JPAAWG 4th General Meeting: Mobile Trends & Threats

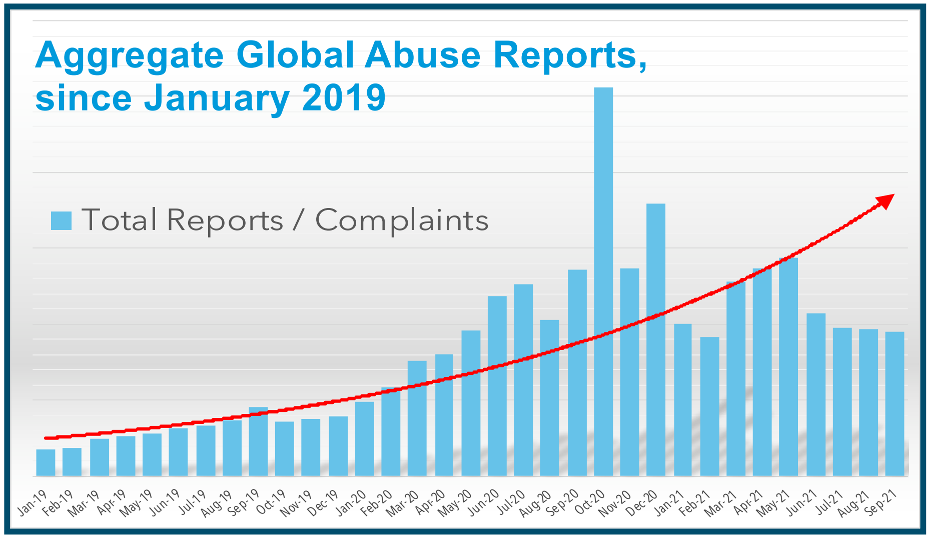
Mike Reading, Sr. Director, Mobile Innovation & Technical Services
Proofpoint, Cloudmark Division

11th November, 2021

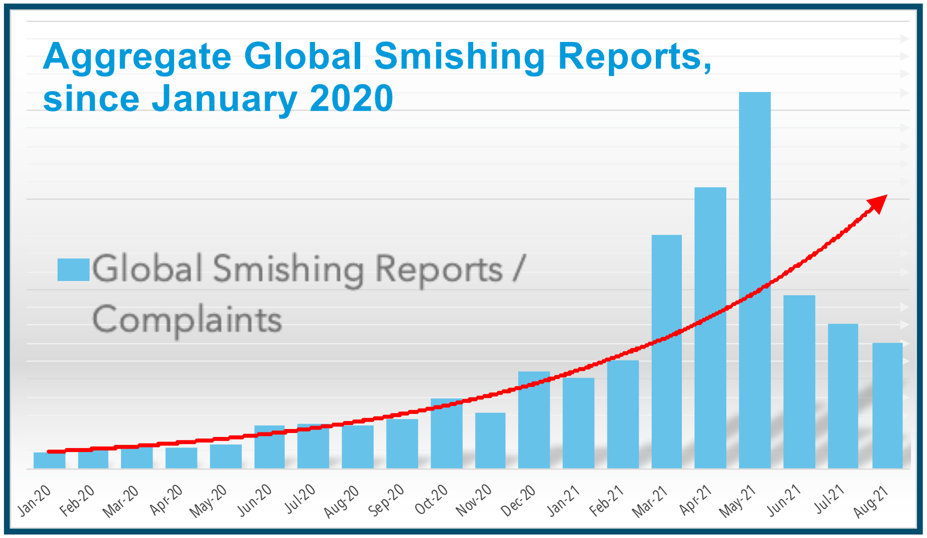
1. Trends Update

Abuse: Smishing and Malware increasing globally and throughout the region

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
- ➢ Midyear slowdowns are common, growth expected to continue in 4Q2021 & 2022
- ➢ Focus today is on threats to Japan and region, primarily **Smishing** and **Malware**

proofpoint.

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,
- 81% of US enterprises,
- 64% of Australian enterprises, and
- 56% of Japanese enterprises report employees have faced smishing attacks

Smish unawareness remains too high globally†

- 69% of people globally are unaware;
- 65% of people in US,
- 75% of people in Australia, and
- 81% of people in Japan are unaware of smishing

According to the Council of Anti-Phishing Japan: "Be aware, SMS [smishing/abuse] tends to be misidentified as genuine"

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

proofpoint.

Smishing Represents a Tangible Risk

Smishing Impacts Players Throughout the Mobile Value Chain

Consumer Impact

- Loss of personal information
- Financial loss
  - Japan: 1.13 billion Yen lost due to online banking fraud according to Statista
  - Australia: A$3.1 million in losses directly related to SMS message scams (Australian Competition & Consumer Commission)
  - US: Greater than $86 million loss from smishing alone, circa 2020 (US Federal Trade Commission)

Mobile Network Operator Impact

- Brand erosion and decreased consumer trust due to consumer vulnerability
- Large volume smishing and malware attacks cause direct impact on MNO operations/expense
- Increased customer support calls and complaints plus follow up with device sanitization causes financial loss

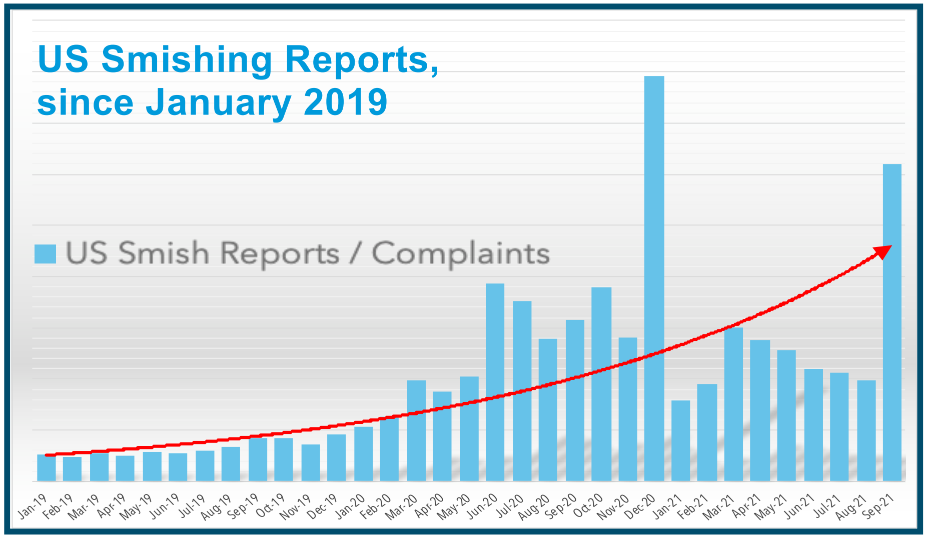
Enterprise/Corporate Impact

- Brand erosion due to impersonation attacks and consumer misidentification of bona fide corporate communications
- In September 76 different brands were abused in Japan[††]
- Top-10 brands abused in Japan represent 82% of attacks; Top-3: Amazon, Apple, and DoCoMo are prominent[††]

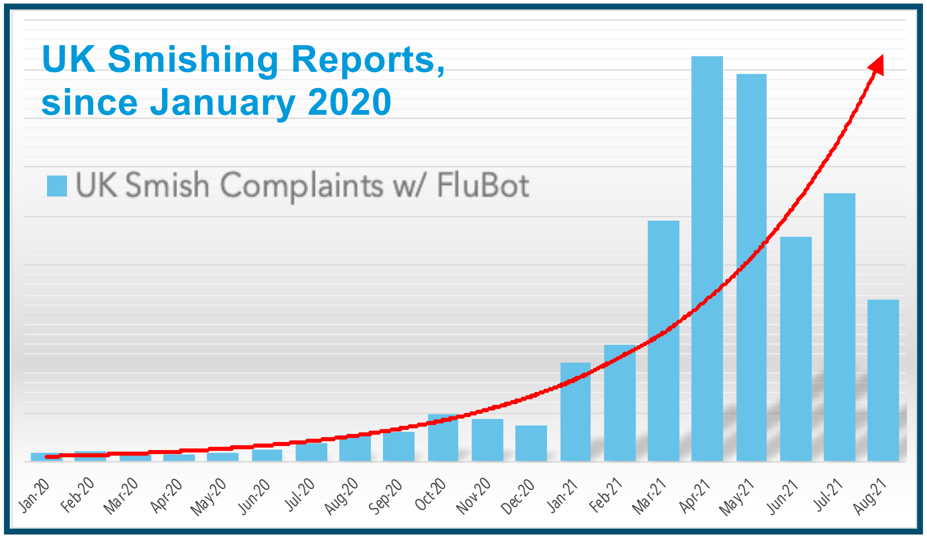
[††] Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/monthly/202109.html

proofpoint.

