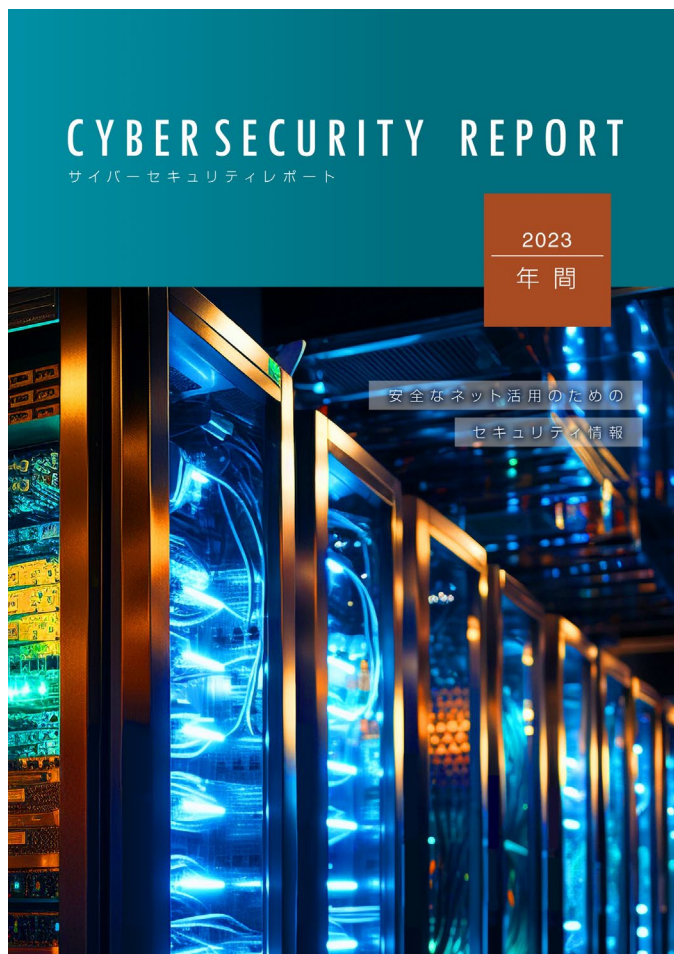


2024年3月27日





2023年サイバーセキュリティレポート 紹介動画



2023年サイバーセキュリティレポート



掲載テーマ一覧

-  **1章** | 2023年マルウェア検出統計
-  **2章** | Goで実装されたマルウェアの脅威動向
-  **3章** | Webの脆弱性からビジネスを守る効果的な方法
-  **4章** | サイバーセキュリティの国際連携の強化

