Q2 2016 CYBERCRIME REPORT

ThreatMetrix®

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

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

www.threatmetrix.com

Foreword

At ThreatMetrix we continuously monitor the changing online environment. If you notice the evolution, you are able to understand the dynamics of the rapidly changing digital commerce space and identify opportunities and threats that digital businesses face. Technology is promising to transform every industry and user interaction. We are well into the 3rd industrial revolution wherein the sharing or village economy is fast becoming the way that innovators are leveraging the urbanization and digitization of consumers. Trust is at the heart of this economy and this is predicated on an organization's ability to distinguish trusted users from fraudsters while continuing to place user experience at the heart of their digital strategy, streamlining access and reducing friction.

Central to this process of digital transformation is the increasing reliance on peer-to-peer feedback and review. Consumers increasingly rely on user generated content to make purchase decisions, whether it be booking travel, choosing a service or buying goods. While it has never been easier for users to create and post online content, reviews, and opinions, the same is also true for fraudsters. Yet many consumers blindly trust much of what they read online, without considering where it might have originated.

The inherent challenge lies in the fact that fraudsters are becoming almost indistinguishable from trusted users, employing a patchwork quilt of tactics to deceive even the most diligent businesses and users. The flood of stolen identity data available in the wild following numerous data breaches means fraudsters often behave more like legitimate users than the real consumers, answering step-up authentications questions with ease.

Businesses must maintain the integrity of their online platform and ensure that every user interaction is trustworthy and legitimate. Data breaches, scams and fake reviews can have an extremely negative impact on user trust, reputation and lifetime value.

The key challenge, however, is that user personas vary enormously across the suite of digital touch points, and the interactions fluid. Mobile apps, for example, are increasingly used for repetitive daily tasks such as checking bank balances or ordering food, but users might switch to a desktop to make a higher value purchase or to perform tasks not currently supported by mobile apps. Analyzing any interaction or platform in isolation cannot build a complete picture of the user's true online behavioral pattern.

The critical currency in authenticating user identities is global digital identities, created from the almost infinite connections a user makes as they transact online across web, mobile and end-point. The ThreatMetrix Digital Identity Network is the largest repository of digital identities in the world and has analyzed approximately 5.2 billion transactions this quarter.

Alisdair Faulkner
Chief Products Officer

Q2
2016

Q2 2016 Report Overview

Overview

The ThreatMetrix Cybercrime Report: Q2 2016 is based on actual cybercrime attacks from April 2016 – June 2016 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 ThreatMetrix Digital Identity Network provides visibility and insight into traffic patterns and emerging threats. The Network analyzes close to two billion transactions per month, around 40% 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.

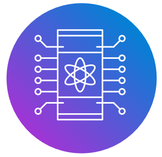
Attacks discussed are from "high-risk" transactions scored by ThreatMetrix customers.

Q2
2016

Key Highlights

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

Over 5.2 billion transactions were analyzed by the ThreatMetrix Digital Identity Network this quarter with 40% coming from mobile devices.



More than 112 million attacks were detected and stopped in real time; a 50% increase over the previous year. In addition, more than 450 million bot attacks were identified and stopped during this period, a 50% increase over previous quarter.

The impact of EMV migration is clearly visible, with massive growth in attacks targeting global online retailers. There were 69 million e-commerce attacks this quarter driven by the billions of stolen credentials available on the dark web.

Around 10% of account creations are now rejected, an increase of 250% from the previous year. This highlights the relentless use of stolen credentials, particularly in e-commerce and media. Although new accounts in financial services are attacked less, alternative payment platforms and e-lenders seem to be more susceptible than traditional institutions, as fraudsters appear to target these new platforms to sign up for quick loans using stolen identities.

Account creations from mobile are growing rapidly and are increasingly being attacked. Creating a new account using mobile often bypasses a lot of the security features that biometrics etc. offer.

Digital authentication continues to be one of the biggest use cases globally.

Q2
2016

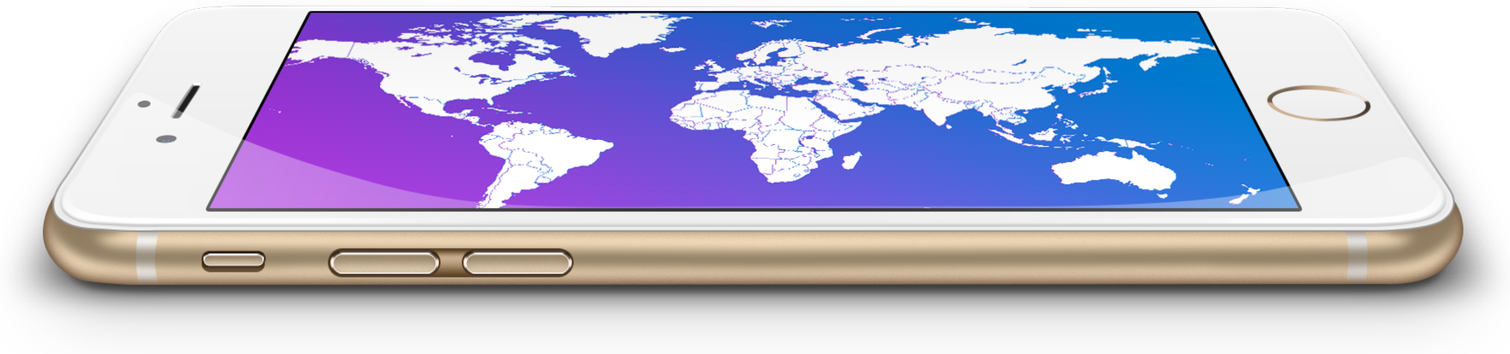
Trends and Surprises

Trends

- Continued growth of attacks across segments. 50% increase in attacks over Q2 2015.
- Impact of EMV mandate on CNP fraud evident in the high levels of attacks on CNP merchants.
- Impact of recent data breaches seen in the increase in new account origination fraud.
- Mobile transactions continue to grow.
- Mobile banking is more popular than ever amongst returning customers in financial services, who continue to login to online banking via mobile apps almost twice as much as via desktop.

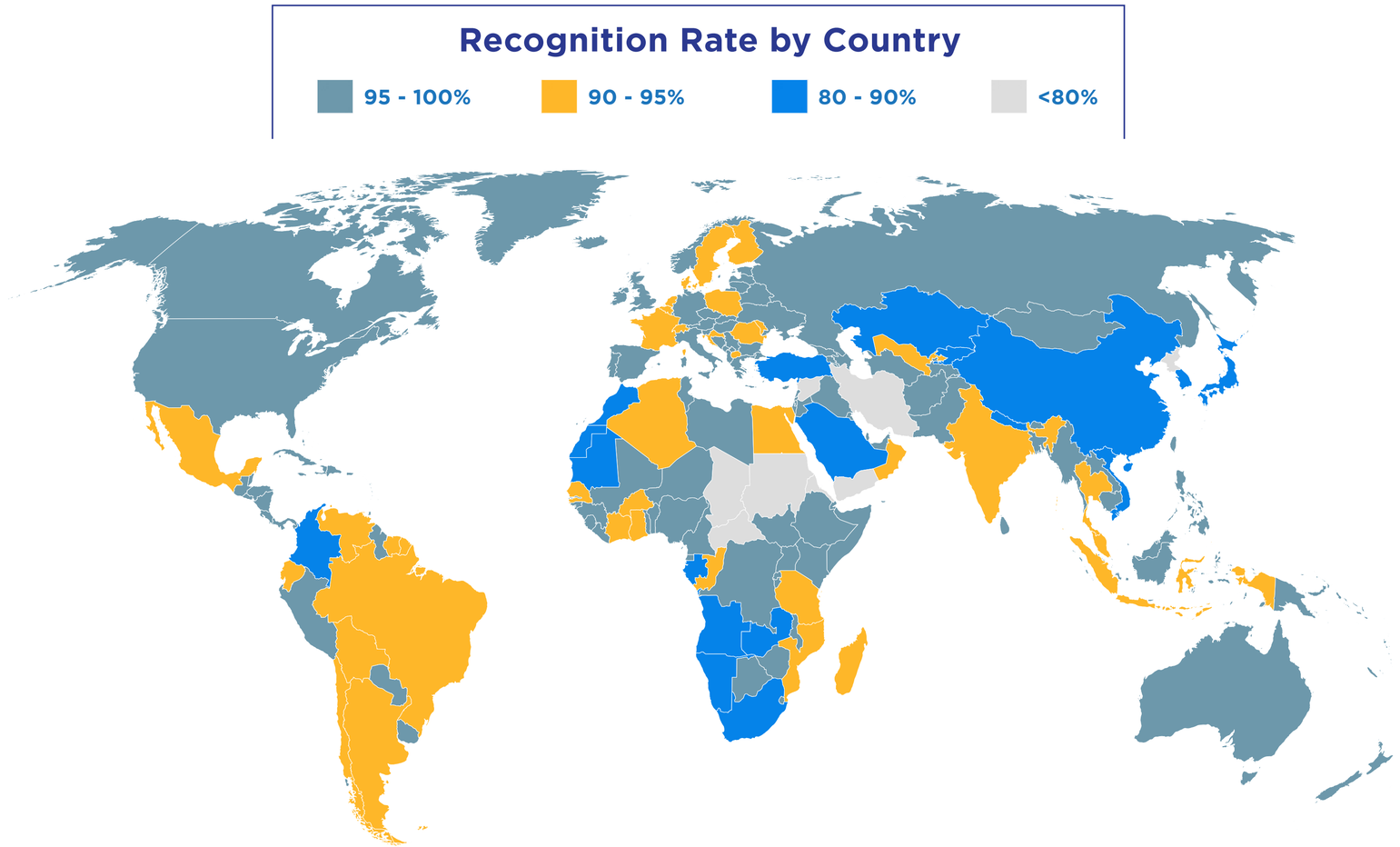
Surprises

- Massive increase in bot attacks targeting financial institutions, particularly FinTechs.
- Emergence of mobile bot attacks targeting mobile apps.
- 500% growth in mobile transactions for financial institutions compared to same quarter last year.
- 25% increase in "mobile only" users for financial institutions compared to last quarter.
- China emerges as one of the big attack destinations.
- Cross-border transactions are growing and continue to be considered riskier.



Q2
2016

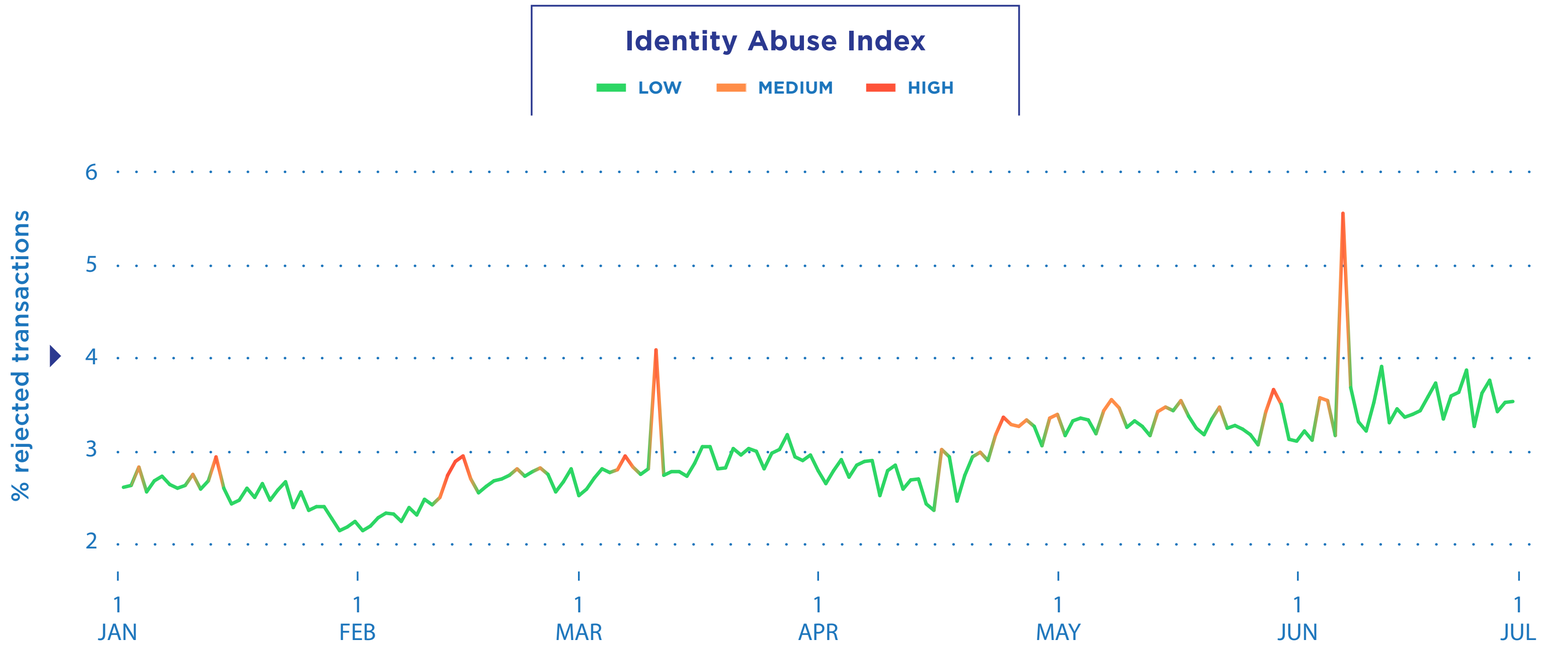
Recognition is Key



Persona (device, identity, behavior) recognition by the ThreatMetrix Digital Identity Network ensures that businesses are able to effectively differentiate between trusted users and potential threats