Regional Smishing Trends: US and UK



US Smishing Reports, since January 2019

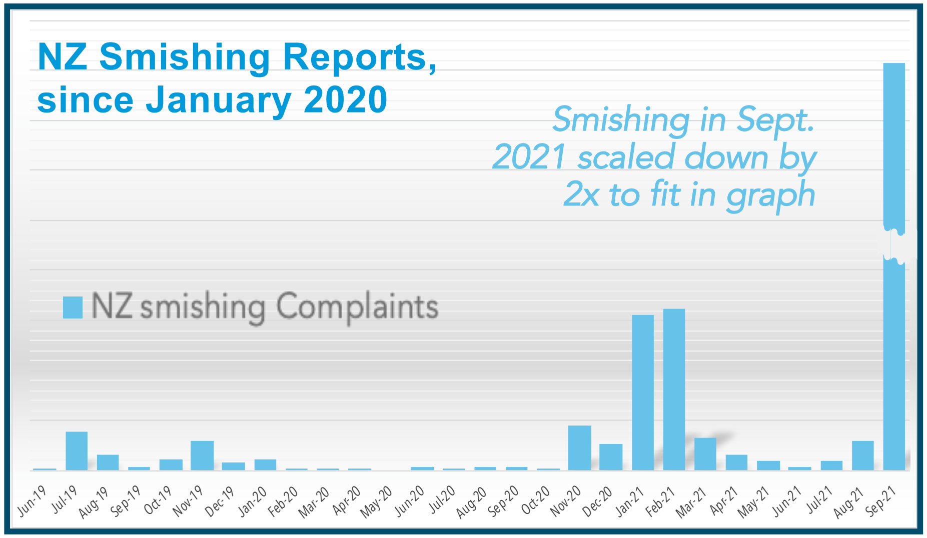


UK Smishing Reports, since January 2020

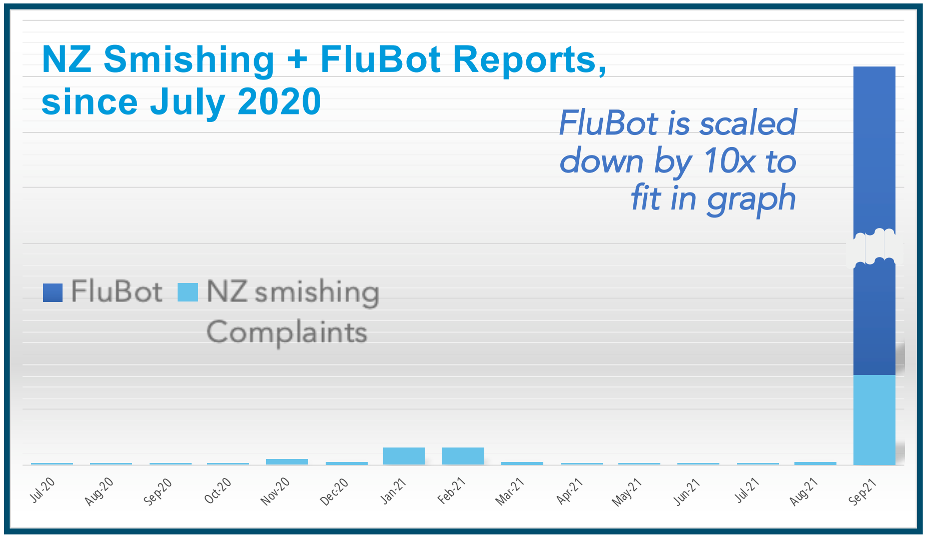
- Midyear (summer) slow down seen again
- UK: reports of smishing nearly nonexistent in UK in early 2019, aggressive growth past couple of years
- US: steady growth in smishing since beginning 2019

proofpoint.

Regional Smishing Trends: New Zealand


NZ Smishing Reports, since January 2020

Smishing in Sept. 2021 scaled down by 2x to fit in graph


NZ Smishing + FluBot Reports, since July 2020

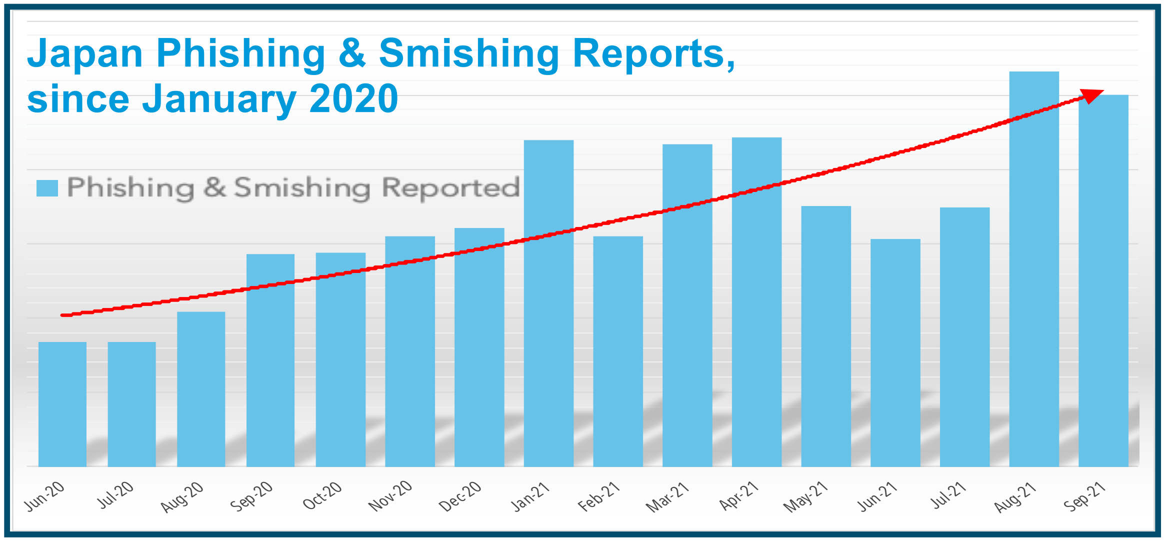
FluBot is scaled down by 10x to fit in graph

- New Zealand smishing increased in late 2020

- FluBot and other attacks (next slides) have driven up complaints in past 30 days

proofpoint.

Regional Smishing Trends: Japan



- Data from Council of Anti-Phishing Japan

- Midyear slowdown as seen elsewhere, growth restarted in August and expected to continue in 4Q2021 & 2022

proofpoint.

