2017 年 8 月 31 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マルウェア付きメール拡散について

1. 概要

最近インターネットバンキングなど金融機関関連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。このようなマルウェアを特に「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し利用者が、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。

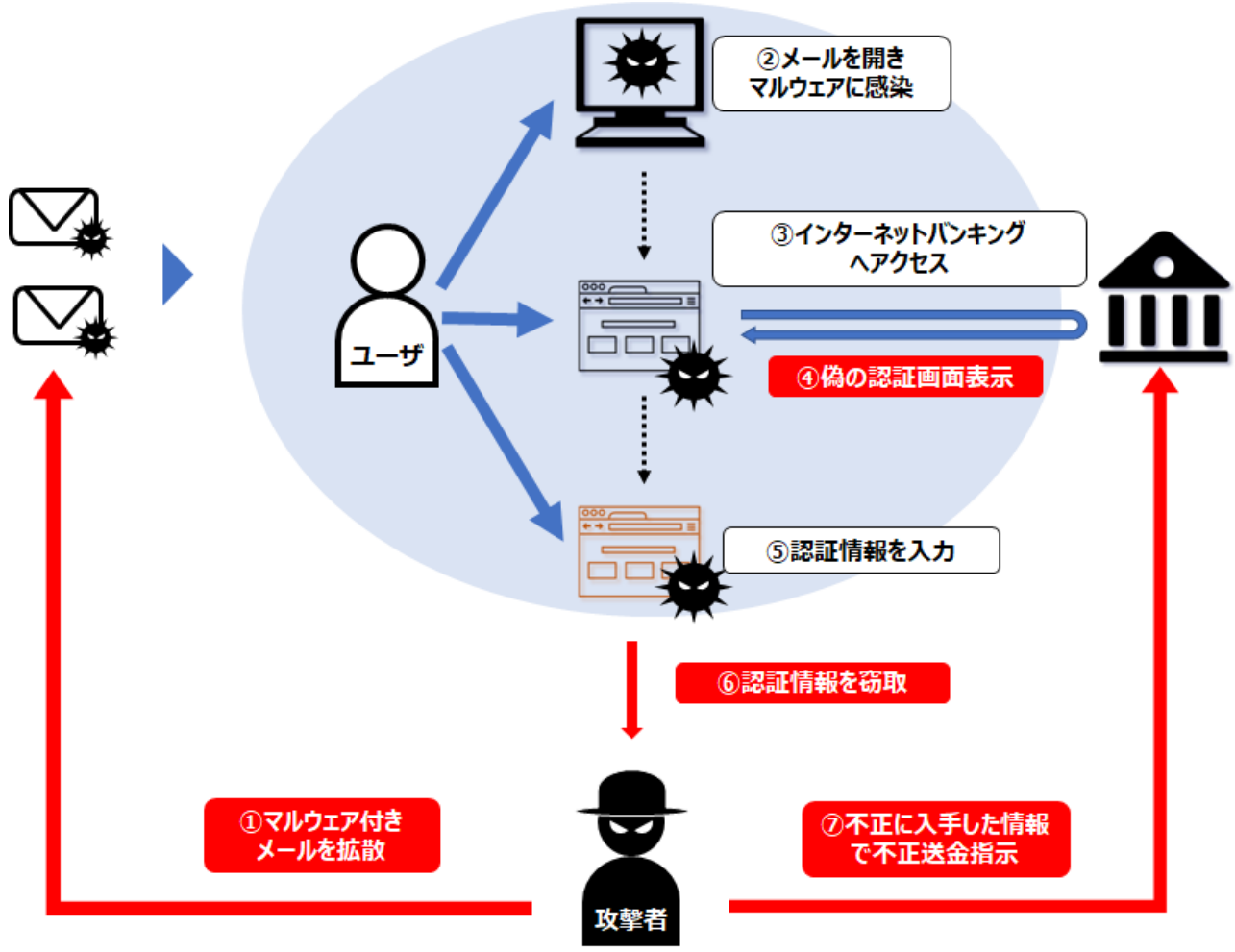
夏休みなどの長期休暇明けは、休暇中に溜まった多数のメールを確認することで注意力が低下し対策が疎かになり、マルウェアに感染する可能性が高くなる傾向があります。不用意に怪しいメールを開かないように注意を払ってください。また、働き方改革に注目が集まる昨今、長期休暇の取得率増加や休暇の分散化によって、システム管理者や利用者が不在になりがちになります。これにより修正プログラム適用やウイルス定義更新が遅れる場合があり、マルウェアへの感染リスクも高くなりますので、なお一層の注意を払ってください。

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は、インターネットバンキングや仮想通貨取引所の利用者を標的に金銭の窃取を目的としたマルウェアでインターネットバンキング詐欺ツールとも呼ばれています。一例として以下のような一連の攻撃活動があります。

① 攻撃者がマルウェア付きのメールを拡散
② ユーザがマルウェア付きメールを開きマルウェアに感染
③ ユーザがマルウェアに感染した PC でインターネットバンキングへアクセス（認証画面要求）
④ マルウェアが偽の認証画面を表示
⑤ ユーザが認証情報を入力
⑥ マルウェアが認証情報を窃取し、攻撃者に送信
⑦ 攻撃者は窃取した情報を利用して不正送金



