



LEXISNEXIS® RISK SOLUTIONS CYBERCRIME REPORT

Global Insights from the LexisNexis® Digital Identity Network®

July-December 2018

Contents

- Foreword
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends
- Conclusion

3
Foreword

4
Overview

9
Transactions & Attacks

26
Regional Trends

33
Evolving Mobile Trends

42
Conclusion

Foreword

News has recently emerged of the first machine learning generated fingerprints. According to Wired.com, a group of computer scientists from New York University’s engineering department has managed to generate a series of “master prints” that not only pass smartphone fingerprint sensors, but can actually masquerade as prints from multiple users. When evolving global regulations are mandating the use of a “foolproof” biometric suite of strong authentication, hackers are already cracking the codes that make them penetrable.

This calls into question the very meaning of strong authentication; is anything really impenetrable? How far should businesses rely on point solutions to protect customer accounts and authenticate online payments? It appears that the only reliable approach to smart authentication is a layered solution that combines real-time elements of a user’s unique behavioral pattern, with customer-focused, strong authentication that is inextricably linked to their online customer journey. Only then can businesses genuinely detect unusual or high-risk scenarios before they pose a risk to security defenses and customer accounts.

The swirling storm of privacy and security continues to loom heavy on the horizon for every digital business, with the first test cases from GDPR starting to make headlines and the California Privacy Act likely not far behind. Consumers should expect the businesses they transact with to protect their online accounts and personal information, but the line between security and data privacy continues to be tested in the process.



Alisdair Faulkner
Chief Identity Officer, LexisNexis® Risk Solutions

If 2018 began with businesses looking for new ways to better authenticate online users - particularly in Europe with the evolution of PSD2 mandating stronger authentication on login and payments transactions – what lengths will the fraudsters of 2019 go to circumvent this security framework? Networks, automation and the use of bots and machines seem central to virtually all the predictions for how cybercrime will evolve this year. Consider, for example:

- AI driven malicious chat bots / robots that can be used to dupe customers into divulging personal information
- Machine learning algorithms used to generate pitch-perfect, social engineering attacks based on real customer data
- IoT devices being taken over by external bots and used to spy on human interactions
- Networked global bot armies targeting multiple industries worldwide
- Networked fraud rings operating across industries – mules using financial services / telco / gaming and gambling companies to siphon money

It is clear that consumers do not expect to have to curtail their online transacting behavior in the quest to thwart cybercrime. Yes, awareness campaigns around social engineering and ransomware threats, for example, are pivotal and non-negotiable. But consumers do not expect fraud and identity controls to interfere with the slick and low-friction online experience they have come to expect from their bank, social media sites and trusted e-commerce brands. The pressure is on businesses to ensure they do not jeopardize customer trust in the process of catching the criminals.



Report Overview

[Foreword](#)[Overview](#)[Transactions & Attacks](#)[Regional Trends](#)[Evolving Mobile Trends](#)[Conclusion](#)

The LexisNexis® Risk Solutions Cybercrime Report is based on actual cybercrime attacks from July – December 2018 that were detected by the LexisNexis® Digital Identity Network® during real-time analysis and interdiction of fraudulent online payments, logins and new account applications.

- The Digital Identity Network provides visibility and insight into transaction patterns and emerging cybercrime threats. LexisNexis Risk Solutions processed 17 billion transactions during the second half of 2018, with 61% originating from a mobile device.
- These transactions are analyzed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioral analytics.
- The Digital Identity Network and its real-time policy engine provide unique insight into users' digital identities, even as they move between applications, devices and networks.
- LexisNexis Risk Solutions customers benefit from a global view of risks, based on the attributes and rules that are custom-tuned specifically for their businesses.
- Attacks discussed are from “high-risk” transactions scored by LexisNexis Risk Solutions customers.



July-December 2018 in Numbers



- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends
- Conclusion

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

17 Billion

Transactions Processed

244 Million

Human-initiated Attacks

Including
103 Million

Mobile Attacks

2.8 Billion

Bot Attacks

61%

Transactions Come from Mobile

United States

Biggest Attacker

Key Highlights



-  Foreword
-  Overview
-  Transactions & Attacks
-  Regional Trends
-  Evolving Mobile Trends
-  Conclusion

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion



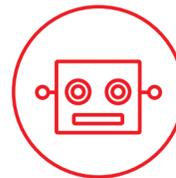
Mobile: Risk and Reward

- Mobile transaction volume and penetration continues to grow, with users favoring mobile for most use cases and in most global geographies.
- The main exception is for e-commerce logins, where the lure of a larger screen seems to account for the 69% in desktop transactions, despite the fact that new account creations and payments are predominantly mobile.



The Network Effect of Fraud

- LexisNexis® Risk Solutions now sees a strong networked pattern of fraud, with the same cybercriminals working across different organizations in the same industry, as well as across different industries, illustrating the global and ever-more connected nature of online fraud. This cross organizational fraud is particularly strong within banking, gaming and gambling, lending and retail.



E-commerce Under Pressure from Bot Volume

- Although sophisticated attacks in e-commerce have actually dropped during this period, the pernicious and widespread impact of high volume automated bot traffic continues to disrupt the industry. The LexisNexis® Digital Identity Network® blocked 2.1 billion bot attacks on e-commerce merchants, a 142% growth compared to the same period last year.
- These identity testing bot attacks can often make up considerably more of an e-commerce merchant's daily transaction volume than good traffic, making a low-friction online experience for trusted customers all the more challenging for merchants to provide.



Financial Services Experience New Risk from Mobile Threats

- In some regions, fraudsters are shifting focus from desktop to mobile attacks. While mobile attacks still make up less than half the attack volume seen in the Digital Identity Network, financial services is experiencing a growth in attacks, particularly in Brazil, U.S., Canada and Italy. Complex mobile attack vectors such as remote access attacks are also appearing.
- The most noticeable growth in mobile attacks is on account logins, as fraudsters attempt to infiltrate user accounts by brute force (using mobile bots) or stealth (using mobile remote access attacks). This contributes to the 107% growth in mobile account takeovers in comparison to the first half of 2018, despite the fact that overall attack rates are low.



Media is Test Bed for Stolen Identity Credentials

- Media still sees the highest penetration of new account creation attacks of all industries. Fraudsters likely see media companies, with their lower barriers to entry, as ideal test beds for stolen credentials. Approximately one in every six new account creation transactions is fraudulent.

The LexisNexis® Risk Solutions Identity Abuse Index



Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

The LexisNexis Risk Solutions Identity Abuse Index shows the percentage of attacks per day across the entire LexisNexis® Digital Identity Network®, mapping the peaks and troughs in attack patterns over the last four years. This provides a clear indicator of the impact large data breaches have on global cybercrime, with the most significant spikes in attacks often coinciding with big data breaches reported in the news. At times, breached identity data may manifest in increased attacks on the

Digital Identity Network before a breach has even been discovered or reported, indicating that fraudsters see the time immediately after a breach as the most lucrative period for launching an attack.

Although 2018 has been less volatile than 2017 overall, the Digital Identity Network has experienced a high volume of global bot attacks originating from diverse and emerging economies, indicating the huge dispersal of breached identity data to all corners of the globe, with

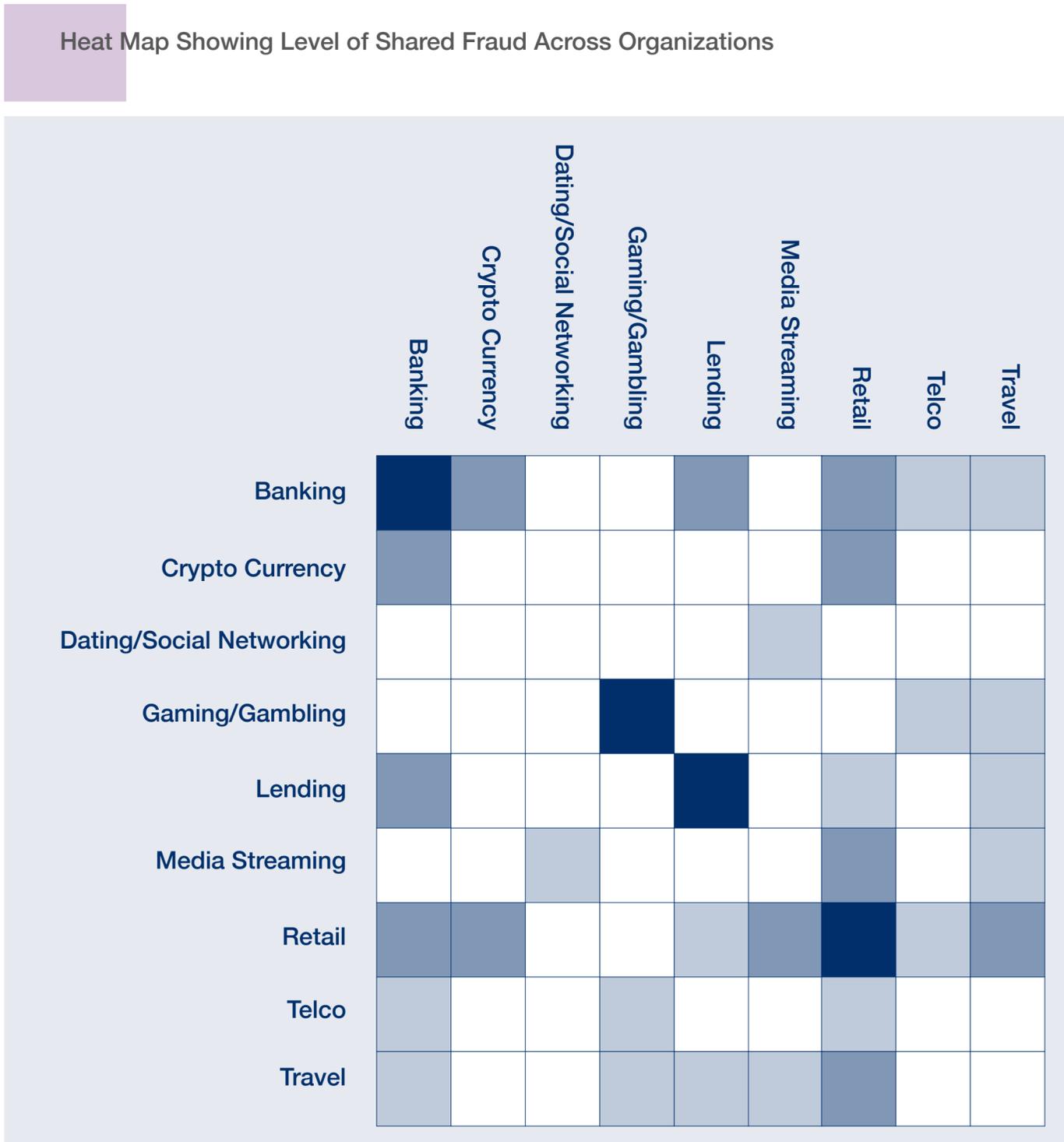
smaller peaks in attacks often representing attacks from new geographies.

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 shows that the exploitation of stolen identity information is automated, disseminating to countries across the globe in an organized and comprehensive way.



The Growing Threat of Networked Cybercrime



The LexisNexis® Digital Identity Network® is seeing a strong footprint of cross-organizational and cross-industry fraud.

This is seen when digital identities have been associated with confirmed fraud attempts by more than one organization within the Digital Identity Network.

The strongest correlation of fraud, (as shown by the darkest colors in the heat map opposite), is for organizations within the same industry, particularly banking, gaming/gambling, lending and retail. However, some strong patterns of shared fraud within different industry groups, such as between banking / cryptocurrency and media streaming / retail, have emerged.

Examples of cross-organizational attack patterns that are encountered in the Digital Identity Network include:

- The same bot targeting multiple organizations, often outside the country where the bot originated.
- Mule accounts linked in networks that span multiple banks in the Digital Identity Network.

This global nature of cybercrime illustrates the value of using a global network of pseudo-anonymized digital identity intelligence to protect global organizations.

- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends
- Conclusion

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion



- Home
- Overview
- Transactions & Attacks**
- Regional Trends
- Evolving Mobile Trends
- Conclusion

Transactions Analyzed by Type

LexisNexis® Risk Solutions transactions span the full spectrum of global industries, from e-commerce, financial services and media to gaming and gambling, insurance, telco and government. LexisNexis Risk Solutions protects transactions across the entire customer journey, from verifying new account applications to streamlining logins, verifying password resets / change of details and authenticating payments.

Logins remain the least attacked transaction type overall, highlighting the fact that businesses are able to build trusted profiles of returning users as they interact regularly online. Globally, account takeover attacks have fallen 48% compared to the first half of 2018, although the picture in financial services is markedly different. Financial services institutions have seen a 37% growth in account takeover attacks since the first half of 2018, and for mobile-only transactions, this rises to 107%.

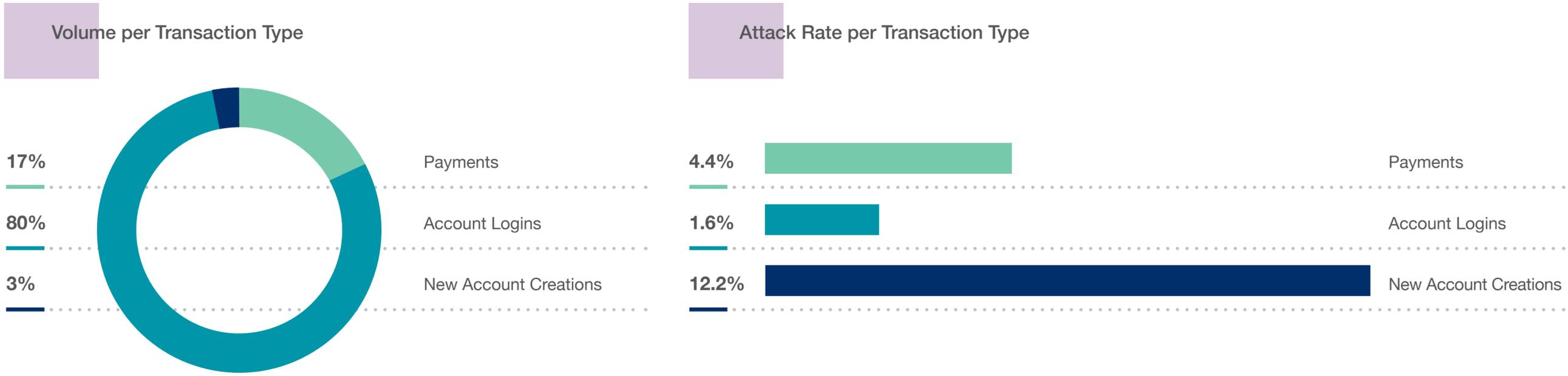
These attacks present a significant risk to customer accounts, where a successful account takeover can lead to the loss of entire account and savings balances.

New account creations, however, still have the highest attack rate of all the use cases analyzed by the LexisNexis® Digital Identity Network®. This is generally an opportunity for cybercriminals to use stolen identity credentials harvested from data breaches to open fraudulent new accounts to perpetrate further criminal activity, such as applying for loans, insurance policies or monetization of stolen credit cards. Around 1 in 8 new account creations in the Digital Identity Network is rejected as fraudulent, highlighting the widespread impact of stolen identity data across geographies and industries. New account creation attacks are growing in financial services and media, as fraudsters potentially see financial services as the more lucrative of the two targets,

while media represents a test-bed for stolen identity credentials.

The Digital Identity Network continues to see significantly more mobile transactions than desktop, with more than 6 in every 10 transactions coming from a mobile device. However, in some industries – particularly financial services - mobile attacks are also increasing, despite the fact that mobile generally remains a safer way to transact than desktop, particularly when a mobile app is being used. This could herald a potential shift in focus for cybercriminals, directing their attention to the opportunity that this volume shift to mobile represents.

The Digital Identity Network recorded 244 million attacks in the second half of 2018, along with 3 billion bot attacks. Although this is a drop in the percentage of human-initiated attacks, bot volume continues to grow as automated, networked attack patterns continue to have a huge impact on digital businesses globally.



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



E-commerce Transactions and Attacks

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

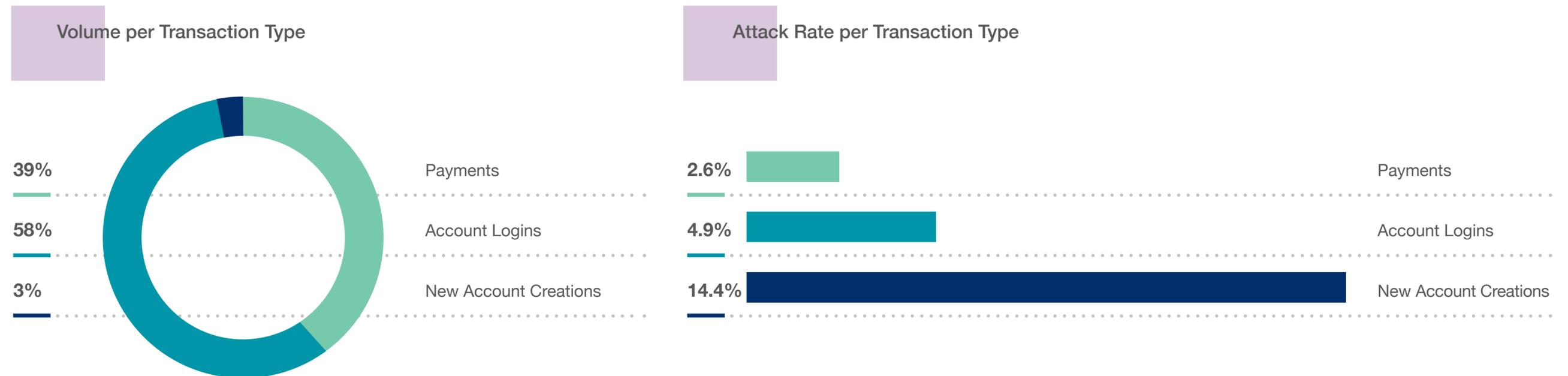
The spread of e-commerce transactions is much more balanced between logins and payments than in financial services, where users are logging into their bank accounts far more frequently via a mobile device, accounting for a higher percentage of logins overall. Account logins in e-commerce are much more desktop based – 69% of logins are via a desktop, compared to 41% of new account creations and 44% of payments - indicating how consumers still prefer to browse goods and services on a larger screen, even if they are happy to open new accounts or make payments via mobile.

