

DATAVISOR ONLINE FRAUD REPORT

MARCH 2017

FOREWORD

WELCOME TO THE INAUGURAL DATAVISOR ONLINE FRAUD REPORT

Data is power.

We've known the potential of Big Data for years and battled to unlock it. Through major advances in computing power and storage, we are finally able to get at the invaluable information and trends it holds, analyze it, and most importantly, use it to inform important business decisions and processes.

Unlocking the power of big data to detect fraud and protect billions of users around the globe is the mission of DataVisor. The problem we are trying to solve is massive. Various state of the market reports indicate:

- ▶ The total estimated cost of global fraud is greater than \$50 billion per year.
- ▶ Global losses on credit, debit, prepaid general purpose, and private label payment cards reached \$16.31 billion last year.
- ▶ Fraud costs e-retailers and merchants more than 7.5 percent of their annual revenue.
- ▶ The total cost of insurance fraud, not including health insurance, is estimated to be more than \$40 billion per year.

This inaugural *DataVisor Online Fraud Report* is an unprecedented look at data, through the broadest lens in the industry, to provide insight into the activities of fraudsters and malicious users found across the globe.

By analyzing more than one billion user accounts, and more than 500 billion events, we detected more than 50 million malicious accounts and want to share our findings with you.

The opportunity to look across such a massive data sample to uncover trends, new attack

patterns, and additional insight into the fraud ecosystem is one that will inform and arm not only DataVisor, but hopefully our customers and anyone who is currently fighting against fraud.

We are at war with active adversaries that are constantly evolving and growing smarter, savvier, and stronger by the day. As more money is filtered into, and accessible by, online technologies, their motivation to break through will rise. We must rise along with it.

We need to evolve our fraud detection methodologies faster, drive forth with innovation and take advantage of new technologies to catch fraudsters as early as possible.

All of this can be done with innovation, and driven by information. You have the data. You have the power.

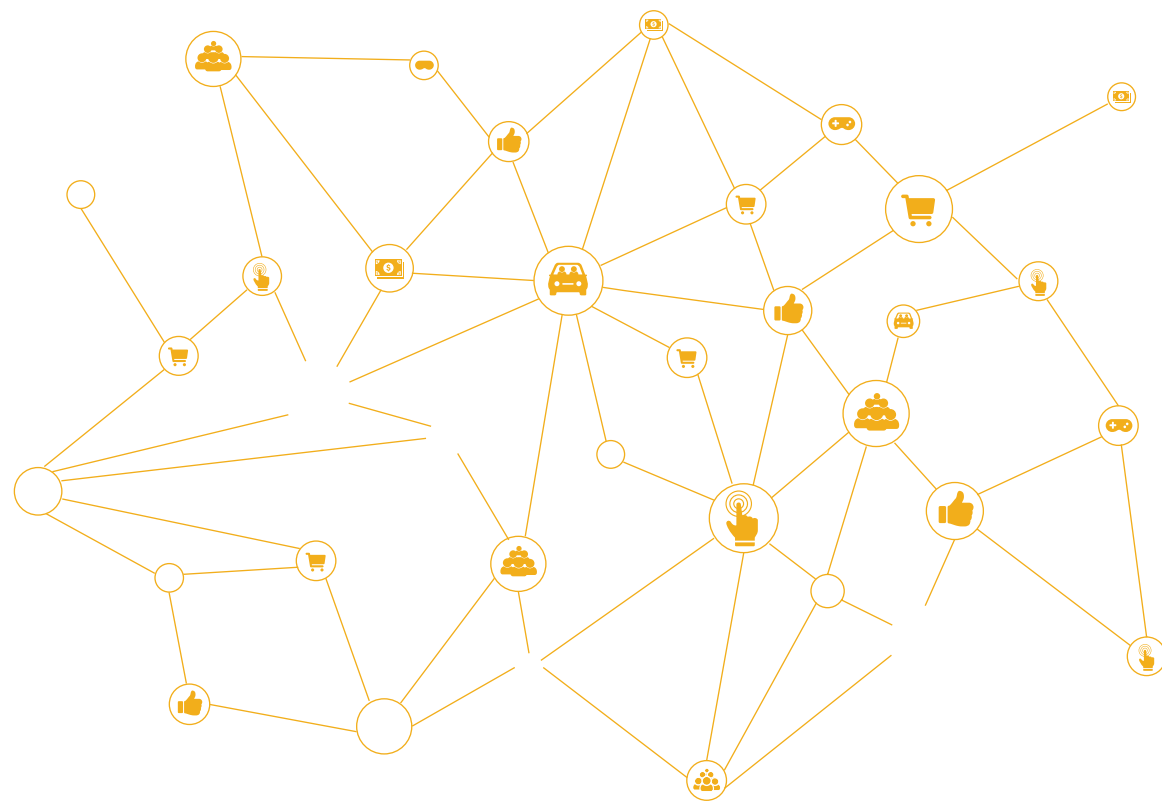


Yinglian Xie

YINGLIAN XIE

CEO & CO-FOUNDER, DATAVISOR

TABLE OF CONTENTS



FOREWORD	2
EXECUTIVE SUMMARY	4
REPORT METHODOLOGY	6
KEY ATTACK TECHNIQUE TRENDS	8
DEVICE PLATFORM	9
OS VERSION	12
BROWSER	14
GEOGRAPHY	15
CLOUD SERVICE	17
EMAIL SERVICE	19
ATTACK CAMPAIGN SIZE	21
AGING ACCOUNTS	22
CONCLUSION	23
GLOSSARY	24
CONTACT US	25

EXECUTIVE SUMMARY

THE TOOLS OF THE TRADE

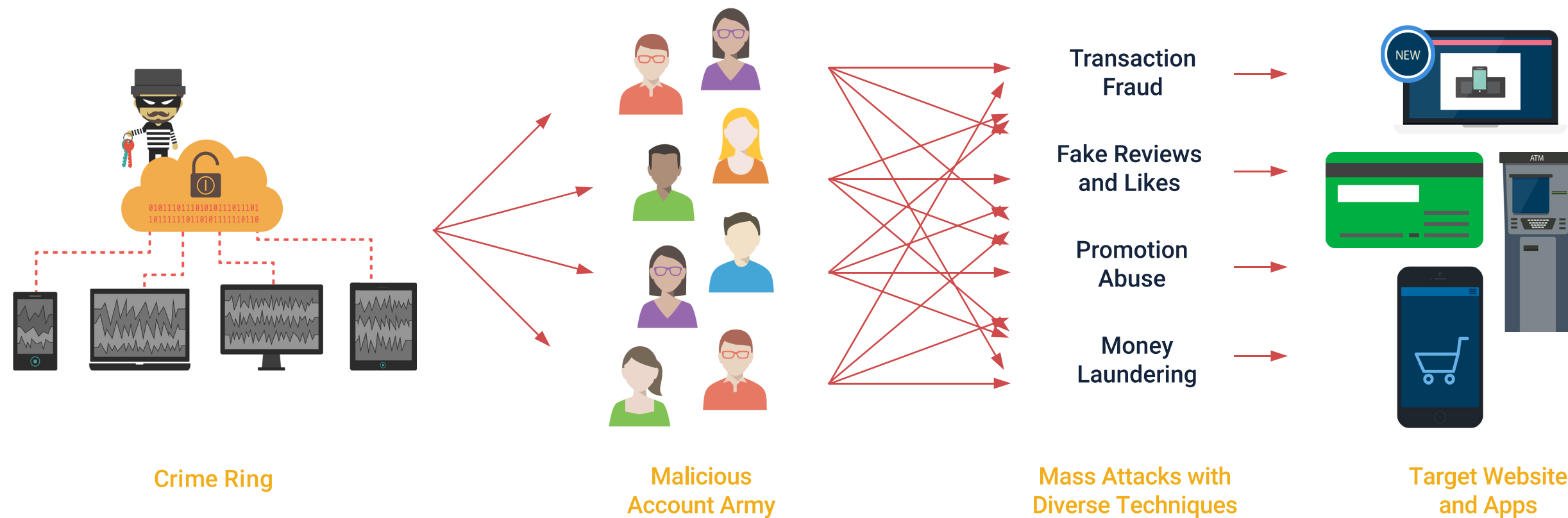
CREATING AN ARMY OF ACCOUNTS

The *DataVisor Online Fraud Report* provides insight into how bad actors are hiding amongst us inside consumer websites and mobile apps. Gone are the days when a single attacker created a single account to use a stolen credit card. In order to make their fraudulent practices economically viable, fraudsters need an army of user accounts to conduct their attacks.

So how do these cybercriminals create such an army? They have two options:

Mass fake account creation: Since it is free to create user accounts on most consumer sites, it is cheap and easy to amass a large army of user accounts this way.

Account takeovers: Nothing is more trusted than a good user account so these are coveted by bad actors. Given the number of breaches recently, compromised accounts are readily available for sale on the dark web.



EVADING DETECTION

To circumvent traditional online fraud solutions, fraudsters will use a variety of tools to appear as a legitimate user. Below are a few examples of the tools they use to scale their operations and hide their tracks:

Cloud hosting services: If you want to create hundreds or thousands of user accounts, you need compute resources. Fraudsters use cloud hosting providers such as AWS to affordably spin up machines and create fake accounts from unique machines and IP addresses.

Anonymous proxies/VPNs: In order to evade IP blacklists, fraudsters will use proxies or VPN services to hide their true IP addresses.

Anonymous email services: Fraudsters use email addresses obtained from anonymous, temporary email services to register new accounts and bypass email verification.

Mobile device flashing and virtual machines: This technique defeats device fingerprinting solutions by repeatedly flashing the OS of the same device, or using emulation software to spin up multiple virtual devices on the same machine.

Sleeper cells: Older accounts are inherently more trusted than new accounts, so bad actors will create and age accounts for months, or even years, before activating them.

KEY QUESTIONS THIS REPORT WILL ANSWER

Through our Global Intelligence Network of more than one billion users across 172+ countries in the world, we were able to identify the favorite tools and attack techniques these bad actors use to create accounts and evade detection.

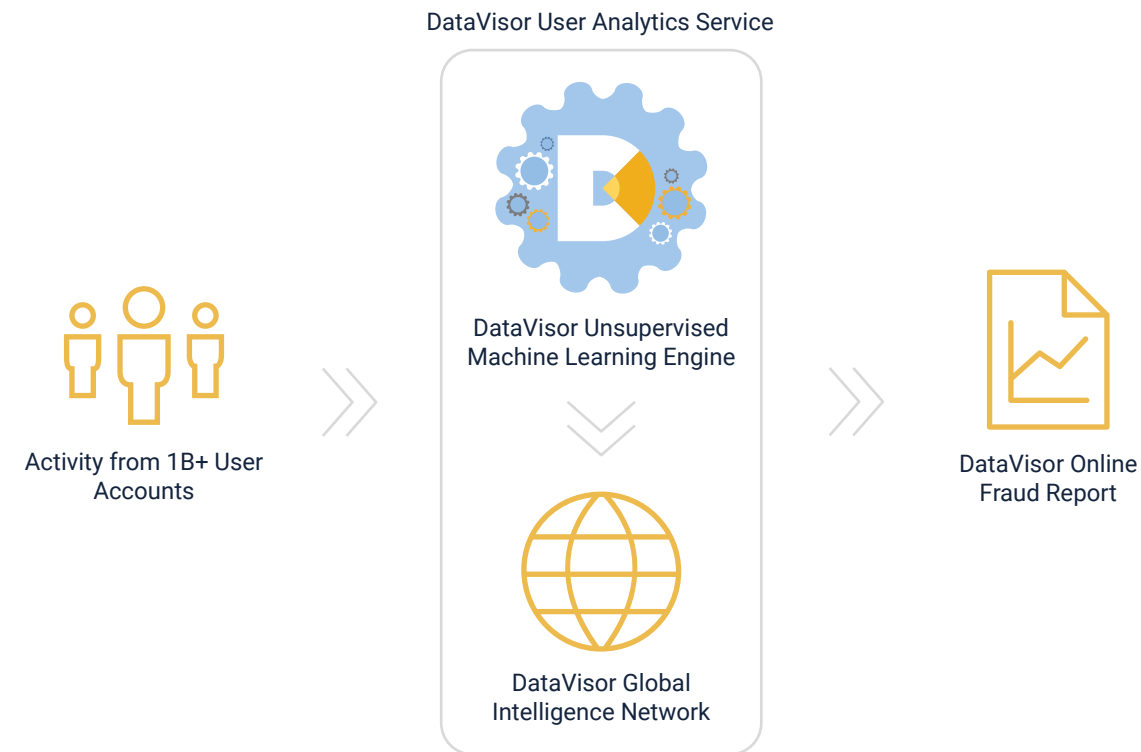
In this report, we will explain:

