WMC GLOBAL

JPAAWG

Text Messaging Updates: SMS Spam and RCS Safety

Jaclyn Abrams
VP Threat Intelligence
WMC Global

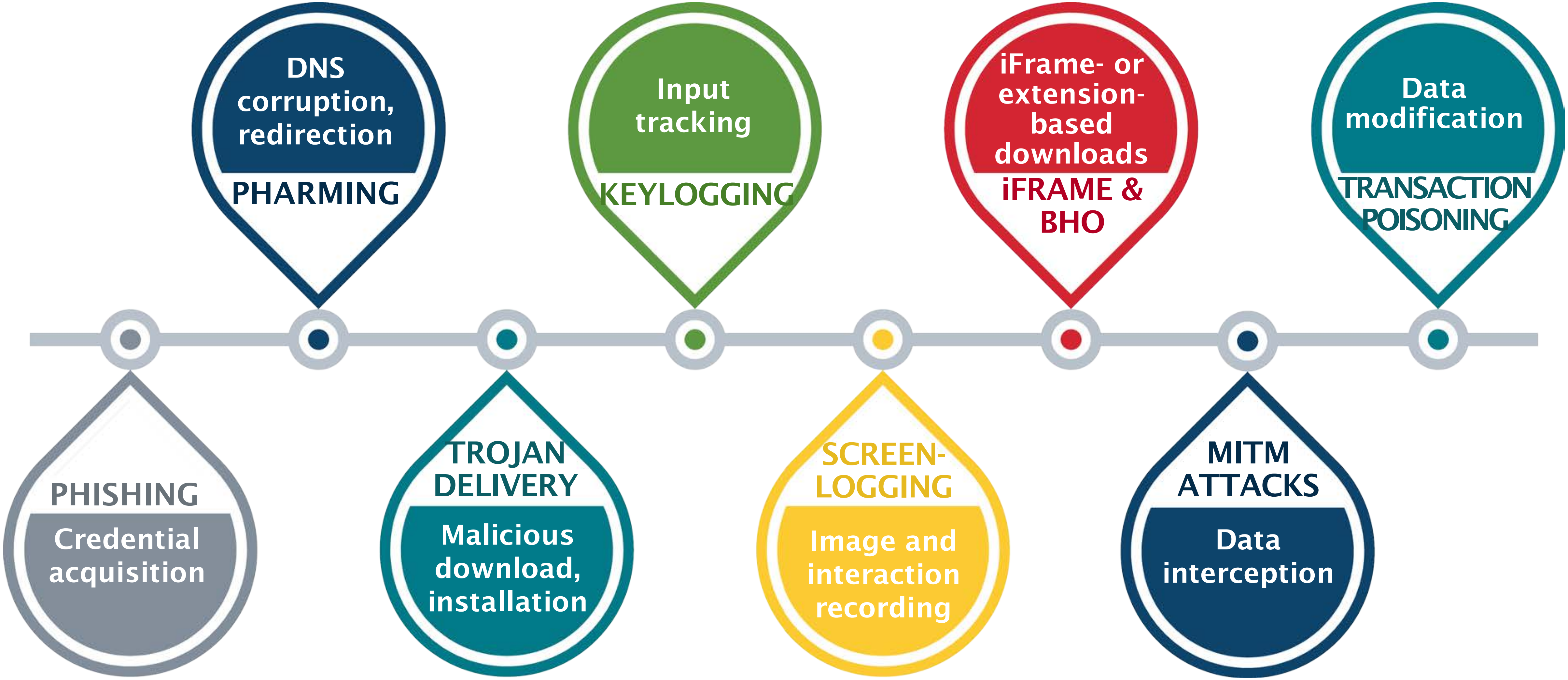
November 7, 2018

TEXT MESSAGING ATTACKS

Update

THREAT TRENDS

Advancing Attack Types



PHISHING
Credential acquisition

PHARMING
DNS corruption, redirection

TROJAN DELIVERY
Malicious download, installation

KEYLOGGING
Input tracking

SCREEN-LOGGING
Image and interaction recording

iFRAME & BHO
iFrame- or extension-based downloads

MITM ATTACKS
Data interception

TRANSACTION POISONING
Data modification

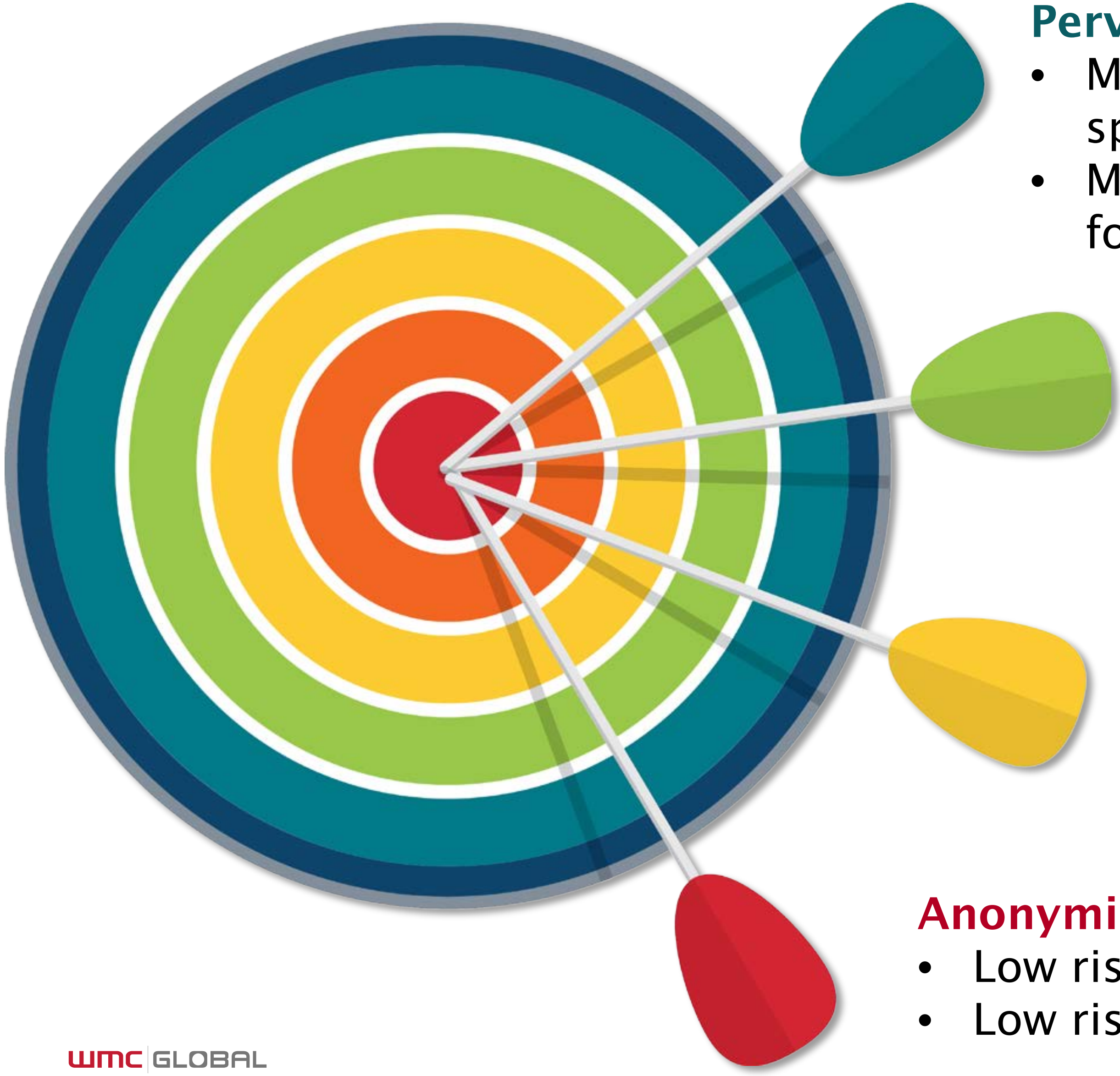
MOBILE SHIFT

Advancing Attack Types

- Email is still the attack delivery vector of choice
  - Corporations use email every day
  - Push media
  - Can carry payloads
  - Easy to spoof
- However, text messages, OTT messaging, and social media are rapidly rising in popularity
  - With the anticipated rise of RCS, text messaging takes on many of the characteristics that makes email so appealing for threat delivery
- Messages—regardless of platform—are only the initiation point for a threat; the real danger occurs once a user engages with the content

MOBILE-TARGETED MESSAGING ATTACKS

SMS is the Gateway to Consumer’s Lives



Pervasiveness

- Mobile accounts for 70% of consumers’ time spent with digital media
- Mobile continues to surpass desktop usage for web access worldwide

Accessibility

- Widely available
- Cross-platform-delivery capable
- Accessible from disparate entry points
- Easy first interaction for various exploits

