ThreatMetrix™
Cybercrime Report: Q2 2015

ThreatMetrix®

Foreword

Consumer behavior has undergone a fundamental shift where accessing information, content, product and services instantly has become the norm. This, coupled with the prevalence of connected devices that track and catalogue every aspect of one's life, is delivering unprecedented convenience. As consumers navigate this digital world, the underlying assumption is that their digital identities remain protected.

While many businesses have taken steps to protect aspects of digital personas critical to their product and services, vulnerabilities exist and the only way to effectively secure your customers and revenue against cyber attacks is by leveraging anonymized shared intelligence built on global profiles of authentication and transaction history.

Using this shared intelligence it is possible to differentiate in real time between a valuable customer and a fraudster using breached or stolen identities, and a legitimate account access versus a bot or malware hack attempt. The data in this report is unique in that it represents an authoritative source of data on actual attacks on our collective digital identities in the wild and reveals the extent and scale to which our collective digital identities are being exploited on a routine basis by sophisticated cyber criminals.

Alisdair Faulkner
Chief Products Officer

Report overview

The ThreatMetrix Cybercrime Report: Q2 2015 is based on actual cybercrime attacks from April 2015 – June 2015 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 registrations.

- The Network analyzes more than one billion transactions per month, nearly a third 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 legitimate end customers' "digital identities," even as they move between applications, devices, and networks.
- ThreatMetrix users benefit from a global view of risks, based on these attributes and custom-tuned rules specific for their businesses.
- Attacks discussed are from "high risk" transactions scored by ThreatMetrix.

Q2 2015 Cybercrime Report – Key Highlights

During this period, billions of transactions were analyzed by the ThreatMetrix Digital Identity Network and more than 75 million attacks were detected and stopped in real time.

ThreatMetrix analyzes transactions from the top customers across industries, the trends observed are representative of the key market trends:

- Trust is critical for conversion and customer loyalty as both financial institutions and retailers strive to establish strong relationships with their users.
- Recognition is key to ensure trusted users are not impacted in the fight against fraudsters. Shared global intelligence is a critical tool to fight crime without inconveniencing customers.
- Digital Identities are the new global currency to protect against attacks from fraudsters across the globe.
- Fraudsters either replay stolen identities using proxies, device, and location spoofing to cloak the true digital Identity or piggy-back on a user's session with malware or Man-in-the-Middle attacks.
- Mobile usage continues to grow, accounting for up to 31% of transactions. With more than 20 million new mobile devices being added to The Network every month, this trend is expected to continue.

Trends and Surprises

Trends

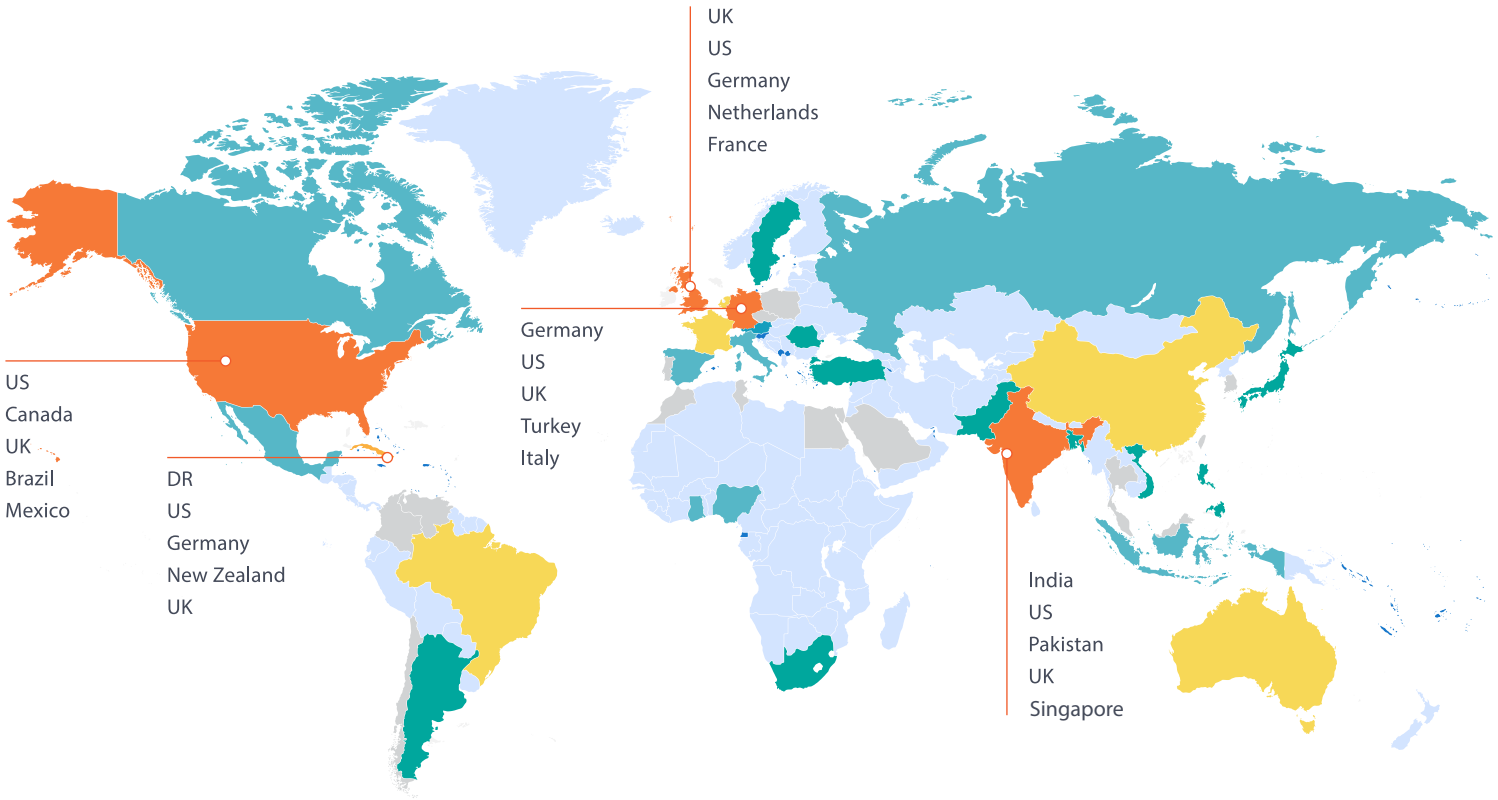
- As commerce goes global and mobile – so does cybercrime.
- Cybercrime surges on the backs of bots and data breaches.
- Mobile usage continues to grow, accounting for up to 31% of transactions.
- Consumers continue to access e-commerce, media and financial services through multiple devices.

Surprises

- India and the Dominican Republic emerged as one of the top 5 attack originators for this period.
- Cybercriminals targeting financial institutions executed more payment and login attacks compared to new account fraud.
- Attacks targeting online lenders spiked during this period.
- Despite the growth of global commerce, cross-border transactions declined at a higher rate than domestic transactions.

Attack Origins by Geography

Total number of attacks detected by geography of origin.



