SophosLabs Threat Intelligence

悪質な攻撃者が、共通のツールと実績のある攻撃手法を用いて、ターゲットを絞った高度な戦術、技術、手法および手順を実行するにつれて脅威の状況は進化し続けています。SophosLabs は、最新のランサムウェアの技術、悪意のあるURLやフィッシング攻撃の着実な増加から、エクスプロイトを使用した脅威の回避と持続性の増加に至るまで、高度なサイバー脅威の伝播に重要な役割を果たす新たなセキュリティ レンドと進化する敵対者の戦術を追跡しています。

セキュリティ組織は、既存のデータ セットとセキュリティ インフラストラクチャを補完する方法として、購入する脅威インテリジェンスの量を増やす必要があることがよくあります。しかし、その代わりに、精選されていないデータの取得を通じて誤検知の数が増加しています。SophosLabs の脅威研究チームと、次世代ツールを活用した高度に自動化されたインフラストラクチャは、高精度で特徴的で、多くの場合独占的なデータセットを開発しました。これらのデータセットは現在市販されており、検出および対応能力の向上に役立ちます。

グローバルTier-1ラボの強味

30年以上にわたる高度なマルウェア分析により、脅威分析を行っているSophosLabsは、パートナーのセキュリティワークフローに対応するパフォーマンス、拡張性、柔軟性を備えた業界トップクラスの脅威インテリジェンスを提供し、パートナーが最善の対応に集中できるようにします。

300,000+/日
疑わしいURLの解析

50万+/日
以前に検知したことのないファイルの解析

80%の悪意のあるURL
正規WEBサイトからのもの

2千+/日
以前に検知したことのないAndriodアプリの分析

5,000万
ニューラル ネットワークの遺伝的類似性比較用のファイル

6億/日
データ保護のために追加されたLive Protectionのイベント

3万+/日
マルウェア対策サンプルをLive Protectionに追加

3億/日
Deep Larningに利用されるファイル

広範囲のデータ

- グローバルで可視性を備えた異種かつ補完的なデータ ソース
- ソフォスのネットワークとエンドポイント製品からのテレメトリ
- 中規模マーケット中心のデータ

データサイエンス

- セキュリティの機械学習
- フィードフォワード、畳み込み、リカレントおよび深層決定方策勾配法によるディープラーニング
- 転移学習とドメイン適応

データの品質

- 誤検知を減らすためのデータ キュレーションプロセス
- PEファイルとURLの継続的な評価

SophosLabs の世界的な脅威研究インフラストラクチャは、地域を越えてマルウェアの傾向とサイバー脅威を追跡します。

SOPHOS

SophosLabs解析プラットフォーム

ソフォスの解析フレームワークは解析レイヤを使って未知の脅威を減らすことを目標にしています。最も一般的に使用されるファイルタイプについて、数秒で判定とインテリジェンスレポートを導き出すことができます。これを実現するためにシグネチャベースの検出、詳細な脅威解析および静的・動的解析モードのAIモデルを組みわせて使用します。解析結果はすべてのSophos製品で使用されます。

SophosLabの解析プラットフォームのアプローチは業界と差別化し、様々な種類の脅威オブジェクトの送信をサポートするための積極的なロードマップを備えた包括的なファイルインテリジェントとURL解析を提供します。

脅威情報は、Sophosのクラウドプラットフォームに安全に接続できるAPIまたはデータフィードを通じて提供されます。

SophosLabsデータサイエンスの違い

一般的なマルウェア対策検出テクノロジは、特定の特性を持つマルウェアを識別するのに効果的です。 インライン製品には、図 1 の青い線の外側にあるファイルを適切に識別して分析するためのリソースがなく、常に高度なマルウェアを通過させます。 フィードフォワード、畳み込み、リカレント、ポリシー グラデーションなどの深層学習技術を追加することで、図 2 のオレンジ色の線の内側に示されているマルウェアに含まれるような、疑わしい属性を持つファイルを識別できます。
このようにして、マルウェア対策ソリューションの有効性を拡張し、検出されなかった多くの多様なマルウェア亜種を検出します。

