Mobile Abuse Recent Trends & Threats

proofpoint®

CLOUDMARK®
A PROOFPOINT COMPANY

- *November 2023*
- *Fumio Igarashi, Senior Solution Architect*

Mobile Abuse Trends

プルーフポイント社: 急速に拡大するスミッシングを観察

世界のスミッシング、166%以上の伸び

スミッシュの攻撃は増加傾向†

- グローバル企業の74% *(横ばい傾向、2022年に74%と報告††)*
- 北米企業の85% (*2022年に75%から上昇と報告*)
- 豪州企業の92% (90%から上昇) 、そして
- 日本企業の56%(74%から減少)、従業員がスミッシング攻撃に直面したことがあると報告

スミッシングに対する認識の低さ (2022 レポートより††)

- 世界全体の23%
- 米国のでは24%
- 豪州での25%、そして
- 日本での17%の人が "smishing "という言葉を正しく認識している

- 攻撃者は、世界と日本国内での成功(と失敗)に基づき戦術を進化させ、使用
- 巧妙な会話による不正行為は増加の一途をたどっており、これを防ぐのはより困難になっている

† Proofpoint. ”2023 State of the Phish”, February 2023.
†† Proofpoint. ”2022 State of the Phish”, February 2022.

proofpoint.

スミッシングの明白なリスク

スミッシングはモバイル・バリューチェーンのすべての人に影響を及ぼす

消費者に与える影響

- 日本: 2023年上半期、フィッシング詐欺による被害額は過去最高の30億円に†
- オーストラリア: 政府の発表によると、フィッシングおよびスミッシングによる被害額は1億6900万豪ドル以上
- 米国: 2022年のフィッシング詐欺による被害額は3億3,000万ドルを超え、2021年の2倍に上る (連邦取引委員会)

移動体通信事業者への影響

- 顧客/加入者からの苦情が増加し、サポートコールが増加、さらにデバイスのサニタイズの可能性についてもフォローアップが必要
- 大量に発生するスミッシングやマルウェア攻撃により、MNOの運営/コストに直接的な影響
- 消費者の脆弱性によるブランド低下と消費者の信頼低下

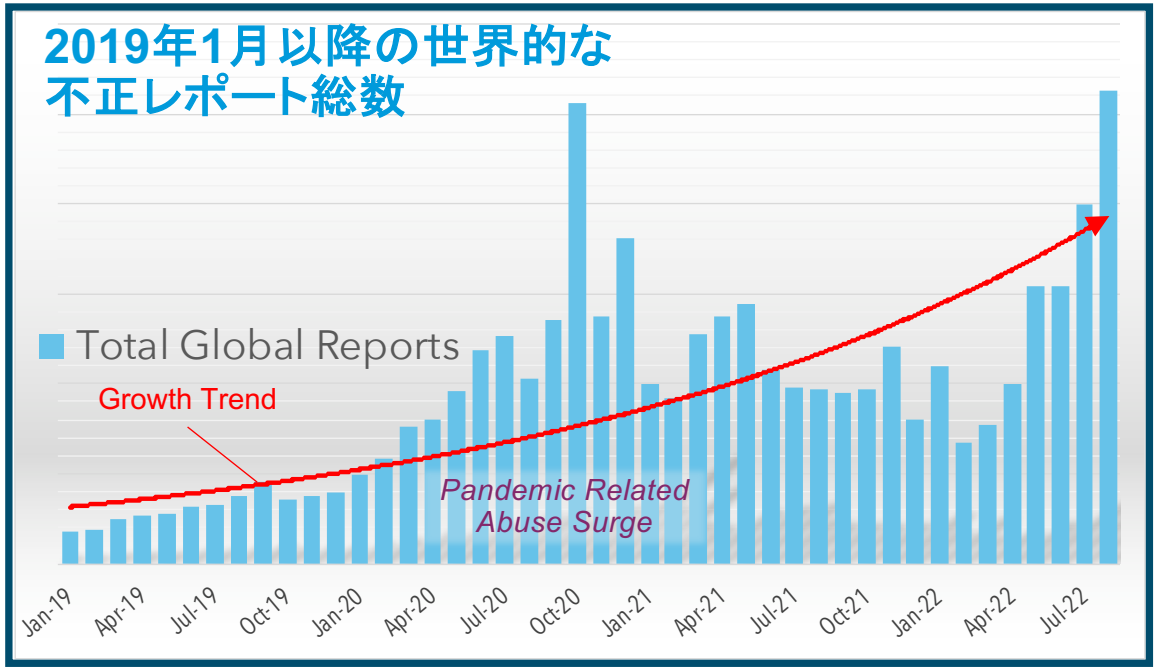
企業/法人への影響

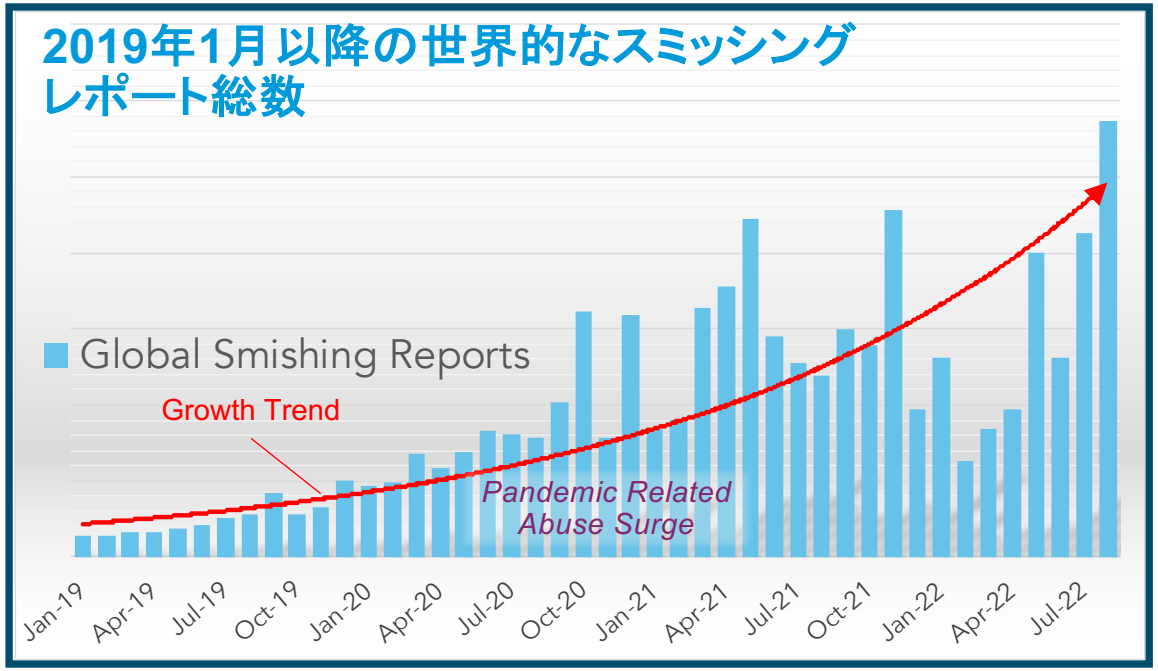
- なりすまし攻撃と消費者による善意の企業コミュニケーションの誤認によるブランド力の低下
- 日本では2023年1～9月に月平均94のブランドが悪用され ††、3月と5月のピーク時には毎月110のブランドが悪用された
- 日本で悪用された上位17のブランド攻撃で94%を占めており、アマゾン (単独で40%)、アップル、携帯キャリアが目立つ ††

† The Japan Times. https://www.japantimes.co.jp/news/2023/08/09/japan/money-stolen-phishing/. 9 August, 2023.

†† Council of Anti-Phishing Japan https://www.antiphishing.jp/report/monthly/202309.html

iOSからのレポート以前のグローバル不正報告



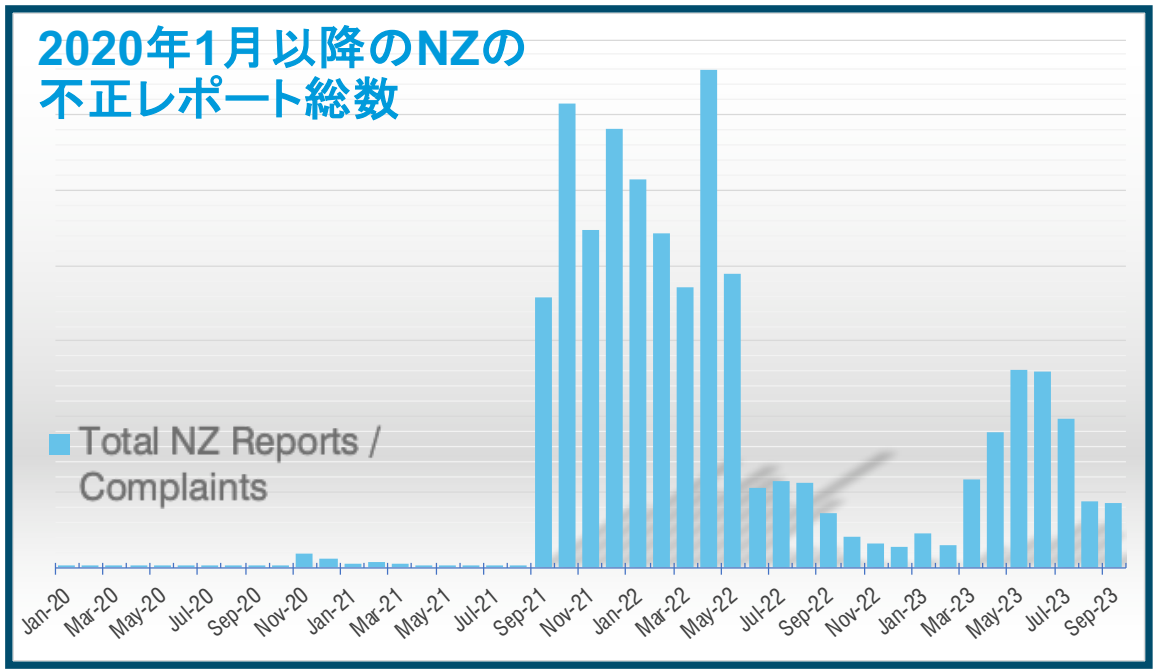


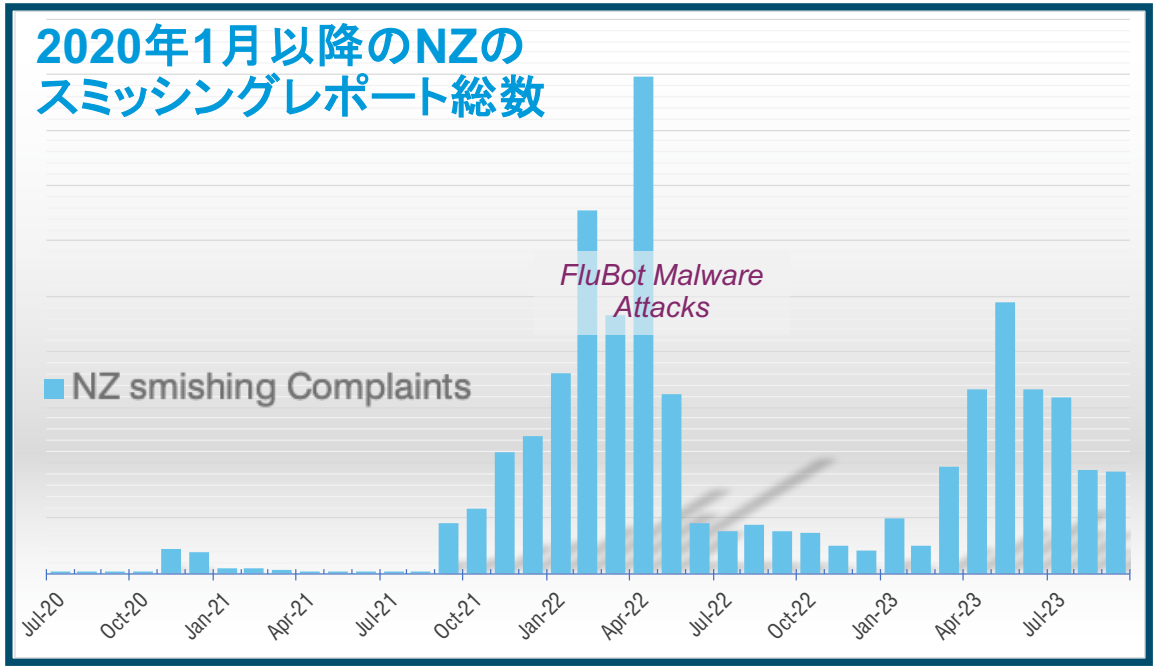
Update: 230705

- 2019年以降、不正は増加しており、月ごとに変動がある
- 特定の攻撃やキャンペーンが複数月の変動を引き起こすことがある
- 次のスライドに示すように、iOSのシンプルなレポートが規模を変える

proofpoint.

