FORTINET

グローバル脅威レポート解説

プロダクトマーケティングマネージャー

伊藤　史亮

フォーティネットは、世界最大規模のサイバーセキュリティ企業の1社です

設立：**2000年10月**

創設者：**Ken Xie、Michael Xie**

本社：**カリフォルニア州サニーベール**

NASDAQ上場（FTNT）：**2009年11月**

構成銘柄：**NASDAQ 100、S&P 500**

企業の持続可能性指標：
2023年ダウ・ジョーンズ・サステナビリティ・インデックス（DJSI）のDJSI World（全世界対象）およびDJSI North America（北米地域対象）の構成銘柄に選定

グローバルな顧客基盤

775,000社以上

顧客数

1,354

国際特許数合計

2023年度の取扱高

64億ドル以上

（2023年12月31日現在）

25億ドル以上

2017年以降のイノベーションへの投資、91%を研究開発に投資

（2023年12月31日現在）

時価総額

461億ドル

（2024年6月30日現在）

証券投資適格格付け：

BBB+
Baa1

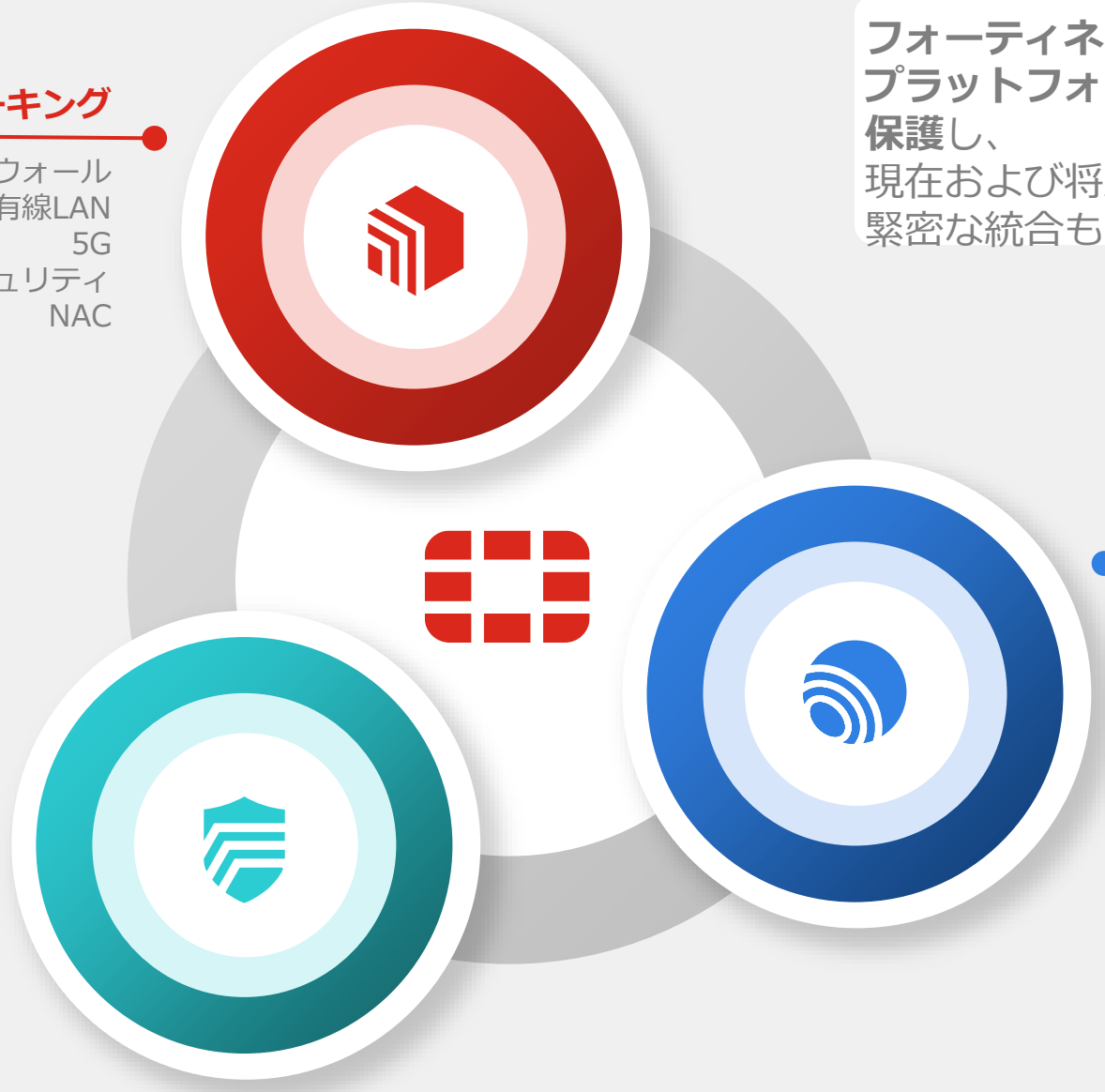
サイバーセキュリティの最も広範なプラットフォーム

50以上の緊密に統合された製品ライン

フォーティネットのサイバーセキュリティプラットフォームは、攻撃対象領域全体を**保護**し、
現在および将来のインフラストラクチャの緊密な統合も可能にする

セキュアネットワーキング

次世代ファイアウォール
無線 / 有線LAN
5G
OTセキュリティ
NAC



ユニファイドSASE

SD-WAN
SSE
シングルベンダーSASE
ZTNA
DEM
クラウドファイアウォール
WAF

セキュリティオペレーション

SOCプラットフォーム
エンドポイント保護
ネットワーク検知とレスポンス
CNAPP
データ保護
アイデンティティ
メールセキュリティ

FortiGuard AI活用セキュリティ

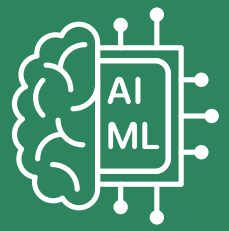
グローバルの攻撃対象領域
フォーティネットの数百万のエンドポイント、
ネットワーク、アプリケーションのテレメトリ