Q2
2016

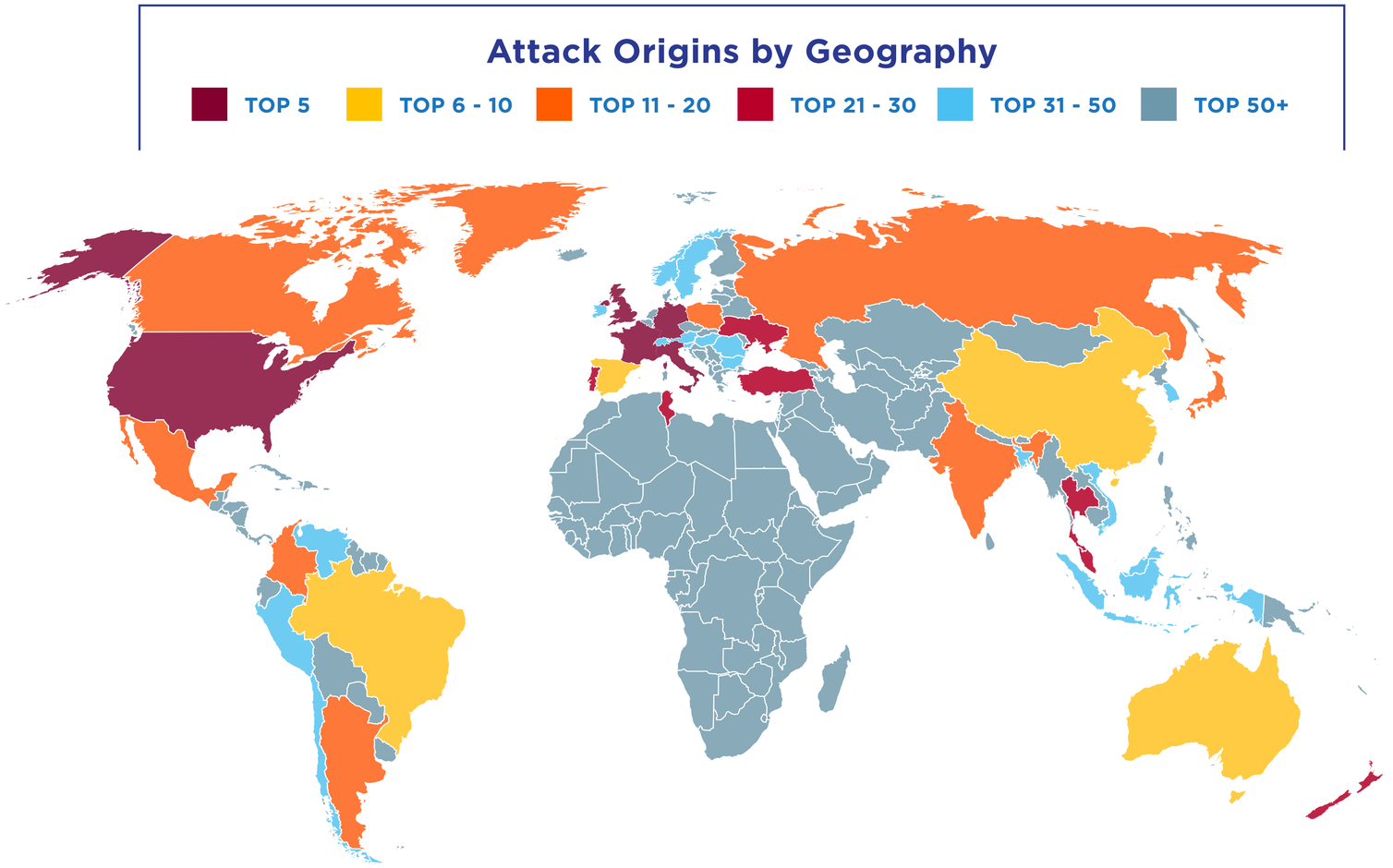
Attacks are Growing in Size, Frequency and Complexity



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, it clearly shows that the exploitation of data breaches and stolen identities is automated, global and co-ordinated.

Q2
2016

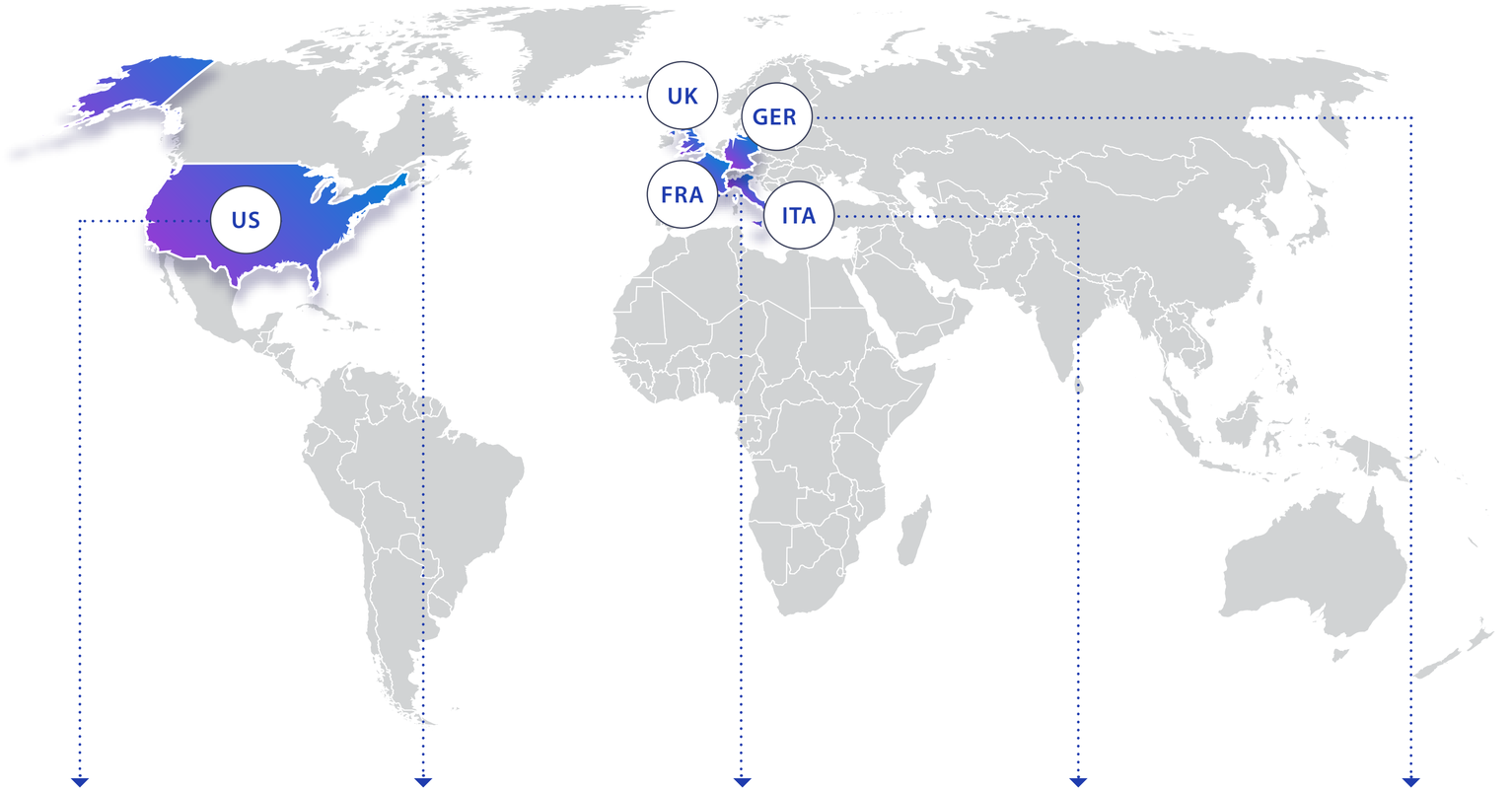
Top Attack Originations



Q2
2016

Top Attack Destinations

ATTACK ORIGIN ATTACK DESTINATION



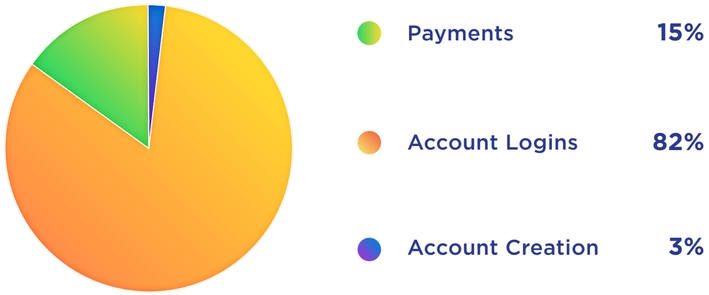
UNITED STATES	UNITED STATES	UNITED STATES	UNITED STATES	UNITED STATES
UNITED KINGDOM	UNITED KINGDOM	UNITED KINGDOM	UNITED KINGDOM	UNITED KINGDOM
BULGARIA	IRELAND	AUSTRIA	AUSTRIA	IRELAND
CHINA	AUSTRIA	IRELAND	GERMANY	AUSTRIA
CANADA	CHINA	LUXEMBOURG	IRELAND	BULGARIA

Q2
2016

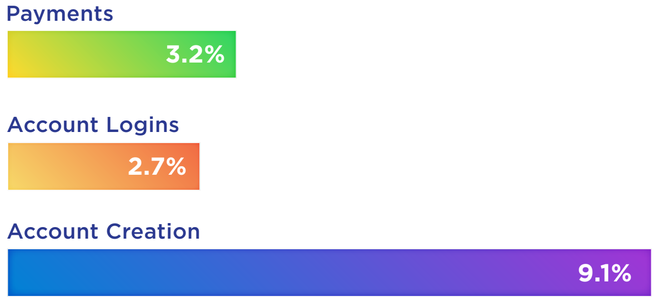
Transactions and Attacks

Transactions Analyzed by Type

Volume per Transaction Type



Reject Rate per Transaction 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 our customers deploy ThreatMetrix to authenticate user identities without impacting consumer experience.

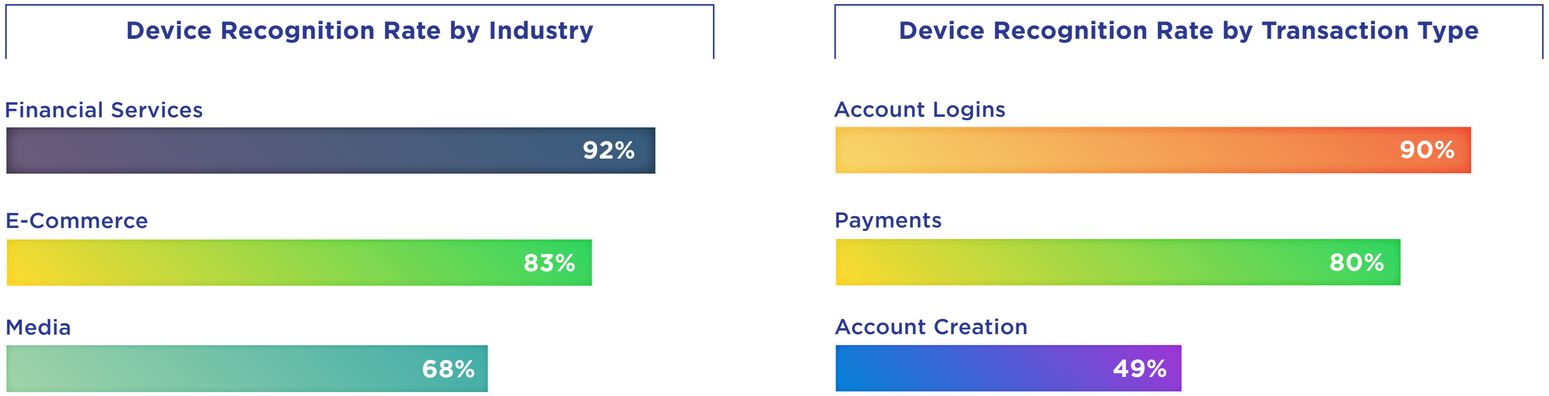
The overall attacks increased by over 50% compared to the previous year. Attacks on new account creations went up 250% compared to the previous year. This large increase in account creation fraud is driven by the increased availability and low cost of stolen identities in the wild, harvested from massive breaches.

50% of transactions come from financial services, however the overall attack levels on financial services are low given high consumer engagement and a high proportion of customers accessing services via their mobile phone / app.

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.*

Q2
2016

Recognition Across Devices – New and Old

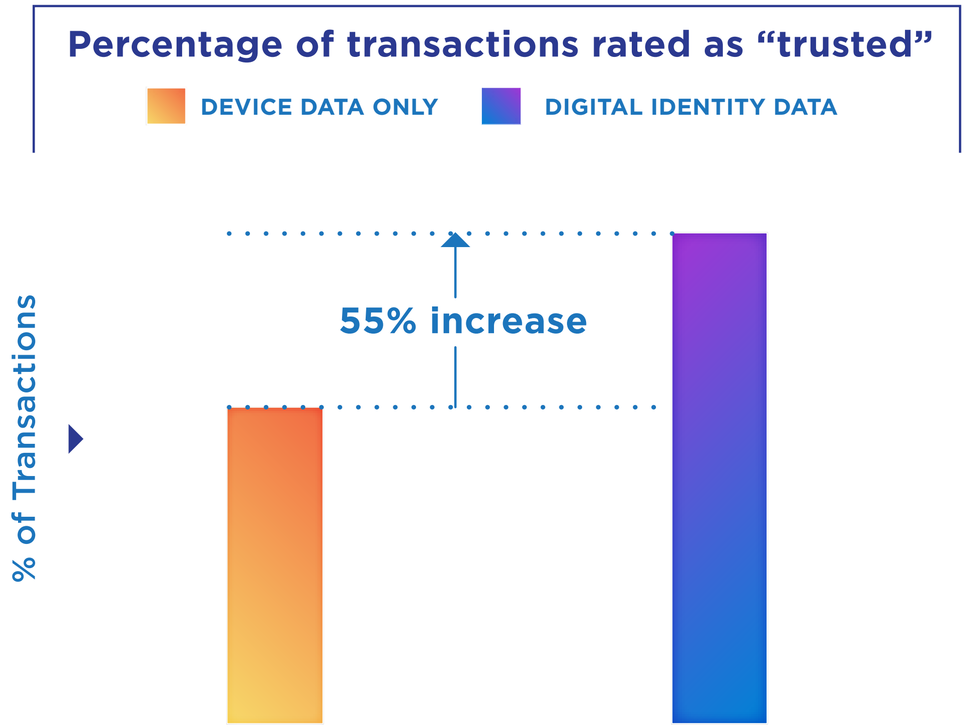


- Online access allows digital consumers to interact with trusted providers more regularly than if they had to visit a physical branch or store. Users can share a much closer relationships with businesses and login to their accounts frequently. This creates a larger volume of transactions from repeat visitors and returning customers.
- The Network continues to grow rapidly with hundreds of millions of new users and associated devices added each month.
- With 87% of transactions coming from recognized devices, other aspects of a user's true digital identity are leveraged to authenticate users in real-time, such as locations, online behavioral patterns and other anonymized personal information.
- The recognition for mobile devices is around 95%. This higher recognition ensures that businesses are able to deliver frictionless experience to their mobile consumers.
- As expected, the device recognition rate is highest for financial services companies and for transaction type "account login" (users logging in regularly to check their account).