図 1: 一般的なマルウェア対策テクノロジー

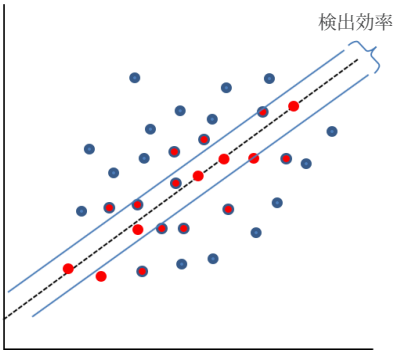
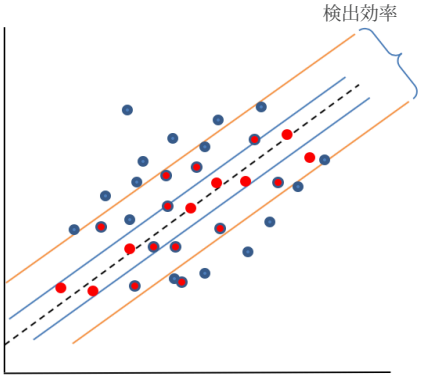


図 2: SophosLabs AIの検出支援



クリーン　マルウェア　疑わしい

- SophosLabの30年以上に渡る脅威解析とマルウェア対策を活用
- SophosLabs の脅威インテリジェンスサービスをソフォス製品で積極的に使用
- SophosLabs の送信ロジックは、さらなる解析が必要な疑わしいファイルの特定に有効
- 判定を迅速に受け取り、Web および電子メール ゲートウェイおよびクラウド製品がブロック/パスの意思決定を迅速に行う際に有効
- EDR、MDR、IR のユースケースに関する詳細なインテリジェンスレポートを取得可能
- 従来の脅威解析とニューラルネットワークモデリングの組み合わせによる進歩的な解析技術を用いた脅威解析プロセス

データソースとキュレーション

すべてはソフォスのネットワーク、エンドポイント、モバイル製品からのテレメトリを様々な補完的なデータソースと集約して、グローバルな可視性を得ることから始まります。ソフォスの自動キュレーションは、エントリの重複を排除し、脅威オブジェクトを分類し、誤検知を減らし、評判を更新します。矛盾する脅威データは、当社の脅威専門家によるレビューのためにエスカレーションされます。

