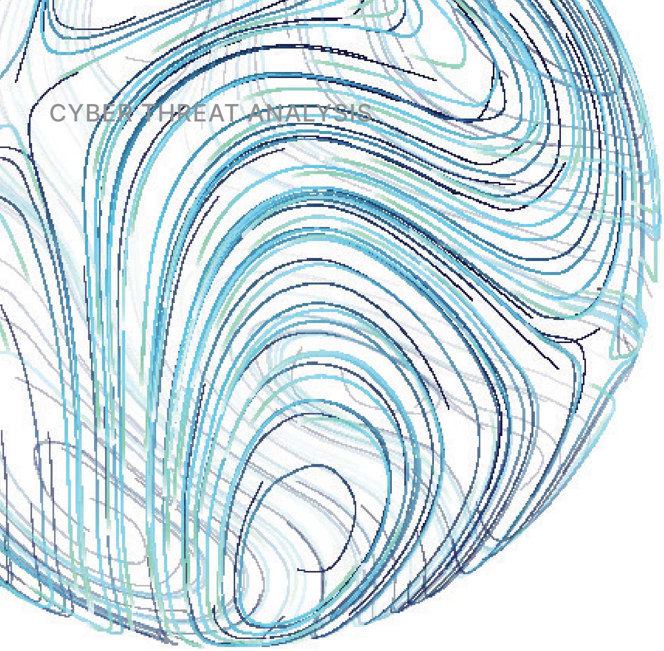
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0302

Cyber Threats to the Black Community



To honor Black History Month, Insikt Group partnered with BEST@RF (Black Empowerment and Support Team) — an employee resource group at Recorded Future that advocates for Black and ethnic minority employees — to conduct research into cyber threats facing the Black community within the United States. The goal of this research is to raise awareness and visibility, as well as provide practical recommendations to aid the Black community in battling the threats they face as a result of systemic racism.

Executive Summary

The Black community is often more heavily impacted by health or financial crises than other groups as a result of large racial wealth gaps stemming from centuries of systemic racism. The ongoing COVID-19 pandemic has been a glaring example of this, as Black Americans, when factoring in age, are more than twice as likely to have died from COVID-19 than White Americans. Applying this context to the cyber threat landscape, Insikt Group investigated a wide array of cyber threats over the last 6 years, including fraud, malware campaigns, and disinformation operations, for evidence of disproportionate or intentional targeting of the Black community by cybercriminals, state-sponsored groups, or nation-affiliated threat actors.

Key Judgments

- Members of the Black community are highly impacted by fraud campaigns compared to other racial and ethnic groups, as disparities in financial literacy and wealth are large barriers to recovering from any resulting financial loss.
- The use of phishing lures based on trending current events extends to social justice movements such as Black Lives Matter. Threat actors will continue to use the movement to victimize users as long as it is lucrative.
- The infrastructure of organizations advocating for racial justice and equality are frequently targets for distributed denial of service attacks. The volume of attempted cyberattacks against these organizations is highly correlated with trends in racial justice movements, as evidenced by a surge in cyberattacks following the murder of George Floyd in May 2020 and subsequent protests.
- Foreign information operations have targeted the Black community since at least 2015 and will likely continue to do so in order to create division and political unrest and undermine political leadership.

The Impact of Fraud in Majority Black Communities

Past research has indicated that minority groups are more likely to fall victim to fraud. A 2004 Federal Trade Commission report indicated that Hispanic and African Americans[1] were more than twice as likely, and American Indians and Alaskan Natives were more than five times as likely, to be victims of fraud compared to White Americans. While these statistics represented all forms of fraud, the findings continue to apply in more recent studies of victimization in online scams.

In June 2020, Federal Trade Commission economist Devesh Raval published a study based on fraud cases handled by the Federal Trade Commision (FTC) between July 2016 and April 2020. The analysis showed a correlation between victimization rates and areas with high Black populations. Areas with a 100% Black population have a 116% higher victimization rate than those with a 0% Black population. The racial gap is even larger for income scams masquerading as payday loans or student debt relief, with victimization rates increasing by 209% and 190%, respectively. The study points out that despite this, victimization rates in majority-Black communities decline as the dollar loss amount rises (see Figure 1). Majority-Black communities are overrepresented by 45% in scams where the average loss was less than $500, compared to 10% overrepresentation when the average loss was over $500. This is likely in large part a result of the fact that Black Americans on average have a lower net worth and less access to credit compared to other racial or ethnic groups, and thus fewer resources to hand over to a threat actor.

[1] Insikt Group generally uses the term “Black” to describe people of African descent, but in some cases will reference “African Americans” when that is the specific demographic indicated in an original source of research or if it is otherwise applicable.

