REPORT

McAfee
Together is power.

McAfee Mobile Threat Report

Pandemic Fears and Mobile Banking Are Popular Malware Targets

McAfee Mobile Threat Report 2021

Banking, Billing Fraud, and COVID-19 Vaccines Are Popular Malware Targets

Mobile malware authors want their malicious code and fake apps to be downloaded and are **constantly testing the waters to see what lures in the most people**. They also need some way to monetize their efforts, to pay for rent, food, and internet access. So, the continued use of banking Trojans, billing fraud, and adware does not come as a major surprise. What is new are the different methods that these bad actors are trying to get apps and malware around or through the security screening of the application stores.

To avoid security screening, many malware authors try to distribute their apps via SMS messages or links on popular social media sites. Others are writing apps with minimal but legitimate functionality, **inserting malicious code during an update when scrutiny is lessened**, and then downloading additional encrypted packages to obfuscate the real malware. They are also learning to abuse features in mobile device operating systems that give them access beyond the intended purpose, such as accessibility services and messaging controls. Operating system developers are continuing their efforts to track down these abuses, restrict usage, limit functionality, and otherwise minimize the opportunity for misuse.

In this edition of our mobile threat report, we take a closer look at some of the popular targets of mobile malware and malicious actors. Global interest in COVID-19 information and vaccinations has prompted bad actors to jump on this bandwagon, to see how many they can **trick with fake apps dressed up in real health department logos**. Others are returning to SMS billing scams but using new tricks to read messages. Finally, one group tried to make money by selling their malware code via auction, only to have the code end up on the web for free.

We hope this provides a useful resource for protecting your mobile devices and personal information and welcome your feedback.

Carlos Castillo
McAfee Manager, Security Research

Raj Samani
McAfee Fellow, Chief Scientist

Authors

This report was researched and written by:

- **Carlos Castillo**
- **Raj Samani**
- **Contributions from the McAfee Advanced Threat Research and Mobile Malware Research team**

Connect With Us

Don't Fall for a Fake Shot

With most of the world still anxious about COVID-19 and getting vaccinated, cybercriminals are targeting these fears with bogus apps, text messages, and social media invitations. Malware and malicious links hidden inside these fakes display ads and try to steal banking information and credentials.

Some of these campaigns started as early as November 2020, before any shots had been officially approved, while others **continue to appear as countries roll out their vaccination programs**. The good news is that these malware campaigns must be customized for each country or region to be effective. This increases the level of discipline and work required, and we expect to see these mostly directed to larger population groups where the potential payoff is worth the additional effort.

SMS Worm Targeting India

One of the earliest coronavirus vaccine fraud campaigns was recorded in India in November 2020, before any vaccines had been approved in the country. This operation started with **SMS and WhatsApp messages that encouraged users to download an app** to apply for the vaccine. Once downloaded, the app displays a simple screen asking for the user's mobile number. The malware behind this is the same family that was involved in India's ban on the Tik-Tok app last July. Once it has been downloaded, this malware sends itself to everyone in the user's contact list via SMS or WhatsApp. Then it continues to display unwanted and fraudulent advertisements to anyone who installed it. The Indian Ministry of Health and Family Welfare are running an active campaign to caution people about this and other fake vaccination apps and messages. The CoWin app on the Google Play store is only meant for healthcare officials. Indian citizens should go to the Ministry's **Co-WIN Portal** or **vaccination information page** to register themselves and book appointments.

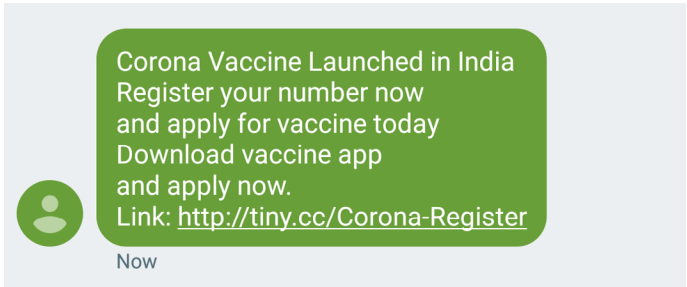

Figure 1. Example of fake COVID-19 vaccine registration SMS message

FAKE VACCINE APPS

What is it?
Fake apps, text messages, and social media invitations for COVID-19 vaccine appointments and registration

