APRIL 2022

DETAILED REPORT

Adversarial Threat Report

Ben Nimmo, Global Threat Intelligence Lead for Influence Operations
David Agranovich, Director, Threat Disruption
Nathaniel Gleicher, Head of Security Policy

Meta

TABLE OF CONTENTS

PURPOSE OF THIS REPORT

Our public security reporting began over four years ago when we first shared our findings about coordinated inauthentic behavior (CIB) by the Russian Internet Research Agency. Since then, global threats have significantly evolved, and we have expanded our ability to respond to a wider range of adversarial behaviors. To provide a more comprehensive view into the risks we see, we're expanding our regular reporting to include cyber espionage, inauthentic behavior, and other emerging harms, all in one place, as part of the quarterly reporting we're testing. We're also sharing threat indicators at the end of this report to contribute to the efforts by the security community to detect and counter malicious activity elsewhere on the internet (See Appendix). We welcome ideas from the security community to help us make these reports more informative and we'll adjust as we learn from feedback.

SUMMARY OF OUR FINDINGS

- Our pilot quarterly threat report provides a comprehensive view into the risks we see across multiple policy violations including Coordinated Inauthentic Behavior (CIB), cyber espionage, and other emerging harms, like mass reporting.
- We took action against two **cyber espionage** operations from Iran. The first network was linked to a group of hackers known in the security industry as UNC788. The second was a separate, previously unreported group that targeted industries like energy, telecommunications, maritime logistics, information technology, and others. More here.
- We removed a hybrid network operated by the Ministry of Internal Affairs of Azerbaijan that **combined cyber espionage with Coordinated Inauthentic Behavior (CIB)** to target civil society in Azerbaijan by compromising accounts and websites to post on their behalf. More here.
- Our findings also include an **update on our enforcements in Ukraine**, including attempts by previously disrupted state and non-state actors to come back on the platform, in addition to spam networks using deceptive tactics to monetize public attention to the ongoing war. More here.
- We removed **Coordinated Inauthentic Behavior** operations from Brazil, Costa Rica and El Salvador, and previously reported networks from Russia and Ukraine. The Brazilian network is the first operation we've disrupted that primarily focused on environmental issues. More here.

- As part of disrupting new and **emerging threats**, we removed a coordinated violating network in the Philippines that claimed credit for bringing websites down and defacing them, primarily those of news entities. More here.
- Under our **Inauthentic Behavior policy against mass reporting**, we removed a network in Russia for abusing our reporting tools by repeatedly reporting people in Ukraine for fictitious violations of Facebook policy, in an attempt to silence them. More here.
- Also under our Inauthentic Behavior policies, we took down tens of thousands of accounts, Pages and Groups around the world for **inauthentically inflating the distribution of their content and abusively building an audience.** We did so through large-scale automated detection, complemented by manual investigations. More here.

01

Removing three cyber-espionage networks from Iran and Azerbaijan

Cyber espionage actors typically target people across the internet to collect intelligence, manipulate them into revealing information, and compromise their devices and accounts. When we disrupt these operations, we take down their accounts, block their domains from being shared on our platform, and notify people who we believe were targeted by these malicious groups. We also share information with security researchers, governments, and our industry peers so they too can take action to stop this activity. We have included threat indicators in the Appendix to this report.

1. UNC788

We took action against a group of hackers from Iran, known in the security industry as UNC788, that targeted people in the Middle East, including Saudi military, dissidents and human rights activists from Israel and Iran, politicians in the US, and Iran-focused academics, activists and journalists around the world. Their malicious activity had the hallmarks of a well-resourced and persistent operation while obfuscating who's behind it. We've been tracking and blocking this group's efforts for a number of years, similar to our peers at other platforms. This latest cyber espionage campaign was active across the broader internet and focused on phishing its targets to steal credentials to their online accounts and sharing links to malicious websites hosting malware.