Despite an overall drop in human-initiated e-commerce attacks throughout the customer journey, the industry continues to experience a high rate of new account creation attacks, with 1 in every 7 transactions rejected as fraudulent. Likewise, e-commerce account takeovers are seen as an easier target than many other industries, with an attack rate of 4.9%.

However, the broader e-commerce story is one of heightened risk from automated bot attacks, with the industry experiencing 2.1 billion bot attacks in the second half of 2018 which, although

consistent with the first half of 2018, is a significant growth in volume year-on-year of 142%.

One of the key challenges for e-commerce merchants, particularly during busy holiday shopping days such as Black Friday and Cyber Monday, is balancing optimized customer experience and low-friction authentication, while also maintaining effective fraud control. At times this might mean accepting a higher percentage of fraud to accept more genuine orders from good customers.



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



E-commerce Trends by Region

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

North America

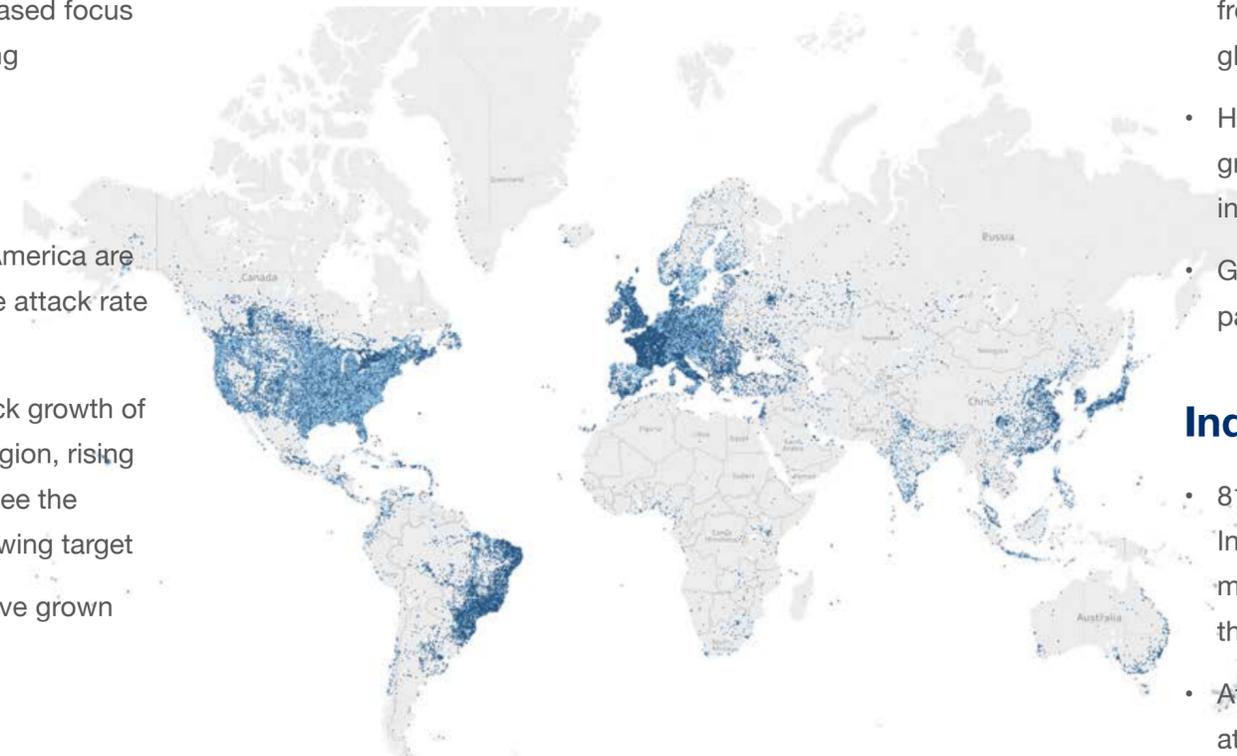
- New account creation transactions from North America are attacked slightly less than the global average at 11%
- Payments transactions from Canada are experiencing a year-on-year growth in attacks - 87% overall and 164% for mobile transactions - indicating a potential increased focus given that payments attacks globally are declining

South America

- New account creation transactions from South America are attacked at a very high rate of 33%, although the attack rate is showing signs of falling in the last six months
- During the same period there was a modest attack growth of 3% on mobile payments transactions from the region, rising to 11% in Brazil, indicating how fraudsters may see the emerging mobile market in e-commerce as a growing target
- Percentage of payments from mobile devices have grown 12% in the region in the last six months alone

EMEA

- New account creation transactions in EMEA are attacked at a slightly higher rate than the global average, at 16.4%. However, this attack rate has actually fallen 19% in the last year



ANZ

- All e-commerce transactions from ANZ see a very low overall attack rate, with just a 5% attack rate on new account creations in comparison to 14% globally
- Likewise, the risk has been decreasing year-on-year, with attack rates falling across all use cases

Asia

- New account creations from SE Asia record a very high attack rate of 41%, with a modest growth rate of 6% year-on-year
- 66% of all payments transactions in the region come from a mobile device, a higher proportion than the global average of 56%
- However, mobile payments are also experiencing a growth in attack rate of 17% year-on-year and 92% in the last six months alone
- Greater China is seeing a similar growth in mobile payments attacks of 54% year-on-year

India

- 81% of all new account creation transactions from India originate from a mobile device, indicating how mobile is driving the growth of digital commerce in the region. This compares to a global average of 59%
- At the same time, new account creations are attacked slightly less than the global average, and the attack rate has dropped in the last six months
- However, payments transactions are subsequently much more vulnerable and attacked at an extremely high rate of 36%, a growth of 153% in the last six months alone

The Rise of Global Bot Attacks Targeting E-commerce



Foreword



Overview



Transactions & Attacks



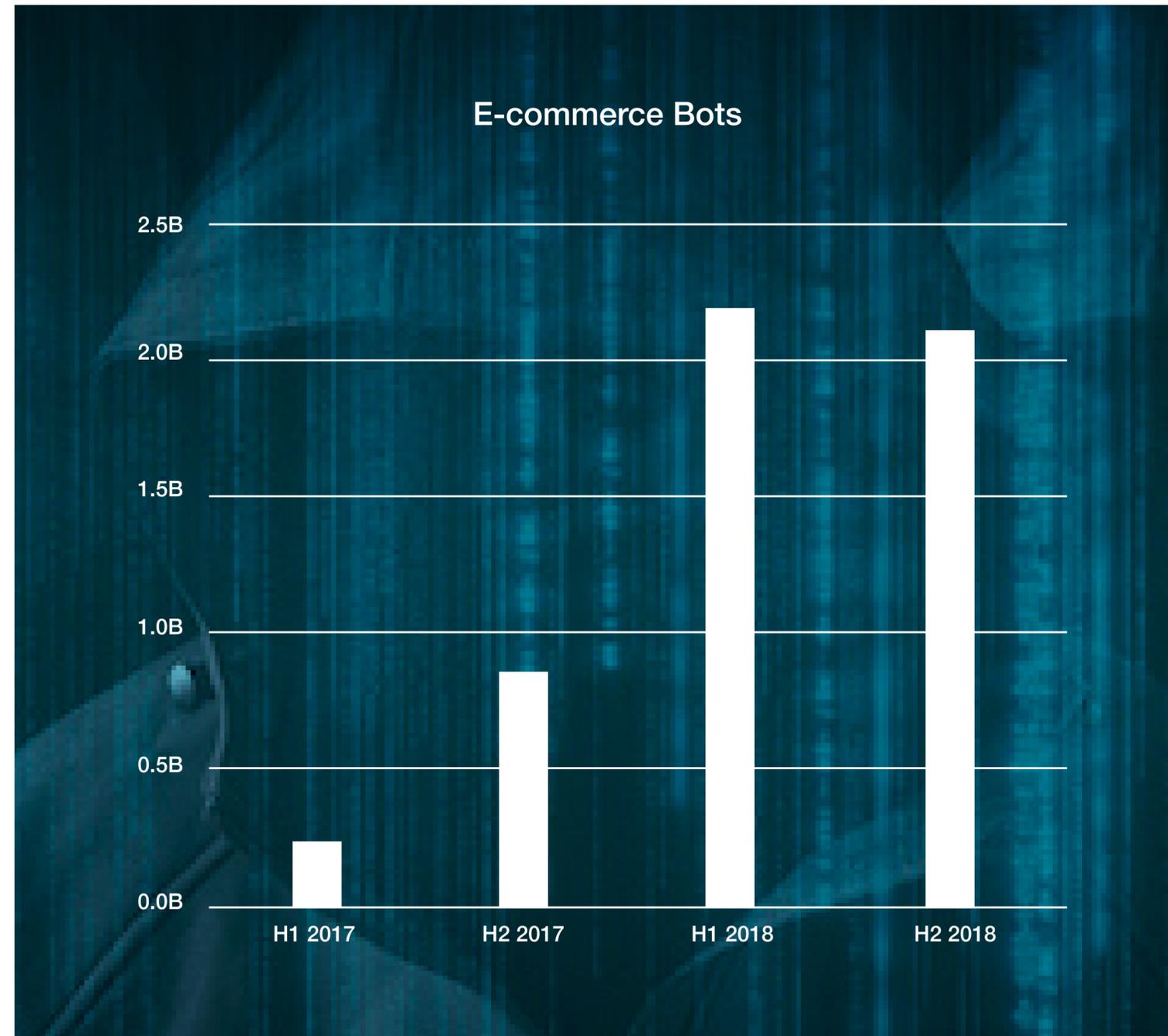
Regional Trends



Evolving Mobile Trends



Conclusion



E-commerce is the key global target for automated bot traffic, with much of it from dispersed global geographies. Top bot originators during the second half of 2018 include Malaysia, Indonesia, Vietnam, Japan, South Korea, Russia, India and Brazil, as well as the U.S.

These are differentiated from the more sophisticated, human-initiated attacks by their high-volume, automated approach that attempts to validate vast lists of stolen identity credentials to use in fraudulent new account creations and account takeover attacks.

Although rate control measures traditionally block the high-velocity attacks, bot controllers are also showing an enhanced level of sophistication with low and slow attacks that mimic legitimate customer behavior to slip just beneath the velocity radar, making them harder to detect. They may also slip in known good credentials to reduce the likelihood of detection.

The risk from automated bot attacks appears to be growing year-on-year, perhaps indicating the fact that cybercrime is developing into an industry in its own right, serving smaller growth economies with stolen identity credentials and the tactics for how best to monetize them.

A successful e-commerce account takeover can yield not only sensitive personal data but also potential access to cards saved on file that can be used for fraudulent, high-value purchases.

European E-commerce Merchant Targeted by Cross-Border Fraud



Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion



This European e-commerce merchant was targeted by a Chinese fraudster attempting to monetize a number of stolen French credit cards.

The fraudster adopted a number of techniques to try and avoid detection, including:

- Using multiple email addresses
- Using multiple devices
- Keeping transaction amounts below \$200
- Using a proxy in the U.S. to disguise true location

LexID® Digital visualizations help to link together this fraudulent behavior, tying the multiple credit cards, email addresses and devices to one account, helping the merchant detect and block this high-risk behavior.



Growth in Online Transaction Volume: Thanksgiving and Christmas

Foreword

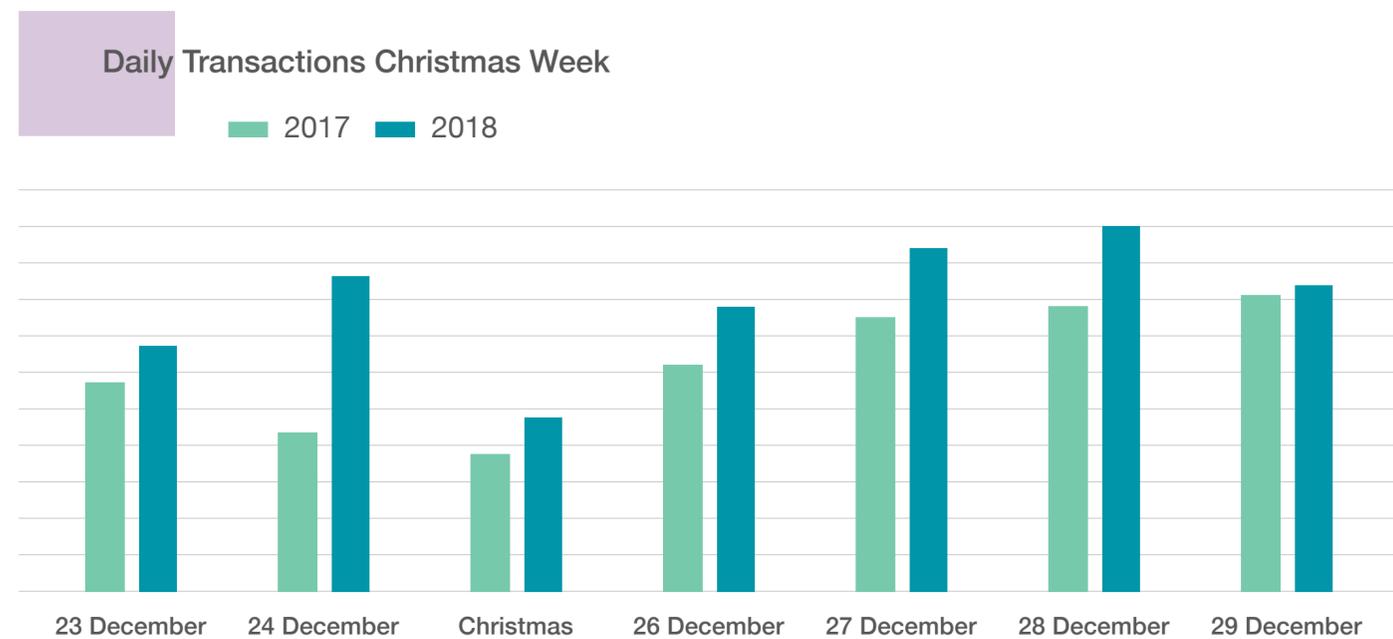
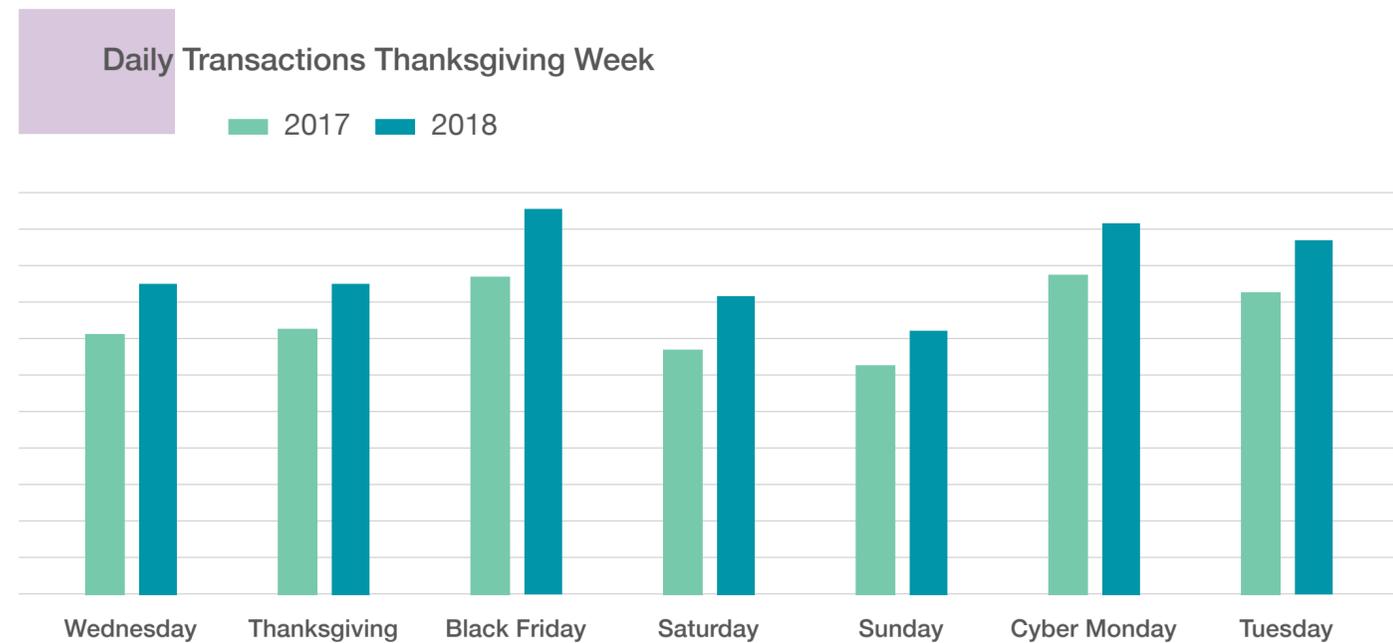
Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion



A group of top retailers in the LexisNexis® Digital Identity Network® saw a 20% growth in transaction volume in comparison to the Thanksgiving shopping week period in 2017. This indicates that holiday shopping continues to migrate from in-store to online as consumers enjoy the flexibility and ease of ordering goods and services from digital devices.

- On Black Friday, transaction volume grew 23% year-on-year
- Payments transactions specifically grew 20%
- In addition, the Digital Identity Network saw a growth in percentage of mobile payments transactions from 52% in 2017, to 59% in 2018, suggesting that consumers are shopping using the convenience of a mobile device, perhaps while on the move or while visiting friends and relatives

Likewise, the Christmas shopping week saw a similar growth in transaction volume, with the biggest growth hitting on 24th December at 61%, followed by 28th December at 30%. The growth on Christmas Eve may be in part down to the fact that in 2017 it fell on a Sunday, whereas 2018 was a Monday, meaning consumers got in an extra full day of shopping instead of stopping for Christmas at the weekend.

Holiday Shopping Attack Patterns



Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

Automated bot attacks were the key attack vector that the LexisNexis® Digital Identity Network® experienced during the Thanksgiving shopping week.