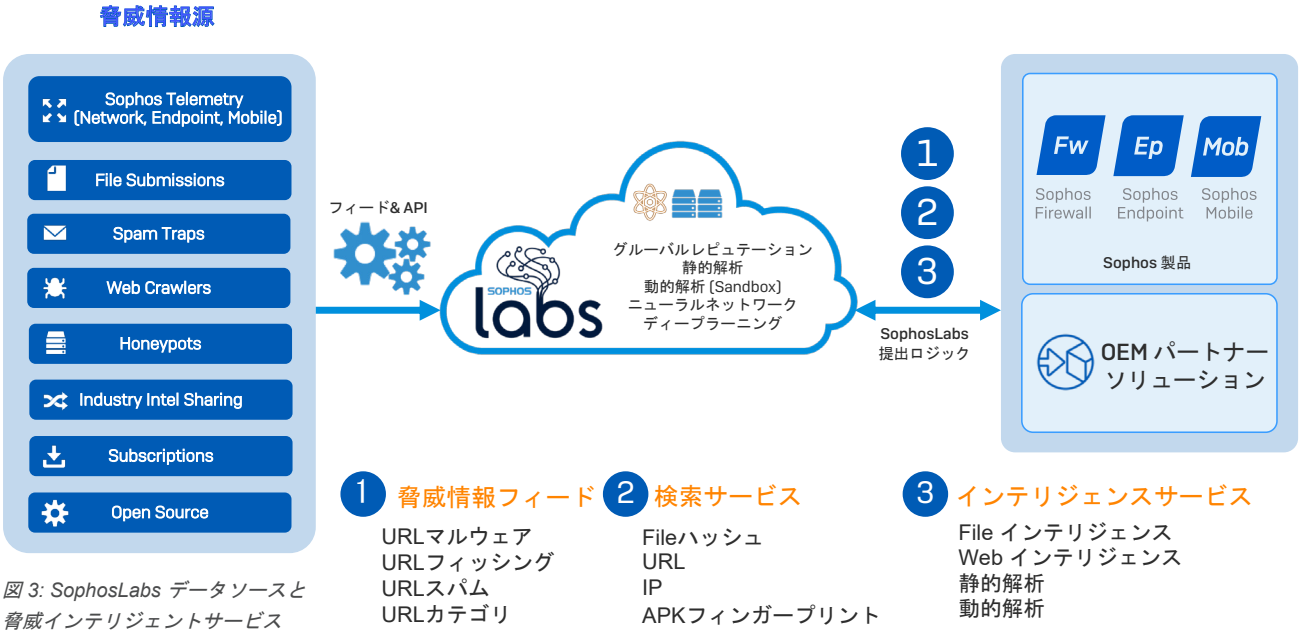


図 3: SophosLabs データソースと脅威インテリジェントサービス

フィード

悪意のあるURL

SophosLabs からの悪意のある URL フィードは、独自の/補完的なデータのかなりの部分を業界の他の企業に提供します。私たちの目標は、大量の生データの代わりに、厳選された悪意のあるURLを使用して正確な脅威インテリジェンスを提供し、独自性と品質を向上させることです。

一般的なカテゴリ	ドメイン	URI	詳細
マルウェアリポジトリ	3,000,000+	60,000,000+	マルウェアを拡散することを目的とした既知の悪質なサイト
マルウェアのコマンド&コントロール	670,000	160,000	既知の悪質なサイト
悪意のあるリダイレクトを伴う感染サイト	16,000	27,000	以前はクリーンだったサイトにマルウェアリダイレクトが含まれていることが判明
好ましくないアプリ (PUAs)	19,000	2,000,000+	不審なアプリとのリンク
フィッシングサイト	560,000	2,000,000	既知のゼロデイフィッシングサイトとリンク
Emailスパムサイト	1,000,000+	52,000	既知のスパムサイトとゼロデイスパムサイト

Webカテゴライズ - 生産性とコンプライアンス

URLデータベースには、Sophosのユーザおよびパートナーを通して集められる何億もの検索情報が含まれています。80以上のカテゴリーで構成され、あらゆる言語をサポートします。

最適化のために同じWebサイトに属する何百ものURIパスが1つのドメイン/サブドメイン・エンティティの下にロールアップされることがあります。ただし、親ドメインとは異なるカテゴリに分類されるURIパスは除きます。この構成により、データベースは一意の各URIパスを分類するよりもはるかに小さく、より効率的に、そして非常に高速になります。

ユースケース

Webフィルタリング:監査、ポリシー、コンプライアンス

一般的な製品とサービス

ゲートウェイとクラウド:次世代ファイアウォール、UTM、Emailセキュリティ

利点

- Web 使用に関する企業ポリシー要件の監査および制御
- 望ましくない可能性のあるアプリをフィルタリングする (PUA)
- URL のローカル データベースを使用してクエリ速度を最適化

クラウド検索サービス

ファイルマルウェアと悪質なURL、多様なURL、Android (APK) フィンガープリント

このサービスは、リアルタイムのマルウェア対策ソリューションをローカルでまだ更新されていない可能性がある最新の脅威データで補完するものです。未知のファイルのハッシュ、URLおよびAPKを検索することでローカルのセキュリティ・ソリューションのギャップを緩和します。

SophosLabsは、脅威解析とディープ・ラーニングの組み合わせを使用して、識別された全ての既知の悪意のある脅威オブジェクトのグローバルなでデーターベースを管理しています。この脅威データベースは、製品に常駐するデータベースが更新される前にクラウド上で入手することができます。

Cloud Lookup Service SDKで公開されている単一のProtocol Buffers (API)を使用して、全てのサービス検索へアクセスできます。SophosのOEM技術専門家は、APIの統合、テストおよび継続的なサポートでパートナーを支援します。

	マルウェアファイル	悪意のあるURL	多様なURL	APKフィンガープリント
量 (2018)	1,000,000,000+	60,000,000	28,000,000	19,000,000
アップデート	2,500	800	1,500	100
頻度	1分	6分	1日	10分

サポートされているファイルの種類:
.exe, .dll, .doc, .docx, .docm, .xls, .xlsx, or .xlsm, .ppt, .pptx, .pptm, .rtf

ユースケース

ブロッキング、スレットハンティング

一般的な製品とサービス

- ゲートウェイとクラウド:次世代ファイアウォール、UTM、Emailセキュリティ、EDR
- SOCaaS, MDR

利点

- 最新の SophosLabs 脅威インテリジェンスへのアクセス
- 即時の応答時間
- API はデバイス上のリソース消費を抑える
- ローカルの脅威データベースを維持する必要無し

