



CLOUDMARK®
A PROOFPOINT COMPANY

TwoFive Abuse Seminar Mobile Trends & Threats Update

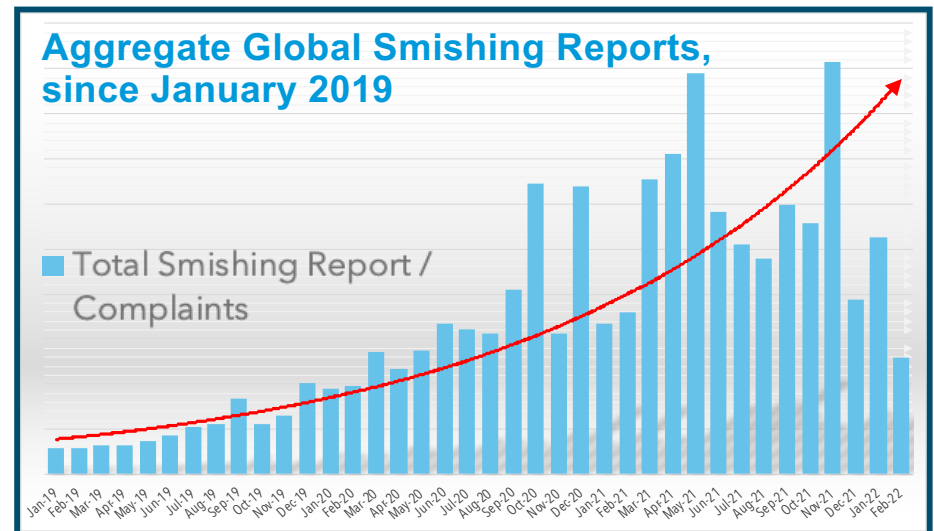
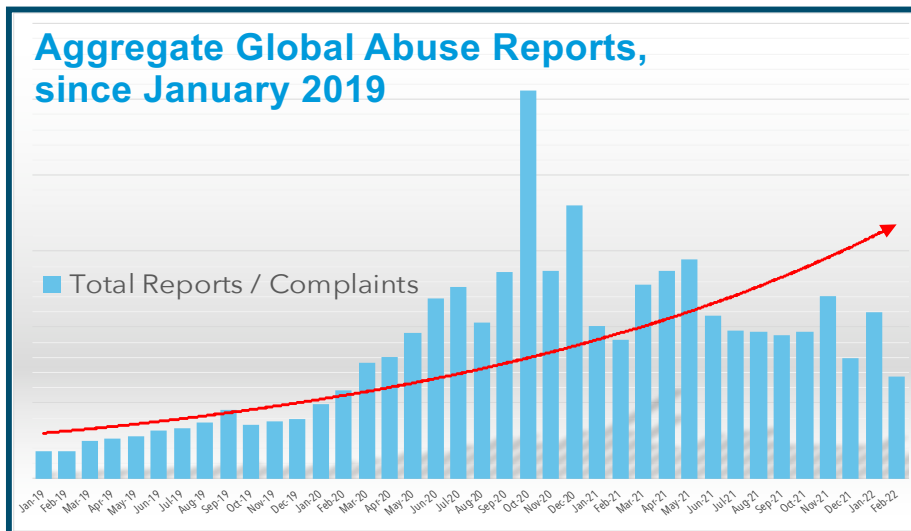
Adam McNeil, Senior Threat Research Engineer
Proofpoint, Cloudmark Division

3rd March, 2022

1. Trends Update

Abuse: Smishing and Malware increasing globally and throughout the region

Global Abuse and Smishing Generally Increasing



- Abuse, spam, smishing, and mobile malware continues to rise
- Month-to-month variations remain common, but trend line is upward with increasing “trickery” and focus on lures that succeed
- Focus today is on threats to Japan and region, primarily **Smishing** and **Malware**

proofpoint.

