Press Release
2019 年 9 月 27 日（金）
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、最新のセキュリティレポートで 著名なコンテンツデリバリネットワークを活用したマルウェアを報告

Kali Linux モジュールがマルウェアトップ 10 リストに入り、対前年比でマルウェアの総数が大幅に増加

2019 年 9 月 27 日（金）－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 2 四半期）を発表しました。今回のレポートでは、攻撃者がマルウェアのホスティングとフィッシング攻撃に利用する最も一般的なドメインを初めて公開し、ランク付けしています。また、よく利用される正規サイトのサブドメインや CloudFlare.net、SharePoint、Amazonaws.com などのコンテンツデリバリネットワーク（CDN）も紹介しています。その他レポートでは著名な Kali Linux のペネトレーションテストツールのモジュールがマルウェアリストのトップ 10 に初めてランクインし、マルウェアの総数が対前年比で 64%増加したことが挙げられています。

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。「今回のインターネットセキュリティレポートでは、マルウェアまたはフィッシングメールを正規のコンテンツホストドメインに隠し、ネットワークに忍び込ませるためにハッカーが使う手法に関する重要な詳細が報告されています。幸いにもこうした攻撃を防御するための方法がいくつかあります。例えば、DNS レベルのフィルタリングにより既知の不正な Web サイトへの接続を防御する方法、高度なアンチマルウェアサービス、詐取された ID 情報を活用した攻撃を防止する多要素認証、またはフィッシングメール対策のための従業員のトレーニングなどがあります。1 つの方法で全ての攻撃を防ぐことは不可能であり、組織が身を守る最善の方法は多層防御のセキュリティサービスを提供する統合型セキュリティプラットフォームを導入することです。」

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、著名なセキュリティ脅威に関する実データ、主要なセキュリティインシデントの詳細分析、そしてあらゆる規模の組織のビジネスおよび顧客データを保護する上で役立つ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 2 四半期の主な調査結果を紹介します：

- **マルウェアやフィッシング攻撃に正規ドメインを悪用 -** ウォッチガードの DNSWatch サービスは、既知の不正ドメインへの接続を DNS レベルで封じ、リダイレクトします。DNSWatch によって防御された著名な不正ドメインを追跡することにより、ウォッチガードではマルウェアやフィッシングメールをホスティングする主なドメインを特定することができます。注目すべきはこれらのドメインには、CloudFront.net（Amazon）などの正規の CDN のサブドメインや my[.]mixtape[.]moe.といった正規のファイル共有 Web サイトが含まれていることです。こうした攻撃手法は目新しいものではありませんが、ウォッチガードの調査ではこれらの攻撃に利用されている特定のドメインを明らかにしています。
- **Kali Linux がトップ 10 マルウェアリストに初登場 -** 著名なハッキング OS の Kali Linux の 2 つのモジュールが、ウォッチガードの主要なマルウェアリストに初めてランクインしました。C&C サーバへのバックドアを作成するマルウェアファミリ Trojan.GenericKD と、Web サーバへのバックドアの作成に利用される Web シェルスクリプト Backdoor.Small.DT の 2 種類がそれぞれリストの 6 位と 7 位にランク付けされました。このことは、悪意のある攻撃者による利用の増加、あるいはホワイトハットハッカーによる Kali Linux を用いたペネトレーションテストの増加のいずれかを示唆しています。

- **マルウェアの総数が対前年比で増加 –** 世界各地のウォッチガードの Firebox が検知したマルウェアの総数が昨年と比較して大幅に増加しました。2019 年第 2 四半期では、ウォッチガードの 3 つのマルウェア検知サービスのうち 2 つが 2018 年第 2 四半期と比較して増加が見られました。対前年比ではマルウェアが 64%増加しており、サービスの 1 つが 58%以上、もう 1 つが 68%以上の攻撃を防御しました。
- **フィッシングが拡散し、Office エクスプロイトマルウェアが増加 –** 2018 年第 4 四半期と 2019 年第 1 四半期に最も拡散したマルウェアリストに登場した 2 種類のマルウェア（偽の感染情報により被害者を恐喝するフィッシング攻撃と Microsoft Office エクスプロイト）がその量においてトップ 10 リストにランクインしました。このことは、こうしたキャンペーンが増加しており、広範なターゲットに対して大量の攻撃を仕掛けていることを示唆しています。ユーザは定期的に Office をアップデートし、アンチフィッシングや DNS フィルタリングのセキュリティソリューションを導入するべきです。
- **ネットワーク攻撃に SQL インジェクションが多発 –** SQL インジェクションが 2019 年第二四半期で検知された全てのネットワーク攻撃の 34%を占め、対前年比で大幅に増加しました（1 つの特定の攻撃が 2018 年第 2 四半期と 2019 年第 2 四半期を比較して 29,000%増加）。SQL データベースあるいは Web サーバを保守している場合、定期的にシステムにパッチを当て、Web アプリケーションファイアウォールを導入するべきです。
- **ヨーロッパと APAC でマルウェアが増加 –** 2019 年第 2 四半期では、マルウェアの約 37%が EMEA 地域を標的にしており、英国、イタリア、ドイツ、モーリシャスへの攻撃が集中しました。次に APAC が全マルウェア攻撃の 36%を占めました。APAC 地域では特に Razy および Trojan.Phishing.MH マルウェアの亜種が多く、Trojan.Phishing.MH の 11%が日本で検知されました。

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 41,229 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 22,619,836 件のマルウェア亜種を防御し（1 デバイス当たり 549 件）、また 2,265,425 件のネットワーク攻撃を防御しており（1 デバイス当たり 60 件）、ネットワーク攻撃の総量は過去の傾向とは反対に 2019 年第 1 四半期と比較して大幅に増加しています。

本レポートの全編では、2019 年第 2 四半期で最も影響のあったマルウェアやネットワーク攻撃の傾向に関する詳細な統計データ、および 2019 年 5 月にボルチモアの都市を麻痺状態に追い込んだ RobbinHood ランサムウェア攻撃（被害総額約 1,700 万ドル）の分析、並びに読者や組織の安全を守る上で役立つベストプラクティスが掲載されています。

MSP Sodinokibi ランサムウェア攻撃に関する分析

またレポートでは、Sodinokibi MSP ランサムウェア攻撃で使用された実際のマルウェアに関する詳細分析も掲載しています。ウォッチガードの脅威ラボの調査では、攻撃者が盗難あるいは漏えいさせた脆弱な ID 情報を活用して管理者権限を取得し、MSP がクライアントのネットワークの監視と管理に利用する正規の管理ツールに不正にアクセスし、セキュリティコントロールを無効にしたところで、PowerShell 経由で Sodinokibi ランサムウェア攻撃を仕掛けたことを突き止めています。

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-q2-2019
（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：角田
Tel： 03-5797-7205 Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： https://www.watchguard.co.jp