ESET Glossary

ユーザー ガイド

この文書のオンラインバージョンを表示するにはこちらをクリックしてください。

Digital Security
Progress. Protected.

Copyright ©2023 by ESET, spol. s r.o.

ESET GlossaryはESET, spol. s r.o.によって開発されています

詳細についてはhttps://www.eset.comをご覧ください。

All rights reserved.本ドキュメントのいかなる部分も、作成者の書面による許可がない場合、電子的、機械的、複写、記録、スキャンなど、方法または手段の如何をと遭わず、複製、検索システムへの保存、または転送が禁じられています。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: https://support.eset.com

改訂: 2023年/4月/19日

1 ESET用語集の概要 1
1.1 アドウェア 1
1.2 ボットネット 1
1.3 誤検出(FP) 2
1.4 パッカー 2
1.5 安全ではない可能性があるアプリケーション 2
1.6 望ましくない可能性があるアプリケーション 2
1.7 ランサムウェア 6
1.8 ルートキット 7
1.9 リターン指向プログラミング 7
1.10 スパイウェア 7
1.11 トロイの木馬 8
1.12 ウイルス 9
1.13 ワーム 9
1.14 クレデンシャルスタッフィング攻撃 9
1.15 DNSキャッシュポイズニング 10
1.16 DoS攻撃 10
1.17 ICMP攻撃 10
1.18 ポートスキャン 10
1.19 SMBリレー 11
1.20 TCP非同期 11
1.21 ワーム攻撃 11
1.22 ARPキャッシュポイズニング 12
2 電子メール脅威 12
2.1 広告 12
2.2 デマ 13
2.3 フィッシング 13
2.4 迷惑メール詐欺の特定 13
2.4 ルール 14
2.4 ホワイトリスト 14
2.4 ブラックリスト 15
2.4 例外 15
2.4 サーバー側での検査 15
2.5 詳細メモリ検査 15
2.6 インターネットバンキング保護 16
2.7 ボットネット保護 16
2.8 DNA検出 16
2.9 ESET LiveGrid® 17
2.10 エクスプロイトブロッカー 17
2.11 Javaエクスプロイトブロック 18
2.12 ESET LiveSense 18
2.13 機械学習 19
2.14 ネットワーク攻撃保護 19
2.15 ランサムウェア保護 19
2.16 スクリプトに基づく攻撃保護 19
2.17 安全なブラウザー 20
2.18 UEFIスキャナー 20
2.19 Canaryファイル 21
2.20 デッドロック 21

ESET用語集の概要

ESET用語集は、現在の脅威と、脅威から保護するESET技術について、包括的な概要を説明します。

トピックは、各章に分けられ、次の内容を説明します。

- 検出 – コンピューターウイルス、ワーム、トロイの木馬、望ましくない可能性があるアプリケーションなどがあります。
- リモート攻撃 – ローカルネットワークまたはインターネット上で発生する脅威
- 電子メール脅威 – デマ、フィッシング、詐欺などがあります。
- ESET技術 - ESETセキュリティソリューションで提供されている製品機能

アドウェア

アドウェアは、広告機能をサポートしているソフトウェアです。広告を表示するプログラムが、このカテゴリーに分類されます。アドウェアアプリケーションは、広告が表示される新しいポップアップウィンドウをインターネットブラウザ内に自動的に開いたり、ブラウザのホームページを変更したりすることがよくあります。アドウェアは、フリーウェアプログラムの開発者がその開発費を賄うことができるように、フリーウェアによく添付されています。

アドウェア自体は、危険ではありません。ユーザーは広告に悩まされるだけです。危険なのは、アドウェアが(スパイウェアと同様に)追跡機能を発揮することもある、という事実にあります。

フリーウェア製品を使用することにした場合には、インストールプログラムに特に注意してください。大半のインストールプログラム(インストーラー)は、アドウェアプログラムを追加でインストールすることをユーザーに通知します。アドウェアのインストールをキャンセルし、アドウェアなしで目的のプログラムをインストールできることが一般的です。

場合によっては、アドウェアをインストールしないと目的のプログラムをインストールできなかったり、機能が制限されてしまうこともあります。これは、そのアドウェアが頻繁にシステムに「合法的に」アクセスする可能性があることを意味します。ユーザーがアドウェアのインストールに同意したからです。この場合、後悔するよりは用心した方が賢明です。アドウェアとして検出されるファイルがコンピューターにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

ボットネット

ボットまたはWebロボットは自動マルウェアプログラムであり、ネットワークアドレスのブロックを検査し、脆弱なコンピューターを感染させます。 これによって、ハッカーが同時に複数のコンピュータを乗っ取り、これらのコンピューターをボット(ゾンビ)に変えることができます。 一般的に、ハッカーはボットを使用して、ネットワークまたはボットネットを形成する多数のコンピューターを感染させます。 ボットネットがコンピューターにあると、分散型サービス拒否攻撃(DDoS)で使用されることができます。また、ユーザーが知らない間にインターネット上での自動乗っ取りを実行するために使用することもできます(迷惑メール、ウイルスの送信、または銀行の認証情報やクレジットカード番号などの個人情報の窃盗など)。

誤検出(FP)

現実的に、100%の検出率保証というものはなく、感染していないオブジェクトが誤って検出に分類されることを完全に回避する方法もありません。

誤検出は、感染していないファイルやアプリケーションが誤ってマルウェアやPUAに分類されることです。

パッカー

圧縮プログラムは、複数の種類のマルウェアを1つのパッケージにロールアップするランタイム自己解凍実行可能ファイルです。

最も一般的な圧縮プログラムにはUPXPE_CompactPKLiteおよびASPackがあります。別の圧縮プログラムを使用して圧縮した場合、同じマルウェアが異なって検出されることがあります。圧縮プログラムには、シグネチャを時間の経過と共に変化させ、マルウェアの検出と削除を困難にする機能もあります。

安全ではない可能性があるアプリケーション

ネットワークに接続されたコンピューターの管理を容易にする機能を持つ適正なプログラムはたくさんあります。 ただし、悪意のあるユーザーの手に渡ると、不正な目的で悪用される可能性がありますESETにはこのようなアプリケーションを検出するオプションがあります。

[**安全ではない可能性があるアプリケーション**]は、市販の適正なソフトウェアに適用される分類です。これには、リモートアクセスツール、パスワード解析アプリケーション、キーロガー(ユーザーが入力した各キーストロークを記録するプログラム)などのプログラムが含まれます。

安全ではない可能性があるアプリケーションがコンピューターに存在して実行されている(しかも、自分ではインストールしていない)ことに気づいた場合には、ネットワーク管理者まで連絡するか、そのアプリケーションを削除してください。

望ましくない可能性のあるアプリケーション

グレイウェアまたは望ましくない可能性があるアプリケーション(PUA)は、ウイルスまたはトロイの木馬などの他のタイプのマルウェアほどはっきりとした意図がない幅広いソフトウェアのカテゴリです。ただし、追加の不審なソフトウェアをインストールし、デジタルデバイスの動作または設定を変更し、ユーザーによって承認または想定されていないアクティビティを実行する可能性があります。

グレイウェアと見なされることができるカテゴリ: 広告表示ソフトウェア、ダウンロードラッパー、各種ブラウザーツールバー、誤解を招く動作のソフトウェア、バンドルウェア、トラックウェア、プロキシウェア(インターネット共有アプリケーション)、仮想通貨マイナー、レジストリクリーナ(Windowsオペレーティングシステムのみ)、他のきわどいソフトウェア、非合法または少なくとも非倫理的なビジネス慣行を使用し、インストールが許可されている場合に、ソフトウェアの動作を認識したエンドユーザーによっては望ましくないと考えられる可能性があるソフトウェア(ただし合法的に見える)。