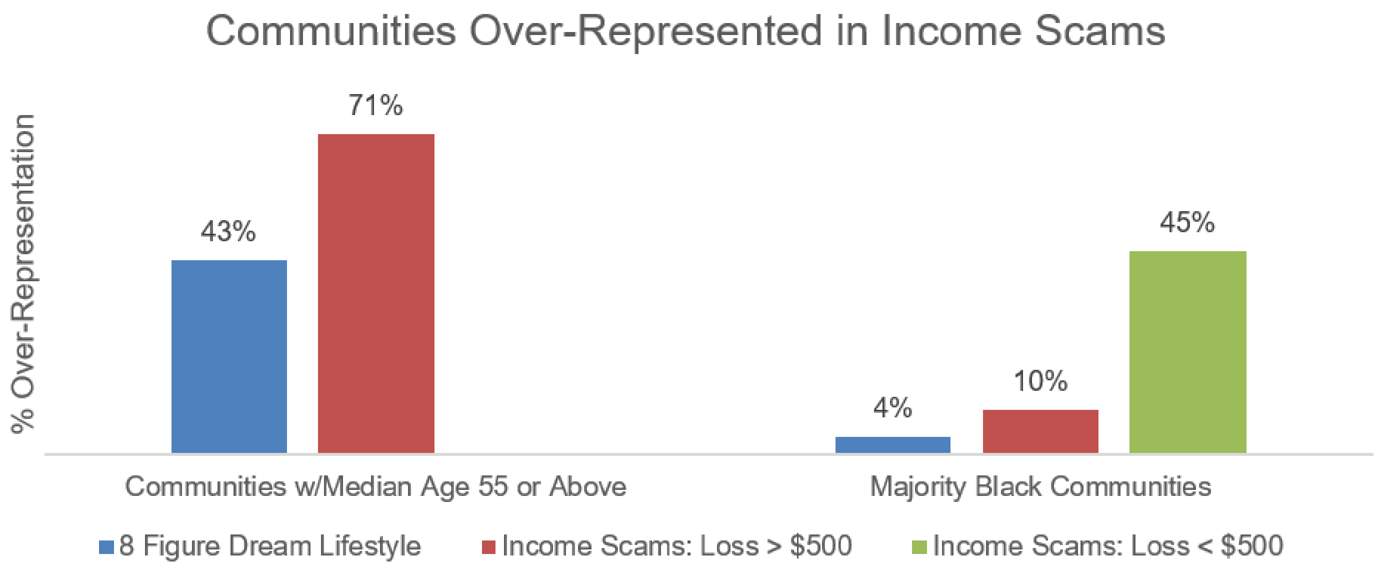


Figure 1: Overrepresentation of communities as victims of income scams. "8 Figure Dream Lifestyle" is a specific income scam referenced in the source FTC article (Source: Federal Trade Commission)

Although recent statistics indicate that higher-income, non-minority households in the United States are more likely to be victims of identity theft (as victims with greater access to credit and more banked funds are prized by cybercriminals), minorities and low-income citizens are often victimized as well. Lower-income individuals are potentially less able to overcome the effects of this form of fraud than those with greater time and funds at their disposal to resolve the resulting issues; a 2001 US Congressional hearing heard testimony that victims typically required 175 hours, the equivalent of 4 working weeks, to fully resolve identity theft problems.

The impact of fraud campaigns on the Black community is further compounded by socioeconomic barriers that make it more difficult for them to recover after victimization. A study of fraud victim complaint behavior showed that as the percentage of Black residents in an area rises from 0% to 100%, the complaint-to-victim ratio falls by 61%. This is likely due to a combination of issues with trusting government entities and financial literacy. Black Americans have historically had lower levels of trust in the US government compared to other racial or ethnic groups. A financial literacy, wellness, and resilience survey conducted by TIAA Institute in 2019 demonstrated a 17% lag in financial literacy among African Americans compared to White Americans. Consequently, many Black Americans may either lack the confidence or awareness to report an instance of fraud, or even avoid reporting out of distrust of law enforcement or other government agencies. Additional data from the TIAA survey showed that only 35% of African Americans believed they could cover a $2,000 emergency expense — compared to 59% of White Americans — making any financial loss due to fraud even more detrimental.

Additional information about fraud methods and services can be found in this recently published Insikt Group report, the first installment in a series on cybercriminal fraud. In the coming months, Insikt Group will publish in-depth reports on 11 fraud methods or services, the threat actors offering them, technical details where applicable, and mitigation recommendations.

Malware Operators Targeting Black Users and BLM Activity

Threat actors routinely capitalize on current events trending in the media by using them as lures in phishing campaigns to catch the attention of potential victims. In Q2 2020, COVID-19-themed malware and lures continued to be used in a similar fashion to Q1 2020; however, analysts observed tactics, techniques, and procedures (TTPs), specifically associated with Trickbot variants, that demonstrate threat actors' ability to evolve as world events and media attention shift. While analysts observed continued use of the COVID-19 theme in Trickbot lures throughout Q2 2020, analysts also observed the malware's operators shift tactics, taking advantage of the Black Lives Matter (BLM) protests that escalated in June 2020.

