要旨

このパンデミックが始まってから見られていたネットワークマルウェアや攻撃のトレンドは、2020年第4四半期も継続しました。オフィスの保護境界で検知されるマルウェア数は非常に少なくなっています。これは多くの従業員がテレワークをしていることからも理解できます。しかし、企業の保護境界では記録的な数のネットワーク攻撃やIPSの検知が見られています。マルウェアに感染させるためのフィッシングなどの電子メール攻撃はテレワーク環境へと攻撃の矛先を変えた一方で、サイバー犯罪者は私たちがオフィスにネットワークやリモートアクセスサービスを導入していることにも気付いています。実際、このパンデミックの発生当初は、新たなリモートワークの要件に対応するために、さまざまなネットワークサービスを導入したのではないでしょうか。つまり、リモートで勤務する従業員を保護するためにはエンドポイントプロテクションが必要ですが、オフィスやクラウド上のすべてのネットワークサービスを保護するために、ネットワークを防御する機能も維持しなければならないのです。

ネットワークで検知されるマルウェアの数は減少傾向にありますが、一方でテレワーク環境のエンドポイントを攻撃するマルウェアは増加しています。**ウォッチガードが新たに買収した**Adaptive Defense 360は、2020年にも膨大な数のマルウェアを検知しブロックしてきました。本四半期のレポートではこれらのエンドポイントマルウェアのトレンドについても説明します。エンドポイントで検知されるマルウェアの中では、ランサムウェアの亜種が減少しています。この原因は、多くのランサムウェアが標的型になっていることと考えられますが、ファイルレスマルウェア、つまり環境寄生型（Living-Off-the-Land）の脅威は888%も増加しました。ネットワークで検知されるマルウェア数が減少しているからといって、決して油断することはできません。むしろ、在宅で勤務する従業員を確実に保護するために、エンドポイントの保護機能を多層化する必要があります。

これらのトレンドの他に注目すべき点として、第4四半期にはゼロデイマルウェア（シグネチャベースの防御を回避するマルウェア）が大幅に増加し、マルウェア全体の61%以上を占めたことがあります。また、暗号化されTLS通信を悪用する脅威は約62%に増加しました。過去のレポートでも述べたように、サイバー犯罪者は、このパンデミックにより攻撃の矛先を変更しているにもかかわらず、攻撃をさらに高度化し、従来型の防御を回避するようになっています。

本レポートでは、ファイルレスマルウェアが増加している状況の詳細、IoTやコンシューマ向けルータを攻撃するトロイの木馬「The Moon」、クリプトマイナーの復活、攻撃に悪用されている上位のドメインの最新のリストなど、他の多くの有用な情報を網羅しています。

2020年第4四半期の重要事項は以下の通りです。

- 前四半期との比較で境界で検知される**マルウェア全体が4%減少**しました。これは、新型コロナウイルスのパンデミックにより多くの従業員がテレワークをするようになったことが原因だと考えられます。
- 悪意のあるファイルの**61%以上**が、シグネチャベースの保護機能では検知されないゼロデイマルウェアでした。前四半期に比べてゼロデイマルウェア数は**11ポイント上昇**しました。
- 暗号化されたチャネルから配信されるマルウェアはわずかに減少しました。**TLSを使用するマルウェアは47%**でした（第3四半期と比較して7ポイント減少）。減少はしていますが、これらのマルウェアは通常のマルウェアよりも高度である傾向があり、**61%以上がゼロデイマルウェア**になっています。
- 全体として、第4四半期に**Fireboxがブロックしたマルウェアのサンプル数は2,060万件**であり、Firebox1台あたりの平均では456件でした。
- **ネットワーク攻撃とユニークエクスプロイトの検知数はこの2年間で見た場合高水準になりました。**ネットワーク攻撃は第4四半期に349万件以上に急増し、ネットワーク攻撃のユニークシグネチャ数は**第4四半期に4%弱**増加しました。これは、サイバー犯罪者が依然として、さまざまなネットワークエクスプロイトを使用して企業を標的としていることを示しています。
- 2020年第4四半期、Fireboxアプライアンスの侵入防止サービス（IPS）は、アプライアンス1台あたり**平均77件の攻撃**をブロックしました。
- 全体の件数は増加しましたが、**アジア太平洋（APAC）地域を標的としたネットワーク攻撃は16ポイント減少**し、AMERとEMEAにおける攻撃数が増加しました。
- 第4四半期中、**DNSWatchは合計1,313,686件の悪意のあるドメインへの接続をブロック**しました。
- ファイルレスマルウェアの攻撃が急増しています。WatchGuard Panda製品の1年間のエンドポイント脅威インテリジェンスによると、**2020年のファイルレスマルウェアの発生率は、2019年に比べて888%増加**しました。
- **ランサムウェアのユニークペイロードの数（ボリュームではない）は減少傾向にあり、2020年には48%以上減少**しました（2019年の4,131件であったユニークペイロード数が2,152件に減少）。ランサムウェアのボリュームの減少傾向は、攻撃者がこれまでは不特定多数を標的としていた広範囲な攻撃キャンペーンから、医療機関や製造業などに的を絞った高度な標的型攻撃へと移行していることを示しています。
- **クリプトマイナーは2019年には小康状態でしたが、2020年に再び増加傾向になりました。ユニーク亜種が前年同期比で25%以上増加**し、2020年にはユニーク亜種が850件に達しました。
- 第4四半期には、**「The Moon」（Linux.Genericウイルス）がウォッチガードの10位以内のマルウェアに登場**しました。これは、LinuxベースのIoTデバイス、NASサーバ、LinksysやSeagateなどのコンシューマグレードのルータを直接標的としています。
- 新しいトロイの木馬（Trojan.Script.1026663）は、多段階のインストール方式で電子メールスキャナを騙します。

ここでは、今期のレポートの一部のハイライトを紹介したに過ぎません。各セクションでは、Panda Securityソフトウェアによるエンドポイントの脅威についての初の年間の分析結果などの詳細情報が掲載されています。このレポートでは、有用な詳細情報と、自社をサイバー攻撃から保護するための多くの戦略やヒントを紹介しています。