ウォッチガード2021年第2四半期最新レポート：マルウェアの91.5%が暗号化通信を利用

ファイルレスマルウェア、ネットワーク／ランサムウェア攻撃が大幅に増加

2021年10月8日（金） ー
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/エンドポイント保護）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2四半期）を発表しました。本レポートでは、ウォッチガードの脅威ラボの研究者によって調査された、マルウェアのトップトレンドやネットワークセキュリティの脅威に関する詳細を報告しています。また、レポートには、2021年の上半期で検知されたエンドポイントの脅威インテリジェンスに基づく新たな知見も含まれています。今回の主な調査結果として、マルウェアの91.5%がHTTPSによる暗号化接続によるものであり、ファイルレスマルウェア脅威の急増、ランサムウェアの劇的増加、そしてネットワーク攻撃の拡大などが挙げられます。

ウォッチガードのCSO（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。「モバイルあるいはハイブリッドでの勤務形態が大半を占めるようになりましたが、従来のネットワークゲートウェイはサイバーセキュリティにおける防御に必ずしも十分に役立つとは限りません。今でも強力なゲートウェイ保護は多層防御型セキュリティの重要な部分を占めていますが、強力なエンドポイント保護（EPP）やエンドポイント検知／レスポンス（EDR）の必要性も増しています。」

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2四半期版）における主な調査結果を紹介します：

　暗号化接続によるマルウェアが急増 －
Q2では、マルウェアの91.5%が暗号化接続経由のものであり、前期比で劇的な増加傾向が見られました。言い換えると、ゲートウェイで暗号化HTTPSトラフィックを調査していない組織は、全マルウェアの90%を見逃しているということになります。
　マルウェアがPowerShellツールを使用して堅牢な保護機能を迂回 －
AMSI.Disable.AがQ1にウォッチガードのトップマルウェアリストに登場しましたが、今期急激に増加し、その数で第二位に、そして暗号化された脅威では一位に躍り出ました。このマルウェアファミリはPowerShellツールを使用してWindowsの各種の脆弱性を悪用します。特筆すべきはその回避技術です。ウォッチガードでは、AMSI.Disable.がPowerShellのAMSI（アンチマルウェアスキャンインターフェース）を無効にするコードを生成し、検知を逃れたマルウェアペイロードでスクリプトセキュリティチェックを迂回することを突き止めました。
ファイルレスマルウェアが増加し、さらに回避能力が向上 －

昨年、スクリプトによる攻撃数全体が前年度比で大幅に増加しましたが、2021年ではわずか半年で、PowerShellなどのスクリプトエンジン由来のマルウェアの検知数が昨年の80%に到達しています。現時点で2021年に検知されたファイルレスマルウェアは昨年比で倍増しています。

リモート勤務へのシフトが増えたにもかかわらずネットワーク攻撃が増加 –
ウォッチガードのアプライアンスがネットワーク攻撃の大幅増を検知し、前期比で22%増え、2018年以来最大数を記録し、Q1では410万件近いネットワーク攻撃が観測されました。今期はさらに100万件増え、ゲートウェイセキュリティの維持と、ユーザにフォーカスした保護を両立させることの重要性が高まっています。

ランサムウェア攻撃が再燃 –
エンドポイントにおけるランサムウェアの総検知数は、2018年から2020年にかけて減少傾向にありましたが、2021年前半にその傾向が崩れ、半年間の総検知数は2020年の通年の検知数にわずかに及ばない結果となりました。2021年の残りの期間、1日のランサムウェア検知数が横ばいであれば、今年のボリュームは2020年と比較して150%以上の増加に達することになります。

大規模なランサムウェア攻撃が「ショットガンブラスト」型の攻撃を凌駕 –2021年5月7日に発生したColonial
Pipelineへの攻撃は、ランサムウェアが脅威として今後も存在することをはっきりと見せつけました。今期のトップセキュリティインシデントとして、この攻撃はサイバー犯罪者が病院、工場の制御システム、インフラなど最も重要なサービスに照準を合わせているだけでなく、こうした影響力の強い標的に対する攻撃を強化していることを示しています。ウォッチガードのインシデント分析では、その影響を検証し、重要インフラのセキュリティの将来像を明らかにするとともに、あらゆる分野の組織がこうした攻撃を防御し、拡散を軽減するための手段を紹介しています。

旧来のサービスが引き続き標的に –
これまでの四半期報告では、通常1つか2つの新しいシグネチャが報告されていましたが、Q2のウォッチガードのトップ10ネットワーク攻撃には、4つの新しいシグネチャが含まれていました。注目すべきは、最も新しいものは著名なWebスクリプト言語のPHPにおける2020年の脆弱性でしたが、他の3つは全く新しいものではありませんでした。その中には、2011 Oracle GlassFish
Serverの脆弱性、2013年に発生した医療記録アプリケーションOpenEMRのSQLインジェクション攻撃、そして2017年に発生したMicrosoft
Edgeのリモートコード実行（RCE）の脆弱性などが含まれています。いずれも古いものではありますが、パッチを適用せずに放置しておくとリスクがあります。

Microsoft Officeを利用した脅威が根強く存在 –
Q2では、最も広範に発生したネットワーク攻撃トップ10リストにおいて、新たに1つ最上位に登場しました。シグネチャ1133630は、前述の2017年のRCEの脆弱性で、Microsoftのブラウザに影響を与えるものです。これは古い脆弱性であり、ほとんどのシステムでパッチが適用されていますが（といいのですが）、まだパッチを適用していないシステムは、攻撃者に先を越されてしまうと大変なことになります。実際に、CVE-2021-
40444として追跡されている非常に類似した重要性の高いRCEのセキュリティ上の欠陥が、今月初め、Windows 10のコンピュータ上のMicrosoft OfficeおよびOffice
365に対する標的型攻撃で積極的に悪用され、話題になりました。Office関連の脅威はマルウェアの中でも特に多く、試行錯誤された攻撃がいまだに目撃されていますが、幸いなことに、これらは従来のIPS防御でも検知されています。

フィッシングドメインが広く認知された正規のドメインを偽装 –
ウォッチガードでは、最近Microsoft
Exchangeサーバを標的にしたマルウェアの使用が増加していることを確認しており、一般的なメールユーザが、機密性の高い場所でリモートアクセスのトロイの木馬（RAT）をダウンロードするようになっています。これは、第2四半期が、2四半期連続でリモートワーカーや生徒がハイブリッドオフィスや学校など、以前のようにオンサイトに戻ったりしたことによるものと思われます

。どのような状況、あるいは場所であっても、強いセキュリティ意識を持ち、必ずしもネットワークセキュリティに接続されていないデバイスから送信される通信を監視することをお勧めします。

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。Q2では、ウォッチガードのアプライアンスは1,660万件以上のマルウェア（1デバイス当たり438件）、520万件近いネットワーク脅威（1デバイスあたり137件の検知）をブロックしています。レポートには、2021年Q2で新たに登場したマルウェアおよびネットワークに関する詳細トレンド、そして2021年前半におけるエンドポイントで検知された脅威の深掘り情報、さらに、あらゆる企業規模、業種に役立つ推奨されるセキュリティ戦略や防御のための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-q2-2021（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、エンドポイントセキュリティ、セキュアWi-
Fi、多要素認証、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18,000社の販売パートナーおよびサービスプロバイダを通じて、250,000社以上の企業に信頼性の高いセキュリティ製品／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・中小企業や分散拠点を持つ大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、多彩な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に応える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