Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

サンドボックス技術

サンドボックス技術は、サンプルファイルの発生源の調査、ふるまい分析に基づく侵入の痕跡（IOC）の収集、未確認の悪意あるオブジェクトの検知を可能にする強力なツールです。

Kaspersky Research Sandbox

ファイルと URL のふるまいに基づいてインテリジェントな意思決定を行うと同時に、プロセスメモリやネットワークアクティビティなどを分析することは、今日の洗練された標的型攻撃やカスタマイズされた脅威を理解するための最適なアプローチとなります。

今日のマルウェアは、悪意のあるアクティビティが白日の下に晒される可能性が生じた場合、あらゆる手法を駆使して自らのコードを実行することを回避します。システムが必要なパラメータを満たしていない場合、悪意あるプログラムはほぼ確実に自分自身を破壊し、痕跡を残すことはありません。悪意のあるコードが実行されるためには、サンドボックス環境はエンドユーザーの通常のふるまいを正確に装うことができる必要があります。

Kaspersky Research Sandbox は、10 年以上かけて進化してきたカスペルスキーのラボ内サンドボックス環境から直接開発されています。このサンドボックスには、カスペルスキーが脅威に関する調査を通じて蓄積してきたマルウェアのふるまいに関するあらゆる知識が組み入れられており、毎日 38 万件以上の悪意のある新規オブジェクトの検知を可能にしています。オンプレミスで開発されたこの強力なテクノロジーは、データが組織の外部にさらされるリスクも防ぎます。

ふるまい分析と堅牢な反回避技術にヒューマンシミュレーション技術を組み合わせたハイブリッドアプローチを提供します。Kaspersky Research Sandbox では、システムイメージを実際の環境に合わせて分析用にカスタマイズすることもでき、脅威検知の精度と調査スピードが向上します。

製品の特徴：

- Windows、Linux、Android 環境でのオブジェクト分析の自動化
- カスタムイメージにより、Windows オペレーティングシステムとアプリケーションにまたがる脅威分析が可能（実際の環境に適用されるもののみ）
- ファイルの実行中に取得された指標とデータに基づく脅威スコアにより、分析されたオブジェクトの危険度を提示
- オンプレミスでの展開により、組織外へのデータの流出を防止
- 先進の反回避技術とヒューマンシミュレーション技術
- 手動でのファイル / URL の送信と RESTful API
- 100 種類を超えるファイルの分析に対応し、詳細な分析レポートを提供
- ネットワークトラフィックのスキャン用の Suricata カスタムルールを追加し、既成の Suricata ルールと併用可能
- ベアメタル展開に対応し、必要なパフォーマンスに応じて簡単に拡大可能

Kaspersky Research Sandbox のハイレベルのアーキテクチャ

本製品はベアメタル展開に対応します。必要なパフォーマンスに応じてハードウェアを構成でき、拡大可能です。各チャネルでのネットワーク接続速度は 100 Mbps 必要で、独立した ISP 接続が少なくとも 1 回線必要です（耐障害性を考慮する場合、2 回線以上を推奨）。ISP は悪意のあるトラフィックを認識し、備える必要があります。

Kaspersky Research Sandbox は、特許取得済みの独自技術を基盤に構築されています（特許番号：US10339301）。マルウェアの実行がトリガーされる状況を正確に作り出すことで、研究者が疑わしいファイルや URL を一度の試行で分析できるようにします。

検知から逃れるために、悪意のあるファイルはまず、現在の環境が仮想マシン内かどうかを調査します。そして、サンドボックスが機能しなくなるまで活動を停止します。そのような場合、特許取得技術により仮想マシン内の時間の流れが加速され、悪意のあるコードが実際より早く実行せざるを得なくなります。

マルウェアは、それが標的としている特定のアプリケーションがサンドボックス内に存在しない場合、悪意のあるふるまいを見せない可能性があります。この課題を解決するために、研究者はログをレビューし、不足しているものを見極め、仮想マシンにそれを追加して、このプロセスを再び実行する必要があります。マルウェアがアプリケーションへのアクセスを試みると、特許取得済みのシステムがこの試行を傍受します。ファイルの実行が終了するまで待つことなく、このプロセスをただちに停止させ、必要なアプリケーションとそのコンテンツを作り出します。

詳細な分析レポート

分析が完了すると、Research Sandbox から分析対象サンプルのふるまいと機能に関する詳細なレポートが提供されるため、適切な対応手順を定義できます：

サマリ

ファイルの実行 / URL の閲覧結果に関する一般的な情報。

検知名

ファイルの実行中に登録された検知のリスト（AV およびふるまい検知）。

トリガーされたネットワークルール

実行されたオブジェクトからのトラフィックの分析中にトリガーされた Suricata ネットワークルールのリスト。

実行マップ

一連のオブジェクトアクティビティとアクティビティ間の関係をグラフィカルに表現したもの。

疑わしいアクティビティ

登録された疑わしいアクティビティのリスト。

スクリーンショット

ファイルの実行 / URL の閲覧中に取得されたスクリーンショットのセット。

読み込まれた PE イメージ

ファイルの実行 / URL の閲覧中に検知された、読み込まれた PE イメージのリスト。

ファイル操作

ファイルの実行 / URL の閲覧中に登録されたファイル操作のリスト。

レジストリオペレーション

ファイルの実行 / URL の閲覧中に検知された、OS レジストリで実行されたオペレーションのリスト。

プロセスオペレーション

ファイルの実行中に登録されたプロセスとファイルとのインタラクションのリスト。

同期オペレーション

ファイルの実行 / URL の閲覧中に登録された、作成された同期オブジェクト（ミューテックス、イベント、セマフォ）のオペレーションのリスト。

ダウンロードされたファイル

ファイルの実行 / URL の閲覧中にネットワークトラフィックから抽出されたファイルのリスト。

ドロップされたファイル

実行されたファイルにより保存（作成または変更）されたファイルのリスト。

HTTPS / HTTP / DNS / IP / TCP / UDP など

ファイルの実行 / URL の閲覧中に登録されたネットワークセッション / リクエスト詳細

ネットワークトラフィックダンプ（PCAP）

ネットワークアクティビティは PCAP 形式でエクスポートできます。

MITRE ATT&CK matrix

エミュレーション中に記録された特定済みのすべてのアクティビティは、MITRE ATT&CK matrix の形式で表示されます。

Kaspersky Research Sandbox は、未知の脅威の検知に最適なツールです。他のどのソリューションより成熟しており、高度な脅威に特化しています。

www.kaspersky.co.jp