Current threats
- Downloads malware that displays unwanted ads
- Forwards itself to user's contact list
- Activates accessibility features for full device control
- Missing out on legitimate vaccine registration or appointment

Future threats
- COVID-19 passports, booster shots, and other pandemic issues

Connect With Us

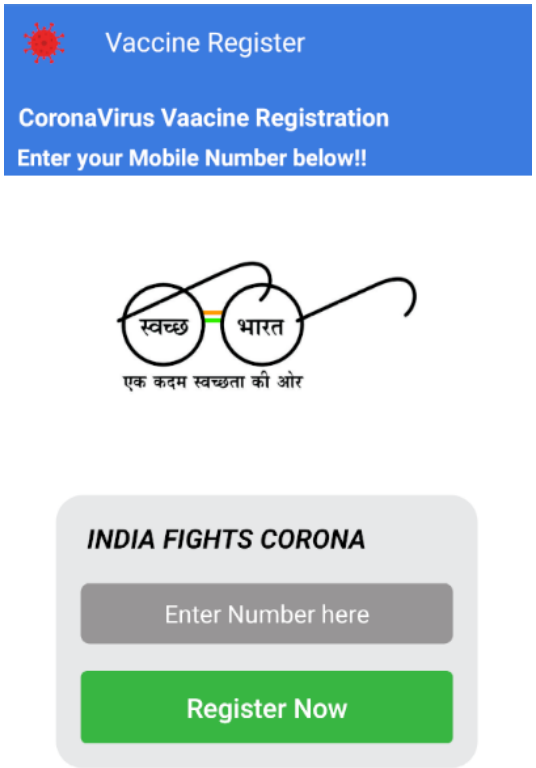

Figure 2. Example of malicious fake COVID-19 vaccine registration app

The resurgent COVID-19 crisis in India has sadly encouraged cybercriminals to continue targeting vaccine registration with fake SMS messages. At the end of April 2021 **@malwrhunterteam** found an updated version of this worm that requests access to contacts and SMS messages and asks to share the fake app on WhatsApp Groups 10 times, so that it can spread itself. None of these actions would of course be requested by a legitimate app.

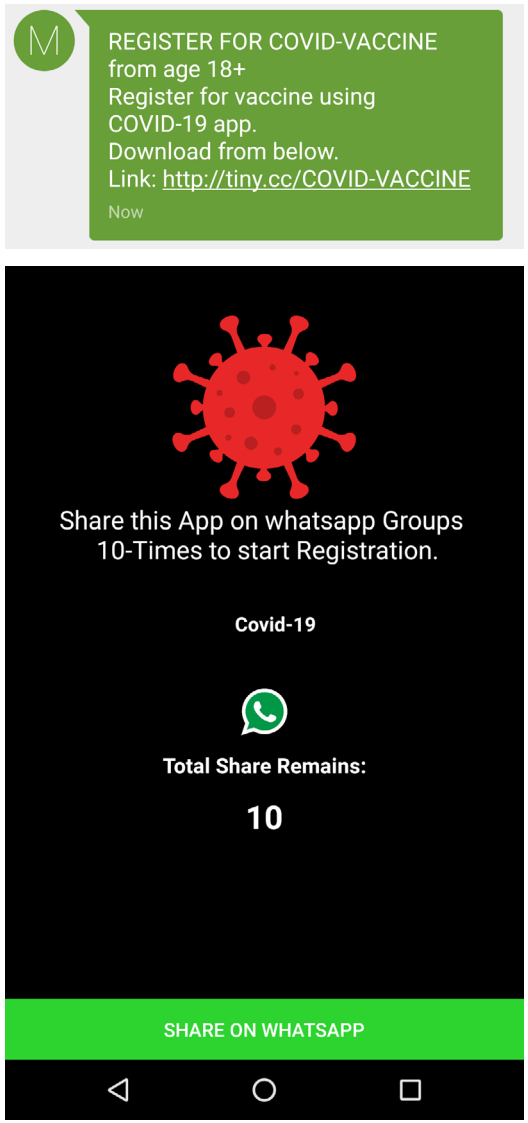

Figure 3. Recent fake COVID-19 vaccine registration SMS message and malicious app sharing request

Not Just Fake Vaccines, Now Fake Oxygen

If preying on users with fake vaccine appointment messages and apps was not enough, cybercriminals are now also targeting India's shortage of oxygen for treating COVID patients. The Director General of Police in the Indian state of Karnataka is warning citizens about a fake oximeter app to heck personal oxygen levels that is being distributed through SMS and WhatsApp. This app does not appear to show anything at all to the user, but is just a straight distribution and execution of the Android-based Anubis banking Trojan.

