Press Release

2017 年 9 月 28 日
株式会社インテリジェント ウェイブ

世界的規模の国内大手金融機関が、イリュージブ社の標的型攻撃対策 Deceptions Everywhere®を導入

Deception（欺瞞）技術により、高度な技能を持つ攻撃者の手動侵入を検知

「未対策の新たな領域には、実効性が高く、新発想の標的型攻撃対策が必要」、“侵入は止められない”認識による導入

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、自社が販売提供する、イスラエルの先進セキュリティソリューションベンダー、illusive networks Ltd.（以下、イリュージブ）の Deception（欺瞞）技術による新しいサイバーセキュリティ対策ソリューション「Deceptions Everywhere®」が、高度な攻撃者の侵入・展開・探索場面における検知対策として、世界的な規模を有する国内の大手金融機関に全社導入となったことを発表します。同製品の国内大手企業への大規模な導入は初となります。

Deceptions Everywhere は、攻撃者の思考を逆手に取る発想から生まれた、まったく新しいコンセプトのサイバー攻撃対策ソリューションで、社内の全てのエンドポイント（サーバー、クライアント機器）に膨大な罠を張り巡らせることで攻撃者を騙し（Deceive）、侵入を検知し（Detect）、リアルタイムかつ即時に調査分析すること（Defeat）により、攻撃対象を隔離するなどの対策を迅速に実行可能にします。本製品のエンジンは、端末やサーバーのメモリーキャッシュに、実際には存在しない各種サーバーへのログイン情報やブラウザの閲覧履歴などを、欺瞞情報（幻-illusion-の情報）として埋め込みます。エンドポイントへのエージェントソフトウェアのインストールは不要。攻撃者に対し実際には存在しない多量のサーバーが存在するネットワークに見せかけ、実在するサーバーにたどり着くことができなくするソリューションです。

当該の大手金融機関は膨大な規模の顧客データ、端末、アプリケーション、ネットワークを有し、国内でも有数の先進的なセキュリティ対策を講じてきていました。同社は、標的型攻撃対策において、これまで攻撃者の侵入防御に万全の対策を導入してきましたが、高度化する一方の攻撃状況を認識し、攻撃のその先＝侵入後、つまり「侵入されても必ず検知し、システムを守る」対策が求められたのです。侵入されることを前提とした対策の導入整備・充実を図るべきとの方針を打ち出し、導入すべきソリューションが検討されました。

導入の目的は、従来対策では防ぐことができず侵入されてしまう高度な攻撃を検知・防御することでした。そのため、従来の侵入防御と同様の概念でなく、全く新しいコンセプトの対策が求められ、イリュージブの Deceptions Everywhere を、攻撃者の行動である侵入、拡大、目的実行の各段階における検知対策・防止対策として選定・導入されました。

攻撃者から侵入されることを前提とした対策の重要性が政府・民間の情報セキュリティ各機関により叫ばれる中、導入実施にいたるケースは未だ稀でした。今回、実際に導入され、当該社のような規模の金融機関がこの対策に正面から取り組んだことは注目に値するといえるものです。

導入規模は数万ライセンスで、5 年一括。当該社は既に多くのセキュリティソリューションが導入され、多数のアプリケーションが稼動しているため、特にエージェントレスであること、および導入・運営が容易であることが重要でした。

当該大手金融機関の情報システム管理部門の責任者は、「サイバー攻撃の進化・高度化が留まることのない中、これからの分野に最適な、新しい概念のソリューションを求めていた当社の要件に合致した製品としてイリューシブの Deceptions Everywhere を導入しました。」と述べています。

IWI は、昨年 6 月の日本での販売開始以来、各方面への製品認知・理解の普及拡大に注力するとともに、イリューシブ社と共同で日本市場のニーズや環境に必要な仕様や機能を開発し、製品に標準実装しています。

■イリューシブ ネットワークスの Deceptions Everywhere について

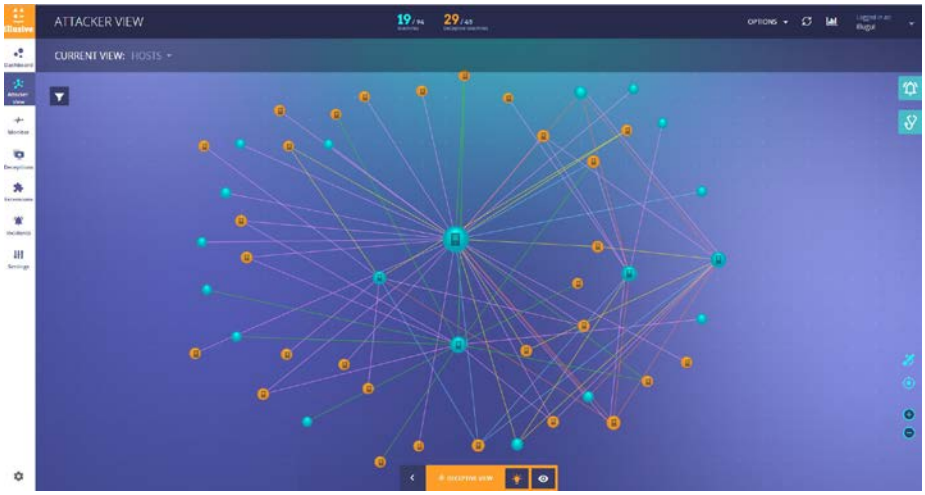
標的型攻撃において攻撃者はエクスプロイトやマルウェアを使用して、特定ターゲットに侵入するためトロイの木馬などの進入路を作り、この進入路を使ってマニュアルで侵入、目的の情報の在処を特定し、搾取します。本製品は、マニュアルでの高度な攻撃を検知することを目的とし、従来の概念にとらわれない新しいコンセプトによるサイバー攻撃対策ソリューションです。検知の視点を攻撃者の活動に特化し、膨大な罠を張り巡らせることで攻撃者を騙し（Deceive）、侵入を検知し（Detect）、リアルタイムかつ即時に調査分析すること（Defeat）により進入路を塞ぎ、攻撃対象を隔離するなどの対策を迅速に実行可能にします。