© 2022 Proofpoint. All rights reserved

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”**
 - **Within US, 73% of the businesses report being compromised at some level due to smishing**

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

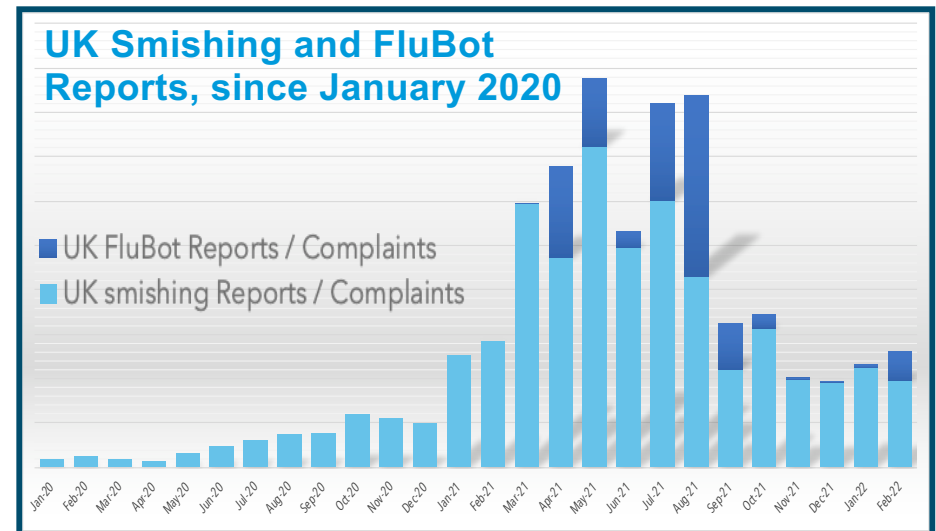
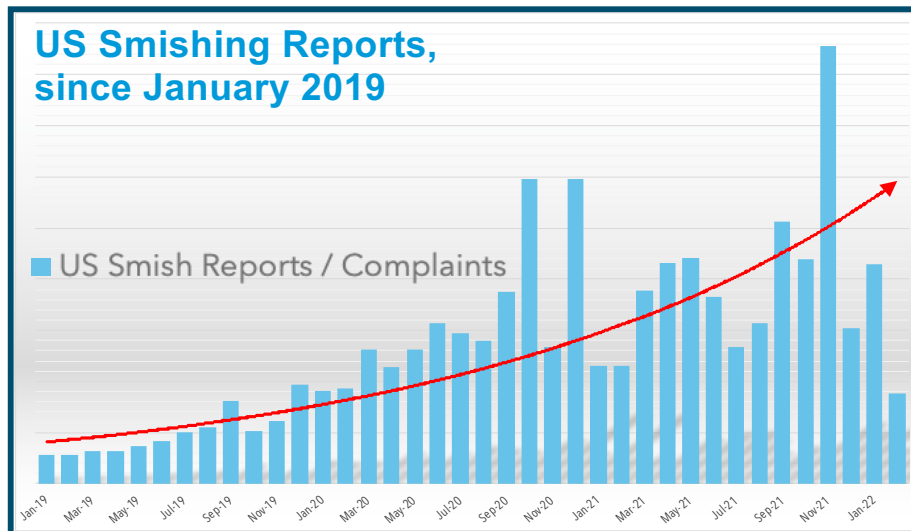
- Brand erosion and decreased consumer trust due to consumer vulnerability
- Large volume smishing and malware attacks cause direct impact on MNO operations/expense
- Increased customer support calls and complaints plus follow up with device sanitization causes financial loss

Enterprise/Corporate Impact

- Brand erosion due to impersonation attacks and consumer misidentification of bona fide corporate communications
- In January 2022, 86 different brands were abused in Japan^{††}, steadily increasing
- Top-10 brands abused in Japan represent 82% of attacks; Top-3: Amazon, Apple, and DoCoMo are prominent^{††}

