SOPHOS
Security made simple.

Sophos Intercept X の新機能

2018年 1月

ディープラーニング技術を用いた新しいマルウェア検出機能

ディープラーニング (深層学習) による検出モデルが、新種・未知のマルウェアや、業務上不要と思われるアプリケーションを検出します。

この検出モデルを追加するのに必要な容量は、わずか 20MB 以下で、頻繁なアップデートは不要です。

データに含まれる重要な特徴をモデル自身で見出して自動的に学習を行うのが特長で、正常なファイルと悪意のあるファイルを高い精度で判別することが可能になります。

- **新しく強化されたエクスプロイト対策**
  - **悪意のあるプロセスマイグレーション** – 攻撃者がリモートから実行する Reflective DLL Injection を検知し、システムで実行中のプロセス間を横断的に移動するのを阻止します。
  - **プロセスの権限昇格** – 権限の低いプロセスから権限の高いプロセスへ昇格させるのを防止する機能です。権限昇格は、システムのアクセス権を取得するためによく使われる手段です。
- **新機能 - 悪質なプログラムの確実な防止**
  - **認証情報窃取防止** – メモリや、レジストリ、ハードディスク内に存在するログインパスワードやハッシュ情報が盗み出されるのを防止します。
  - **Code Cave の悪用** – アプリケーションに挿入された悪意のあるコードを検出します。マルウェアを常駐化させたり、ウイルス対策製品を回避するのによく使われる手段です。
  - **APC プロテクション** – Application Procedure Calls (APC) の悪用を検出します。APC は、コードインジェクション「Atom Bombing」の一機能として使われることが多く、また最近では、ランサムウェア「WannaCry」と「NotPetya」の拡散手段として利用された「EternalBlue」や「DoublePulsar」などの攻撃ツールでも使われました。 攻撃者は、APC を使って別のプロセスにコードを注入し、実行を可能にします。
- **プロセスロックダウンの強化**
  - **ブラウザのプロセスロックダウン** – 基本的な動作制限として、悪意のある PowerShell コードがブラウザから起動されるのを阻止します。
  - **HTA ロックダウン** – ブラウザから起動される HTML アプリケーション (HTA) に対して、ブラウザと同様にプロセスロックダウンを適用します。
- **レジストリ保護機能**
  - **Application Verifier の悪用防止** – Application Verifier DLL の置き換えを阻止し、ウイルス対策ソフトや、その他の常駐プロセスが回避されるのを防止します。

検知項目	ユーザー通知	根本原因解析	管理者対応	セキュリティの状態	プロセスの停止
認証情報窃取	○	○	必要 (警告)	赤	○
Code Cave	○	○	不要 (イベント)	緑	○
リモートからの Reflective DLL Injection	○	○	必要 (警告)	赤	○
権限昇格	○	○	必要 (警告)	赤	○
APC プロテクション	○	○	不要 (イベント)	緑	○
Application Verifier	×	×	不要	緑	N/A
ロックダウン (ブラウザからの PowerShell 起動)	○	○	不要 (イベント)	緑	○
ロックダウン (ブラウザからの HTA)	○	○	不要 (イベント)	緑	○

ディープラーニングによるマルウェア検出

新しく追加されたディープ ラーニング モデルは、シグネチャを利用せず、すべての実行可能ファイルを実行前に評価し、マルウェアあるいは業務外ソフトウェアと、正規アプリケーションを区別することができます。

ソフォスは、機械学習に対して独自のアプローチを取っており、広く普及している従来の機械学習に優先して、ディープ ニューラル ネットワークの開発に積極的に取り組んできました。単純な機械学習は、現在もなお、セキュリティ業界で主流を占めていますが、機械学習のコミュニティでは、今や過去のものとなりつつあります。