Rise in Package Delivery Lures

Watch Out for Bogus Delivery Notifications / Alerts

- Last few months has seen increasingly lure activity related to delivery services, package delivery notifications and exceptions
- Increase is consistent globally
  - Seen within New Zealand and Japan
  - Lures for downloading malware have leveraged parcel and package delivery
- Marked change from six to nine months ago

Global Reported 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%

US Reported 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%

NZ Reported Smish+FluBot - 3Q2021	
Parcel / Package Notification	**83.7%**
Picture and Image Related	14.5%
Financial / Banks	0.1%
Miscellaneous and Other	1.8%

2. Smishing & Threat Examples

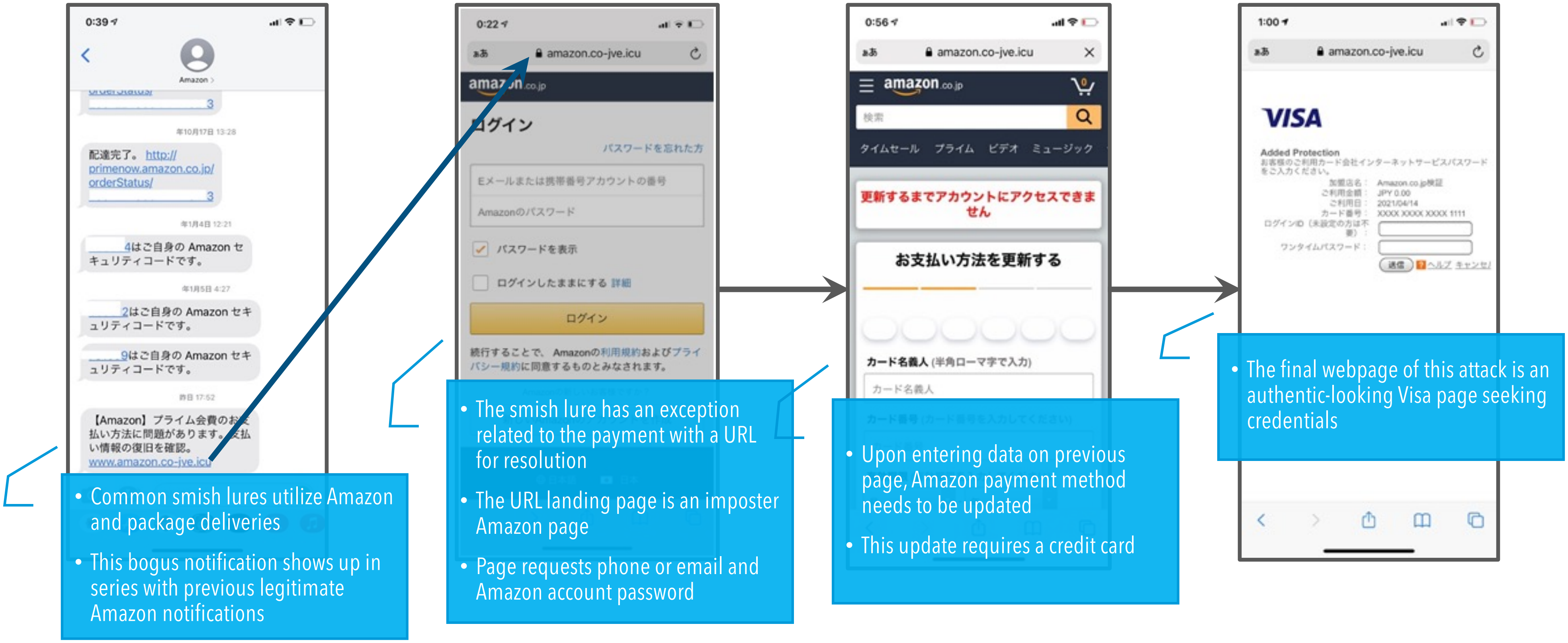
Regional: Smishing Examples

Malware: Overview and Insights

MoqHao and the Roaming Mantis group

proofpoint.

Package Delivery Smish Leading to Credential Theft



0:39

Amazon

[redacted]3

年10月17日 13:28

配達完了。http://primenow.amazon.co.jp/orderStatus/[redacted]3

年1月4日 12:21

[redacted]4はご自身の Amazon セキュリティコードです。

年1月5日 4:27

[redacted]2はご自身の Amazon セキュリティコードです。

[redacted]9はご自身の Amazon セキュリティコードです。

昨日 17:52

【Amazon】プライム会費のお支払い方法に問題があります。支払い情報の復旧を確認。www.amazon.co-jve.icu

- Common smish lures utilize Amazon and package deliveries
- This bogus notification shows up in series with previous legitimate Amazon notifications

0:22

amazon.co-jve.icu

amazon.co.jp

ログイン

パスワードを忘れた方

Eメールまたは携帯番号アカウントの番号

Amazonのパスワード

☑ パスワードを表示

☐ ログインしたままにする 詳細

ログイン

続行することで、Amazonの利用規約およびプライバシー規約に同意するものとみなされます。

- The smish lure has an exception related to the payment with a URL for resolution
- The URL landing page is an imposter Amazon page
- Page requests phone or email and Amazon account password

0:56

amazon.co-jve.icu

amazon.co.jp

検索

タイムセール　プライム　ビデオ　ミュージック

更新するまでアカウントにアクセスできません

お支払い方法を更新する

カード名義人 (半角ローマ字で入力)

カード名義人

- Upon entering data on previous page, Amazon payment method needs to be updated
- This update requires a credit card

1:00

amazon.co-jve.icu

VISA

Added Protection

お客様のご利用カード会社インターネットサービスパスワードをご入力ください。

加盟店名：Amazon.co.jp検証

ご利用金額：JPY 0.00

ご利用日：2021/04/14

カード番号：XXXX XXXX XXXX 1111

ログインID（未設定の方は不要）：

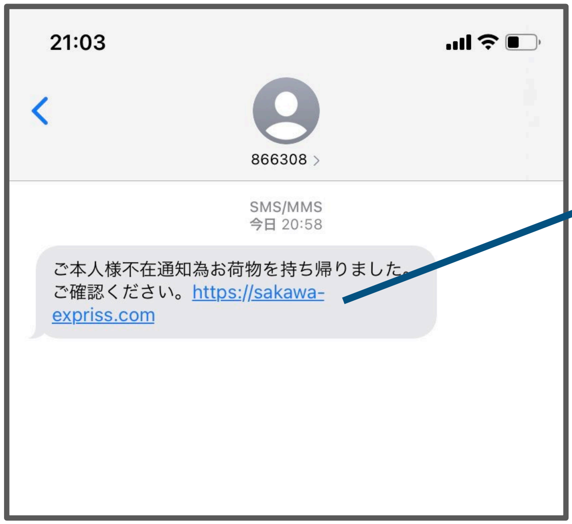
ワンタイムパスワード：

送信　ヘルプ　キャンセル

- The final webpage of this attack is an authentic-looking Visa page seeking credentials

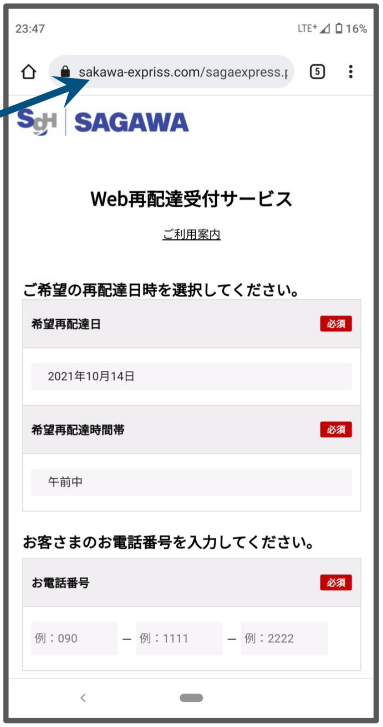
proofpoint.

Japan Smishing Examples - Sagawa



SMS/MMS
今日 20:58

ご本人様不在通知為お荷物を持ち帰りました。ご確認ください。https://sakawa-expriss.com



Web再配達受付サービス

ご利用案内

ご希望の再配達日時を選択してください。

希望再配達日 必須

2021年10月14日

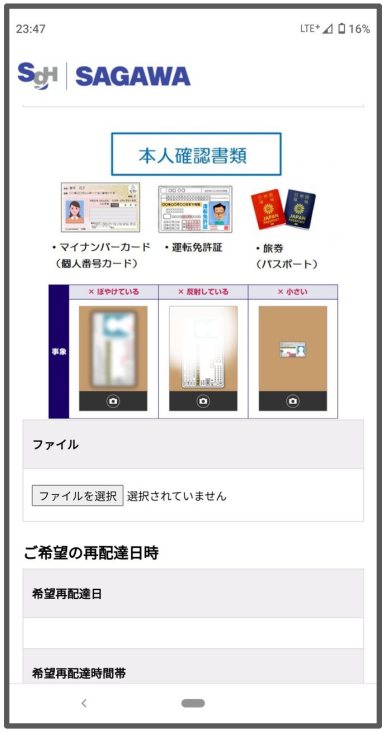
希望再配達時間帯 必須

午前中

お客さまのお電話番号を入力してください。

お電話番号 必須

例：090 – 例：1111 – 例：2222



本人確認書類

・マイナンバーカード（個人番号カード）　・運転免許証　・旅券（パスポート）

ファイル

ファイルを選択 選択されていません

ご希望の再配達日時

希望再配達日

希望再配達時間帯

- In this particular smishing attack, parcel delivery is alerted because the “recipient” was not home
- Recipient becomes a victim if tricked to schedule another delivery and provide personal information

Some source images from
https://twitter.com/NaomiSuzuki_/media

proofpoint.

