ThreatMetrix

2017
Q2 CYBERCRIME REPORT

160 W Santa Clara St
San Jose, CA, 95113
United States

Telephone: +1 408 200 5755
Fax: +1 408 200 5799
sales@threatmetrix.com

threatmetrix.com

FOREWORD

"In the midst of chaos, there is also opportunity"

- The Art of War

Over the last few years, we have seen Cybercrime morph into a somewhat unique position in terms of crime classification, elevating out of the mere subset of cybersecurity and into the realm of a full blown criminal industry in its own right.

From Nation States to Cyber espionage; hacktivists to organized crime rings, although the attack motivations differ, attackers and methods are often the same. While recent global attacks on foreign governments and national infrastructures have brought the involvements of Nation States into sharp focus, continued attacks on businesses worldwide demonstrate the prevalence of global, networked crime rings that buy, trade and augment stolen identity data as well as perpetrate increasingly successful, large-scale attacks. Theirs is a highly-organized business that thrives on knowledge sharing and a well-skilled workforce.

Whether it be these organized outfits or an opportunistic petty criminal harnessing snippets of stolen information to appear more credible, the victim is always the end consumer. In an increasingly digital world, identity is the new currency and hence the impact of fraud on one's identity goes beyond financial losses. With the proliferation of identity data on the dark web and the rise of computational propaganda on the internet, many customers don't anticipate the longevity with which their stolen identity data can persist in perpetrating ongoing cyberattacks. Vulnerable customers are particularly susceptible to the effects of social engineering and phishing attempts, as hackers appear ever-more credible by combining information harvested from the dark web with convincing and professional emails/phone calls.

This makes a customer-first approach more critical than ever and if global digital businesses are to win against this multi-identity behemoth, they must look for the opportunity in amongst this increasingly organized chaos. And opportunity is not purely about having the best cyber-defenses, it is about taking a holistic approach to genuinely understanding the make-up of transacting users, and understanding the intricacies of their online footprint in order to accurately detect the infiltration of a fraudster.

Stolen credentials, validated identities and information are the fuel that stokes the value of cybercrime shares; digital identities are the counterpart for global digital businesses. ThreatMetrix digital identities comprise the crowdsourced intelligence from thousands of global businesses and billions of yearly transactions, collating intelligence and connections between devices, locations, identity information and threats, looking beyond isolated events and static information to the context of every transaction and the user who is making it.

Alisdair Faulkner, CPO

Q2

Cybercrime Report 2017

OVERVIEW

Knowledge Sharing and Crowdsourced Intelligence: Fighting the Cybercrime Behemoth

Cybercrime continues to grow, with organizations being attacked more than ever before. ThreatMetrix detected and stopped 144 million attacks this quarter and 300 million bot attacks.

The complex, networked nature of cybercrime attacks can be seen in the following key trends analyzed this quarter:

- The evolution of emerging economies in the cybercrime landscape as identity data trickles down to all regions of the globe following large-scale breaches
- The regional variations in attack vector trends, with South America emerging as a hub for new account origination fraud
- The emergence of highly organized criminal gangs targeting multiple organizations within the ThreatMetrix Network
- The rise in mobile attack rates as attackers turn their attention towards the growing mobile economy

To counter such trends, ThreatMetrix is pioneering the sharing of knowledge and information across key industry groups to better identify crime syndicates. This has been particularly successful in financial services, as fraudsters targeting one global bank can be accurately identified by other banks in the ThreatMetrix Network.

However, in the ever-evolving world of cybercrime, authentication continues to be a mainstay of global digital businesses; accurately recognizing trusted returning users and promoting a frictionless online environment builds a loyal customer base, reduces attrition and helps businesses better identify anomalous behavior.

Report Overview

The ThreatMetrix Cybercrime Report: Q2 2017 is based on actual cybercrime attacks from April – June 2017 that were detected by the ThreatMetrix Digital Identity Network (The Network) during real-time analysis and interdiction of fraudulent online payments, logins and new account applications.

The Network provides visibility and insight into traffic patterns and emerging threats. The Network analyzes close to two billion transactions per month, over 47% of which originate from mobile devices.

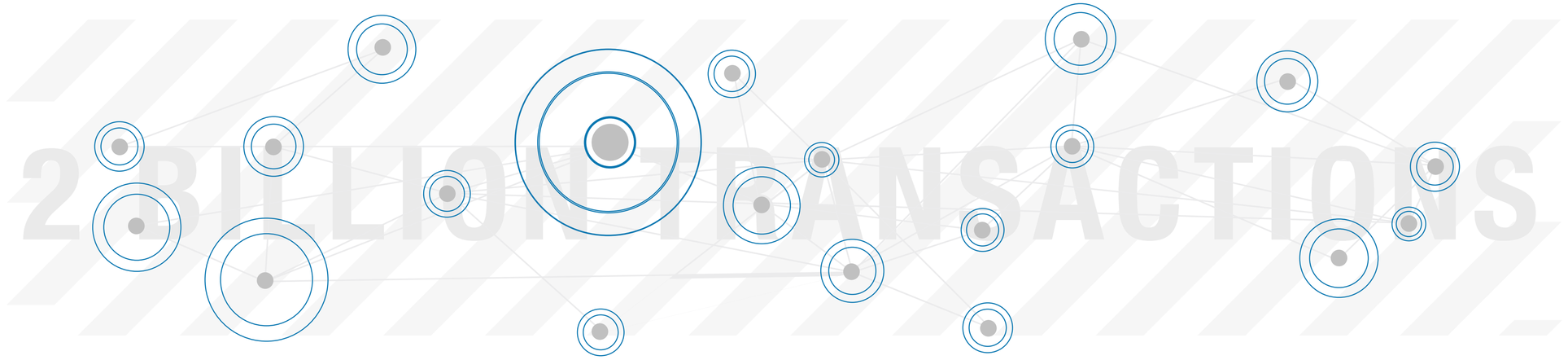
These transactions are analyzed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioral analytics.

The Network and its real-time policy engine provide unique insight into users' digital identities, even as they move between applications, devices, and networks.

ThreatMetrix customers benefit from a global view of risks, based on these attributes and rules that are custom-tuned specifically for their businesses.

Attacks discussed are from "high-risk" transactions scored by ThreatMetrix customers.

CYBERCRIME REPORT



Key Highlights

CYBERCRIME REPORT

ThreatMetrix analyzes transactions from top organizations across industries. Trends observed are representative of the key market trends:

Attacks continue to grow in size, complexity and frequency

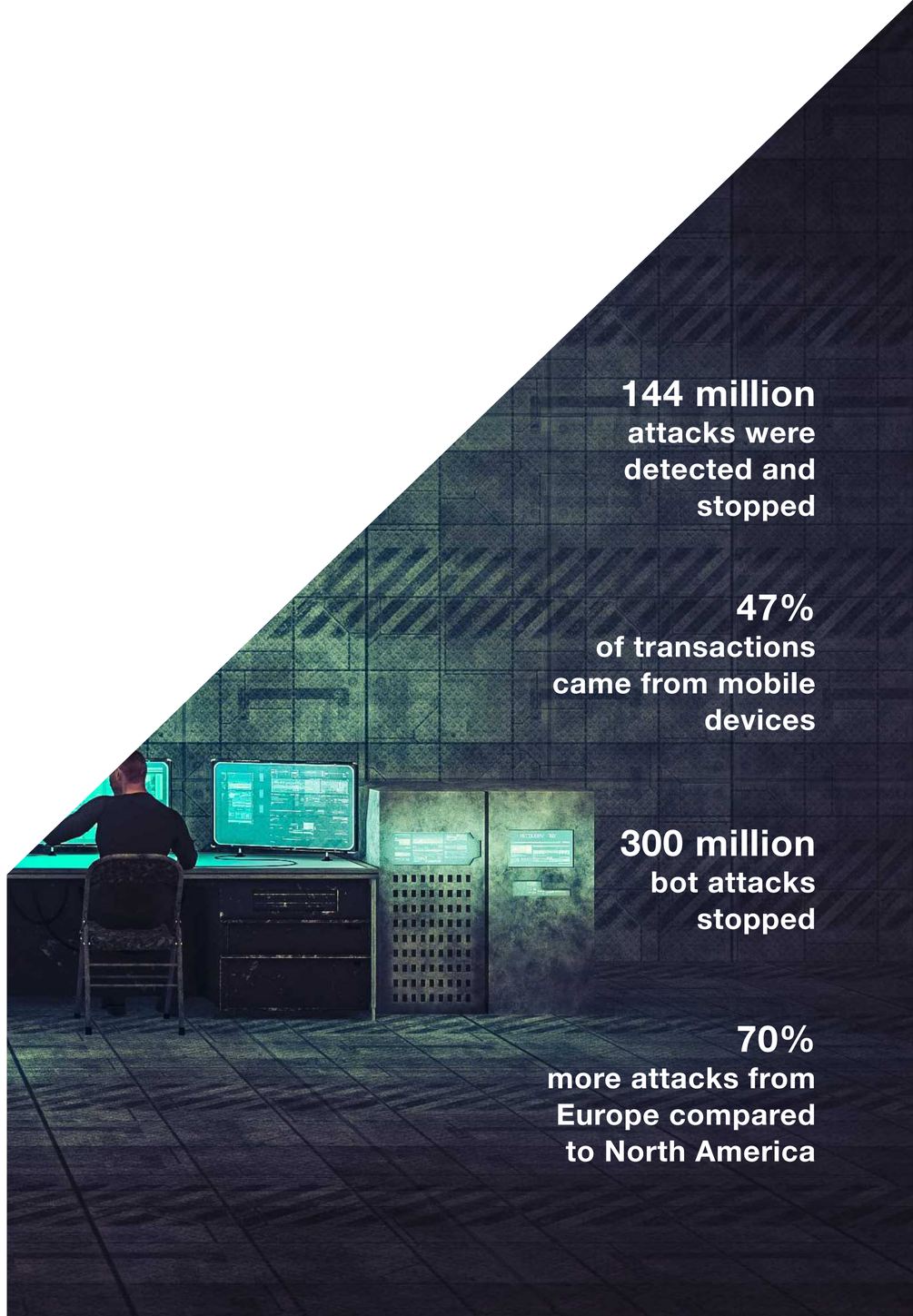
- Q2 2017 represented the highest levels of attacks detected and stopped by the ThreatMetrix Digital Identity Network:
  - 144M attacks were detected and stopped in real time; around 100% increase over Q2 2015.
  - The Network also stopped over 300M bot attacks predominantly originating from US, Germany, China, India, Vietnam, Brazil and Russia.

Regional anatomy of attacks

- Europe continues to be the hotbed of cybercrime growth with 70% more attacks compared to North America; European transactions are therefore riskier, and are twice as likely to be attacks compared to North America.
- South America is a global hub for new account origination attacks that target global media companies, while Europe is the key originator of account takeover attacks that mainly target US eCommerce merchants and European banks.

The evolving mobile story

- 47% of transactions now come from mobile devices, rising to 55% for new account creations highlighting the growing level of engagement consumers have with opening and managing key accounts on their mobile device.
- Mobile transactions are starting to be attacked more, particularly new account creations and payments, as fraudsters turn their attention towards the growing prevalence of mobile commerce.

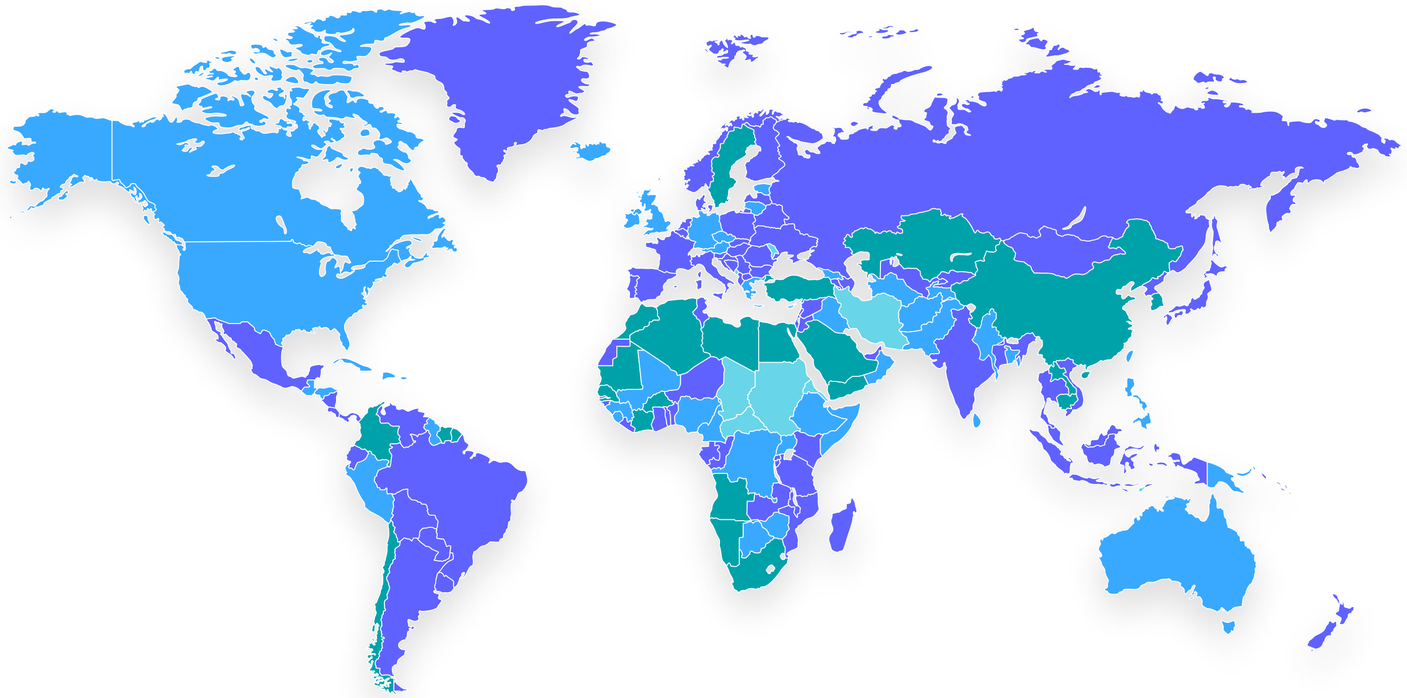


Using Digital Identity Intelligence to Enhance Recognition

CYBERCRIME REPORT

Recognition rate by country

95-100% 90-95% 80-90% <80%



Accurate recognition of a user's digital identity (based on device, identity, location and threat intelligence and combined with behavioral analytics) ensures that businesses are able to effectively differentiate between trusted users and potential threats, blocking high-risk events in real time.

As mobile usage continues to increase, so too does the overall recognition rate, driven by higher customer engagement and therefore more trusted customer interactions.

It therefore correlates that attack rates are lower when recognition rates are higher.

CYBERCRIME REPORT

Attacks are Highly Influenced by Global Breaches, With Frequent, Sustained Peaks

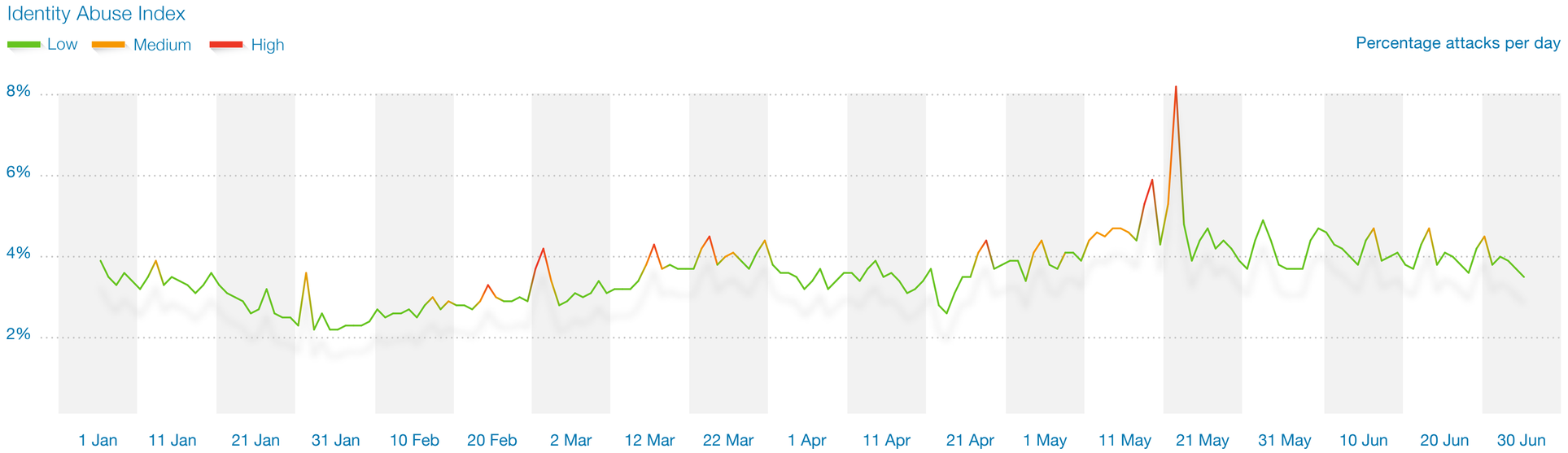
The 2017 data breach story has evolved from isolated attacks on large businesses and institutions to networked attacks targeting multiple key infrastructures and organizations, potentially originating from other nation states. Identity information is the primary ammunition in the cybercrime war for criminals that have access to the latest tools to launch mass scale attacks and fewer and fewer organizations are immune to this problem.

