本レポートの要旨

この四半期は、マルウェア全体の件数が 2 四半期連続で減少するという、通常では考えられないトレンドが確認されました。しかしながら、この減少は間違いなく、コロナウイルスの感染爆発よって在宅勤務が増加し、会社のネットワークの境界の背後で働く時間が減少したことと関係しています。その一方で、**ウォッチガードが最近買収した Adaptive Defense 360** などのエンドポイントアンチマルウェア製品では、これほどの減少は確認されませんでした。また、この四半期に、高い回避能力を持つ脅威が大幅に増加しました。行動ベースの検知エンジンである APT Blocker で検知されたマルウェアが第 1 四半期より 12% 増加しましたが、これはシグネチャベースの検知を回避するマルウェア亜種の増加を意味するものであり、より高度な検知エンジンによる対策が必要です。

エクスプロイトという観点では、従業員がオフィスを利用しない状況にもかかわらず、ネットワーク攻撃が前四半期と比べて 6% 増加しました。これは、サーバやネットワークのワークロードが今なおクラウドやネットワークの境界の背後に置かれていることを意味しています。また、多くの従業員が VPN を利用し、これらのサービスをリモートで利用していると我々は見ています。

本レポートでは、これらの件数を始めとする高レベルの統計だけでなく、いくつかのマルバタイジングの脅威や巧妙なトロイの木馬も紹介します。さらには、フィッシングやその他の脅威を仕掛ける犯罪者が正規のドメインを悪用する例が引き続き確認されており、TLS 経由で拡散する新たなレベルのマルウェアも見つかりました。

2020 年第 2 四半期のこれ以外の注目すべきトレンドは以下の通りです。

- 境界で検知されたマルウェアが全体として前**四半期比で 8% 減少**しました。これは、ほとんどの従業員が今なお在宅勤務を継続しているためと考えられます。
- ウォッチガードのさらに高度なマルウェア検知エンジンである **APT Blocker** の検知は**前四半期比で 12% 増加**しました。これは、お客様を標的とするマルウェアがさらに高度化し、シグネチャベースの検知を回避するようになっていることを示しています。
- 今四半期は、TLS 経由で送り込まれるマルウェアが減少し、**暗号化された通信チャネルを使用するマルウェアは 34.2%** にとどまりました。
- **ゼロデイマルウェアの割合は引き続き高く、脅威全体の 67.2%** を占めました。
- Firebox が第 2 四半期にブロックしたマルウェアサンプルは、全体で 2,810 万件、**Firebox あたり平均 674 件弱**でした。
- **Gnaeus がこの四半期のマルウェアの首位に入っただけでなく**、上位のマルウェアが完全に入れ替わりました。Gnaeus は、この四半期のマルウェアの 20% を占め、イタリア、トルコ、米国の順にこのマルウェアの影響を大きく受けました。
- **有名なグレイウェアで Wi-Fi ハッキングツールである AirCrack が、マルウェアの上位に入りました。**このツールは、本来は侵入テストのツールではあるものの、犯罪者であるハッカーも様々な無線攻撃にこれを利用しています。
- ウォッチガードの不正侵入防止サービスは、**175 万件のネットワーク攻撃をこの四半期にブロックし、前四半期比 6% 増**を記録しました。これは、**Firebox 1 台あたり平均 42 件の攻撃**をブロックしたことになります。
- **Web アプリケーション攻撃はこの四半期も引き続き、最も広範囲に拡散したネットワーク攻撃でした。**
- **DNSWatchでは、cloudfront.net、sharepoint.com、verizonwireless.comなどの正規のサイトをサイバー犯罪者がマルウェアやフィッシング攻撃に利用する例が引き続き確認されました。**

本レポートでは、そのいくつかの例を詳しく解説し、対策のヒントも提示します。敵の行動を知り、どのように撃退するためのヒントを本レポートでご確認ください。