ウォッチガード、最新のセキュリティレポートでMacマルウェア、不正なOfficeドキュメント、Webアプリケーションエクスプロイトの増加を報告

2019年第1四半期のインターネットセキュリティレポートでセキュリティの多層防御の必要性の高まりを示唆

2019年6月27日（木）
ー企業向け統合型セキュリティプラットフォーム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1四半期）を発表しました。2018年第4四半期と比較してマルウェアの総検知数は62%の大幅増を示しており、レポートでは、サイバー犯罪者が不正なMicrosoft Officeドキュメント、Macマルウェア、Webアプリケーションエクスプロイトを含む、広範囲に及ぶ多彩な攻撃テクニックを駆使していると報告しています。こうした結果は、2019年に入ってハッカーが偽のOfficeドキュメントや他の攻撃手段を活用することにより、ID情報の窃取やランサムウェアといった広く知られている戦術をさらに強化していることを裏付けており、広範かつ多様な脅威ベクターに備えるべく、組織は高度な防御体制を敷くことが求められます。

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。「最新レポートの主な調査結果は、今日の複雑化した脅威の情勢における、セキュリティの多層防御の重要性を浮き彫りにしました。DNSレベルのフィルタリングによる不正なWebサイトへの接続やフィッシング攻撃の防御、不正侵入検知・防御によるWebアプリケーション攻撃の回避、あるいは多要素認証による窃取されたIDを用いた攻撃の防止など、各種の対策がありますが、昨今のサイバー犯罪者は多様な攻撃メソッドを活用していることは明らかであり、組織は包括的なセキュリティサービスを提供する統合型のセキュリティプラットフォームで身を守ることが最善の策であると言えます。」

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、セキュリティに関する知見、調査、ベストプラクティスが含まれており、組織がオンライン上の犯罪者から身を守り、データを保護する上で役立つ情報が盛り込まれています。以下に2019年第1四半期の主な調査結果をご紹介します：

攻撃者が引き続き不正なOfficeドキュメントを利用：2019年第1四半期では、Fireboxの17%以上が不正なOfficeドキュメントを防御し、このカテゴリにおいて最も拡散したマルウェアリストに2つの脅威がランクインしており、1つがトップ10マルウェア攻撃のリストに入っています。これらの不正なドキュメントの半数はEMEAで防御されており、東ヨーロッパの国々で顕著な傾向が見られました。ユーザは、不審なOfficeドキュメントの開封を避け、マクロを有効化しようとする添付

ファイルの脅威に留意するべきです。

Mac
OSマルウェアが増加：Macマルウェアは、2018年第3四半期のウォッチガードのトップ10マルウェアリストに初めて登場し、現在2種類の亜種が流行しており、それらは2019年第1四半期のリストにランクインしています。こうしたMacベースのマルウェアの増加は、Macはウイルスやマルウェアとは無縁であるといった神話が崩れ、全てのデバイスやシステムに対する高度な脅威保護の仕組みを導入することの重要性が高まっています。

WebアプリケーションがSOARをエクスプロイト：第1四半期ではネットワーク攻撃の総数は減少しましたが、Webアプリケーション攻撃は急激に増加しました。ウォッチガードのIPSサービスは、ID窃取の一般的な手法である多くのクロスサイトスクリプティング（XSS）やSQLインジェクション（SQLi）の脆弱性をエクスプロイトする攻撃者を防御しました。今回2つのSQLi攻撃がウォッチガードのトップ10ネットワーク攻撃リストに登場し、Web
XSS攻撃の1つがネットワーク攻撃のトップ10リスト全体の10%以上を占めました。

DNSフィルタリングが500万以上の不正サイトを防御：ウォッチガードのDNSWatchサービスでは、5,192,883件に及ぶ不正なディスティネーションへのアクセスの試みを阻止し、また既知のマルウェアをホスティングするドメインへの接続で50万件以上、感染したWebサイトへの接続数187,101件、そして既知のフィッシングサイトへの接続数61,096件を防御しました。感染したWebサイトの特定と防御は困難な場合があるため、DNSレベルのフィルタリングは、ユーザが意図せずにマルウェア感染、ID窃取、あるいはボットネットのC&Cシステムの被害に遭わないためには非常に重要となります。

ファイルレスマルウェアが台頭：今期は、ファイルレスの脅威がウォッチガードのトップ10マルウェアおよびトップ10ネットワーク攻撃リストに登場しました。マルウェアサイドでは、PowerShellベースのコードインジェクション攻撃が第1四半期に初めてトップ10リストに入り、著名なファイルレスのバックドアツールとして知られるMeterpreterもネットワーク攻撃のトップ10リストに登場しています。この2つの傾向は、サイバー犯罪者が回避型の脅威カテゴリの利用に引き続き着目していることを示唆しています。

Mimikatzマルウェアが73%急増し、脅威ランキングのNo.1を維持：この著名なオープンソースツールは第1四半期で発見された全てのマルウェアの20.6%を占め、一般的にパスワード窃取に利用され、多くのネットワーク侵入の裏で暗躍しています。Mimikatzはウォッチガードのトップ10マルウェアリストの常連であり、個々のアカウントで個別に長く複雑な文字列のパスワードを設定することの重要性が浮き彫りにされました。さらに、サイバー犯罪者は継続的してID窃取にフォーカスしているため、組織は規模を問わず多要素認証ソリューションを採用し、正規のユーザアカウントへの攻撃を阻止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42,372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23,884,979件以上のマルウェア亜種を防御し（1デバイス当たり564件）、また989,759件の

ネットワーク攻撃を防御しています（1デバイス当たり22件）。

本レポートの全編では、2019年第1四半期で最も影響のあったマルウェアや攻撃の傾向を明らかにし、110万ドル（約1億1,770万円）に及ぶ損失をもたらした仮想通貨Ethereum Classic（ETC）に対する過去に類を見ない「51%攻撃」に関する詳細分析を行っており、読者や組織が安全を守る上で役立つサイバーセキュリティのアドバイスも掲載されています。

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-q1-2019
（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：角田
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