CLOUDMARK®
A PROOFPOINT COMPANY

Smishing and Malware Update

Mike Reading
Sr. Director, Mobile Innovation & Technical Services
Proofpoint, Cloudmark Division

mreading@proofpoint.com

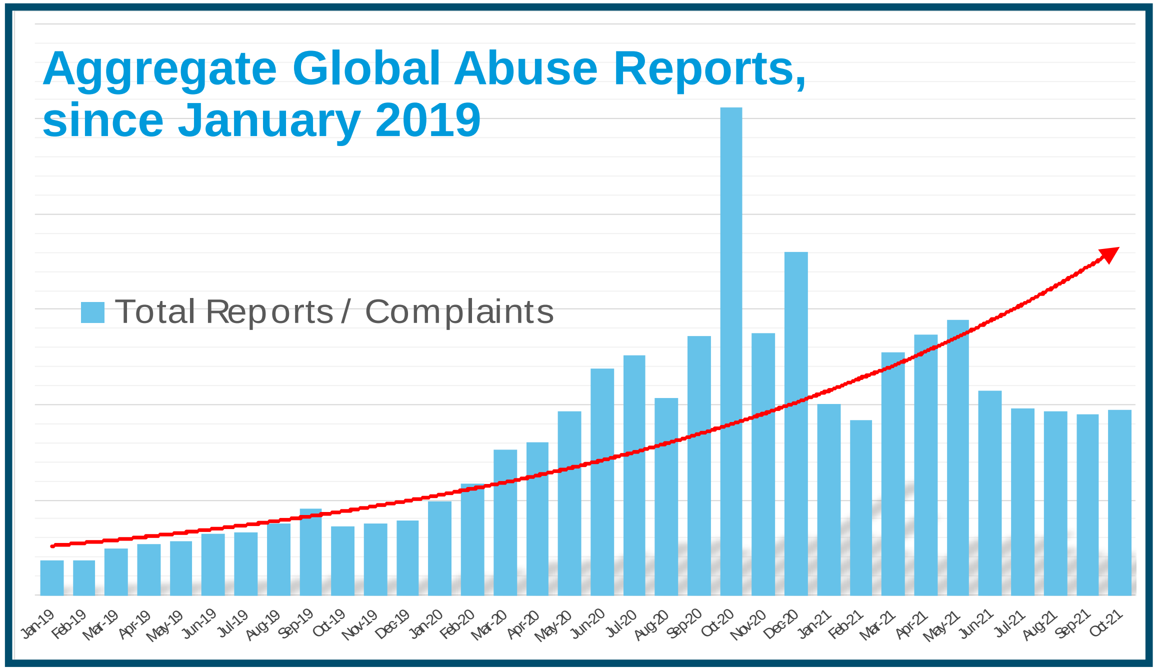
2nd November, 2021

Trends Update

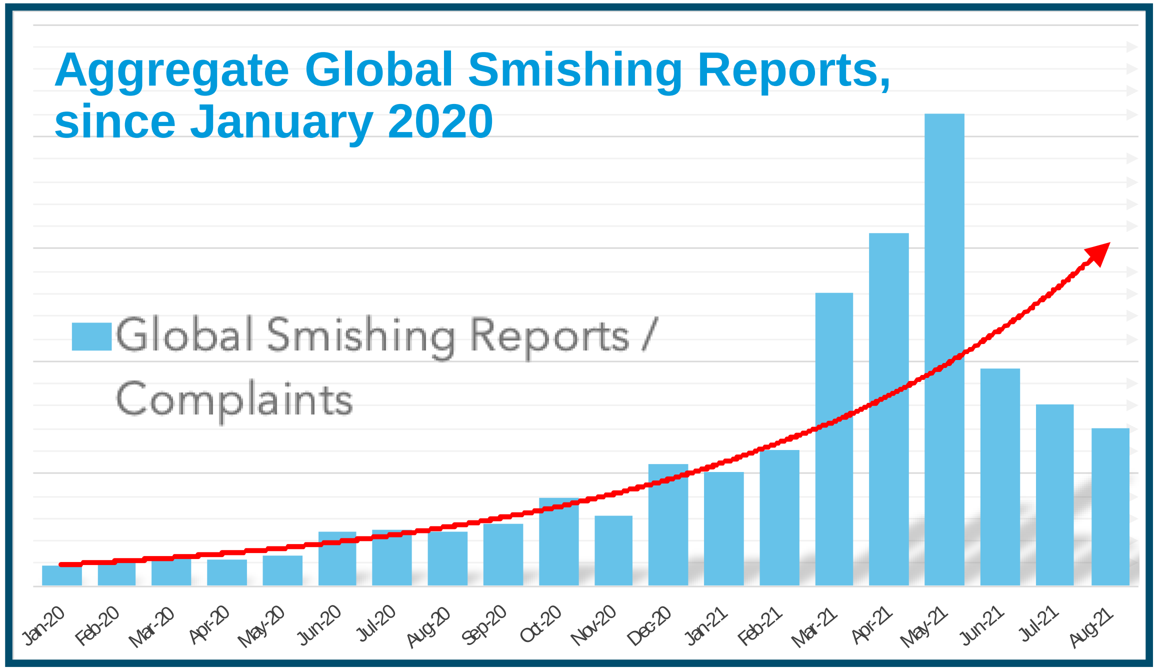
Abuse: Smishing and Malware increasing globally

proofpoint.

Global Abuse and Smishing Generally Increasing



Aggregate Global Abuse Reports, since January 2019



Aggregate Global Smishing Reports, since January 2020

- ➢ Abuse, spam, smishing, and mobile malware is on the rise
- ➢ Mid- to late-year slowdowns are common, growth expected in 4Q2021 & 2022
- ➢ Focus for today’s presentation is trends related primarily to **Smishing** and **Malware**

Proofpoint Witnessing Rapid Expansion in Smishing

270% increase in Global smishing reports 1H 2021 versus 2H 2020

Smish attacks are on the rise†

- ➢ 61% of Global enterprises,
- ➢ 47% of French enterprises,
- ➢ 56% of German enterprises, and
- ➢ 62% of UK-based enterprises report employees have faced smishing attacks

