2019年12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11月のマルウェアレポートを公開
～新しい脆弱性を悪用した新種のランサムウェア「NextCry」を発見～

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11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。情報が公開されて間もない脆弱性を悪用した新種のランサムウェア「NextCry」が発見されました。

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11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11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/malware1911.html 】

■ トピック

・「VBA」で作成された「VBA/TrojanDownloader.Agent」が倍増

2019年11月は、Office製品で使われているプログラミング言語「VBA」で作成されたダウンローダー「VBA/TrojanDownloader.Agent」が10月に比べ約2倍増加しました。「VBA/TrojanDownloader.Agent」は通常、バンキングマルウェアなど他のマルウェアをダウンロードしますが、今月の傾向としては、10月に大きな被害をもたらした「Emotet」のダウンローダーとして使われるケースも見受けられました。

・公開されて間もない脆弱性を悪用した新種のランサムウェア「NextCry」を発見

オンラインストレージサービス「NextCloud」上のデータを暗号化する新種のランサムウェア「NextCry」が発見されました。PHPの実行環境「PHP-FPM」の脆弱性が本ランサムウェアの侵入経路として用いられました。キヤノンMJのマルウェアラボは、脆弱性の情報が公開されてからわずか10日程で新種のランサムウェアの攻撃に悪用されていることを確認しています。

本レポートではキヤノンMJマルウェアラボによる「NextCry」の調査・分析結果とその対策について解説をしています。

● 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11月マルウェアレポート”の主な内容＞

■ 11月の概況

11月に国内で最も多く検出されたマルウェアは10月に引き続き「HTML/ScrInject」でした。「HTML/ScrInject」はWebサイト閲覧時にHTMLに埋め込まれた不正スクリプトを実行します。

また、Office製品で使われているプログラミング言語「VBA」で作成されたダウンローダー「VBA/TrojanDownloader.Agent」は、10月に比べ約2倍増加しました。「VBA/TrojanDownloader.Agent」は通常、バンキングマルウェアなど他のマルウェアをダウンロードしますが、今月の傾向としては、10月に大きな被害をもたらした「Emotet」のダウンローダーとして使われるケースもありました。

■【解説】公開されて間もない脆弱性を悪用した新種のランサムウェア「NextCry」

オンラインストレージサービス「NextCloud」上のデータを暗号化する新種のランサムウェア「NextCry」が発見されました。Webサイトのパフォーマンスを向上させるために用いられる、PHPの実行環境「PHP-FPM（FastCGI Process Manager）」の脆弱性が本ランサムウェアの侵入経路として用いられました。キヤノンMJのマルウェアラボは、脆弱性の情報が公開されてからわずか10日程で新種のランサムウェアの攻撃に悪用されていることを確認しています。

「PHP-FPM」の脆弱性を悪用して「NextCloud」に送り込まれた本ランサムウェアは、「NextCloud」に保存されるデータを暗号化し、ユーザーが「NextCloud」の管理画面や操作画面にアクセスすると脅迫文を表示します。その脅迫文には「AES-256」を用いてデータを暗号化したことや復旧にはビットコインの支払いと指定のメールアドレスに連絡する旨が記載されています。

サイバー犯罪者は絶えず攻撃の機会を狙っており、新しい脆弱性をみつけるとすぐに攻撃をして大きな被害をもたらします。サイバー犯罪から身を守るためには、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。

本レポートではキヤノンMJマルウェアラボによる「NextCry」の調査・分析結果と対策を解説しています。

■ 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。