2019年6月7日

NEWS RELEASE

キヤノンマーケティングジャパン株式会社

2019年4月のマルウェアレポートを公開
～バックドア型マルウェア Plead を用いた新たな攻撃を台湾で観測～

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4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。台湾で確認されたバックドア型マルウェア Plead を用いた新たな攻撃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4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4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/malware1904.html】

■ トピック

・VBA で記述されたダウンローダーが最多

2019年4月に国内で最も多く検出されたマルウェアは VBA/TrojanDownloader.Agent 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。

・バックドア型マルウェア Plead を用いた新たな攻撃を確認

ESET 社は2019年4月に、Plead を用いた新たな攻撃を台湾で確認しました。Plead はバックドア型のマルウェアで、これまでも東アジアの組織を狙った攻撃に使われてきました。バックドアは「裏口」を意味するマルウェアで、攻撃者がシステムに侵入した際、次回以降侵入しやすくする目的で設置され、感染した場合、情報が窃取されるほか感染端末を不正行為の踏み台として使われる恐れがあります。

今回の手法では、正規アプリケーションにおけるアップデートの仕組みを悪用しています。マルウェアレポートでは、Plead の感染プロセスの事例を紹介します。

● 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4月マルウェアレポート”の主な内容＞

■ 4月の概況

2019年4月に国内で最も多く検出されたマルウェアはVBA/TrojanDownloader.Agent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。国内におけるVBA/TrojanDownloader.Agentの検出数は年初から徐々に増加しており、4月の検出数は1月の3倍以上となりました。

■【解説】バックドア型マルウェアPleadの感染プロセスと対策

ESET社は2019年4月に、Pleadを用いた新たな攻撃を台湾で確認しました。Pleadはバックドア型のマルウェアで、これまでも東アジアの組織を狙った攻撃に使われてきました。今回の手法では、正規アプリケーションにおけるアップデートの仕組みを悪用しています。

今回悪用されたアプリケーションは、アップデートの際に暗号化されていないHTTP通信を用いており、アップデートファイルの検証が行われていませんでした。また、Pleadに感染したPCに接続されていたルーターには外部から管理パネルにアクセスされる脆弱性があったことも明らかになっています。攻撃者はそれらの隙を突いてMITM（中間者）攻撃を行った可能性が高いとみられています。

最終的に実行されるPleadはPC上の情報窃取などを行います。Pleadは、2018年には日本国内においても検出されており、再び国内で攻撃が発生する恐れがあります。

4月はESET社によりPleadバックドアの活動が確認されました。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。