Cost Effectiveness

- Inexpensive infrastructure
- Scalable
- Repeatable

Anonymity

- Low risk of attribution
- Low risk of retaliation

ATTACK ENTRY POINTS

Shared Codes and Over-the-Top Platforms

Unvetted and Shared Codes

- Grey route to ecosystem entry
- Multiple layers behind registered entities enable obfuscation
  - Enables code swapping
  - Masks actual message senders
  - Enables snowshoeing
- In the last year, abuse on shared codes has skyrocketed as blocking has become more aggressive in other areas

Over-the-Top Platforms

- Entry via Over-the-Top (OTT) platforms offering SMS forwarding options
  - Harder to track OTT account ownership without direct engagement with OTT services
  - Circumvents upfront safeguards and per-code volume caps
  - Facebook and Twitter SMS forwarding are major source of these attacks

ATTACK CATEGORIES

Popular Attack Types

Social Engineering

- Credential phishing
- Fake accounts set up on Facebook, LinkedIn, and Twitter impersonate known individuals within an organization and engage with employees as trusted entities
- Buying and selling scams, especially over Craigslist
- Event and issue-based attacks
  - Lottery jackpots
  - Holidays or major events (sports, elections, etc.)
  - Health care open enrollment periods

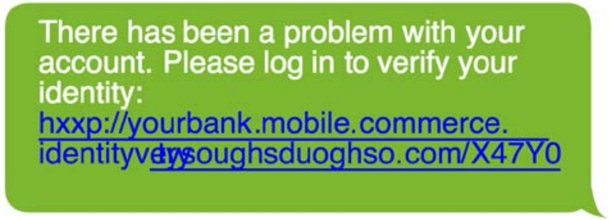
Malware Distribution

- Contributing factors
  - Kaspersky forecasted that espionage will be shifting heavily to mobile and apps
  - Mobile banking has seen a rapid rise in popularity, and is thus a prime target
- SMS used as attack delivery vector, prompting link and media interaction
  - Malware delivery sites
  - Side-loaded apps
  - RCS file transfer
- Bespoke exploit kits can be created to capture specific desired data (e.g., SpyEye)
  - SMS generation and receipt to defeat 2FA

ANATOMY OF AN ATTACK

Core Components

Attack Message



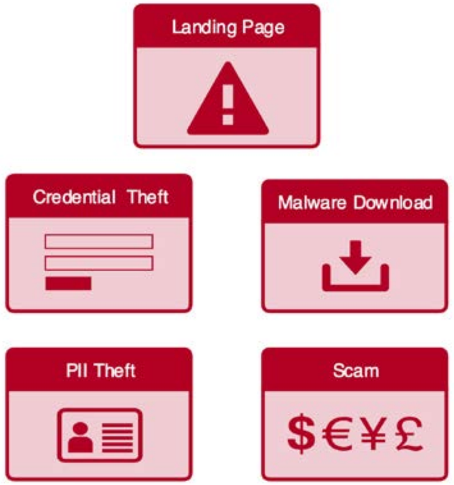
There has been a problem with your account. Please log in to verify your identity: hxxp://yourbank.mobile.commerce.identityvdysoughsduoghso.com/X47Y0

- Variable text generation
- Variable URL generation

Redirects

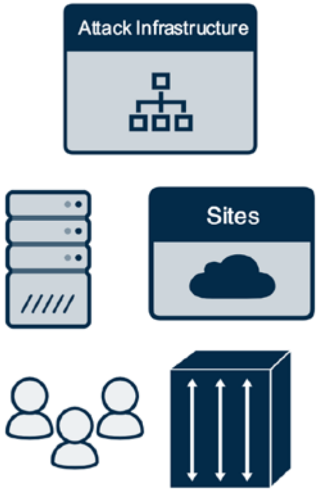
- Variable redirect chain
  - Device
  - Location
  - OS
  - Access time
  - Operator network

