



CLOUDMARK®
A PROOFPOINT COMPANY

Phishing/SMiShing/Spam Trends Globally & Best Practices for Protection

Dermot Harnett, Proofpoint, Cloudmark Division
2nd March, 2021

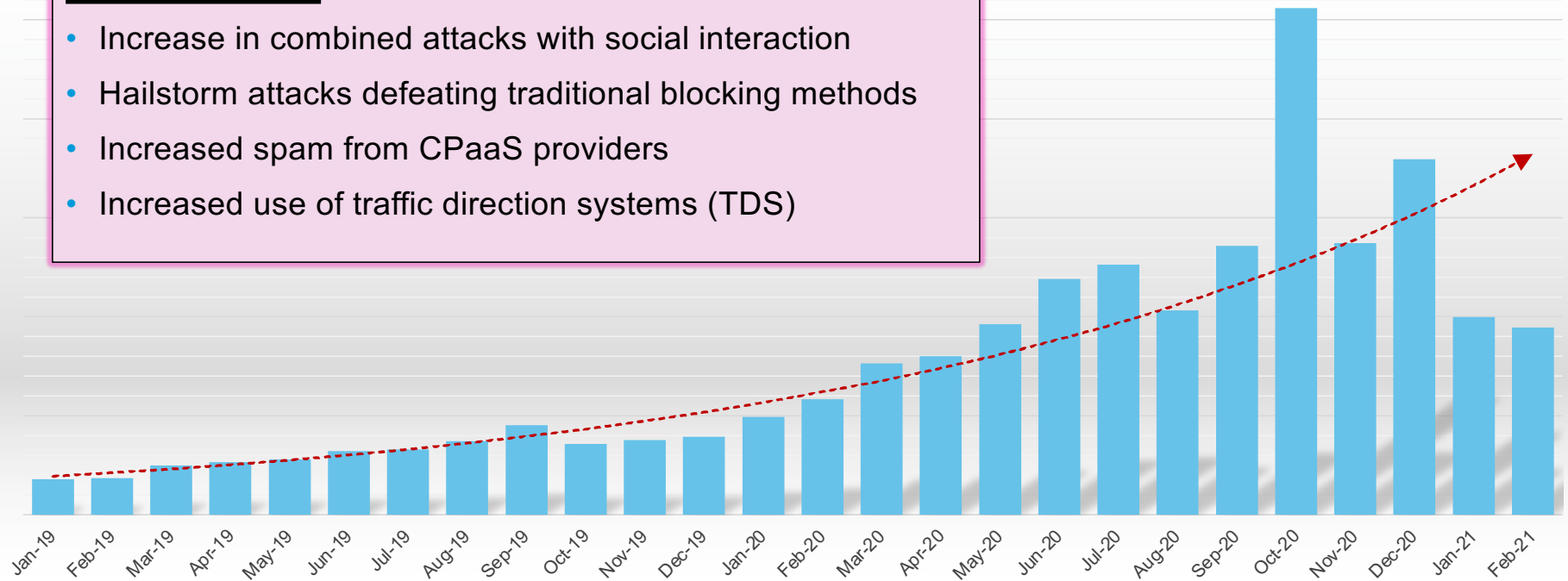
Global Trends

Mobile Spam Reports Continue to Grow

Global Malicious Reports Trend 2019 – current

Growth Drivers

- Increase in combined attacks with social interaction
- Hailstorm attacks defeating traditional blocking methods
- Increased spam from CPaaS providers
- Increased use of traffic direction systems (TDS)



Mobile Abuse Source Diversifying

CPaaS and Aggregator Abuse

- Low barrier to entry
- Multiple new phone numbers can be obtained
- Ease of automation with ability to send messages via an API
- SMS Hyperloop specialize in sending affiliate spam

