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、回避型マルウェアが急増していると報告

macOSアドウェアと2017
Excelエクスプロイトの蔓延、並びに新型コロナウイルス関連のフィッシング攻撃で使用されたキーロガーマルウェア分析を報告

2020年4月13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4四半期）を発表しました。2019年第4四半期では回避型マルウェアの急増が見られ、ウォッチガードのFireboxセキュリティアプライアンスで検知されたマルウェアの3分の2が、シグニチャベースのアンチウイルスソリューションをかいくぐっていたことが判明しました。今では、難読化されたマルウェアや回避型マルウェアは例外ではなく一般的になっており、組織は規模を問わず、こうした攻撃を検知・防御できる高度なアンチマルウェアソリューションの導入が急務となっています。

さらに、ウォッチガードは2017年に発見されたMicrosoft Excelの脆弱性をエクスプロイトする広範なフィッシングキャンペーンも検知しています。「dropper（ドロッパー）」と呼ばれるマルウェアは、他の数種類のタイプのマルウェアをユーザのシステムにダウンロードします。Agent Teslaと呼ばれるキーロガーも含まれており、2020年2月の新型コロナウイルス勃発の恐怖につけこんだフィッシング攻撃でも使用されています。

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。「第4四半期の調査結果から、攻撃者は常に攻撃手法を進化させていることが分かりました。検知されたマルウェアの3分の2が旧来のシグニチャベースの防御をすり抜けており、またMacアドウェアのような新種の攻撃も増加しているため、規模の大小を問わず企業は多層防御のセキュリティに投資するべき段階に入っていると言えます。特に高度なAIや振舞いベースのアンチマルウェアテクノロジ、およびDNSフィルタリングなどの堅牢なフィッシング防御機能などが重要となっています。」

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には、企業、サービスプロバイダ、エンドユーザが今日のセキュリティ脅威から身を守るために役立つデータ、トレンド、調査結果、そしてベストプラクティスが盛り込まれています。以下に2019年第4四半期の主な調査結果を紹介します：

2019年第4四半期で検知されたマルウェアの68%が回避型マルウェア
これは2019年の年間平均値である35%から比べると劇的に増加しています。ウォッチガードのUTM

アプライアンスでは3つのアンチマルウェアサービスを提供しています。1つ目がシグニチャベースのアンチウイルス、2つ目がIntelligentAVと呼ばれる機械学習検知エンジン、そして3つ目がAPT
Blockerと呼ばれる振舞いベースのソリューションです。例えマルウェアがシグニチャベースのAVを回避しても、残り2つのソリューションのいずれかにより検知することができます。
　Microsoft Excelエクスプロイトが依然として頻繁に使用されている －
2017年に見つかった脆弱性を悪用したエクスプロイトは、ウォッチガードのトップ10マルウェアリストの第7位を占めており、特に英国、ドイツ、ニュージーランドで多く確認されました。フィッシング攻撃によりマクロをエクスプロイトし、Agent
Teslaなどのキーロガーや、Razyのようなトロイの木馬を含む、他のタイプのマルウェアをダウンロードし、インストールします。
　新型コロナウイルスフィッシング攻撃で用いられたAgent Teslaキーロガーの分析
ウォッチガードのレポートには、2020年2月
の新型コロナウイルスに対する恐怖を巧みに操ったフィッシング攻撃で使用された、Agent Teslaキーロガーに関する分析も掲載されています。Agent Teslaは、先に述べたMicrosoft Excelの脆弱性を利用したドロッパーマルウェア経由で配信されたマルウェアの１つです。
　Macアドウェアが2019年第4四半期で急増
ウォッチガードが2019年第4四半期で検知した上位にランキングされている感染Webサイトで悪用されており、Bundloreと呼ばれるmacOSアドウェアがAdobe
Flashアップデートに成りすましています。この傾向は、2020年2月
に出されたMalwareBytesレポートにおいてMacマルウェア、特にアドウェアが増加しているとの報告と一致しています。
　SQLインジェクション攻撃が2019年におけるネットワーク攻撃のトップに －
SQLインジェクション攻撃が2018年と2019年の間で8000%も上昇しており、2019年で最も多発したネットワーク攻撃となり、被害額も甚大になっています。
　マルウェアの自動配信を利用するハッカーが増加
多くの同様の攻撃が一国の全てのFireboxの70-
80%で検知されていることから、攻撃者は攻撃の自動化を進めていることが推測されます。

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40,000台以上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34,500,000件以上のマルウェアを防御し（1デバイス当たり859.5件）、また約1,879,000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47件）。

本レポートの全編では、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防御における主要なベストプラクティス、並びに2019年10月
に発生したMacyの支払いカードデータの侵害で使用された、MageCart
JavaScriptマルウェアに関する詳細分析が掲載されています。

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-q4-2019
（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

【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