Cybercriminals continue to target financial institutions and payments providers that offer rich identity bounty if their defenses are breached.

An Identity Abuse Index level of High (shown in red) represents an attack rate of two standard deviations from the medium term trend. Aggregated over all global transactions, this clearly shows that the exploitation of data breaches and stolen identities is automated, global and coordinated.

Key spikes this quarter represent sustained attacks on some large global organizations as cybercriminals continue to mass test identity credentials before launching attacks on other corporations.

Attacks from some of the high-risk nations such as Pakistan also demonstrate how cybercrime can potentially be the revenue generator for other organized crime.



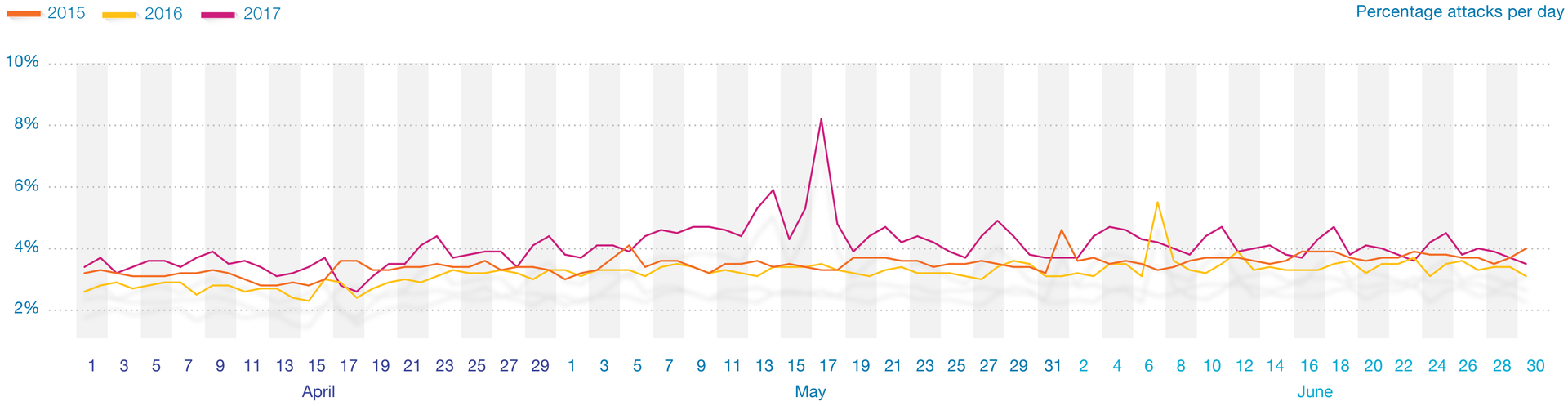
An Evolving Threat Landscape – 2015-2017

The growth and intensity of global cybercrime attacks is evident when looking at cybercrime data from the previous two years. Not only has the overall percentage of attacks increased steadily over the same time period for three years, but the attack patterns have changed and the peaks have grown more pronounced, as stolen identity data continues to have a greater and greater impact on global attacks.

It is clear that the fraudsters are opportunists, constantly looking to exploit gaps that arise in the period just after a big data breach or attack. For example, we see a huge spike in attack rates mid-May just after the WannaCry ransomware attack, indicating that fraudsters potentially took advantage of customer caution around carrying out online transactions in the wake of the attack, providing a better cover of disguise if the fraudster wanted to attack from a new location / device.

CYBERCRIME REPORT

Daily Attack Rates for Q2 (2015/2016/2017)

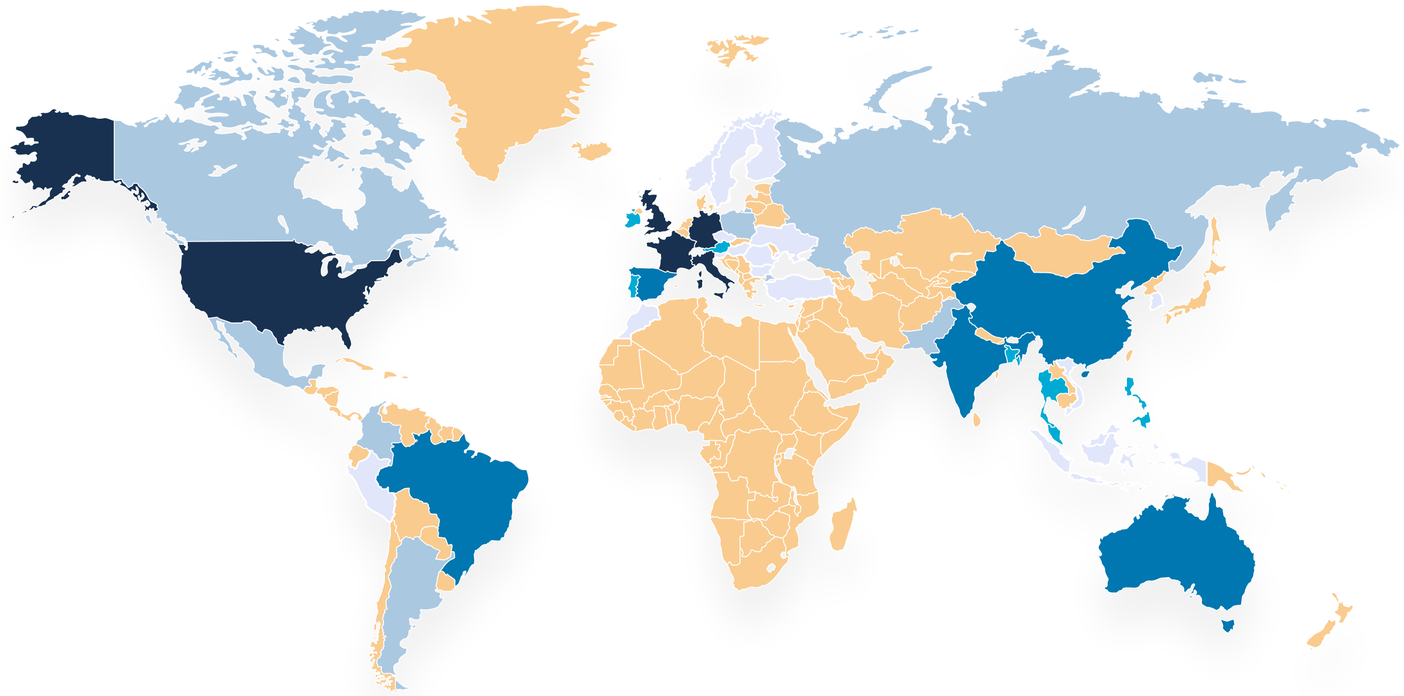


Attack Origins by Geography

CYBERCRIME REPORT

Attacks per Country of Origin

top 5 top 6-10 top 11-20 top 21-30 top 31-50 top 50+



Based on total number of attacks detected by geography of origin

Attack origins continue to shift and morph with every quarter, with an increasing number of attacks appearing from emerging and growth economies.

Q1 2017 saw an increase in attacks coming from several emerging economies with a particular prevalence in Central and South American regions including Cuba, Ecuador, Guatemala, Peru and Puerto Rico.

Q2 2017 sees a similar shifting pattern, however, attack increases came more from Middle-Eastern and Eastern European geographies including Croatia, Egypt, Georgia, Hungary, Israel, Morocco and Turkey.

The largest increase in attacks came from Pakistan, while Bangladesh and Vietnam were two other notable countries that spawned more cyberattacks.

What is clear is that breached identity data is filtering down to countries across the globe, and that cybercrime is becoming ever more global and networked.

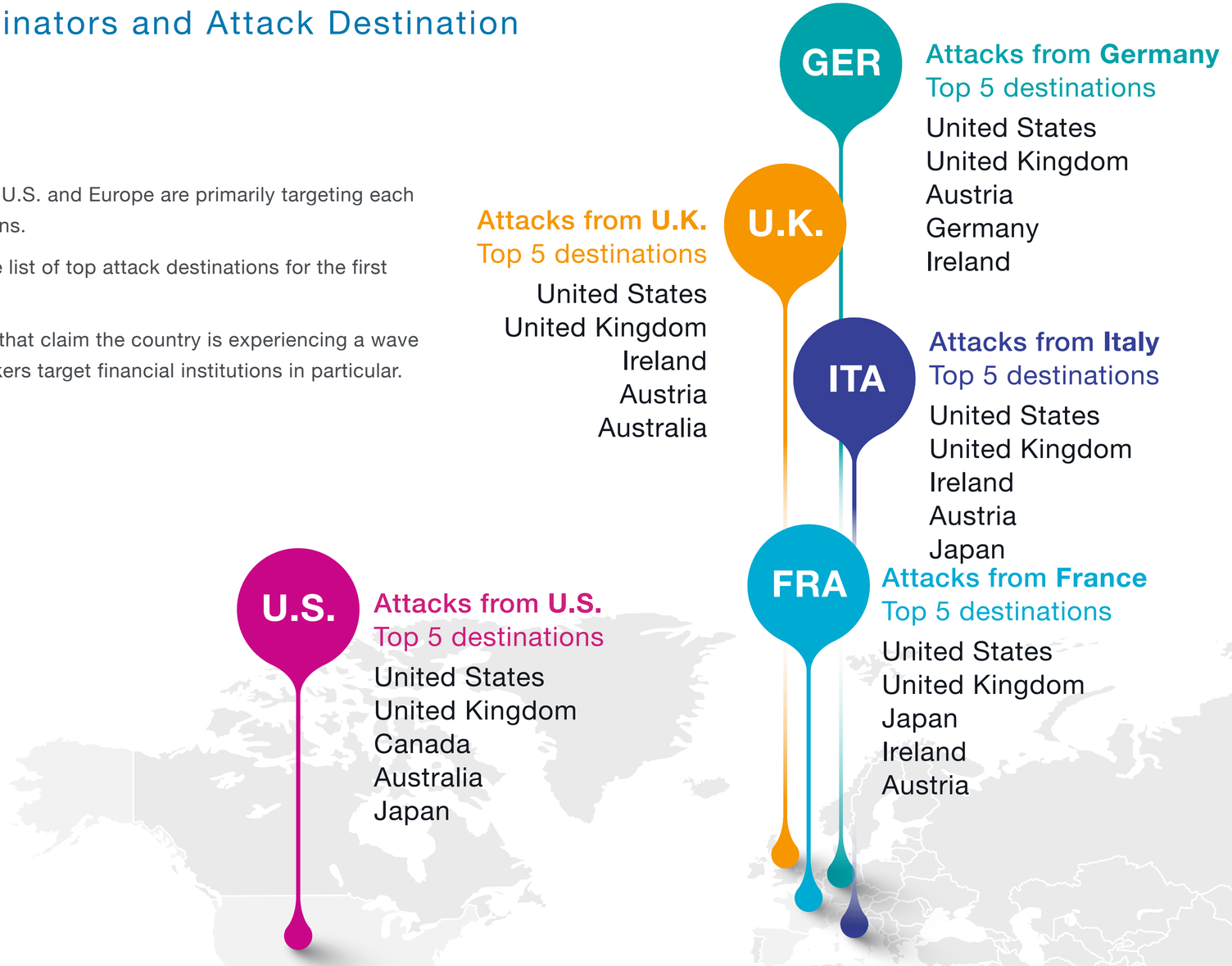
CYBERCRIME REPORT

Top Attack Originators and Attack Destination

The strongest economies of U.S. and Europe are primarily targeting each other and other similar nations.

Japan has emerged onto the list of top attack destinations for the first time this year.

This echoes several reports that claim the country is experiencing a wave of increased attacks as hackers target financial institutions in particular.



Transactions Analyzed by Type

ThreatMetrix transactions span eCommerce, financial services, insurance and media sectors and cover the authentication, payments and account creation use cases.

Attack levels show no signs of abating; we continue to see quarter-on-quarter growth in attack volumes making Q2 2017 the biggest attack quarter with over 144 million attacks.

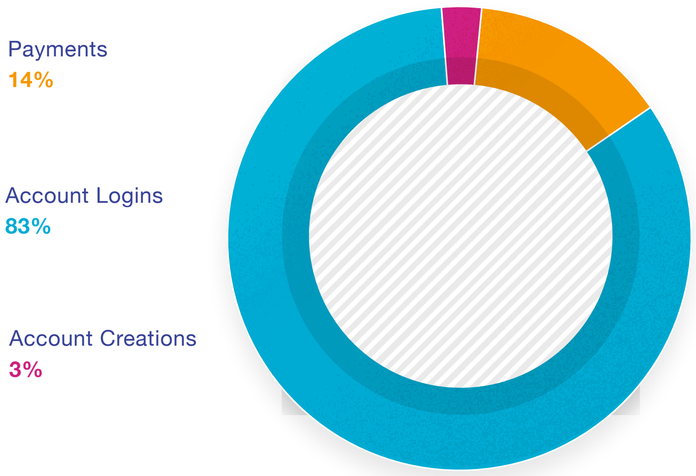
The growth in attacks continue to outpace transaction growth illustrating the heightened risk levels over the previous years with almost 100% more attacks this quarter compared to 2015.

Attacks also continue to rise across all use cases with a near 30% rise in account creation attacks since last quarter alone.

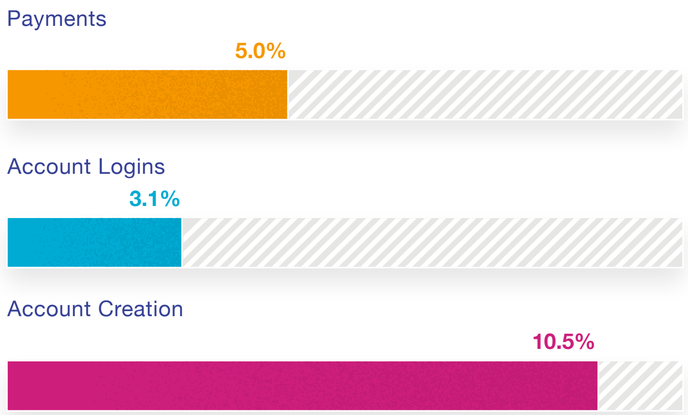
New account creation fraud now represents more than one in every ten new applications, driven by the increased availability and low cost of stolen identities in the wild, as fraudsters buy and trade stolen identity data to create near-perfect identities to use in large-scale attacks.

Mobile transaction volumes have grown 40% year-on-year with strong growth figures for new account creations and logins in particular, illustrating the increasing popularity of opening and managing accounts on a mobile device.