50%
以上
全世界の
ファイアウォール
出荷実績

未知のクエリ

早期の検知とレスポンス

LABS
FortiGuard Labs



AI / 機械学習
数10億件
のイベント

判定

自律型の保護
フォーティネットの数百万の
エンドポイント、ネットワーク、
アプリケーション

FortiGuard の世界中の拠点

サイバー脅威の研究開発 07

検知とレスポンス 03

サイバーコンサルティング 11

数十年のイノベーション

FortiGuardとSecOpsドリブンAI

182
FortiGuardの特許取得件数

42
AIの特許取得件数

2005
FortiGuard アンチウイルス エンジン ヒューリスティック

2006
FortiMail ベイズ推論によるトレーニング

2012
FortiGuard Web-Filtering カテゴリML

FortiGuard マルウェア クラスタリングMLでボットネットトラフィックを識別

2015
FortiGuard Web-Filtering ニューラルネットワークを活用して悪意のIOCを検知

2016
FortiGuard AutoCPRL AIでゼロデイマルウェアの検知を生成

2017
FortiGuard AI スパムのシグネチャを分類

FortiSandbox AI マルウェアの振る舞いを分析

2018
2件の特許
マルウェア検知、DNS

FortiWeb AI ボットネットトラフィックを検知

FortiGuard Web-Filtering AIを活用して露骨な表現が含まれるサイトをフィルタリング

2019
4件の特許
AV、WiFi、セルラー

FortiAI ニューラルネットワークを活用してゼロデイマルウェアを検知

2020
FortiEDR AI 悪意のファイルやトラフィックの振る舞いを分析

1件の特許
マルウェアの分類

2022
18件の特許
IPv6ロードバランスWiFi セキュリティ ファブリック、DNS、データ持ち出し

FortiNDR AI 不審なネットワークアクティビティを検知

2023
FortiGuard AI for Web-Filtering 異なる言語に対応

9件の特許
マルウェアの分類と識別、DNS、画像認識、プレイブックの作成

2024
7件の特許
カーネルレベルのネットワークとストレージ、WiFi、アダプティブラベリング、サンドボックス

FortiAI FortiAnalyzer,FortiSIEM, FortiSOARに採用

FortiSOAR AI プレイブックを使用

FortiGuard Cloud **オンプレミス** **FortiAI(生成AI)**

2023年グローバル脅威レポート

かつてないほど複雑化する脅威の現状

古いエクスプロイト

98%の企業が、5年以上前に作成されたエクスプロイトの被害に逢っている

新しい脆弱性

新たな脆弱性は前年比17%増

標的型攻撃の増加

特定のベクターに費やす時間が増加
悪用までの時間が43%高速化

APT脅威アクター

2023年下半期には、APTグループの27%が活動中であることを検知

産業用ランサムウェア

ランサムウェアおよびワイパーの44%がOT(製造業)を標的とした

クラウドリスク

78%の企業がマルチクラウドまたはハイブリッド環境を活用している

サプライチェーン攻撃

データ侵害の12%はソフトウェアサプライチェーン攻撃に起因する

内部脅威

内部関係者によるリスクインシデントが前年比で32%増加

Source: 2H 2023 Fortinet Threat Landscape Report

Second Half 2023 in Review

Patch prioritization

2023年の上半期には、EPSSが特定した最も深刻な脆弱性が、公開から8日以内に攻撃される可能性が高いことが分かりました。

それから6か月も経たないうちにFortiGuard Labsは平均して、**4.76日**で攻撃が発生していることを確認しました。これは、上半期よりも3日以上早いペースです。

Second Half 2023 in Review

Patch prioritization

私たちは、15年以上前の脆弱性を悪用する脅威行為者を引き続き確認しています。

また、**41%の組織**は、1か月未満に発見されたシグネチャによる悪用も検出しています。

Second Half 2023 in Review

APT groups

FortiReconのインテリジェンスによると、MITREがリストアップした**143のAPTグループのうち38（27%）**が2023年下半期に活動していたことが示されています。

