2019年2月26日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2018年年間マルウェアレポートを公開
～国内外の政府機関や重要インフラを狙う APT 攻撃を解説～

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、2018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、2018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紹介します。

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マルウェアラボを中核に、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、2018年に検出されたマルウェアについて分析した年間レポートを公開しました。

2018年年間マルウェアレポート＜https://eset-info.canon-its.jp/malware_info/trend/detail/190226.html＞

＜トピック＞

■ 2018年マルウェア検出統計

2018年に国内で最も検出されたマルウェアは VBA/TrojanDownloader.Agent で、マルウェア検出数全体の12.1％を占めており、他の国々と比較して日本国内における検出数が際立って多いことが特徴です。JS/Adware.Agent や HTML/FakeAlert が続いて多く検出されています。

■ 不特定多数を狙ったメール攻撃

2018年も不特定多数を狙った多くのメール攻撃を確認しました。iqy ファイルを悪用した攻撃手法、画像ファイルにデータを隠蔽する「ステガノグラフィー」を用いた攻撃手法、Word 文書内にコマンドを隠蔽する攻撃手法について解説します。有名企業になりすましマルウェア感染を狙うメールや、セクストーション（性的脅迫）などの脅迫メールについても紹介します。

■ 政府機関や重要インフラを狙う APT（Advanced Persistent Threat）攻撃

APT とは高度で持続的な脅威のことで、攻撃に使われるマルウェアや手法が高度で攻撃活動が長期間にわたる点で通常のサイバー攻撃と区別されます。政府機関など機密性の高い情報を保持する組織や、インフラ事業者が標的とされることが多く確認されています。本レポートでは2018年に活動が確認された APT グループ「APT10」と「Turla」を紹介します。

■ Web 上で動作するアドウェアが増加

アドウェアは Advertising Software の略語で、広告を表示させる機能を持つソフトウェアです。意図しないタイミングでの広告表示、ブラウザーのホームページ変更、デスクトップやブラウザーにツールバーを追加させるような迷惑行為を行うアドウェアは、2018年国内において多く観測されました。

■ サイバーセキュリティを支える技術「マルウェア解析」

マルウェアは、現在、多くのサイバー攻撃で使用され、サイバー犯罪者にとって攻撃インフラの一つとなっています。サイバー攻撃で使用されているマルウェアを解析し、動作を明らかにすることは、サイバー攻撃の全容を解明する上で重要な要素です。本レポートでは3つのマルウェアの解析手法「表層解析」、「動的解析」、「静的解析」について紹介しています。

● 一般の方のお問い合わせ先 ：ESET サポートセンター　050－3786－2528
● 報道関係者用ホームページ ：canon.jp/newsrelease ● ESET ホームページ：https://eset-info.canon-its.jp/

＜2018年年間マルウェアレポートの主な内容＞

■ 2018年マルウェア検出統計

2018年に国内で最も検出されたマルウェアはVBA/TrojanDownloader.Agentです。マルウェア検出数全体の12.1％を占めており、他の国々と比較して、日本国内における検出数が際立って多いことが特徴です。JS/Adware.Agent（全体の9.6％）、HTML/FakeAlert（全体の6.3％）がそれに続きます。

VBA/TrojanDownloader.AgentはMicrosoft Office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型のマルウェアです。ファイル形式はMicrosoft Excel文書（拡張子.xls/.xlsm等）あるいはMicrosoft Word文書（拡張子.doc/.docm等）であることが大半です。一般的にばらまき型のメールに添付されることで配布拡散されます。

JS/Adware.AgentはWebブラウザー上で不正な広告を表示するJavaScriptです。国内では、7月下旬以降に検出数が急増しています。

HTML/Fakealertは偽の警告文を表示するスクリプトの検出名です。「Windowsセキュリティシステムが破損しています」等の偽警告メッセージを表示し、PC修復ツールと称したソフトウェアをユーザーに購入させようとします。

世界全体では、JS/CoinMiner（全体の6.0%）やJS/Adware.Agent（全体の5.8％）が多く検出されています。

■ 不特定多数を狙ったメール攻撃

マルウェア情報局では、2018年に、数点のマルウェアを添付したばらまき型メールを紹介しました。このようなメールに添付されているマルウェアは、ほとんどがダウンローダーです。ダウンローダーを実行すると別のマルウェアをダウンロードし、実行します。本レポートでは8月に紹介した「iqyファイルを悪用した攻撃手法」、10月に紹介した「ステガノグラフィーを用いた攻撃手法」、そして11月後半以降多く観測されている「オブジェクト内にコマンドを隠蔽する攻撃手法」についてそれぞれ紹介します。