- ▶ What device platform is used most to conduct attacks
- ▶ Which operating system are used most frequently by fraudulent accounts
- ▶ What are the most popular browsers for fraudsters
- ▶ Where are the most fraudulent accounts located geographically
- ▶ What percentage of bad actors use cloud hosting providers to launch attacks
- ▶ Which email domains are used the most to register fake accounts
- ▶ What is the average size of a fake account army
- ▶ How long do fraudsters age accounts before they attack

REPORT METHODOLOGY

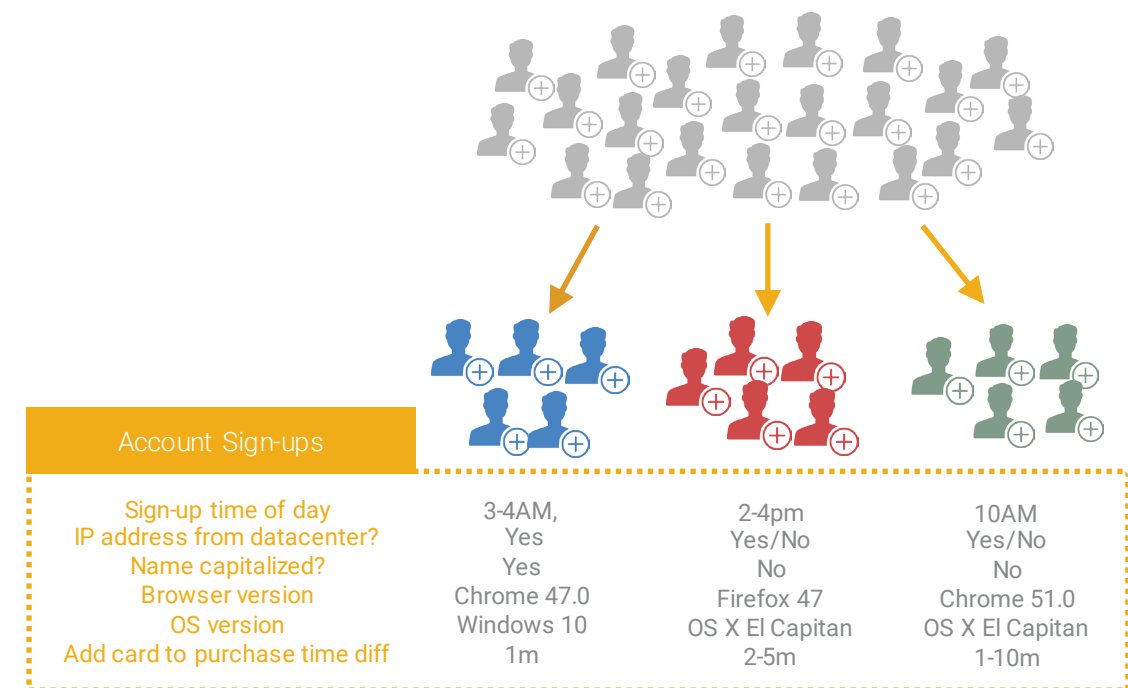
THE DATAVISOR APPROACH

DataVisor is able to provide unique insight into the online fraud threat landscape as a byproduct of using our unsupervised machine learning approach on more than a billion user accounts across some of the largest Internet properties in the world.



HOW THE DATAVISOR ONLINE FRAUD REPORT IS CREATED

While other fraud solutions also have a lot of data, what separates DataVisor from the pack is how we analyze it. Our unsupervised machine learning engine looks at all events and all users in a global view, then detects groups of malicious users by linking them together by a variety of shared attributes. Not only is this approach effective at detecting large numbers of fraudulent users, but it also has the byproduct of creating an extremely rich array of telemetry signals.



DATAVISOR'S UNSUPERVISED MACHINE LEARNING ENGINE VIEWS THOUSANDS OF ACCOUNT AND EVENT ATTRIBUTES SIMULTANEOUSLY TO LINK TOGETHER CORRELATED ACTIVITY INTO MALICIOUS CAMPAIGNS

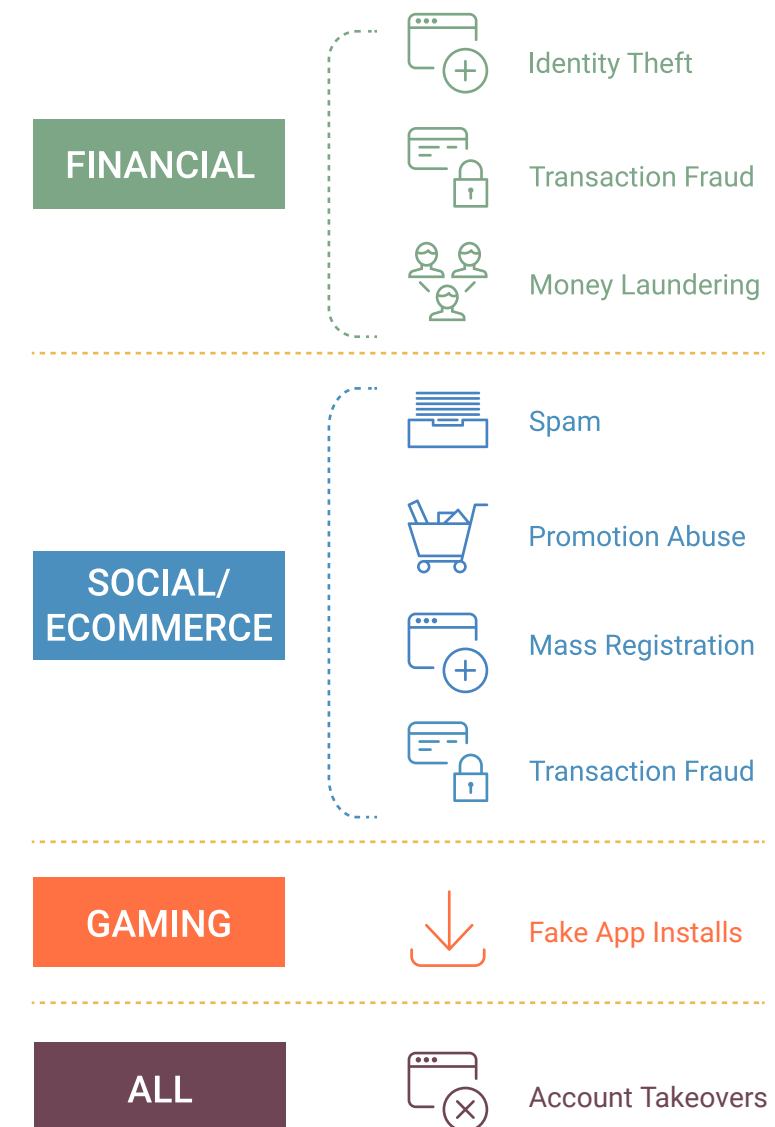
DATAVISOR GLOBAL INTELLIGENCE NETWORK

Telemetry, in DataVisor's use case, is the process of aggregating anonymized signals across our global client database of more than one billion users. Since our engine correlates hundreds of different attributes to detect fraud groups, we have been able to assemble an impressively broad array of signals into the DataVisor Global Intelligence Network. This report, which spans the last six months of 2016, is based on the following telemetry signals gathered by the DataVisor User Analytics Service:

-  410 million IP addresses
-  5.3 million user agent strings
-  3.6 million email domains
-  160,000 device types
-  300,000 OS versions
-  520 cloud hosting providers across 39 million IP addresses
-  700,000 phone prefixes

DAMAGE TYPES






In addition to the array of telemetry signals, the *DataVisor Online Fraud Report* is also informed by an extensive breadth of use cases from various industries across the world. This visibility allows our report to showcase how fraud attacks differ, depending on the type of damage conducted, between online services across the Financial, Social, Gaming, and other industries.



DATAVISOR EXAMPLE DAMAGE TYPES

KEY ATTACK TECHNIQUE TRENDS

AT-A-GLANCE

01. **82%** of all fraudulent accounts are created from desktop machines as opposed to accounts created from mobile devices.
02. A user from an  platform is **8x** more likely to be fraudulent than a user from an  device.
03. **18%** of accounts originating from cloud hosting provider IP addresses are fraudulent - used to host attacks and hide their tracks.
04. **53%** of fraudulent accounts are registered with email addresses from popular email services from Google  Microsoft  or Yahoo  to blend in with good users.
05. The fraudulent account armies targeting social platforms are **17x** larger than those targeting financial services - averaging **160** accounts per campaign.
06. **44%** of fraudulent accounts created remain “sleeper cells” for seven days or longer.

DEVICE PLATFORM

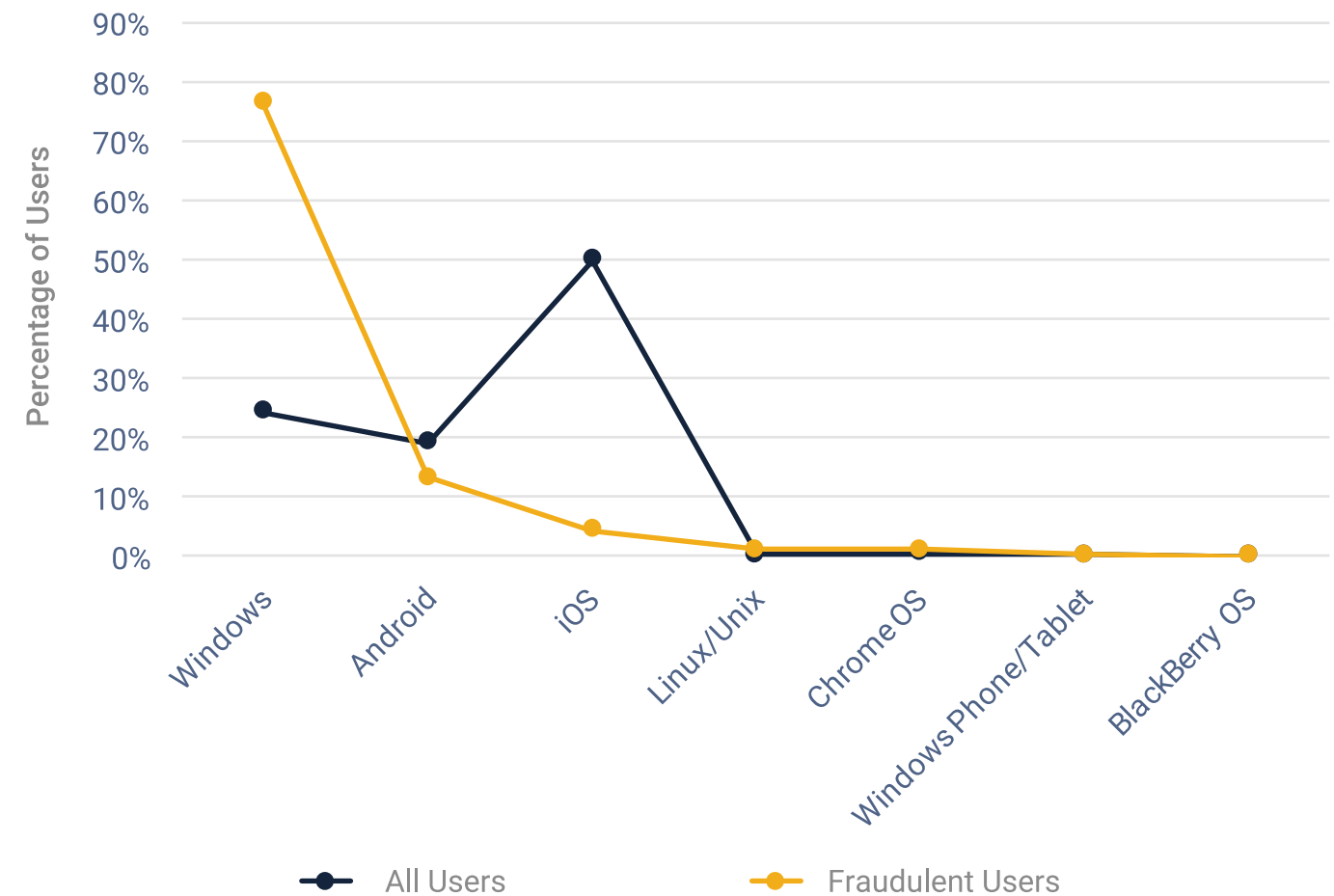
MOBILE VS. PC: THE PATH OF LEAST RESISTANCE WINS

Most users access online services through mobile devices. Wireless communication has become an ubiquitous (and essential) tool in our everyday lives, and many online services provide customized mobile interfaces that make accessing your social network, finding nearby restaurants, mobile banking, or shopping on the go easier than ever.

