proofpoint®

モバイルアビュースの進化

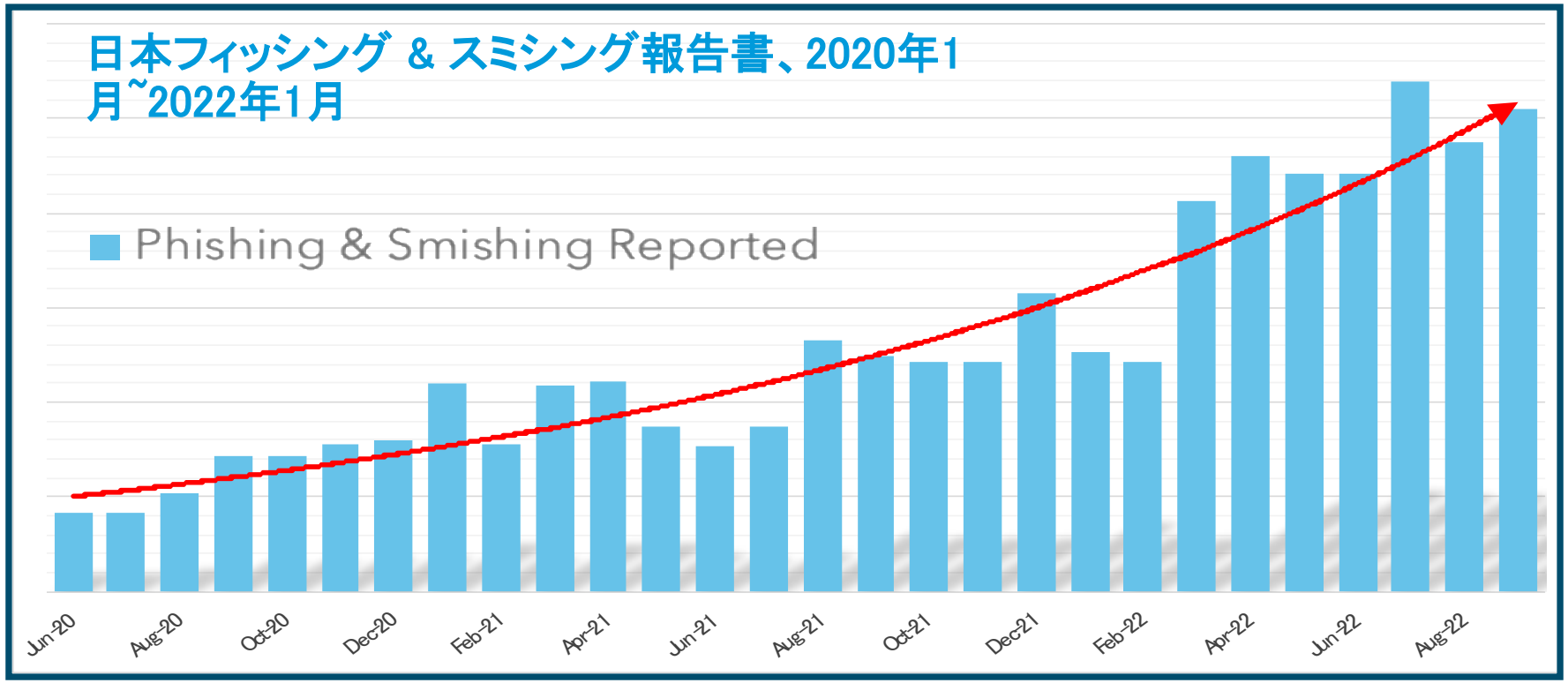
2022年11月

モバイル・プロダクト・マネジャー　マイケル・ブラム

議題

- モバイルフィルタリング精度の課題
  - URLの追跡
  - 暗号解読戦術
- モバイルアビューズの戦術
- ビジネス・メッセージ

