アンラボ・セキュリティレター

Press Ahn

2018.1　Vol.49

高度化された脅威、なぜ可視化が重要なのか

高度化された標的型攻撃対応ソリューション「AhnLab MDS」新バージョンリリース

高度化された脅威、なぜ可視化が重要なのか

昨年セキュリティの話題の中心には常にランサムウェアがあった。2017年冒頭から発生したランサムウェアによる大型事件に注目が集まっていた中でインテリジェントな標的型脅威(Advanced Persistent Threat、以下APT)もまた急展開していたのである。昨年、韓国の大手ウェブホスティング会社のランサムウェア感染事例に関して政府機関の科学技術情報通信部では、APTとランサムウェアが結合されたタイプの攻撃だと発表している。

もちろんAPT攻撃の変化に歩調を合わせて対応ソリューションも持続的に発展し続け、ネットワーク上のサンドボックスベース対応から、最近はエンドポイントとネットワークの統合対応にシフトしつつある。APT攻撃の侵入ルートが多様化するにつれリアルタイムな対応を可能にする統合的な可視化が重要になってきた。アンラボはインテリジェントな対標的型脅威ソリューション「AhnLab MDS(以下MDS)」を全面的にリニューアルし、脅威の可視化を強化した新バージョンをリリースした。

「可視化(Visibility)」はセキュリティ脅威に対応する第一要素に挙げられる。多様な攻撃手法が登場したことにより、どのような脅威がどこからどのように侵入し、何を狙っているのか、このような原因をどれだけ迅速かつ正確に把握できるかが対応(Response)の成功率を左右するからだ。

APT攻撃が持続的に発生し、新・変種ランサムウェアが急増している中で「脅威の可視化」はこれにも増して重要になってきている。

脅威の可視化は、大きく脅威の▲侵入ルート、▲タイプと動作、▲標的(ターゲットシステム)、3つの要素で構成される。

Channel	Payload	Victim
侵入ルート (ネットワーク、エンドポイント)	タイプと動作	標的 (ターゲットシステム)

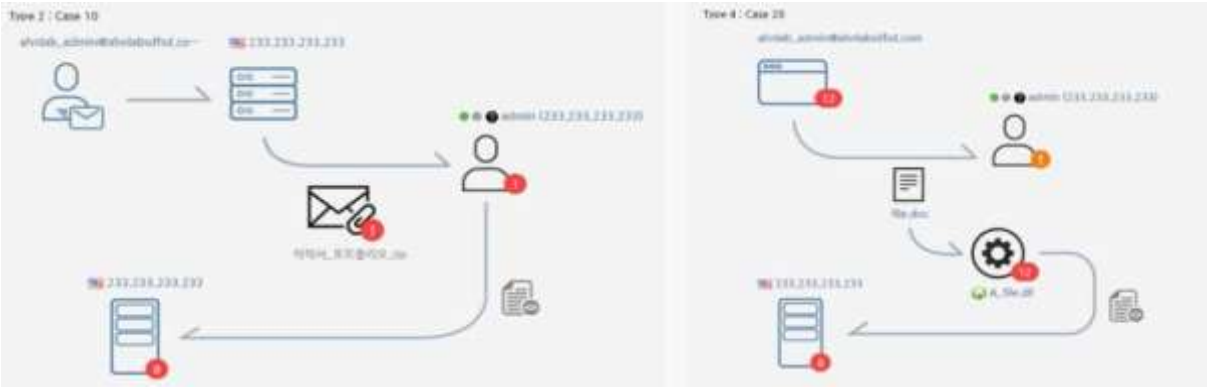
[図1] 脅威の可視化の三要素

脅威の多くは企業のユーザーやシステムが使用する多様なアプリケーションとサービスを通じて内部に侵入する。

代表的な侵入ルートとしては Web、メール、ファイル送信および共有システムなどのネットワーク区間がある。最近は USBなどの記憶装置からエンドポイントシステムに直接入ってくるケースも増えている。内部に侵入する脅威を迅速に検知・対応するためには脅威のタイプと動作のほか、脅威の侵入ルートも含めて標的にされたシステム(攻撃対象)まで一目で把握することが求められる。