Volume per transaction type



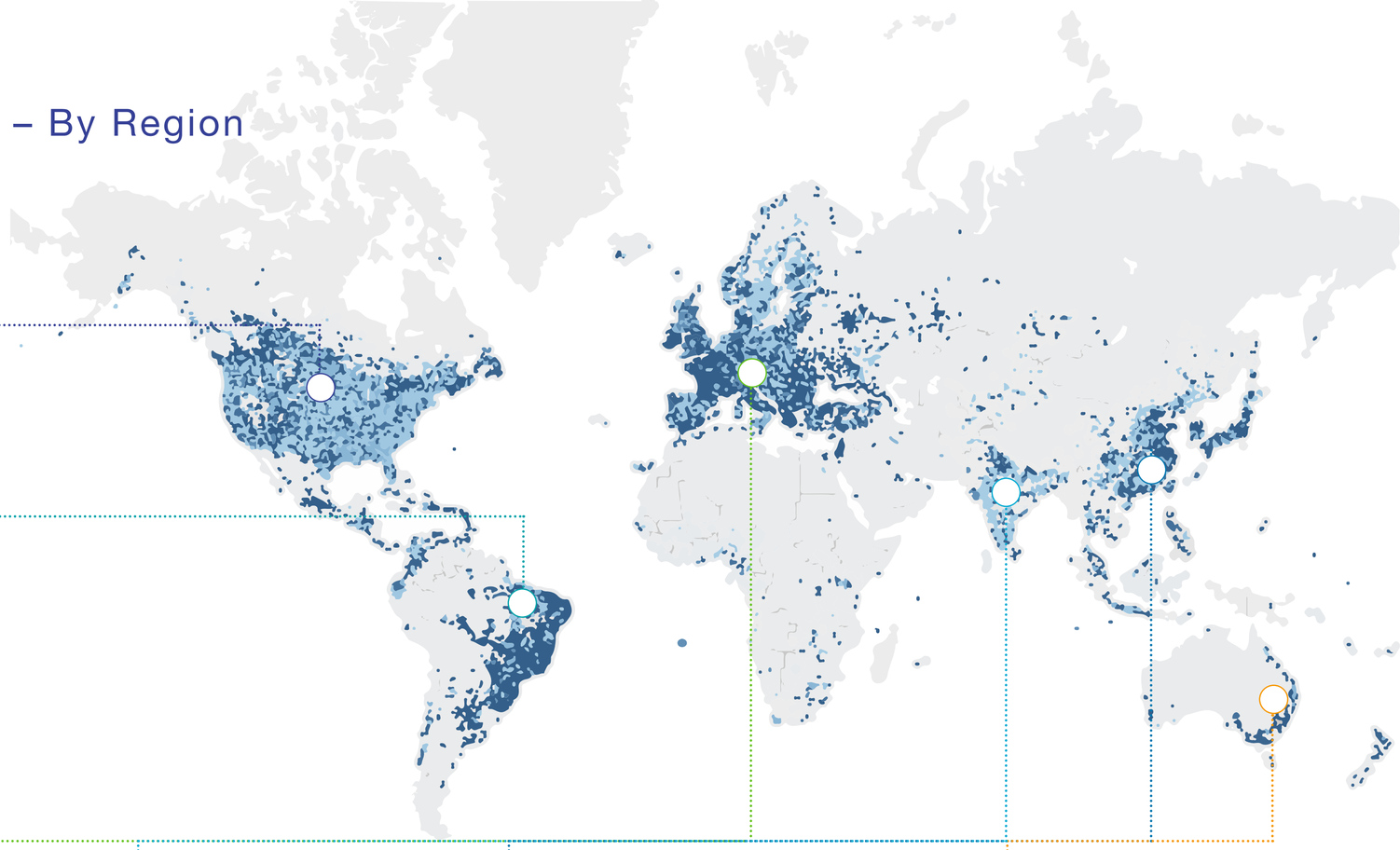
Attack rate per transaction type



Attack Percentages are based on transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically in real time dependent on individual customer use cases.

CYBERCRIME REPORT

Anatomy of Transactions – By Region



U.S.

- Businesses in the U.S continue to be the target of attacks from cybercriminals across the globe

SOUTH AMERICA

- Over 45% of all new account origination attacks come from Brazil, and primarily target digital goods that are easily consumed
- Payments is the largest use case, indicating a strong cross-border corridor
- Mobile penetration, while lowest, is growing

EUROPE

- Transactions from Europe are two times more likely to be attacked than those from North America
- Over half of all account takeover attacks originate in Europe, targeting U.S. eCommerce merchants and European banks
- Most mobile region: 53% of all transactions are mobile

INDIA

- Two times more mobile transactions compared to 2016
- IP spoofing is the biggest attack vector

ASIA

- Strong growth in organized attacks from the region, primarily focusing on account takeovers and payment fraud
- Highest instance of device spoofing and identity spoofing

AUSTRALIA

- Strong mobile penetration at 47% of all transactions
- Device spoofing continues to be the biggest attack vector
- 83% of all attacks in Australia are account takeover attacks

Country Showcase – **Canada**

Canada has one of the highest adoption rates of digital banking, internet usage and smartphones, making Canadian customers truly digital-first.

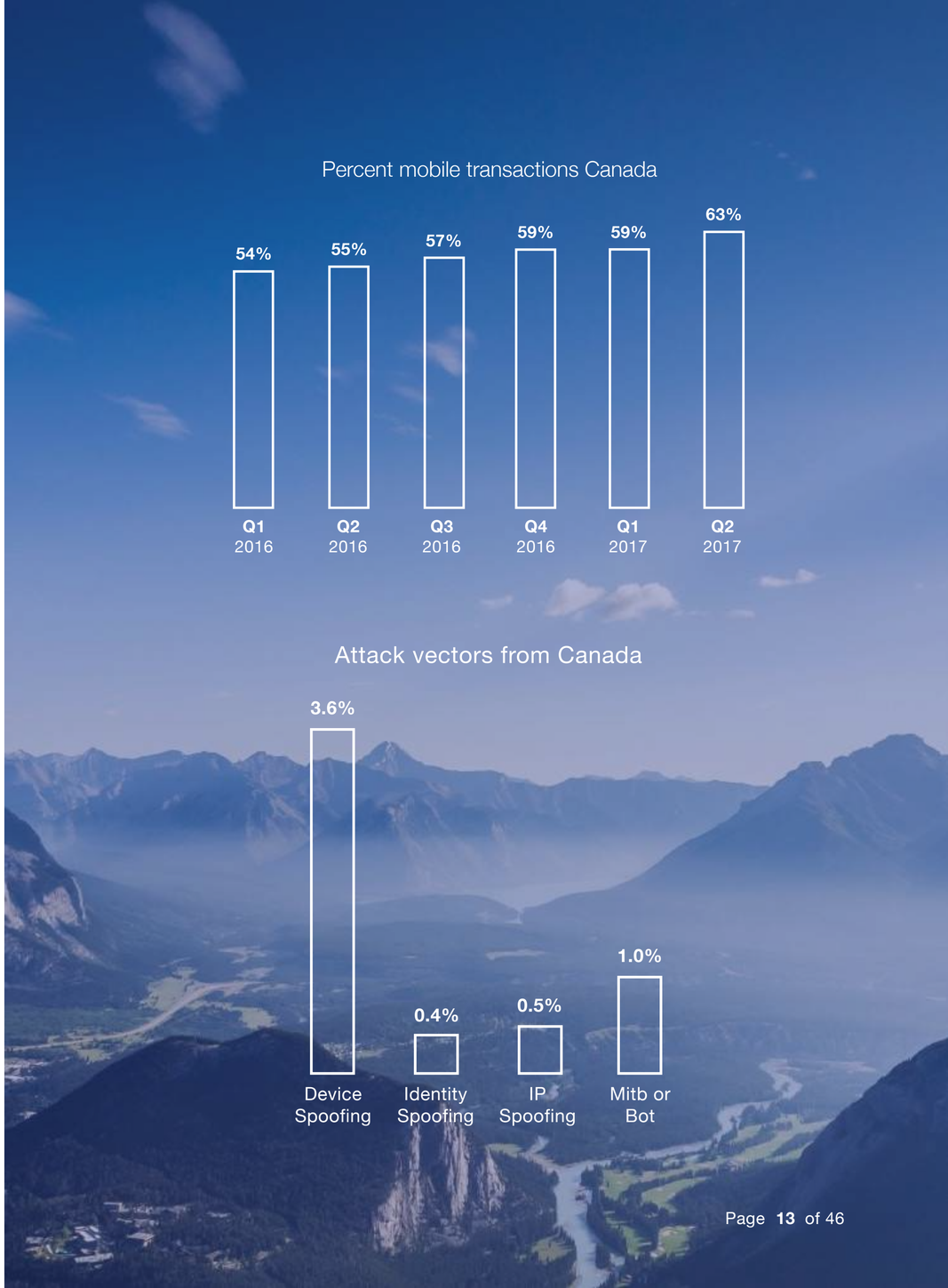
This highly-banked customer base constantly accesses their banking services on the go as showcased by the high share of mobile transactions. This makes trust a key business imperative.

In addition, mobile transactions are growing quarter-on-quarter, which potentially explains the overall low attack rates as mobile transactions continue to be safer than desktop.

With a high volume of digital interactions, Canadian businesses continue to be one of the prime targets for cyber attacks from across the globe.

Device spoofing is the biggest attack vector as fraudsters delete and change browser settings in order to modify their device identity or fingerprint, or try and appear to come from a victim's device.

Note: The bar charts represent percentage of total transactions that were recognized as attacks



CYBERCRIME REPORT

Country Showcase – India

India is a fast-growing digital economy with strong growth across eCommerce, FinTech and online banking.

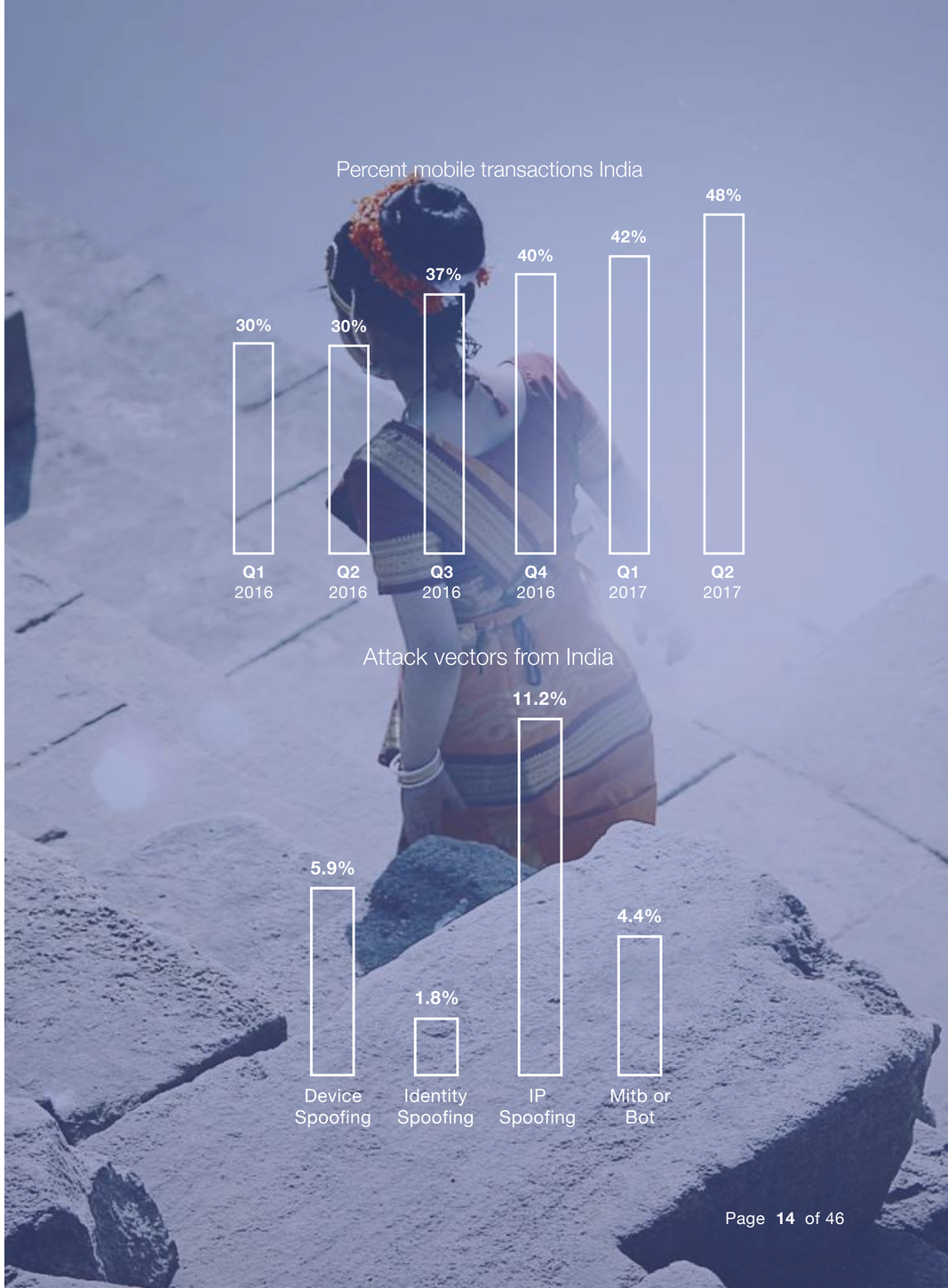
While a large proportion of the population remains unbanked/underbanked, internet and mobile penetration is growing rapidly. As such, mobile is quickly becoming the bridge to drive financial inclusion where traditional forms of banking methods aren't accessible. This is evidenced by the fact that mobile transactions now make up around half of all India's transactions.

Despite the consumer shift towards online commerce, digital sophistication and knowledge of security and fraud risk is still relatively immature, making consumers more vulnerable to social engineering / phishing attacks. This contributes to high overall attack rates.

In addition, card penetration is still low, which creates logistics challenges around payments: many retailers still favor a cash on delivery payment method. Although this provides flexibility for consumers, it adds significant logistics costs for merchants, with higher volumes of rejected orders and multiple delivery attempts to customers who aren't home.

This emerging digital landscape has fueled strong pockets of fraud, as India emerges as both a fraud originator and a destination for attacks. Indeed, one in ten transactions in India is rejected. Cash on delivery fraud sometimes happens in collusion with a shipping company, which has prompted retailers to block transactions/shipping in certain regions. This contributes to the high IP spoofing rates, as fraudsters attempt to bypass location blocks.

Note: The bar charts represent percentage of total transactions that were recognized as attacks



CYBERCRIME REPORT

eCommerce Transactions and Attacks

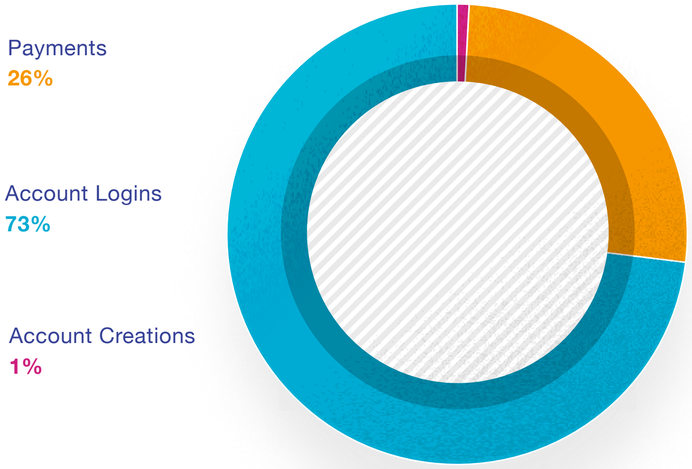
The eCommerce industry experienced 88 million attacks this quarter. As a percentage of overall transactions, this attack rate has increased 41% year-on-year.

In tandem, the proportion of mobile transactions in eCommerce has similarly grown by almost 40% year-on-year, and nearly 20% just since last quarter, illustrating the continuing drive for consumers to open and manage accounts on their mobile device.

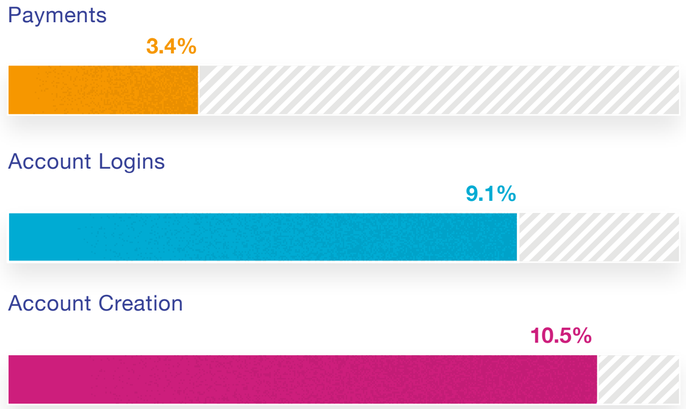
Login transactions continue to be attacked much more heavily in eCommerce than in other industries, as fraudsters look to capitalize on the growing propensity to save credit card information to selected trusted brands. A breached account offers increasing opportunities to steal data as well as make future fraudulent purchases.

Login attacks also offer cybercriminals the stage to create fake travel reviews, manipulate listings information and even monetize stolen credit card details, making eCommerce accounts a potential fertile breeding ground for sustained and pernicious attacks.