危険な可能性があるアプリケーションは、合法的な(商業的な場合もある)ソフトウェアですが、攻撃者によって悪用される可能性があるアプリケーションです。 このようなタイプのアプリケーションの検出は、ESETソフトウェアのユーザーが有効または無効にできます。

場合によっては、ユーザーが、リスクよりも望ましくない可能性があるアプリケーションを使用する利

点があると感じることがあります。 このため、このようなアプリケーションには、トロイの木馬やワームなどの他のタイプの悪意のあるソフトウェアと比べ、低いリスクのカテゴリが割り当てられています。

- 警告 – 不審なアプリケーションの検出
- 設定
- ソフトウェアラッパー
- レジストリクリーナー
- 望ましくないコンテンツの可能性があります

> **図解手順**
> ESET Windowsホーム製品で望ましくない可能性のあるアプリケーション(PUA)を検査して削除するには、ESETナレッジベース記事を参照してください。

警告 – 不審なアプリケーションの検出

望ましくない可能性があるアプリケーションが検出されたら、実行するアクションを決定できます。

1.**駆除/切断**: アクションを終了し、システムに侵入するPUAを防止します。
Webサイトからのダウンロード中にはPUA通知の**切断**オプションが表示され、ディスクのファイルでは**駆除**オプションが表示されます。

2.**無視**: このオプションではPUAがシステムに入るのを許可します。

3.**検出から除外する**: コンピューターに既にある検出されたファイルを今後中断せずに実行できるようにするには、**詳細オプション**をクリックし、検出から除外の横にあるチェックボックスをオンにし、**無視**をクリックします。

4.**検出から署名を除外する**: 特定の検出名(署名)によって特定されたすべてのファイルが、今後(既存のファイルやWebダウンロードから)中断せずにコンピューターで実行できるようにするには、**詳細オプション**をクリックし、**検出から署名を除外する**の横のチェックボックスを選択して、**無視**をクリックします。同じ検出名の追加の検出ウィンドウが直後に表示される場合は、無視をクリックして閉じます(追加のウィンドウは、検出から署名を除外する前に発生した検収津に関連付けられます)。



設定

ESET製品をインストールするときには、次のように、望ましくない可能性があるアプリケーションの検出を有効にするかどうかを決定できます。



警告

望ましくない可能性があるアプリケーションは、アドウェア、ツールバーをインストールしたり、他の望ましくない危険なプログラム機能を含んでいたりすることがあります。

これらの設定は、いつでも、プログラム設定で修正できます。望ましくない、危険、または不審なアプリケーションの検出を有効または無効にするには、次の手順に従ってください。

1. ESET製品を開きます。

2. **F5**キーを押して、**詳細設定**にアクセスします。

3. **検出エンジン**（前のバージョンでは、**ウィルス対策**または**コンピューター**）をクリックして、**望ましくない可能性のあるアプリケーションの検出を有効にする**、**安全でない可能性があるアプリケーションの検出を有効にする**、**不審なアプリケーションの検出を有効にする**から任意のオプションを有効または無効にします。**OK**をクリックして確認します。



図解手順

PUAを検出または無視するように製品を設定する詳細な手順については🛈ESETナレッジベース記事をご覧ください。

- ESET NOD32 Antivirus / ESET Internet Security / ESET Smart Security Premium
- ESET Cyber Security for macOS / ESET Cyber Security Pro for macOS
- ESET Endpoint Security / ESET Endpoint Antivirus for Windows
- ESET Mobile Security for Android

ソフトウェアラッパー

ソフトウェアラッパーは、特別なタイプのアプリケーション修正で、ファイルホスティングWebサイトの一部で使用されます。 これは、ダウンロードするつもりのプログラムをインストールするサードパーティ製のツールですが、ツールバーやアドウェアなどの追加ソフトウェアもインストールします。 追加されたソフトウェアは、Webブラウザのホームページや検索設定を変更する場合があります。 また、多くの場合、ファイルホスティングWebサイトはソフトウェアベンダーやダウンロード受信者に、修正が行われたことを通知しないため、通常はオプトアウトオプションが非表示になっています。 このため🛈ESETはソフトウェアラッパーを望ましくない可能性があるアプリケーションのタイプに分類しています。ユーザーはダウンロードするかどうかを決定できます。

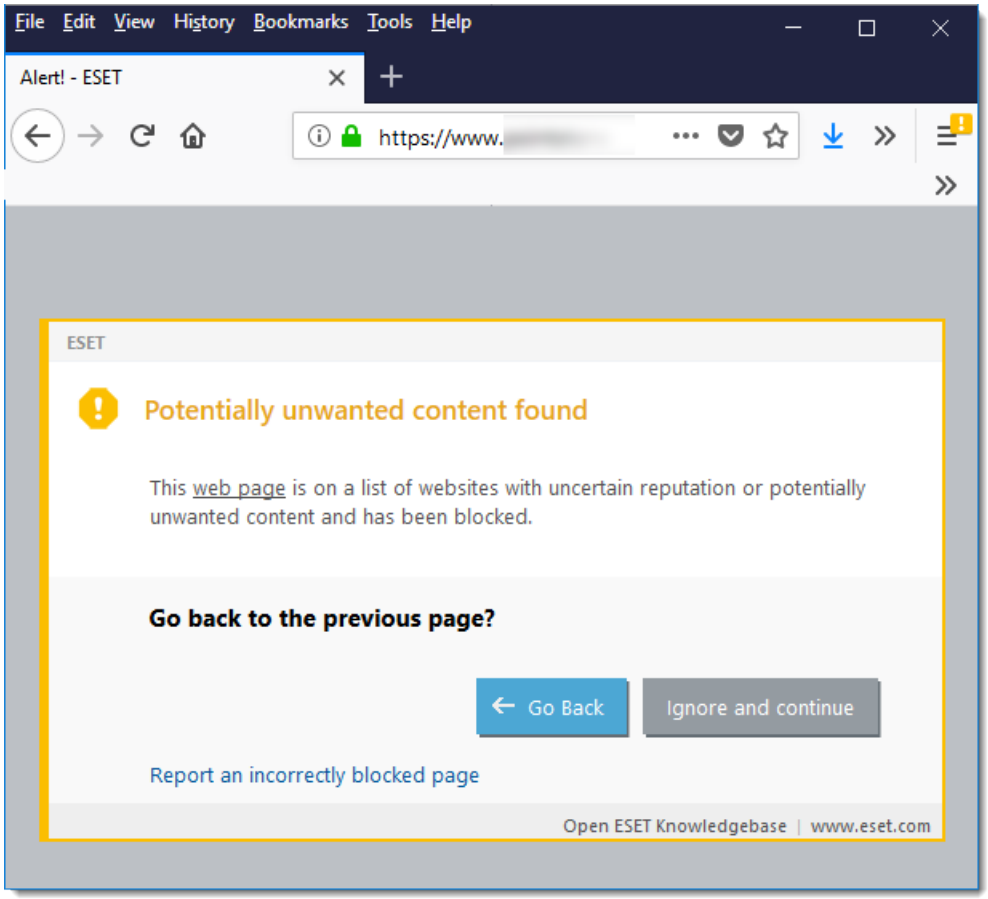
レジストリクリーナー

レジストリクリーナーは、Windowsレジストリデータベースで定期的なメンテナンスまたはクリーニングが必要であることを提案できるプログラムです。レジストリクリーナーを使用すると、コンピュータシステムにとってリスクとなる可能性があります。また、一部のレジストリクリーナーは、「無料のスキャン」の結果に基づいて、その利点に関する資格がないか、検証不能であるか、根拠がない主張を行ったり、コンピュータシステムに関する誤解を招くレポートを生成します。このような誤解を招く主張やレポートは、通常、支払う前にレジストリクリーナーを評価させずに、正式バージョンまたはサブスクリプションを購入するように説得しようとします。このような理由のため🛈ESETはこのようなプログラ