従来の機械学習に比べ、ディープラーニングが優れている点は以下のとおりです。

- 生データに含まれる特徴を自動的に見つけ出し、高い精度でデータを認識します
- ディープラーニングでは、大量のデータ (ビッグデータ) からセキュリティ脅威情勢を幅広く「暗記」して普遍化し、新種の脅威を検知できるようになるなど、簡単にスケーリングすることが可能です
- 現在主流の人工知能 (AI) テクノロジーであるため、業界最先端の技術革新のメリットを享受できます
- 検知精度が高く、誤検知率が低いほか、他の機械学習を用いた検知システムに比べ、はるかに少ないメモリ消費量で動作します

Intercept X が悪意のある実行可能ファイルを検出する仕組み

ディープ ニューラル ネットワークは、従来型ウイルス対策製品のようにシグネチャベースやヒューリスティックベースのスキャンを実行する代わりに、もっともマルウェアに近いと判定したソフトウェアの特徴を自身で選び出すことができます。こうしたディープラーニングのモデルは、脅威が検出を回避する手口や、不正ソフトウェアの作成方法、さらに、それをインストール・起動させる手段など、コードに含まれる特徴を学習していきます。この情報が、複数のステージから構成されるディープラーニングのアルゴリズムで評価され、対象のソフトウェアがどの程度マルウェアや業務外ソフトウェアに似通っているかを判定し、スコアの高さに基づいて、マルウェア、業務外アプリ、正規アプリに分類します。この一連の処理は、20MB にも満たない大きさのディープ ラーニング モデルによって、わずか 20ミリ秒のうちに行われます。

攻撃検出時の動作

ディープラーニングモデルがマルウェアを検知すると、Intercept X で、検知されたマルウェアが「サプレッションリスト」(誤検知項目のリスト) に含まれていないかどうかが確認されます。誤検知の低減については後述しますが、このサプレッションリストを使用することにより、きわめて高いマルウェア検知率と、低い誤検知発生率の両立を実現しています。

検知した悪意のあるソフトウェアは、自動的に隔離され、同時に根本原因解析が開始します。正常なファイルを誤って検出した場合は、管理者が検出された項目をローカルの許可リストに追加することにより、ファイルを元の場所へ戻すことができます。

マルウェアの実行を未然に防ぐため、エンドポイントのセキュリティは「緑 (正常)」の状態です。

対処方法

攻撃を実行前に検出した場合であっても、管理者が、根本原因解析 (RCA) レポートからデバイスへの侵入経路を確認し、感染拡大を防止するための対策を講じることを推奨します。

管理者が誤検知と判断した場合、イベントの表示画面からその場で、検出されたアプリケーションを許可リストに追加できます。リストに追加すると、すべての該当するデバイスで自動的にアプリケーションが元の場所に戻されます。また、ファイルハッシュや、署名証明書、ファイルパス、ファイル名などの情報が登録されるため、次回からは誤検出されなくなります。

誤検知の低減

新バージョンには、検知したマルウェアを格納する隔離エリアが、新たに追加されました。マルウェアのアクティビティを検知した場合、Sophos Clean は、指示に応じて、ファイルそのものと、関連するレジストリのエントリ、リンク、ファイルなどすべての項目を削除します。その項目は隔離エリアに格納され、管理者は、Sophos Central の検出イベントの画面から項目をリリースすることが可能です。

検知されたマルウェアや、業務上不要と思われるアプリケーション (PUA) の隔離をリリースした場合、ファイルは、グローバルな許可するアプリケーションリストに追加され、エンドポイント上の元の場所へ戻されます。許可するアプリケーションリストにファイルを追加する際、管理者は、ファイルのハッシュ値、署名証明書、またはファイル名 / パスを選択することができます。この情報に基づき、次回からファイルの検出が抑制され、正常どおり実行されるようになります。

