2019年6月28日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年5月のマルウェアレポートを公開
～新たに発見された脆弱性 BlueKeep が悪用される危険性を解説～

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、2019年5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。新たに発見された Windows のリモートデスクトップサービスに関連する脆弱性 BlueKeep 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5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5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/malware1905.html】

■ トピック

・メールに添付された VBA で記述されたダウンローダーが継続して検出

2019年5月に国内で最も多く検出されたマルウェアは、4月と同様に VBA/TrojanDownloader.Agent で、1月に比べて5倍以上の検出数でした。本マルウェアは、VBA（Visual Basic for Applications）で記述されたダウンローダーで、実行されるとバンキングマルウェアなどをダウンロードします。主にメールの添付ファイルとして拡散されています。5月の検出では、5月27日と30日にばらまかれたメールに添付された VBA/TrojanDownloader.Agent.MUV の検出が大部分を占めています。

・WannaCryptor の大規模感染から２年、新しい脆弱性 BlueKeep が発見される

ランサムウェア WannaCryptor（別名：WannaCry）は、2017年5月に確認されてから世界規模で感染を拡大し、日本を含む約150ヶ国で23万台以上のコンピューターに被害を与えたと言われています。WannaCryptor では EternalBlue と呼ばれるプログラムが悪用されましたが、このプログラムを悪用した攻撃は現在も継続して観測されています。

そのような状況の中、新たに BlueKeep と呼ばれる Windows のリモートデスクトップサービスに関連する脆弱性が発見されました。この脆弱性は、EternalBlue と同様に、マルウェアを他のコンピューターに感染させる目的で悪用される恐れがあります。

● 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5月マルウェアレポート”の主な内容＞

■ 5月の概況

2019年5月に国内で最も多く検出されたマルウェアは、4月と同様にVBA/TrojanDownloader.Agentでした。VBA/TrojanDownloader.Agentの検出数は、5月27日、30日にばらまかれたメールに添付されたVBA/TrojanDownloader.Agent.MUVの検出が大部分を占めています。

VBA/TrojanDownloader.Agent.MUVで使用されたエクセルファイル内の画像は、ぼかしが掛かったような表示になっています。はっきりとした画像を見るために「コンテンツの有効化」を押させることを狙っている可能性があります。

■【解説】EternalBlueを悪用した攻撃の継続と新たに発見された脆弱性BlueKeep

2017年5月、6月は、ランサムウェアWannaCryptorの大規模感染により多くのコンピューターでEternalBlueを悪用した攻撃を検出しました。その後、WannaCryptorの脅威が収束するとともに、EternalBlueを悪用した攻撃も減少しましたが、2017年9月頃から増加に転じ、現在ではWannaCryptorの大規模感染時を上回る数のクライアントで攻撃が観測されています。

EternalBlueを悪用した攻撃が継続して観測される中、マイクロソフトは2019年5月にWindows XPなどのサポートを終了した製品を含むオペレーティングシステムに対して異例の更新プログラムを提供しました。この更新プログラムで修正される脆弱性はリモートデスクトップサービスに関連する脆弱性で、別名BlueKeepと呼ばれています。

2019年5月25日時点で、この脆弱性を悪用したサイバー攻撃は確認されていません。しかし、ランサムウェアWannaCryptorの時と同様に、脆弱性が明らかになった数か月後に脆弱性を悪用したマルウェアが拡散され、世界的な大規模感染につながる恐れがあります。

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。