Recent SMS Malware

- 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	✗	✓	✓	✓	✓	✗	✓
MoqHao	✓	✓	✓	✓	✗	✓	✗

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

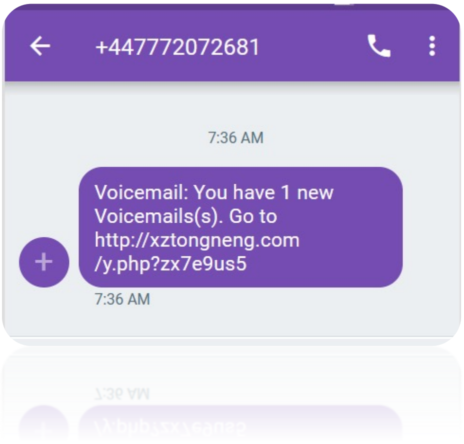
- FluBot may attack North America
  - Some "stray sightings" from UK and Germany numbers
  - A few messages from Belgium in Spanish to US numbers
  - Pattern of attack has been one country focus at a time

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

proofpoint.

TeaBot / FluBot Walkthrough

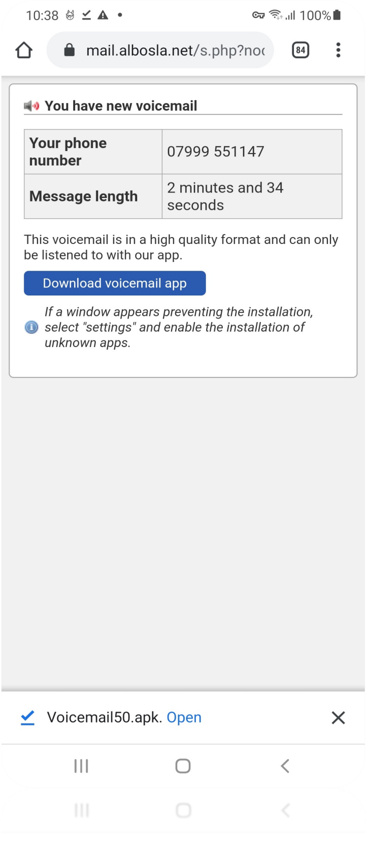


+447772072681

7:36 AM

Voicemail: You have 1 new Voicemails(s). Go to http://xztongneng.com/y.php?zx7e9us5

7:36 AM



10:38 · 100%

mail.albosla.net/s.php?noc

You have new voicemail

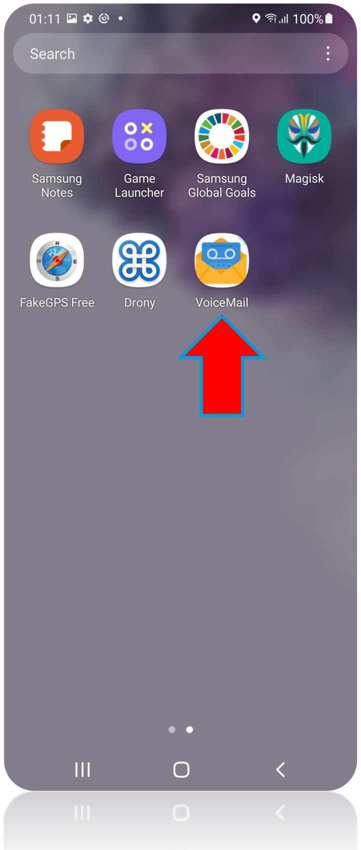
Your phone number	07999 551147
Message length	2 minutes and 34 seconds

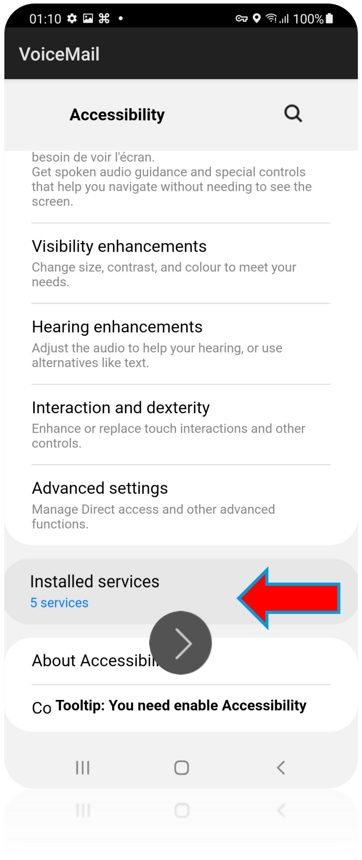
This voicemail is in a high quality format and can only be listened to with our app.

Download voicemail app

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

Voicemail50.apk. Open ✕





01:10 · 100%

VoiceMail

Accessibility

besoin de voir l'écran.
Get spoken audio guidance and special controls that help you navigate without needing to see the screen.

Visibility enhancements
Change size, contrast, and colour to meet your needs.

Hearing enhancements
Adjust the audio to help your hearing, or use alternatives like text.

Interaction and dexterity
Enhance or replace touch interactions and other controls.

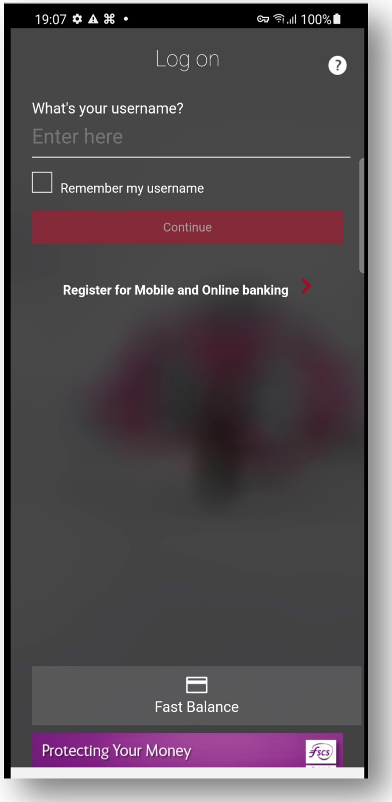
Advanced settings
Manage Direct access and other advanced functions.

Installed services
5 services

About Accessibil

Co **Tooltip: You need enable Accessibility**

TeaBot / FluBot Walkthrough



19:07 100%

Log on

What's your username?

Enter here

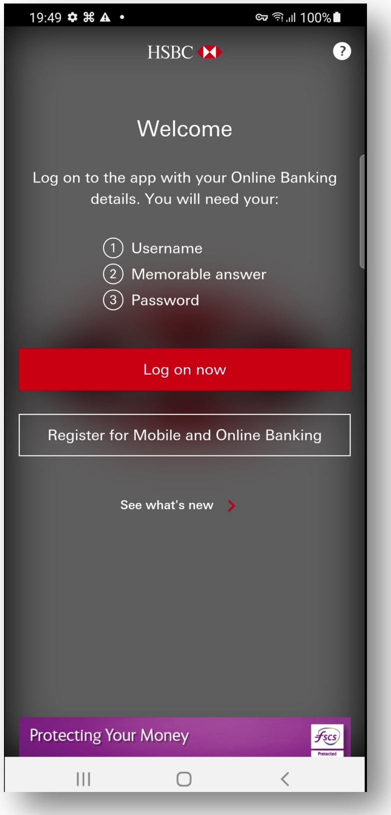
□ Remember my username

Continue

Register for Mobile and Online banking

Fast Balance

Protecting Your Money



19:49 100%

HSBC

Welcome

Log on to the app with your Online Banking details. You will need your:

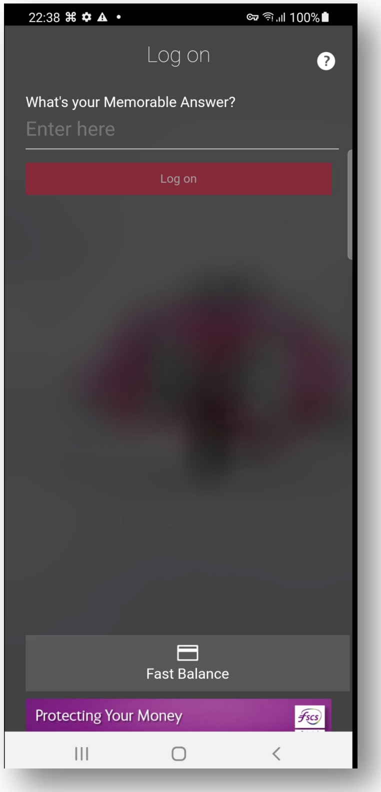
1. Username
2. Memorable answer
3. Password

Log on now

Register for Mobile and Online Banking

See what's new

Protecting Your Money



22:38 100%

Log on

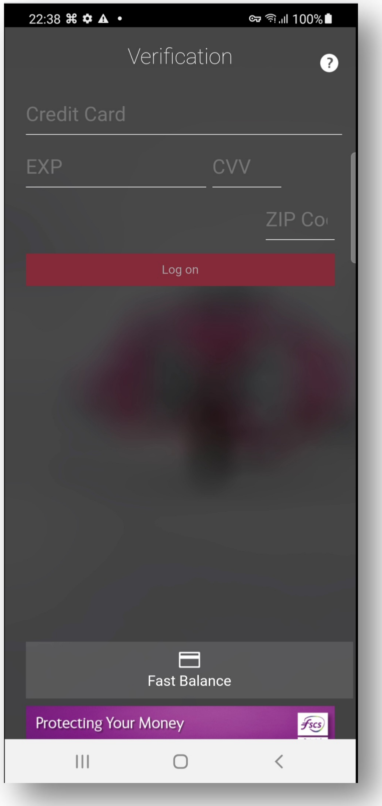
What's your Memorable Answer?

Enter here

Log on

Fast Balance

Protecting Your Money



22:38 100%

Verification

Credit Card

EXP

CVV

ZIP Co

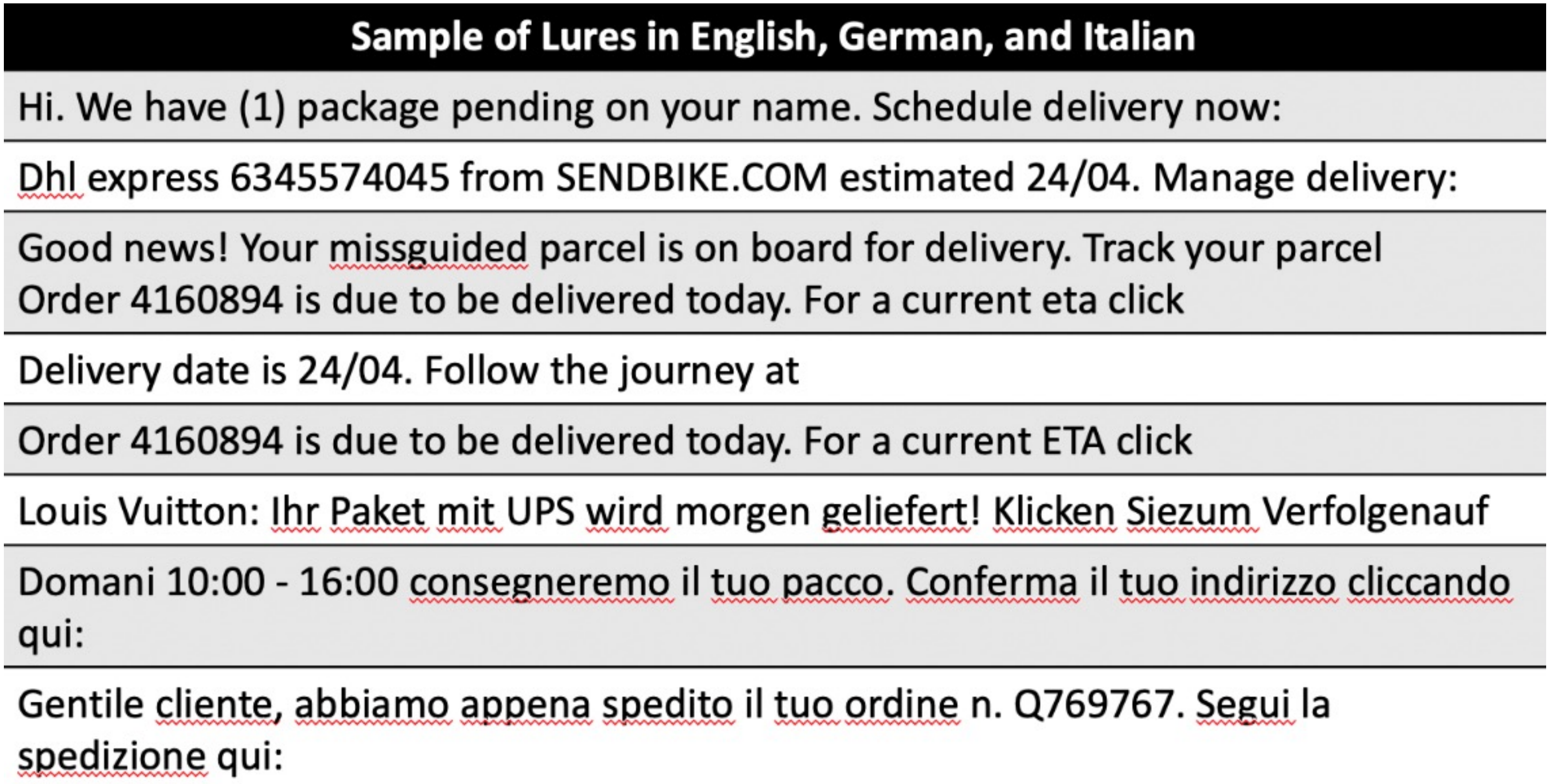
Log on

Fast Balance

Protecting Your Money

proofpoint.

FluBot Example Messages



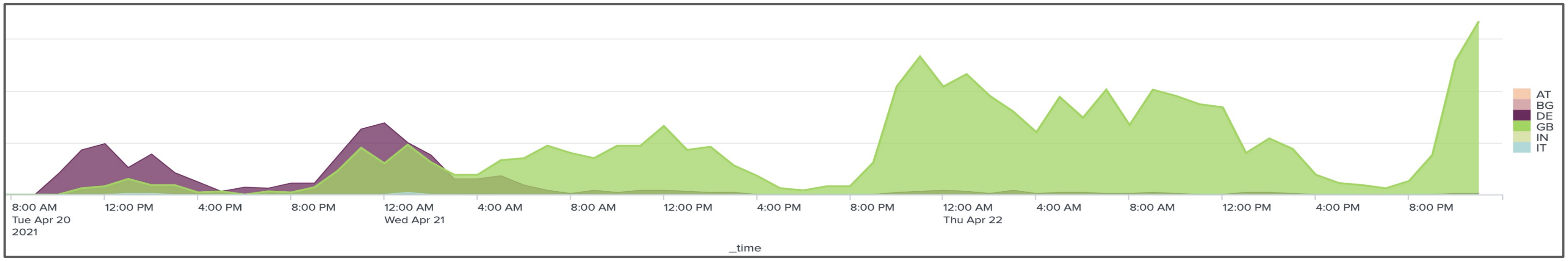
Sample of Lures in English, German, and Italian
Hi. We have (1) package pending on your name. Schedule delivery now:
Dhl express 6345574045 from SENDBIKE.COM estimated 24/04. Manage delivery:
Good news! Your missguided parcel is on board for delivery. Track your parcel Order 4160894 is due to be delivered today. For a current eta click
Delivery date is 24/04. Follow the journey at
Order 4160894 is due to be delivered today. For a current ETA click
Louis Vuitton: Ihr Paket mit UPS wird morgen geliefert! Klicken Siezum Verfolgenauf
Domani 10:00 - 16:00 consegneremo il tuo pacco. Conferma il tuo indirizzo cliccando qui:
Gentile cliente, abbiamo appena spedito il tuo ordine n. Q769767. Segui la spedizione qui:

