
LexisNexis®
RISK SOLUTIONS
ThreatMetrix®
EMEA
CYBERCRIME REPORT
Global Insights from the ThreatMetrix®
Digital Identity Network®

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Foreword

The EMEA region is a patchwork quilt of cultures and languages, defined as much by its diversity as by the commonalities shared by geographical proximity. These unique factors create a complex cybercrime landscape that continues to be shaped by evolving consumer behavior, economic growth and technological development. This is evidenced by the transaction trends and attack patterns seen in the ThreatMetrix® Digital Identity Network® during the first quarter of 2019.

At the same time the region is in the midst of huge regulatory reform. One year on from GDPR and on the cusp of the Strong Customer Authentication (SCA) mandate for PSD2, businesses are being forced to address customer security, streamlined authentication and fraud control in equal measure.

The handling of personal information is now front and centre of the consumer psyche. Since the advent of GDPR in May 2018, the BBC reports that there have been nearly 90,000 notifications of data breaches and over 140,000 complaints from the public across EU countries that have implemented the regulation.

Consumers now have more control over their data than ever before – a real game-changer for companies that historically developed their own corporate privacy policies. As reports on data breaches and fake news stories fuel headlines across the world, consumers are now demanding a greater say in how their data will be used. Trust and brand loyalty, in addition to large fines, are key risks for companies who violate the privacy of today's consumer.

At the same time PSD2 is mandating that financial services organizations more rigorously authenticate the identities of consumers accessing account services and making payments, presenting a further challenge around how personal data is collected, stored and verified. This is an interesting paradox when the regulation is also seeking to promote open banking.

It has been over a decade since Clive Humby was credited as saying that 'data is the new oil', but the analogy still holds true today. However, the ownership of, and responsibility for, data is returning to the consumer, despite the fact that businesses are under greater scrutiny than ever before to differentiate between trusted consumers and bad actors.

This continues to drive a metronomic tension between security and streamlined access to online goods and services, with businesses constantly balancing the somewhat competing demands of effective fraud detection and low user friction. Consumers do not expect the care of their personal data, or strong authentication strategies, to come at the expense of laborious identity verification processes or unnecessary step ups. Likewise, businesses must continue to protect and prioritize the interests of vulnerable customers who may be more susceptible to unwittingly sharing their personal data or less able to authenticate themselves via the usual channels.

This is particularly important given cybercriminals are in a continual drive to modify their attack methods to target new weaknesses. In many cases this path of least resistance is not a vulnerability in online processes, but comes from consumers themselves. They are unwittingly becoming involved in pitch perfect scams that lead to them divulging personal credentials, downloading malware or allowing remote access, thereby giving the fraudster unfettered access to personal accounts and customer data. Education, along with clear messaging at key points in the customer journey – such as at the point a user initiates a new payment - becomes an important part of the journey towards better awareness and account protection. Likewise, banks must ensure that vulnerable customers are not left exposed.

Organizations that succeed in this landscape of robust regulatory reform, diverse consumer behavior and complex fraud will be those that can accurately differentiate consumers from fraudsters in real time, layering low-friction authentication solutions that promote rather than hinder a streamlined user experience.

This relies on having a single user view across the entire consumer journey; combining physical and digital identity verification, authentication and fraud detection capabilities so that businesses can truly know their customer, wherever, whenever and however they choose to interact.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Report Overview

The ThreatMetrix EMEA Cybercrime Report: Q1 2019 is based on cybercrime attacks detected by the ThreatMetrix Digital Identity Network (The Network) from January – March 2019, during real-time analysis of consumer interactions across the online journey, from new account creations, to logins and payments.

- The ThreatMetrix Digital Identity Network provides unique insight into transaction patterns and emerging cybercrime threats.
- These transactions are analyzed for legitimacy based on hundreds of attributes, including device identification, geolocation, previous history and behavioural 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, leveraging global rules within bespoke policies that are custom-tuned specifically for their businesses.
- Attacks discussed are from "high-risk" transactions scored by ThreatMetrix customers.
- ThreatMetrix processed 3.1 billion transactions in EMEA during Q1 2019, with 71% originating from a mobile device, one of the highest figures of all regions globally.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

EMEA in Numbers: Q1 2019

EMEA | Rest of the World

3.1 Billion
Transactions Processed

5.4 Billion

71%
% Mobile Transactions

55%

87 Million
Bot Attacks

235 Million

1.6%
Attack Rate

2.3%

43 Million
Human-initiated Attacks

90 Million

Including

14 Million
Mobile Attacks

38 Million

UK
Biggest Attacker by Volume

US

Key Highlights

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

EMEA represents a less risky online environment than the rest of the world, despite pockets of growing attack rates for some industries and use cases:

- EMEA is one of the most mobile regions in the world, with 71% of transactions originating from a mobile device, compared to 55% globally. This is one of the key factors that drives a lower overall attack rate in the region, given that mobile transactions in our Network remain significantly safer than desktop transactions overall. Mobile transactions in EMEA are attacked at a rate of 0.7%, while desktop transactions are attacked at a rate of 3.8%.
- However, there is also evidence in the ThreatMetrix Network that fraudsters are adapting to changing consumer behavior as transaction volume shifts to mobile; turning their attention towards mobile attacks. Attacks on new account creations from the mobile channel in media, for example, have increased 41% year-on-year in EMEA.

Evidence continues to support a strong pattern of highly organized, networked cybercrime:

ThreatMetrix has detected a number of instances where fraudsters are working across organizations both within the same industry, and across different industries, in order to:

- Maximize the monetization of stolen credentials
- Use a network of fraudulent bank accounts to launder money from, for example, other bank accounts, credit cards, loans or fintech providers
- Reduce the likelihood of detection by working multiple fraudulent accounts simultaneously

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

The ThreatMetrix® Identity Abuse Index

The ThreatMetrix® Identity Abuse Index shows the percentage of attacks per day across the entire ThreatMetrix Network, mapping the peaks and troughs in attack patterns over the quarter. This can help highlight 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.

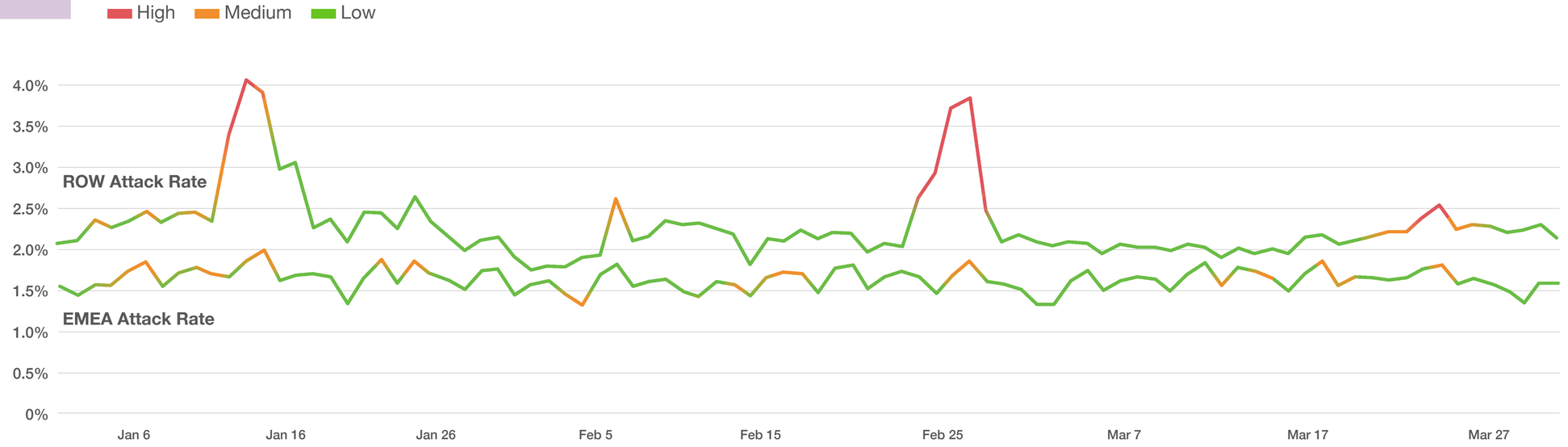
At times, breached identity data may manifest in increased attacks on The Network before a breach has even been discovered or reported, indicating that fraudsters see the time immediately after a breach as the most lucrative period for launching an attack.

In Q1 2019, The Network recorded two significant peaks in attacks globally. However, these were far less noticeable in the EMEA region. The attack peak in January was targeting a global e-commerce merchant, with attacks coming from US, Canada, Chile and Switzerland; while the peak in February was dominated by an attack on a multinational bank, specifically originating in the US.