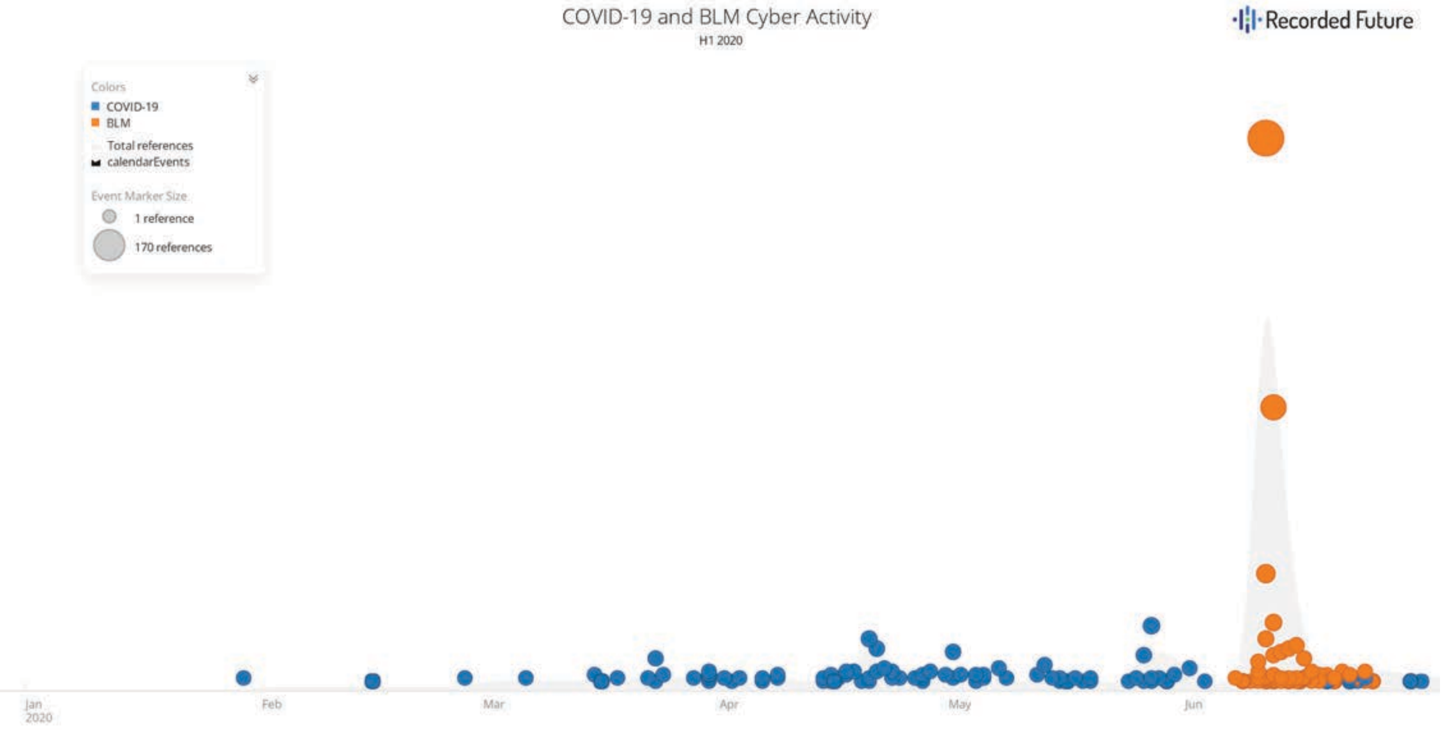


Figure 2: COVID-19 cyber events and BLM cyber events in H1 2020
(Source: Recorded Future)

Figure 2 illustrates the change in tactics that threat actors took in June when the BLM protests began following the murder of George Floyd — threat actors began to shift their phishing lures from COVID-19 themes to BLM themes. Trickbot is an advanced banking trojan that attackers use to steal payment credentials from victims. On June 10, 2020, Swiss security firm Abuse.ch identified a Trickbot malware sample delivered via an email with the subject line "Subject: Speak out anon about Black Lives Matter". On June 26, 2020, Trickbot samples delivered from a malspam campaign using the subject "Black Lives Matter" as a lure were shared on social media. The "e-vote" themed DOC files contain embedded macros that, when enabled, launch a document exploit to download files from malicious URLs.

The operators of Babuk Locker — a ransomware family that first surfaced in early January 2021 — have also stated that while they generally do not target non-profit organizations, this policy does not apply to organizations that support BLM or the LGBTQIA+ (Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, Asexual) community. While initial infection vectors for Babuk Locker have not been confirmed, it is very likely that the malware is distributed via phishing emails, which remains one of the main methods of distribution for ransomware operators.

Security teams should educate employees on new and emerging TTPs used by threat actors, especially emails with themes related to worldwide events, as they could be the initial entry point of a major network compromise.

Cyberattack and Information Operations

Distributed Denial of Service Activity Targeting Black Lives Matter

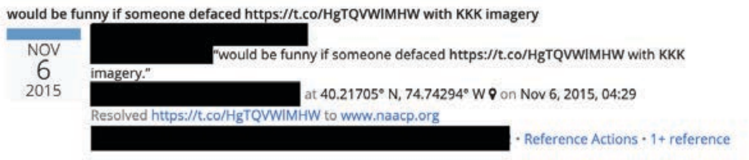
The official BLM website, blacklivesmatter[.]com, has been repeatedly targeted by distributed denial-of-service (DDoS) attacks following its registration in late 2014. In 2016, ArsTechnica reported that blacklivesmatter[.]com was targeted shortly after establishing a relationship with eQualitie, "a Canadian not-for-profit organization that gives digital support to civil society and human rights groups". According to a December 2016 report from eQualitie, there were "more than a hundred separate denial-of-service incidents against the official Black Lives Matter website" in the seven-month period between April and October 2016. Analysis of the DDoS activity by eQualitie indicated that there was not one consistent DDoS attack type but rather a variety of methods, likely employed by various groups who were "jumping on board in response to callouts made on social media and covert channels". eQualitie further indicated that some of these efforts, specifically those employing Joomla and WordPress reflection attacks, were likely coordinated. Efforts, like the April 2016 DDoS attack launched by threat actor "_s1ege" with the Black Horizon software, were claimed by Ghost Squad Hackers, whereas activity conducted by "bannedoffline", who employed WordPress reflection attacks coordinated from machines hosted by bulletproof providers and targeted the BLM website in May 2019, were not directly affiliated with a specific threat group. Overall, eQualitie indicated that the primary TTPs conducted during the observation period included the use of open-source denial-of-service tools like Slow Loris, GoldenEye, and Black Horizon, reflection-type attacks using WordPress and Joomla, and HTTP floods.

In June 2020, the DDoS mitigation and information security company Cloudflare reported that, in the days that followed the murder of George Floyd, the company "saw a large uptick in cyberattacks, particularly cyberattacks on advocacy organizations fighting racism". According to the report, Cloudflare indicated that the work to block incoming HTTP traffic requests amounted to tens of billions of requests per day and constituted an average increase from the month prior of about 20%. The greatest volume of traffic occurred on Sunday, May 31, 2020 with "26% more cyberattacks than the same Sunday a month prior". Cloudflare indicated that advocacy groups fighting for racial justice and equality were the most frequently targeted resources with government websites, such as police and fire departments, as well as military websites also seeing significant increases from the month prior.

