

高度な未知のマルウェア解析エンジン

McAfee Advanced Threat Defense (ATD)

システムの課題

ネットワーク IPS、メールセキュリティ、エンドポイントでも高機能なマルウェア検知や防御を活用したい。

怪しいファイル入手した時のためにマルウェアの解析ツールを社内で使いたい。

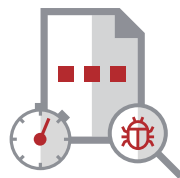
解決のご提案

サンドボックスを含む動的解析や詳細な静的解析により既知、及び未知のマルウェア検知エンジンを様々なセキュリティ製品と連携させることができます。

また、入手したサンプルファイルを解析してファイルの動作やシステムへの影響をレポートで確認することもできます。

攻撃ツールの入手が容易になり、旧来の検知技術の回避も容易な現在、未知のマルウェア対策が重要になりました。マカフィーの高度なマルウェア解析エンジンは既知のマルウェアは確実に高速に効率よく検知し、未知のマルウェアは複数の手法で詳細に解析することができるだけでなく、様々な製品と連携することで運用の自動化を促進します。

高速検知



- ・シグネチャレピュテーションで既知のマルウェアを高速に検知
- ・未知のマルウェアをエミュレーションで高速振り舞い解析

動的解析



- ・サンドボックスによる振り舞いの詳細解析
- ・API 等の特徴を機械学習して解析に活用

静的コード解析



- ・難読化されたマルウェアもアンパックして内部コードを詳細に解析
- ・サンドボックスを回避する未知のマルウェアも解析



レポートと STIX/OpenIOC 対応

サマリと詳細レポート出力、及び解析結果を STIX や OpenIOC で共有できます。
詳細レポート (ファイル、プロセス、レジストリ、通信、関連してダウンロードされたファイル、等)
逆アセンブラ及び API レポート



様々な OS をサポート

Win XP, 7, 8/8.1, 10
Win Server 2003, 2008, 2012/2012 R2, 2016
Android



複数仮想イメージで解析

より正確な解析結果を得るために複数の異なる環境で解析を行うことができます。



ユーザ操作モード解析

ユーザ操作が伴うマルウェアを正確に解析するためにインタラクティブに解析を実行できます。

高度な解析機能を様々なシステムに提供

McAfee Advanced Threat Defense は様々なシステムと連携して、高度な未知のマルウェア解析機能を提供することで、検知や防御にかかる運用負担を軽減します。

SIEM連携 Enterprise Security Manager

自動的に解析結果 (IoC) を SIEM と共有し、過去ログをバックトレースし潜伏している脅威を可視化します。

Webセキュリティ連携 Web Gateway

Web 経由の未知のマルウェアをリアルタイムにブロックしエンドポイントを保護します。

IPS連携 Network Security Platform

ネットワークで検出したマルウェアを解析し侵入を検知します。

操作しやすい運用画面

サンプルのアップロードや詳細なレポートを確認することができます。

エンドポイントや他社製品連携 Threat Intelligence Exchange

エンドポイントや他社製品との連携して被害を最小化します。

Email Gatewayコネクター

様々なメールセキュリティ製品と連携します。

製品ラインアップ

タイプ	モデル	対応仮想イメージ数	備考
アプライアンス	ATD-3100	最大30	1U 10G/1G/100M対応I/F
アプライアンス	ATD-6100	最大60	
仮想アプライアンス	ATD-VM1008	最大8	追加仮想イメージ (ATD-VM+8SB) を購入することで最大64イメージまで拡張することができます。
仮想アプライアンス	ATD-VM1016	最大16	
仮想アプライアンス	ATD-VM3032	最大32	
仮想アプライアンス	ATD-VM6064	最大64	

製品情報はこちらをご覧ください <http://www.mcafee.com/jp/products/advanced-threat-analysis/index.aspx>



マカフィー株式会社

www.mcafee.com/jp

東京本社 〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL: 03-5428-1100 (代) FAX: 03-5428-1480

西日本支店 〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL: 06-6344-1511 (代) FAX: 06-6344-1517

・製品、サービスに関するお問い合わせは下記へ

McAfee, McAfeeのロゴ、マカフィーは米国及びその他の国におけるMcAfee LLCの商標または登録商標です。その他の商標または登録商標はそれぞれその所有者に帰属します。Copyright © 2017 McAfee LLC.

●製品、サービス、サポート内容の詳細は、最寄りの代理店または弊社事業部までお問合せください。●製品の仕様、機能は予告なく変更する場合がありますので、ご了承ください。

MCABR-ATD-1707-MCA