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

- **Social engineering:** This group used a combination of low-sophistication fake accounts and more elaborate fictitious personas, which they likely used to build trust with potential targets and trick them into clicking on phishing links or downloading malicious applications. Some of these personas posed as human rights activists or academics.
- **Phishing:** This campaign also relied on a network of phishing websites that hosted event landing pages or files where people were asked to login with their Google credentials to register.
- **Malware:** To compromise people's accounts and devices, this group copied and modified a legitimate Android application — a birthday calendar app — so it could extract contact information and send it to the attacker's remote server. They also developed remote access-capable malware for Android that disguised as a Quran, a chat app to retrieve people's contacts list, text messages, files, location information, and activate camera and microphone. We named this previously unreported malware strain HilalRAT (remote access trojan), after seeing "hilal'' in several of the malware samples we analyzed. In the Appendix, we're also sharing a Yara rule to help the security community identify it.

2. Previously unreported hacking group from Iran

We took action against a previously unreported hacking group from Iran that targeted or spoofed companies in multiple industries around the world. This included energy companies in Saudi Arabia, Canada, Italy, and Russia; the information technology industry in India and United Arab Emirates; the maritime logistics industry in UAE, Iceland, Norway, Saudi Arabia, US, Israel, and India; telecommunications companies in Saudi Arabia and UAE; and the semiconductor industry in Israel, US, and Germany. This activity had the hallmarks of a well-resourced and persistent operation while obfuscating who's behind it.

This group used similar TTPs to another threat actor dubbed Tortoiseshell that we reported on last year, but in this case we saw different targeting, technical infrastructure, and distinct malware. We identified the following TTPs used by this group across the internet:

- **Social engineering:** This campaign ran elaborate fictitious personas across social media platforms, including Instagram, LinkedIn, Facebook, and Twitter, to make them appear more credible and help withstand scrutiny. They often posed as recruiters for real and fake companies in the industry or region that each persona targeted, as part of what

appeared to be a social engineering scheme to trick people into clicking on malicious links or installing malware.

- **Fake and spoofed legitimate corporate websites:** This operation included a network of fictitious corporate recruiting websites, as well as spoofed domains of legitimate companies. It also relied heavily on email phishing to social engineer people to download malware, likely in an attempt to gain information and access to corporate systems.
- **Interactive targeting and exploit protection:** This group took steps to conceal their activity and protect their malicious tools by embedding interactive features in them that would only send the malicious payload after the targets interacted with the attacker in real time. For example, an interview app would launch a built-in chat function for an attacker to supply a password to start an interview. When the target entered the password, it activated the delivery of the malware. A chess app also required a passcode, supplied by the hackers, to launch the game and the malware delivery.
- **Malware**: This group built unique malicious applications disguised as a VPN app, a salary calculator, an audio book reader, or a chat app. They developed malware on the VMWare ThinApp virtualization platform, which allowed them to run it on many different systems and hold malicious payload back until the last minute, making malware detection more challenging. The final payload included full-featured remote-access trojans, capable of running commands on the target's device, access and send files, take screenshots, and download and execute additional malware.

3. A hybrid operation from Azerbaijan

We disrupted a complex network in Azerbaijan that engaged in both cyber espionage and coordinated inauthentic behavior. It primarily targeted people from Azerbaijan, including democracy activists, opposition, journalists, and government critics abroad. This campaign was prolific but low in sophistication, and was run by the Azeri Ministry of Internal Affairs. It combined a range of tactics — from phishing, social engineering, and hacking to coordinated inauthentic behavior.

This operation targeted websites and the online accounts of democracy activists, opposition, and journalists in Azerbaijan in pursuit of what appears to be two goals: obtain personal information about the targets and promote particular narratives about them or on their behalf. They focused on news websites and a number of internet services, including Facebook, Twitter,

LinkedIn, YouTube, and Russian VK and OK. It is another example of a hybrid espionage and CIB campaign, similar to the unconnected and separate activity by Ghostwriter, a threat actor that most recently targeted Ukraine.