Note: *recognition rates plotted are the % of transactions where the device is a returning device to The Network*

Q2
2016

Digital Identities - Ability to Recognize Trusted Users

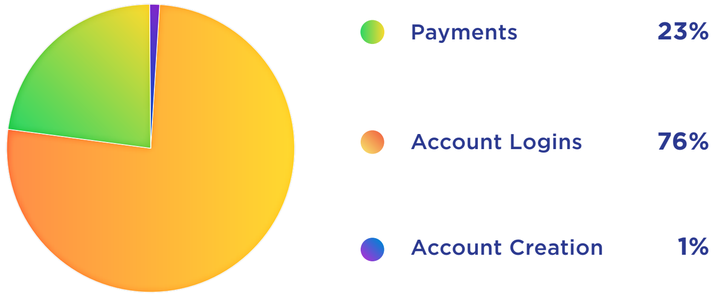


- Having a single view of how a user’s unique digital identity is made up across industries, channels and interactions is going to become more and more crucial.
- The ThreatMetrix Digital Identity Network enables businesses to analyze the various components of a user’s digital identity in real time.
- The ability to recognize a trusted user goes up with incremental data elements, giving businesses a robust way to identify legitimate consumers.

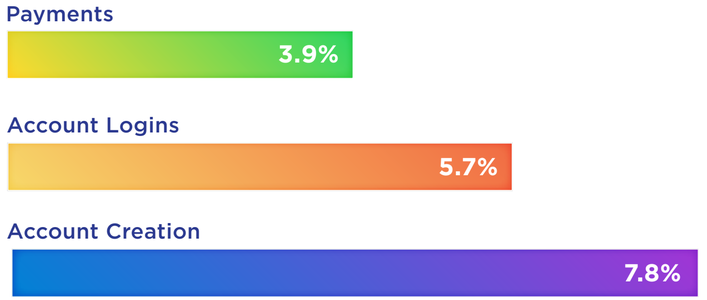
Q2
2016

E-Commerce Transactions and Attacks

Volume per Transaction Type



Reject Rate per Transaction Type



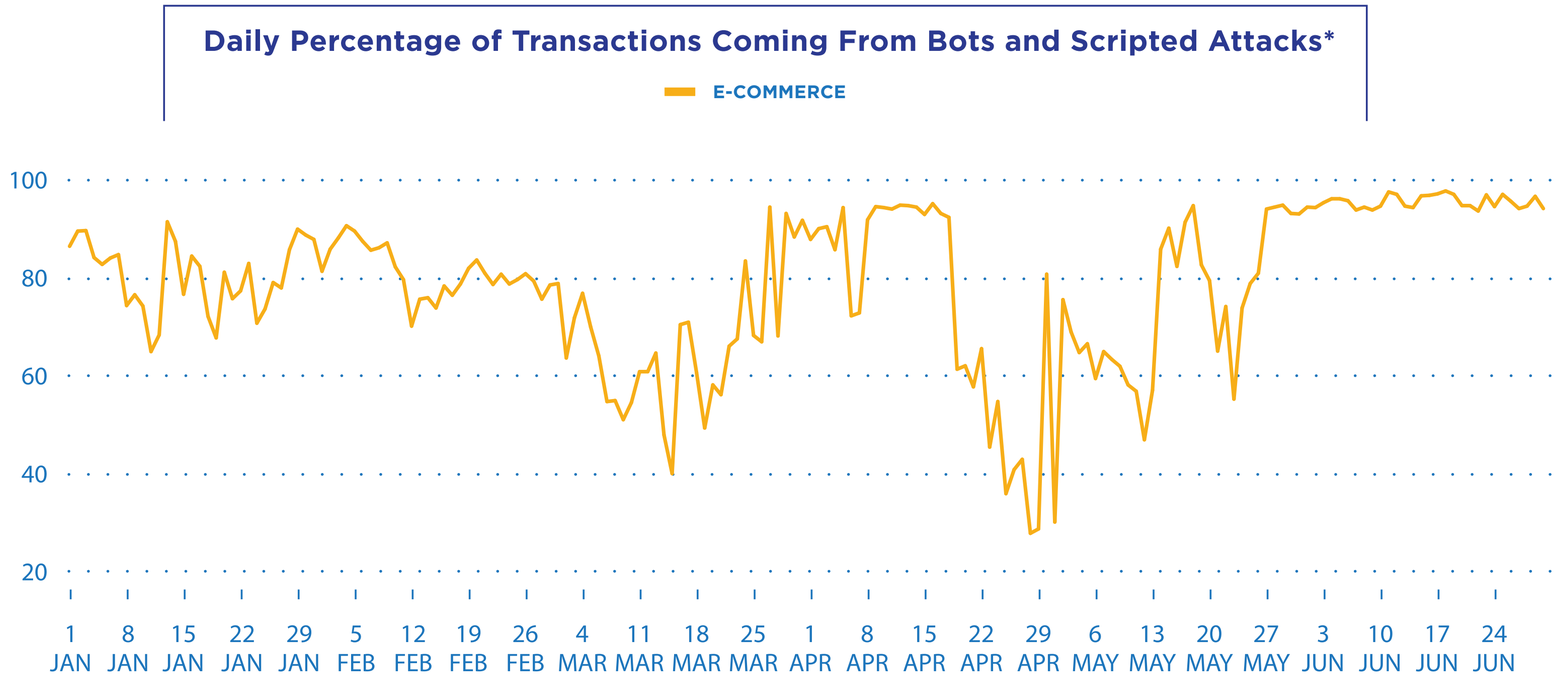
This quarter saw the highest level of attacks on e-commerce with more than 69 million rejected transactions, representing 90% increase over the previous year and a 12% increase over the previous quarter.

We are beginning to see the aftermath of last year's EMV migration, with fraud targeting e-commerce retailers growing at a rapid pace. Reject rates went up across all use cases. As businesses prepare for the back-to-school and holiday shopping season, they will increasingly have to balance fraud and risk management with strong customer authentication.

As with previous quarters, attacks targeting user identities to access personal and payment information are continuing to grow. To access this rich consumer data, logins are increasingly targeted by fraudsters. It is much more lucrative to access a trusted credit card saved in a valid customer account than it is to attempt to re-use a stolen card that has a limited shelf life.

***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.*

Threat Detection – A Constantly Evolving Cat and Mouse Game



Leading online retailers were attacked relentlessly by bots, botnets and other scripted attacks. With so many high profile breaches in recent months, fraudsters have easy access to user credentials that they can exploit individually or part of mass identity testing sessions. Over 400 million bot attacks were detected this quarter for e-commerce merchants across the globe.

Bot attacks have evolved from being large volume distributed denial of service (DDoS) or spam attacks, to low-and-slow bots, designed to evade rate and security control measures and mimic trusted customer behavior / login patterns.

Unlike previous quarters, these attacks resulted in continued spikes in volume throughout the quarter as the fraudsters sliced down the list of user credentials. These low velocity attacks are distributed but grouped and hard to detect.

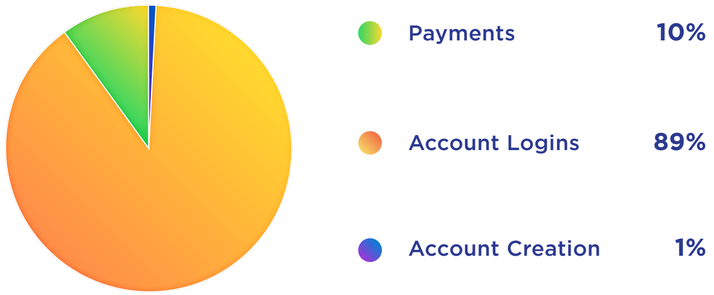
ThreatMetrix uses context-based information to perform behavioral analysis of users to differentiate between a human and a bot the moment they land on the site.

Data for leading retailer

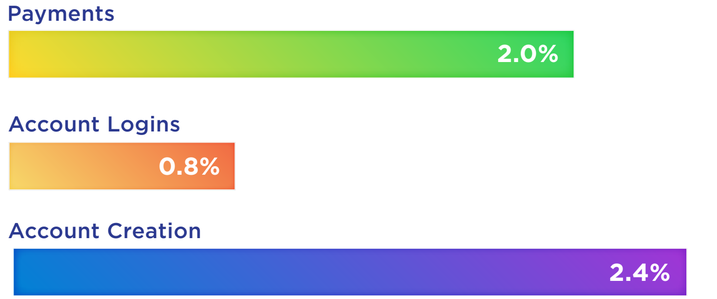
Q2
2016

Financial Services Transactions and Attacks

Volume per Transaction Type



Reject Rate per Transaction Type



Financial services transaction growth is primarily driven by mobile. Digital banking transactions have grown by 140% over the last year with mobile transaction growing 500% compared to Q2 2015.

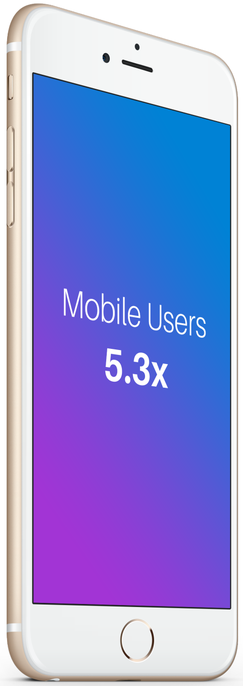
Digital consumers are increasingly able to access their banking services on the go, leading to nearly 50% of transactions coming from mobile. As such digital banking authentication is one of the biggest use case for financial services globally: several million logins a day for a mid-sized bank. In addition, more customers are becoming mobile only.

Attacks on payment transactions for financial services doubled compared to the previous quarter. Given the large volume, the risk exposure due to illegal money transfers and potential brand damage is extremely high.

Financial services organizations are less likely to block suspicious transactions outright, subjecting them instead to further review. Hence, the rejected transactions shown don't include access attempts that typically result in challenging a user to provide additional information. For example, some implement two-factor step-up authentication if they do not recognize a user's device for a given account.

***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.*

Mobile Banking Driving High Customer Engagement



How many times a week do customers log in to their bank account?

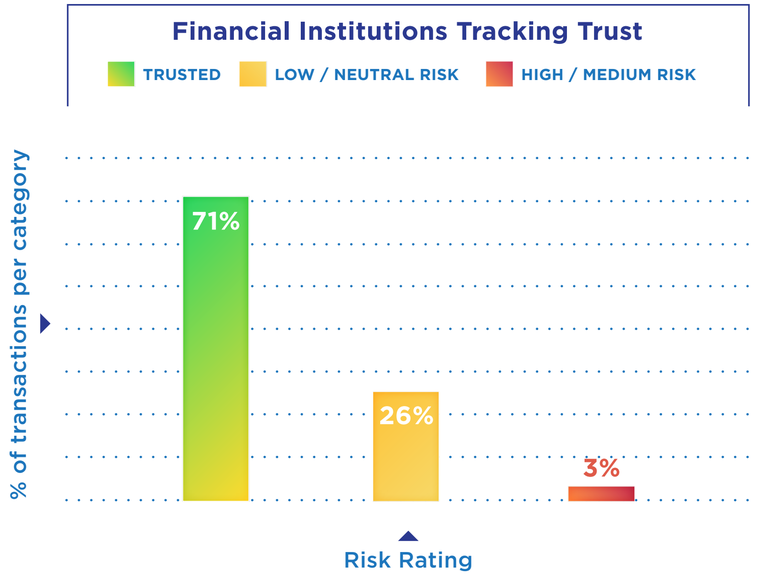
Nearly 50% of financial services transactions are mobile. Mobile has higher user engagement with nearly twice as many mobile logins as desktop per customer.

This highlights user behavior of accessing accounts more frequently due to the simplified access provided by a native app. Financial institutions need to adjust existing risk models to reflect diverse user behavior across different digital channels.

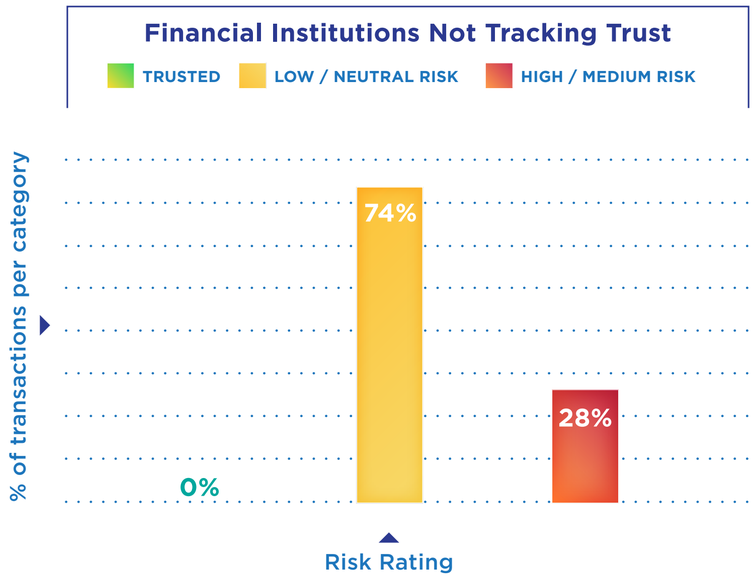
Q2 2016 was the strongest mobile quarter for ThreatMetrix with more than 5 times the number of mobile transactions in financial services compared to the previous year.

Q2
2016

Trust is Critical



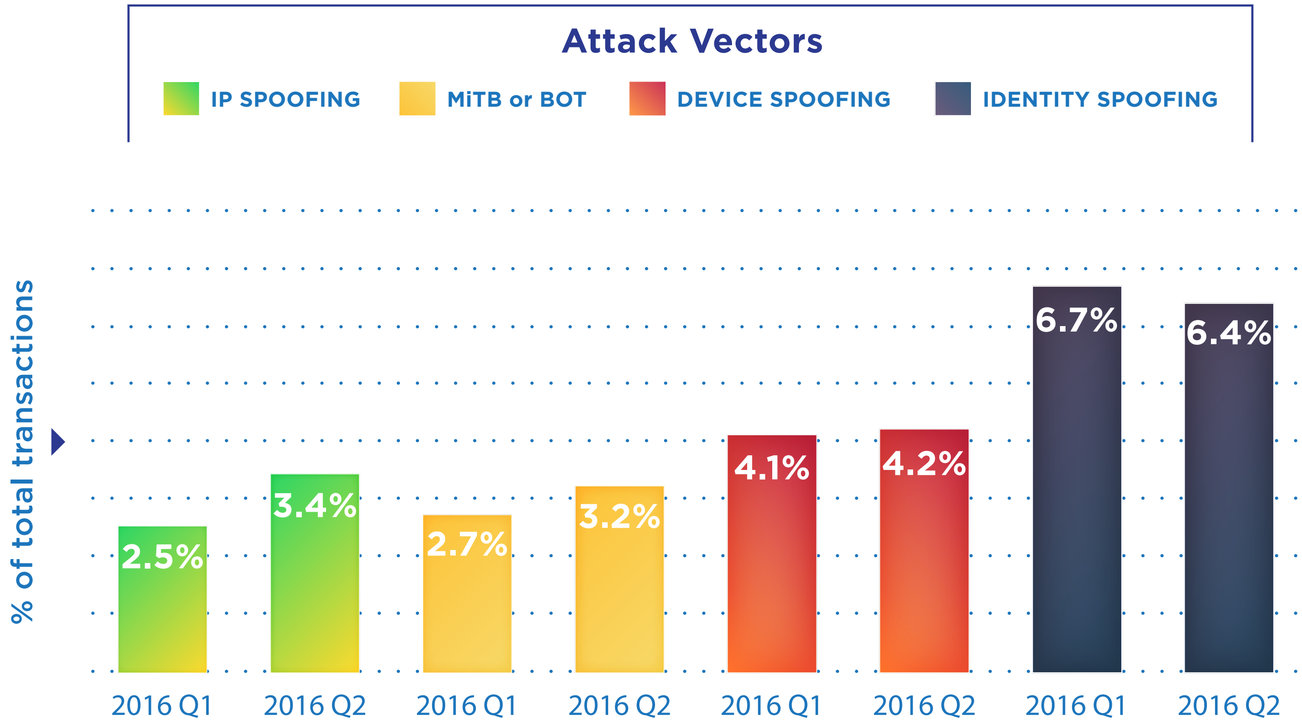
By scoring transactions based on the relative trustworthiness of the user (trust can be associated dynamically with any combination of online attributes such as devices, email addresses, card numbers etc.), businesses can positively identify returning customers and hence deliver an enhanced customer experience with virtually no associated friction.