Country ranking
by attack origins

Top 5

- United States
- United Kingdom
- Germany
- India
- Dominican Republic

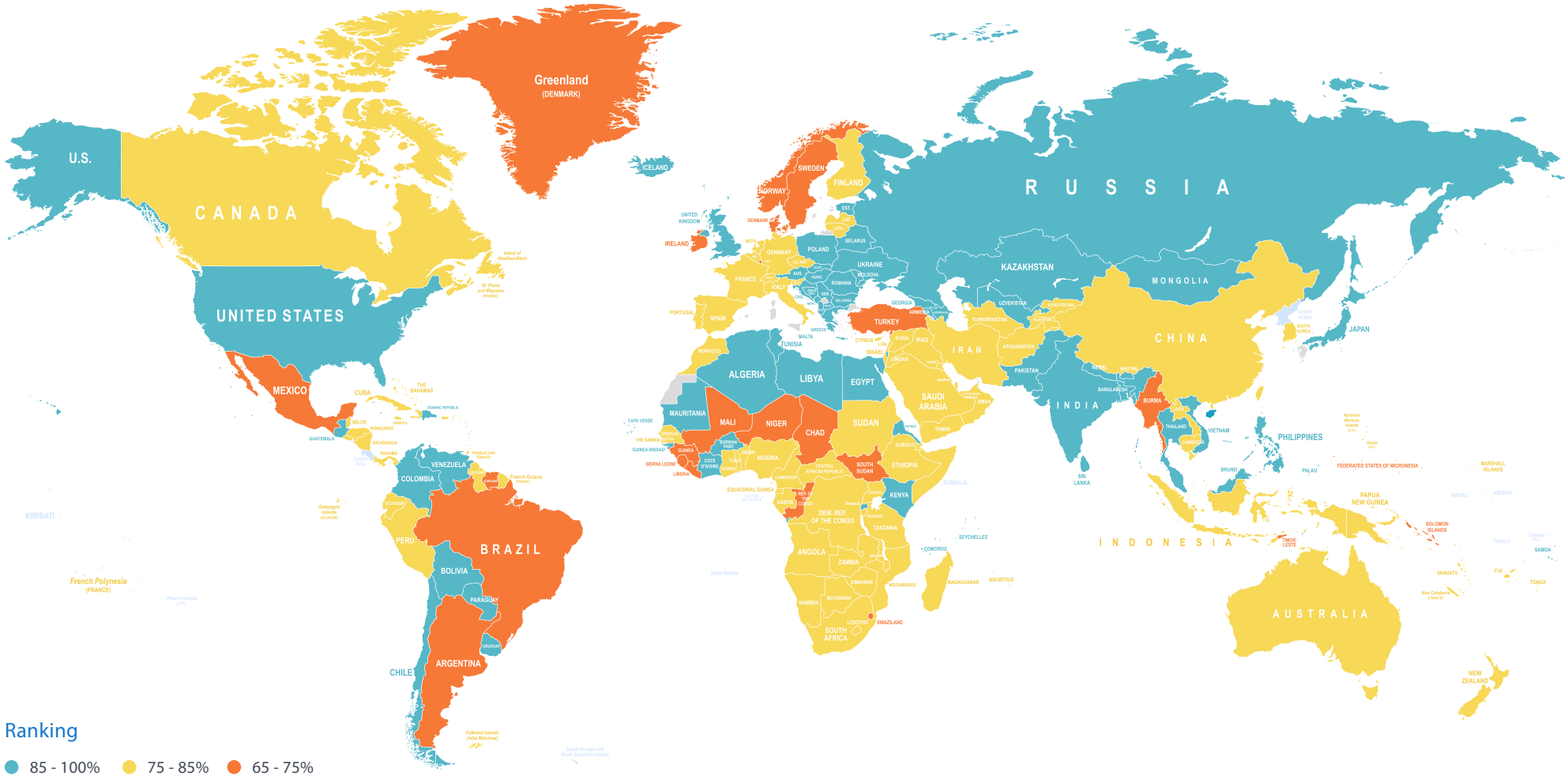
- Top 6 - 10
- Top 11 - 20
- Top 21 - 30
- Top 31 - 50
- 50+

Top 5 attack targets for attacks originating from US, UK, Germany, India and Dominican Republic

ThreatMetrix®

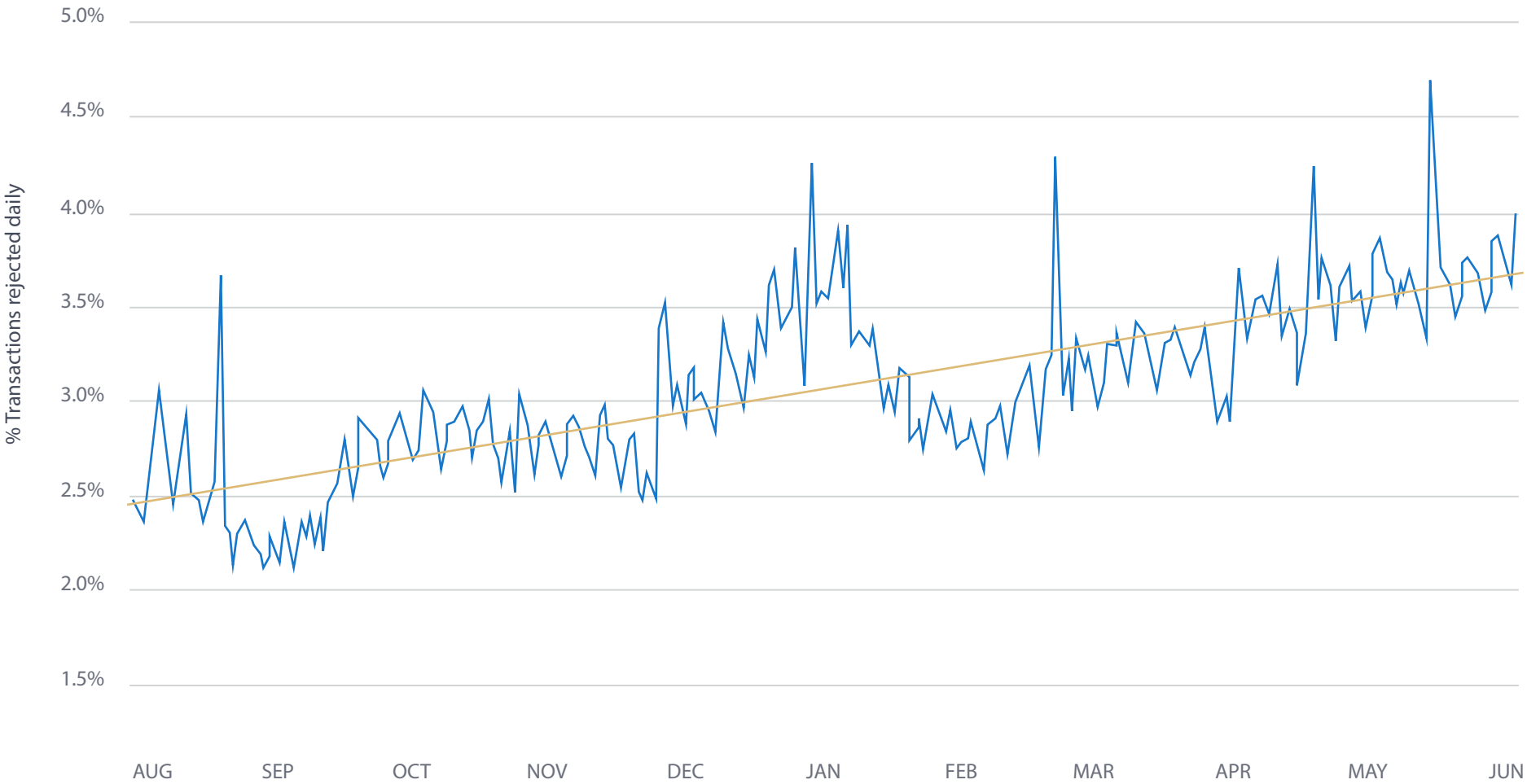
Recognition is The Key

Persona (device, identity, behavior) recognition by the ThreatMetrix Digital Identity Network.