NZの不正とスミッシングが一般的に増加中



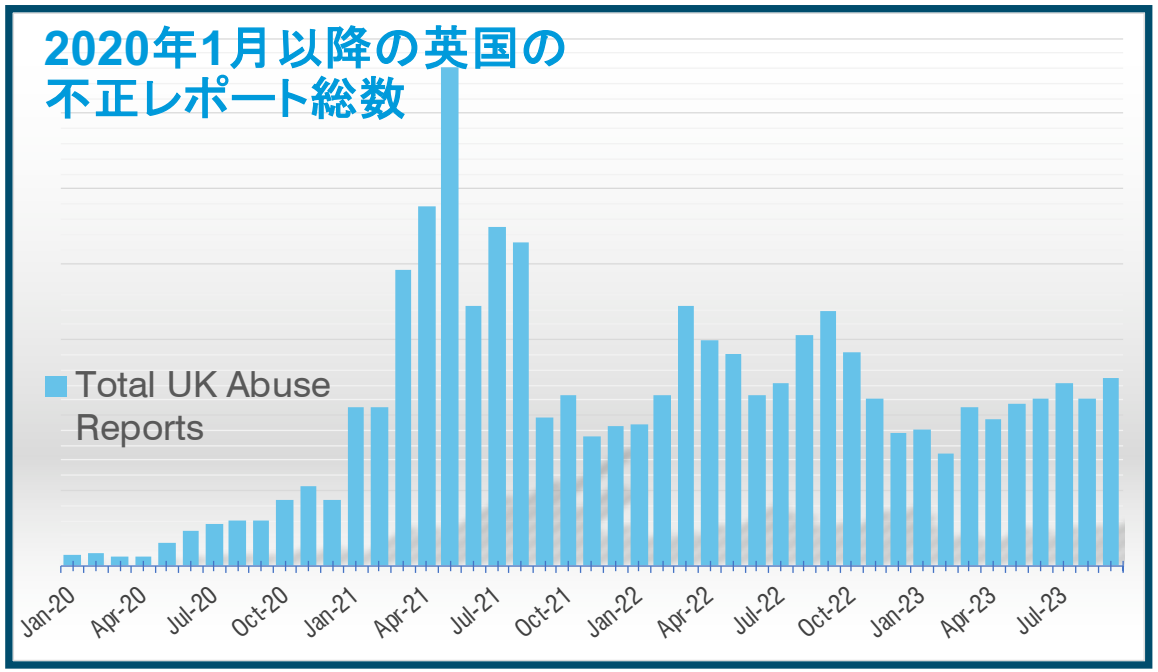


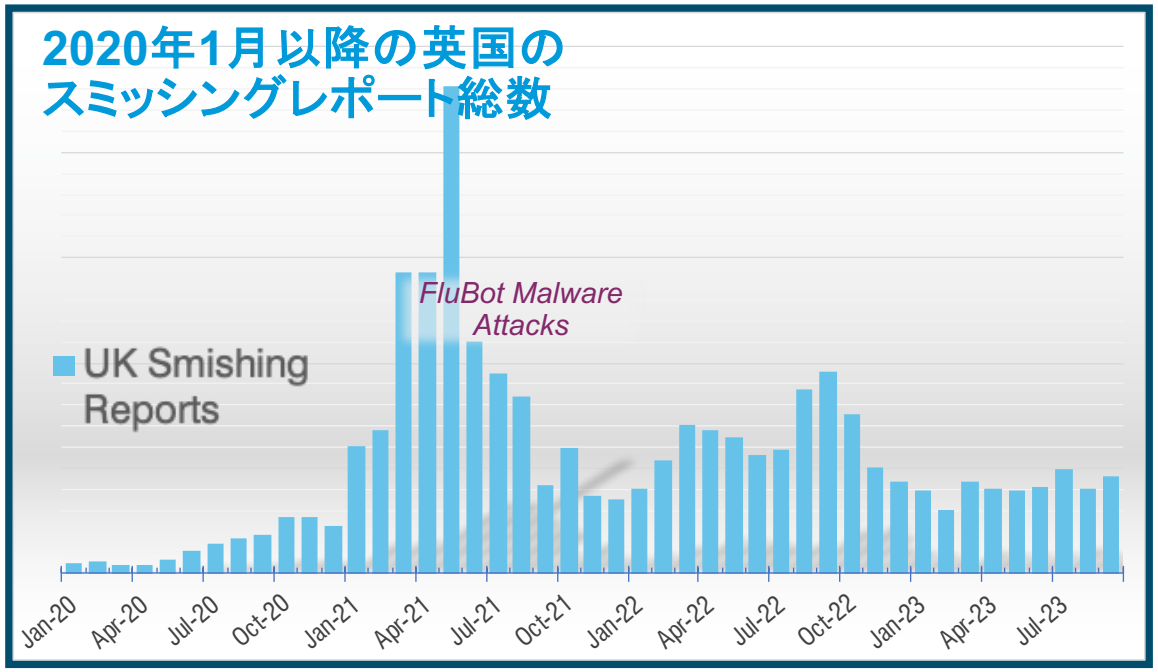
Update: 231006

- 他地域と同様、前月比で変動あり
- 2021年後半から2022年前半にかけて、FluBotが不正の大きなスパイクを引き起こした
- FluBotが減少した後、全般的な攻撃は減少したが、FluBot以前と比較すると再び増加

proofpoint.

英国における不正とスミッシングの増加



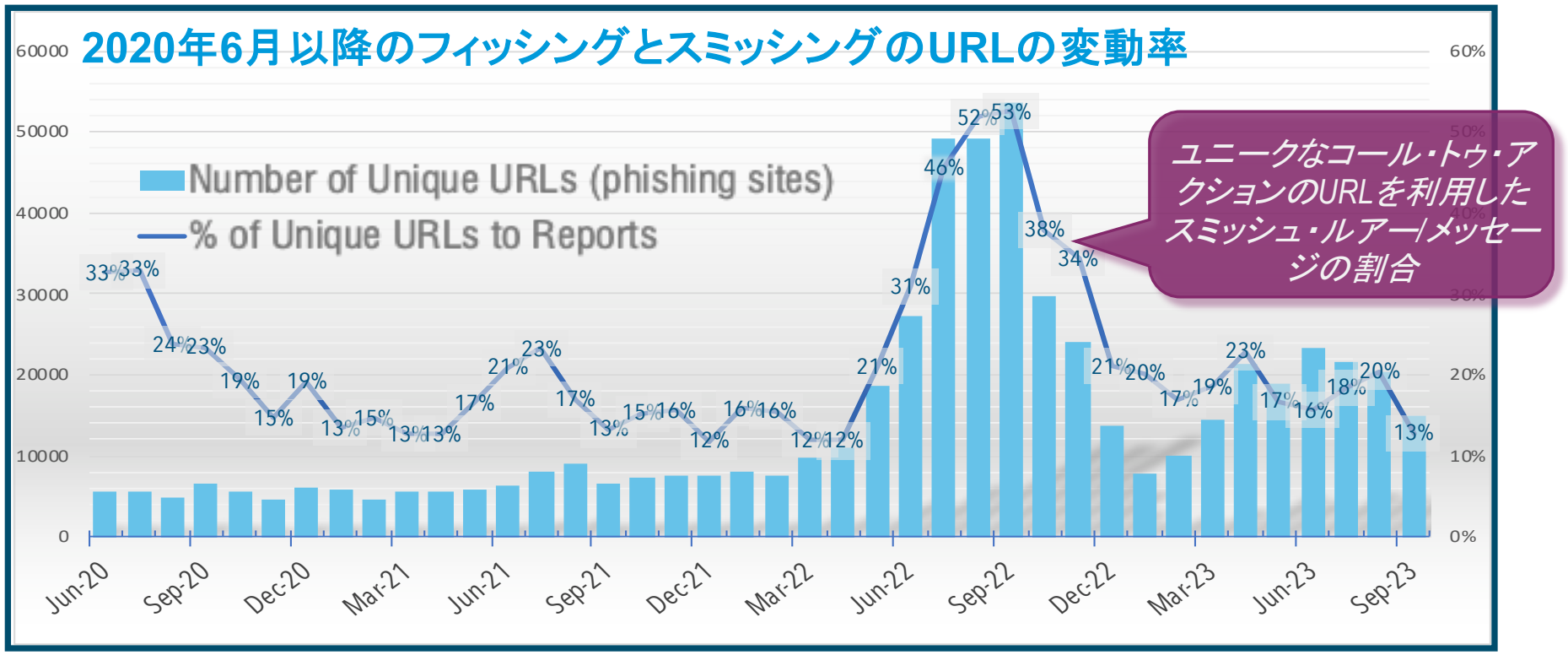


Update: 231006

- 前月比で再び変動
- 2021年、FluBotが不正の大きなスパイクを引き起こした
- iOS向けシンプルレポートの提供開始

proofpoint.

URLローテーションが示す巧妙さ



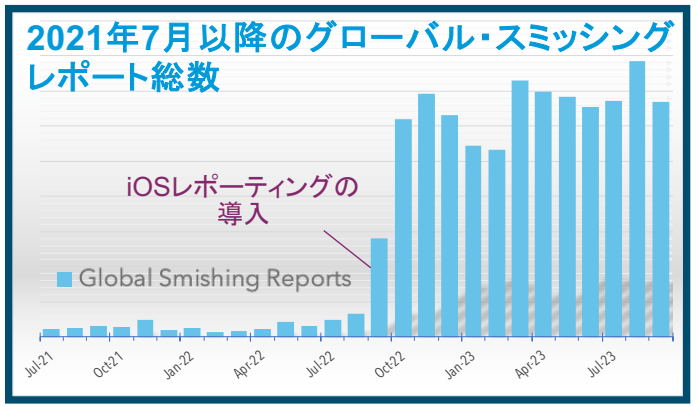
Update: 231006

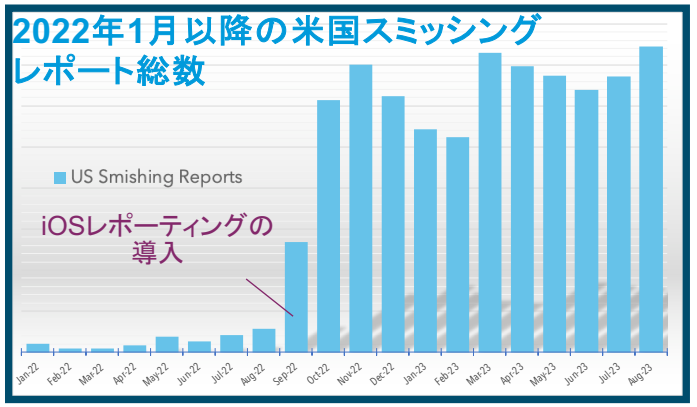
- URLのローテーションは通常、20%超の範囲にとどまる
- 他地域と同様に攻撃者が手口を変えるにつれて、従来のシステムではキャンペーンを検知することが難しくなる傾向

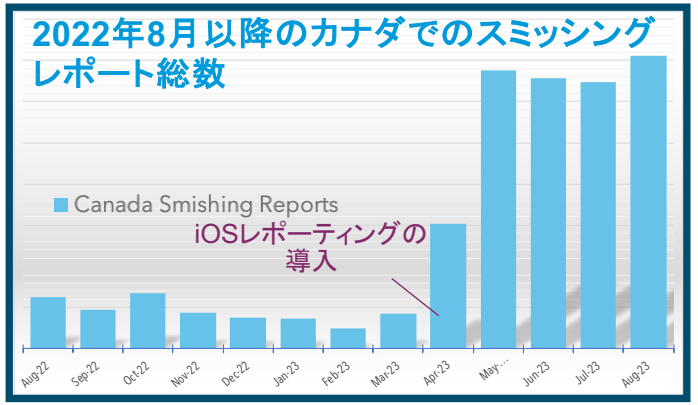
Source: Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/monthly/202308.html

proofpoint.

シンプルレポートと関連するアナウンス







- iOSのシンプルレポートの導入により、ここ数ヶ月のレポート数に偏りが生じている
- 報告されたスパムのレベルが増加したが、スミッシングも増加した（グラフ参照）
- **良いニュース:** データがよりリッチになり、より高いレベルの洞察が得られるようになった
- **洞察力の向上がプロテクションの改善につながる**

proofpoint.

英国におけるシンプルレポート

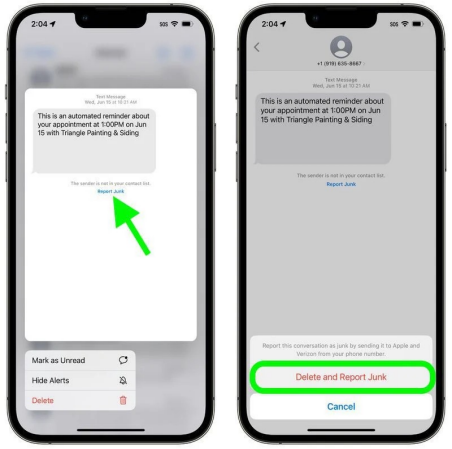
- AndroidとiOSが「ワンクリック」不正レポートをネイティブにサポート
  - MNOとProofpointのCloudmark部門にレポートが提供
  - レポートが分析され、MNOはMobile Abuse Visibility Solution (MAVS)を通じて脅威インテリジェンスと洞察にアクセス可能

“受け取りたくないメッセージを報告することで、モバイル消費者は自分自身とエコシステムを守ることが可能になります。... 簡略化されたスミッシング報告の誕生は... 不正の報告をより主流にするでしょう。”

