2016 年 12 月 2 日
株式会社セキュアソフト

注意喚起：増加するランサムウェアの脅威

2016 年 4 月にランサムウェアに関する注意喚起を掲載しましたが、半年経った今でもランサムウェアの脅威は増加しています。トレンドマイクロでは、Q3（2016 年第 3 四半期（7~9 月））のランサムウェアの検出台数が３４２００台で Q2 の約 4 倍であるとの情報を公開しています。ランサムウェアの脅威増加の原因のひとつに、標的型メールの巧妙化があります。最近では、「お世話になります。以上、宜しくお願いいたします」といった日本語での標的型メールが増加し文面がとても巧妙化されています。また、マルウェアをメールに添付するのではなく、本文や添付した PDF ファイルにクラウド・オンラインストレージサービス（ファイル共有サイト）の URL を記載して、URL にアクセスさせることでマルウェアをダウンロードさせるといった、アンチウイルスソフトなどで検出されないよう巧妙化されています。

巧妙な標的型メールへの対策について弊社製品を例に紹介します。

■ランサムウェアに感染しても影響がない仮想環境でのインターネット接続

SecureSoft i-コンテナ（以下、i-コンテナという）ではローカル環境※1 とインターネットアクセス環境を論理的に分離するため、仮にランサムウェアに感染してデータが暗号化されデータが見られなくなったとしても、i-コンテナを再起動するだけで i-コンテナ内の情報は初期化されるため、ローカル環境に影響は及びません。また、ローカル環境と i-コンテナ内は分離されているためウィルスの拡散を防止します。

※1:インターネットに接続しないオフラインの作業環境

i-コンテナを利用したランサムウェアへの対策の一例

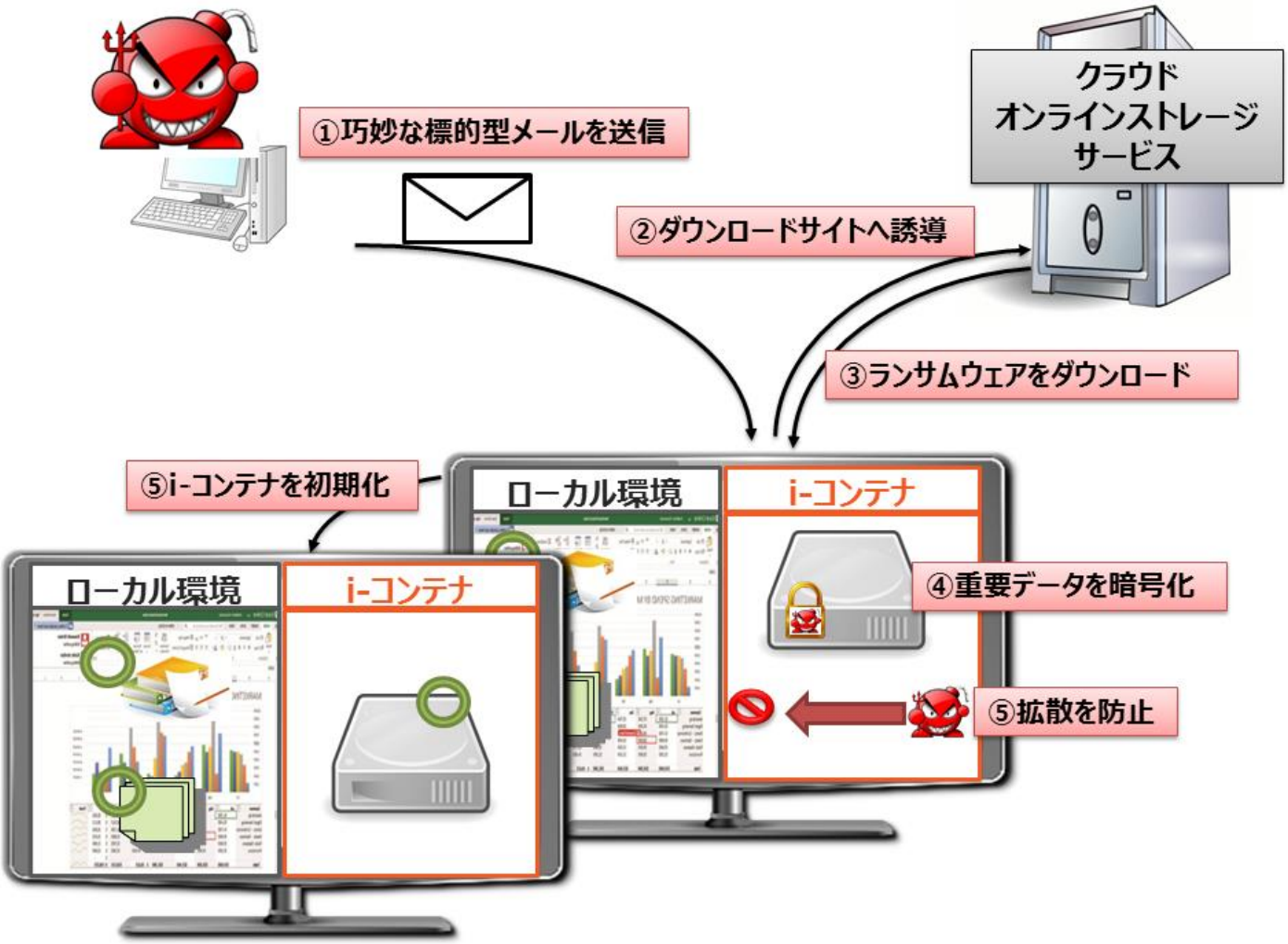
① 巧妙な標的型メールを送信
攻撃者は「お世話になります。以上、宜しくお願いいたします」といった日本語での標的型メールを送信します。

② ダウンロードサイトへ誘導
利用者は業務に関する資料のダウンロード用 URL だと思い、メール本文に記載されている URL にアクセスします。

③ ランサムウェアをダウンロード
利用者は攻撃者が用意したランサムウェアをオンラインストレージサービスからダウンロードします。

④ 重要データを暗号化
i-コンテナ内でランサムウェアが実行され重要データが暗号化されます。重要データが暗号化されているため、メールの閲覧や Web ブラウジング等ができなくなります。ランサムウェアはネットワーク内で拡散を試みますが、ローカル環境と i-コンテナは分離しているので感染拡散を阻止します。

⑤ i-コンテナを初期化
利用者が i-コンテナを再起動することで初期化され、暗号化されていたデータが初期状態に戻ります。また、i-コンテナ内のランサムウェアも除去されます。



以上