Key fraud typologies included the following:

- A payments platform saw a high volume of bot attacks using session replay during the holiday shopping period, indicating how fraudsters are potentially capitalizing on the higher than average transaction volumes to try and overwhelm organizations with high volume automated traffic. These bot attacks originated in the U.S. and Vietnam and were likely testing stolen credit card credentials, potentially to use in further targeted fraud attacks during the holiday shopping period.
- Another organization experienced a large bot attack targeting logins, testing 20 million stolen account credentials, beginning on Cyber Monday and continuing throughout the week. These bots originated in the U.S., Vietnam and China.
- The Digital identity Network also saw an increase in attacks on new loan applications for one financial institution, which saw the attack rate rise from 13% to 60% on Black Friday.

As expected, average basket values across digital retail traffic was significantly higher than normal on key holiday shopping days. This was also true for fraudulent transactions.

Average basket value good transactions: 95 USD

Average basket value rejected transactions: 260 USD

Bot Attacks
Using Session Replay

20 million
Stolen Account Credentials

Attack Rate
Increased from 13% to 60%

Average Basket Values
Higher During Holiday Week

	Good Transactions		Rejected Transactions
--	-------------------	--	-----------------------



Financial Services Transactions and Attacks

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

Financial services organizations continue to walk the tightrope between maintaining robust security with a low friction, streamlined customer experience, while at the same time managing the sometimes competing demands of privacy and regulatory reform.

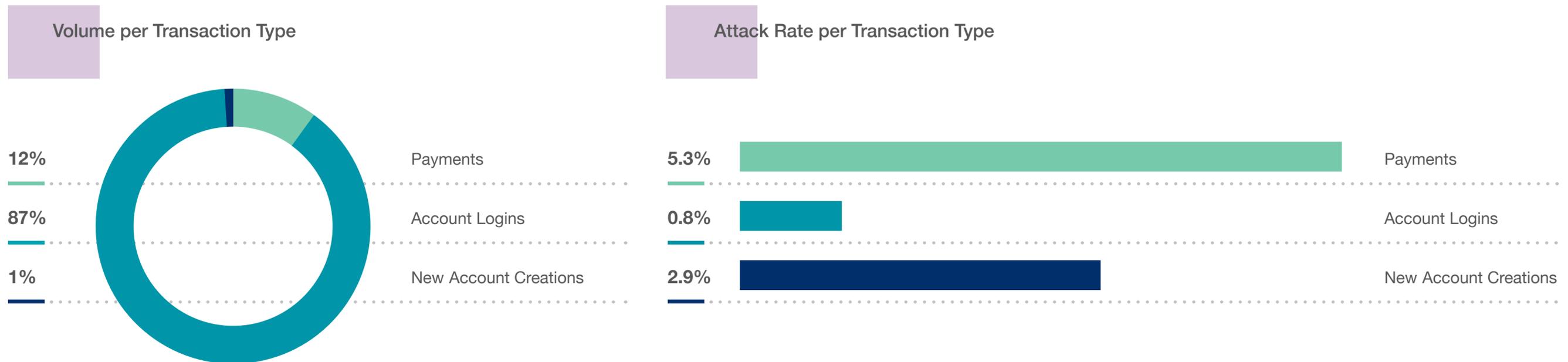
Customers are increasingly opting to bank online, with a preference for full service mobile banking apps over desktop sessions in many regions. The onus is on banks to ensure that integrated and low friction digital authentication capabilities form an inextricable part of the customer experience, in order to align security with the online experience customers expect.

This reality is reflected in the growth of financial services transactions; 67% of financial services transactions now come from a mobile device, a growth of 13% year-on-year, indicating a growing preference for mobile transacting over desktop.

While payments still experience the highest attack rate, the risk to payments transactions is actually decreasing 17% year-on-year, while the risk to new account creations appears to be growing; 35% in the last six months overall and 29% for mobile transactions. This potentially indicates the fact that cybercriminals see more opportunity in fraudulent new bank accounts that can be used to launder money or take out multiple loans / other products that can be used for financial gain.

However, the most marked growth in attack risk comes from account takeovers on the mobile channel, which have grown 107% in comparison to the first half of 2018 (compared to 37% for overall transactions) and 53% year-on-year (compared to a drop of 10% for overall transactions). This indicates a potential shift in focus as fraudsters target the volume shift to mobile, with account takeovers offering immediate access to customer balances and personal credentials.

In line with this, identity spoofing has grown 20% compared to the first half of 2018 in financial services. Sophisticated impersonation attempts are being used to predominantly try and take over existing accounts.



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

Financial Services Trends by Region



Foreword



Overview



Transactions & Attacks



Regional Trends



Evolving Mobile Trends



Conclusion

North America

- North America is experiencing strong growth in financial services attack rates: year-on-year they have grown 48%, but for mobile transactions this rises to 116%
- Consistent with global figures, the biggest growth in risk comes from account takeovers: overall attack rates have grown 81% year-on-year and 211% for mobile transactions
- Likewise, new account creation attacks are growing 23% and are attacked at a higher rate than the global average at 3.5%

South America

- South American financial services transactions are the most likely to be attacked, at 12.3% of the total volume, and 9.8% for mobile-only
- This indicates the region's vulnerability to financial services fraud, as online and mobile offerings continue to evolve
- The risk to mobile transactions in particular appears to be growing; financial services attacks have grown 38% overall, but mobile attacks have grown 51% year-on-year
- Although the LexisNexis® Digital Identity Network® sees a growth in attacks across all use cases, new account creations see the biggest growth, at 130% year-on-year

EMEA

- As a region, EMEA has seen a drop in financial services attacks, however, there are pockets of growth in some key countries, particularly France, Germany and Italy
- France currently has a high-attack rate on login transactions at 10%, a growth of 199% year-on-year, along with a modest growth in new account creation and payments attacks. Account logins from Russia have also been prone to attack during the second half of 2018
- Likewise, Germany has an attack rate of 14% for new account creations, a growth of 66% year-on-year
- Italy has seen a growth in new account creation (33%) and payments attacks (18%) year-on-year

ANZ

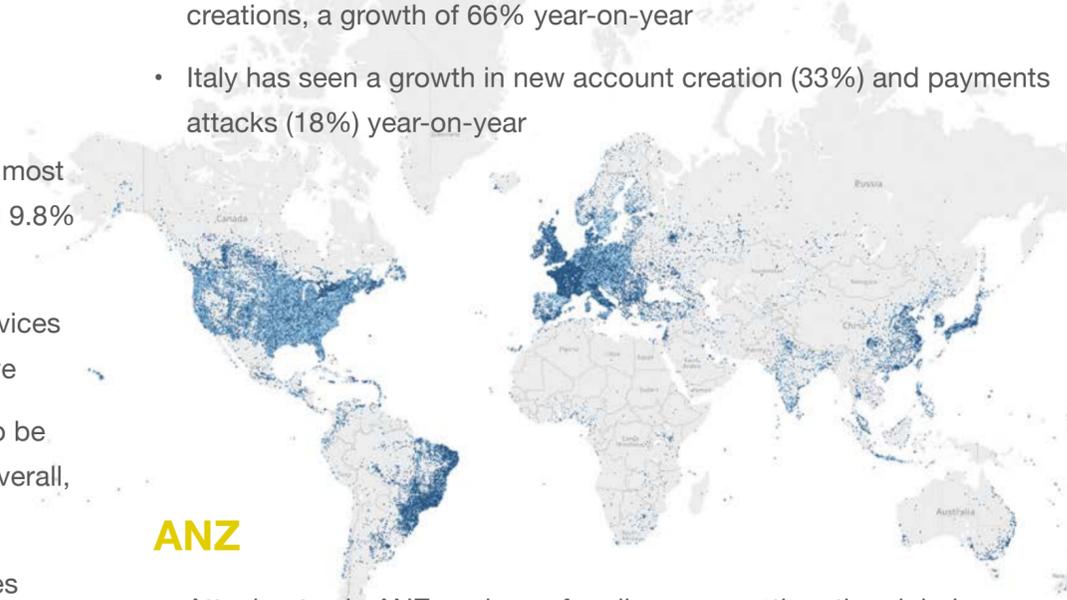
- Attack rates in ANZ are lower for all use cases than the global average for financial services, potentially indicating a reduced threat level for the region
- Despite this, the new account creations attack level has grown 19% in the last six months, suggesting that fraudsters are seeing the potential for identity-based attacks on the industry. In Australia specifically, this figure rises to 33%

Asia

- As a region, SE Asia has seen a drop in financial services attacks on logins and payments transactions in the last year, however, new account creation attacks have grown considerably. There was a 78% growth in attacks year-on-year overall, and 105% growth on mobile new account creation transactions, highlighting the influence of breached identity data on the region
- Japan specifically has seen strong growth in attacks on mobile logins in comparison to the first half of 2018
- These attempted account takeovers have grown 326% compared to the first half of 2018

India

- Almost one in every four new account creation transactions originating in India is an attack, the highest of any region globally, illustrating the widespread impact of stolen identity data on the region. This is a growth of 39% year-on-year
- Payments transactions in the region also have a very high attack rate of 16.2% although this has started to fall year-on-year indicating a potential shift to more complex / lucrative attacks



Uncovering New Predictors of Fraud in Financial Services



Mobile Tethering

Fraudsters often remain one step ahead of organizations in the race to defraud banks and good customers, looking for new and covert ways to slip beneath the radar of fraud detection.

The LexisNexis® Digital Identity Network® has identified that tethering a device to the internet via a mobile hotspot is a key fraud indicator in financial services:

Desktop transactions that are carried out with a mobile tether are 2.4 times more likely to be fraud than a transaction with a device connected via WiFi / fixed-line broadband.

The reasons for this are varied:

- Fraudsters know they are more traceable by law enforcement when they use a fixed-line broadband. Fraudsters running emulators and scripts are still predominantly doing so from a desktop, and a mobile hotspot protects such activity from being traced.
- Mobile tethering also gives flexibility of time and location, allowing fraudsters to be nearer their point of “cashing out”. For example, during an account takeover attempt they can physically locate themselves near a branch to extract account balances before being detected.





Growth of LexisNexis® Risk Solutions Strong ID in the LexisNexis® Digital Identity Network®

Foreword

As global regulations evolve, so too does the edict for a layered approach to authentication which incorporates risk-based and strong customer authentication (SCA) processes.

Registering a device, and then binding it with a user credential, enables a reliable and consistent verification of the transaction.

Although mobile is the more obvious channel for this authentication process, given that the majority of transactions are made on a mobile device, financial services organizations are also aware that there is still a sizable population who transact on desktop, and therefore the requirement for a LexisNexis Risk Solutions Strong ID for web solution is also imperative.

Overview

Transactions & Attacks

The onus is very much on businesses to deliver a strong customer authentication journey, whilst also maintaining low-friction and unnecessary disruption of a user's login or payments journey.

LexisNexis Risk Solutions Strong ID, (available for both Browser and Mobile App SDKs), provides a unique tamper resistant identifier that cryptographically binds a specific device to a user's identity, making the device an authentication factor for regulations requiring SCA.

Regional Trends

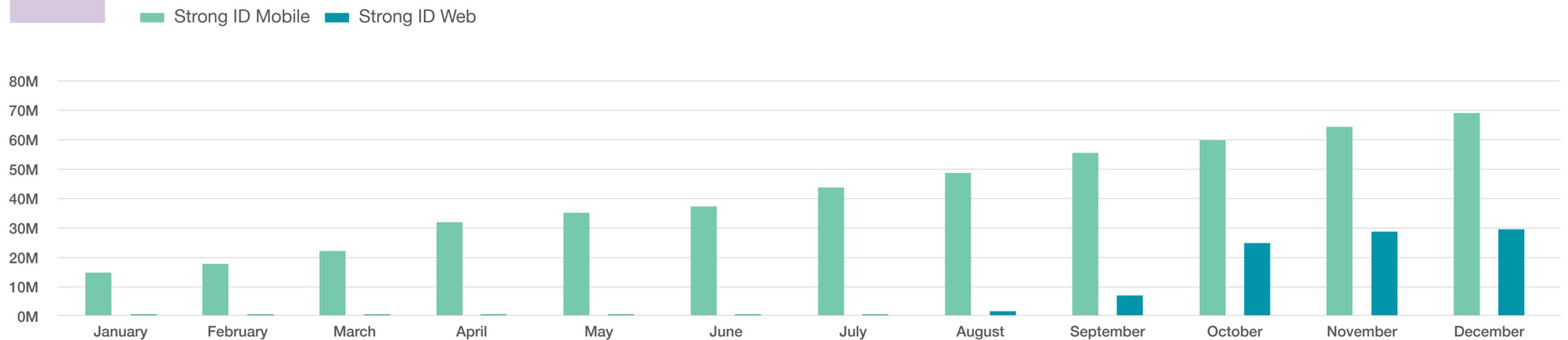
Evolving Mobile Trends

Device binding allows users to transact on trusted devices without the need for repetitive authentications.

This helps prevent an attacker from impersonating a trusted device and enables legitimate customers to benefit from a low-friction authentication token.

Conclusion

Strong IDs in the Digital Identity Network, by Month



Fintech Providers Remain a Key Vulnerability



Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

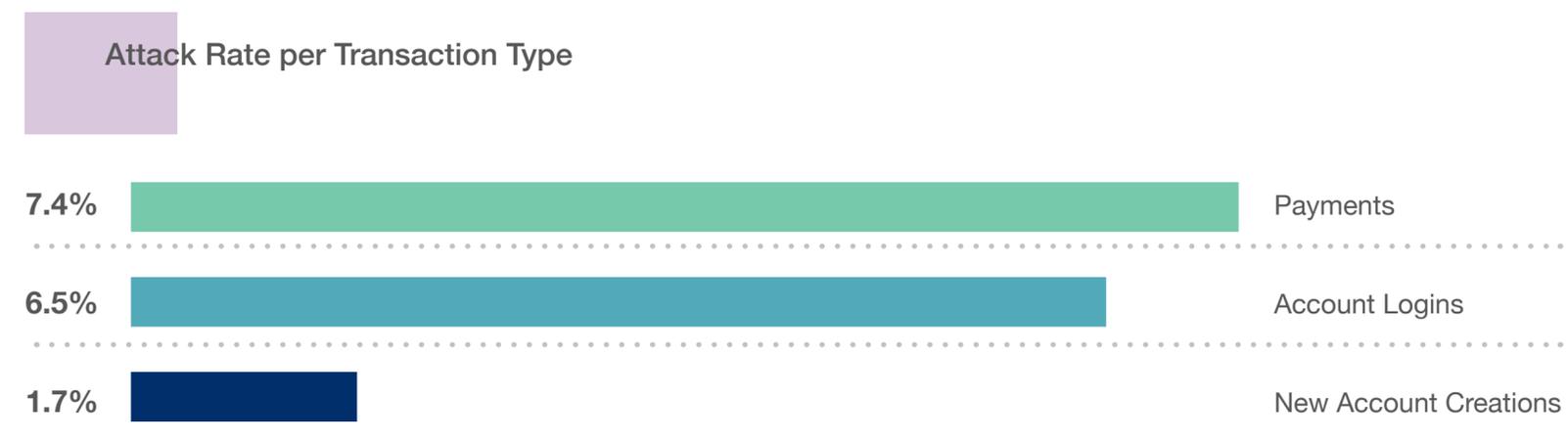
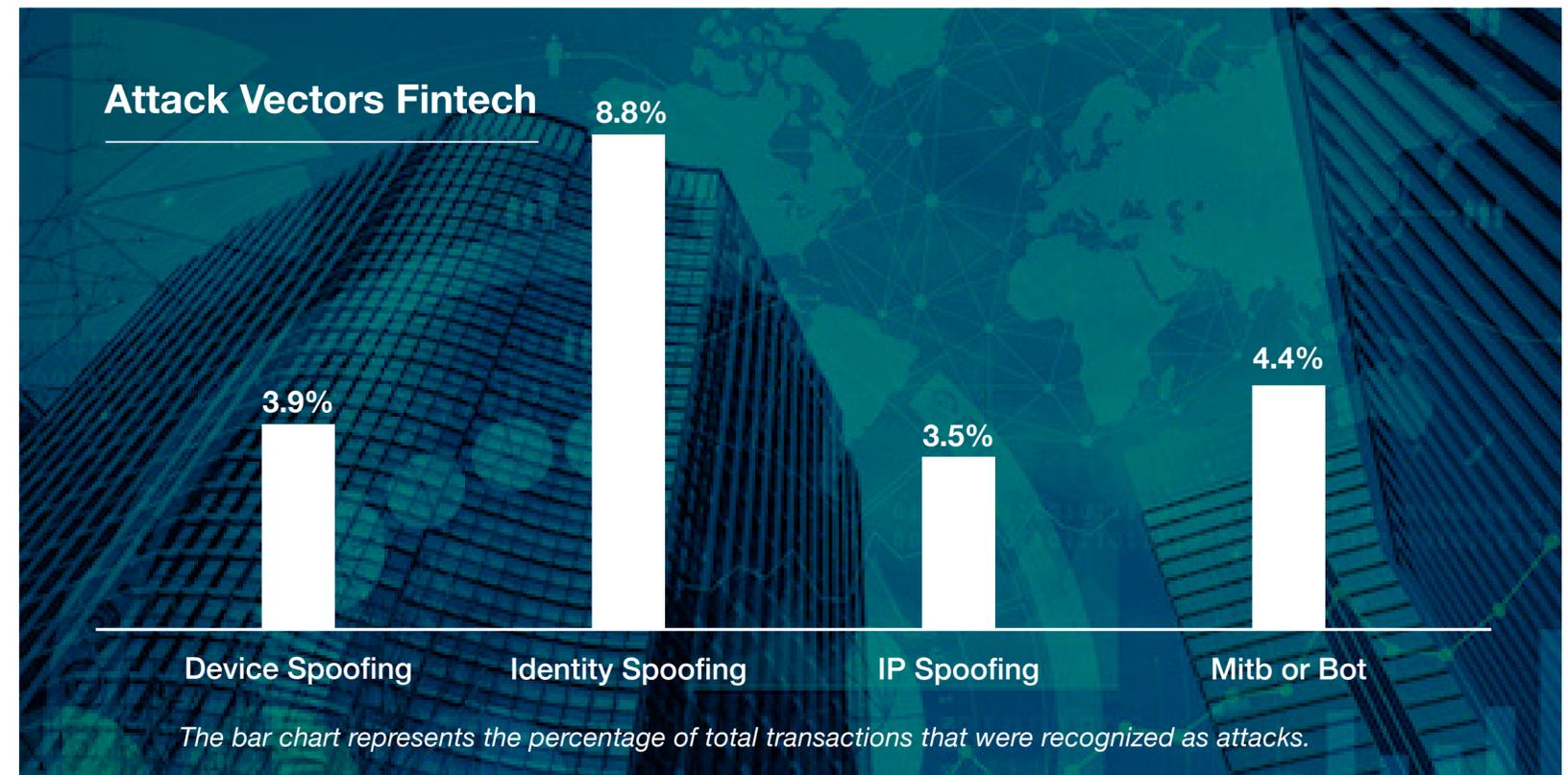
Fintech providers in the financial services industry remain susceptible to account takeovers and payments fraud, particularly digital wallet and remittance companies.

