アンラボ・セキュリティレター

Press Ahn

2021.9　Vol.93

EDR 導入後の変化

EDR 導入後の変化

新型コロナウイルス感染症患者に対する疫学調査は、患者の感染経路や動線などの因果関係を把握し、更なる感染拡大を防ぐために行われる。調査を経て収集した情報を分析し、インサイトを導き出すことで、適切な対策案の樹立も可能となる。

同じような概念を持つソリューションが、サイバーセキュリティにおいても脚光を浴びている。それは、脅威検知&対応ソリューションの「EDR」だ。市場調査機関である「ガートナー (Gartner)」によると、EDR のグローバル市場規模は、2015 年の 2 億 3800 万ドル (円換算：約 261 億円) から、2020 年には 15 億ドル (円換算：約 1646 億円) までに成長している。特に、45.3% にものぼる年平均成長率は、注目すべき数値と言えるだろう。

組織が EDR を正しく使用し、導入効果を最大限に引き出すためには、まず先に EDR への根本的な理解が必要となる。今回は、高度化する攻撃手法、および防御技術に関する発展経緯を紐解き、EDR が必要な理由や、導入後のセキュリティシステムの変化について説明する。

EDR の理論的背景を理解するには、まず初めに攻撃の高度化や防御技術がどのように発展してきたかを調べる必要がある。尚、攻撃および防御には様々な技術が駆使されているが、今回は ▲社会工学的技法、▲ファイルレス攻撃、▲行為ベース検知などの核心部分について説明していく。

社会工学的技法を用いた巧妙な流入方法

依然として変わらないハッカー達の共通点とは何か。それはセキュリティの脆弱性を見つけ、執拗に攻撃を仕掛けてくるという点であろう。これは、より容易な方法で大きな利益を生み出すためである。こうした観点から、近年、攻撃者の多くが Web、メール、そして脆弱性を攻撃経路として選んでいる。セキュリティパッチが未適用の応用プログラム、また脆弱性のある Web サイトへのアクセスを利用したマルウェア感染などがその例だ。こうした経路は、過去にも数多くの攻撃に利用されてきたが、時代の変化や攻撃ポイントの分散により、高度化かつ組織化している。

こうした攻撃に対する防御が容易でない理由は、攻撃者が主に"社会工学的"技法を使用しているためだ。社会工学的技法とは、人間の心理を利用した攻撃手法で、攻撃対象を騙し、攻撃者の思惑通りに行為を進める方法である。罠で獲物をおびき寄せる狩りと同じ概念だ。もし攻撃対象が罠にかかれば、攻撃者は望んだ結果を簡単に手に入れることができてしまう。

代表的な事例として、不正なメールを送信し添付ファイルを実行させたり、不正な URL のクリックを誘導する方法が挙げられる。こうした攻撃は、攻撃者の思惑通りに対象者が行為に及ぶという前提のもとで行われている。人は誰しも失敗を犯す可能性がある。特に、緊急時や問題が発生した状況では、誤った判断を下す可能性がより高まる。攻撃者はこうした心理を利用してくるのだ。彼らは攻撃経路を設定する際、セキュリティにおける最も脆弱な部分は、"人"であることを前提に攻撃を仕掛けてくる。

高度化する攻撃手法、 ファイルレス攻撃の増加

上記のように、近年の攻撃は巧妙な手口でセキュリティの脆弱性を狙ってくる。それだけでなく、検知を迂回し痕跡を残さないよう、攻撃動作のパターンも進化を重ねている。

過去に発生したサイバー攻撃のほとんどは、ファイル形式のマルウェアが利用されていた。我々にも馴染み深い実行ファイル、スクリプトファイル、文書ファイルなど、個別ファイルにマルウェアを仕込む手法だ。
また、防御側はアンチウイルス (AV) ソリューションを用い、ディスク内に存在するファイル形式のマルウェアを、検知・遮断することでシステムを保護してきた。

