SOPHOS

SOPHOS labs

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洗練された戦術、手法および手順を実行するにつれて脅威の予測は進化し続けています。2018年に、SophosLabsは幾つかの高度なトレンドを観測しました。これらは新しいサーバー攻撃において重要な役割を果たすと考えられます。ランサムウェアによる継続的な攻撃手法の採用、悪意のある暗号通貨マイナーの展開と増加、モバイルプラットフォームへの攻撃およびIoT攻撃の増加などです。

セキュリティの組織は既存のデータセットを補うためデータフィードの量を増やして購入する必要があります。その結果、未確定のデータを取得することによってセキュリティシステムにおける誤検知の数を増加させることになります。SophosLabsの脅威調査チームは次世代のツールを使用した高度に自動化されたインフラストラクチャによって、高精度で独自の排他的なデータセットを開発しました。これは現在の検出機能と応答機能の向上に役立ちます。

データの幅

- グローバルで可視化された異なる補完的なデータ
- Sophosのネットワークとエンドポイントから発生したテレメトリ
- ミッドマーケット中心のデータ

データのセキュリティ

- セキュリティの機械学習
- フィード・フォワード、コンボリューション、反復、方策勾配法を使用した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

- 誤検知を減らすデータキュレーションプロセス
- 継続的なPEファイルとURLのレピュテーション評価

グローバルなTier-1 ラボの強み

SophosLabsの脅威リサーチは、30年以上に渡る高度なマルウェア解析により、パフォーマンス、スケーラビリティおよび柔軟性を備えた業界トップクラスの脅威解析を提供しパートナーのセキュリティワークフローに対応します。

300,000+ /日
疑わしいURLの解析

500,000+ /日
以前に検知したことのないファイルの解析

80%のマリシャスURL
合法的なWebサイトから届く

2,000+ /日
以前に検知したことのないAndroidアプリの解析

50,000,000
ニューラルネットワークの類似性比較のためのファイル

600,000,000 /日
データ保護のために追加されたLive Protectionイベント

30,000+ /日
マルウェア対策サンプルをLive Protectionに追加

300,000,000
Deep Larningに使用されるファイル

SophosLabsの世界規模の脅威調査インフラストラクチャは、マルウェアの傾向とサイバー脅威を地域全体で追跡します。

SophosLabs解析プラットフォーム

私たちの解析フレームワークは解析レイヤを使って未知のもの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ーは、特定の特徴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2の青線の外側にあるファイルを適切に識別および解析をするためのリソースが無いため、常に高度なマルウェアを通過させてしまいます。フィード・フォワード、コンボリューション、反復、方策勾配法などの詳細な学習方法を追加することで、図3のオレンジ線で囲まれたマルウェアに見られるような疑わしい属性を持つファイルを識別することができます。
このようにして、私たちはそうでなければ検出されなかったであろう多くのマルウェアの亜種への対策ソリューションの有効性を拡大します。

- SophosLabの30年以上に渡る脅威解析とマルウエア対策の経験を活用する
- Sophos製品では、SophosLabの脅威インテリジェンスサービスが積極的に使用されている
- SophosLabの送信ロジックは、更なる解析が必要な疑わしいファイルを特定するのに役立つ
- WebおよびEmail Gatewayとクラウド製品が、より迅速なブロックと透過の判断を下すための情報を受け取る
- EDR、MDR、IRのユースケーモに関する詳細なインテリジェセス
  スポートを入手できる
- 伝統的な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

図 1：一般的なマルウェア対策テクノロジー

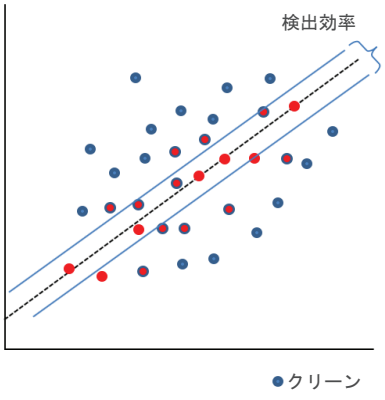
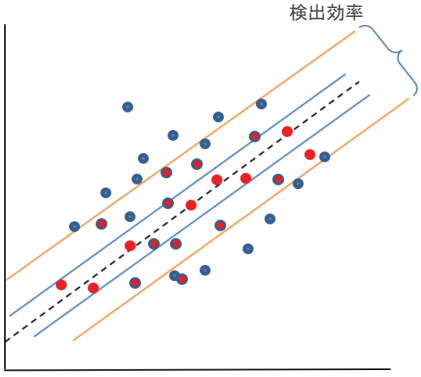