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

- **Compromised and spoofed websites**: This group operated across the internet, with over 70 websites and domains that they either ran themselves or compromised. They targeted sites in Azerbaijan and, to a lesser extent, Armenia; a small number of sites had Russian or Turkish domains. Once they compromised these websites, the group harvested databases containing usernames and passwords, likely to further compromise online accounts of their targets who might have reused the same credentials across the internet. They also, at times, hosted credential phishing content on these websites.
- **Malware and other malicious tools**: This group scanned websites in the region for "low-hanging fruit" web vulnerabilities, using tools like Burpsuite and Netsparker. They then used publicly known techniques to compromise vulnerable sites before uploading one of numerous web shells in order to maintain persistent access. Similarly, to crack hashes obtained from compromised sites, they used publicly available hash-cracking tools. In its targeting of people, this threat actor is known to use both Windows and commodity surveillanceware for Android.
- **Credential phishing**: In its phishing activity, this group relied on compromised and spoofed websites where they asked people to enter their social media credentials so they could cast their vote in political polls. Through it, an attacker would obtain people's credentials to take over their online accounts. This operation also attempted to drive people to their phishing web pages by sharing links to them on social media, including through compromised accounts of public figures or accounts posing as members of Facebook's security team, many of which were detected and disabled by our automated systems.
- **Industry reporting**: Our findings corroborate previous public reporting about some of this activity by OC-Media and Qurium.
- **Coordinated Inauthentic Behavior**: The individuals behind this activity used fake and compromised accounts to run Pages and post as if they were the legitimate owners of these Pages and accounts. They typically posted in Azeri, including critical or compromising commentary about the government opposition, activists, journalists, and other members of civil society in Azerbaijan.

02

Ukraine security update

Since the start of the Russian invasion of Ukraine, our teams have been on high alert to detect and disrupt threats and platform abuse, including attempts to come back by networks we removed before. We've shared our findings with our peers at tech companies, independent researchers, governments, law enforcement and targeted individuals, when possible. You can find our previous security update on Ukraine here.

Our Key Findings

Nation state actors

Government-linked actors from Russia and Belarus engaged in cyber espionage and covert influence operations online. This activity included interest in the Ukrainian telecom industry; both global and Ukrainian defense and energy sectors; tech platforms; and journalists and activists in Ukraine, Russia, and abroad.

These operations appear to have intensified shortly before the Russian invasion. For example, we detected and disrupted recidivist CIB activity linked to the Belarusian KGB who suddenly began posting in Polish and English about Ukrainian troops surrendering without a fight and the nation's leaders fleeing the country on February 24, the day Russia began the war. Prior to that, this particular threat actor primarily focused on accusing Poland of mistreating migrants from the Middle East. On March 14, they pivoted back to Poland and created an event in Warsaw calling for a protest against the Polish government. We disabled the account and event that same day.

Known persistent threat actors

First, following our last security update on Ukraine, we've seen a further spike in compromise attempts aimed at members of the Ukrainian military by Ghostwriter, a threat actor tracked by the security community. As we've shared before, Ghostwriter typically targets people through email compromise and then uses that to gain access to their social media accounts across the internet. Since our last public update, this group has attempted to hack into the Facebook accounts of dozens of Ukrainian military personnel. In a handful of cases, they posted videos calling on the Army to surrender as if these posts were coming from the legitimate account owners. We blocked these videos from being shared.

Second, we detected and took down an attempt to come back by a network we removed in December 2020 and linked to individuals associated with past activity by the Russian Internet Research Agency (IRA). Their off-platform activity appears to have begun last year and centered around a website, posing as an NGO focused on civil rights in the West. They unsuccessfully attempted to create Facebook accounts in late 2021 and January 2022. Throughout January and February of this year, the website published about police violence in the West, but since the invasion, their articles blamed Russia's attack on NATO and the West and accused Ukrainian forces of targeting civilians.

Politically-aligned non-state actors

We detected and took down an attempt to come back by the network we removed in December 2020 and linked to people in the Luhansk region of Ukraine. This activity centered around two websites promoting pro-Russian commentary in the Caucasus and Ukraine, and a small number of accounts on Facebook, Telegram, VK, and OK. In early March, the Ukraine-focused site appeared to have been taken over to direct its audience towards a Telegram channel showing photos of Russian casualties.

We also removed a network in Russia for violating our Inauthentic Behavior policy against mass reporting. The network coordinated to falsely report people in Ukraine and also in Russia for various violations, including hate speech, in an attempt to have them and their posts removed from Facebook. More details on this network can be found here.

Financially motivated actors

As is typical for major world events and critical societal issues, we're seeing scammers around the world turn to the war in Ukraine to amass an audience and monetize everyone's attention to this humanitarian crisis. We know that at first glance, these activities can be mistaken for state-backed influence operations, when in fact they come from scammers who use socio-political themes as a form of spam or clickbait lures.