ThreatMetrix®

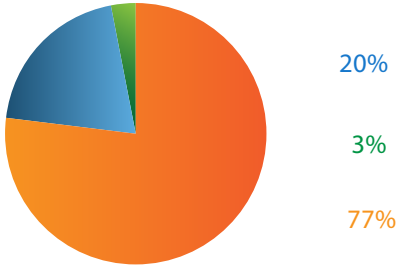
Data Breaches & Bots Driving Cybercrime Surge



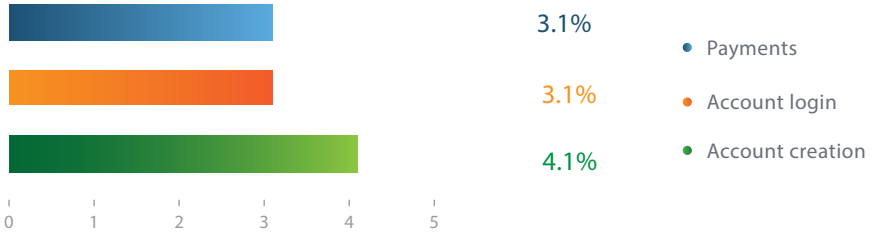
Transactions Analyzed by Type

- ThreatMetrix transactions span e-commerce, financial services, and media sectors and cover the authentication, payments and account originations use cases.
- Logins and payments continue to be the biggest use cases as customers deploy ThreatMetrix to verify their uses' digital identities without impacting consumer experience.
- New account creation continues to be high risk as fraudsters use stolen stolen credentials harvested from massive breaches.

Volume by Transaction Types



Attacks by Transaction Type

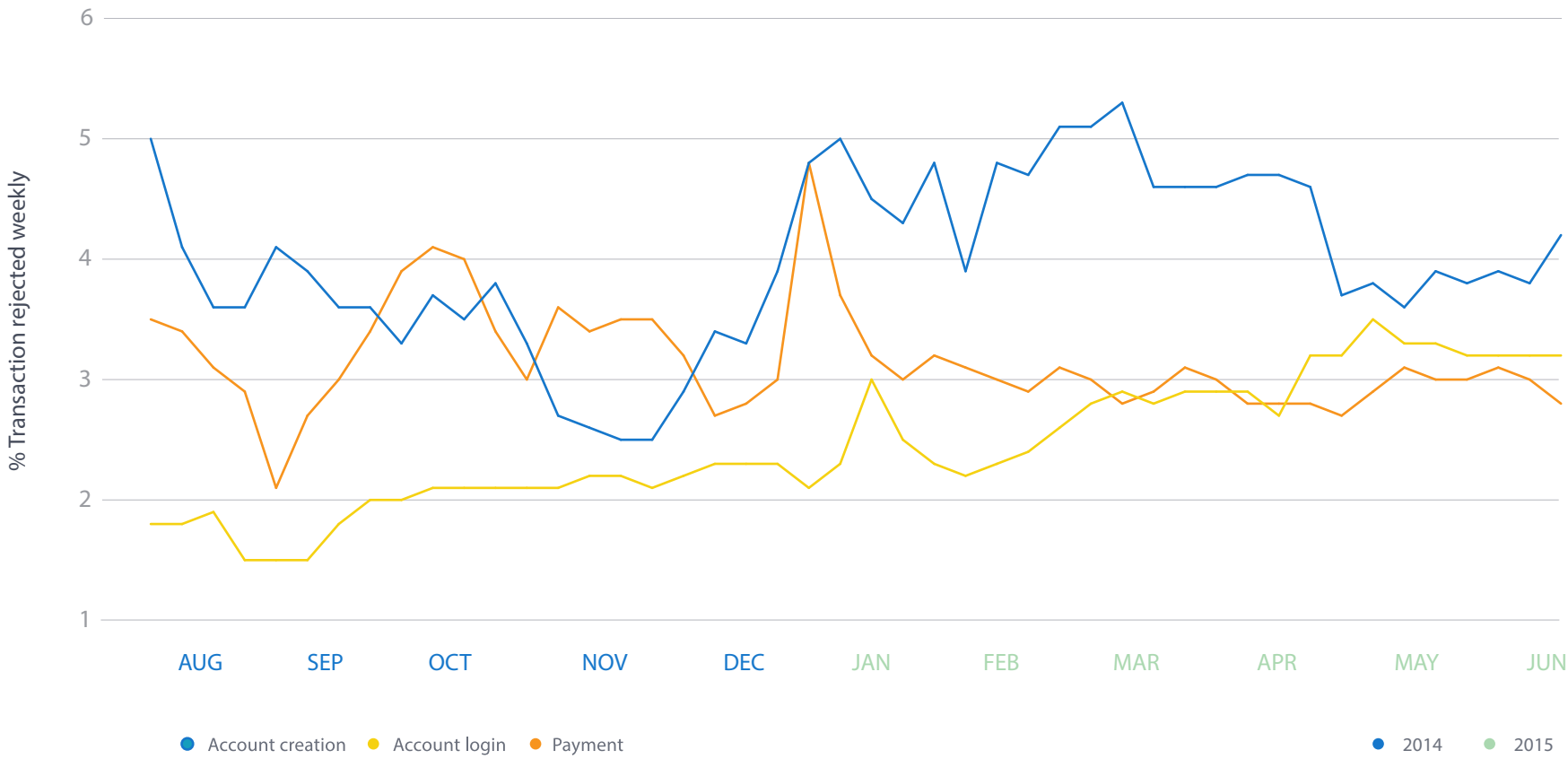


Note

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.

Risk Trends By Transaction Type

- The attack levels are steadily increasing across across all use cases.
- Fraudsters are increasingly targeting diverse data sets to effectively stitch together the consumers' credentials.

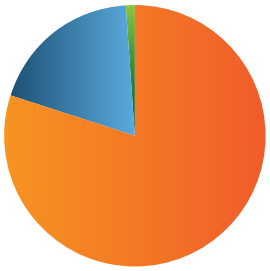


E-Commerce Transactions and Attacks

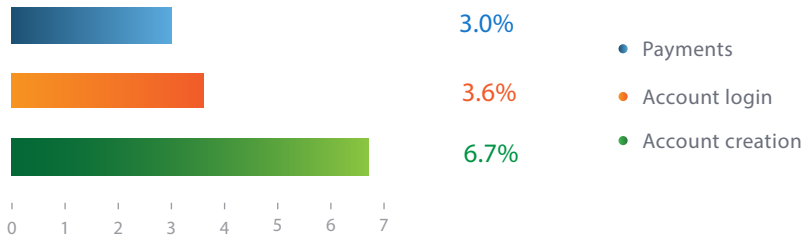
With the continued growth of online and mobile commerce, retailers are trying to create more meaningful relationships with their trusted customers through mobile applications and accounts on file. As a result, payments and account logins continue to be a much larger portion of total transactions with customers revisiting their shopping carts to complete purchases.