Although there is no attribution for the DDoS activity aimed at advocacy groups, government, and military websites, Cloudflare indicated that one attacker, likely using a hacked server in France, was especially persistent, hitting an advocacy group continuously for over a day. Cloudflare blocked those malicious HTTP requests and kept the site online.

Online Threats and False Claims

In addition to DDoS attacks, there were instances of online threats, specifically threats of defacements against Black organizations dating back to 2015. On November 6, 2015, a now-suspended social media account shared a post that suggested that it would be "funny" if someone defaced the website of the National Association for the Advancement of Colored People (NAACP) with racist imagery.



would be funny if someone defaced https://t.co/HgTQVWlMHW with KKK imagery

NOV
6
2015

[redacted] "would be funny if someone defaced https://t.co/HgTQVWlMHW with KKK imagery."

[redacted] at 40.21705° N, 74.74294° W on Nov 6, 2015, 04:29

Resolved https://t.co/HgTQVWlMHW to www.naacp.org

[redacted] · Reference Actions · 1+ reference

Figure 4: Post from a now-suspended social media account suggesting that it would be "funny" if someone defaced the NAACP website with racist imagery (Source: Recorded Future)

In addition to social media threats, the NAACP was also subjected to false claims, distributed via social media. A January 13, 2021 NAACP post indicated that their organization became aware of claims online that suggested "the NAACP has received information about white nationalist groups initiations during the weekend after the [2020 US Presidential] election, and previously during the fourth of July weekend". The NAACP indicated that the false claim appeared to have been distributed by the Huey P. Newton group, a gun rights organization that has no affiliation with the NAACP.

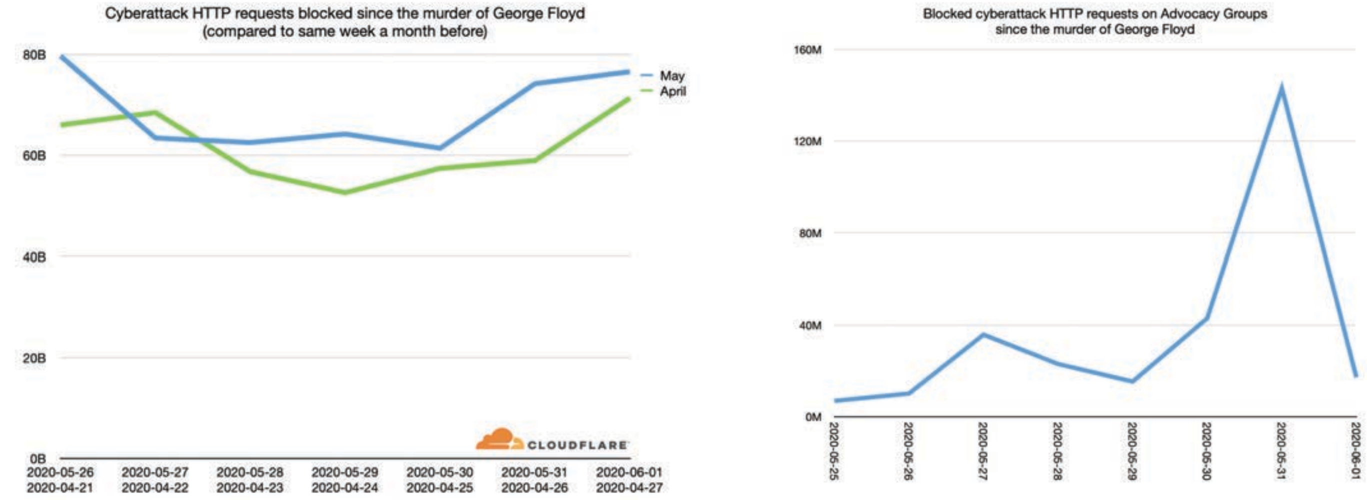


Figure 3: (Left) Month-over-month comparison of DDoS activity aimed at racial advocacy groups, and (right) the increase in the targeting of these same groups following the murder of George Floyd (Source: CloudFlare)

Foreign Disinformation Targeting Black Communities

Foreign information operations (IO) and disinformation campaigns targeting the Black community in the US have been conducted from abroad with identified, online campaigns conducted by Iranian and Russian state-linked entities. These campaigns can be traced back to at least 2015 and continued through 2020. More broadly, we identified the following patterns:

- Foreign threat actors, some with potential nation-state backing, have co-opted social media to distort or amplify content impacting Black communities, such as the BLM movement, police violence, and racial identity to divide or antagonize, as well as to depress voter turnout among Black communities.
- Foreign state-sponsored media outlets in Iran, China, and Russia reported on issues impacting Black Americans, particularly the BLM movement and prominent individuals killed by police in 2020, including George Floyd and Breonna Taylor. A sentiment analysis conducted on these foreign reports over the last year indicate a largely neutral-to-negative tone.
- Kremlin-aligned or Russia state-backed overt and covert disinformation organizations have been very active in targeting Black American communities, and have been so since Soviet times. Iranian-based threat actors and state-sponsored media have been active on social media throughout 2020 in engaging in coordinated inauthentic behavior against Black communities. Chinese state-sponsored media and threat actors have been less active than Russian or Iranian groups and media outlets, but have produced neutral-to-negative coverage of events impacting Black communities in 2020.

