【Technical Report16-06】

2016 年 4 月 28 日
株式会社セキュアソフト

注意喚起：ランサムウェアの脅威急増とセキュアソフト i-コンテナ活用について

1. ランサムウェア被害の増加

4 月 13 日に IPA からランサムウェア感染に関する注意喚起がなされており、実際に被害に合う企業が急増しています。IPA への相談件数は、2 月と 3 月を比較すると 17 件から 96 件と約 5.6 倍に増加しており、そのうち約 88%で被害を確認しています。

ランサムウェア感染時の被害を最小限にとどめるため、普段より以下の対処をされることをお勧めいたします。

- アンチウィルスソフトの最新化を怠らない。
- 心当たりのないメールの添付ファイルを開かない。
- フリーソフト等のインストール時に提供元に注意する。
- データのバックアップを定期的に実施する。

2. SecureSoft i-コンテナ活用によるランサムウェアの回避

SecureoSoft i-コンテナは PC 上にインターネット接続専用環境と通常環境の分離を実現するソリューションです。
i-コンテナを活用する以下の構成を取ることで、ランサムウェアの被害を回避することが可能です。

【構成条件と攻撃からの対処ロジック】

1. **インターネットアクセス環境側でメール受信を Web ブラウザメール利用とする。**
   悪質なランサムウェアが添付されたメールのファイルを開いたり、不正サイトからランサムウェアをダウンロードしてしまった場合においても、i-コンテナにより分離された環境だけが攻撃対象となり、被害が発生しません。
   さらに、i-コンテナの仮想ドライブ初期化機能により、i-コンテナ終了時にランサムウェア自体も削除されるため、安全が確保されます。

2. **大事な業務データは通常業務環境側での利用・保管・管理とする。**
   i-コンテナの機能により、通常業務環境側のデータ領域と、i-コンテナによるインターネット利用のデータ領域は分離されるため、i-コンテナ内に侵入したランサムウェアは発症することができません。

【図】i-コンテナ環境に侵入したランサムウェアの分離イメージ

セキュアソフト　コンテナ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

以上