Rogue Apps Emerging



Money SMS | Make Money Online

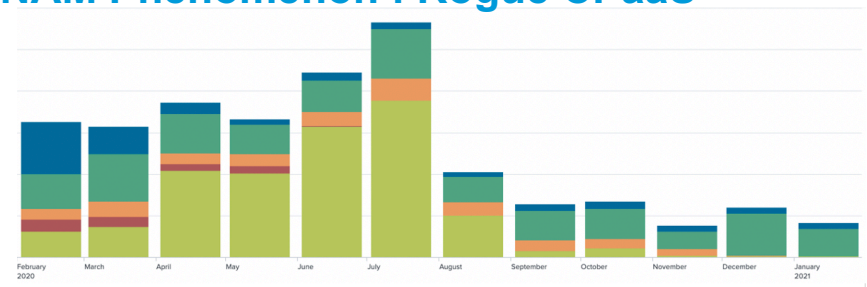
Money SMS Business

★★★★★ 2,835

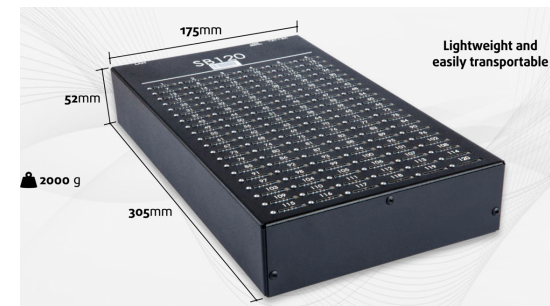
Everyone

Add to Wishlist

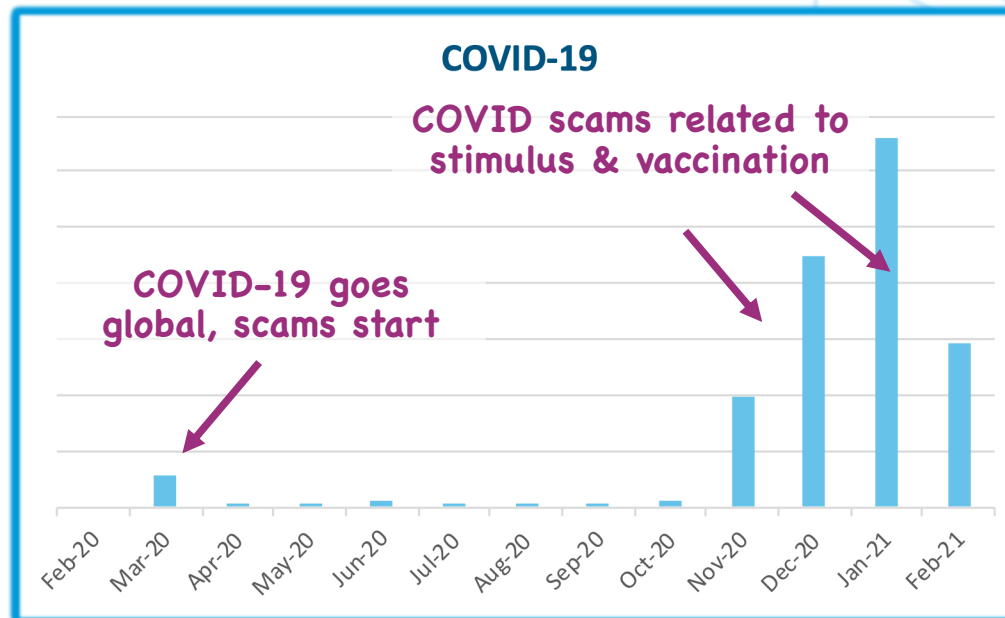
NAM Phenomenon : Rogue CPaaS



Advanced SIM Box Capabilities



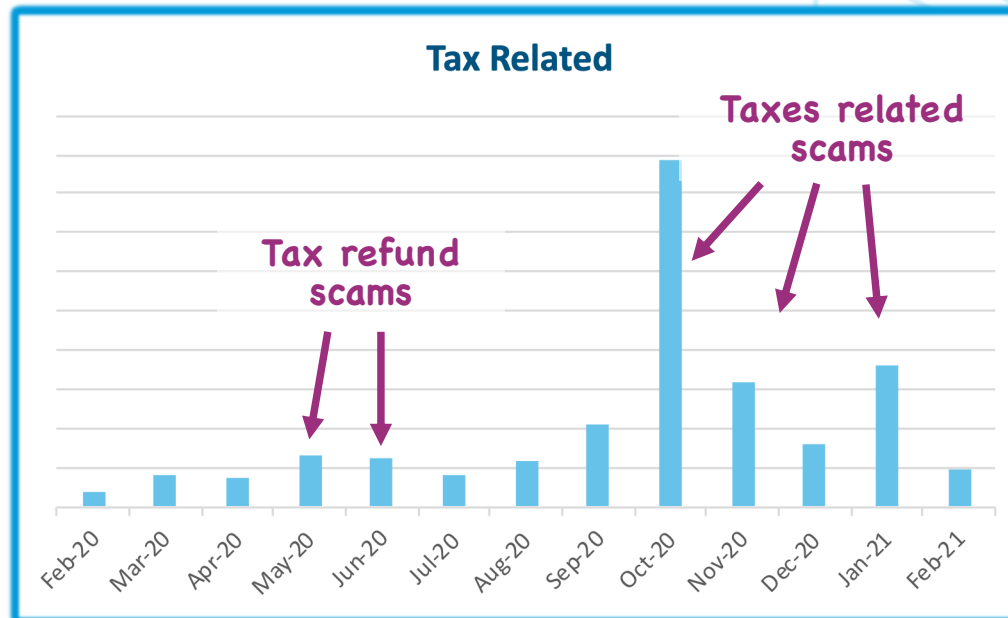
Attacks Leverage Current Events: COVID



Growth Drivers

- First SMS COVID-19 attack observed February 27th, 2020
- 29% of attacks come from suspect Bulletproof hosting CPaaS Vendors
- Note: Attack frequency not shown to scale

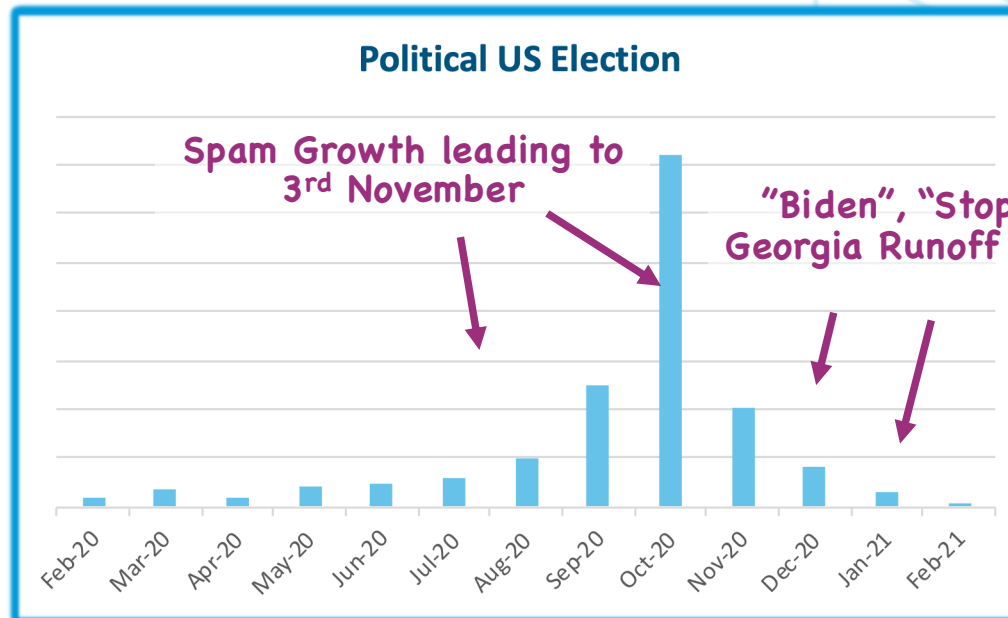
Attacks Leverage Current Events: Taxes



Growth Drivers

- Scammers quick to respond
- Linking lock-down policies to tax rebates, etc.
- Note: Attack frequency not shown to scale