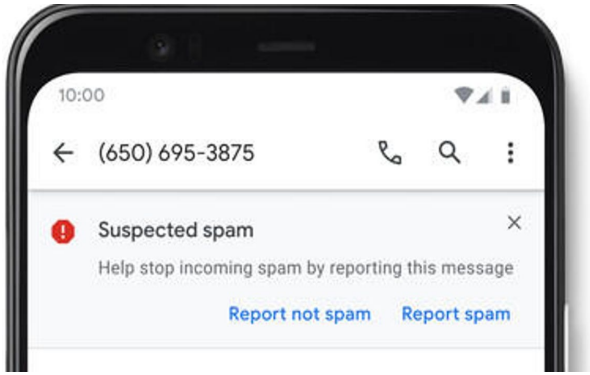
Hamish MacLeod, CEO

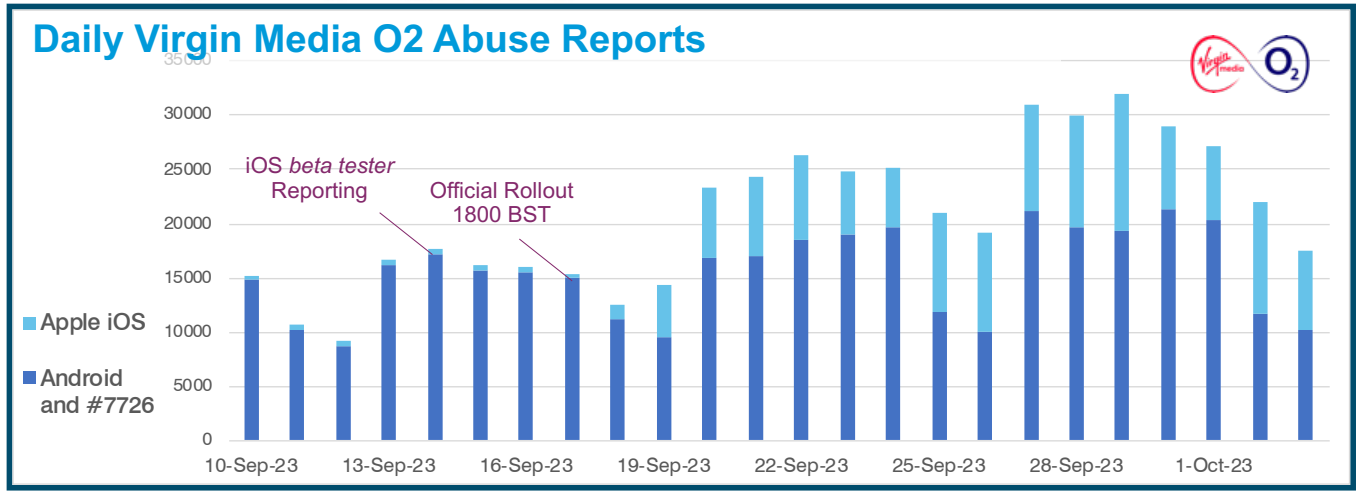
Mobile UK

iOS



Android





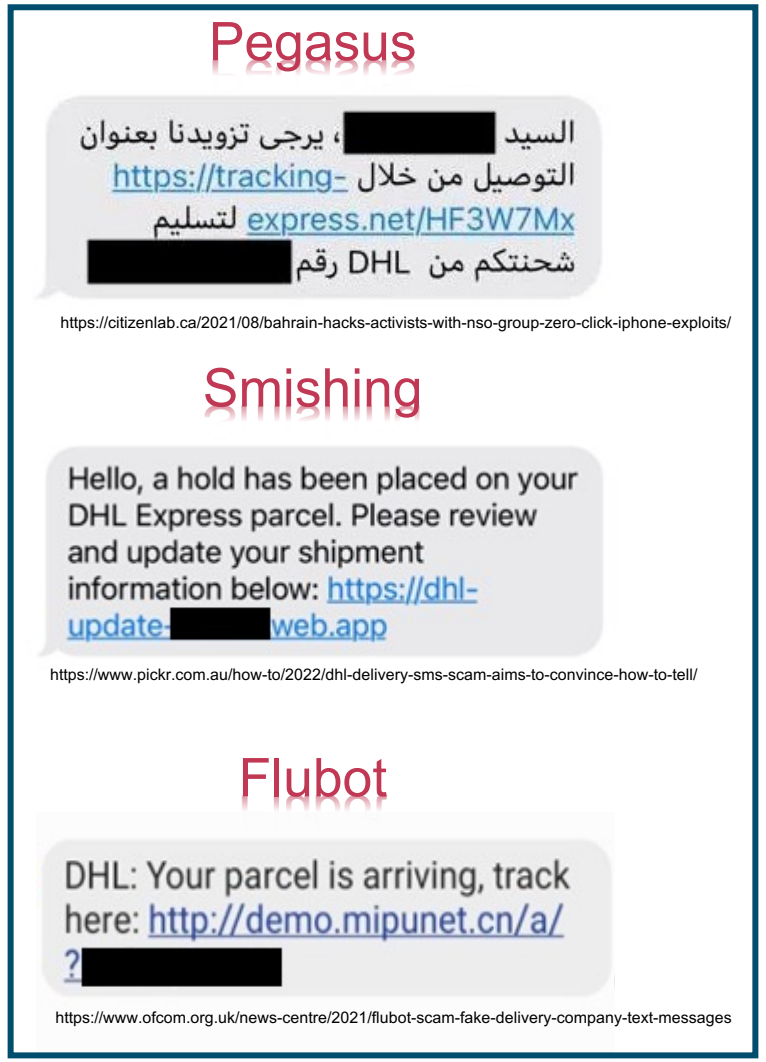
proofpoint.

Major Threats

SMSの脅威の現状

- 一般的なSMSの脅威の概要
  - 大規模なキャンペーン（例：FluBot）は一般的ではない
  - 主に標的型または準標的型キャンペーンに遭遇する

- 脅威を識別する上での課題
  - マルウェアとスミッシングはしばしば似たようなメッセージング戦術を使用
  - 両者を区別するには、それぞれのリンクを実行する必要がある
    - 正しい地域
    - デバイス/設定
    - 言語

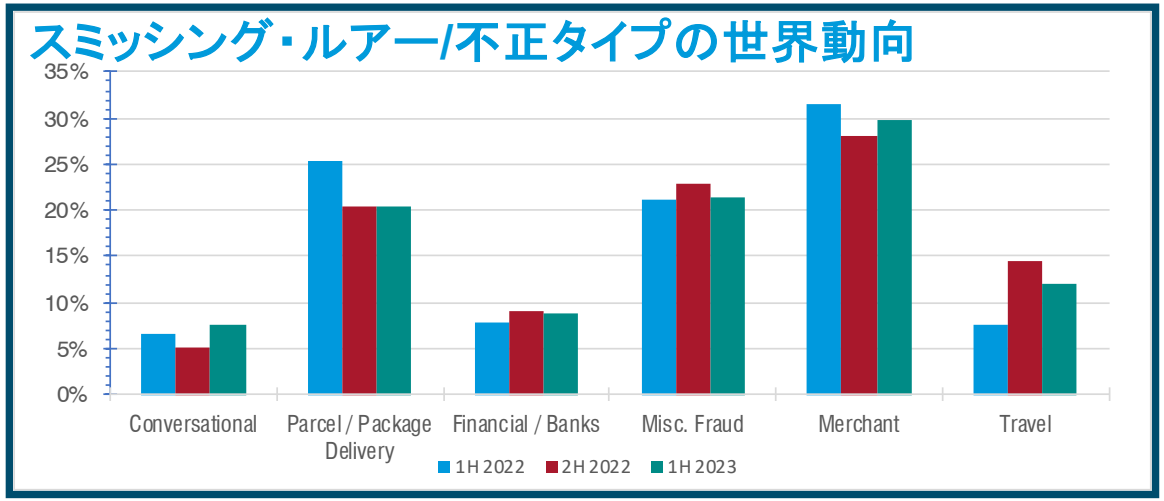


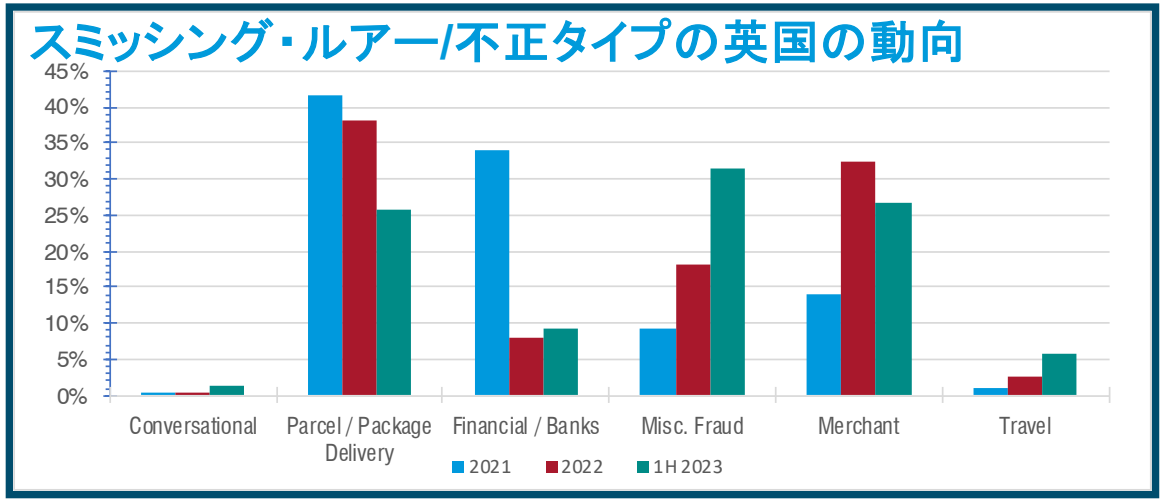
直近の不正の傾向

- 攻撃者は大手（企業）ブランドを活用し続けている
- 荷物のデリバリは、最大ではないにせよ、依然として最も利用されている攻撃の「おびき寄せ手段」の一つである
- 特定のイベントやソーシャルトレンドが標的
- 会話による（会話型の）攻撃が増加

スミッシングと不正の変化

- 宅配業と商業関連が依然として顕著なスミッシング・カテゴリー
  - 宅配業は、DHL、UPS、FedEXなど、さまざまなグローバルブランドで顕著である
  - Amazon/Amazonデリバリーは、ほとんどの地域でマーチャントカテゴリーの大部分を占めている
- 世界的に増加する会話型の不正 -- 表示している割合よりも高い可能性
  - ほとんどの会話型攻撃は、標的をSMS/MMSからOTT（LINE、WhatsAppなど）に移すことを目的としている
  - 初期のOTTメッセージの報告は、形式などの理由で低いことが多い

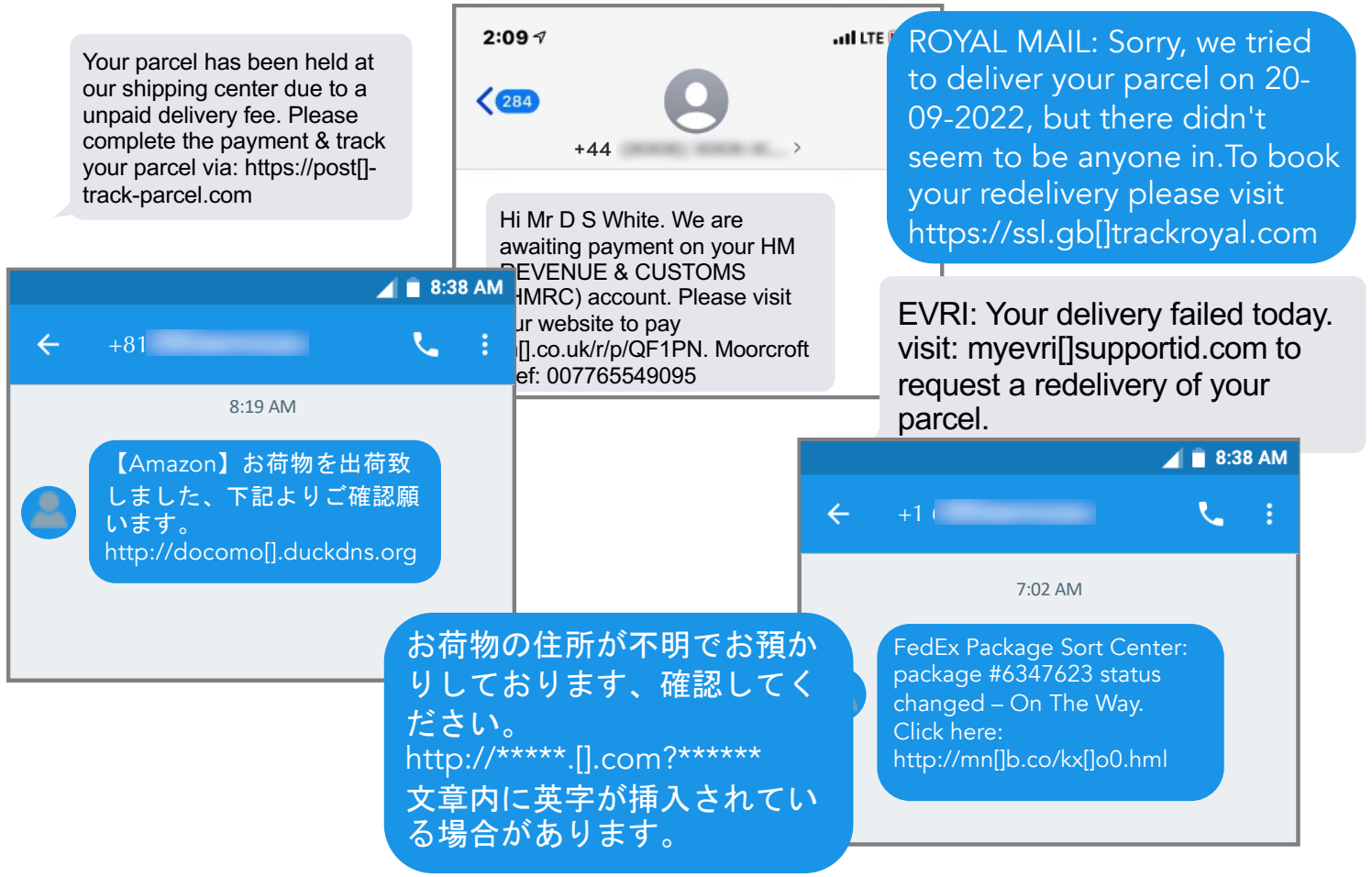




proofpoint.

世界的に多発する宅配業の不正

- 宅配型ルアーは各地域のiOS/Android端末ユーザーを狙う
- 最も一般的な宅配サービスがターゲット
- 税関の警告、一般的な料金や罰金、その他の例外が典型的

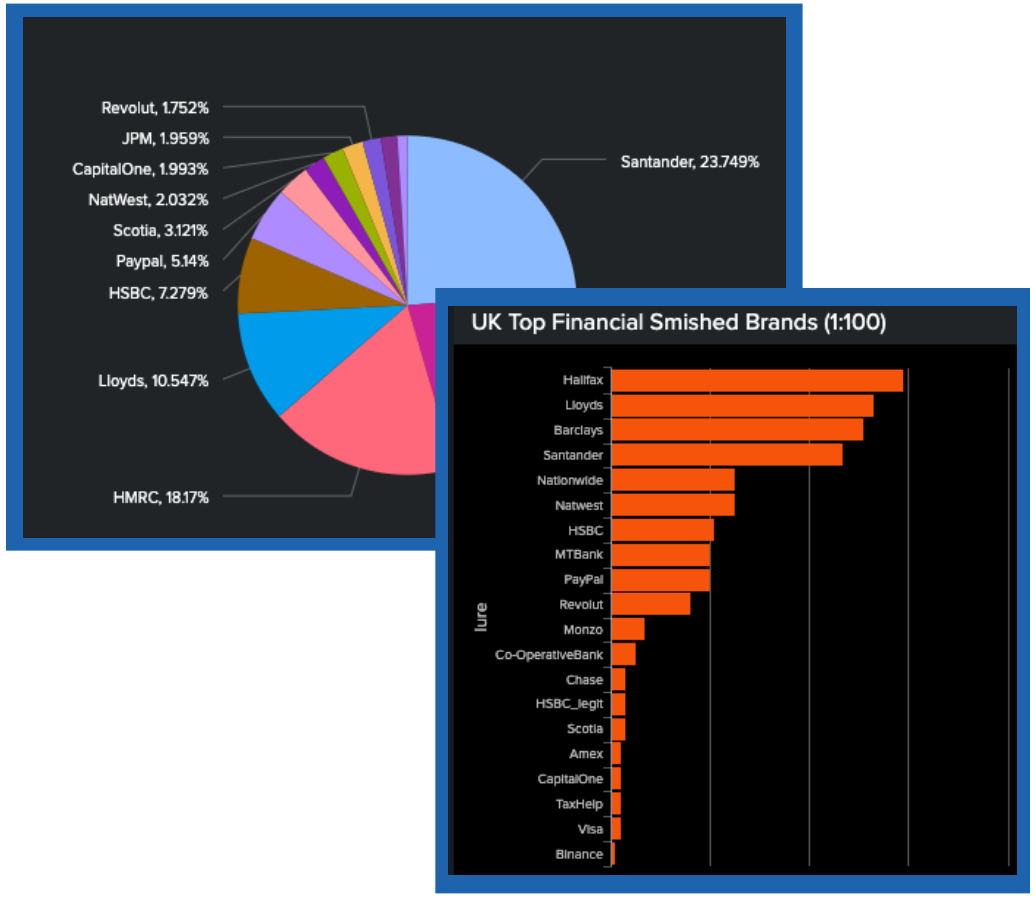


proofpoint.