- High download of retailers' mobile applications across connected devices ensures that consumers move sequentially between several screens for everyday activities like booking a hotel or shopping for electronics.
- The Network is able to track and provide intelligence across these devices to identify trusted consumers.
- More attacks for login and payment events were detected in this period.

Transactions by Type



Attacks by Transaction Type



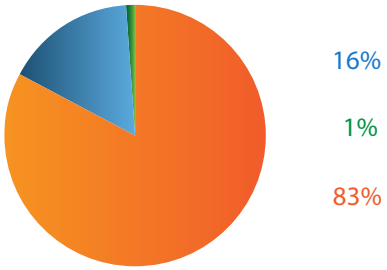
Note

E-Commerce includes retail, airlines, gambling, gaming, travel, marketplaces, ticketing and digital goods businesses.

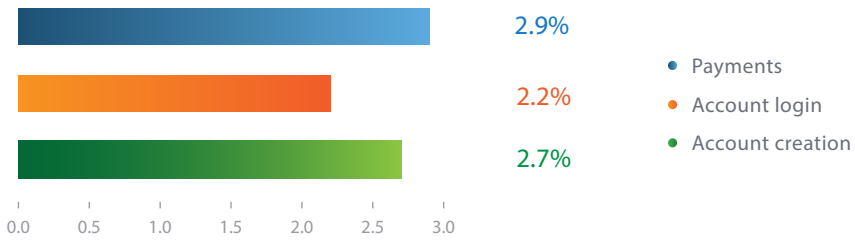
Financial Services Transactions and Attacks

- Financial Institutions continue to be big targets for organized attacks across the globe. The impact of breaches and consumer credentials in the wild was more evident in this segment with a substantial increase in fraud rates across all transaction types.
- Mobile has long been positioned as the tool to drive financial inclusion for the unbanked and under banked. The ThreatMetrix Digital Identity Network has become online lenders' chosen way for identity verification to differentiate good customers from fraudsters.
- The prevalence of crimeware tools was also evidenced by the increase in payment and login fraud over the previous period. As such, the network detected more than 25 million attacks during this period, ~30% increase over the first quarter of 2015.

Transactions by Type



Attacks by Transaction Type



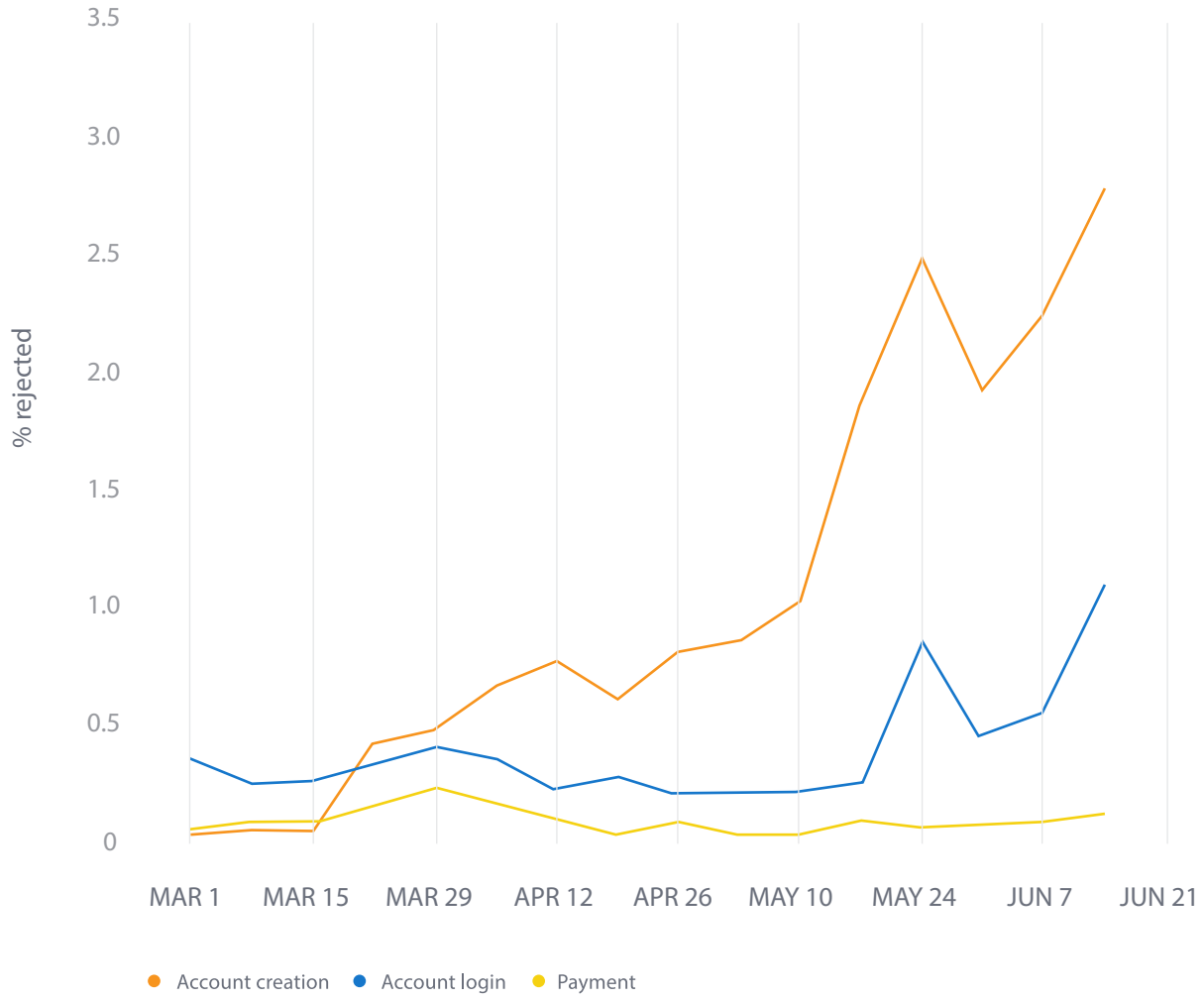
Note

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

Online Lending

- Digital commerce is driving the growth of online lending.
- As more and more institutions create financial products to target the unbanked and under-banked population, this segment is becoming the target of attacks.
- These attacks primarily focus on new account originations and sometimes on payment disbursements.

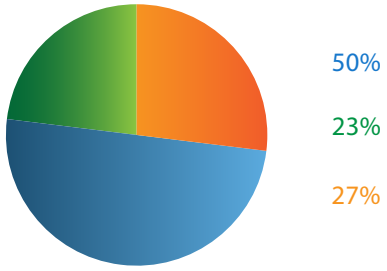
Online lenders - weekly % rejected transactions



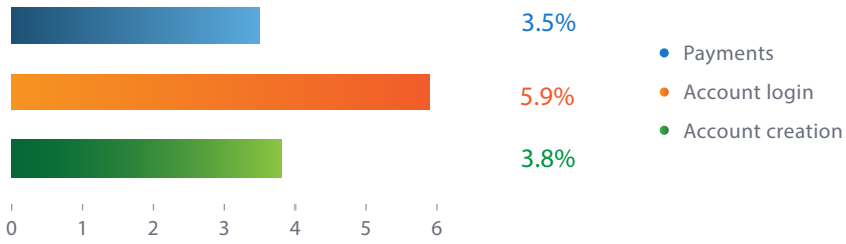
Media Transactions and Attacks

- The media industry continues to be the primary target for fraudsters looking to access paid content, spam members and to test the validity of the stolen credentials.
- Modest sign-up and authentication requirements along with user password sharing across sites continue to attract the highest rate of cybercrime attacks per transaction. Criminals are increasingly using media sites to test the validity of stolen credentials. As such, the attack levels continue to be higher than other industries.
- The big driver of fraudulent transactions are people illegally accessing content outside of approved geographies combined with spamming and fraudulent account creation using bots.
- More than 15 million attacks were detected and stopped by the network during this period.