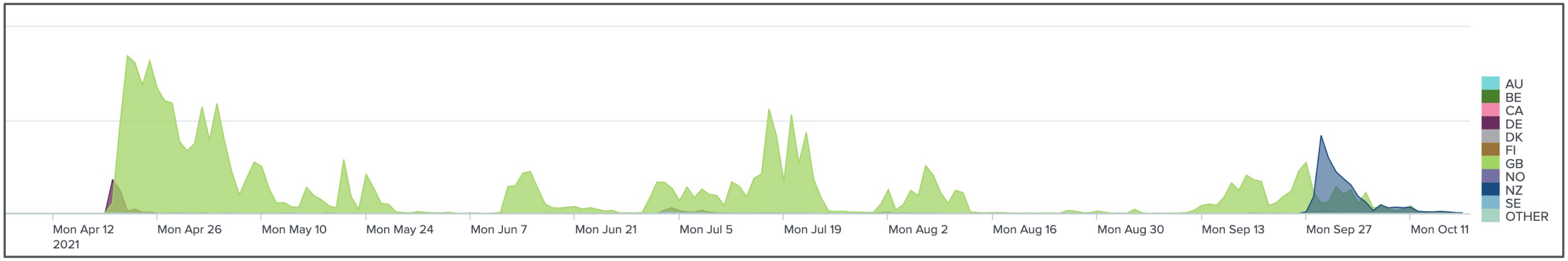
proofpoint.

FluBot Update

Tracking FluBot – systematic movement from one country to another

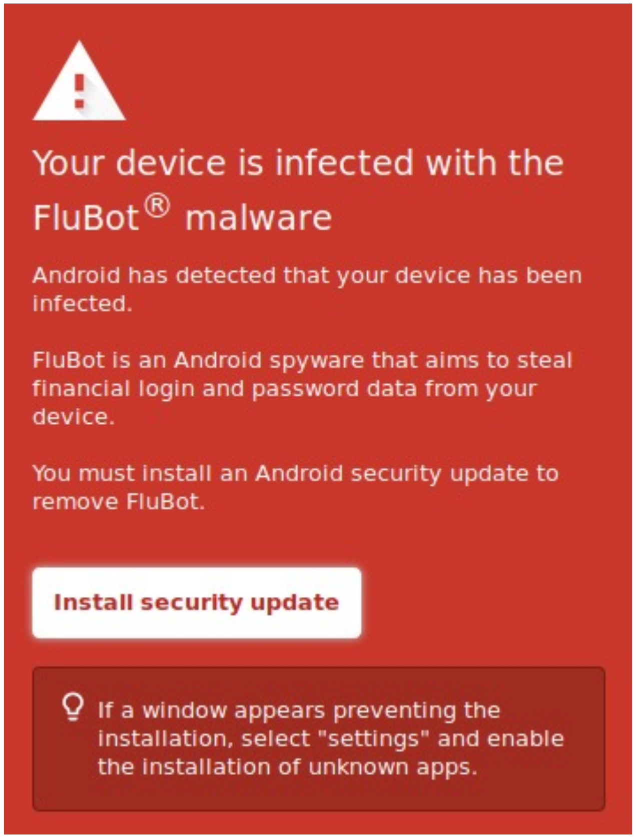
- UK FluBot v4.0 attack initiated from German mobiles, April 20th using package delivery lures (initially DHL)
- NZ FluBot attack was initiated on about September 27th using delivery lures as well





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.

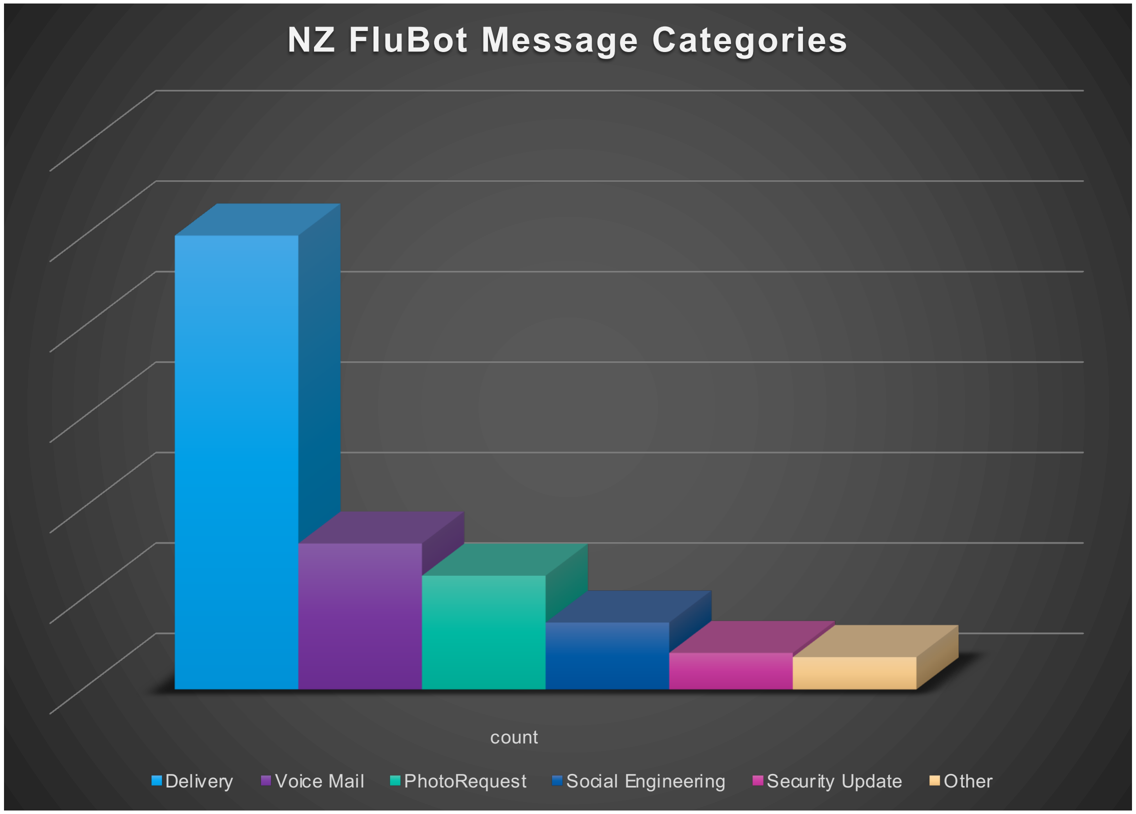
FluBot is an Android spyware that aims to steal financial login and password data from your device.

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.

NZ Message Categories (simplified)

Lure
Delivery
Voice Mail
Photo Request
Social Engineering
Security Update
Other



Roaming Mantis

Threat group utilizing SMS attack vector to target Android and iOS since 2017

Highly Attacked Regions

- Japan,
- South Korea,
- China,
- Bangladesh,
- Russia,
- India,
- Iran,
- Vietnam