While everything is moving toward mobile, fraudsters and their armies of fake accounts appear to have a preference toward desktop platforms. Our data shows 82% of fake accounts originated from desktop machines, compared to only 18% from mobile platforms.

It is not hard to see why fraudsters prefer desktop — there is no reliable device fingerprint that can be used to uniquely track web users. Creating the appearance of a different user can be as simple as clearing the browser cookie and/or spoofing the user-agent string. By contrast, mobile apps sit directly on the devices and collect more accurate device identifiers, or monitor user behavior within the app, making it harder for fake accounts to avoid detection. Also it is much easier for fraudsters to use emulation software to create hundreds or thousands of virtual devices, which appear as uniquely legitimate users, on desktop as opposed to mobile. When possible, people will opt for the path of least resistance - and fraudsters are no different.

PLATFORM DISTRIBUTION AMONG ALL USERS VS. FRAUDULENT USERS



WINDOWS IS THE PLATFORM OF CHOICE FOR FRAUDSTERS AT 76% OF THE BAD ACCOUNTS DETECTED ACROSS THE DATAVISOR GLOBAL INTELLIGENCE NETWORK.

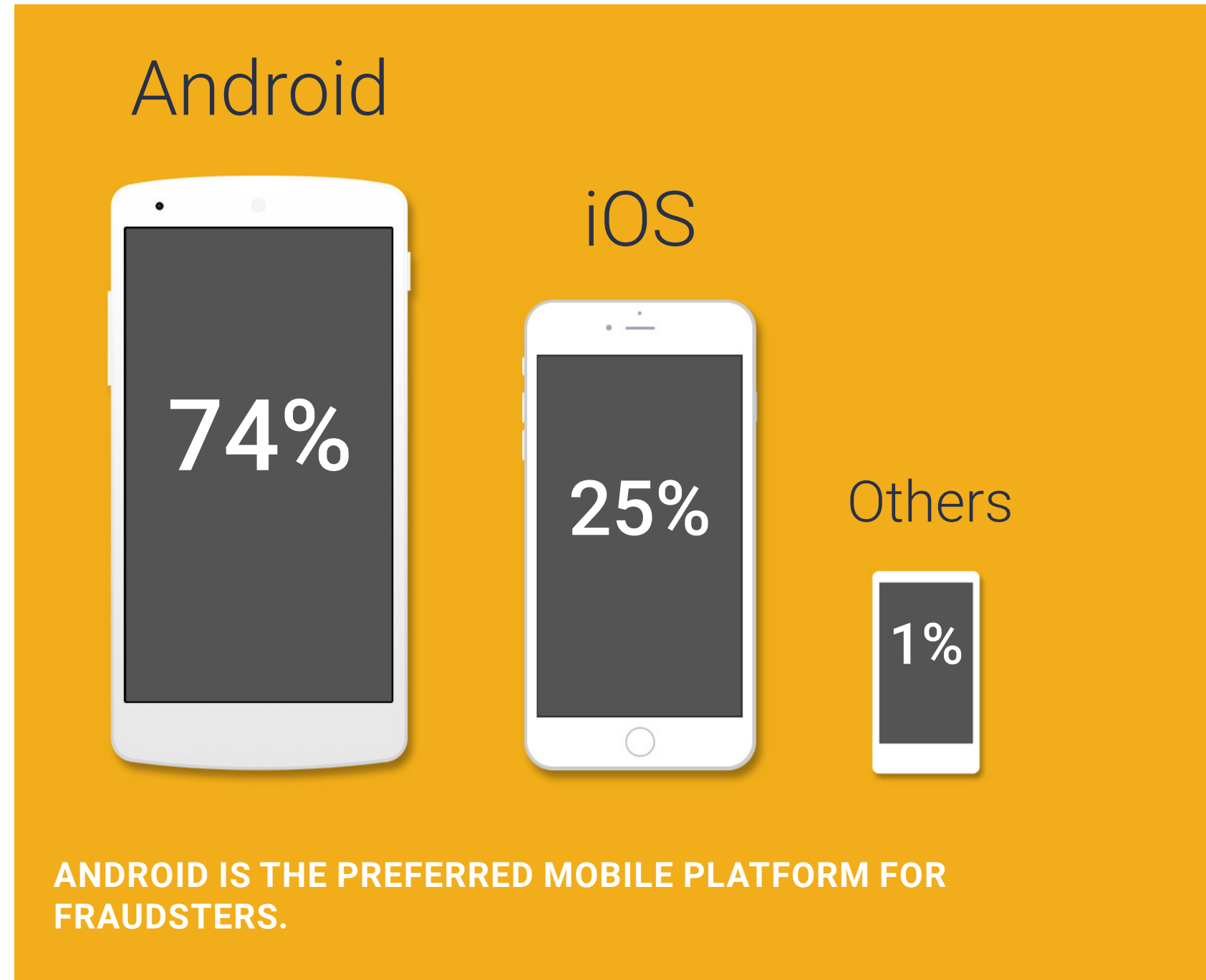
DEVICE PLATFORM

IOS VS. ANDROID: DROIDS ARE THE PHONES FRAUDSTERS ARE LOOKING FOR

A closer look at the mobile devices used by fraudsters also shows a big difference across platforms: there are 3x more fraudulent accounts from Android devices compared to those from iOS. Android, being an open source operating system, gives users (including fraudsters) the flexibility to make system-level customizations and add new features. There are also more apps available for Android systems compared to iOS, some of which are specifically designed to spoof GPS location services on the device, forge network requests, automate human-like activities, or provide other functionalities convenient for conducting fraud.

In our observations, a user from an Android platform is 8x more likely to be fraudulent than a user from an iOS device. When an online service is "mobile only," criminals will opt for Android as the best platform for attacks.

PERCENTAGE OF FRAUDULENT ACCOUNTS ACROSS MOBILE PLATFORMS

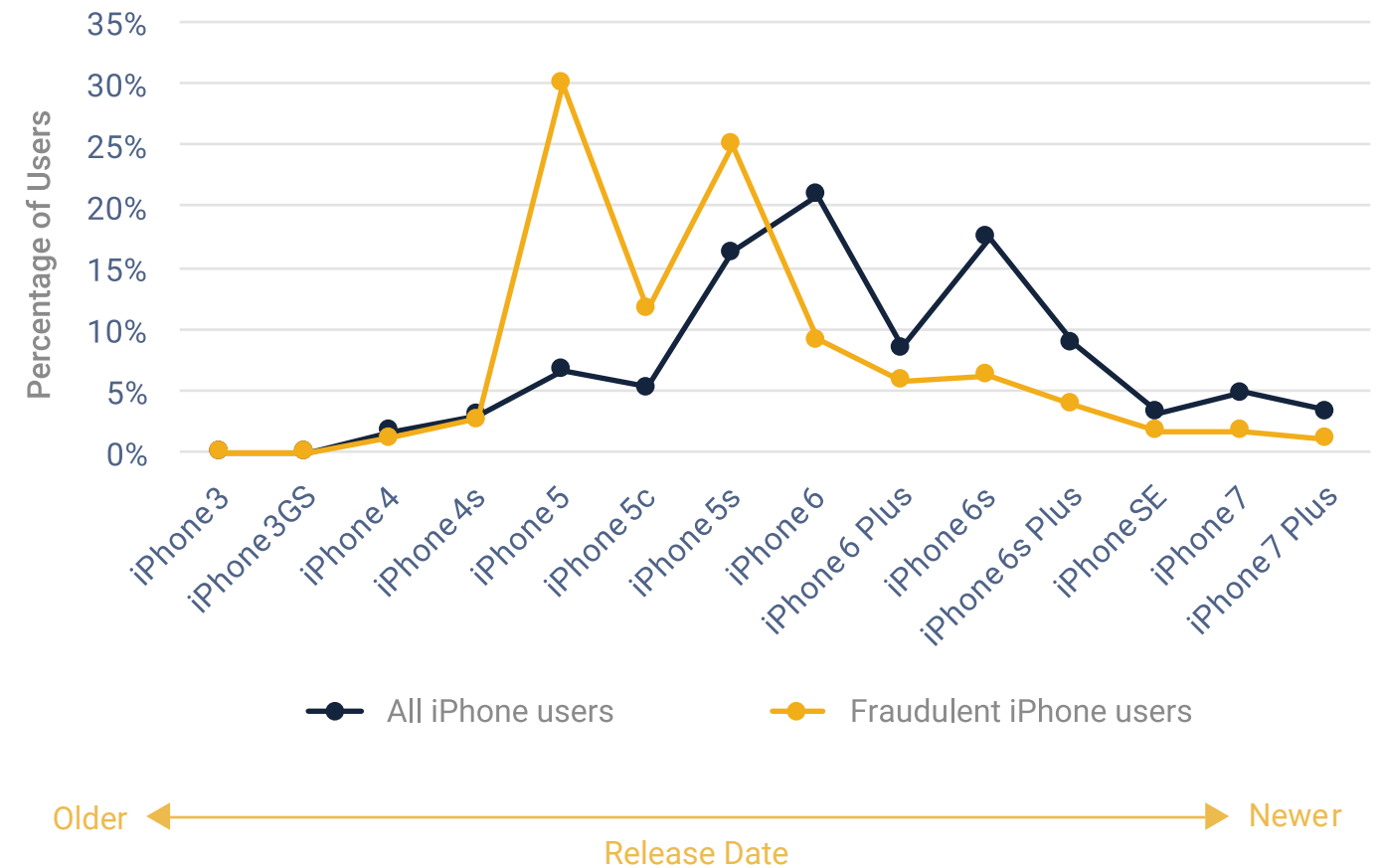


DEVICE PLATFORM

DEVICE HARDWARE: WHY YOU WON'T SEE FRAUDSTERS IN LINE FOR THE NEW IPHONE

What do fraudsters do when they want to attack iOS-based apps? Since it is difficult to virtualize iOS devices due to the more closed Apple architecture, most fraudsters are forced to use physical hardware to conduct attacks on iOS-based apps. However, creating a test bench of hundreds or thousands of iOS devices could get very expensive very quickly. According to our research, fraudsters lag behind in terms of iOS hardware, preferring older mobile device models. Among fraudulent accounts from iOS platforms, the most popular device models are iPhone 5, 5s, and 5c – four-year old models as of 2017. Considering that the starting price for the latest version, the iPhone 7 Plus, is more than \$700, the iPhone 5/5s/5c certainly appear as much more cost-effective options to create an army of fake accounts.

DEVICE MODEL DISTRIBUTION AMONG ALL IPHONE USERS VS. FRAUDULENT IPHONE USERS



FRAUDSTERS LAG UP TO FOUR GENERATIONS BEHIND WHEN USING IPHONES FOR ATTACKS.

