

ウォッチガード、2024年第1四半期最新インターネットセキュリティレポートを発表： 企業向けスマートTVを標的としたマルウェア「Pandoraspear」が広く検知

エンドポイントでのマルウェア検知が急増、 年明けに Chromium ベースのブラウザが広範に狙われる

2024年6月21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（2024年第1四半期）を発表しました。本レポートでは、第一四半期に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、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傾向の詳細を報告しています。

本レポートの主な調査結果としては、当四半期におけるマルウェアのネットワーク全体の検知数が前四半期と比較してほぼ半減した一方で、エンドポイントを標的としたマルウェアの検知数は 82%増加しました。ランサムウェアの検知数は 2023 年第 4 四半期と比較して 23%減少し、ゼロデイマルウェアの検知数は 36%減少しました。また、オープンソースの Android OS を搭載したスマートテレビを狙うマルウェア Pandoraspear が、最も多く検知されたマルウェアのトップ 10 にランクインし、企業のセキュリティにとって IoT デバイスの脆弱性が潜在的なリスクであることが浮き彫りになりました。

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。「2024 年第 1 四半期のインターネットセキュリティレポートの調査結果は、インターネットに接続されたデバイスの安全性を確保することの重要性を、ビジネス目的か娯楽目的かにかかわらず、あらゆる規模の組織で実証しています。最近の多くの侵害ケースで見られたように、攻撃者はあらゆる接続デバイスを通じて企業ネットワークに足場を築き、水平移動して重要なリソースに甚大な損害を与え、データを流出させることができます。こうした状況の中、すべてのデバイスとエンドポイントの広範な監視を含む、マネージドサービスプロバイダーが管理可能な統合型のセキュリティアプローチを採用することが、組織にとって今や必須になっています。」

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（2024 年第 1 四半期版）における主な調査結果を紹介します：

- WatchGuard Firebox 1 台あたりの平均マルウェア検知数は、第 1 四半期に約半分（49%）に激減し、暗号化された接続を介して配信されたマルウェアの量は、第 1 四半期に 14 ポイント増の 69%に達しました。
- マルウェアファミリー Mirai の新しい亜種は、侵害されたシステムにアクセスするために新しいエクスプロイト（CVE-2023-1389）を使用することで TP-Link Archer デバイスを標的とし、今四半期で最も広まったマルウェアキャンペーンの 1 つに浮上しました。この Mirai の亜種は、世界中の WatchGuard Firebox の約 9%で観測されました。

- 今四半期は、Chromium ベースのブラウザが、Web ブラウザやプラグインを攻撃源とするマルウェアの総量の 4 分の 3 以上（78%）を生成していることが判明し、前四半期（25%）と比較して大幅に増加しました。
- 2023 年に初めて確認された、広く使用されている HAProxy Linux ベースのロードバランサーアプリケーションの脆弱性が、今四半期のネットワーク攻撃の上位に入りました。この脆弱性は、一般的なソフトウェアの弱点がいかに広範なセキュリティ問題につながるかを示しています。

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。

インターネットセキュリティレポートの最新版（2024 年第 1 四半期）の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-q1-2024>（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ーと提携しており、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> をご覧ください。

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>

WatchGuard は、WatchGuard Technologies, Inc.の登録商標です。その他の商標は各社に帰属します。

【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>