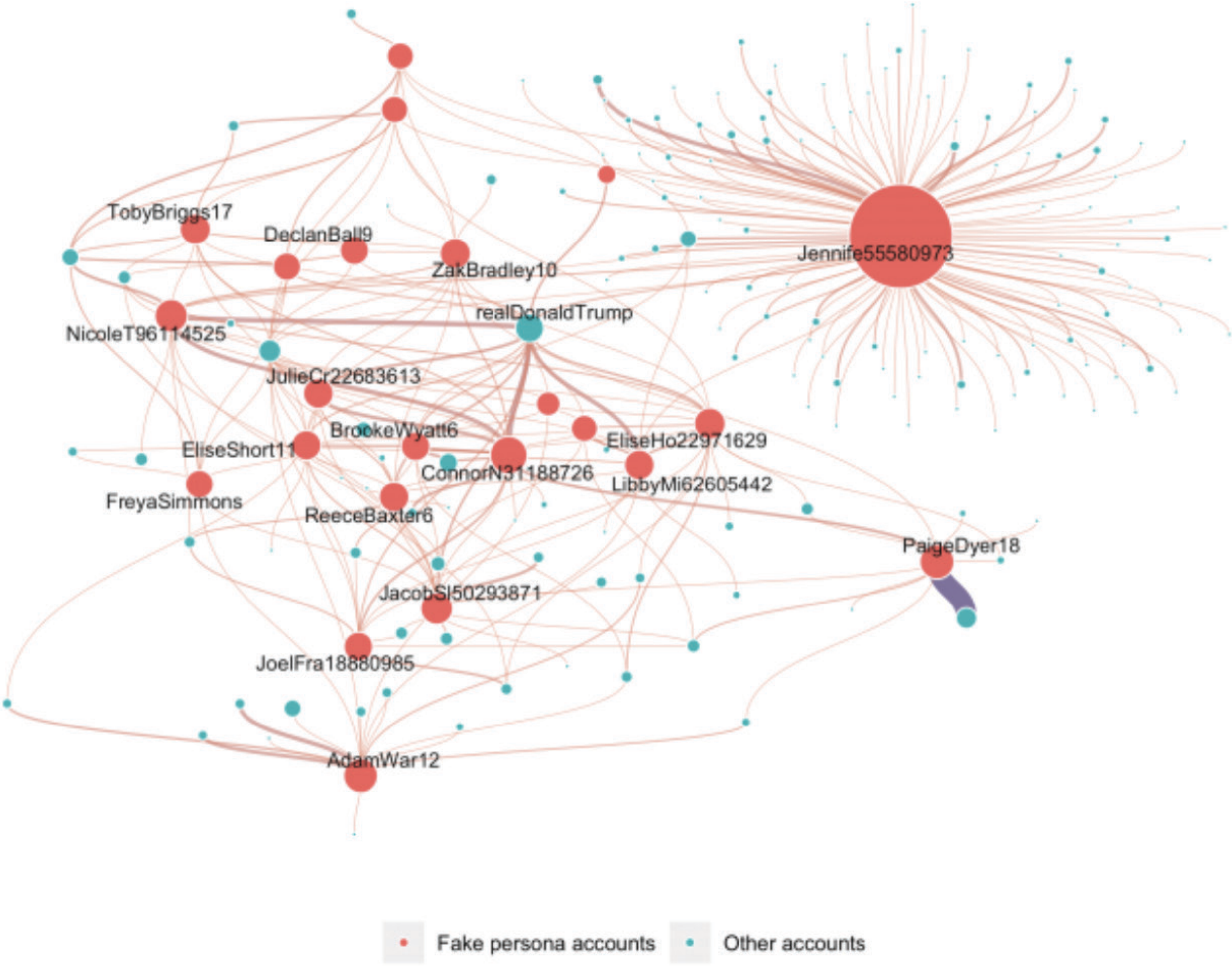


Figure 5: Interactions between fake personas and other accounts
(Source: Stanford Internet Observatory)