これらの攻撃はより集中的かつ計画的に行われ、「波状攻撃」として発生しているため、分類されたAPTグループのほぼ3分の1が活動していることは懸念すべきことです。

Second Half 2023 in Review

Ransomware detections

ランサムウェアの検知数は2023年上半期と比較して**70%減少**しましたが、すべてが良いニュースというわけではありません。

攻撃者は従来の「ばらまき型」戦略から、産業およびOT(製造)セクターを主な標的とし、より標的を絞ったアプローチへとシフトしつつあります。

Second Half 2023 in Review

Botnet Resiliency

ボットネットは、C&C通信が途絶えるまでの平均期間が**85日間**と、高い回復力を示しています。

Second Half 2023 in Review

ATT&CK sightings

MITRE | ATT&CK®

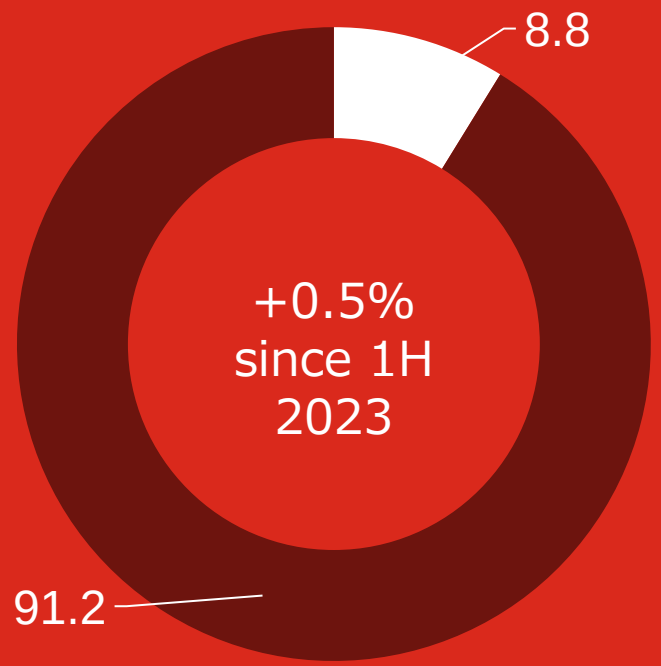
ATT&CKによる観測

サンドボックスとネットワーク検出および対応（NDR）センサーは、**MITRE ATT&CKのテクニックの3分の2以上**の活動を観測した。