In EMEA, attack rates are more stable across the quarter, but nevertheless follow similar peaks and troughs to global trends, with smaller peaks recorded at the same time as the global attacks in January and February. This indicates that attacks often have a global footprint, despite originating from diverse 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 across all transactions, this shows that the exploitation of stolen identity information is disseminating to all global geographies in an organized and comprehensive way and resulting in networked, worldwide attacks.

Identity Abuse Index EMEA vs Rest of the World



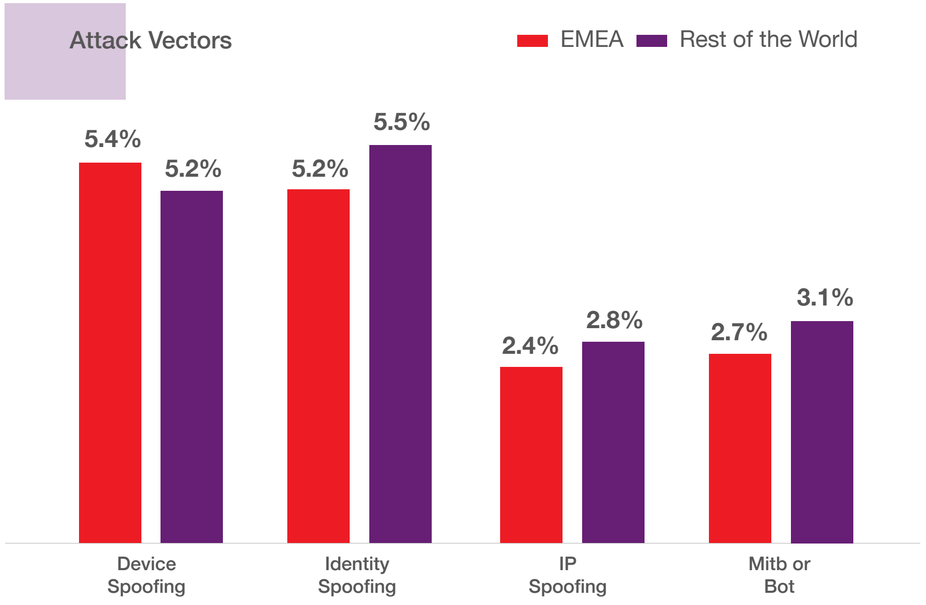
Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Transaction Patterns & Attack Rates in the EMEA Region

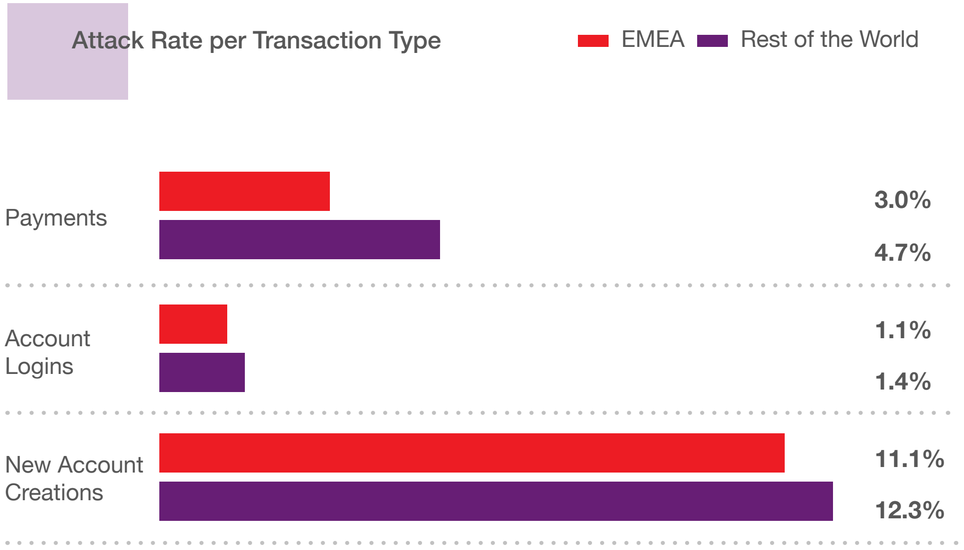
ThreatMetrix transactions span the full spectrum of global industries, from e-commerce, financial services and media, to gaming and gambling, telco and insurance. ThreatMetrix protects transactions across the entire customer journey, from digital onboarding, to streamlining logins, verifying password resets/change of details and authenticating payments.

Attack patterns in EMEA are broadly consistent with the rest of the world, albeit the attack rate is lower. Logins remain the safest transaction type, while new account creations are the most risky transaction, attacked at a rate of more than one in ten transactions.

Interestingly, device spoofing is more prevalent in EMEA than in the rest of the world. This may be when a fraudster is using a virtual machine to impersonate a good customer device, or when a fraudster is attempting to bypass normal device fingerprinting techniques, for example by repeatedly wiping cookies, or using a jailbroken or rooted phone. EMEA transactions have a higher percentage of events coming from jailbroken and rooted phones in comparison to the rest of the world.



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



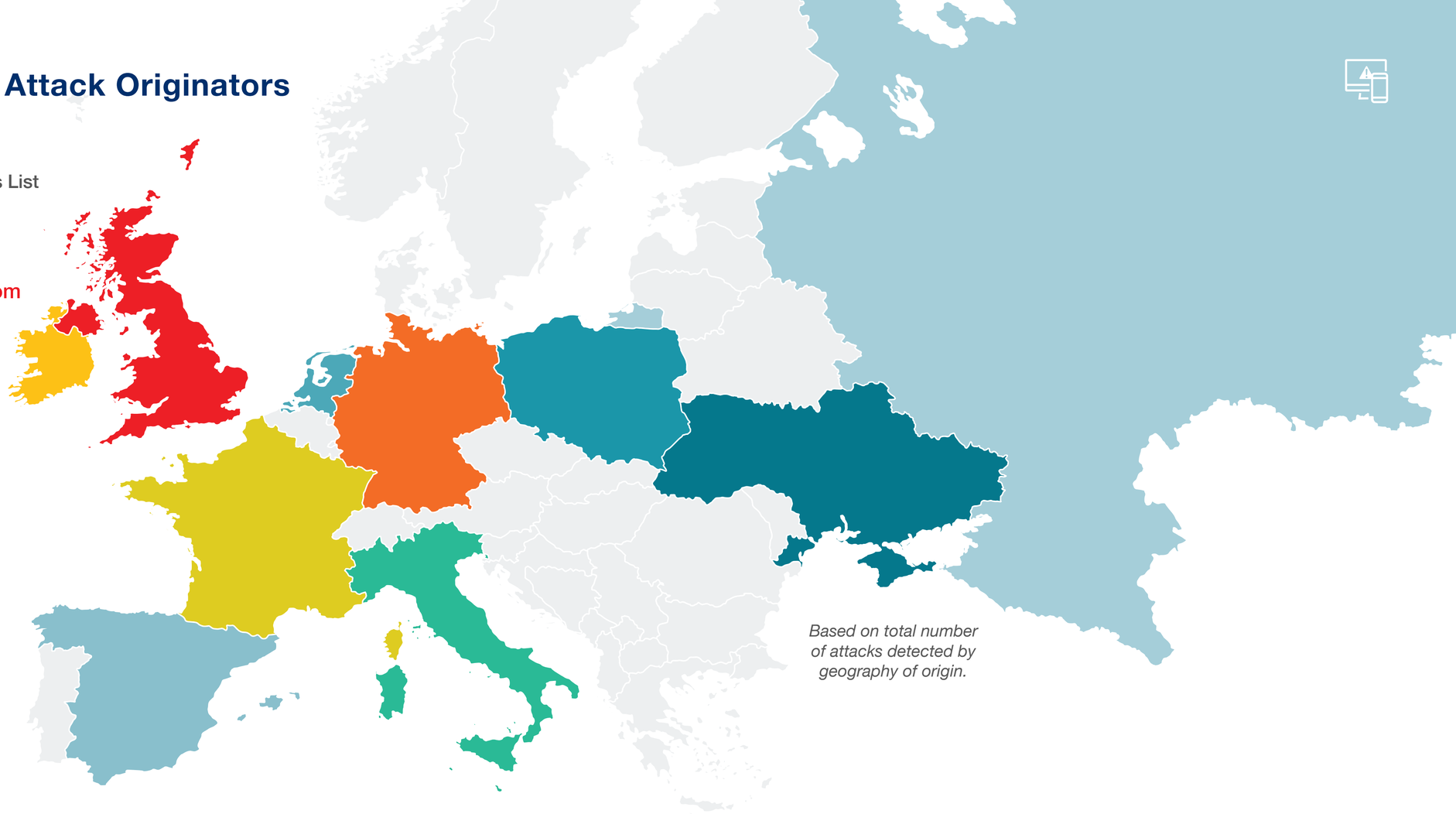
Attack rate is based on percentage of transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically and in real time depending on individual customer use cases.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

EMEA Top Attack Originators

Top 10 Attackers List

#1 United Kingdom
#2 Germany
#3 Ireland
#4 France
#5 Italy
#6 Russia
#7 Spain
#8 Netherlands
#9 Poland
#10 Ukraine



Based on total number of attacks detected by geography of origin.