OS VERSION

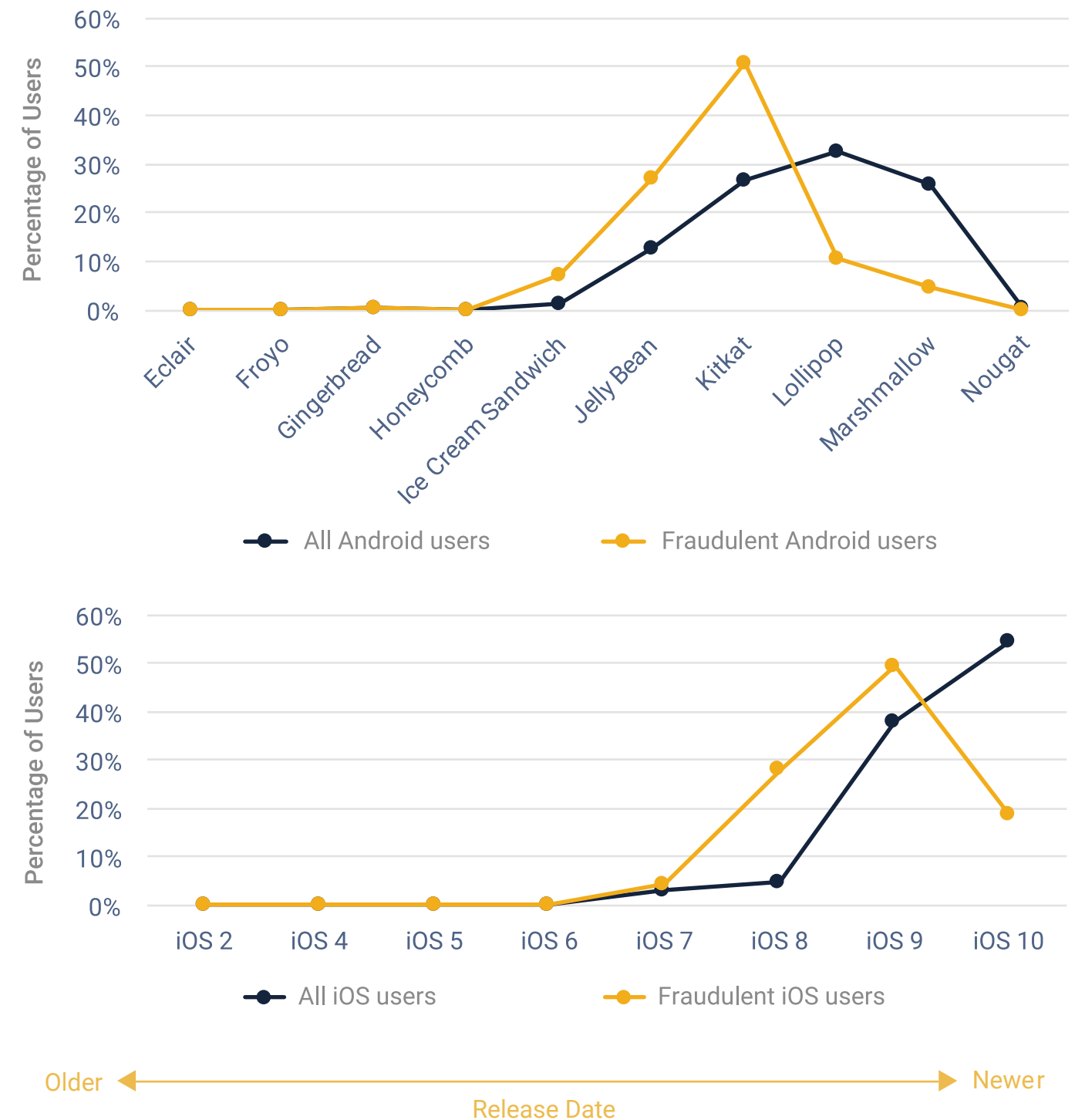
MOBILE OS VERSIONS: FRAUDSTERS LAGGING BEHIND

When it comes to the mobile OS versions used by fraudsters, there appears to be a preference toward one that's just slightly dated: old, but not too old. This could be due in part to newer OS versions having security enhancements that make it harder to run their hacking tools, or perhaps fraudsters are using older hardware that cannot run new OSs efficiently (or are not supported by new OSs). Whatever the reason may be, the popular mobile OSs used by fraudulent accounts are often a couple steps behind the latest version.

The most popular Android versions among fraudsters are "Kitkat" (4.4 - 4.4.4) and "Jelly Bean" (4.1 - 4.3.1), which make up 77% of fraudulent accounts originating from Android devices. Similarly, iOS 9 is used by the majority of fraudulent accounts originating from Apple devices, while normal users have largely moved on to iOS 10.

FRAUDSTERS LAG UP TO TWO VERSIONS BEHIND WHEN USING MOBILE DEVICES FOR ATTACKS.

ANDROID AND IOS VERSION DISTRIBUTIONS AMONG ALL USERS VS. FRAUDULENT USERS



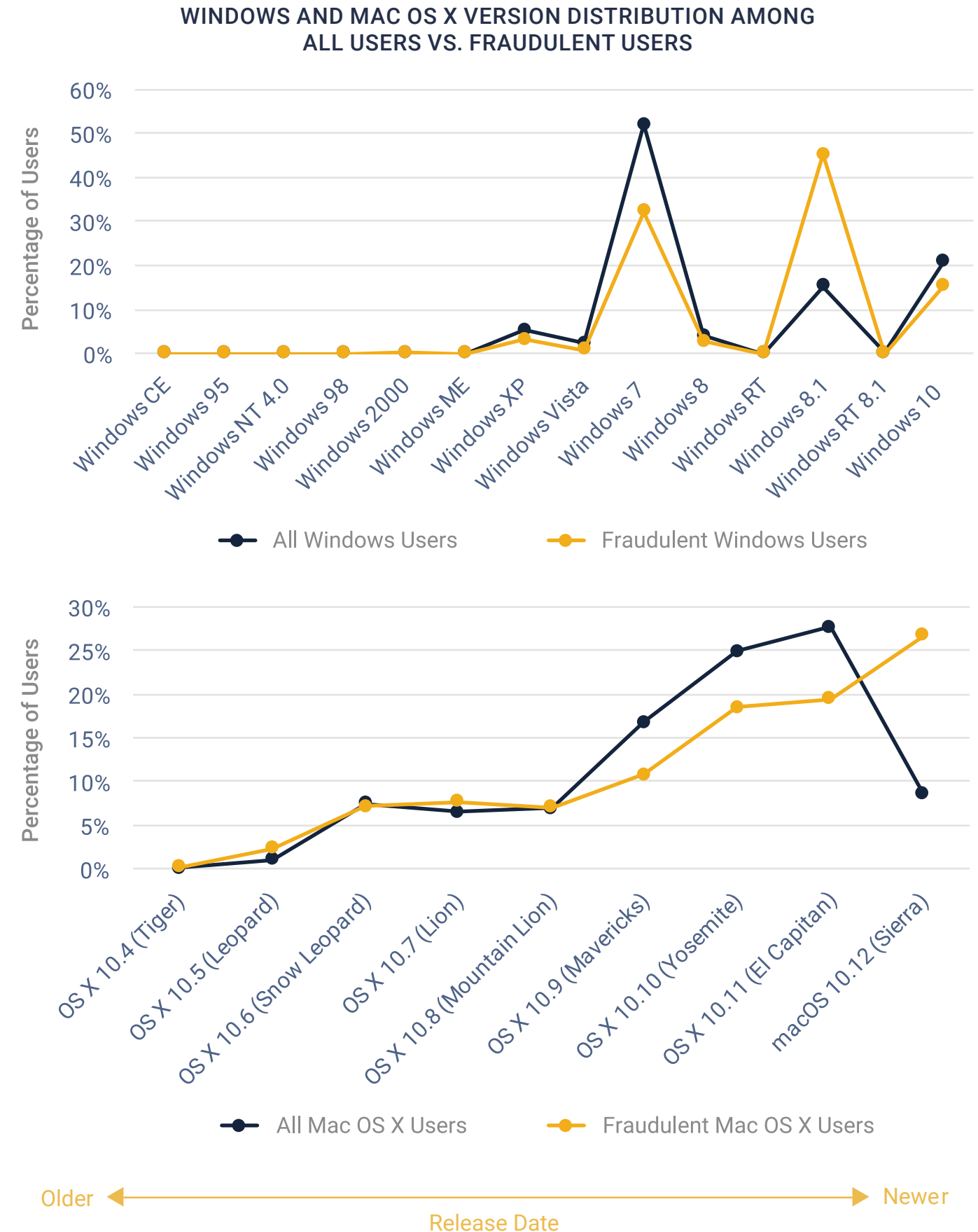
OS VERSION

DESKTOP VERSIONS: FRAUDSTERS ARE TECH-SAVVY

While mobile fraudsters lag a few versions behind normal users, fraudsters from desktop systems seem to be ahead of the curve. For both Windows and Mac OS X, there is a higher fraction of fraudulent accounts using newer OS versions than normal users. For example, Windows 7, released in 2009, is still the most widely adopted version, but the majority of fraudulent accounts from Windows platforms use Windows 8 or later. Similarly, 27% of fraudulent accounts from Mac OS X systems are running the latest version (10.12, "Sierra"), while its adoption rate is only 8% among normal users.

Compared with the older, cheaper phones used for mobile fraud attacks, these desktop machines are more likely to be the fraudsters' work machines - from which they develop custom tools and launch attacks - and so are commonly kept up-to-date. It is also easier to upgrade desktops, since they are less hardware-constrained than mobile devices (older devices cannot run the latest iOS or Android version effectively). In addition, attacks hosted from cloud hosting providers are most likely using off-the-shelf images with the latest Windows or Linux operating systems.

DIFFERENT FROM MOBILE ATTACKS, FRAUDSTERS USE THE LATEST OS SOFTWARE WHEN LAUNCHING ATTACKS FROM DESKTOP MACHINES.



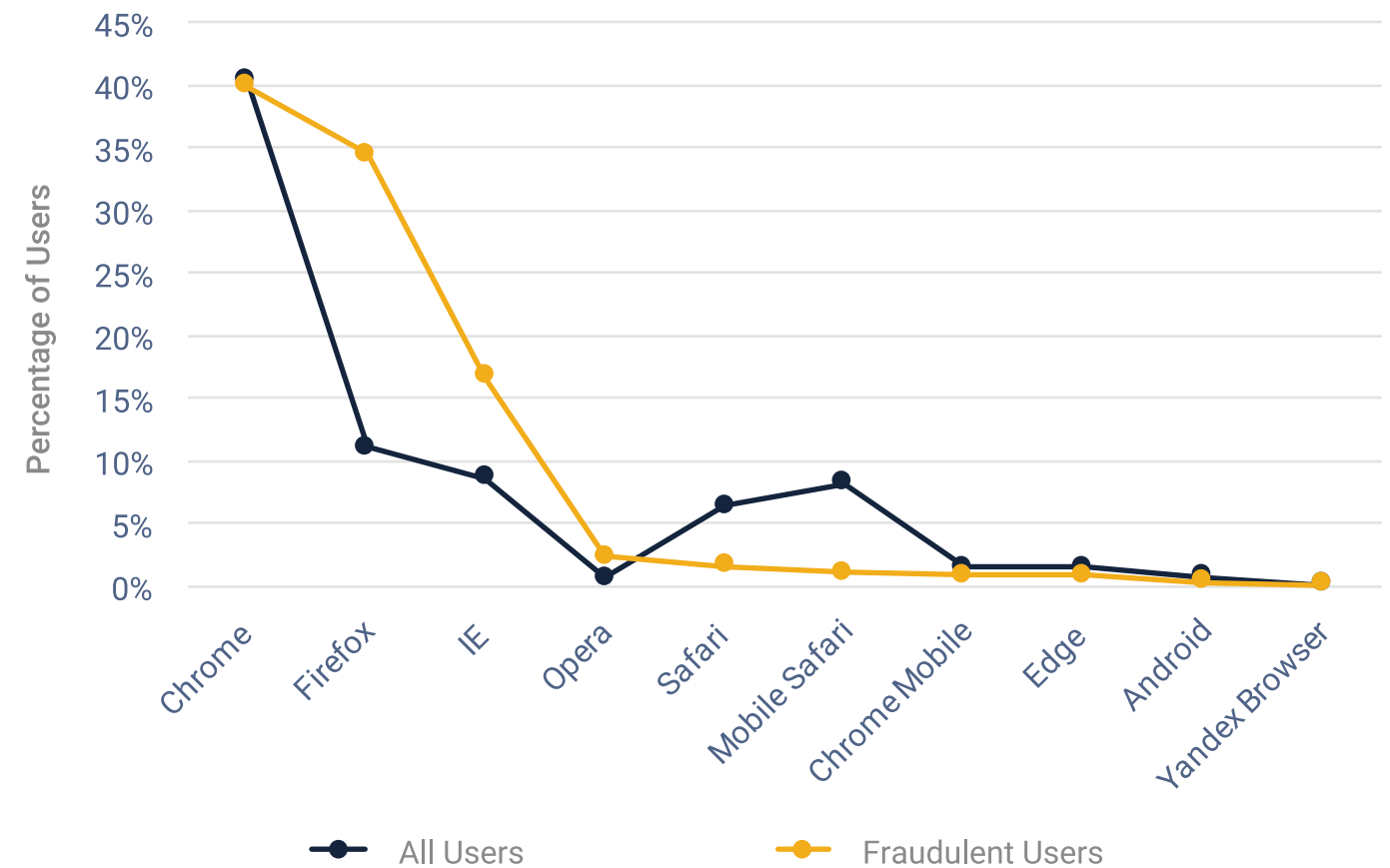
BROWSERS

FRAUDSTERS - THEY'RE JUST LIKE US!