地域フィッシング&スミシングの複合トレンド:日本

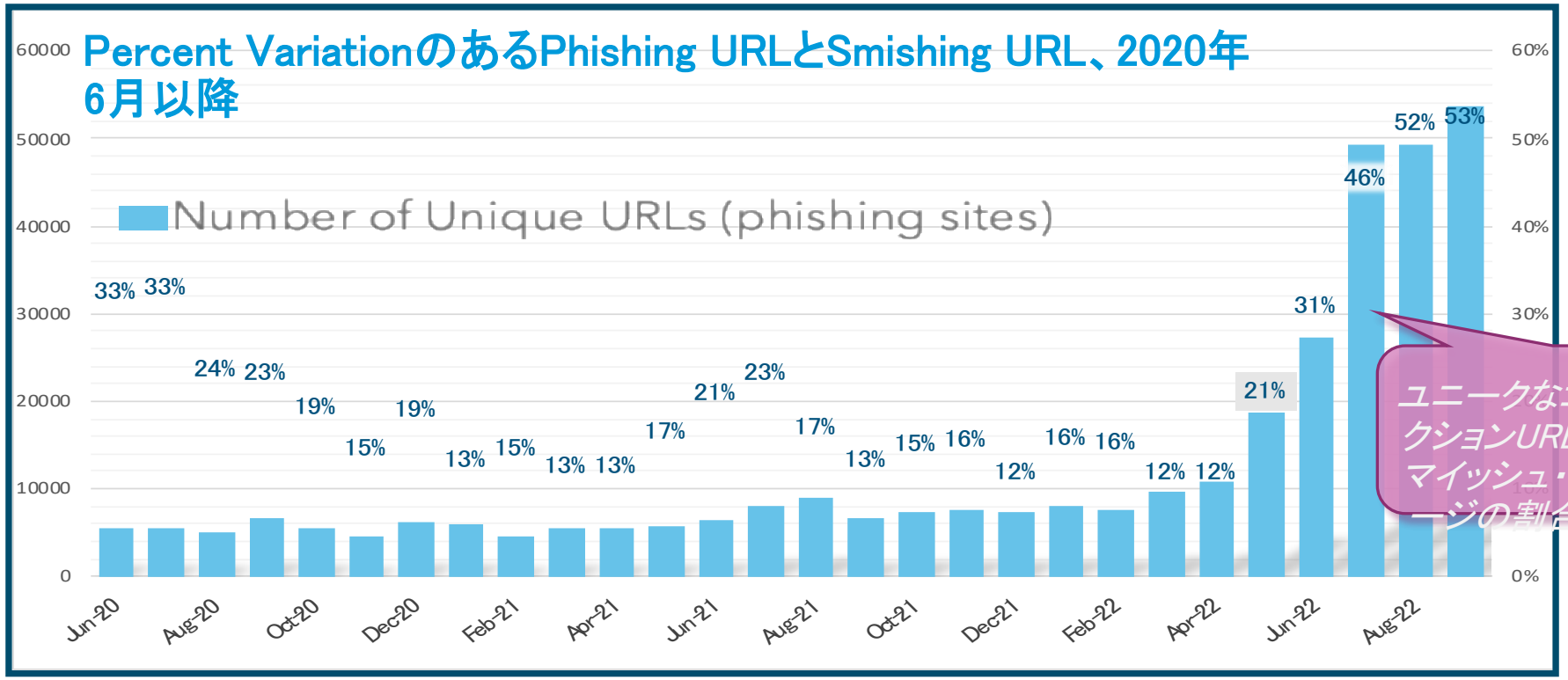


- フィッシング対策協議会資料
- Eメールとモバイルの両方で一貫した悪用の増加

出所:フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202210.html

proofpoint.

