本レポートの要点

ここ数四半期、ネットワークベースとエンドポイントでのマルウェア検知数は、どちらも上下動を繰り返していました。一方が増加すれば他方は減少し、その逆もまた然りといった状況が繰り返されています。第 2 四半期は、マルウェア検知はすべてのウォッチガード製品で減少し、ネットワークベースでは前四半期比で 24% 減、エンドポイントでは 39% 以上減少しました。しかし、シグネチャベースの防御を回避し、よりプロアクティブな手法によってのみ検知される未知のマルウェアやゼロデイマルウェアは増加しています。

それに対し、ネットワーク攻撃は 32%増加し、さまざまな脆弱性を標的とする一意のネットワーク攻撃も増加しています。この四半期の主な事例としては、2019 年の Nginx の脆弱性を狙った攻撃、ProxyLogin の欠陥に対する継続的な攻撃、HP Intelligent Management Center や Oracle Enterprise Manager Grid Control を標的とした脆弱性のエクスプロイトが確認されました。

不正サイトについては、チベット人を標的にしたサイト、トラップが仕掛けられた EC サイト、不正 PowerShell 実行のトリガーとなるポップアップといった、多数の侵害されたサイトを観測しました。

2024 年第 2 四半期のレポートの注目点を紹介します。

- **ネットワークベースのマルウェア検知数は 24% 減少しました。**一方で、挙動ベースのマルウェア対策 APT Blocker によって**検知されたマルウェアの数は 168% と大幅に増加しました。**
- **エンドポイントマルウェア検知数は前四半期比で 39% 減少しました。**これまでの数四半期、エンドポイントとネットワークベースのマルウェア検知は反比例してきました。一方が増加すると他方は減少するという状況が続いていましたが、今回、初めて両方が減少しました。
- **第 2 四半期は、マルウェアの 43%は暗号化された接続（TLS）経由で拡散しましたが、**これは第 1 四半期と比べ 10% 減少しています。
- それぞれのネットワークマルウェア検知サービスにおける「Firebox あたりの」マルウェア検知の結果は以下のとおりです。
  - **Firebox あたりの平均マルウェア検知数の合計：**935（約 24%減
  - **Firebox あたりの GAV による平均マルウェア検知数：**366（35%減）
  - **Firebox あたりの IAV による平均マルウェア検知数：**368（37%減）
  - **Firebox あたりの APT Blocker による平均マルウェア検知数：**201（168% 増）
- **ウォッチガード**への報告に同意していただいた、現在アクティブである（ライセンスされている）すべての Firebox でいくつかのサービスをご利用いただき、すべてのマルウェア検知サービスが有効になっていた場合、2024 年第 2 四半期のマルウェア検知は、361,312,985 だったと推定されます。
- **検知されたマルウェアの 46% は、シグネチャベースの手法を回避するゼロデイマルウェアでした。**ゼロデイマルウェアとは、シグネチャベースの防御を回避し、よりプロアクティブな手法によってのみ検知される未知のマルウェアです。さらに、暗号化された接続内でのゼロデイマルウェアが増加し、TLS を介したマルウェアは全体の 56% を占めました。
- **Trojan.html.hidden.1.gen を検知するシグネチャは、最も広範囲で観察されたマルウェア亜種の 4 位になりました。**このシグネチャが検知した最も一般的な脅威カテゴリは、ユーザのブラウザから認証情報を収集し、その情報を攻撃者が管理するサーバに配信するフィッシングキャンペーンでした。興味深いことに、脅威ラボが観察したこのシグネチャのサンプルは、ジョージア州のバルドスタ州立大学の学生と教職員を標的にしていました。
- **2019 年に検知された NGINX の脆弱性は、前四半期に脅威ラボのネットワーク攻撃の 50 位にも入りませんでしたが、2024 年第 2 四半期にはネットワーク攻撃の検知数で 1 位になりました。**この脆弱性は、米国、EMEA（ヨーロッパ・中東・アフリカ）、APAC（アジア太平洋）で約 724,000 件検知され、ネットワーク攻撃の全検知数の 29% を占めました。
- **Fuzzbunch ハッキングツールキットが、エンドポイントマルウェアの検知数で 2 位になりました。**このツールキットは、Windows オペレーティングシステムを攻撃するために使用されるオープンソースのフレームワークとして機能し、2016 年にハッカー集団である The Shadow Brokers が米国 NSA（国家安全保障局）との関連が指摘される Equation Group を攻撃した際に盗まれたものです。
- **2024 年第 2 四半期のネットワーク攻撃が 33%増加しました。**アジア太平洋地域での検知がネットワーク攻撃検知数の 56% を占め、前四半期比で 2 倍以上になりました。
- **ProxyLogon は引き続き 10 位に入っています。**これは、Microsoft Exchange Server のリモートコード実行の脆弱性で、かなり前にパッチが適用されているはずですが、今も 2 位を維持しています。
- **エンドポイントマルウェア検知数が全体として 39% 以上**減少しました。

これらは 2024 年第二四半期においてウォッチガードのセキュリティ製品がブロックした脅威の一部です。これら脅威に関する詳細や脅威に対する実践的なヒントと戦略については、本レポートで解説します。