Press Release
2024 年 4 月 12 日（金）
ウォッチガード・テクノロジー・ジャパン株式会社

ウォッチガード、2023 年第 4 四半期最新インターネットセキュリティレポートを発表：脅威を大幅に加速させる回避型マルウェアが急増

環境寄生型攻撃の復活、サイバー攻撃のコモディティ化の継続、ランサムウェアの減少

2024 年 4 月 12 日（金） - 企業向け統合型サイバーセキュリティソリューション（ネットワークセキュリティ／セキュア Wi-Fi／多要素認証／エンドポイントセキュリティ）のグローバルリーダーである WatchGuard（R）Technologies の日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、代表執行役員社長 谷口 忠彦、以下ウォッチガード）は、四半期毎に発行している**「インターネットセキュリティレポート」**の最新版（2023 年第 4 四半期）を発表しました。本レポートでは、ウォッチガードの脅威ラボの研究者たちによって分析された、マルウェアのトップトレンドやネットワークセキュリティおよびエンドポイントセキュリティの脅威に関する詳細を報告しています。データから得られる主な調査結果としては、回避型マルウェアの急増がマルウェア全体の大幅な増加につながったこと、攻撃者がオンプレミスのメールサーバを格好の標的として悪用していること、また、ランサムウェアの検知数が減少を続けており、これは法執行機関によるランサムウェア恐喝グループの国際的な摘発活動の結果である可能性があることなどが挙げられます。

ウォッチガードの CSO（チーフセキュリティオフィサー）、Corey Nachreiner（コリー・ナクライナー）は次のように述べています。「脅威ラボの最新の調査によると、攻撃者は古いソフトウェアやシステムを含め、標的となる脆弱性を探しながら様々なテクニックを駆使しており、組織はこのような脅威から身を守るために、徹底的に防御するためのアプローチを採用しなければなりません。組織が依存しているシステムやソフトウェアを更新することは、これらの脆弱性に対処するための重要なステップです。マネージドサービスプロバイダーが運用する最新のセキュリティプラットフォームでは、組織が必要とする包括的かつ統合されたセキュリティを提供し、最新の脅威に対抗することができます。」

以下に、ウォッチガードの最新インターネットセキュリティレポート（2023 年第 4 四半期版）における主な調査結果を紹介します：

- **第 4 四半期は、回避型、基本型、暗号化型のすべてのマルウェアが増加し、マルウェア全体の増加に拍車：** Firebox 1 台あたりの平均マルウェア検知数は、前四半期から 80%増加し、ネットワーク境界に到達するマルウェアの脅威が大幅に増加したことを示しています。地域別では、マルウェア件数の増加の大部分は、南北アメリカとアジア太平洋地域に影響を及ぼしています。
- **TLS とゼロデイマルウェアも増加：**マルウェアの約 55% が暗号化された接続を介して到達しており、これは第 3 四半期から 7%増加しています。ゼロデイマルウェアの検知数はすべてのマルウェア検知数に対して、前四半期の 22%から 60%に急増しました。しかしながら、TLS を用いたゼロデイマルウェアの検知率は 61%に低下し、第 3 四半期から 10%減少しました。

