Press Release
2023 年 7 月 24 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 2023 年第 1 四半期最新インターネットセキュリティレポート：ブラウザを活用した新たなソーシャルエンジニアリングが増加

新たにトップ 10 入りしたマルウェアの 4 分の 3 が中国とロシア発、環境寄生型攻撃も増加

2023 年 7 月 24 日（月）－ 企業向け統合型サイバー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／エンドポイントセキュリティ）のグローバルリーダーである 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（2023 年第 1 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たちによって分析された、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およびエンドポイントセキュリティの脅威に関する詳細を報告しています。主な調査結果として、ブラウザを利用したソーシャルエンジニアリング戦略を活用したフィッシング、国家が関与している新たなマルウェア、ゼロデイマルウェアの急増、環境寄生型（LotL：living-off-the-land）攻撃の増加といった点が挙げられます。また、本レポートでは脅威ラボチームによる四半期単位でのランサムウェアの追跡・分析に特化したセクションも設けられています。

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。「組織は増え続ける複合型脅威から身を守るために、既存のセキュリティソリューションや戦略にもっと積極的に注意を払うべきです。今回のレポートで脅威ラボがまとめた重大テーマとそれに対応するベストプラクティスでは、環境寄生型攻撃に対してマルウェアへの多層型防御を強く強調しており、専門のマネージドサービスプロバイダーが運用する統合型セキュリティプラットフォームを活用すれば、シンプルかつ効果的に対応できると説明しています。」

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（2023 年第 1 四半期版）における主な調査結果を紹介します：

- **ブラウザを利用したソーシャルエンジニアリングが新たなトレンドに：**現在の Web ブラウザは、ポップアップの不正使用を防止する機能を強化しているため、攻撃者はブラウザの通知機能を利用して同様のタイプのインタラクション（やり取り）を促すことに軸足を移しています。また、今四半期の悪質ドメインの上位リストで注目すべきは、SEO ポイズニング行為に関与する新たな攻撃先です。
- **Q1 のトップ 10 リストにおける新たな脅威の 75%が中国とロシアの攻撃者：**ウォッチガードのトップ 10 マルウェアリストに登場した新たな脅威の 4 分の 3 が国家と強い結び付きがありますが、これらの悪意ある攻撃者が実際に国家に支援されているとは限りません。一例として今期のトップ 10 マルウェアリストに初めて登場した Zusy マルウェアファミリーが挙げられます。脅威ラボが発見した Zusy の例では、中国の国民を標的としており、悪質なブラウザをインストールするアドウェアが使用されており、このブラウザはシステムの Windows 設定を乗っ取り、デフォルトのブラウザとして使用されます。

- **Office 製品を狙った攻撃の継続、およびサポートが終了した Microsoft ISA ファイアウォールを標的とした攻撃が増加：**Threat Lab のアナリストは、今四半期も引き続き、Office 製品を狙ったドキュメントベースの脅威が最も広範にマルウェアリストに含まれていることを確認しています。また、ネットワーク面では、Microsoft のファイアウォール「Internet Security and Acceleration（ISA）Server」（現在は販売終了）に対する不正行為が比較的増えています。この製品の販売が終了してから長い期間が経過しており、アップデートも行われていないことを考えると、攻撃者がこの製品を標的としていることは驚くべきことです。
- 環**境寄生型（LotL：living-off-the-land）攻撃が増加：**Q1 の DNS 分析でレビューされた ViperSoftX は、オペレーティングシステムに含まれる組み込み型ツールを活用したマルウェアの最新例です。四半期を追うごとに、Microsoft Office や PowerShell をベースとしたマルウェアが報告されていることから、PowerShell のような一般的なツールの正当な使用と不正な使用を区別できるエンドポイントプロテクションの重要性が浮き彫りになっています。
- **Linux ベースのシステムがマルウェアの標的に：**Q1 におけるマルウェア検知数のトップリストに新たに登場したものの 1 つに、Linux ベースのシステムを標的にするマルウェアが挙げられます。Windows がエンタープライズ分野でトップシェアを占めていますが、組織は Linux や macOS にも注意を払う必要があることを痛感させられます。エンドポイント検知／レスポンス（EDR）を展開する際には、必ず Windows 以外のマシンも含め、システム環境を総合的にカバーすることが大切です。
- **検知数の大半を占めるゼロデイマルウェア：**今四半期は、暗号化されていない Web トラフィックを介したゼロデイマルウェアの検知数が 70%を占め、暗号化された Web トラフィックを介したゼロデイマルウェアの検知数はなんと 93%を占めています。ゼロデイマルウェアは、IoT デバイスや設定ミスのあるサーバ、および WatchGuard EPDR（エンドポイント保護／防御／レスポンス）のような強固なホストベースの防御を使用していないデバイスに感染する可能性があります。
- **ランサムウェア追跡データに基づく新たな知見：**今期、脅威ラボでは恐喝サイトに公開された 852 人の被害者を集計し、51 の新しいランサムウェア亜種を発見しました。これらのランサムウェアグループは、驚くほど高い割合で被害者を公表し続けており、中には著名な組織や Fortune 500 企業も存在します。（ウォッチガードの四半期ごとの脅威ラボリサーチの一環として、今後もランサムウェアの追跡トレンドや分析結果を報告する予定です。）