Smish unawareness remains too high globally†

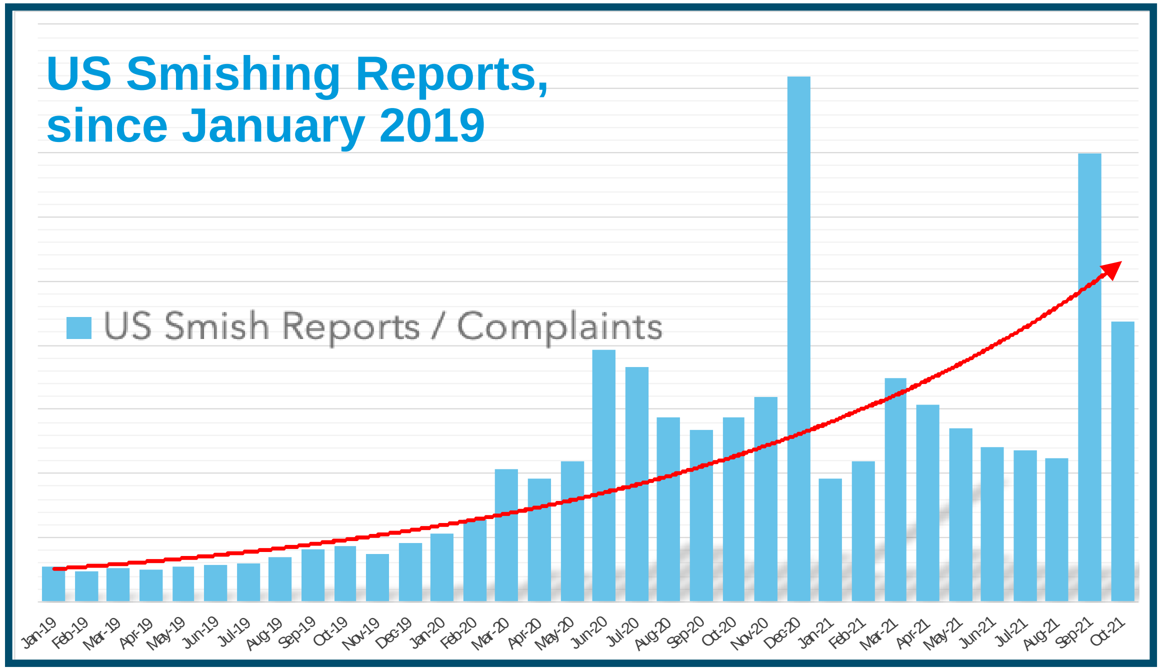
- ➢ 69% of people globally are unaware;
- ➢ 40% of people in France,
- ➢ 82% of people in Germany, and
- ➢ 70% of people in the UK are unaware of smishing

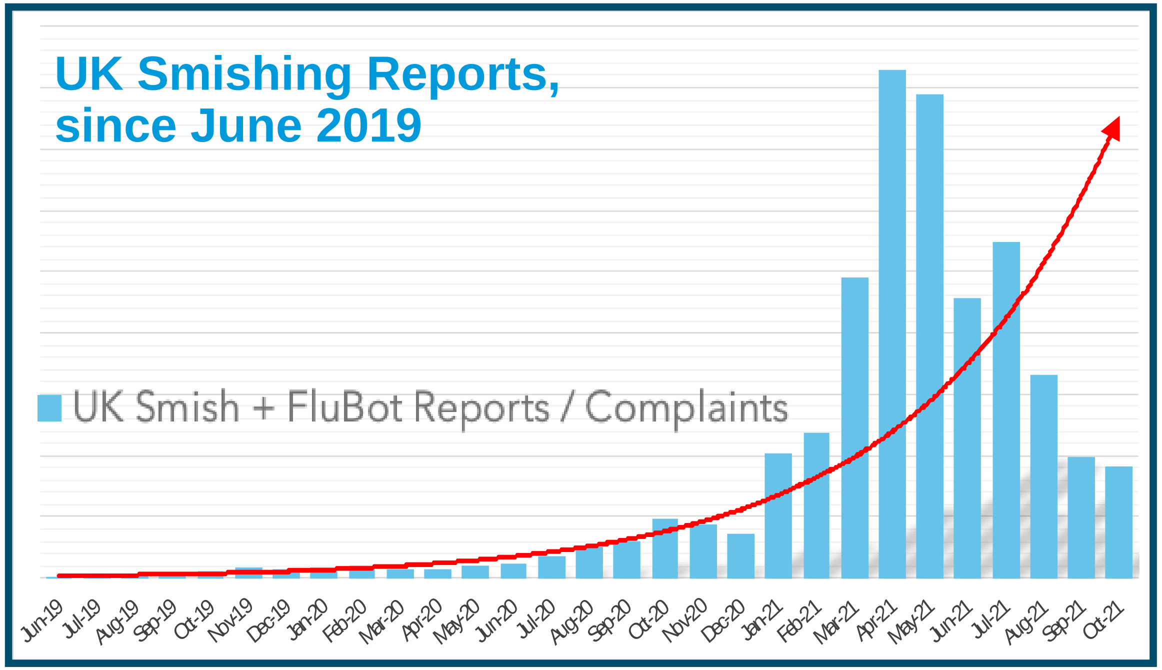
Mobile Messaging remains highly trusted and has a 98% open rate

† Proofpoint. "2021 State of the Phish", 2021. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish/

proofpoint.

Regional Smishing Trends: US and UK





- ➢ Mid / late year slow down seen again
- ➢ UK: reports of smishing nearly nonexistent in UK in early 2019, aggressive growth past couple of years, fall off the last few months but still expecting it to pick back up
- ➢ US: steady growth in smishing since beginning 2019

Rise in Package Delivery Lures

Watch Out for Bogus Delivery Notifications / Alerts

- Last few months has seen increasingly lure activity related to delivery services, parcel/package delivery notifications and exceptions

- Increase to Top- 1 or 2 is consistent globally
  - UK seeing a small rise in NHS related attacks
  - New Zealand has seen images/picture scams
  - Lures for downloading malware have leveraged parcel and package delivery

- Marked change from six to nine months ago

Global Smishing - 3Q2021	
Parcel / Package Notification	**48.4%**
Merchant & Consumer Brands	9.9%
Media & Comms Providers	6.7%
Financial / Banks	5.5%
Miscellaneous and Other	29.4%

UK Smishing + FluBot - 3Q2021	
Parcel / Package Notification	**59.8%**
Financial / Banks	18.1%
Voicemail Notification	13.7%
Miscellaneous / Other	8.4%

US Smishing - 3Q2021	
Parcel / Package Notification	**25.8%**
Merchant & Consumer Brands	17.8%
Media & Comms Providers	14.2%
Financial / Banks	8.9%
Miscellaneous and Other	33.3%

proofpoint.