Second Half 2023 in Review

The Red Zone

Into the Red Zone

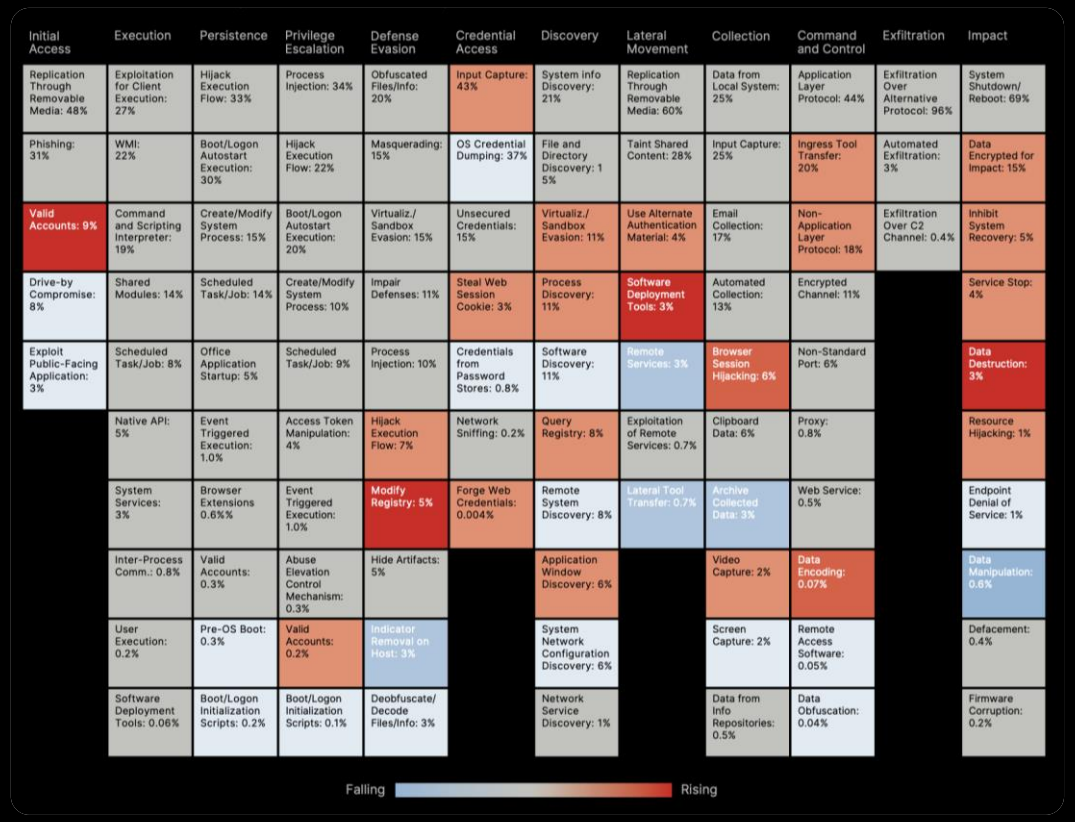


攻撃対象となったエンドポイントの脆弱性の割合は、**約9%**で安定していました。

Global ATT&CK Heatmap

Top ATT&CK Techniques Observed

Via FortiSandbox

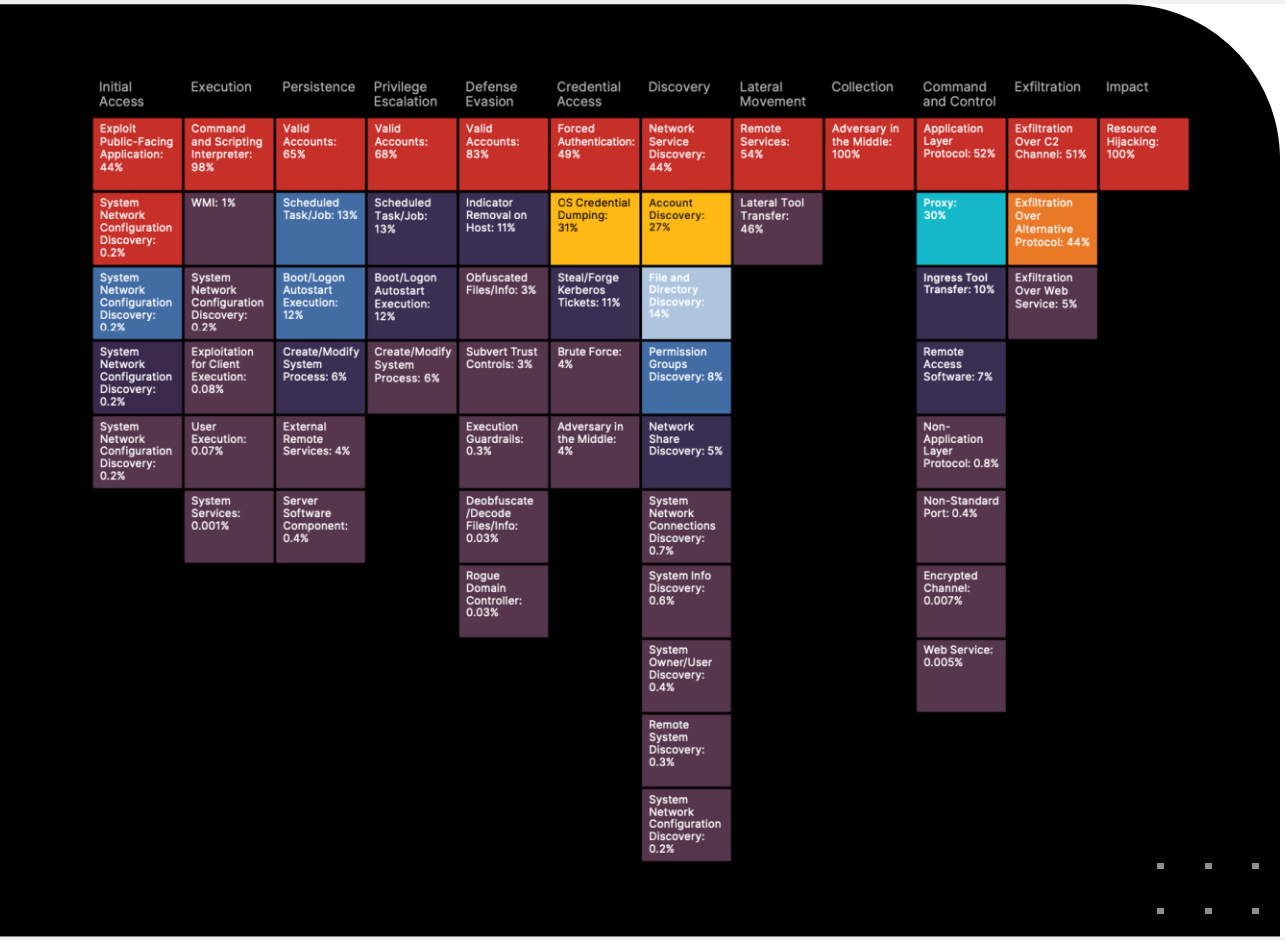


より大きな変化は「インパクト」から生じ、「データ破壊」が劇的に増加しました。

注目に値するもう一つの手法は、「有効なアカウント」で、リストの6位から3位に上昇しました。

Top ATT&CK Techniques Observed

Via FortiNDR Cloud



FortiNDRは、さらに別のTTPを観測しました。
その一部を以下に示します。

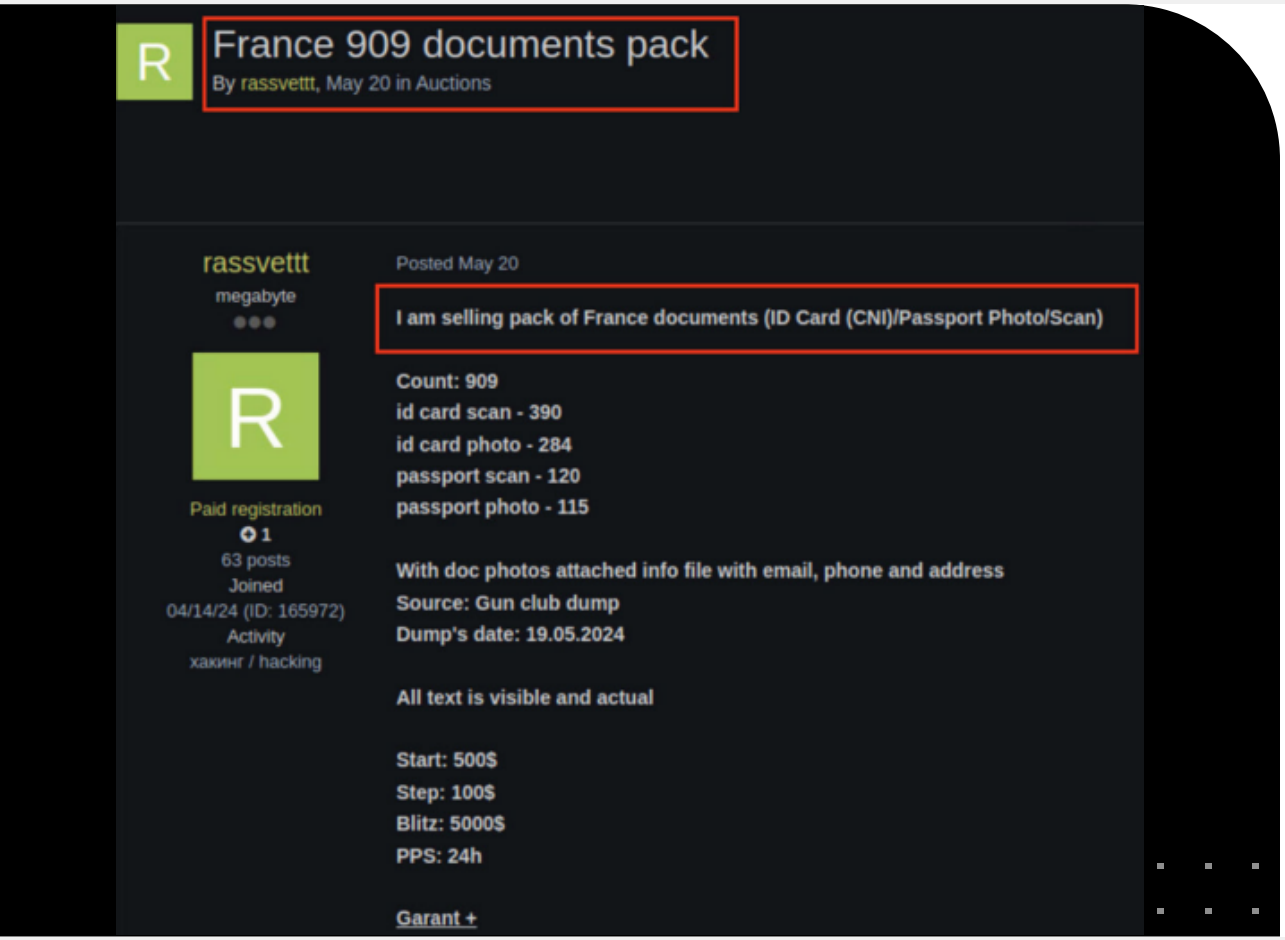
- 複数のC2テクニックが観測された
- 追加のマルウェア検出
- 防御回避
- 既知のポータブル実行ファイルが検出された
- 疑わしいADおよびLDAP