Transactions by Type



Attacks by Transaction Type



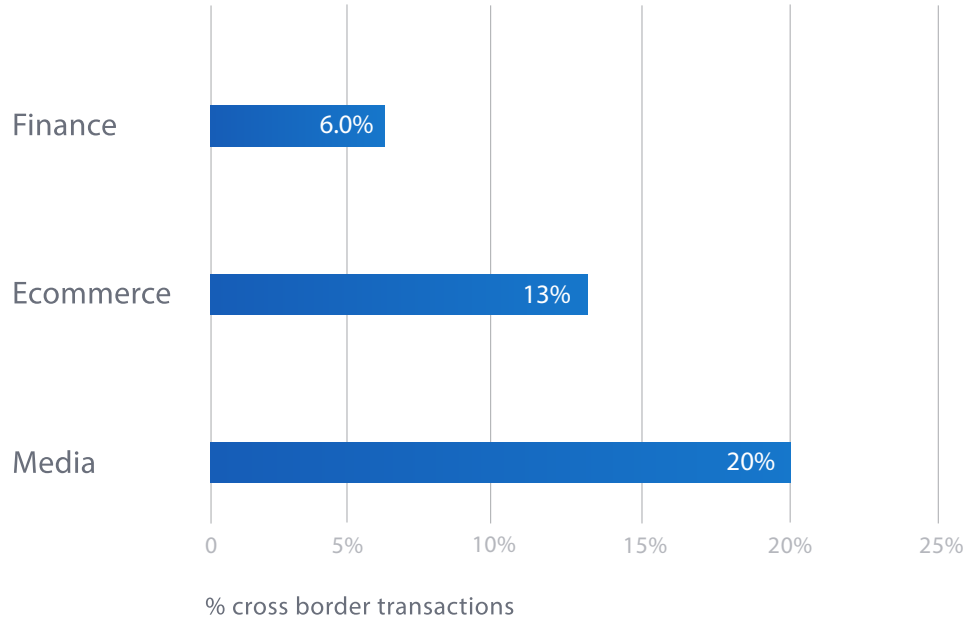
Note

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

Cross Border On the Rise

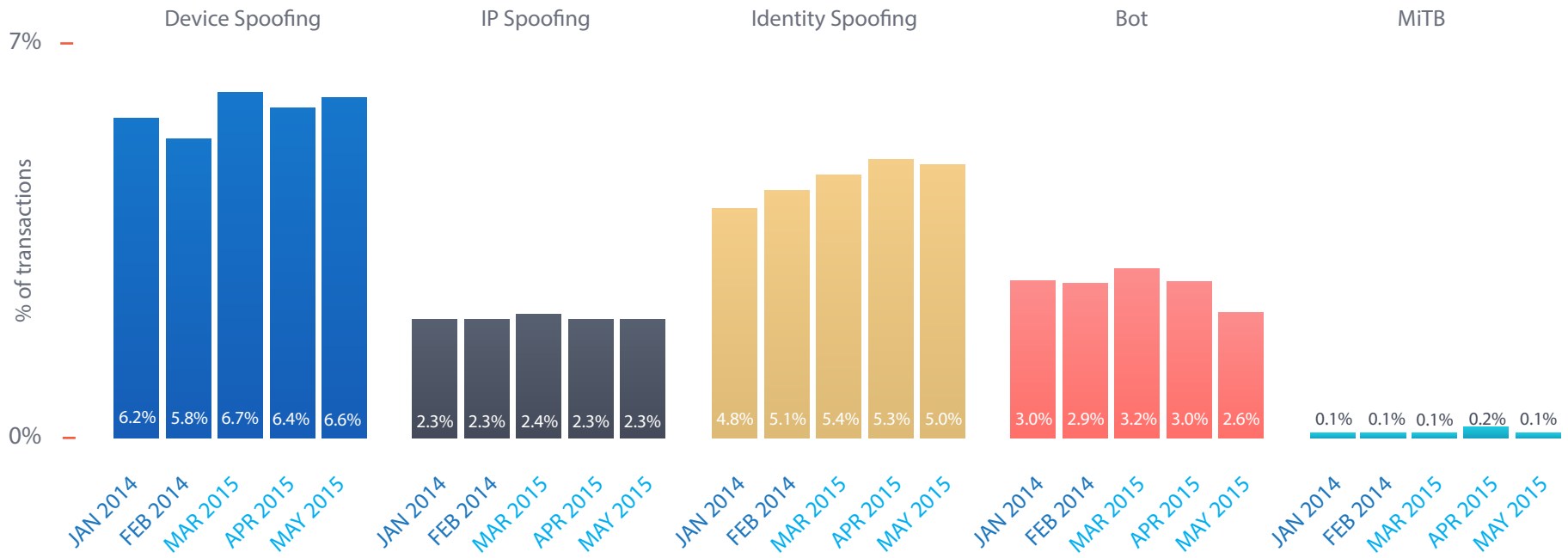
- Cross-border transactions are easy attack targets given it is hard for businesses to know the true digital identities of the customers. As such, businesses decline these transactions at a much higher rate compared to domestic transactions; sometimes three times more than domestic transactions.
- However, declining service or access to a good customer causes irreparable damage to the consumer relationship and lifetime value.