誤検知抑制には、お客様固有の誤検知抑制リストの他に、ソフォスが管理するグローバルな抑制機能も活用します。ソフォスの誤検知抑制機能は、Live Protection 機能が有効になっている時は自動的に照合を行い、ソフォスからエンドポイントにフットプリントデータを配信します (ネットワーク接続時)。この仕組みにより、きわめてアグレッシブな形で、ディープラーニングによるマルウェア検出 / 不要と思われるアプリケーション検出が可能となり、 誤検知率を抑えつつ、積極的な検出を行うディープ ラーニング モデルが実現します。

また、他社のソリューションは、設定や調整に長期間を要するものが多いのに対し、ソフォスのディープラーニングモデルは、複雑な設定なしで導入後すぐに利用できるという大きな利点があります。

認証情報窃取防止

Intercept X では、攻撃者がプロセスを制御して、ユーザーや管理者の認証情報をデバイスから盗み出すのを阻止することができます。攻撃者は、さまざまな OS のコンポーネントをターゲットにし、ユーザーや管理者のパスワード (またはハッシュ化されたパスワード) をデバイスから盗み出します。攻撃者が利用するパスワード取得ツールは数十種類にもおよび、代表的なものには、LSASS (Local Security Authority Subsystem Service) をターゲットに認証情報を抽出する「mimikatz」や、ハッシュ化したパスワードを SAM (Security Account Manager) データベースから盗み出す「hashdump」などがあります。

Intercept X が認証情報の窃取を防止する仕組み

Intercept X は、攻撃者が使用する多種多様なツールを検知するのではなく、LSASS ランタイムメモリや、SAM データベースのレジストリに対する認証されていない操作や、ハードディスクから直接認証情報を抽出する動作を検知します。また、さまざまなマルウェアや侵入ツール、ハッキングツールを使用して、本製品の防御機能をテストした結果、LSASS や SAM データベースとやり取りを行う正規のソフトウェアを誤検知することなく、高い防御力を発揮することを確認しています。

攻撃検出時の動作

Intercept X が認証情報の窃取を検知した場合、攻撃を実行しているプロセスを停止し、エンドユーザーに通知を表示します。

これと同時に、根本原因解析が開始され、調査のためのアクティビティに関する警告が管理者に送信されます。

エンドポイントのセキュリティステータスは「赤 (異常)」に変わり、管理者が調査を完了して警告を消去するまでこの状態が続きます。

対処方法

攻撃が実行時に検出された場合は、たとえプロセスを停止しても、その後同じ手口で不正侵入が繰り返されたり、攻撃者がデバイスへのアクセスを維持している可能性があります。たとえば、エンドユーザーが、悪意のあるソフトウェアのインストールを許可したり、マクロの有効化やその他のアクションを実行したりするように仕向けるのは不正侵入の代表的な手口ですが、エンドユーザーの許可なしでひそかに侵入する手口も存在します。

攻撃を検知すると、自動的に警告が生成され、認証情報を窃取する試みがあったことと、インシデントの調査が必要なことが管理者に通知されます。また、Intercept X の根本原因解析機能で、調査に役立つインシデントレポートが自動的に生成されます。

プロセス保護 (Code Cave)

Code Cave とは、正規のソフトウェアを改ざんして、別のアプリケーションを埋め込み、悪用するテクニックを指します。具体的には、正規ソフトウェアのプログラム内の「Code Cave」と呼ばれる普段使用しないセクションに別のアプリケーションが埋め込まれます。Code Cave は、大半のアプリケーションに存在し、この部分にコードを埋め込んでも、元のアプリケーションは問題なく動作します。Code Cave に埋め込まれる実行コードは、単なるリモートシェルの起動コードであることが多く、攻撃者は、この小さなコードを足掛かりに他の操作を実行します。このタイプの攻撃を行うには、デバイスに不正侵入してソフトウェアをインストールするか、Code Cave に悪意のあるコードが埋め込まれているアプリケーションをユーザーがインストールするように仕向ける必要があります。