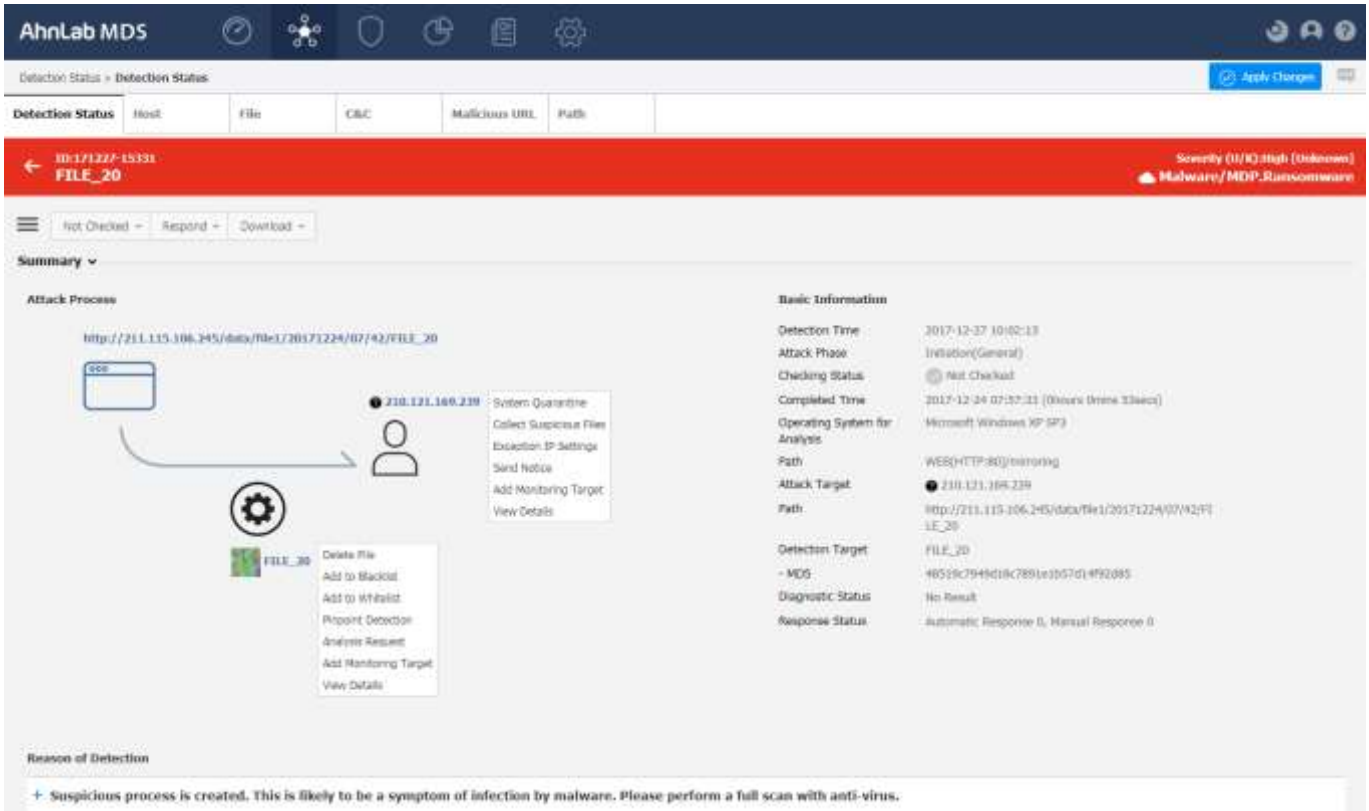
MDS の優れた可視化機能

アンラボは最新の脅威に対する効果的な対応と、セキュリティ管理者の業務の効率化の機能を強化したMDSの最新バージョンをリリースした。最新バージョンは様々なルートから侵入する脅威を一目で把握できる直感的な「攻撃フローチャート」を提供する。
フローチャートでは仮想マシンで分析したマルウェアの情報をわかりやすく表示し、同マルウェアの詳細な行動分析レポートも提供している。



