MORPHISEC
Moving Target Defense

INTELLIGENT WAVE INC.

Press Release

2018 年 10 月 25 日
株式会社インテリジェント ウェイブ

“マルウェアが実行不可能な状況”を作り出す プロアクティブ防御

攻撃を成立させない、新世代のエンドポイントセキュリティ対策製品

イスラエル発・新セキュリティソリューション「Morphisec」

メモリー空間の配置を毎回ランダマイズして攻撃を無効化

10 月 2 日、米 国土安全保障省・科学技術局から、金融機関への
サイバー攻撃を防御する技術でアワードを受賞（海外企業で初）

株式会社インテリジェント ウェイブ（本社：東京都中央区、代表取締役社長：井関 司、以下：IWI）は、マルウェアの“実行が不可能な状況”を作り出す新世代のエンドポイントセキュリティ対策製品「Morphisec」（モルフィセック）につき、同製品を開発しグローバルで展開するイスラエルの IT セキュリティ企業、Morphisec 社と国内販売契約を締結し、本日より同製品の販売を開始します。

標的型攻撃の 80%はエンドポイントからの侵入で、侵入の 75%で感染の際にファイルレスのメモリー内攻撃が行われているとされています（ポネモン研究所（米ミシガン州）2017 年 11 月発表の調査）。脆弱性を突くエクスプロイト対策が特に重要である所以です。

これまでのエンドポイント保護製品は、既存マルウェアを基にした検知から、AI を使った既存マルウェアテクニックからの推測による検知へと進化してきましたが、今「攻撃を成立させない」考え方で、未知の攻撃からの保護も可能にした Morphisec の登場によりさらなる進化を遂げようとしています。

Morphisec は、マルウェアが悪用する OS やアプリケーションのメモリーアドレスをプロセス生成毎に変化させることで、マルウェアや脆弱性を悪用するコードの実行を不可能にする、新世代のエンドポイントセキュリティ対策製品です。未知の攻撃やゼロデイ攻撃、ファイルレスマルウェア、プロセスの空洞化など、高度な攻撃を実行不可能にします。シグネチャーベース、振る舞い検知、AI などの防御製品と全く異なった技術を用いているため、過去の対策手法に依存しない製品です。

従来の製品は、攻撃動作の実行を見つける反応型検知であり、本質的に攻撃者優位（後追い）です。対して Morphisec は攻撃目標（脆弱性、dll、アプリのメモリー空間）を変化させることで、マルウェアの実行ができなくするものであり、唯一の防御者優位のソリューションといえます。

■Morphisec の特長

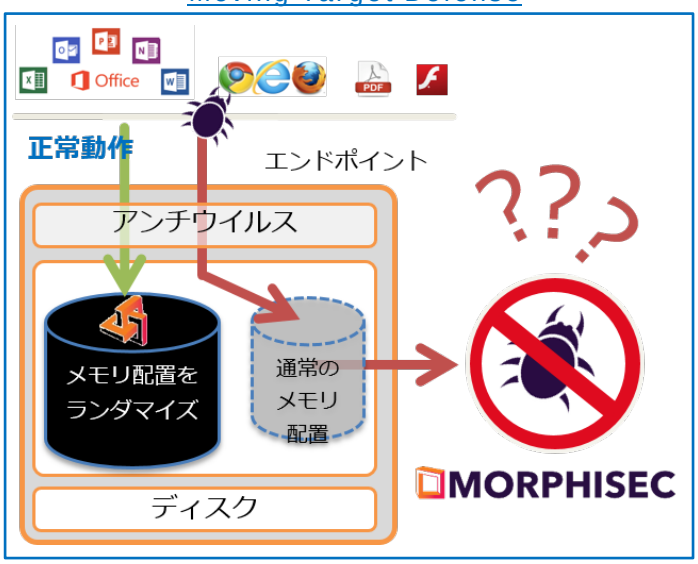
●1 Moving Target Defense（MTD）

「Moving Target Defense」は、アプリケーションが起動するたびにローディングするメモリーアドレスを毎回ランダマイズすることにより、攻撃を防御するのではなく攻撃を成立させなくする技術で、Morphisec の中核技術です（特許取得済）。シグネチャー更新が不要であるため、オフラインでも問題なく動作します。

