本レポートの要点

第3四半期に、ネットワークマルウェアの検知数が全体として増加しました。未加工のマルウェア検知数は14%増加し、ウォッチガードの挙動検知サービスであるAPT Blockerによって阻止された高度な回避型の脅威は129%も増加しました。これに対し、暗号化された接続（TLS）経由で検知されたマルウェアは、過去2四半期と比較して大幅に減少しました。マルウェアに関する注目点として、Stackedと呼ばれる電子メールベースのドロッパファミリが10位までのマルウェアと5位までの暗号化されたマルウェアにいくつか入ったこと、中国のWebサイトが商品化されたアドウェアやパスワードスティーラを配布していたことなどが挙げられます。

第3四半期は第2四半期とは異なり、ネットワーク攻撃が大幅に増加しました。注目すべきは、リモートコード実行につながる可能性のあるMicrosoft Exchangeの重大な脆弱性であるProxyLoginで、これがネットワーク攻撃で首位になり、ネットワーク攻撃全体の10%を占めました。この重大な脆弱性にはかなり前にパッチが適用されているはずですが、適用されていないのであれば、これが警鐘になるはずです。

ネットワークベースのマルウェア検知と比較すると、エンドポイントマルウェアについては、少なくとも一意のマルウェア検知数が前四半期比で減少しました。これは必ずしもマルウェアの純粋な数の減少を意味するものではなく、第3四半期に検知された一意のマルウェア亜種の減少を意味します。ただし、ウォッチガードのエンドポイント製品が検知した侵害指標（IoC）の数はこの四半期に増加しました。配布ベクトルでは、スクリプトベースのマルウェアが引き続き首位になりましたが、数四半期前と比べると大幅に減少しました。しかしながら、Windowsファイルベースのマルウェア配布が増加して、僅差で2位になりました。いずれにしても、攻撃者は、不正スクリプトと悪用されることの多いWindowsファイルの両方を環境寄生型（LotL）手法に利用しています。一方の増加あるいは他方の減少のどちらかということになりますが、いずれにしても、多くの攻撃者がLotLマルウェアを配布するようになっていることを示しています。

以上は、本レポートで紹介する内容の一部に過ぎません。第3四半期のいくつかのハイライトを以下に示します。

- **ネットワークベースのマルウェアの合計検知数が14%増加し、**特にAPT Blockerサービスによるマルウェア検知が129%増と驚異的に増加したことは、高度な回避型のマルウェアが増加し続けていることを示しています。
- **それぞれのネットワークマルウェア検知サービスにおける「Fireboxあたりの」マルウェア検知の結果：**
  - **Fireboxあたりの平均マルウェア検知数の合計：1,343**（14%増）
  - **FireboxあたりのGAVによる平均マルウェア検知数：507**（2%減）
  - **FireboxあたりのIAVによる平均マルウェア検知数：474**（6%減）
  - **FireboxあたりのAPT Blockerによる平均マルウェア検知数：362**（129%増）
- 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3四半期のマルウェア検知は100,925,107**だったと推定されます。注意点として、この数はデータの共有に同意していただいたFireboxのみのものであり、これらは世界中のすべてのアクティブなFireboxの一部ではあるものの、実際にはこの数が大幅に大きいはずです。
- **エンドポイントランサムウェア攻撃が90%近く増加しました。**表面的には、エンドポイントランサムウェアの検知数が第3四半期に減少したように見えますが、マルウェア脅威の10位以内に初めて入ったMedusaランサムウェア亜種は、脅威ラボの自動シグネチャエンジンの汎用シグネチャによって検知されたものです。このMedusaの検知数を考慮すると、ランサムウェア攻撃は前四半期比で89%増加しました。
- 驚いたことに、**暗号化（TLS）に隠れるマルウェアの割合が、第3四半期に48%に減少**しました。数四半期にわたって増加が続いた後のこのトレンドは驚きではありますが、半数近いマルウェアが暗号化されたトラフィック経由で到着するため、暗号化されたトラフィックをスキャンすることを引き続き強くお勧めします。
- **ゼロデイマルウェアがマルウェア全体の69%を占めました。**ゼロデイマルウェアとは、シグネチャベースの防御を回避し、機械学習によるマルウェアモデルや挙動分析によってのみ検知されるマルウェアのことです。この割合が第2四半期より大幅に増加し、さらには、TLS経由で検知されたゼロデイマルウェアが76%に増加しました。
- **第3四半期に検知された5位までのTLSマルウェアのうちの4つが、電子メールベースのドロッパであるStackedでした。**Stackedが含まれていた、5位までの暗号化されたマルウェアのすべてではないものの、ある亜種は、一般的には請求書などの重要な文書の確認と称して、不正ファイルが添付された電子メールで到着します。Stackedの2つの亜種は、検知数でも10位までに入りました。
- **ネットワーク攻撃が前四半期比で16%増加しました。**
- **ProxyLoginが、第3四半期に最も多く試行されたネットワーク攻撃でした。**これは、Microsoft Exchange Serverのリモートコード実行の脆弱性で、かなり前にパッチが適用されているはずです。
- **ウォッチガードのエンドポイント保護製品は、10万台のマシンあたり171の一意のマルウェア亜種をブロックし、**第2四半期より83%も増加しました。

- **スクリプトマルウェアの配布が減少し続けている**のに対し、Windowsファイルなどの他のマルウェアベクトルが増加しています。
- **攻撃者が正規のリモート管理ツールを攻撃に利用するようになっています。**新たに上位に入ったフィッシングドメインの1つが、テクニカルサポート詐欺に利用され、事前に構成された不正バージョンのTeamViewerを被害者にダウンロードさせることで、攻撃者によるそのコンピュータの完全リモートアクセスを可能にすることがわかりました。

以上は、この四半期のレポートで紹介する内容の一部に過ぎません。四半期ごとの変化にこのようなパターンが見られる理由、注目すべき攻撃やマルウェアの詳細、そして何よりも、これらのトレンドに対する最善の防御のヒントを知りたいという方は、本レポートのこれ以降のセクションをぜひお読みください。