ウォッチガード、マルウェアの総数は減少したものの、回避型の脅威が12%増加したと報告

2020年第2四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、JavaScriptマルウェア攻撃、Microsoft Excelベースの脅威の増加には多層型防御のセキュリティが必要

2020年9月30日（水）
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（2020年第2四半期）を発表しました。本レポートの特筆すべき調査結果として、Q2ではマルウェアの総検知数が8%減少したにもかかわらず、攻撃の70%にゼロデイマルウェア（アンチウイルスのシグニチャを回避するタイプ）が占めており、前期と比較して12%増加したことが挙げられます。

ウォッチガードのCTO、Corey
Nachreiner（コリー・ナクライナー）は次のように述べています。「COVID-19の世界的パンデミックに合わせてオペレーションを順応させたのは何も企業だけではなく、サイバー犯罪者も同じです。（おそらくリモートワークが増加したため）Q2にマルウェアの検知数全体が減ったにもかかわらず、洗練された攻撃が増加したことは、攻撃者が従来のシグニチャベースのアンチマルウェア対策を回避するような戦術に移行していることが伺えます。全ての組織は振舞いベースの脅威検知、クラウドベースのサンドボックス、そして多層型防御のセキュリティサービスを利用し、コアネットワークとリモートワーク人材を保護するべきです。」

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、組織、パートナー、顧客が身を守るために役立つ最新のマルウェアとネットワーク攻撃のトレンド、深掘りされた脅威調査、および推奨されるセキュリティのベストプラクティスが盛り込まれています。以下に2020年Q2の主な調査結果を紹介します：

　攻撃者が引き続き回避型の暗号化された脅威を活用
Q2の総検知数の3分の2以上がゼロデイマルウェアであり、34%が暗号化されたHTTPS接続経由の攻撃でした。組織で暗号化されたトラフィックを発見できない場合、脅威の3分の2を見過ごす計算になります。暗号化を用いた脅威の割合がQ1と比較して64%減少したとは言え、HTTPSが暗号化されたマルウェアは劇的に増加しています。FireboxセキュリティアプライアンスでHTTPSインスペクションを実行しようとしている管理者は増えているようですが、決して十分とは言えません。
　JavaScriptベースの攻撃が増加
スキャムスクリプトTrojan.GnaeusがウォッチガードのQ2トップ10マルウェアリストの1位にランクインし、マルウェア5件に対して1件近く占めています。攻撃者はGnaeusマルウェアにより、難

読化コードを用いてユーザのブラウザを制御し、目的のWebサイトから強制的に攻撃者が設定したドメインにリダイレクトさせます。また、別のポップアップスタイルのJavaScript攻撃J.S. PopUnderは、Q2における最も波及したマルウェアの1つであり、難読化されたスクリプトがユーザのシステムプロパティをスキャンし、検知対抗戦術としてデバッグの試みをブロックします。組織がこうした脅威に対抗するには、ユーザが未知のソースからブラウザの拡張機能をロードするのを防ぎ、最新のパッチを当てることで常にブラウザを最新の状態に保ち、信頼できるアドブロッカーを使用し、アップデートされたアンチマルウェアエンジンを維持するべきです。

攻撃者がマルウェアを隠すために暗号化されたExcelファイルを使用するケースが増加 - XML-Trojan.Abracadabraが、ウォッチガードのトップ10マルウェア検知リストに新たに登場し、4月に最初に発見されて以来急増しています。Abracadabraは、パスワードが「VelvetSweatshop」（Excelドキュメントのデフォルトのパスワード）である暗号化されたExcelファイル形式で配信されるマルウェアです。一度開いてしまうと、Excelが自動的にファイルを復号化し、スプレッドシート内のVBAスクリプトが実行ファイルをダウンロードし、起動させる仕組みになっています。デフォルトのパスワードを使用することにより、マルウェアは多くの基本的なアンチウイルスソリューションをバイパスします。なぜならファイルは、最初は暗号化されており、その後でExcelによって復号化されるからです。組織は、不審なソースからのマクロを決して起動させてはならず、クラウドベースのサンドボックスを活用して、感染してしまう前に危険性のあるファイルの真の目的を安全に検証するべきです。

エクスプロイト能力の高い旧来のDoS攻撃が復活

6年前に登場したDoS（サービス拒否）攻撃がWordPressやDrupalに影響を与えており、その数においてウォッチガードのQ2トップ10ネットワーク攻撃リストに名を連ねました。この攻撃は、パッチが当てられていない全てのDrupalやWordPressに悪影響を及ぼし、DoS攻撃によってインストールされているハードウェアのCPUやメモリを消耗させてしまいます。これらの攻撃数は多かったものの、特にドイツの数十件のネットワークが集中的に狙われました。DoS攻撃は、ユーザネットワークへの持続したトラフィックが必要であるため、攻撃者は標的を意図的に選定している可能性が高いことを意味しています。

マルウェアドメインがコマンド＆コントロールを活用した攻撃を頻発

今期ウォッチガードのトップマルウェアドメインリストに新たに2つのデスティネーションが加わりました。最も多かったのはfindresults[.]サイトであり、Dadobra trojanにC&Cサーバを使用し、難読化ファイルと関連するレジストリを作成することで攻撃が開始され、機密データを漏えいさせて、ユーザがWindowsシステムを起動したときに追加マルウェアがダウンロードされるようにします。また、あるユーザがウォッチガードチームにCioco-froll[.]comの存在を報告しており、別のC&Cサーバを用いてAsproxボットネットをサポートし、C&Cビーコンにより攻撃者はパーシスタンスが確立され、ボットネットが利用可能になったことを知ることができます。DNSファイアウォールを活用することにより、組織はこのようなアプリケーションプロトコルとは別の接続経路を持つ脅威を検知し、ブロックすることに役立てることができます。

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、世界中の約42,000台以上のウォッチガード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2,850万件以上のマルウェア（1デバイス当たり684件）、175万件以上のネットワーク脅威（1デバイスあたり42件）をブロックしています。また、Fireboxアプライアンスで410件の攻撃シグネチャを検知・ブロックしており、Q1と比較して15%増加し、2018年Q4以降最大となっています。

本レポートの全編では、今日の中小／中堅企業に影響を与えている主なマルウェアに関する知見

やネットワークのトレンド、並びに組織の防御に役立つセキュリティ戦略およびベストプラクティスが掲載されています。また、ハッキンググループShinyHuntersにより最近頻発している情報漏えいに関する詳細分析も含まれています。

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-q2-2020（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