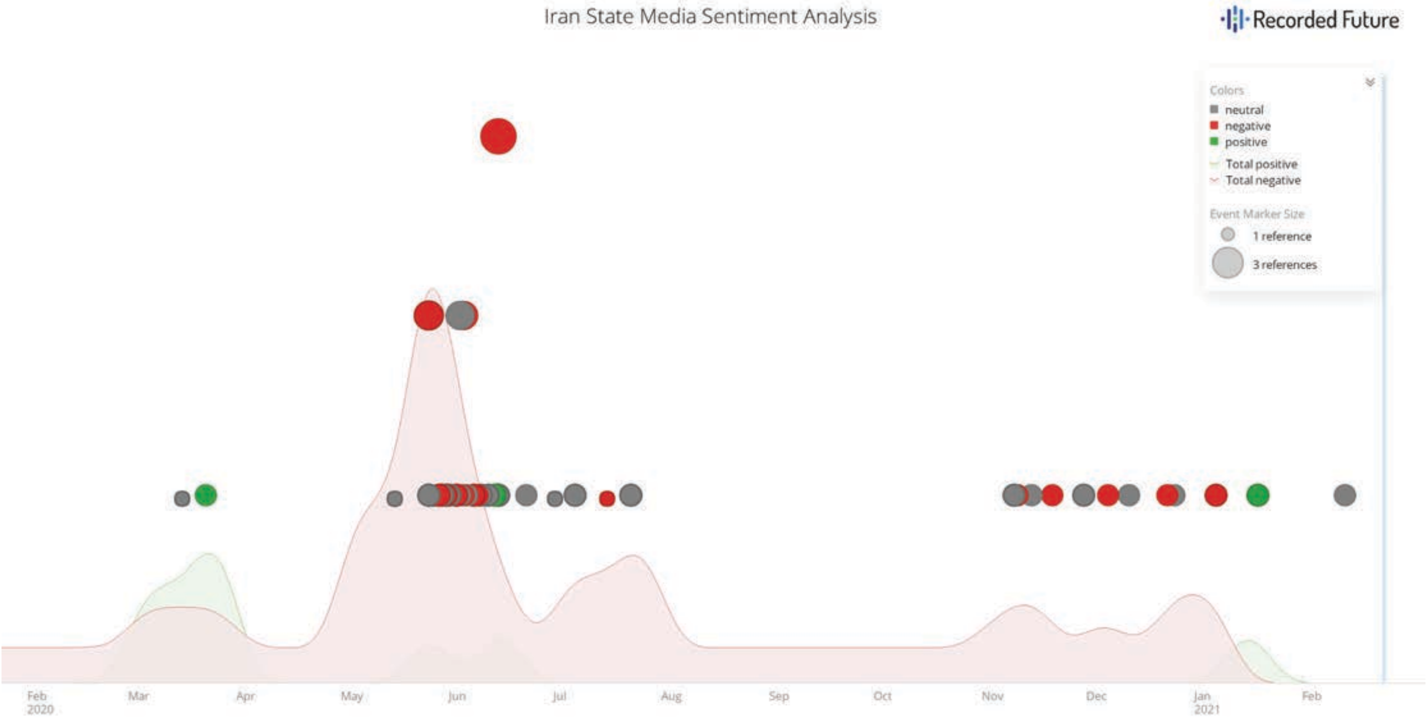


Figure 6: Sentiment analysis of Iranian state-sponsored media sources discussing the BLM movement, and the killings of prominent Black individuals in 2020 and 2021 (Source: Recorded Future)

Iran

On October 8, 2020, the Stanford Internet Observatory described a campaign attributed to Iran in which threat actors hijacked existing social media accounts and created fake accounts with stolen data from existing accounts to distribute content and narratives associated with BLM. The campaign was initiated around or before January 2020, operated primarily in English and Arabic, incorporated images and memes in their content, and employed hashtags, such as #black_lives_matter, likely in an attempt to increase visibility. The Stanford Internet Observatory indicated that the majority of the operation employed stolen accounts which interacted with the fake accounts; both sets of account networks also attempted to reach out to outside users and prominent figures online, such as then-President Donald Trump. According to the Stanford Internet Observatory, "The majority of the fake accounts stole their bios from real accounts on [social media], most of which were from users located in the United Kingdom. The bios from real accounts ranged from those of government officials, to a primary school teacher, to TV presenters and journalists. A majority of the real accounts that bios were stolen from had large followings (the largest had 508,800 followers), though some were relatively small (101 followers)".

In addition to content that was supportive of BLM, memes, and images shared by these accounts some of the false personas — specifically those that claimed to be journalists — shared links to various news stories without adhering to a specific theme. The Stanford Internet Observatory concluded that the totality of the activity suggested that the operation was relatively small in scope, in its nascent stages when it was disrupted, and failed to have a "significant impact". However, it also suggested that this is not the first instance in which Iranian-linked threat actors attempted to employ themes relating to the Black community to "to denigrate American society and political leaders". Based on the findings relating to this activity, it is likely that future efforts by Iranian state-sponsored threat actors may employ similar approaches to information operations.

We found approximately 180 references on the Recorded Future Platform in Iranian state-sponsored media to the BLM movement, as well as to prominent individuals killed by police, in 2020 and 2021. Sentiment analysis showed that most of these 180 references were either neutral or negative in tone.

Russia

Russian state-sponsored "active measures" campaigns, disinformation, and information operations have been ongoing (1, 2) since the Soviet era. Aspects of these operations rely on the exploitation of sensitive social issues to exacerbate existing divisions, and Russian state-sponsored operations have persistently and continually targeted Black communities within these efforts.

A US Senate Intelligence Committee report on Russian active measures campaigns and interference in the 2016 US election provides some insight into how Russia's Internet Research Agency (IRA) developed accounts and targeted Black communities. Specifically, the report stated the following: "No single group of Americans was targeted by IRA information operatives more than African Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016". According to the report, content posted to social media tended to focus on socially contested issues such as racial justice protests by National Football League (NFL) players or human rights concerns relating to police brutality. The IRA accounts would establish personal and organizational accounts on either side of such issues and attempt to increase polarization through the use of emotionally charged rhetoric, evocative images, and memes.

The Senate Intelligence Committee report revealed that 4 of the top 10 social media accounts on image sharing websites were overtly premised around the Black cultural issues, community, or interests. Collectively, these 4 accounts had more than 769,126 followers on 1 platform alone, with the top account among these generating "over 28 million interactions".

In addition to the apparent effort to generate divisive attitudes in relation to racial issues, the accounts controlled by the IRA posted content that appeared designed to disenfranchise Black voters. According to a University of Wisconsin research study published in September 2018, "clear evidence exists that the IRA operated voter suppression campaigns. It deliberately targeted nonwhite voters, especially African Americans, by promoting their racial/ethnic identity early on, but attempted to suppress votes when closer to the election". The voter suppression effort was not only limited to 2016 but also extended to the 2020 US presidential election, as evidenced by an October 2020 NPR report, which indicated that widespread campaigns "to depress turnout among people of color by fueling cynicism and distrust in the political process" increased in advance of the November 2020 election.