Since the war began, we've investigated and removed tens of thousands of accounts, Pages and Groups using both automated and manual systems. We've seen spammers from around the world use inauthentic behavior tactics including streaming live-gaming videos and reposting popular content including other people's videos from Ukraine as a way to pose as sharing live updates. Some of the spammers switched names repeatedly to trick people into following them so they can try making money by either driving people to off-platform ad-filled websites or selling them merchandise. We also took down multiple clusters of long-abandoned compromised accounts that suddenly shifted to being run from Russia. Many of them shared identical pro-separatist videos and amplified accounts in their own clusters, likely as part of paid inauthentic engagement.

Account security

We strongly encourage people in Ukraine and Russia to strengthen the security of their online accounts, including email and social media. To help keep your online accounts safe and protect access to social media and other websites blocked in your country:

- Download a VPN app on your devices to ensure access to blocked sites, like social media, through an encrypted connection.
- Enable two-factor authentication using a third-party authentication app like Google Authenticator or Duo.
- Do not reuse your password. Passwords should be strong and unique for each of your accounts.

03

Removing four networks for coordinated inauthentic behavior

We view CIB as coordinated efforts to manipulate public debate for a strategic goal where 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 re-establish a presence on our platforms by 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.

1. Brazil

We removed a network of 14 Facebook accounts, nine Pages, and 39 Instagram accounts for violating our policy against coordinated inauthentic behavior. This network originated in Brazil and targeted domestic audiences in that country.

The people behind this activity relied on fake accounts— some of which were detected and disabled by our automated systems —targeting people across multiple social media platforms, including Facebook, Instagram, and Twitter. This activity ran in what appears to be two phases. First, in 2020, the operation posted memes about social and political issues, including land reform and the COVID-19 pandemic. They abandoned this activity after a couple of months, having gained almost no engagement. In 2021, they created Pages that posed as fictitious NGOs and activists focused on environmental issues in the Amazonas region of Brazil. They posted about deforestation, including arguing that not all of it is harmful, and criticizing legitimate environmental NGOs who spoke out against deforestation in the Amazon.

In addition to posting original memes, they also shared mainstream media content and posts by Greenpeace and nature photographers, likely in an attempt to make these accounts look more credible. In one instance, we saw this operation use a profile picture, likely generated using artificial intelligence techniques like generative adversarial networks (GAN).

We found this network as a result of our investigation into suspected coordinated inauthentic behavior in the region. Although the people behind it attempted to conceal their identities and coordination, our investigation found links to individuals associated with the Brazilian Military[1].

- *Presence on Facebook and Instagram:* 14 Facebook accounts, nine Pages, and 39 accounts on Instagram.
- *Followers:* About 1,170 accounts followed one or more of these Pages and about 23,600 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around $34 in spending for ads on Facebook and Instagram, paid for in Brazilian real.

2. Costa Rica and El Salvador

We removed 233 Facebook accounts, 84 Pages, two Groups, and 27 Instagram accounts for violating our policy against coordinated inauthentic behavior. This network originated in Costa Rica and El Salvador and targeted primarily Costa Rica and El Salvador.

The people behind this activity used fake accounts — some of which were already detected and disabled by our automated systems — to run Pages posing as news outlets, post memes, comment on their own and other people's content, and drive people to off-platform domains. This network also amplified content from the Pages of local politicians and businesses. They would typically post on both sides of the political spectrum, including in support of competing political candidates running against each other. Some of these accounts had profile pictures likely generated using artificial intelligence techniques like generative adversarial networks (GAN).

[1] The process of attributing violating activity to particular threat actors has been long debated by the security community. Meta's approach to attribution relies on the available technical and investigative signals at our disposal. When, based on the available evidence, our expert investigative teams do not see clear evidence of command and control, but do see a number of individuals associated with the entity behind the operation, Meta will attribute the activity to "individuals linked to the entity."

The individuals behind this operation posted primarily in Spanish about news and current events in Central America. They also posted supportive commentary about one telecom company in Costa Rica and criticism of its competitors.

We found this network after reviewing public reporting about an off-platform portion of this activity and took action ahead of the election in Costa Rica. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to Noelix Media, a PR firm with offices in Costa Rica and El Salvador. Noelix is now banned from our platform.