Having grown up in the niche that was created by the sometimes less agile established banks, Fintechs traditionally tailored their goods and services to an online-only, sometimes mobile-only, consumer base.

In addition they have often targeted the unbanked and underbanked population, in geographies where identity verification services are less prevalent.

This accounts for the much higher instance of identity spoofing attacks in Fintech - 8.8% in comparison to the overall figure for financial services institutions at 4.2%. Identity spoofing attacks coming from Asia, South America and Africa, targeting Fintech companies, are high, for example.

Digital wallet and remittance companies provide a prime target for fraudsters seeking quick monetization of stolen credentials. Given that in some growth economies, these services provide a primary means for making digital payments, vulnerable customers and first time users may also be more exposed to the risk of social engineering.



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



Spotlight: CertifID Secures \$775M in Wire Transfers, Leads Fight Against Real Estate Wire Fraud



CertifID was founded in 2017 by Lawrence Duthler and Tom Cronkright. In 2015, Duthler and Cronkright became victims of wire fraud, sending \$180,000 to a criminal posing as a legitimate buyer. An ongoing investigation into the crime uncovered a sophisticated global network of fraudsters, using stolen identities to hijack communications and target lucrative real estate deals. As a result, Duthler and Cronkright identified the need for a solution that would give real-time identity verification while securing send and receive wiring instructions for companies.

The Business Problem

The FBI estimates that \$1 billion is lost from wire fraud every year. Fraudsters target the buyer in a real estate transaction with sophisticated phishing attacks that compromise email accounts. Fraudsters access the communications around a real estate transaction to send incorrect wiring information to the buyer, or social engineer a spoofed account, using these compromised accounts. The buyer will then act on this false information that they assume is correct. In reality, they are sending funds directly to the fraudster.

The Solution

In partnership with LexisNexis® Risk Solutions, CertifID is able to genuinely recognize trusted users, piecing together their digital identity from the complex digital footprint created as users transact online. Used in conjunction with Knowledge Based Authentication, Two Factor Authentication, and Bank Account Certification, CertifID leverages the LexisNexis® Digital Identity Network® to digitally verify users.

Results

- 95.5% identity confirmation rate
- \$42M of “high-risk” wire transfers mitigated
- \$775M in safe wire transfers
- \$2.3B in guaranteed funds protection



The need to confirm identity at critical points in a transaction is crucial in today’s environment. LexisNexis Risk Solutions delivers real-time insights that we use to manage our identity process.”

Tom Cronkright, CEO, CertifID

DISCLAIMER: This case study is not meant to indicate that the same or similar results can or will be obtained in other cases or situations. Results will vary depending on the facts and circumstances of your business.

- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends
- Conclusion

Cryptocurrencies



Foreword

Since its inception in the early 2000s, the cryptocurrency market has attracted millions of new investors and revolutionized payments, investments and banking.

Overview

Operating outside the jurisdictions of countries and governments, with anonymity and security sitting at the core of the system, cryptocurrencies allow investors to break away from traditional markets, free from brokers and banks.

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

Cryptocurrencies, however, operate in a landscape of heightened risk, with anonymity and a lack of judicial oversight presenting a significant opportunity for fraudsters to launder money and finance global cybercrime.

Attempting to infiltrate cryptocurrency exchanges and compromise digital wallets, cybercriminals are leveraging stolen identity credentials and tapping into the latest technologies to open fraudulent accounts and process fraudulent payments.

Through the use of behavioral biometrics techniques (for example keyboard and mouse interactions), it is sometimes possible to identify behavior that does not represent usual customer behavior, but rather is more suggestive of stolen identity or payments details being re-used by a fraudster. By using these techniques, the fraud detection rates of some existing rules can be improved by 100%.





Media Transactions and Attacks

- Foreword
- Overview
- Transactions & Attacks**
- Regional Trends
- Evolving Mobile Trends
- Conclusion

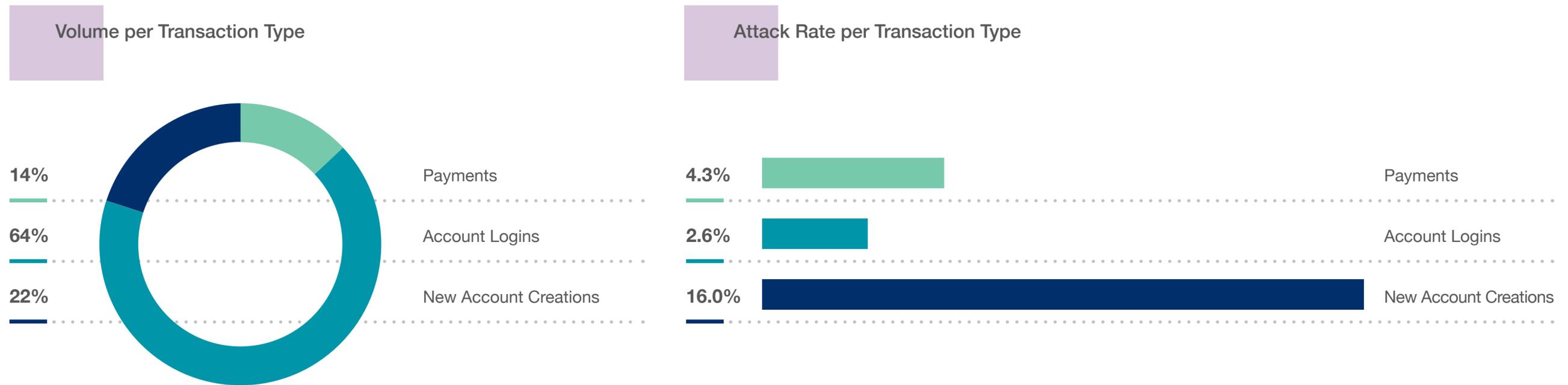
The media industry represents a gateway to digital transactions either for young adults signing up to social media and content streaming sites, or for those new to digital transacting in emerging and growth economies. As a result, the LexisNexis® Digital Identity Network® sees a higher proportion of new account creation transactions in media than in other industries. Interestingly, the industry is slightly less mobile than financial services – 49% of all transactions are mobile. As with e-commerce transactions, however, this is primarily driven by a

lower mobile penetration for account logins: consumers seem more happy to open new accounts and make payments on a mobile device.

New account creation attacks are more prevalent in media organizations than in any other industry, with an attack rate of 16%, a growth of 14% in comparison to the first half of 2018. Media accounts, by virtue of their low barriers to entry and generally less robust security measures, are prime targets for identity testing attacks. Globally, media

attacks have grown in comparison to the first half of 2018.

Media transactions are more susceptible than any of the other core industries to device spoofing (11% of total transactions), identity spoofing (10% of total transactions), IP spoofing (5% of total transactions) and bot attacks (7% of total transactions). In the second half of 2018 the media industry was hit by 211M bot attacks, a growth of 16% in comparison to the first half of 2018.



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



Media Trends by Region

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

North America

- New account creation and login transactions from North America are particularly vulnerable to attack: new account creation attack rates have grown 45% year-on-year while login attack rates have grown 20%

South America

- South American new account creation and payments transactions continue to be particularly susceptible to attacks. New account creations are rejected at a rate of 23%, with payments at 25%, indicating the areas vulnerability to identity testing along with the monetization of stolen credit cards
- However, the threat to these transactions does appear to be dropping somewhat: new account creation attack rates have dropped 17% year-on-year, while payments attack rates have reduced 22%

EMEA

- Attack rates on new account creation transactions from EMEA have grown 32% overall and 70% for mobile-only transactions
- France, Germany and Italy in particular see a strong growth in attacks on new account creation transactions
- Germany has the highest attack rate of all new account creation transactions at 41% and growing. Likewise, payments attacks are extremely high at 19% and continue to grow
- Russia has the highest percentage of account takeovers at 19%

Asia

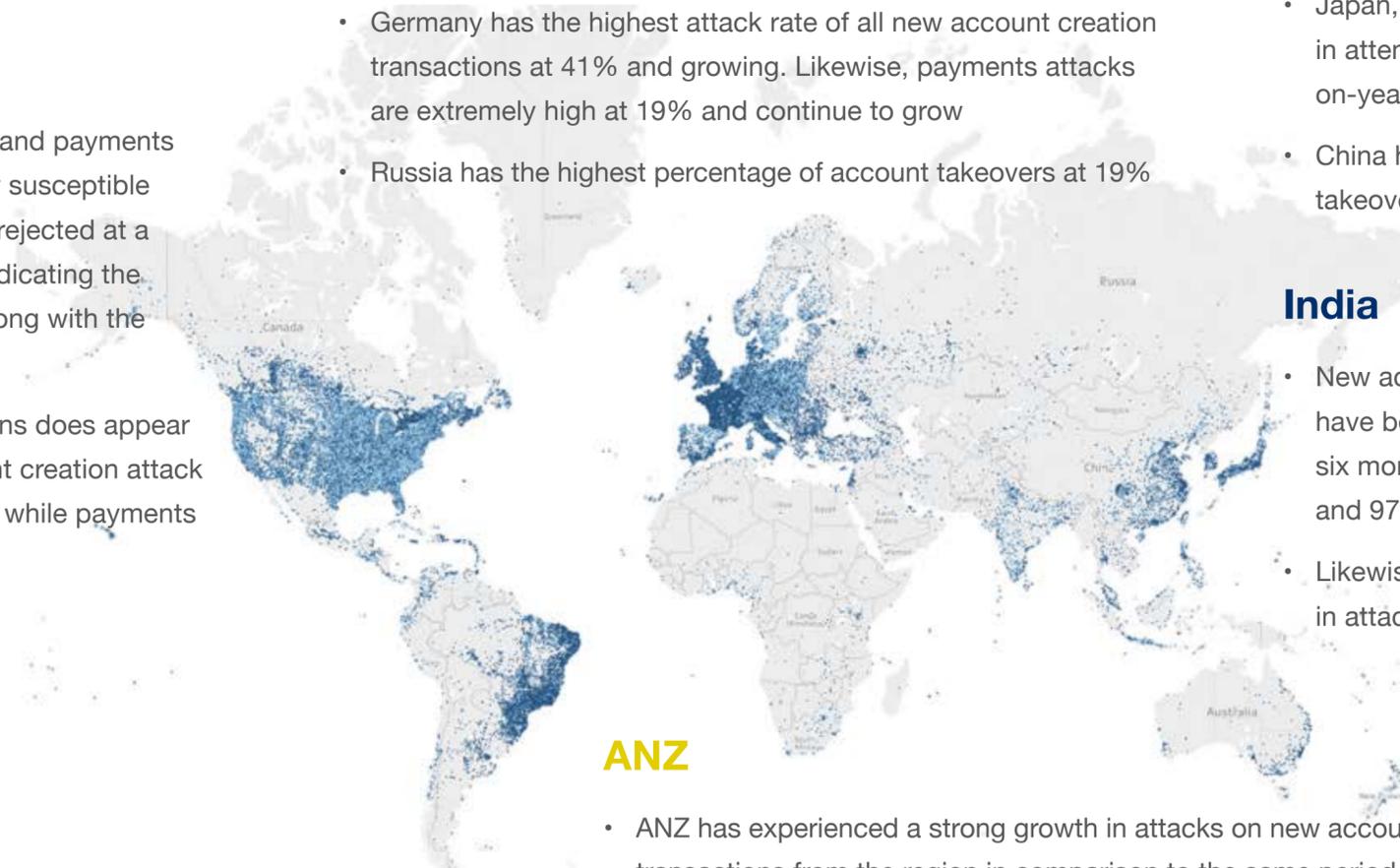
- New account creation transactions from SE Asia have experienced significant growth in attacks specifically in the last six months, with attacks growing 48% overall and 114% for mobile transactions
- Japan, however, has seen a more consistent growth in attempted account takeovers; 33% overall year-on-year and 50% for mobile transactions specifically
- China has the second highest percentage of account takeovers at 17%

India

- New account creation attacks originating from India have become more susceptible to attack in the last six months in particular, with a growth of 75% overall and 97% for mobile transactions
- Likewise, payments transactions have seen a growth in attack rates of 29%

ANZ

- ANZ has experienced a strong growth in attacks on new account creation transactions from the region in comparison to the same period last year
- Attack rates have grown 259% overall and 330% for mobile new account creations, illustrating the region's vulnerability to identity testing attacks
- Australia specifically has also experienced a growth of 47% in account takeover attacks on media transactions year-on-year



Proliferation of Bot Traffic Testing Stolen Identity and Credit Card Data

[Foreword](#)[Overview](#)[Transactions & Attacks](#)[Regional Trends](#)[Evolving Mobile Trends](#)[Conclusion](#)

The latter half of 2018 saw particularly strong bot activity targeting media transactions, with the majority of the bot volume originating in Asian countries. Given that the predominant raison d'être for a bot attack is testing huge lists of stolen identity or credit card data, media organizations are often seen as a soft target given they are keen to subscribe new customers and tend to have fewer barriers to entry.

A number of notable attacks occurred on several media organizations within the LexisNexis® Digital Identity Network® during the second half of 2018, including the following:

- [Attacks on a communications and telco provider, attempting to take over existing customer accounts:](#)
 - » Large bot attacks from Taiwan involving device spoofing and identity spoofing, likely testing lists of stolen identity credentials
 - » Bot attacks from Hong Kong involving IP spoofing
 - » Large identity spoofing attack from South Korea
- [Attacks on a media companies new account subscription processes, to test stolen credit cards:](#)
 - » Large IP Spoofing attacks from the Philippines and Japan
 - » Credit card BIN testing bots, using a proxy to appear to be from a different location, to test stolen credit card data

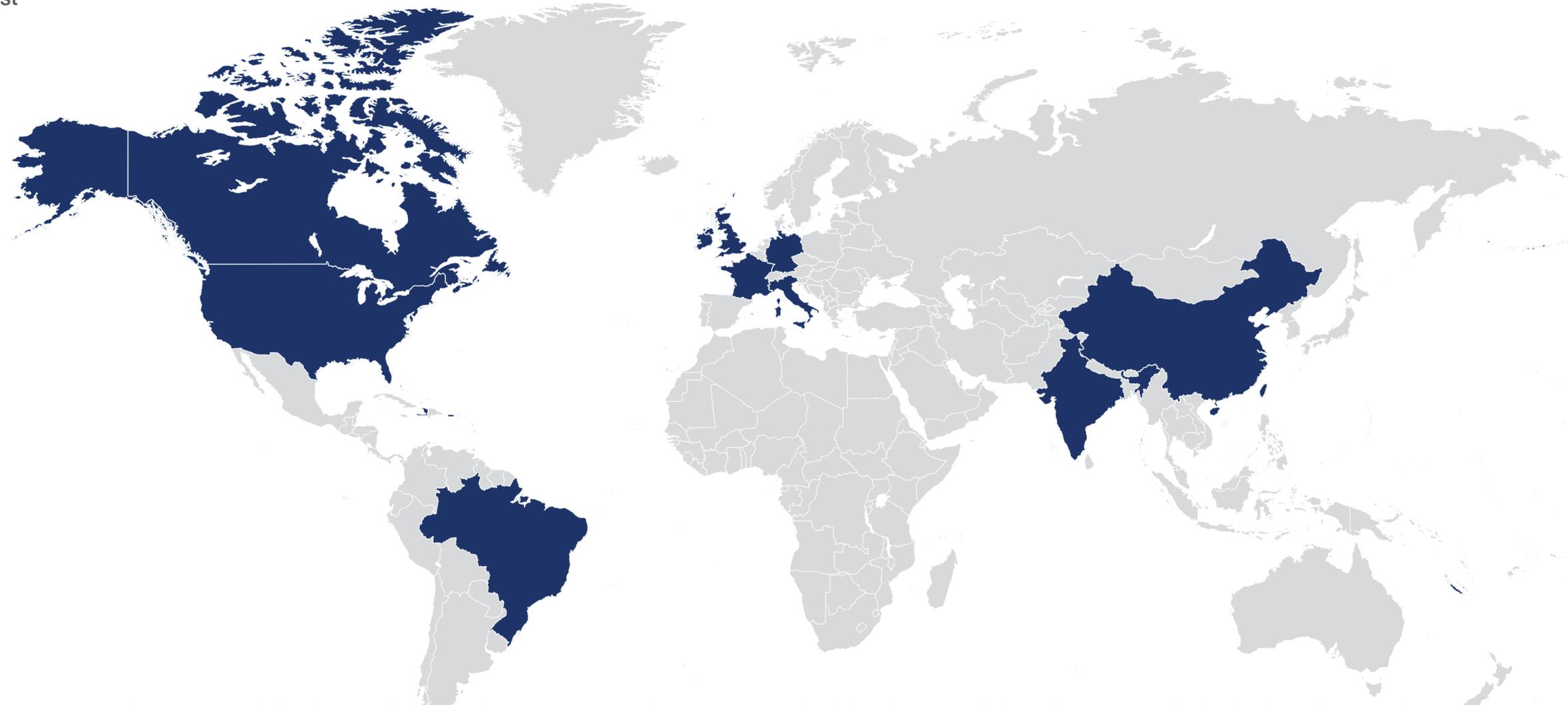




Attack Origins by Geography

Top 10 Attackers List

- #1 United States
- #2 Canada
- #3 Germany
- #4 Brazil
- #5 United Kingdom
- #6 India
- #7 France
- #8 Ireland
- #9 China
- #10 Italy



Cybercrime continues to be a growth industry with highly organized, customizable services and regional outposts in emerging economies.

Historically, the economic powerhouses of the U.S., UK and other large European nations have formed the mainstay of the LexisNexis® Digital Identity Network's® largest attack volumes.

