本レポートの要点

第2四半期は、マルウェアはやや減少（3.8%）しましたが、ネットワーク攻撃は引き続き増加しました。これは、今日のハイブリッドワークに見られるトレンドと完全に一致しています。サイバー犯罪者は、オフィスに今も残るサーバやネットワークソフトウェアへのネットワーク攻撃を続けていますが、在宅勤務のユーザを標的にマルウェア攻撃を仕掛けています。

マルウェアの件数は減少しているものの、それ以上に気になるトレンドも確認されました。91%以上のマルウェアが暗号化された接続経由で到着しているという事実は、HTTPSトラフィックを復号化してスキャンしていないユーザにとって非常に悪いニュースです。この対策を実行している組織は約20%であるため、残りの80%はネットワーク経由で到着するマルウェアの10件に9件を見逃してしまうことになります。多くの組織が有効なエンドポイント保護を導入し、到着するマルウェアを捕捉できていることを願うばかりです。シグネチャによる保護で検知されない脅威であるゼロデイマルウェアが第2四半期に約10%減少したのは良いニュースですが、問題は、ゼロデイがマルウェア全体の64%、すなわち3分の2を占めるということです。

エンドポイントに到達する脅威に注目すると、アンチウイルス（AV）製品を回避する可能性が高いスクリプトベースの攻撃が、すでに昨年1年間の80%も検知されており、このまま行けば確実に昨年を上回ることになるでしょう。また、ランサムウェアが大幅に増加しました。以上が、本レポートで紹介するこの四半期のトレンドの要点です。

2021年第2四半期の脅威環境の概要

- **マルウェアの91.5%が、暗号化された接続経由で密かに到着**するようになっています。これは、Fireboxやネットワークセキュリティ対策のTLS復号化機能を利用していないIT管理者にとって、悪いニュースです。Web接続を復号化してセキュリティスキャンを実行していない場合、ネットワーク制御は、第2四半期に到着したマルウェアのほとんどを見逃してしまったことになります。

- 全体では、**境界のマルウェア検知数が約4%減少し**、第2四半期の検知数は約1,660万でした。脅威インテリジェンスデータを報告するFireboxがわずかではあるものの1%増加したにもかかわらず減少し、**Firebox 1台あたりのマルウェアの平均検知数は438**となりました。

- XML.JSLoaderとAMSI.Disable.Aという2つのマルウェア亜種が、セキュアWeb接続で検知されたマルウェアの90%以上を占め、Gateway AntiVirusの検知数全体の12%を占めました。

- **ゼロデイマルウェアは、過去最高だった前四半期から9%減少しましたが、**それでも64.1%とマルウェア全体の約3分の2を占めました。シグネチャベースのオプションよりプロアクティブなマルウェア検知制御を利用していない場合、導入することをお勧めします。

- **ネットワーク攻撃の件数は前四半期に続いて、過去3年間で最高を記録**しました。Fireboxの不正侵入防止サービス（IPS）は、**第2四半期に520万件のネットワークエクスプロイト**を検知し、前四半期比で22.3%増となりました。2四半期連続でネットワーク攻撃が大幅に増加しました。

- FireboxアプライアンスのIPSは2021年第2四半期に、**アプライアンス1台あたり**平均**137件の攻撃をブロックし**、前四半期比で21%増となりました。

- 地域別では、**北米・中南米（以下、AMER）が最も多くのネットワーク攻撃を受けており、Fireboxあたりの平均IPSヒット数は1,744**でした。ヨーロッパ・中東・アフリカ（以下、EMEA）ではデバイスあたりのヒット数が764、アジア太平洋地域（以下、APAC）では316でした。

- **報告対象のFireboxは第2四半期に、過去最高となる730万件の不正ドメインをブロックしました。**ウォッチガードのDNSファイアウォールであるDNSWatchによる検知数は、第1四半期にすでに281%増を記録しましたが、このトレンドがこの四半期も継続し、不正ドメインの検知数がさらに45%増加しました。

- ウォッチガードのエンドポイント製品は2021年上半期に、**2020年通年の約80%**に相当するファイルレス攻撃や環境寄生型攻撃をすでに検知しました。これは、スクリプトを活用する脅威の検知に基づくものです。このトレンドが仮に続けば、今年は環境寄生型攻撃が大幅に増加することが予想されます。

- 2021年上半期の**ランサムウェア検知数は、2020年の通年の検知数にわずかに下回る数である**ため、この増加傾向が続けば、2021年のランサムウェア検知数の合計は、少なくとも昨年の150%になるでしょう。

以上の注目すべき統計値を念頭に、第3四半期の予測を解説し、雨具を用意して荒天に備え、サイバー攻撃から働く環境を保護するための方法を提案します。以下の分析とセキュリティに関するヒントをぜひご活用ください。