エグゼクティブサマリー

第 1 四半期には、データを報告する Firebox の台数が増加しているにもかかわらず、記録的なマルウェア数が報告された 2019 年第 4 四半期と比較して、全体的にマルウェアは減少しました。このわずかな減少は、企業が 3 月上旬からテレワークへと業務形態を移行せざるを得なくなったことに関連している可能性があります。マルウェアは、組織のユーザーの自宅の作業環境も標的としています。マルウェアは前年比では増加しており、64% 以上のマルウェアが従来型のシグネチャベースの防御を回避しています（このようなマルウェアはゼロデイマルウェアと呼ばれます）。今四半期の最大のニュースは、暗号化されたネットワークトラフィックを使用して、多くのマルウェアがセキュリティコントロールを回避していることです。HTTPS トラフィックなど TLS 接続を復号化するように設定された Firebox で、マルウェアの一部を分析したところ、マルウェアの 3 分の 2 以上が暗号化されたチャネルから配信されていることが明らかになりました。暗号化された Web 接続を復号化し、スキャンしなければ、多くのマルウェアが見過ごされる恐れがあります。本レポートでは、新しく明らかになったこの暗号化チャネルの問題の他に、関連するマルウェア検体のいくつかを詳しく取り上げます。また、最も多いネットワーク攻撃と悪意のあるドメインについて説明し、新型コロナウイルス（COVID-19）に関連するいくつかのサイバー攻撃についても説明します。

2020年第1四半期のハイライトは以下の通りです。

- **マルウェアの 67% は、暗号化された通信チャネルを使用しており、**TLS トラフィックを復号化してスキャンするアプライアンスで検出されました。HTTPS を復号化してコンテンツを検査していない場合、組織に侵入するマルウェアの 3 分の 2 を見逃している恐れがあります。

- **ゼロデイマルウェアは、TLS を復号化しない Firebox で検出された全脅威の 63.7% を占めました。**しかし、**TLS トラフィックを復号化してスキャンする Firebox ではこの割合は 72%** に上昇します。これは、サイバー犯罪者が暗号化によって攻撃を隠蔽しているだけでなく、これらの暗号化されたチャネルを介して、高度なマルウェアを展開している傾向があることを示しています。

- 全体では、**第 1 四半期に Firebox がブロックしたマルウェアの検体数は 3,120 万であり、**昨年の第 4 四半期に比べてわずかに減少しています。**1 台の Firebox あたりのマルウェア検体数は 730 個以上**になっています。

- ユーザーから認証情報を盗み出す**トロイの木馬「Cryxos」**が復活しています。

- **グレイウェアのリモートデスクトップ製品である Ammyy Admin が、ウォッチガードのマルウェアの上位リストに入りました。**従業員にテレワークをさせる場合、安全ではないリモートデスクトッププログラムに注意してください。

- 第 1 四半期、**Firebox は 166 万件のネットワーク攻撃をブロックしましたが、**これは Firebox1 台あたりでは約 38 件の攻撃数になります。これは前四半期に比べてわずか **19% 減少**したことになります。

- 第 1 四半期の**ネットワーク脅威の第一位は SQL インジェクション攻撃となり、2 四半期連続でした。**

- **Bellsyscdn[.]com は、**Bondat ワームの C&C、Monero クリプトマイニング、WordPress 関連の攻撃をホスティングしており、**今四半期にブロックされたマルウェアドメインの半分以上を占めました。**

- **DNSWatch では、多くの暗号化関連の攻撃を確認しブロックしました。**Monero クリプトマイニングに関連する 6 つのドメインが上位リストに入りました。

これらがレポートのハイライトです。では、今後影響を受ける可能性が高い脅威を詳しく見ていきましょう。本レポートの最後までご覧いただくと、現在のサイバー脅威の全容を把握でき、組織を守るためのアドバイスをご確認いただけます。