When tracking trust, we see a 9 times reduction in high-risk transaction scores. Operational costs and manual reviews associated with reviewing high-risk transactions can be focused on the genuinely risky cases while trusted customers experience less friction.

Q2
2016

FinTech Attack Vectors



Digital commerce is providing a launch platform for internet-only banks, remittance companies, online lenders and alternative payment providers to respond with more agility to meet the evolving needs of digital consumers. These companies are including the unbanked and underbanked population, who previously had little access to traditional banking services.

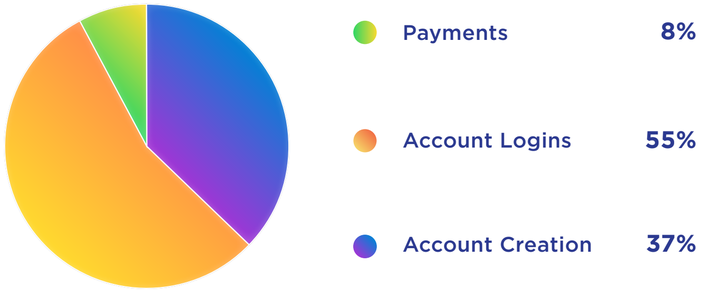
These providers have been successful by leveraging dynamic user data to make smarter decisions in real time with minimum user friction. However, their innovative approaches have also attracted fraudsters that look at these services as a way to make quick profit using stolen and synthetic credentials.

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

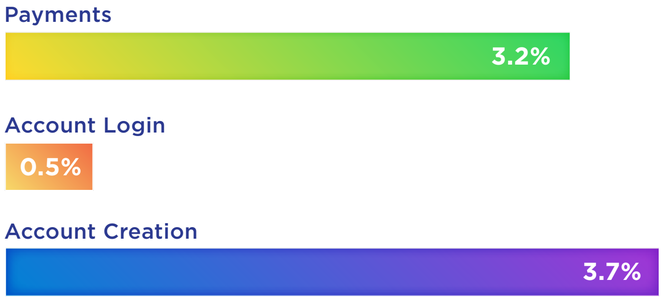
Q2
2016

E-lenders Deep Dive

E-lender volume per transaction type



E-lender attacks per transaction type



Digital commerce is driving the growth of online lending with more institutions creating financial products to target the unbanked and underbanked population. This segment is becoming the target of attacks as fraudsters attempt to exploit new platforms / application procedures.

Attacks on payment disbursement transactions are also growing.

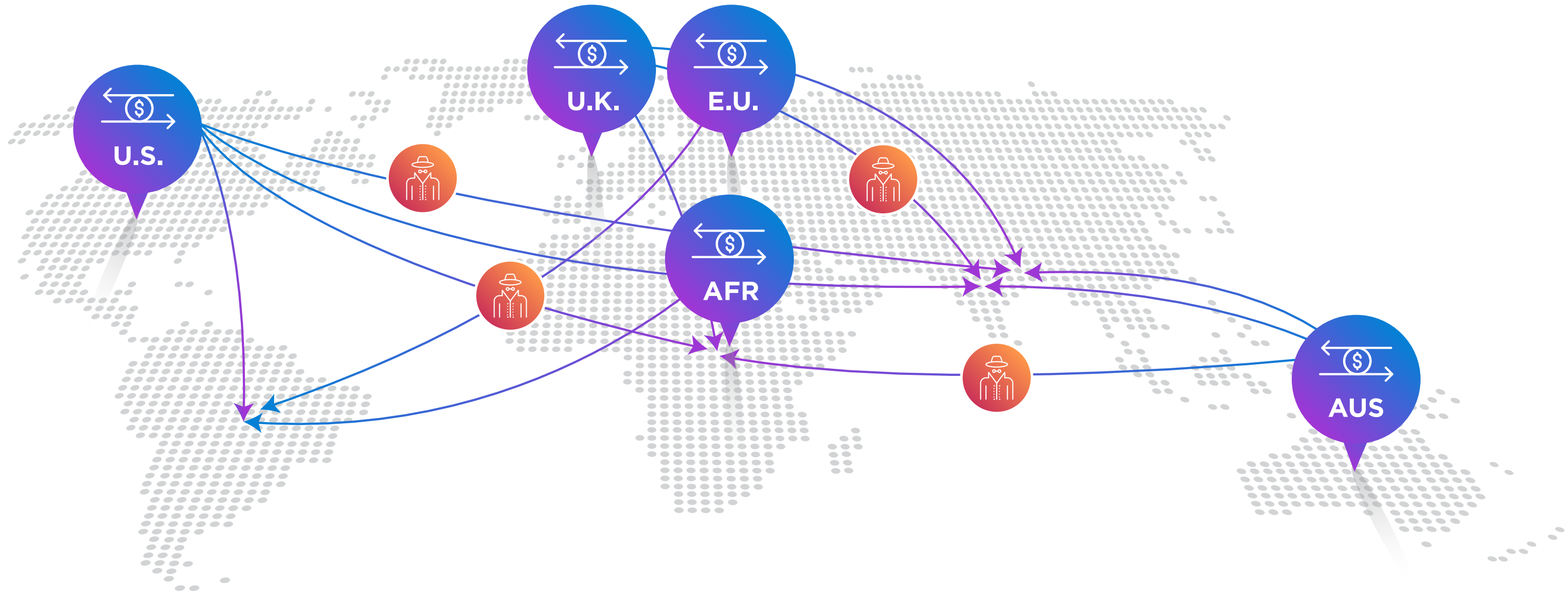
New loan application fraud continues to grow on the back of massive data breaches that expose user identities and malware used to intercept user credentials. Cybercriminals exploit this stolen data to dupe unsuspecting businesses, using cloaking technologies such as proxies or spoofed locations to mask their true identities and whereabouts.

The challenge for online businesses is that these profiles are becoming increasingly indistinguishable from authentic identities because they are created using a jigsaw of stolen data.

The Network analyzes transactions from some of the biggest lenders across to globe and enables them to avoid a Bustout / Ponzi fraud scenario where fraudsters use loans from one lender to pay another. This pattern continues until they inflate the loan value to the maximum possible, and then default on the loan repayments.

***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.*

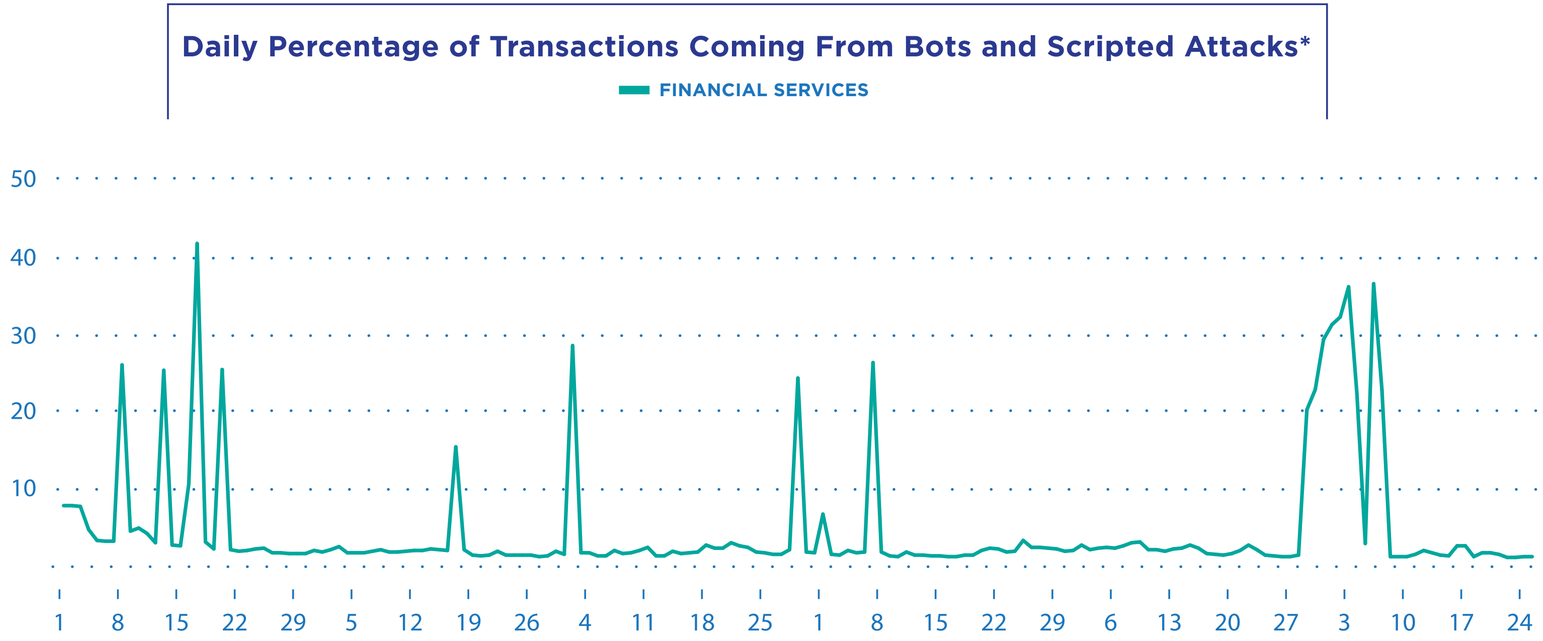
A Connected World – Remittance Corridors



- Digital consumers are increasingly open to trying new payment methods as evidenced by the growth of digital wallets.
- At the same time, P2P remittances are growing as consumers are increasingly mobile and traveling across the globe. These remittance corridors are targeted by fraudsters.

Q2
2016

Evolving Bot attacks Target Financial Transactions



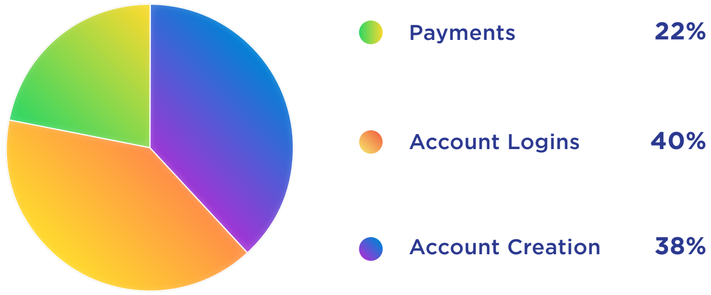
- Fraudsters have large-scale networks of infected devices available at their disposal to inundate online systems with large volumes of fraudulent transactions. They also use scripts (often in conjunction with bots) to perpetrate such transactions.
- These spikes in bot attacks represent millions of attacks targeting a single organization. A significant portion of these attacks target FinTech providers' new account application processes. ThreatMetrix detected millions of credential testing attempts using bots / scripts.

**Data for a leading financial institution*

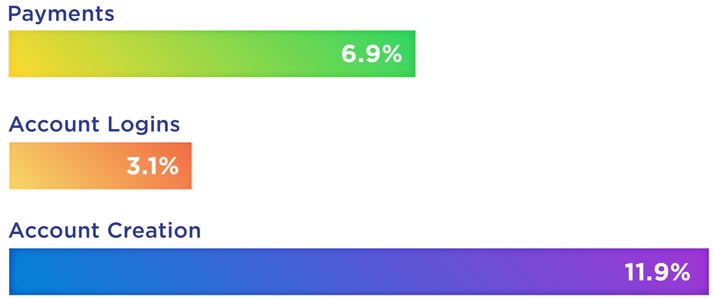
Q2
2016

Media Transactions and Attacks

Volume per Transaction Type



Reject Rate per Transaction Type



ThreatMetrix detected and stopped nearly 25 million fraudulent new account originations, payments, and bogus reviews and listings during this period. Fraudulent new account registrations increased 350% over the previous year; rising ahead of the summer travel season

Media and entertainment volumes have grown steadily over the past few years as more content is made available on-demand through digital channels.