10月に攻撃が確認された、画像ファイルにデータを隠蔽する「ステガノグラフィー」という攻撃手法では、画像ファイルをダウンロードするExcelファイルを添付したメールがばらまかれました。Excelのマクロが実行されると、攻撃者の用意したサーバーから画像ファイルをダウンロードされます。この画像には、ステガノグラフィーが使用され、PowerShellスクリプトが隠蔽されており、攻撃者の用意したサーバーからバンキングマルウェアをダウンロードし、感染させる処理が記載されています。

2018年に確認されたマルウェア付きのメールの多くはExcel文書形式のダウンローダーでしたが、11月後半からはExcel文書形式ではなく、Word文書形式のダウンローダーを複数確認しています。このWord文書形式のダウンローダーは、マクロのコード内ではなく本文中のオブジェクト内にコマンドを隠蔽しています。

■ 政府機関や重要インフラを狙うAPT攻撃

APT攻撃は2009年に発生した大手IT企業への攻撃（Operation-Aurora）や2010年のStuxnetを用いたイランの核燃料施設への攻撃をきっかけとして、その脅威が広く知られるようになりました。国内における代表的な事例としては、2011年の重工メーカーに対する攻撃や2015年の日本年金機構に対する攻撃が挙げられます。さらに2015年と2016年にはウクライナの送電施設に対する攻撃の結果、首都キエフで停電が発生しました。このようにAPTによるサイバー攻撃の被害はインターネット上だけに留まらず、現実社会にも大きな影響を与えています。

本レポートでは日本の組織を継続的に攻撃しているAPTグループ「APT10」と米国や欧州を中心に活動するAPTグループ「Turla」を紹介します。

■ Web 上で動作するアドウェアが増加

国内アドウェア検出数は前年比で264% も増加しました。アドウェアはローカル環境上で動作するもの（ファイル形式：Win32, OSX, etc.）と Web 上で動作するもの（ファイル形式：JS, HTML, etc.）の2種類があります。

2018年に国内で観測されたアドウェアのうち、ローカル環境上で動作する Win32は減少しました。一方で、Web 上で動作するものは大幅に増え、これに起因してアドウェア全体の検出数が増加したことがわかります。

2018年に多く確認されたアドウェアによる広告は、偽のセキュリティ製品を宣伝するものです。ユーザーの端末にセキュリティの問題がないにもかかわらず、問題が確認されたことを通知し、偽のセキュリティ製品のダウンロードを推奨してきます。

■ サイバーセキュリティを支える技術「マルウェア解析」

2018年に新しく発見されたマルウェアの数は、1億3750万件に上り、依然として多くの新しいマルウェアが発見されています。

また、2018年上半期マルウェアレポートで紹介したように、ダークウェブやディープウェブ上の“Crime as a Service”（CaaS）では、日々新しいマルウェアが開発されており、技術力のないサイバー犯罪者でもマルウェアを簡単に利用することができます。マルウェアは、サイバー犯罪者にとって、なくてはならない攻撃インフラの一つとなっています。

多くのサイバー攻撃に使用されているマルウェアを解析し、動作を明らかにすることは、サイバー攻撃の全容を解明する上で非常に重要な要素です。たとえば、情報システム部門の担当者であれば、社内で見つかったマルウェアを解析することで、感染経路や感染範囲の特定、感染拡大への対策（二次被害の防止）、復旧方法の検討などを行うことができます。

本レポートでは3つのマルウェアの解析手法「表層解析」、「動的解析」、「静的解析」について、またマルウェア解析を妨害する仕組み「解析妨害」を紹介します。

■ マルウェアやセキュリティに関する情報を「マルウェア情報局」で公開中

キヤノン MJ では、インターネットをより安全に活用するために、マルウェアや各種セキュリティに関する情報を提供しています。こちらも合わせてご覧ください。

マルウェア情報局
【https://eset-info.canon-its.jp/malware_info/】

マルウェア情報局は、キヤノン MJ が国内総販売代理店として取り扱う ESET 製品に関する情報や、マルウェアの情報を提供するポータルサイトです。本サイトでは、スロバキアのセキュリティベンダー ESET 社が発信するニュースを中心に、キヤノン MJ のサイバーセキュリティに関する研究を担うマルウェアラボが発信するレポートを掲載しています。