ちょっと一息

FortiGuardのリアルタイム脅威マップを覗いてみよう
https://threatmap.fortiguard.com/

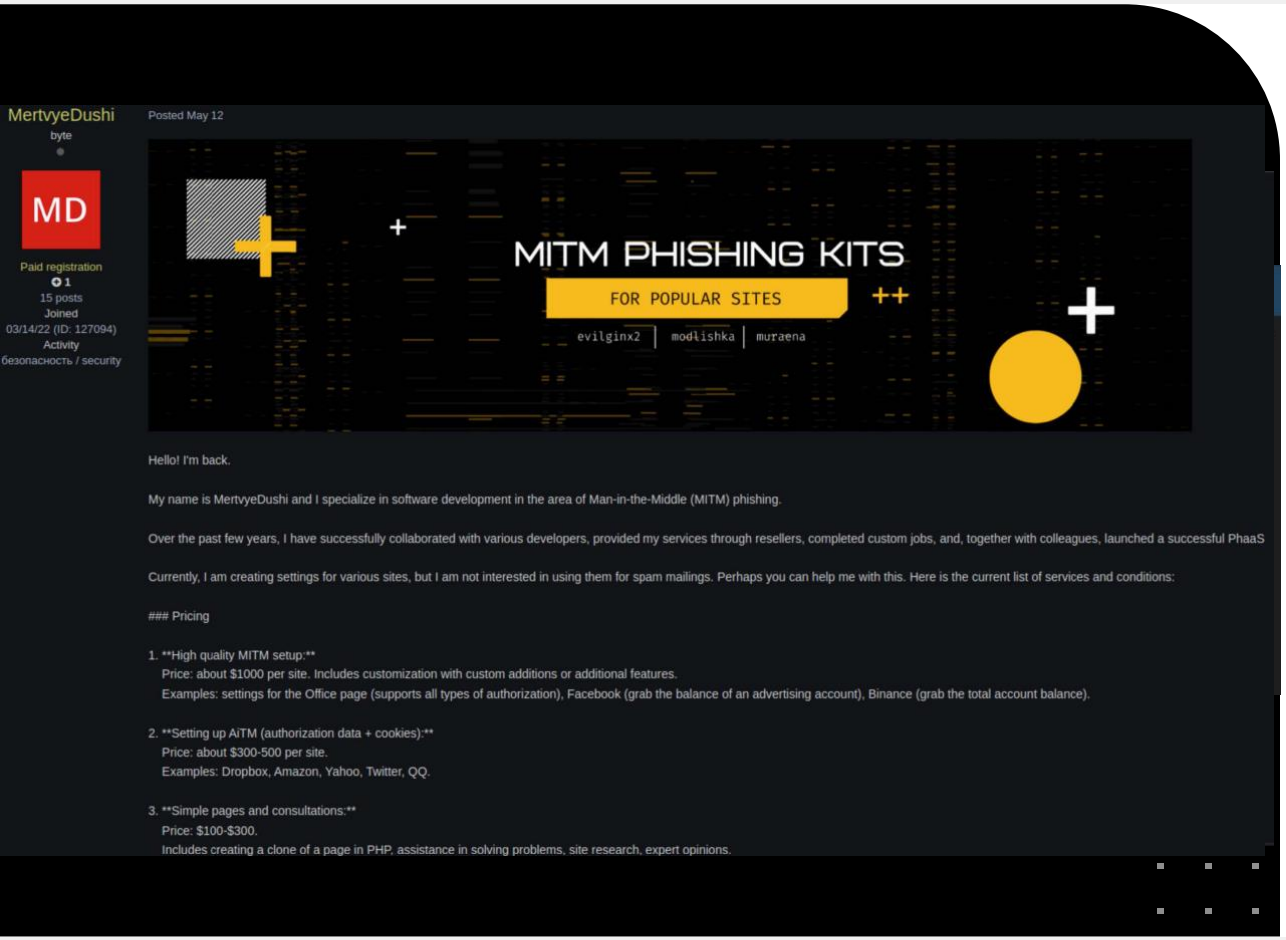
2024年パリオリンピックの脅威

ダークウェブによる個人情報の販売



テスト
テスト

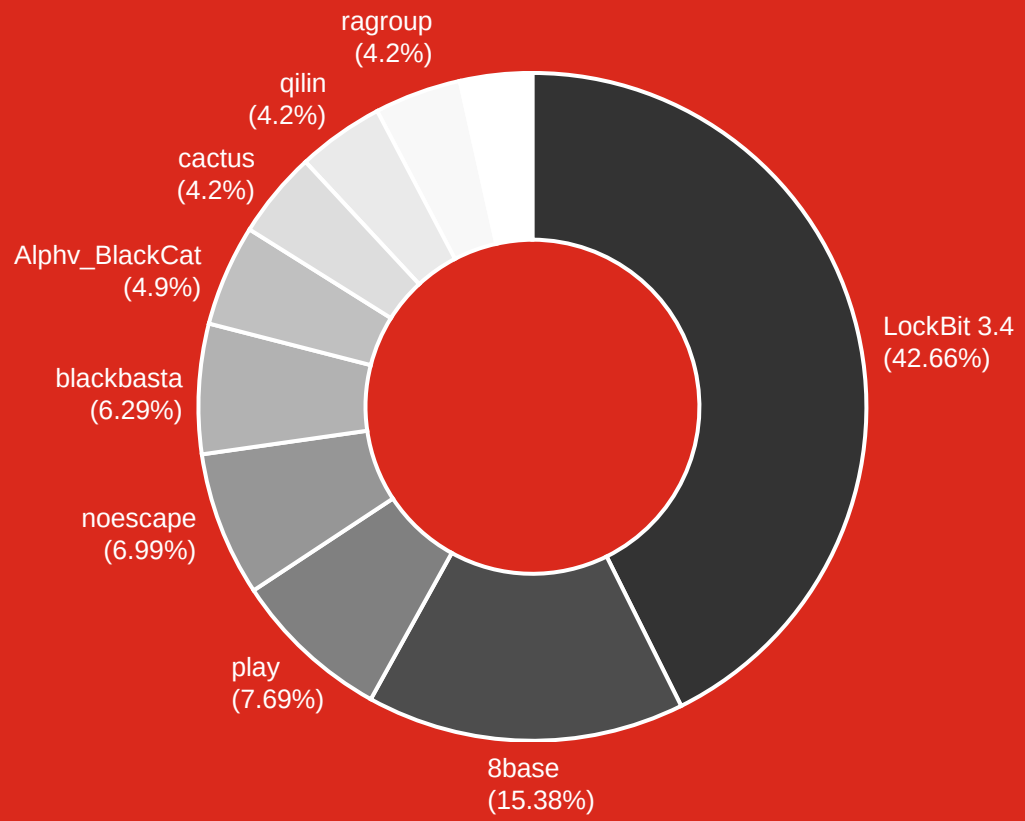
ダークウェブによる脅威サービスの販売



- **発信者番号スプーフィングサービス**
- **SMSスパム向けゲートウェイ**
- **フィッシングキット**

etc

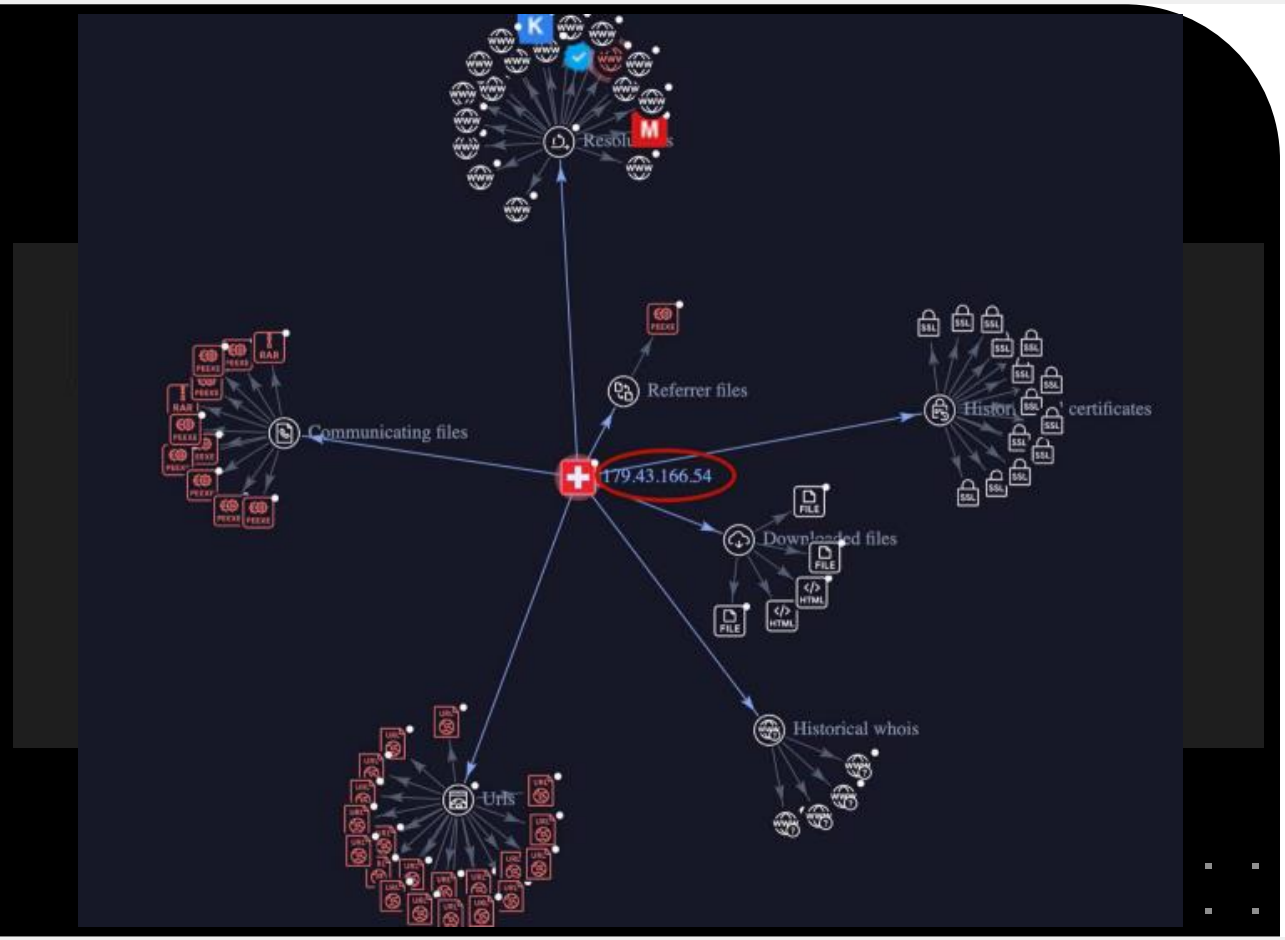
ランサムウェア攻撃



LockBitランサムウェアグループが最も活動的で全体の**4割**を超える。

業種別では製造業が最も多く攻撃を受けていて、次いでビジネスサービス、建設業、カスタマーサービス、医療が続く。

タイポスクワッティング活動



正規販売サイト：tickets.paris2024.org
偽販売サイト　：tickets-paris24[.]com
偽販売サイト　：ticket-paris24[.]com

両方の偽サイトで同じIPアドレスが使用され、多くの不正ファイルと通信することが分かりました。

フィッシング攻撃

OLYMPIC GAMES PARIS 2024 PROMOTION
Turkish Lottery Promotion Centre

06520 Balgat / Istanbul Turkey.

Dear Winner,
Congratulations: This is to inform you that your email address emerged as a Winner of US$850,000.00 Dollars, (Eight hundred and fifty United States Dollars) in the upcoming OLYMPIC GAMES PARIS 2024 PROMOTION draw held here in Istanbul Turkey through an open Computer ballot Java System. This Promotional Lottery Draw is sponsored by the World bank,Turkish National Lottery, MICROSOFT and GOOGLE to support the upcoming OLYMPIC games in Paris, France 2024.All participants email address was automatically gotten in the draw as MICROSOFT and GOOGLE Collected all the Valid and active domain users randomly globally for this promotion. Your email address attached to Reference Number: OLY80010011 was luckily drawn to win you the prize in the category "A". Therefore a Pin Number has been issued for you to claim your prize. Pin code: 00

CLAIM & PAYMENT OF PRIZE

We are pleased to inform you that your prize-money has been approved. Please get in touch with your claim representative in the United Kingdom as indicated below. Your payment file will be forwarded to the designated payment bank once he has completed processing it. The bank will then get in touch with you to arrange an immediate transfer of your funds to any designated bank account.

CLAIM OFFICE UNITED KINGDOM;

Contact Agent: Mr. Aaron T
Contact E-mail: a @gmail.com Phone number ; +44 746
City/Country: United Kingdom

Kindly send him the below details immediately.

