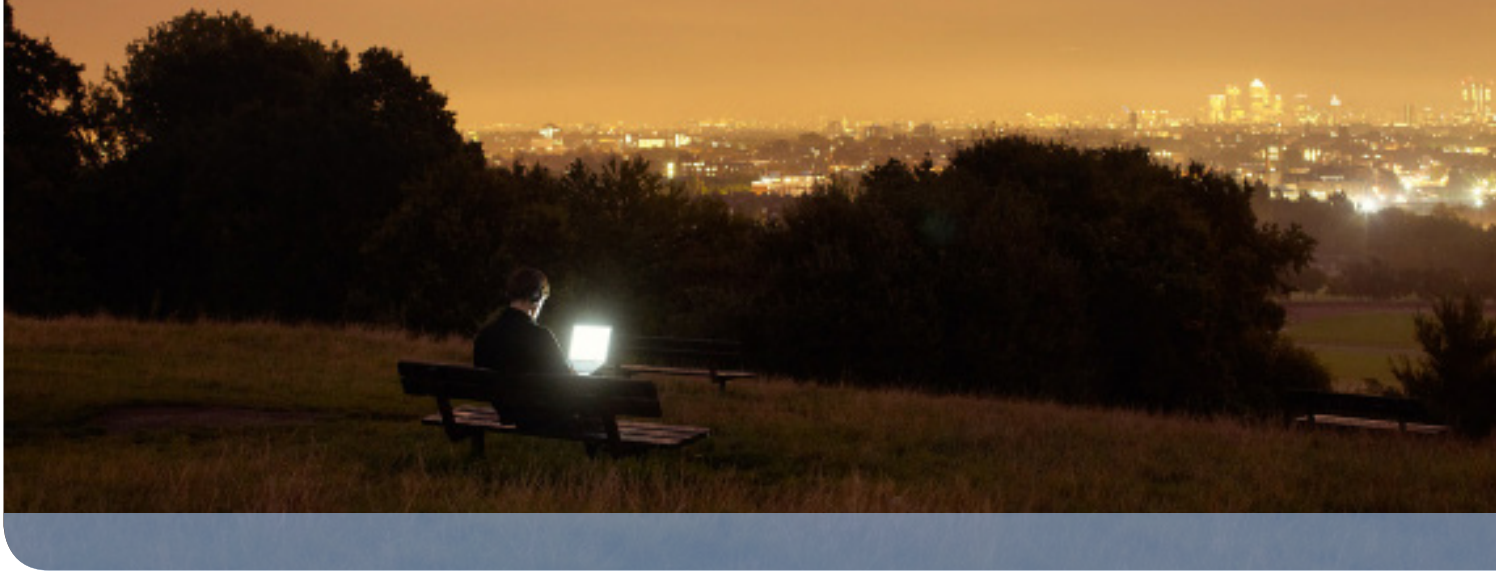


エフセキュア ディープガード

新たな脅威に対するプロアクティブなオンホスト保護

1. プロアクティブな動作分析

この数年間、セキュリティプログラムが対応に追われた最も困難な問題の1つは、攻撃方法の多様化です。特に、インターネット上でホスティングされているか、またはインターネット経由でアクセス可能なアプリケーション、ネットワーク、サービスが増加していることから、マルウェアがホストマシンに到達できる攻撃経路は多様化しています。特に懸念されているのは、コンピュータにインストールされているアプリケーションの脆弱性を悪用し悪意のあるコードを実行するオンラインベースの攻撃がますます増えていることです。

最新の攻撃への対策に伴う困難は、この10年ほどに起きた以下のような脅威環境の大きな変化によって生じています。

マルウェアの急激な増加
悪意のあるプログラムの生成プロセスを自動化したマルウェア作成キットが初めて広く利用可能になった2000年代半ばから、アンチウイルスラボで見つかるマルウェアのサンプル数が爆発的に増加しました。毎月数十万個の新種や亜種が生み出され、増殖しています。数が圧倒的であるだけでありません。これらの亜種の多くは、莫大な数量でアンチウイルスプログラムを圧倒することを目的に、数日または数時間という短期間だけ生き残るよう設計されています。