Attacks Leverage Current Events: Politics/Elections



Growth Drivers

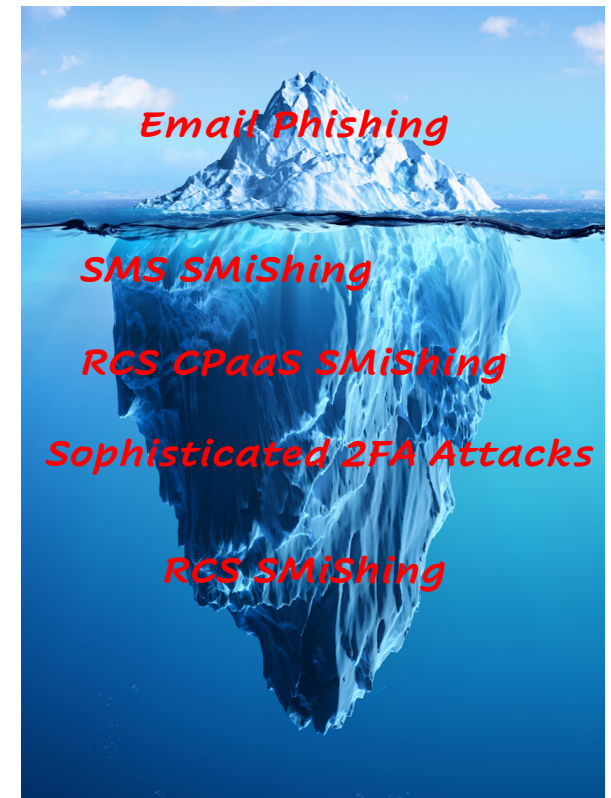
- Elections drove growth in unwanted messaging
- Note: Attack frequency not shown to scale

Attacks Spotlight

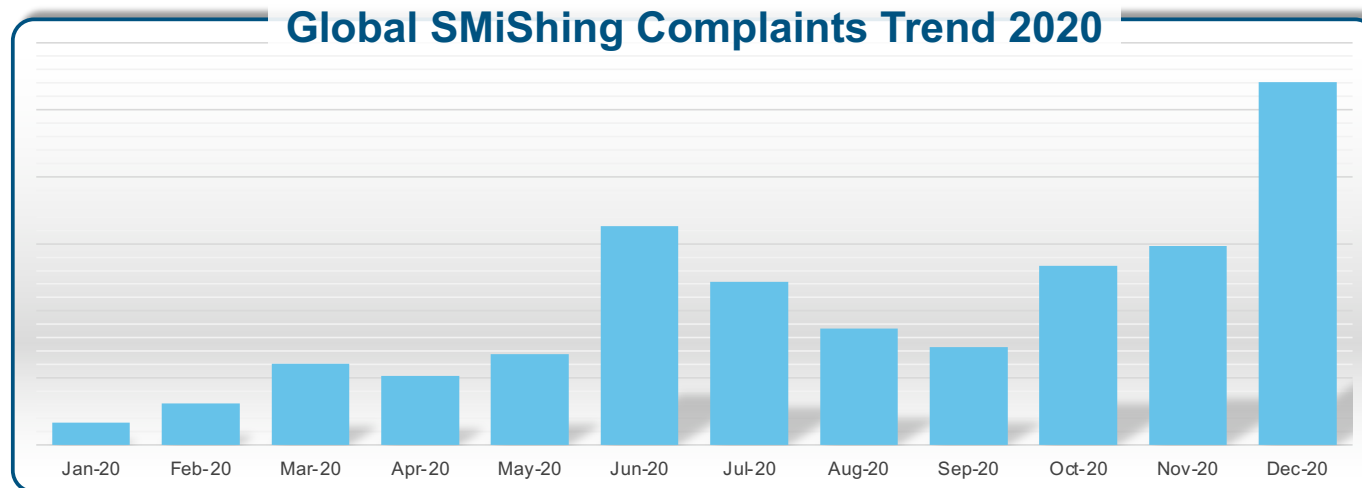
Mobile phishing ("smishing"), Bitcoin ATM
Survey Scam

Mobile Phishing, “SMiShing” Growing Quickly


- High “open rates” – 98% read and 8x CTR of email – means consumers don’t ignore mobile messages
 - Mobile Messaging → fastest growing marketing channel
 - 79% of smartphone users purchase based on mobile comms
 - B2C: 197% channel expansion 2015–2017 & CAGR of 7.2% 2019–2027
 - Fraud and Identity threat are rapidly increasing
 - 72% of adults are unfamiliar with SMiShing
 - Initially targeting financial institutions, now high-profile brands like Apple, Amazon, H&M, Lloyds, Walmart ... targeted
- **If subscriber trust erodes, commercial use and forecasted growth will evaporate**



Global SMiShing Complaints Increasing Significantly



Global Growth Drivers

- Mobile Phishing  328%
- 36% from CPaaS providers and aggregators
- COVID-19 fuels growth in smishing
- Recent phishing study showed 50% of attack originated from proxies

Global SMiShing Variations

Attack Type	Example	UK Top Bank SMiSh Reports	US Top Bank SMiSh Reports
Attack Type 1 – typosquatting	ALERT:Account locked for verification visit http://bbofa.online/n	> 1 %	5 %
Attack Type 2 – smishing with brand name in URL	Bank of America : Did you request a funds transfer for \$6,017 on 12/05? Confirm : http://B0fa1x.app.link	90 %	26 %
Attack Type 3 – generic smishing, name drop in message	BOFA -BANKINGAccount suspension, review immediately: http://9nh06.app.link	9 %	69 %

