Press Release
2025 年 4 月 25 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、2024 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：サイバー犯罪者が高度で暗号化された接続を悪用するネットワークマルウェアが 94%増加

クリプトマイナーの検知数の増加、ゼロデイマルウェアの急増、エンドポイントマルウェアの減少、Linux ベースの脅威の増加

2025 年 4 月 25 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 4 四半期）を発表しました。本レポートでは、第 4 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観測された、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主な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には、脅威の着実な増加が反映され、ネットワークベースのマルウェア検知数が 94%（前四半期比）増加したことが含まれています。同時に、Gateway AntiVirus（GAV）の検知数が 6%増加し、Advanced Persistent Threat（APT）Blocker の検知数が 74%増加するなど、すべてのマルウェアの検知数が増えていることが示されています。そして最も顕著に増加したのは、IntelligentAV（IAV）が提供するプロアクティブな機械学習による検知数で 315%となっており、暗号化されたチャネルから侵入するゼロデイマルウェアのような高度な回避型マルウェアに対して、よりプロアクティブなマルウェア対策サービスによる捕捉の役割が高まっていることを示しています。回避型攻撃が大幅に増加したことは、攻撃者が難読化や暗号化に注力し、従来の防御方法に課題を突き付けていることを示唆しています。

また、脅威ラボは、クリプトマイナーの検知率が前四半期比で 141%増と大幅に増加したことを確認しました。暗号通貨マイニングは、ビットコインを含むいくつかのブロックチェーン上で暗号通貨を取得するための通常プロセスです。悪意のあるコインマイナーは、ユーザーの認識や同意なしにコインマイナーをインストールする実行ソフトウェアを使用しているようです。ビットコインの価格と人気が上昇するにつれ、クリプトマイナーの検知も、脅威アクターが用いる悪意のある手法として目立っています。

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。「2024 年第 4 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からは、攻撃者が旧来の習慣や、悪用しやすい脆弱性や欠陥に依存し続けている一方で、従来の防御を回避するために回避型マルウェアのテクニックを活用している、といったサイバーセキュリティの状況が明らかになりました。このデータは、基本的な警戒を怠らないことの重要性を示しています。すなわち、システムを積極的に更新し、異常なアクティビティを監視しつつ、ネットワークやエンドポイント全体で避けられない悪用の試みを捕捉するために多層防御の仕組みを活用することです。そうすることで、企業は今四半期に示された脅威を大幅に軽減し、攻撃者や進化する脅威情勢に備えることができます。」

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（2024 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 四半期には、ゼロデイマルウェアの割合が 53%に戻り、過去最低だった第 3 四半期の 20%から大幅に増加しました。これは、マルウェアが暗号化された接続を経由して侵入するケースが増加しており、暗号化されたチャネルでは通常、より巧妙で回避型の脅威を用いるという、本レポートの以前の見解を補強するものです。
- 当四半期のマルウェアの脅威は、ユニーク数で 91%減と大幅に減少しました。これは、単発の標的型攻撃が減少し、一般的なマルウェアが増加したためと考えられます。しかし、脅威が減少したからといって、防御をすり抜けようとする脅威に迅速かつ真摯に対処しなければ、単純な攻撃で終わってしまうというわけではありません。
- ネットワーク攻撃は、前四半期から 27%減少しました。脅威ラボの調査結果によると、今四半期は、多くの試行錯誤を経て成功しているエクスプロイトが上位にランクインしており、攻撃者が自分たちの知っている攻撃手法に固執していることが浮き彫りになっています。
- 上位のフィッシングドメインリストは前四半期と変わらず、持続的でインパクトの強いフィッシングインフラが引き続き使用されていることを浮き彫りにしています。SharePoint を標的としたフィッシングドメインは、正規のログインポータルを模倣して認証情報を取得することが多く、攻撃者が依然としてビジネスメール詐欺（BEC）の手口を悪用し、Office 365 サービスに依存している組織を標的としていることを示唆しています。
- マルウェアをロードするために外部のマルウェアに依存するのではなく、PowerShell、Windows Management Instrumentation（WMI）、Office マクロなどの正規のシステムツールを悪用する環境寄生型攻撃（LotL）がトレンドとなっています。この傾向は、PowerShell インジェクションやスクリプトを活用したエンドポイント攻撃手法の 61%に見られ、エンドポイント攻撃ベクトル全体の約 83%を占めています。この約 83%のうち、97%は PowerShell によるものであり、やはり PowerShell が脅威アクターの攻撃手段の大部分を担っていることがわかります。
- 上位 10 件のネットワーク検知の半数以上が、一般的な Web アプリの欠陥を利用した通常のシグネチャでした。この傾向は、攻撃者が確実なスタイルの攻撃を大量に狙っていることを浮き彫りにしています。

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 4 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-q4-2024（英語版）

*本資料は、本社が発表したプレスリリースの翻訳版です。

【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 X（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。
X： https://twitter.com/WatchGuardJapan
Facebook： https://www.facebook.com/watchguard.jp

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