AppGuard® *powered by Blue Planet Works*

完全に WannaCry ランサムウエアを阻止し、脆弱性のある OS も完全防御

2017 年 5 月 13 日に欧州 100 か国で Windows OS の脆弱性を狙うランサムウエア（WannaCry、または WCry）が猛威を振るい、7 万 5000 件以上の被害が出たと各メディアで伝えられました。メディアによると、ウイルスは、米国家安全保障局（NSA）が開発し保管していたものとみられ、ハッカー集団が盗み出したとされております。Microsoft 社の Windows OS の脆弱性が狙われ、被害は全世界へと一気に拡大しました。

Blue Planet-works 社が提供する AppGuard®セキュリティーソリューションは、この脅威を完全に阻止、遮断し、例え脆弱性のある OS をも完全に防御致します。この度の攻撃においても、AppGuard®テクノロジ搭載のデバイスは完全に防御され、攻撃を未然に阻止・遮断しております。

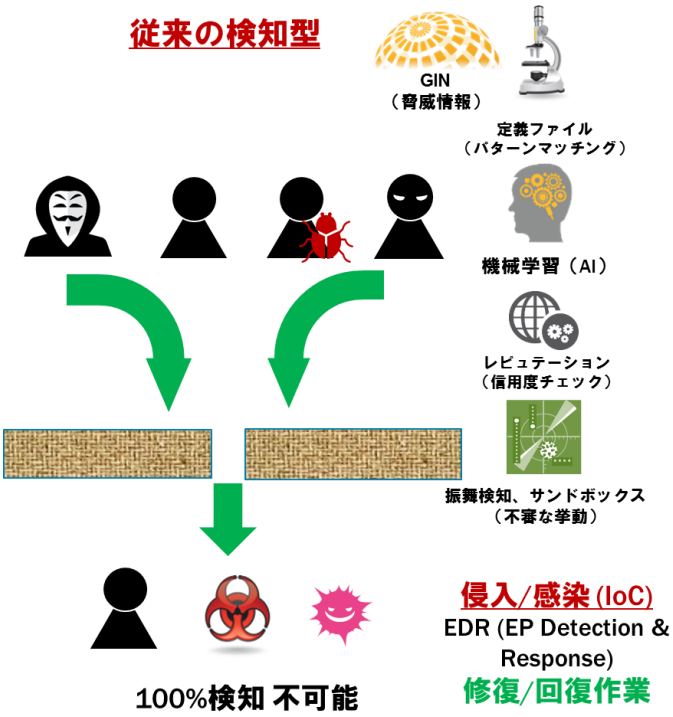
AppGuard®テクノロジの仕組み：

AppGuard®セキュリティ・フレームワークの基本理念は、「システムを正しく機能させ、安全に動作させます」。言い換えれば、システムが安全に動作すれば、脅威からも防御されている事になります。シンプルにしますと、システム上での不正動作、不正行為を完全に遮断する仕組みになっております。つまり、OS に脆弱性があろうが、今回のようなマルウエアが未知のランサムウエアであろうが、ゼロデイ攻撃であろうが、既知のマルウエアであろうが、ファイルを持たない Fileless マルウエア、実行ファイルを持たないスクリプト型の攻撃、メモリに直接アクセスして不正に情報を奪取する行為など全てを完全に阻止し、その不正行為そのものを完全遮断致します。

AppGuard®のエンジンは、非常に軽量で、高速に動作します。エンジンそのものは、1MB 以下と他のセキュリティーソリューションと比べ、大幅に軽量です。また、実際に不正行為そのものを阻止する（正常動作のみ可能にする）テクノロジを Isolation Technology と呼んでおります。運用面においても AppGuard®テクノロジは、とても軽快であり、一度システムにインストールすれば、アップデート無しでシステムを防御致します。

従来の「検知型」のセキュリティ・テクノロジーとの違い

今までのセキュリティ・テクノロジは、多くの脅威情報（検体の標本）を収集し（Global Intelligence Network – 通称 GIN）それらを基にパターンマッチング（標本との比較）を行う技術がベースになっております。パターンマッチングには、古くからある定義ファイル型（シグネチャー）、このコンセプトを応用した機械学習/Machine Learning 型、標本と比較してある基準値を超えた疑わしいものをエミュレーター上で起動させるサンドボックスや振舞検知型、レピュテーション型（ファイルを標本と比較した信用度調査）などがありますが、これらは全て「検知型」と言われ、比較する脅威情報（検体の標本）がベースとなっており、新種のマルウエアや今までとは全く違う脅威の場合は、検知が難しくなります。結果的に、検知型は理論上 100%の検知が不可能です。その反面、Blue Planet-works 社が提供する AppGuard®テクノロジは、基本概念が異なります。シンプルに、システムの原理原則の部分で「不正行為をさせない事により、システムが安全にかつ正常に動作・機能させます」。これにより、システムを脅威より完全防御しております。脅威の種類は未知であろうが、既知であろうが、関係ありません。システムに対しての不正な行為そのものを完全に阻止し、遮断致します。



上記の理由により、この度、世界的な猛威を振るったランサムウエア、WannaCry に対しても、AppGuard®テクノロジは、システムを完全に防御し、不正な行為を遮断し、システムを守りました。