URLローテーションの高度化

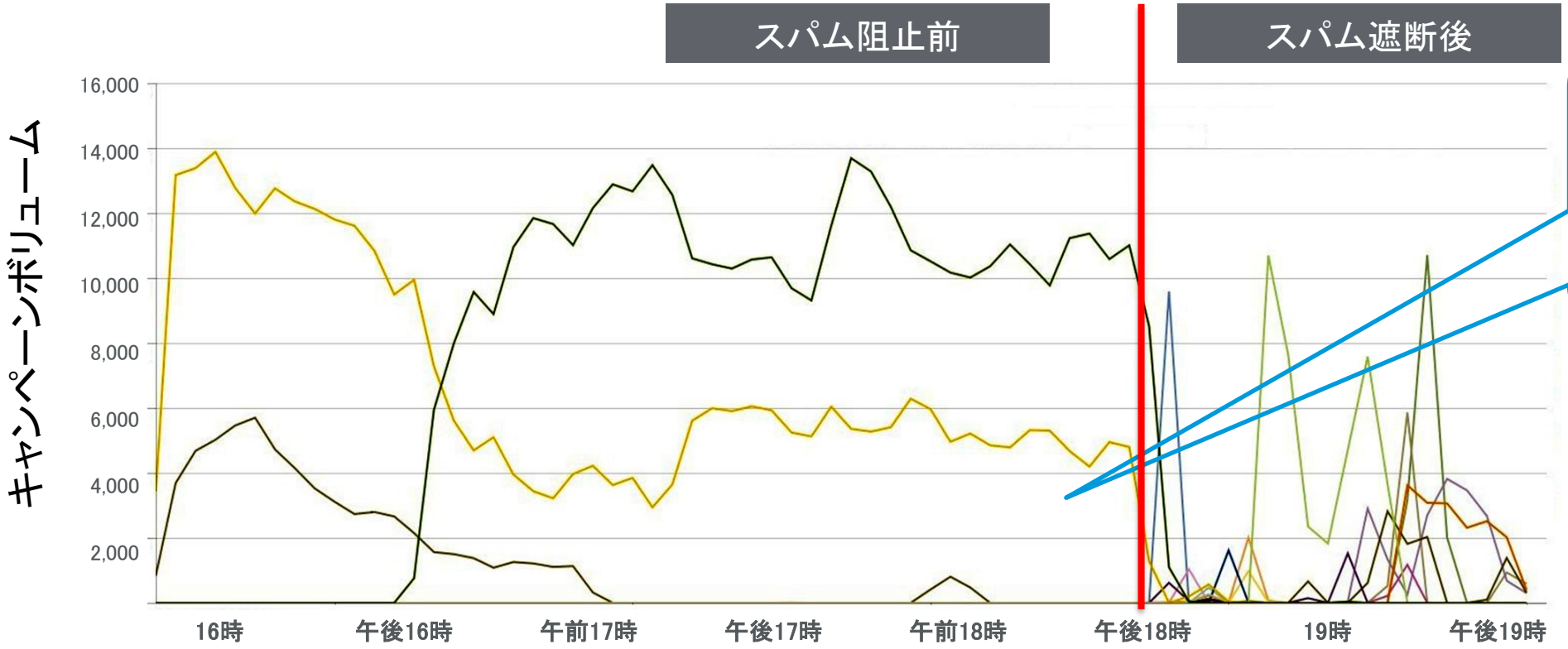


- URLローテーションの増加:攻撃時の固有URLの増加
- 攻撃者が戦術を変えるにつれて、他の地域と一致して、伝統的なシステムがキャンペーンを検知するのはより困難になる。

出所:フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202210.html

proofpoint.

基本的な阻止戦術



基本的な防御ここで追加されたが、攻撃はつぎつぎと変化し、今では見つけにくくなり、多くの防御が追加された。

防衛における基本的概念

見かけ上、複雑性が低く、攻撃のバリエーションが少ないため、次の操作でブロックしやすくなります。

- URLブロック
- 番号ブロックリスト
- 単純容積制限

新たな攻撃ー防御が難しい

突然変異が速い発作

- より多くの送信番号
- ランダム/暗号化されたコンテンツ
- URLのローテーション

proofpoint.

ホモグリフによる難読化

Content	MD5
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	cef216367b00556002ebec6b0506d62b
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	B45ffb99292c8b0322e3bfb6b511cea8
В ДЕЯ CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	E93930dfaebbd97de6223e4f48eb43e6
В ДЕЯ CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е!!!	Cde986d7ec8c265c28f7dbc4c8c1f260
В ДЕЯ CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е!!!	316ec752879e96a7fde8fefdc1b4401e
В ДЕЯ CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	B7b457e9df87cc8987e15234e12b9d37
В ДЕЯ CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	0776f26681a5ef28583d2b9540f4b1b7
В ДЕЯ CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е!!!	751dc1f08aa731c7c79d11bdbd1cc465

ホモグリフによる難読化

Content	MD5
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	cef216367b00556002ebec6b0506d62b
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	B45ffb99292c8b0322e3bfb6b511cea8
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	E93930dfaebbd97de6223e4f48eb43e6
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	Cde986d7ec8c265c28f7dbc4c8c1f260
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	316ec752879e96a7fde8fefdc1b4401e
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	B7b457e9df87cc8987e15234e12b9d37
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	0776f26681a5ef28583d2b9540f4b1b7
В Д Е Я CONCEPT CLUB ц е н ы п р о д о л ж а ю т т а я т ь ! С к и д к и д о 70%! С п е ш и т е !!!	751dc1f08aa731c7c79d11bdbd1cc465

http://unicode.org/cldr/utility/confusables.jsp

proofpoint.

