-articles-35666510/details
Advertising for freelance video creators	The network advertised for people to voice videos according to its script
Advertising for paid protesters	https://twitter[.]com/new_observation/status/1562640310273921025
Directing audience to off-platform content	Directing audience towards network's website, blogs and YouTube channel
Partnering with real NGO	The network partnered with a real NGO in Uganda

	The network's logo featured on a banner and T-shirts at an on-the-ground event in Uganda run by the partner NGO
Posting about individuals	The network posted hostile commentary about Uyghur activists and critics of China

7. VENEZUELA/US-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Registering a company	Predictvia, a Florida-registered firm
Acquiring Facebook accounts	21 accounts
Acquiring farmed Facebook accounts	The network used some Facebook accounts with Cyrillic names that nevertheless posted in Spanish, and were likely acquired from account farms in Eastern Europe
Acquiring Facebook Pages	88 Pages
Registering domains	eleccionesguate2023[.]com
	catrachonews[.]com
	hondurasleaks[.]com
Registering emails on own domains	Configure eleccionesguate2023[.]com with Titan.email service
	Configure catrachonews[.]com with Titan.email service
Acquiring Twitter accounts	https://twitter[.]com/eleccion gt2023
	https://twitter[.]com/catracho_news
	https://twitter[.]com/LeaksHonduras
	https://twitter[.]com/legion_504
Acquiring Medium blogs	notihonduras504.medium[.]com
	vozanoticias.medium[.]com

Disguising assets	
Creating cross-platform personas	The network created fake personas (see below) with the same naming convention and branding across websites, Facebook and Twitter
Creating fake "fact check" persona	Elecciones Guate 2023
Creating fake "news outlet" persona	Catracho News
Creating fake "hacktivist" persona	Hondurasleaks
Evading detection	
Privacy protecting website registrations	Registering domain with Hosting Concepts B.V. d/b/a Registrar[.]eu
	Registering domains with realtimeregistrar[.]com
Indiscriminate engagement	
Amplifying with fake accounts	Sharing on Facebook
	Sharing on Twitter
Targeted engagement	
Commenting on specific posts	The network often posted long-form comments below other people's posts
Using audience-specific hashtags	The network's Twitter accounts used hashtags appropriate to the region and audience they were targeting
Tagging media, institutions and influencers	The network's Twitter accounts occasionally tagged politicians in the target countries. No indication that they engaged in return.
Posting about individuals	The network posted hostile commentary about the mayor of San Juan in Guatemala and the President of the Honduran Congress, and positive commentary about the Liberal Party in Honduras.

Advertising to promote posts	About $1,650 in spending for ads on Facebook and Instagram, paid for mostly in US Dollars
Enabling longevity	
Changing accounts	According to the Internet Archive, the "HondurasLeaks" website linked to twitter[.]com/leakshonduras until at least January 18, 2022, but changed the link to twitter[.]com/legion_504 some time before February 1, 2022.

8. TOGO/BURKINA FASO-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Creating a political marketing company	gpci[.]info
Registering websites	etoileducontinent[.]info
	afriqueactualite[.]info
	LePotentieldafrique[.]net
	lavoixdafrique[.]info
	leuropeafrique[.]info
	lepanafricanisme[.]info
	lemessagerafricain[.]info
	lereveilafricain[.]info
	lemondeactualite[.]info
	infodafrique[.]net
	lanouvellelettre[.]info
	linfodumonde[.]net
	afriqueevenementiel[.]com
	lintelligentdafrique[.]info
	loccident[.]info
	lanouvelleducontinent[.]info
	lequotidiendafrique[.]net
	lemondeenvrai[.]net

	sursautdafrique[.]info
	lafrique[.]info
	afriquelibre[.]net
	miroirdafrique[.]info
	atalakou[.]info
	Ouaga24[.]info
	ledementi[.]net
	dounia[.]info
	lemeilleurdafrique[.]com
	afriktimes[.]info
Acquiring Facebook accounts	145 accounts
Acquiring Facebook Pages	142 Pages
Acquiring Instagram accounts	26 accounts
Disguising assets	
Creating fake "news outlet" personas	The websites controlled by the network are listed above
Creating fake "grassroots" personas	The network created "grassroots" accounts and Facebook Pages to amplify its content
Evading detection	
Privacy protecting website registrations	Registering domain with fastdomains[.]com
	Registering domains with online[.]net
	Registering domains with bookmyname[.]com
Indiscriminate engagement	
Amplifying with fake accounts	Sharing on Facebook

Targeted engagement	
Posting to reach selected audience	Posting into Groups focused on local events in Burkina Faso
Directing audience to off-platform content	Directing audience towards network's websites
Posting about individuals	The network posted positive comments about military ruler Captain Ibrahim Traoré
Advertising to promote posts	About $500 in spending for ads on Facebook and Instagram, paid for mostly in US Dollars
Enabling longevity	
Changing persona	We assess this network to be an attempt to come back by a network we took down in April 2021 and attributed to Aimons Notre Afrique (ANA), an NGO in the Central African Republic.

9. GEORGIA-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	82 accounts
Acquiring Facebook Pages	27 Pages
Acquiring Facebook Groups	9 Groups
Acquiring Instagram accounts	2 accounts
Acquiring TikTok accounts	http://tiktok[.]com/@juurnalistebi
	http://tiktok[.]com/@igaribashvili
	https://www.tiktok[.]com/@irakli4georgia
Disguising assets	
Creating complex personas	The network created elaborate fictitious personas posing as pro-government citizens of Georgia
Creating fake "grassroots" personas	The network's fake personas posed as pro-government activists and organizations
Gathering information	
Monitoring breaking news (inferred from posting activity)	The network reacted to events in Georgia in real time, indicating an ability to track and respond to breaking news. The method used to do this is not known.
Coordinating and planning	
Working to a shift pattern	The network operated around the clock, including posting in the middle of the night (Georgia time). The method used to coordinate this is not known.
Indiscriminate engagement	

Amplifying with fake accounts	Sharing on Facebook
Targeted engagement	
Commenting on specific posts	The network often posted long-form comments below other people's posts
Posting to reach selected audience	Posting into Groups focused on local events in Georgia
Posting about individuals	The network posted hostile commentary about Georgian opposition activists and protesters
Advertising to promote posts	About $33,540 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.