The economic powerhouses of the United Kingdom and Germany are the top two cybercrime attackers by volume in EMEA. Likewise Ireland, France and Italy are often in the top five attackers list, indicating that a booming digital economy often goes hand-in-hand with a significant cybercrime industry.

However, the inclusion of countries like Poland and the Ukraine indicate that growth and emerging economies are increasingly making their mark on the cybercrime world stage. Mirroring worldwide trends, this highlights the widespread dissemination of breached identity data to countries across the globe.

Regardless of origin, there is a common methodology of fraudsters trying to hide within high volume digital traffic, or seeking to exploit new vulnerabilities in emerging fintech processes as digital economies grow and develop globally.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Cybercrime Risks Across the Customer Journey in EMEA, Q1 2019

New Account Creations

Attack Rate Per Industry

15.9%	E-commerce	
1.4%	Financial Services	
13.1%	Media	

RISK

- High new account creation attack rate in both e-commerce and media as fraudsters use these industries as test beds for stolen identity credentials, often via automated bot attacks.
- E-commerce transactions from EMEA see a higher attack rate than ROW.

Logins

Attack Rate Per Industry

3.2%	E-commerce	
0.7%	Financial Services	
1.7%	Media	

RISK

- The percentage of e-commerce login attacks on mobile is higher than desktop for EMEA, and growing in comparison to Q4 2018.
- Growth in mobile account takeovers in media as a result of bot activity.

Payments

Attack Rate Per Industry

3.1%	E-commerce	
3.1%	Financial Services	
2.2%	Media	

RISK

- Growth in mobile payments across all industries, particularly financial services.
- Some peaks in payment attacks on media organizations, testing stolen credit cards.

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.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

E-commerce New Account Creations at Heightened Risk

E-commerce

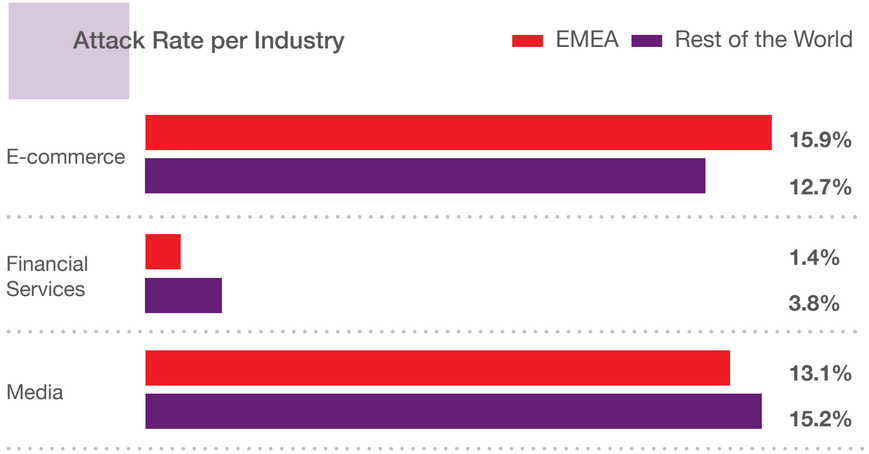
- Mirroring global trends, e-commerce merchants in EMEA see a high rate of new account creation attacks, with the attack rate in EMEA exceeding that of the ROW.
- Q1 2019 saw a growth in the attack rate on mobile new account creations for e-commerce merchants.
- Many of these attempted account creations are fraudsters testing stolen credentials via automated bot attacks.

Financial Services

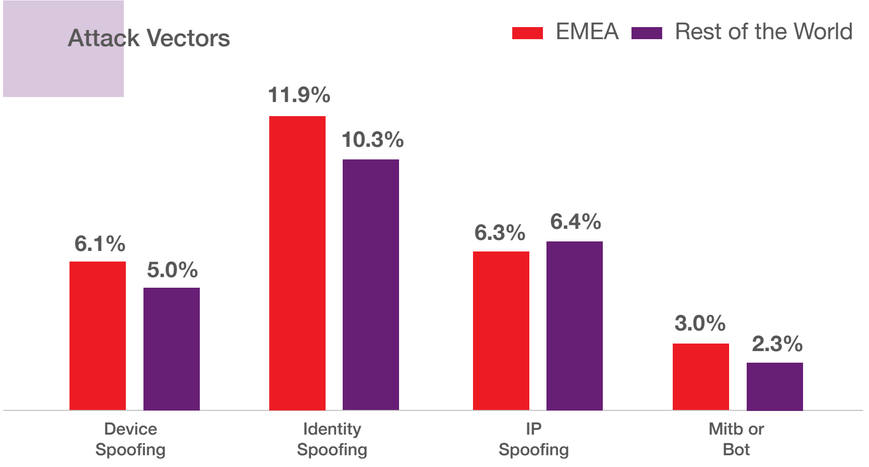
- The new account creation attack rate is lower in EMEA than in ROW.
- Attack rates in EMEA are falling year-on-year, driven by market maturity and a prioritization of digital-first processes for new products and services.
- Meanwhile attack rates in ROW are growing, in part driven by vulnerabilities in North America from recent social security compromises which have fueled applications using spoofed identity credentials.

Media

- The attack rate on media new account creations is slightly lower in EMEA than ROW.
- The attack rate from the mobile channel is increasing 41% YOY in EMEA.
- This is likely driven by the fact that media sees the highest penetration of mobile new account creations at 69%, and fraudsters are therefore following suit by targeting this volume shift.



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 bar chart represents the percentage of total transactions that were recognized as attacks.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Evidence of Growth in Account Takeovers on the Mobile Channel

E-commerce

- The overall attack rate for e-commerce logins is lower in EMEA than globally.
- However, the attack rate on mobile transactions specifically is higher in EMEA than ROW.
- E-commerce sees a significantly lower percentage of mobile login transactions in comparison to other industries.

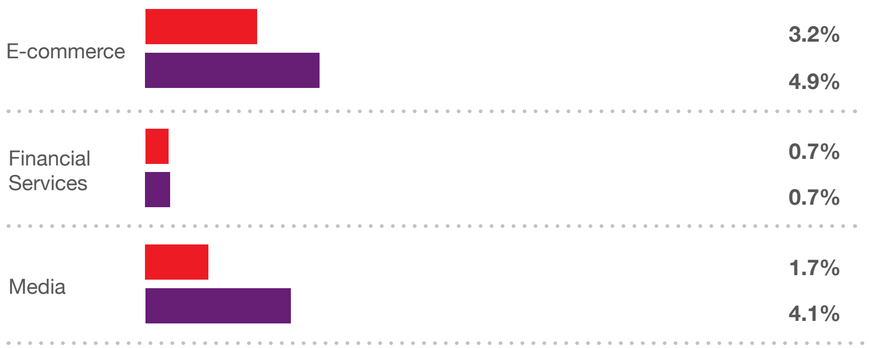
Financial Services

- Financial services logins in EMEA see one of the highest percentages of mobile transactions, of any use case or region, at 84%. This far outstrips the ROW figure of 57% and is largely driven by full service mobile banking apps.
- The attack rate on these mobile transactions remains extremely low, at 0.1% due to ongoing advances made in financial services fraud protection.
- This has also shifted fraud towards lower volume, higher value social engineering attacks.