頻繁に変化するメッセージ

Jeniffer,Apply This Daily and Observe Your Bags Under Eyes and Lines And Wrinkles Fade AwayVisit EraseWrinklesX.us to learn moretxt 4 to quit

Nasem,Apply This Once A Day and Watch Your Bags Under Eyes and Old Wrinkles Fade AwayGo to FreeWrinkleFaceX.us to read moreRply 9 to unsub

Tamra,Apply This Every Day and Observe Your Eye Bags and Wrinkles DisappearGo to FreeWrinkleFaceX.us to learn moretxt 2 to unsub

Elaina,Apply Like This Once A Day and Look At Your Eye Bags and Old Wrinkles Fade AwayGo to WrinklesEraserX.us to learn moretxt 2 to quit

Christine,Apply Like This Daily and Look At Your Eye Bags and Wrinkles EvaporateGo to WrinklesEraserX.us to learn moreRply 4 to unsub

Tracy,Apply Like This Daily and Look At Your Puffyness and Old Wrinkles EvaporateSee EraseWrinklesX.us for infoRply 7 to unsub

Joy,Apply This Every Day and Look At Your Eye Bags and Lines And Wrinkles Fade AwayGo to EraseWrinklesX.us to learn moreRply 7 to end

Jolene,Apply This Every Day and Observe Your Bags Under Eyes and Wrinkles DisappearGo to FreeFromWrinklesX.us for infotxt 2 to quit

Sherry,Apply Like This Once A Day and Look At Your Bags Under Eyes and Lines And Wrinkles DisappearGo to WrinklesEraserX.us for infoRply 2 to cancel

Tracy,Apply This Every Day and Observe Your Under Eye Bags and Lines And Wrinkles DisappearVisit AntiAgingFormulaX.us for infoRply 5 to cancel

Catherine m,Apply This Every Day and Look At Your Under Eye Bags and Old Wrinkles DisappearVisit WrinklesEraserX.us to see howRply 1 to end

Miriam,Apply Like This Every Day and Watch Your Bags Under Eyes and Wrinkles Fade AwayVisit WrinklesEraserX.us to learn moretxt 2 to unsub

Joy,Apply This Daily and Observe Your Under Eye Bags and Old Wrinkles EvaporateGo to AntiAgingFormulaX.us to read moretxt 6 to end

https://en.wikipedia.org/wiki/File:Whac-a-mole_-_Tokyo_-_Jan_7_2020.webm#file

proofpoint.

スミッシングの影響

モバイル・バリュー・チェーンのすべての人に影響を与えるスミッシング

消費者への影響

- 個人情報の紛失
- 財務上の損失
  - 日本:統計からは、オンライン銀行詐欺により11.3億円の損失
  - オーストラリア:SMSメッセージ詐欺に直接関連する310万豪ドルの損失(オーストラリア消費者競争委員会)
  - 米国:2020年頃、スミッシングだけで8600万ドルを超える損失(米国連邦取引委員会)

モバイルネットワークオペレータの影響

- 消費者の脆弱性によるブランドの低下と消費者の信頼の低下
- 大量のスマイシングやマルウェア攻撃がMNOの運営・経費に直接影響を与える
- 顧客サポートコールや苦情の増加、および機器の衛生に関するフォローアップは、財務上の損失を引き起こす。

企業・企業への影響

- 偽装攻撃によるブランドの侵食、真正な企業コミュニケーションの誤認
- 9月には、日本では76の異なるブランドが乱用された。
- 日本で乱用されている上位10ブランドは、攻撃の82%を占めている。 トップ3:アマゾン、アップル、ドコモが目立つ