Global SMiShing Complaints Increasing Significantly



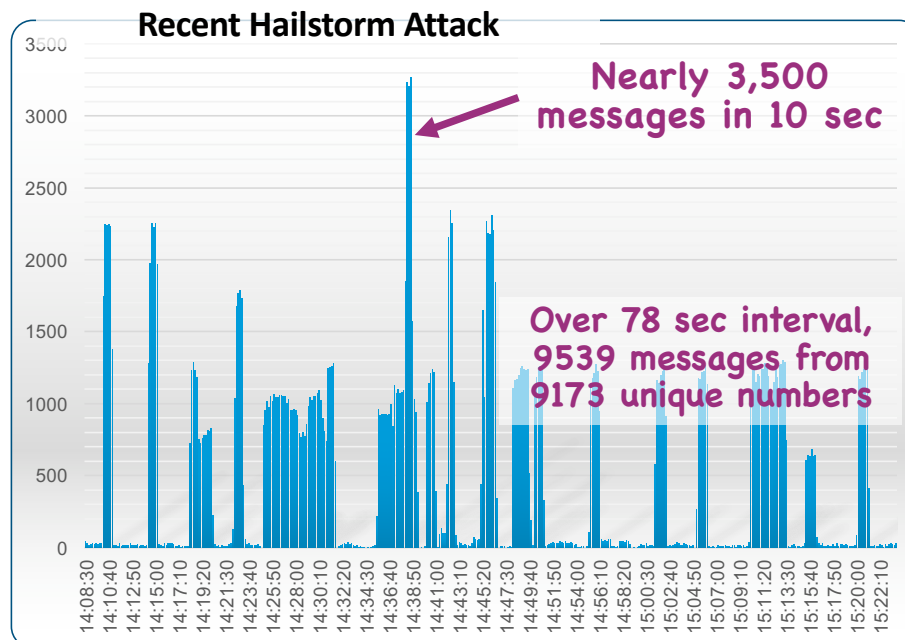
	Bank Reports	US Top Bank SMiSh Reports
Tier 1 – typosquatting	1 %	5 %
Tier 2 – phishing/smishing with brand	90 %	26 %
Tier 3 – generic smishing, name drop in msg body	9 %	69 %

*targeting Top 5 US/UK Banks

over 5,000 attacks since presentation start

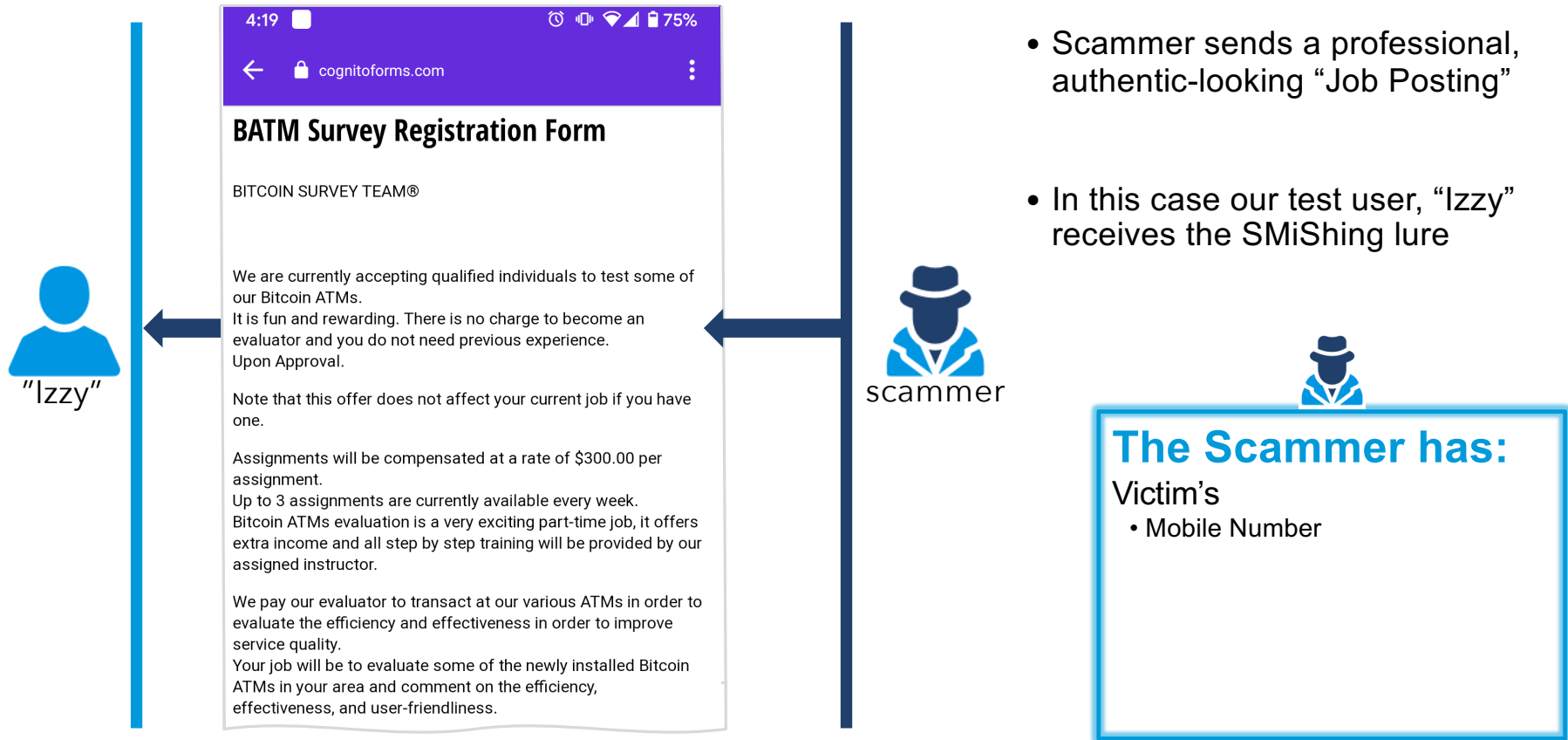
Scammers are Sophisticated: Hailstorm Attack