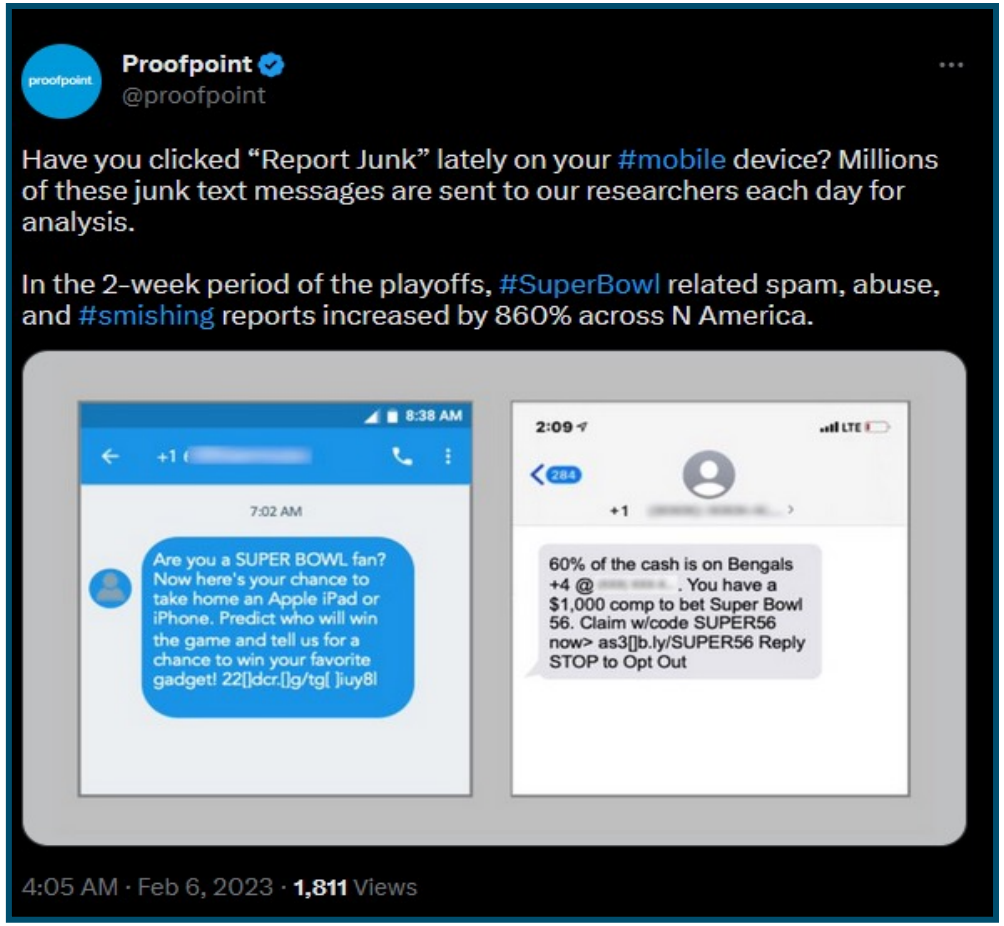
バンク・スミッシングの例

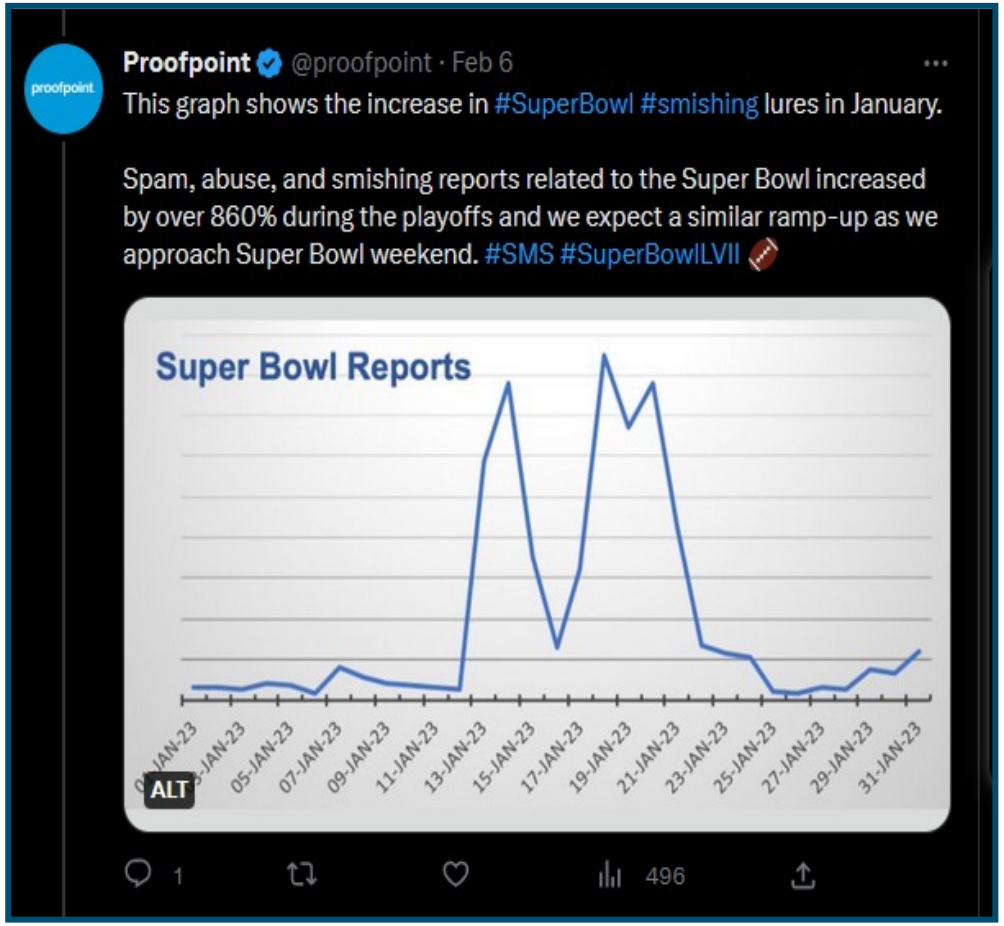
金融向けルアーは通常、スミッシングメッセージの約10%で使用されるが、しばしば人々や企業に最悪の損失と影響を与える

Count	Bod
334	HSBC-FRAUD: A transaction has been attempted on 09/05 at 17:43. If this was not you, proceed at: hxxps:[redacted][.]com/
165	Jyske bank phish - body="Jyskebank. \nNetbank angreb følg instruktioner og sikre kontoindestående: hxxps://jyskebank-opdater-nu[redacted]/" sent from "Jyskebank"
80	HSBC: A payment was attempted from a NEW DEVICE on 29/04 at 16:10. If this was NOT you, please visit: hxxps://hs[redacted]]com/
65	"Alertt" - S A N T A N D E R: An attempt to add H Mohammed on your account was successful on 30/08. If this was NOT you please visit: hxxps://onl[redacted]22[.]com
60	UBS: A transaction has been attempted on 10/04 at 14:47. If this was not you , proceed at: hxxps://ubs[redacted]com/



プルーフポイント社のギャンブルに関するツイート（ポスト）- 米国の動向





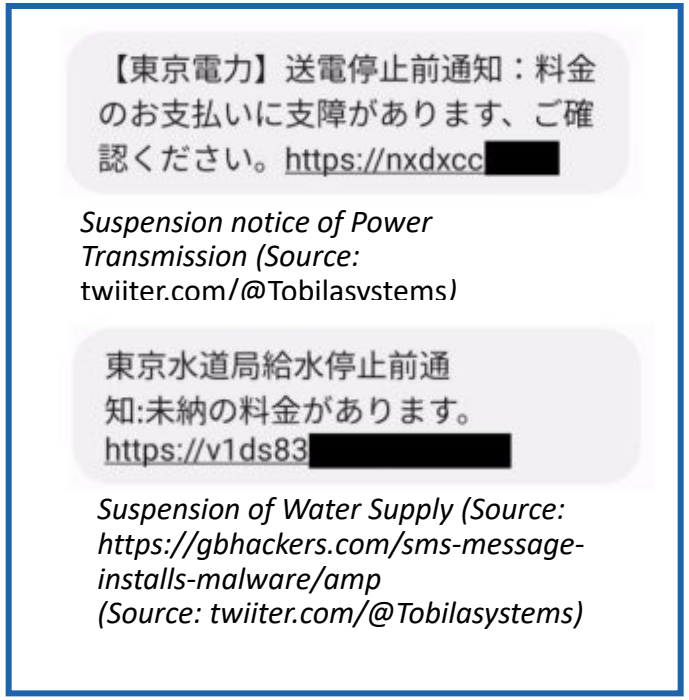
proofpoint.

プルーフポイント社のモバイルマルウェアの追跡状況

	Target OS	App Impersonation	Financial Impersonation	Multi-Modal (Social Media)	Credential Theft	Microphone and Camera	SMS Spreading	Privilege Escalation	Primary Geography
SpyNote		✓	✓	✗	✓	✗	✗	✓	Japan
TianySpy		✓	✓	✗	✓	✗	✗	✗	Japan
KeepSpy		✓	✓	✗	✓	✗	✗	✗	Japan
FluBot		✓	✓	✗	✓	✗	✓	✓	Asia, UK, & Europe
TeaBot		✓	✓	✓	✓	✗	✓	✓	UK & Europe
TangleBot		✗	✓	✓	✓	✓	✗	✓	North America
MoqHao		✓	✓	✓	✓	✗	✓	✗	North America, Europe, Asia, Japan
BRATA		✓	✓	✗	✓	✗	✓	✗	UK, Europe, South American

日本 - SMS SpyNote キャンペーン

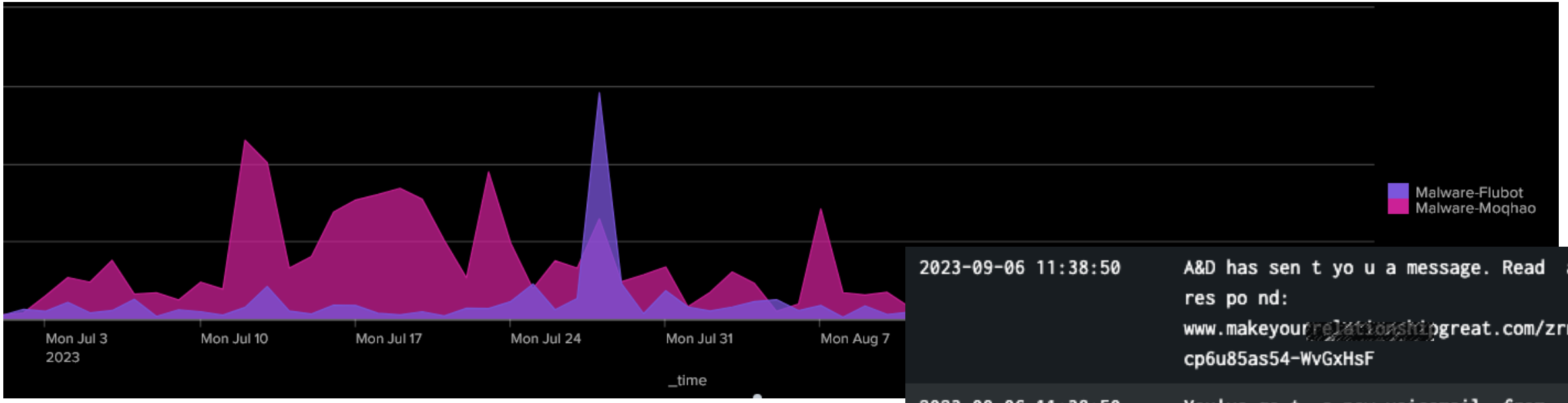
- キャンペーン概要
  - 日本のAndroidユーザーを狙ったスミッシング
  - 電力会社を装ったSMS
  - 緊急の支払いアラートでクリックを促す
- 悪意のあるペイロード
  - リンクダウンロード: SpyNote マルウェア
  - SpyNote はデータを盗み、デバイスを悪用
- SpyNote Malware
  - 2022年の情報流出 サイバー犯罪者に広く利用される
  - 悪用、窃取、本物のアプリに偽装



Suspension notice of Power Transmission (Source: twiiter.com/@Tobilasystems)

Suspension of Water Supply (Source: https://gbhackers.com/sms-message-installs-malware/amp (Source: twiiter.com/@Tobilasystems)

Moqhao / FluBot のトラッキング (UK)