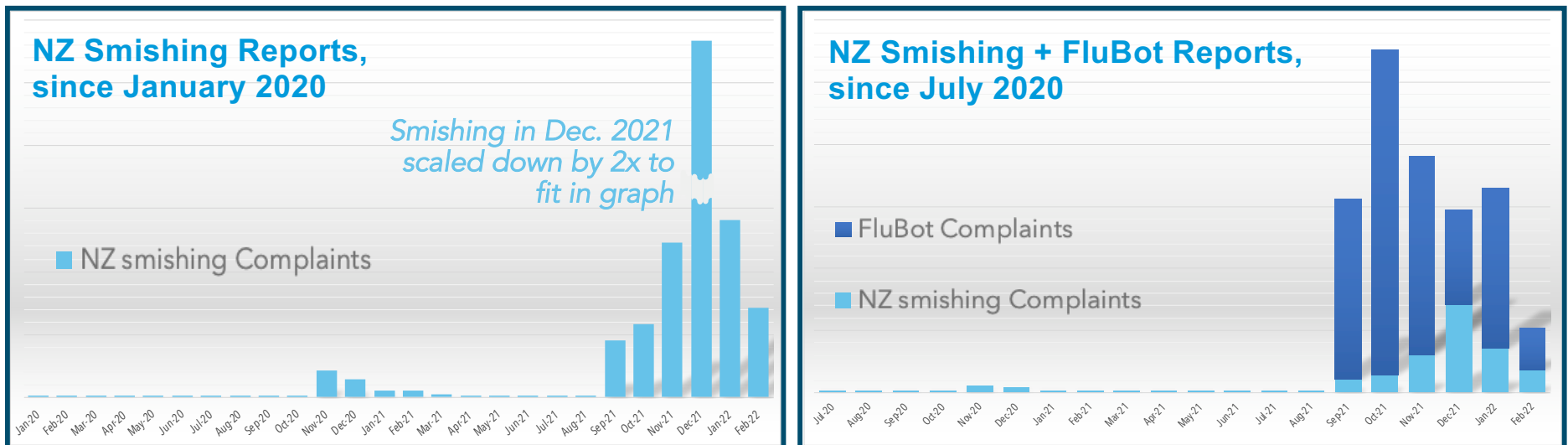
^{††} Council of Anti-Phishing Japan
<https://www.antiphishing.jp/report/monthly/202109.html>

Regional Smishing Trends: US and UK



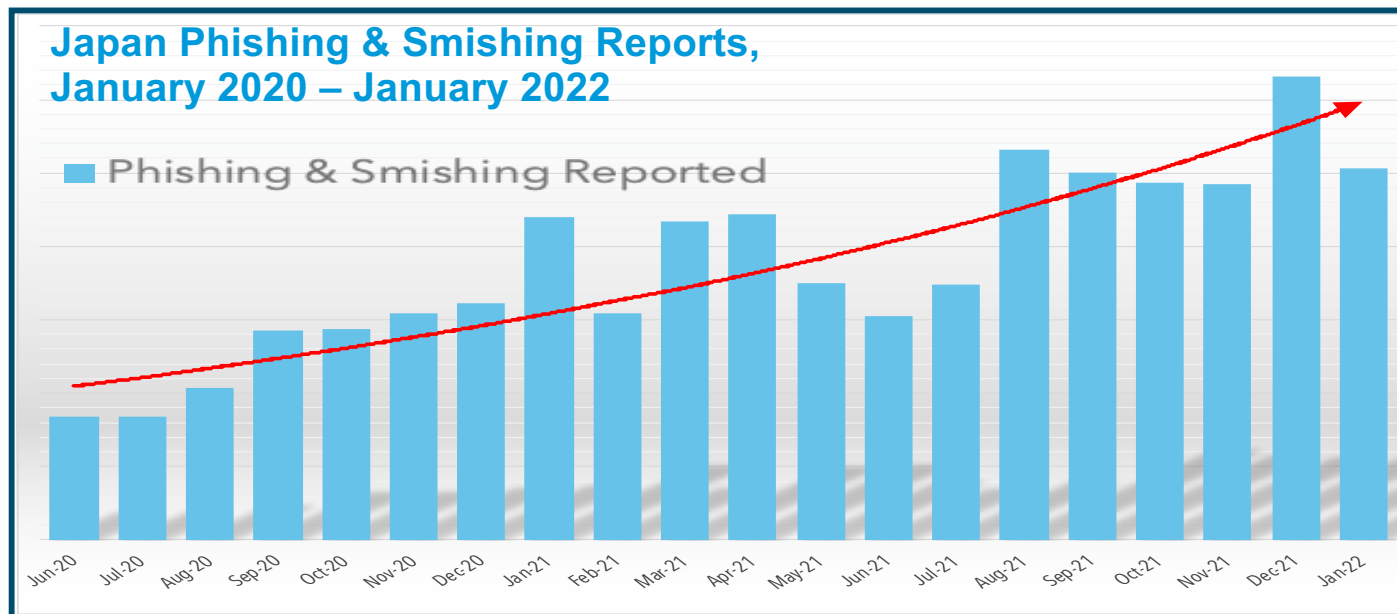
- Mid- to late-year slowdowns are common, there is variance, but trend is upward
- US: steady growth in smishing since beginning 2019
- UK: reports of smishing nearly nonexistent in UK in early 2019, aggressive growth past couple of years, including FluBot attack starting April 2021