Landing Page



- Interaction points
- Data collection
- Malware installation

Supporting Infrastructure



- Sites
- Servers
- Accounts
- IPs

Threat Actor Information

- Identity
- Location
- Contact info
- Relationships

US-TARGETED ATTACKS

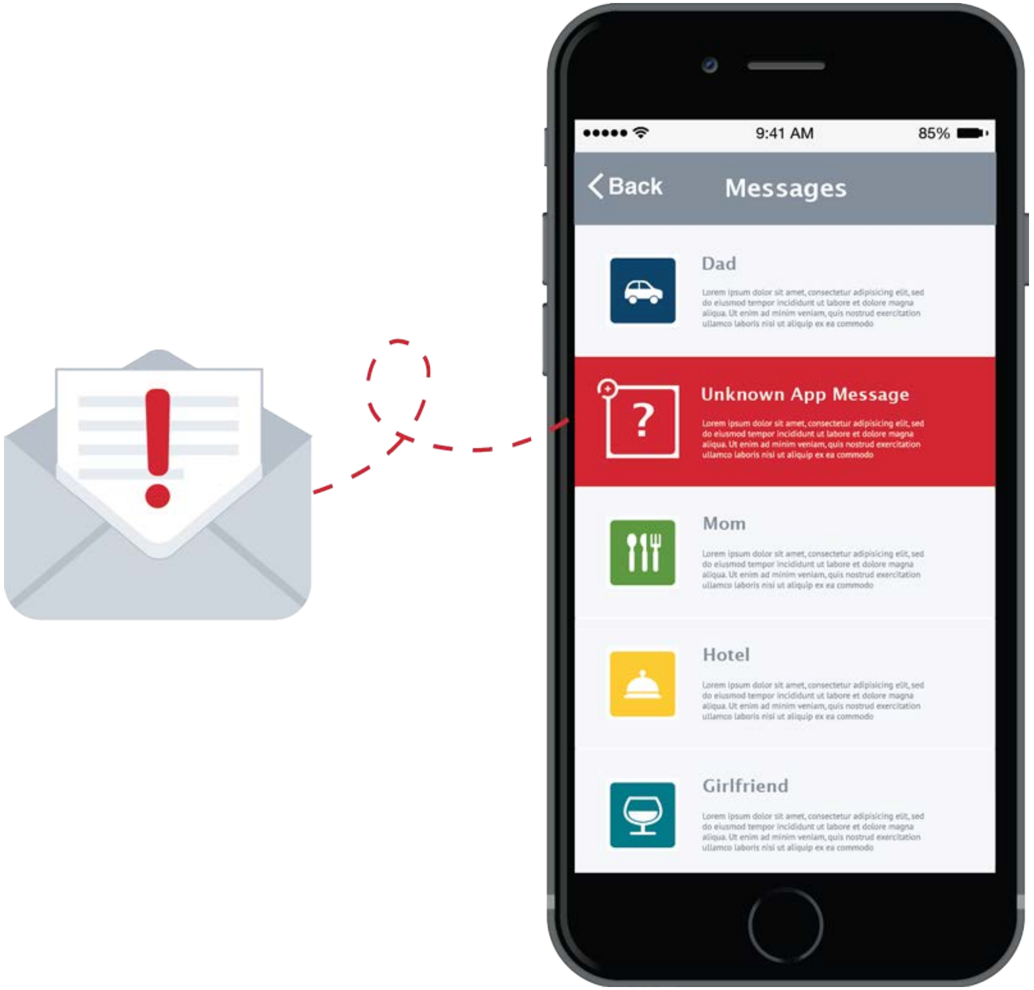
Recent Attacks

- **Political Messages**
  - Not attacks, per se, but high complaint volumes
  - Spikes during election lead-up and periods of high political engagement
- **Socially Engineered Swatting**
  - Messaging sent to multiple recipients threatening bodily harm and containing another phone number, intending to implicate the contained phone number as an involved party
- **Phish Hopper**
  - Pervasive attack targeting major brands
  - Leverages a flexible phishing kit to hop between major brands
    - Facebook
    - Wells Fargo
    - Bank of America
    - Chase
  - Shifts IPs
- **Coinbase Phishing**
  - Increased interest in phishing bitcoin accounts
  - Attacks ramp up over holidays to evade detection
  - Attack shifts domains, IPs, and sending accounts continuously, phasing the transition between infrastructure

JAPAN-TARGETED ATTACKS

Recent Attack Example

- Malware Distribution
  - Sagawa Express-branded attack
    - Urged users to download app-disguised malware
    - Some versions of the attack also collected user PII
    - Malware stole IDs, passwords, and credit card information
    - Malware hijacked devices to send additional smishing messages
- Phishing
  - SMS, email, and fake app attacks targeting LINE, Amazon, MyJCB, AppleID, BitCoin credentials



