2019年9月20日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年上半期マルウェアレポートを公開
～ダークウェブ上で取引される脆弱性情報について注意喚起～

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、2019年上半期の国内マルウェア動向に関するレポートを公開しました。本レポートでは、2019年上半期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は、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」として毎月定期的に発行しています。

このたび、2019年上半期に検出されたマルウェアについて分析したレポートを公開しました。

2019年上半期マルウェアレポート
【https://eset-info.canon-its.jp/malware_info/trend/detail/190920.html】

＜トピック＞

■ 2019年上半期マルウェア検出統計

2019年上半期に日本国内で最も検出されたマルウェアはJS/Danger.ScriptAttachmentで、検出数全体の12.3%を占め、2019年は多数の攻撃が確認されています。日本の芸能人の名前が件名に含まれていることから、日本のユーザーを狙った攻撃と考えられます。

■ Emotetの感染を狙ったばらまき型メール

Emotetはバンキングマルウェアの一種で、追加のモジュール（機能）をダウンロードすることで、ネットワーク内で感染を拡大したり、メールの情報を窃取したりすることにより、周囲のPCやネットワークに影響を及ぼします。主にメール経由で侵入し、添付ファイルやメール本文内のリンクからダウンロードしたファイルを実行することで感染します。感染を狙ったばらまき型メールは、昨年11月に日本で確認されて以来、2019年上半期も複数回ばらまかれたことが確認されています。

■ GandCrabの終焉

2018年初頭に登場して以来、継続的に観測されているGandCrabは2019年上半期に日本国内で最も多く検出されたランサムウェアで、このランサムウェア感染を狙ったばらまき型メールによる攻撃を、ESETでは“Love You”malspam campaignと呼んでいます。2019年5月末、突如GandCrab作成者は、サイバー犯罪者向けの提供サービスをやめることを発表しました。本トピックではGandCrabが流行した要因や攻撃事例について解説します。

■ 圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア

2019年2月、多くの圧縮・展開ソフトウェアが利用しているライブラリ UNACEV2.DLL に脆弱性（以下、本脆弱性）が発見され、その脆弱性を悪用するマルウェアが数多く確認されています。

本脆弱性はディレクトリトラバーサルの脆弱性です。ディレクトリトラバーサルとは、通常はアクセスできないディレクトリやファイルにアクセスする脆弱性（攻撃手法）のことです。攻撃者によって細工された圧縮ファイルを展開した場合、任意のフォルダーに悪意のあるファイルが展開されるおそれがあります。本トピックではバックドア型マルウェアの事例を紹介します。

■ 売買される脆弱性情報

ソフトウェアにおける「脆弱性」とは、オペレーティングシステムやプログラムの不具合、設計上のミスなどが原因で発生するセキュリティ上の欠陥を意味します。現在、脆弱性は、多数発見・報告されており、その数は増加傾向にあります。

このような状況の中で、発見された脆弱性がサイバー攻撃に悪用される事例も多く確認されており、組織にとって大きな脅威となっています。また、ディープウェブやダークウェブ上では、脆弱性情報や脆弱性を悪用したプログラムなどが商品として取引されており、技術力のないサイバー犯罪者でも比較的簡単に利用することが可能です。本トピックでは脆弱性を利用したサイバー攻撃の現状と、ディープウェブやダークウェブで売買される脆弱性の事例を紹介します。

● 一般の方のお問い合わせ先　：ESET サポートセンター　050－3786－2528
● ESETホームページ　：https://eset-info.canon-its.jp/
● ニュースリリースホームページ　：canon.jp/newsrelease

＜“2019年上半期マルウェアレポート”の主な内容＞

■ 2019年上半期マルウェア検出統計

2019年上半期に日本国内で最も検出されたマルウェアはJS/Danger.ScriptAttachmentです。マルウェア検出数全体のうち12.3%を占めています。JS/Adware.Agent（全体の10.6%）、HTML/FakeAlert（全体の9.0%）がそれに続きます。

JS/Danger.ScriptAttachmentは電子メールに添付された悪意のあるJavaScriptで、2019年1月以降多数の攻撃が確認されています。攻撃に使われた電子メールの件名には日本の芸能人の名前が含まれており、日本のユーザーを狙った攻撃と考えられています。

JS/Adware.AgentはWebブラウザー上で不正な広告を表示するJavaScriptで、2019年上半期の間、常に一定数検出されていますが、6月に特に多く検出されています。

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で、ファイル形式はMicrosoft Word文書（拡張子.doc/.docm等）あるいはMicrosoft Excel（拡張子.xls/.xlsm等）文書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。日本国内における検出数は、世界の国と地域の中で最多です。

■ Emotetの感染を狙ったばらまき型メール

Emotetは当初、バンキングマルウェアとして利用されていましたが、現在では他のマルウェアのローダーとして使われています。モジュール型のマルウェアであり、追加モジュール（機能）をダウンロードすることで様々な活動を行います。ネットワーク内に感染を拡大するワーム機能、メールの情報を窃取する機能、TrickBotなどの他のマルウェアをダウンロードする機能などの様々な機能が存在します。また、攻撃者により頻繁に更新・機能追加されています。