Features of Attack Chain

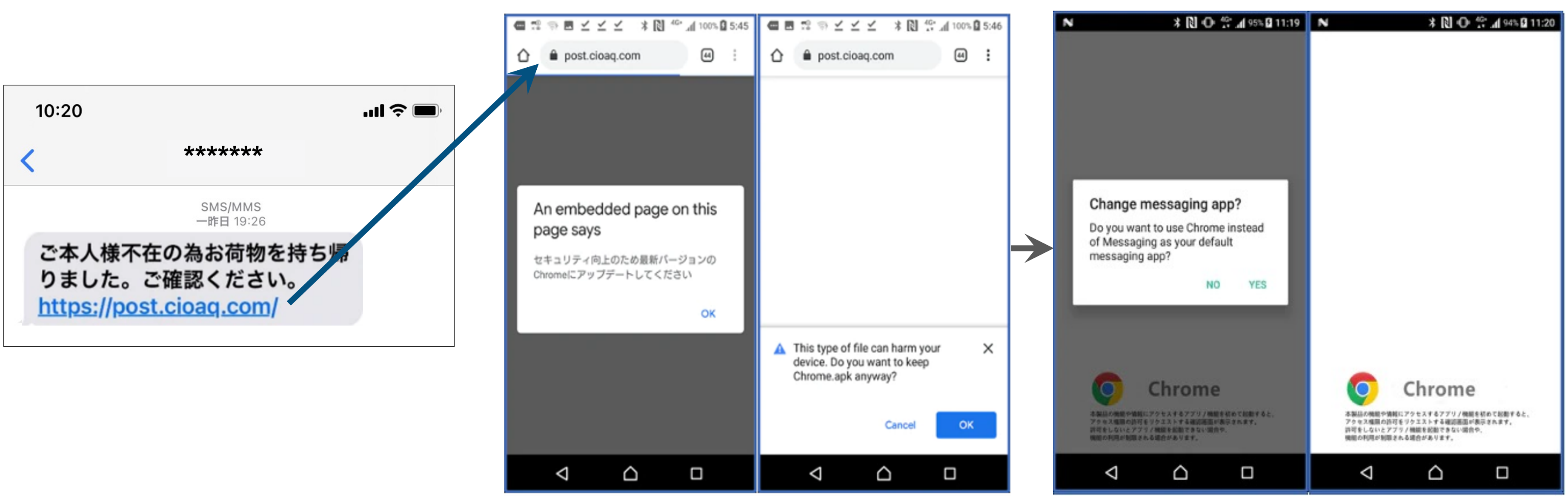
- Multilingual
- DNS Hijacking
- App (Android & iOS) local phishing
- Banking Trojan
- Crypto mining
- Message stealer
- Backdoor

Leveraging multiple malware

- MoqHao (XLoader),
- FakeSpy
- FakeCop (SpyAgent)
- Wroba (Funkybot)
- SmsSpy

- ➢ Chinese speaking attack group that leverages various malware packages and Remote Access Trojans (RATs)
- ➢ Primary objective appears to be the theft and harvesting of personal information and credentials from devices

Roaming Mantis - SmsSpy



SMS/MMS
一昨日 19:26

ご本人様不在の為お荷物を持ち帰りました。ご確認ください。
https://post.cioaq.com/

An embedded page on this page says

セキュリティ向上のため最新バージョンのChromeにアップデートしてください

This type of file can harm your device. Do you want to keep Chrome.apk anyway?

Change messaging app?

Do you want to use Chrome instead of Messaging as your default messaging app?

本製品の機能や情報にアクセスするアプリ／機能を初めて起動すると、アクセス権限の許可をリクエストする確認画面が表示されます。許可をしないとアプリ／機能を起動できない場合や、機能の利用が制限される場合があります。

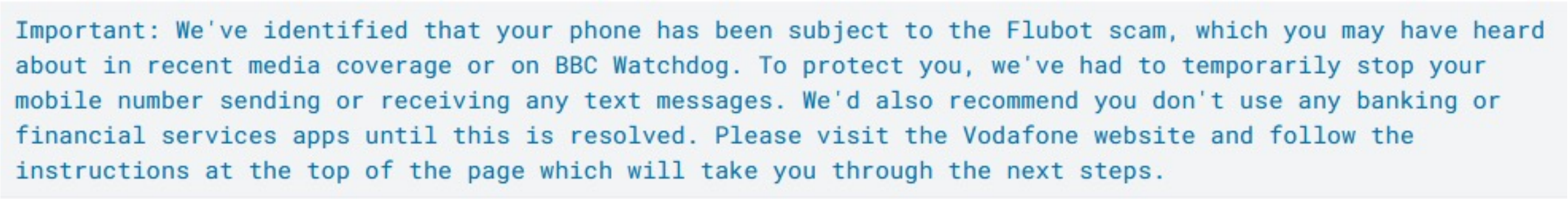
本製品の機能や情報にアクセスするアプリ／機能を初めて起動すると、アクセス権限の許可をリクエストする確認画面が表示されます。許可をしないとアプリ／機能を起動できない場合や、機能の利用が制限される場合があります。

Landing page from McAfee SmsSpy example

- ➢ SmsSpy is a frequent malware used by the Roaming Mantis attack group
- ➢ If the victim installs and authorizes the malware, SmsSpy becomes the messaging app and takes over full control of the device

FluBot

Mobile Network Operation Sends Customer Notifications



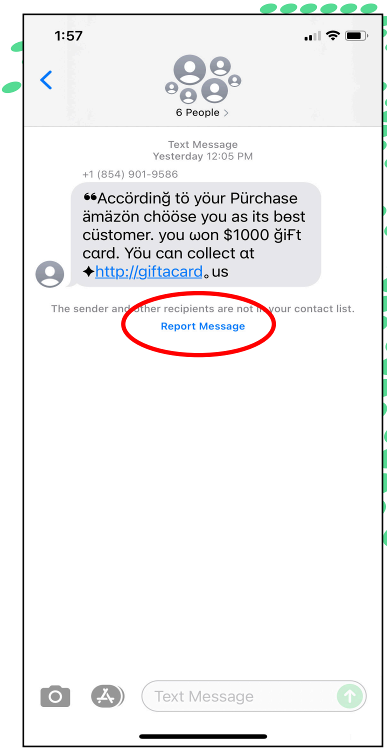
Important: We've identified that your phone has been subject to the Flubot scam, which you may have heard about in recent media coverage or on BBC Watchdog. To protect you, we've had to temporarily stop your mobile number sending or receiving any text messages. We'd also recommend you don't use any banking or financial services apps until this is resolved. Please visit the Vodafone website and follow the instructions at the top of the page which will take you through the next steps.

Best Practices

General, Spam Reporting Service, and areas for innovation

proofpoint.

Best Practice Tracking Smishing/Spam: End-User Reporting



1:57

6 People

Text Message
Yesterday 12:05 PM

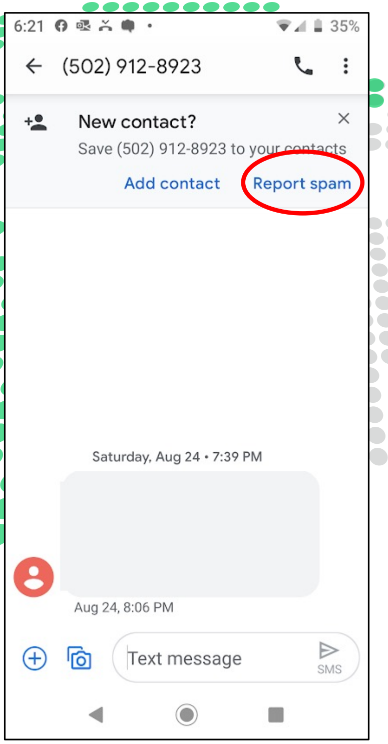
+1 (854) 901-9586

❝Accördinğ tö yöur Pürchase ämäzön chööse you as its bəst 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

Text Message



6:21 35%

(502) 912-8923

New contact?