Code Cave が悪用される大きな理由の 1つは、ユーザーや管理者の目から逃れられやすいという点です。コードが埋め込まれてもアプリケーションは問題なく動作するので、埋め込まれた別のアプリケーションが実行されていることに気づきにくいのです。たとえば、改ざんされたアプリケーションが、通常デバイスにインストールされている標準的な業務ツールであった場合、従来型のウイルス対策製品で問題が検出されたとしても、その業務ツールがマルウェアであるとは考え難いでしょう。管理者は、ウイルス対策製品の誤検知と見なして、問題のアプリケーションを除外リストに追加してしまうかもしれません。このようにして、エンドポイントにマルウェアを潜伏させるだけでなく、埋め込んだアプリケーションの実行を管理者が許可するように仕向けることさえもできてしまいます。

Intercept X が Code Cave を阻止する仕組み

Code Cave を悪用してアプリケーションに別のソフトウェアを埋め込むためのツールは多数存在しますが、従来型のウイルス対策製品は、Code Cave にコードを挿入したときに残される痕跡や、明らかな特徴のみに着目するものがほとんどです。それに対し、Intercept X は、そうした従来のアプローチではなく、アプリケーションそのものに対して、Code Cave が悪用されていないかどうか評価を行います。ソフトウェアの初期実行時にアプリケーションを評価し、Code Cave 内に埋め込まれている別のアプリケーションの存在を検出すると、アプリケーションを停止します。

攻撃検出時の動作

Intercept X は、Code Cave の悪用を検出すると、アプリケーションを停止するとともに、ユーザーに通知を表示します。

これと同時に、根本原因解析が開始され、調査のためのアクティビティに関する警告が管理者に送信されます。

最後に、Sophos Clean によってデバイス上のマルウェアが除去されます。

対処方法

Code Cave の悪用が検出された場合、管理者は根本原因解析を確認し、どのようにしてコードを埋め込まれたアプリケーションがデバイスにインストールされたのかを確認する必要があります。攻撃者は、あらかじめ別の手段でデバイスを感染させておいたうえで、侵入先のデバイスに確実に潜伏できるように、Code Cave を悪用した攻撃を仕掛けたのかもしれません。この攻撃がブロックされたことで、攻撃者が他の攻撃手段や侵入手段を探っていることも考えられます。エンドユーザーが、コードが埋め込まれているアプリケーションをダウンロードするように仕向けられた場合は、その段階で攻撃を阻止できることが多いでしょう。しかし、攻撃者が、どのようにデバイスに侵入しようとしたのか、侵入経路を確認しておくと、トレーニングの実施や追加ポリシーの適用など、今後の対策の検討に役立ちます。

プロセス保護 (悪用防止 – リモートから実行される Reflective DLL Injection)

プロセスマイグレーションは、デバイスに最初に常駐化しようとしたとき、権限昇格を実行したり、アクセスを継続する目的で、別のプロセスへ移動するためによく使われるテクニックです。ブラウザを閉じたり、感染プロセスを終了するといったエンドユーザーの操作に関わることなくコントロールを維持したがります。攻撃者はシステムプロセスに移動できるのがもっとも望ましいです。

マイグレーションを実行すれば、リモートからの Reflective DLL Injection の継続が可能になります。一般的な DLL インジェクションに関する詳細は、MITRE による説明 (英語) をご覧ください。リモートからの Reflective DLL Injection も類似の攻撃ですが、既に感染させているプロセスから、別のプロセスを操作して DLL を読み込み、任意のコードを実行するため、より対応が難しくなります。

Intercept X が悪意のあるマイグレーションを阻止する仕組み

Intercept X は、プロセスの振る舞いを常時監視し、リモートプロセスにメモリを割り当て、プロセスに DLL を注入しようとする動作を検知します。通常では起こり得ない動作であるため、Intercept X が検知した場合は、その動作が悪質なものであり、感染システム上で継続的な攻撃活動や、マルウェアのスクリプトが実行されているといえます。