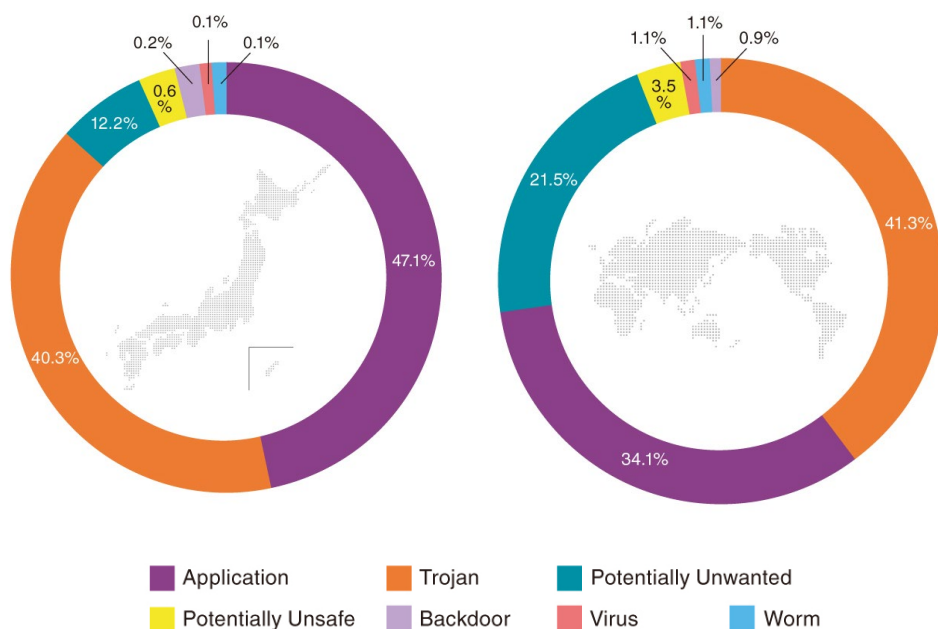
サイバーセキュリティ情報局にて公開中



概要

2023年にESET製品で検出されたマルウェアの統計を解説
本レポートから新たにカテゴリー別マルウェア検出統計も掲載しています。

マルウェア検出数のカテゴリー別割合



マルウェア検出数のカテゴリー別割合を分析

非常に小さい割合ですが、感染後に大きな被害を起こす可能性がある
Virus、Worm、Backdoorに着目

想定される被害

- 攻撃者による端末操作
- ネットワークを通じた感染拡大

これらの脅威は端末内部で潜伏することがよくあるため、
マルウェアの侵入に気付ける体制を構築することが重要

甚大な被害をもたらすマルウェアもあるため、検出数の大小にかかわらず脅威について知ることが重要



概要

近年注目度が高まっているGoで実装されたマルウェアの動向を解説
Goがマルウェア開発に用いられる要因について3つの観点からの考察も掲載しています

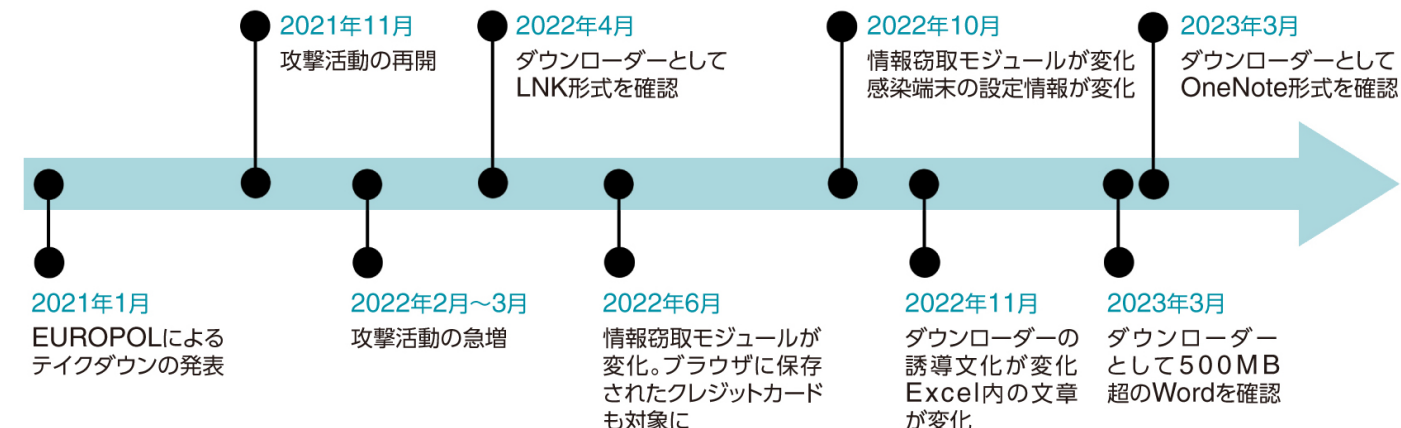
攻撃者はマルウェアを変化させ続けている

Ex) Emotet

- 新しいダウンローダー形式の導入
- 情報窃取モジュールのアップデート
- セキュリティ製品回避手法

近年ではマルウェアの実装言語も変化

Emotetの変化タイムライン



Goがマルウェア開発言語として注目度が高まっている理由を3つの観点から考察

1. クロスコンパイル機能
2. 解析難易度
3. セキュリティ製品回避

セキュリティ製品のすり抜けや攻撃の痕跡が変化するため動向に注視が必要

概要

ペネトレーションテストとWAFの基本的な概念、強み、運用上のポイントを解説
ペネトレーションテストがWAFを補完した事例についても掲載しています

	強み	弱み
ペネトレーションテスト	<ul style="list-style-type: none">・ WAFで防げない脆弱性を発見できる・ セキュリティ向上に向けた具体的なアドバイスが得られる	<ul style="list-style-type: none">・ 実施までに入念な準備が必要・ 攻撃を常時防ぐ目的には向かない
WAF	<ul style="list-style-type: none">・ 自動的に攻撃に対処できる・ リアルタイムに常時稼働できる	<ul style="list-style-type: none">・ すべての攻撃を防ぐことはできない・ 検出ルールを改善するには専門知識と作業工数が求められる



強みを生かして組み合わせる

組み合わせのポイント

1. WAFの活用 2. 継続的なペネトレーションテスト 3. セキュリティポリシーの見直し 4. より広範囲なセキュリティの洞察

セキュリティ対策は単純にツールを導入すれば終わるものではなく、継続的な評価と向上のプロセスが不可欠

概要

サイバー犯罪者を検挙した事例紹介やサイバー犯罪の国際化について解説
サイバーセキュリティにおける国際連携について日本の各省庁の動向も掲載しています

国際連携によってサイバー犯罪を検挙した事例

Ragnar Locker

主に**大企業を標的**として、ファイル暗号化・身代金要求を行うランサムウェアグループ
窃取したデータを公表するという「**二重の恐喝**」も行います



2023年10月、Ragnar Locker掃討作戦が実施されました

フランスが作戦を主導

チェコ、ドイツ、日本、ラトビア、オランダ、スペイン、スウェーデン、ウクライナ、アメリカを含む11か国が参加

➡ Ragnar Lockerが使用していたサーバーなどの**インフラを差し押さえ**、
開発者とみられる**主犯格をフランスで逮捕**しました

各国の国際連携に対する攻撃者の動向に注意が必要



サイバーセキュリティ情報局のご紹介

キヤノンマーケティングジャパンが提供する最新のセキュリティ情報

最新のセキュリティ動向やキーワード解説のほか

サイバーセキュリティラボがまとめた

マルウェア動向を詳細なレポートにて提供

情報収集にご活用ください

サイバーセキュリティ情報局

検索



3CX社のハッキング被害から学ぶ、サプライチェーン攻撃の脅威と対策

サポート対象外となったトレーディング・ソフトウェアが、トロイの木馬化されることによって攻撃が始まった事件がある。本記事では、3CX社の事件から得られた教訓

2024.3.5

アクセスランキング

1 スマホがウイルスに感染！不安に思ったら試したい5つの方法

2 そのウイルス警告は本物ですか？iPhoneが発する警告表示の意味とは？

イの木馬に感染したらどうな
どう対処すればよいのか？

ス警告だと判断できる？把
き正常な警告とは

イルスに感染したらどうな
除の対策を解説

まされるのか？その確認方
のか？

ルに感染したらどうな
感染する可能性は？

どう解除する？そもそも解



ご視聴ありがとうございました。