Cross border reject rate across by industry



Top Attack Vector Trends

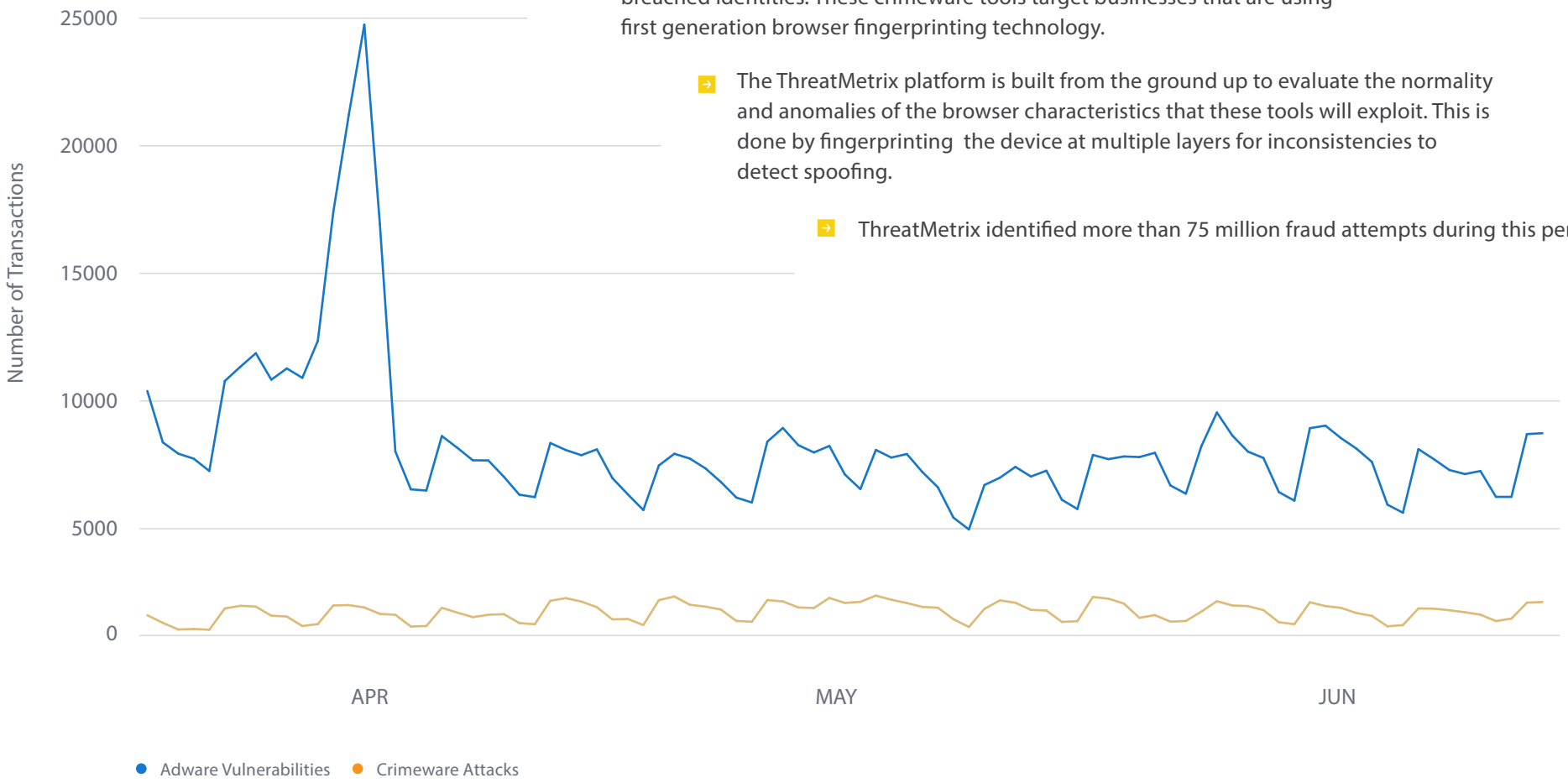
- Attack vectors are analyzed in real time by the ThreatMetrix Digital Identity Network's global policies. Some attacks use multiple vectors. Device spoofing remains the top attack vector.
- As crimeware tools gain traction, The Network is seeing more and more traffic that is cloaked, especially for new account creation where the fraudsters use stolen identities along with these tools to defraud businesses.



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

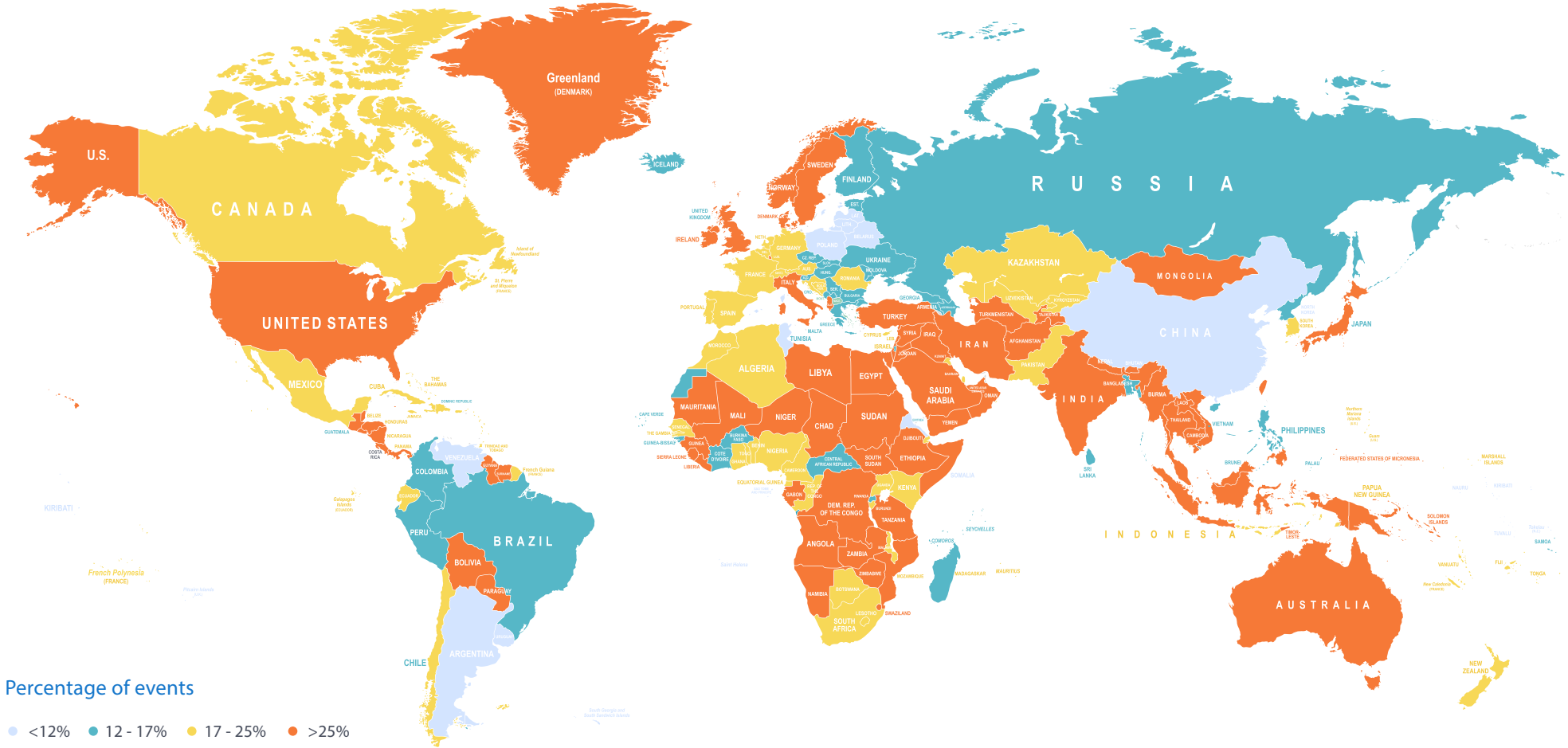
Crimeware and Adware Attack Trends

- Impersonation or "spoofing" attacks continue to rise, driven by availability of more sophisticated device spoofing tools combined with hacked and breached identities. These crimeware tools target businesses that are using first generation browser fingerprinting technology.
- The ThreatMetrix platform is built from the ground up to evaluate the normality and anomalies of the browser characteristics that these tools will exploit. This is done by fingerprinting the device at multiple layers for inconsistencies to detect spoofing.
- ThreatMetrix identified more than 75 million fraud attempts during this period.