Regional Smishing Trends: New Zealand



- New Zealand smishing increased in late 2020
- FluBot and other attacks have driven up complaints since late 2021

Regional Smishing Trends: Japan



- Data from Council of Anti-Phishing Japan
- Midyear slowdown as seen elsewhere, growth restarted in August and generally has continued

Rise in Package Delivery Lures

Watch Out for Bogus Delivery Notifications / Alerts

- Last few quarters have seen increasingly lure activity related to delivery services, and package delivery notifications
- Increase is consistent globally
 - Seen within New Zealand and Japan
 - Lures for downloading malware have leveraged parcel and package delivery
- Marked change in lures from 2020 and early 2021

proofpoint.

© 2022 Proofpoint. All rights reserved

UK Reported Smishing - 4Q2021

Parcel / Package Notification	70.5%
Merchant & Consumer Brands	1.9%
Financial / Banks	1.6%
Picture and Image Related	0.5%
Telecoms & Media	0.4%
Miscellaneous and Other	25.1%

Global Smishing - 4Q2021

Merchant & Consumer Brands	28.9%
Parcel / Package Notification	26.0%
Telecoms & Media	16.9%
Financial / Banks	5.1%
Picture and Image Related	1.3%
Miscellaneous and Other	21.9%

NZ Reported Smish+FluBot - 4Q2021

Parcel / Package Notification	80.6%
Picture and Image Related	7.9%
Merchant & Consumer Brands	7.7%
Financial / Banks	0.9%
Telecoms & Media	0.4%
Miscellaneous and Other	2.5%

2. Smishing & Threat Examples

Regional: Smishing Examples

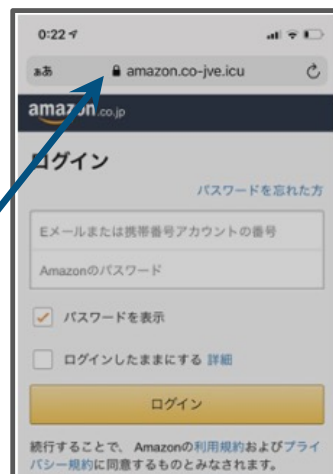
Malware: Overview and Insights

MoqHao and the Roaming Mantis group

Package Delivery Smish Leading to Credential Theft



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



- 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

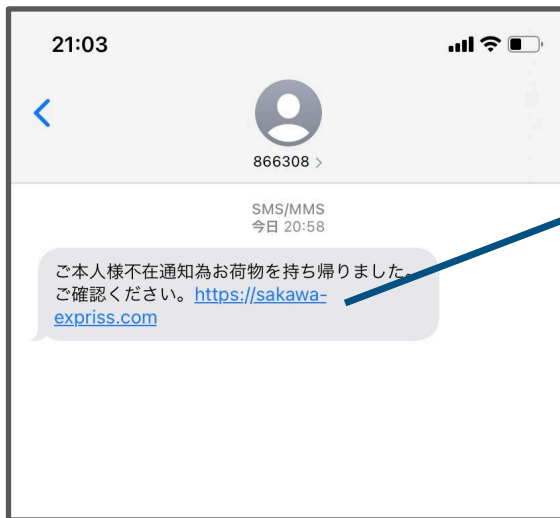


- Upon entering data on previous page, Amazon payment method needs to be updated
- This update requires a credit card