オンラインに移行する攻撃
マルウェアが電子メールの添付ファイル経由で配布されるのが一般的だった時代は過ぎ去りました。今日、最も一般的な攻撃方法は、侵害された正当なサイトや、検索エンジンまたは侵害されたサイトからトラフィックをハイジャックする悪質サイトを訪問している間に、密かにダウンロードが行われる「ドライブバイダウンロード」です。マルウェア配布者や攻撃者は、標的とするコンピュータへの直接配信から広範なオンラインの世界に移動することで、ターゲットオーディエンスを増やしているだけでなく、感染の防止をますます難しくしています。攻撃サイトを特定し、ユーザがそのサイトを訪問することを防ぐメカニズムがなければ、攻撃が発生したという明白な兆候もなく、ユーザのコンピュータが食い物にされてしまいます。

マルウェアがサイバー犯罪ツールに変化
感染による影響も、組織犯罪者達がサイバー犯罪に手を染めるようになってから変化してきました。最近のデータ・個人情報の盗難、金融詐欺はすべてマルウェアが絡んでいる犯罪行為です。被害額が驚くべき額に昇ることもあります。たとえば、米国連邦捜査局（FBI）は、2012年上院公聴会[1]で、2011年のゴーストクリック作戦で壊滅させたクリックボット詐欺で、1400万ドルもの「不正利益」が上げられていたことを報告しています。ほとんどの関係当局には、サイバー犯罪者を摘発するリソースやサイバー犯罪を訴追する政治的意志が欠けています。そのため、サイバー犯罪者にとってオンライン上での活動を続け、さらにそれを改善していくための強力な金銭的インセンティブが存在します。

概要
本ホワイトペーパーでは、ホストベースの動作分析とエクスプロイトのインターセプトをコンピュータセキュリティの必須要素にしたコンピューティングの動向と進歩について説明します。さらに、エフセキュアのセキュリティ製品であるホスト型侵入防止システム（HIPS）「ディープガード」の技術と方法論の概要について説明します。

ディープガードは、悪意のある動作を効率的に発見して阻止するダイナミックでプロアクティブな動作分析技術を採用しています。2013年には、インストールされているプログラムの脆弱性を悪用する試みを検出しブロックすることでマルウェア感染を防ぐ、エクスプロイトインターセプトモジュールが導入されました。ディープガードは、ユーザエクスペリエンスへの影響を最小限に抑えた、軽量かつ包括的なエンドポイント保護を提供します。

主な特徴
- 新たな脅威から保護するために最新の検出技術を採用したアップデート可能なスキャンエンジン
- 遅延して実行される悪意のあるアクションから保護する継続的なアプリケーション監視
- エクスプロイトインターセプトモジュールが、ドキュメントベース攻撃を含むエクスプロイト攻撃を認識してブロック

利点
- シグネチャデータベースのアップデート前でも、既知および新しい脅威に対する即時のオンホスト保護を提供
- コンピュータにインストールされているプログラムに対するエクスプロイト攻撃を阻止
- 不審な活動を認識してブロック
- マルウェア感染による機密性の高いデータまたは個人情報の損失の可能性を低減

「マルウェアは新しいトリックと機能を取り入れながら常に進化しています。しかし変わらないことが1つあります。それは、マルウェアは常に悪意のある動作であるということです」。

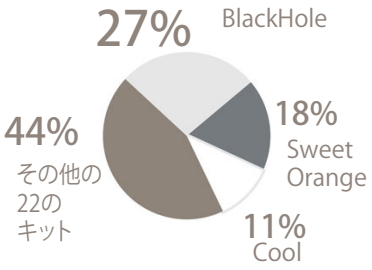
Mika Stahlberg
エフセキュアラボCTO

頻繁に標的にされる人気ソフト
ほぼすべてのソフトで脆弱性は見つかる可能性がありますが、サイバー犯罪者やその他の攻撃者が特に関心を持つのは、Javaランタイム環境（JRE）、Adobe Reader、Microsoft Office、ウェブブラウザなどの人気アプリケーションの脆弱性です。これらのプログラムにはユーザが数百万人いることから、主要ターゲットにされています。