Media

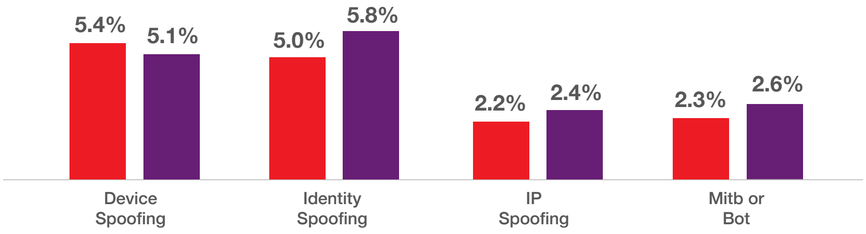
- Media logins are attacked at a lower rate in comparison to the ROW. This may be due, in part, to the fact that the percentage of mobile transactions is much higher in EMEA, and these tend to be safer than desktop transactions.
- However, there is a small growth in account takeovers from the mobile channel in EMEA in comparison to last quarter. Some of these account takeovers are from mobile bots.

Attack Rate per Industry



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.

Attack Vectors



The bar chart represents the percentage of total transactions that were recognized as attacks.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

EMEA Payments Safer than ROW, with Mobile Payments Growing Across all Industries

E-commerce

- E-commerce payment transactions have a strong mobile footprint, at 61%, compared to 55% for the ROW.
- This perhaps explains the slightly lower attack rate in EMEA in comparison to ROW.

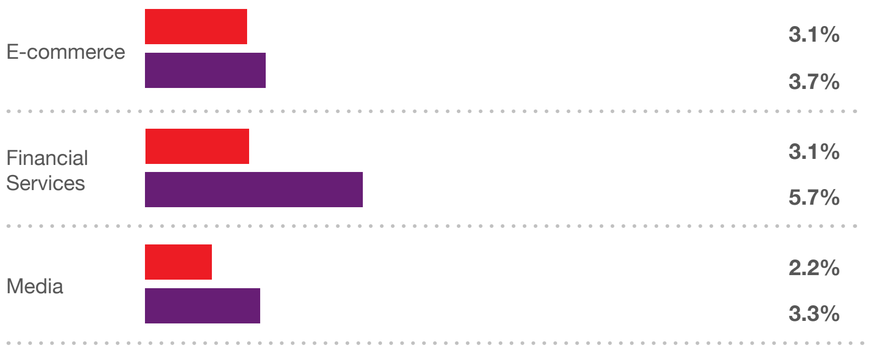
Financial Services

- Financial services payments in EMEA are attacked at a lower rate in comparison to the ROW.
- This is perhaps explained by the prevalence of financial transactions via full service mobile banking apps which can leverage the in-built security features of mobile devices for authentication.

Media

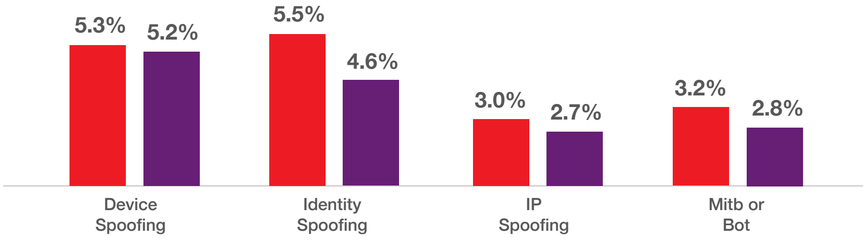
- Media payments in EMEA see a very high prevalence of mobile transactions at 81%, higher than the global figure of 77%.
- Attack rates are subsequently low, and reasonably stable. Fraudsters also likely see e-commerce and financial services organizations as a more lucrative target for extracting money than media companies.

Attack Rate per Industry



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.

Attack Vectors

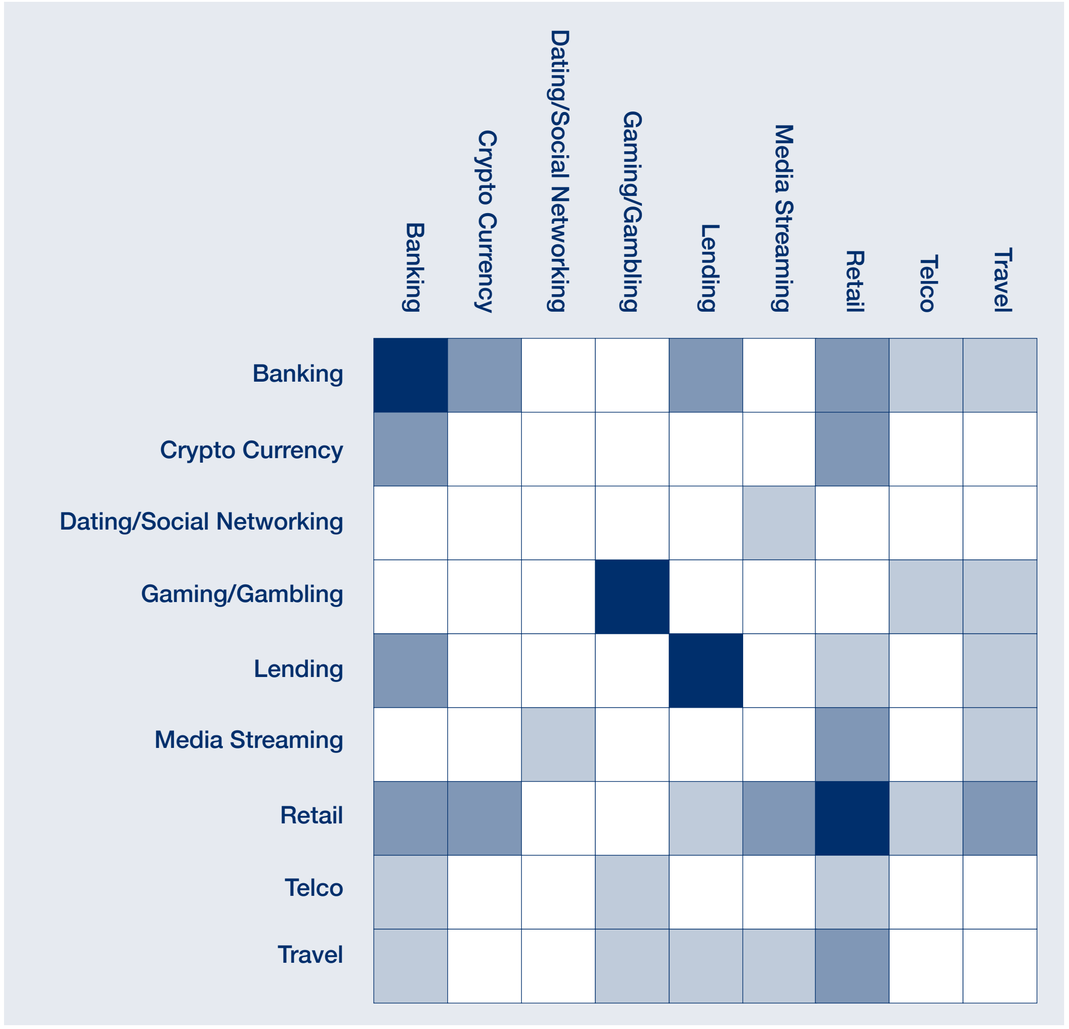


The bar chart represents the percentage of total transactions that were recognized as attacks.

Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

The Growing Threat of Networked Cybercrime

Heat Map Showing Level of Shared Fraud Across Organizations



Within the ThreatMetrix Network, there is a strong footprint of cross-organizational and cross-industry fraud.

This is seen when digital identities are associated with confirmed fraud attempts by more than one organization within The Network.

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

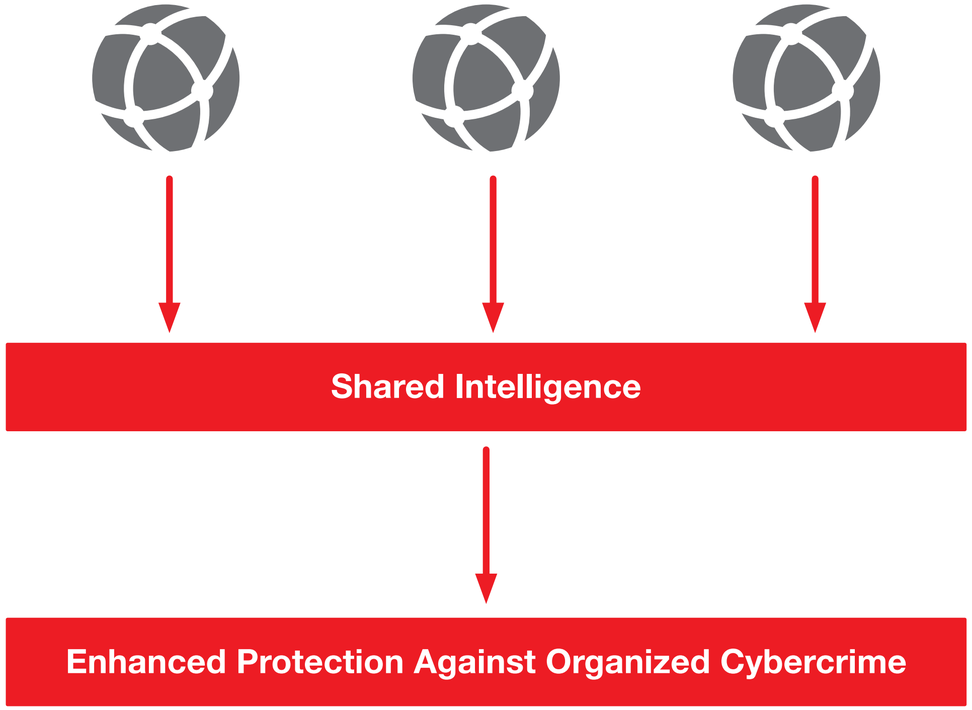
Examples of cross-organizational attack patterns that ThreatMetrix encounters in The Network include:

- A criminal working across a number of UK banks, operating multiple mule accounts to siphon proceeds of crime.
- Patterns of fraudulent activity across media, financial services and payments providers to maximize the monetization of stolen credentials.