However, the last two years have seen a noticeable shift towards growth economies making their mark on the cybercrime world stage, with Brazil entering the top 5 attackers list for the second time in the last 12 months, and India taking up 6th place.

This reality serves to highlight the widespread and pernicious impact of breached identity data; the lifeblood of global cyberattacks.

This period has seen a growth in attacks from Canada, Columbia, Ukraine, South Africa and Ghana.



Top Attack Originators and Attack Destinations

Historically, fraudsters in the largest attacking nations have tended to attack local geographies, perhaps seeing their close neighbors as easier targets than regions that are more remote. Fraudsters in the U.S. continue attacking the U.S. and Canada; while fraudsters in Brazil continue attacking Brazil, Columbia and Argentina.

A growing pattern of dispersion, however, is emerging. U.S. fraudsters, for example, are also targeting Bulgaria and Japan, while Canadian fraudsters are targeting Japan and Hong Kong.

Interestingly, consumers in Japan are on the top attack list for three of the biggest, and most economically advanced attacking nations, indicating the fact that cybercriminals potentially see this economic powerhouse as a prime target.



1 Attacks from U.S.

Top 5 destinations:

- United States
- Canada
- United Kingdom
- Bulgaria
- Japan



2 Attacks from Canada

Top 5 destinations:

- United States
- Canada
- United Kingdom
- Japan
- Hong Kong



4 Attacks from Brazil

Top 5 destinations:

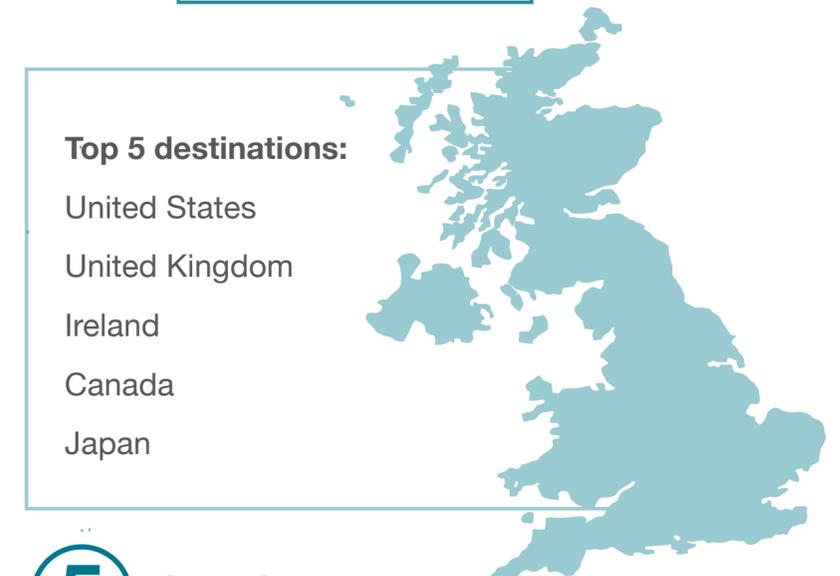
- United States
- Brazil
- Argentina
- United Kingdom
- Colombia



3 Attacks from Germany

Top 5 destinations:

- United States
- United Kingdom
- Ireland
- Germany
- Canada



5 Attacks from UK

Top 5 destinations:

- United States
- United Kingdom
- Ireland
- Canada
- Japan

- Home
- Foreword
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends
- Conclusion



Top 10 Attack Originators 2015-2018

How Often has Country Been in Top Ten Attack Originators over the Last 4 Years

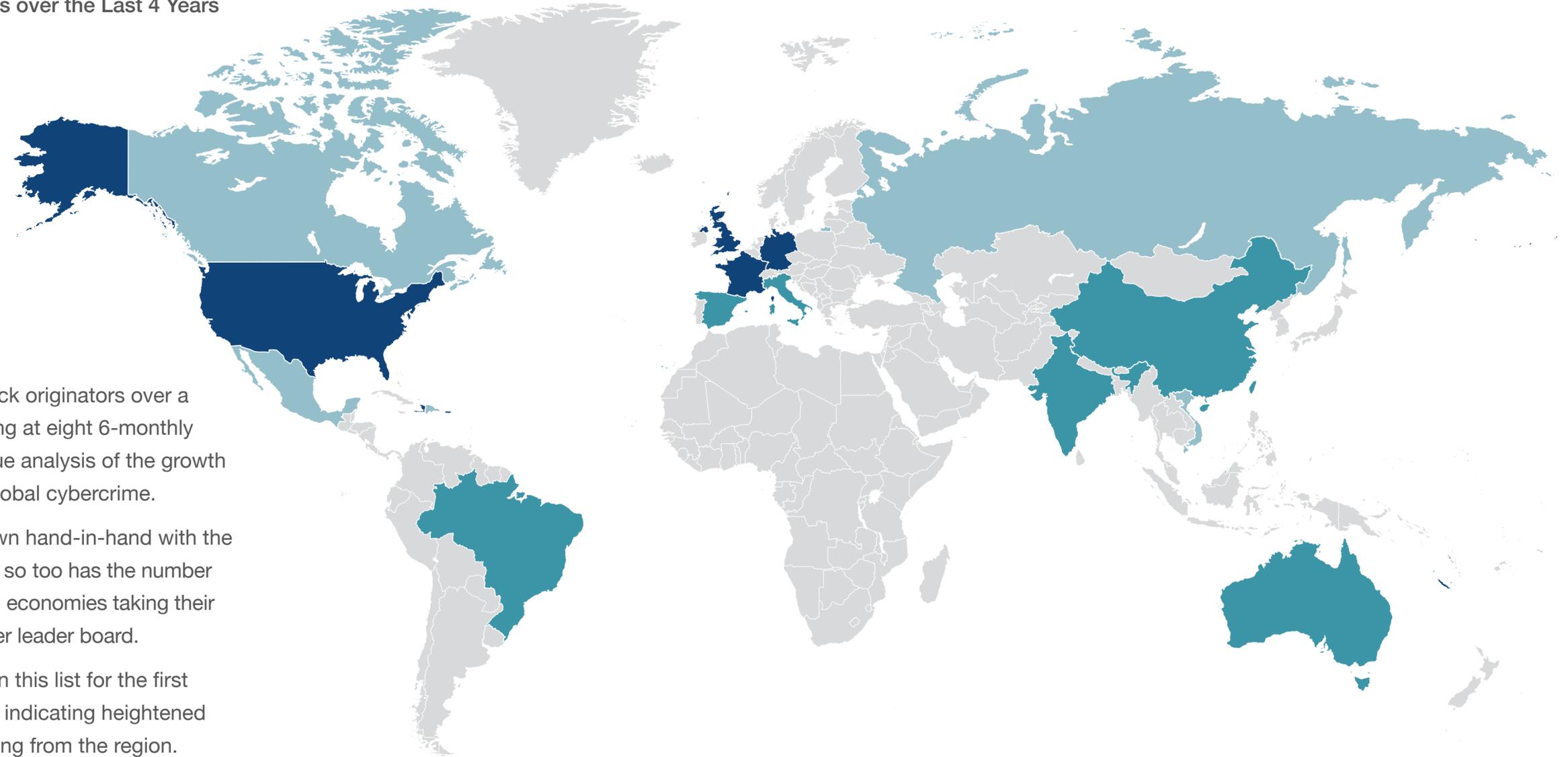
Always



Mostly



Sometimes



Analysis of the top attack originators over a four-year period, (looking at eight 6-monthly periods), allows a unique analysis of the growth and dissemination of global cybercrime.

As cybercrime has grown hand-in-hand with the global digital economy, so too has the number of growth and emerging economies taking their place on the top attacker leader board.

Ireland has appeared on this list for the first time during this period, indicating heightened fraudulent activity coming from the region.

- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends
- Conclusion

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

Region Spotlight: LATAM



- Foreword
- Overview
- Transactions & Attacks
- Regional Trends**
- Evolving Mobile Trends
- Conclusion

Latin America is an incredibly diverse region, encompassing numerous languages, dialects and countries, and is in the midst of immense digital growth.

Fraudsters have been quick to identify opportunities to exploit stolen identity credentials for monetary gain, as people in the region continue to embrace online shopping and adopt mobile transacting.

This has led the LATAM region to emerge as a hotbed of new account creation fraud, with new account creations remaining the riskiest use

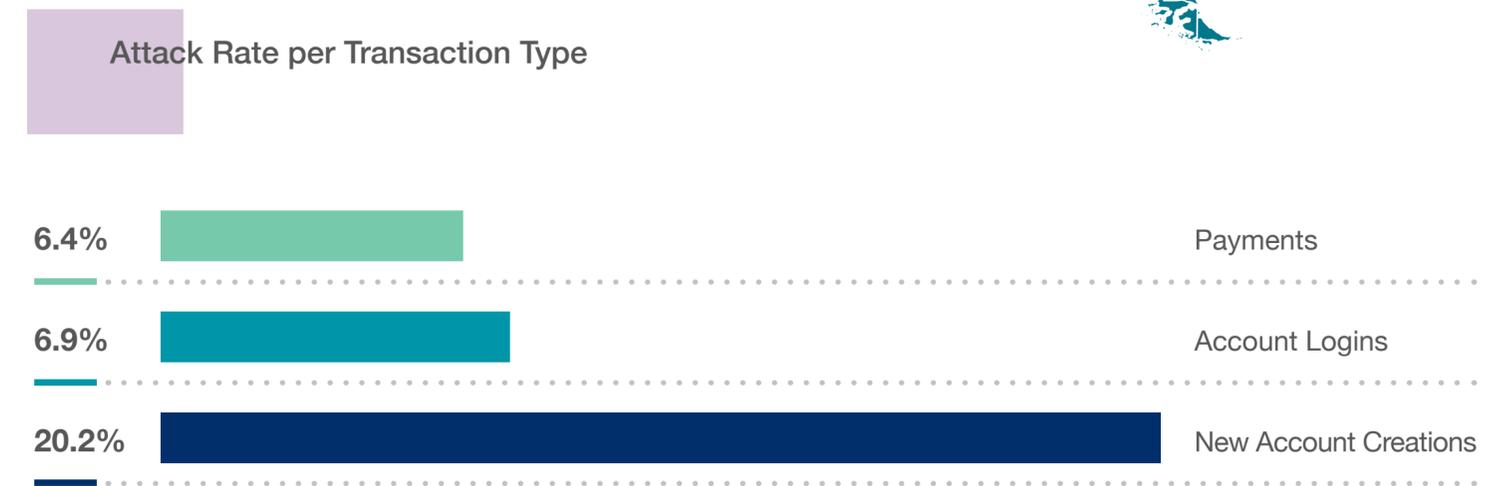
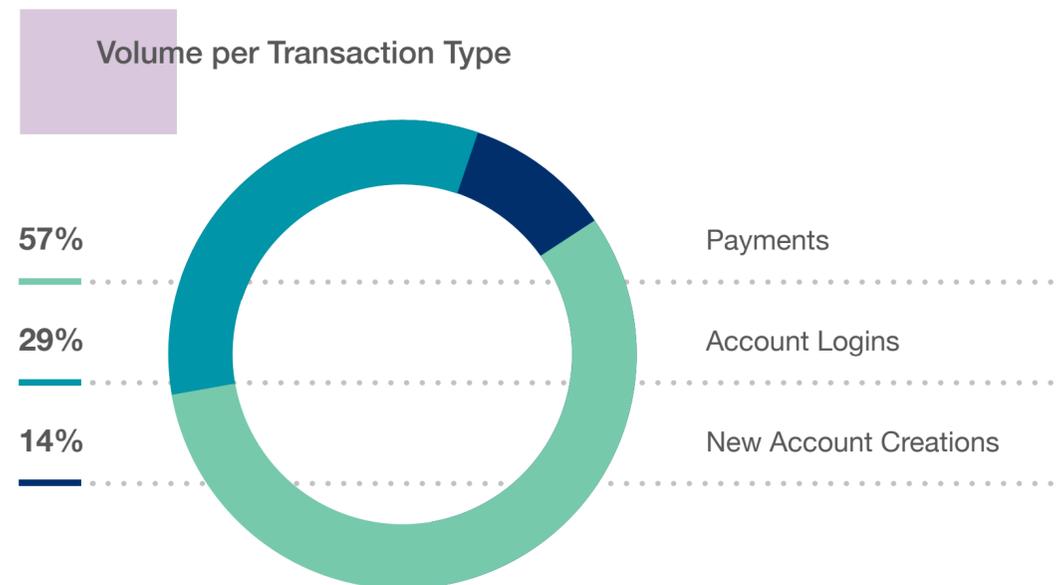
case at 20.2% of the total volume and above the all-industry average of 12.2%.

Although indicating a heightened-risk environment for new account creations, the risk associated with the use case is falling year-on-year. The risk associated with payments, however, is increasing every year, with the attack rate increasing 18% when compared to 2017.

Greater risk is associated with mobile payments, with attacks having increased 52% in just one year. The growth in attacks on mobile payments is driven by the region's booming mobile payments market that shows no signs of slowing.

LATAM Countries

- | | |
|--------------------|------------------|
| Argentina | Haiti |
| Bolivia | Honduras |
| Brazil | Martinique |
| Chile | Mexico |
| Colombia | Nicaragua |
| Costa Rica | Panama |
| Cuba | Paraguay |
| Dominican Republic | Peru |
| Ecuador | Puerto Rico |
| El Salvador | Saint Barthelemy |
| French Guiana | Saint Martin |
| Guadeloupe | Uruguay |
| Guatemala | Venezuela |



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



LATAM: Financial Services Attacks

Latin America, as a fast growing economy, is seeing a surge in online and mobile transacting. This is particularly true in the financial services industry. Mobile adoption and increasingly technologically-savvy consumers are driving financial inclusion in a region where a high proportion of unbanked and underbanked customers exist.

However, fraudsters are exploiting this growth, reflected in the fact that the attack rate has increased substantially across all use cases in just one year; the attack rate on new account creations has increased 105%, rising to 118% for mobile new account creations, while the attack rate on account logins has increased 172%, and 116% for mobile-only logins.

Although modest in comparison to logins and new account creations, the attack rate on payments increased by 17%, rising to 36% for mobile payments.

Identity spoofing continues to be the most prevalent attack vector in the LATAM region, outpacing the global all-industry average.