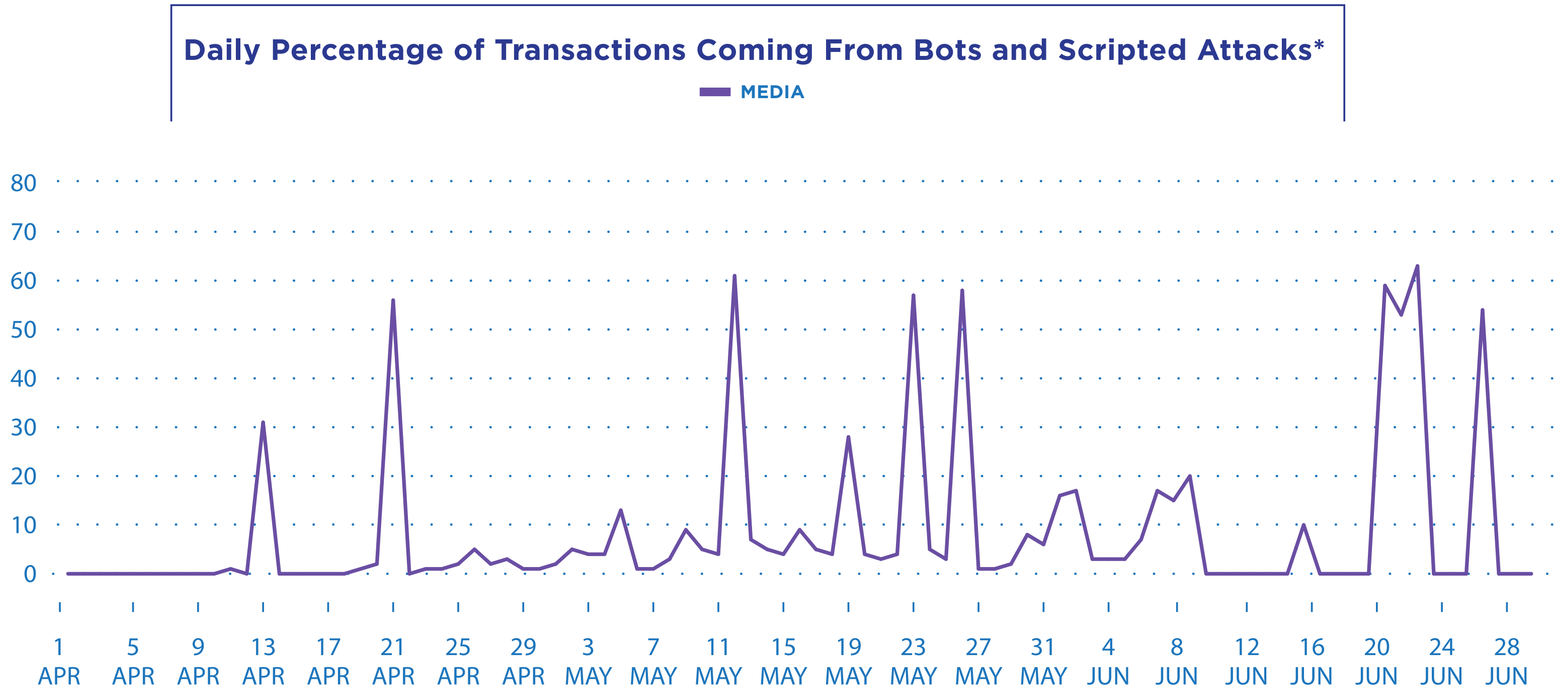
This industry attracts the highest rate of cybercrime attacks per transaction as a result of their modest sign-up requirements. Accounts can easily be created or breached thanks to user password sharing across sites, and the easy availability of stolen credentials on the dark web.

The majority of attacks against these sites are fraudulent account creations, motivated by the potential to target a large audience for advertising, distributing malware and confidence scams.

These fraudulent registrations are also used to create fake reviews or content. User generated content needs to be continually reviewed to ensure that malicious content is caught early and does not jeopardize the reputation of a media organization.

***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.*

Emerging Threat Vector – Botnets

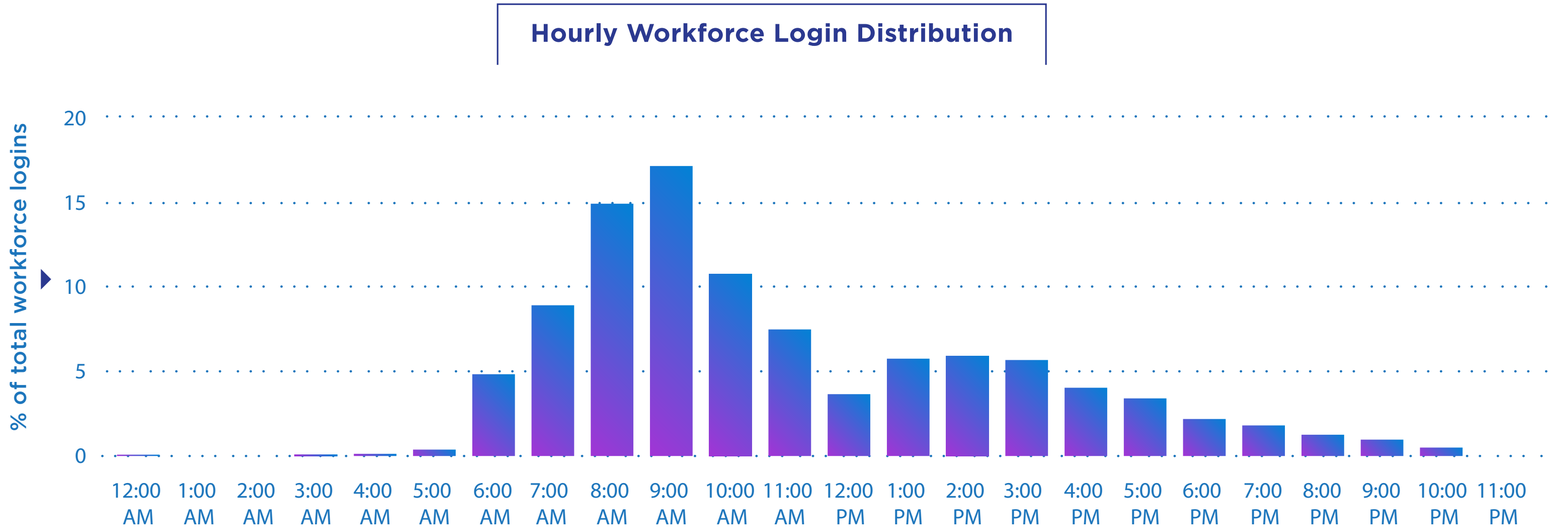


- This segment is now also under attack from fraudsters using bots and scripts to test the validity of lists acquired from the dark web. These attacks are attempts to run massive identity testing sessions on organizations which overwhelm their system and network resources.
- Fraudsters are increasingly cultivating accounts at these "user generated content" sites to use them at a later date to propagate malicious content as well as spam users.

**Data for leading media provider*

Q2
2016

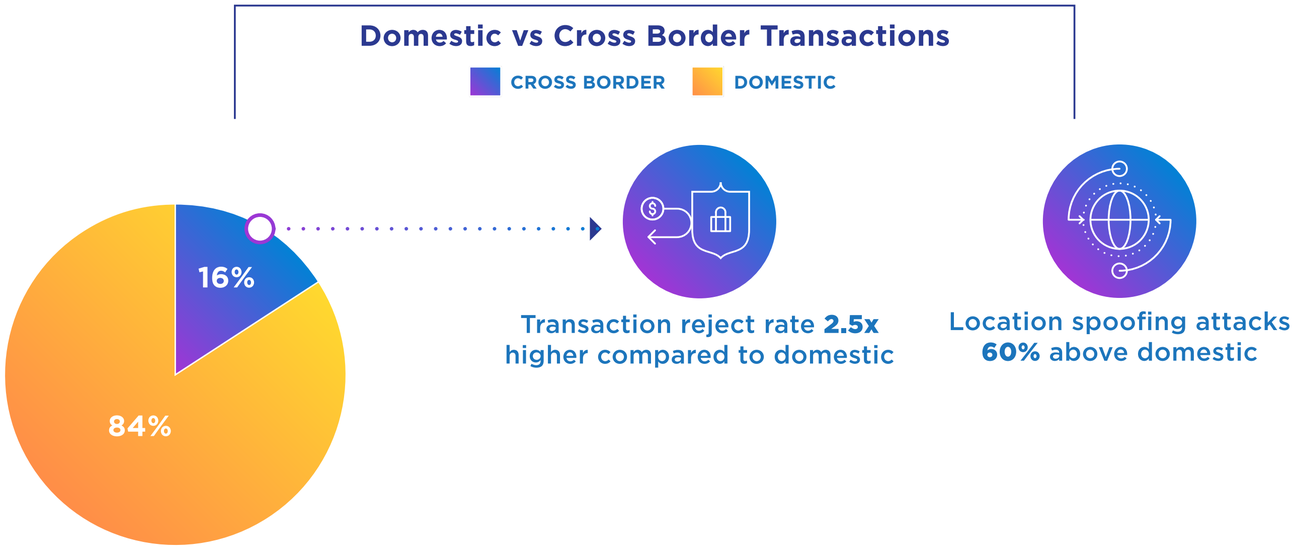
Workforce Logins – Threat from Within



- In a digital world, what has traditionally been considered as "enterprise" is morphing into "web" as employees work remotely and login in from diverse global locations, across many devices.
- Employee logins are increasingly being attacked as they can often be a gateway to larger networks of data and information.
- Attack levels follow a fairly consistent hourly pattern, with increased attacks seen around midday, which is associated with a period of low productivity.

Q2
2016

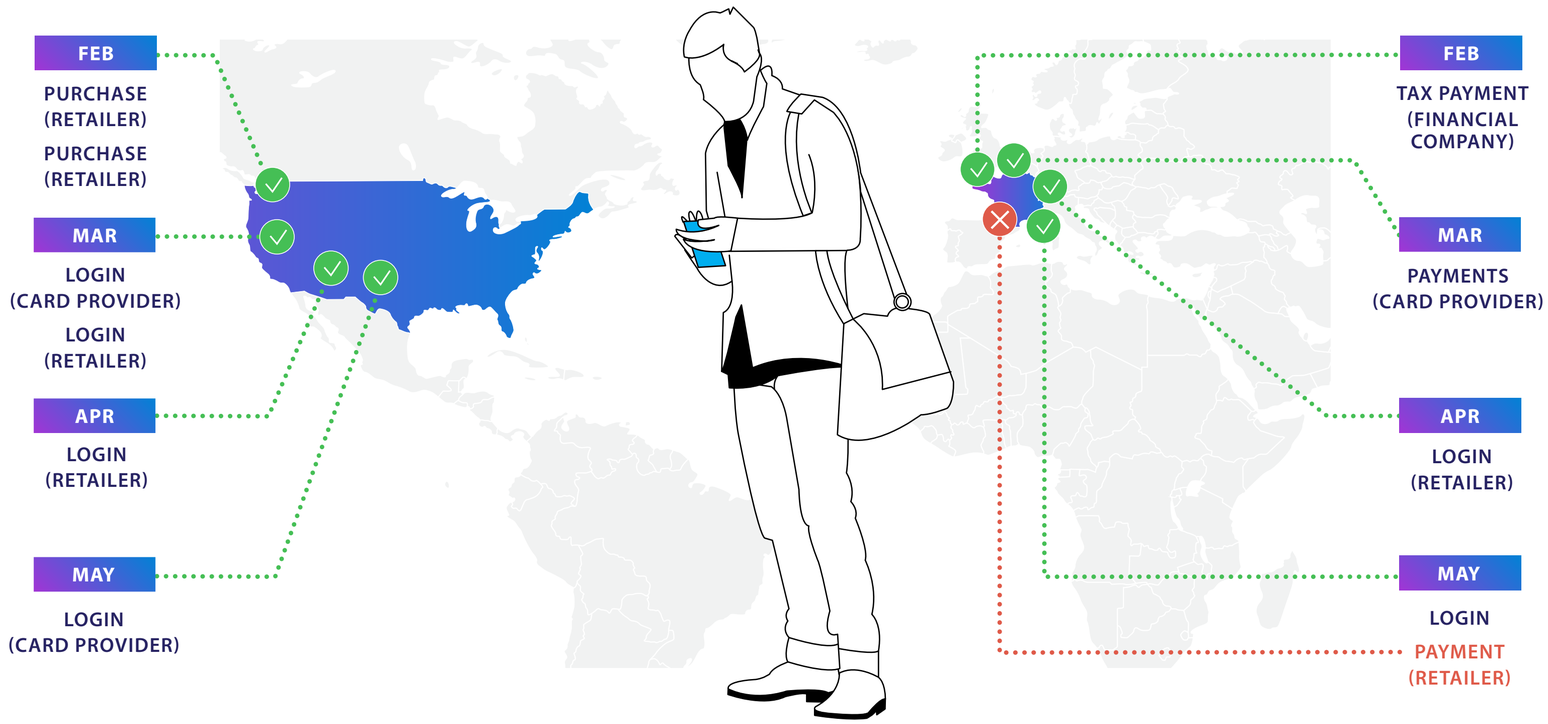
Cross-border Transactions – Business Without Borders



- 16% of transactions in The ThreatMetrix Digital Identity Network are now cross-border transactions.
- As more consumers travel extensively and look to access services / content outside their home country, the global cross-border transaction volume is growing.
- However, as businesses extend their products and services to a global audience, they are becoming more susceptible to global cyber attacks.
- Most businesses approach cross-border transactions with caution; hence the reject rate is 2.5 times higher than domestic transactions. A big driver of this is the custom rules set by businesses that often reject transactions from specific countries.
- Fraudsters try to cloak / spoof their location to bypass these rules. As a result, location spoofing attacks for cross- border transactions were 60% above domestic transactions.

Tracking a Digital Customer - Business Without Borders

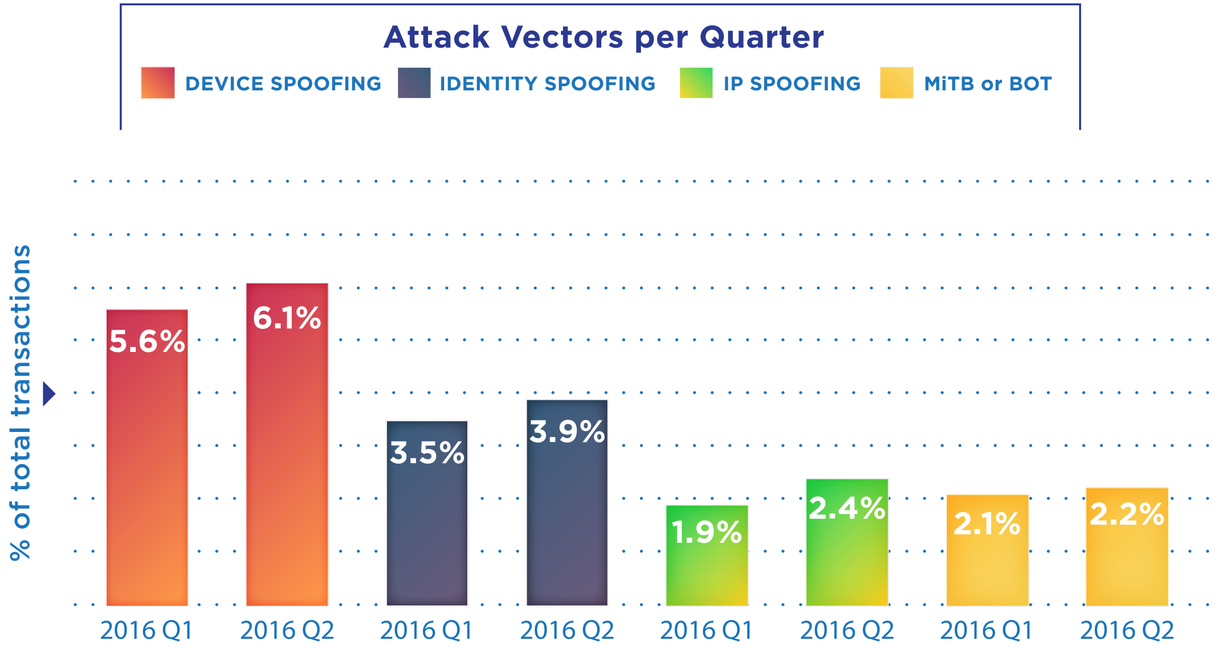
An example of one user (a unique digital identity from The Network) traveling between the U.S. and Germany, using the same device and email address to do multi-organization and cross-border transactions. Our global Network can recognize this user, building trust as he transacts online in order to let him make frictionless cross-border transactions



- Final transaction rejected based on static legacy fraud rules that do not take into account the full digital identity of the user.
- The transaction was made using the same trusted device that is seen elsewhere in the Network.
- By leveraging all known information relating to the transaction, (e.g. device history, locations, behaviors and identity data), ThreatMetrix customers can confidently recognize trusted customers even if aspects of their online behavior change.