Fraudsters use the same web browsers you do. The most common browsers among fraudsters are Chrome, Firefox, and Internet Explorer, accounting for more than 90% of fraudulent accounts. These browsers are equally popular among normal users, although there are also a significant number of normal users from Safari. Since we have previously established desktop and Android are the preferred platforms for fraudsters, it is not surprising that Chrome, Firefox and IE are the predominant browsers used in attack campaigns.

These common browsers, while popular among both fraudulent and normal users, are still made up largely of normal users. This is not the case for some lesser known browsers. The browser with the highest fraction of fraudulent accounts - with 94% of its users being fraudulent - is Comodo Dragon, a Chromium-based browser that includes extensive security and privacy features, such as disabling web tracking, using Comodo's DNS servers instead of the ones hosted by the internet service provider, etc. Fraudsters may have preferred this browser for its privacy features.

THE BROWSER DISTRIBUTION AMONG ALL USERS AND FRAUDULENT USERS, FOR THE TOP BROWSERS WITH THE HIGHEST NUMBER OF FRAUDULENT USERS



FRAUDSTERS USE THE SAME BROWSERS AS YOU DO, PREFERRING CHROME, FIREFOX, AND IE.

GEOGRAPHY

NORTH AMERICA/EUROPE-BASED ONLINE SERVICES: FIGHTING A GLOBAL ADVERSARY

Fraudsters are everywhere. The map to the right shows the countries hosting the highest number of fraudulent accounts that target online services based in North America and Europe. U.S. and China host the highest number of fraudulent accounts, but Southeast Asia and Eastern Europe are producing their fair share of malicious accounts as well. As more online services expand internationally, we expect to see an increase in global attacks and collaboration between fraud groups in different regions.

COUNTRIES HOSTING THE HIGHEST NUMBER OF FRAUDULENT ACCOUNTS FOR ONLINE SERVICES BASED IN NORTH AMERICA AND EUROPE



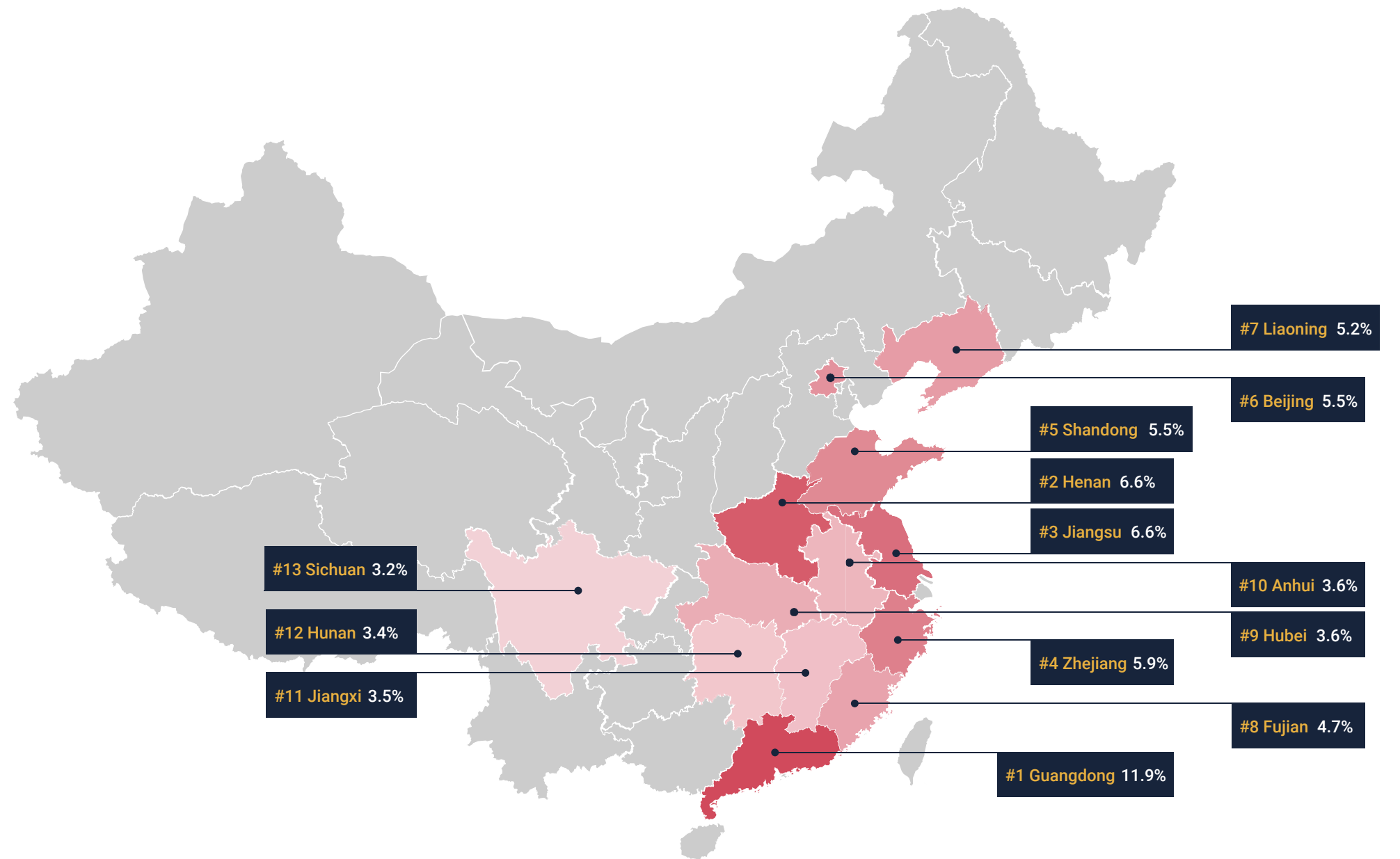
U.S. AND CHINA HOST THE HIGHEST NUMBER OF FRAUDULENT ACCOUNTS.

GEOGRAPHY

CHINA-BASED ONLINE SERVICES: FIGHTING THE ENEMY FROM WITHIN

While online properties based in North America and Europe are attacked by global fraudsters, China-based online services are attacked more by fraudsters in their immediate region. Ninety-five percent of fraudulent accounts that target China-based services originate from within China. The map to the right shows the percentage of fraudulent accounts hosted by the top provinces with the most fraud. It is interesting that most of the coastal provinces are highlighted - likely due to larger populations in those locations and the presence of fraudster communities in bigger cities.

PROVINCES HOSTING THE HIGHEST NUMBER OF FRAUDULENT ACCOUNTS FOR ONLINE SERVICES IN CHINA



MOST ATTACKS ON CHINA SERVICES ORIGINATE FROM WITHIN CHINA.

CLOUD SERVICE

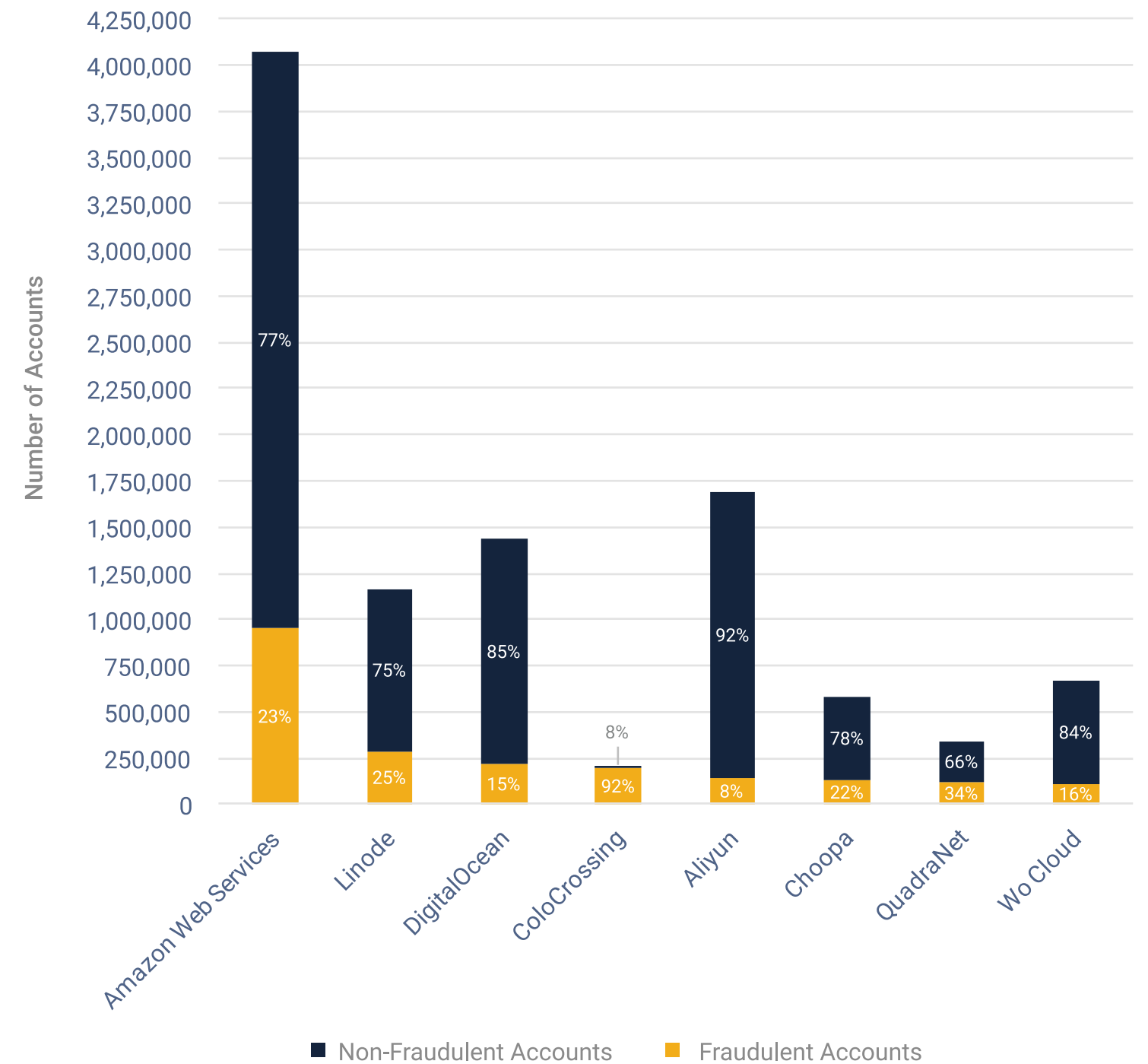
BY VENDOR: AMAZON THE TOOL OF CHOICE

Businesses and consumers are not the only ones moving to the cloud. Fraudsters also take advantage of the infrastructure of cloud services, dedicated/virtual hosting, and anonymous proxies to conduct attacks. The cloud allows fraudsters to both significantly increase the number of attack campaigns they can conduct, attributed to the elasticity and compute capacity of these services, and easily hide behind legitimate network sources and thus remain anonymous.