Mobile Transaction Prevalence

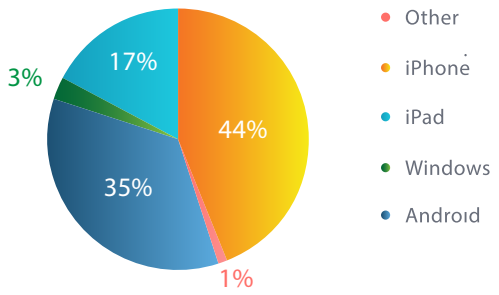
Uptick in mobile phone ownership and usage of mobile services is a global phenomenon with consumers from both developed and emerging economies increasingly using their connected devices.



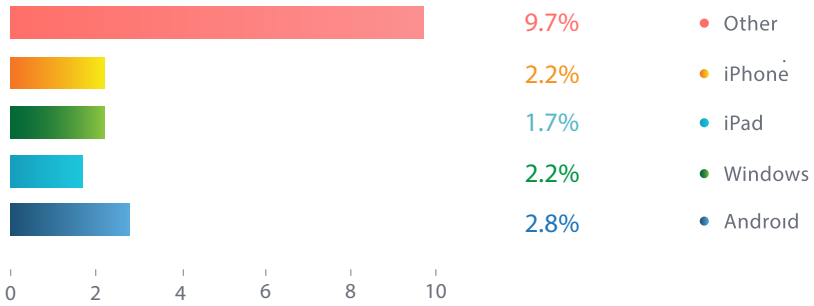
Mobile Transactions and Attacks

- As mobile transactions grow, so do the attacks targeted toward mobile devices and platforms. Spoofing or cybercriminals imperfectly impersonating a given mobile device (shown as "Other") constitute the most common source of these mobile attacks. ThreatMetrix's layered approach effectively detected and stopped these fraudulent transactions from devices masking their operating system (OS).
- iOS devices (iPhone and iPad combined) accounted for nearly two-thirds of total mobile transactions. Android showed strong growth driven by customer deployment, release of new mobile SDK for Android and high Android growth rates especially in emerging markets.
- Despite Android's dominance in the market and browser share, iOS generates nearly twice the number of payments, logins, and authentications than other mobile operating systems combined.
- Consumers prefer access on the go as evidenced by the higher usage of iPhones over iPad.

Volume per Mobile OS / Device



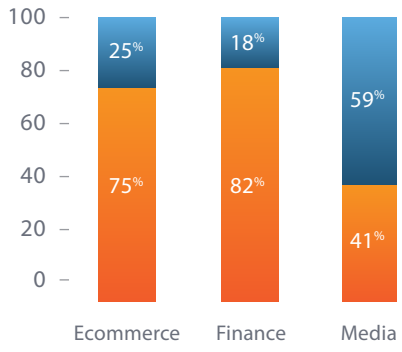
Attack per Mobile OS / Device



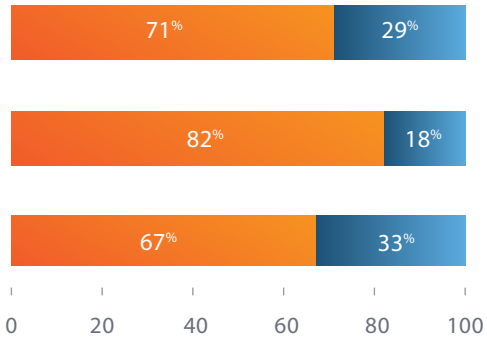
Mobile vs. Desktop Transactions and Attacks

- Mobile device-based commerce represented nearly one-third of the total transactions analyzed. This number continues to grow across industries and transaction types.
- Mobile usage for financial institutions declined for this period due to the high number of tax filing transactions that are more efficient via desktop.
- The prevalence of stolen identities and tools to enable cloaking/spoofing is causing a continued increase in the attacks targeted at mobile devices.

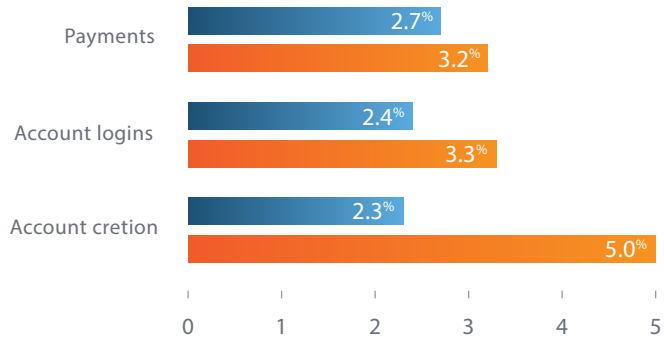
Mobile vs Desktop Transactions by Industry