Mobile Malware on The Rise

- Attackers are increasingly using malware to steal credentials and other personal information
- Globally multiple mobile malware variants have been seen in 2020 and 2021
- Software and implementations vary but there is similarity between the attacks

	App Impersonation	*Financial Impersonation*	*Multi-Modal (Social Media)*	*Credential Theft*	*Microphone and Camera*	*SMS Spreading*	*Privilege Escalation*
FluBot	✓	✓	✗	✓	✗	✓	✓
TeaBot	✓	✓	✓	✓	✗	✓	✓
TangleBot	✗	✓	✓	✓	✓	✗	✓

proofpoint.

FluBot is Sophisticated, Multipronged Attack

- Once granted access, FluBot acts as:
  - Internet access
  - Voice & USSD calls
  - Processing notifications
  - Sending & reading messages
  - Deleting applications
  - Accessing contact lists

  And can act/operate as:
  - Contacts/phonebook thief
  - Banking credential thief
  - SMS spammer/worm
  - spyware
- The app uses display overlays for various banking apps and Google Play verification to steal bank card information
- FluBot sends the victim's contacts and other information to attacker's C2
  - C2 uses a load distribution algorithm to instruct the infected device to generate new "starting" smish messages

- FluBot is **hard to uninstall**
  - Needs factory reset or booting in safe mode
- FluBot may attack North America
  - Some "stray sightings" from UK and Germany numbers
  - A few messages from Belgium in Spanish to US numbers
  - Pattern of attack has been one country focus at a time

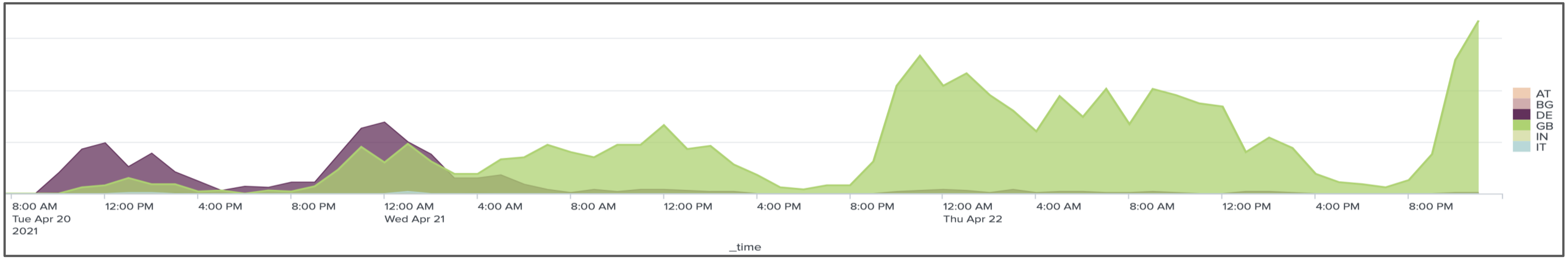
Sampling of FluBot "Overlay" Apps
(>200, incl. variations, detected in UK)

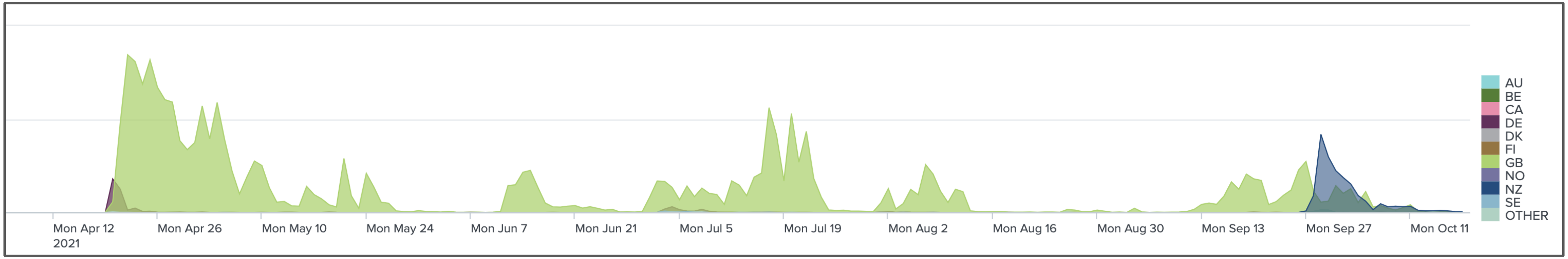
La Caixa	Liberbank	Vivid
Santander	Open Bank	Binance
BBVA	WiZink	Commerzbank
Kutxabank	Grupo Cajamar	Comdirect
Ibercaja Banco	Coinbase	Starfinanz
Traktorpool	Beobank	Mediolanum
Barclays	Starling Bank	BanInter

FluBot Update

Tracking FluBot – systematic movement from one country to another

- UK FluBot v4.0 attack initiated from German mobiles, April 20th using package delivery lures (initially DHL)
- NZ FluBot attack was initiated on about September 27th using delivery lures as well