これらのアプリケーションの多くには既知の脆弱性が複数存在しますが、ほとんどがベンダーからリリースされたセキュリティパッチで修正されます。しかし、修正プログラムを開発し、影響のあるすべてのコンピュータに展開するまでの間は、ユーザのコンピュータは脆弱なままです。さらに、まだパッチが公開されていない、新しい脆弱性やゼロデイ脆弱性が定期的に見つかっており、ユーザにつけ入るスキが生まれてしまいます。

エクスプロイトキットによって攻撃が容易に
BlackHole、Cool Exploit、Sweet Orangeなど、商用グレードのエクスプロイトキットの出現により、攻撃ウェブサイトを訪問してから数秒以内にユーザコンピュータのスキャンおよびエクスプロイトプロセスを自動化することが可能になりました。これにより、サイバー犯罪者が新たな被害者にマルウェアを感染させるために必要な技術的専門知識のレベルが大幅に下がっています。

表 1: 最も一般的なオンライン エクスプロイトキット、2013年第1四半期 [2]



エクスプロイトキットによって、脆弱性の悪用がニッチ的活動から一般的な攻撃へと変貌しました。エクスプロイト型の方法で配布されたマルウェアの数が増えたことをきっかけに、マルウェアがコンピュータに侵入する前にインストール済プログラムの脆弱性を悪用する試みをブロックできる、オンホストセキュリティソリューションが求められるようになりました。

標的型攻撃が検出を困難に
標的型攻撃には、不明確なエクスプロイトと配信のメカニズムが含まれる場合があります。これらの攻撃は通常、狙った被害者が興味を持つトピック、よく使用するオペレーティングシステム、使用しているセキュリティプログラムを考慮し、彼らのプロフィールに合わせて慎重に細工されたドキュメントまたは実行可能ファイルを使用します。このような攻撃が持つ極めて特有な性質により、従来のシグネチャベースの検出では検出は特に困難です。

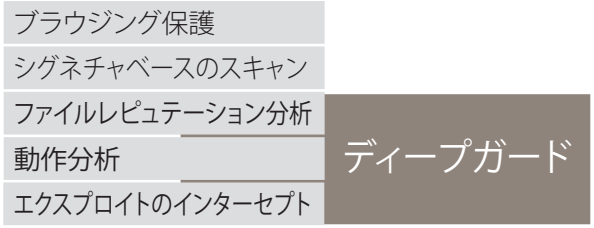
クリーンなプログラムを識別することがさらに重要に
グローバルに流通しているクリーンまたは悪意のないアプリケーションは何百万本にも及び、通常のユーザが一度に精通できる数をはるかに超えています。プログラム数の多さ、インターネットからの入手し易さ、プログラムのアップデートを常に把握しておく必要性を考えると、セキュリティソリューションがユーザ主導によるローカルのホワイトリストおよびブラックリストのみに頼ることだけでは適切な保護を提供できなくなっています。

一般的なコンピュータで使われているプログラムの大半はクリーンであるため、悪意のないソフトを正しく識別することが、本当に有害なプログラムを特定し、それに対処するための大きな一歩です。セキュリティプログラムのパフォーマンスを最適化し、さらに、ユーザエクスペリエンスへの影響を最小限に抑えるために、クリーンなファイルに対する誤検出を排除することも重要です。

今日のますます複雑になっているコンピューティング状況と、流動的な脅威環境がもたらすさまざまな問題を考えると、今や、従来のシグネチャベーススキャンは、エンドポイントセキュリティへの多層的なアプローチのわずか一層に過ぎません。クラウドベースファイルとWebレピュテーションチェック、HIPS（ホスト型侵入防止システム）、動作分析は、最新のプロアクティブ保護システムに不可欠な構成要素となっています。

2. 多層的な保護

エフセキュアのセキュリティに対する多層アプローチは以下のモジュールで構成されています。それぞれのモジュールが、その脅威環境特有の側面に対処し、総合的に完全なソリューションを提供するように設計されています。



前述したように、今や、ほとんどの攻撃やマルウェアのダウンロードはオンラインで発生しています。予想される感染ポイントへのエクスポージャを防ぎ、攻撃がマシン環境に到達する前に保護を開始することが理想的です。そこで、ブラウジング保護の出番です。