Short Bursts of traffic designed to outpace filtering updates/blocking techniques

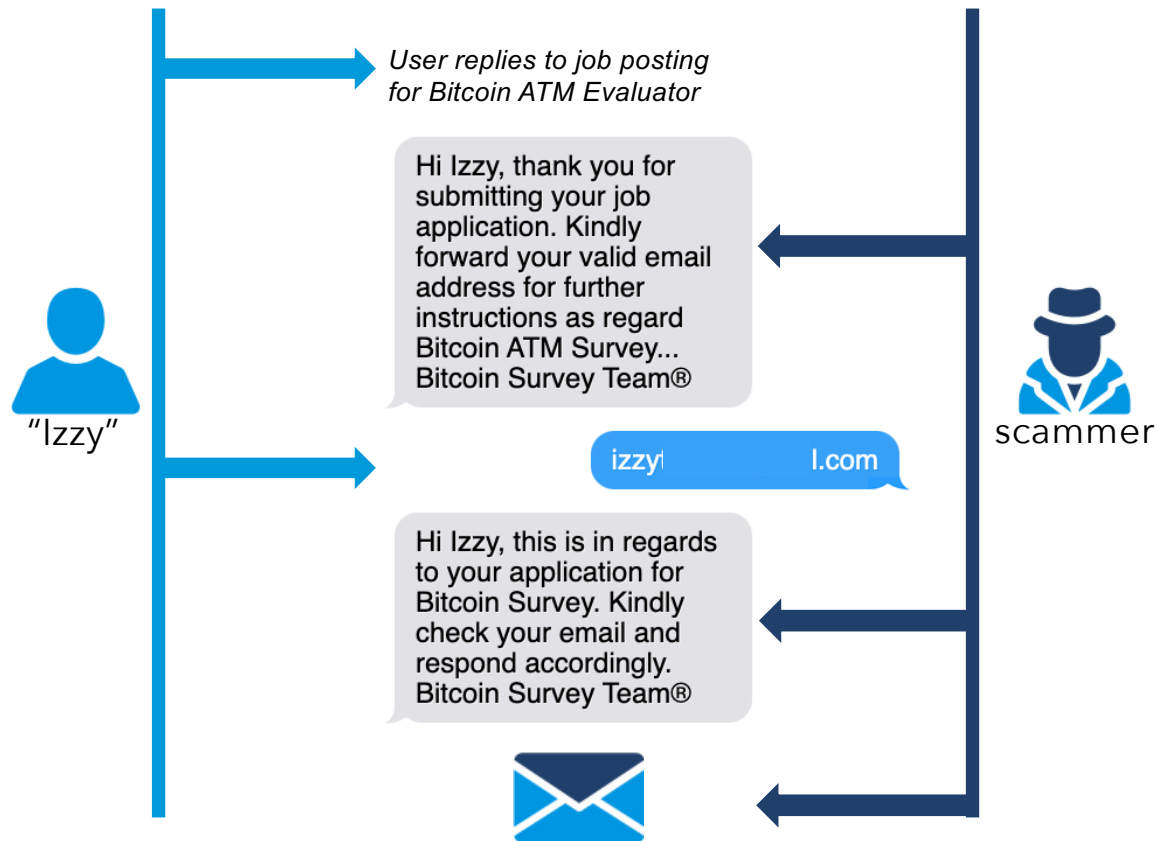


- Traffic sent in bursts across numerous phone numbers utilizing canary accounts to confirm delivery
- Bursty traffic effective against volumetrics
- Requires more advanced classification and clustering techniques to identify and respond

Bitcoin ATM Survey Job Posting Scam - Stage I



Bitcoin ATM Survey Job Posting Scam - Stage II



- Izzy responds to role to assess and evaluate local Bitcoin ATMs
- Initial communications through Mobile Messaging then survey instructions are sent through a separate email

The Scammer has:

Victim's

- Mobile number
- Name
- Physical address (from application)
- Email address

Bitcoin ATM Survey Job Posting Scam - Stage III



- Scammer sends email with instructions, implying that there is a wiring of Bitcoin in survey process

