本レポートの要点

前回のレポートでは、マルウェアとネットワーク攻撃の両方が大幅に増加し、特にネットワークで検出されるマルウェアは、パンデミック以前のレベルに戻りました。これは、企業の業務が正常化しつつあり、従業員がオフィスに復帰していることを示している可能性があります。しかし、今回の 2022 年第 1 四半期のレポートでは、ネットワークマルウェア全体で 10% 以上減少し、ネットワーク攻撃も 19% 減少しています。

一方で、エンドポイントで検出されたマルウェアは 38% 増加しました。新型コロナウイルスの感染者が急増したために在宅勤務が再び増えたのか、オフィスと自宅の両方を利用するハイブリッドワークの新しい形が定着しつつあるのかは分かりません。確定的なことは言えませんが、四半期ごとの増減はあるものの、すべての脅威が前年同期比で増加しています。脅威の総量は増加していますが、ゼロデイマルウェア（シグネチャ検出を回避する脅威）と暗号化接続を利用するマルウェアの両方は減少しています。これらの脅威を検出できるより最先端のセキュリティ機能を使用していない組織にとって、これは朗報ですが、いずれの脅威の数値も未だに高い水準にあることから、挙動ベースのマルウェア検出と、TLS トラフィックを復号化して検査できるネットワークテクノロジを活用することをウォッチガードは推奨します。一方、エンドポイントを標的とする脅威は依然として高い水準にあります。

そのため、WatchGuard の EPDR などの適切なエンドポイントの保護・検知・対応（EPP/EDR）製品を導入し、リモートワーカーを標的とする回避型の巧妙なマルウェアを検出できるようにする必要があります。エンドポイントを標的とするマルウェアの多くは、悪意のあるスクリプト（主に PowerShell を使用）として侵入しています。そのため、正規の PowerShell は許可しながら、不正な PowerShell を検出してブロックできるエンドポイントセキュリティコントロールを必ず導入してください。

2022 年第 1 四半期の要点を以下に示します。

- シグネチャベースの検出数が増加する一方で、第 1 四半期は、**マルウェア全体で見ると前四半期比で 10.4% の減少となりました。**とはいえ、それ以前の四半期と比較すると、ネットワーク境界（オフィス）で検出されたマルウェアは、パンデミック前のレベルに戻っています。脅威データを提供している Gateway AntiVirus（GAV）および APT Blocker（APT）デバイスでは、それぞれ 1,360 万と 780 万の脅威が検出されています。
- **Emotet が復活しました。**昨年初め、世界各国の捜査機関が広く拡散していたボットネットの C2 インフラストラクチャを掌握してボットネットを壊滅しました。素晴らしい成果を得ることができましたが、ウォッチガードの**アナリストは Emotet の脅威**は、新しい管理者に引き継がれ新しい亜種として復活する可能性があることを警告してきました。第 1 四半期には、**Emotet 関連の脅威が、マルウェアの上位 10 件の 3 件を占めており、最も拡散している脅威の 1 つとなっています。**
- **60.1% のマルウェアが引き続き、暗号化された接続に潜んでいます。**この数値は、2022 年第 4 四半期から 6.6 ポイント低下しましたが、依然として、多くのマルウェアが HTTPS トラフィックを復号化しないソリューションを回避しています。
- **Office 文書を使用するマルウェアが引き続き増加しています。**上位 10 位にあるマルウェア 3 件は、いずれも悪意のあるコードが仕掛けられた Office ファイル（Word や Excel）を介して拡散します。このような Office 文書がすべて正規のファイルだと考えているユーザーには、決してそうではないことを警告してください。
- **半数以上（57.8%）のマルウェアがシグネチャ検出を回避していますが、この回避率は減少傾向にあります。**シグネチャ検出を回避するマルウェアは、ゼロデイマルウェアと呼ばれます。2 四半期連続でゼロデイマルウェアが減少しており、第 1 四半期は前期から 7.8 ポイント減少して 57.8% となりました。これは、従来型のアンチウイルス対策にのみ依存している組織にとっては朗報ですが、それでも、マルウェアの半分以上がシグネチャを回避していることに注意が必要です。また、TLS 経由で配信されるゼロデイマルウェアも減少し、33.7 ポイント減の 44% となっています。
- **第 1 四半期にはヨーロッパ、中東、アフリカ（EMEA）地域が最も多くのマルウェアの標的となっており、その割合は 57% に上ります。**残りのマルウェアは、南北アメリカ（AMER）とアジア太平洋（APAC）にほぼ均等に分散しています。
- ネットワーク攻撃は、第 4 四半期には 4 年ぶりの高水準となりましたが、**この四半期では 17% 減少しました。**IPS のヒット数は前四半期と比較して約 470 万件減少していますが、前年の同四半期と比較すると約 10% 増加しています。
- **Firebox はアプライアンスあたり平均 ~60 件の攻撃をブロックしました。**アプライアンスあたりの数値は大幅に減少したように見えますが、前四半期から報告対象の Firebox の台数のカウント方法が「ボックスあたり」の平均に変更されたことが影響したものと考えられます。
- **EMEA では、第 1 四半期に検出されたネットワーク攻撃は非常に少なく、6% 程度にとどまりました。**APAC が多くのネットワーク攻撃を受けているのと同様に、これまでの四半期とは大きく異なる変化となっています。
- **2022 年第 1 四半期には Log4shell の脆弱性が大きく狙われました。**この攻撃は、トップ 10 の 8 位にランクインしており、攻撃者は、パッチが適用されていない Log4j サーバを標的としています。
- **第 1 四半期に Firebox がブロックした悪意のあるドメインは 750 万件**で、前四半期から 31% 増加しました。
- エンドポイントに関する統計では、**エンドポイントで検出されたマルウェアは、2022 年第 1 四半期に 38% 増加しました。**
- **2022 年第 1 四半期に、マルウェア検知の約 88% をスクリプトが占めました。**これは、脅威者がシグネチャベースの検知を回避するために、従来のマルウェアから環境寄生型攻撃へと移行していることを示しています。さらに重要なのは、**スクリプトベースのマルウェアの 99% 以上を PowerShell が占めていることです。**
- **ランサムウェアの検出数は 80% 増加し**、すでに昨年の同時期の 3 倍の水準に達しています。ウォッチガードのアナリストは、この上昇について第 1 四半期に LAPSUS$ ランサムウェアグループによる活動が活発化したことと関係があると考えています。

さまざまな攻撃の可能性に基づいてセキュリティ対策を講ずるときに、ウォッチガードの四半期レポートが提供しているデータ指標を活用し、効果的なセキュリティ対策が可能になることを願っています。ここからはさらに詳細な情報と重要な分析結果について説明しますので、リラックスできるお好きな飲み物を楽しみながら、前四半期で最も多く検出された脅威の詳細をご確認ください。