- *Presence on Facebook and Instagram:* 233 Facebook accounts, 84 Pages, two Groups, and 27 accounts on Instagram.
- *Followers:* About 212,000 accounts followed one or more of these Pages, around 10 accounts joined one or more of these Groups, and about 2,000 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around $128,000 in spending for ads on Facebook and Instagram paid for primarily in US dollars and Costa Rican colón.

3. Russia and Ukraine

We reported this enforcement as part of our security update on February 27, 2022.

We removed a small network of 27 Facebook accounts, two Pages, three Groups, and four Instagram accounts for violating our policy against coordinated inauthentic behavior. This network operated from Russia and Ukraine and targeted primarily Ukraine.

We uncovered a relatively small network of 27 Facebook accounts, two Pages, three Groups, and four Instagram accounts targeting people in Ukraine across multiple social media platforms and through their own websites. This network used fake accounts and operated fictitious personas and brands across the internet — including on Facebook, Instagram, Twitter, YouTube, Telegram, Odnoklassniki, and VK — to appear more authentic in an apparent attempt to withstand scrutiny by platforms and researchers. These fictitious personas used profile pictures likely generated using artificial intelligence techniques like generative adversarial networks (GAN). We took down this operation, blocked their domains from being shared on our platform, and shared information with other tech platforms, researchers, and governments.

The fake accounts claimed to be based in Kyiv and posed as news editors, a former aviation engineer, and an author of a scientific publication on hydrography — the science of mapping water. This operation ran a handful of websites masquerading as independent news outlets, publishing claims about the West betraying Ukraine and Ukraine being a failed state.

Our investigation found links between this network and another operation we removed in April 2020 and connected to individuals in Russia, the Donbas region in Ukraine, and two media organizations in Crimea — NewsFront and SouthFront, now sanctioned by the US government.

- *Presence on Facebook and Instagram:* 27 Facebook accounts, two Pages, three Groups, and four accounts on Instagram.
- *Followers*: About 3,450 accounts followed one or more of these Pages and about 415 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around $200 in spending for ads on Facebook and Instagram paid for primarily in Russian ruble and US dollars.

4. Russia

We reported this enforcement as part of our CIB update on February 16, 2022.

We removed a small network of three Facebook accounts for violating our policy against coordinated inauthentic behavior. This network originated in Saint Petersburg, Russia and targeted primarily Nigeria, Cameroon, Gambia, Zimbabwe, and Congo.

The people behind this activity used fake accounts to create fictitious personas, posing as a media editor or as a Europe-based Arab-speaking executive at a PR agency. These accounts had profile pictures, likely generated using artificial intelligence techniques like generative adversarial networks (GAN). We saw two short periods of activity — both largely unsuccessful. First, this operation tried to solicit freelance help to write articles about Syria through the Arabic-language journalist Groups. After a period of inactivity, they appear to focus on Africa in an attempt to co-opt media outlets into publishing stories on their behalf about African politics, including criticism of French influence in Africa. We're notifying people who we believe have been contacted by this network.

We found this activity as part of our internal investigation into suspected coordinated inauthentic behavior with links to the activity we had disrupted in August 2020. Although the people behind it attempted to conceal their identities and coordination, our investigation found links to individuals associated with the past activity by the Russian Internet Research Agency.

- *Presence on Facebook:* three Facebook accounts.

04

Removing a mass reporting network in Russia

Under our Inauthentic Behavior policies, we remove mass reporting activity when we find adversarial networks that coordinate to abuse our reporting systems to get accounts or content incorrectly taken down from our platform, typically with the intention of silencing others.

Russia

We removed a network of about 200 accounts operated from Russia. The individuals behind it coordinated to falsely report people for various violations, including hate speech, bullying, and inauthenticity, in an attempt to have them and their posts removed from Facebook. The majority of these fictitious reports focused on people in Ukraine and Russia, but the network also reported users in Israel, the United States, and Poland.

The people behind this activity relied on fake, authentic, and duplicate accounts to submit hundreds — in some cases, thousands — of complaints against their targets through our abuse reporting tools. Many of this network's accounts were detected and disabled by our automated systems. Their coordinated reporting increased in mid-February, just before the invasion of Ukraine. Likely in an effort to evade detection, the people behind this activity coordinated targeting of mass reporting in their cooking-themed Group, which had about 50 members when we took it down.