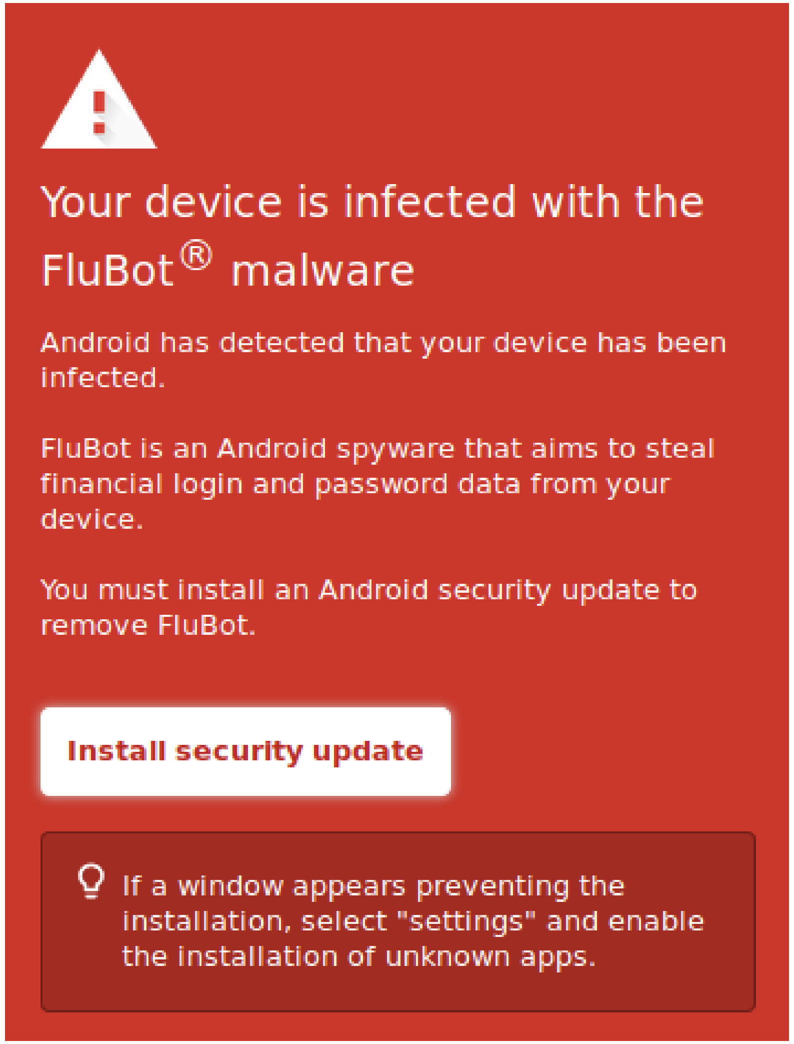




proofpoint.

FluBot in New Zealand

- First detected September 27th
- Initially using Package Delivery notifications and Picture warnings
- Peaked on September 29th
- Since October, primary Lures include
  - Delivery
  - Voicemail
  - Photo Requests
  - Social Engineering
  - Security Updates



Your device is infected with the FluBot® malware

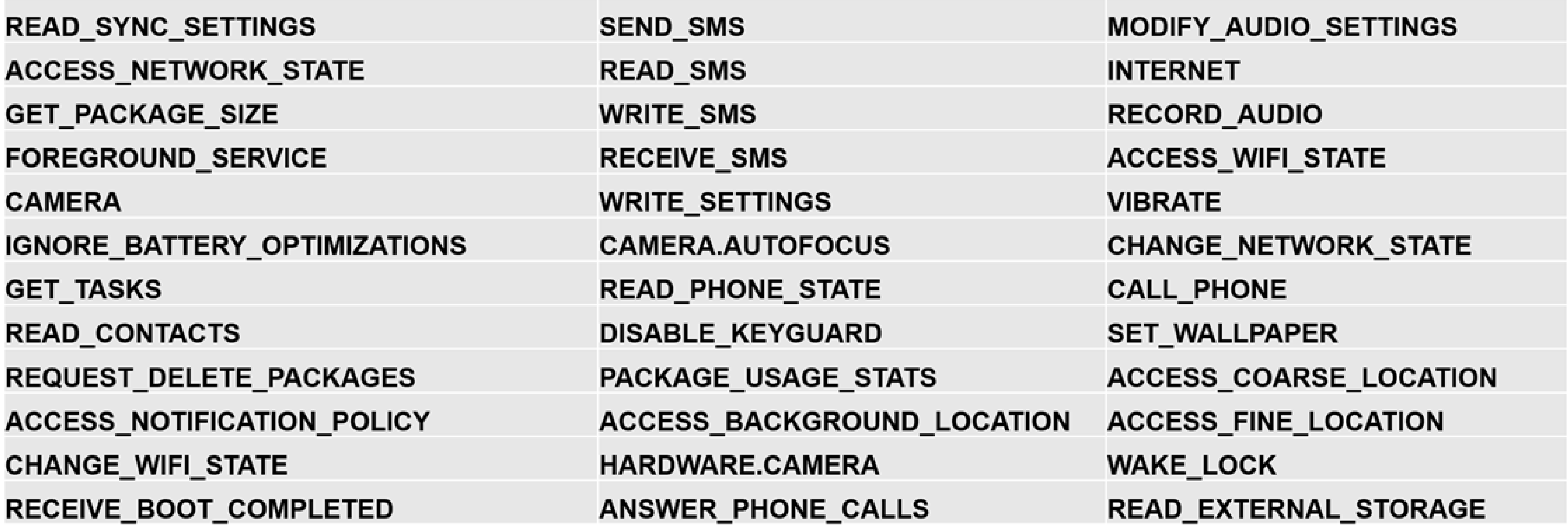
Android has detected that your device has been infected.

FluBot is an Android spyware that aims to steal financial login and password data from your device.

You must install an Android security update to remove FluBot.

If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.

TangleBot – Permissions to Control Device Functions

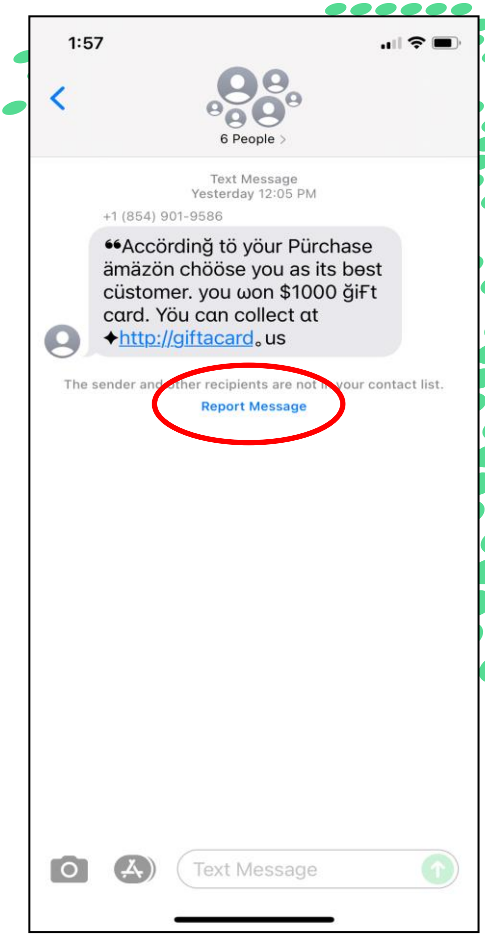


READ_SYNC_SETTINGS	SEND_SMS	MODIFY_AUDIO_SETTINGS
ACCESS_NETWORK_STATE	READ_SMS	INTERNET
GET_PACKAGE_SIZE	WRITE_SMS	RECORD_AUDIO
FOREGROUND_SERVICE	RECEIVE_SMS	ACCESS_WIFI_STATE
CAMERA	WRITE_SETTINGS	VIBRATE
IGNORE_BATTERY_OPTIMIZATIONS	CAMERA.AUTOFOCUS	CHANGE_NETWORK_STATE
GET_TASKS	READ_PHONE_STATE	CALL_PHONE
READ_CONTACTS	DISABLE_KEYGUARD	SET_WALLPAPER
REQUEST_DELETE_PACKAGES	PACKAGE_USAGE_STATS	ACCESS_COARSE_LOCATION
ACCESS_NOTIFICATION_POLICY	ACCESS_BACKGROUND_LOCATION	ACCESS_FINE_LOCATION
CHANGE_WIFI_STATE	HARDWARE.CAMERA	WAKE_LOCK
RECEIVE_BOOT_COMPLETED	ANSWER_PHONE_CALLS	READ_EXTERNAL_STORAGE

