株式会社JSecurity

侵入後の被害を軽減する新しいアプローチのランサムウェア対策

バックアップ機能を一体化して実現した高い防御力

世界中で猛威を振るった「WannaCry」をはじめランサムウェアが流行している昨今、ユーザーにとって、その対策は急務だ。しかも攻撃者は高度な手口を駆使しており、既存セキュリティでは感染を防ぎきれない。そこで新たなアプローチとして、ファイルを毀損するランサムウェア特有の活動を検知してそれを防ぎ、あらかじめファイルを保護して実害を抑えるというセキュリティソフトが登場した。JSecurityが提供している「AppCheck」だ。

アンチウイルスも バックアップも対策には万全でない

世界的に流行した「WannaCry」や「Petya」をはじめ、ランサムウェアが猛威を振るっている。攻撃者の言いなりに身代金を支払ってしまうユーザーも少なくないが、必ずしも元に戻してもらえるとは限らない。しかも近年のランサムウェアは、セキュリティを回避するさまざまな手口を取り入れており、対策は年々難しくなっているとされる。

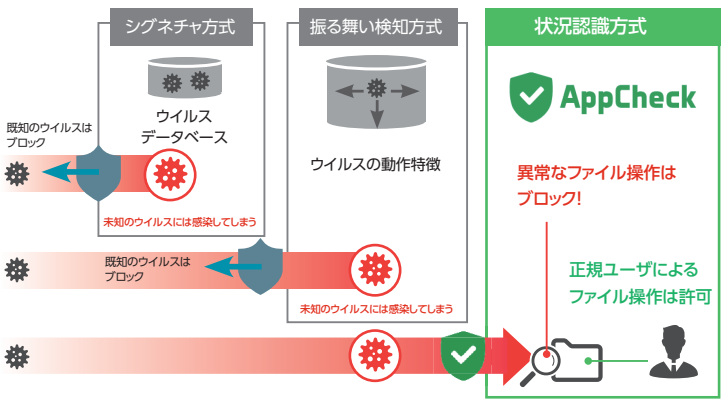
対策として一般的なのはアンチウイルスソフトだが、その伝統的な検知技術であるシグネチャ方式は、セキュリティベンダーがマルウェアの検体を入手してからパターンファイルとして登録するまでにタイムラグがあるのが課題だ。攻撃者はそのタイムラグを利用し、ベンダーが間に合わないうちに新種を作っては拡散させることで、被害を増やしている。

そこでベンダー側でも振る舞い検知やサンドボックスなどの新たな検知技術を取り入れてきているが、これらも一長一短あり、決して万全な対策とは言い切れない。そもそもアンチウイルスは、マルウェアを検知してブロックすることを基本とするものであり、何らかの方法でコンピュータ内に侵入してしまった場合の被害軽減には適さない。

被害を軽減する策としては、バックアップによるファイル保護が有効だ。とはいえ、バックアップ先までランサムウェアの標的にされては意味がないので、何らかの方法でランサムウェアから保護されたバックアップを作成することが最低条件となる。また、もしランサムウェアの活動に気付かず上書きバックアップを行ってしまえば正常なデータが失われることになるため、その回避策も欠かせない。一般的なバックアップツールでは、こういった対策が必ずしも万全とは言えないのが課題だ。

ランサムウェア保護の 新たなアプローチ

ランサムウェアを検知するセキュリティと、ファ



従来のアンチウイルスとAppCheckのマルウェア検知の比較

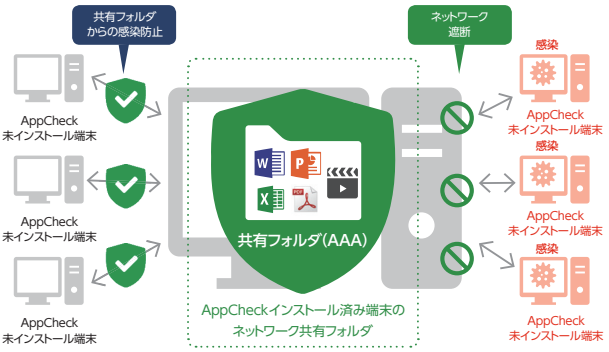
イルを守るバックアップ。これら両方の機能を備えることで、より実効性の高い防御を実現できる。その新たなアプローチを実装したソリューションが、JSecurityのAppCheckである。

本ソリューションは、いわばランサムウェアなどのファイルを毀損するマルウェアからファイルを保護するソフトウェアといったところだ。まず、指定したファイルやフォルダを定期的に安全な領域へバックアップすることで事前の備えとしている。加えてリアルタイムのバックアップ・復元機能を搭載し、マルウェアによる変更や削除などのファイル毀損行為から保護することができる。このリアルタイムバックアップ機能は、マルウェアによる異常なファイル操作を検知する状況認識技術によって発動し、先回りしてファイルの保護を行う。

具体的には、例えば連続していくつものファイルを書き換えるような動作や、書き換えられた後の内容などを総合的に判断し、ユーザーによる正当な操作とランサムウェアなどによる異常な操作を識別する。近年のマルウェアでは、アンチウイルスが持つ多彩な検知技術を回避しようとさまざまな策が講じられているが、この状況認識技術は実環境での動作結果そのものをリアルタイムに監視しているため、そうした回避策がほとんど意味をなさないこともポイントだ。

さらにAppCheckは、定期／リアルタイムのバックアップ以外のさまざまな保護機能も備えている。例えば、一部のランサムウェアはディスクの起動領域やパーティション情報が格納されるマスターブートレコード（MBR）などを改変することがあるが、それに対抗するMBR保護機能も搭載した。

ネットワーク経由で感染を拡大しようとするランサムウェアに対しては、その拡大を阻止する働きを持つネットワーク遮断機能や共有フォルダ保護機能を搭載している。ちなみにAppCheckにはWindows Server版も用意されており、Windowsベースのファイルサーバ やNASなどもランサムウェアから保護することができる。



ネットワーク遮断機能で共有フォルダも保護可能

既存の対策と組み合わせ一歩先のランサムウェア対策を

AppCheckのコア技術の1つである状況認識技術は、アンチウイルスのパターンファイルと違って頻繁な更新が不要で、長期間に渡って安定した防御性能を発揮することができる。例えば、世界中で猛威を振るったWannaCryに対しては、約2年前にリリースされた認識エンジンで防ぐことができたという。

しかも、AppCheckはアンチウイルスと違って負荷も軽い。シンプルなソフトゆえ設定や操作は簡単でユーザーにも親しみやすく、クラウドサーバを通じた集中管理もオプションで可能だ。

さらに、本製品は既存アンチウイルスとの共存が可能であり、アンチウイルスにないアプローチを用いた状況認識技術によって、アンチウイルスを補完するかたちでセキュリティを強化するとしても有効だ。同様に、既存のバックアップツールとも補完関係にあるといえるだろう。

JSecurityによると、その独自性と効果を高く評価してAppCheckを扱い始めた国内の販売／SIパートナー企業も多いとのことだ。前述のように既存環境に追加するだけで利用できるため、アンチウイルスソフトの移行よりずっとハードルが低い。ランサムウェアによる損失を避けたいなら、検討してみる価値はあるだろう。

JSECURITY

株式会社 JSecurity

〒160-0022　東京都新宿区新宿6-29-20 MATSUDA BLD. 7F
お問い合わせ　TEL.03-5155-1915（代表）
https://appcheck.jp/