We observe that 18% of accounts originating from cloud service IP ranges are fraudulent. Malicious accounts are 7x more likely to use cloud services than normal users. The figure to the right shows the top cloud services hosting the highest number of fraudulent accounts. In some cases, more than 90% of accounts originating from a cloud service are fraudulent, though others see a much smaller fraction of fraudulent accounts.

MALICIOUS ACCOUNTS ARE 7X MORE LIKELY TO USE CLOUD HOSTING PROVIDERS THAN NORMAL USERS.

TOP CLOUD HOSTING SERVICES WITH THE HIGHEST NUMBER OF FRAUDULENT ACCOUNTS



CLOUD SERVICE

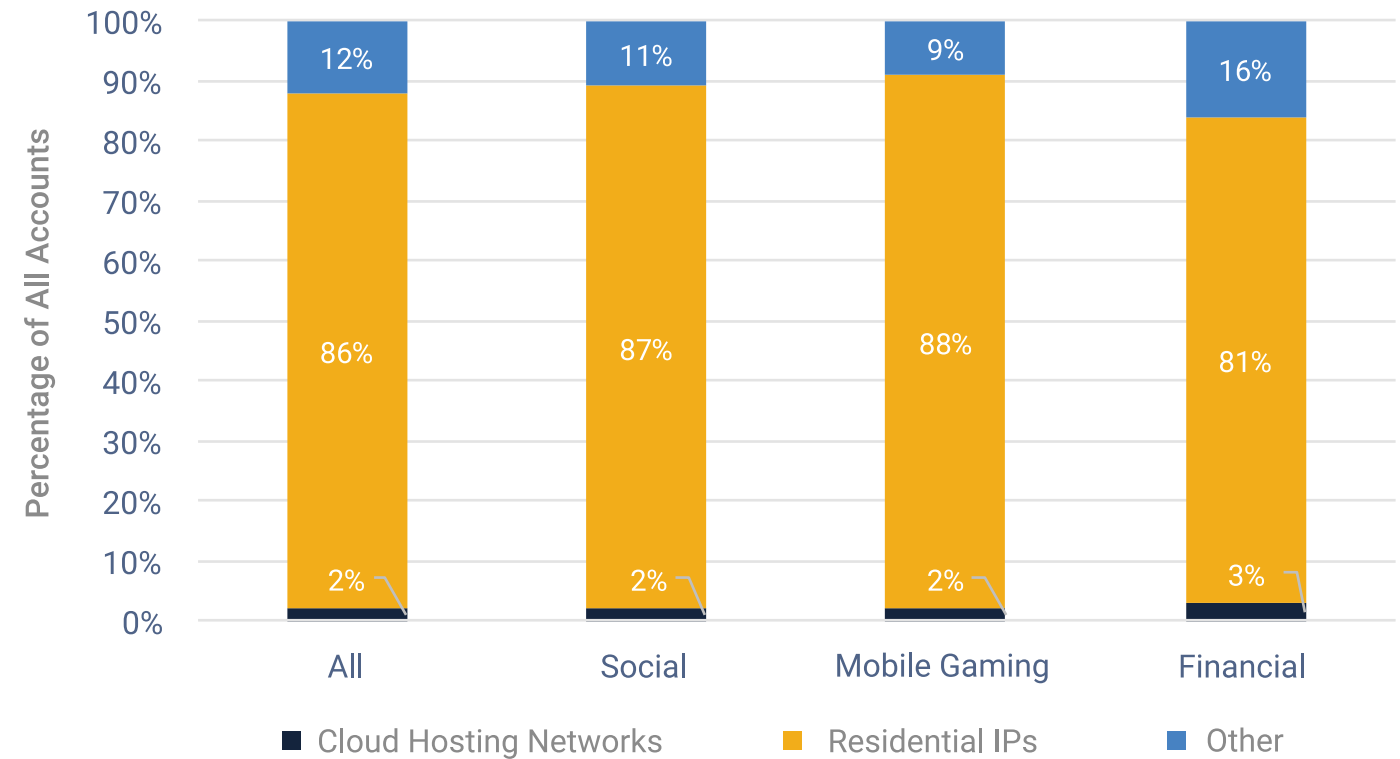
BY NETWORK TYPE: RESIDENTIAL VS. CLOUD

Approximately 86% of users access online services from residential IP ranges. This is not surprising, since online services largely tailor to consumers. Fraudulent accounts, on the other hand, appear to originate from very different types of networks compared to normal users. Our data shows that 39% of fraudulent accounts using a U.S. IP address are from cloud hosting networks, and only 37% are from residential networks.

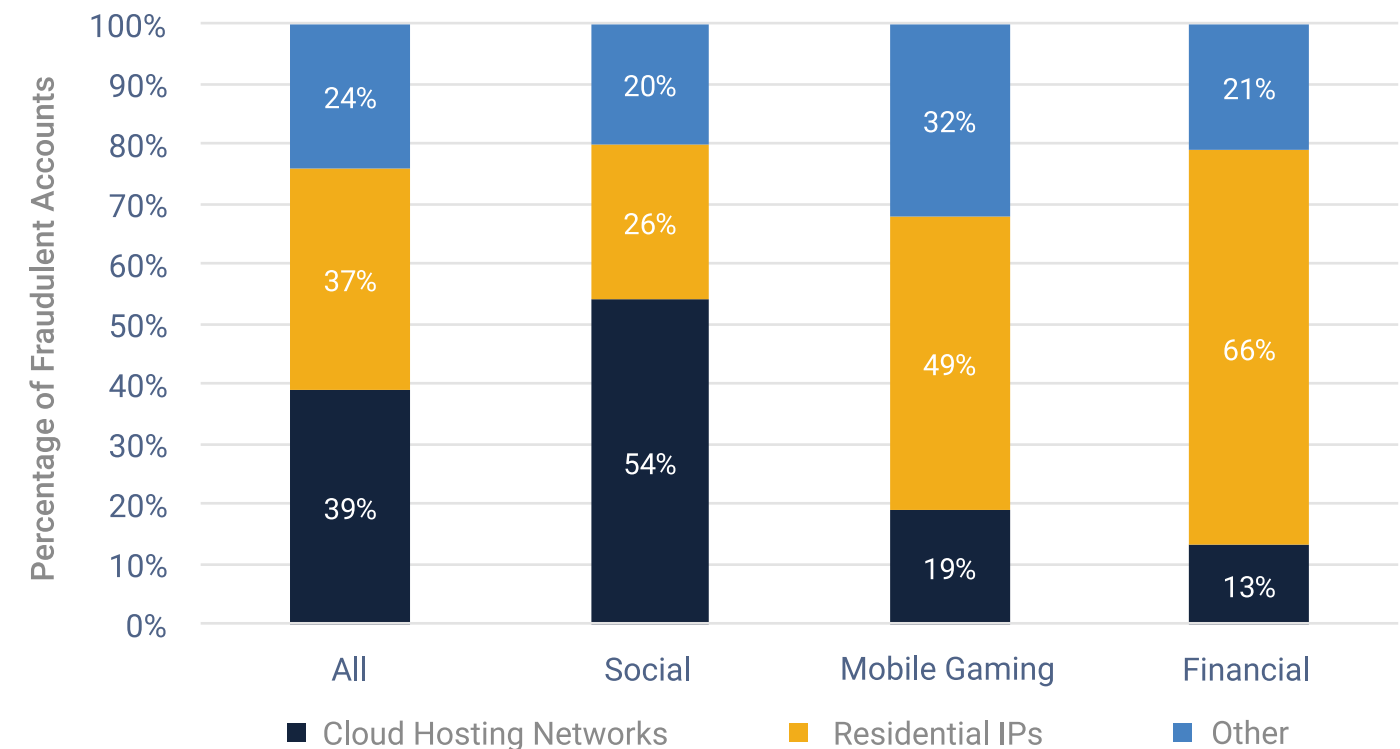
There is much variation among fraudsters targeting different online service verticals as well. Fifty-four percent of the fraudulent accounts on social platforms originated from cloud hosting networks, while two-thirds of fraudulent accounts on financial services are from residential networks. This difference can be attributed to the nature of the attacks – social platforms are frequented by massive waves of fake account registrations made scalable by cloud infrastructure, whereas financial fraudsters are more stealthy, conducting attacks with a combination of scripts and manual work. For mobile gaming, where one of the most costly fraud attacks is user acquisition fraud, fake app installs are commonly performed from cloud hosting networks located in the targeted region, with subsequent engagement activities (e.g., logins, in-app events) generated by mechanical Turks from offshore sites.

39% OF FRAUDULENT ACCOUNTS IN THE U.S. ORIGINATE FROM CLOUD HOSTING NETWORKS.

U.S. IP ADDRESS DISTRIBUTION



U.S. IP ADDRESS DISTRIBUTION (FRAUDULENT ACCOUNTS)



EMAIL SERVICE

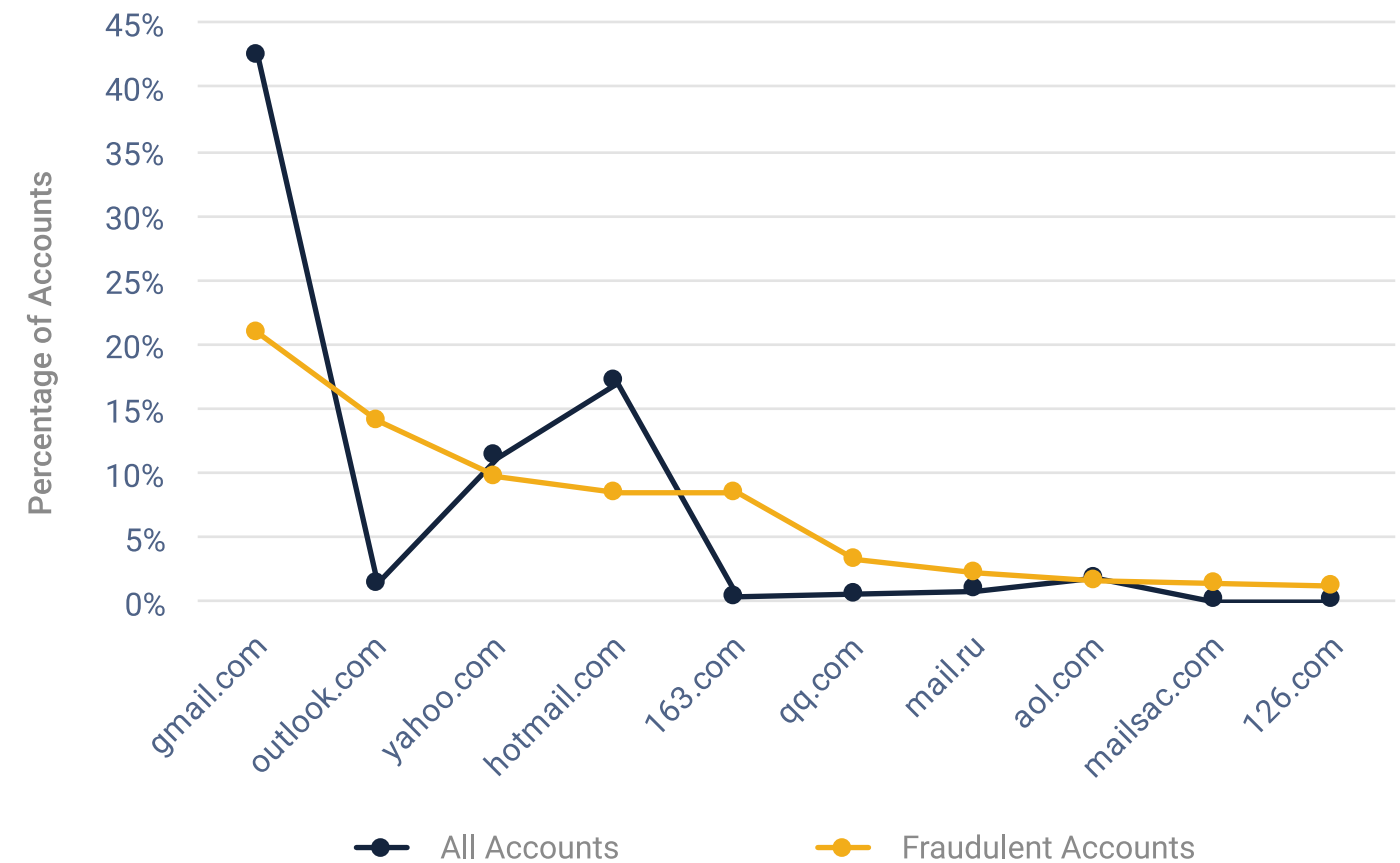
BY VENDOR: GMAIL IS THE FAVORITE FOR REGISTERING ACCOUNTS

Email addresses are among the most common, and often the only, information required to register new accounts on an online service. There are plenty of email services to choose from, but the common ones used by fraudulent accounts are largely similar to those used by normal users, e.g., Gmail, Outlook, and Yahoo.

