2019年7月26日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年6月のマルウェアレポートを公開
～日本語環境をターゲットにしたばらまき型メールが急増～

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6月のマルウェア検出状況に関する最新のレポートを公開しました。6月は、日本語環境を狙ったばらまき型メールが急増しており、弊社マルウェア情報局からも注意喚起しています。

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、国内で利用されているウイルス対策ソフトウェア「ESETセキュリティ ソフトウェア シリーズ」のマルウェア検出データを基に、2019年6月のマルウェア検出状況を分析し最新のレポートを公開しました。

2019年6月のマルウェア検出状況に関するレポート
【https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1906.html】

■トピック

・悪意のある広告を表示させるアドウェアが国内外を問わず上位を占拠

2019年6月は、悪意のある広告を表示させるアドウェアが多数検出され、第1位はJS/Adware.Agentで、第2位はJS/Adware.Subpropでした。これら2種類のアドウェアは、海外でも非常に多く検出されています。

・日本語環境を狙ったばらまき型メール

6月には、マルウェアDOC/Agent.DZも猛威を振るい、6月17日から6月30日までの14日間で極めて多く検出されました。このマルウェアの検出は6月17日にばらまかれたメールに添付されたExcelファイルが大半を占めており、そのExcelファイルのVBA（Visual Basic for Applications）のコードとPowerShellのコマンドには、Long Dateフォーマットの日付文字列を利用して日本語環境を検知し、感染対象を絞る処理が記述されていました。

攻撃者は、日本語環境でしか動作しないように解析妨害を施し、自動解析で動作しないようにすることや解析を遅らせることで、検知を遅らせ感染拡大を狙っていた可能性があります。

● 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6月マルウェアレポート”の主な内容＞

■ 6月の概況

2019年6月の国内で最も多く検出されたマルウェアはJS/Adware.Agentで、第2位はJS/Adware.Subpropでした。どちらも、悪意のある広告を表示させるアドウェアでWeb閲覧中に実行されます。表示された悪質な広告をクリックすると不正なWebサイトへアクセスし、別のマルウェアをダウンロードされる可能性があります。

また国内では、6月17日に登録されたマルウェアDOC/Agent.DZが検出され、6月全体の国内検出数上位5位にランクインしました。DOC/Agent.DZは、6月17日から6月30日までの14日間で極めて多く検出されましたが、日本以外ではほとんど検出が確認されていません。

【解説】日本語環境を狙ったばらまき型メール「DOC/Agent.DZ」について

DOC/Agent.DZの検出は、6月17日にばらまかれたメールに添付されたExcelファイルが大半を占めています。メールの件名は「Re: 請求書の送付」、「ご案内 [お支払い期限 :06月18日]」などで、トータル7種類の件名が確認されています。添付されたExcelファイルのマクロを有効化すると、画像ファイルPCにダウンロードされます。これは2018年10月のマルウェアレポートで紹介した、データを画像ファイル内に隠蔽する「ステガノグラフィー」を用いた攻撃手法です。

このExcelファイルのVBAProjectは簡単には解除できない方法でロックが掛けられており、攻撃者がVBAコードの解析の妨害をしていると考えられます。VBAコードを抽出し分析したところ、コード内のスクリプトにLong Date形式で日付を取得する処理の記述があり、日本語などの一部言語の場合は「YYYY年MM月DD日」というフォーマットで取得されます。このスクリプトで取得した日付の文字列に「年」が含まれている場合は、Excelのセル内の難読化された文字列を解読し、ダウンロードコマンドが作成されますが、含まれていない場合はそのまま終了します。このダウンローダーは、VBAコードのwmicコマンド経由でPowerShellを起動しダウンロード処理を行います。

PowerShellのコマンドはExcelのVBAコードと同様に日本語環境を検知する処理に加えて、インストールされているアンチウイルスソフトの情報やCPUの情報を攻撃者のサーバーに送信する処理が記載されており、巧妙化しています。これらのことからDOC/Agent.DZは日本語環境を狙ったマルウェアと考えられます。

今後も新種のマルウェアが流行する可能性があり、常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■ 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。

※ ESETは、ESET, spol. s r.o. の商標です。Visual Basic、PowerShellは、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。