Press Release
2022 年 4 月 15 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 2021 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：ネットワーク攻撃が過去 3 年間で最多

EMEA におけるネットワーク攻撃検知数が 4 倍に増加し、マルウェアの検知数も他の地域の約 2 倍に

2022 年 4 月 15 日（金）－ 企業向け統合型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（2021 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の脅威に関する詳細を報告しています。注目すべきは、回避型マルウェアの検知数が過去最多となったことが判明しました。また、高度化された脅威は 33%増加し、ゼロデイの脅威がかつてないほど高い水準に達しています。ネットワークの検知数も増加傾向が続いており、北米／中米／南米が大半を占めています。

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。「ハイブリッド勤務への移行が続く中で、攻撃対象領域が拡大しており、組織が塞ぐべき潜在的なセキュリティホールが増えています。ゼロデイの脅威がかつてないハイレベルで推移しており、攻撃対象領域もネットワークゲートウェイを越えて、IoT、ホームネットワーク、モバイルデバイスにまで及んでいるため、企業は拡大が著しい脅威情勢に迅速かつ効率的に適応可能な、真の統合型のセキュリティアプローチを採用する必要があります。組織はハッカーに対抗するために、日常的にシステムのアップデートやパッチの適用といったシンプルながら非常に重要な対策を確実に実施するべきです。」

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（2021 年第 4 四半期版）における主な調査結果を紹介します：

- **ネットワーク攻撃の総検知数が引き続き増加し、ネットワークセキュリティの複雑性が浮き彫りに：**ネットワーク侵入の検知数が増加の一途をたどり、過去 3 年間の四半期で最大の検知数を記録し、前四半期比では 39%増となりました。これは、旧来の脆弱性が引き続き狙われていることと、組織のネットワークが拡大していることが原因だと考えられます。次々に新しいデバイスがオンラインでつながり、古い脆弱性はパッチが当てられないまま残っているため、ネットワークセキュリティがより複雑化しています。
- **EMEA で世界の他の地域よりも高い割合でマルウェアの脅威を検知：** Q4 においてマルウェアの脅威から最も狙われた地域は欧州、中東、アフリカでした。事実、EMEA では、Firebox 1 台あたりのマルウェア検知数（49%）が、世界の他の地域（ 北米／中米／南米：23%、APAC：29%）のほぼ 2 倍以上になっています。
- **暗号化接続で配信されたマルウェアの 78%が回避型：**全体として、検知されたマルウェアの 67%は暗号化接続によって配信されており、これらのマルウェア検知のうち、78%が基本的な検知機能を回避するゼロデイマルウェアの脅威でした。これは、前四半期に見られた傾向をそのまま引き継いでいます。これらの脅威は、ファイアウォールで受信トラフィックを復号化およびスキャンすることで、ゲートウェイで阻止できることが多いのですが、残念ながら多くの組織がこの手順を怠っています。

- **Office を悪用した新たなマルウェアが台頭：**Q4 では、Q3 の調査結果と同様に、Office ドキュメントを標的としたマルウェアのインシデントが目立ちました。今四半期は CVE-2018-0802 が前四半期から 1 つ順位を上げ、マルウェアトップ 10 の 5 位に浮上し、最も普及しているマルウェアリストにも名を連ねています。研究者たちは、このマルウェアはこれまでの CVE-2017-11882 に代わって、Office を悪用した攻撃のトップになったのではないかと推測しています。
- **Emotet が復活：**今期、ウォッチガードが検知したトップマルウェアのドメインリストに、新たに 2 つのマルウェアのドメインが追加されました。これらのドメインの 1 つである Skyprobar[.]info は、他のペイロード向けの C2（C&C）および配信インフラのマルウェアに進化したバンキング型トロイの木馬（バンキングトロジャン）である Emotet にリンクされています。米国の法執行機関による直接的な妨害もあって減少していた Emotet マルウェアは、2021 年第 4 四半期に復活を遂げました。

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 2,390 万件以上のマルウェア（1 デバイス当たり 313 件）、590 万近いネットワーク脅威（1 デバイス当たり 75 件）を防御しています。レポートには、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詳細トレンド、そして Log4Shell の脆弱性、さらに、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.com/wgrd-resource-center/security-report-q4-2021（英語）
*日本語レポートは後日公開予定。

【WatchGuard Technologies について】
WatchGuard（R）Technologies は、ネットワークセキュリティ、エンドポイントセキュリティ、セキュア Wi-Fi、多要素認証、ネットワークインテリジェンスを提供するグローバルリーダーとして、全世界で約 18,000 社の販売パートナーおよびサービスプロバイダを通じて、250,000 社以上の企業に信頼性の高いセキュリティ製品／サービスを提供しています。ウォッチガードのミッションは、中堅・中小企業や分散拠点を持つ大企業がエンタープライズレベルのセキュリティをシンプルに利用できるようにすることです。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。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