Fake App Targeting Chile

A more dangerous fake vaccine malware campaign was first seen in the middle of February 2021, targeting people in Chile. This malicious app uses the official icon of the Chilean Ministry of Health (Ministerio de Salud) but did not appear until two months after the government started to vaccinate the country's population. The filename of this app is Vacuna_COVID19_Chile.apk, leading with the Spanish word for vaccine, but the malware behind this is a common banking Trojan. During installation the app tells users that they need to activate accessibility services for the application to work correctly and displays instructions for how to do this. Google continues to improve Android's accessibility features to address this kind of abuse, but unfortunately there are still some ways to exploit them for malicious purposes. Once the fake vaccination app has this access, it can **take full control of the device, access the user's data, and download additional malware** components.

Continuing Popularity of COVID-related Malware

Unfortunately, bad actors are continuing to exploit people's fear of COVID-19 and uncertainty about vaccinations with mobile malware. According to the **McAfee COVID-19 Dashboard**, **more than 90 percent of all pandemic-related malware is Trojans** like those used in the Chilean app. Cybercriminals are always adapting their techniques, looking for lures that will draw in the largest population for the least effort. These few early examples of vaccine-driven campaigns are just a harbinger of what is to come if they are successful in convincing enough people to download the app or click on the message.

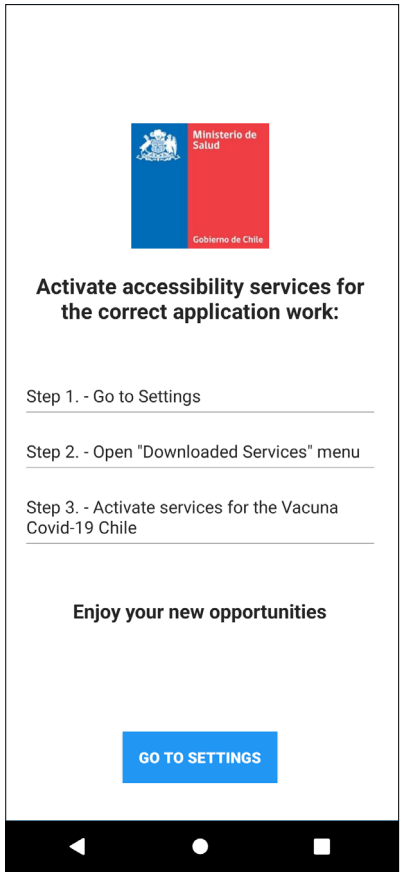

Figure 4. Screenshot of malicious fake vaccination registration app asking the user to activate accessibility services

Connect With Us

That's Not What I Signed Up for

Many unscrupulous sites try to trick you into signing up for unwanted subscriptions and premium services or make it difficult to cancel. These fraudulent apps masquerading as legitimate ones take it a step further and hijack your SMS messages to sign up without your knowledge or consent.

These apps are unfortunately quite popular, targeting users in Southwest Asia and the Middle East and **recording more than 700,000 downloads** from the Google Play Store before being detected and removed. To avoid detection, they submit a clean version of the app to Google's review process and then introduce malicious code during a later update.

Android/Etinu

On the Google Play Store these **apps look like picture editors, keyboard themes, wallpapers, and camera-related filters**. After a user downloads a version that has been updated with the malware, the apps download additional malicious code that is decrypted with keys provided by a remote server. McAfee Mobile Security tags this malware as Android/Etinu and notifies users when it is detected.