ブラウジング保護は、侵害された正当なサイトまたは完全に悪意のあるサイトを、ユーザが誤って訪問することを防ぐために、ウェブサイトのセキュリティについて批判的評価を提供します。悪意のあるサイトや、または不審な機能を含んでいるサイトで

あることが分かっていれば、ユーザはそのサイトに入らないよう警告されます。インターネット上にある数百万ものサイトと、変動し続けているセキュリティの変化に効率的に対処するため、ブラウジング保護機能は、既知の安全なファイルや悪意のあるファイルおよびウェブサイトのデータベースを備えたエフセキュアのセキュリティクラウド（4ページ参照）への照合クエリを活用しています。エントリは、レスポンスアナリストによって維持されるルールに基づいて、リアルタイムで自動アップデートされます。

ブラウザ保護は既知の悪質サイトへの訪問をほぼ防ぐことができますが、未評価のサイト、新しい侵害サイトや悪質サイトに遭遇する可能性や、マルウェアがリムーバブルメディアなどの他の方法でホストマシンに侵入する可能性は常に存在します。もし不審なファイルがコンピュータに到達した場合、複数の層から成るセキュリティチェックを通ることになります。

ファイルを受信、インストール、変更するたびに、コンピュータが従来のシグネチャ検出エンジンを使用してスキャンし、既知の脅威であるかどうかを判断します。スキャンエンジンは、カスタム、ファミリ、ジェネリック、ヒューリスティック検出を使用して、特定のマルウェア、類似機能を持つマルウェアファミリ、悪意のある物理的特徴や動作パターンを幅広く識別します。ファイルの特性が、以前に検出されたことのあるマルウェアに一致すればブロックされます。

より高度な技術に比べて看過されがちですが、シグネチャベーススキャンは現在までにわかっている大多数のマルウェアを識別してブロックできます。シグネチャベーススキャンは、DownadupやMelissaなど、かなり昔に発生してピークを過ぎているものの、ユーザ環境に残って新しい被害者に感染し続けている長引く脅威からユーザを保護できる効果的な方法です。このチェックの有効性は、最新の検出によりシグネチャデータベースを最新の状態に維持しているかに左右されます。

ファイルが既知の脅威として識別されなかった場合、エフセキュアのクラウドインフラストラクチャにクエリが送信され、そのファイルについて利用可能な最新のメタデータが収集されます。続いて、ディープガードによって分析が処理されます。ディープガードは動作分析をまとめて処理し、アプリケーションの起動時と実行中に不審なファイルの監視とエクスプロイトのインターセプトを行います。

3. ディープガードの詳細機能

簡単に言うと、ディープガードはアプリケーションの動作を観察し、悪影響を及ぼす可能性のあるアクションが完了することを防ぎます。このタスクは一見シンプルですが、実は非常に重要なものです。というのも、このプロアクティブなオンザフライ監視とインターセプトは、新しい脅威だけでなく、未知の脆弱性を狙った脅威に対しても最も重要な最終防衛線として機能するためです。

動作ベースの分析は、マルウェアを特定するためのシグネチャを作成するためにアナリストがマルウェアの実際のサンプルを入手しなければならないという、シグネチャベーススキャンの弱点をカバーします。絶えず作成・配布されているマルウェアの膨大な数を考えれば、アンチウイルスラボがサンプルを入手して分析し、検出を発行する前に、ユーザ環境において少なくとも1人が、新種の脅威に感染してしまいます。

動作ベースの検出は、新しいマルウェアが初めて出現したときから、その脅威に関する最初のシグネチャ検出が発行されるまでの重大な空白期間をカバーします。ディープガードは、独自の物理的特性から悪意のある動作パターンへと重点を移すことで、実際のサンプルを入手して検査する前であっても、有害なアクションを行うプログラムを識別してブロックすることができます。