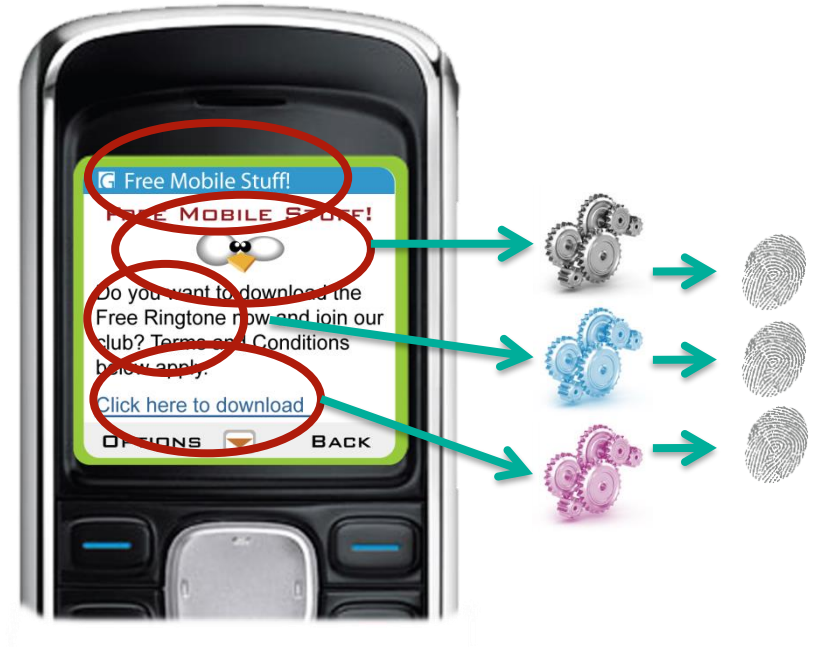
†† Council of Anti-Phishing Japan
https://www.antiphishing.jp/report/monthly/202109.html

proofpoint.

モバイルアビューズの戦術

proofpoint.

フィンガープリント



- フィンガープリントはメッセージ内容のインジケータを表す。
  - URL
  - コンテンツ文字列
  - 電話番号(本文中)
  - …
- フィンガープリントは、メッセージのメタデータインジケータを表すことも可能。
  - メッセージに含まれる文字セットのタイプ
  - メッセージ内のURLの存在
  - コンテンツ内の不明瞭化の表示
  - …
- フィンガープリントは強力で、簡単に拡張可能。
  - フィンガープリントエンジンは、コードの変更や新しいソフトウェアの導入を必要とせずに、新しいタイプのフィンガープリントを生成するために簡単に拡張できます。
  - 高度な前処理・正規化機能

proofpoint.

フィンガープリントエンジン

- フィンガープリントエンジンは、さまざまな種類のコンテンツをターゲットに
  - 前処理/「正規化」
  - URL:TLD、マルチレベルドメイン、URI
  - 文字列/ワードパターン
  - 画像
  - バイナリ/実行可能コンテンツ

- フィンガープリントに合わせて新しい方法で調整できる適応フィンガープリントエンジン
  - 調整可能なマッチングパターン
  - 内蔵lua/スクリプタブルエンジン

proofpoint.

「インジケータ」フィンガープリント:例

- 以下のメッセージ

[◌ア◌マ◌ゾ◌ン]プライム会◌費のお支◌払い方◌法に問◌題があります:https://amazon-reset.com

- 以下の指紋を生成する可能性があります。
  - **インジケータ指紋:**
    - a=aksifue51sx:22　　メッセージにUnicodeカタカナ/漢字が含まれていることを示します。
    - a=ksjfuka2fkah:22　　メッセージにUnicodeアラビア文字が含まれていることを示します。
    - dsfksd9w2:22メッセージにUnicodeのゼロ幅文字が含まれていることを示します。
    - a=ksifn8skahs:10　　メッセージにURLが含まれていることを示します。
  - **コンテンツフィンガープリント**
    - a=9sdfnadafka:8　　URL amazon-reset.comを表すユニークな指紋
    - a=jasnasd8faa:9　　ボディ内容文字列のハッシュを表す指紋

正規化

- コンテンツ正規化エンジン
  - 指紋の前にコンテンツ上で実行する前処理エンジン
  - メッセージ/コンテンツに複数の変換を適用する
  - 状況の変化と詐欺の戦術に基づいて新しい変換を適用するために、簡単かつ動的に更新することができます。
  - リモート・アップデート・メカニズムを使用して分散された新しい命令

- 変換例
  - Visit www.ama***zo***n-r***e***s***e***t.com

  ➔ “Visit www.amazon-reset.com”

  - 「1-456-**CIT-BANK**を呼んでパスワードを確認してください」を

  「1-456-**248-2265**を呼び出してパスワードを確認してください」に正規化

proofpoint.