しかし、次に攻撃者は、AV ソリューションの検知・遮断を迂回するため、様々な手法を開発し始めた。その代表的な例が、ファイルレス (Fileless) マルウェアだ。直訳すると、「ファイルがない」という意味を持つこのファイルレスマルウェア。正確な定義としては、「悪意ある機能を作動させるコードがメモリ内でのみ実行され、システムに被害を及ぼすタイプの攻撃」である。

ファイルレスマルウェアは、メモリ内でのみ作動する「インメモリマルウェア (in-memory malware)」と、「LOL (Living Off The Land) ツール」を用い、ターゲットのシステム内に残る攻撃痕跡を最小限に抑えるのが特徴だ。尚、 LOL とは"自給自足"を意味しており、攻撃時に外部ツールではなく、対象システム内にあるパワーシェル (PowerShell) などの正常なツールを用いることが由来となっている。

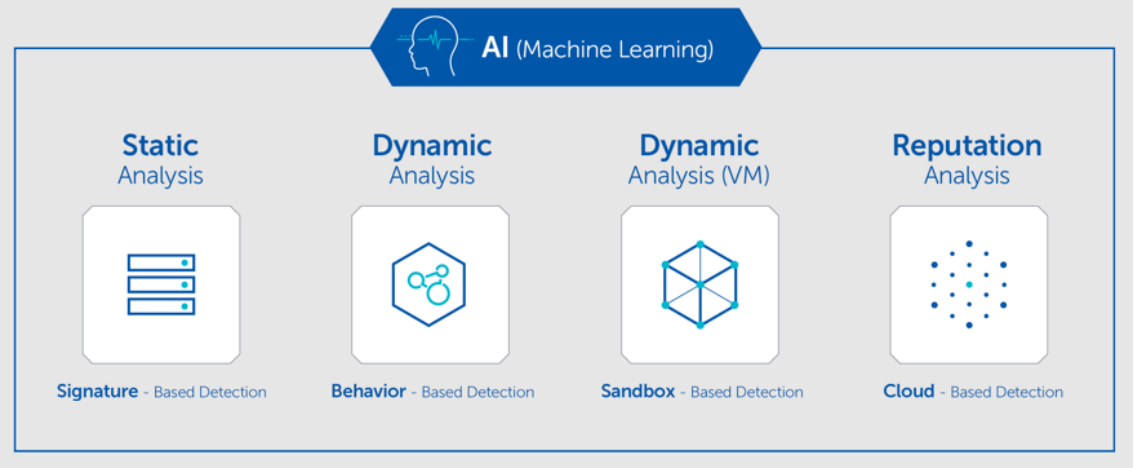
実際に、ハッカーがファイルレス攻撃を成功させたと仮定してみよう。防御側からすると、スキャン対象であるファイル形式のマルウェアが存在しないため、ファイルのモニタリングを行う AV ソリューションを介しての検知・遮断が困難となる。また、攻撃を受けた後もファイルが存在しないため、ファイルのハッシュ (Hash) 値を確認することも不可能だ。すなわち、攻撃を追跡する手がかりが足りず、被害復旧後に対応システムを構立する上でも、限界に直面することになる。

反対に、攻撃者の立場から見たファイルレス攻撃は、不正なファイルを利用していた従来の手法に比べ、AV ソリューション検知を迂回することで攻撃成功率が高まり、なおかつ追跡の危険性がある痕跡を最小限に抑えられる。文字通り「一石二鳥」の効果が得られるわけだ。

セキュリティ技術の発展、ポイントは"行為ベース"検知

次は、攻撃手法の高度化に対し、セキュリティ技術がどのように発展してきたかを見てみよう。セキュリティにおける攻撃と防御は、追いつ追われつの関係にある。特定のセキュリティ技術が登場すると、攻撃者はこれを迂回する攻撃手法を開発する。さらに、この攻撃手法を検知し防御可能な新技術が登場する、この繰り返しだ。

サイバー攻撃に対する検知技術には、▲シグネチャベース検知、▲行為ベース検知、▲仮想環境下で動的分析を行う行為ベース検知、▲レピュテーション分析を介したクラウドベース検知など、大きく 4 つに整理することができる。近年、この 4 つの検知技術に、マシンラーニング技法を適用する場合もある。