Top Attack Methods

Top Attack Vector Trends



ThreatMetrix identified more than 100 million fraud attempts during this period. This represents a 49% growth over the previous year.

Attack vectors are analyzed in real time by the ThreatMetrix global policies. Some attacks use multiple vectors.

All attacks vectors, especially impersonation or "spoofing" attacks are growing, driven by availability of more sophisticated device spoofing tools combined with hacked and breached identities.

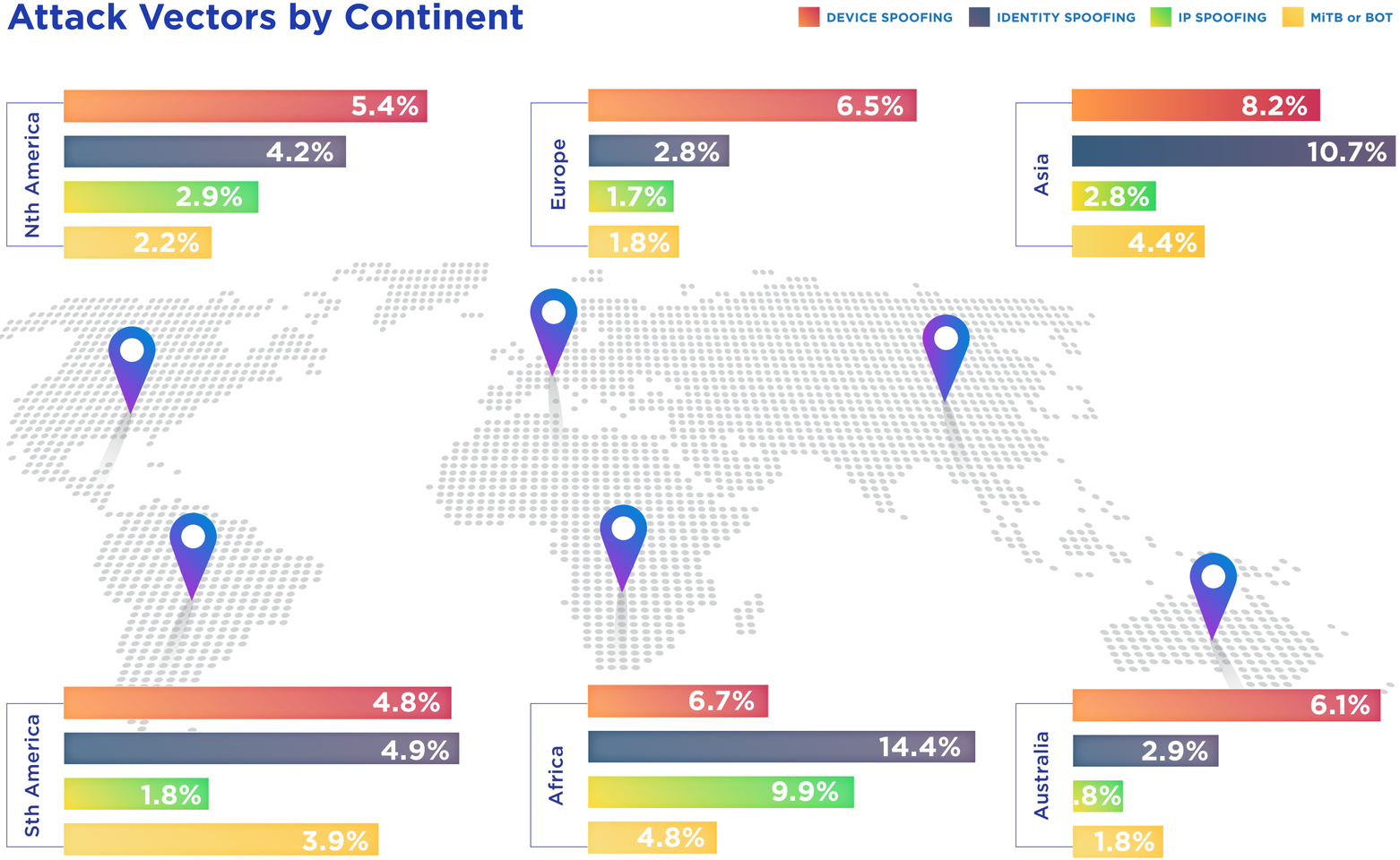
New account creations are especially vulnerable wherein the fraudsters use stolen identities along with these tools to defraud businesses.

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

Criminals are increasingly stitching together the various aspects of consumer data (made available through breaches) to open new accounts, steal payment information and take over existing user accounts. These attacks are detected by analyzing the end user's true digital identity to identify anomalies and potential fraud.

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

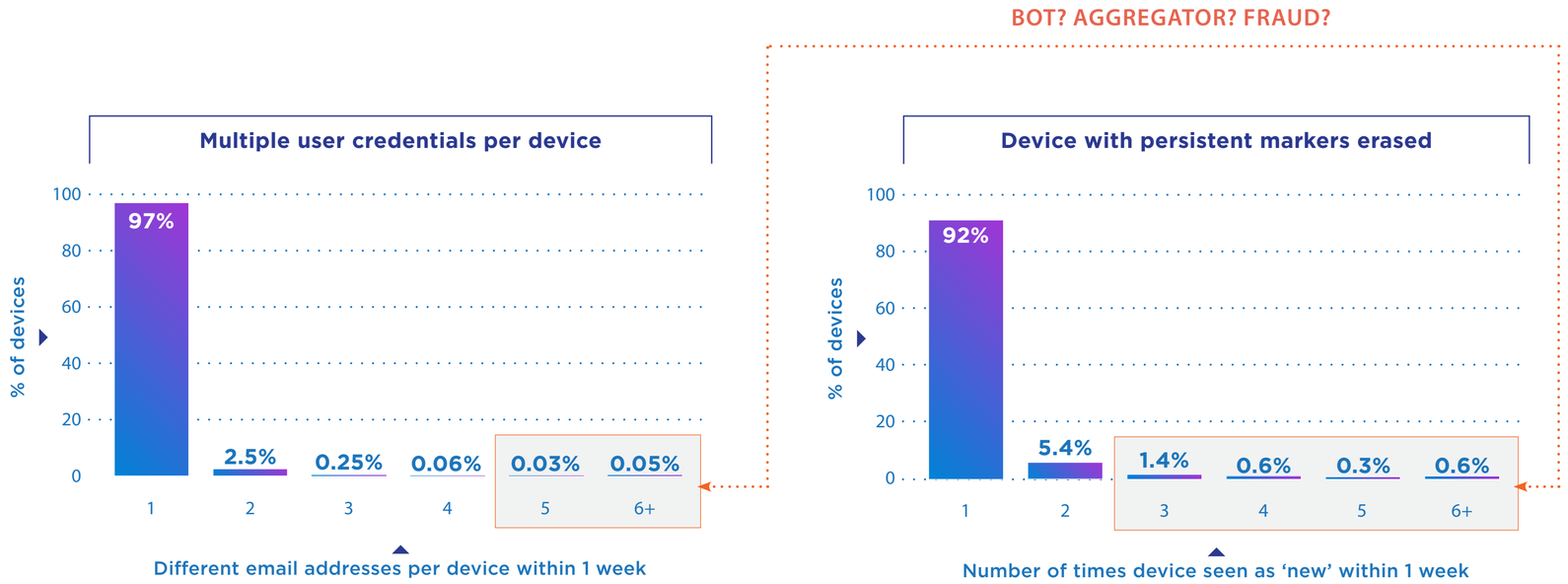
Attack Vectors by Continent



- With 4 billion user identities compromised since 2013, spoofing or impersonation attacks are growing across the globe. Identity spoofing continues to be the biggest attack vector in regions where organized identity verification tools are not as prevalent.
- Identity spoofing is the biggest attack vector in emerging markets such as Africa, Asia and South America.
- Global businesses need the ability to incorporate regional variances without impacting the online experience for legitimate users.

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

Device and Identity Spoofing



The ability to recognizing returning customers is critical to delivering a great user experience. It is crucial for companies to be able to leverage contextual data to differentiate a good returning user from a fraudster.

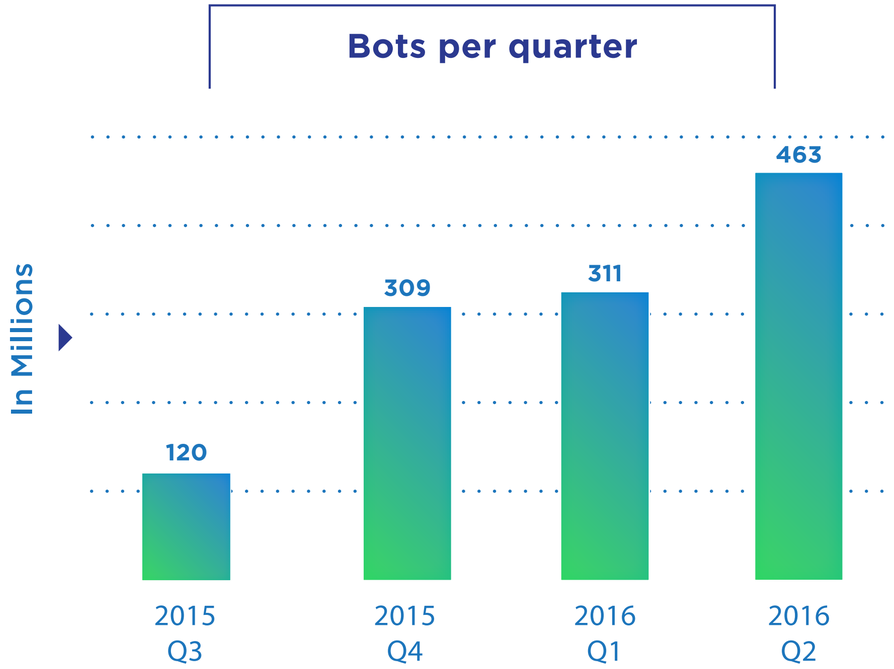
There are certain device anomalies that can help digital businesses identify high-risk transactions. Digital users tend to access multiple products and services from the same device but usually only have one or two sets of credentials associated with that device.

Fraudsters however often try to test multiple user credentials, such as email addresses, using a single device. Likewise good customers clear out the cache / cookies from time to time, but doing so frequently can be indicative of potential fraud.

Companies need to evaluate individual data points against user behavioral analytics to determine risk.

Q2
2016

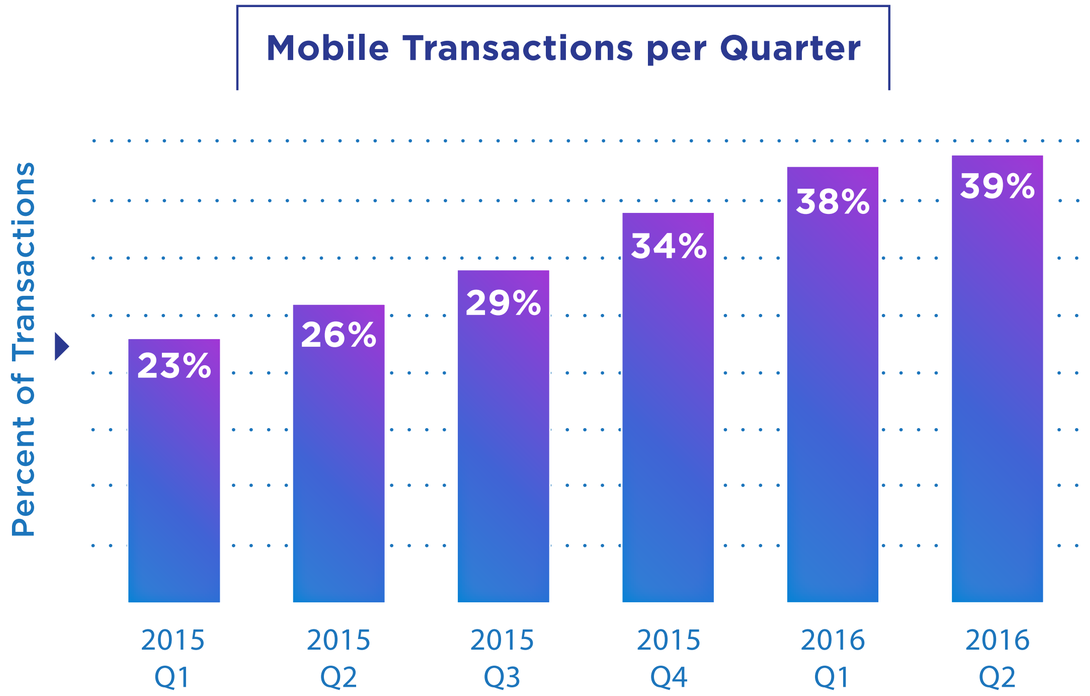
The Evolution of Bots Over Time



- The biggest risk facing digital businesses is the rise of bot armies designed to evade rate and security control measures and mimic trusted customer behavior / login patterns.
- Attack patterns and methods are constantly evolving: once attacks start getting detected / blocked, the fraudster controlling the bot army “tunes” the transaction list.
- The attack strategy varies from toning down the velocity to avoid controls, to launching distributed but grouped attacks to overload a server’s processing capability. Sometimes, fraudsters knowingly sneak in good transactions to trick the system.

