Press Release

2023 年 12 月 18 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 3 四半期最新インターネットセキュリティレポートを発表：リモートアクセスソフトウェアの悪用が増加

エンドポイントへのランサムウェア攻撃が 89%増加し、暗号化された接続を介したマルウェアが減少

2023 年 12 月 18 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 3 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。データから得られる主な調査結果としては、リモートアクセスソフトウェアの悪用事例の増加、貴重な認証情報を窃取するためにパスワードスティーラーやインフォスティーラーを使用するサイバー攻撃者の増加、およびエンドポイント攻撃を開始するために、スクリプティングの利用から他の環境寄生型（LOTL）テクニックの採用へと移行する攻撃者が出現していること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。「攻撃者は、攻撃キャンペーンにおいてさまざまなツールや手法を使い続けているため、企業は最新の手口を常に把握し、セキュリティ戦略を強化することが重要です。ファイアウォールやエンドポイント保護ソフトウェアを含む最新のセキュリティプラットフォームは、ネットワークやデバイスを保護する高機能を提供しています。しかし、ソーシャルエンジニアリングの手口を用いた攻撃に関しては、悪意のある攻撃者が組織に侵入する上でエンドユーザーが最後の防衛線になります。組織としては、ソーシャルエンジニアリングに関する教育を行うとともに、マネージドサービスプロバイダーが効果的に管理できる多層防御を提供する統合型のセキュリティアプローチを採用することが肝要です。」

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 3 四半期版）における主な調査結果を紹介します：

- **マルウェア対策の検知を回避するために、リモート専用管理ツールおよびソフトウェアを使用する攻撃者が増加：**このことは FBI と CISA の両者も認知しており、例えば、脅威ラボがフィッシング詐欺のトップドメインを調査する中で、ユーザーが設定済みの TeamViewer の未承認バージョンをダウンロードし、攻撃者がそのコンピュータにフルリモートアクセスできるようにする技術サポート詐欺を発見しています。
- **Medusa ランサムウェアの亜種が第 3 四半期に急増し、エンドポイントランサムウェア攻撃が 89%増加：**表面的には、エンドポイントランサムウェアの検知数は第 3 四半期に減少したかのように見えます。しかし、マルウェア脅威のトップ 10 に初めてランクインした Medusa ランサムウェアの亜種が、脅威ラボの自動シグネチャエンジンの汎用シグネチャで検知されました。Medusa の検知数を考慮すると、ランサムウェア攻撃は前四半期比で 89%増加しています。
- **攻撃者がスクリプトベースの攻撃から軸足を移し、他の環境寄生型（LOTL）テクニックの採用が増加：**悪意のあるスクリプトは、第 2 四半期に 41% 減少した後、第 3 四半期には 11% 減少しました。それでも、スクリプトベー

スの攻撃は依然として最大の攻撃ベクトルであり、攻撃全体の 56%を占めており、PowerShell のようなスクリプト言語は、環境寄生型（LOTL）攻撃でよく使用されています。また、Windows の 環境寄生型（LOTL）バイナリは 32%増加しています。脅威ラボの研究者によるこれらの調査結果は、攻撃者が複数の環境寄生型（LOTL）のテクニックを利用し続けていることを示しており、おそらく PowerShell やその他のスクリプティングに対する保護が強化されたことに対応していると考えられます。このように環境寄生型（LOTL）攻撃は、エンドポイント攻撃の中で最も多くを占めています。

- **暗号化接続を介して侵入するマルウェアが 48%に減少：**つまり、検知されたマルウェアの半数弱が暗号化されたトラフィックを介して侵入したことになります。この数値は、前四半期から大幅に減少しているため、注目に値します。ただし、全体で検知されたマルウェアの総数は 14%増加しました。
- **第 3 四半期に検知された暗号化マルウェアのトップ 5 のうち 4 つが、悪意のあるペイロードを配信するメールベースのドロッパーファミリー：**上位 5 件のうち 1 件を除くすべての亜種には、Stacked という名前のドロッパーファミリーが含まれており、メールによるスピアフィッシングの添付ファイルとして送信されています。攻撃者は、知人の送信者から送信されたように見せかけ、請求書やレビュー用の重要なドキュメントと偽り、悪意のあるファイルを添付したメールを送信し、エンドユーザーを騙してマルウェアをダウンロードさせようとします。Stacked の亜種である Stacked.1.12 と Stacked.1.7 の 2 つは、マルウェア検知数トップ 10 にもランクインしています。
- **コモディティ化したマルウェアが出現：**マルウェア脅威のトップ 10 に、新たなマルウェアファミリーである Lazy.360502 がランクインしました。Lazy.360502 は、アドウェアの亜種である 2345explorer や Vidar パスワードスティーラーを配信します。このマルウェア脅威は、認証情報窃取ツールを提供する中国の Web サイトに接続し、窃取した認証情報に対して攻撃者が代金を支払うことができる「サービスとしてのパスワードスティーラーツール」のように動作しているように見え、コモディティ化したマルウェアがどのように使用されているかを示しています。
- **第 3 四半期でネットワーク攻撃が 16%増加：**ネットワーク攻撃で標的とされた脆弱性の第 1 位は ProxyLogon で、検知されたネットワーク攻撃全体の 10%を占めました。
- **ネットワーク攻撃のトップ 50 に、新たに 3 つのシグネチャが登場：**これらには、バッファオーバーフローを引き起こす 2012 年の PHP Common Gateway Interface Apache の脆弱性が含まれます。もう 1 つは、サービス拒否攻撃を引き起こす可能性のある 2016 年の Microsoft .NET Framework 2.0 の脆弱性が悪用されています。また、2014 年のオープンソース CMS である Drupal に SQL インジェクションの脆弱性が確認され、この脆弱性により、攻撃者は認証を必要とせずにリモートから Drupal を悪用することができます。

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。

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-q3-2023（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