[図 1] サイバー攻撃に対する 4 つの検知技術

まず初めに、シグネチャベース検知では、ファイルに存在するデータパターンを確認し、マルウェアの有無を検知する。例えば、BlueCrab ランサムウェアに見られるデータパターンがファイルに存在する場合、BlueCrab ランサムウェアと診断し検知する方法だ。しかし、攻撃者はこのデータパターンを変更することで、シグネチャ検知を迂回することができてしまう。伝統的なシグネチャベースの AV ソリューションのみでは、最新攻撃を防ぎきれないとされる理由がここにある。

攻撃者がシグネチャベース検知を様々な方法で迂回しだすと、セキュリティ企業側は、マルウェアの行為自体は不変であるという点に着目し、「行為ベース検知」技術を開発した。例えば、特定のファイルを作成し、レジストリにあるコードを記録したり、ネットワークにアクセス行為が行われた場合、マルウェアと検知する手法である。

また、企業・組織に流入するファイルの行為分析を仮想環境で行い、マルウェアを遮断する技術も多く用いられている。一般的に「サンドボックス (Sandbox) ベース検知」としても知られているが、仮想環境で行われる動的行為の関連情報を分析し、正常かどうかを判断するものだ。

それ以外にも、各ファイルから収集した情報をもとに検知する、「クラウドベース検知」もある。これは、どれほど多くのユーザーが使用しているファイルなのか、どのようなコード署名が使用されているか、ユーザーレピュテーションはどうかなど、様々な情報を総合して悪性の有無を判断する手法だ。

EDR の役割：従来のセキュリティシステムの限界を補完

攻撃手法の高度化、およびセキュリティ技術の発展を総論すると、攻撃者は巧妙な手口でセキュリティの脆弱性を狙い、攻撃の痕跡を最小限に抑えることで、防御側が簡単には対応できないよう画策する。これに対しセキュリティは、不正なファイルではなく、攻撃者の行為に焦点を置き技術を発展させてきた。

前述したファイルレス攻撃は、昨今様々な種類のマルウェアに一貫して用いられている。そのため、現在非常に重要な技術として注目されているのが、この行為ベース検知だ。特に、企業や機関を狙った標的型攻撃は、様々な検知技術を回避できるハイレベルな技術力を備えている。こうした侵害に迅速に対応するためには、未知の脅威に至るまで検知を行い、追跡 (Threat Hunting) していくことが重要となる。

このことから、従来の普遍化した AV やネットワークベースのセキュリティシステムに、一歩先の検知・対応力が追加で要求されている。AV やネットワーク中心の対応だけでは、実際に感染が発生したエンドポイントに対し、十分な情報 (ログ) を確保できず、感染経路や潜在的な脅威を把握することが困難であるからだ。

こうした限界点を補完してくれるのが、この「EDR (Endpoint Detection & Response)」である。ガートナーの定義によると、EDR はエンドポイントにて、持続的なモニタリング、および対応力を提供してくれるセキュリティソリューションだ。EDR は基本的に、▲セキュリティ侵害検知、▲セキュリティ侵

害調査、▲エンドポイントでのセキュリティ制御、▲対応・解決のためのガイドおよび対応など、様々な機能を提供している。ポイントとなるのは、ログを含めた詳細な脅威情報や、攻撃フロー図をユーザーに提供し、脅威の種類・行為および攻撃段階に応じて、適切な対策案を提示するという点だ。

EDR の概念と必要性を、より直感的に理解できるよう、以下に 2 つの説明を補足する。

1 つ目は、従来のセキュリティシステムに対する自問から始まる。新しいものへの必要性を理解しようとする際、適切な基準を立てた後、数学でいう逆算のように、現在の状況から遡ることで正しい回答を得ることができる。こうした観点から、従来のセキュリティシステムにおける限界点をまとめたものが [表 1] である。

