Press Release
2020 年 12 月 23 日（水）
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、COVID-19 が セキュリティ脅威情勢に与えた影響の詳細レポートを発表

2020 年第 3 四半期インターネットセキュリティレポート：COVID-19 関連の脅威トレンド、ネットワーク攻撃の増加、米国の SCADA システムを標的としたマルウェアなど

2020 年 12 月 23 日（水）－ 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/エンドポイントプロテクション）のグローバルリーダである 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（2020 年第 3 四半期）を発表しました。主な調査結果として、COVID-19 がセキュリティ脅威情勢に与えた影響を報告しており、攻撃者は引き続きリモートワークへのシフトが進行しているにもかかわらず、企業ネットワークを標的とし、パンデミック関連の不正ドメインやフィッシングキャンペーンが増加していることが判明しました。

ウォッチガードの CTO、Corey Nachreiner（コリー・ナクライナー）は次のように述べています。「COVID-19 のインパクトが拡大しており、私たちの脅威インテリジェンス（情報）では、攻撃者がどのように戦術を変えてきているかについての重要な知見を提供しています。セキュリティに関しては「ニューノーマル（新常態）」などなく、企業にとって 2021 年およびそれ以降もエンドポイントとネットワークの保護対策を強化することが最優先事項であることは間違いありません。また、情報セキュリティに対する多層防御も重要であり、回避型および暗号化された攻撃や、高度なフィッシングキャンペーンなどによる被害を軽減するようなサービスが必要になります。」

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には、進化し続ける脅威情勢の中で台頭し、影響を及ぼしている最新のマルウェアとネットワーク攻撃のトレンドに関して、企業、パートナー、顧客が身を守るために役立つデータ、専門分析、そして実用的な知見が盛り込まれています。以下に 2020 年 Q3 の主な調査結果を紹介します：

- **ネットワーク攻撃数とユニークシグニチャの検知数が 2 年ぶりに最大に** - ネットワーク攻撃が Q3 に 330 万件を超え、前期と比較して 90%増を記録し、2 年ぶりに最大となりました。また、ネットワーク攻撃のユニークシグニチャ数も引き続き上昇傾向にあり、同様に 2 年ぶりに最大数に達しています。これらの調査結果は、企業におけるリモートワークの増加にかかわらず、ネットワークベースのアセットやサービスの保護を維持・強化することを優先しなければならないことを示唆しています。
- **COVID-19 詐欺が増加** – Q3 では、正規のパンデミックサポートを目的とした Web サイトで COVID-19 アドウェアキャンペーンが実行され、ウォッチガードの感染 Web サイトトップ 10 リストに入りました。また、ウォッチガードは、Microsoft SharePoint を活用して、国連を装った本物まがいのログインページをホスティングしたフィッシング攻撃を検

知し、メールには、COVID-19 による国連からの中小企業救済に関する偽メッセージが含まれていました。これらの調査結果は、今後も攻撃者がグローバル規模での健康の危機を取り巻く恐怖、不確実性、猜疑心を悪用し、ユーザを誘惑して騙していくことを物語っています。

- **企業が多くのフィッシング攻撃を受け、不正リンクをクリック** – Q3 ではウォッチガードの DNSWatch サービスが累計 2,764,736 の不正ドメイン接続を防御し、一組織に換算すると 499 の接続をブロックしたことになります。さらに細かく見てみると、各組織は 262 のマルウェアドメイン、71 の感染 Web サイト、そして 52 のフィッシングキャンペーンの被害に遭っていた可能性があります。前述した巧妙な COVID-19 詐欺の増加と合わせると、このような調査結果は DNS フィルタリングサービスや、ユーザのセキュリティアウェアネストレーニングの導入が重要であることを示しています。
- **攻撃者が米国の脆弱な SCADA システムを標的に** – ウォッチガードの、Q3 で最も波及したネットワーク攻撃リストに新たに加わったのは、よく知られた SCADA（監視制御とデータ取得）制御システムにおける、以前パッチが適用された認証バイパスの脆弱性を攻撃するものです。この手の脆弱性はリモートコードの実行不具合ほど深刻ではありませんが、それでも攻撃者がサーバ上で稼働している SCADA ソフトウェアを制御できる可能性があります。Q3 では攻撃者がこうした脅威を用いて米国のネットワークの約半数を標的にし、来年は産業制御システムが攻撃者の恰好の標的となるかもしれないことを示唆しています。
- **最も蔓延したマルウェア亜種として LokiBot に似たものが登場** – LokiBot に酷似するパスワードスティーラー Farelt が、ウォッチガードの Q3 で最も波及したマルウェア検知リストのトップ 5 にランクインしました。Farelt ボットネットが、LokiBot と同じコマンド&コントロールの仕組みを使用しているかどうかは定かではありませんが、同一グループ SilverTerrier がこの 2 つのマルウェア亜種を作成した可能性が高いと言えます。このボットネットは多くのステップを踏んでアンチウイルス制御をバイパスし、ユーザにマルウェアをインストールさせようと試みます。ウォッチガードはこの脅威を研究する中で、データが示す以上に多くのユーザがこのマルウェアの標的にされた強力な証拠を発見しました。
- **Emotet が存続** – バンキング型トロイの木馬と既知のパスワードスティーラーとして知られる Emotet が、Q3 で初めてウォッチガードのマルウェアリストのトップ 10 に入り、ドメイン配信マルウェアのトップ 10 にも入りそうな勢いを示しました。わずかな接続数の差で 11 位でしたが、これは特筆すべきことであり、ウォッチガード脅威ラボやその他の研究チームが、Emotet の感染において、ネットワークの速度が落ちる兆しもなく、Trickbot や Ryuk ランサムウェアのようなペイロード（悪意のあるコード）も追加でダウンロードさせられているのを確認しています。

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の調査結果は、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、稼働中のウォッチガー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。Q3 では、世界中で 48,000 台近くのウォッチガードアプライアンスがインターネットセキュリティレポートのデータに貢献しています（過去最大数）。今期これらのアプライアンスは 2,150 万件以上のマルウェア（1 デバイス当たり 450 件）、330 万件以上のネットワーク脅威（1 デバイスあたり約 70 件の検知）をブロックしています。また、Firebox アプライアンスで 438 件のユニークな攻撃シグネチャを検知・ブロックしており、Q2 と比較して 6.8%増加し、2018 年 Q4 以降最大となっています。

本レポートの全編では、今日の大企業や中小／中堅企業が最新のセキュリティ脅威から身を守るために役立つきめ細かい調査結果や、防御のための重大なベストプラクティスが掲載されています。また、2020 年 7 月に、ビットコイン詐欺を推進するために 130 の著名人のアカウントを攻撃した歴史的な Twitter ハッキングについての詳細分析も含まれています。

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-q3-2020（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、セキュア Wi-Fi、多要素認証、高度なエンドポイントプロテクション、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として、全世界で約 10,000 社の販売パートナーとサービスプロバイダより 80,000 社以上の企業にエンタープライズクラスのセキュリティ製品と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・中小企業や分散型企業を含むすべての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、数多くの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への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