ムをPUAに分類し、許可またはブロックするオプションを提供します。

望ましくないコンテンツの可能性があります

ESET製品でPUA検出が有効な場合、PUAを推奨するレピュテーションがあるWebサイトや、システムやブラウジング経験に否定的な影響を与える可能性があるアクションを実行するようにユーザーの判断を誤らせる評価があるWebサイトは望ましくない可能性があるコンテンツとしてブロックされます。アクセスしようとしているWebサイトが望ましくない可能性があるコンテンツに分類されたという通知を受信した場合は、**戻る**をクリックして、ブロックされたWebページから移動するか、**無視して続行する**をクリックして、サイトの読み込みを許可することができます。



このトピックの詳細については、ESETナレッジベース記事を参照してください。

ランサムウェア

ランサムウェア(ファイルコーダー)はマルウェアの一種であり、デバイスをロックしたり、デバイスの内容を暗号化したりして、内容に再びアクセスするために金銭を強請り取ります。この種類のマルウェアには、あらかじめプログラミングされた支払期限が設定されたビルトインのタイマーが実装されていることがあり、この期限を満たす必要があります。期限を守らない場合は、価格が上がったり、最終的にデバイスにアクセスできなくなります。

デバイスを感染させ、ファイルコーダーがそのデバイス上の共有ドライブの暗号化を試行する場合があります。このプロセスにより、マルウェアがネットワーク上に拡散しているかのように見えることがありますが、実際にはそうではありません。この状況は、ファイルサーバーの共有ドライブが暗号化されているが、サーバー自体にマルウェア感染がある(ターミナルサーバーではない場合)ときに発生します。

ランサムウェアの作成者は、公開鍵と秘密鍵という鍵のペアを生成し、公開鍵をマルウェアに挿入します。ランサムウェア自体はトロイの木馬の一部であるか、電子メール、ソーシャルネットワーク、また

はインスタントメッセンジャーで受信できるファイルや画像のように見えることがあります。コンピューターに侵入した後、マルウェアはランダムな対称鍵を作成し、デバイスのデータを暗号化します。ランサムウェアはデータを復号するために金銭の支払いを要求します。デバイスに表示される支払要求メッセージは、システムが違法な活動で使用されたという内容や、違法なコンテンツを含んでいるという内容の虚偽の警告である場合があります。ランサムウェアの被害者は、提示された支払方法によって身代金を支払うように要求されます。一般的に、このオプションは、デジタル(暗号)通貨、高額料金のSMSメッセージ、プリペイドバウチャーなどの追跡が難しい方法です。支払いを受け取った後、ランサムウェアの作成者はデバイスをロック解除するか、秘密鍵を使用して、対称鍵を復号し、被害者のデータを復号します。ただし、この処理は保証されません。

> **ランサムウェア保護の詳細**
>
> ESET製品は複数レイヤーの技術を使用し、デバイスをランサムウェアから保護します。ランサムウェアからシステムを保護するためのベストプラクティスについては、ESETナレッジベース記事を参照してください。

ルートキット

ルートキットとは、自己の存在を隠しながら、インターネットからの攻撃者が、システムに無制限にアクセスできるようにする悪意のあるプログラムです。ルートキットは、システムにアクセス(通常はシステムの脆弱性を悪用します)した後、オペレーティングシステムのさまざまな機能を使用して、ウイルス対策ソフトウェアによる検出を免れます。具体的には、プロセス、ファイル、およびWindowsレジストリーデータを隠します。そのため、通常のテスト技術を使用して検出することはほとんどできません。

ルートキットから保護するための検出処理には2つのレベルがあります。

1.システムへのアクセスを試みているときには、まだシステム内には存在しないので、活動していません。このレベルなら、たいていのウイルス対策システムはルートキットを排除できます(ウイルス対策システムが、ルートキットに感染しているファイルを実際に検出したと仮定した場合)。

2.通常の検査で検出されない場合ESETユーザーはアンチステルス技術を利用して、アクティブなルートキットを検出して駆除できます。

リターン指向プログラミング

リターン指向プログラミング(ROP)は、一般的なコード再利用攻撃です。攻撃者は、悪意のある結果をもたらす既存のコードを制御フローを誘導しますROP攻撃は、スタック破壊攻撃の高度なバージョンです。通常は固定長バッファーの意図するデータ構造外のプログラムの呼び出しスタックで、メモリアドレスに書き込まれると、スタックバッファーオーバーフローが発生します。

ROPはターゲットシステムでのコードの実行を可能にするエクスプロイト技術です。呼び出しスタックの制御を取得することで、攻撃者は、コンピューターで実行中の既存の信頼できるソフトウェアのフローを制御し、意図された以外のタスクを実行するようにそのソフトウェアを操作します。

スパイウェア

このカテゴリーには、本人の同意も認識もないまま個人情報を送信するすべてのアプリケーションが該当します。スパイウェアは、追跡機能を使用して、アクセスしたWebサイトの一覧、ユーザーの連絡先リストにあるメールアドレスや、記録されたキーストロークなどのさまざまな統計データを送信します。

スパイウェアの作成者は、こうした手法はユーザーのニーズと関心に関するデータをさらに見つけ、的

を絞った広告を出せるようにすることが目的であると主張します。問題は、有益なアプリケーションと悪意のあるアプリケーションとの間に明確な境界線がなく、しかも、引き出された情報が悪用されることはない、とだれも断言できないことです。スパイウェアが収集したデータには、セキュリティコード PIN 銀行の口座番号などが含まれていることがあります。スパイウェアはフリーバージョンのプログラムの作成者が、プログラムに同梱していることがよくあります。これは、収益を上げたり、そのプログラムを購入するよう動機を与えるためです。プログラムのインストール中に、スパイウェアが含まれていることをユーザーに知らせることもよくあります。これは、スパイウェアが含まれない有料バージョンにアップグレードするよう促すためです。

スパイウェアが組み入れられている、よく知られているフリーウェア製品の例としては P2P (ピアツーピア) ネットワークのクライアントアプリケーションがあります Spyfalcon や Spy Sheriff を始めとする多数のプログラムは、スパイウェアの特定のサブカテゴリに属します。これらは一見、スパイウェア対策プログラムに見えますが、実はそれ自体がスパイウェアプログラムなのです。

スパイウェアとして検出されるファイルがコンピューターにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

スパイウェアのサブカテゴリであるキーロガーには、ハードウェアベースのキーロガーとソフトウェアベースのキーロガーがあります。ソフトウェアベースのキーロガーは、単一の Web サイトまたはアプリケーションに入力された情報のみを収集できます。高度なキーロガーは、コピー/貼り付けした情報を含め、入力したすべてを記録できます。モバイルデバイスを対象にした一部のキーロガーは、通話、メッセージングアプリケーション、位置情報、マイクとカメラキャプチャからの情報を記録できます。

トロイの木馬

従来、コンピューター分野でのトロイの木馬は、自己を有益なプログラムに見せかけ、ユーザーを騙して実行させようとするマルウェアの1つのクラスとして定義されてきました。