- Once fully installed, TangleBot has access to a myriad of Android OS permissions, enabling device control and manipulation
- Underlying control enables TangleBot threats to evolve and expand
  - Camera and Microphone access could lead to possible biometric authentication avoidance

Best Practice: Monitoring Abuse Via End User Spam Reporting

Best Practice Tracking Smishing/Spam: End-User Reporting



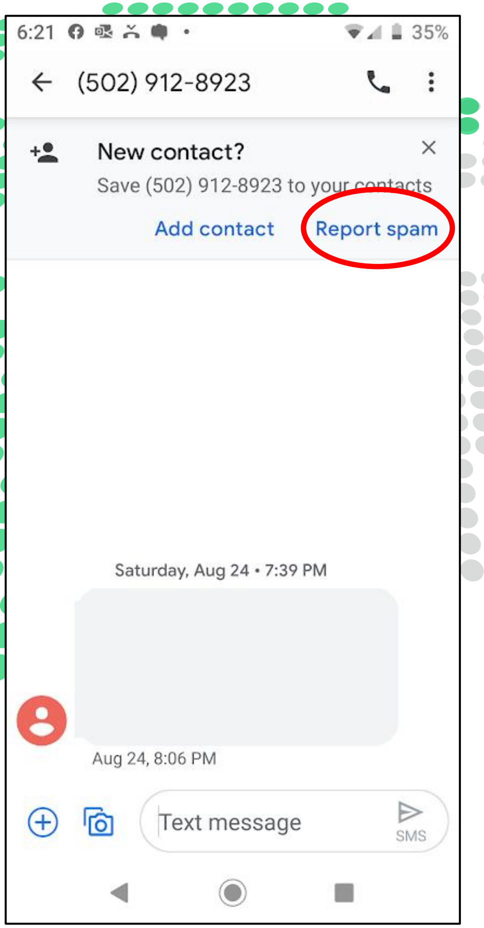
Text Message
Yesterday 12:05 PM

+1 (854) 901-9586

‶Accördinğ tö yöur Pürchase ämäzön chööse you as its best cüstomer. you ωon $1000 ğiFt card. Yöu can collect at ✦http://giftacard。us

The sender and other recipients are not in your contact list.

Report Message



New contact?

Save (502) 912-8923 to your contacts

Add contact   Report spam

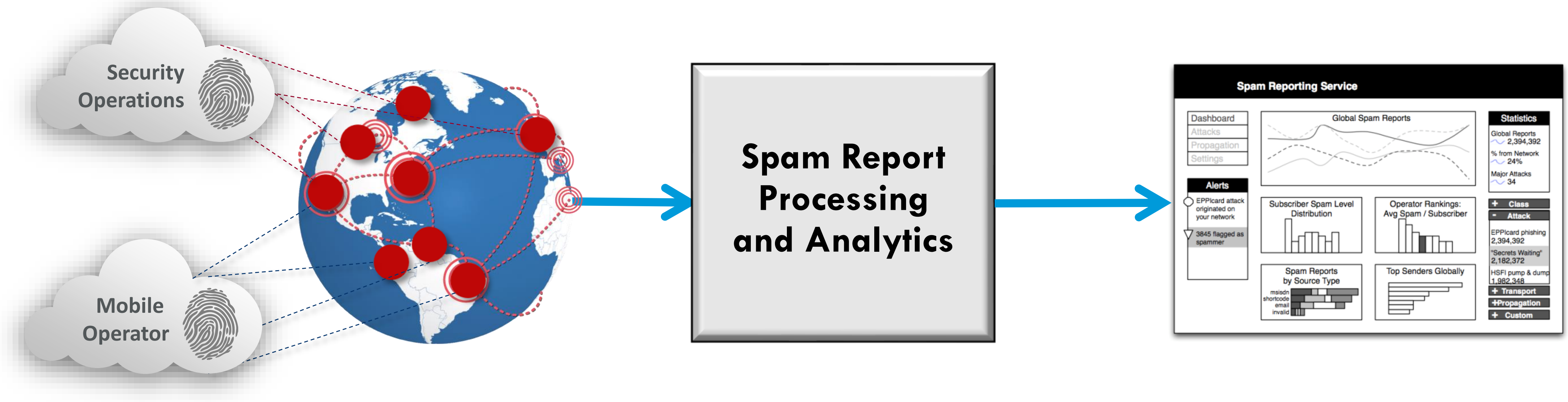
Saturday, Aug 24 • 7:39 PM

Aug 24, 8:06 PM

- Subscribers are best placed to alert Networks to abuse
  - ➢ One-Click makes reporting easy
  - ➢ Notifications delivered within seconds of attacks launching
- Already Adopted Across major areas:
  - ➢ North America,
  - ➢ South America,
  - ➢ the UK,
  - ➢ New Zealand
- Multiple New Territories planned

Mobile Message Abuse Reporting

Consolidated View of Global Spam Reports



Mobile subscribers

Report spam to global operators

Spam Reporting Service

Correlation of originating and receiving spam for on & off-net sources per MNO

Spam Reporting Service Dashboard

On- & off- network abusive senders, abusive message volumes & aggregate operator volumes

proofpoint.