A small fraction - around 2% - of fraudulent accounts are more extreme, registering with anonymous, temporary email addresses from providers such as Mailsac, Guerrilla Mail, Temp Mail, Fake Mail Generator, etc. These services allow users to receive messages at a randomly-generated, temporary email address instead of their real email and avoid spam. However, the lax signup process at these services also makes them targets for abuse. Fraudsters use these temporary mailboxes to receive account confirmation emails when registering fake accounts, bypassing the need to create email accounts in advance.

We believe fraudsters use these common email domains, such as Gmail, to appear more like a legitimate user, since domains from suspicious sources like Fake Mail Generator are more likely to be blacklisted by rules-based fraud detection solutions.

THE EMAIL DOMAIN DISTRIBUTION AMONG ALL USERS VS. FRAUDULENT USERS, FOR THE TOP 10 EMAIL DOMAINS MOST USED BY FRAUDULENT USERS



FRAUDSTERS USE COMMON EMAIL DOMAINS TO REGISTER ACCOUNTS SO THEY APPEAR MORE LIKE LEGITIMATE USERS.

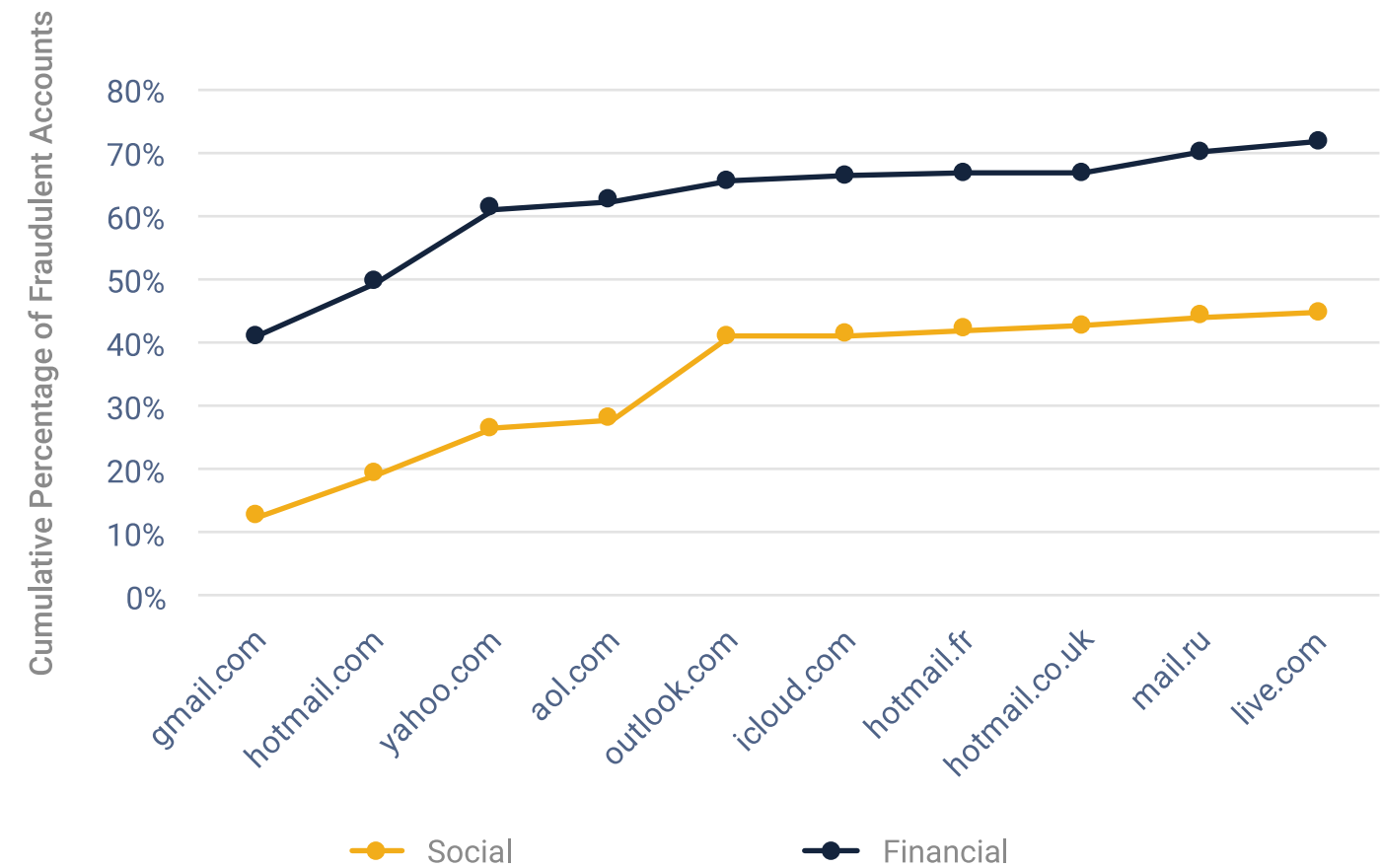
EMAIL SERVICE

SOCIAL VS. FINANCIAL: FINANCIAL FRAUDSTERS TRY HARDER TO BLEND IN

While most fraudulent accounts use emails from popular mail services, the degree to which these domains are preferred by fraudsters differs across online service verticals. Fraudulent accounts targeting financial services are more likely to use reputable email domains, e.g., that are common among normal users, such that they can appear legitimate and blend in with other users. By contrast, fake accounts on social platforms are more liberal about signing up using obscure domains, including those that the fraudsters registered for the purpose of creating email accounts en masse. This allows them to bypass phone, CAPTCHA, or other two-factor verification checks often required for public email services.

The figure to the right shows the cumulative fraction of fraudulent accounts that registered with an email address from the top 10 most popular email services across all users. For fraudulent accounts on financial services, 72% signed up with an email address from the top 10 email services, while this number is only 45% for fraudulent accounts on social platforms.

THE CUMULATIVE PERCENTAGE OF FRAUDULENT ACCOUNTS THAT REGISTERED WITH AN EMAIL ADDRESS FROM THE TOP 10 MOST POPULAR EMAIL SERVICES



FRAUDULENT ACCOUNTS TARGETING FINANCIAL SERVICES ARE MORE LIKELY TO USE REPUTABLE EMAIL DOMAINS THAN THOSE TARGETING SOCIAL PLATFORMS.

ATTACK CAMPAIGN SIZE

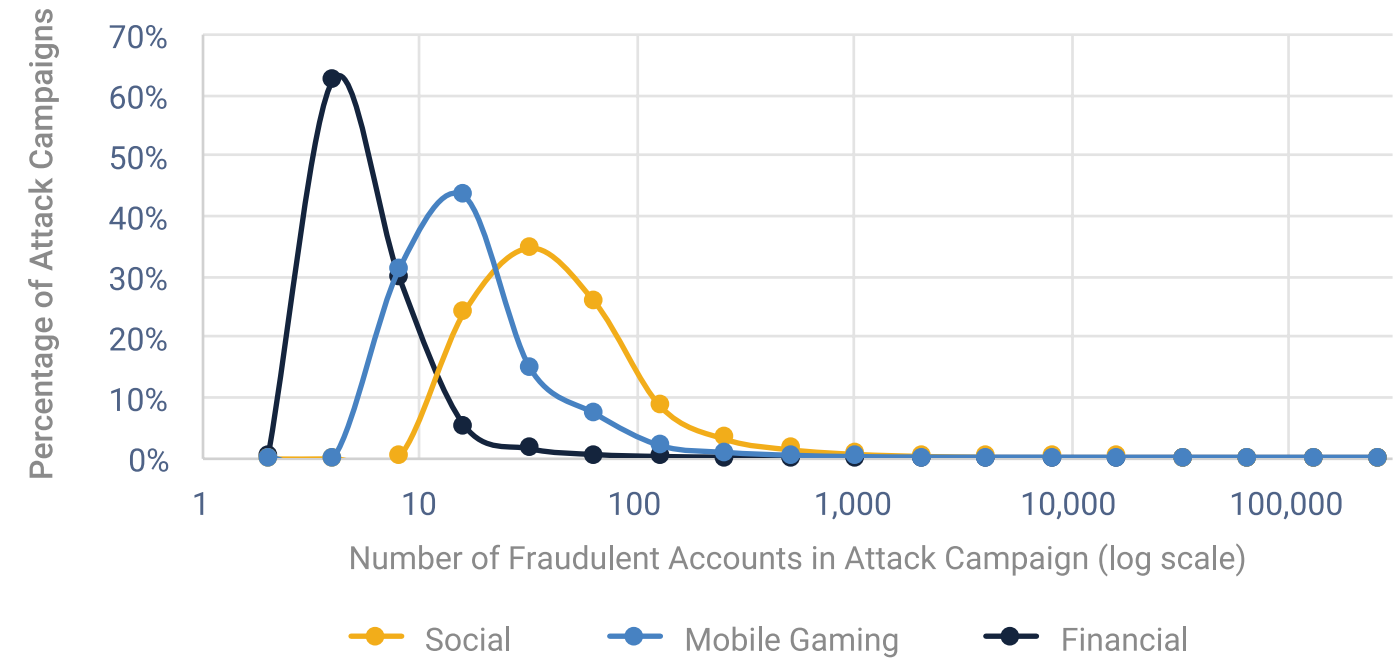
THE RISE OF THE SOCIAL BOTS

When it comes to the scale of fraud attacks, social platforms are hardest hit - the average attack campaign contains 160 fraudulent accounts, with the biggest ones having hundreds of thousands of fraudulent accounts. The large campaign size, together with the extensive use of cloud hosting services, shows that most of the attacks on social platforms are likely carried out by automated scripts. Social attacks are orchestrated this way due to the economics of spam and fake social reviews. In order to make it financially attractive for the fraudsters, they must conduct hundreds or thousands of attacks on a social platform and need a huge army of fake accounts to conduct these attacks.

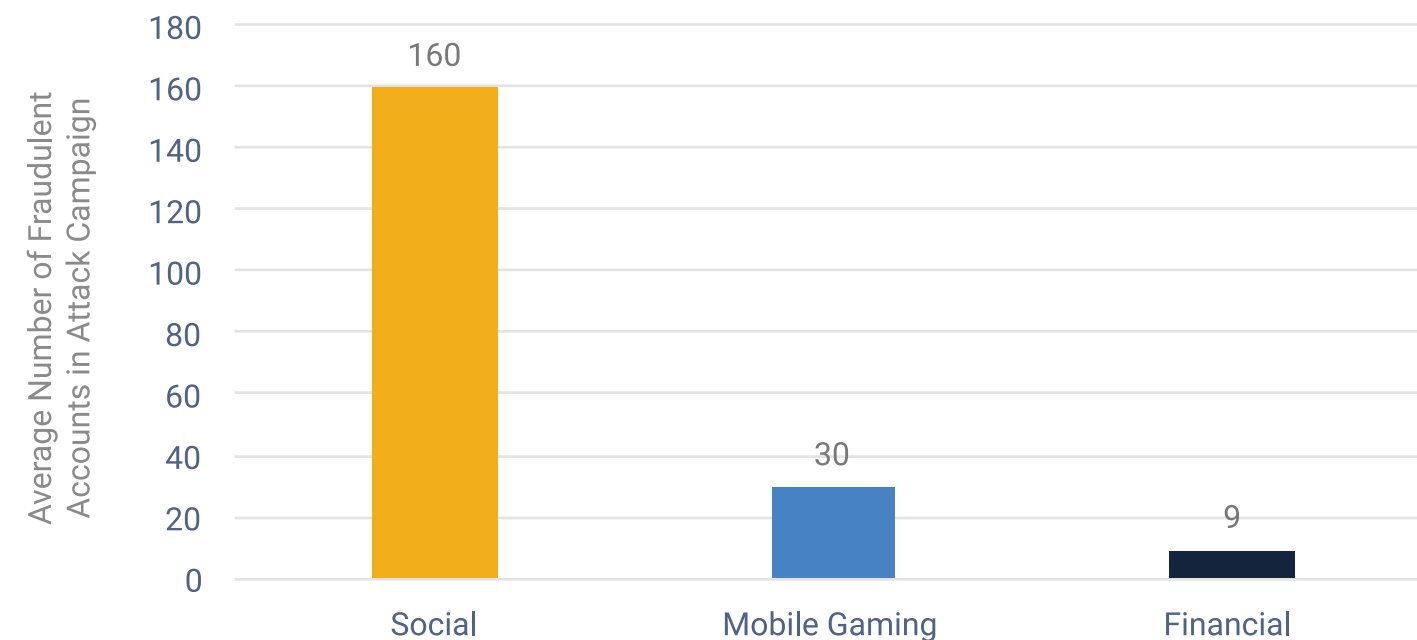
At the other end of the spectrum are fraudsters targeting financial services. In this case, the attacks are more stealthy, and likely manual, so as to blend in with normal users to avoid detection. The average attack campaign on financial services contains only nine fraudulent accounts. The reason for smaller campaigns may be due to fraudsters obtaining a higher profit margin from attacks on financial services, compared to social platforms where a large army of fake accounts are required to achieve the same result.