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

Japan Smishing Examples - Sagawa

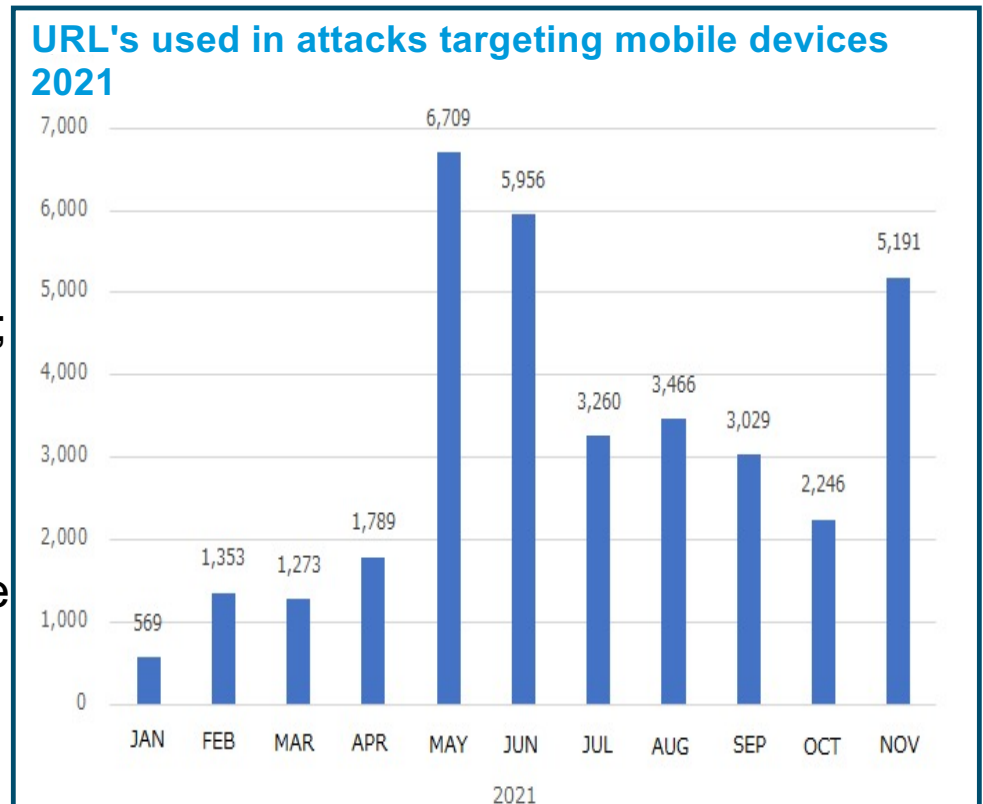


- In this smishing attack, parcel delivery is alerted because the “recipient” was not home
- Recipient becomes a victim if tricked to schedule another delivery and provide personal information

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

Regional Malware Trends: Japan

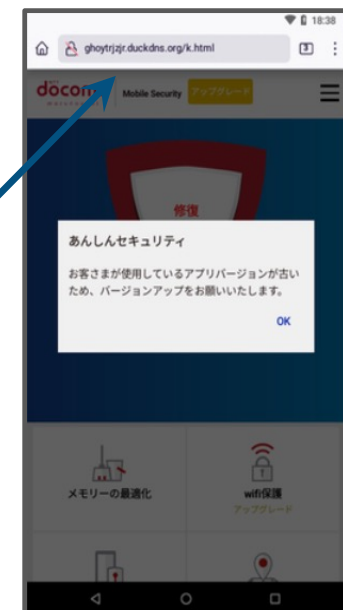
- Data from JPCert
- URL's targeting mobile devices increasing
- Midyear slowdown as seen elsewhere; growth restarted in 4Q2021 & 2022
- Trend is consistent globally
 - URL's for downloading malware have leveraged parcel and reservation apps, Covid-19, and financial messages.



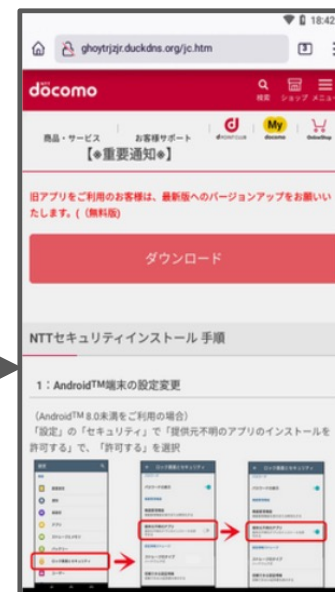
Package Delivery Smish Leading to Malware

- Common malware lures utilize delivery notices, reservation apps for Covid-19 vaccination
- SMS messages direct users to visit websites hiding behind URL shortener services or Dynamic DNS providers

- Malicious websites may be crafted to appear as legitimate websites from known companies



- Fake notice for Docomo Anshin Security



- The page informs the user how to install the malicious application to their device



- The final page delivers the malware file.
- Installation is not complete until user completes the installation process

FluBot Aggressive Mobile-based Malware Attack

Sophisticated worm-like malware attack. In the wild in Europe since November, 2020

Mobile Network Operator (MNO) Impact

- Brand erosion and decreased consumer trust due to consumer vulnerability
- Increased customer complaints and tech support follow up assisting subscribers to sanitize devices







