2019年4月25日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年3月のマルウェアレポートを公開
～圧縮・展開ソフトウェアの脆弱性を悪用したランサムウェアを確認～

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3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。圧縮・展開ソフトウェアの脆弱性を悪用したマルウェアについて解説しています。

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3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3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/malware1903.html】

■ トピック

・JavaScriptで記述されたアドウェアが増加

2019年3月の国内マルウェア検出数は、検出数が急増した2019年1月と比較して減少しました。3月に国内で最も多く検出されたマルウェアは、JavaScriptで記述されたアドウェアであるJS/Adware.Agentでした。JS/Adware.Agentは、Web閲覧中に不正な広告を表示させる恐れがあります。2番目に多く検出されたマルウェアは、VBA（Visual Basic For Applications）で記述されたダウンローダーであるVBA/TrojanDownloader.Agentでした。JS/Adware.AgentとVBA/TrojanDownloader.Agentは、2018年の年間を通して非常に多く観測されたマルウェアで、2018年に国内で検出されたマルウェアのうち、前者が2番目、後者が1番目に多く検出されました。これらのマルウェアに対しては、引き続き警戒が必要だと考えられます。

・圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア

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、本脆弱性を悪用するマルウェアが確認されています。

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恐れがあります。マルウェアレポート内では、本脆弱性を悪用した事例として、ランサムウェアJNEC.a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3月マルウェアレポート”の主な内容＞

■ 3月の概況

2019年3月に最も多く検出されたマルウェアは、JavaScriptで記述されたアドウェアで、Web閲覧中に不正な広告を表示させる恐れのあるJS/Adware.Agentでした。2番目に多く検出されたマルウェアは、VBA（Visual Basic For Applications）で記述されたダウンローダーであるVBA/TrojanDownloader.Agentでした。JS/Adware.AgentとVBA/TrojanDownloader.Agentは、2018年の年間を通して非常に多く観測されたマルウェアで、2018年に国内で検出されたマルウェアのうち、前者が2番目、後者が1番目に多く検出されました。これらのマルウェアに対しては、引き続き警戒が必要だと考えられます。

2019年1月と2月に猛威を振るったJS/Danger.ScriptAttachmentは、検出数が大幅に低下し、2月後半のピーク以降、目立った活動は確認されませんでした。

■【解説】ランサムウェアJNEC.aの感染プロセスと対策

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、本脆弱性を悪用するマルウェアが確認されています。マルウェアレポート内では、本脆弱性を悪用した事例としてランサムウェアJNEC.aを紹介します。

ランサムウェアJNEC.aの拡散には細工が施された圧縮ファイルが使用されています。拡張子は.rarですが、実体はACE形式の圧縮ファイルです。JNEC.aがPC上のファイルを暗号化し、暗号化が完了すると、ファイルを元に戻すための対価としてビットコインを要求する画面がデスクトップに表示されます。2018年11月以降攻撃者ウォレットに対する入金がないことや、サンプルの観測数が少ないことから、本マルウェアの拡散は限定的と考えられます。

本脆弱性を悪用するマルウェアを作成するためのツールキットがハッキングフォーラム等で公開されています。2019年4月5日時点で既に288個のマルウェア（またはマルウェアの可能性があるファイル）が作成されたことを示す記載もあります。このようなサイトが存在することから、今後も本脆弱性を悪用した攻撃が発生することが予想されます。

詳しい感染プロセスと対策については、マルウェアレポートで紹介しています。

3月は圧縮・展開ソフトウェアの脆弱性を悪用した攻撃が確認されました。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。