トロイの木馬の範囲は非常に広いので、多くのサブカテゴリーに分類されることもよくあります。

- ダウンローダー– インターネットから他の脅威をダウンロードする機能を備えた悪意のあるプログラム。
- ドロッパー– 被害を受けるコンピューターに他の種類のマルウェアを取り込む悪意のあるプログラム。
- バックドア– リモートの攻撃者と通信して、コンピューターにアクセスし制御権を乗っ取れるようにする悪意のあるプログラム
- キーロガー –（キーストロークロガー）– ユーザーが入力した各キーストロークを記録し、リモートの攻撃者にその情報を送信するプログラム。
- ダイヤラー– ユーザーのインターネットサービスプロバイダーではなく有料情報サービスを介して接続するよう設計された悪意あるプログラム。 新しい接続が作成されたことにユーザーが気づくのは、ほとんど不可能です。 ダイアラーで被害を被るのは、ダイヤルアップモデムを使用するユーザーのみです。このモデムは今日ではあまり使用されていません。

コンピューター上のファイルがトロイの木馬として検出された場合、削除することをお勧めします。悪意のあるコードしか入っていない可能性が高いからです。

ウイルス

コンピューターウイルスとは、コンピューター上の既存ファイルに事前にまたは後から追加される悪意あるコードのことです。 ウイルスは生物学上のウイルスにちなんで名付けられました。同じような手法でさまざまな場所に蔓延していくからです。 「ウイルス」という用語は、あらゆる種類の脅威を意味するかのように誤って使用されることがよくあります。 この用法は徐々に敬遠されるようになり、より正確な用語「マルウェア」(悪意のあるソフトウェア)へと次第に言い換えられています。

コンピューターウイルスは、主に実行可能ファイルとドキュメントを攻撃します。コンピューターウイルスの動作を簡単に説明します。ファイルに感染した後で、元のアプリケーションの実行よりも前に、悪意あるコードが呼び出されて実行されます。ウイルスは、ユーザーが書き込み権限を持つすべてのファイルに感染することができます。

コンピューターウイルスの目的と重大さは、多種多様です。ハードディスクからファイルを意図的に削除できるウイルスもあり、このようなウイルスは大変危険です。一方、実質的には被害を及ぼさないウイルスもあります。作成者が単にユーザーを困らせ、自分の技量を誇示することが目的であるに過ぎないものもあります。

コンピューターがウイルスに感染し、駆除できない場合、詳しい検査を実査するためにESETリサーチラボに送ってください。 場合によっては、感染したファイルは、駆除不可能であるためクリーンなコピーに置き換える必要があるほどに、改ざんされていることがあります。

ワーム

コンピューターワームとは、感染先のコンピューターを攻撃しネットワークを介して蔓延する、悪意のあるコードの入ったプログラムを指します。ウイルスとワームの基本的な違いは、ワームは独自に伝播できる点にあります。ワームは宿主ファイル(またはブートセクター)に依存しません。ワームはアドレス帳の電子メールアドレスを介して広がるか、またはネットワークアプリケーションのセキュリティ上の脆弱性を悪用します。

したがって、ワームはコンピューターウイルスよりはるかに実行可能性が高いです。インターネットは広く普及しているため、ワームはリリースから数時間、場合によっては数分で世界中に蔓延することがあります。自己を単独で急速に複製できる能力があるので、他の種類のマルウェアよりはるかに危険です。

システム内でワームが活性化すると、多くの不都合な事態が引き起こされることがあります。ファイルの削除、システムパフォーマンスの低下だけでなく、プログラムが動かなくなることすらあります。コンピューターワームはその本来の性質ゆえに、他の種類の侵入物の"輸送手段"となります。

コンピューターがワームに感染した場合は、感染ファイルを削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

クレデンシャルスタッフィング攻撃

クレデンシャルスタッフィング攻撃は、漏洩した資格情報データベースのデータを使用するサイバー攻撃です。攻撃者はボットと他の自動化方法を利用し、漏洩したデータを使用しながら、多数のWebサイトのアカウントにログインします。攻撃者は、複数のWebサイトやサービスでログイン資格情報を使い回しているユーザーを利用します。攻撃が成功すると、攻撃者はアカウントとこのアカウントに保存されたユーザーのデータに完全にアクセスできます。攻撃者はこのアクセスを悪用して、個人データを盗み、ID窃盗、詐欺取引、迷惑メールの送信、その他の悪意のある行為を実行できます。

DNSキャッシュポイズニング

DNS(ドメインネームサーバ)キャッシュポイズニングを使用すると、ハッカーは任意のコンピューターのDNSサーバーを騙し、偽のデータを提供して正規の（本物の）データであると信じさせることができます。特定の期間キャッシュされる偽の情報を利用して、攻撃者はDNSからのIPアドレスの返答を書き換えることができます。その結果、インターネット上のWebサイトにアクセスしようとするユーザーが、本来のコンテンツではなくコンピューターウイルスやワームをダウンロードさせられることがあります。

DoS攻撃

DoS(サービス拒否)とは、対象のユーザーがコンピューターやネットワークを使用できないようにする行為です。攻撃を受けるユーザー間の通信は、妨害されるので、正常に機能し続けることはできなくなりますDoS攻撃にさらされたコンピューターは通常、再起動する必要があります。そうしないと、正常に機能しません。

大半の場合、標的とされるのはWebサーバーであり、その目的はある程度の期間、それらのサーバーをユーザーが使用できなくすることです。

ICMP攻撃

ICMP (Internet Control Message Protocol)は人気が有り、広く使用されているインターネットプロトコルです。これはネットワーク接続されたコンピューターが様々なエラーメッセージを送信する為に主に使用されます。

リモートアタッカーは、ICMPプロトコルの脆弱性を悪用しようとしますICMPプロトコルは、認証を必要としない一方向の通信用に設計されています。 そのため、リモートアタッカーは、いわゆるDoS (Denial of Service)攻撃、つまりサービス拒否攻撃や、認証されていないユーザーに受信および送信パケットへのアクセス権を与える攻撃を開始することができます。

ICMP攻撃の一般的な例としてpingフラッドICMP_ECHOフラッド、およびsmurf攻撃がありますICMP攻撃にさらされたコンピューターは処理速度が大幅に低下し(これは、インターネットを使用する全てのアプリケーションに該当します)、インターネットへの接続に関する問題が発生します。

ポートスキャン

ポートスキャンは、ネットワークホスト上のどのポートが開いているかの特定に使用されます。ポートスキャナーは、そのようなポートを見つけるためのソフトウェアです。

ポートとは、受信データと送信データを処理する仮想的な出入口のことです。これは、セキュリティの観点からは重要です。ネットワークが大規模な場合、ポートスキャナーが収集した情報が、潜在的な脆弱性を特定するのに役立つことがあります。このような使用法は、合法です。

ただし、ポートスキャンは、セキュリティを低下させようとするハッカーが悪用することもよくあります。ハッカーが行う最初の手順としては、パケットが各ポートに送信されます。その応答の種類に応じて、使用中のポートを判断することができます。スキャン自体は無害ですが、潜在的な脆弱性をあらわにし、攻撃者がリモートコンピューターを制御できるようにする可能性もあることに注意してください。

ネットワーク管理者は、未使用のポートをすべてブロックし、使用中のポートを無許可のアクセスから保護するよう勧められています。

SMBリレー

SMB RelayとSMB Relay 2は、リモートコンピューターに攻撃を仕掛けることができる特殊なプログラムです。 このプログラムは、Server Message Blockファイル共有プロトコルを利用します。このプロトコルはNetBIOSの上位層で機能します LAN内でフォルダーやディレクトリーを共有する場合、このファイル共有プロトコルを使用するのが一般的です。