We found this network as a result of our internal investigation into suspected inauthentic behavior in the region. Our review identified limited links between this activity and a network from Russia that we took down for CIB in 2019.

05

Removing a coordinated violating network in the Philippines

We remove coordinated violating networks when we find people — whether they use authentic or fake accounts — working together to violate or evade our Community Standards.

This primarily behavior-based enforcement complements our existing content policies, under which we already remove violating content and accounts violating our Community Standards, including incitement to violence, bullying and harassment or harmful health misinformation. We recognize that, in some cases, these content violations are perpetrated by a tightly organized group, working together to amplify their members' harmful behavior and repeatedly violate our content policies. In these cases, the potential for harm caused by the totality of the network's activity exceeds the impact of each individual post or account. To address these organized efforts more effectively, we've built enforcement protocols that enable us to take action against the core network of accounts, Pages, and Groups engaged in this behavior. As part of this framework, we may take a range of actions, including reducing content reach and disabling accounts, Pages, and Groups.

Philippines

We removed a network of over 400 accounts, Pages, and Groups in the Philippines that worked together to systematically violate multiple policies against coordinated harm, bullying and harassment, hate speech, misinformation, and incitement to violence, and evade enforcement.

The people behind this activity claimed to be hacktivists and relied primarily on authentic and duplicate accounts to post and amplify content about Distributed Denial of Service (DDoS) attacks, account recovery and defacing and compromising of websites in the Philippines. They commented about a DDoS attack against the sites of the Nobel Prize in December 2021 which

was confirmed to be unsuccessful, and accused public figures in the Philippines of being Communists (a tactic known as “red-tagging”).

This network claimed credit for bringing websites down and defacing them, primarily those of news entities. They also offered cyber security services to protect websites from attacks, like the ones they themselves claimed to have perpetrated. Finally, this group publicly invited new members to join and carry out DDoS attacks.

06

Removing inauthentic behavior

What is Inauthentic Behavior? While CIB is typically designed to mislead people about who is behind an operation to manipulate public debate for a strategic goal, Inauthentic Behavior (IB) is primarily centered around amplifying and increasing the distribution of content. It is often (but not exclusively) financially motivated, and shares many tactics with spam and scam activity.

How do we enforce against IB?

This year, we took down tens of thousands of accounts, Pages, and Groups around the world for engaging in inauthentic inflation of content distribution and abusive audience building. We rely on a range of enforcement levers against IB — from warnings, to reducing the distribution of content, to removing IB actors and clusters of activity from our platform (more in our Inauthentic Behavior report here).

IB operators typically focus on quantity, rather than the quality of engagement. For example, they may use large numbers of low-sophistication fake accounts to mass-post their content or to like it. They may also try to monetize people's attention by either driving them to off-platform websites filled with ads or selling t-shirts and other goods. In response to detection and removals, they typically try to aggressively reconstitute their activity. Because they so often work at scale, we counter IB through large-volume automated detection and enforcement, complemented by manual investigations to help us identify new tactics or gaps in detection.

This approach allows us to learn and improve our defenses in response to adversarial adaptation, while removing these clusters of activity at scale, no matter whether they aim to promote celebrity gossip or socio-political clickbait with an aim to amass an audience.

Here are some of the deceptive strategies we've seen IB operators use to artificially boost their engagement:

Context switching

IB operators often seek to mislead and grow their audience by claiming to be dedicated to one popular topic, then switching to another unrelated one when it becomes viral. They are well-attuned to their target audiences and will quickly pivot to post about the latest news or scandals to deceive people into clicking links to their sites. Unsurprisingly, politics has also become a common spammy lure. These activities can be and are often mistaken for politically-motivated influence operations at first glance, when in fact they are using political themes as another form of clickbait, similarly to celeb-bait or puppy memes.