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

Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

ThreatMetrix Consortium Facilitates Trusted Data Sharing to Help Businesses Detect and Block Fraudsters Operating Across Organizations



- Consortium allows ThreatMetrix customers to share information to collectively fight fraud.
- Consortium creates an industry-focused, peer-based layer that complements an organization's local intelligence and the global shared intelligence harnessed through the ThreatMetrix Digital Identity Network.
- This enables businesses with common goals, challenges or fraud risks to share their negative and positive data attributes in real time, across an agreed set of Consortium members and contributors.
- It also allows for more targeted real-time risk assessments, while maintaining logical separation of Consortium member data.
- Organizations can see greater context within the data; understanding, for example, which other organization has blacklisted a device and why. This insight supports smarter and more contextualized fraud decisions.
- Businesses can also create targeted lists for different use cases, for example, account takeover and mule detection.

Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

Tracking a Fraudster Across Multiple Organizations and Industries

One EMEA Fraudster Operating out of East London

Using One Device but Attempting to Bypass Device Fingerprinting

Media Company

- Fraudster logs in to account at Media Company – suspected account takeover
- Fraudster attempts two new account creations in quick succession, from the same email address
- These are flagged as high-risk and blocked
- **This information could be accessed by other organizations to detect future high-risk behavior**

Bank A

- Fraudster goes to Bank A and carries out two logins on two different accounts, neither of which are flagged as high-risk
- **Context from previous interactions with the media company could alert Bank A to potential high-risk scenarios**

Bank B

- Fraudster then goes to Bank B and attempts a series of account takeovers
- The Fraudster also attempts to transfer funds out of victims' accounts
- These transactions are detected as high-risk and blocked
- **Further fraudulent activity at Bank B could be shared within a trusted consortium of organizations**

Payments Company

- Fraudster makes a payment at payment company
- Transaction is flagged as neutral and not stopped
- **Payment company may choose to block these transactions with more context on previous high-risk behavior**

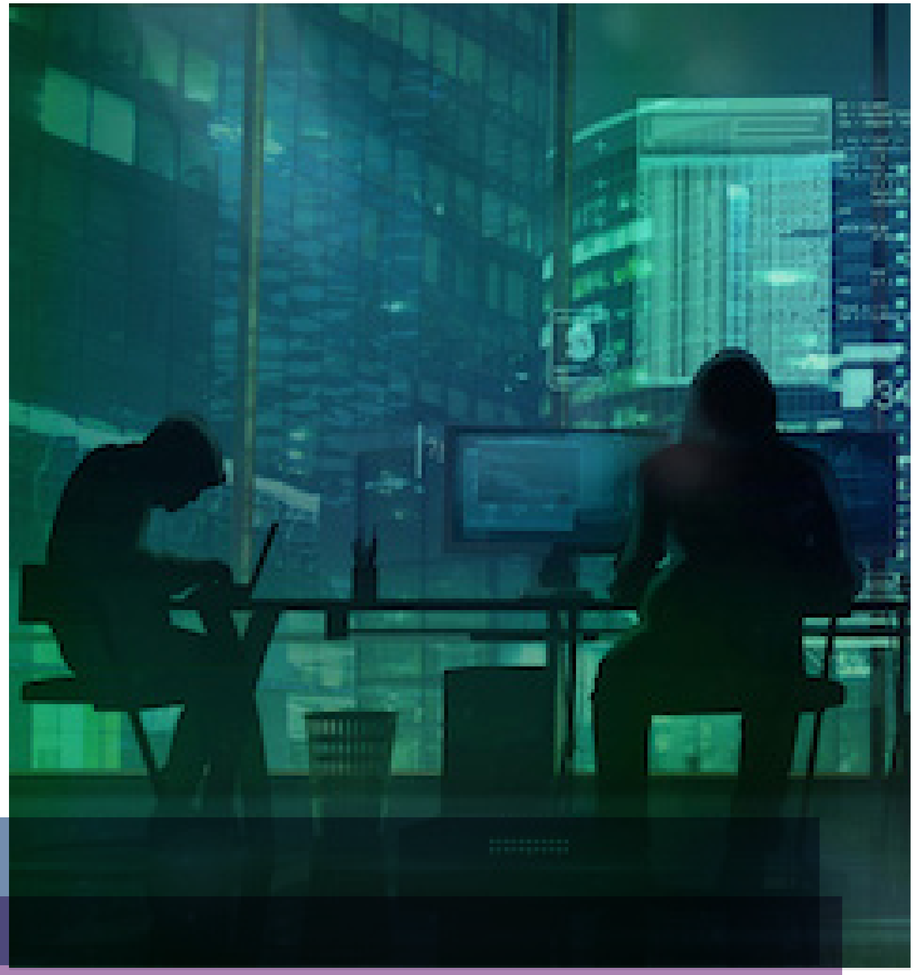
Fintech FS Provider

- Fraudster attempts to sign up for four new accounts over a period of two days, with an FS provider offering credit products
- Fraudster uses four different email addresses. Transactions are all blocked
- **Repeated high-risk behavior could add richer behavioral context to intelligence shared between organizations**

The Power of The Digital Identity Network enables organizations to tag and share anonymized intelligence related to high-risk behavior in real time, benefitting from a shared view of risk.

Tracking the Path of a Fraudster Across the UK Banking Network

Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion



Fraudster:

- One fraudster operating out of Portugal and Nigeria.

Target:

- 4 UK banks and money transfer company.

Method:

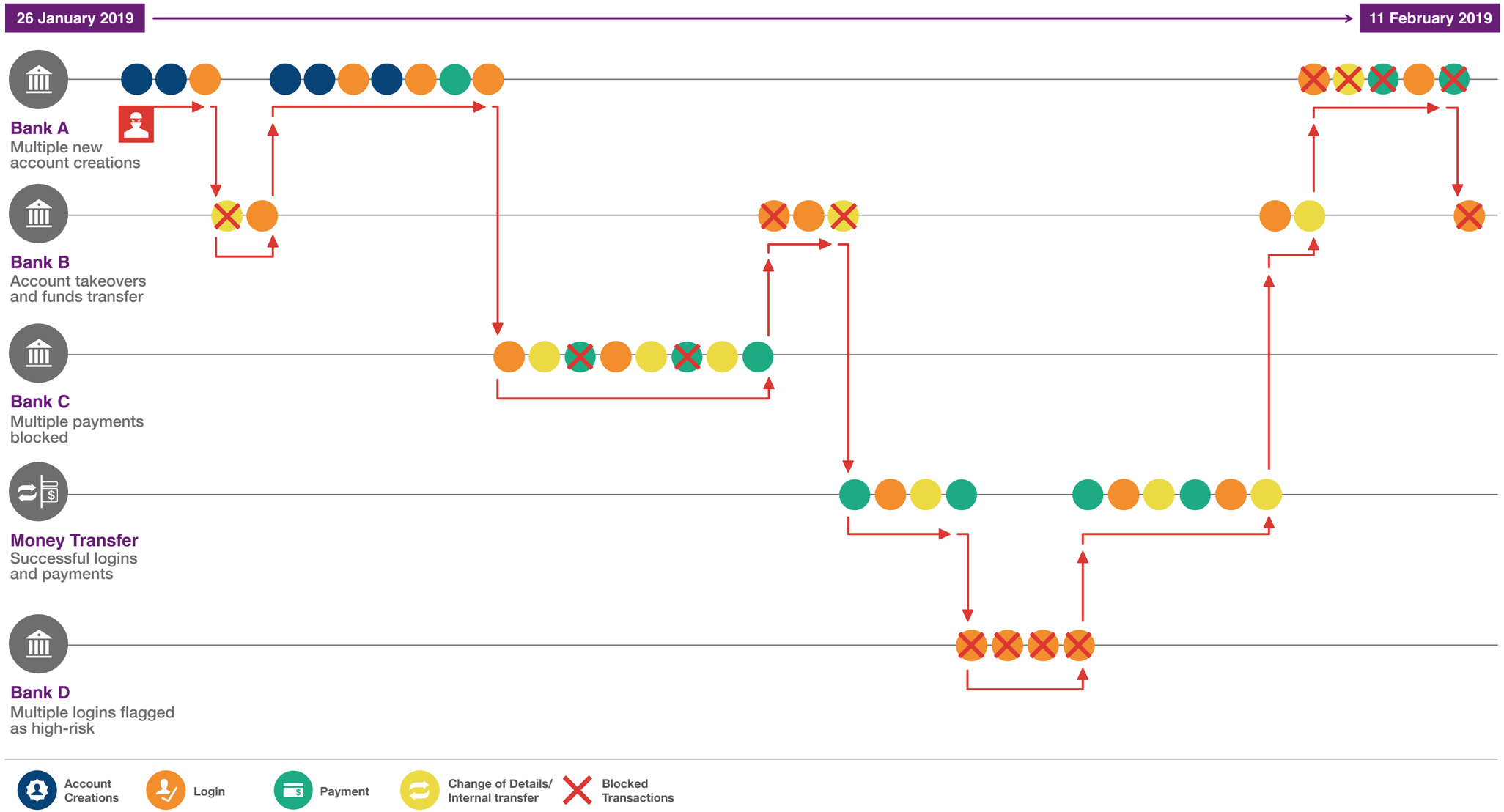
- Fraudster used one device but was attempting to bypass device fingerprinting.
- Fraudster carried out multiple fraudulent transactions across 5 different organizations to launder money and avoid detection.
- While some of these these transactions were flagged as high-risk, or blocked as fraud, some were processed.

ThreatMetrix Digital Identity Network Benefit

- The power of The Digital Identity Network enables organizations to tag and share anonymized intelligence related to high-risk behavior in real time, benefitting from a shared view of risk.
- The power of a trusted Consortium enables organizations to share specific data related to known fraudulent devices / mule accounts, for example, across a defined group of UK banks.
- ThreatMetrix customers manage their own risks, tailoring rules to their own risk appetite.
- Persistent device recognition provides a common identifier across the Network.
- A unified Digital Identity enables fraudsters to be tracked across devices, locations and credentials.
- Leveraging customer performance and feedback informs better and more dynamic decisions.

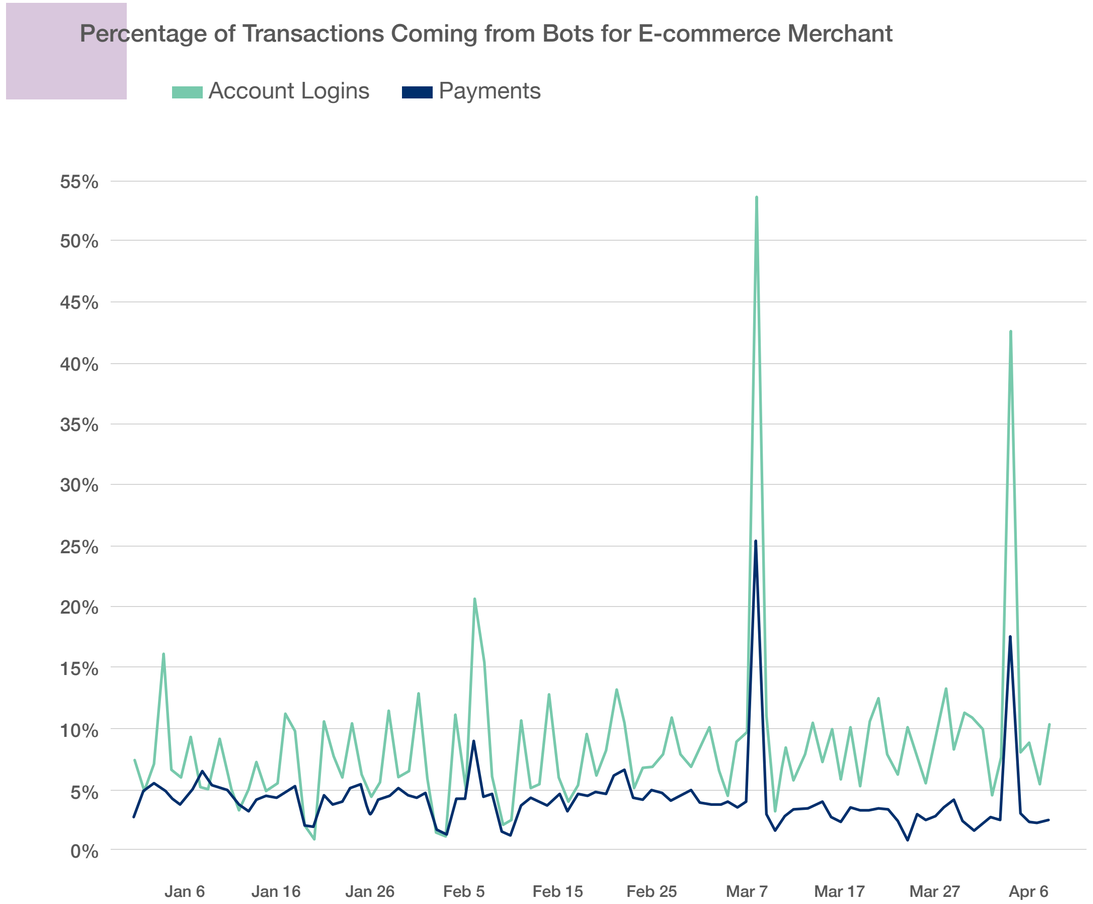
Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

Tracking the Path of a Fraudster Across the UK Banking Network



Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

Attack Spotlight: Large Bot Attack from Netherlands Targets European E-commerce Merchant



Fraudster:

- Bot Operator in the Netherlands

Target:

- French e-commerce merchant

Method:

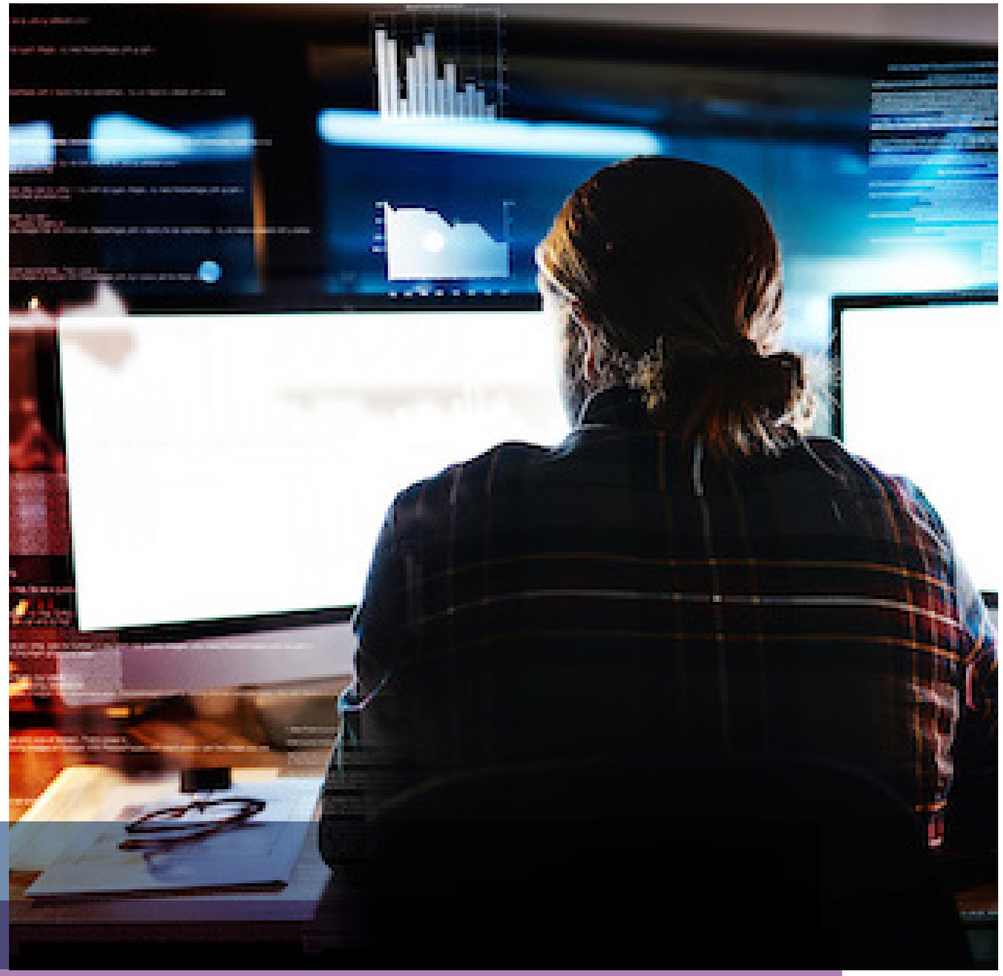
- High velocity attacks targeting payments, using either stolen credit cards or existing customer accounts to access a saved card on file.

