Press Release
2022 年 10 月 7 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 2 四半期最新インターネットセキュリティレポート：マルウェア全般が減少するも、暗号化されたマルウェアは急増、Office の脆弱性を積極的に悪用

SCADA システムが標的となり、Emotet の復活も継続

2022 年 10 月 7 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 2 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。データから判明した主な内容は、マルウェア全体の検知数が 2021 年上半期のピーク時から減少していること、Chrome や Microsoft Office に対する脅威が増加していること、そして Emotet ボットネットの復活が続いてい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。「第 2 四半期のマルウェア攻撃は、過去最高を記録した第 1 四半期から減少しましたが、検知されたマルウェアの 81%以上が TLS 暗号化接続を介しており、引き続き懸念すべき増加傾向を示しています。これは、脅威者がより捕捉しにくいマルウェアに依存するように戦術を変化させていることを反映している可能性があります。」

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 2 四半期版）における主な調査結果を紹介します：

- **Office エクスプロイトは、他のどのマルウェアのカテゴリーよりも引き続き拡散：**実際、今四半期のトップインシデントは、Follina Office エクスプロイト（CVE-2022-30190）で、4 月に初めて報告され、5 月下旬までパッチが適用されませんでした。Follina は、不正なドキュメントを介して配信され、Windows Protected View と Windows Defender を回避することができ、国家を含む攻撃者によって積極的に悪用されています。他の 3 つの Office エクスプロイト（CVE-2018-0802、RTF-ObfsObjDat.Gen、CVE-2017-11882）は、ドイツとギリシャで広く検知されました。
- **エンドポイントにおけるマルウェアの検知数は全体的に減少するも、一部は増加：**エンドポイントにおけるマルウェアの検知総数は 20%減少しましたが、ブラウザを悪用するマルウェアは全体で 23%増加し、中でも Chrome は 50%の急増を記録しました。Chrome での検知数が増加した理由の 1 つとして、さまざまなゼロデイエクスプロイトが根強く残っていることが考えられます。第 2 四半期も、エンドポイントにおける検知数の大部分（87%）をスクリプトが占めています。
- **トップ 10 のシグネチャがネットワーク攻撃検知数の 75%以上を独占：**今期は、新しいシグネチャ（WEB Directory Traversal -7 と WEB Directory Traversal -8）を含め、産業機器やプロセスを制御する ICS およ

び SCADA システムを標的とするものが増加しました。この 2 つのシグネチャは非常によく似ており、前者は 2012 年に特定の SCADA インターフェイスソフトウェアで初めて発見された脆弱性を悪用し、後者はドイツで最も広く検知されています。

- **復活した Emotet が大きくクローズアップ：**前四半期から Emotet の感染数は減少していますが、Emotet は依然としてネットワークセキュリティの最大の脅威の 1 つとなっています。この四半期に検知されたマルウェアのトップ 10 および暗号化されたマルウェアのトップ 5 の 1 つである XLM.Trojan.abracadabra（Emotet ボットネットを拡散する Win Code インジェクタ）は、日本国内で広く確認されました。

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。Q2 では、ウォッチガードのアプライアンスは 1,810 万以上のマルウェア（1 デバイス当たり 234 件）、420 万超のネットワーク脅威（1 デバイス当たり 55 件）を防御しています。レポートには、2022 年 Q2 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.com/wgrd-resource-center/security-report-q2-2022（英語版）
*日本語版のレポートは後日公開予定。

【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

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