Foreword

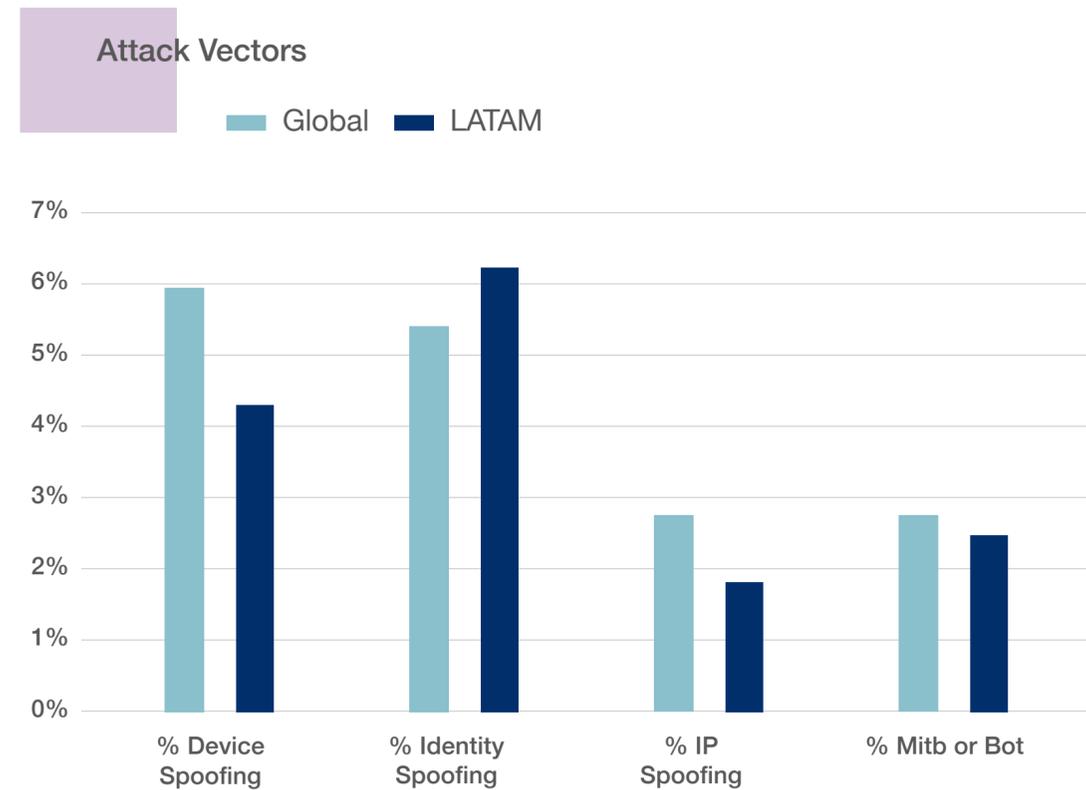
Overview

Transactions & Attacks

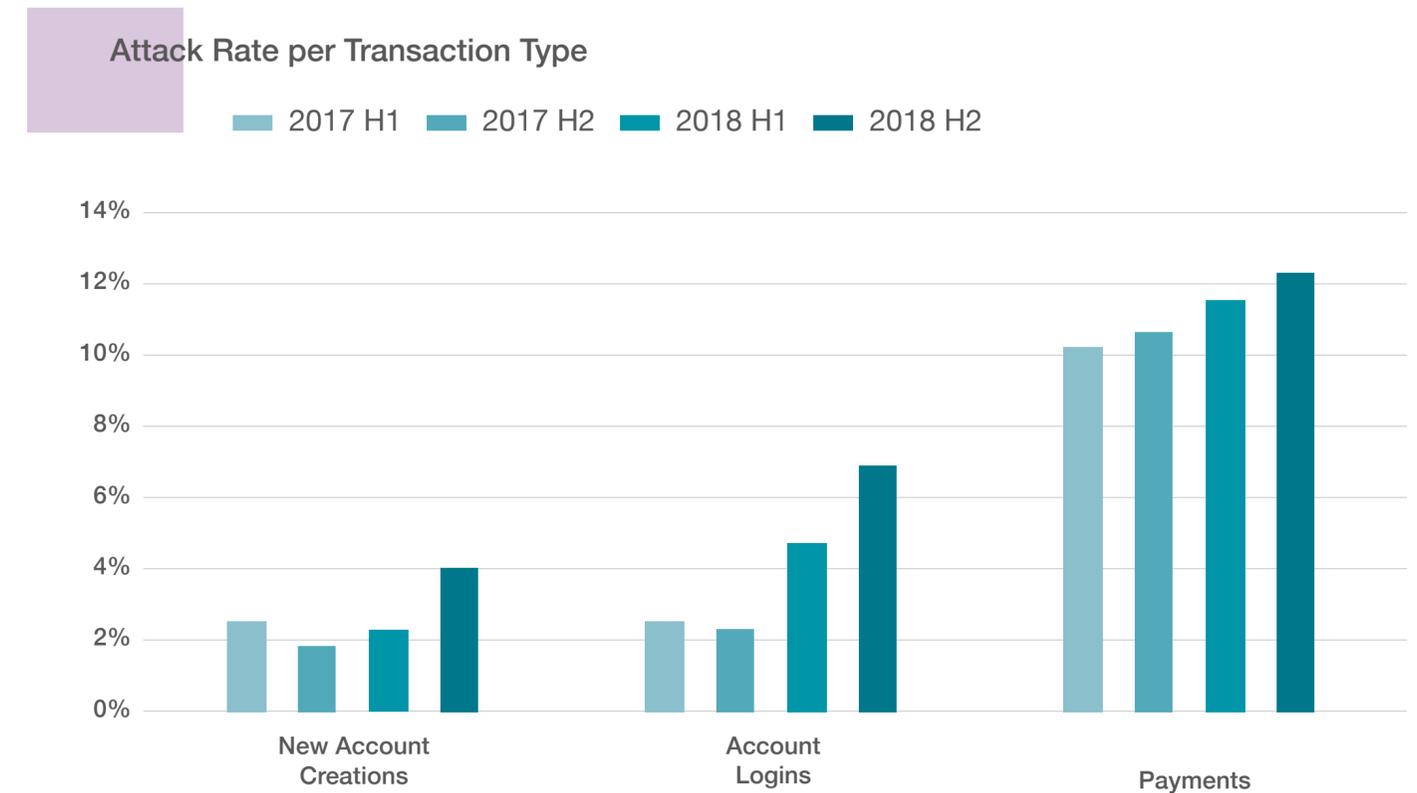
Regional Trends

Evolving Mobile Trends

Conclusion



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



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

LATAM Countries Target Charities to Test Stolen Credit Cards



Foreword

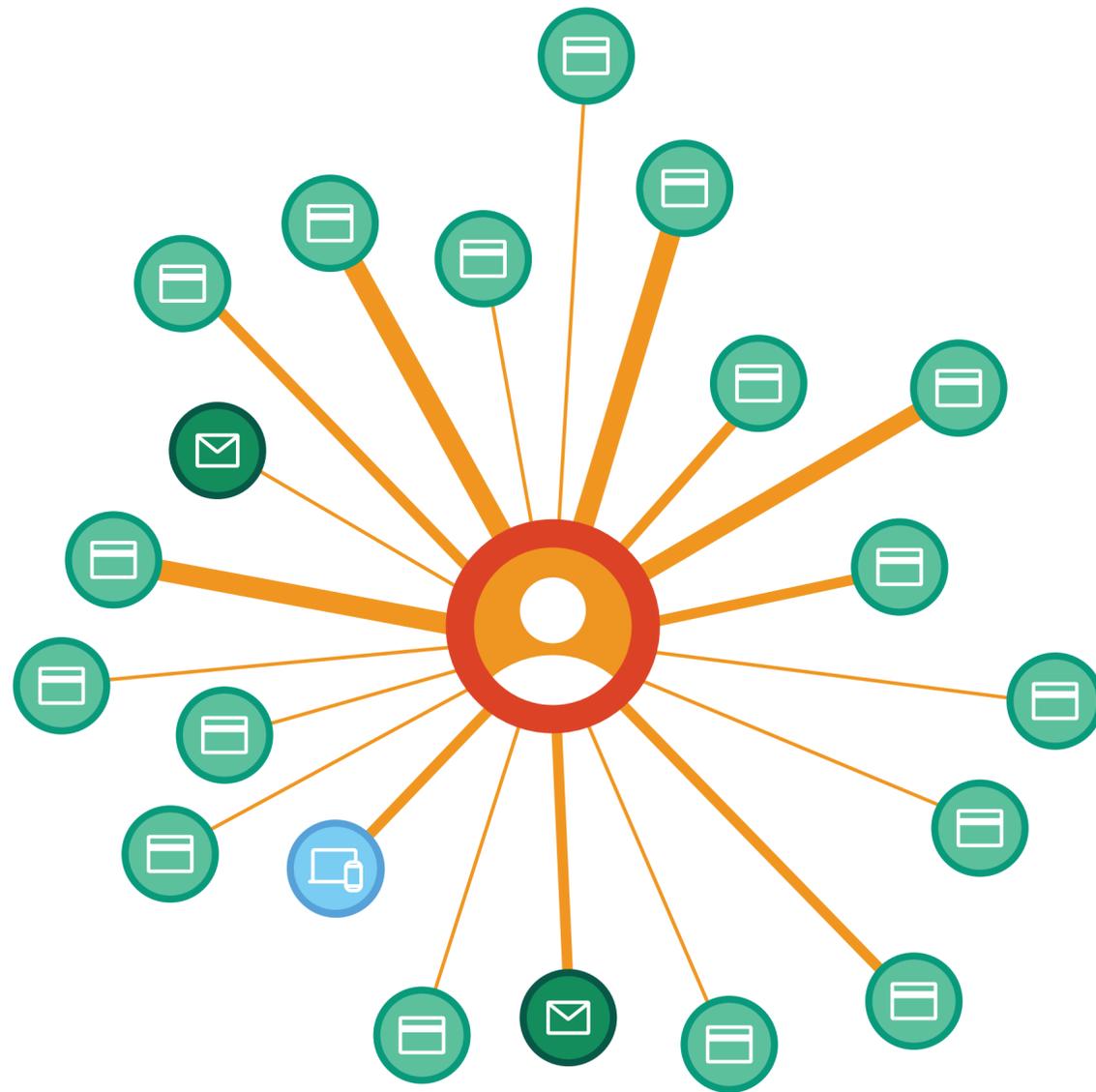
Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion



Bot attack testing credit cards with 1 or 5 dollar payments at charity websites. Bots mostly from Brazil.

The LexisNexis® Digital Identity Network® identified a number of attacks originating from LATAM, targeting several global charities, with attacks seen coming from Brazil, Dominican Republic and Mexico.

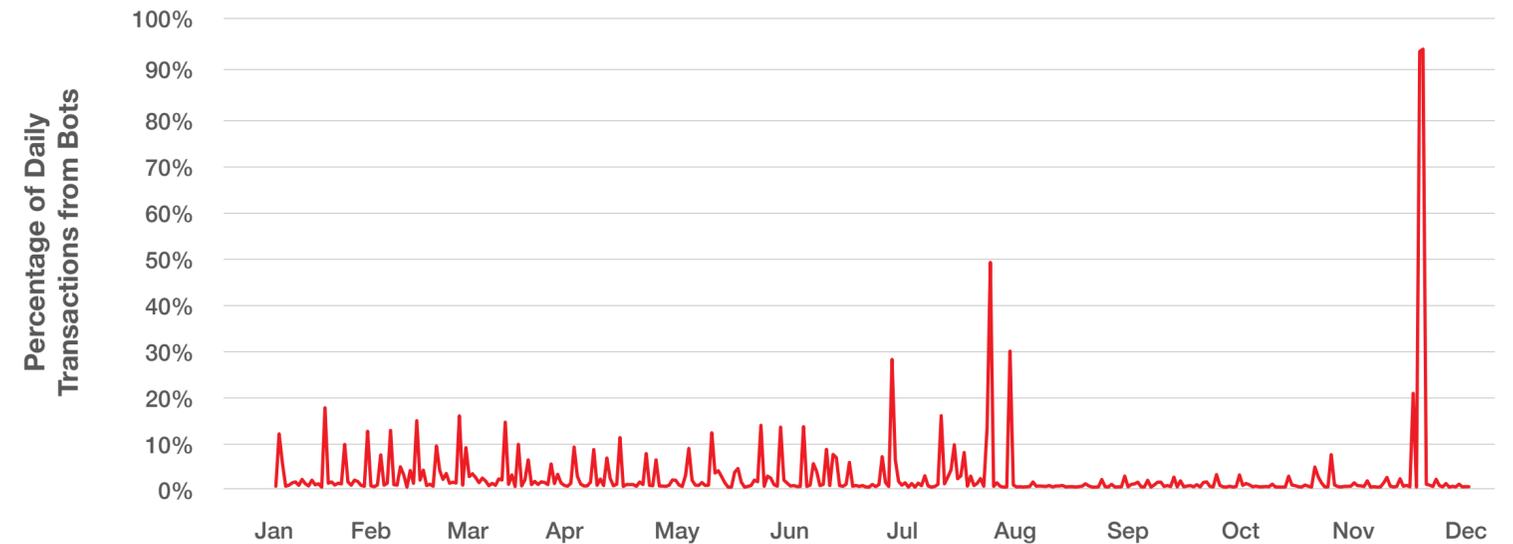
Fraudsters often target charities in the knowledge that such organizations have modest security requirements and offer a perfect test bed for stolen identity credentials.

The Digital Identity Network identified and blocked a bot attack that was being used to test credit card numbers, making small, one or five dollar, payments.

A large attack originating from Brazil was seen in mid-December, with attacks in November originating from Dominican Republic and Mexico.

Once a payment is successful and the stolen credit card validated, the fraudster often goes on to make a bigger purchase or payment on another service or website.

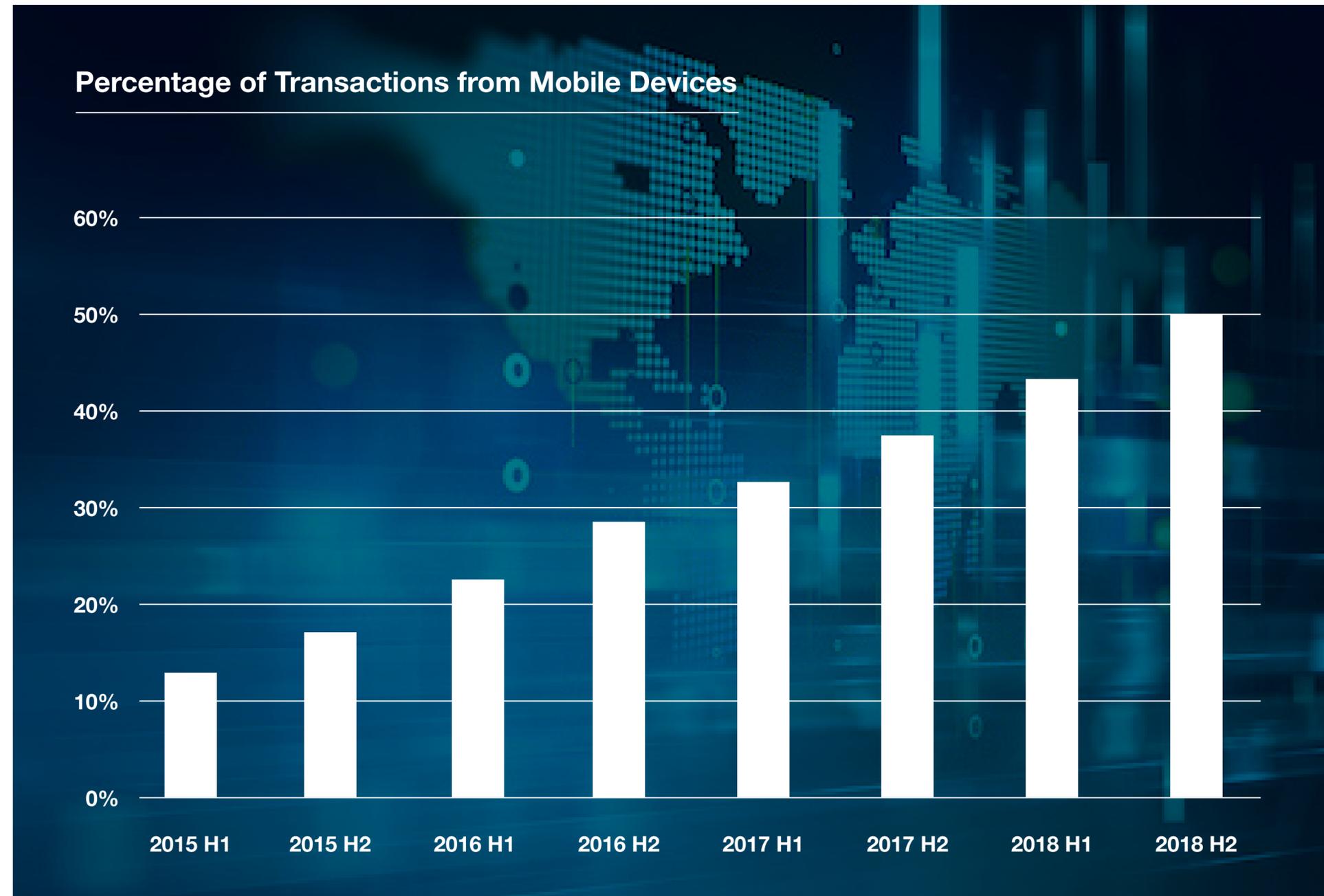
Bots Targeting Charities



Mobile Adoption in LATAM



- Home
- Overview
- Transactions & Attacks
- Regional Trends**
- Evolving Mobile Trends
- Conclusion



In line with global trends, LATAM is seeing consistent growth in mobile transactions.

Mobile transactions accounted for half of total transactions in the second half of 2018, a 33% growth in penetration year-on-year. This reflects the pace at which consumers in LATAM are adopting mobile, driving digital growth and development in the region.

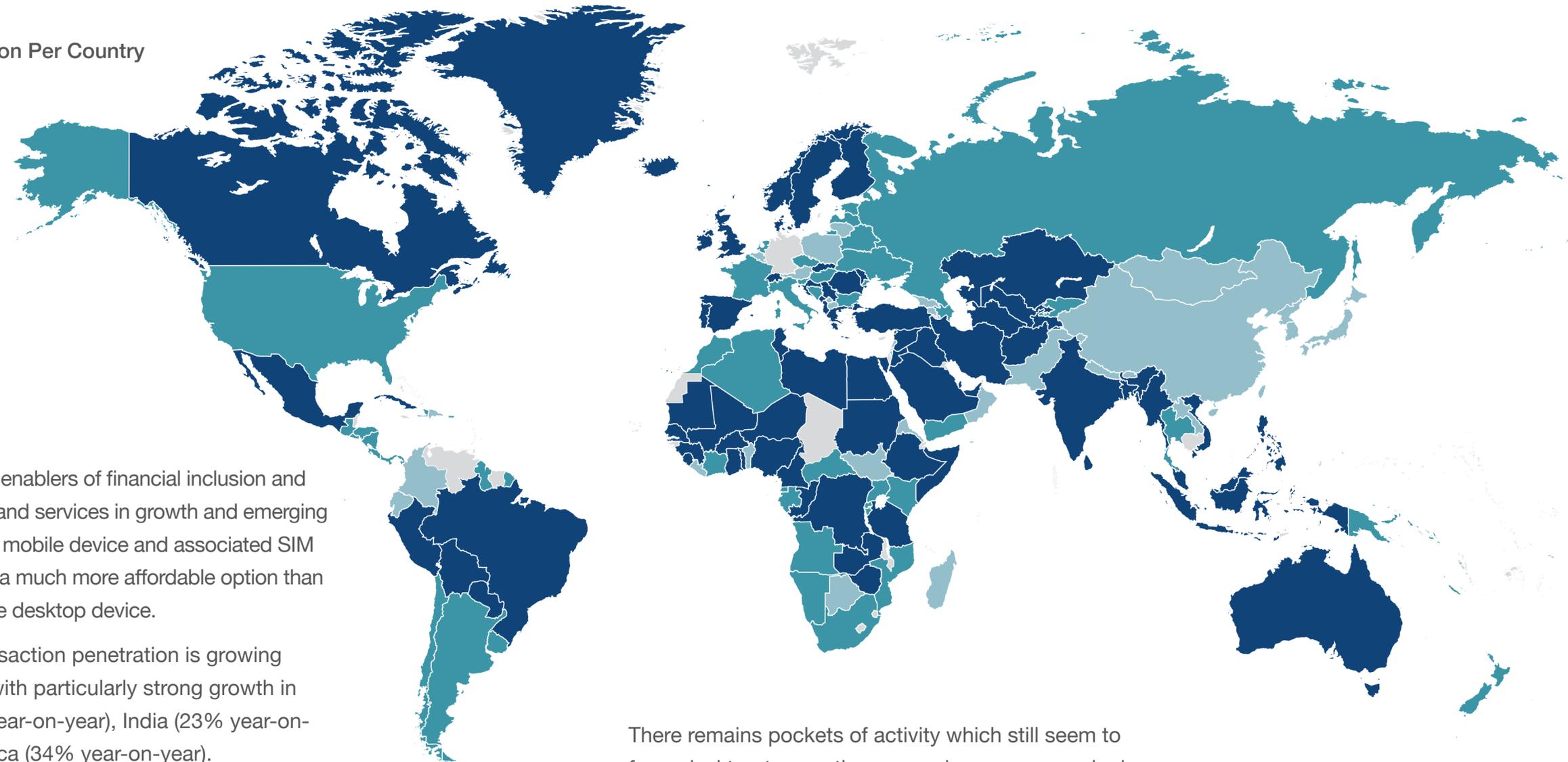
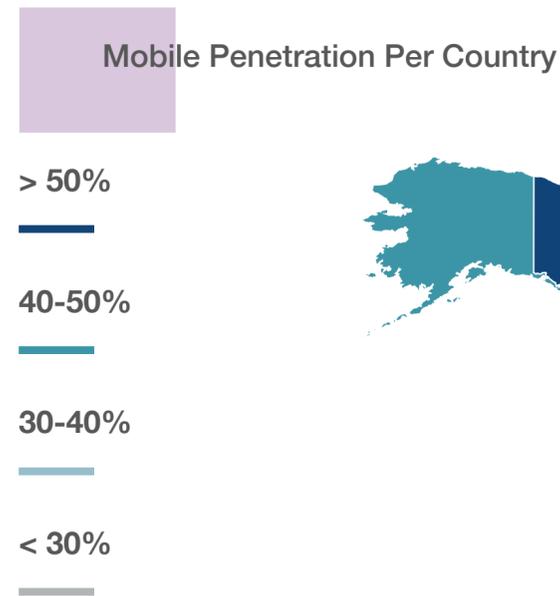
However, the growing risk of cybercrime accompanies such digital growth, with fraudsters targeting mobile transactions.