Mobile vs Desktop Transactions by Type



Mobile vs Desktop Attacks by Transaction Type

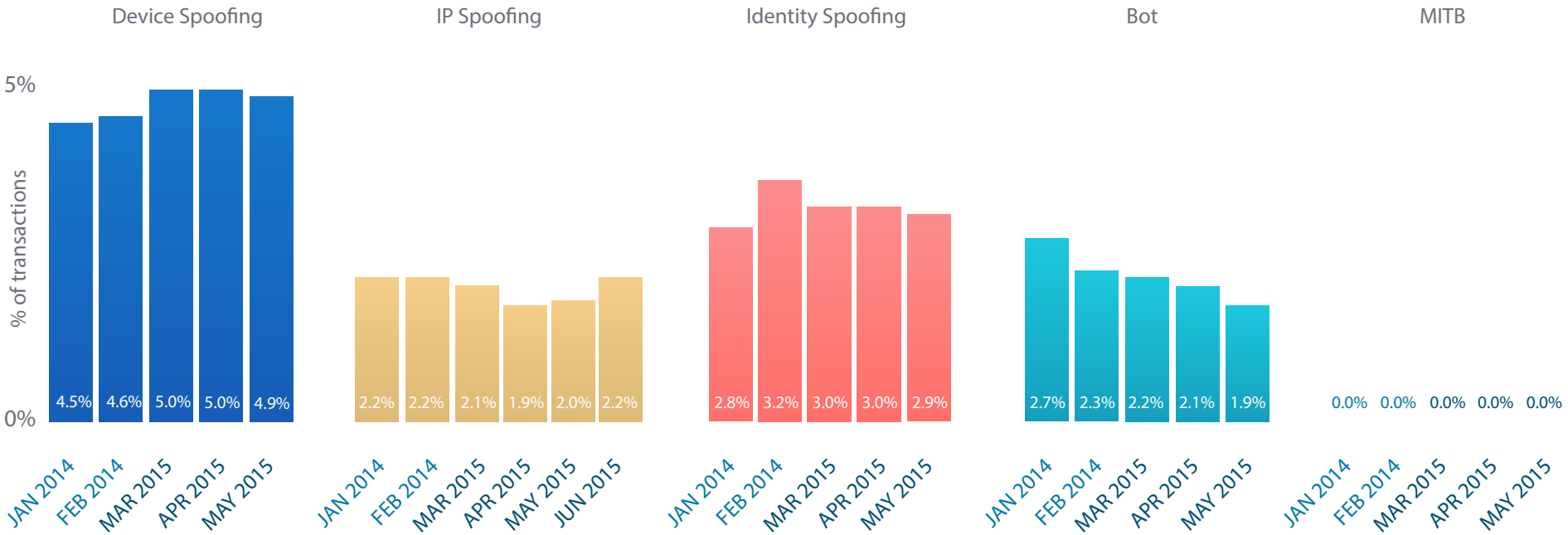


Desktop Mobile

ThreatMetrix®

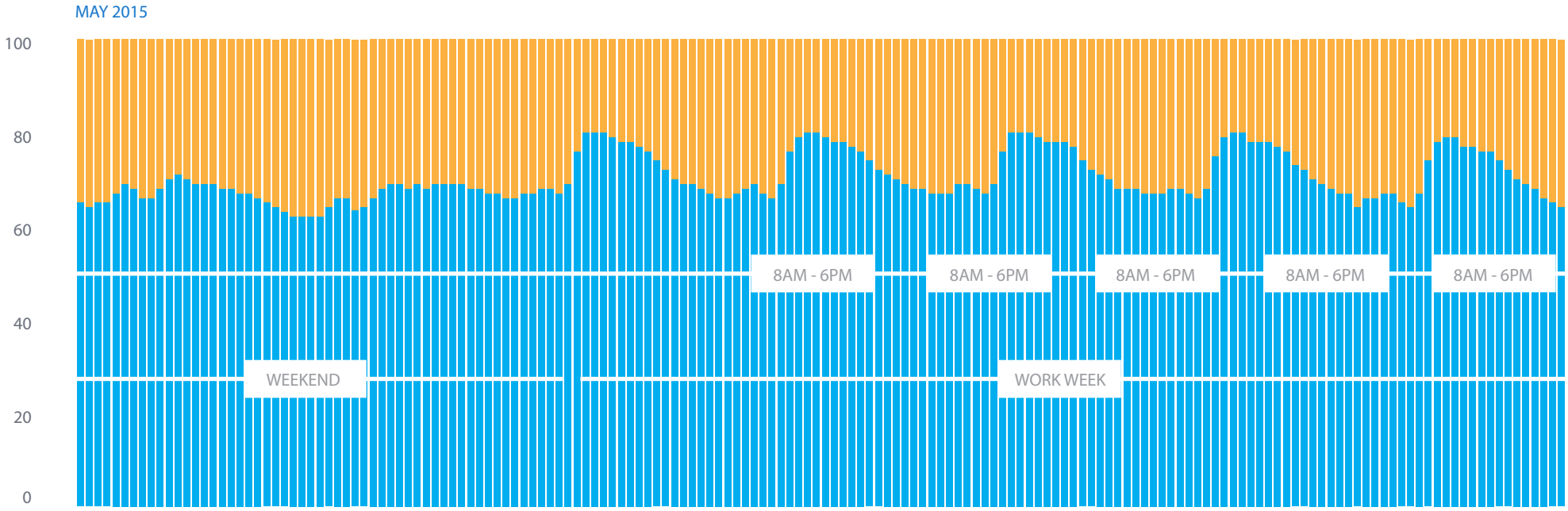
Mobile Transaction and Attack Trends

- Growth of mobile and the prevalence of stolen identities in the wild is causing an increase in mobile attacks.
- Fraudsters increasingly impersonate other devices to facilitate their attacks.



Mobile Transaction Trends – Daily

- Usage of mobile continues to grow as more customers switch to mobile to access content, conduct commerce transactions and buy products and services.
- Mobile usage increases during off-hours and weekends as users increasingly rely on their connected devices to access services/view content.
- The data below represents the number of transactions and not actual usage. Consumers move seamlessly between devices and hence actual mobile usage during the work week could potential be higher than the number of profiled transactions/events.



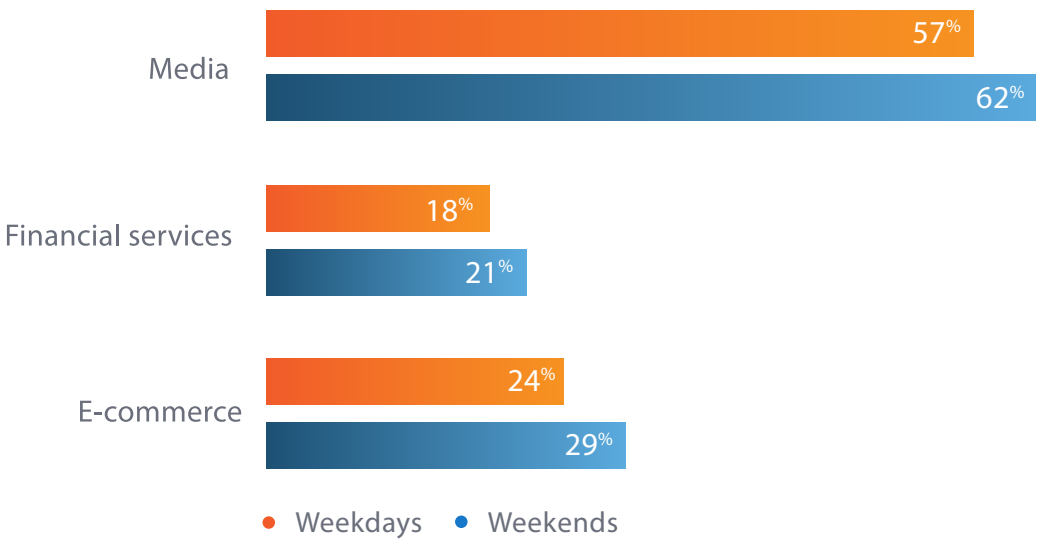
Note

- Data normalized for timezones

Mobile Transaction Trends – Weekday Vs. Weekend

- Mobile usage was up 10% compared to Q4 2014 and Q1 2015.
- Use of mobile to sign up for services continues to be a leading use case. This makes it critical for businesses to eliminate friction for trusted users while stopping fraudsters.

% Mobile transactions weekends vs weekdays



In Summary

- Growth of connected devices is changing the payment and commerce landscape. The number of devices carried by an average consumer has increased and so has usage. As such, companies are trying to embrace a “mobile-first" approach to deliver a better consumer experience on connected devices. Meanwhile, consumers continue to seamlessly move between devices to access information, content and services as well as complete transactions, leaving digital footprints that are increasingly breached by cybercriminals to perpetrate fraud across industries.
- Cybercrime is a well organized global phenomenon with criminals fast adopting new technologies and tactics to attack businesses. With their sophisticated technology and strong knowledge sharing across organized crime rings, nation states and decentralized cyber gangs, these cybercriminals continue to attack traditional and non-traditional sources of consumer data to stitch together identities that can exploited.
- The ThreatMetrix Digital Identity Network empowers businesses with real-time intelligence to recognize their trusted consumers across channel, location and devices. The Network enables businesses to reduce fraud and operational costs without compromising customer experience.
- ThreatMetrix delivers advanced fraud protection, frictionless authentication, and customer protection through a real-time collective response using intelligence gathered from billions of transactions in the ThreatMetrix Digital Identity Network.

Glossary: Industry Types

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

E-Commerce includes retail, airlines, gambling, gaming, travel, marketplaces, ticketing and digital goods businesses.

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

Glossary: 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.

Glossary: 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: 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

For More Information:

For more information on how ThreatMetrix® can prevent fraud and reduce transaction friction, visit our website at **www.threatmetrix.com** or contact **sales@threatmetrix.com.**

ThreatMetrix®