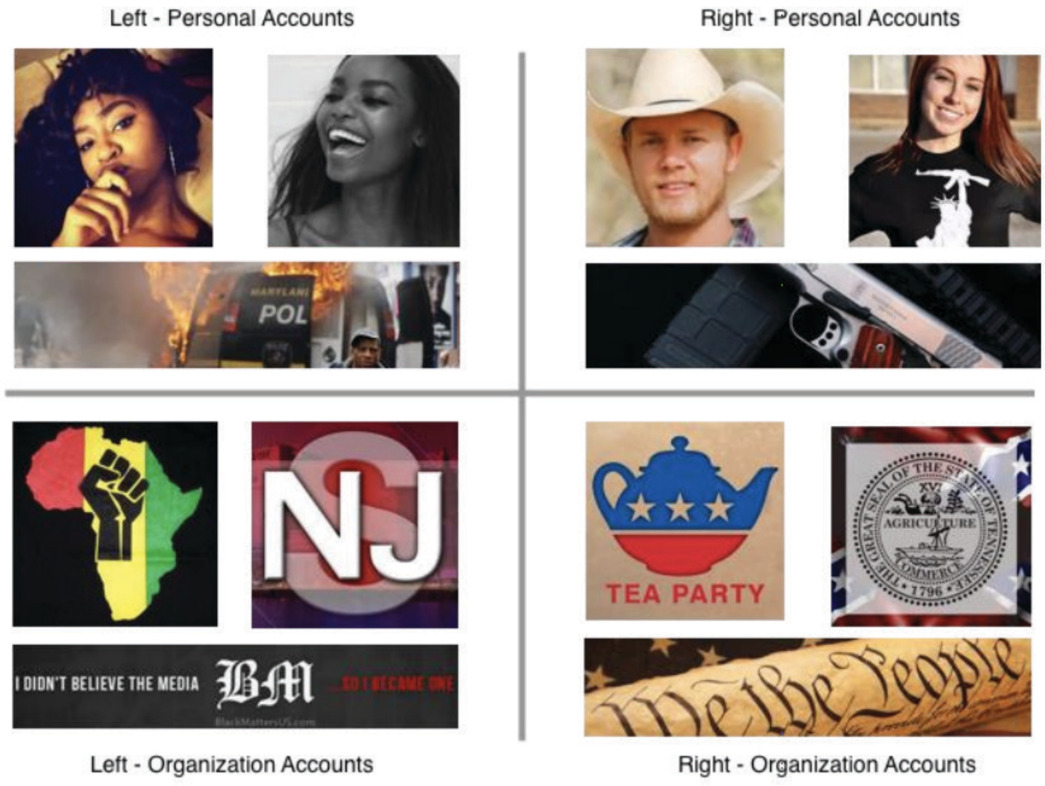

Left - Personal Accounts
Right - Personal Accounts
MARYLAND
POL
NJ
TEA PARTY
I DIDN'T BELIEVE THE MEDIA
BM
...SO I BECAME ONE
BlackMattersUS.com
We the People
Left - Organization Accounts
Right - Organization Accounts

Figure 7: Example of some of the approaches to imagery featured on IRA accounts which aligned themselves on either side of the racial spectrum (Source: University of Washington)

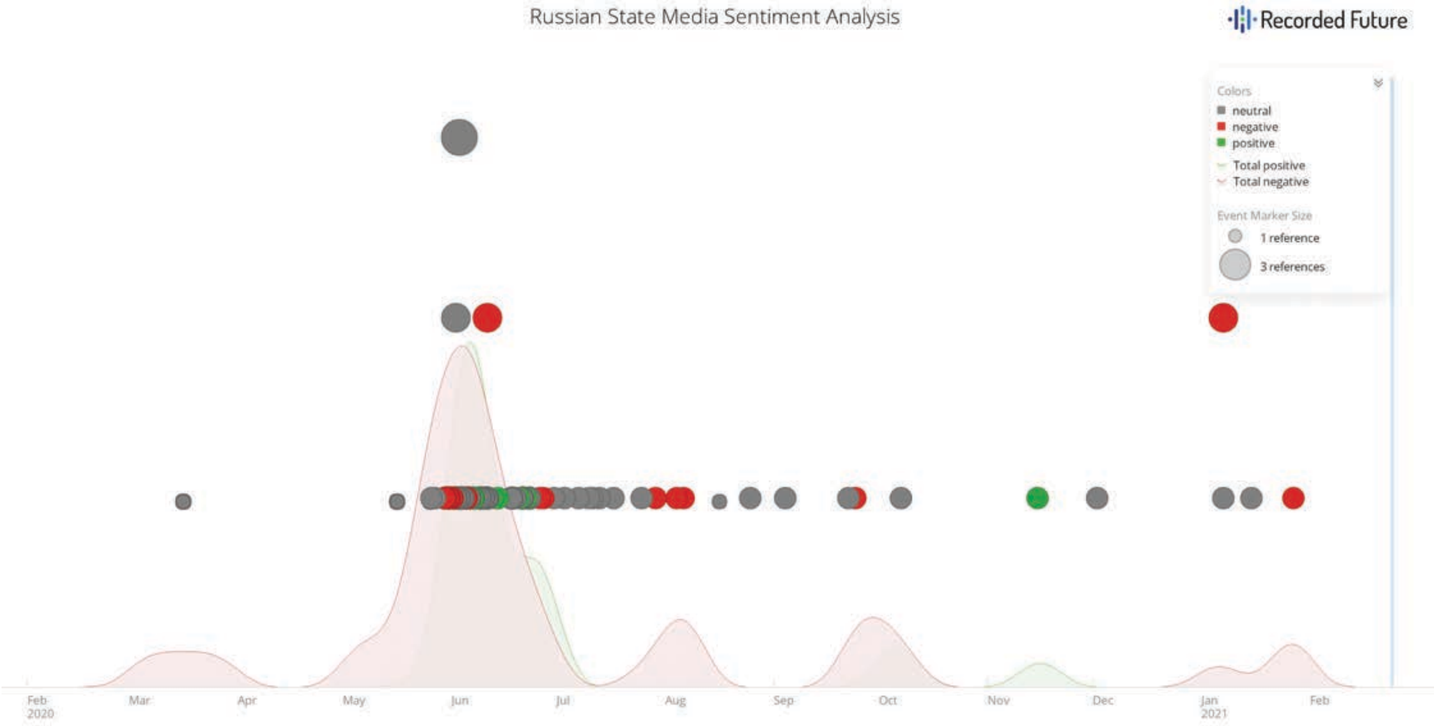


Figure 8: Sentiment analysis of Russian state-sponsored media sources discussing the BLM movement, and the killings of prominent Black individuals in 2020 and 2021 (Source: Recorded Future)

Since February 2020, there have been over 7,000 references in Russian state-sponsored media, fringe websites, and disinformation websites discussing the BLM movement, as well as the murders of George Floyd and Breonna Taylor. The overwhelming majority of these articles appeared on the Russian state-sponsored media outlet, RT.