#	限界点
1	収集できない対象の場合、分析することは不可能
2	分析できない場合、マルウェアもしくは正常かどうか検知することは不可能
3	マルウェアを検知できない場合、対応することは不可能
4	分析結果をパターン化できない場合、同様の脅威を自動検知することは不可能
5	パターン化への作業自体を自動化できない場合、新種の脅威にリアルタイムで対応することは不可能

[表 1] 従来のセキュリティシステムにおける限界点

EDR は、様々な脅威経路のモニタリングや、検知・対応のパターン化および自動化により、[表 1] に記した従来のセキュリティシステムの限界点という否定的な見方を、肯定的な見解に変えてくれる。これにより、EDR の価値や必要性が自ずと理解できるだろう。企業は、[表 1] の内容を自問しながら、EDR の根本的な必要性について検討することが可能だ。

2 つ目に、EDR を実生活で例えるなら、犯罪現場に監視カメラを設置することと似ている。前述した新型コロナウイルス感染症の疫学調査と同じような概念で、全経路で発生する異常行為を検知し、蓄積された情報を分析することで、犯人の追跡捜査に役立てるのだ。また、分析により導き出したインサイトをもとに、潜在的な脅威への対応戦略を樹立することで、事前予防にも繋がる。

EDR は、エンドポイント上で発生する様々な行為を、どれほど迅速かつ包括的に検知できるかが重要である。そのため、検知済みの端末以外の被害拡散状況など、エンドポイント領域にて発生した侵害行為を追跡できるよう、可視性 (Visibility) の提供が必要不可欠となる。さらに、追加被害が発生しないよう、感染端末の隔離やネットワークの遮断、さらに脆弱性を探し出し、パッチを適用するなどの対応も可能でなければならない。この全ての行為に関する目的は、脅威の潜伏期間と被害を最小限に食い止めるためのものだ。

また、EDR は単独で機能するわけではない。その効果が最大限に発揮されるのは、AV など従来のセキュリティソリューションと連携した時だ。現在の市場動向を見てみると、EPP (Endpoint Protection Platform) と EDR の融合型プラットフォームを提供する傾向にある。こうした形で、脅威検知・対応・遮断および駆除などの力量を有機的にサポートする企業が、セキュリティ面で強さを見せている。

アンラボも同様に、AhnLab EDR と AhnLab EPP の統合型プラットフォームから、エンドポイントへのセキュリティ力を提供している。AV ソリューションである「V3」をはじめ、EPP を構成している様々なエンドポイントセキュリティソリューションと連動し、「既知の脅威」から、新種マルウェアやゼロデイ脆

弱性を悪用した「未知の脅威」、また、内在しているがいつ発現するか予測不能な「見えない脅威」まで、ユーザーが効果的に対応できるようサポートしている。

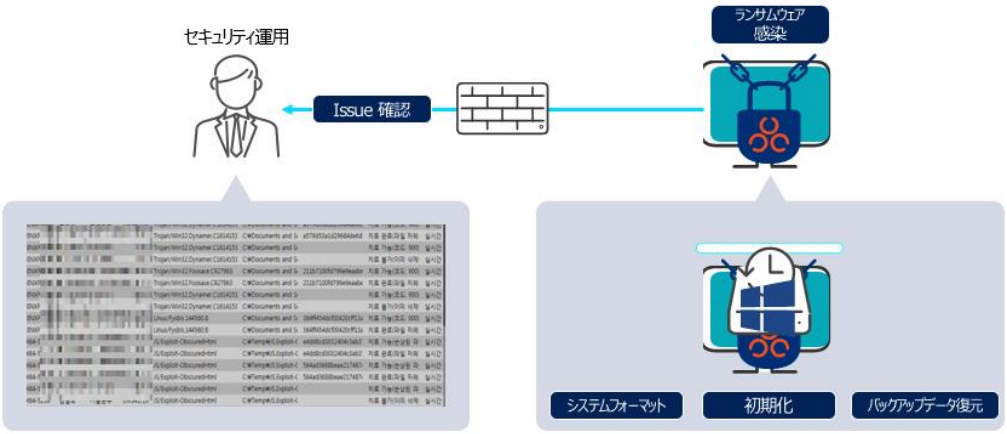
さらに、AhnLab EDR はより効果的かつ機先を制する対応をとるため、必要に応じて運営中のセキュリティソリューションと連携し、管理することも可能だ。AhnLab EPP サーバーで収集したデータと、AhnLab EDR サーバーで端末の異常行為から分析したログを、運営中の APT ソリューションとともに、SIEM (Security Information & Event Management) で統合的に管理する。脅威情報の統合管理システムでは、EPP にて活用可能な API を介し、告知事項の送信、マルウェア検知、ファイル収集・削除など、様々なコマンドが送られる。こうした統合セキュリティシステムを構成することで、潜在的な被害への予防も可能となる。