RCS

Emerging Threats

RCS DEPLOYMENT

Japan Leads the Way

64 Operators Across 45 Countries

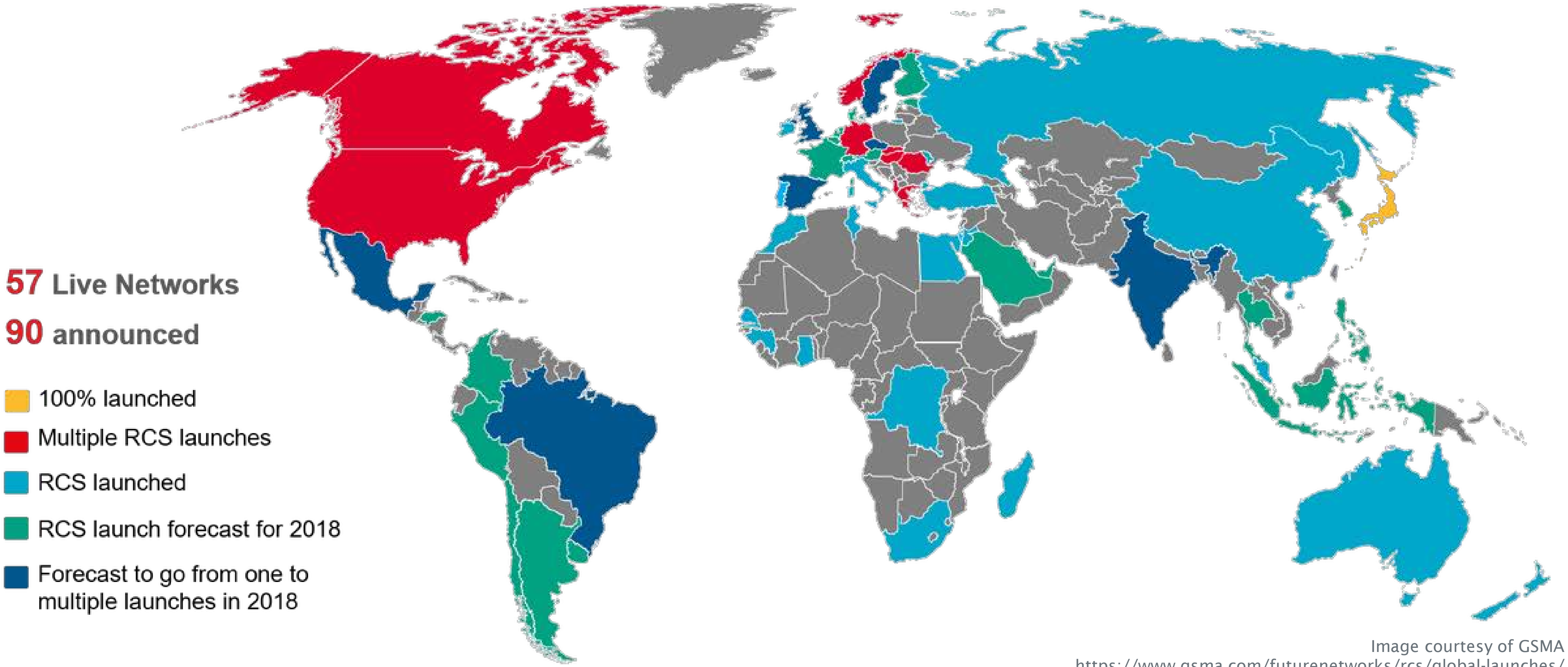

57 Live Networks
90 announced
🟨 100% launched
🟥 Multiple RCS launches
🟦 RCS launched
🟩 RCS launch forecast for 2018
🟦 Forecast to go from one to multiple launches in 2018

Image courtesy of GSMA
https://www.gsma.com/futurenetworks/rcs/global-launches/

RCS CAPABILITIES

Enhanced Experiences and Interactivity

- RCS brings app-like functionality to text messaging
  - Typing indicators
  - Read receipts
  - Link interactions
  - File transfers
  - Interaction components
  - Embedded branding
  - Multi-device messaging
  - Geolocation
- Introduces Messaging as a Platform (MaaP) functionality for A2P Messaging
  - Certified senders with branding and logos
  - Chatbots
  - Rich cards
  - Purchase of items sold by chatbots
  - Privacy controls
  - Spam protections