攻撃検出時の動作

Intercept X は、前述の手法で攻撃者が別プロセスに横断的な移動をしようとする動きを検知すると、攻撃を実行しているプロセスを停止し、エンドユーザーに通知を表示します。

これと同時に、根本原因解析が開始され、調査のためのアクティビティに関する警告が管理者に送信されます。

エンドポイントのセキュリティステータスは「赤 (異常)」に変わり、管理者が調査を完了して警告を消去するまでこの状態が続きます。

対処方法

攻撃を実行時に検出した場合は、デバイスで攻撃活動が継続している可能性があります。たとえ攻撃の実行プロセスを停止しても、その後同じ手口で不正侵入が繰り返されたり、攻撃者が別のプロセスへのアクセスを維持している可能性もあります。

検出時には警告が生成され、プロセスマイグレーション (Reflective DLL Injection をリモート実行する目的の) を検出したことと、デバイスの詳しい調査が必要であることが管理者に通知されます。また、Intercept X の根本原因解析機能で、調査に役立つインシデントレポートが自動的に生成されます。

プロセス保護 (権限昇格)

多くの場合、システムに潜入した時点の不正プログラムは、その後に展開する攻撃を実行するのに必要なレベルの権限を持っていません。認証情報の窃取からプロセスマイグレーションにいたるまで、権限昇格の手段は多岐にわたりますが、こうした経路は Intercept X によって塞がれるため、攻撃者は他の手段を使わざるを得ません。まず思い浮かぶのは、特権を持つプロセスの認証トークンを盗み出し、別のプロセスに注入して権限を昇格させるテクニックです。

デバイス上で実行されているすべてのプロセスは、認証トークンを保有しており、オペレーティングシステムは、このトークンを使用してプロセスに許可されている特権を判定します。このため、攻撃者は、システムプロセスの認証トークンを盗み出そうとする場合があります。システム特権を持つプロセスの認証トークンを盗み出し、それを利用できれば、攻撃者は、管理者パスワードを探り当てたり、プロセスマイグレーションで権限を取得したりすることなく、何でもできるようになります。セキュリティパッチ未適用の Windows デバイスに存在するカーネルの脆弱性を突いて、特権を持つトークンをプロセスから取得し、目的遂行のために利用するテクニックは、数多くドキュメントが公開され、特権を持つトークンを盗む手口の数を考えると、公に知られていない OS やカーネルの脆弱性は、まだまだ存在することが推察できます。

Intercept X がトークンの窃取を阻止する仕組み

Intercept X は、特権トークンの窃取に利用される多様な既知の脆弱性ではなく、認証トークンをプロセスに注入し、権限を昇格する動作を検知します。正規のソフトウェアで、このような動作が行われることはないため、攻撃活動によるものであるといえます。Intercept X は、権限昇格攻撃に利用される脆弱性の種類や、未知・既知にかかわらず、その動作を検知して攻撃から防御します。

攻撃検出時の動作

プロセスを停止し、エンドユーザーに通知を表示します。これと同時に、Sophos Clean がマルウェアのクリーンアップを開始します。

また、根本原因解析機能では、攻撃プロセスの開始方法や、根本原因や検知された権限昇格がデバイスに及ぼす影響が自動的に割り出されます。

攻撃によりデバイスが不正侵入された可能性が高く、詳しい調査が推奨されるため、エンドポイントのセキュリティステータスは「赤 (異常)」に変わります。

対処方法

他のエクスプロイト検出時と同様に、管理者は、根本原因解析のレポートを確認し、攻撃の展開手法や侵入経路を究明する必要があります。

調査が終了したら、警告を消去し、感染前と同様の操作をデバイスに許可します。

プロセス保護 (APC の悪用 – AtomBombing)

AtomBombing は、攻撃者が正規のアプリケーションにマルウェアや別のコードを仕込むために使う手法です。最近発見された比較的複雑な手法で、OS の ATOM テーブルや非同期プロシージャコールといった仕組みを悪用します。AtomBombing の詳細については、こちら (英語) をご覧ください。