【図　1】ばらまき型攻撃によるバンキングトロージャン感染と活動イメージ

3.　ばらまき型攻撃によるバンキングトロージャンの拡散

2017年7月下旬以降、バンキングトロージャン「DreamBot」（別名：Ursnif、Gozi など）への感染を狙ったマルウェア付きメールが多数配信（ばらまき）されています。これらの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。
以下に、注意喚起情報と一例を記載します。

・日本サイバー犯罪対策センター（JC3）

「インターネットバンキングマルウェアに感染させるウイルス付メールに注意」
https://www.jc3.or.jp/topics/virusmail.html

※ばらまき型攻撃によるメールの一例

件名	「請求書」
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	「00000.xls」
本文の例	赤沼 様 いつもお世話になっております。 06,07 月分請求書を添付しましたのでご確認お願い致します。 ┌──────────────────────┐ 携帯: 090-1389-0000 └──────────────────────┘

4. 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 PC をマルウェアに感染させない対策が必要です。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 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。

⑵ 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。

また、日本サイバー犯罪対策センター（JC3）では DreamBot や Gozi への感染状況を確認することも可能です。

- 日本サイバー犯罪対策センター（JC3）
  「DreamBot・Gozi 感染チェックサイト」
  https://www.jc3.or.jp/info/dgcheck.html

5. SecureSoft i-コンテナ及び 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。

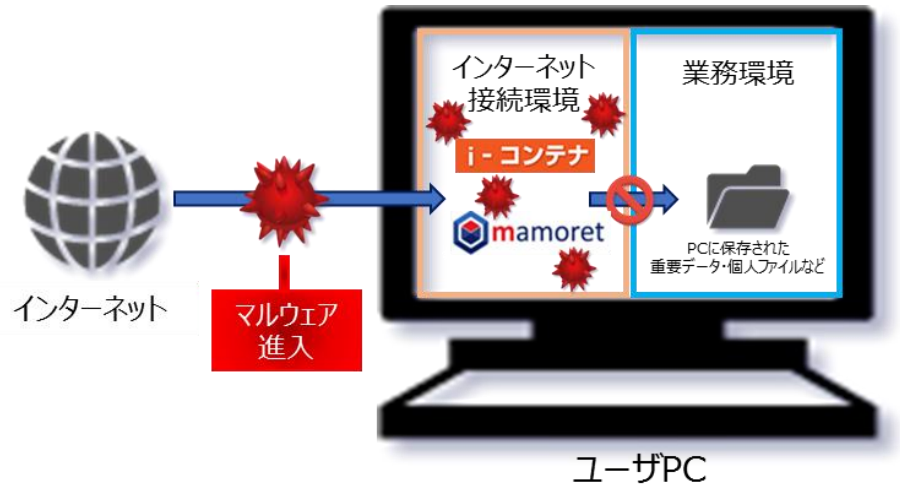
⑴ 対策概要

SecureSoft i-コンテナ及び SecureSoft mamoret（以下、i-コンテナ／mamoret）は、それぞれコンテナ技術を利用したインターネットアクセス専用のネットワーク分離ソリューションです。

上記**「4-(2)-③」**に記載した十分なセキュリティ対策を施すには、i-コンテナ／mamoret を使用することをお勧めいたします。

⑵ i-コンテナ／mamoret とは

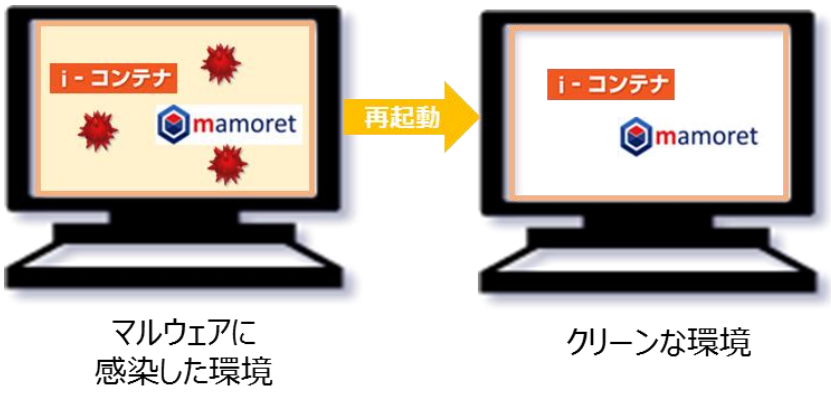
１台の PC を通常業務環境用のデータ領域とインターネット接続用のデータ領域に分離するソフトウェアです。
万が一、マルウェアがインターネット接続環境に侵入しても通常業務環境のデータを保護することができます。



【図　2】i-コンテナ／mamoret による業務環境の保護イメージ

また、i-コンテナ／mamoret には自動初期化機能があり、i-コンテナ／mamoret 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事が出来ます。



【図　3】インターネット接続専用環境の初期化イメージ

⑶　i-コンテナ／mamoret を使用した運用例

i-コンテナ／mamoret 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 メールはインターネット接続環境で閲覧

メールをインターネット接続環境で閲覧することで、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。

【i-コンテナ利用の場合】

メールソフト[1]や Web メールを利用します。

【mamoret 利用の場合】

Web メールを利用します。

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、i-コンテナ／mamoret 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 i-コンテナ／mamoret 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 i-コンテナ／mamoret 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

[1] 対応するメールソフトについては弊社までお問い合わせください。

«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