ディープガードの歴史

2006
ヒューリスティック分析技術を導入
ディープガード1.0が既存のシグネチャベースの検出技術を補完するために動作分析を導入。プログラムが起動されると、ディープガードはマルウェアに共通する機能がないかを調べる静的チェックと、マルウェアの動作を評価するための仮想サンドボックス内でのプログラムのエミュレーションの、2つのテストを実行。既知のマルウェアと一致した機能または動作を示さないプログラムは、通常通り実行を許可。典型的なマルウェアの特性を持つ、または悪意のあるルーチンがあれば、実行をブロック。

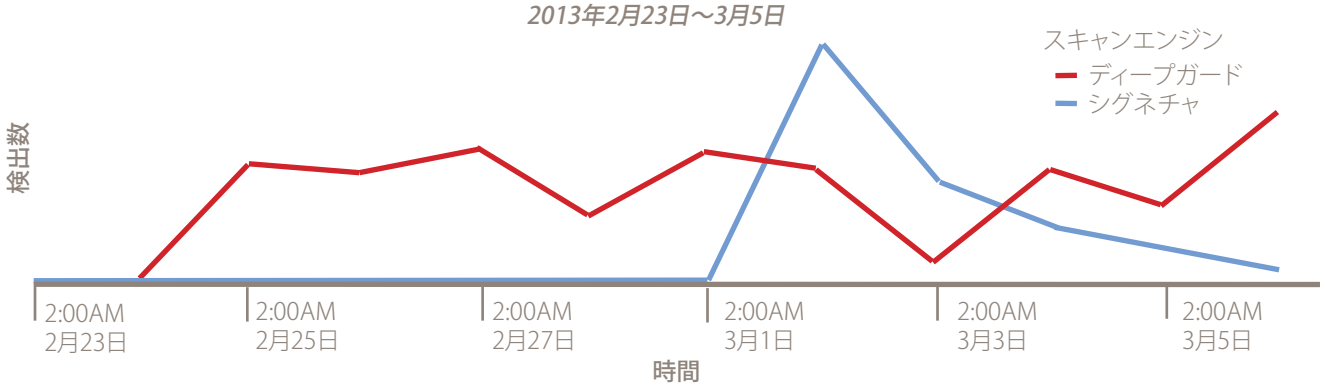
2008
クラウド参照を搭載した初めてのAV製品
ディープガード2.0は、シグネチャスキャンとエミュレーションに加え、セキュリティクラウドを照会して不審なファイルのレピュテーションをほぼ瞬時にチェック。レスポンスラボアナリストが、ファイルレピュテーション情報を常時監視・アップデートし、極めて重要な人間の知性を自動化されたプロセスに提供。

2010
ディープガード検出ロジックにファイルメタデータを使用
ディープガード3.0に、シグネチャ検出と動作分析レイヤーに加え、脅威の潜在性を測定するため、ファイルの新規性、発見日、関連オブジェクトなどファイルのメタデータを使用するコンポーネントを搭載。この機能により、マルウェアの機能または動作をさらに調査する必要なく、既知の悪質サイトからファイルがダウンロードされたかどうかなどのレピュテーションベースの要素を使用してマルウェアを特定可能に。

2011
普及率ロジックにより新規なファイルに対する効果が向上
ディープガード4.0は、スキャンエンジンを改良し、アップデート可能な検出機能とベータ検出を使用して誤検出を削減。また、新規なファイルと悪意のあるファイルの識別に使用される普及率ロジックも改善。AV-Comparativesの*2011プロダクト オブ ザ イヤー*に輝いたほか、AV-Testの*2012 Best Protection Award*[3]を受賞したことが、この機能の実力を証明。

2013
エクスプロイトベースの攻撃に対する保護を強化
一般的なアプリケーションの脆弱性を狙うエクスプロイトを利用したマルウェア感染が、頻繁に利用される攻撃方法になる。ディープガード5.0は、よく標的にされるプログラムと潜在的な攻撃ファイルの実行時動作を監視するモジュールを含む、強化された動作ベース検出ロジックを導入。この広範な動作分析アプローチにより、標的にされている脆弱性に関係なく、エクスプロイトベース攻撃を識別および阻止できます。