Smart Phone (iOS & Android) One-Click Reporting

SMS/MMS Abuse One-Click Reporting

- Smishing, malware, and spam reporting integrated into Apple and Android message apps
  - “Single-click” spam reporting of SMS, MMS, and RCS
- Visibility to messaging traffic from unknown senders, full message reporting
- Call to action feedback (URL & phone numbers)

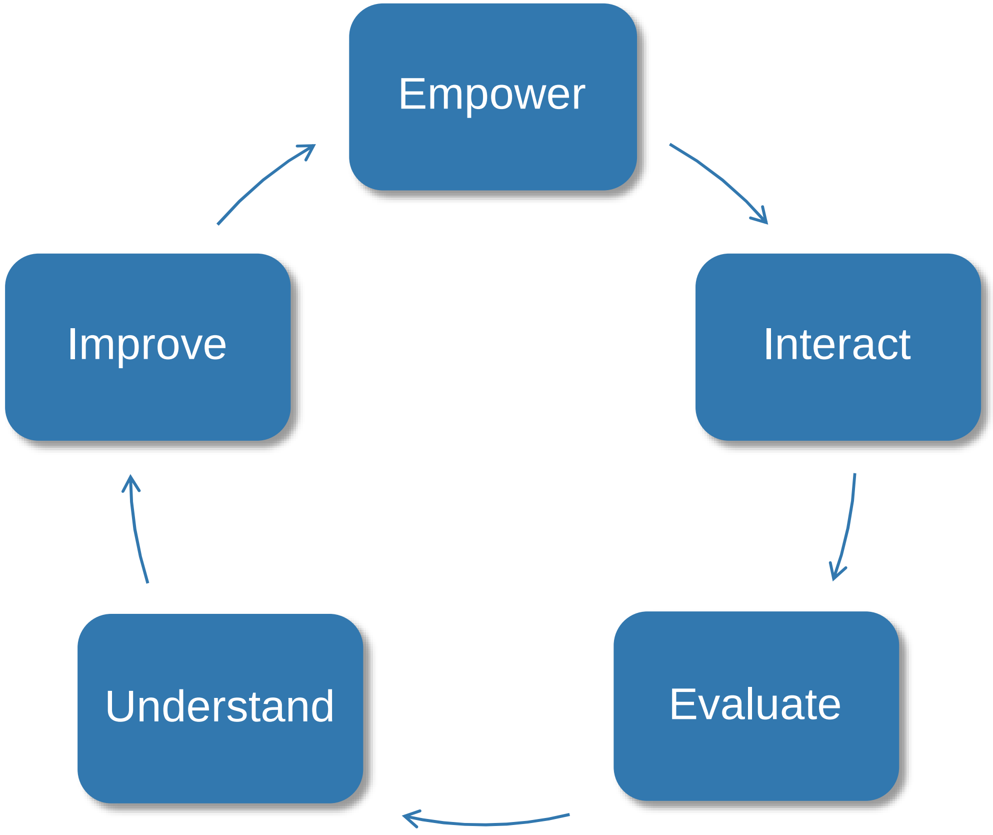
Voice Abuse One-Click Reporting

- Voice spam reporting integrated into Apple and Android message apps
  - “Single-click” spam reporting of unwanted calls
  - Ability to classify call type
- Ability to proactively block calls within Mobile Operator’s network or at the subscriber handset/device

Android

iOS

Subscriber Reporting Enables A Mobile Feedback Loop



- Spam Reporting Service provides actionable data and insight to the MNO
  - ➢ ***Empowers*** the end-user/subscriber to act on smishing, abuse, and spam
  - ➢ Provides MNO an opportunity to ***Interact*** with their customer
  - ➢ Allows the MNO to measure and ***Evaluate*** network solution and protections
  - ➢ Let's the MNO ***Understand*** nature of attacks and abuse affecting network and subscribers
  - ➢ Enables the MNO to act on the feedback to ***Improve*** network performance and customer perception

proofpoint.

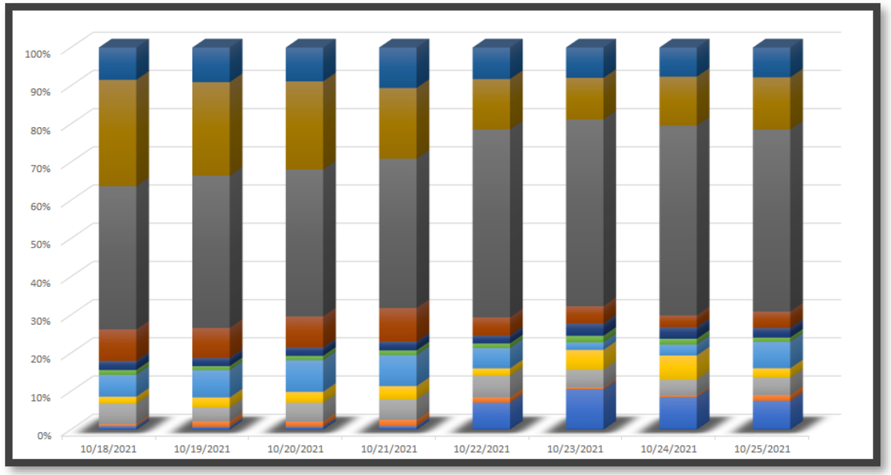
Value of Spam Reporting Service to the MNO

- Actionable data and insight to the MNO
  - ➢ Necessary information for takedown of malicious sites
  - ➢ Attack information to improve network filtering/response

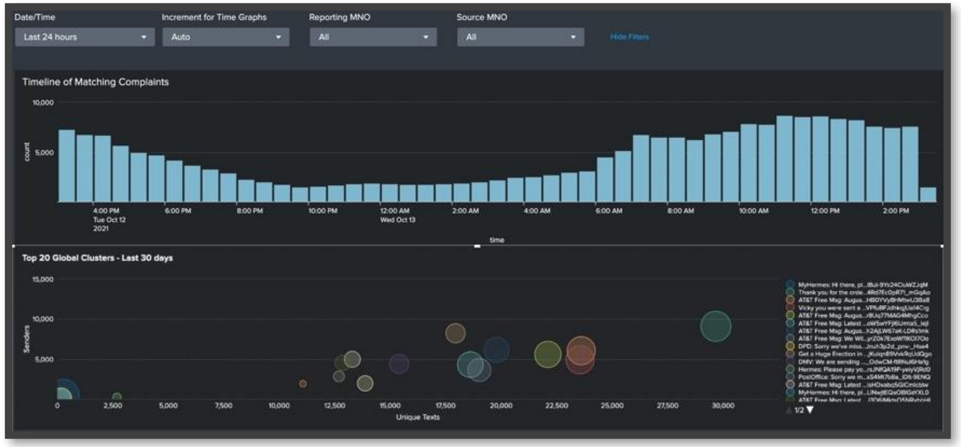
- Enables visualization and deep forensics
  - ➢ Network metrics to drive strategy and measure results
  - ➢ Detailed network and attack trend analysis
  - ➢ Nature, methods, and impacts of attacks and threats

- Empowers MNOs to develop efficient security strategies, optimize network resources, and avoid costly spam, customer complaints, and inter-carrier billing investigations

Spam Complaint Sources (Previous Week)



