2019年4月5日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年1月、2月のマルウェアレポートを公開
～日本を標的としたランサムウェア GandCrab 感染を狙う攻撃を観測～

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1月、2月のマルウェア検出状況に関するレポートを公開しました。1月以降に急増した悪意のある JavaScript ファイルや、ランサムウェア GandCrab の感染を狙った malspam※1などについて解説しています。

キヤノン MJ のマルウェアラボは、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1月と2月のマルウェア検出状況を分析しレポートを公開しました。

2019年1月、2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/malware1902.html】

■ トピック

・メールに添付された悪意のある JavaScript ファイルが急増

2019年1月と2月の国内マルウェア検出数は、2018年12月と比較して増加しました。国内で最も多く検出されたマルウェアは、電子メールに添付された悪意のある JavaScript ファイルである JS/Danger.ScriptAttachment でした。JS/Danger.ScriptAttachment は、メールに添付されたファイル名が、Love_you_<数字>となっていたことから、ESET ではこの攻撃を “Love You” malspam campaign と呼んでいます。

・ランサムウェア GandCrab の感染を狙った malspam

1月、2月はランサムウェア GandCrab の感染を狙った malspam を数多く観測しています。1月初旬から確認されている Love you malspam は、JavaScript 形式のダウンローダーが含まれた zip ファイルが添付されており、ダウンローダーを実行するとランサムウェア GandCrab やスパムボット Phorpiex、コインマイナーなどさまざまなマルウェアに感染する恐れがあります。GandCrab に感染するとファイルが暗号化されたりさまざまな情報を収集されたりします。

マルウェアレポート内では、ランサムウェア GandCrab の感染フローと対策について解説しています。

※1 malware spam または malicious spam の略です。ここでは、マルウェア感染を狙ったスパムメールを指します。

● 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1月2月マルウェアレポート”の主な内容＞

■ 1月と2月の概況

電子メールに添付された悪意のあるJavaScriptファイルであるJS/Danger.ScriptAttachmentは、2018年12月はほとんど検出されていませんでしたが、年明けとともに検出数が急増しています。これは、1月以降にJavaScriptを含むファイルが添付されたメールが多数確認されているためです。JS/Danger.ScriptAttachmentの件数は、2番目に多く検出されたHTML/ScrInjectの割合に対して大きく差をつけています。

世界全体において1月と2月に検出されたJS/Danger.ScriptAttachmentのうち、86%は日本で確認されました。そのため、“Love You” malspam campaignは、日本を主なターゲットとした攻撃であったことが推測されます。

■【解説】ランサムウェアGandCrabの感染フローと対策

Love you malspamでは、メールに添付されたJavaScript形式のダウンローダーを実行するとランサムウェアGandCrab、スパムボットPhorpiex、コインマイナー、ダウンローダー、システム設定ツールなどさまざまなマルウェアに感染する可能性があります。

このmalspamは、日本をターゲットにした攻撃と考えられ、件名が日本の芸能人の名前になっているメールがばらまかれています。しかし現段階ではメールの件名や本文、GandCrabの脅迫画面が日本語にはなっていないため、完成度はそこまで高くありませんが、GandCrabに感染するとファイルが暗号化されたりさまざまな情報を収集されたりします。

マルウェアレポート内では、ランサムウェアGandCrabの感染フローと対策について解説しています。

1月、2月はランサムウェアGandCrabの感染を狙ったmalspamが数多く観測されました。このmalspamでは複数のマルウェアに感染する可能性があります。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。