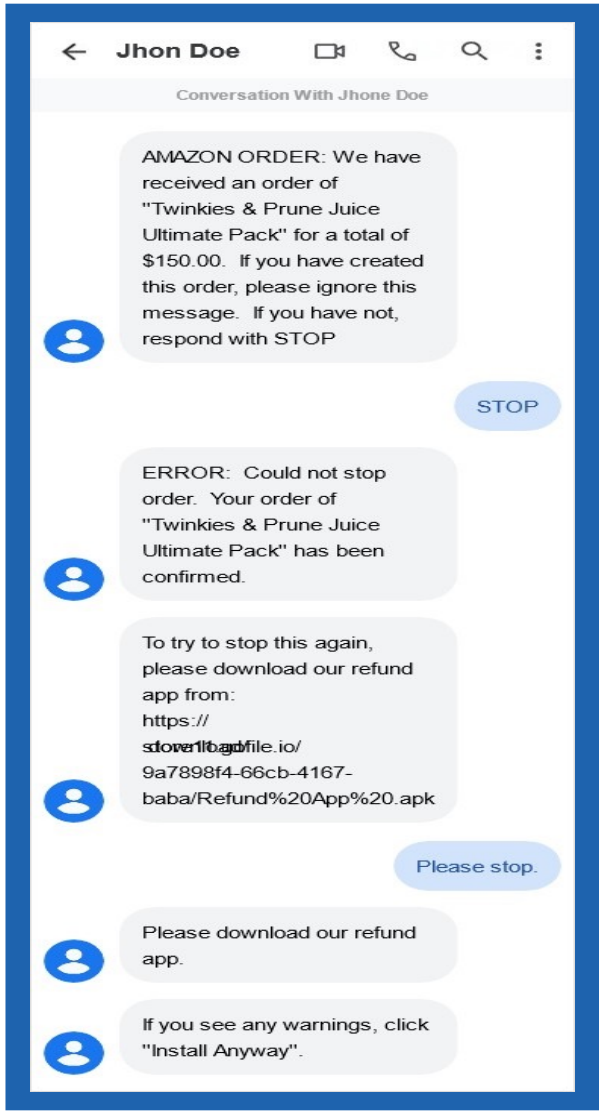


2023-09-06 11:38:50	A&D has sen t yo u a message. Read ar res po nd: www.makeyour[redacted]ogreat.com/zrn/ cp6u85as54-WvGxHsF
2023-09-06 11:38:50	You've go t a new voicemail from your b oss cute0204.info/izz/? [redacted] b6
2023-09-06 08:48:14	Package shipped https://w7.[redacted]/? o0jd8s9nw116dk0i
2023-09-06 08:47:20	Special notification: https://da[redacted]/? 8sqx5nv7cami6y229o

マルウェアのドメイン生成メカニズムとURLパターン は、
マルウェアに関連するメッセージング不正を追跡するために
使用される

標的型キャンペーン

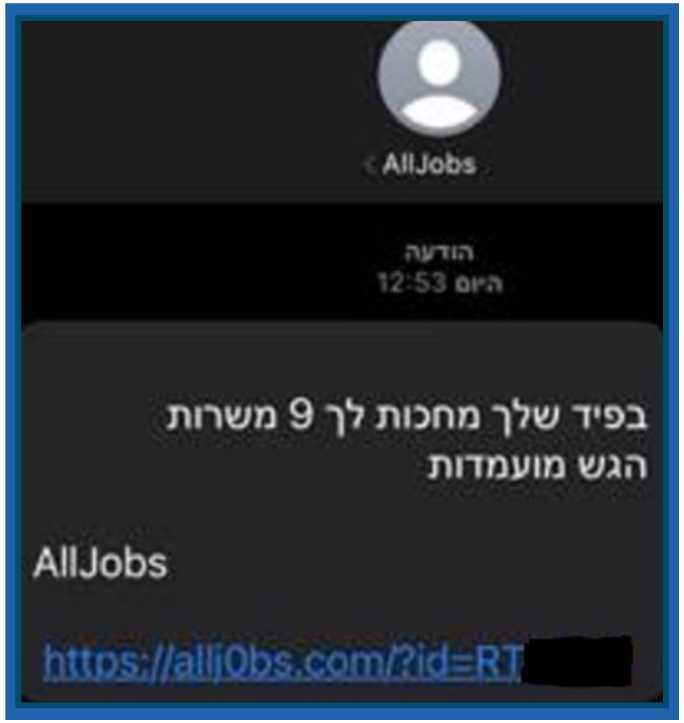
- ターゲットを絞ったSMSマルウェア
  - 特定の個人または小規模グループに焦点を当てる
  - カスタマイズされた欺瞞的なメッセージ
- 卑劣なデリバリー手法
  - 会話形式で、信頼関係を模倣する
  - 受信者の関与を促す
- 目立たず、影響が大きい
  - 目立たない作戦（電子メールとは異なる）
  - 価値の高いターゲットを狙う
- 騙しの手口
  - 信頼できる団体になりすます
  - 対応の緊急性を利用する



proofpoint.

イスラエル - 職務偽装キャンペーン

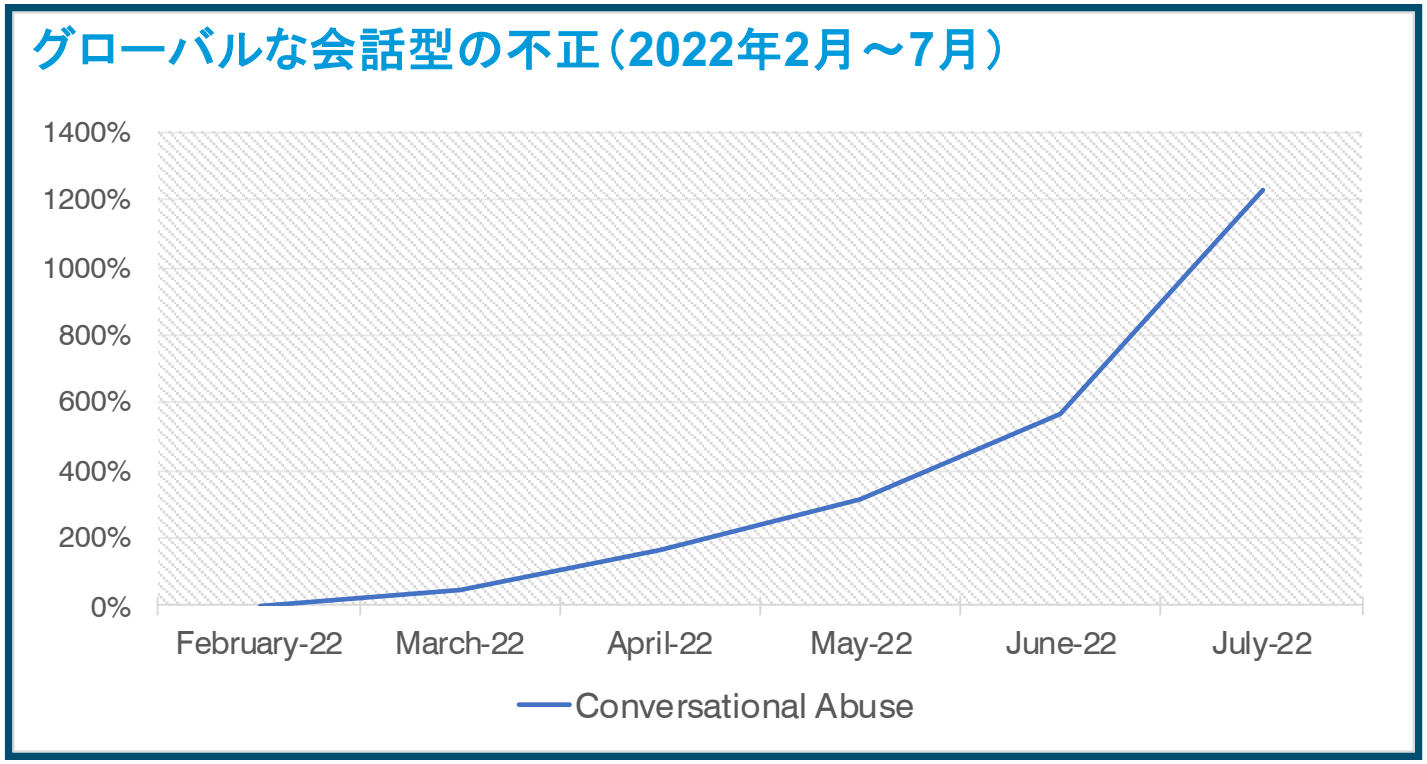
- キャンペーン概要
  - イスラエルの求職者をターゲットにしたSMSキャンペーン
  - 仕事関連の誘い文句で被害者を騙す
- 悪意のあるペイロード
  - SMS内のリンクをクリックすると、ブラウザ・コードが起動
  - デバイスのカメラへのアクセスを試みる可能性
- データ盗難と投稿
  - 被害者から個人情報が盗まれる
  - 攻撃者グループ「Yooz E Cyber」 が被害者データを投稿



https://www.ynetnews.com/business/article/b1hebc00ya

会話型/ソーシャル・エンジニアリング詐欺

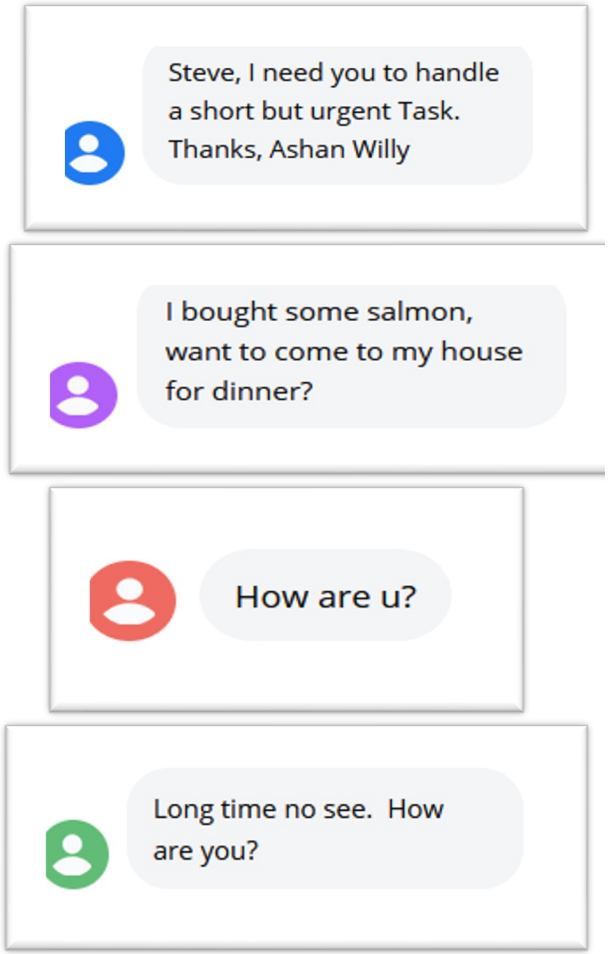
- 現時点での**検知件数**は比較的低いまま
- Fastest growing trend of 2022
- 12x growth
- 2022年に最も急成長するトレンド
- 12倍の成長
- 多くの場合は *マルチモーダル* -- メッセージングプラットフォームとサービスに影響
  - SMS
  - ソーシャルメディア
  - オンライン・コミュニティ
- 2023年まで継続

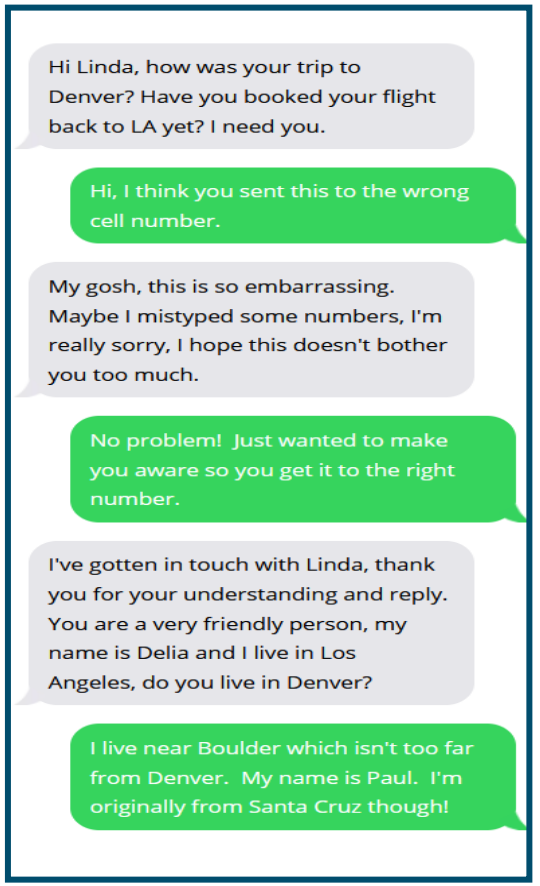


proofpoint.