ローカルネットワーク通信内では、パスワードハッシュが交換されます。

SMB Relayは、UDPポート139と445で接続を受信し、クライアントとサーバー間で交換されるパケットを中継して、そのパケットを書き換えます。 接続して認証した後、クライアントは接続を切断されます SMB Relayは、新しい仮想のIPアドレスを作成します。 新しいアドレスには、コマンド"net use \\192.168.1.1"でアクセスできます。 これ以降、このアドレスは、Windowsのネットワーク機能で使用できます SMB Relayはネゴシエーションと認証以外のSMBプロトコル通信を中継します。 クライアントコンピューターが接続している限り、リモートの攻撃者はこのIPアドレスを利用できます。

SMB Relay 2はSMB Relayと同じ原理で機能しますがIPアドレスではなくNetBIOS名を使用する点が異なります。 両方とも「中間者攻撃」という攻撃を実行できます。 この攻撃では、リモートの攻撃者は、2つの通信端末間で交換されるメッセージの読み取り、挿入、および変更を密かに行えます。 このような攻撃にさらされるコンピュータは、応答しなくなるか、突然に再起動することがよくあります。

攻撃を避けるため、認証パスワードか認証鍵の使用をお勧めします。

TCP非同期

TCPハイジャック攻撃に使われる技術です。それは、着信パケットの連続番号が予想される連続番号と異なっているプロセスによってトリガされます。 予期しない順序番号を持つパケットが棄却されます（それらは現在の通信ウィンドウ内に存在する場合バッファー記憶域に保存されます ）。

非同期処理では、双方の通信端末が、受信パケットを破棄します。リモートの攻撃者はこの部分に侵入して、正しいシーケンス番号を持つパケットを送り込むことができます。 通信を操作したり、変更したりすることもできます。

TCPハイジャック攻撃の目的は、サーバー/クライアント通信やピアツーピア通信を妨害することです。多くの攻撃は、各TCPセグメントに認証を使用することで回避できます。 また、使用しているネットワークデバイス向けの推奨設定を使用してください。

ワーム攻撃

コンピューターワームとは、感染先のコンピューターを攻撃しネットワークを介して蔓延する、悪意のあるコードの入ったプログラムを指します。ネットワークワームは、さまざまなアプリケーションに存在するセキュリティ上の脆弱性を悪用します。インターネットを使用できるので、ワームはリリースから数時間以内に世界中に蔓延することがあります。

大半のワーム攻撃(SasserやSqlSlammerなど)は、ファイアウォールの既定のセキュリティ設定を使用するか、または保護されていないポートと未使用のポートをブロックすることにより、防ぐことができます。また、最新のセキュリティパッチでオペレーティングシステムをアップデートすることも重要です。

ARPキャッシュポイズニング

アドレス解決プロトコル(ARP)は、データリンクレイヤ(MACアドレス)とネットワークレイヤ(IPアドレス)のアドレス間を変換しますARPキャッシュポイズニング攻撃によって、攻撃者は、ネットワークのARPテーブル(MACとIPデバイスマッピング)を破損させることで、ネットワークデバイス間の通信を傍受することができます。

攻撃者は、誤ったARP応答メッセージを既定のネットワークゲートウェイに送信し、MACアドレスが別の宛先IPアドレスに関連付けられていることを通知します。既定のゲートウェイがこのメッセージを受信し、ネットワーク上の他のすべてのデバイスに変更をブロードキャストすると、他のネットワークデバイスへのすべてのターゲットのトラフィックが攻撃者のコンピューターを経由します。このアクションにより、攻撃者は、意図する宛先に転送する前に、トラフィックを検査または変更できます。

電子メール脅威

電子メールは、多数の利点を備えた通信形態です。

しかし、匿名性が高いため、電子メールとインターネットには迷惑メールなどの不正な活動の余地があります。迷惑メールには、受信者側が送信を要求していない広告、デマ、悪意のあるソフトウェア(マルウェア)の拡散があります。送信費が最小限であること、また、迷惑メールの作成者には新しいメールアドレスを入手するさまざまなツールがあることから、ユーザーに対する迷惑行為や危険性は増加しています。さらに、迷惑メールの量や多様性のために、規制することは非常に困難です。メールアドレスを長く使用するほど、迷惑メールエンジンデータベースに登録される可能性が高くなります。

回避策をいくつか紹介します。

- 可能な場合、インターネットに電子メールアドレスを公開しない。
- 信頼できる個人のみにメールアドレスを知らせる。
- 可能な場合、一般的なエイリアスを使用しない。複雑なエイリアスを使用するほど、追跡される可能性が低くなります。
- 受信ボックスに既に着信した迷惑メールに返信しない。
- インターネットフォームに記入する際に注意する。特に、"はい。お知らせを受け取ります"のようなオプションには注意してください。
- 仕事専用のアドレスと、友人との通信専用のアドレスなど、"専用の"電子メールアドレスを使用する。
- 電子メールアドレスを定期的に変更する。
- 迷惑メール対策ソリューションを使用する。

広告

インターネット広告は、最も急速に普及している広告の一つです。マーケティング上の主な利点は、コストが最小限である、直接性のレベルが高い、さらにメッセージがほぼ瞬時に配信される、という点です。多くの企業では、メールをマーケティングツールとして使用して、既存顧客および見込み客と効果的に連絡を取り合っています。

この種の広告は、適正なものです。ユーザーは製品に関する商業上の情報を受け取ることに関心がある可能性があるからです。しかし、多くの企業が、受信者側が送信を要求していない商業メッセージを大量に送っています。このような場合、メール広告は迷惑メールになってしまいます。

一方的に送信されてくるメールの量が実際に問題になっており、減少する兆しはありません。こうしたメールの作成者はたいてい、迷惑メールを適正なメッセージに見せかけようとします。

デマ

デマは、インターネットを通じて広がる偽情報です。デマは、通常電子メールやICQやSkypeなどの通信ツール経由で送信されます。メッセージ自体はジョークや都市伝説であることがほとんどです。

コンピュータウイルスとしてのデマは、受信者に恐怖、不安、および疑念(FUD)を抱かせ、ファイルの削除、パスワードの詐取、その他、システムを不正に操作する検出不能なウイルスがあると信じこませます。

一部のデマは、他のユーザーにメッセージを送信するよう求め、デマを拡散させます。携帯電話によるデマ、援助を求める訴え、海外からの送金の申し出などがあります。ほとんどの場合、作成者の意図を突き止めることは不可能です。

知り合い全員に転送するよう求めるメッセージは、確実にデマであると考えられます。インターネット上には、適正なメールであるかどうかを確認できるWebサイトが多数あります。デマの疑いがあるメッセージを受け取った場合は、転送する前にインターネットで検索してみてください。

フィッシング

フィッシングとは、ソーシャルエンジニアリング(機密情報を入手するために、ユーザーを操ること)のさまざまな手法を用いる犯罪行為を指します。その目的は、銀行の口座番号やPINコードなどの機密データを入手することです。

入手するための一般的な手口は、信頼できる人物や企業(金融機関や保険会社など)を装い、メールを送ることです。 このメールは本物そっくりに見えることがあり、成り済ます相手が使用しているグラフィックやインターネットコンテンツが含まれているのが一般的です。 データの確認や金融業務を装い、個人データを入力するようユーザーに指示します。たとえば、銀行の口座番号やユーザー名とパスワードなどです。 このようなデータは、いったん提出すると、簡単に盗まれ悪用されてしまいます。

銀行、保険会社、およびその他の合法的な企業は、受信者側が送信を要求していないメールでユーザー名とパスワードを入力するよう要求することなど、決して行いません。

迷惑メール詐欺の特定

通常、いくつかの指標を参考にすることで、メールボックス内の迷惑メール(受信者が送信を要求していないメール)を特定することができます。メールが少なくとも次の基準のいくつかを満たしている場合、迷惑メールの可能性があります。