- If user confirms receipt, the Scammer sends account requests

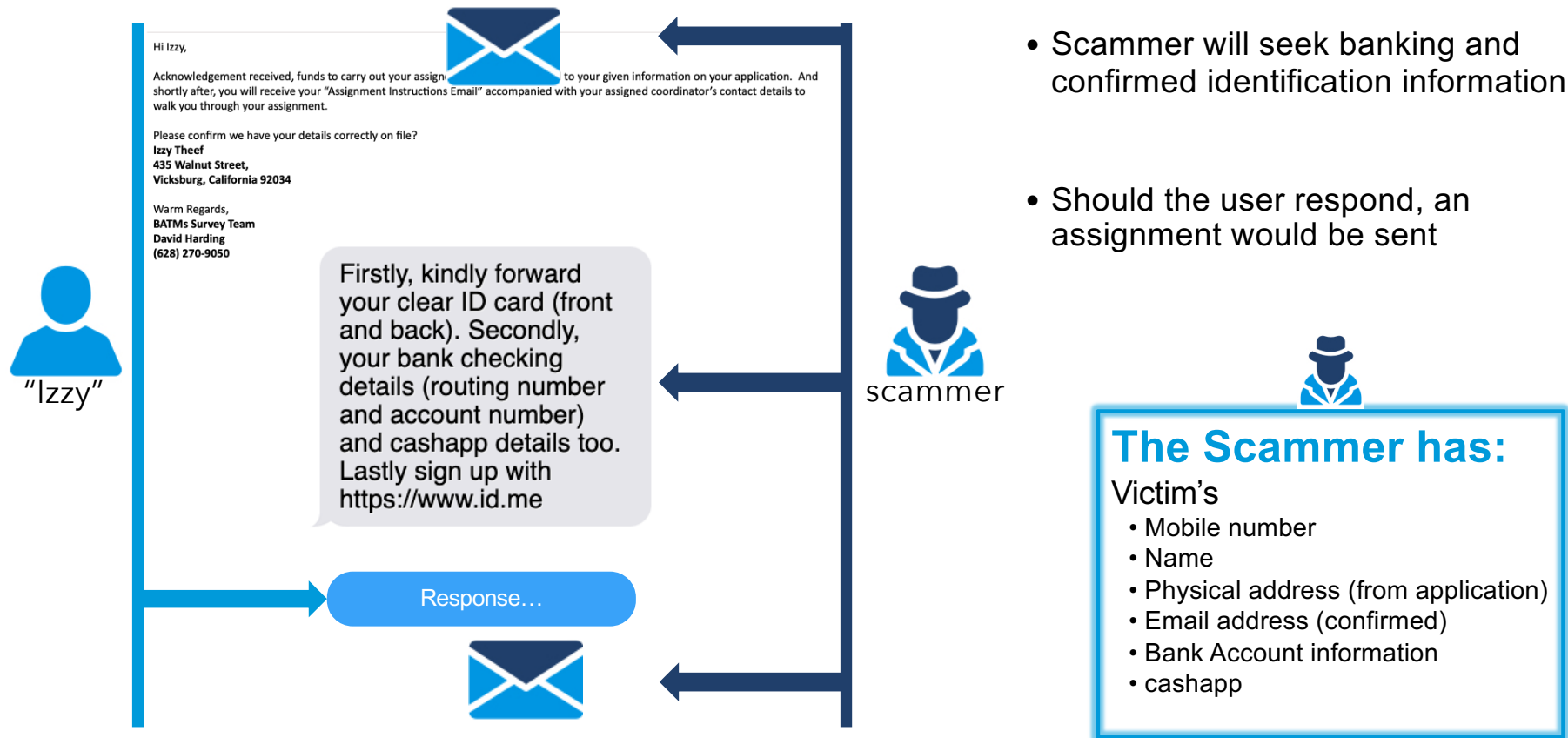


The Scammer has:

Victim's

- Mobile number
- Name
- Physical address (from application)
- Email address

Bitcoin ATM Survey Job Posting Scam - Stage IV



Bitcoin ATM Survey Job Posting Scam - Stage V

Email from Scammer includes QR code for Bitcoin wallet for deposit



"Izzy"



The \$2000 that will be deposit on the debit card includes your first Bitcoin ATM Survey assignment payment of \$1000 and the rest funds will be use to survey at the Bitcoin ATM locations. Do you understand?

If the scanner correctly verifies wallet by scanning the QR code.



Scammer

- Scammer will seek banking and confirmed identification information
- Scammer will transfer (and then revoke \$2,000) to Izzy for Izzy to deposit \$1,000 in Bitcoin wallet



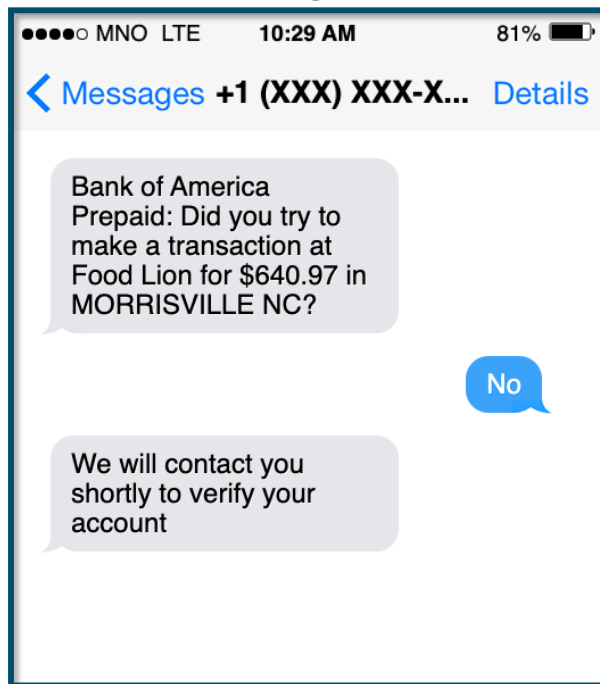
The Scammer has:

Victim's

- Mobile number
- Name
- Physical address (from application)
- Email address (confirmed)
- Bank information
- cashapp
- \$1,000 *clean*

2FA Harvesting using Multi-Modal Attack

Stage 1



Stage 2 – Voice

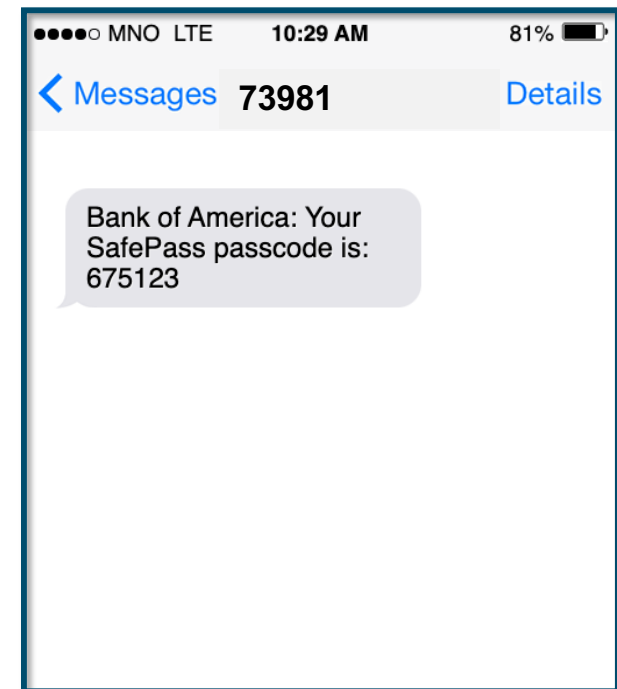


+1 (XXX) XXX-XXXX

“We need to access your account to verify the information”