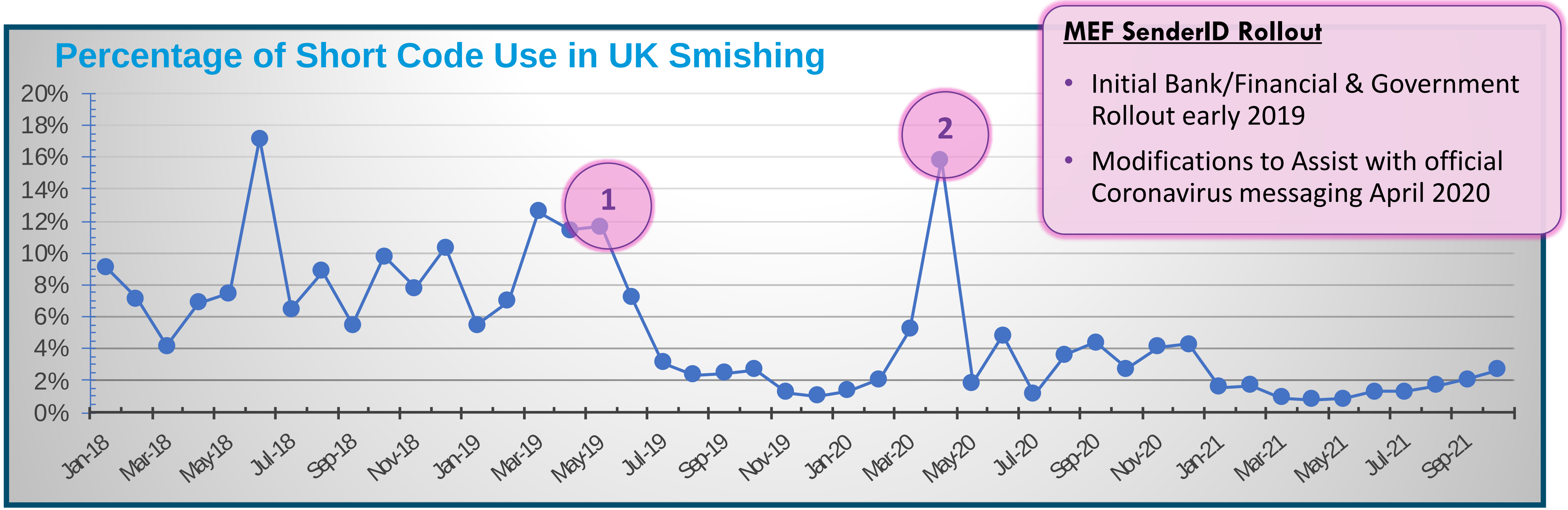
Trend Visualization & Attack Monitoring


Date/Time: Last 24 hours
Increment for Time Graphs: Auto
Reporting MNO: All
Source MNO: All

Hide Filters
Timeline of Matching Complaints
10,000
5,000
count
4:00 PM
Tue Oct 12
2021
6:00 PM
8:00 PM
10:00 PM
12:00 AM
Wed Oct 13
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
time
Top 20 Global Clusters - Last 30 days
15,000
10,000
5,000
Senders
0
2,500
5,000
7,500
10,000
12,500
15,000
17,500
20,000
22,500
25,000
27,500
30,000
Unique Texts
MyHermes: Hi there, pl...lBul-9Ys24CluWZJqM
Thank you for the orde...4Rd7Fc0pR71_mGqAo
AT&T Free Msg: Augus...HB0YVyBHMtwU38aB
Vicky you were sent a ...VPfuRFJdhkqjUal4Crg
AT&T Free Msg: Augus...rBUq77MAG4MhgCco
AT&T Free Msg: Latest ...oW5wYFj6Umra5_lejl
AT&T Free Msg: Augus...h2AjLW67aK-LDRs1mk
AT&T Free Msg: We Wil...yrZ0k7EsoWfIKOI7Oo
DPD: Sorry we've miss...Jnuh3p2d_pnv_Hse4
Get a Huge Erection in ...jKulqn89VvkRqUdQgo
DMV: We are sending ...OdwCM-f8RNul6Ha1g
Hermes: Please pay yo...rsJNfQA19P-yeIyVjRd0
PostOffice: Sorry we m...xS4Mt7b8a_iDb-9ENQ
AT&T Free Msg: Latest ...isHDxabq5GiCmIcblw
MyHermes: Hi there, pl...LINwjtEQaOBlGdYXL0
1/2

proofpoint.

SenderID Rollout And the Effect


Percentage of Short Code Use in UK Smishing

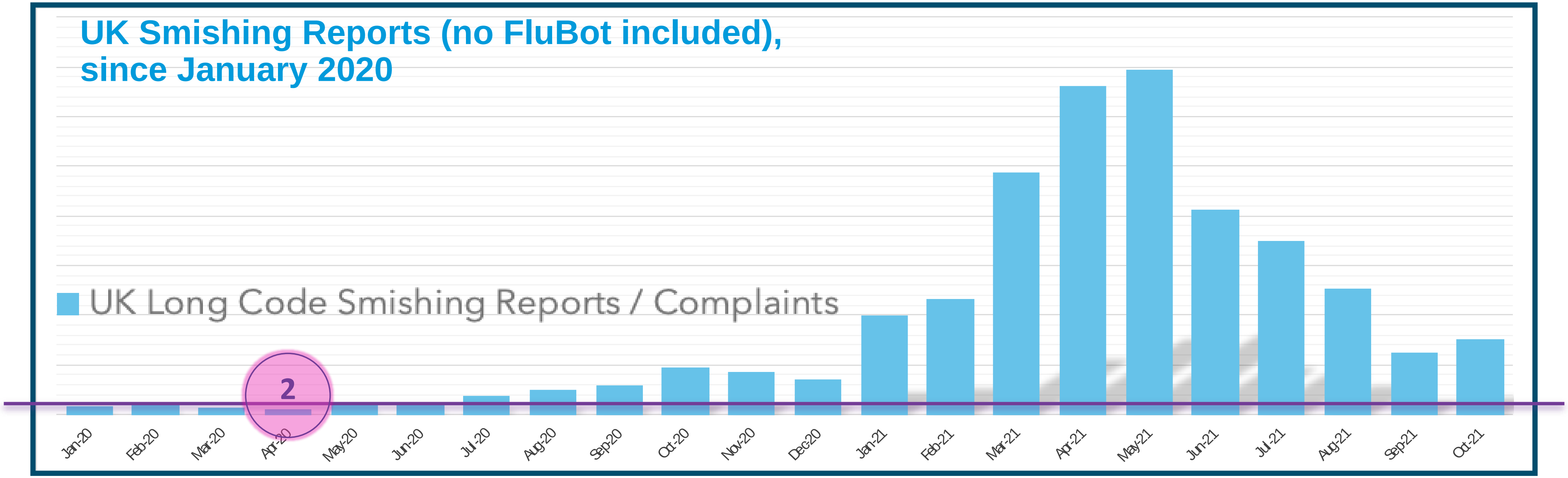
MEF SenderID Rollout

- Initial Bank/Financial & Government Rollout early 2019
- Modifications to Assist with official Coronavirus messaging April 2020

