本レポートの要点

この四半期のマルウェアのトレンドは、前回のレポートと対をなすものでした。2023年第4四半期に、ネットワークベースのマルウェア検知数が増加し、エンドポイントでのマルウェア検知数が減少したのに対し、2024年第1四半期に、ネットワークマルウェアの検知がほぼ半減（49%）しました。これに対し、エンドポイントマルウェアの件数は75%以上増加して、前回とまったく逆の結果になりました。

L前四半期に、ウォッチガードの挙動学習と機械学習を活用したアンチマルウェアサービスが検知した回避型マルウェアが増加しました。この四半期に、ウォッチガードの高度マルウェア検知の結果がすべて減少しましたが、シグネチャベースの検知数がネットワークとエンドポイントの両方の製品で増加しました。より高度な検知サービスを使用しないとマルウェアの半分以上を見逃すことになると何年も前から指摘してきましたが、この四半期は古き良きシグネチャベースの検知でそのほとんどが検知されました。

ネットワーク攻撃についてもほぼ同様で、前回のレポートでネットワーク攻撃が10%減少しましたが、この第1四半期に13%増加しました。前四半期は、攻撃者が試行した一意のネットワークエクスプロイト（攻撃のタイプがより多様であることを意味します）が多くなりましたが、この四半期は、一意の攻撃が16%減少しました。ただし、両方の四半期にいくつかの共通点もあります。ProxyLogon（リモートコード実行を可能にするMicrosoft Exchangeの重大な脆弱性）が引き続き、10位までのネットワーク攻撃の2位に入りました。以前も指摘しましたが、1年以上前にパッチを適用していない場合は、今すぐ適用することをお勧めします。

- **ネットワークベースのマルウェア検知数が、49%とほぼ半減しました。**これが驚きであるのは、80%上昇した前四半期と明らかに正反対であるためです。また、APT BlockerとIntelligentAV（IAV）のすべてのプロアクティブアンチマルウェアサービスによるマルウェア検知数も大幅に減少しました。わずかに増加したのは、シグネチャベースのGateway AntiVirus（GAV）サービスだけです。しかしながら、暗号化された接続経由で検知されたマルウェアの数は増加しました。
- 一方で、エンドポイントマルウェア検知数は**大幅に増加し、前四半期比で75%以上も増加**しました。これは、ある程度は納得できることです。ネットワークで検知されるマルウェアが少なければ、エンドポイントでより多くの脅威を目にすることになるからです。
- **暗号化（TLS）に隠れるマルウェアの割合が、第1四半期に69%に増加しました。**繰り返しになりますが、HTTPS Webトラフィックを復号しない限り、ネットワーク経由のマルウェアの半分以上を見逃すことになります。これは無料で有効にして利用できる機能です。
- 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は以下のとおりです。
  - **Fireboxあたりの平均マルウェア検知数の合計：1,224**（約49%減）
  - **FireboxあたりのGAVによる平均マルウェア検知数：562**（8%増）
  - **FireboxあたりのIAVによる平均マルウェア検知数：587**（58%減）
  - **FireboxあたりのAPT Blockerによる平均マルウェア検知数：75**（85%減）
- ウォッチガードへの報告に同意していただいた、現在アクティブである（ライセンスされている）すべてのFireboxでいくつかのサービスをご利用いただき、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、**2024年第1四半期のマルウェア検知は、5億件に迫る472,991,544**だったと**推定**されます。
- **第1四半期に、ゼロデイマルウェアがマルウェア全体に占める割合が36%に低下しました。**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、よりプロアクティブな手法によってのみ検知されるマルウェアのことです。これまではゼロデイマルウェアの割合がはるかに大きく、50%以上でした。長い間、これほど下落したことはありませんでした。前四半期にはシグネチャベースの検知が多く検知されたことになりますが、よりプロアクティブなアンチマルウェアサービスをお勧めすることに変わりありません。
- オープンソースのAndroid OSを搭載するスマートテレビを標的にする**Pandoraspearボットネットが最も広範囲で検知された10位までのマルウェア**に入ったことは、企業のセキュリティにおけるIoTデバイスの脆弱性の潜在的なリスクを強調するものです。
- TP-LinkのArcherデバイスを標的にするマルウェアであるMiraiファミリの新しい亜種が、この四半期に最も広範囲で確認されたマルウェアキャンペーンの1つとして登場しました。この**Mirai亜種は、世界中のFireboxの約9%で観察されました。**
- **ネットワーク攻撃が、前四半期比（QoQ）では13%増加**しましたが、前年同期比（YoY）では大幅に減少しました。一方、攻撃者が使用するネットワークエクスプロイトの多様性を示す一意のネットワーク攻撃は16%減少しました。
- **HAProxyの脆弱性が、この四半期のネットワーク攻撃の上位に入りました。**HAProxyは、Linuxベースのロードバランサアプリケーションです。2023年に最初に特定されたこの脆弱性は、人気のソフトウェアの脆弱性がいかに広範囲のセキュリティ問題につながるかを示しています。
- **ProxyLogonは引き続き、第1四半期に悪用された上位の攻撃の2位になりました。**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が、今も2位を維持しています。
- **ネットワーク攻撃の検知数の10位までのエクスプロイトが、全検知数の57%を占めました。**これらの脆弱性がこのような割合であることから、攻撃者（およびペネトレーションテスタ）がインターネットでスパムを送信していることがわかります。

- **エンドポイントマルウェアの純粋な検知数が75%以上も増加**し、前四半期より大幅に増加しました。おそらくこのように増加したのは、ネットワークベースのマルウェア保護が減少したためです。
- **ウォッチガードのエンドポイント保護製品がブロックした一意のマルウェアの数は10万台のマシンあたり88**にとどまり、2023年第4四半期との比較で18%以上減少しました。ただし、これは感染数とは関係なく、マルウェアの確実に一意である、場合によってはシグネチャベースの保護を回避することもある、新しい亜種の数です。マルウェア検知数が増加した一方で、マシンあたりの一意の亜種が減少した場合、攻撃者が多くの被害者に古い亜種のマルウェアをスパムで送信している可能性を示しており、そうであれば、シグネチャベースの手法で容易に検知されます。
- **エンドポイントランサムウェア攻撃が引き続き減少し、23%近く減少しました。**最近、ランサムウェアの増加に歯止めがかかっているようです。おそらくは、捜査機関がLockbitなどの多くのランサムウェアグループを解体したことが、この減少につながっています。これらの亜種は解体されたものの、いずれは復活することが予想されます。
- この四半期に、**Webブラウザやプラグインに対する攻撃を起点とするマルウェア全体の4分の3以上（78%）がChromiumベースのブラウザから生成され、**前四半期（25%）から大幅に増加したことがわかりました。
- **不正スクリプトは、最も広範囲で確認されたマルウェア配布ベクトルとして減少し続けています。**PowerShellとJavaScriptの不正スクリプトがマルウェアを配布する最も一般的なLotL（環境寄生）手法であることに変わりありませんが、Windowsバイナリの増加に伴い、その数が引き続き減少しました。
- **DarkGateは、悪意のAWSと偽のAkamaiのサブドメインを利用して被害者を誘導します。**忘れてならないのは、正規のドメインであっても、顧客が危険なサブドメインを作成できる場合もあるということです。それと同時に、攻撃者は依然として、正規のドメインに似たドメインも執拗に悪用しようとしています。

この四半期の以上のハイライトを以降のセクションで詳しく解説します。ここで忘れてならないのは、本レポートは、これらの攻撃トレンドを興味本位で紹介するものではなく、実用的な防御のヒントと戦略を解説するものだということです。