- 送信元アドレスが連絡先リスト内の連絡先のものでない。
- 多額のお金が提供されるが、最初に少額を提供する必要がある。
- データの確認や金融業務を装い、銀行の口座番号やユーザー名とパスワードなどの個人データを入力するよう求められる。

• 外国語で記載されている。

• 関心のない製品を購入するよう求められる。購入することにした場合は、メールの送信元が信頼できるベンダであることを確認してください(本来の製品製造元に問い合わせてください)。

• 迷惑メールフィルターを騙そうとして、単語のスペルを間違えている。 たとえば"viagra"の代わりに"vaigra"と記載している場合などです。

ルール

ウイルス対策ソリューションと電子メールクライアントに関する限りでは、ルールを使用すると、メール機能を操作することができます。 ルールは次の2つの論理的部分で構成されます。

1.条件(たとえば、受信メッセージが、ある特定のアドレスから送信されたか、特定の電子メール件名が付いたものである)

2.アクション(たとえば、メッセージを削除したり、指定フォルダに移動したりする)

ルールの数と組み合わせは、迷惑メール対策ソリューションに応じて異なります。このルールは、迷惑メール(受信者側が送信を要求していないメール)を防ぐための手段となります。よくある例は、次のとおりです。

1. 条件:受信メールに、迷惑メールメッセージ特有の語がいくつか含まれる。
2. アクション:メッセージを削除する。

1. 条件:受信メールに、拡張子が.exeの添付ファイルが含まれる。
2. アクション:添付ファイルを削除し、メッセージをメールボックスに配信する。

1. 条件:雇用者からの受信メッセージである。
2. アクション:メッセージを"仕事"メールを指定のフォルダに移動する。

管理し易くし、迷惑メールのフィルタリングの効果を向上させるため、迷惑メール対策プログラムで複数のルールを組み合わせて使用することをお勧めします。

ホワイトリスト

一般に、ホワイトリストとは、受け入れられる物や人物、または許可を与えられている物や人物の一覧を指します。「電子メールホワイトリスト」(許可されたアドレス)という用語は、ユーザーがメッセージを受信したいと思う相手の連絡先の一覧を意味します。このようなホワイトリストは、電子メールアドレス、ドメイン名、またはIPアドレスで検索するキーワードに基づきます。

ホワイトリストを"除外モード"で使用すると、一覧にないアドレス、ドメイン、またはIPアドレスからのメッセージは、受信されません。除外モードでない場合には、そのようなメッセージは削除されず、別の仕方でフィルタリングされます。

ホワイトリストは、ブラックリストとは正反対の原則に基づきます。ホワイトリストの保守は、ブラックリストより簡単です。ホワイトリストとブラックリストの両方を使用して、迷惑メールをより効果的

にフィルタリングすることをお勧めします。

ブラックリスト

一般にブラックリストとは、受け入れられないかまたは禁止されている品目や人物の一覧のことです。仮想世界では、そのような一覧に掲載されている全ユーザーからのメッセージを拒否するためのテクニックです。

ブラックリストには、2種類あります。ユーザーが迷惑メール対策ソフトウェアを使用して作成したブラックリストと、定期的にアップデートされる、専門機関が作成したインターネット上にある専門的なブラックリストがあります。

迷惑メールを防ぐには、ブラックリストの使用は不可欠ですが、保守が困難です。ブロックすべき新しい項目が毎日現れるからです。迷惑メールをより効果的にフィルタリングするには、ホワイトリストとブラックリストの両方を使用することをお勧めします。

例外

通常、例外リスト(例外のリスト)には、偽装されている可能性がある電子メールアドレスと迷惑メールの送信に使用されている可能性がある電子メールアドレスが含まれます。例外リストに登録されているアドレスから送信されたメールに対しては、迷惑メールの検査を常に行います。既定では、既存メールクライアントのアカウントにあるすべての電子メールアドレスは、例外リストに入っています。

サーバー側での検査

サーバー側での検査とは、受信したメッセージ数とユーザーの反応に基づいて、大量の迷惑メールを特定するための手法のことです。 各メッセージは、その内容に基づいて、固有のデジタル"痕跡"を残します。 この固有のID番号でメールの内容を知ることはできません。 2通のメッセージが、同じであれば痕跡も同じであり、異なれば痕跡も異なります。

あるメッセージが迷惑メールとしてマークされた場合、その痕跡がサーバーに送信されます。サーバーが同じ痕跡(ある特定の迷惑メールメッセージに対応します)をさらに受信すると、痕跡は迷惑メール痕跡データベースに格納されます。受信メッセージを検査する際に、メッセージの痕跡がサーバーに送信されます。サーバーはユーザーにより迷惑メールとして既にマークされているメッセージに対応する痕跡に関する情報を返します。

詳細メモリ検査

詳細メモリ検査はエクスプロイトブロックとともに動作し、難読化または暗号化を使用することで、マルウェア対策製品の検出を回避するように設計されたマルウェアに対する保護を強化します。 標準のエミュレーションまたはヒューリスティックでは脅威が検出されない場合、詳細メモリ検査によって、不審な動作を特定し、システムメモリに現れたときには脅威をスキャンできます。 このソリューションは、非常に難読化されたマルウェアに対しても有効です。

エクスプロイトブロックとは異なり、詳細メモリ検査は実行後方式です。つまり、脅威が検出される前に、一部の悪意のあるアクティビティが実行されているリスクがあります。ただし、他の検出技術が失敗した場合は、追加レイヤーのセキュリティが実装されています。

インターネットバンキング保護

オンラインバンキングと決済の保護は、オンライン処理中に金融データを保護するための強化された保護レイヤーです。

ESET Smart Security PremiumとESET Internet Securityには、安全なブラウザーが開くように事前定義されたWebサイトのビルトインリストが含まれています。Webサイトを追加したり、製品の設定でWebサイトのリストを編集したりできます。

すべてのブラウザーを保護を有効にすると、すべてのサポートされているWebブラウザーを安全モードで起動できます。

この新機能の詳細については、次のESETナレッジベース記事をお読みください。

- ESET Banking and Payment保護を使用する方法
- ESET Windowsホーム製品でインターネットバンキング保護を一時停止または無効にする
- ESETインターネットバンキング保護 – 一般的なエラー

HTTPS暗号化通信の使用は、ブラウジングの保護に必要となります。次のブラウザーはインターネットバンキング保護をサポートしています。

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

任意のWebブラウザーでインターネットバンキング保護を開く

製品メニューの**ツール**タブから直接インターネットバンキング保護を開くときにはWindowsで既定に設定したWebブラウザーで開きます。そうでない場合は、任意のWebブラウザー(製品メニューからではない)を開くときに、保護されたWebサイトのリストのWebサイトがESETで保護されたのと同じ種類のWebブラウザーにリダイレクトされます。

ボットネット保護

ボットネット保護は、ネットワーク通信プロトコルを解析して、マルウェアを検出します。 ボットネットマルウェアは、過去数年間変更がないネットワークプロトコルとは対照的に頻繁に変更されています。この新しい技術によってESETは、検出を逃れ、コンピューターをボットネットネットワークに接続しようとするマルウェアを無効にできます。

DNA検出

検出タイプには、非常に固有のハッシュから、悪意のある動作とマルウェア特性の複雑な定義であるESET DNA検出までがあります。悪意のあるコードは、攻撃者が簡単に修正したり、難読化したりすることができますが、オブジェクトの動作はそれほど簡単には変更できませんESET DNA検出は、この原

