エグゼクティブサマリー

2019 年第 4 四半期にはゼロデイマルウェア（リリース後の数日から数週間にシグネチャベースの保護で見逃されたマルウェア）が急増し、検出された全マルウェアのうち、過去最高となる 68%を占めました。2018 年と 2019 年の平均約 37%から増加しており、2019 年第 4 四半期はマルウェアに関して最悪な四半期となりました。また、引き続き数多くの悪意のある Excel ドロッパーが確認されているほか、マルウェアリストの上位には以前よりも多くの Mac アドウェアが入っています。Web アプリケーション攻撃は、SQL インジェクション攻撃を筆頭に、ネットワーク脅威のリストを埋め続けています。最後に、Macy’ s の e コマースサイトで 10 月に発生したデータ漏洩を第 4 四半期に分析したので、その結果に基づいて、攻撃者が悪意のある JavaScript「MageCart」を使用してクレジットカード情報をスキミングした方法を説明します。

2019 年第 4 四半期のインターネットセキュリティレポートでは、上記以外にも次のようなトピックを取り上げています。

- **ゼロデイマルウェア（シグネチャベースの防御をすり抜けて侵入する回避型マルウェア）が、全マルウェアの 68%という記録的な割合にまで急増しました。これは、昨年の平均 37%から増加しています。**これに対応して、ウォッチガードの IntelligentAV および APT Blocker がブロックしたマルウェアの量も急増しました。

- **第 4 四半期、Firebox は 3,450 万件のマルウェアサンプルをブロックしました。**これは、1 台の Firebox につき約 860 件のマルウェアで史上最高となります。

- **Microsoft Excel の古い脆弱性が現在も高い頻度で悪用されています。**第 4 四半期に最も多かったマルウェアのリストで 7 位だったのは 2017 年の Microsoft Excel の脆弱性でした。これは、攻撃者がこの脆弱性を今も実際に悪用していることを示しています。

- **Mac アドウェアがトップ 10 リストに返り咲きました。**2019 年第 4 四半期にセキュリティ侵害を受けた上位 Web サイトの 1 つは、Adobe Flash のアップデートになりすます macOS アドウェア「Bundlore」をホスティングしていました。

- **2019 年第 4 四半期、Firebox は 188 万件のネットワーク攻撃をブロックしました。**これは、1 台あたり約 47 件の攻撃を阻止したことになります。

- SQLインジェクション攻撃は、2018年と比較して、2019年第4四半期に8000%も増加し、最も一般的なネットワーク攻撃となりました。

- **ネットワーク攻撃の半分近くが、3 つの地域**（AMER、EMEA、APAC）のいずれかに分類されました。

- **Macy’ s の e コマースサイトが MageCart の攻撃を受けました。**MageCart は、顧客がクレジットカードの取引を行う際に、その情報をスキミングする JavaScript の脅威です。

- 攻撃者が引き続き正規の画像共有サイトを使用してマルウェアを拡散していることが、DNSWatch により明らかになりました。セキュリティ侵害を受けた上位サイトの詳細については、DNS のセクションを参照してください。

主なトピックを把握したところで、詳細を見ていきましょう。本レポートを最後までお読みになれば、集中的に対応する必要があるサイバー脅威を理解し、安全の確保に役立つヒントを得ることができるはずです。