<ステップ 1> 攻撃者からターゲットを見えなくする

アプリケーション、Web ブラウザ、または OS が起動され、メモリー空間にロードされると、

Moving Target Defense



Morphisec は、ライブラリー関数やライブラリーアドレスなど各実行プロセスの内部配置をランダマイズします。ランダマイズされたメモリー空間（上図の「メモリ配置をランダマイズ」）を攻撃者が予測することは不可能になります。

<ステップ 2> メモリーマッピング

正常なアプリケーションはランダマイズされたメモリー空間で通常通りに実行されるとともに、Morphisec はランダマイズされる前のオリジナルのメモリーマッピングをトラップとして準備します。（上図の「通常のメモリ配置」）

<ステップ 3> 攻撃者を欺き、中立化

攻撃者の悪意あるコードは、新しいメモリーマッピングを知る術がなく、いかなる必要な機能にもアクセスできないため、実行ができません。攻撃は、オリジナルのメモリーマッピングを標的にし続けますが、それはおとりに過ぎません。

<ステップ 4> トラップと管理

おとりのメモリーマッピングに対する攻撃が検知されると、フォレンジック分析のために Morphisec Management Dashboard または SIEM に記録されます。

●2　Install & Forget!・・追加設定・更新が原則不要

企業の導入・展開においては、一度インストールすれば、後は何もする必要がありません。またアプリケーションがメモリーにロードされる瞬間だけアクティブとなるサービスであるため、以下のような特長を持ちます。

・インストール後の再起動必要なし
・シグネチャー更新が不要のためオフライン環境でも問題なく動作
・追加の設定項目なし
・DB、シグネチャーのためのキャッシュメモリー不要
・アプリケーションへの依存なし
・誤検知がほとんどない
・インジェクション対象が少ないため競合が発生しにくい
・CPU・メモリー負荷が非常に低い
・ネットワーク負荷がない

非常に軽量なエージェント「Protector」

・最小限の CPU、メモリー消費にて動作する
・2MB DLL、ユーザーモードでの動作、MSI
・Windows 7、8、10、2008、2012、2016 に対応

●3　管理サーバー未接続でも防御が可能

端末単体で保護が完結するため、独立したネットワーク環境（Morphisec 管理サーバーと未接続）での利用も可能です。Morphisec は、オフィス環境の Windows サーバーや PC はもちろんのこと、社外持ち出し端末（ノート PC）やメモリーリソースの乏しい端末、工場の制御系 PC、ATM、POS 端末、など非常に広範な用途が想定されます。

●4　ASLR（Address Space Layout Randomization）との相違

重要なデータ領域の位置をランダムに配置することで「脆弱性を悪用した不正なコードの実行を難しくする」セキュリティ機能として Windows Vista 以降、Windows に標準搭載されてきた ASLR は、Morphisec とは大きく異なるものです。ASLR のアドレスランダマイズ基数更新は、OS 起動のタイミングで変更するのみでブルートフォースに弱く、2017 年には脆弱性が発見され米セキュリティ研究機関から注意喚起がなされるなど、利用には注意が必要となるだけでなく、攻撃防御では不完全です。

★米政府よりサイバー攻撃防御技術でアワードを受賞

本年 10 月 2 日に Morphisec は、海外企業では初めて、アメリカ合衆国国土安全保障省（DHS）の科学技術局から、金融機関へのサイバー攻撃を防御する技術に関してアワードを受賞しました。仮想デスクトップインフラストラクチャ（VDI）の全体的なパフォーマンスを低下させることなく、金融機関を攻撃から保護するためのサイバーセキュリティ製品の開発とテストをサポートしたことが評価されたものです。

https://www.dhs.gov/science-and-technology/news/2018/10/02/news-release-israeli-morphisec-gets-200k-cybersecurity-tech