Attack:

- 80,000 payments attempted from 55,000 accounts in one day.
- Evidence shows the bot operator continually adapted the attack method to try and avoid detection, by reducing the payment value.
- This technique was also trying to reduce the likelihood of step-up authentication.

Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

Attack Spotlight: Multinational Bank Uncovers Fraudulent Behaviour By Linking Multiple New Account Creations to One Single Location



Fraudster:

- One cybercriminal targeting out of hours activity from the same location, with a layered use of devices and accounts.

Target:

- Multinational Bank

Method:

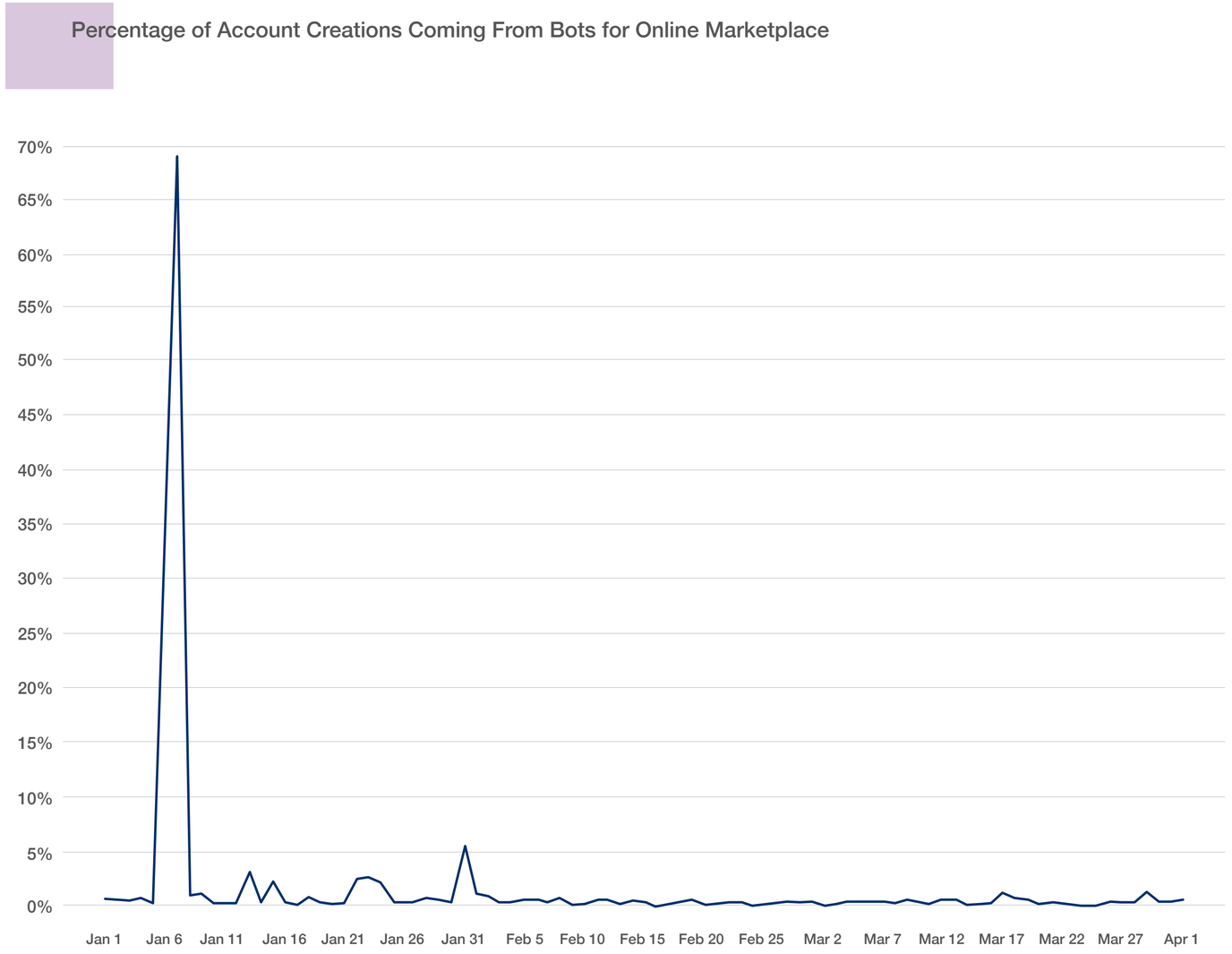
- Account takeover of existing customer accounts to make fraudulent payments.

Attack:

- Over a 4-week period, the fraudster used multiple devices to access multiple good customer accounts, so that the fraud could not be tied back to a single device.
- A number of new accounts were also registered.
- Over 200 payments were made to 27 beneficiary accounts.
- The fraud was detected by identifying behavioural anomalies and linking the underlying data of the network connection to prove that the fraud was coming from one unique location.
- Proving the value of an open visibility of network data and contextual insights.

Foreword
Overview
Transactions & Attacks
Fraud Typologies
Mobile
Region Spotlight
Conclusion

Attack Spotlight: Online Marketplace Targeted by Russian Bots Attempting to Open Fraudulent New Accounts



Fraudster:

- Bot Attacker in Russia

Target:

- European Online Marketplace

Method:

- Fraudster attempts to create multiple fraudulent new accounts through high velocity credential testing.

Attack:

- The bot operator attempted almost 30,000 new account creations using a small number of devices / IP addresses, but testing multiple stolen email addresses. At times this volume made up 70% of all daily account creation traffic for the merchant.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Mobile Reward & Risk: EMEA Leads the World in Mobile Transacting, But Fraudsters Are Following Suit

Mobile Financial Services Transactions

In EMEA, 4 in every 5 financial services transactions come from a mobile device, driven by mature, full service mobile banking apps.

80% vs **57%**

EMEA — Rest of the World

Mobile vs Desktop Attack Rate

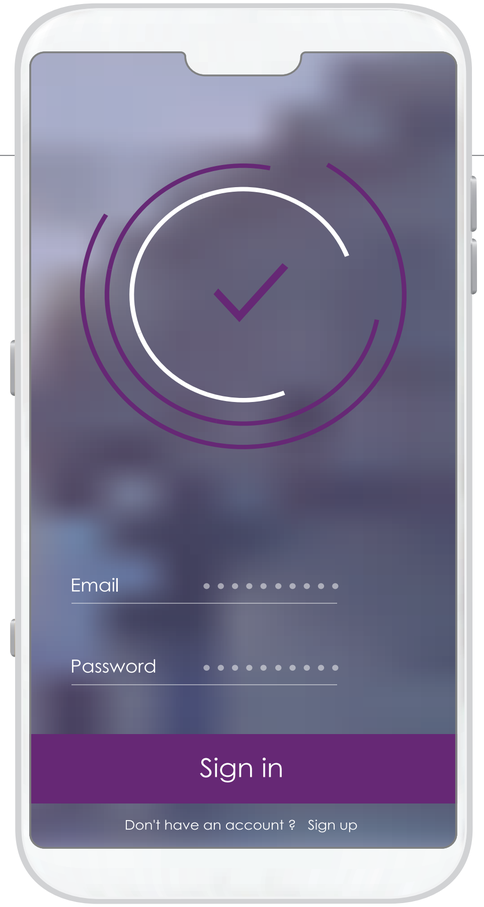
Transacting on a mobile remains safer than via a desktop; desktop transactions are attacked 5X more than mobile ones.

0.7% Mobile vs **3.8%** Desktop

Media

Media industry sees greatest risk from growth in attacks on the mobile channel, as fraudsters follow the behavioural shift of consumers.