Volume per transaction type



Attack rate per transaction type



Attack Percentages are based on transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically in real time dependent on individual customer use cases.

Diverse Factors Shaping the eCommerce industry

CYBERCRIME REPORT

The eCommerce industry continues to be shaped by several key factors:

- Logistics is one of the key competitive differentiators for retailers as they seek to be the destination of choice for habitual and everyday purchases.
- Customer behavior is changing with fewer purchases happening in-store and long online browse-to-purchase cycles.
- EMV continues to drive payment fraud online while availability of identity data is causing an increase in account takeover fraud.
- Growth in cross-border transaction traffic as digital customers expect to be able to purchase from an increasingly global marketplace.
- Seasonality still affects the industry with increased traffic around key shopping periods like back-to-school and holiday periods.
- New business models are emerging including the rise of the sharing economy, installment purchases and instant online loans.
- The importance of a low-friction customer experience is paramount. Intervention, slow paths to purchase and poor online user experiences all cause cart abandonment and/or defection to a competitor.

eCommerce transaction volumes follow a fairly cyclical weekly pattern throughout with small peaks and troughs registered each week.

Overall attack rates are fairly high in comparison to some other industries, driven by high new account creation and login attacks.

Evolving Patterns of Holiday Shopping

2016 revealed that holiday shopping is no longer the nail-biting 100m sprint, but rather day three in a five-day cricket test match; exploding out of the confines of a few key days to be a year round phenomenon, with multiple shopping peaks.

Consumers are constantly on the lookout for deals, and retailers are attempting drive conversion and maximize transaction volumes and basket sizes year-round.

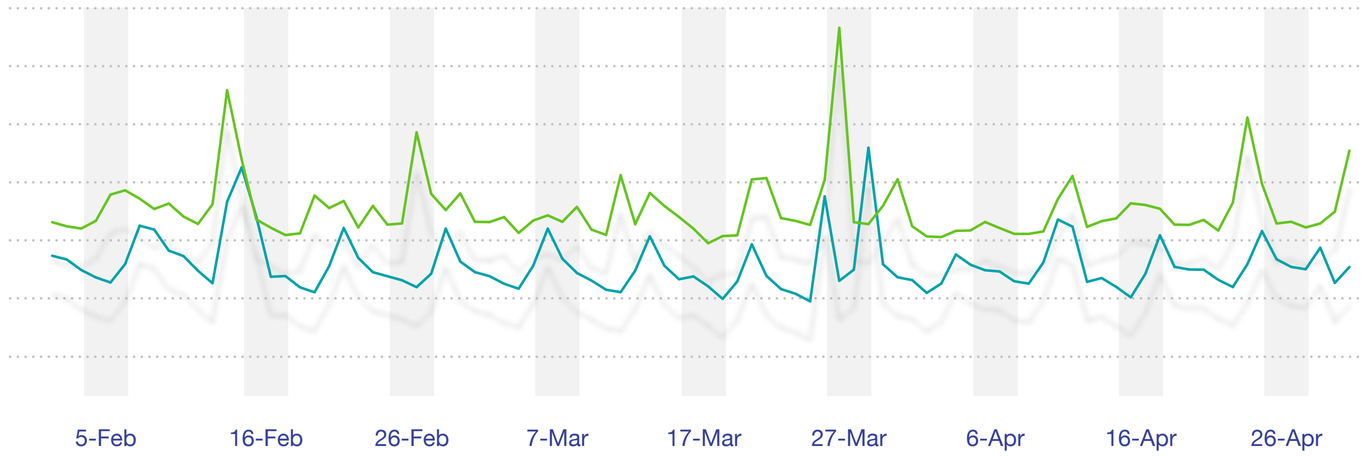
Easter has recently been reported as one such busy shopping peak, particularly around electronic sales.

Similar trends are starting to emerge in the Network, with peak transaction volumes evolving year-on-year around March and April, coinciding with the Easter holiday period.

Easter Peaks

Merchant One Merchant Two

Payment transactions for two online merchants



CYBERCRIME REPORT

2017 Holiday Predictions

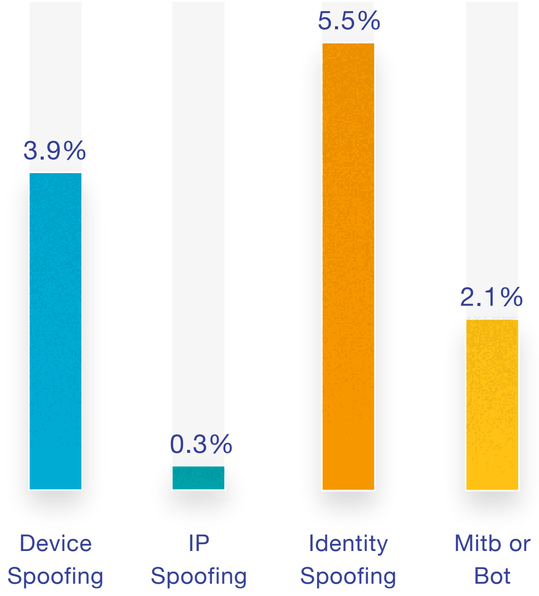
CYBERCIMRE REPORT

- Holiday shopping will become a year-long commitment with sustained transaction peaks during key shopping days.
- Online commerce will outpace in-store, with the biggest disparity during the holiday season.
- Retailers will see a volume shift to non-traditional methods of purchasing and gifting, including gift cards/ gift card trading, online subscriptions, travel bonuses etc.
- This move towards digital gifting along with the adoption of same day shipping will better enable last minute shoppers.
- Mobile engagement will continue to grow and cross-device recognition will be imperative.
- Cross-border traffic will form a growing slice of key retailers' digital commerce with other geographies looking to access deals during the holiday period.
- Fraudsters will capitalize on rising gift card trends and increase fraudulent gift card purchases made with stolen credit cards while also attacking gift card merchant sites.

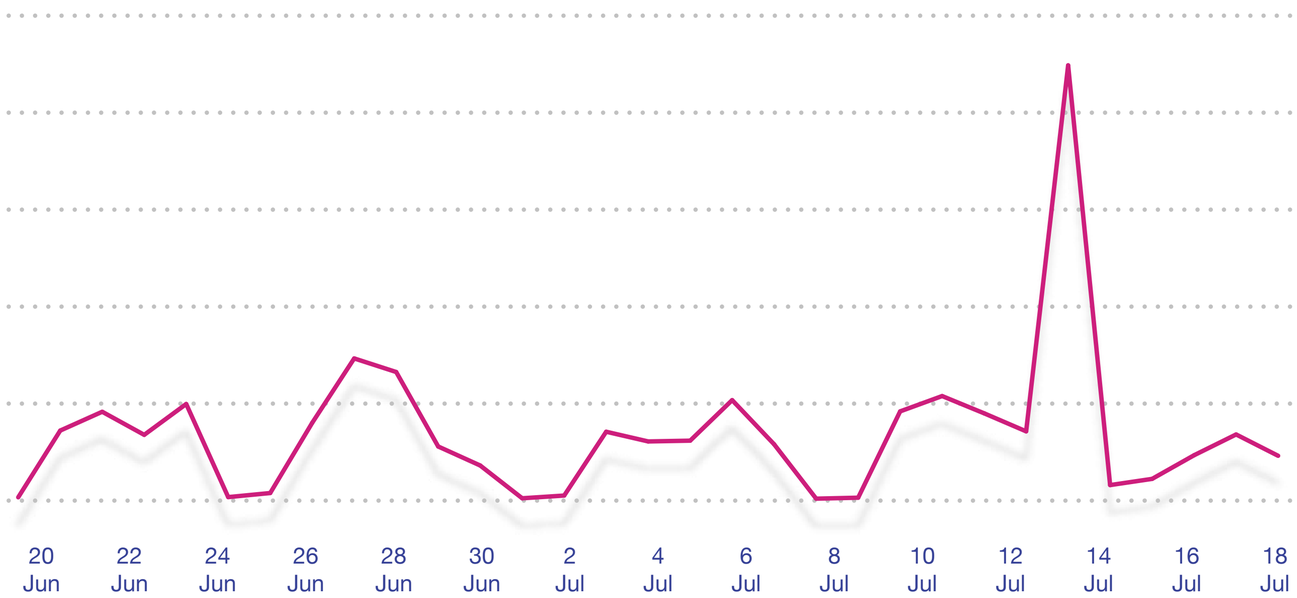
CYBERCIMRE REPORT

The Rise of Shopping Loans

Attack vectors



Daily bot attacks



Online shopping requires access to digital payments which is sometimes difficult for the unbanked and underbanked. At the same time, many millennials don't have credit cards; the most prominent payment method online.

To effectively access these customers, new providers have emerged to provide instant loans to purchase items from their partner retailers. These providers offer instant loans of up to $10,000 as a payment option at checkout with interest-free periods.

This offers consumers access to instant funds to buy what they need, and in turn gives merchants the ability to target new demographics.

Fraudsters are opportunists and are currently preying on the rising popularity of shopping to apply for funds using stolen credentials.

The Network sees suspicious transactions (account creations, logins and payments) coming from the same device using different email addresses, as fraudsters attempt to take out fraudulent loans or hijack trusted user accounts.

Device and identity spoofing attacks are particularly prevalent for this sub-industry, as fraudsters dupe unsuspecting businesses into believing they are a legitimate, trusted customer by using stolen credentials from the dark web.

In addition, the Network also detected constant credential testing bot attacks on this sub-industry.

CYBERCRIME REPORT

The Growing Popularity of the Ridesharing Economy

Nothing has been more transformative to travel in recent years than the growth of the ridesharing economy.

A truly mobile-first industry, ridesharing has simplified and globalized access to cheap and simple transport for a highly-mobile customer base.

Along with strong customer demand, this industry is also constantly battling fraudsters that try to use the business model to monetize stolen credentials.

This can be done in a variety of ways:

- Taking a trip using a stolen card
- Propagating two-party fraud using a “fake driver” account to go with a “customer” using stolen credentials
- Creating fake accounts to launder/make money/make false insurance claims

ThreatMetrix detected an attack on a ridesharing organization in the Network, where 30K devices had “Mock Location” settings enabled while using the app. This has the same effect as a DDoS style attack: the company didn’t have the drivers to meet demand, forcing some genuine users to switch to a competitor service.

Evolving Threats in Gaming and Gambling

CYBERCIMRE REPORT

The gaming and gambling industry continues to be a hot target for fraudsters, from new player bonus abusers to fraud rings taking part in collusive play or using stolen credit cards to make fraudulent bets.

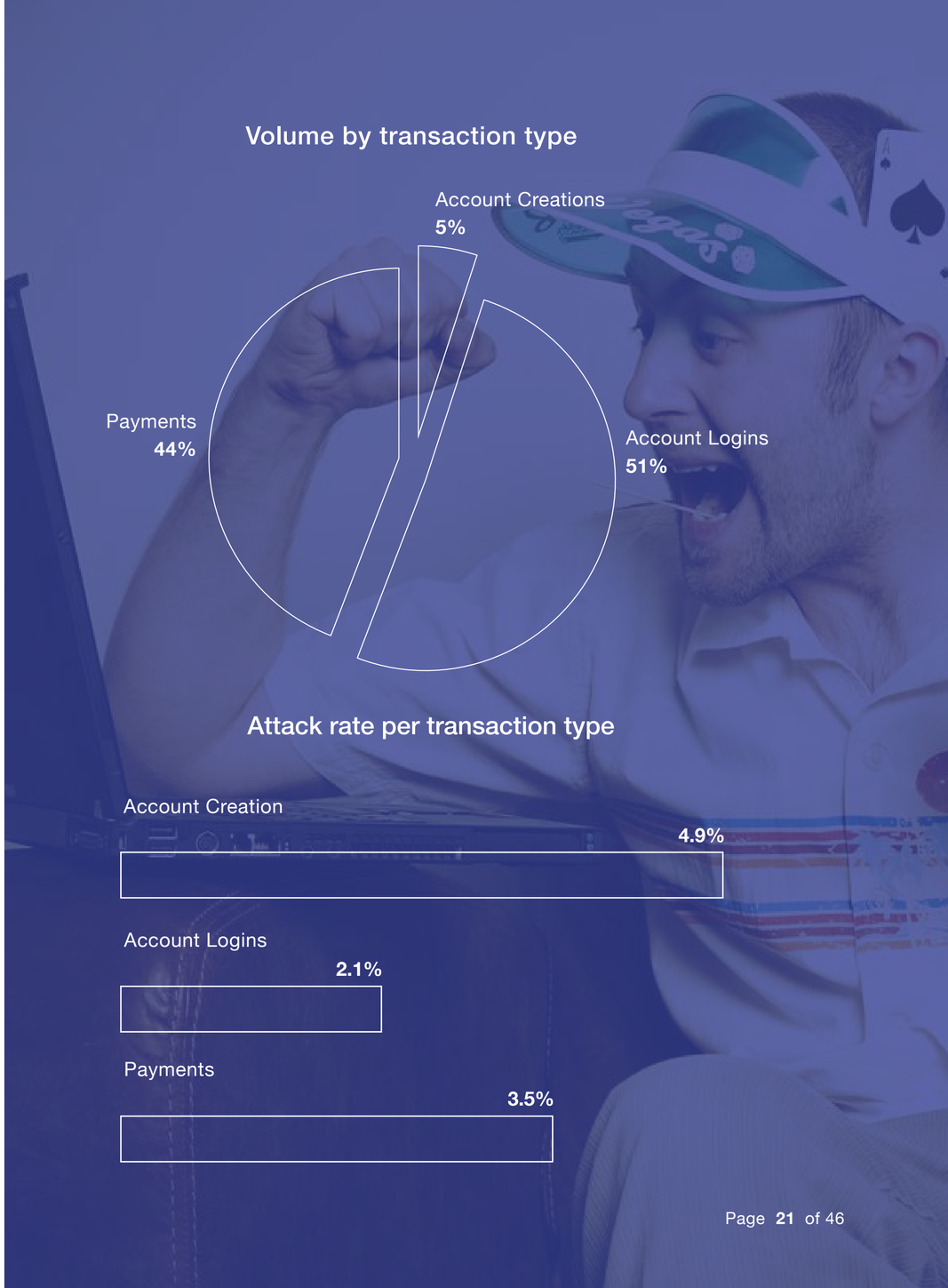
The rise of mobile engagement and in-play betting has put the onus on real-time detection of high-risk activity. Mobile transactions account for more than half of all traffic.

In addition, gambling companies are under increasing pressure to comply with regional regulations that encourage responsible behavior; this includes detection of problem gamblers and self-excluders that may have returned to bad habits using stolen or borrowed credentials.

The industry also sees a high proportion of cross-border traffic, with 35% of transactions originating outside the country of origin. However, this varies greatly by regions with some specific local trends / nuances in betting patterns and a number of organizations opening in strategic geographies which attract a higher proportion of cross-border traffic.

As expected a large proportion of gambling transactions are payments and despite the risks, the current attack levels are reasonably controlled compared to other industries.

However attack rates are showing signs of some growth, particularly in new account creations and payments, indicating the fact that fraudsters may be cultivating fraudulent accounts to make bets with stolen credit cards.



Bots Attempt to Take Over Accounts in Gambling

The gaming and gambling industry saw a number of sustained bot attacks throughout the quarter, with bots making up half of all daily traffic at the height of large attacks.

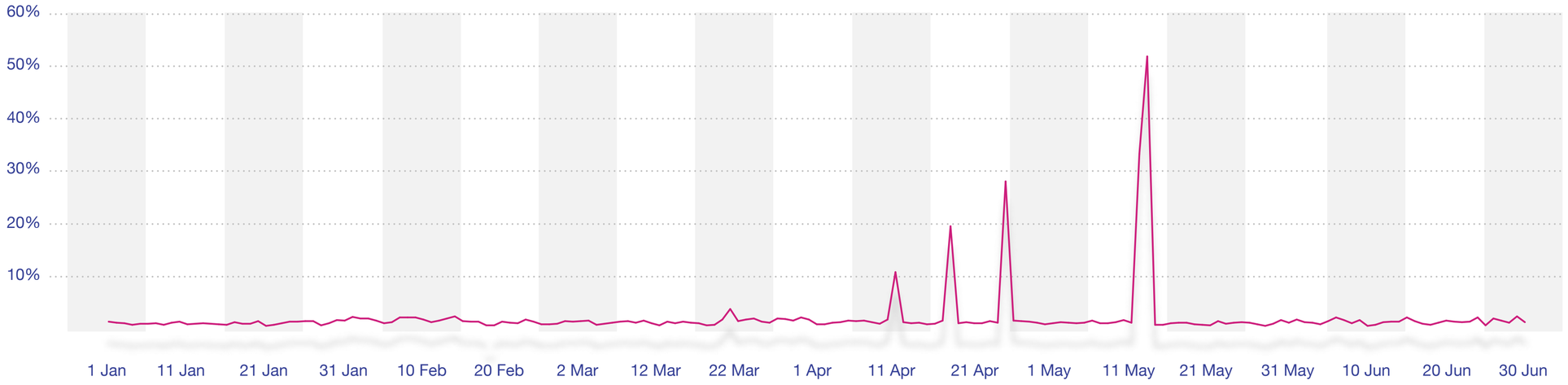
These bots were predominantly targeting account logins, indicating fraudsters trying to hack in to good user accounts using stolen credentials harvested from the dark web / data breaches.

