2021年3月9日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2020年 年間のマルウェアレポートを公開
～暴露型ランサムウェアの攻撃事例と Emotet の観測状況を解説～

キヤノンマーケティングジャパン株式会社（代表取締役社長：坂田正弘、以下キヤノン MJ）は、2020年の国内マルウェア検出状況に関する年間レポートを公開しました。本レポートでは、2020年に検出されたマルウェア、および発生したサイバー攻撃事例について解説します。

キヤノン MJ グループはセキュリティソリューションベンダーとして、サイバーセキュリティに関する研究を担うサイバーセキュリティラボを中核に、最新の脅威やマルウェアの動向の情報収集および分析を行い、セキュリティ対策に必要な情報を「マルウェアレポート」として定期的に発行しています。このたび、2020年に国内で検出されたマルウェアおよび発生したサイバー攻撃事例について解説した年間レポートを公開しました。

2020年 年間マルウェアレポート＜https://eset-info.canon-its.jp/malware_info/trend/detail/210309.html＞

＜トピック＞

■ 2020年年間マルウェア検出統計

2020年に国内で検出されたマルウェアの多くは Web ブラウザー上で実行される脅威で、検出数上位10種のうち8種を占めており、JS/Adware.Subprop が最多でした。

マルウェア以外のネットワーク攻撃では、新型コロナウイルスの影響でリモートワークが増加し、それに伴いリモートデスクトッププロトコル（RDP）を狙ったブルートフォース攻撃（総当たり攻撃）を検出する Incoming.Attack.Generic が最多となりました。

■ 特定の組織を標的にする暴露型ランサムウェアの攻撃事例

2020年もランサムウェアによる攻撃が多く確認された中、攻撃の対象が不特定多数から特定かつ規模の大きい組織へ標的が絞られ、それに伴い身代金の要求額も増加しています。

2020年4月頃初めて確認された Ragnar Locker は暴露型ランサムウェアと呼ばれ、その中でも被害件数が多く、6月～12月の間に少なくとも22組織の機密情報を取得・公開したと攻撃者グループは主張しています。

■ Emotet の継続的な活動とさらなる攻撃手法の巧妙化

2020年もマルウェア Emotet は多数検出されました。9月以降、アンチウイルスベンダーのサポートセンターを装う事例など、Emotet の感染を狙うばらまき型メールに新しいテンプレートが確認されました。本レポートでは、他2件の事例や Emotet への対策について解説しています。

■ 継続的に検出される VBA で作成されたダウンローダーの主流テクニック

ローカル環境で動作するマルウェアで最も多く検出された VBA/TrojanDownloader.Agent は、近年継続的に多く検出されています。本レポートでは、侵入経路やダウンロードサーバーと通信するまでの挙動、検出回避や解析妨害の機能と対策について解説しています。

● マルウェア情報局ホームページ：https://eset-info.canon-its.jp/malware_info/

● ニュースリリースホームページ：canon.jp/newsrelease ● ESETホームページ：https://eset-info.canon-its.jp/

＜2020年 年間マルウェアレポートの主な内容＞

■ 2020年年間マルウェア検出統計

国内、全世界ともに最も多く検出されたマルウェアである JS/Adware.Subprop は、偽の Adobe Flash Player のアップデートや有名ベンダーの Web バナーを悪用し、悪意のあるコンテンツや不要なソフトウェアを配布するスクリプトの検出名です。

マルウェア以外のネットワーク攻撃で最も多く検出された Incoming.Attack.Generic は、RDP のデフォルトのポート番号である「3389」以外のポートを狙ったブルートフォース攻撃です。RDP や SMB などの通信プロトコルに対するブルートフォース攻撃などの検出以外に、通信プロトコルの脆弱性を悪用した攻撃も検出されています。2020年は RDP 経由で侵入した PC に対してランサムウェアを感染させる事例も確認されており、メールの添付ファイルによる感染と異なり、感染するまで気づきにくいと考えられています。