For example, in the early stages of the war in Ukraine, we investigated a tip from a journalist and took down a network of Instagram accounts run from the US, some of which claimed to be reporting live from the front lines in Ukraine. They attempted to monetize, including by selling thematic merchandise through their website. After the Russian invasion began, this cluster quickly switched from posting about “scary driving” and “Airsoft videos'' to military themes. In another case, we took down a Page run from Vietnam that shifted from posting videos about “life hacks” and jewelry to posting about military hardware and the Ukraine conflict — all to drive people towards an off-platform website.

Posing as authentic communities in different countries

IB networks also often pretend to be based in one country, when in fact they’re operated out of a completely different one. This tactic often goes hand in hand with the “context switching” we described above. It includes foreign spammers and scammers flocking to any hot-button issue relevant in a particular country or region — like an election or socio-political crisis or natural disaster — to amass an audience and monetize their attention.

For example, multiple Vietnam- and Bangladesh-based spam clusters posed as supporters of the Canadian Trucker Convoy to cash in on people’s interest in this protest. In one case, they created Groups for convoy supporters or Facebook Pages designed to look like they were providing updates on the convoy, and then posted links to e-commerce websites or links to third-party affiliate marketing sites.

Mass posting, liking, and sharing content to make it appear more popular

Typically, IB actors rely on basic fake accounts to like, comment, or share content in an effort to create the false perception that the content is organically popular. In one case we investigated last quarter, a cluster of fake accounts created in Bangladesh appeared to have changed hands and been used as part of fake engagement efforts to comment on, like, and share content by the Page of a former US Senate candidate from Arizona.

This behavior may increase the number of likes and shares on the target posts, but our investigations over the years have found that it rarely, if ever, leads to actual engagement among real people. These amplification clusters often manifest as an engagement "bubble" or "click clique", where only its own members like and comment on each other's posts instead of real people outside that bubble.

In focus: Philippines election

As with any major civic event, we've seen IB operators from various countries, including the Philippines, Vietnam, US, and Thailand, become active on the margins of the upcoming Philippines elections in May, using the common IB tactics we described above. They appeared to focus on growing their audiences for either eventual monetization or to make their clients' content appear more popular than it really is.

Context switching

We've removed several clusters of activity that switched the focus of their Pages and Groups to the elections as they attempted to increase their following. In one case, a network included a series of Pages that shifted from non-political to political themes and, in some cases, shifted back to other unrelated topics. One Page that mainly shared non-political dance videos renamed itself to become "Bongbong Marcos news," while another Page that started off as supporting a politician later changed its name to "Your Financial Answer" and began posting loan advice. Among these clusters, we saw adversarial attempts to evade our automated name-change detection, including one Page that changed its name eight times over eight years, gradually shifting it from "History and Trivia Philippines" to focusing on particular political candidates.

Deceptive efforts to pose as authentic communities in different countries

We removed multiple clusters of activity from Vietnam, Thailand, and the US that posed as members of local communities in the Philippines in an apparent attempt to monetize people's attention on the election. In February, we identified a cluster of Pages operated by spammers in Vietnam who used VPNs to make it look like they are based in the Philippines. They posed as supporters of political campaigns or local news entities and used names like Philippines Trending News, Duterte Live, Related to Francis Leo Marcos, and Pinas News. They claimed to share live footage while purporting to be local news sources on the ground in an attempt to drive people to their clickbait websites filled with ads.

Inauthentic engagement

We identified several efforts to post at high, spam-like rates to drive people to particular Pages or off-platform websites. In one case, we found a social media management agency that used fake accounts and duplicate Pages to inauthentically amplify both political and entertainment content. The agency used a network of over 700 accounts to post, share, and comment on posts and share content through large Groups.

In other cases, we found and removed inauthentic engagement activity run by the same people in support of multiple candidates in the same election at once. In the lead-up to the elections, we've taken down about a dozen clusters of activity focused on fake engagement.

We're continuing to closely monitor the situation in the lead-up to the May election in the Philippines and will take action if we find violating activity attempting to leverage people's interest in the election using IB tactics.