クラウド・ファイル・インテリジェンス

SophosLabsは、1日に50万を超える固有のファイルについて詳細な解析を行っています。

ファイルの種類は、Sophosのファイルスキャン技術であるTrue File Type (TFT)を使用して確認され、拡張子に関係なくファイルの内容が識別されます。

サービスへ送られる全てのファイルは、Cloud File Intelligence Service SDKで公開されている単一のRESTful APIを使用してアクセスできます。SophosのOEM専門技術者は、APIの統合、テストおよび継続的なサポートでパートナーを支援します。

静的解析

SophosLabs は、判定結果を大幅にスピードアップし、豊富なインテリジェンスレポートを提供する詳細な静的解析を提供します。従来の脅威分析技術と機械学習モデルを組み合わせることにより、SophosLabs は一般的なファイル タイプに対して数秒で判定を下すことができます。

ディープラーニング モデル	マルウェアの 検出と評価	事前ファイル情報
‣ 遺伝的類似性 ‣ ファイルパスの類似性 ‣ 悪意のある属性	‣ PEファイルの評価 ‣ 深層ファイルスキャン – yara, antivirus ‣ 業界検知をカバー	‣ ファイルのプロパティと　メタデータ ‣ 作成者、日付、地域、言語、ファイル・フォーマット、バージョン、サイズ、ページ数、リンクの存在、アクティブコンテンツの存在(マクロ、フォーム等)、OLEオブジェクト、署名

サポートされているファイルの種類:
.exe, .dll, .doc, .docx, .docm, .xls, .xlsx, or .xlsm, .ppt, .pptx, .pptm, .rtf

ユースケース

ブロッキング、インテリジェンス/レポート

一般的な製品とサービス

- ゲートウェイとクラウド:次世代ファイアウォール、UTM、Emailセキュリティ、EDR
- SOCaaS, MDR

利点

- Office ドキュメント、PDF、PE、XML、アーカイブなどを含む、これまでに見たことのないファイルの高度な検出
- 数秒で判定とインテリジェンスを導き出す（可能な場合）
- SophosLabs のスマートロジックは、さらなる解析で不審なファイルを特定
- あらゆる規模のネットワークを保護できる拡張性

動的解析（クラウドサンドボックス）

SophosLabsクラウドサンドボックスは、最新の分析技術を利用して悪意のあるファイルを特定し、未知のファイルに対する比類のない可視性を実現します。

主な機能

マルウェアと好ましくないアプリ(PUA)の検出	既知のマルウェア	その他の悪意のある行為
‣ Sophosのアンチウイルスとメモリ ‣ Sophos Intercept Xディープ・ラーニング、CryptoGuard、WipeGuardテクノロジー	‣ Yaraパターンの深層メモリスキャン ‣ 動作パターン – マルウェアに起因する IOC	‣ 回避 - 反サンドボックスおよび反仮想マシン戦術 ‣ クリプトマイニング ‣ 欺くテクノロジー

サポートされているファイルの種類：
.exe, .dll, .doc, .docx, .docm, .rtf, .xls, .xlsx, .xlsm, .ppt, .pptx, .pptm, .pdf, .xml, .mso, .zip, .bzip, .gzip, .rar, .tar, .lha/.lzh, .xz

SophosLabsのデータのプライバシーと保持

- SophosLabsに提出された顧客データは、ヨーロッパ、北米、アジア太平洋地域の 3 つの地域データ処理ユニットで保存および処理されるため、顧客は自分の地域内にデータを保管できます
- これらの地域ユニットは、顧客データの明確な PII 境界を確保するために、密閉されたユニットとして構築されています
- SophosLabsは、顧客が送信したファイルのハッシュを外部の脅威インテリジェンスソースでチェックする場合がありますが、実際のファイルを第三者と共有することはありません
- SophosLabsは、分類されたすべての悪意のあるファイルを保持し、解析後はファイルをタイムリーにクリーンアップします

セキュリティ ポリシーの詳細については、次のサイトをご覧ください
https://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx

OEM Contact
Email: oem@sophos.com

詳細は
www.sophos.com/ja-jp/oem

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2022. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

22-06-27 DS-JP (PS)