本レポートの要点

2022年第2四半期も前回のレポートと同様に、マルウェア攻撃とネットワーク攻撃の両方が減少しました。しかしながら、ネットワークマルウェア検知が減少したもののエンドポイントマルウェア検知が増加した前四半期とは異なり、マルウェア検知が全体として減少しました。件数が減少した理由を示す証拠はありませんが、脅威環境が好転したわけではありません。事実、暗号化された接続経由で到着するマルウェアが増加し、少なくとも、この情報から確認できるいくつかのデバイスで81%以上になりました。残念ながら、データの共有に同意していただいたFireboxでHTTPS接続のマルウェアを復号して捕捉するように構成されているのは一部に過ぎません。おそらく、マルウェアが減少したように見えるのは、TLSトラフィックを復号しないデバイスで暗号化によってマルウェアが隠れているためでしょう。いずれにしても、件数は前四半期比で減少したものの、パンデミックの大部分を占めた時期と比較すると今なお高水準にあると言えます。

一方、シグネチャベースの検知を回避するマルウェアであるゼロデイマルウェアは、半数強にとどまりました。APT BlockerやIntelligentAVなどのより高度なアンチマルウェアサービスを利用していない場合は、Total SecurityをFireboxパッケージに追加してこれらの回避型の脅威を捕捉することをご検討ください。あるいは、Adaptive Defense 360（AD360）やWatchGuard EPDRなどのプロアクティブなマルウェア検知の機能を提供するエンドポイント製品を利用することもできます。

いずれにしても、件数が減少したものの、確認された脅威の影響が大きいことに変わりありません。**2022年第2四半期レポートのハイライトは以下のとおりです。**

- 第2四半期に**ネットワークベースのマルウェアの検知数が前四半期比で15.7%減少**しました。これには、ウォッチガードのGAV（Gateway AntiVirus）サービスで検知された基本的なマルウェア（検知数は1,170万件弱）とAPT Blockerなどの高度アンチマルウェアサービスで検知された回避型やゼロデイのマルウェア（検知数は640万件弱）の両方の減少が含まれます。

- **Emotetの復活が続いています。**FBIと複数の国の捜査機関が昨年初めに、あるボットネット亜種のコマンド&コントロール（C2）インフラストラクチャを解体に追い込みましたが、トロイの木馬のEmotetやボットネットの検知数が多い状態が続いています。しかしながら、Emotetの検知数は2022年第1四半期以降に減少しています。

- **81%以上のマルウェアが暗号化に隠れています。**マルウェアが数年前からセキュアWebサイトで使用されているSSL/TLS暗号に隠れるようになっていると警告してきましたが、第2四半期はその傾向がさらに顕著になり、マルウェアの大半がTLS経由で到着するようになりました。最新の脅威をブロックするには、HTTPSの復号を有効にする必要があります。

- **半数以上（53.1%）のマルウェアがシグネチャ検知を回避**しますが、これらについても第1四半期から約4%減少し、第2四半期に3四半期連続でゼロデイマルウェア（シグネチャのないマルウェア）が減少しました。このタイプの回避型マルウェアがある程度減少したのは歓迎すべきことですが、それでもマルウェアの半数以上がシグネチャを回避していることになります。また、暗号化された接続で到着するマルウェアに限定すると、この数字は80%以上になります。マルウェアを暗号化して送り込む犯罪者の多くがシグネチャ検知も回避しようとすると推測されます。

- ソフトウェア脆弱性を悪用してマルウェアを送り込む**不正文書（Word、Excel、RTF）が引き続き確認**されています。本レポートでは、第2四半期に発見されたFollinaについて解説します。

- **EMEA（ヨーロッパ・中東・アフリカ）が引き続き最大の標的であり、**この地域のFireboxに合わせて正規化すると**マルウェアのヒット数の52%**を占めました。残りのマルウェアは、AMER（北米・中南米）とAPAC（アジア太平洋）にほぼ均等に分散し、APACが若干多くなりました。