ウォッチガードの Unified Security Platform（R）（統合型セキュリティプラットフォーム）アプローチやウォッチガードの脅威ラボのこれまでの四半期ごとのリサーチアップデートと同様、この四半期レポートで分析されているデータは、ウォッチガードのリサーチ活動に賛同するウォッチガードのネットワークおよびエンドポイント製品を利用するお客様から、匿名により収集した脅威インテリジェンスに基づいています。

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、ウォッチガード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。Q4 では、ウォッチガードのアプライアンスは 1,570 万以上のマルウェア（1 デバイス当たり 194 件）、230 万超のネットワーク脅威（1 デバイス当たり 28 件）を防御しています。レポートには、2022 年 Q4 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トレンド、そしてあらゆる企業規模、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。

今回の 2023 年第 1 四半期の分析では、脅威ラボチームはレポート結果の正規化、分析、および提示に用いる方法を変えました。これまでの四半期ごとの調査結果は、主に（世界の総合計数として）集計し、発表されていましたが、今四半期以降のネットワークセキュリティの調査結果は、報告された全てのネットワークアプライアンスにおける「デバイスごとの」平均値として発表しています。本レポートの全文には、今回の変更に関する詳細や、新たに採用された手法の背景にある理論的根拠に加え、2023

年第 1 四半期における新たなマルウェア、ネットワーク、ランサムウェアの動向、推奨されるセキュリティ戦略、そしてあらゆる規模や業種の企業にとって重要な防御のヒントなどの詳細が記載されています。

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-q1-2023（英語版）

*日本語版は追って掲載する予定です。

【WatchGuard Technologies について】

WatchGuard（R）Technologies, Inc.は、統合型サイバーセキュリティにおけるグローバルリーダーです。ウォッチガードの Unified Security Platform（TM）（統合型セキュリティプラットフォーム）は、マネージドサービスプロバイダー向けに独自に設計されており、世界トップクラスのセキュリティを提供することで、ビジネスのスケールとスピード、および運用効率の向上に貢献しています。17,000 社を超えるセキュリティのリセラーやサービスプロバイダと提携しており、25 万社以上の顧客を保護しています。ウォッチガードの実績豊富な製品とサービスは、ネットワークセキュリティとインテリジェンス、高度なエンドポイント保護、多要素認証、セキュア Wi-Fi で構成されています。これらの製品では、包括的なセキュリティ、ナレッジの共有、明快さと制御、運用の整合性、自動化という、セキュリティプラットフォームに不可欠な 5 つの要素を提供しています。同社はワシントン州シアトルに本社を置き、北米、欧州、アジア太平洋地域、ラテンアメリカにオフィスを構えています。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

【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