会話型詐欺

- 増加傾向にある会話型詐欺
- 従来の詐欺を現代風にアレンジ
  - 419
  - ロング・コン
  - 会話重視型
- 攻撃者はターゲットの信頼を築き、信用を得ようとする
- 初期はモバイル・メッセージ・ベース
  - ほとんどの会話型攻撃は、標的をSMS/MMSからOTT（LINE、WhatsAppなど）に誘導させることを狙う
  - 最初のOTTメッセージの報告は、フォーマットなどの関係で低いことが多い

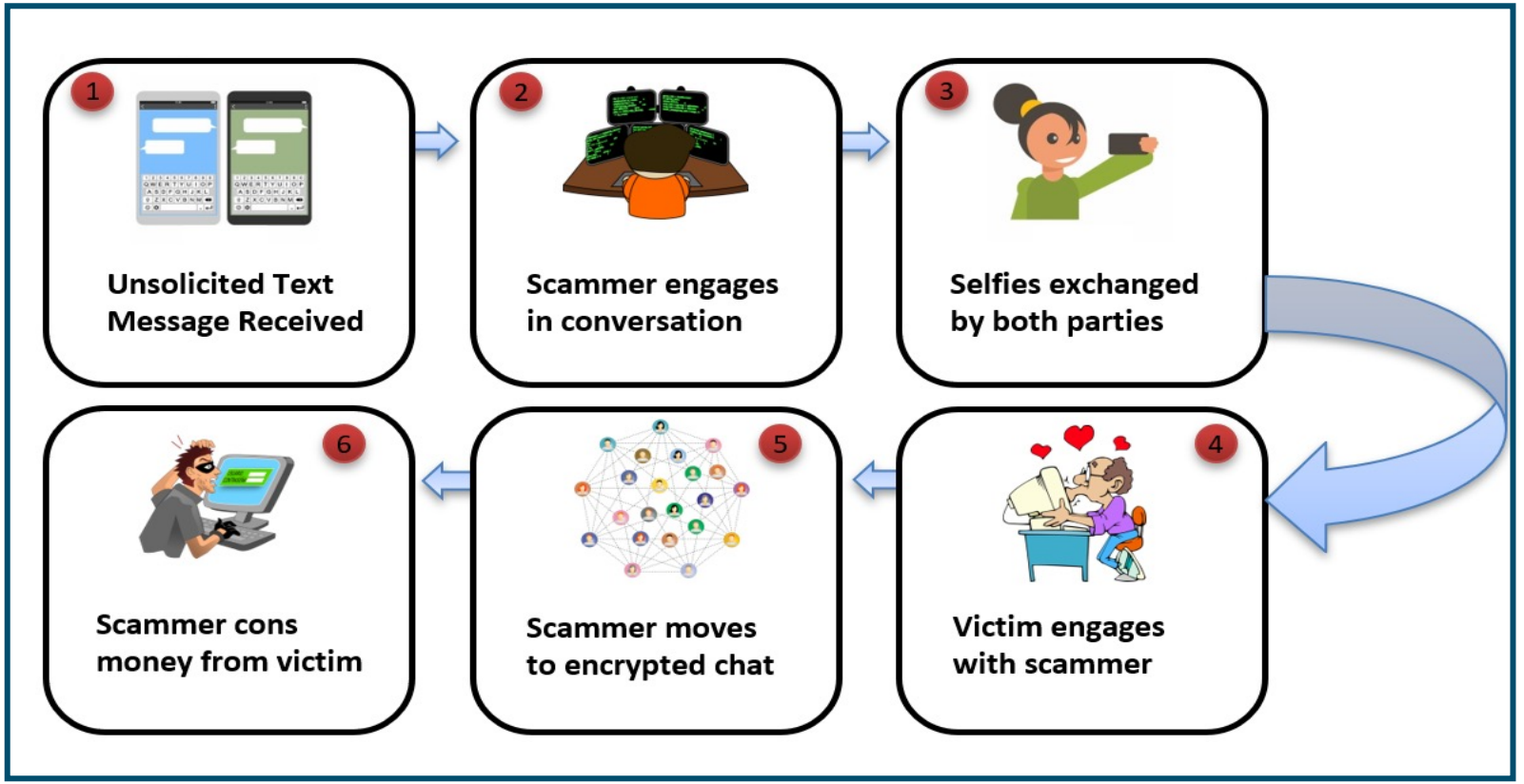




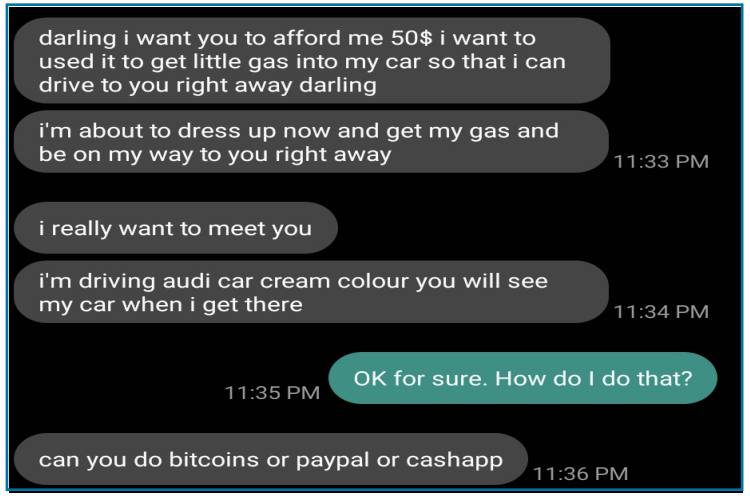
proofpoint.

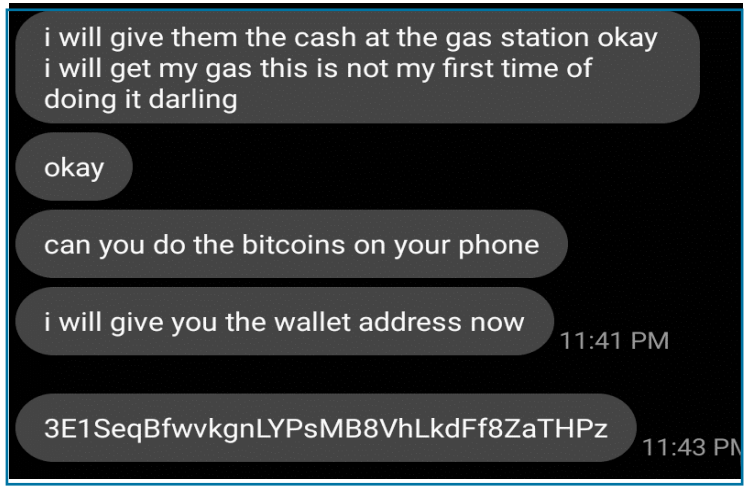
会話型: 多様なタイプでありながら似たようなパターン

- なりすまし
  - "こんにちは、お母さん/ママ"
  - "ジョン？”
- エグゼクティブ詐欺
- 求人詐欺
- ギフトカード詐欺
- ロマンス詐欺
- 豚の屠殺詐欺