知的政策

"Signal"フィンガープリントを使用すると、次のようになります。

a=aksifue51sx:22
a=ksjfuka2fkah:22
dsfksd9w2:22
a=ksifn8skahs:10

contains_unicode_katakana
contains_unicode_arabic
contains_unicode_zerowidth
contains_url

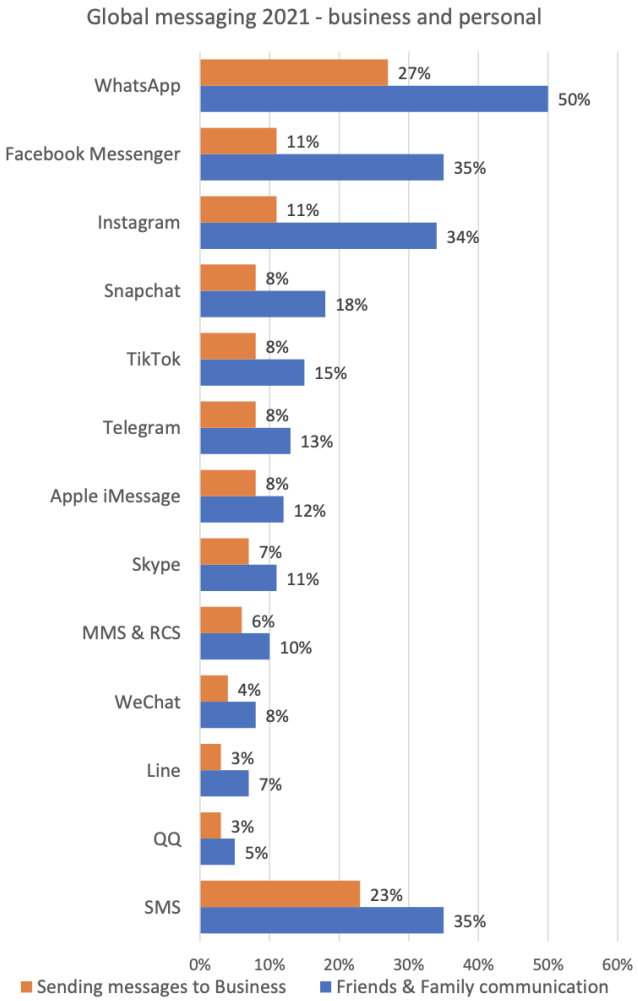
インテリジェントインジケーターの組み合わせによるBLOCK

proofpoint.

ビジネス・メッセージ

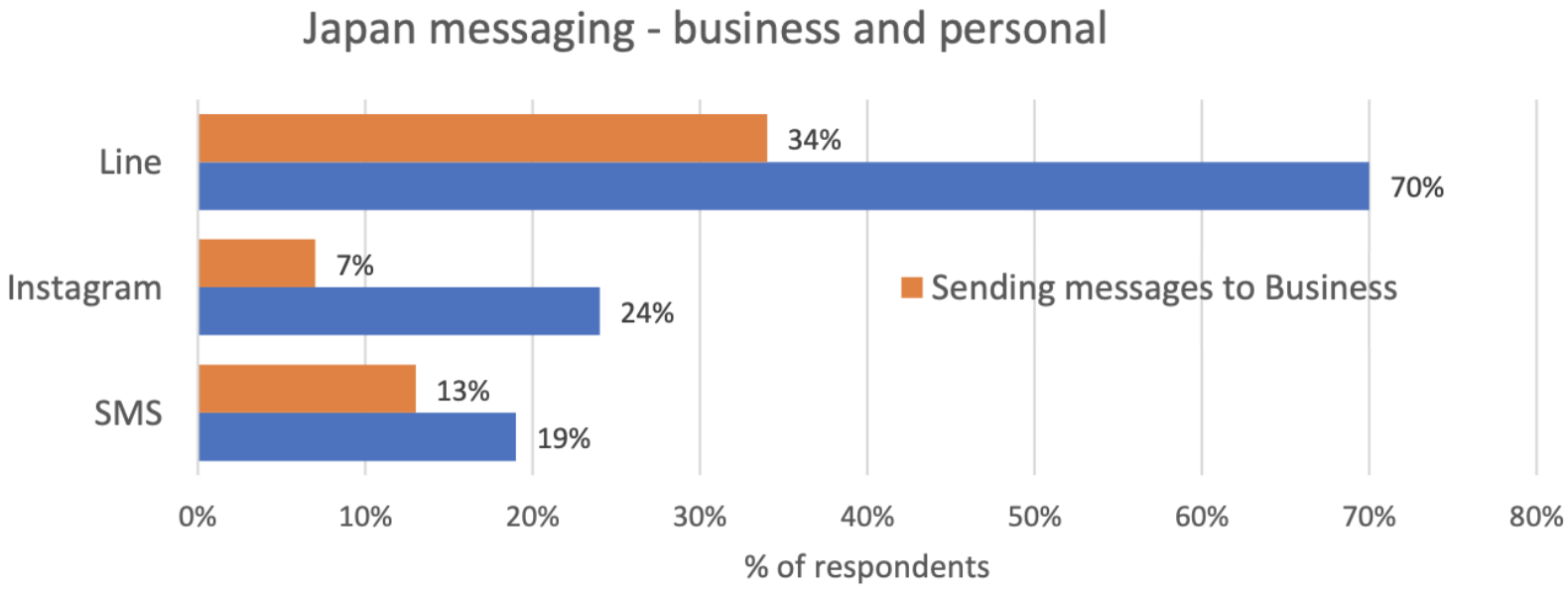
proofpoint.