A successful attack may provide the fraudster opportunity to steal more identity data, access card-on-file details to make large bets or to steal account credit.

CYBERCIMRE REPORT

Daily bot attacks

Gaming / gambling



CYBERCRIME REPORT

Financial Services Transactions and Attacks

Financial services growth continues to be driven by mobile transactions, as users adopt mobile banking as one of the primary means for accessing and managing accounts. 54% of all financial services transactions in the Network originate from mobile devices.

Overall login transaction volumes have grown 35% year-on-year and mobile logins 46%. This proliferation of login transactions allows financial institutions to build a more complete picture of their transacting users, developing trust over time, hence the low attack rates.

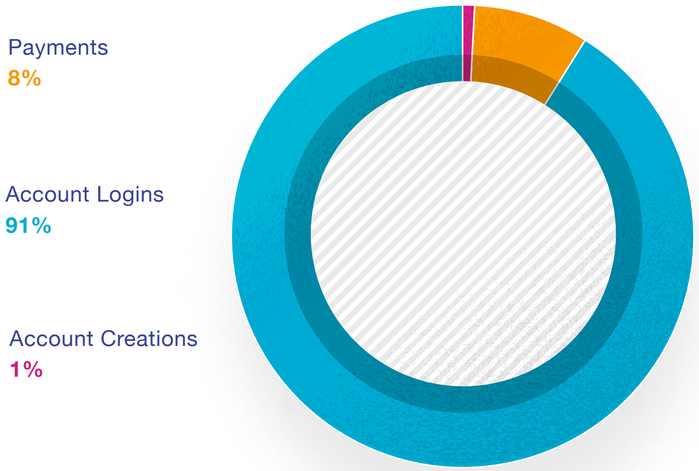
Interestingly, however, mobile account creations are now growing faster than any other use case – 141% year-on-year – as users are embracing mobile banking as a full-service operation, rather than to just check bank balances on the move.

Account creation attacks have continued to increase – 200% compared to 2015. This is driven by the availability of complete user credentials on the dark web that fraudsters look to monetize by applying for new loans or other financial products.

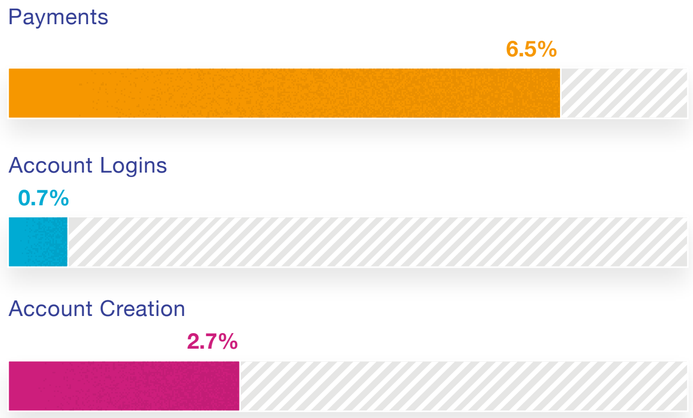
While account logins attack rates look low, organizations are less likely to block suspicious transactions outright, subjecting them instead to further review. Hence, the attack rate shown doesn't include access attempts that typically result in a challenge / step-up response.

Payments transactions are particularly susceptible, however, as fraudsters target new and emerging FinTech providers to try and make a quick buck on, for example, fraudulent remittance. This is highlighted in the fact that the percentage of rejected payment transactions has grown 160% year-on-year.

Volume per transaction type



Attack rate per transaction type



Attack Percentages are based on transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically in real time dependent on individual customer use cases.

The Power of a Networked Consortium to Identify and Block Fraud

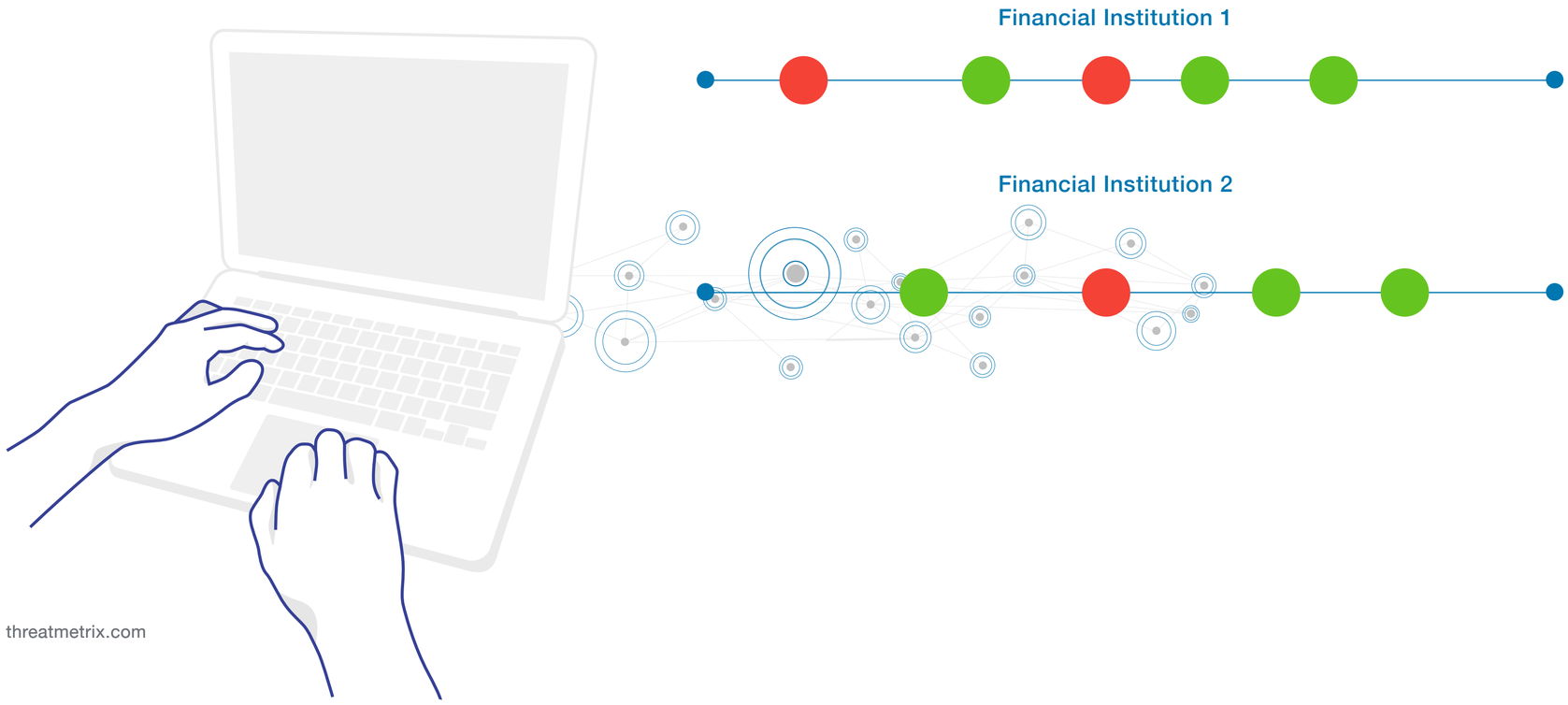
Leveraging Dynamic Shared Intelligence

Financial services fraud is a complex and interconnected beast, with fraud rings targeting multiple organizations for maximum gain.

By sharing threat intelligence across financial institutions, ThreatMetrix can enable banks to better identify and block fraudsters who are working across the industry.

The diagram below illustrates a scenario from the Network where one financial institution identified a device as high-risk and put it on the blacklist.

Another financial institution looking at the same device, identifies key accounts as recipients of fraudulent funds because of this shared intelligence.



The Evolving Mobile Story in Financial Services

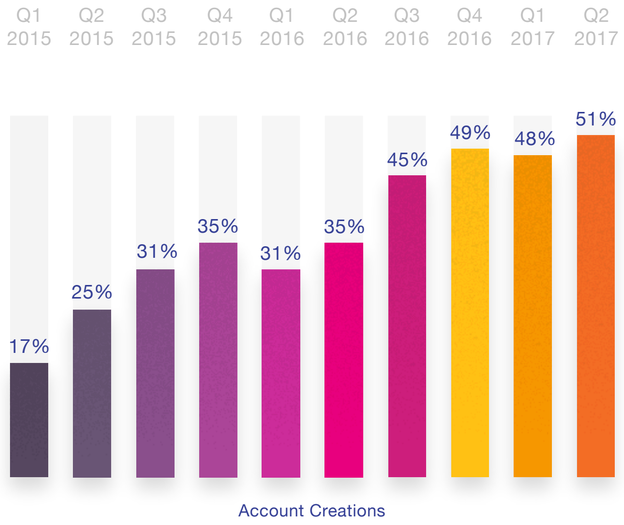
Mobile transactions continue to transform the face of digital banking, as users drive the ongoing development of full-service banking apps that often negate the need to visit a branch.

This growth is particularly prevalent in account creation and login transactions; payments are currently growing at a more conservative pace, as consumers are perhaps more reluctant to type in payment credentials on a mobile device.

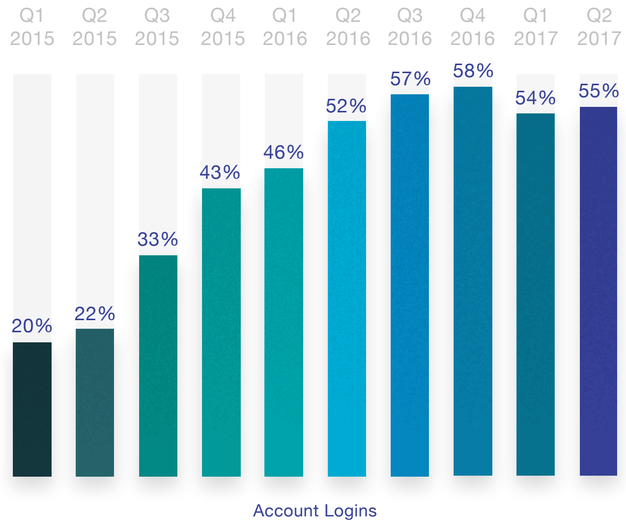
The growth of account creation transactions is reflected in the comparatively high identity spoofing attacks on mobile transactions; fraudsters see the opportunity to sign up for new accounts in the mobile channel using stolen / spoofed credentials, using these as a gateway to further attacks.

CYBERCIMRE REPORT

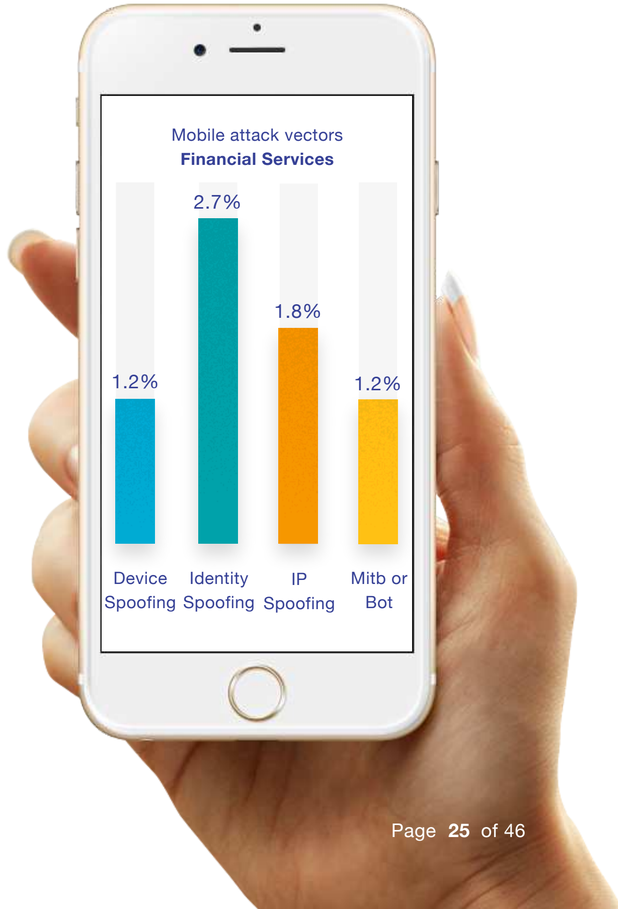
Percentage mobile transactions - **Financial Services**



Account Creations



Account Logins



Changing Rules of the Financial Services Game: Open Banking

CYBERCIMRE REPORT

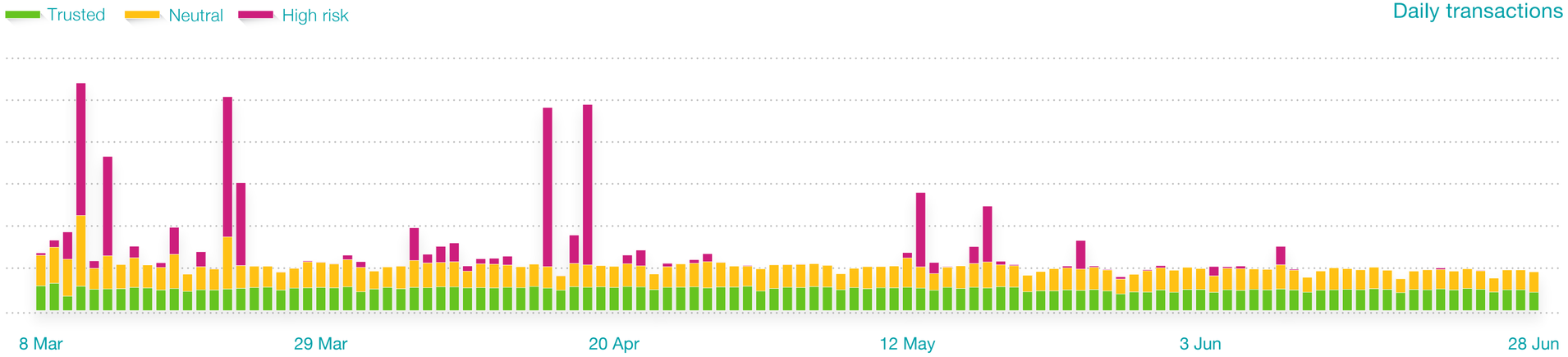
Open Banking: Opportunity and Threat

- Open Banking is one of biggest factors driving the pace of change in the financial services industry, bringing new opportunities for innovation, knowledge sharing and an enhanced customer experience.
- However without the right defenses in place, this global drive has the potential to allow new routes for fraudsters to exploit customer data.

Bot Attack on Global Bank's Financial Exchange

- One such example that ThreatMetrix detected and blocked was for a large US financial institution that was experiencing high volume credential testing bot attacks on its financial exchange.
- This was causing internal servers to crash and was leaving customer data vulnerable. The bank needed a fraud solution that could provide insight into activities occurring on its financial exchange and block fraudulent traffic without causing friction for legitimate customers.
- ThreatMetrix detects bot attacks using context-based information to perform behavioral analysis of users during periods of normal operation and compares such data to that gathered during an attack, enabling the bank to differentiate between a human and a bot the moment they login/transact.

High volume bot attacks targeting global bank's financial exchange



FinTech Attack Vectors

CYBERCIMRE REPORT

Open banking and PSD2 represent a huge opportunity for emerging FinTechs to grow and innovate, working alongside traditional financial institutions in a complementary capacity.