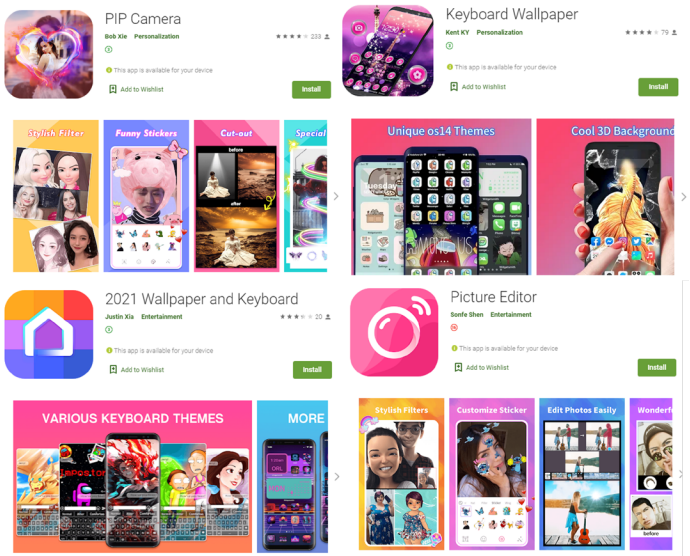

Figure 5. Screenshot of some of the malicious apps detected with billing fraud code in Google Play

ANDROID/ ETINU

What is it?
Billing fraud malware that reads SMS messages notifications to subscribe users to premium-rate services

Current threats
- Masquerades as legitimate apps
- Clean version that updates itself with malware
- Steals SMS messages
- Automates SMS activity to sign up for premium services

Future threats
- Widely distributed multi-stage malware that can easily add new targets and threats

Stealing SMS Messages

Once installed, the Android/Etinu malware steals incoming SMS messages using a Notification Listener function, but without triggering the SMS read permission or read receipts. As a result, the app can **process information in the messages without alerting the user** that messages have been read. It uses these capabilities to make purchases and sign up for premium services and subscriptions that get charged to the user's account.

Android/Etinu gets its fraud instructions from command-and-control servers that provide it with detailed information on the addresses and messages to send to make unwanted purchases. For example, subscribing to music services or downloading jokes, games, or premium video. After sending the initial purchase request, the malware **intercepts the responses, processes and responds with the confirmation details, and hides all of this from the user**. Criminals profit by getting a commission for their "sales" or by directing purchases to quasi-legitimate services that they have a relationship with.

Review Permissions When Installing Apps

The Notification Listener function has many valid uses but is vulnerable to eavesdropping and we expect malware campaigns to continue to leverage these techniques. As a user, it is critical to **review requested permissions when installing apps on your device** and watch for settings that are inconsistent with the app's intended functions. This access is dangerous, so Android cautions users who are about to enable this feature, warning users that an app "will be able to read all notifications, including personal information such as contact names and the text messages you receive".

Opening Up Banking Malware

Banking Trojan variants are contributing to a significant increase in malware activity targeting hundreds of financial institutions around the world, encouraged by an expanding campaign that began in Brazil and the release of source code by a Russian-speaking group.

McAfee Mobile Security detected a 141 percent increase in Banking Trojan activity between Q3 and Q4 2020, heavily driven by the release of the Cerberus source code. Most Banking Trojans are distributed via mechanisms such as phishing SMS messages to avoid Google's screening process, but **both threat groups have managed to evade the security process** and get apps onto Google Play.

Android/Brata

Brazilian Remote Access Tool Android (BRATA) is a popular banking Trojan that has repeatedly managed to get onto the Google Play store in different variants, tricking thousands of users into downloads before each app is caught and removed. During 2020, the McAfee Mobile Research team found **at least five different apps based on this malware** in the store. The earliest versions of these apps were focused on Brazil, and the apps check to see what country the user is downloading from and if Portuguese from Brazil is the configured language. If these conditions are not met, the app either prevents the download or skips the installation and exits. Other variants have targeted Spain and more recently moved to attack the U.S. market.

These malicious apps appear as some type of security scanner, with names such as OutProtect, PrivacyTitan, GreatVault, SecureShield, and DefenseScreen. If the target conditions such as country and language are not met, the apps simply display a screen saying that no problems were found and exit, which is probably how they avoid detection by automatic screening tools. If the conditions are met, they **pretend to scan the mobile apps installed on the device, looking for apps related to the targeted financial institutions**. If one is found, the malware notifies the user that a popular app, such as Google Chrome, WhatsApp, or a fake PDF reader, is out of date and urging an immediate update.