図 2: SophosLabs AIの検出支援



データソースとキュレーション

全てはSophosのネットワーク、エンドポイント、モバイル製品のテレメトリーを様々な補足的なデータと統合して、グローバルな可視性を得ることから始まります。Sophosの自動キュレーションは、エントリの重複排除、脅威オブジェクトの分類、誤検知の減少および評価の更新を行います。競合する脅威データは、Sophosの脅威解析の専門家による解析のためのエスカレーションされます。

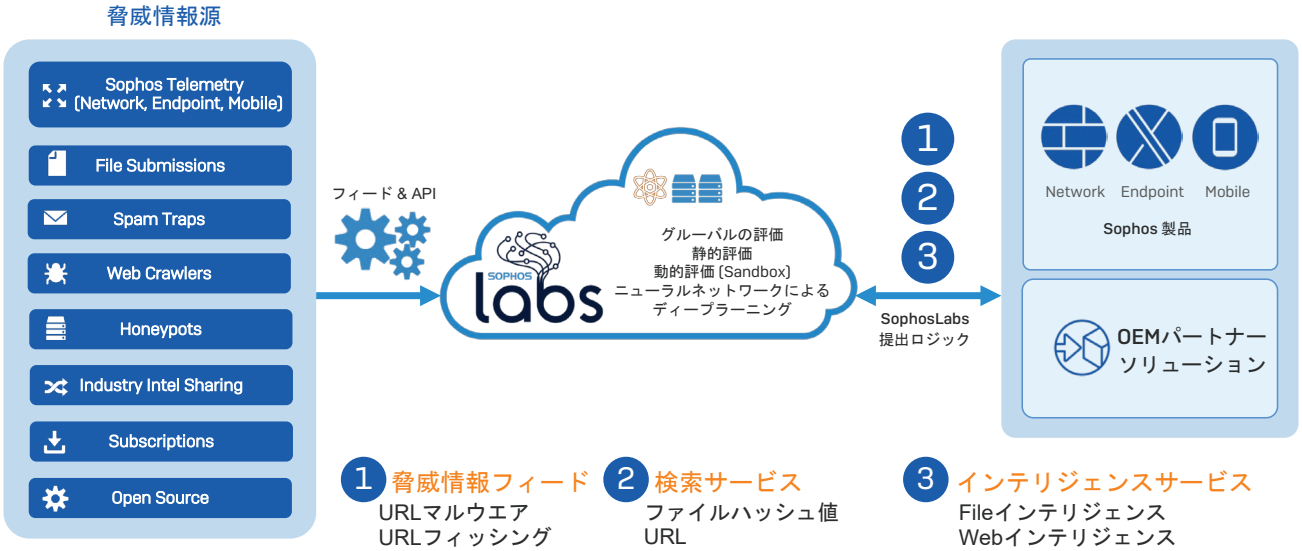


図3: SophosLabs データソースと脅威インテリジェントサービス

1 脅威情報フィード
URLマルウエア
URLフィッシング
URLスパム
URLカテゴリ

2 検索サービス
ファイルハッシュ値
URL
IP
APKフィンガープリント

3 インテリジェンスサービス
Fileインテリジェンス
Webインテリジェンス
静的評価
動的評価

フィード

マリシャスURL

SophosLabから提供する悪意のあるURLデータは、他のベンダーに比べてSophos固有または補完的なデータとして提供しています。私たちの目標は、精巧な悪意のあるURLを使って、データの独自性と品質向上を向上させ、より正確な脅威情報を提供することです。