Sentiment analysis of the approximately 7,000 references observed in Russian state-sponsored media showed a largely neutral or negative sentiment towards the BLM movement and prominent individuals killed by police in 2020 and 2021.

China

Over the course of the last year, there were over 2,400 references found on the Recorded Future Platform in Chinese state-sponsored media discussing the BLM movement, as well as the murders of George Floyd, Breonna Taylor, and prominent individuals killed by police in 2020 and 2021.

Sentiment analysis of the approximately 2,400 references across Chinese state-sponsored media showed that the vast majority of references to the BLM movement and prominent individuals who were killed by police officers between 2020 and 2021 was neutral or negative, with few positive mentions.

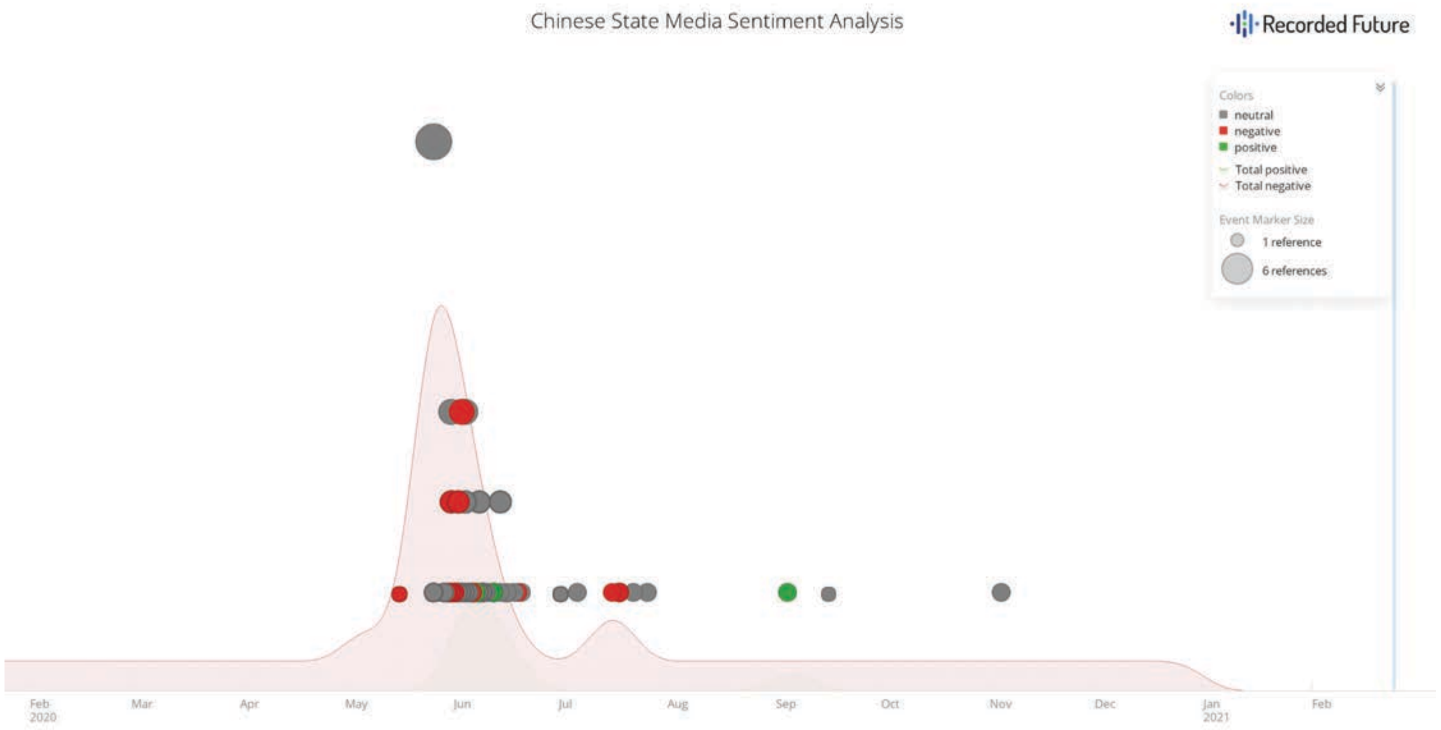


Figure 9: Sentiment analysis of Chinese state-sponsored media sources discussing the BLM movement, and the killings of prominent Black individuals in 2020 and 2021 (Source: Recorded Future)

Outlook

Fraud and resulting financial loss will continue to disproportionately impact members of the Black community as long they face socioeconomic disadvantages resulting from systemic racism. Threat actors have demonstrated that they have no qualms with targeting or victimizing any marginalized individual or community and will continue to do so. While these threats are very unlikely to decrease without systemic actions from both federal and local governments, Insikt Group wants to empower members of the Black community and allies to take ownership of their security wherever possible.

Users should also be vigilant in securing all online accounts by using long, complex passwords and multi-factor authentication. Users should also make sure passwords across accounts are unique and change passwords periodically. Password managers, such as LastPass, can help facilitate all of these security measures.

Members of the Black community and allies should take full advantage of free educational resources such as those provided by the FTC related to fraud, phishing, and general best practices for privacy, identity, and online security. Users should also report any income scams or fraud victimization to their financial institutions and local law enforcement. US-based users can submit reports to reportfraud.ftc.gov, a new fraud reporting platform launched by the FTC in October 2020.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.