理を利用するために設計されました。

コードと、その動作の根源である正確な「遺伝子」を深く分析し、ESET DNA検出を行います。これを使用して、ディスクにあるか、実行中のプロセスメモリにあるかどうかに関係なく、潜在的に不審なコードを評価しますDNA検出は、特定の確認済みのマルウェアサンプル、確認済みのマルウェアファミリーの新しいバリアント、または悪意のある動作を示す遺伝子を持つ未確認または未知のマルウェアさえも特定できます。

ESET LiveGrid®

ESET LiveGrid®高度早期警告システム上に構築されたESETThreatSense.Netはユーザーが世界中で提出したデータを収集し、ESETのリサーチラボに送信します。 世界中の不審なサンプルとメタデータを提供することでESET LiveGrid®によって、お客様のニーズに即時に対応し、最新の脅威に対するESETの対応力を確保できます。

ESETのマルウェア研究者はこの情報を使用して、グローバル脅威の特性とスコープの正確なスナップショットを構築し、適切な目標に集中できるようにしますESET LiveGrid®データは、自動処理の優先度設定において重要です。

また、レピューテーションシステムを導入し、マルウェア対策ソリューションの全体的な効率を改善します。ユーザーは、このプログラムのインターフェイスまたはコンテキストメニューから直接、実行中のプロセスとファイルのレピューテーションを確認し、ESET LiveGrid®にある詳細情報を取得できます。実行ファイルまたはアーカイブがユーザーのシステム上で検査されているときに、まずハッシュタグがホワイトリストおよびブラックリスト項目のデータベースに対して比較されます。ホワイトリストで検出された場合、検査されたファイルはクリーンと見なされ、今後の検査対象から外されるように設定されます。ブラックリストで検出された場合、脅威の特性に応じて適切なアクションが実行されます。一致するものがない場合、ファイルは徹底的に検査されます。この検査の結果に基づいて、ファイルは脅威または脅威以外に分類されます。このアプローチは、検査のパフォーマンスに対して大幅に好ましい影響を及ぼします。このレピューテーションシステムによって、1日に数回更新されるウイルスデータベース経由で署名がユーザーのコンピューターに配信される前に、マルウェアサンプルを効果的に検出できます。

ESET LiveGrid®レピューテーションシステムとESET LiveGrid®フィードバックシステムは、新しく検出された脅威に関連して、コンピューターに関する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、そのファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、およびコンピューターのオペレーティングシステムについての情報が含まれます。

ESET LiveGrid®サーバー

ESET LiveGrid®サーバーはブラチスラバ、ウィーン、サンディエゴにありますが、これらはクライアントからの要求に応答するサーバーにすぎません。送信されたサンプルの実際の処理は、スロバキアのブラチスラバでのみ実施されます。

ESET製品でESET LiveGrid®を有効または無効にする

ESET製品でESET LiveGrid®を有効または無効にする詳細と図解手順については、ESETナレッジベース記事をご覧ください。

エクスプロイトブロッカー

エクスプロイトブロッカーは、Webブラウザ PDFリーダー、電子メールクライアントMicrosoft Officeコンポーネントおよび製品などの一般的に利用されるアプリケーションタイプの保護を強化し、ROP攻撃から保護します。既定では、エクスプロイトブロッカーは、すべてのESET Windowsホーム製品ESET製

品(Windowsサーバー版)、ESETエンドポイント製品(Windows版)で使用可能で有効です。

エクスプロイトを示す可能性がある不審な活動のプロセスの動作を監視します。

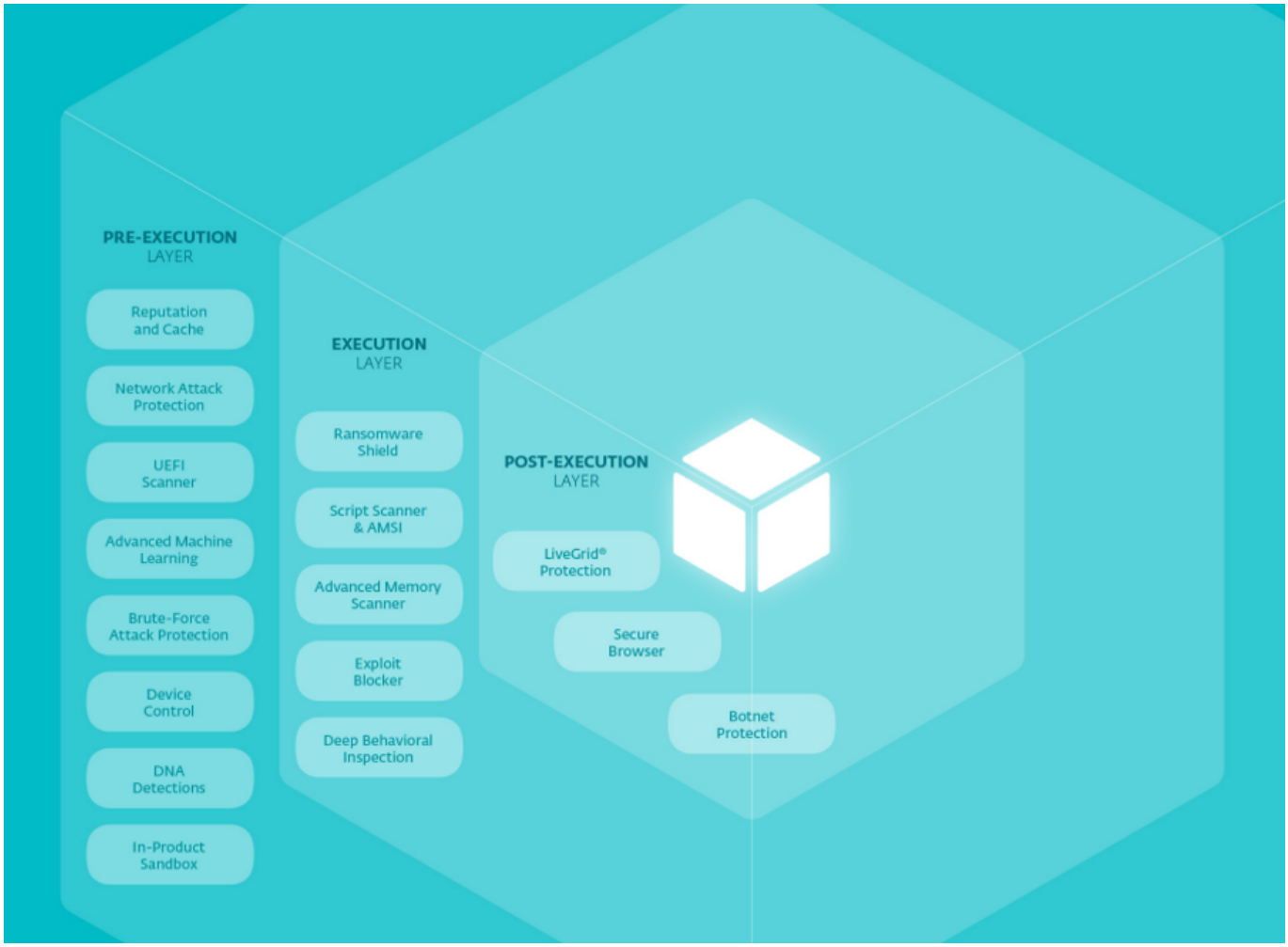
エクスプロイトブロッカーによって不審なプロセスが特定されると、プロセスがただちに停止され、脅威に関するデータがESET LiveGrid®に送信されます。このデータはクラウドシステムに送信されます。このデータはESETリサーチラボによって処理され、すべてのユーザーを未確認の脅威とゼロデイ攻撃(設定済みの修正策がない新しくリリースされたマルウェア)からより効果的に保護するために使用されます。