AhnLab EDR の製品特長や、主な機能に関する詳細は、オンラインセミナーから視聴可能だ。

EDR 導入前 VS 導入後

次に、組織の脅威対応プロセスが EDR の導入前後でどう変化するのか、EDR を導入・運営している A 社の事例からその差を見てみよう。

まず、EDR 導入前の A 社では、ユーザーの PC にマルウェアの感染履歴が確認されると、管理者がユーザーの負担を軽減するため、システムフォーマットもしくは初期化を行い、バックアップデータがある場合は復元し業務を再開していた。しかし、この過程では、ワクチン管理サーバーにユーザー PC のマルウェア感染履歴はあるものの、マルウェアがどこから流入し、どこに拡散されたかなどを確認することはできなかった。単に保存されたログから、感染履歴があることを確認するだけに留まっていたのである。

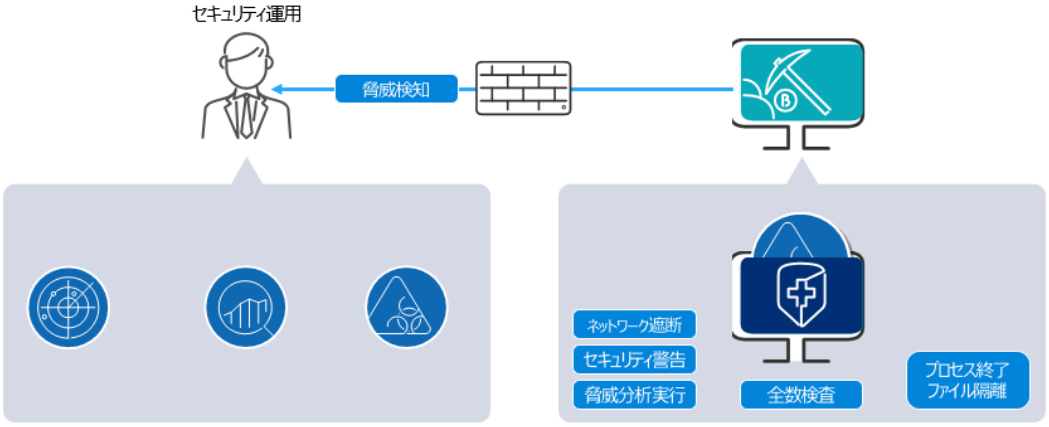


[図 2] EDR 導入前の脅威対応プロセス

すなわち、脅威分析を介した予防対策の樹立が不可能であり、事後対応の履歴管理のみが可能であった。それだけでなく、遮断した脅威に関しても、遮断経緯を正確に分析することができないため、持続可能なセキュリティ戦略の樹立ではなく、常に防御に依存するほかなかった。