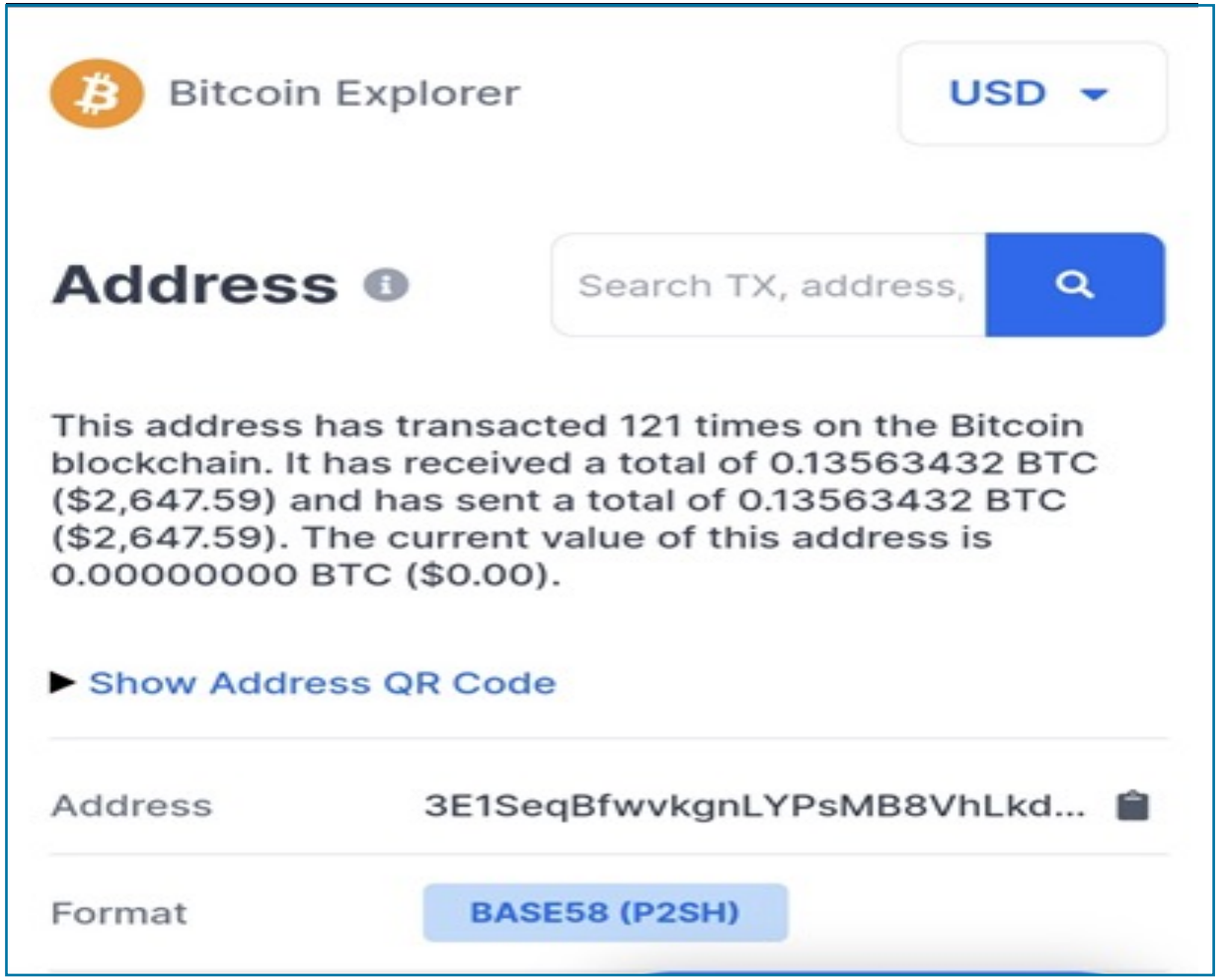


ロマンス詐欺

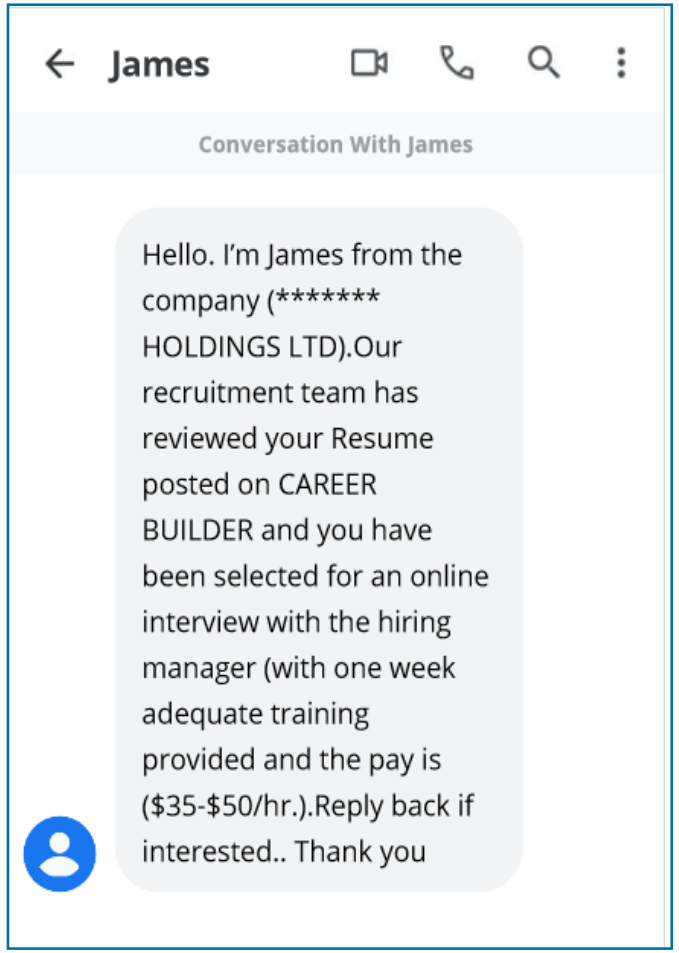


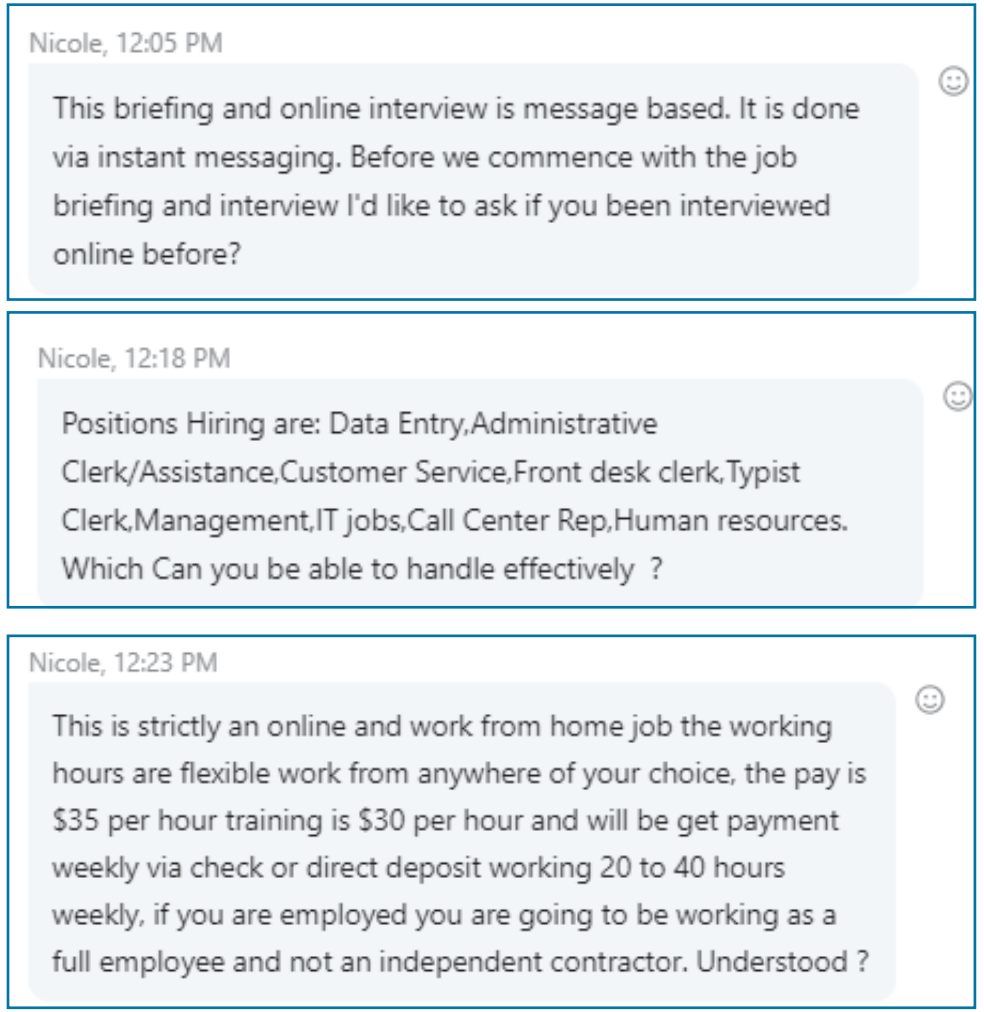


ロマンス詐欺 - 取引

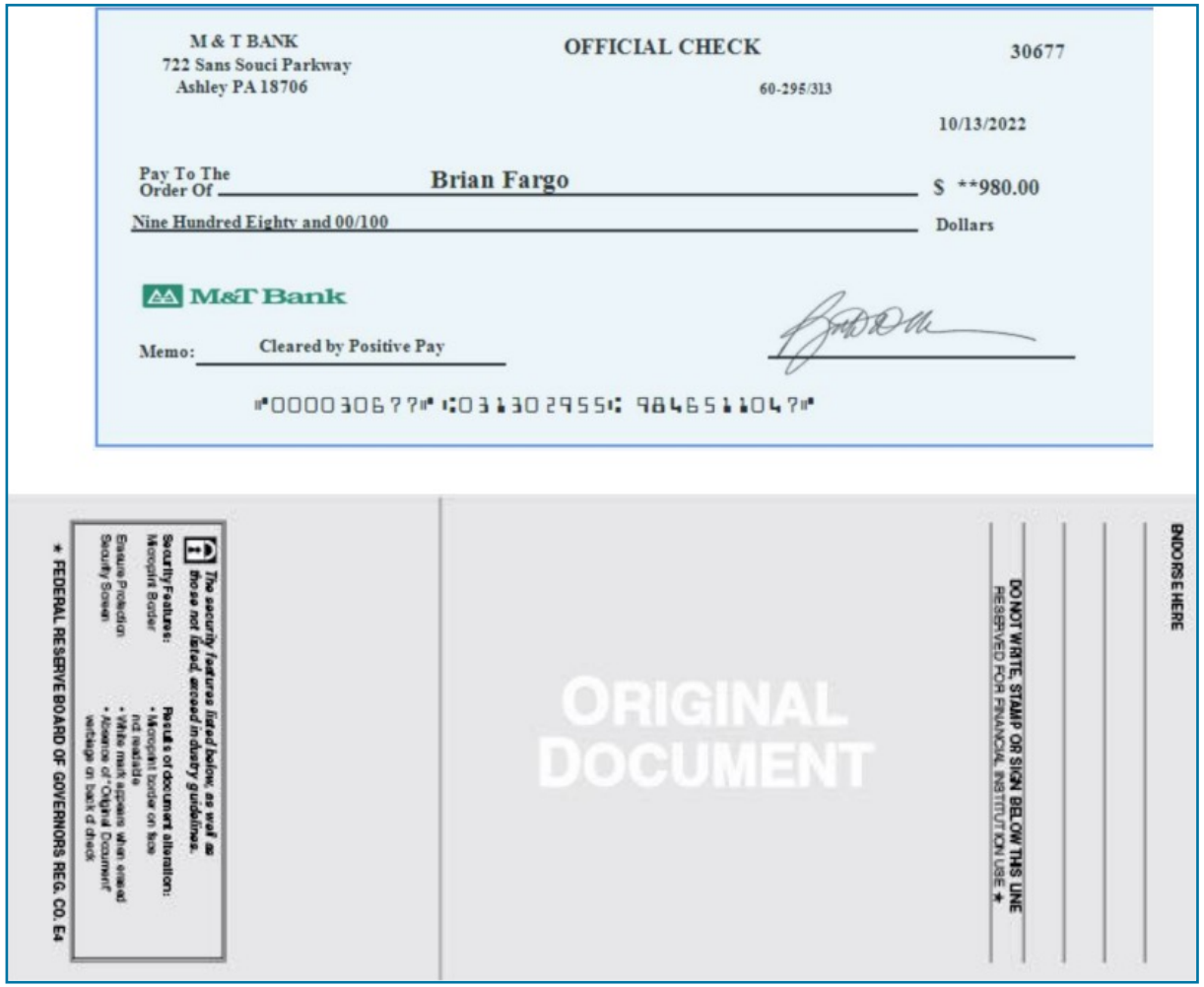


求人詐欺

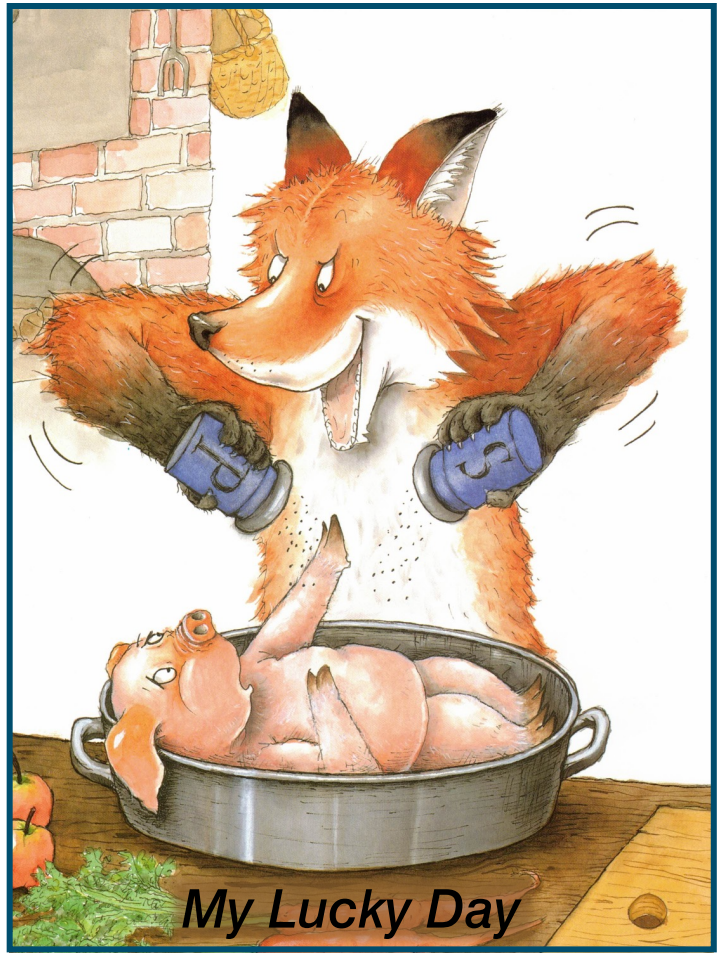




求人詐欺 - 不正な小切手



豚の屠殺詐欺 (Pig Butchering)



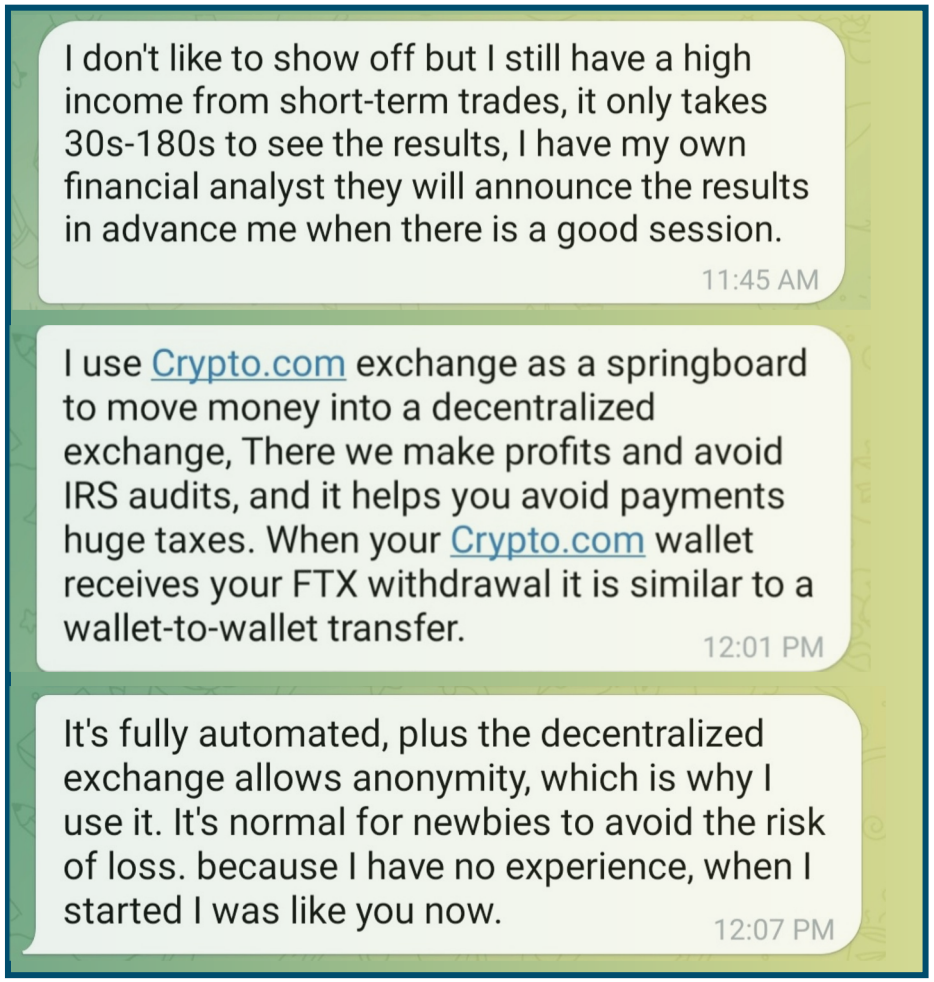
Source: Kasza, Keiko. “My Lucky Day”. 8 September, 2005.

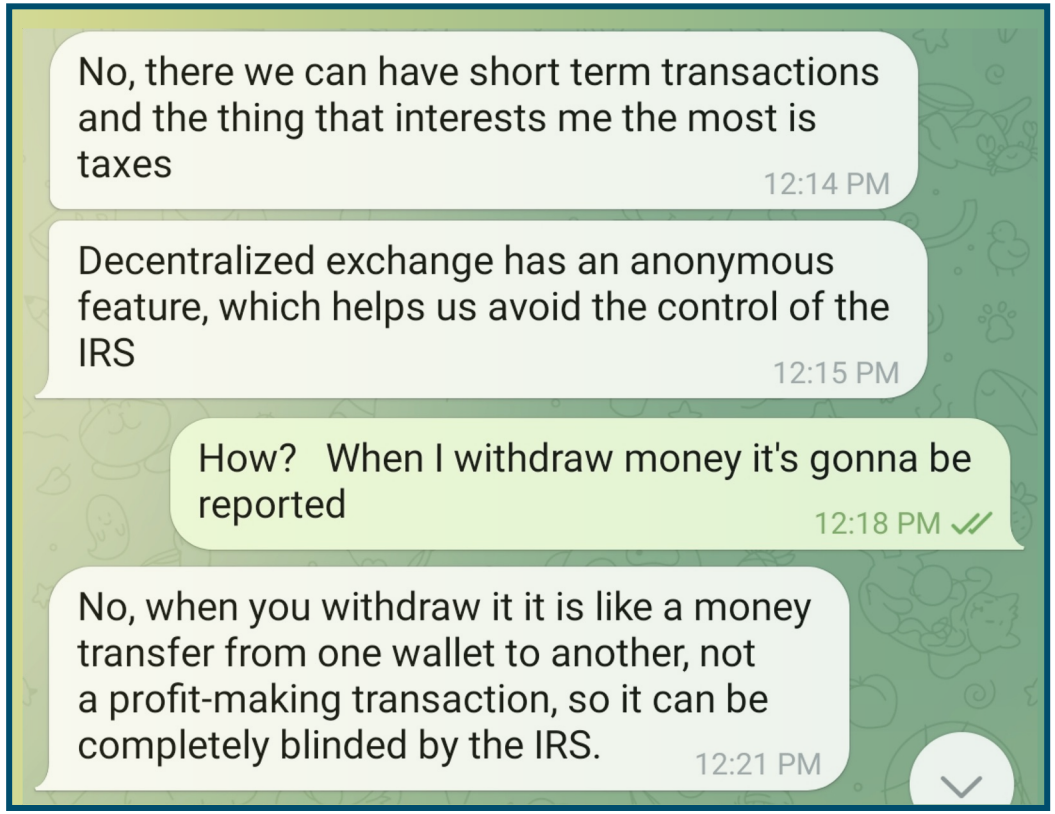
- 最も一般的な会話型詐欺
  - SMS/MMSから始まる長文詐欺
  - 暗号化されたプライベートなOTTに移行することが多い
- 暗号通貨やある種の為替取引を伴うことが多い
  - 外国為替（FX） 取引が一般的
- 名前の由来は、屠殺の前に豚を太らせる（sha zhu pan）から
- 攻撃者
  1. ターゲットと信頼関係を結ぶ
  2. ターゲットに種をまいたり投資したりして関係を強固にし、（現在の）被害者を動かして収益を増やす

豚の屠殺とOTT/暗号化プラットフォームの利用

proofpoint.