Mobile

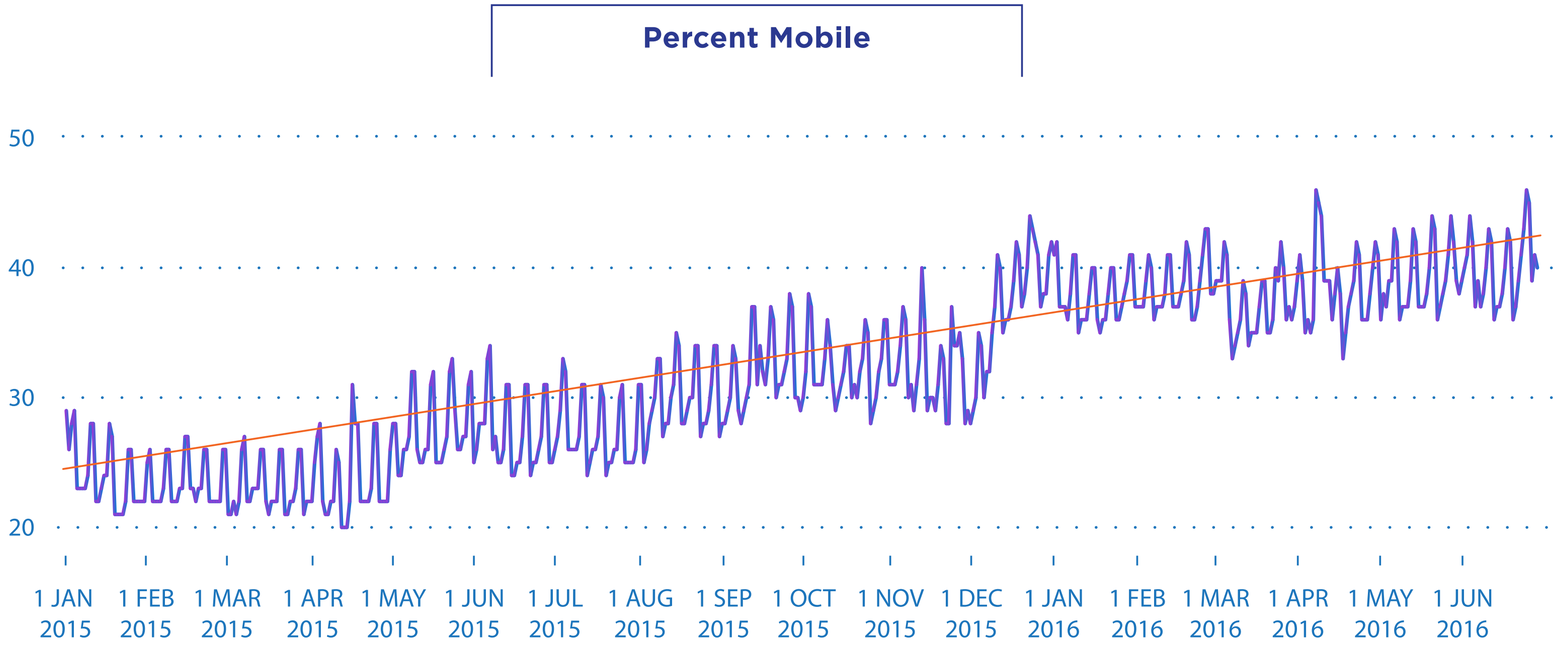
Growth of Mobile Transactions



- Mobile transactions grew 200% compared to the previous year, primarily driven by the increase in account logins using mobile devices.
- The use of mobile to sign-up for or login to online accounts, or pay for goods and services, continues to grow for all industries and is a leading use case.
- The growth in mobile has also resulted in a continued rise in attacks using stolen identities and compromised devices, making application integrity, device security and identity verification far harder to control.

Q2
2016

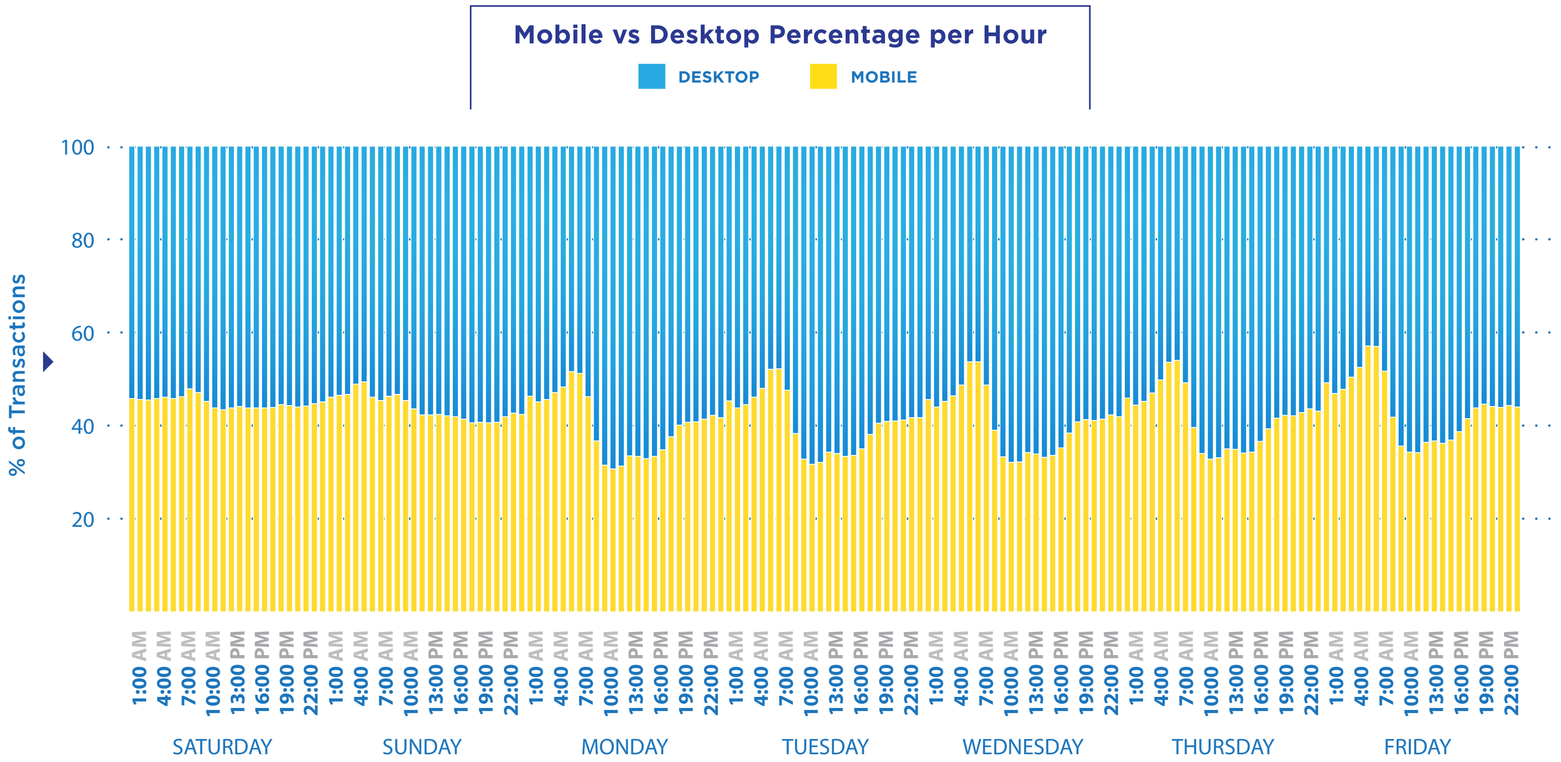
Percent Mobile Transactions per Day



The ThreatMetrix Digital Identity Network, coupled with powerful real-time decision analytics, allows the vast majority of mobile transactions and authentication attempts to be verified in real time against trusted patterns of behavior without adding friction to users or placing addition burden on business processes.

Q2
2016

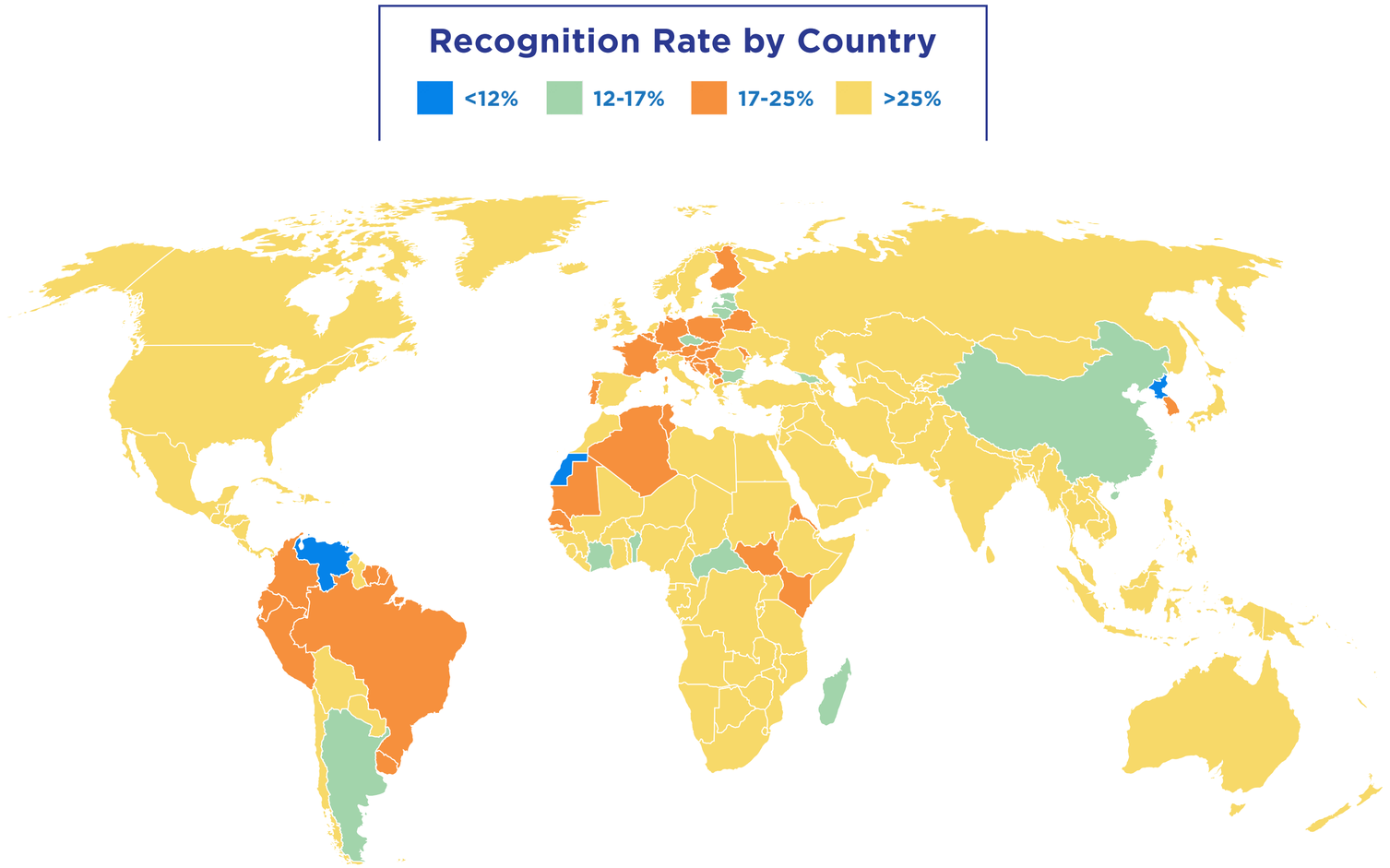
Hourly Mobile Usage



Mobile transactions highest outside working hours, rising in the evening and through the night.

Q2
2016

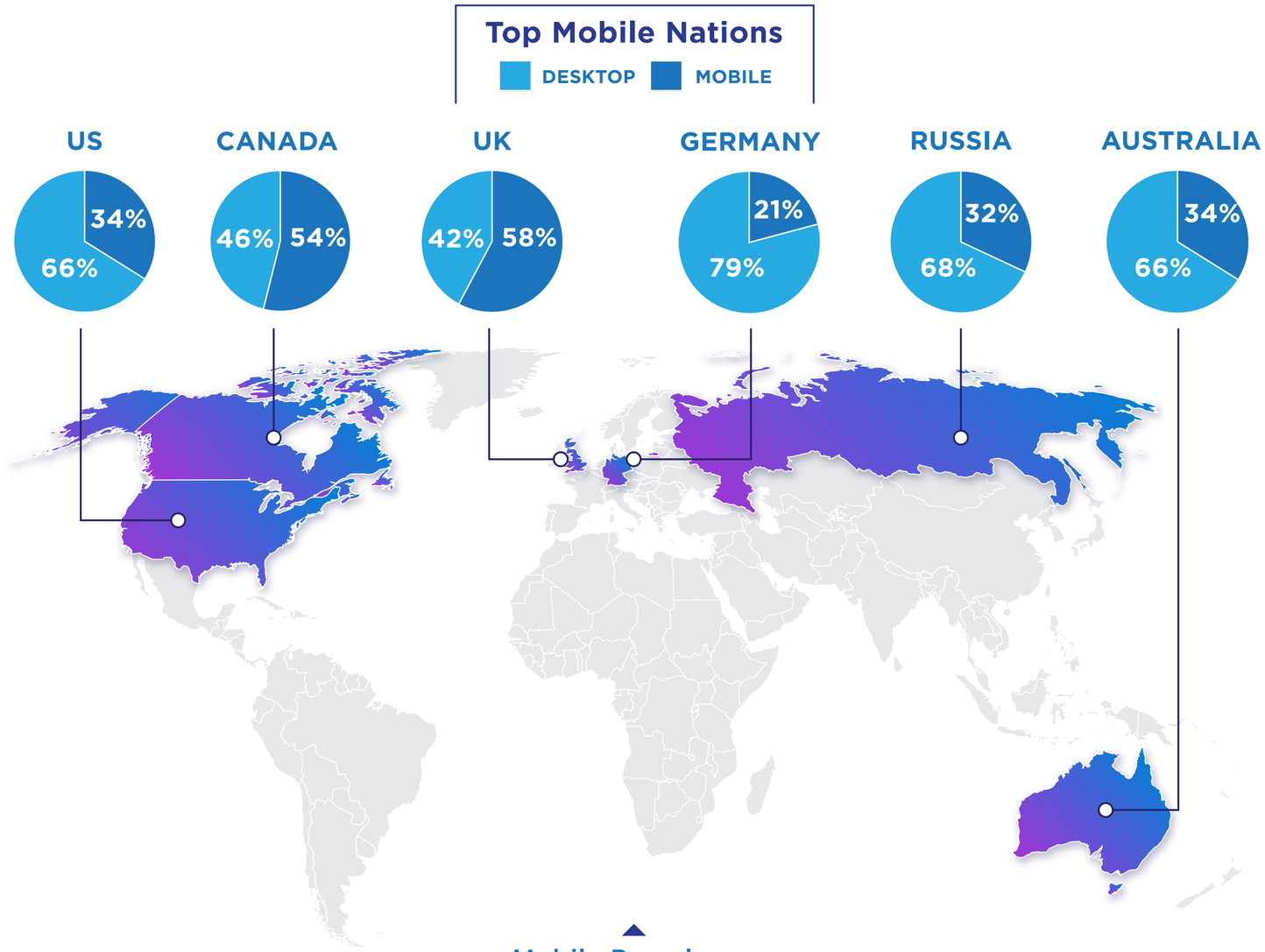
Mobile Transaction Prevalence



- The network analyzes mobile transactions from over 200 countries and territories across the globe.
- With each quarter, mobile transactions are growing across developed and emerging economies. Mobile-only users are also growing.