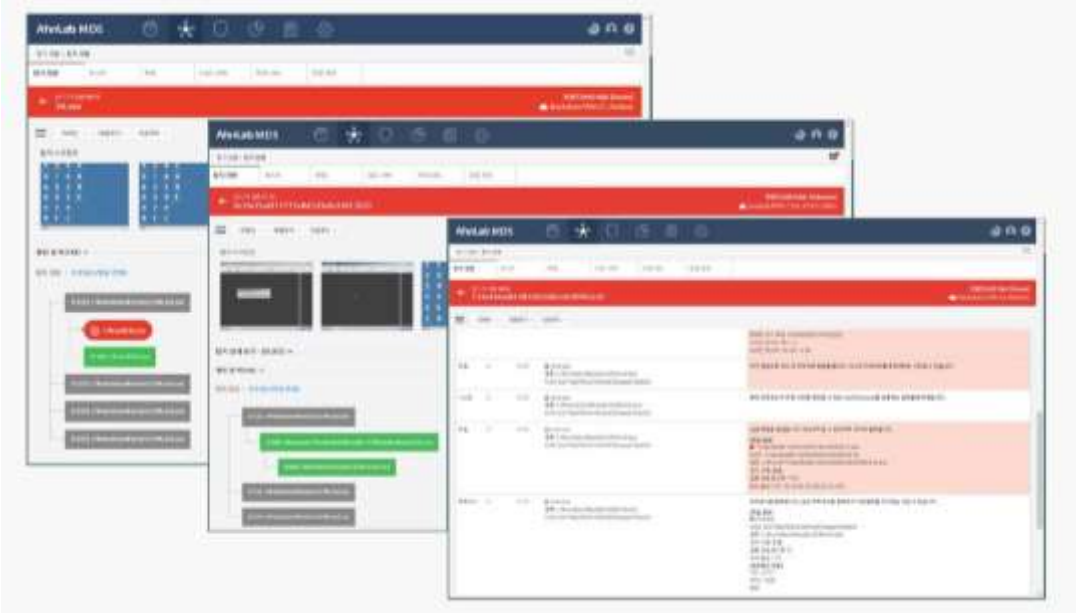
[図2] MDSの攻撃フローチャート：メール攻撃(左)とウェブ攻撃(右)

各種のダッシュボードは脅威に対するリアルタイム・アクション対策も提供する。セキュリティ管理者は攻撃フローチャートと詳細分析レポートから内部に侵入された脅威を正確に把握し、リアルタイムな対応も可能になる。



