Press Release
2023 年 5 月 26 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 2022 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：エンドポイントランサムウェアが急増し、ネットワーク検知のマルウェアが減少

暗号化接続によるマルウェアデリバリが増加し、トラフィックを復号化しない組織はよりハイリスクに

2023 年 5 月 26 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（2022 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。主な調査結果として、ネットワーク上で検知されたマルウェアが減少したのに対して、エンドポイントランサムウェアが 627%と急増し、フィッシングキャンペーンに関連したマルウェアが引き続き脅威となっている点が挙げられます。

マルウェアが全体的に減少しているにもかかわらず、HTTPS（TLS/SSL）トラフィックを復号化する Firebox を対象としたウォッチガードの脅威ラボの研究者によるさらなる分析では、マルウェアの発生率が高く、マルウェアの活動が暗号化トラフィックに移行していることを示しています。本レポートでデータを提供している Firebox のうち、暗号化通信を検査しているのはわずか 20%程度であることから、マルウェアの大部分は検知されないままであることが分かります。暗号化されたマルウェアの活動は、最近の脅威ラボのレポートでも繰り返し取り上げられているテーマです。

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。「私たちのデータや調査において、継続的かつ懸念される傾向として、暗号化、あるいはより正確にはネットワーク境界での復号化の欠如が、マルウェア攻撃トレンドの全体像を隠していることが挙げられます。セキュリティの専門家が HTTPS インスペクションを有効にして、これらの脅威が被害を及ぼす前に特定し、対処できるようにすることが重要です。」

以下にウォッチガードのインターネットセキュリティレポート（2022 年第 4 四半期版）における主な調査結果を紹介します：

- **エンドポイントランサムウェアの検知が 627%に上昇：**この急増により、ランサムウェアを未然に防ぐための最新のセキュリティ制御や、優れた災害復旧や事業継続（バックアップ）計画などの必要性が明らかになりました。
- **マルウェアの 93%が暗号化の背後に潜んでいる：**脅威ラボの調査によると、ほとんどのマルウェアは、セキュリティで保護された Web サイトで使用される SSL/TLS 暗号化に隠れていることが引き続き示されています。第 4 四半期もその傾向は続いており、82%から 93%に増加しています。こうしたトラフィックを検査しないセキュリティの専門家は、ほとんどのマルウェアを見逃している可能性が高く、エンドポイントセキュリティにマルウェアの捕捉を任せていることになります。
- **ネットワーク上のマルウェア検知数が、第 4 四半期に前四半期比で約 9.2%減少：**過去 2 四半期に渡ってマルウェアの検知数が全般的に減少しています。しかし、前述の通り、暗号化された Web トラフィックを考慮すると、マルウェ

アは増加しています。脅威ラボチームは、この減少傾向は全体像を示していないかもしれないと考えており、この動向を確認するためには、HTTPS インスペクションを活用したより多くのデータが必要だと考えています。

- **エンドポイントマルウェアの検知数が 22%増加：**ネットワークマルウェアの検知数が減少する一方で、エンドポイントでの検知数は第 4 四半期に増加しました。これは、マルウェアが暗号化されたチャネルにシフトしているという脅威ラボチームの仮説を裏付けるものです。エンドポイントでは、脅威ラボのエンドポイントソフトウェアが確認できるようにブラウザが復号化するため、TLS の暗号化はそれほど重要ではありません。主要な攻撃ベクトルのうち、スクリプトに関連するものが最も多く、全検知数の 90%を占めています。ブラウザマルウェアの検知では、攻撃者は Internet Explorer を最も多く標的とし、検知の 42%を占めており、次いで Firefox が 38%でした。
- **非暗号化トラフィックにおいて、ゼロデイまたは回避型マルウェアが 43%に減少：**マルウェアの検知数全体に占める割合は依然として大きいものの、脅威ラボチームがここ数年で確認した中では最も低い数値です。とはいえ、TLS 接続に注目すると、話は全く変わってきます。**暗号化された接続を利用するマルウェアの 70%がシグネチャを回避しています。**
- **フィッシングキャンペーンが増加：**本レポートのトップ 10 リストに掲載（一部は一般的なリストにも掲載）されたマルウェアのうち、3 種類はさまざまなフィッシングキャンペーンを支援するものです。最も多く検知されたマルウェアファミリーである JS.A gent.UNS は、悪意のある HTML を含み、著名な Web サイトを装った正規のドメインへユーザーを誘導します。別の亜種である Agent.GBPM は、「PDF Salary_Increase」というタイトルの SharePoint フィッシングページを作成し、ユーザーのアカウント情報にアクセスしようとします。トップ 10 の最後の新しい亜種である HTML.Agent.WR は、フランス語で偽の DHL 通知ページを作成し、既知のフィッシングドメインにつながるログインリンクを提供します。フィッシングやビジネスメール詐欺（BEC）は、依然としてトップクラスの攻撃ベクトルの 1 つであるため、適切な予防防御策とセキュリティアウェアネス（意識）のトレーニングプログラムの両方を用意して、防御に努めるべきです。
- **プロキシログインの悪用が引き続き増加：**このよく知られている重要な Exchange の問題に対する悪用は、第 3 四半期の 8 位から前四半期に 4 位へと上昇しました。この問題は、とっくにパッチが適用されているはずですが、そうでない場合、セキュリティの専門家は、攻撃者がこの問題を標的にしていることを知る必要があります。古い脆弱性は、攻撃者が侵害することができれば、新しい脆弱性と同様に有用なものとなり得ます。さらに、多くの攻撃者は、Microsoft Exchange Server や管理システムをターゲットにし続けています。組織は、これらの分野の防御にどのように注力するべきかを認識し、把握しておく必要があります。
- **ネットワーク攻撃量が前四半期比横ばい：**厳密には 35 ヒット増加し、わずか 0.0015%の増加でした。次に小さい変化は、2020 年第 1 四半期から第 2 四半期にかけての 91,885 件ですので、このわずかな変化は注目に値します。
- **LockBit が依然としてランサムウェアグループおよびマルウェアの亜種として流行：**脅威ラボチームは引き続き、LockBit の亜種を頻繁に目にしており、このグループは、ランサムウェアで企業を（その関連会社を通じて）侵害することに最も成功しているようです。前四半期から減少したものの、LockBit は再び最も多くの公的な恐喝被害者を出し、ウォッチガードの脅威ラボが追跡したのは 149 人でした（第 3 四半期は 200 人）。また、第 4 四半期には、脅威ラボチームが新たに 31 のランサムウェアと恐喝グループを検知しました。

四半期ごとに発行されるウォッチガードの調査レポートは、脅威ラボの調査活動をサポートするためのデータ共有に賛同いただいている、ウォッチガードアプライアンスオーナーによる匿名の Firebox データに基づいています。Q4 では、ウォッチガードのアプライアンスは 1,570 万以上のマルウェア（1 デバイス当たり 194 件）、230 万超のネットワーク脅威（1 デバイス当たり 28 件）を防御しています。レポートには、2022 年 Q4 で新たに登場したマルウェアおよびネットワークに関するトレンド、そしてあらゆる企業規模、業種に役立つ推奨されるセキュリティ戦略や防御のための重要なヒントなどが盛り込まれています。

レポート全文は以下よりダウンロードできます。
https://www.watchguard.co.jp/contents/apps/wp-content/uploads/WG_Threat_Report_Q4_2022_JA.pdf
（日本語版）

【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