Save (502) 912-8923 to your contacts

Add contact Report spam

Saturday, Aug 24 • 7:39 PM

Aug 24, 8:06 PM

Text message

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group

GSMA

MEF
Mobile Ecosystem Forum

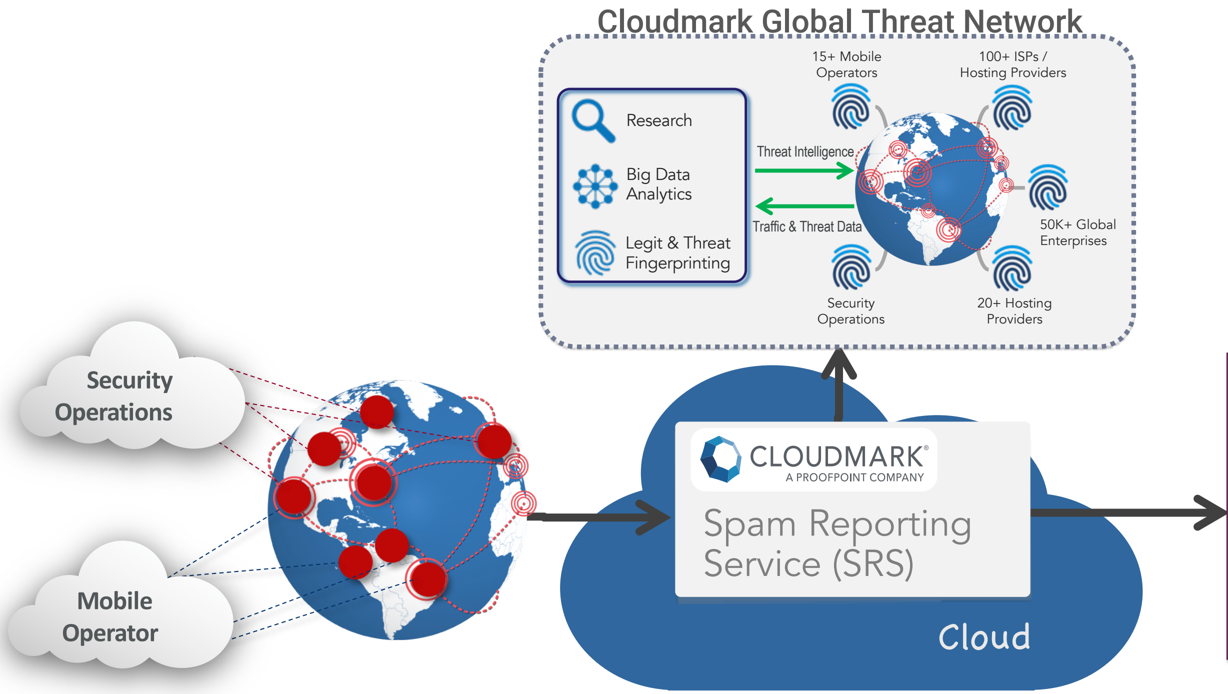
proofpoint.

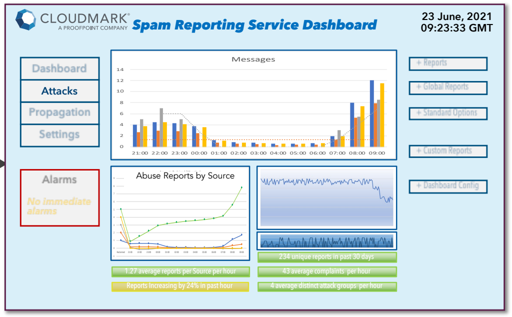
CLOUDMARK
A PROOFPOINT COMPANY

Google

- 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

Cloudmark Spam Reporting Service: Abuse Reporting





234 unique reports in past 30 days

1.27 average reports per Source per hour

43 average complaints per hour

Reports Increasing by 24% in past hour

4 average distinct attack groups per hour

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

Consolidated view of Spam:- on- & off- network abusive senders, abusive message volumes & aggregate operator volumes

proofpoint.

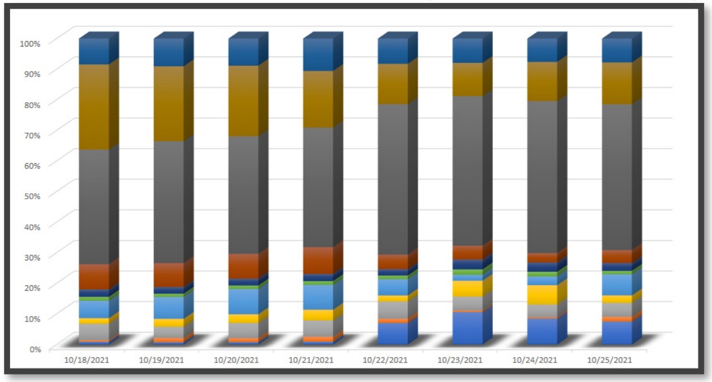
Value of Spam Reporting Service to the MNO

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

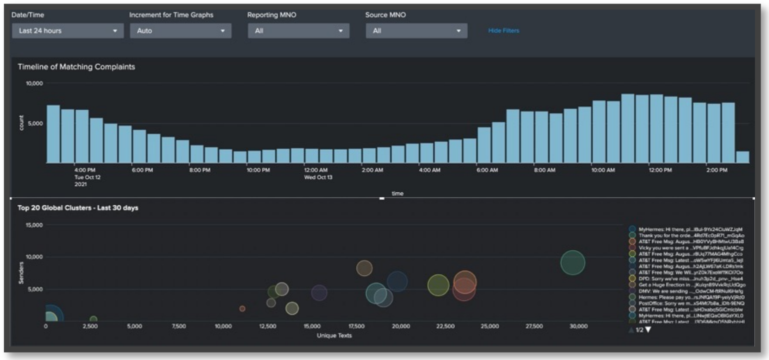
- Enables visualization and deep forensics
  - Network metrics to drive strategy and measure results
  - Detailed network and attack trend analysis
  - Nature, methods, and impacts of attacks and threats

- 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)

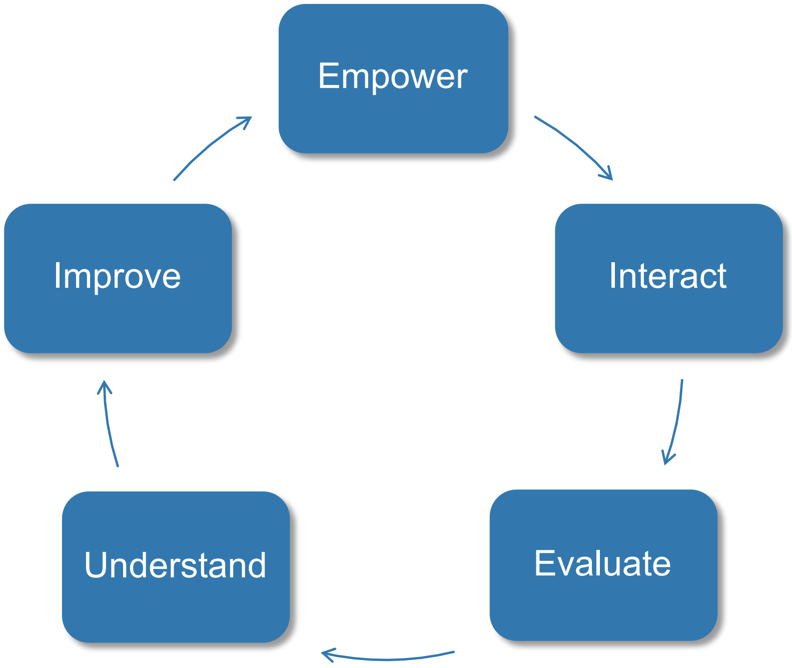


SMS Trend Visualization & Attack Clustering


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-9Yx24CiuWZJqM
Thank you for the orde...4Rd7Ec0pR71_mGqAo
AT&T Free Msg: Augus...HB0YVyBHMtwU3Ba8
Vicky you were sent a ...VPfuBFJdhkqjUa14Crg
AT&T Free Msg: Augus...r8Uq77MAG4MhgCco
AT&T Free Msg: Latest ...oW5wYFj6Umta5_lejl
AT&T Free Msg: Augus...h2AjLW67aK-LDRs1mk
AT&T Free Msg: We Wil...yrZ0k7ExoWTlKOl7Oo
DPD: Sorry we've miss...Jnuh3p2d_pnv-_Hse4
Get a Huge Erection in ...jKulqn89VvkRoUdQgo
DMV: We are sending ..._OdwCM-f8RNu6He1g
Hermes: Please pay yo...rsJNfQA19P-yeiyVjRd0
PostOffice: Sorry we m...xS4Mt7b8a_iDlt-9ENQ
AT&T Free Msg: Latest ...isHDxabc5GlCmicblw
MyHermes: Hi there, pl...LlNwjtEQsOBlGdYXL0
1/2

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.

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.

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

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.

Collaboration with Organizations Around the Globe

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

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 protections
   - Enabling and improving subscriber, end-user, reporting mechanisms and tools
   - Need major brands to issue alerts when their brand is smished/phished

proofpoint®