News Release

2017 年 5 月 16 日

ランサムウェアから重要情報を守る「SecureSoft コンテナシリーズ」

株式会社セキュアソフト

ランサムウェア「Wanna Cryptor」（別名：WannaCrypt、WannaCry、WannaCryptor、Wcry）が猛威を奮っており、国内大手企業での被害も観測されています。株式会社セキュアソフトが提供する「SecureSoft コンテナ シリーズ」は今回のようなランサムウェア被害を防止できる最適なソリューションです。Securesoft i-コンテナ(以下 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企業向け製品です。また、Securesoft mamoret（以下 mamoret）は、インターネット接続はブラウジングだけという利用者向けの製品です。i-コンテナ/ mamoret を活用して、ランサムウェアの被害を防止することが可能です。

■ SecureSoft i-コンテナ / SecureSoft mamoret によるランサムウェア対策とは

ランサムウェアを始めとするマルウェアは外部から様々な手法で PC に配布され、実行されます。感染経路の多くはメールでの添付ファイル、不正サイトからのダウンロード、そして今回の「Wanna Cryptor」ように脆弱性を利用した通信等です。このような巧妙な手法で PC に侵入されても SecureSoft コンテナシリーズではランサムウェアをサンドボックス環境に隔離することで被害を防ぐことが可能です。

対策 1．メールの添付ファイルによる感染を防ぐ

～i-コンテナ／mamoret のインターネットアクセス環境側で Web ブラウザのみ利用～

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でも、i-コンテナ/ mamoret 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/ mamoret の仮想ドライブ初期化機能により、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。

対策２．大事な業務データはインターネットアクセス環境と完全分離

～通常業務環境側での利用･保管･管理～

i-コンテナ/ mamoret 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/ mamoret によるインターネット利用のデータ領域は分離されているため、万が一、ランサムウェアが i-コンテナ/ mamoret 内に侵入しても、大事な通常業務環境のデータは暗号化されず、被害を防ぐことが可能です。

【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（mamoret も同様）

「SecureSoft コンテナ シリーズ」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

■SecureSoft i-コンテナによる「Wanna Cryptor」対策システム構成のポイント

① i-コンテナをインストールする場合、i-コンテナ環境からはインターネット、ローカル環境からはイントラネットのみアクセス出来るように事前に設定します。

② マルウェアの最初の感染経路はインターネットからの為、i-コンテナインストール後に侵入したマルウェアは i-コンテナ環境でダウンロード、実行されます。このような場合、i-コンテナ環境からアクセス可能なネットワークはインターネット環境のみの為イントラネットへの拡散を遮断し、マルウェアによる直接的な被害も i-コンテナ環境に限定されローカル環境に影響を及ぼしません。

③ 万が一、社内にローカル環境側でマルウェアに感染した PC がある場合、i-コンテナをインストールしているかに関わらず、445 ポートを通じて他 PC に拡散される可能性がある為、社内にある全ての PC に i-コンテナをインストールし、インターネットへのアクセスは i-コンテナ環境からのみ可能に制限する事が重要となります。

■更なる防御に SecureSoft Sniper シリーズ

ネットワークセキュリティ対策製品「SecureSoft Sniper シリーズ」では、今回のランサムウェア拡散の原因である SMBv1 脆弱性を利用した不正な通信を検知する下記シグネチャをリリースしました。やむを得ず Windows アップデートができないシステムでは Sniper IPS/ONE による対策で検知・防御が可能です。

対象シグネチャ：

[3477] MS Windows SMB SrvOs2FeaToNt RCE

[3484] MS Windows SMB Doublepulsar Kernel Dll Injection

セキュアソフトでは Securesoft コンテナシリーズ、SecureSoft Sniper シリーズを利用して様々な脅威からお客様の安心・安全に寄与してまいります。

■製品に関するお客様からのお問い合わせ先

株式会社セキュアソフト 営業本部担当 柴田 和幸

製品お問い合わせ窓口：TEL 03-5464-9966

(受付時間：9 時～17 時／土・日・祝日は除く)

お問い合わせ Web フォーム： https://www.securesoft.co.jp/contact/

■報道関係者様からのお問い合わせ先

株式会社セキュアソフト 広報担当 岡﨑 由佳

〒150-0011 東京都渋谷区東 3-14-15 MO ビル 2F

TEL：03-5464-9966 FAX：03-5464-9977 E-Mail：press@securesoft.co.jp