- **上位 5 つのマルウェアのうち、2 つの亜種が DarkGate ネットワークにリダイレクト：**最も広く検知されたマルウェアのトップ 5 の中には、JS.Agent.USF と Trojan.GenericKD.67408266 が含まれています。どちらのマルウェアもユーザーを悪意のあるリンクにリダイレクトし、被害者のコンピュータに DarkGate マルウェアをダウンロードしようとします。
- **環境寄生型の手法が急増：**第 4 四半期はスクリプトベースの脅威が復活し、エンドポイント攻撃のベクトルとしてスクリプトが最も増加し、検知された脅威は第 3 四半期から 77%増加しました。脅威ラボの調査では、PowerShell がハッカーがエンドポイントで使用する攻撃ベクトルのトップでした。ブラウザを悪用した攻撃も大幅に増え、56%増加しました。
- **最も拡大したネットワーク攻撃の上位 5 件のうち、4 件が Exchange サーバへの攻撃：**これらの攻撃は、特に ProxyLogon、ProxyShell、ProxyNotShell 攻撃のいずれかと関連しています。ProxyLogon シグネチャは、2022 年第 4 四半期に最も拡散されたネットワーク攻撃のトップ 5 に 4 位で初登場し、2023 年第 4 四半期には 2 位に上昇しました。これらの攻撃は、セキュリティの脅威を軽減するために、オンプレミスのメールサーバへの依存を減らす必要性を示しています。
- **サイバー攻撃のコモディティ化が進み、「サービスとしての被害者攻撃（victim-as-a-service）」化する傾向：**Glupteba と GuLoader は、第 4 四半期に最も流行したエンドポイントマルウェアのトップ 10 に再びランクインし、当四半期に分析された最も多発した亜種として返り咲きました。Glupteba は、世界的な規模で被害者を狙ったマルウェアが流行していることもあり、特に手強く巧妙な敵対勢力として注目に値します。多面的な「サービスとしてのマルウェア：MaaS」である Glupteba の悪意のある機能には、追加のマルウェアのダウンロード、ボットネットとして偽装、機密情報の窃取、および非常にステルス性の高い暗号通貨のマイニングなどが含まれます。
- **ランサムウェアの恐喝グループを阻止する取締り活動：**第 4 四半期も、脅威ラボはランサムウェアの検知数が前四半期と比較して減少していることを報告し、2023 年最後の 3 ヵ月間から全体数が 20%減少しました。ウォッチガードの脅威アナリストは、公にされているランサムウェアの侵害の減少も指摘しており、この傾向は、ランサムウェアの恐喝グループに対する法執行機関の継続的な取締まり努力によるものだとしています。

ウォッチガードの Unified Security Platform（R）（統合型セキュリティプラットフォーム）アプローチやウォッチガードの脅威ラボのこれまでの四半期ごとのリサーチアップデートと同様、この四半期レポートで分析されているデータは、ウォッチガードのリサーチ活動に賛同するウォッチガードのネットワークおよびエンドポイント製品を利用するお客様から、匿名により収集した脅威インテリジェンスに基づいています。

レポート全文は以下よりダウンロードできます。
https://www.watchguard.com/wgrd-resource-center/security-report-q4-2023（英語版）

*日本語版は追って掲載する予定です。

【WatchGuard Technologies について】

WatchGuard（R）Technologies, Inc.は、統合型サイバーセキュリティにおけるグローバルリーダーです。ウォッチガードの Unified Security Platform（TM）（統合型セキュリティプラットフォーム）は、マネージドサービスプロバイダー向けに独自に設計されており、世界トップクラスのセキュリティを提供することで、ビジネスのスケールとスピード、および運用効率の向上に貢献しています。17,000 社を超えるセキュリティのリセラーやサービスプロバイダと提携しており、25 万社以上の顧客を保護しています。ウォッチガードの実績豊富な製品とサービスは、ネットワークセキュリティとインテリジェンス、高度なエンドポイント保護、多要素認証、セキュア Wi-Fi で構成されています。これらの製品では、包括的なセキュリティ、ナレッジの共有、明快さと制御、運用の整合性、自動化という、セキュリティプラットフォームに不可欠な 5 つの要素を提供しています。同社はワシントン州シアトルに本社を置き、北米、欧州、アジア太平洋地域、ラテンアメリカにオフィスを構えています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多彩なパートナーを通じて、国内で拡大する多様なセキュリティニーズに応えるソリューションを提供しています。詳細は https://www.watchguard.co.jp をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向は Twitter（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。また、最新の脅威に関するリアルタイム情報やその対策法は SecplicityJP までアクセスして下さい。
SecplicityJP： https://www.watchguard.co.jp/security-news

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041
東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
マーケティング担当
Tel： 03-5797-7205 Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： https://www.watchguard.co.jp