Q2
2016

Top Mobile Nations

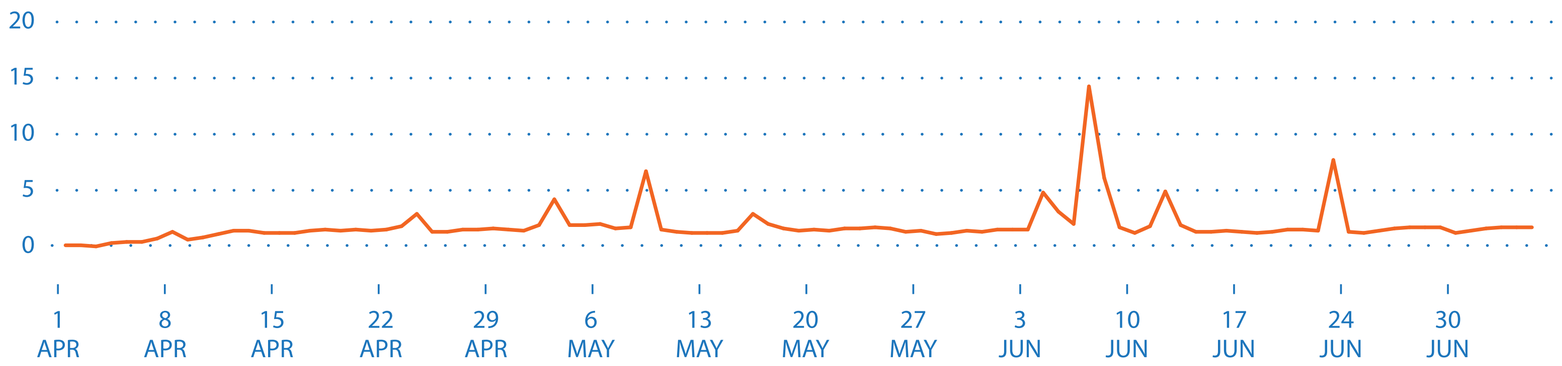


Mobile Prevalence

Q2
2016

Bots Cross Over to Mobile

Daily Percentage of Mobile App Transactions Coming From Bots and Scripted Attacks*



With the continuing trend away from online to mobile transactions, cybercriminals are following suit.

ThreatMetrix has been tracking the rise in online bot attacks for several quarters, and has now identified the emergence of sophisticated bot attacks on the mobile app channel.

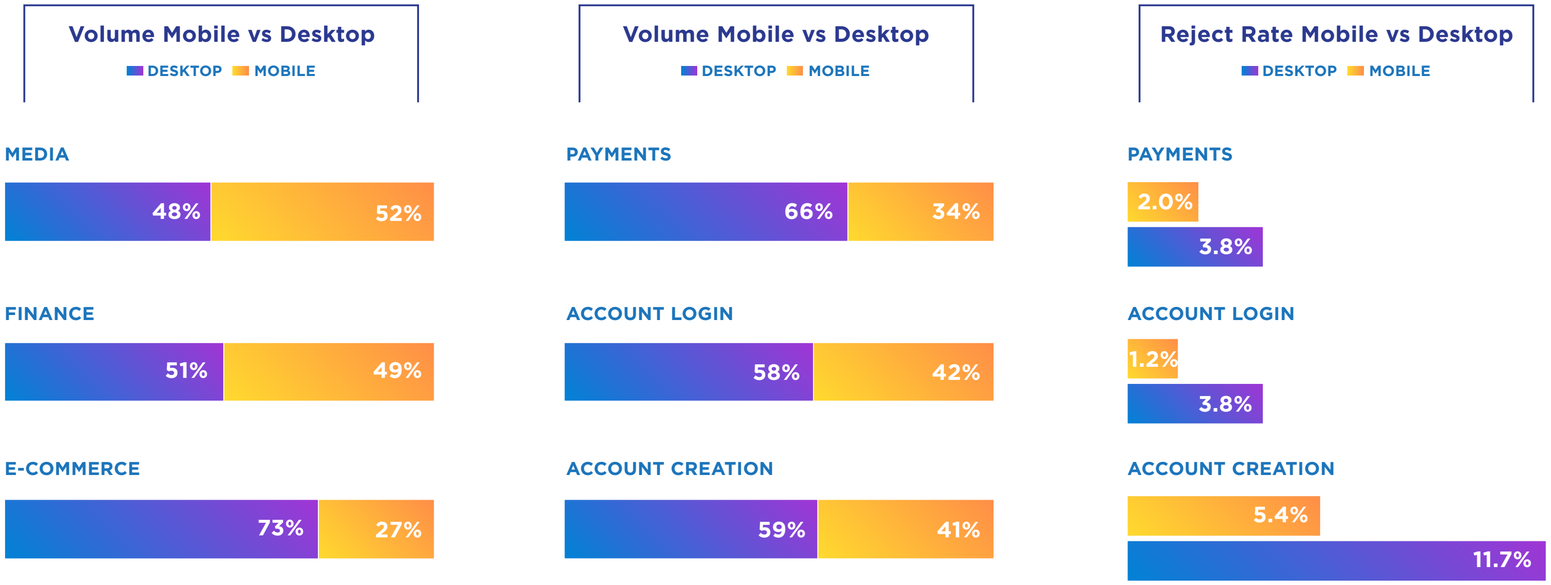
Cybercriminals are reverse engineering mobile apps, in order to then be able to emulate requests sent by the app to the online retailer or bank.

At first glance, these events appear to be genuine app traffic, but a closer look reveals anomalies indicating bot traffic attempting to access customer accounts.

**Data for a leading retailer*

Q2
2016

Mobile Versus Desktop Transactions and Attacks



Mobile-based commerce represented 39% of the total transactions analyzed. This represents a 160% year-on-year growth in transactions originating from mobile devices.

The biggest growth is coming from financial institutions whose share of mobile has grown from 20% the previous year to 49% in Q2 2016, driven by user adoption as well as deployment of digital banking solutions.

Mobile is fast becoming the leading way for consumers to access payments and commerce. Logins using mobile devices grew almost 250% compared to the previous year.

Account creation attacks targeting mobile devices are increasingly driven by the prevalence of stolen identities and tools to enable device cloaking / spoofing.

Q2
2016

Mobile Transaction and Attack Trends

This diverse landscape of mobile attacks provides cybercriminals with the opportunity to inflict huge damage to business reputation, customer trust and long term revenue.

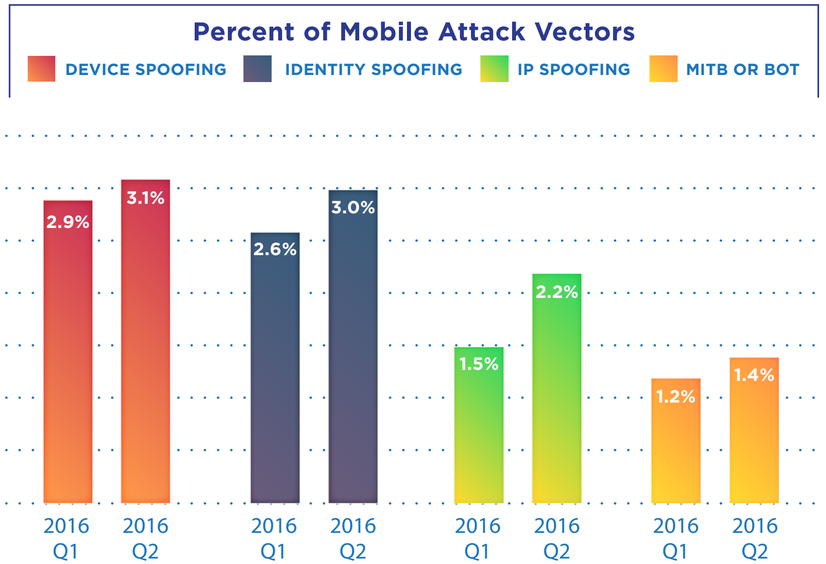
To compound the risk, mobile app delivery teams rarely have the full spectrum of specialized skills required to address all attack vectors and continuously monitor the threat environment to identify and mitigate new and emerging threats.

Mobile apps are vulnerable, in part, because they exist outside the security perimeter of the online business. They provide fraudsters with direct access to elements of the merchant's business process, which makes the business vulnerable to a wide variety of attacks, from OS level malware in the host device to malicious / pirated 3rd party apps that can be leveraged to steal sensitive personal credentials.

Businesses must adopt a robust approach to securing mobile transactions and native apps; maintaining privacy and confidentiality without marring the user experience with friction.

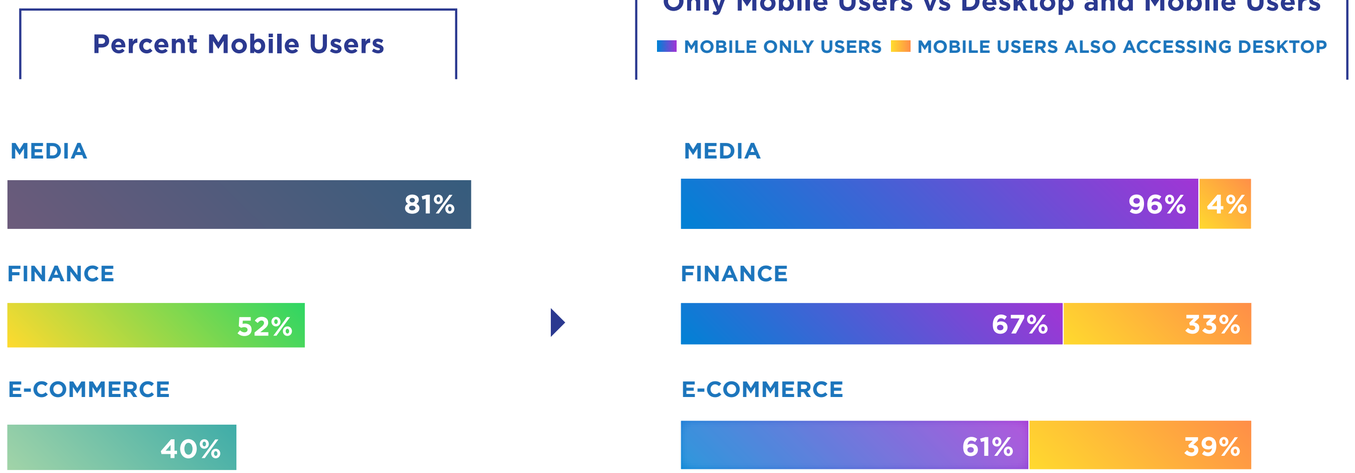
The emergence of mobile bot attacks shows how fraudsters are evolving their attack vectors to capitalize on the growth of mobile.

Device spoofing and identity spoofing are the most prevalent attack vectors in the Network as fraudsters attempt to dupe businesses into believing their transaction comes from a trusted device / user.



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

Cross-device Usage



- Cross-device usage continues to grow: more users accessed their bank account, made payments, streamed content and signed up for new accounts using connected devices.
- Mobile-only users are growing across industries, highlighting the fact that digital transformation strategies are paying off.
- As consumers move seamlessly between screens on connected devices, they expect their experience to be consistent and frictionless. This requires a holistic recognition of trusted returning users that looks beyond just devices. Businesses need to evolve from a "mobile-first" approach to a "digital-first" approach.
- Some e-commerce companies, particularly in event / travel ticketing where last-minute / time sensitive purchases are common, see very high volumes of mobile transactions. It is particularly critical that these markets authenticate users in real time to avoid frustrating transaction abandonment.

Conclusion

Conclusions

One of the key themes to emerge from this quarter's report, is the complex interconnectivity of the online world. This is seen between online personas, devices, locations, platforms and transactions. The digital landscape is intricately connected, with users transacting in unique and unpredictable ways.

Individual user personas must be analyzed in the context of every piece of information available about the way that user transacts online. Analyzing, for example, individual device behavior, or mobile behavior belies the complexity of how users transact across devices and platforms.

ThreatMetrix Digital Identities allow our customers to really analyze the myriad connections between devices, locations and anonymized personal information and online behaviors to get a clear and unique view of risk.

The complexity of building accurate Digital Identities must feed into any fraud models if businesses are to effectively and accurately predict and detect fraud patterns of the future. The behavior of online users, and the ingenuity of fraudsters continues to evolve quicker than the best machines.

Behavioral analytics must be able to detect unusual or high-risk changes in user behavior that do not inhibit the user from transacting freely but also protect them from potential fraud.

Likewise, machine learning models are only as good as the data they receive. The ThreatMetrix Smart Learning solution combines dynamic and real time global intelligence from the ThreatMetrix Digital Identity Network with customer truth data to produce a more accurate machine learning model that can be highly predictive of fraud.

Online authentication continues to be a key use case globally and this must evolve to become bespoke to each user, targeting the right type of authentication based on who the user is, what hardware platform they are using, what system / resource / application they are trying to access, and the level of risk associated with what they are trying to do.

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.

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

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

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.

Q2
2016

Contact

AMERICAS

SAN JOSE

160 W Santa Clara St
Suite 1400
San Jose, CA, 95113

Telephone: +1 408 200 5755
Fax: +1 408 200 5799

NEW YORK

5 Penn Plaza, 23rd Floor
Suite 1400
New York, NY 10001

Telephone: +1 212 896 3987

NORTH / SOUTH AMERICA

Telephone: +1 408 200 5700

SALES

Email: sales@threatmetrix.com

SUPPORT

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

PARTNERS

Email: partners@threatmetrix.com

INTERNATIONAL

NETHERLANDS

The Base | 3/F, Tower C
Evert van Beekstraat 1-79
1118 CL Schiphol
Netherlands

Telephone: +31 (0)20 800 0638

LONDON

Golden Cross House
8 Duncannon Street
London, WC2N 4JF, United Kingdom

Telephone: +44 (0) 207 484 5120

FRANCE

Tour EGEE
9/11 Allee de l'Arche
92671 Courbevoie Cedex
France

Telephone: +33 1 49 97 15 62

EUROPE/MIDDLE EAST/AFRICA

Telephone: +31 (0)70 8200 509

SYDNEY

Suite 1202, Level 12, Tower B
799 Pacific Highway
Chatswood, 2067 Australia

Telephone: +61 2 9411 4499

AUSTRALIA/NEW ZEALAND

Telephone: +61 (0) 2 8073 4215

HONG KONG

Telephone: +852 36698341