本レポートの要点

ビジネスは正常に戻りつつあるのでしょうか？第4四半期にマルウェアやネットワーク攻撃が大幅に増加し、マルウェアについては、パンデミック前の通常の水準に戻りつつあるようです。第4四半期に脅威が増加した理由はいろいろ考えられますが（長期休暇やショッピングシーズンで関連する攻撃が増えたなど）、従業者がオフィスに戻ったことも一因でしょう。COVIDのパンデミックが開始した時期に、本レポートでマルウェアが最初に減少に転じました。在宅勤務への移行に伴い、従業員がオフィスのFireboxから不正リンクを閲覧することはなくなりました。オフィスを閉鎖していた企業の多くが第4四半期にオフィスでの業務を再開するようになりました。ハイブリッドワークがなくなることはおそらくありませんが、従業員がオフィスに戻れば、ネットワークの脅威も通常の水準に戻ることになるでしょう。

全体として脅威が増加したことで、ウォッチガードが検知したゼロデイマルウェア（シグネチャベースの防御を突破するマルウェア）の割合は、66%弱と比較的高水準で推移しています。さらに、そのゼロデイマルウェアの67%は依然として、暗号化された（セキュアWeb）接続経由で到着しています。この2つの数字を合わせて考えると、暗号化された接続を経由する不正プログラムの約78%がシグネチャを回避したことになり、サイバー犯罪者がこの2つの手法を使用することで回避能力を向上させようとしていることがわかります。

エンドポイントの場合、ほとんどのマルウェアは不正スクリプトとして開始し、従来のファイルベースの防御を回避する可能性が高く、ランサムウェアは減少していますが、標的型ランサムウェア攻撃は今も猛威を振るっています。ランサムウェアの数は減少していますが、大規模の標的型攻撃の効果は引き続き高いようです。

2021年第4四半期の要点を以下に示します。

- **マルウェアは前四半期比で約40%増加し、**パンデミック前の水準に戻りました。Gateway AntiVirus（GAV）の検知数は1,300万件を超え、APT Blocker（APT）の検知数は1,100万件近くを記録しました。
- **66.7%のマルウェアが引き続き、暗号化された接続経由で到着しています。**これは第3四半期比で3ポイントの減少ですが、サイバー犯罪者が引き続き、従来型の防御を暗号化で回避しようとしていることを示しています。**暗号化された接続経由で到着するマルウェアの77.7%が、シグネチャによる検知を回避**しています（ゼロデイマルウェア）。
- **第4四半期にGAVの検知数が最多だったのは、LavasoftのAdawareです。**AdawareにはPUP（Potentially Unwanted Program、不要なプログラム）が付属していることが多く、GAVはこれをマルウェアとしてブロックします。
- **古いボットネット、Zum.Andromが再び上位に入りました。**HTTPやHTTPSのコマンド&コントロール（C2）メカニズムを使用することが多い最新のボットネットとは異なり、Zum.Andromは、ボットネットが古くから主要通信手段として使用してきたインターネットリレーチャット（IRC）を今も使用しています。このボットネットは、圧縮されたRARファイルを添付した電子メールで送信される傾向があり、これはおそらく、圧縮ファイルでマルウェア検知を回避しようと攻撃者が考えているためです。
- **ゼロデイマルウェアは、第3四半期から2ポイント弱減少し、**マルウェア全体の約3分の2である65.6%を占めました。APT Blockerなどの行動分析サンドボックスを使用して、このような回避型のマルウェアを捕捉する必要があります。
- **第4四半期にネットワーク攻撃が4年ぶりの高水準となる570万件を記録しました。**これは前四半期の39%増で、2018年第4四半期以降で最多です。ネットワーク攻撃の検知は増加し続けているため、管理者には、Fireboxの不正侵入検知・防御サービス（IPS）の活用をお勧めします。
- **Fireboxは2021年第4四半期に、アプライアンスあたり平均75件の攻撃をブロックしました。**アプライアンスあたりで大幅に減少したように見えますが、この四半期から報告対象のFireboxの台数のカウント方法の変更が「ボックスあたり」の平均に影響したものと考えられます。
- **北米・南米（AMER）では、他の地域と比べてはるかに多くのネットワーク攻撃が第4四半期に確認されました。**ネットワークエクスプロイトの61%弱がAMERで検知されました。以下の順位では、ヨーロッパ・中東・アフリカ（EMEA）とアジア太平洋（APAC）が逆転し、EMEAが10%弱だったのに対して、APACが約29%になりました。これまでは、最下位がAPACの定位置でした。
- **Fireboxが第4四半期にブロックした不正ドメインは550万件**で、2ポイント弱減少しました。数四半期ぶりに、DNSWatchの有害ドメインの検知数が減少しました。
- **2021年第4四半期に、マルウェア検知の約86%をスクリプトが占めました。**これはおそらくは、シグネチャベースの検知を回避する目的でLofL（環境寄生型）攻撃を集中的に仕掛けるサイバー犯罪者が増えているためです。
- エンドポイント製品では、ランサムウェアは減少していますが、クライトマイナーに大きな変動はありません。

以上のように、若干の変化はありましたが、このような変化を認識し、変化に合わせて防御を調整すれば、恐れる必要はありません。これらの変化とその対策として推奨される防衛策について、本レポートで詳しく解説します。