■ 特定の組織を標的にする暴露型ランサムウェアの攻撃事例

従来のランサムウェア攻撃は不特定多数に対し、ばらまき型メールで侵入しファイルの暗号化によって数万円の身代金を要求するものでした。しかし、特定の組織に対し巨額の身代金を払わざるを得ない状況を作り出す「人手によるランサムウェア攻撃」と「二重の脅迫」と呼ばれる新しい2つの手法が増加しており、IPA（情報処理推進機構）は注意喚起を行っています。サーバーへの不正アクセスを利用して組織に侵入（人手によるランサムウェア攻撃）し、暗号化する前の窃取した機密情報を公開すると脅迫（二重の脅迫）することで、数百万円～数億円の身代金を要求する攻撃事例が確認されています。

二重の脅迫を用いるランサムウェアは暴露型ランサムウェアと呼ばれています。その一つである Ragnar Locker は特に被害が多く、特徴の一つに攻撃の隠密性の高さが挙げられます。2020年5月の攻撃事例では、攻撃プログラムに埋め込まれた仮想化ソフトウェア VirtualBox のイメージを展開し、VirtualBox 上（ゲスト OS）のランサムウェアがホスト OS 上のファイルを暗号化することで、セキュリティソフトウェアによる検出を巧みに回避しています。

■ Emotet の継続的な活動とさらなる攻撃手法の巧妙化

Emotet はモジュールやほかのマルウェアをダウンロードし、情報窃取などを行うマルウェアで、主要な感染経路は電子メールです。メールに添付されたダウンローダー（多くが Microsoft Office 形式のファイル）が Emotet をダウンロード・実行することで感染します。

2020年9月以降、Emotet への感染を狙ったばらまき型メールにいくつか新しいテンプレートが確認されました。

9月上旬にはアンチウイルスベンダーのサポートセンターを装ったメールが観測されています。この手法には、実在するアンチウイルスベンダーの名前を使用することで、ユーザーの警戒心を解く狙いがあると考えられます。

9月下旬にはパスワード付き ZIP ファイルが添付されたメールが確認されました。この手法を用いた攻撃者の狙いとして、セキュリティ製品による検知を回避できること、さらには国内企業ではパスワード付き ZIP ファイルの利用が習慣化していて、警戒心を持たずに展開するユーザーが多いと考えられることの2点が挙げられます。

10月中旬にはアップデート通知を装う Word テンプレートを用いて、ユーザーのクリックを誘導する攻撃が確認されました。

■ 継続的に検出される VBA で作成されたダウンローダーの主流テクニック

VBA/TrojanDownloader.Agent は Microsoft Office 製品で利用されるプログラミング言語の VBA（Visual Basic for Applications）で作成されたダウンローダーで、Emotet の感染を狙った攻撃にも使用されています。VBA/TrojanDownloader.Agent の主な侵入経路はメールで、ばらまきメールの添付ファイルとなっていることが大半です。添付ファイルを実行すると Microsoft Office がデフォルトで設定している保護機能を解除させるための画像や文章が表示されます。ユーザーが文章の指示通りに「コンテンツの有効化」をクリックすると、マクロが実行され、最終的に攻撃者が目的とするマルウェアがダウンロードされます。

このダウンローダーはセキュリティ製品による検出の回避、解析者による解析の妨害の機能を複数保有しています。本レポートでは4つの主流テクニックを紹介しています。1つ目はVBAコードを解析者が閲覧できないように、コードにパスワード保護を施したり、プロジェクトにロックをかけたりする「パスワード保護」、2つ目はシグネチャベースのセキュリティ製品による検知を回避したり、解析に時間がかかるようにしたりするため不要な処理を記述した「ダミーコード」、3つ目はセキュリティ製品による検知を回避したり、解析者による解析を遅らせたりする「難読化」、4つ目は解析環境と検知するとダウンロードサーバーとの通信は行わず、処理を終了させる「解析環境の検知」です。