ウォッチガード、最新のインターネットセキュリティレポートで、Equifax社に対する脆弱性攻撃と類似した手法の攻撃が増加していると報告

マルウェア/ネットワーク攻撃が大幅に増加し、そのうちゼロデイマルウェアが半数を占める

2019年12月23日（月）

ー企業向け統合型セキュリティプラットフォーム（ネットワークセキュリティ／セキュアWi-Fi／多要素認証）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（2019年第3四半期）を発表しました。マルウェアとネットワーク攻撃が前期同様に増加傾向にある中、同社の2019年第3四半期におけるネットワーク攻撃トップ10リストに、Equifax社の大規模な情報漏えいを含む複数のApache Strutsの脆弱性が初めて登場しています。レポートではまた、Microsoft Officeのエクスプロイトや正規のペネトレーションテストツールなどを用いたゼロデイマルウェアが多数検知されたことに着目しています。

ウォッチガードのCTO、Corey Nachreiner（コリー・ナクライナー）は以下のように説明しています。「私たちの最新の脅威インテリジェンスの分析により、サイバー犯罪者の攻撃手法がさらに多様化・洗練化されていることが判明しています。犯罪者は悪名高い手法のみならず、回避型のマルウェアキャンペーンや我々が日常的に使用している製品、ツール、ドメインの乗っ取りも実行しています。攻撃者は戦術を常に変えており、組織は規模を問わずコアネットワークからユーザのエンドポイントまで、多層防御型のセキュリティサービスを用いて自社、顧客、そしてパートナーを保護する必要があります。」

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、企業が今日のセキュリティ情勢を把握し、進化する脅威に目を配り、身を守るために役立つデータ、トレンド、調査結果、そして防御手段に対するアドバイスが盛り込まれています。以下に2019年第3四半期の主な調査結果を紹介します：

Equifax社の情報漏えいで使用された、主要な脆弱性を標的とした新たなネットワーク攻撃が登場 - ウォッチガードの最も著名なネットワーク攻撃リストに登場した「Apache Struts 2リモートコード実行」では、攻撃者がPythonをインストールするかもしくはカスタムHTTPリクエストにより、僅か数行のコードで脆弱性をエクスプロイトし、無防備なシステムに対するシェルアクセスを可能にしています。この脅威は、Apache Strutsにおける別の2つの脆弱性とともに第3四半期のネットワーク攻撃トップ10リストに入っており、ネットワーク攻撃の総数を8%押し上げています。Equifax社の大規模情報漏えいでは、この

ような重大な脆弱性が露わになり、Web管理者が既知の不具合に即時にパッチをあてることがいかに重要であるかを示しています。
　Microsoft Officeのエクスプロイトが引き続き標的に - Microsoft Office製品に影響を及ぼす2種類のマルウェア亜種がその数において第3四半期のウォッチガードのマルウェアトップ10リスト、並びに最も拡散したマルウェアトップ10リストに名を連ねています。このことは、Officeを標的とした攻撃の活用頻度と、標的対象数の両面において被害が及んでいることを示しています。2種類のマルウェアはともにメールでの配信を起点としており、組織にとって、フィッシング攻撃や不正な添付ファイルを用いたその他の攻撃を特定するためのユーザに対するトレーニングと教育の重要性が増していると言えます。
　ゼロデイマルウェアのインスタンスが50%増加し、マルウェア全般の検知数が増加 - 過去の四半期におけるマルウェア検知数は約38%でしばらく推移していましたが、今回ゼロデイマルウェアの第3四半期における総検知数は半数を占めるまでに至りました。検知されたマルウェアの総数は2019年第2四半期と比較すると4%増加し、2018年第3四半期と比べると60%も増えています。第3四半期におけるマルウェア攻撃の半分は、従来のシグニチャベースソリューションをバイパスしており、進化する高度な脅威を防御できる多層防御型のセキュリティサービスが必要であることを示唆しています。
　サーバー犯罪者が攻撃に正規のペネトレーションテストツールを活用　Kali Linuxペネトレーションテストツールに関わる2種類の新たなマルウェア亜種がウォッチガードの第3四半期のマルウェア数トップ10リストに加わりました。1つはPowerShellのトロイの木馬Boxterであり、不正プログラムをユーザが意図せずにデバイスにダウンロード/インストールさせます。もう1つはHacktool.JQで、Mimikatz（検知数が第2四半期と比較して48%、2018年第3四半期と比較して16%低下）以外の認証攻撃ツールとしてリストにランクインしています。これらの検知数の増加は、正規のペネトレーションテストの実施によるものなのか、あるいは悪意のある攻撃者が直ちに利用できるオープンソースツールを活用した結果であるかは定かではありません。組織は引き続きアンチマルウェアサービスによりデータ詐取を防ぐ必要があります。
　アメリカ大陸を標的としたマルウェア攻撃が大幅に増加 2019年第3四半期におけるマルウェア攻撃の総数の42%以上が北米、中米、南米に集中しており、第2四半期の27%と比較して大幅に増加しています。このことは、攻撃者が前期と比べて標的対象地域を大幅に変更したことを示しています。EMEAとAPAC（第2四半期のマルウェアの標的対象地域でトップ）の第3四半期におけるマルウェア攻撃の総数はそれぞれ30%と28%でした。明確な同期は不明ですが、こうした傾向は攻撃者がアメリカ大陸のユーザを特に意識して新たなマルウェアキャンペーンを展開し始めたことを示しています。

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ドUTM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。今日、世界中の約37,000台の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。今期これらのアプライアンスは23,000,000件以上のマルウェア亜種を防御し（1デバイス当たり623件）、また2,400,000件近くのネットワーク攻撃を防御しています（1デバイス当たり65件）。

本レポートの全編では、2019年第3四半期で最も影響のあったマルウェアやネットワーク攻撃の傾向、およびDNSWatchで収集されたマルウェア、感染Webサイト、フィッシングリンクに関係する不正ドメインの四半期トップリスト、さらにカザフスタンのHTTPS解読キャンペーンに関する分析、並びに今日の脅威情勢下であらゆる規模の組織の安全を守る上で役立つ主要なベストプラクティスが掲載されています。

カザフスタンの国家規模のHTTPS解読キャンペーンに関する分析
本レポートには、カザフスタンが第3四半期で国内の全てのHTTPSトラフィックの傍受・解読を開

始したことに関する詳細を掲載しています。また、HTTPSの暗号化と復号化、その他の国で開始されている類似したプログラム、エンタープライズネットワークセキュリティにおけるHTTPSの暗号化の役割、そして全ての組織がこうした例を元に活用できるベストプラクティスについて、ウォッチガードの脅威ラボが解説しています。

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-q3-2019
（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、そしてネットワークインテリジェント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

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

Generated by ぷれりりプレスリリース
https://www.prerele.com