ANDROID/BRATA AND CERBERUS

What is it?
Banking Trojans with multiple variants distributed both inside and outside Google Play

Current threats
- Takes full control of devices by abusing accessibility services
- Displays phishing webpages to steal banking credentials
- Monitors keystrokes, records screen, and captures screen lock info
- Able to conduct covert surveillance and intercept communications

Future threats
- Leak of source code has enabled more criminals to leverage these techniques, spawning new variants and a significant increase in activity

Clicking the "Update Now" button downloads additional malicious code and asks the user to enable accessibility services, which gives the app broad control of the user's device. The malware **uses this capability to override various warnings and security settings**, including a recent addition that disables the Google Play Protect functionality.

Analyzing the malware over the past year shows an **increasing list of targeted financial apps and related phishing websites across multiple countries**, showing that the group(s) behind this campaign are quite active. The phishing websites are designed and loaded to look like sign in screens of the targeted banking apps, tricking the user into revealing their banking credentials.

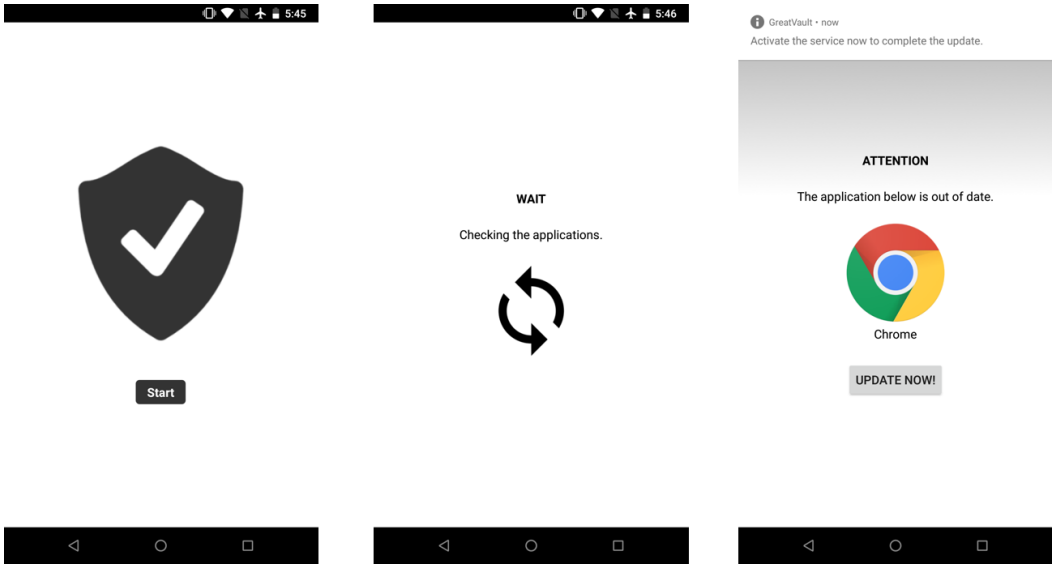

Figure 6. Screenshots from one BRATA malware variant

Android/Cerberus

Another banking Trojan family that has been contributing to the malware increase is known as Cerberus. This remote access Trojan enables attackers to take control of the user's device, intercept SMS messages and two-factor authentication codes, and steal credentials with overlays for hundreds of banking and shopping apps. The authors had been renting their code in a malware-as-a-service model and then tried to sell the code and client list via auction. Whether **intentionally or accidentally, the source code was released in September 2020** without a buyer, spawning an immediate increase in malicious apps and infections based on the code.

Summary

Mobile malware is always experimenting with new ways to sneak onto your device and make some coin.

2021 is shaping up to be a year of **malware misinformation and sneak attacks**. Last year, cybercriminals expanded the methods they used to hide attacks and frauds, making them more difficult to identify and remove. As many of those vulnerabilities have been closed or tightened, these bad actors continue to experiment with new lures and techniques to bypass security screening.