➢ SenderID has a demonstrable, positive affect on UK-based smishing

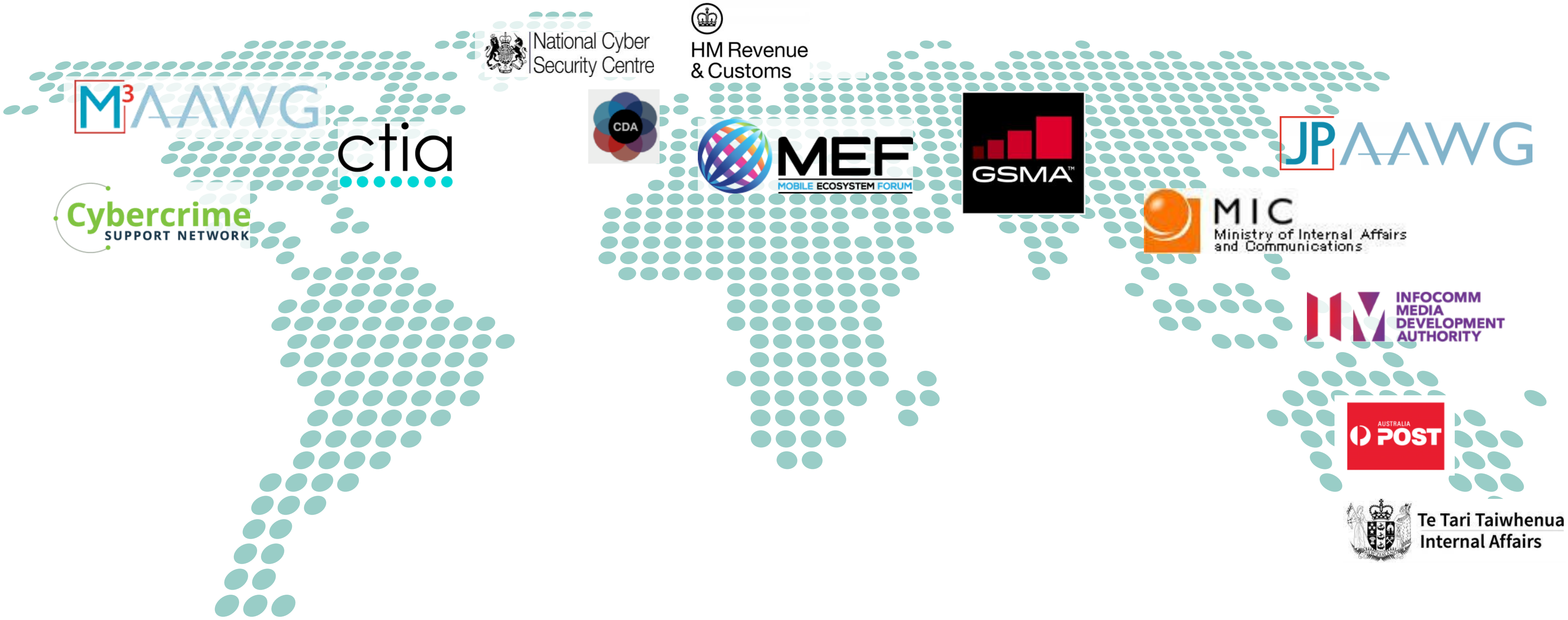
proofpoint.

Next Focus for UK Protection: Long Code



- Since the SenderID update to support UK government coronavirus messaging, Long Code abuse has never come back “down” to that level
- SenderID has been widely successful and now we need to address Long Code

Global Initiatives to Endorse Subscriber Spam Reporting


M3AAWG
ctia
Cybercrime SUPPORT NETWORK
National Cyber Security Centre
HM Revenue & Customs
CDA
MEF MOBILE ECOSYSTEM FORUM
GSMA
JPAAWG
MIC Ministry of Internal Affairs and Communications
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
AUSTRALIA POST
Te Tari Taiwhenua Internal Affairs

Subscriber Abuse Reporting Maintains Privacy

Spam Reporting Services Generally

- Voluntary service and abuse reporting which is end-user/subscriber initiated
- Spam Reporting Service content is encoded to protect user identification

Cloudmark Implementation of Spam Reporting Service

- Proofpoint and Cloudmark utilize SOC II compliant hosted facilities
  - Secured facilities
  - Encrypted file systems
- Proofpoint and Cloudmark maintain strict Data Access Controls
  - Customer has access to ONLY their specific data – silo'd data structure
  - Proofpoint and Cloudmark employees limited by need-to-access restrictions following the Principal of Least Privilege (PLP) concept
- Proofpoint and Cloudmark utilize strict obfuscation techniques on all data to protect PII

proofpoint.

Interested in Future Smishing, Spam & Abuse Reporting

- M3AAWG Mobile-Tech Committee has an ongoing effort focused on "**Advancing and evolving uniform spam and smishing reporting**"

- Objectives of the initiative:
  - ➢ Identify interested industry partners/participants
  - ➢ Collect requirements
  - ➢ Raise awareness of existing services
  - ➢ Share best practices

- For information or to participate, please email:

  mobile-tech-chair@mailman.m3aawg.org

proofpoint®

Reducing Abuse – Doing What You're Doing and…

What else is needed?

1. More/continued collaboration across the ecosystem: MNOs, government entities, pertinent industry groups, and major consumer brands
2. Need to discourage attackers by making it **less easy** and **less lucrative** to perform smishing
   - Making it less easy…making it more difficult to attack – encouraging more deployment of anti-abuse infrastructure improvements in the MNO
   - Making it less lucrative requires continued and increased collaboration (better tracking, increased likelihood of arrests)
3. Provide better User experience and protection
   - Enabling and improving subscriber, end-user, reporting mechanisms and tools
   - Need major brands to issue alerts when their brand is smished/phished

proofpoint.