Deceptions Everywhere のエンジンは、エージェントレスで端末やサーバーのメモリーキャッシュに、実際には存在しない各種サーバーへのログイン情報やブラウザの閲覧履歴などを、欺瞞情報（幻-illusion-の情報）として埋め込みます。これにより攻撃者には実際には存在しない多量のサーバーが存在するネットワークに見せかけます。仮に攻撃者がサーバー間を 3 台横移動すると欺瞞サーバー（存在しない幻の欺瞞サーバー）の比率は 99.2%にまでなり、実在するサーバーにたどり着くことはできません。

同時に、Deceptions Everywhere は欺瞞サーバーへの攻撃者からのアクセスを検知し、警告を挙げ、リアルタイムに攻撃パターンを調査することで、攻撃の影響度の分析が可能となります。一方で、IT 管理者やユーザーには、欺瞞サーバーは見えず、運用に一切支障は来しません。導入には、既存ネットワークの内側に、illusive Management Server、illusive TRAP Server、illusive R-TRAP Server を設置するだけ、エンドポイントへのエージェントのインストールは不要です。

Deceptions Everywhere®の特長：

- 欺瞞情報で攻撃者の行動を翻弄。騙すことにより攻撃を成功させない
- 万が一攻撃者が侵入しても、確実にその攻撃を検知できる
- 過検知・誤検知（フォールス ポジティブ）が発生しない（理論値はゼロ）
- エージェントレス（エンドポイントへのエージェントのインストールは不要）、かつ簡単な操作
- 既存環境へのインパクト、影響がゼロ（ネットワークへの影響もほとんどない）
- ソフトウェア形態で提供。必要なハードウェアはサーバー3 台。仮想サーバーも可



攻撃者からみたネットワーク（ブルーが実在するサーバー、オレンジが欺瞞サーバー）

■セキュリティ市場における Deception 技術（欺瞞）

囮（おとり）のサーバーにより攻撃を無効化する考え方・技術「Deception」には、1998 年に現れた HoneyPot と呼ばれるシステム製品があります。2012 年に現在の HoneyPot2.0 が現れるまで、数年おきに進化変遷を遂げてきたソリューションですが、イリューシブの Deception 技術は、HoneyPot とは大きく異なります。

HoneyPot が仮想 LAN セグメントごとにサーバーを置いて欺瞞情報を設置するのに対し、イリューシブは、エンドポイントごとに欺瞞情報を設置します。イリューシブは、欺瞞情報のソフトウェア的な生成で攻撃者を欺き誘導するため、ネットワーク内に 3 台のサーバーを投入すれば稼働可であり、展開は一度の処理で完了します。HoneyPot に比べネットワーク構造への依存がなく、当初多額の物理・仮想サーバー導入コストは不要となります。完全自動で、エージェントレスであるため、導入、拡張が容易です。

エンドポイントに基づく欺瞞技術であるため、実際のエンドポイントに配布された欺瞞情報を用いて、 各エンドポイントを攻撃者にとって回避不能の罠（攻撃検知センサー）として活用します。早期かつ高精度な攻撃検出を行い、同時にリアルタイムでエンドポイントのさまざまなフォレンジック情報を収集することで攻撃リスクを完全に可視化し、攻撃に迅速かつ的確な対応が可能となります。

偽装テクノロジー「Deception」は、米ガートナー社の 6 月 14 日（米国）発表による「2017 年の注目すべきセキュリティのトップ・テクノロジー」11 項目の中に挙げられています。本製品は既に、米国の金融超大手、ドイツの医療系大手のメルク社、などへの大規模な導入が相次いでいます。

以上

【イリューシブ ネットワークス社について】

illusive networks Ltd.は、2014 年 9 月、Check Point 社の R&D で Endpoint Security Management のチームリーダーであった Ofer Israeli 氏と、サイバーセキュリティ特化の VC である TEAM8 により設立されたイスラエルの新興セキュリティベンチャー。現 CEO は、Ofer Israeli 氏。2 回のラウンドを経て現在の資本金は 3000 万ドル。ニューヨークとテルアビブに拠点を持ち、イスラエル軍セキュリティ機関「8200」や様々なセキュリティ企業出身の技術者で構成される開発拠点をテルアビブに構える。Deception における 2 つの特許を所有し、他 3 つの特許を申請中。従業員は約 70 名。顧客企業は、金融、小売、法律事務所、保険、医療機関、エネルギー、通信など。幾多のアワード受賞歴を保有。

【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（JASDAQ：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「パロアルトネットワークス社 Traps」、攻撃者を騙して侵入を検知し、進入路を塞ぎ、隔離する「イリューシブ社 Deceptions Everywhere®」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