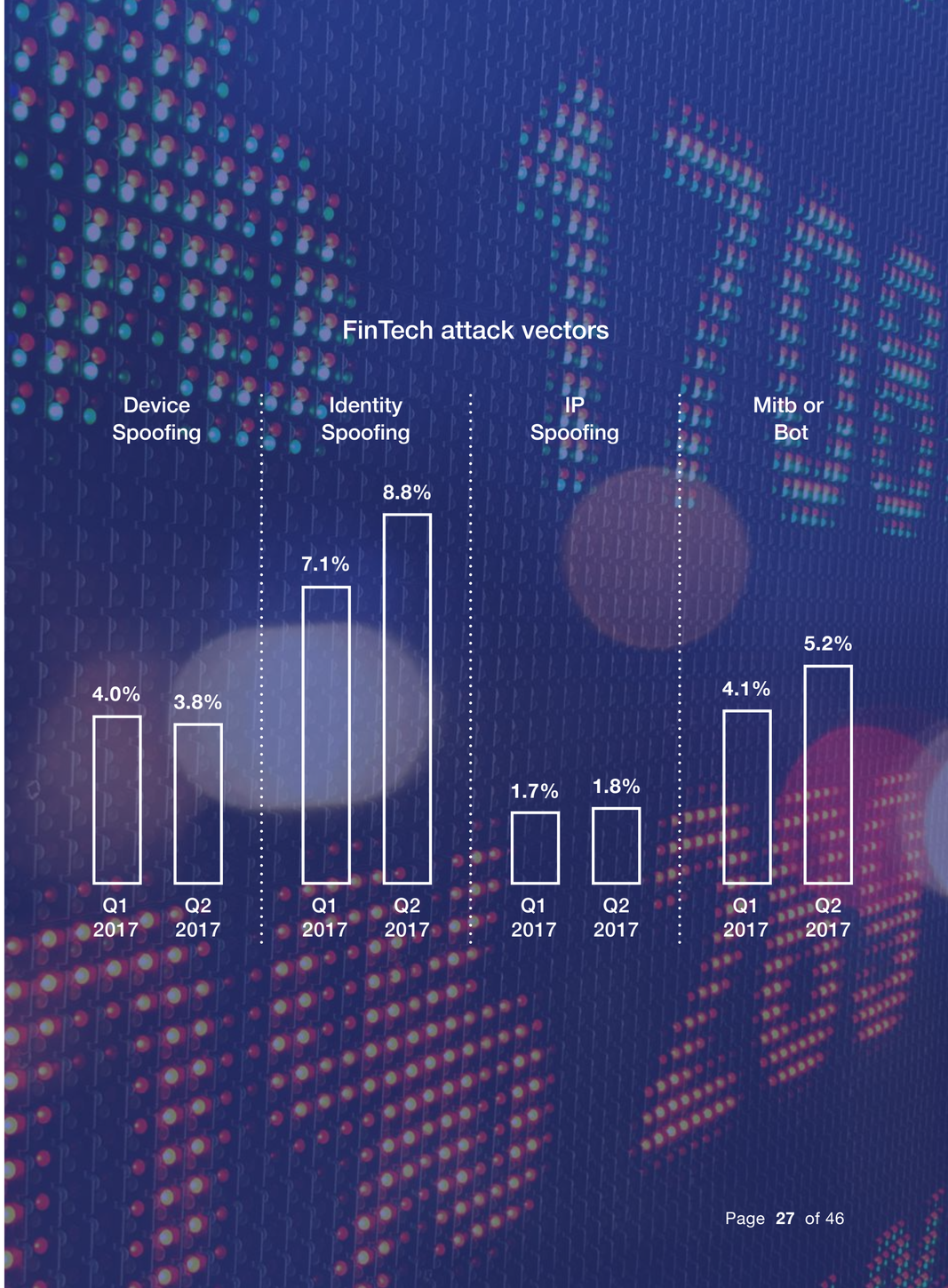
However, Fintech providers are still more prone to attack, as fraudsters increasingly target vulnerabilities in their emerging platforms / business models in order to hijack accounts, sign up for fraudulent loans and monetize stolen credentials.

The Network continues to see higher attacks for FinTech than for traditional financial services institutions. This is set within the context of continued growth in digital wallets and online remittances.

Identity spoofing continues to be the biggest attack vector, driven by easy access to complete customer credentials on the dark web. Location spoofing is less common as many providers don't have regional biases.

At the same time fraudsters are using bots to mass test identity credentials and infiltrate trusted user accounts.

Note: The bar charts represent percentage of total transactions that were recognized as attacks



Remittance – Global Corridors

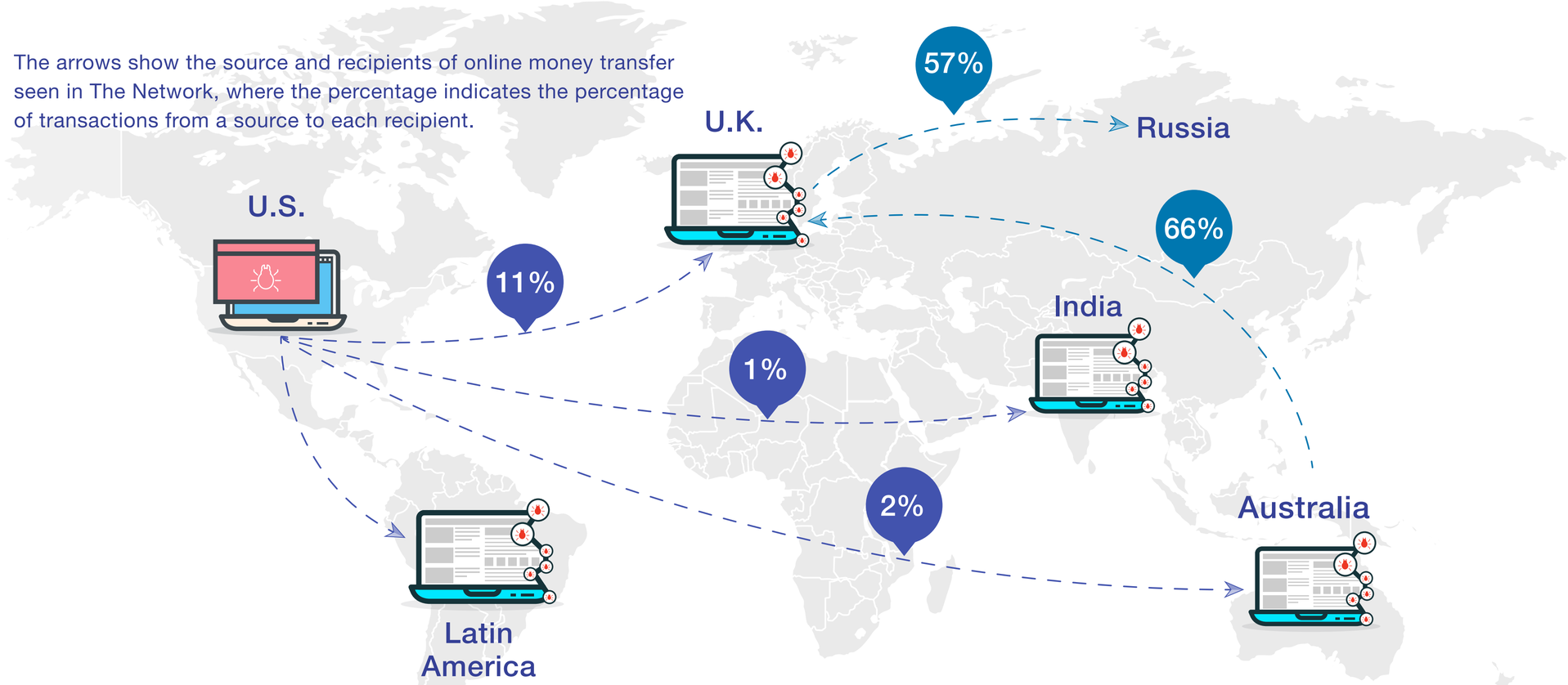
Digital consumers are increasingly open to trying new payment methods as evidenced by the growth of digital wallets.

P2P remittances are also growing as consumers become increasingly mobile, travelling frequently worldwide. This has prompted a growth in services that can offer fast, simple and friction-free money transfers online.

These online companies provide improved accessibility in comparison to traditional remittance providers, and often offer a cheaper service than international bank transfers.

However these remittance companies are key prey for fraudsters, whether through compromising user accounts to intercept payments or to launder money from a mule account to an account in another region.

The arrows show the source and recipients of online money transfer seen in The Network, where the percentage indicates the percentage of transactions from a source to each recipient.



CYBERCIMRE REPORT

Case Study: Supporting Real-time Remittance for **TimesofMoney**

TimesofMoney
ToMorrow. Today.

Business Problem

TimesofMoney is constantly looking for ways to stay at the forefront of digital payments innovation and improve the online customer experience.

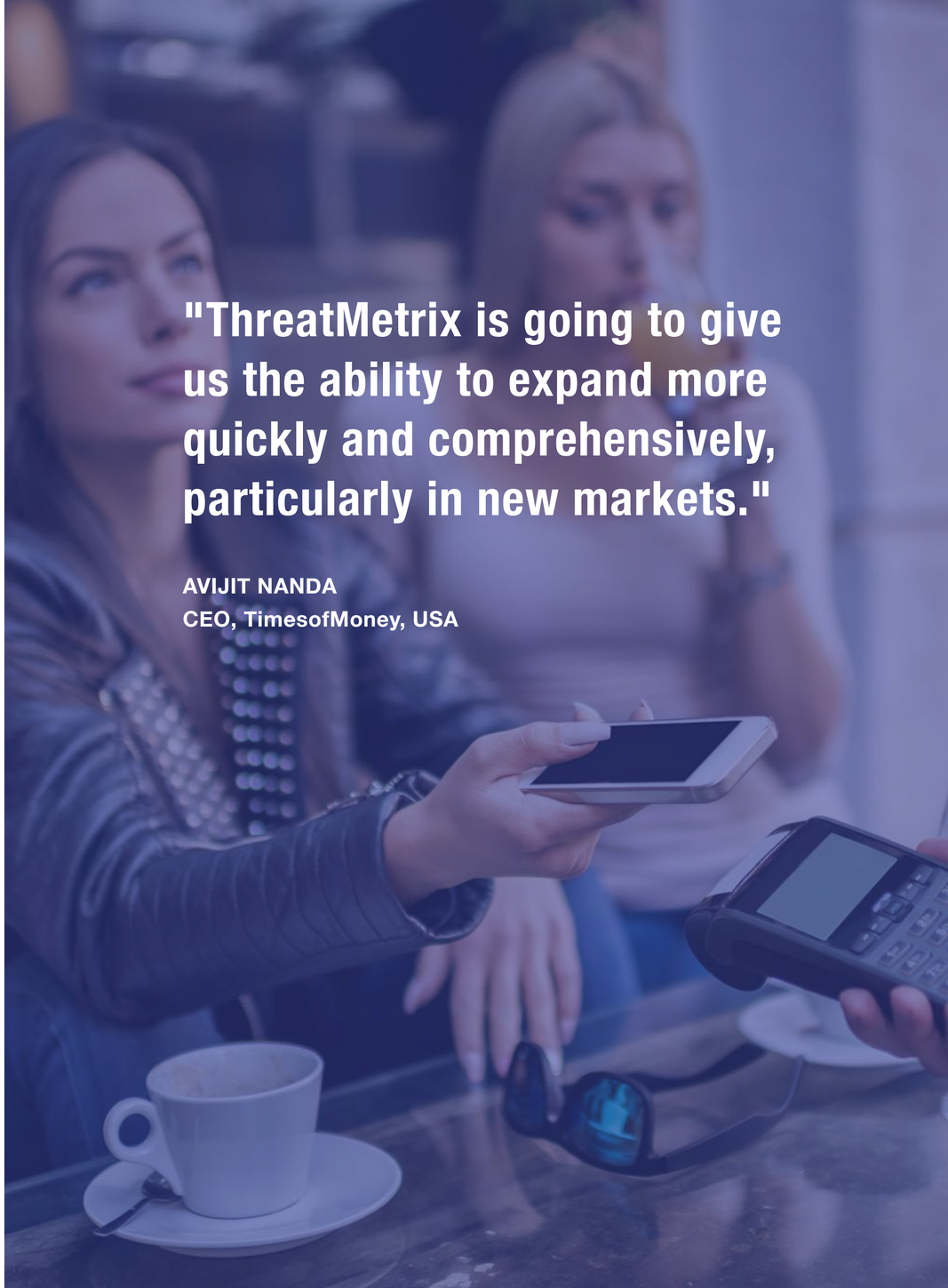
However it was experiencing fraudsters attempting to cloak their true locations/ use stolen and spoofed identities in order to takeover existing customer accounts. This led to increased customer friction with long transfer times and high manual reviews.

The Solution

Leveraging intelligence from the ThreatMetrix Digital Identity Network, TimesofMoney can accurately distinguish between legitimate customers and potential fraudsters real time, while improving money transfer times and streamlining the customer experience.

Results

- Dramatically improved transfer times, reducing friction and expanding product offerings to include real-time payment options
- Accurately detected and stopped fraudsters using stolen and spoofed identities
- Shifted fraud review process from entirely manual to predominantly automatic, reducing operational costs and better utilizing resources



"ThreatMetrix is going to give us the ability to expand more quickly and comprehensively, particularly in new markets."

AVIJIT NANDA
CEO, TimesofMoney, USA

CYBERCRIME REPORT

Media Transactions and Attacks

Travel review sites, holiday marketplaces and social media organizations rely heavily on a currency of trust between members and users; cybercrime activity can seriously jeopardize the reputation and integrity of media platforms.

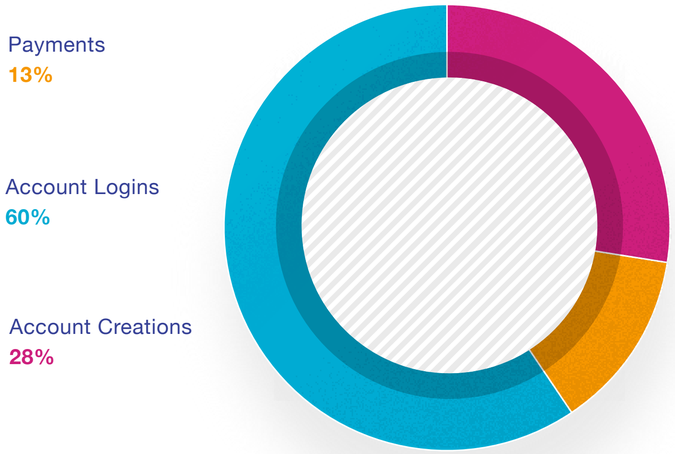
Media sees the highest overall attack rates of all industries at 13% of total transactions, illustrating the industry's vulnerability to account takeover and fraudulent new registrations for the purposes of fraudulent reviews, fake news, phony listings etc.

ThreatMetrix detected and stopped 28 million media attacks this quarter, representing a 22% rise in attacks year-on-year.

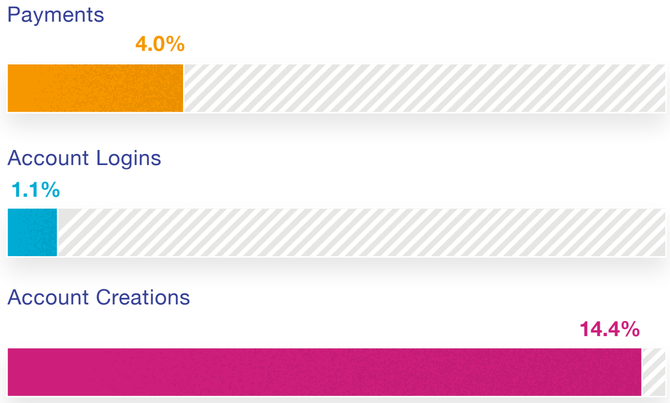
The biggest driver of the attack growth was the 527% increase in new account origination attacks since 2015, as fraudsters across the globe look to use the modest sign up requirements and security features of many media organizations to test stolen identity credentials, cultivating opportunities to monetize stolen credit cards.

As many organizations across content storage, media streaming, content sharing, online gaming, social networking etc. have deployed a premium model and offer free trials to potential customers, fraudsters look to use new account creations to game the system, either taking up multiple free trials or selling accounts online at a reduced rate.

Volume per transaction type



Attack rate per transaction type



Attack Percentages are based on transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically in real time dependent on individual customer use cases.

The Continued Rise of Global Transactions

CYBERCIMRE REPORT

Cross-border commerce continues to grow quarter-on-quarter; more than one in four transactions in the Network are now cross-border.

Growth of digital commerce and the digital mobility of connected users has made it possible for businesses to access a far more global pool of customers.

