2019年9月27日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年7月、8月のマルウェアレポートを公開
～ランサムウェア「Sodinokibi」の被害が世界中で拡大～

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7月、8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。世界中で被害が広がっているSodinokibiと呼ばれるランサムウェアの脅威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7月、8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7月、8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/malware1908.html 】

■ トピック

・Microsoft Office 数式エディターに存在する脆弱性を悪用するマルウェアの検出が増加

2019年7月はMicrosoft Office数式エディターに存在する脆弱性（CVE-2017-11882）を悪用するマルウェアWin32/Exploit.CVE-2017-11882が再びランクインし、8月も引き続き上位に入っています。Win32/Exploit.CVE-2017-11882は今年初めから徐々に検出数が増加し、2019年6月には脆弱性発見時（2017年11月）の検出数を上回りました。

・ランサムウェア Sodinokibi の脅威

2019年4月以降、Sodinokibiと呼ばれるランサムウェアが国内外で猛威を奮っています。

キヤノンMJのマルウェアラボが確認した事例では、本ランサムウェアに感染するとディスク上のファイルを暗号化し、データの回復を困難にします。身代金として、0.11862719ビットコイン（2019年9月現在およそ129,000円）が要求されます。

Sodinokibiが特に多く検出されている国はアメリカやカナダで、日本においては世界で6番目に多く検出されています。Sodinokibiの特長として、感染経路が多岐にわたることが挙げられますが、本マルウェアレポートレポートでは最も代表的な「メールの添付ファイル経由の感染」について詳細に解説しています。

● 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/business/
● ニュースリリースホームページ　：canon.jp/newsrelease

＜“2019年7月8月マルウェアレポート”の主な内容＞

■ 7月、8月の概況

2019年7月、8月に国内で最も検出されたマルウェアは、6月に引き続きJS/Adware.Agentでした。本マルウェアは、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。

また、7月はMicrosoft Office数式エディターに存在する脆弱性（CVE-2017-11882）を悪用するマルウェアWin32/Exploit.CVE-2017-11882が再びランクインし、8月も引き続き上位に入っています。CVE-2017-11882に対処した修正プログラムは2017年の11月の時点で公開されましたが、未だにその脆弱性を悪用する攻撃が続いています。Win32/Exploit.CVE-2017-11882は他のマルウェアのダウンローダーとして動作するマルウェアです。キヤノンMJのマルウェアラボでは、Win32/Exploit.CVE-2017-11882がバンキングマルウェアやRAT（遠隔操作ツール）などのダウンローダーとして使われている事例を確認しています。

■【解説】ランサムウェアSodinokibiの脅威

2019年4月以降、Sodinokibiと呼ばれるランサムウェアが国内外で猛威を奮っています。

8月の中旬にはアメリカ・テキサス州で23か所の地方自治体がSodinokibiの被害にあったほか、8月末にはアメリカの数百か所以上の歯科医院で同ランサムウェアの感染が発生しています。Sodinokibiが特に多く検出されている国はアメリカやカナダで、日本においては世界に6番目に多く検出されています。

Sodinokibiの特長として、感染経路が多岐にわたることが挙げられますが、本マルウェアレポートでは最も代表的な「メールの添付ファイル経由の感染」について詳細に解説しています。キヤノンMJのマルウェアラボが今回確認したメールでは、実在する運送会社を装い、出荷ラベルを送付するとの名目で受信者が添付ファイルを開くよう誘導しています。メールに添付されたzipファイルを開きexeファイルを実行するとSodinokibiランサムウェアに感染し、ディスク上のファイルが暗号化されデータの回復が困難になります。データを復旧するには、身代金として0.11862719ビットコイン（2019年9月現在およそ129,000円）が要求されます。

Sodinokibiは感染手法が最も洗練されたランサムウェアの一つで、今後その手法がさらに巧妙化することも考えられます。また、最近のランサムウェアは個人だけではなく、政府機関や医療機関など重要度の高いデータを持つ組織を狙う傾向にありますので注意が必要です。

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。