The mobile attack rate in South America is one of the highest of all regions, at 8.9%.



Will Mobile Penetration Reach Saturation?

- Foreword
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends**
- Conclusion



Mobile is one of the key enablers of financial inclusion and access to online goods and services in growth and emerging economies. Access to a mobile device and associated SIM or monthly tariff is often a much more affordable option than buying a more expensive desktop device.

As a result, mobile transaction penetration is growing in virtually all regions, with particularly strong growth in Greater China (105% year-on-year), India (23% year-on-year), and South America (34% year-on-year).

Globally the mobile transaction rate is growing 16% year-on-year. Given that 61% of all transactions are mobile, rising to 68% in financial services, 67% for new account creations and 62% for logins globally, (and growing in all cases), it will be interesting to track when this growth rate starts to slow.

There remains pockets of activity which still seem to favor desktop transacting – namely e-commerce logins – perhaps because when browsing goods and services online, a larger screen continues to be more practical. It will therefore be incumbent on digital retailers to design the best possible mobile apps for viewing and interacting with their products and services on a smaller screen.



Prevalence of Operating Systems by Region

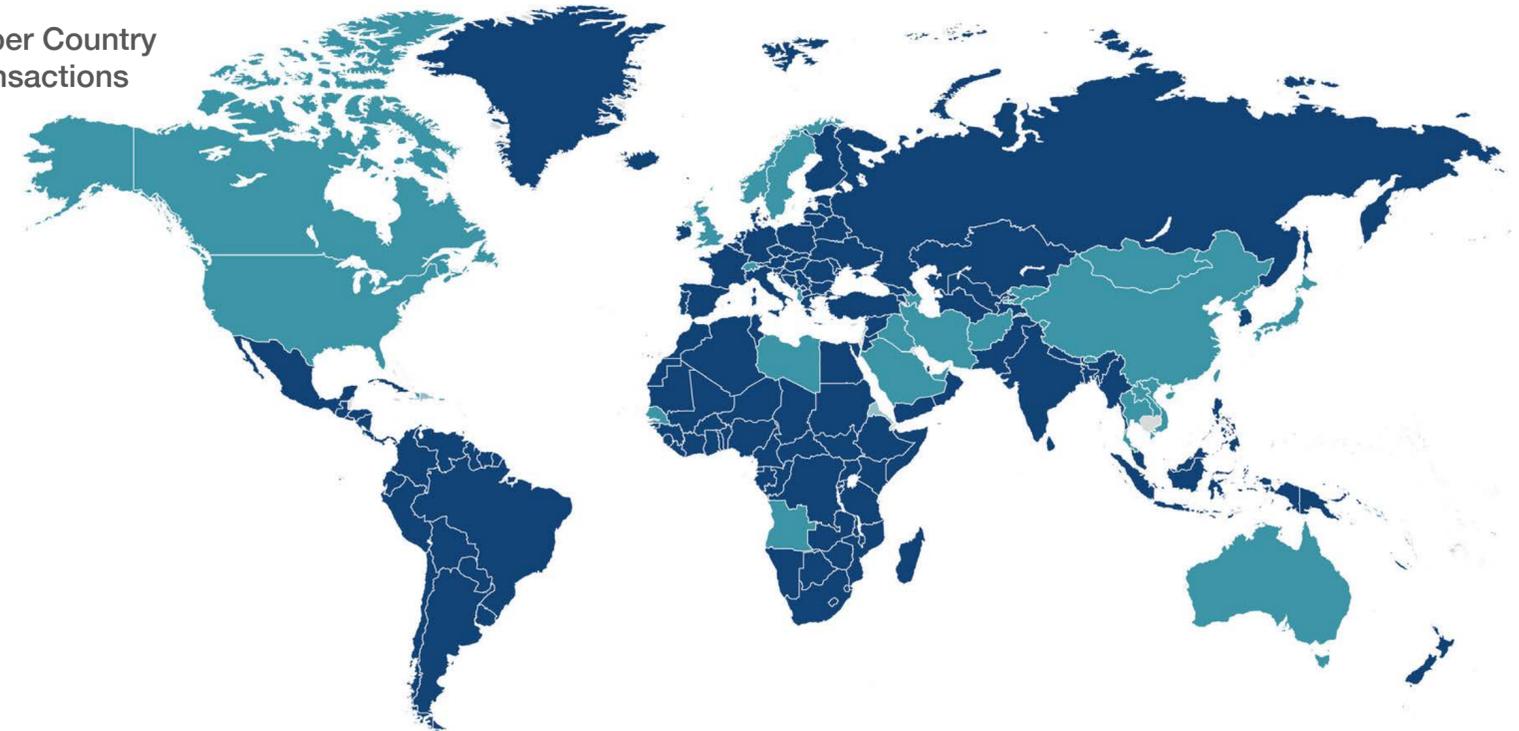
- Foreword
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends**
- Conclusion

The iOS operating system tends to be more prevalent in the most highly developed regions, while Android often has lower entry level costs and therefore tends to have higher penetration in growth and emerging economies.

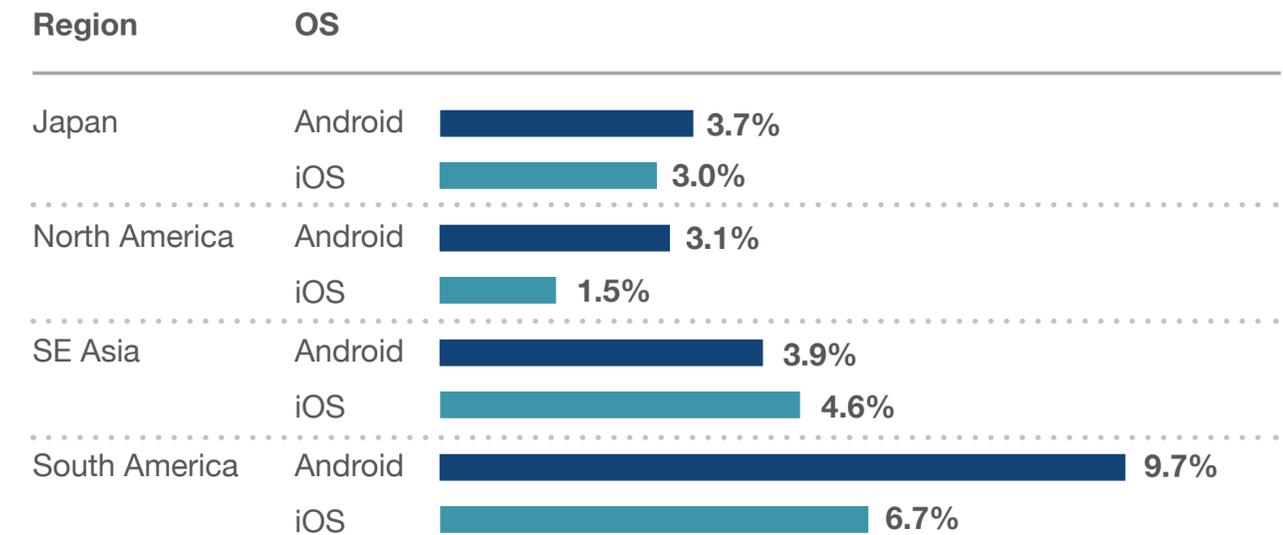
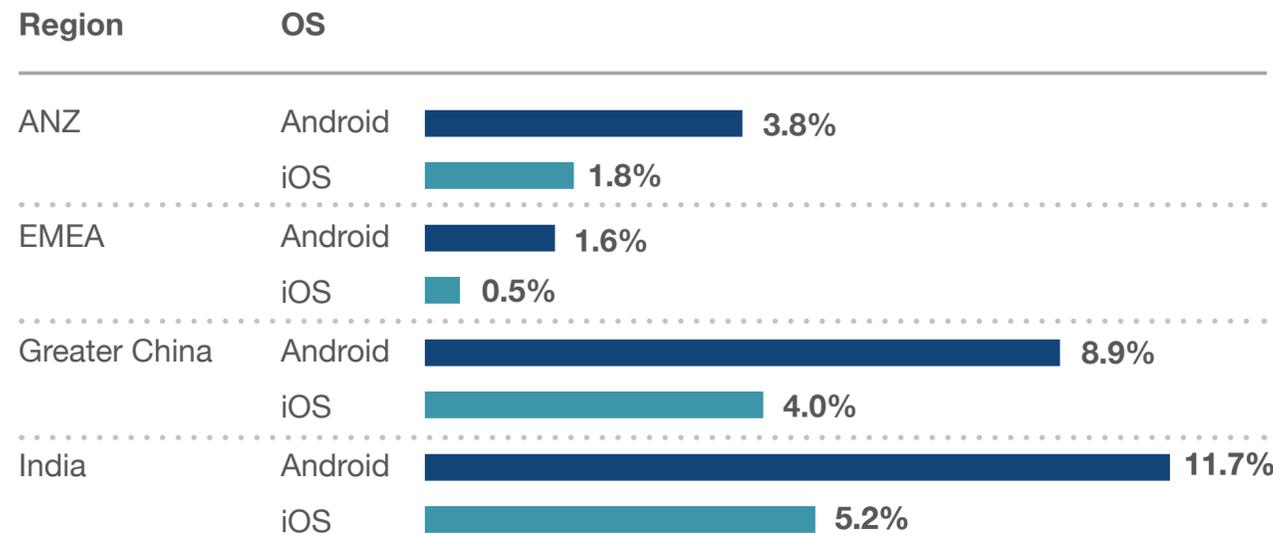
Attack rates on Android are generally higher than iOS.

Main Operating System per Country Based on Number of Transactions

Android
iOS



Android vs iOS Mobile Attack Rate Per Region



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

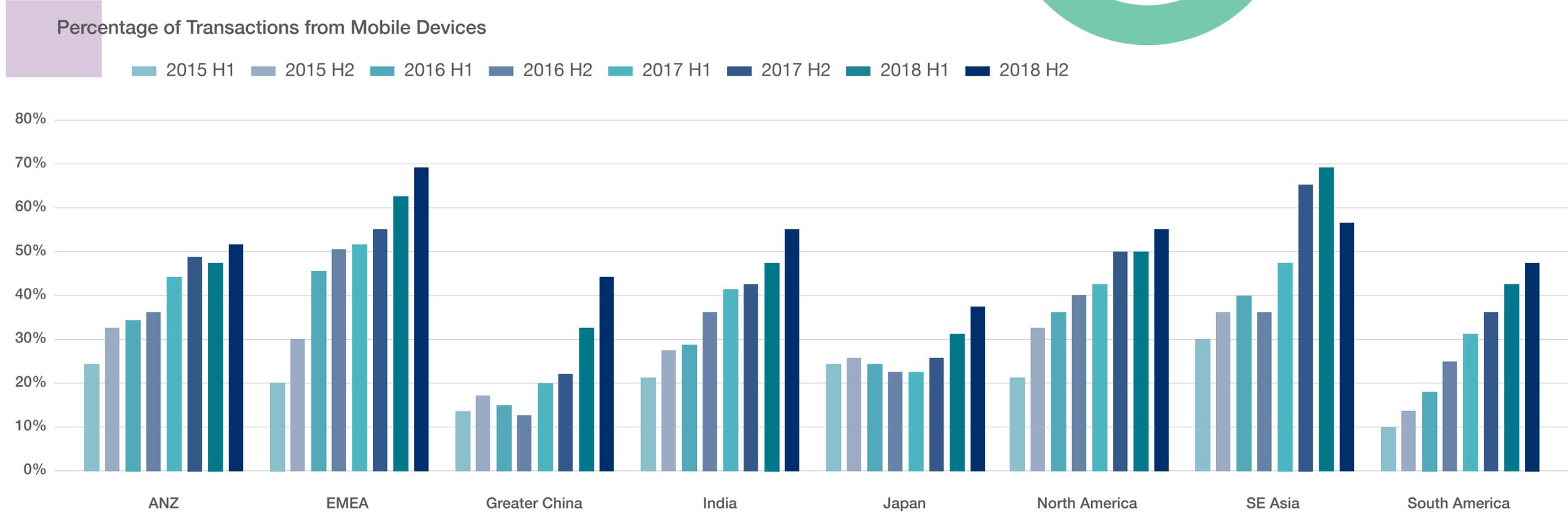
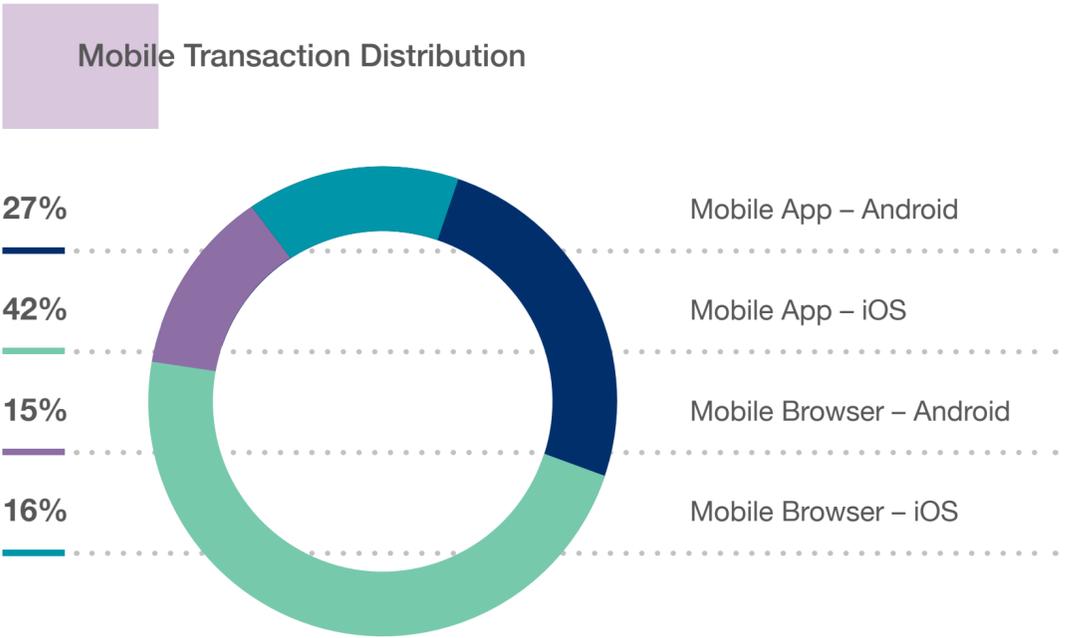


The Evolution of Mobile Transaction Patterns

EMEA continues to drive mobile penetration volume, with steady growth year-on-year.

Several other emerging economies are experiencing strong growth in mobile penetration, notably Greater China and South America, as mobile drives financial inclusion and access to online goods and services for a large proportion of the population who may not have desktop devices.

Globally, the LexisNexis® Digital Identity Network® sees more transactions coming from mobile apps over mobile browsing, perhaps because of the ease of transacting via a mobile app.



- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends**
- Conclusion

Mobile Driving Financial Inclusion in Growth Economies



- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends**
- Conclusion

Foreword

Mobile financial services transaction volume and penetration rate continues to grow considerably in several emerging economies, such as India and South East Asia.

Overview

This highlights the fact that mobile is becoming a key enabler for financial inclusion for the unbanked and underbanked consumer population, who can use mobile devices to carry out money transfers to relatives abroad, sign up for microloans and access online banking services when physical branch facilities are not available.