ユビキタス・メッセージ・チャネル



グローバルSMS/MMSは強力なコマーシャルチャンネル

回線後、SMSは日本のメインチャネル



proofpoint.

MEF MOBILEECOSYSTEMFORUM.COM

ビジネスメッセージ管理プラットフォーム

- 合法的なキャンペーンに関する高度な視覚化とフォレンジック知識を獲得し、加入者を標的とした乱用から保護する。
- A2Pコンテンツを特定し、正しいパスにあることを確認し、適切に評価され、貨幣化されていることを確認する。
- モバイル、企業、規制要件を維持するためのポリシーの管理と実施

価値:

- ビジネス・メッセージの用途に応じた正確な価格設定(2FA、広告、通知、ファースト・レスポンダー)
- あなたの顧客がビジネス・メッセージを「欲しい」と見なすようにする。つまり、不正な送信慣行を緩和する。
- ビジネス・メッセージ用の単一の管理ソース

ソリューション機能

ビジネス・メッセージング・ストリーム(強化されたメトリック/分析)への可視性

送信者、ブランドまたはキャンペーンの可視性。

キャンペーンを完全に管理するコントロールパネル

現在受け入れ可能な使用および/またはポリシー定義を評価し、管理する。

行動や測定基準に基づいてキャンペーンを特定する

プロトコルコンテキスト認識(SMS、MMS、およびRCS-MaaP)

専門的に管理されたクラウドソリューションは、コールアウトまたはインラインのいずれかとして提供されます。

ソリューション:モバイルメッセージセキュリティプラットフォーム
JIRA: PMMS

Internal Use Only – Sales Enablement

ビジネス・メッセージの用途に応じた正確な価格設定(2FA、広告、通知、ファースト・レスポンダー)

あなたの顧客がビジネス・メッセージを「欲しい」と見なすようにする。つまり、不正な送信慣行を緩和する。

ビジネス・メッセージ用の単一の管理ソース

- ソースに関わらず、すべてのA2Pベンダーでの可視性
- SPAM/不正管理
- SPAM、AUP違反、管理されていないSTOP要求などを検出するための現在のキャンペーンに関するSRSからの継続的なフィードバック
- オペレータ宛のALL A2Pメッセージの単一接続管理ポイント。
  - キャンペーンの送信者全員に一貫性を持たせる
  - 執行オプション、すなわちブロッキング/スロットリング、コンテンツ監査、MNO AUPガイドライン、CTIAガイドラインなど
  - 10DLCの管理目標をサポートする柔軟な管理ツール

proofpoint.

ソリューション:ビジネスメッセージ管理プラットフォーム
JIRA: PBMM

ポリシー管理と施行を伴うビジネスメッセージの単一制御点

- キャンペーン・レジストリーの順守
- SRS(7726)による顧客フィードバックループ
- CTIAとAUPの施行
- SPAM/不正防止
- 広範な分析能力
- 停止メッセージの監視