Javaエクスプロイトブロック

Javaエクスプロイトブロッカーは既存のエクスプロイトブロック機能の拡張版です。Javaを監視し、エクスプロイトのような動作を探します。ブロックされたサンプルはマルウェアアナリストに送信できます。アナリストは署名を作成し、別のレイヤ(URLブロック、ファイルダウンロード、など)でこれらをブロックできます。

ESET LiveSense

ESETには、ESET LiveSenseと組み合わせて使用される独自の独自の専有的な階層型保護技術が使用されます。次の図は、ESETのコア技術の一部を示し、システムのライフサイクル中に脅威を検出し、最終的にブロックできる期間と場所を示します。



機械学習

ESETは、1990年から機械学習アルゴリズムを活用して、脅威を検出してブロックしてきました。1998年には、ニューラルネットワークがESET製品の検出エンジンに追加されました。

機械学習にはDNA検出が含まれます。これは、機械学習に基づくモデルを使用して、クラウド接続の有無に関係なく、効果的に処理を行います。機械学習アルゴリズムは、初期段階の受信サンプルの仕分けや分類でも重要であり、受信サンプルを仮想の「サイバーセキュリティマップ」に配置します。

ESETは独自の社内機械学習エンジンを開発しました。ニューラルネットワーク(深層学習、長・短期記憶など)の能力を組み合わせて、手動で選択した6つの分類アルゴリズムを使用します。これにより、結果が連結され、受信サンプルを感染なし、不審な可能性、悪意の可能性に正しくラベリングできます。

ESETの機械学習エンジンは、DNA、サンドボックス、記憶分析、行動特性の抽出といった他の保護技術と調和するように微調整されており、検出率を可能なかぎり高め、誤検出数を可能なかぎり低く抑えます。

ESET製品の詳細設定でスキャナーを設定する

- ESET Windowsホーム製品(13.1以降)
- ESET Windowsエンドポイント製品(7.2以降)

ネットワーク攻撃保護

ネットワーク攻撃保護はファイアウォールの拡張であり、ネットワークレベルで既知の脆弱性のエクスプロイトの検出能力が強化されます。SMB、RPC、RDPなどの広く使用されるプロトコルで一般的なエクスプロイトの検出機能を導入することで、拡散するマルウェア、ネットワーク実行攻撃、パッチがリリースまたは展開されていない脆弱性の利用に対する保護において重要なレイヤーを追加します。

ランサムウェア保護

ランサムウェア保護は、行動に基づく検出手法であり、ランサムウェア/ファイルコーダーに共通の方法でファイルを修正しようとするアプリケーションとプロセスの動作を監視します。 アプリケーションの動作が悪意があると見なされた場合、またはレピュテーションに基づく検査によって不審なアプリケーションが示された場合、そのアプリケーションがブロックされ、プロセスが停止するか、ユーザーがそれをブロックまたは許可するかを確認します。

ランサムウェア保護が正しく動作するにはESET LiveGrid®を有効にする必要があります。ESET LiveGrid®が有効でESET製品で動作していることを確認するには、ESETナレッジベース記事を参照してください。

スクリプトに基づく攻撃保護

スクリプトに基づく攻撃保護にはWebブラウザーのJavaScriptに対する保護と、PowerShellのスクリプトに対するAntimalware Scan Interface (AMSI)保護があります。

HIPS
この機能が動作するにはHIPSを有効にする必要があります。

スクリプトに基づく攻撃保護は次のWebブラウザーをサポートします。

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

> **サポートされているWebブラウザーを使用**
> Webブラウザーの最低サポートバージョンは、ブラウザーのファイル署名が頻繁に変更されるため、異なる場合があります。 最新バージョンのWebブラウザーは常にサポートされます。

安全なブラウザー

安全なブラウザーは、オンライン閲覧中に機密データを保護するために設計された追加の保護レイヤーです(オンライン取引中の金融データなど)。

ESET Endpoint Security 8以降には保護されたブラウザが開くように事前定義されたウェブサイトのビルトインリストが含まれています。 ウェブサイトを追加したり、製品のコンフィグレーションでウェブサイトのリストを編集したりできます。安全なブラウザーはインストール後に既定で無効です。

この新機能の詳細については、次のESETナレッジベース記事をお読みください。

HTTPS暗号化通信の使用は、ブラウジングの保護に必要となります。 安全なブラウザーを使用するには、お使いのWebブラウザーが以下に示す最小要件を満たしている必要があります。

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

> ARMプロセッサーが搭載されているデバイスではFirefoxおよびMicrosoft Edgeのみがサポートされます。

任意のWebブラウザーでESET安全なブラウザーを開く

製品メニューの**ツール**タブから直接ESET安全なブラウザーを開くときにはESET安全なブラウザーは既定に設定したWebブラウザーで開きます。そうでない場合は、任意のWebブラウザー(製品メニューからではない)を開くときにESET内部リストがESETで保護されたのと同じ種類のWebブラウザーにリダイレクトされます。

UEFIスキャナー

Unified Extensible Firmware Interface (UEFI)スキャナーは、ホストベースの侵入防止システム(HIPS)の一部であり、コンピューターのUEFIファームウェアを保護しますUEFIはブートプロセスの最初にメモリに読み込まれるファームウェアです。 コードは、主基板に半田付けされたフラッシュメモリチップにあります。 感染すると、攻撃者は、システム再インストールおよび再起動の影響を受けないマルウェアを展開できます。 また、このマルウェアは、このレイヤーはほとんどのマルウェア対策ソリューションで検査されないため、マルウェア対策ソリューションによって検出されずに残る可能性があります。

UEFIスキャナーは自動的に有効にされます。 メインプログラムウィンドウでコンピューターの検査を手動で開始するには、**コンピューターの検査** > **詳細検査** > **カスタム検査**をクリックし、**ブートセクタ/UEFI**ターゲットをクリックします。

> コンピューターが既にUEFIマルウェアによって感染した場合は、次のESETに送信ナレッジベース記事をお読みください。
> コンピューターがUEFIマルウェアに感染しました。どうすればよいでしょうか。

Canaryファイル

Canaryファイルは、不正なデータアクセス、コピー、または修正の早期検出を支援するための、実際の文書に配置された偽のコンピューター文書です。

デッドロック

デッドロックとは、各コンピュータープロセスが、別のプロセスに割り当てられたリソースを待機している状態です。この状況では、必要なリソースが、別のリソースの解放を待機している別のプロセスによって占有されているため、どのプロセスも実行されません。デッドロックが発生しないように回避することが重要です。デッドロックの発生はリソーススケジューラーによって検出できます。これにより、オペレーティングシステムは、異なるプロセスに割り当てられたすべてのリソースを追跡できます。次の4つの条件が同時に該当する場合は、デッドロックが発生する可能性があります。

- **プリエンプティブアクションがない** – プロセスがタスクを完了した後に、リソースを占有しているプロセスが自発的にリソースを解放できます。
- **相互排他** – 共有リソースへのアクセスを制御するために使用される特殊なタイプのバイナリセマフォ。これにより、現在の優先度の高いタスクをブロックし続ける時間を可能なかぎり短くすることができます。
- **占有して待機** – この状態では、1つ以上の他のリソースを同時に待機している間に、プロセスが1つ以上のリソースの占有を停止する必要があります。
- **循環待機** – すべてのリソースタイプの合計順序を課します。循環待機では、すべてのプロセスが列挙の昇順でリソースを要求する必要もあります。

デッドロックを処理するには、次の3つの方法があります。

- システムをデッドロック状態にしません。
- デッドロックを発生させます。デッドロックが発生したときには、プリエンプションを実行してデッドロックを処理します。
- デッドロックが発生した場合は、システムを再起動します。