41% growth in mobile new account creations YoY



Mobile vs Desktop Volume per Transaction Type

Mobile Desktop

Login transactions have strongest mobile footprint, as full service apps drive quick and simple account checking.

Foreword
Overview
Regional Trends & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Region Spotlight: UK and Continental Europe

UK Rest of Europe

2.2 Billion
Transactions Processed
0.8 Billion

80%
% Mobile Transactions
43%

0.4%
Attack Rate
4.7%

8 Million
Human-initiated Attacks
30 Million

Including
3.5 Million
Mobile Attacks
8 Million

UK 8M
Biggest Attackers by Volume
Germany 6M

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

UK's Advanced Digital Economy Drives High Mobile Penetration and Lower Attack Rates

Mike Hulett, head of operations at Britain's National Cyber Crime Unit estimated that in 2017, around half of all fraud in the UK involved an element of cyber, illustrating just how deeply entrenched cybercrime is in UK digital business.

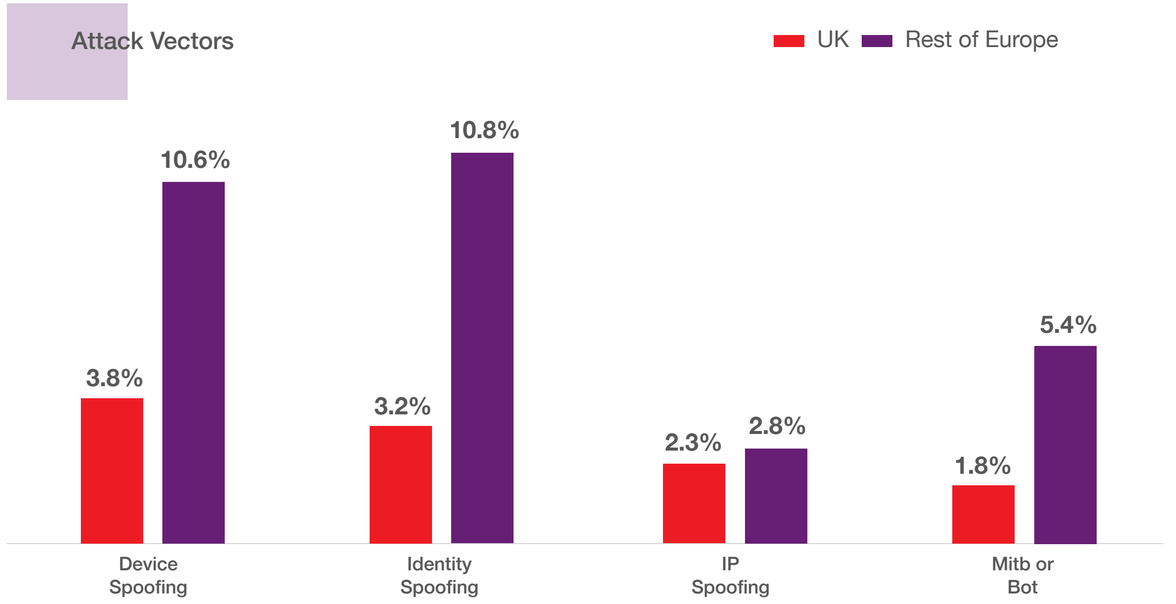
As a result, the UK has some of the most advanced cybersecurity strategies globally, focusing as much on identifying the behavioural patterns of good, trusted customers as blocking fraudsters. This means that unusual and high-risk behavior can be more easily identified in real time.

As the online digital economy continues to grow and replace many traditional forms of brick and mortar / in-person commerce, organizations have had to place greater emphasis on the security of customer credentials, robust digital identity verification, low-friction authentication and effective fraud control.

This likely contributes to the lower overall attack rates in the UK. Desktop transactions in the UK are attacked at a rate of 1.2%, versus 6% in Continental Europe. Mobile transactions are attacked at a rate of 0.2% versus 2.9% in Continental Europe. In part this is driven by high volumes of login transactions – growing 61% YOY - which enable companies to build accurate and detailed profiles of good customers, making it easier to detect high-risk behaviour in real time.

Continental Europe sees a much stronger prevalence of device spoofing, identity spoofing and bot attacks in comparison to the UK, indicating that the UK's strong investment and relative maturity in fraud, identity proofing and authentication strategies is paying off.

However, the simplicity of this lower attack rate story potentially belies the complexity of the cybercrime landscape in the UK, which continues to succumb to complex networks of mules, sophisticated scams that trick unwitting consumers to become complicit in divulging sensitive credentials and evolving mobile attacks.



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

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Conclusion

While theories abound about how fraudsters are set to test defences as we approach the PSD2 deadline for Strong Customer Authentication, trends and patterns uncovered in the EMEA region set some level of expectation about what organizations can expect to see globally.

While some growth economies of Eastern Europe are taking their place on the European cybercrime stage, the economic powerhouses of the UK and Germany continue to be the biggest originators of cyberattacks by sheer volume.

EMEA continues to outpace the rest of the world when it comes to mobile transaction penetration. This plays a contributory role in lower overall attack rates given that mobile transactions are attacked less than desktop ones. However, the dominance of mobile transacting is something of a double-edged sword. Fraudsters are seeing some new opportunities in the volume shift to mobile; looking to hide within the growing volume of good customer traffic. This is resulting in notable pockets of attack growth, for example on new account creations in media.

The identification of networked, cross-organizational, cross-industry fraud indicates just how complex an industry cybercrime has become in its own right. Fraudsters are looking for ways to maximize monetary gain and minimize detection, all the while posing as legitimate and trusted customers. This often means working across multiple banks, juggling several mule accounts simultaneously, and siphoning proceeds of crime across a complex network.

Single point solutions are unlikely to succeed in winning this war against such networked, globally-connected cybercrime. Fraudsters are playing businesses at their own game; 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 defence 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, physical identity and authentication capabilities that can help businesses meet regulatory requirements, streamline the customer experience and detect complex and evolving fraud.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Glossary

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 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.

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. 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.

ThreatMetrix ID™

ThreatMetrix ID™ 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. ThreatMetrix ID 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 Network helps accurately recognize the same returning user behind multiple devices, email addresses, physical addresses and account names.

Foreword
Overview
Transactions & Attacks
Industry Trends
Mobile
Region Spotlight
Conclusion

Data Processed and Analyzed

From the 3.1 billion transactions processed from EMEA in Q1 2019, ThreatMetrix uses subsets to conduct detailed analysis.

Differentiating between automated bot attacks and sophisticated human-initiated attacks:

- ThreatMetrix differentiates between simple threats, like automated bots (78 million) and human-initiated/ sophisticated attacks (43 million) based on the profiling data within our Network.
- For the sophisticated attacks, ThreatMetrix considers a subset of 2.7 billion of the 3.1 billion transactions. These are 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
Industry Trends
Mobile
Region Spotlight
Conclusion

Contact

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

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

Toronto
Exchange Tower, 130 King Street West,
Suite 1804,
Toronto, Ontario, M5X 1E3, Canada

London
99 Bishopsgate, 3rd Floor
London, EC2M 3AL, United Kingdom
Telephone: +44 (0) 20 3239 2601

Brazil
Rua Bela Cintra, 1200 – 5to piso
CEP 01415-000 Bela Vista,
Sao Paulo – SP
+55 11 4862 3824

Mexico
Paseo de la Reforma 243, P15
Edificio Mapfre
06500 Cuauhtemoc, Mexico City
+52 55 4755 0043

Paris
ThreatMetrix c/o Elsevier
65, rue Camille Desmoulins
92130 Issy-les-Moulineaux
France
Telephone: + 33 1 71 16 55 00

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

Munich
Theresienhöhe 28
80339, Munich
Germany
Telephone: +49 89 24440 7057

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

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

Singapore
3 Killiney Road,
#08-08 Winsland House 1
Singapore 239519

Hong Kong
Telephone: +852 36 698 341

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

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

Partners
Email: partners@threatmetrix.com

Public Relations
Email: pr@threatmetrix.com

LexisNexis® RISK SOLUTIONS | ThreatMetrix®

ThreatMetrix® — now LexisNexis® Risk Solutions, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymized digital identities, ThreatMetrix ID™ delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time. ThreatMetrix is recognized as the sole leader in the 2017 Forrester Wave for risk-based authentication.

For more information, or a demonstration of how the ThreatMetrix solution can work for your business, contact us at:

T +1 408.200.5755
F +1 408.200.5799

sales@threatmetrix.com
www.threatmetrix.com