■国内販売戦略

導入実績・ターゲット　今回の発売リリースにより日本での展開を開始する Morphisec は、既に米国の金融、ハイテクマニュファクチャリング、欧州大手製造、米ホテルチェーンなど、Forbes500 企業を含む多数の企業に導入されています。国内でも金融、製造、小売、通信など、既存顧客以外の分野を含めた幅広い業種に対し、オフィス内端末以外に加え、製造・設備など独立ネットワークでのさまざまな環境の端末への導入を提案していきます。

本ソリューションの価格は、対象端末毎の年間サブスクリプションライセンスで、契約台数の規模や多年度契約により価格は異なりますが、最小単位で 1 台あたり年間 5,000 円（税別）となります。初年度は売上目標 2 億円を計画しています。

今後 IWI は本ソリューションを、自社開発の情報漏洩対策製品「CWAT」、パロアルトネットワークス社のサイバーセキュリティ対策製品「Traps」、あるいはイスラエルを中心とした海外開発ベンダーが提供する各セキュリティ製品と組み合わせ、統合的なソリューションやサービスを開発し提供していきます。

IWI では取扱い製品を**自社内導入**していくことを基本としています。本製品も自社導入を通して実運用に精通し、顧客サポートの改良や品質向上に繋げていくとともに、Morphisec 社に対して国内市場向けの改善要求の提示などを行っていきます。

以上

【Morphisec（モルフィセック）について】

イスラエルの国立サイバーセキュリティセンター（ベングリオン大学サイバーリサーチラボ）からスタートした Morphisec（モルフィセック）社は、一貫して攻撃の優位に立ち組織を維持し続ける Moving Target Defense 技術によって、サイバーセキュリティのゲームのルールを根本的に変貌させます。製品「Morphisec Endpoint Threat Prevention」は、ゼロデイ攻撃など先進攻撃からダメージを受ける前にリアルタイムで防御します。

設立は 2014 年 7 月。2016 年 5 月に製品をリリースし、2018 年 10 月時点ではイスラエル南部地区のベエルシェバと米ボストンの両本社で約 100 名の従業員という規模となっており、7 つの特許を取得済。Fortune500 の米製造会社など、グローバルで 150 万台のエンドポイントに導入されています。

https://www.morphisec.com/

【インテリジェント ウェイブについて】

株式会社インテリジェント ウェイブ（東証二部：4847）は、情報システムのソリューションプロバイダーとして、クレジットカード決済システムにおけるオンラインネットワーク基盤のシステム構築事業を主軸に、証券市場向け超高速株価情報システムなど、金融業界向けシステムの開発・構築・保守に強みを持ち、コンポーネント・テクノロジーを統合したシステムソリューションを提供しています。

一方で、急増の一途を辿る企業への脅威に対応するため、セキュリティシステム事業の拡充深耕を継続しており、時代の要請に応えて進化し続ける内部情報漏洩対策製品「CWAT」を核に、高度標的型攻撃対策としてのエンドポイントソリューション「Traps」（パロアルトネットワークス社）、攻撃者を騙して侵入を検知し、進入路を塞ぎ、隔離する Illusive Networks 社「Deceptions Everywhere」、CSIRT 運用を自動化するオートメーションツールの Ayehu 社「eyeShare」、APT 攻撃予兆自動検出ソリューション「SecBI」など、広範な領域をカバーする先進のセキュリティソリューションを統合的に提供しています。
詳しくは http://www.iwi.co.jp/ または http://www.iwi-security.jp/ をご参照ください。

※記載の商品名、会社名は各社の商標または登録商標です。

読者からのお問い合わせ先：	報道関係のお問い合わせ先：
株式会社インテリジェント ウェイブ セキュリティソリューション本部 TEL：03-6222-7300　FAX：03-6222-7301 iwi_security@iwi.co.jp	IWI セキュリティソリューション広報事務局 (株)アルサープ内 河端・川口 TEL：03-4405-8773 iwi-security@alsarpp.co.jp