2018 年 8 月 10 日
株式会社セキュアソフト

注意喚起：バンキングトロージャンに感染させる

拡張子“iqy”添付ファイル付きメールの国内大量拡散について

1. 概要

今月に入りインターネットバンキングなど金融情報の窃取を目的としたマルウェア付きメールが、日本国内で多数配信されています。メールの添付ファイル拡張子が”iqy“と見慣れないもので、海外では以前から確認されておりましたが、国内を狙った日本語による大量のメールが確認されております。

このような金融情報の窃取を目的とした、マルウェアを「バンキングトロージャン」と称します。バンキングトロージャンに感染すると、利用者のログイン・パスワードなどの情報を窃取され、利用者が気付かないうちに銀行口座から不正に金銭を引き出されてしまう被害に遭う恐れがあります。またバンキングトロージャンの中にはインターネットバンキングのみならず仮想通貨の取引所やウェブウォレットから不正に送金するものも確認されています。

夏休みなどの長期休暇明けは、休暇中に溜まった多数のメールを確認することで注意力が低下し対策が疎かになり、マルウェアに感染する可能性が高くなる傾向があり、不用意に怪しいメールを開かないように注意を払ってください。

日頃から被害の遭遇や拡大を未然に防止する対策を講じることが重要です。以下にバンキングトロージャンの攻撃手法と一般的な対策、セキュアソフトのソリューションによる対策をご紹介します。

2. バンキングトロージャンとは

バンキングトロージャンについて、弊社より昨年の 8 月にニュースリリースをさせて頂いております為、詳細は下記のリンクもご参照ください。

「Technical Report 17-08 注意喚起：バンキングトロージャンに感染させるメール拡散について」
https://www.securesoft.co.jp/news_mt/2017/08/post-71/

3. バンキングトロージャン拡散の手法

今回の、バンキングトロージャン感染の手法は、メールのアタッチファイルの拡張子が「.iqy」であることが最大の特徴です。

配信されるメールには添付ファイルの開封を促す、日本語の内容が件名や本文に記載されております。また、添付ファイル名としては「月」+「数字列」や、「受信者名」+「数字列」といった例が確認されております。

弊社でも今回のメールを多数確認しております。以下に、注意喚起情報と例を記載します。

■ 参考情報

独立行政法人情報処理推進機構（IPA）
「IQY ファイルを悪用する攻撃手口に関する注意点(第二版)」
https://www.ipa.go.jp/files/000068065.pdf

「月」+「数字列」パターンの「.iqy」添付メールの一例

件名	お世話になります
送信元	国内インターネットプロバイダのメールアドレス
添付ファイル名	8 月・000000.iqy
本文の例	お世話になります。 いつもお世話になっております。 XLS 版にて送付致します。 添付ファイルのご確認、宜しくお願い致します。

「受信者名」+「数字列」パターンの「.iqy」添付メールの一例

件名	写真送付の件
送信元	国内インターネットプロバイダのメールアドレス
添付ファイル名	xxx・000000.iqy
本文の例	xxx 様 いつもお世話になっております。 XLS 版にて送付致します。 添付ファイルのご確認、宜しくお願い致します。

4. 「.iqy」拡張子添付メールからのバンキングトロージャン感染対策

被害に遭わないためには、PCをマルウェアに感染させない対策が必要です。「.iqy」ファイルはMicrosoft Excelに関連付けられている為、ファイルを開くExcelが起動されます。

「.iqy」拡張子ファイル対策や、一般的なマルウェアの感染防止対策とインターネットバンキング利用時の推奨事項は以下の通りです。ぜひ、参考にしてください。

⑴ 「.iqy」拡張子ファイルへの対策

① Excelのオプションを開く
② オプションメニューより、「セキュリティセンター」を開く
③ セキュリティセンターメニューより、「ファイル制限機能の設定」を開く
④ Microsoft Office クエリファイルの「開く」にチェックを入れる
※本設定は、日常的に「.iqy」ファイルを使用しない場合のみ実施して下さい。

