Press Release
2021 年 7 月 12 日（月）
ウォッチガード・テクノロジー・ジャパン株式会社

ウォッチガード最新レポート：脅威の約 75%が 従来のアンチマルウェアソリューションを回避

2021 年第 1 四半期インターネットセキュリティレポート： ゼロデイマルウェアの数が過去最高を記録、ネットワーク攻撃が増加、今期の主なマルウェア攻撃など

2021 年 7 月 12 日（月）– 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（2021 年第 1 四半期）を発表しました。特筆すべきは、Q1 に検知された脅威の 74%はゼロデイマルウェアであり、従来のシグニチャベースのアンチウイルスソリューションを回避し、検知を逃れています。またレポートでは、ネットワーク攻撃率の上昇に関する新たな脅威情報や、攻撃者が旧来のエクスプロイトを偽装して再利用しようとする方法、および Q1 に発生した上位のマルウェア攻撃なども取り上げています。

ウォッチガードの CTO（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。「Q1 では過去最高レベルのゼロデイマルウェアが検知されました。回避型マルウェアの数が従来の脅威を実質的に超えており、組織は増加する巧妙な脅威の先を行くために、防御体制をさらに充実させていく必要があると言えます。これまでのアンチマルウェアソリューションだけでは、今日の脅威情勢に対抗するには不十分です。全ての組織には、多層型でプロアクティブなセキュリティ戦略が求められており、機械学習や振舞い分析などにより、新たな複合型の脅威を検知し、防御していく必要があります。」

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（2021 年第 1 四半期版）における主な調査結果を紹介します：

- **ファイルレスマルウェアの亜種が爆発的に増加 -** XML.JSLoader は不正なペイロードであり、ボリュームと拡散度合いの両方において、初めてウォッチガードのマルウェア検知トップリストに登場しました。また、HTTPS インスペクションにより Q1 で最も検知された亜種でもあります。ウォッチガードが特定したサンプルは、XML 外部エンティティ（XXE）攻撃によってシェルを開き、ローカルの PowerShell の実行ポリシーを回避してコマンドを実行し、実際のユーザや被害者から隠れて非インタラクティブな方法で実行されます。このことは、ファイルレスマルウェアが普及し、高度なエンドポイント検知／レスポンス機能が必要になってきていることを示す一つの例になります。
- **正規の PDF ファイルを装ったランサムウェア攻撃 -** ランサムウェアローダーZmutzy は、Q1 における暗号化されたマルウェア亜種のボリュームでトップ 2 に浮上しました。Nibiru ランサムウェアに関連するこの脅威は、メールに添付された ZIP ファイルや、悪意のある Web サイトからのダウンロードにより被害を受けます。ZIP ファイルを実行すると、実行ファイルがダウンロードされますが、被害者には正規の PDF に見えます。攻撃者は、ファイル名にピリオドの代わりにカンマを使用し、アイコンを調整して、悪意のある ZIP ファイルを PDF に見せかけます。この種の攻撃は、フィッシングに関する教育やトレーニングの重要性を浮き彫りにするとともに、このような亜種によってランサムウェアに感染した場合に備えて、バックアップソリューションを導入することの大切さを示唆しています。

- **引き続き IoT デバイスを攻撃 -** ウォッチガードの Q1 マルウェアリストのトップ 10 には入りませんでしたが、Linux.Ngioweb.B の亜種は、最近 IoT デバイスを標的として攻撃者に利用されています。このサンプルの最初のバージョンは、WordPress が稼働している Linux サーバを標的としており、初期攻撃には EFL（Extended Format Language）ファイルが利用されています。このマルウェアの別バージョンでは、IoT デバイスをコマンド＆コントロールサーバとやり取りするボットネットに変えてしまいます。
- **ネットワーク攻撃が 20%以上増加 -** ウォッチガードのアプライアンスが 400 万以上のネットワーク攻撃を検知し、前期と比較して 21%増加し、2018 年以来最も多い件数を記録しました。企業のサーバやオフィスに置かれているアセットは、リモートやハイブリッド勤務への移行が進んでいるにもかかわらず、いまだに攻撃者にとって格好の標的であるため、組織はユーザの保護とともに境界セキュリティを維持しなければなりません。
- **旧来のディレクトリトラバーサル攻撃の手法が復活 -** ウォッチガードは Q1 に新たな脅威シグニチャを検知しました。この脅威には、キャビネット（CAB）ファイル経由のディレクトリトラバーサル攻撃が含まれており、Microsoft が設計したアーカイブフォーマットで、可逆的なデータ圧縮と電子証明書の組込みを目的としています。ウォッチガードのネットワーク攻撃トップ 10 リストに新たに登場し、このエクスプロイトは、従来の手法を用いて不正な CAB ファイルをユーザに開かせたり、ネットワーク接続されたプリンターに成りすまし、感染した CAB ファイル経由でプリンタードライバーをインストールさせるたりする方法をとっています。
- **HAFNIUM のゼロデイ攻撃により、脅威への戦術とレスポンスのベストプラクティスの重要性が増大 -** Q1 に Microsoft は、HAFNIUM が各種の Exchange Server における 4 つの脆弱性を使用したと報告しています。攻撃は、ほとんどのメールサーバのようにインターネットに公開されているパッチが適用されていないサーバに対して、認証されていないシステムのリモートコードの実行および任意のファイルの書込みアクセスを行います。ウォッチガードは脆弱性を分析し、HTTPS インスペクション、タイムリーなパッチ適用、そしてレガシーシステムのリプレースの重要性を指摘しています。
- **攻撃者がクリプトマイニングキャンペーンで正規のドメインを利用 -** ウォッチガードの DNSWatch サービスが Q1 に、クリプトマイニングの脅威に関連した数種類の不正な感染ドメインをブロックしました。クリプトマイナーマルウェアは、最近の暗号通貨市場の価格高騰や、無防備な被害者からリソースを簡単に吸い上げられることから、ますます増加しています。

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。今期、ウォッチガードのアプライアンスは 1,720 万件以上のマルウェア（1 デバイス当たり 461 件）、420 万件近いネットワーク脅威（1 デバイスあたり 113 件の検知）をブロックしています。レポートには、2021 年 Q1 に登場した新たなマルウェアやネットワークトレンド、HAFNIUM による Microsoft Exchange Server のエクスプロイト、そして読者向けの防御に対する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-q1-2021（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