“You will soon be receiving a passcode from 73981. Please read me the passcode once you receive it”

Stage 3



** Exact verbal conversation was not captured/recorded by Proofpoint

Best Practices

Best practices for combatting Phishing/SMiShing/Spam

Threats are Evolving

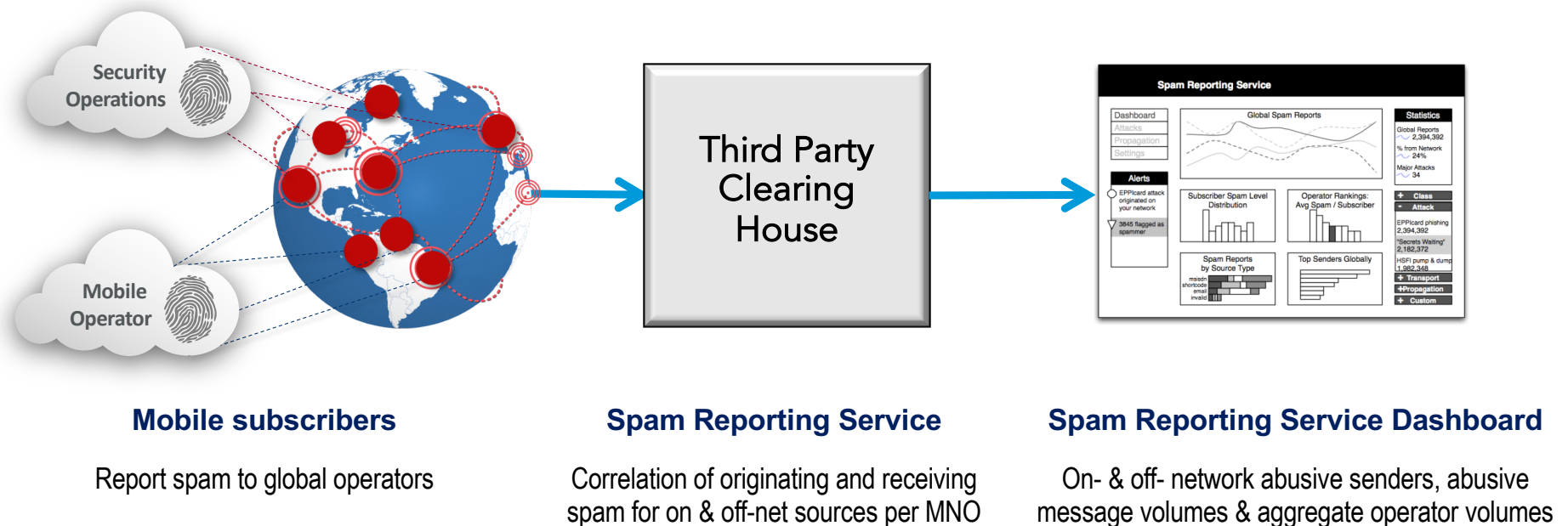
- Spam and Phishing/SMiShing via MMS now common
 - Operators adding MMS and RCS protection
- Basic Content Filtering Upgraded to Campaign Cluster-based detection
 - Advanced, high-speed campaign identification technologies
 - Enables identification of snowshoe sending patterns
- Outsourcing Abuse Management
 - Hiring outside experts for abuse detection and management
- SMS Hub Ingress Filtering
 - Minimal filtering for malicious content by intercarriers
 - Carriers now looking to filter traffic in the cloud, before delivery to local messaging platforms