Intercept X が AtomBombing を阻止する仕組み

Intercept X は、APC の悪用を検知します。以前から Intercept X に実装されているさまざまなエクスプロイト防止機能と同様に、カーネルレベルでプロセスの振る舞いを監視し、このタイプの動作を検出することが可能です。

攻撃検出時の動作

アプリケーションの悪用を停止し、エンドユーザーに通知を表示します。

また同時に、Sophos Clean がマルウェアのクリーンアップを開始するほか、根本原因解析機能が、攻撃プロセスの開始方法や、マルウェアが及ぼした影響を自動的に割り出します。

対処方法

他のエクスプロイトを検出した場合と同様に、管理者は、根本原因解析レポートから攻撃の開始方法を確認し、必要な対策を検討する必要があります。

レジストリ保護 (Application Verifier の悪用防止 – DoubleAgent)

この攻撃手法は、前述の例とはまた別のレジストリの悪用テクニックです。具体的には、アプリケーションの起動時に実行するソフトウェアが登録されているレジストリを変更します。Microsoft Application Verifier の本来の意図は、開発者がアプリケーションの問題を発見したり、その原因を突き止めたりできるようにすることですが、この機能を利用した攻撃では、実行中のアプリケーションの防御機能を回避し、権限を乗っ取ることが可能です。この攻撃手法は 2017年、ニュースに取り上げられました。ウイルス対策製品の多くが、自身のレジストリの変更を防ぐことができず、悪意のあるアプリケーションの実行が可能である点が注目されたからです。しかし、実際に Application Verifier が悪用されれば、ウイルス対策製品ばかりでなく、OS 上のアプリケーションすべてに影響が及ぶ恐れがあります。詳細については、Sophos Naked Security の記事をご覧ください。

Intercept X がレジストリキーの変更を阻止する仕組み

Intercept X は、Application Verifier の使用時に、認証された Windows の DLL を強制的に実行するため、たとえ攻撃者がレジストリの変更に成功し、攻撃を実行に移した場合でも、不正に変更されたレジストリはアプリケーションによって無視されます。

また、注目すべき点は、既存の他社製ウイルス対策製品の追加機能として、Intercept X を導入した場合、他社製ウイルス対策製品も DoubleAgent (Application Verifier を悪用した攻撃) から防御されることです。

攻撃検出時の動作

Application Verifier を悪用して別のアプリケーションを起動する目的でレジストリが変更された場合、エンドユーザーへの通知も、警告の生成も行われません。認証された Microsoft Windows のツールのみを強制的に起動します。

プロセスロックダウンの強化 (ブラウザと HTML アプリケーション)

Intercept X には従来より、プロセスタイプに基づき、さまざまな悪意のある動作を阻止する「プロセスロックダウン機能」が実装されています。今回さらにロックダウン機能を拡張し、Web ブラウザによる PowerShell の実行防止や、ブラウザから起動される HTML アプリケーション (HTA) のプロセスロックダウンが可能になりました。

Intercept X がブラウザから起動されるアプリケーションを阻止する仕組み

Intercept X は、ブラウザからアプリケーションが起動されると、そのアプリケーションを自動的にブラウザとして識別し、対応するロックダウンが作動して、PowerShell などが実行する悪意のある動作を阻止します。ロックダウンは、カーネルレベルでアプリケーションの振る舞いを監視する Intercept X の特性を活かした機能で、常にアプリケーションと並行して実行されます。

攻撃検出時の動作

こうしたアプリケーションの挙動を検出した場合、アクティビティは未然に阻止され、ユーザーに通知が表示されます。

同時に、管理者が確認するためのイベントも生成されます。

また、このタイプの悪意のある動作を検知すると、インシデントの調査に役立つ根本原因解析が自動的に開始されます。

ソフォス株式会社営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

2017-11-30 (MP)

SOPHOS