本レポートの要点

第3四半期にマルウェアとネットワークの件数はそれぞれ、3.4%と21%の減少を示しました。数四半期にわたって複数の製品で検知数が減少しましたが、この四半期に増加に転じました。この分野では減少トレンドが確認されたものの、エンドポイントでのマルウェア検知数は増加し、2020年通年の検知数を上回りました。

これまでと同様、かなりの割合のマルウェアが、暗号化された接続を経由して送り込まれました。これは、ウォッチガードのIPS（不正侵入防止サービス）で検知されるネットワークシグネチャに共通するトレンドです。このようなトラフィックが多くの場合に今もインスペクションから除外されていることがわかっています。そのため、ウォッチガードを始めとするセキュリティ業界の企業が、多層防御を採用しています。マルウェアの検知数が全体としては減少していますが、Fireboxあたりの平均検知数がこの四半期に増加しました。

2021年度第3四半期の脅威環境の概観は以下のとおりです。

- **GAV（Gateway AntiVirus）サービスとAPT Blockerサービスの間の境界で検知されたマルウェアの総数は約1,600万件で、**第2四半期から3.4%減少しました。マルウェアの件数は減少しましたが、Firebox 1台あたりの平均検知数は454となり、第2四半期の438から増加しました。
- **TLS経由で到着したマルウェアが接続全体の69.8%を占めました。**前四半期より減少しましたが、その割合が大きいことに変わりありません。IT管理者がこれらの到着する接続の暗号化の解除を検討しない限り、可視性のギャップは解消されません。
- **この四半期はゼロデイマルウェアの割合が67.2%になり、約3ポイント増加しました。**TLS経由のゼロデイマルウェアが、前四半期の31.6%から47%へと大幅に増加しました。
- XML.JSLoader亜種がこの四半期も、トラフィックが最多の暗号化マルウェアの首位に立ちました。**また、ヒット数が2位の亜種であるTearspearは、初めて上位に入ったダウンローダです。**
- ネットワーク攻撃の件数は2021年第1四半期をわずかに下回る水準に戻り、第3四半期に410万件弱のネットワークエクスプロイトがFirebox IPS（不正侵入検知・防御サービス）で検知されました。**2四半期連続で20%以上増加した後に、21%減少したことになります。**
- Fireboxあたりの平均検知数も件数と同様のトレンドを示し、2021年第1四半期の水準に戻りました。Fireboxアプライアンスあたり平均116件の攻撃がブロックされました。**第2四半期との比較で21%減少しましたが、第1四半期より3ポイント増加しました。**
- 5位までのIPS攻撃シグネチャは引き続き拡大しており、上位の標的である国の数も引き続き増えています。**この四半期はオーストラリアがこれに加わり、最も拡散した上位の攻撃の標的になった国が合計10か国となりました。**この国の数が四半期によって6～7の間で推移し、第2四半期は9か国でした。
- **DNSWatchが検知した不正ドメインへのアクセス数は560万件で、**前四半期から23%減少しました。前四半期の検知数は730万件でした。2020年第4四半期のブロックされたドメインが130万件だったことを考えると、大幅な減少とは言えません。
- **エンドポイント製品は2021年に、**2020年度通年の累計の10%増となる、**スクリプティング攻撃を起源とするマルウェアを**すでに処理しています。
- **この四半期末までのランサムウェア検知数も、すでに2020年度通年の検知数を超えています。**すでに2020年通年の105%であることから、次の四半期のデータを加算すると、件数がさらに増加すること予想されますが、105%のままである可能性も皆無ではありません。

以上の統計データを念頭に置いて、2021年度第3四半期のセキュリティレポートをお読みください。前四半期からの件数の増減に注目するのは重要なことですが、通年や前年比にも目を向ける必要があります。この四半期の活動を振り返り、今後のセキュリティ対策にとってのこれらの指標の意味を考えてみましょう。