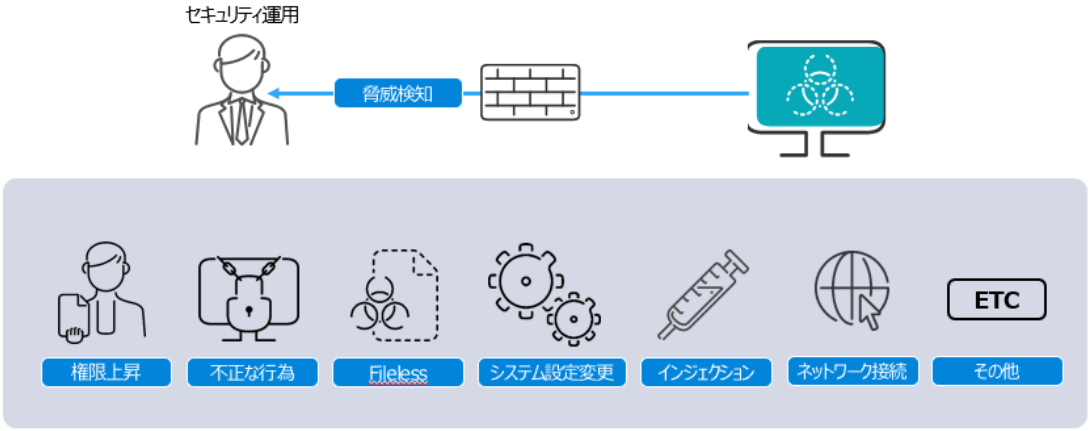
しかし、EDR の導入後、こうした状況が大きく変わる。

まず、マルウェアへの感染警告が発生した場合、EDR システムから脅威を分析し、流入経路、流入後に作成されたファイル、ファイルのネットワーク通信履歴など、マルウェアの行為イベントを全て分析に活用した。
さらに、分析情報を活用することで脆弱性を解決し、ユーザー PC のセキュリティ強化に繋げることも可能となった。



[図 3] EDR 導入後の脅威対応プロセス

また、従来の未知の脅威に関しても、ユーザー PC で異常行為が発生すると、管理者は EDR から警告アラームを受信する。その後、EDR は事前に定義された規則をもとに、脅威を分析し全体ユーザーを対象に検査を行ったり、マルウェアの"疑い"があるファイルに対しても、ファイルの収集やプロセスを終了を行った。さらに、必要に応じてマルウェアのネットワーク拡散を防止するため、ユーザー PC のネットワークを隔離し、孤立させることも可能となった。



[図 4] EDR の行為検知

ファイル形式のマルウェア以外にも、主な脅威を紹介する際に前述したファイルレス悪性行為、さらに疑いのあるファイルの権限昇格 (Privilege Escalation) 行為、文書・写真ファイルを検索し暗号化を試みるランサムウェア行為、従来のシステム設定を故意に変更しようとするシステム設定変更行為など、様々な行為検知から分析・対応を単一コンソールで行うことが可能となった。

結論 : EDR 導入は既製品でなく特注品で

上記では、EDR の必要性について様々なセキュリティ概念や導入事例を挙げながら説明してきた。高度化する脅威を考慮すると、EDR が必要不可欠なソリューションであることは間違いない。しかし、導入時に画一的な思考でアプローチすることは避けるべきである。

例えば、我々は服を購入する際も様々な要素を考慮する。その服が必要かどうかから始まり、ブランド、サイズ、手持ちのアイテムと似合うかなど、色々なことを総合的に考え購入を決める。その理由は、自分自身に合わなければ効用価値が下がるためである。いくらデザインが気に入ったハイブランドの服でも、購入者のサイズが M にもかかわらず XL を買った場合、その服自体が似合わず価値が落ちてしまう。

EDR にも同様のことが言える。EDR の導入を検討しているユーザーは、現在の組織の規模やビジネス・IT 状況、導入目的、費用などの様々な要素を明確にすべきである。特に、EDR は検知・分析情報が多く、本質的な意味で「重い」ソリューションである。そのため、活用方案も綿密に構想しなくてはならない。もしも構想に限界を感じ、明確な答えを出せない場合は、アンラボのような外部の専門企業にコンサルティングを受けるのも良案と言えるだろう。

守るべきものが日々増えていく中、今もそしてこの先も、より多くの企業が EDR を"知能的に"活用し、安全なビジネス環境を創造していければと願う。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)