Media and eCommerce businesses are recognizing the potential of a global consumer base and are working hard to lower their attack rates, using more than just static legacy rules to accept or reject transactions. Meanwhile, banking and finance still remains a primarily domestic activity.

As digital commerce takes on this more global footprint, businesses are running into the cybercrime counterpart: global and well-organized criminal networks. Organizations therefore approach cross-border transactions with caution.

The attack rate for cross-border transactions is 6.2 times higher than for domestic transactions. A big driver of this is the custom rules set by businesses that often reject transactions from specific countries.

By leveraging global digital identities, businesses are able to more accurately detect fraudsters without declining transactions from good customers.

Cross-Border Transactions are:

1.6x Times more likely to be device spoofing

1.6x Times more likely to be identity spoofing

1.3x Times more likely to be IP spoofing

6.2x Times more likely to be rejected

Case Study: ThreatMetrix and **CyberSource** Help Global Businesses Grow

CYBERCRIME REPORT

CyberSource®

The ThreatMetrix/Cybersource Partnership

Dynamic shared intelligence from the ThreatMetrix Digital Identity Network underpins CyberSource's Decision Manager; a market-leading fraud management platform that dramatically increases global fraud visibility.

Securing Cross-Border Transations

ThreatMetrix has the largest repository of digital identity data in the world, analyzing the almost infinite connections that consumers make as they transact online, across tens of thousands of global websites. This intelligence helps CyberSource more accurately secure cross-border transactions, even when fraudsters attempt to spoof devices or locations to evade detection.

Benefits

- Improved automation of fraud detection with high-risk transactions detected and flagged in real time resulting in fewer manual reviews
- Real-time detection of location and device spoofing
- Accurate identification of automated bot attacks

"By partnering with ThreatMetrix, we can offer best-in-class fraud detection services to our merchants, enabling them to more accurately profile the true identity and behavior of connecting users."

SCOTT BODING
Senior Director, Risk Solutions Product Management, CyberSource

TOP ATTACK METHODS

Top Attack Vector Trends

ThreatMetrix identified 144 million fraud attempts during this period. This represents a 33% growth over the previous year.

Attack vectors are analyzed in real time by ThreatMetrix global policies. However, cybercriminals are constantly changing their tactics by leveraging multiple attack vectors, making the attacks more pervasive, complex and harder to detect.

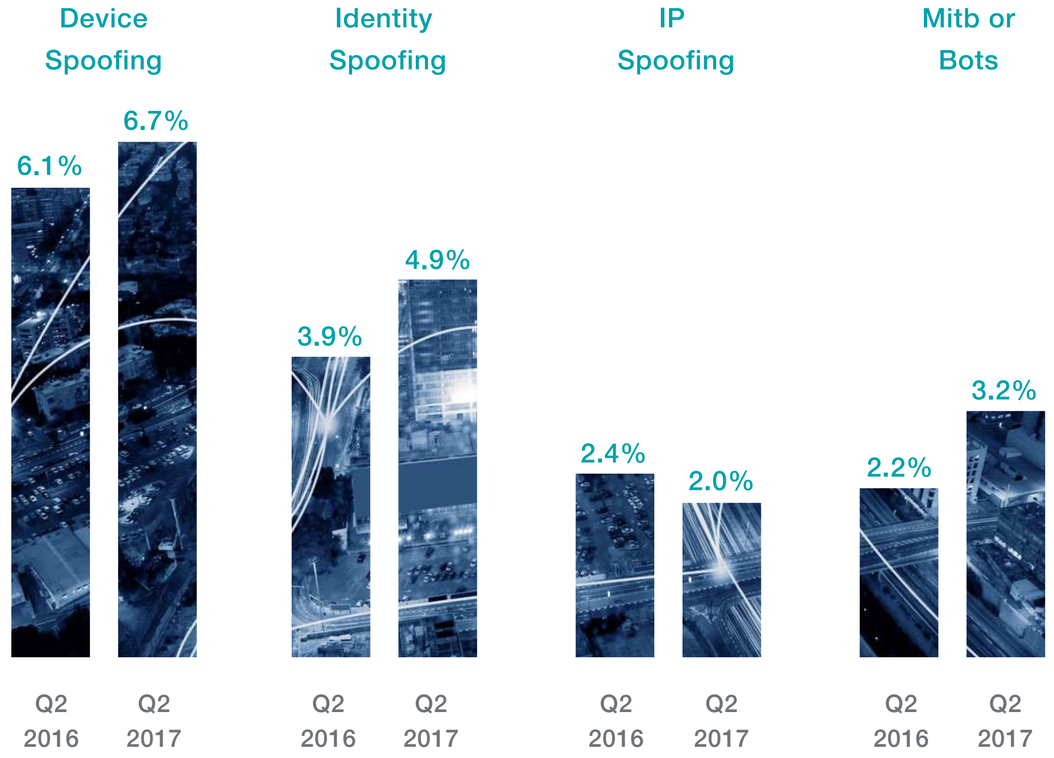
The Network saw continued growth in device spoofing, identity spoofing and Malware/Man-in-the-Browser (MitB)/bot attacks (which are categorized as a single group).

Malware, Man-in-the-Browser (MitB) and bots are the most malevolent attacks. Their ability to quietly compromise many online authentication systems means these attacks are normally reserved for operations with large payouts.

ThreatMetrix counters this growth in complex, multi-vector attacks using digital identity intelligence, combined with behavioral analytics, to accurately distinguish fraudsters from legitimate users.

Note: The bar charts represent percentage of total transactions that were recognized as attacks

Attack vectors compared to Q2 2016



Stolen Credentials Emerging from the Darknet: How Data Fuels Attacks

CYBERCIMRE REPORT

The Darknet is an encrypted network sitting apart from the existing internet that most users access. Specific software or tools are required to access the Darknet.

Darknet presents fraudsters with the opportunity to trade stolen identity data harvested from the omnipresent data breaches we see in the news. The use of these credentials is becoming more and more pernicious; we see this through their increased prevalence in The ThreatMetrix Digital Identity Network.

By continuously monitoring the Darknet, ThreatMetrix is able to detect and stop the use of these stolen credentials in the Network. 82% of stolen credentials on the Darknet have been seen in the Network. This shows the direct path of stolen credentials in live and persistent fraud attacks.

ThreatMetrix

Fraudsters Validate Lists of Stolen Data Via Large-scale Bot Attacks

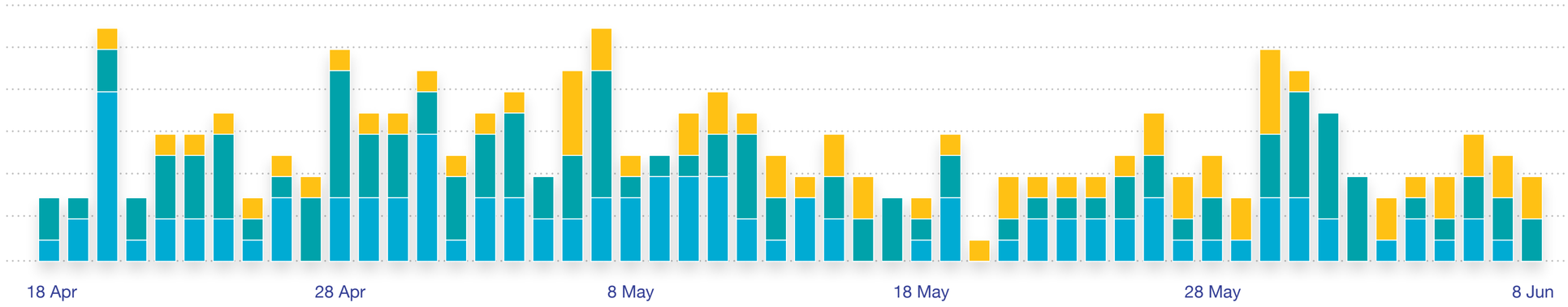
Bot attacks continue to have a huge impact on the daily traffic volumes of all major industries, with a particularly strong prevalence in eCommerce and financial services which offer the largest financial gains.

These automated bots take the form of huge identity testing attacks to validate stolen identity data traded on the dark web.

Rather than mass DDoS attacks, these bots are often adopting a low-and-slow attack pattern to slip just beneath the radar of traditional rate-control barriers, masquerading as legitimate customer traffic to trick the system.

CYBERCIMRE REPORT

Daily number of organizations being attacked by bots, per industry

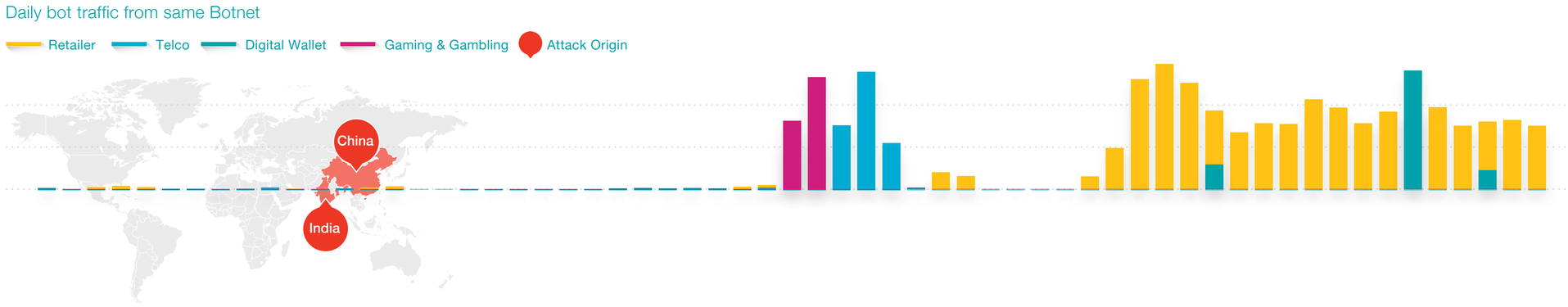


Casting the Net Wide: The Same Bots Targeting Multiple Companies

Gaining access to customer credentials from the dark web is only the first step to monetization.

These credentials need to be tested and validated before they can be used. Identifying the business where a customer may have their account requires these account validation attacks to be carried out across multiple businesses to increase likelihood of success.

By using shared intelligence, the Network identified these automated attacks targeting organizations across retail, financial services, telco and gambling industries.



Fraudsters use Stolen Credentials to Target Multiple Organizations with Account Takeover and Login Attacks

The networked nature of fraud is becoming more and more evident, with complex interrelationships detected between numerous fraudulent devices / accounts.

One such example is multiple linked devices attempting to register fraudulent new accounts and takeover existing trusted customer accounts across different organizations.

Once stolen data has been harvested and validated it can be used by organized fraud rings to perpetrate large-scale, networked attacks across a number of different organizations for maximum effect.

Such data can also make social engineering attacks more successful: users are duped into believing the communication is coming from a genuine organization because the fraudster uses real identity information to appear more legitimate.

Identifying Fraudsters Using Stolen Credentials Alongside Trusted Customers

As breaches continue to proliferate, more stolen identity data is appearing in global attacks.

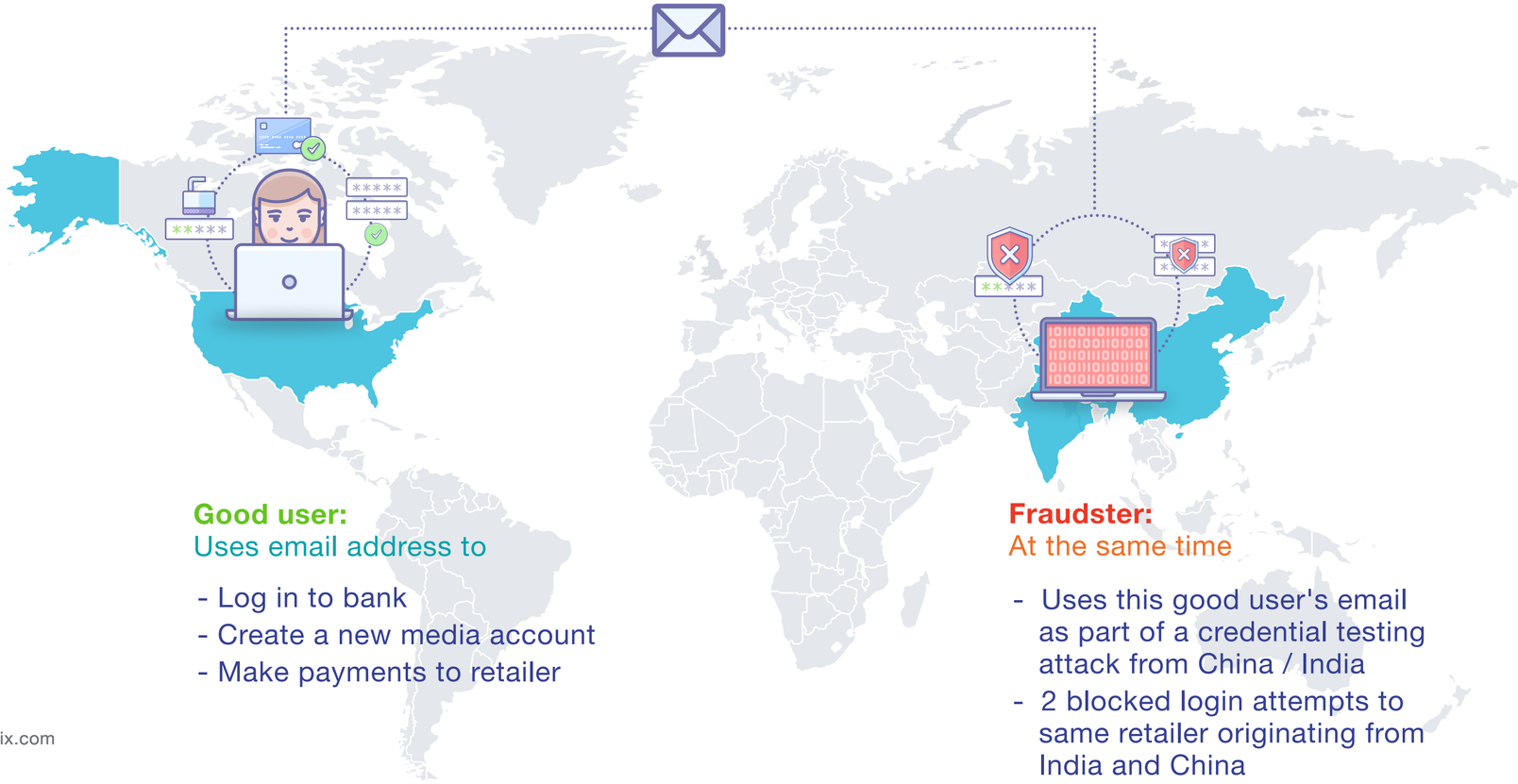
Fraudsters often transact with stolen data at the same time as the legitimate customer.

The challenge for global digital businesses is to be able to accurately differentiate trusted user behavior from high-risk behavior in real time.

Recognition of a returning user is enhanced using the full spectrum of digital identity data, incorporating device intelligence, locations and anonymized email addresses/credit cards for example.

By using these additional data elements ThreatMetrix is able to rate more transactions as trusted compared to using just device data as well as more accurately detect a potential fraud attack.

End users therefore enjoy a more streamlined online experience with less associated friction.