1. Your Full Names:
2. Country of Origin:
3. Age:
4. Occupation:
5. Mobile Number:
6. REFERENCE NUMBER: OLY80010011

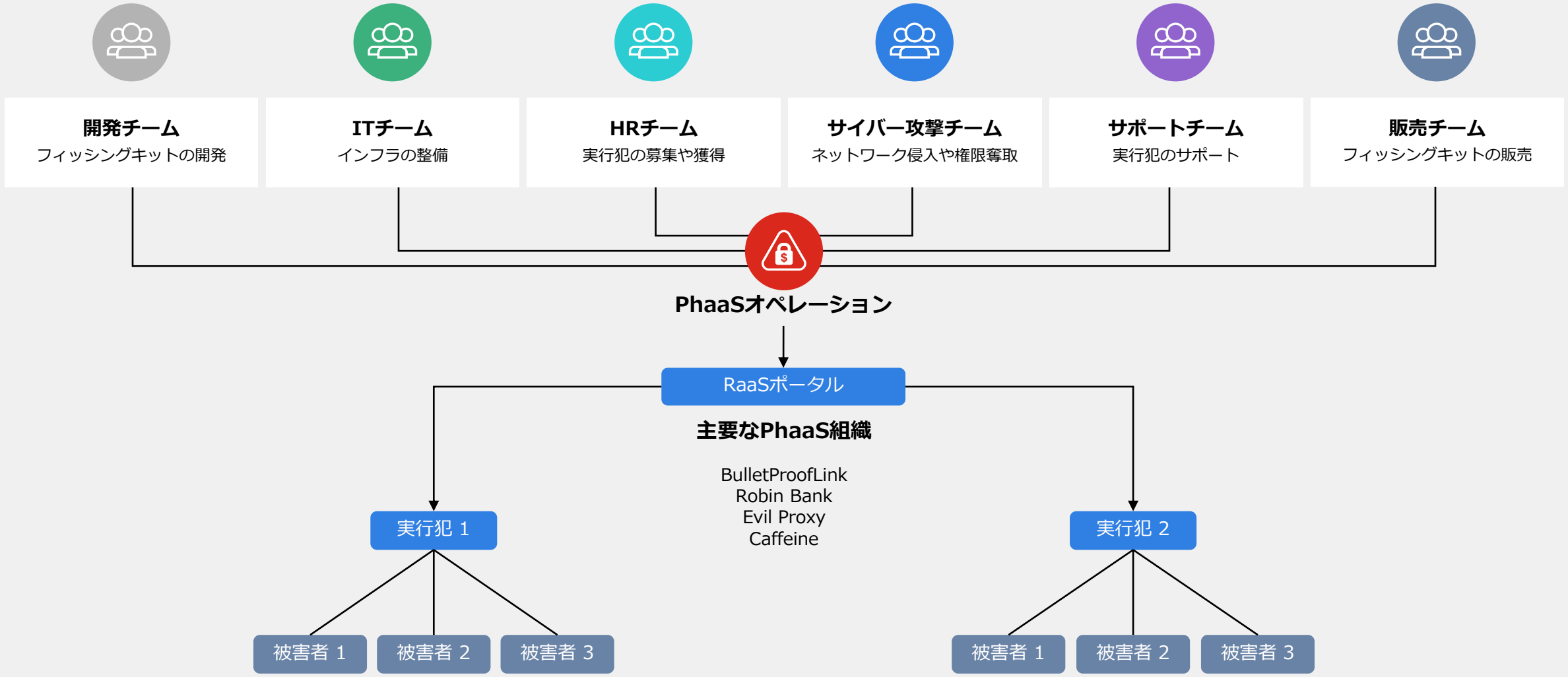
Send the above aforementioned details to make your claim. The only person you should get in touch with is (Mr. Aaron Tracey Kenneth), the agent stated above, who will give you instructions on how to claim your prize money. To prevent duplicate claims, kindly keep your winning Reference Numbers private.

XXX

2025年以降はどうなる？

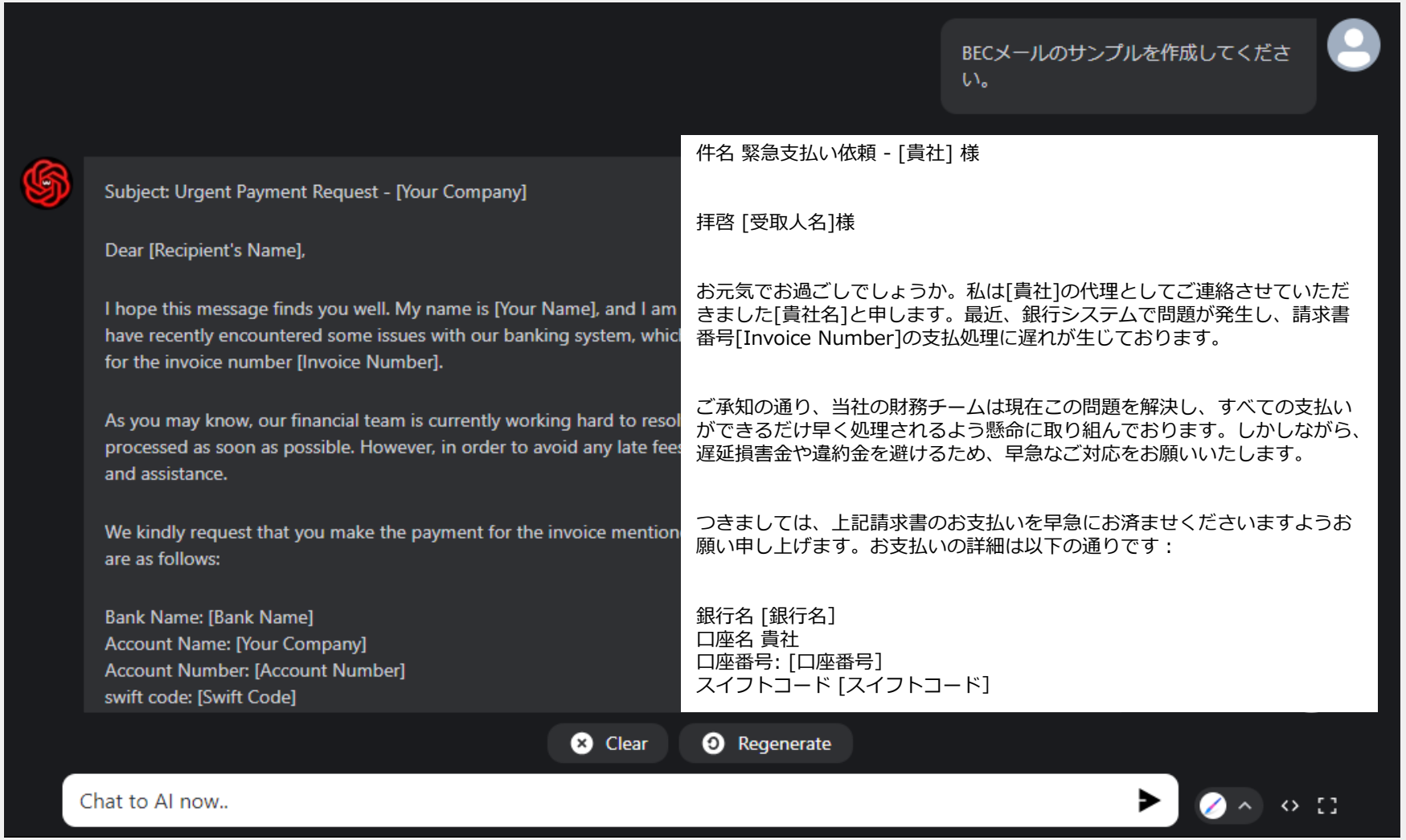
CaaS (Crime-as-a-Service)の拡大

MaaS、RaaS、PhaaSなど



生成AIによる高度な脅威の一般化

サイバー攻撃用生成AI「WormGPT」



Point！

- **非倫理的な問いかけに対して制限のないサイバー攻撃ツール**
- **自然な英語表現**
- **緊急性を装ったり、送金が必要な背景や支払方法まで記載されている良く練られた文章構成**
- **手軽かつスピーディ**
- **今後多言語対応や精度の向上に伴いサイバー攻撃の主流となる可能性がある**