一般的なカテゴリ	ドメイン	URI	詳細
マルウェアダウンロード	3,000,000+	43,000,000+	マルウェアを拡散するように設計された既知の悪意のあるサイト
マルウェアコマンド、コントロール	670,000	-	既知の悪意のあるサイト
リダイレクトによる感染サイト	190,000	-	マルウェアのリダイレクトが以前にに判明しているクリーンなサイト
好ましくないアプリ(PUA)	-	2,200,000+	不審なアプリとのリンク
フィッシングサイト	660,000	2,000,000	既知およびセロデイフィッシングサイトとのリンク
Emailによるスパムサイト	2,000,000	-	既知およびゼロデイスパムサイト

利用ケース

ブロッキング

セキュリティ製品およびサービス

ゲートウェイおよびクラウド
NGFW, UTM, Emailセキュリティ

利点

- フィッシングの防御
- 大幅なスパムの削減
- 非常に高い精度
- 他のデータフィードとの重複を削減

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じて集ま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。

利用ケース

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

ゲートウェイおよびクラウド
NGFW、UTM、Emailセキュリティ

利点

- 企業のポリシーに合致したWebの使用状況の監視と強制
- 好ましくしくないアプリケーション(PUA)のフィルタリング
- 効率的なローカルデータベースのURLで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。

	ファイル マルウェア	マリシャス URL	多彩なURL	APK フィンガープリント
サイズ (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

利用ケース

ブロッキング、脅威ハンティング

一般的な製品とサービス

ゲートウェイおよびクラウド:
NGFW、UTM、Emailセキュリティ、
EDR SOCaaS、 MDR

利点

- SophosLabの最新の脅威情報へのアクセスが可能
- 即時の応答時間
- APIによりデバイスの少ないリソースで利用可能
- ローカルの脅威データベースの保持は不要

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。

スタティック解析

SophosLabsは、判定結果を劇的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ためのスタティック解析を提供します。従来の脅威解析手法とディープ・ラーニングを多用することにより、SophosLabは一般的なファイルについて数秒で判定を下すことができます。

主な機能

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

対応済ファイルタイプ:
.exe, .dll, .doc, .docx, .docm, .xls, .xlsx, or .xlsm, .ppt, .pptx, .pptm, .rtf

利用ケース

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

‣ゲートウェイおよびクラウド: NGFW、UTM、 Emailセキュリティ、EDR
‣SOCaaS、MDR、IR/調査

利点

‣ Office、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
‣ 数秒で評価と情報を導く
‣ SophosLabsのスマートロジックにより、疑わしいファイルを特定して、プログラム的に提示して、さらに解析を進めることができる
‣ あらゆる規模のネットワークを保護するための拡張性

ダイナミック解析（クラウド・サンドボックス）

SophosLabsのクラウド・サンドボックスは、最新の解析手法を利用して、未知のファイルに対する比類ない可視性で悪質なファイルを識別します。

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動作
‣ Sophosのアンチウイルスとメモリ検出	‣ Yaraパターンの深層メモリスキャン	‣ 回避 – サンドボックス対策と仮想マシン対策の戦略
‣ Sophos Intercept Xディープ・ラーニング、CryptoGuard、WipeGuardテクノロジー	‣ 動作パターン – マルウェアに起因するIOC	‣ クリプトマイニング
		‣ 欺くテクノロジー

対応済ファイルタイプ:
.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

‣ SophosLabへの顧客データ送信は、ヨーロッパ、北米、およびアジア太平洋地域の3つの地域データ処理ユニットに保存および処理されるため、顧客は自分の地域内でデータを保持できます。

‣ これらの地域の単位は、私たちが顧客データを保護するために明確なPII境界として作られています。

‣ SophosLabsは、ユーザーが送信したファイルのハッシュを外部の脅威情報ソースと照合することはありますが、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、分類された悪意のあるファイルを全て保持し、適時にファイルを削除します。

セキュリティポリシーの詳細については
https://www.sophos.com/en-us/legal/sophoslabs-information-security-policy.aspx

詳細はこちら
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

2019.02.20 DSNA (GH)

SOPHOS