Transactions & Attacks

Regional Trends

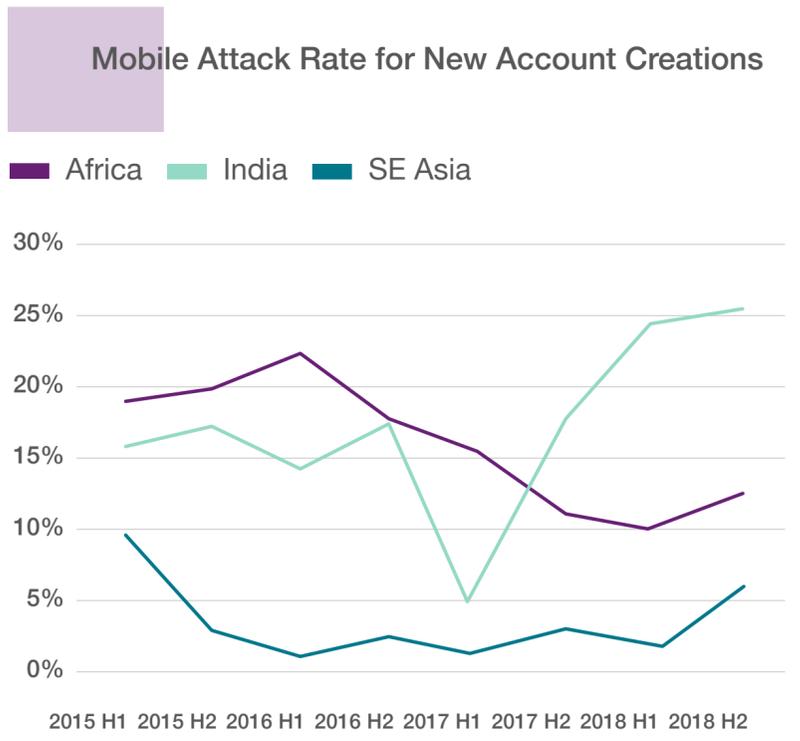
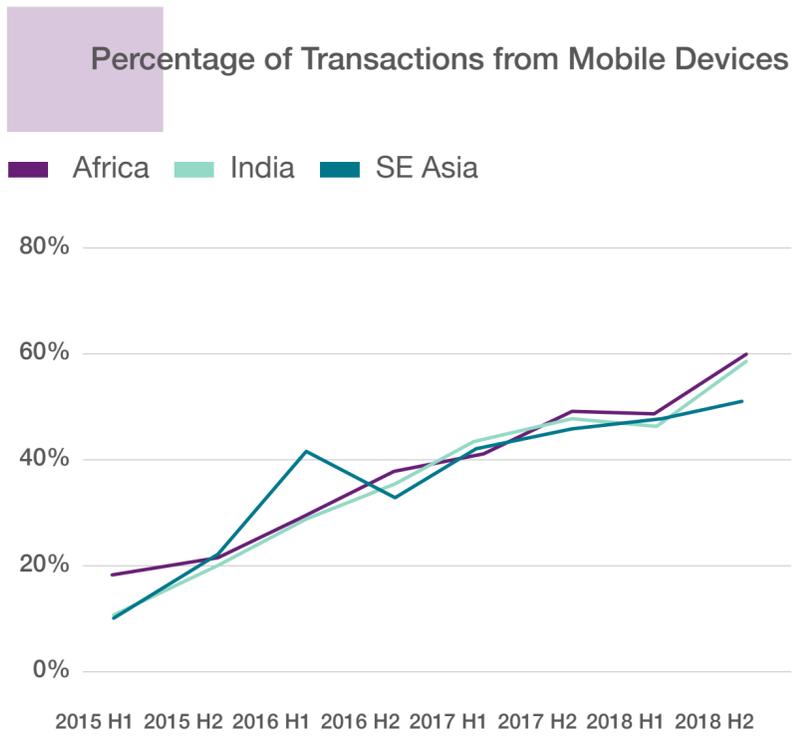
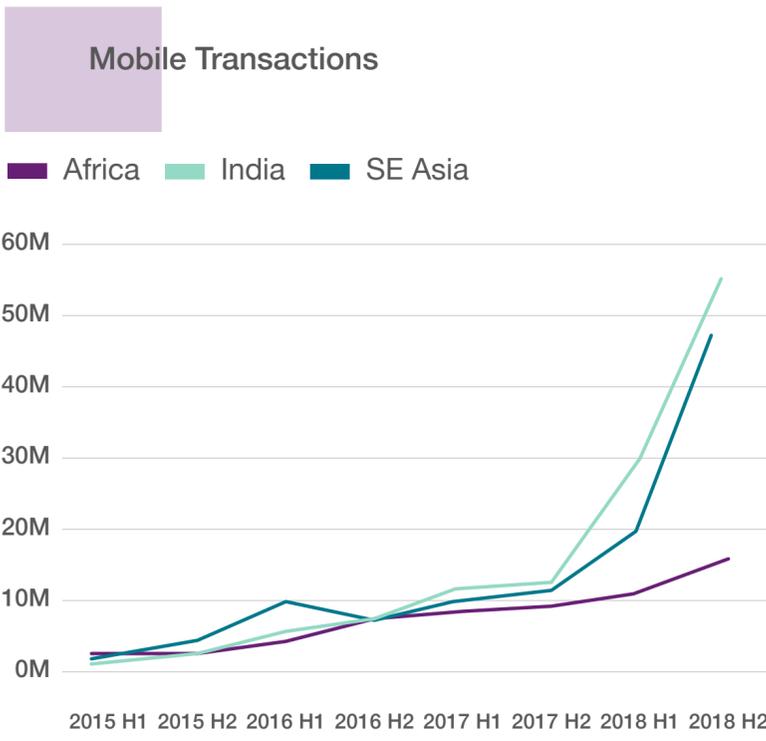
Evolving Mobile Trends

Conclusion

Although the overall attack rate on financial services transactions from these regions is declining, there are pockets of growth in attacks, specifically in the targeting of new account creations originating from a mobile device. New account creations often represent the key point of vulnerability as fraudsters attempt new app registrations to sign up for a new bank account or loan. This represents a significant threat to driving take up of new financial products and services in regions where access to such services can be low.

The attack rate for new account creations on a mobile device coming from India is extremely high at one in every four transactions, and has grown 47% year-on-year.

The attack rate for mobile new account creations from SE Asia is a more modest 7%, however the risk posed to these transactions is growing significantly at 105% compared to the same period last year.



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



The Growing Threat of Mobile Attacks

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

Mobile vs Desktop Attack Rate



Android vs iOS Attack Rate



Android vs iOS Attack Rate – Mobile Browser



Android vs iOS Attack Rate – Mobile App



Mobile transactions in the LexisNexis® Digital Identity Network® still remain safer than desktop, making up 61% of the volume of transactions, but only 42% of the overall volume of attacks. This is in part due to the built-in security features of mobile operating systems and in particular native mobile apps, making them harder to spoof or take over. The Digital Identity Network sees a higher attack rate on Android devices over iOS, and the safest way to transact on a mobile devices remains through a mobile app rather than through a browser session.

However, fraudsters always go where the money is and with a continual volume shift to mobile, it is likely that mobile attacks will similarly continue to rise. The Digital Identity Network is already seeing an evolution of attack types on mobile transactions, as fraudsters tried and tested desktop attack methods, such as bots and remote access attacks, target the mobile channel.

This attack growth is more pronounced in certain regions, and for some core use cases. Key threats include:

- Financial services sees a growth of 35% in mobile attacks year-on-year, with the biggest growth in risk coming from mobile account takeovers, which has seen a growth of 53% year-on-year.
- Media sees a growth of 7% in mobile new account creation attacks year-on-year, as well as a growth of 24% on mobile payments transactions year-on-year.

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

Evolution of Mobile Fraud: Remote Access Attacks on Mobile



- Foreword
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends**
- Conclusion

Social Engineering / Remote Access Attack on Mobile

During the second half of 2018, the LexisNexis® Digital Identity Network® detected a number of attacks using social engineering and remote access software on a mobile device, targeting financial services institutions.

LexisNexis® Risk Solutions implemented real-time behavioral profiling of the end-to-end online session including account registrations, logins, change of details and preferences,

account navigation, creation of new beneficiaries and payments profiling to detect anomalies indicative of malware or illegitimate use of remote access software.

The Attack Method



Fraudster impersonates person / department in trusted position, under the guise of fixing a time-sensitive problem such as live hack or imminent virus.



Fraudster convinces customer to download some remote access software to “protect their account”.



Fraudster then has access to customer account, with the potential to steal account credentials, change details, make payments and transfers etc.

Social engineering attacks have arguably become one of the most pernicious forms of cyber warfare of the last two years, particularly those targeting financial institutions.

Fraudsters make use of the full gamut of stolen identity credentials, as well as publicly available / phished information, to launch pitch-perfect attacks that often fool even the most tech savvy victims into divulging personal details, authenticating a login session that the fraudster can piggy-back, or setting up a new payments beneficiary.

The challenge for banks and customers is that initial contact – either by email, SMS or phone call – can almost exactly replicate a genuine piece of communication. Likewise fraudsters can pretend to be from an IT company calling to fix a problem on the customer’s machine, or even law enforcement trying to stop a live account takeover.

Banks need the ability to detect behavior that may be indicative of a social engineering threat while also doing more to educate customers as to how, when and why they will contact customers. This largely comes down to genuinely understanding how customers behave and transact and detecting unusual changes to this behavior.

Evolution of Mobile Fraud: App Cloning



Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

Mobile is central to the sharing economy, an economic peer-to-peer model based on the acquiring of goods or services among a community based online. From banking and hotels, to transport, the sharing economy has disrupted many industries and businesses across the world.

Fraudsters have been quick to see the opportunity of new goods and services delivered via mobile, evolving attacks to exploit weaknesses in apps.

A transportation company was seeing bonus abuse on its ride hailing app, with fraudsters targeting the increased commission drivers receive through completing a set number of journeys.

Fraudsters would create fake passenger accounts to qualify for these bonuses. Using an app that allows users to clone and run multiple accounts of the same app simultaneously, fraudsters were able to have a driver and passenger app on the same device. As passenger and driver, the fraudster could accept rides from the fake passenger to clock up multiple journeys that didn't actually happen.



Evolution of Mobile Fraud: Mobile Bots



- Home
- Overview
- Transactions & Attacks
- Regional Trends
- Evolving Mobile Trends**
- Conclusion

Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

During 2018, the LexisNexis® Digital Identity Network® started to feel the impact of mobile bot attacks, in addition to the more traditional desktop bots. In the second half of 2018, LexisNexis® Risk Solutions customers were hit by 189 million mobile bots, a 12% growth compared to H1 2018, indicating that fraudsters are seeing the value of developing mobile-based automated attacks.

Like its desktop counterpart, a mobile bot is a type of malware that runs automatically on a mobile device. Once a device is infected, through a worm, virus or trojan via malicious emails, apps or websites, the fraudster has complete access to the device and its contents.

Once in control of a device, fraudsters can steal identity credentials and financial information, install or remove applications, take over accounts and use the device to launch brute force attacks.

Mobile bots can infect thousands of devices over a period of time, creating a botnet capable of disrupting an entire mobile network. The Mirai botnet, which targeted online consumer devices like IP cameras and routers, was used in some of the largest and most disruptive distributed denial of service (DDoS) attacks. One attack caused major internet platforms and services to be unavailable for users across Europe and North America.



Layers of Defense for Mobile Apps



Foreword

Overview

Transactions & Attacks

Regional Trends

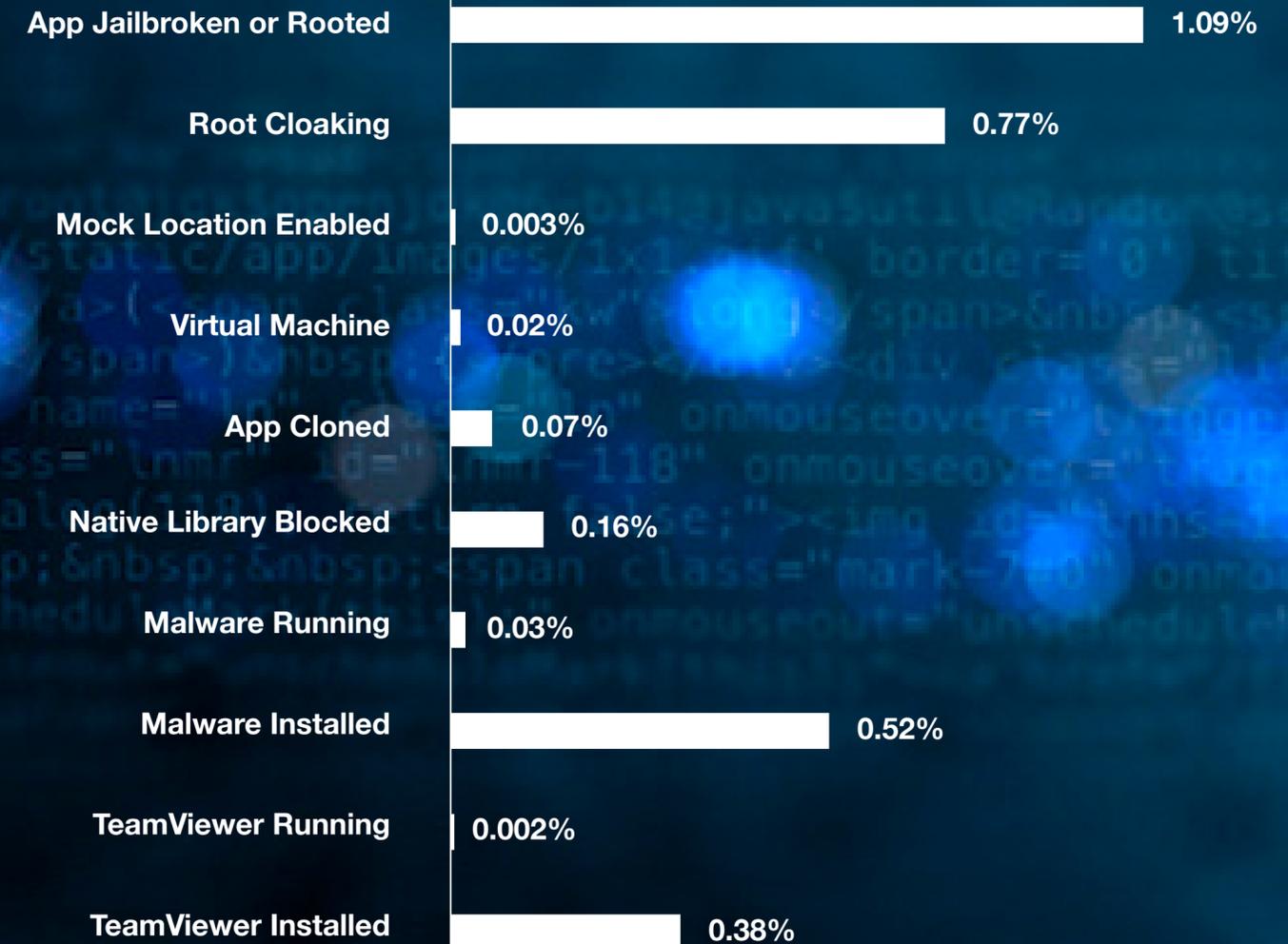
Evolving Mobile Trends

Conclusion

Being able to detect potential risks on a mobile app can help businesses protect themselves and their customers from malicious threats. The LexisNexis® Risk Solutions Mobile SDK can detect a number of potentially high-risk scenarios in real time, which can often be indicators of current or future fraud. For example:

- Identifies devices that have been jailbroken or rooted
- Identifies devices on which fraudsters have attempted to mask the signs of a rooted device
- Evaluates all installed applications on android devices and verifies them against a signature database of over 15 million mobile apps
- Detects presence of Malware either being installed, and/or running
- Detection of apps using a mock location for their GPS data
- Detects instances where a genuine app has been cloned, either from scratch or using cloning software, on the same device
- Detects the presence of remote access software such as Team Viewer being either installed and / or running

Mobile App Health Indicators – % of Mobile App Transactions



Conclusion

[Foreword](#)[Overview](#)[Transactions & Attacks](#)[Regional Trends](#)[Evolving Mobile Trends](#)[Conclusion](#)

Predicting the future patterns and modus operandi of cybercrime often feels like betting high dollar chips in a poker game. There are rarely any winners. However, as 2019 progresses, it is likely that trends seen in the latter half of 2018 will continue to evolve and add to the already complex cybercrime landscape.

What will be the key consumer trends and cybercrime drivers in 2019? Mobile will continue to play a major role this year, with consumers embracing mobile transacting for almost every online use case. Businesses will continue to be challenged as to how they can improve the mobile experience for transactions that are less “small-screen” friendly, such as comparing goods on an e-commerce website.

However, as consumers increasingly adopt a mobile-first approach, it is also likely that fraudsters could adopt a similar mindset, following this volume shift with evolved and highly targeted attacks. The LexisNexis® Digital Identity Network® has already seen evidence of this during 2018 as what have traditionally been more desktop-based attack vectors – for example bot and remote access attacks – move across onto mobile.

We could also see fraudsters leveraging artificial intelligence, applying AI to improving the success of social engineering, as well as automating manual processes. This could lead to a machine vs machine scenario, with AI attacks from fraudsters testing the AI defenses of their targets. The ability to better understand genuine customer behavior, and accurately differentiate this from a robot or a synthetic identity, becomes more pivotal than ever before.

It is clear from this complex and evolving battleground that single point solutions are unlikely to succeed in winning the war against cybercrime. Fraudsters are playing businesses at their own game by behaving like good customers, using AI to increase the success of attacks and employing global networks of machines and humans to launch attacks both at a network level, and on individual customer accounts.

A layered defense of fraud, identity and authentication capabilities, executable in real time, and across the entire customer journey, is the most robust solution to a growing problem. This relies on uniting world-class digital identity intelligence with physical identity and authentication capabilities that can help businesses meet regulatory requirements, streamline the customer experience, reduce friction and detect and block complex fraud.



Glossary



Foreword



Overview



Transactions & Attacks



Regional Trends



Evolving Mobile Trends



Conclusion

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, gambling, gaming and online dating sites.

Common Attacks

New 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 LexisNexis® 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.

Desktop Versus Mobile

Desktop Transactions are transactions that originate from a desktop device such as computer or laptop.

Desktop Attacks are attacks that target a transaction originating from a desktop device.

Mobile Transactions are transactions that originate from a handheld mobile device such as tablet or mobile phone. These include mobile browser and mobile app transactions.

Mobile Attacks are attacks that target transactions originating from a mobile device, whether browser or app-based.

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. LexisNexis® Risk Solutions 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. LexisNexis Risk Solutions 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.

LexID® Digital

LexID Digital is the technology that brings our digital identity intelligence to life; helping businesses elevate fraud and authentication decisions from a device to a user level as well as unite offline behavior with online intelligence. LexID Digital has the following benefits:

- Bridges online and offline data elements for each transacting user
- Goes beyond just device-based analysis and groups various other entities based on complex associations formed between events
- Consistently identifies a person irrespective of changes in devices, locations or behavior. Intelligence from the Digital Identity Network helps accurately recognize the same returning user behind multiple devices, email addresses, physical addresses and account names.

Data Processed and Analyzed



Foreword

Overview

Transactions & Attacks

Regional Trends

Evolving Mobile Trends

Conclusion

From the 17B transactions processed in the second half of 2018, LexisNexis® Risk Solutions uses subsets to conduct detailed analysis.

Bot attacks and sophisticated attacks:

- LexisNexis Risk Solutions differentiates between simple threats, like automated bots (2.8B) and human-initiated/sophisticated attacks (244M).
- For the sophisticated attacks, LexisNexis Risk Solutions considers a subset of 10.3B of the 17B transactions - categorized as known sessions related to individual events.
- This excludes a variety of events; for example, high volume bot traffic (bad and good/tolerated bots, such as auction bots), events that failed to gather any digital intelligence due to unsuccessful profiling and customers with attack rates considered to be outliers.





Foreword



Overview



Transactions & Attacks



Regional Trends



Evolving Mobile Trends



Conclusion

For more information:

risk.lexisnexis.com/FIM-EN

Americas:

+1 408 200 5755

+1 800 953 2877

EMEA:

+44 203 2392 601

APAC:

+61 2 9411 4499



About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com

About ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time.

LexisNexis, LexisNexis, LexID, and the Knowledge Burst logo are registered trademarks of RELX. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Copyright © 2019 LexisNexis Risk Solutions.

Learn more at www.risk.lexisnexis.com/fraud. NXR14118-00-1019-EN-US