Go Where the Headlines Are

As a global misinformation and malware target, there has been nothing bigger than the COVID-19 pandemic and vaccines. Cybercriminals are **aiming fake apps at vaccine registration programs** in a few countries to see if the effort of customizing for each country is worth the potential payoff. So far India and Chile have been attacked with these campaigns, and we expect to see others if these ones are successful.

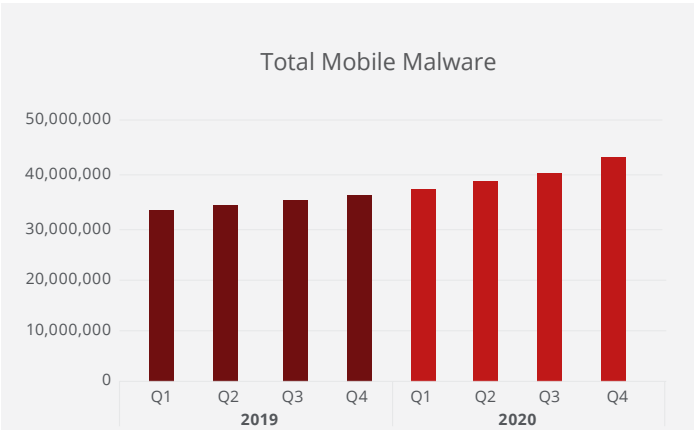

Figure 7. Total mobile malware detections by quarter.

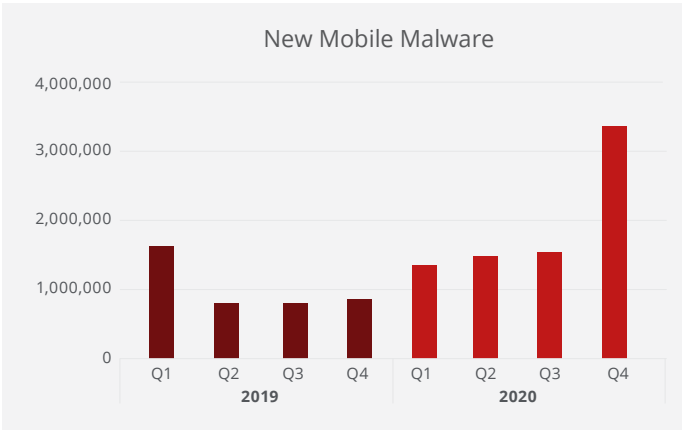

Figure 8. New mobile malware detections by quarter.

Connect With Us

Looking Back to Billing Fraud

An older attack technique of fraudulently charging users for premium SMS messages and subscriptions has resurfaced as malware authors learn to **exploit vulnerabilities in tools meant for automating messaging and notification functions**. Both telecom companies and operating system developers are having to take steps to address these attacks and build stronger safeguards.

Banks are Where the Money Is

Finally, the old expression that people rob banks because that is where the money is continues to hold true for mobile malware. Banking Trojan attacks are increasing as **malware authors add coverage for more financial institutions** and offer their code to others in Malware-as-a-Service models. The release of source code for a popular banking Trojan only adds more fuel to these campaigns.

What to Do

While threat tactics continue to change as criminals adapt and respond to detection and enforcement techniques, there are a few steps users can take to limit their exposure and risk.

Stay on the app stores
While some malicious apps do make it through the screening process, most of the attack downloads appear to be coming from social media, fake ads, and other unofficial app sources. Before downloading something to your device, do some quick research about the source and developer. Many of these have been flagged by other users.

Watch requests for settings and permissions
Many malicious apps get the access they need by asking the user to grant them permission to use unrelated privileges and settings. When installing a new app, take a few moments to read these requests and deny any that seem unnecessary, especially for accessibility services and message notification access.

Use security software
Comprehensive security software across all devices, whether they are computers, tablets, or smartphones, continues to be a strong defensive measure to protect your data and privacy from cyberthreats.

Update software
Developers are actively working to identify and address security issues. Both operating systems and apps should be frequently updated so that they have the latest fixes and security protections.

Monitor your IDs
Use identity protection monitoring tools to be aware of changes or actions that you did not make. These may have been caused by malware and could indicate that your phone or account has been compromised.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

6220 America Center Drive
San Jose, CA 95002 USA
888.847.8766
www.mcafee.com

JUNE 2021