豚の屠殺はなぜ魅力的なのか？





Best Practices

エコシステムの保護

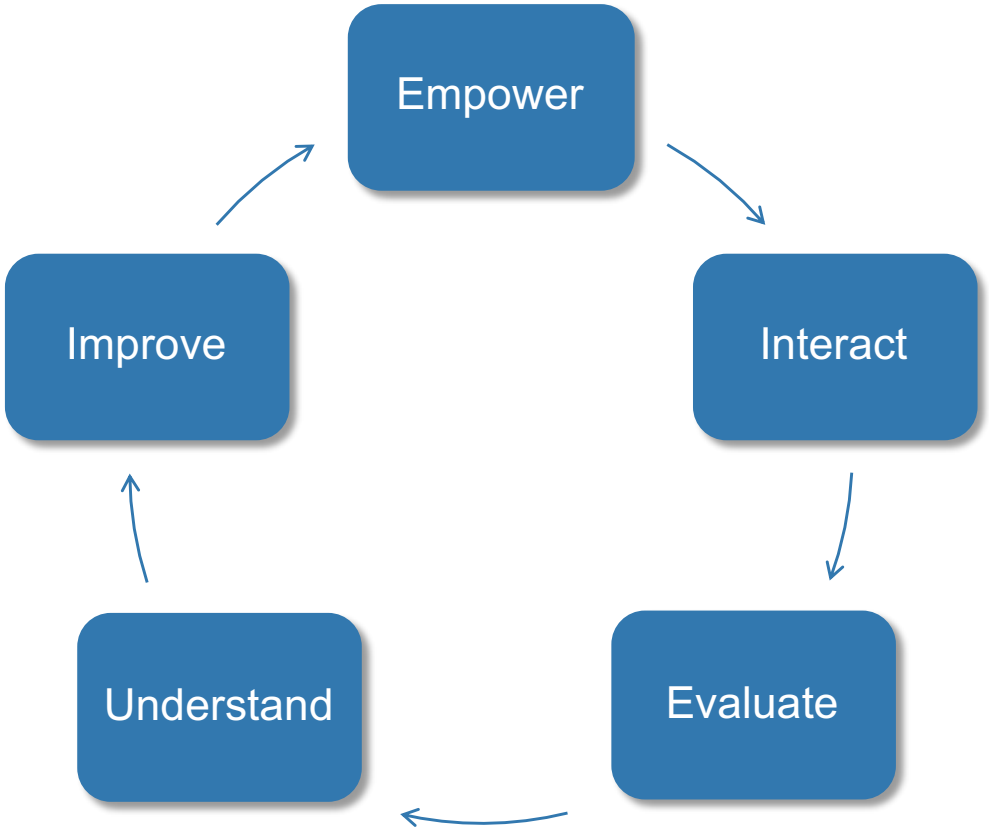
- 他に何が必要か？エコシステム戦略とコラボレーション！
- 人々に力を与える
  - エンドユーザーが問題を報告できるようにする（アンドロイドとiOSのレポートデータを活用する）
  - 詐欺や典型的な詐欺に対する一般市民の意識を高める - セキュリティ意識
  - 悪用されたブランドや企業とのコラボレーション - ユーザーアラート
- 脅威の管理とブロック
  - 脅威をリアルタイムでブロックできるネットワークシステムを活用する - 攻撃の連鎖を断ち切る
  - スミッシングの実行が容易でなく、儲からないようにする – コラボレート
- 詐欺師の追跡
  - 脅威のソース（SMS、MMS、OTP、A2Pなど）を特定するシステムを利用する
  - 当局と協力し、逮捕に必要な情報を提供する

プルーフポイントのCloudmark MAVS: グローバルスタンダード

モバイル不正の可視化ソリューション(Mobile Abuse Visibility Solution)が北米、英国、ニュージーランドのオペレーターに採用

その他の複数の国でも新たな事業者との契約が進行中

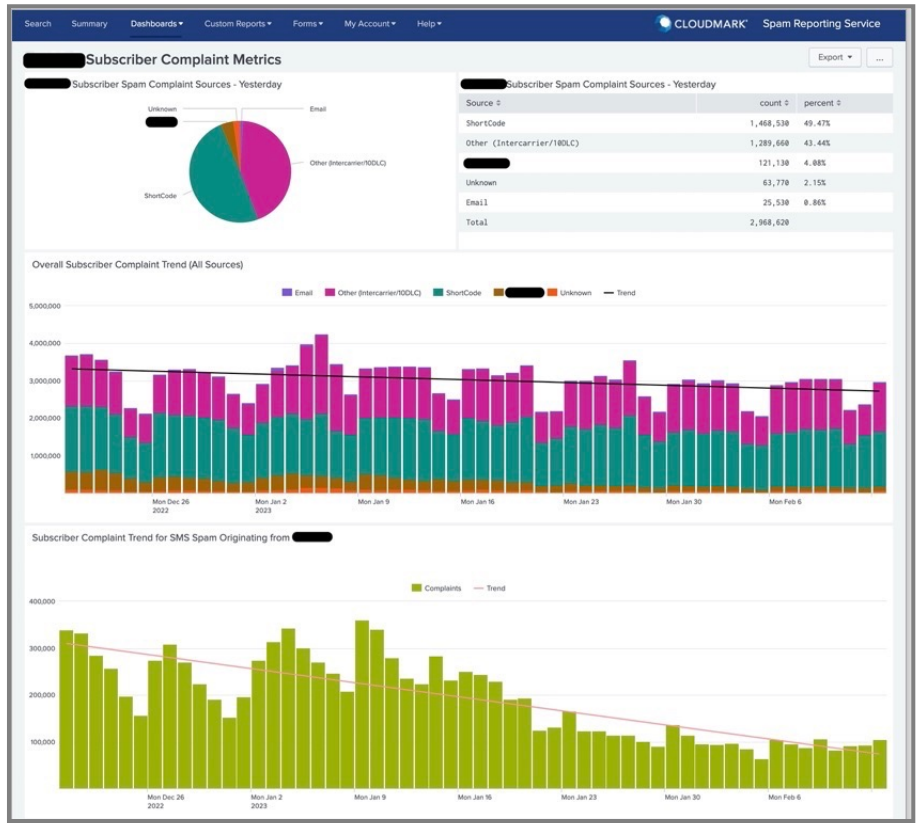
MAVSのフィードバック: 組織全体の価値をもたらす



- **Empower** 迷惑なメッセージ、スミッシング、不正、スパムに対する加入者のアクションを強化
- **Interact** メッセージングプロバイダーおよび企業へのフィードバックによる顧客との対話
- **Evaluate** ネットワークソリューション、保護、その他の機能強化の評価
- **Understand** フォレンジック・ツールによる攻撃と不正の理解、脅威情報のアンラップ処理
- **Improve** ネットワークパフォーマンス、セキュリティ、顧客認知度の向上

Mobile Visibility Abuse (モバイル不正の可視化) ダッシュボード

圧倒的な洞察力とデータ



- カスタマイズ可能なパネルにより、個々の不正メッセージ、トラフィック、攻撃キャンペーンをこれまでにない形で表示可能
- 使いやすいフォレンジック・ツールが情報と洞察を分解
- フォレンジックデータは、消費者の利益や情報を保護する法執行機関を支援
- リアルタイムのアラートと通知により、攻撃、脅威、スパムへの迅速かつタイムリーな対応が可能

脅威のブロック: アンサンブル・アプローチ

- 業界は人工知能と機械学習に**騒然と**しています
  - MLはAIのサブセットである
  - AIだけではメッセージング不正の検知と防御の解決策にはならない
- プルーフポイントのCloudmarkは、クラウドソーシングのグローバルな共有インテリジェンスを開発しました
  - AI/MLをリードするための大規模な投資とコミットメントが、当社の研究を推進
  - グローバル脅威ネットワークは常にフィードバックを提供し、現存する最も広範で豊富な脅威データを表している
- **検知と保護のベストプラクティス:** AI/ML、ルール、新しいアルゴリズム、広範で質の高いデータ、専門家の介入のハイブリッド／アンサンブル

ML: メッセージング・セキュリティの万能薬ではない

長所

+ 傾向をより一般化しやすい
+ "異常"を識別しやすい
+ 言語にとらわれない
+ 概念を抽象化できる
+ BECや標的型攻撃であるスミッシングやフィッシングの脅威に対して、コンテンツと行動分析が上手く一致する

短所

– トレーニング（モデルのキャリブレーション）には時間がかかり、データを必要とする
– 監視なしで単独で行った場合、高い偽陽性率となる
– モデルの再トレーニングに時間とコストがかかる
– サンドボックスなしではURLや添付ファイルの分類に苦慮する

アンサンブルの素材

ProofpointのCloudmarkソリューションで連携するさまざまな機能コンポーネント

Sender Status

- 送信パラメータに関する送信者とメッセージの動作分析
- 発信者の評価
- サービスクラス
- メタデータ（SMPPタグ、Xヘッダーを含む）

Messaging Clustering (ML)

- 類似している、あるいは同じ攻撃キャンペーンと見なされないかもしれないメッセージの高度なグループ化
- 統計的言語学による分類 (SLC)

Fingerprinting (ML)

- インテリジェンス、MLによる分類、メッセージ、関連情報、メタデータの分析
- 20年以上にわたる精度の改善

Additional AI & ML Subsystems

- CTA分析により、悪意のあるサイトやリンクされたコンテンツを特定
- Malicious URL Classifier (MUC)が悪意のある確率を判定し、AIベースのサンドボックスで評価
- URL Behavior ClassifierはURLの傾向、種類、評判などを分析

Behavior Analysis

- トラフィック挙動分析
- AIが、コンテンツ、送信者と受信者のレピュテーション、関係性によって作成されたSLCクラスタからパターンを特定
- 受信ネットワークと終端アドレス情報

Industry Abuse Feeds

- カナリアトラップやハニーポットなど、グローバルに展開されたライブ評価ツールが、新たなキャンペーンの可能性について洞察力を提供
- 業界情報交換により、新たな攻撃の可能性のある市場を提供

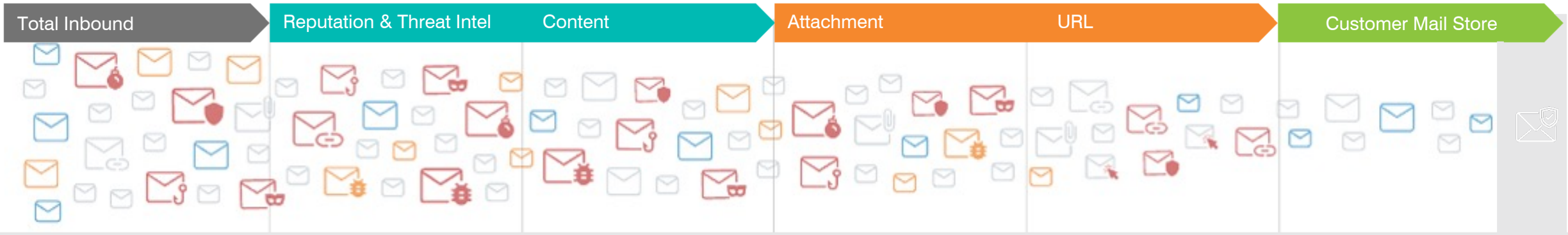
Operator Input / Acceptable Use

- 顧客ポリシーが使用パラメータを制御
- 国や地域特有の法的要件により、利用ポリシーを推進

Managed Oversight

- 自動化されたプロセス、データフィード、脅威の傾向を、現場でのセキュリティの深い経験を持つ専門の脅威エンジニアが監視
- 監視により迅速な微調整が可能

Email: 先端技術とAIのアンサンブル



Threat Intelligence and Analysis
AI / ML Functions
Advanced Algorithms
Threat Expert Oversight
Process Key

- Class of Service
- SMPP Tags/ X–Headers
- External Meta-Data
- Behavioral Analysis: Sender
- Global Threat Network
- Intelligent Industry Data Feeds

- Message Clustering
- Fingerprint Engines
- Statistical Linguistic Categorization
- Advanced BEC (Enterprise) Feed
- Managed Security Services
- Security Operation Center

- Behavioral Analysis: Content
- File Content Signatures
- Malicious Macros
- Malware & Virus Detection

- Malicious URL Classifier*(MUC)
- URL Content Signatures
- Preemptive Scanning ML
- 4th Gen. Phish / Smish ML
- 2nd Generation Computer vision*
- URL / Domain Analysis

- *AI/ML、ルール、革新的アルゴリズム、豊富で高品質なデータ、専門家の介入による多層的なアンサンブル*
- *アンサンブルは、クラス最高のレスポンスと保護を保証すると同時に、長期的な成功を確実にするためのモジュール式の改善機能を提供*

• Future
NB: Not all solutions use all these components

プルーフポイントのクラウドマークソリューション@ Work

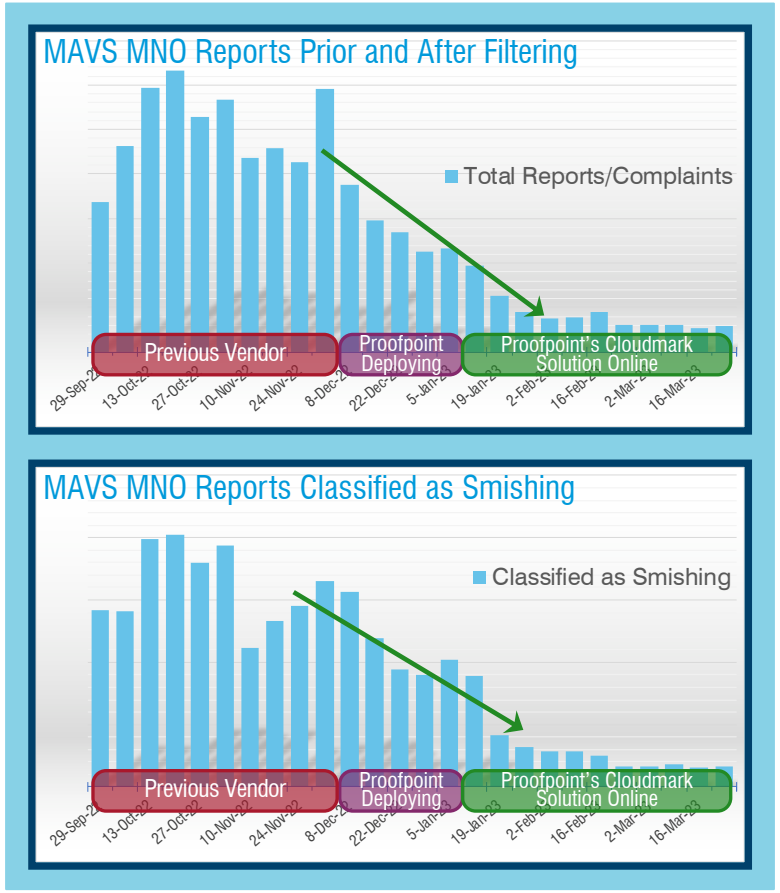
US Tier-1 Improves Protection with Proofpoint

- モバイル・メッセージング・セキュリティ・プラットフォームを米国のTier1 MNOに導入
  - 1億1000万人以上のアクティブな加入者数
  - MNOは、迅速かつ市場をリードするベンダーへの移行を歓迎: プルーフポイント
  - セキュリティの強化と加入者満足度向上のため、既存システムをリプレース
- 個人向け（P2P）とビジネス向け（A2P）のすべてのメッセージングを保護
- 既存のMAVSの全国展開と連携し、すべての脅威と迷惑トラフィックの可視性を向上

Proofpoint Dramatically Reduces Abuse

- 85.4% 報告・苦情件数の削減
- 86.3% スミッシングレポートの削減
- プラットフォームは、すべてのメッセージングトラフィック、コールトゥアクション (CTA)、URL、添付ファイルを可視化
- スミッシングの検知と保護に特化した高度なテクノロジーソリューションをオーダー

† complaints for unwanted, spam, and abuse originating within the MNO. Reduction comparing two-month period before deployment and two-months period after



proofpoint.


proofpoint®