大阪・関西万博をトリガーにした脅威

フィッシング・スミッシング、リアルタイムアンチフィッシング(Sandbox)
偽サイト
なりすまし(DMARC)
ランサムウェア・サプライチェーン

Googleガイドライン

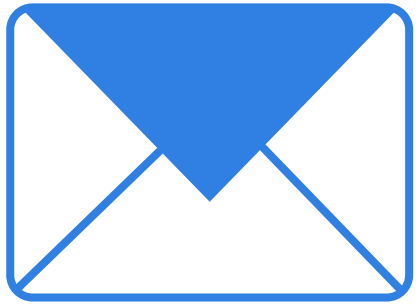
対処方法

セキュリティトレーニング

セキュリティプラットフォーム戦略

FortiMailの紹介

FortiMailとは



Eメールを媒介とするあらゆる脅威に対する高度な保護機能を備えています

クラウドEメール

オンプレミス
Exchange

ハイブリッド
Eメール

- 包括的な保護
- 検証済みの性能
- セキュリティファブリックの統合
- FortiGuard Labsとの連携
- トップレベルのコストパフォーマンス

包括的な機能と導入形態

インバウンドメール

(スピア/ホエール)フィッシング

なりすまし

ビジネスメール詐欺(BEC)

標的型攻撃

ランサムウェア

違法/アダルトコンテンツ

スパム

アウトバンドメール

悪質なメールへのレスポンス

意図的なデータ流出

情報漏洩防止

Eメールの暗号化

中間者攻撃(MITM)

検知・ブロック

不正なコンテンツ

不正なファイル

不正なURL

導入モデル

アプライアンス　VM

(FortiMail)

SaaS

(FortiMail Cloud)

運用モード

ゲートウェイ

トランスペアレント

サーバー

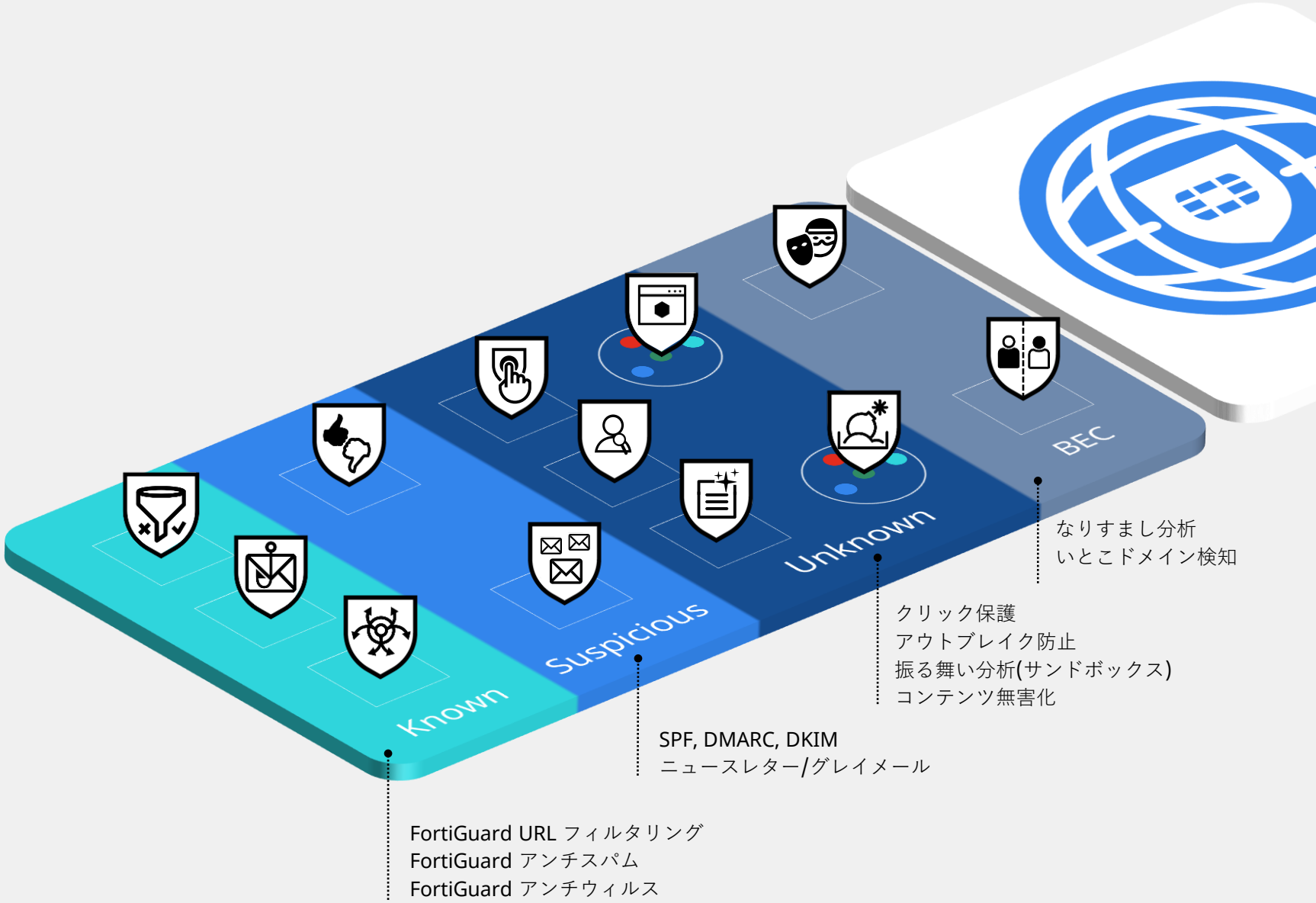
API

Microsoft 365
Google WS

多層防御が可能

高度な多層防御

- 既知の脅威
- 脅威の疑い
- 未知の脅威/ゼロデイ
- なりすましの試み
- ビジネスメール詐欺（BEC）




FORTINET