Good user:
Uses email address to

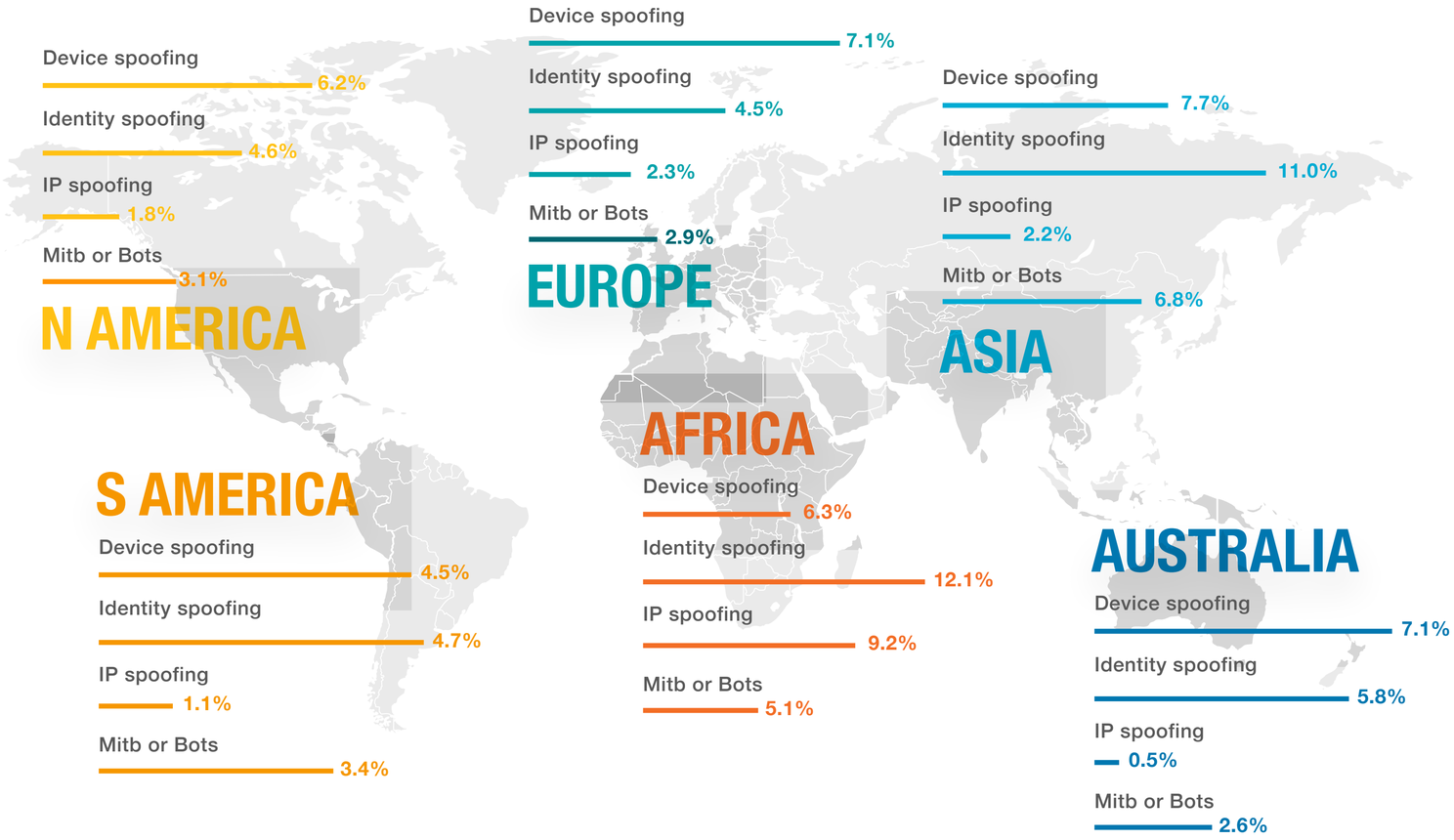
- Log in to bank
- Create a new media account
- Make payments to retailer

Fraudster:
At the same time

- Uses this good user's email as part of a credential testing attack from China / India
- 2 blocked login attempts to same retailer originating from India and China

CYBERCIMRE REPORT

Attack Vectors by Continent



Key attacks vectors are growing across the globe driven by availability of more sophisticated device spoofing tools combined with hacked and breached identities.

Growth in identity spoofing attacks reinforces that identity is the foundation of the evolving attack landscape. Cybercriminals have access to sophisticated tools to tailor attacks around testing, validating, augmenting and exploiting stolen and spoofed identity credentials.

Identity spoofing continues to be the leading attack vector in emerging economies, as well as for industries that target unbanked and underbanked populations, as organized identity verification tools are not as prevalent for these users.

Global businesses need the ability to incorporate regional variances and gaps in identity verification services, without impacting the online experience for true digital customers. This relies on being able to tap into a user's holistic digital identity in order to validate normal behavior and detect unusual or high-risk patterns.

Mobile Versus Desktop Transactions and Attacks

Mobile-based commerce represented 47% of the total transactions analyzed by The Network in Q2 2017.

Mobile transactions have grown almost 411% since 2015 with biggest growth continuing to come from financial institutions; transaction volume here has grown nearly eight times compared to Q1 2015.

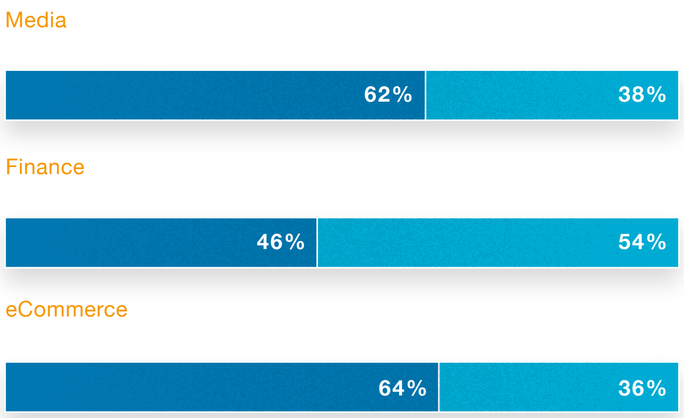
55% of account creations now come from mobile, demonstrating how retailers are focusing on building relationships with their customers in the mobile space, prioritizing mobile sign-up and login procedures. Mobile account creation has grown from 35% in Q2 2015 to 55% today, and mobile account logins 18% to 48%, showing just how pivotal mobile transacting has become for key account functions.

Mobile apps encourage a high proportion of returning customers with users saving card details to a handful of trusted brands to reduce friction at the payments stage.

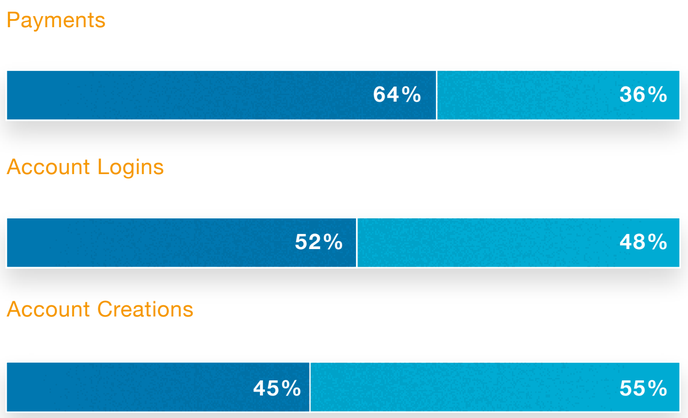
The prevalence of stolen identities and tools to enable cloaking / spoofing is causing attacks targeted at mobile devices to evolve and increase. Fraudsters are continually using unsecured wireless networks to intercept user credentials, encouraging users to download hacked versions of legitimate applications from third party stores, or looking for ways to intercept personal information that can be inadvertently leaked by legitimate mobile applications.

MOBILE

Volume desktop vs mobile per industry



Volume desktop vs mobile per transaction type



CYBERCIMRE REPORT

The Growing Threat of Mobile Cybercrime

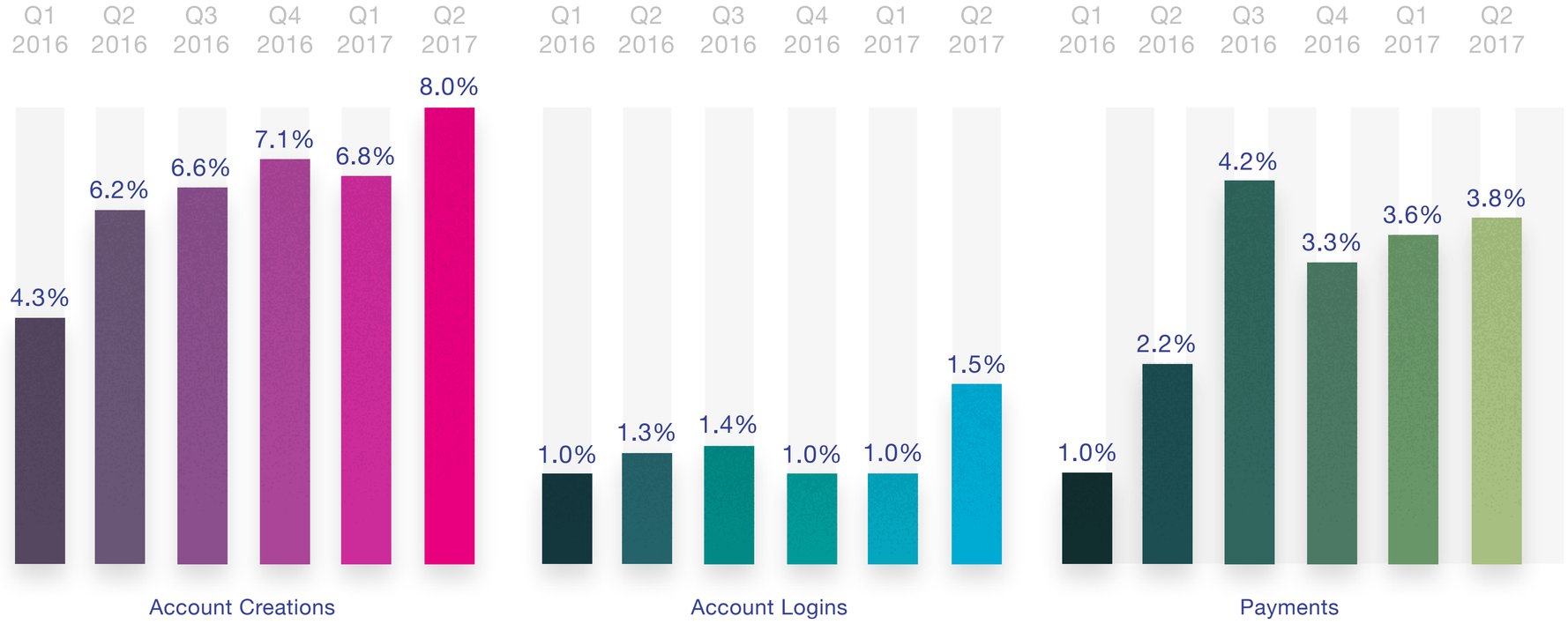
Mobile transactions have consistently been attacked less than desktop, with fraudsters generally exploiting the vulnerabilities of desktop sessions rather than the more secure mobile app sessions.

However it is evident that as mobile transactions continue to proliferate, cybercriminals are turning their attention to mobile attacks.

At the same time, fraudsters often use sophisticated tools to launch organized attacks that mimic mobile transactions/applications.

Account creation and payments transactions are particularly vulnerable in the mobile space, both for mobile browsers and mobile apps, as fraudsters open and cultivate fraudulent accounts to monetize stolen credentials and make fraudulent payments.

Mobile attacks per quarter



Conclusion

CONCLUSION

"Cybercrime is a growth industry where the returns are great and the risks are low"

- McAfee

One of the key features of the cybercrime we see in the Network this quarter is the complex, interconnected, networked nature of attacks as fraudsters use stolen identity credentials to cultivate lists, launch botnet attacks, compromise trusted user accounts and open accounts that purport to be legitimate for nefarious purposes. Organized fraud rings are launching attacks on multiple organizations across the Network to maximize usage and success of stolen data.

This is similarly seen in wider news reports as cyber attacks have evolved from lone wolf perpetrators to encompassing cross-border networks and even nation states. Cybercrime is a fully functioning industry and the only successful defense is a competing Network that harnesses and shares dynamic global intelligence.

The ThreatMetrix Digital Identity Network crowdsources intelligence from thousands of global companies across billions of yearly transactions. We use this intelligence to create unique digital identities which comprise device, location, identity and threat intelligence. Every day, ThreatMetrix adds key intelligence to the Network which allows its customers to better understand the digital footprint of transacting users and build ever more intricate digital identities. When combined with behavioral analytics, business can more accurately distinguish high-risk behavior in real time, before a transaction is processed.

It's easy to look at this ongoing fight from the point of view of the business and the fraudsters attacking it. Yet actually our true focus should be on the end user. They are the ones, after all, who power the business, and can change the success of it by defecting to a competitor if their online experience does not live up to expectations. Businesses must continue to strive for the perfect balance between customer experience and security; cyber defenses must not prompt increased friction. Passive, risk-based decisions must be augmented with low friction step-up solutions when required to prioritize an exceptional online experience.

Glossary

CYBERCIMRE REPORT

Industry Types

Financial Services includes mobile banking, online banking, online money transfer, lending, brokerage, alternative payments and credit card issuance.

FinTech includes companies that use technology to make financial services more efficient with a purpose of disrupting incumbent financial systems and corporations that rely less on software.

ecommerce includes retail, airlines, travel, marketplaces, ticketing and digital goods businesses.

Media includes social networks, content streaming, gambling, gaming and online dating sites.

Common Attacks

Account Creation Fraud: Using stolen, compromised or synthetic identities, typically through a spoofed location, to create a new account to access online services or obtain lines of credit.

Account Login Fraud: Attacks targeted at taking over user accounts using previously stolen credentials available in the wild or credentials compromised by malware or Man-in-the-Middle attacks.

Payments Fraud: Using stolen payment credentials to conduct illegal money transfers or online payments via alternative online payment methods such as direct deposit.

Percentages

Transaction Type Percentages are based on the number of transactions (account creation, account login and payments) from mobile devices and computers received and processed by the ThreatMetrix Digital Identity Network.

Attack Percentages are based on transactions identified as high risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically, in real time dependent on individual customer use cases.

Glossary

CYBERCIMRE REPORT

Attack Explanations

Device Spoofing: Hackers delete and change browser settings in order to change their device identity or fingerprint, or attempt to appear to come from a victim's device. ThreatMetrix-patented cookieless device identification is able to detect returning visitors even when cookies are deleted or changes are made to browser settings. To differentiate between cybercriminals and legitimate customers who occasionally clear cookies, only high risk / high velocity cookie deletions (such as a high number of repeat visits per hour / day) are included in the analysis.

Identity Spoofing: Using a stolen identity, credit card or compromised username / password combination to attempt fraud or account takeover. Typically, identity spoofing is detected based on high velocity of identity usage for a given device, detecting the same device accessing multiple unrelated user accounts or unusual identity linkages and usage.

IP Address Spoofing: Cybercriminals use proxies to bypass traditional IP geolocation filters, and use IP spoofing techniques to evade velocity filters and blacklists. ThreatMetrix directly detects IP spoofing via both active and passive browser and network packet fingerprinting techniques.

Man-in-the-Browser (MitB) and Bot Detection: Man-in-the-browser attacks use sophisticated Trojans to steal login information and one-time-passwords (such as SMS out-of-band authentication messages) from a user's browser. Bots are automated scripts that attempt to gain access to accounts with stolen credentials or create fake accounts and transactions.

Crimeware Tools: Crimeware refers to malware specifically designed to automate cybercrime. These tools help fraudsters create, customize and distribute malware to perpetrate identity theft through social engineering or technical stealth.

Low and Slow Bots: Refers to low frequency botnet attacks designed to evade rate and security control measures, and thus evade detection. These attacks use slow traffic that not only appears legitimate but also bypasses any triggers set around protocols and rules.

Contact

CYBERCIMRE REPORT

San Jose (Corporate Headquarters)

160 W Santa Clara St, Suite 1400
San Jose, CA 95113
Telephone: +1 408 200 5755
Fax: +1 408 200 5799

London

201 Borough High Street
London, SE1 1JA, United Kingdom
Telephone: +44 (0) 20 3239 2601

Paris

13 Rue Camille Desmoulins
92130 Issy-les-Moulineaux
France
Telephone: +33 (0) 1 58 04 24 03

New York

Empire State Building, Suite #4805
350 Fifth Avenue New York, NY 10118
Telephone: +1 212 896 3987

Sydney

Suite 1202, Level 12, Tower B
799 Pacific Highway
Chatswood NSW 2067
Australia
Telephone: +61 2 9411 4499

Amsterdam

The Base, Tower C
Evert van de Beekstraat 1
1118 CL Schiphol
The Netherlands
Telephone: +31 (0) 20 800 0637

Tokyo

Otemachi Bldg. 4F FINOLAB
1-6-1 Otemachi, Chiyoda-ku,
Tokyo 100-0004 Japan
Phone: +81-(0)3-4530-9576

Hong Kong

Telephone: +852 36 698 341

Munich

Theresienhöhe 28
80339, Munich
Phone: +49 89 24440 7057

SALES

Telephone: +1 408 200 5700
Email: sales@threatmetrix.com

SUPPORT

Telephone: +1 408 200 5754 / +1 888 341 9377
Email: tmsupport@threatmetrix.com

PARTNERS

Email: partners@threatmetrix.com

PUBLIC RELATIONS

Email: pr@threatmetrix.com