なぜ未だに EDR 及び XDR 製品がランサムウェア攻撃を打破できないのか
2021 年 12 月 16 日 Minerva のブログから

エンドポイント検出応答（EDR）とは企業組織の IT システムと各社員が使用している端末をマルウェア、ランサムウェア又は他のタイプに悪意コードから防御するためのセキュリティ製品です。結果として各企業組織の規模に関わらず EDR 製品をネットワークセキュリティへ追加することで IT セキュリティ強化実施を行っていると言えるでしょう（EDR 製品の成長率の記事）。

しかし EDR 製品を導入されてもランサムウェア攻撃を受けた企業組織は存在します。実は EDR 製品販売数が多くなるに従い、企業組織が年々にわたり、マルウェア攻撃の被害を受けた企業組織者数もまた比例しているという事実がございます。 IBM の”Cost of a Data Breach Report 2021”によると、マルウェア検知と防御数が平均で 287 日という急激な増加傾向にあります。

多くの企業組織が EDR 又は XDR 製品を導入することにより攻撃を防げるのか？

各 EDR 製品によりけりです。私たちは EDR がマルウェア及びランサムウェア攻撃から 100% 防御できないのかそして検知よりも防御することがなぜ必須条件であるかを重要視します。
EDR と XDR 製品はなぜ未知のマルウェアとランサムウェア攻撃から防御できないのか？

EDR 製品は人間の体内機能作用に例えることができ、ウィルスが体内に入ると抗体機能が働きます。EDR がネットワーク内に悪意のある行動が検知されたら、感染悪化を防ぐため、人の抗体機能と同様に攻撃をストップさせます。

この抗体機能はマルウェアやランサムウェアが攻撃実行後に検知されダメージをストップします。しかし EDR 製品の欠点を言うと、EDR 製品は、攻撃を防御する前にシステム感染をさせないといけないという点です。これでは攻撃を完全に防御することができないということです。

EDR と XDR 製品がどれだけ洗練されたソリューションと言われても、先制防御できなければ意味がありません。AI を搭載し他の最新テクノロジーを採用している XDR 製品でも悪意のあるコードを検知することは可能でしょうが、マルウェアに対処（レスポンス）する前にマルウェアに攻撃実行させないと防御できないという欠点です。

マルウェア攻撃を防御するためには、毒には毒を以て制す。

あなたの IT システムに影響を及ぼすマルウェア攻撃から防御するためには、先制防御が必須です。最良の方法はマルウェアの悪性と性格行動を利用することで、防御できるということではないでしょうか。

例えばファイルレス攻撃は正当なソフトウエアを利用しあなたのシステムへ侵入します。そしてハードドライブ上ではなく、仮想メモリー（RAM）内で稼働を始めます。この結果、EDR 製品では検知及び防御することが非常に困難であるという事です。しかしマルウェアの検知回避手法を逆手にとって攻撃を防御することが可能になります。

例えば悪意のあるコードがサンドボックス環境で検知回避をする場合、OS に対し仮想マシンにいるのか又はレゾリューションはどうなのかなどのクエリーを開始します。仮想環境にいるとか 800×600 レゾリューション（典型的サンドボックスのレゾリューション）にいるなどと答えを返すと、マルウェアは検知されるのを恐れるため、攻撃を実行しません。

Minerva を開発した経緯

EDR 製品はプロアクティブで能動的というより受動的なソリューションであるからこそ前述で説明したようにマルウェアによるシステム攻撃やデータ詐取を確実に防御する特性を備えておりません。そこでエンドポイントセキュリティ製品でマルウェアが攻撃を開始する前に防御できる製品を開発したいという経緯があります。

前述で説明をしました攻撃防御戦術と Minerva 独自のマルウェア防御手法（特許取得済）を実装することで、マルウェア攻撃手法を特定する必要なく攻撃を先制防御できます。その結果、不正アクセスやデータ詐取、ランサムウェア攻撃などシームレスな防御が可能です。

Minerva 製品（Minerva Armor）についてのお問い合わせは Pico Technologies（info@pico-t.co.jp）までお願い致します。