本レポートの要点

冒頭で述べたように、第 1 四半期のネットワーク攻撃やマルウェアの全体としてのトレンドは、パンデミックが続いていた他の四半期から大きな変化はなく、ネットワークマルウェアが全体として減少し、エンドポイントマルウェアが増加しました。ネットワーク攻撃は、パンデミックが始まって以降、四半期ごとに増加しています。マルウェアは当然ながら在宅勤務のユーザを標的にしますが、ネットワークエクスプロイトは引き続き、オフィスやクラウドに置かれたサーバを標的にします。

トレンドは繰り返すものですが、新たな脅威も確認されました。例えば、ゼロデイマルウェア、すなわち、最初の数日間はシグネチャベースで検知されないマルウェアが過去最高となる 74% に上昇しました。これは、シグネチャベースの 保護では第 1 四半期にマルウェアの 4 分の 3 近くを検知できなかったことを意味します。プロアクティブなマルウェア防止を採用しない限り、大量のマルウェアが従来の防御を回避することになるでしょう。フィッシング攻撃が急増したことで、DNSWatch サービスでブロックされた不正ドメインの数も大幅に増加しました。

本レポートでは、ProxyLogin ゼロデイの詳細、IoT デバイスを標的にして拡散した Linux マルウェアファミリ、巧妙に仕掛けられた XML スクリプトで拡散するファイルレスの脅威などについて解説します。

2021年第1四半期の脅威環境の要点を以下に示します。

- **ゼロデイマルウェアが第 1 四半期に 74% と過去最高を記録しました。**すなわち、シグネチャベースの保護だけではマルウェアの 4 分の 3 近くを検知できず、今日の脅威からの保護を可能にするには、プロアクティブなマルウェア検知が必要です。ゼロデイマルウェアとは、ポリモーフィックで回避能力のある、初めて確認された日（ゼロデイ）にはシグネチャベースの保護機能を回避してしまうマルウェアのことです。
- 全体として、**第 1 四半期に境界のマルウェア検知数は 16%減少し**、1,720 万件となりました。ただし、報告対象の Firebox の減少を差し引いて考える必要があり、**Firebox あたりで見ると、平均 461 のマルウェアが検知され、検知数は 1 ポイントと若干ながら増加しました。**
- **Ursu、Trojan.IFrame、XML.JSLoader、Zmutzy、Zum.Androm の 5 つの新しいマルウェアファミリがマルウェアの検知数の 10 位以内に入り**、新しいマルウェアサンプルがかなり多様化した四半期になりました。
- **暗号化された接続で送信されるマルウェアが、第 1 四半期に 44%弱に減少しました。**これは、2020 年第 4 四半期と比べると 3 ポイント、第 3 四半期と比べると 10 ポイントの低下です。
- 過去には、暗号化された接続で送り込まれるゼロデイマルウェアがこれより多かったこともありましたが、第 1 四半期に**暗号化された接続で拡散するマルウェアに占めるゼロデイマルウェアの割合が 60.3%で**、これは、この四半期のゼロデイマルウェア全体の割合より少ない数字です。
- **ネットワーク攻撃の件数が過去 3 年で最高を記録しました。**ネットワーク攻撃の **IPS ヒット数が第 1 四半期に 420 万以を記録しました。**報告対象のデバイスが 17% 減少したことを考えると、このネットワーク攻撃の件数はさらに注目に値します。
- 2021 年第 1 四半期に Firebox アプライアンスの IPS（不正侵入検知・防御サービス）はアプライアンスあたり平均 113 の攻撃をブロックし、前四半期比で 47%の大幅な増加となりました。
- **アジア太平洋地域で確認されたネットワーク攻撃は、約 3%に過ぎません。**北米・中南米とヨーロッパ・中東・アフリカのネットワーク攻撃の件数はほぼ同じですが、Firebox あたりで換算すると、**北米・中南米のデバイスでは他の地域より少なくとも 2.6 倍の攻撃が確認されています。**
- **DNSWatch は第 1 四半期に 500 万以上の不正ドメインをブロックしました。**2020 年第 4 四半期に比べて 281%という大幅な増加であるだけでなく、報告対象デバイスが 17%減少したにもかかわらず、このような高さであったことは、特に注目に値します。
- 不正スクリプト（今期は XML に見つかりました）が、ファイルレスマルウェアの拡散方法として引き続き使われています。
- 10 位以下まで範囲を広げると、Linux.Ngioweb.B という、一般ユーザ向けデバイスを感染させて IoT のボットネットに組み込む別の Linux の脅威も見つかります。
- **ProxyLogin Exchange Server の深刻度の高い脆弱性を狙うエクスプロイトが、3 月 24 日（IPS へのアクセスが開始された日）から 3 月末に 1,600%以上増加**しました。これらの脆弱性の修正から時間が経過していますが、パッチを適用していないと、侵害されていることが予想されます。これらの脆弱性の詳細については、この四半期の主な出来事をお読みください。

以上が、第1四半期の脅威環境の概要です。これらのトレンドの詳細と、いくつかの脅威やネットワークに侵入して被害者を感染させる方法や手法について、本レポートの以降のセクションで解説します。