RCS CAPABILITIES

Examples

Verified Sender

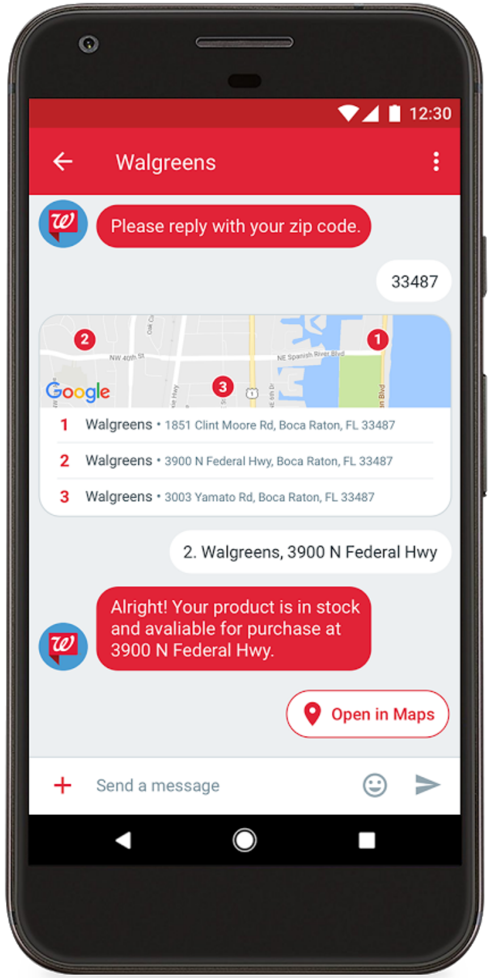
Vetted and identified

Custom Branding

Names, colors, logos

Suggested Actions

URLs, maps, calendars, dialers



Please reply with your zip code.

33487

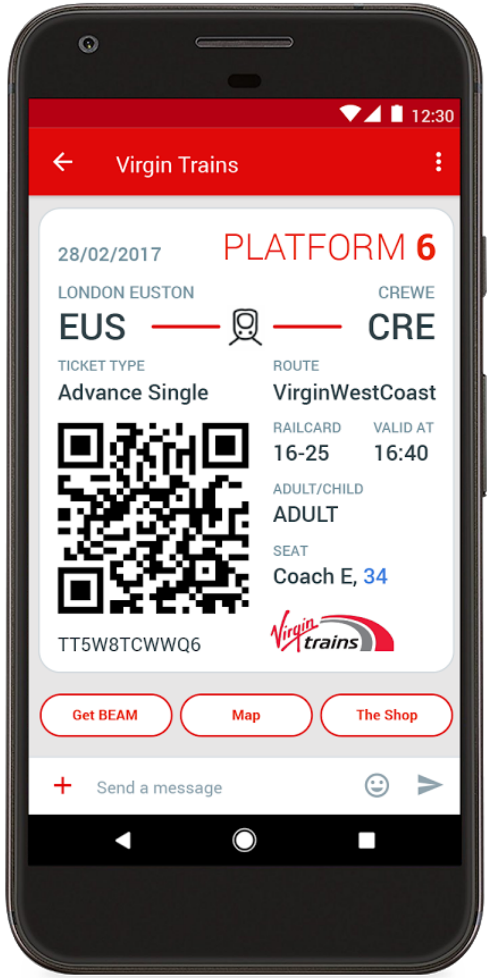
1 Walgreens • 1851 Clint Moore Rd, Boca Raton, FL 33487

2 Walgreens • 3900 N Federal Hwy, Boca Raton, FL 33487

3 Walgreens • 3003 Yamato Rd, Boca Raton, FL 33487

2. Walgreens, 3900 N Federal Hwy

Alright! Your product is in stock and avaliable for purchase at 3900 N Federal Hwy.



28/02/2017 PLATFORM 6

LONDON EUSTON EUS — CREWE CRE

TICKET TYPE: Advance Single

ROUTE: VirginWestCoast

RAILCARD: 16-25

VALID AT: 16:40

ADULT/CHILD: ADULT

SEAT: Coach E, 34

TT5W8TCWWQ6

Rich Cards

Images, videos, GIFs

QR Codes

Tickets, tracking, redemptions

Suggested Replies

Customized response options

Image courtesy of GSMA

RCS SAFETY

Areas for Planning

- **Verified Sender Onboarding**
  - Vetting requirements
  - Verification procedures
  - Proof of identity/impersonation prevention
- **Entity and Message Blocking**
  - Thresholds for blocking implementation
  - Prohibited behaviors
  - Abuse pattern establishment
  - User-level vs. operator-level blocking
- **Abuse Reporting and Spam Control**
  - Recipients
  - Attack data sharing
  - Systems and implementations
- **Interactivity Management**
  - Redirection
  - Downloads
  - File transfers

QUESTIONS?

CONTACT ME

Jaclyn Abrams
VP Threat Intelligence
WMC Global
jaclyn.abrams@wmcglobal.com