本レポートの要点

2023年第2四半期は、統計上の異常値を減らし、データ精度を改善するための新たな手法を採用してきました。このため、新たな結果の一部を過去のレポートの値と直接比較することが難しいケースもありました。それにもかかわらず、いくつかの重要なトレンドと脅威を継続的に特定することができました。第2四半期には、ネットワークマルウェアの検知数は全体的に増加した一方で、巧妙で回避型の「ゼロデイマルウェア」は全般的に大幅に減少しました。しかし、暗号化された接続から配信されるゼロデイマルウェアの数は、依然として高止まりしています。また、Linuxベースのマルウェアが、これまでよりも多く10位までに入りました。

ネットワーク攻撃（IPSの検知数）は2023年第2四半期に大幅に減少しました。この結果は、最も一般的なトレンドを特定できるように異常値を除外する新しい手法を採用したことが大きな原因となっています。大きな変化に見えるかもしれませんが、過去のレポートにおける高い数値は、同じように異常値による影響があった可能性があります。全体として、10位までのネットワーク攻撃は、攻撃者が悪用する方法を簡単に見つけることができる古いソフトウェアの脆弱性で占められています。米国のCISAは最近、サイバー犯罪者が古い脆弱性を標的にしていることを確認しています。

ウォッチガードのエンドポイントマルウェア製品では、マルウェアの検知数全体的にやや減少しており、若干異なるデータを示しています。しかし、複数のマシンに影響するマルウェアは増加傾向にあります。ランサムウェアの検知数は引き続き減少しており、前四半期比で21.6%減少しました。ランサムウェアの検知数が減少したとは言え、ランサムウェアグループは引き続き多くの企業に侵入して恐喝しています。本レポートでもいくつかの事例を紹介します。配信方法については、悪意のあるスクリプトや環境寄生型（LotL）の手法が依然として高い割合を占めていますが、若干減少しつつあり、Windowsに固有のマルウェア・ファイルが多く利用されるようになっています。

本レポートの後半では、ユーザがアクセスできないようにブロックした上位のマルウェアやフィッシングドメインに関する情報などさらに多くの詳細について説明します。

2023年第2四半期の要旨を以下に紹介します。

- **今四半期のレポートから、「Firebox 1台あたり」のマルウェアボリュームを報告しています。**以下に、それぞれのマルウェア検知サービスでのマルウェアの結果を示します。
  - **Firebox 1台あたりの平均マルウェア検知数の合計：**1,177
  - **GAVが検知したFirebox 1台あたりの平均マルウェア数：516**（マルウェア全体の43.8%）
  - **IntelligentAV（IAV）が検知したFirebox 1台あたりの平均マルウェア数：503**（マルウェア全体の42.7%）
  - **APTが検知したFirebox 1台あたりの平均マルウェア数：**158（マルウェア全体の13.4%）
- ウォッチガードへの報告に同意していただいたすべてのFireboxで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、**2023年第2四半期のマルウェア検知は88,450,373**だったと推定されます。この数字は、ウォッチガードとデータを共有することに同意したFireboxのみを表しています。しかし、ウォッチガードのTotal Securityサービスを利用していない、あるいは適切に設定していない場合は、多くのマルウェアを見逃している可能性があります。
- **エンドポイントのランサムウェア検知数は22%減少**前四半期の73%の減少から引き続き減少しました。減少しているにも関わらず、ランサムウェアによる恐喝は依然として活発であり、最新情報を取り入れて常にランサムウェアの防御戦略を更新しておく必要があります。これは、10万台エンドポイントあたり981件の攻撃をブロックしたことになります。これは第1四半期と比較して8.2%減少しています。
- **95.6%のマルウェアが暗号化され隠ぺいされています。**前期より1ポイント低下しましたが、全般的には依然として高水準です。これまでも、マルウェアがセキュアWebサイトで使用されるSSL/TLS暗号に隠れるようになったと説明してきましたが、このトラフィックをインスペクションしないと、ネットワークセキュリティのほとんどのマルウェアを見逃してしまいます。エンドポイントのマルウェア保護はセーフティネットの役割を果たしますが、暗号化されたトラフィックをスキャンすることを強く推奨します。
- **ゼロデイマルウェアは、全マルウェアのわずか11%にまで減少し、**過去最低を記録しました。これだけ減少した原因は不明ですが、**暗号化された接続で配信されているマルウェアの割合は66%と、依然として高くなっています。**現在、攻撃者は主に暗号化された接続を介してマルウェアを配信していると考えられます。
- **4つのタイプのLinuxベースのマルウェアが10位までに入っており、**前四半期には攻撃者がLinuxを標的にする傾向が強まっています。ランサムウェアのエンドポイントでの検知数は減少しており、10万台エンドポイントあたりわずか465件となり、前四半期比では21.6%減少し、前年同期比では72.4%も減少しました。
- 最も拡散しているマルウェアは、**Officeドキュメントとアドウェアです。最も拡散した上位のマルウェア**とは、純粋な数が最多ではなかったものの、被害者が最多だったマルウェアのことです。この四半期のリストでは、Office製品を標的としたドキュメントベースの脅威が引き続き見られましたが、上位にはいくつかのアドウェアも見られています。
- **ネットワーク攻撃は前四半期比で約80%減少しました。**しかし、これはウォッチガードがデータを分析するときに、外れ値を排除する方法を変更したことが原因だと考えられます。
- **サイバー犯罪者は、古いソフトウェアに存在する脆弱性を今もなお攻撃しています。**
- **Fireboxの上位1%で検知総数の41.5%を占めています。**これは、ごく一部のデバイスが依然として最も多くの攻撃を受けていることを示しています。
- **地域的にはネットワーク攻撃は全世界でほぼ均等に分散しています。**EMEAは平均より少し多く、APACでは攻撃が最も少なくなっています。外れ値を排除するように変更する前は、この地域分布には大きな偏りがありました。
- **エンドポイント10万台あたりで981件の攻撃がブロックされました。**

- **リンク短縮ドメインや乗っ取られたWordPressブログが悪意のある目的に利用されています。**今四半期に最も多くブロックされた悪意のあるドメインを調査したところ、野球に関連するWordPressのブログとドメイン短縮型ドメインサービスが新たな標的となっていることが分かりました。

- **マルウェアを配信する方法としてスクリプトが使用されるケースは減少**していますが、Windowsファイルなどを使用してマルウェアを配信する他の方法が増加しています。マルウェアを配信するために、PowerShellなどのスクリプトは最も多く使用されていますが、前四半期比では大幅に減少しています。一方、Windowsファイルを悪用して配信されるマルウェアは増加しています。

ここで紹介した概要は、本レポートに含まれるデータの一部に過ぎません。各セクションで説明しているマルウェア、脅威、攻撃の具体例を参照いただくと、防衛に役立つ情報を確認いただけます。本レポートを読み進めていただき、これらのトレンドの詳細と、自社を守るヒントをぜひご確認ください。