4-⑴に記載している、【「.iqy」拡張子ファイルへの対策】が困難な場合は、下記対応にてマルウェア感染を防止可能となります。

① 「.iqy」拡張子ファイルクリックにて、Excel起動後に表示されるセキュリティに関する通知で、「有効にする」をクリックしない
② 誤って有効にするをクリックした場合でも、cmd.exeの実行を確認する警告プロンプトで、「いいえ」を選択することでマルウェア感染を防ぐことが可能

⑵ マルウェアの感染防止対策

① 常に最新のウイルス定義ファイルに更新する。
② 常に最新の修正プログラムを適用する。
③ メールの添付ファイルやダウンロードしたファイルは、開く前にウイルス検査を行う。

⑶ インターネットバンキング利用時の推奨事項

① 銀行が提供する中でセキュリティレベルの高い認証方法を採用する。
② 銀行が指定した正規の手順で電子証明書を利用する。
③ セキュリティ対策が十分な端末を使用する。

5. SecureSoft mamoret による対策

以下に SecureSoft のソリューションを使用したバンキングトロージャン感染対策を紹介します。

⑴ 対策概要

SecureSoft mamoret 及び mamoret BE（以下 mamoret/mamoret BE）は、それぞれコンテナ技術を利用したブラウジング専用のネットワーク分離ソリューションです。

上記**「4-(3)-③」**に記載した十分なセキュリティ対策を施すには、mamoret を使用することをお勧めいたします。

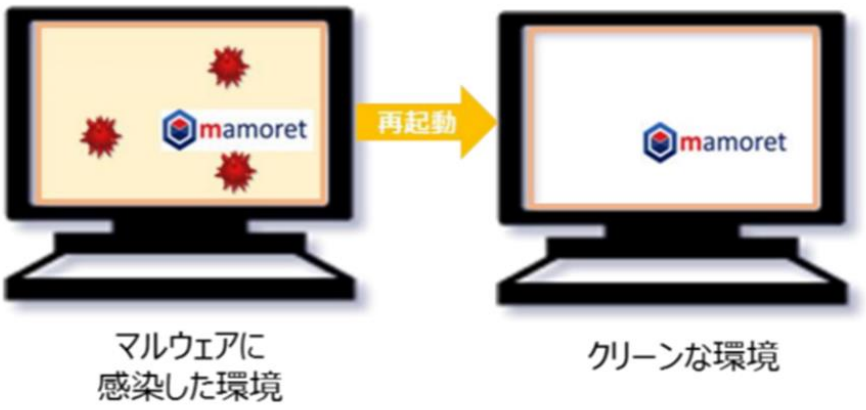
⑵ mamoret/mamoret BE とは

1 台の PC を通常業務環境用のデータ領域とインターネット接続用のデータ領域に分離するソフトウェアです。

万が一、マルウェアがインターネット接続環境に侵入しても通常業務環境のデータを保護することができます。

また、mamoret/mamoret BE には自動初期化機能があり、mamoret/mamoret BE を再起動すると次回起動時には、クリーンなインターネット接続環境が利用可能となります。

万が一、マルウェアに感染しても再起動を実施するとマルウェアを完全に除去することが出来ます。



【図　1】インターネット接続専用環境の初期化イメージ

⑶ mamoret/mamoret BE を使用した運用例

mamoret/mamoret BE を使用したインターネットバンキング利用時の運用例を以下に紹介します。

① メールはブラウザを利用した Web メールで閲覧

メールを Web メールで閲覧することで、ばらまき型攻撃による通常業務環境へのマルウェア感染を防ぎます。

② インターネットバンキングはインターネット接続環境を初期化してから利用

万が一、インターネット接続環境がマルウェアに感染していたとしても mamoret/mamoret BE を再起動することでクリーンな環境になります。インターネットバンキング利用の際は、必ず mamoret/mamoret BE を再起動してから使用してください。

上記の運用を行うことにより、万が一、マルウェアに感染してもバンキングトロージャンによる被害を回避することが可能です。

SecureSoft mamoret/mamoret BE についての詳しい内容は、下記 URL をご参照ください。

https://www.securesoft.co.jp/products/#container

«お問合せ先»

株式会社セキュアソフト

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-5464-9966

FAX 03-5464-9977

sales@securesoft.co.jp