Best Practices to Combat Mobile Abuse

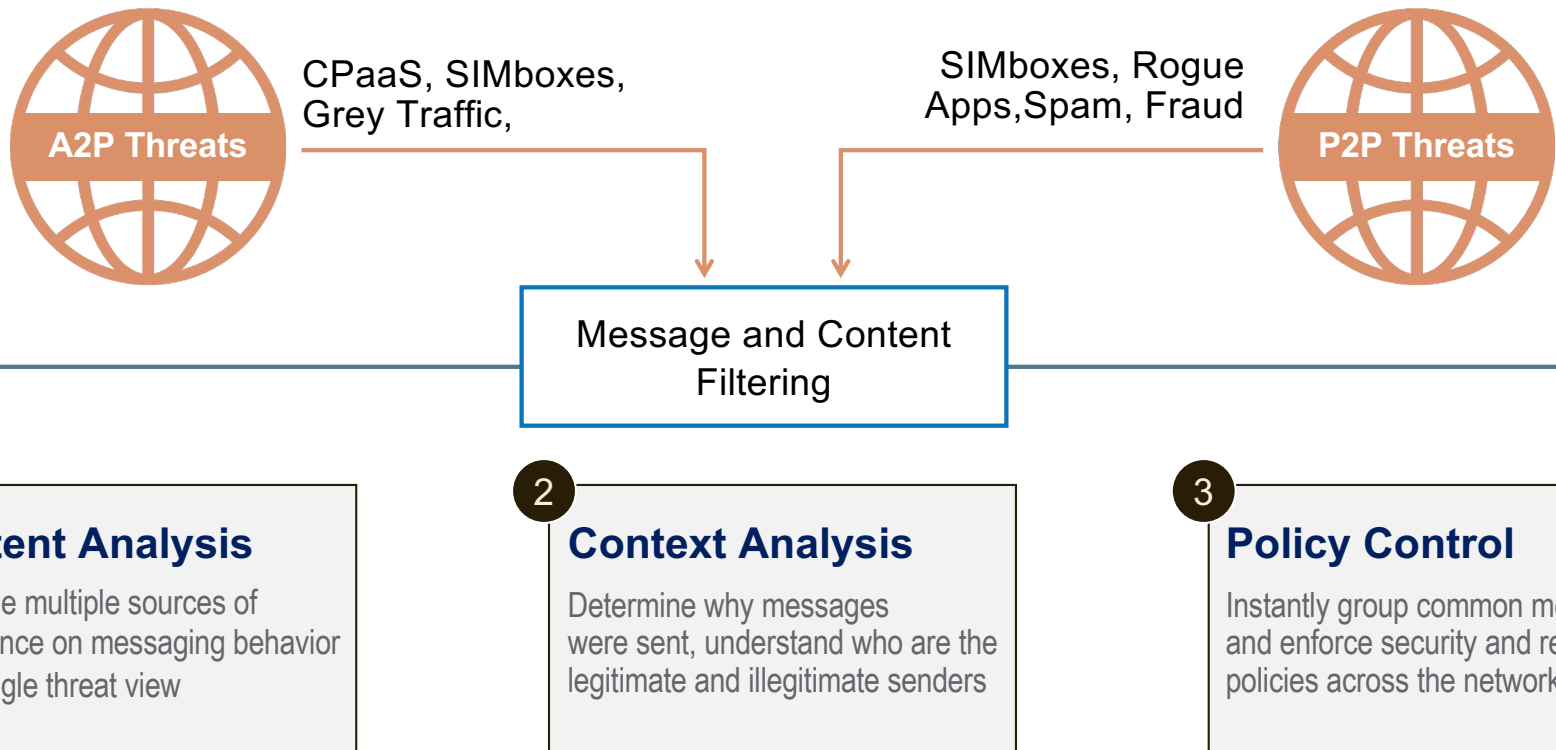
- Encourage mobile message abuse reporting
 - 7726/"SPAM" short code in use in N. and S. America, United Kingdom, and New Zealand
 - Native messaging app-based abuse reporting, 1-click or swipe reporting
- Push for similar laws to Canadian Anti-Spam Legislation (CASL)
 - Lower spammer's profit margin
 - Require opt-in permission for commercial/business-to-consumer emails
 - Right of private legal recourse against spammers
- Deploy multilayered mobile threat detection and defense solutions
 - **Detect**, **Block**, and **Report** malicious content prior to delivery
 - **Categorize** known threats for better and rapid response
 - **Monitor** sender behavior and abusive content
- Educate subscribers/end-users to reduce risk and encourage reporting

Mobile Message Abuse Reporting

Consolidated View of Global Spam Reports

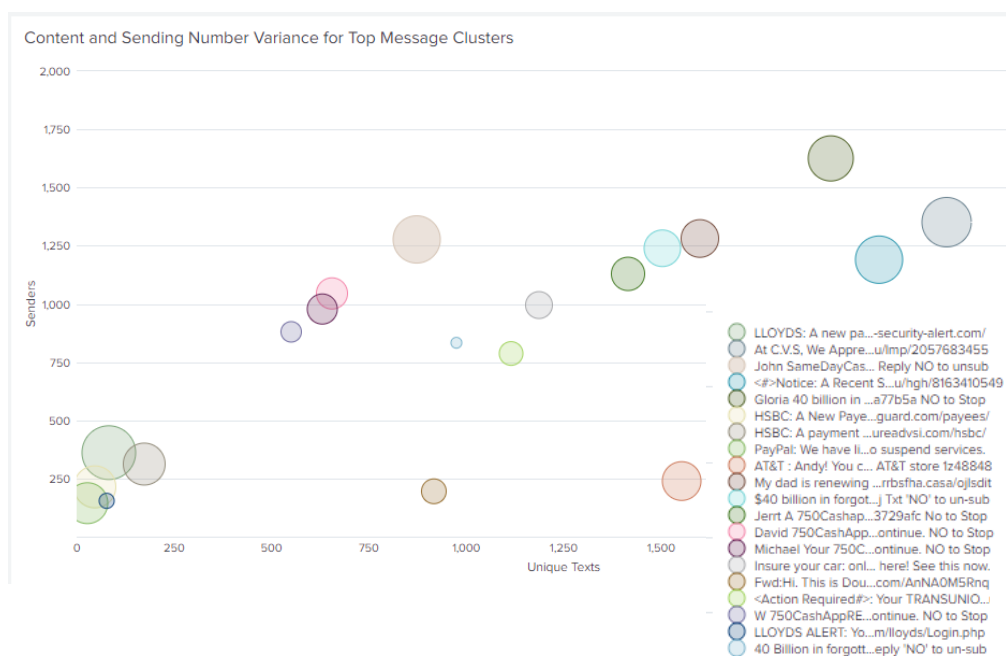


In-Network Abuse Mitigation



AI: Automated Clustering

Advanced Clustering of Threats Improves Response Time and Detection Accuracy



- Threats are Clustered based on content
- Spammers attempt to game system
 - Changing/using multiple phone numbers
 - Modifying message content
- Advanced detection and AI key to providing wide-spread protection

Multifaceted/Comprehensive Protection Needed

- Mobile abuse is increasing exponentially, growing more sophisticated, and threatens Consumers, Operators, and Commercial brands
 - Without mitigation, trust will be eroded
- **Over 10,500 attacks on top UK/US banking brands since presentation start***
- Comprehensive technology and a multifaceted approach provides best protection and value to Mobile Operators, Subscribers, and Brands/Commercial Senders
- This best Threat Protection is available through a combination:
 - User reporting
 - Threat content and data collection for future identification and response
 - Rapid content processing and filtering including predictive techniques both ML and AI for categorization, marking/flagging, and detection
 - Human interaction from analyst with broad and deep threat knowledge



CLOUDMARK[®]
A PROOFPOINT COMPANY

Questions?

Thank you!

© 2021 Proofpoint. All rights reserved