CylancePROTECT+
メモリ保護

複雑な構成を必要としないメモリ保護

CylancePROTECT は、世界初の数学と機械学習をベースにしたエンドポイント保護製品であり、事前に知られていないマルウェアであっても、それを検出し、実行を防止できます。また、マルウェアの可能性のあるファイルを、100 ミリ秒以内に解析できます。CylancePROTECT は、オペレーティングシステム（OS）とメモリの 2 つのレイヤーでファイルのエクスプロイトを検出し、悪意のあるペイロードの配布を防止します。

CylancePROTECT のメモリ保護機能は一般的なホスト型侵入防止システム（IPS）の機能と似ていますが、CylancePROTECT は複雑な構成を必要としません。このメモリ保護機能により、セキュリティに新たなレイヤーが加わり、データ実行防止、アドレス空間レイアウトのランダム化、高度な緩和エクスペリエンスツールキットなどの OS の基本的な保護機能が強化されます。

多くの侵害イベントでは、良性のプロセスが悪意のあるペイロードのコードによって利用されます。最も一般的な事例として、ユーザーが悪意のある Web サイトを参照したり、悪意のあるドキュメントを実行したりすることが挙げられます。こうした状況では、悪意のある新しい実行可能ファイルを作成または実行する必要はなく、ブラウザーやアプリケーションのメモリ内で攻撃者のペイロードのコードが実行されてしまいます。CylancePROTECT をサーバーに展開した場合、バッファオーバーフローや解放済みメモリ使用などの一般的な脆弱性を利用した多くのエクスプロイトが、メモリ保護機能によって防止されます。

CylancePROTECT のメモリ保護モジュールは、保護対象のプロセスにロードされるエージェントのダイナミックリンクライブラリと、構成を提供し、情報を受け取り、イベントに対応するサービスコンポーネントによって構成されています。エージェントは、状態を維持し、セキュリティ侵害の兆候である特定のハードコードされた動作を監視するため、さまざまなユーザーモジュールの API（アプリケーションプログラムインターフェイス）関数をフックします。そのような動作が検出されると、フックされた API 関数の実行を許可する前に、サービスにイベントが通知されます。サービスは応答を返し、エージェントが実行すべきアクションを通知します。エージェントが行うアクションには以下のものがあります。

- 違反を無視し、実行を許可する
- 違反に関する警告を生成するものの、実行を許可する
- 違反をブロックし、警告を送信する
- プロセスを完全に終了させる

CylancePROTECT の管理者は、ポリシーの中でこれらのアクションを簡単に構成できます。メモリ保護は 32 ビットと 64 ビットのいずれのプロセスでも有効であり、パフォーマンスに大きなオーバーヘッドを発生させずに保護を行うよう設計されています。

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)

201803-FF002