Subscriber and Enterprise Employee Impact

- Loss of Personal information and data
- Smishing of banking credentials
 - FluBot places “overlay” screens impersonate legitimate apps to steal login credentials directly from the subscriber
- 15k to 20k infected devices in UK
- 3k to 4k infected devices in the NZ alone

- Lures have varied
 - Initially used package delivery lures, including DHL, FedEx, Correos, Royal Mail, others...
 - Subsequent lures have included
 - Google, and other, fake voice-mail notifications
 - generic “message” alerts and notifications
 - In low quantities using BBC, awards, boarding passes, and miscellaneous retailers
 - In the UK and Europe current most prominent lures are the voicemail notification and shipping lures
- Authentic-looking message or notification has link to compromised website prompting download of legitimate-looking Android Application Package (APK)

Recent SMS Malware

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

	Target OS	App Impersonation	Financial Impersonation	Multi-Modal (Social Media)	Credential Theft	Microphone and Camera	SMS Spreading	Privilege Escalation	Geographic Region
<i>FluBot</i>		✓	✓	✗	✓	✗	✓	✓	UK / Europe
<i>TeaBot</i>		✓	✓	✓	✓	✗	✓	✓	UK / Europe
<i>TangleBot</i>		✗	✓	✓	✓	✓	✗	✓	North America
<i>Moqhao</i>		✓	✓	✓	✓	✗	✓	✗	Asia / Japan
<i>TianySpy</i>	 	✓	✓	✗	✓	✗	✗	✗	Japan

Roaming Mantis

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

Highly Attacked Regions

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

Features of Attack Chain

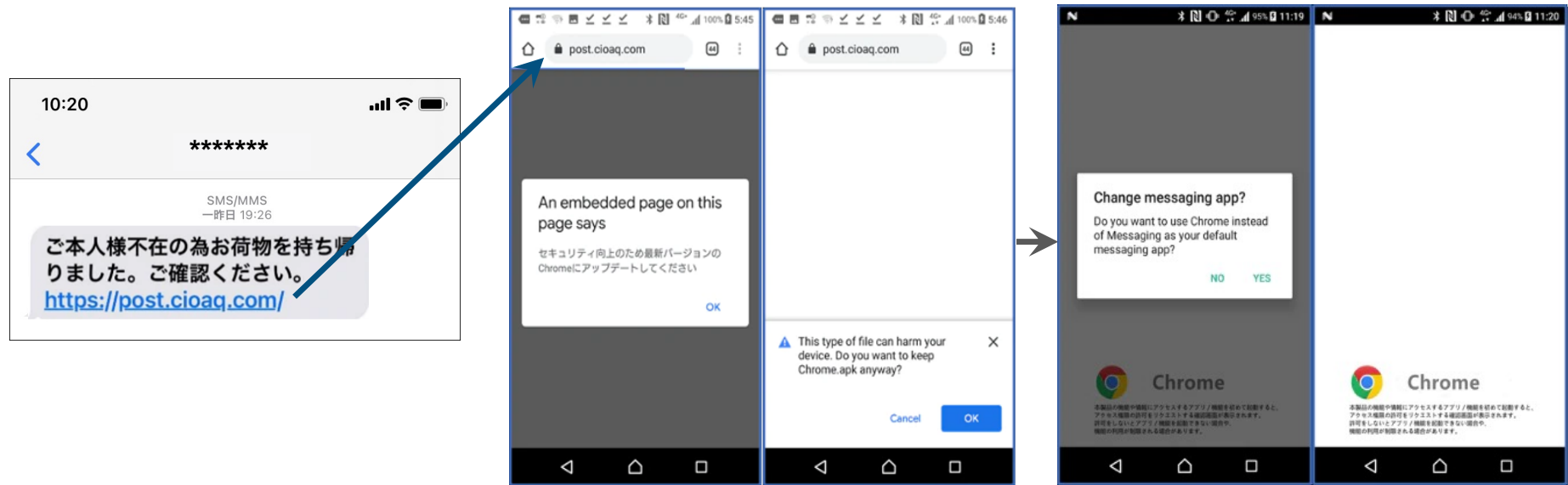
- Multilingual
- DNS Hijacking
- App (Android & iOS) local phishing
- Banking Trojan
- Crypto mining
- Message stealer
- Backdoor

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



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

Collaboration with Organizations Around the Globe



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®

© 2022 Proofpoint. All rights reserved