FRAUDULENT ACCOUNT ARMIES TARGETING SOCIAL PLATFORMS ARE 17X LARGER ON AVERAGE THAN THOSE TARGETING FINANCIAL SERVICES.

THE DISTRIBUTION OF THE SIZE OF ATTACK CAMPAIGNS ON DIFFERENT ONLINE SERVICE VERTICALS



THE SIZE OF THE AVERAGE ATTACK CAMPAIGN ON DIFFERENT ONLINE SERVICE VERTICALS



AGING ACCOUNTS

DON'T SLEEP ON THE SLEEPER CELLS

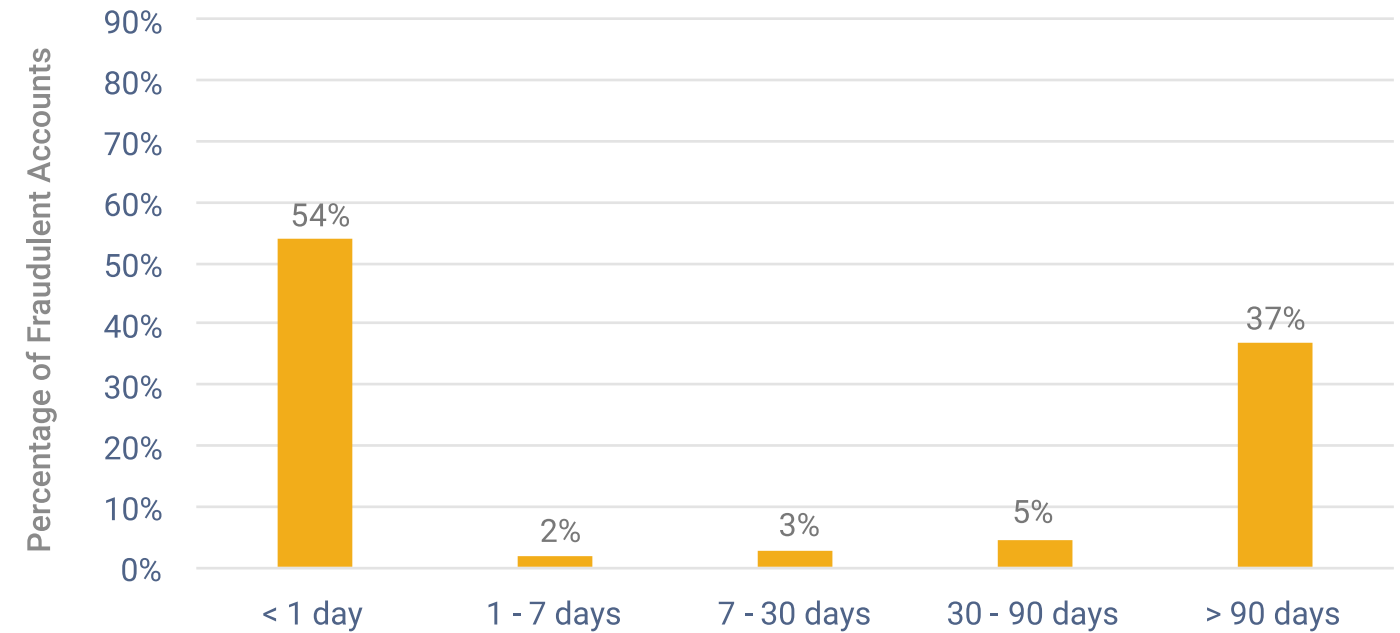
Most fraudulent accounts are short-lived. They are created for the purpose of launching an attack on the online service, and are quickly used and then abandoned. However, some fake accounts stick around for a long time, going undetected while performing normal user activities such as logging in, updating a profile, following other users, etc. These “sleeper cell” accounts are often used for testing or carrying out the attack in stages, and can lie in wait for months, or even years, before being used in an attack.

We took a close look at the fraudulent accounts created during the first three months of the second half of 2016. While 56% launched an attack within seven days of account signup, 37% have yet to attack even after three months.

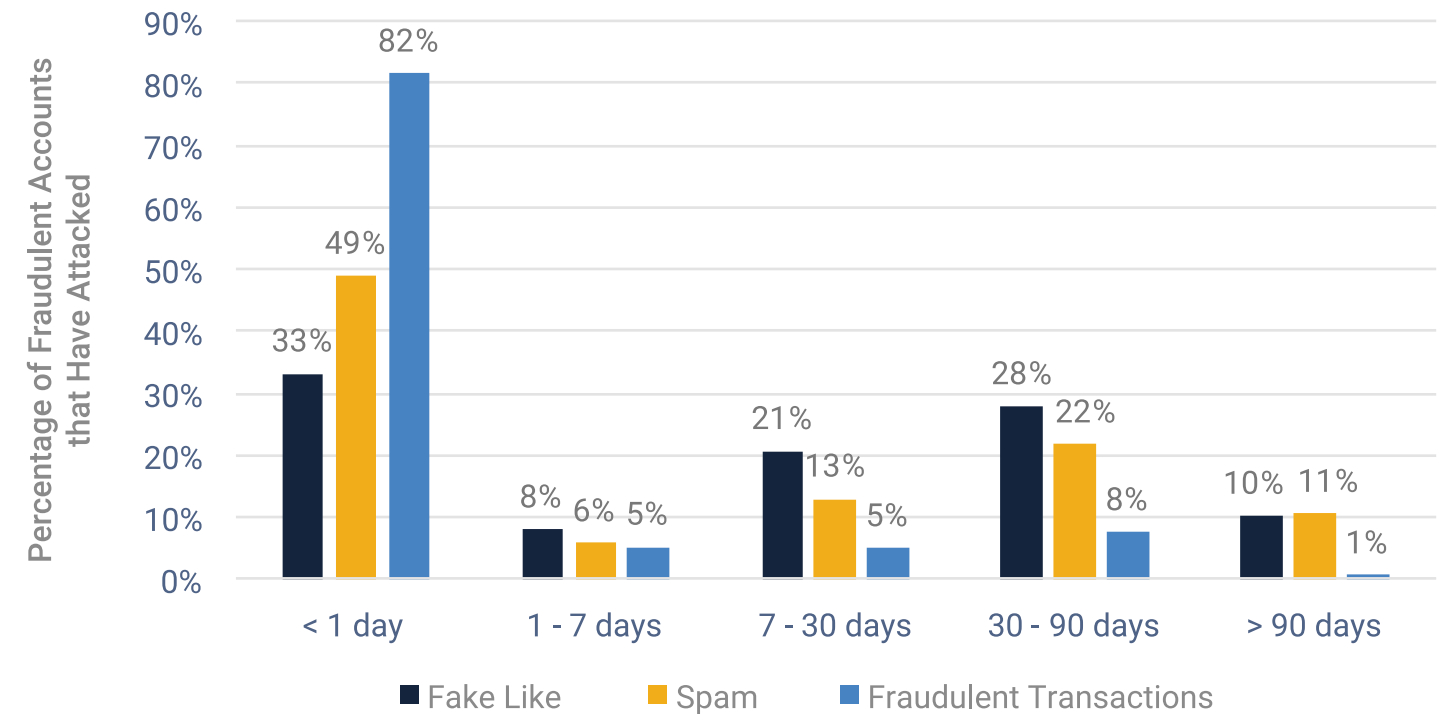
For those fraudulent accounts that launched attacks, we find that accounts used in social attacks, e.g., fake likes and spam, tend to have a longer sleep time compared to those used for financial attacks. One reason is that social attacks require a certain degree of trust from the victim to be successful, so having a longer history can help the fake accounts appear legitimate to normal users. By contrast, financial attacks are constrained by time, since stolen financial information (e.g., credit card numbers, banking information) expires quickly.

44% OF FRAUDULENT ACCOUNTS SLEEP MORE THAN SEVEN DAYS BEFORE ATTACKING.

THE “SLEEP” TIME DISTRIBUTION OF FRAUDULENT ACCOUNTS



THE “SLEEP” TIME DISTRIBUTION OF FRAUDULENT ACCOUNTS BY ATTACK TYPE, FOR ACCOUNTS THAT STARTED ATTACKING



GLOSSARY

ACCOUNT TAKEOVER: An attack type when a criminal gains access to a legitimate user's account, often through phishing, weak passwords, or buying compromised credentials on the dark web.

ATTACK CAMPAIGN: A group of fraudulent accounts controlled by the same attacker.

FAKE APP INSTALLS: A form of ad fraud based on the paid installations of a new app by fake or fraudulent accounts instead of real users.

MASS REGISTRATION: The creation of an army of fake accounts by a bad actor which will be used to conduct fraud.

MOBILE DEVICE FLASHING: A common technique for simulating the appearance of multiple new, distinct mobile devices by overwriting the current version of the mobile operating system with a custom version.

PROMOTION ABUSE: Exploitation or misuse of first-time user promotions, virtual currency arbitrage, out-of-policy virtual goods transfers, coupons/promo codes, etc.

SLEEPER CELLS: Fraudulent accounts that are created then stay dormant for a significant period of time.

SUPERVISED MACHINE LEARNING: A machine learning approach that uses labeled data to determine additional characteristics of the data sample automatically.

TELEMETRY: The process of gathering data together from disparate sources or clients to provide a global view

TRANSACTION FRAUD: An unauthorized or illegitimate use of credit card or bank account funds

UNSUPERVISED MACHINE LEARNING: A machine learning approach that does not rely on

rules or labeled data, but instead identifies patterns of correlated attributes.

USER AGENT STRING: A string identifying the system and browser version, language settings, screen resolution, plugins, etc., sent from the browser to a web server.

VIRTUAL CURRENCY ARBITRAGE: An attack type where a fraudster simulates his or her presence in different countries using proxy servers, purchases virtual goods with virtual currency in one location (generally one with weaker currency), and resells them at another location (generally one with stronger currency) and pockets the price difference.

CONTACT US

FOR MORE INFORMATION ON DATAVISOR SOLUTIONS:

info@datavisor.com
www.datavisor.com

MOUNTAIN VIEW (CORPORATE HEADQUARTER)

883 N. Shoreline Blvd. Suite A200
Mountain View, CA 94043

BEIJING

北京市朝阳区阜通东大街1号院
望京SOHO塔一C座1602
100102

ACKNOWLEDGEMENT

AUTHORS/CONTRIBUTORS

- ▶ Ting-Fang Yen, Research Scientist, DataVisor Threat Labs
- ▶ Dary Hsu, Product Marketing Manager
- ▶ Lisa Mokaba, Head of Media Relations
- ▶ Patrick Murray, VP Products
- ▶ Catherine Lu, Product Manager