Emotetに感染した場合、ワーム機能によりネットワーク内に感染が拡大し、対処するためには、1インシデントあたり最大で100万ドル（日本円でおよそ1億600万円：2019年8月20日現在）を要するとも言われています。また、2019年5月、都内の医療機関においてもEmotetの亜種と推定されるマルウェアの感染が報告されています。

Emotetの感染を狙ったばらまき型メールは、2018年11月に日本で確認されて以来、2019年上半期も複数回ばらまかれたことを確認しています。現在は一時的に検出が減少していますが、今後は攻撃者により機能が追加され、活動が活発になる恐れがあります。また、ばらまき型メールのメール本文や添付ファイルの日本語がより高度になっていく可能性があるため、今後とも注意が必要です。

■ GandCrabの終焉

GandCrabは感染した端末上のファイルを暗号化し、復号するための身代金を要求するランサムウェアです。欧州刑事警察機構（ユーロポール）によると、2018年初頭に登場してからわずか1ヵ月で5万人もの被害が出たことが報告されています。2019年上半期においては、日本国内で最も多く検出されたランサムウェアでした。

このように非常に流行していたランサムウェアでしたが、2019年5月末、突如GandCrab作成者が提供サービスをやめることを発表しました。発表内で作成者は、20億ドル以上の収益を上げたことを表明しました。GandCrabが多く検出された主な要因として、頻繁に新しいバージョンが出現するため対策が難しかったこと、ダークウェブ上に存在するサイバー犯罪者向けサービスのRansomware as a Service (RaaS) で販売されていたため、容易に攻撃が可能であったことが考えられます。

2019年1月、2月はGandCrabの感染を狙ったばらまき型メールが多数観測されました。メールには2019年上半期マルウェア検出統計で1位となったJS/Danger.ScriptAttachmentが添付されており、件名や添付ファイルの名前にはLove youといった文字列が含まれていた時期があったことからESETではこの攻撃を“Love You”malspam campaignと呼んでいます。件名には日本の芸能人の名前がローマ字で記載されている時期もあり、日本のユーザーを狙った攻撃と推測されます。メール添付されているzipファイルは、GandCrabではなくダウンローダーです。zipファイルを解凍し、ダウンローダーを実行すると、C&Cサーバーと通信を行い、最終的にGandCrabをはじめ、様々なマルウェアをダウンロードします。

■ 圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア

ライブラリUNACEV2.DLLの脆弱性（以下、本脆弱性）はディレクトリトラバーサルの脆弱性です。ディレクトリトラバーサルとは、通常はアクセスできないディレクトリやファイルにアクセスする脆弱性（攻撃手法）のことです。攻撃者によって細工された圧縮ファイルを展開した場合、任意のフォルダーに悪意のあるファイルが展開されるおそれがあります。

本脆弱性を悪用するマルウェアがいくつか確認されていますが、ここではバックドア型マルウェアの事例を紹介します。このバックドアは本脆弱性を悪用した圧縮ファイルに格納されています。圧縮ファイルを展開するとユーザーが指定したフォルダーに3つのMicrosoft Office 文書が展開されます。これらのファイルは、元の圧縮ファイルはマルウェアではないとユーザーに信じさせるためのおとり（デコイファイル）であると考えられます。

デコイファイルの展開と同時に、スタートアップフォルダーに自己解凍形式の圧縮ファイルwinword.exeが展開されます。スタートアップフォルダーに含まれるプログラムはPC起動時に自動で実行されます。winword.exeは実行（展開）時に、Windows標準機能のregsvr32によって、OCX形式 のプログラムがシステムに登録されるコマンドを実行し、最終的にバックドアモジュールをメモリ上にロードします。

■ 売買される脆弱性情報

ソフトウェアにおける「脆弱性」とは、オペレーティングシステムやプログラムの不具合、設計上のミスなどが原因で発生するセキュリティ上の欠陥を意味します。2019年5月に、リモートデスクトップサービスに関連する脆弱性BlueKeepが発見され、マイクロソフトがWindows XPなどサポートを終了したOSに対して、異例の更新プログラムを提供したことが話題となりました。現在、脆弱性は、多数発見・報告されており、その数は増加傾向にあります。

このような状況の中で、発見された脆弱性がサイバー攻撃に悪用される事例も多く確認されており、組織にとって大きな脅威となっています。サイバー攻撃に使用される脆弱性の中には、長期にわたり継続的にサイバー攻撃に使用される脆弱性も存在し、代表的な例として2年前に世界規模で感染を拡大したランサムウェアWannaCryptor（別名：WannaCry）で使用されたEternalBlueが挙げられます。

ディープウェブやダークウェブ上では、脆弱性情報や脆弱性を悪用したプログラムなどが「商品」として取引されています。たとえば、Microsoft Officeの脆弱性を悪用したマルウェアを作成できるサービスや、脆弱性情報を売り買いできるサービス、脆弱性などを利用したサイバー攻撃を代行するハッキングサービス、マルウェアの販売サービス（Malware as a Service）なども存在します。このようにディープウェブやダークウェブ上では、脆弱性情報や脆弱性を悪用したプログラムなどが商品として取引されており、技術力のないサイバー犯罪者でも比較的簡単に利用することが可能です。

■ 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 が日本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。