Appendix: Threat indicators

1. UNC788, Iran

Domains & C2s

- bnt2[.]live
- archery.dedyn[.]io
- market.vinam[.]me
- signin.dedyn[.]io
- Market.dedyn[.]io

Hashes

- 43535540e94b39279af925e9548dce7f
- 9b91427d195b8b7e75fbbc29a798bede
- aaa55f1e48aba8856661fedc0074e81a
- 6e0ec6bd0bef489c83c2dce4876de5c8
- 70875705e8bc3887cec4ef1873cdb152
- aa7330d2d360cac61394843d8af730bb
- ab533be4ff9c99e8a03bc4cd413badb6

Yara rule

```
rule hilal_rat_dex: {
  meta:
    source = "Facebook"
    date = "2022-04-07"
    description = "Detects custom android rat impersonating various
applications that siphons phone details to a C2."
  strings:
    $class0 = "Lcom/hilal/SysUpdater/MainActivity;"
    $class1 = "Lcom/hilal/adm/R;"
    $file0 = "cacaca.dat"
    $file1 = "ccc.dat"
    $file2 = "fifi.dat"
    $file3 = "smr.dat"
    $file4 = "smse.dat"
```

```
    $typo0 = "Erron in Decryption"
    $typo1 = "GetDevcie"
    $sec1 = "6123cc12ef9bd0bf1592c69bf769853fb0a00084" // AES key
    $cmd0 = "/Aud"
    $cmd1 = "/Cam"
    $cmd2 = "/Upd"
    $cmd3 = "/Con"
    $func1 = "CamStart"
    $func2 = "AudStop"
    $func3 = "AudStart"
    $func4 = "DownFi"
    $func5 = "ScrSht"
    $func6 = "CamList"
    $func7 = "CamStop"
    $func8 = "ListExplore"
    $interesting_string0 = "isMyServiceRunning?"
    $interesting_string1 = "Checking new version... Please wait..."
    $notification_service0 = "**********  onNotificationPosted"
    $notification_service1 = "********** onNOtificationRemoved"
    $phnum = "PhNumber"
  condition:
    filetype_dex and
    10 of them
    or all of ($file*)
    or all of ($func*)
    or all of ($interesting_*) and all of ($notification_*)
}
```

2. Previously unreported group (Iran)

Domains & C2s

- alharbitelecom[.]co
- apply-jobs[.]com
- applytalents[.]com
- appslocallogin[.]online
- careers-finder[.]com
- cloudgoogle[.]co
- cortanaservice[.]com
- cortanaupdate[.]co
- defenderupdate[.]ddns[.]net
- edge-cloudservices[.]com
- elecresearch[.]org
- enerflex[.]ddns[.]net
- enerflex[.]org
- etisalatonline[.]com
- exprogroup[.]org
- freechess[.]live
- funnychess[.]online
- getadobe[.]ddns[.]net
- getadobe[.]net
- globaltalent[.]in
- googleservices[.]co
- googleupdate[.]co
- helpdesk-product[.]com
- khaleejtimes[.]co
- librarycollection[.]org
- linkedinz[.]me
- listen-books[.]com
- lukoil[.]in
- mastergatevpn[.]com
- microsoftcdn[.]co
- microsoftdefender[.]info
- microsoftedgesh[.]info
- mideasthiring[.]com
- office-shop[.]me
- onedrivelive[.]me
- onedriveupdate[.]net
- online-audible[.]com
- online-chess[.]live
- outlookde[.]live
- outlookdelivery[.]com
- remgrogroup[.]com
- saipem[.]org
- sauditourismguide[.]com
- savemoneytrick[.]com
- sharepointnotify[.]com
- sparrowsgroup[.]org
- supportskype[.]com
- talent-recruitment[.]org
- talktalky[.]azurewebsites[.]net
- thefreemovies[.]net
- updateddns[.]ddns[.]net
- updatedefender[.]net
- updatedns[.]ddns[.]net
- updateservices[.]co

3. Azerbaijan

Domains

- localadmin[.]online
- localadmin[.]ru
- analyzeryandex[.]000webhostapp[.]com
- vote2021[.]w3spaces[.]com

Credential phishing URLs

- localadmin[.]online/votes/security
- localadmin[.]online/vote
- localadmin[.]online/vote/fb/login.html

4. CIB: Costa Rica, El Salvador

Domains

- latinoamericareporta[.]com
- revistadcr[.]com

5. CIB: Russia, Ukraine

Domains

- kavkazru[.]press
- politica[.]in[.]ua

6. CIB: Russia, Ukraine

Domains

- monitor-ua[.]com
- ukraine2day[.]com