[図3] 攻撃フローチャートをベースにしたガイド

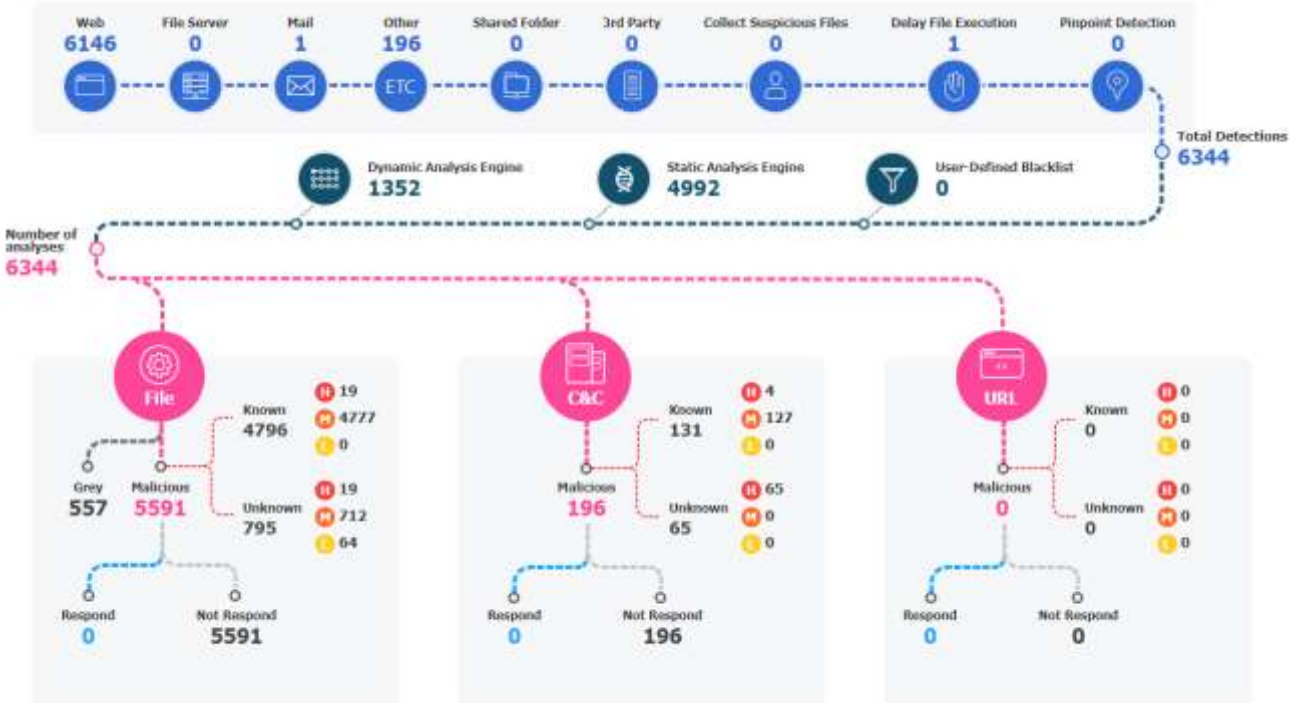
分析レポートも大幅に改善され、ファイルとプロセスの関係についてさらに分かりやすく詳細な情報を提供する。詳細分析レポートは、英語、中国語、韓国語で提供される。



[図4] 詳細な分析レポート

可視化に基づくリアルタイム対応

脅威に対する効果的な対策を講じるには、内部に侵入した脅威の全体図を把握しなければならない。MDSはダッシュボードから侵入ルート、分析状況、脅威の行為を一目で把握できる「攻撃フローチャート(Threat Flow)」を提供する。[図5]のフローチャートから、セキュリティ管理者は組織の全体的な検知・対応状況をモニタリングしてアクションできる。



[図5] 侵入ルート別イベントの脅威フローチャート

最近はセキュリティソリューションの検知を回避・迂回するために、ネットワークパケットを細分化したり(Packet Splitting)、暗号化トラフィック(SSL)を利用する攻撃手法がメインになっている。エンドポイントにおける脅威情報の収集と対応へのニーズが増加している理由がここにある。
エンドポイントで対応するためには、エージェントとの連動が必須であり、特に自動及び手動対応が可能な専用エージェントが要求される。MDSは設計段階からエンドポイントとネットワークの連携を前提に開発されたソリューションであり、専用エージェントを通じて自動・手動対応可能であることはもちろんのことエンドポイントに直接侵入した脅威を収集する。AhnLab V3やアンラボのエンドポイントセキュリティ管理製品を導入済みの場合は MDSエージェントを「V3」や「APC」エージェントと統合タイプとして利用できるため、ソリューションの導入と運用がさらにスムーズになった。
またセキュリティ管理者が追加対応できるように対応プロセスに応じた管理ページも提供している。エージェントをグループ(Grouping)に整理して各グループに共通ポリシーや個別ポリシーも適用できるため、部署単位やユーザー単位に細かなポリシーを適用できる。
MDSの新バージョンでは脅威の可視化と便利な管理機能を一層強化し、さらに効果的な対応が可能になった。

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)