表 2: URAUSYランサムウェアの検出数
2013年2月23日～3月5日



たとえば、2013年4月に報告されたZeusクライムウェア感染攻撃のうち80%がそれまで見つかっていない亜種に関連しています。これらの事例において、ディープガードはファイルの悪意のある動作を認識し、攻撃をブロックすることで感染を阻止しました。その後、これらのサンプルを識別するためにシグネチャデータベースがアップデートされました。一方で新種の脅威に直面したユーザには、ディープガードのプロアクティブな分析が感染に対する即時の保護を提供します。

2011年には、完全に書き換えられたディープガードエンジンが導入されました。このエンジンでは、(多くの機能強化が実現されましたがその中でも特に)ハードコードスキャンロジックの使用からアップデート可能な検出データベースへの切り替えが行われました。レスポンスラボのアナリストは常に、脅威環境を監視し、悪意のある動作を識別する最善の方法を決定するために最新の脅威を分析しています。この研究結果に基づいてスキャンエンジンをアップデートできるため、新種の脅威に対するディープガードの効果は常に維持されます。

マルウェアの亜種のほとんどは短命であるという性質を考えると、シグネチャ検出の有効性は、検出されるマルウェアの期限が切れるまでの短期間となる傾向にあります。一方で、マルウェアの動作は変異しにくいため、ディープガード検出は、はるかに長い期間にわたってマルウェアを効果的に識別できます。たとえば、2012年7月12日、シグネチャデータベースに600の新検出が追加されましたが、ディープガードに新しく検出されたのは1つだけでした。9カ月後の2013年3月、同じデータベースを使用して、最新のマルウェアサンプルのランダムなコレクションに対してテストを実施した結果、シグネチャ検出の「過去の」セットよりも12倍多く、新しいマルウェアの感染をブロックすることが明らかになりました。

ディープガード検出機能のプロアクティブ性と寿命を表2(上記)に示しています。この表は、Urausyランサムウェア亜種のエフセキュア内部システムからの統計に基づいています。ディープガード検出機能は、亜種を早期に識別して感染攻撃をブロックし、その後もそれを継続できましたが、同等のシグネチャ検出はピークに達した後、新しいUrausy亜種が登場するにしたがって急速に低下しました(シグネチャ検出のピークの方が高い理由は、ディープガードよりも前の防御層であるためです。これらのシグネチャ検出がなければ、ディープガードのピークのほうが高くなったはずです)。

セキュリティクラウド

2008年から稼働しているセキュリティクラウド(旧リアルタイムプロテクションネットワーク)は、エフセキュアのクラウドネットワークです。このクラウドネットワークにはクライアントマシンにインストールされているエフセキュアのセキュリティ製品のパフォーマンスをサポートおよび強化する、さまざまなデータベースと自動分析システムを含まれています。このネットワークのインフラストラクチャは、世界中の複数のデータセンターに位置するサーバによってホスティングされています。

セキュリティクラウドに接続されたクライアント　コンピュータは、他の保護されたコンピュータによってユーザ環境内で見つかった脅威に関する最新情報を取得できるため、はるかに効率的かつ効果的なレスポンスを実現します。ファイルまたはURLなどの新しいオブジェクトが、あるクライアントで見つかった場合、当該製品は強力に暗号化されたオブジェクトレピュテーションサービスプロトコル(ORSP)を使用して、そのオブジェクトのレピュテーション詳細についてセキュリティクラウドに問い合わせます。ファイルサイズと匿名パスなどのオブジェクトに関する匿名のメタデータが、セキュリティクラウドに送信されます。これらのクエリは完全に匿名であり、IPアドレスは保存されないため、クライアントのプライバシーは守られます。

セキュリティクラウドの自動分析システム(1日あたり最高8百万回の決定を実行)は、送信されるメタデータを、社内データベースおよびその他のさまざまなソースから得られた情報と合わせて評価することで、ディープガードの事前セキュリティ評価ステージの間、オブジェクトについて十分な情報に基づいた最新のリスク評価を行うことができます。このため、セキュリティクラウドに接続されている他のコンピュータで検出済みの脅威を直ちにブロックできます。これによりクライアント上でオブジェクトの分析を実行する必要もなくなり、ユーザエクスペリエンスへの影響が低減されます。

セキュリティクラウドを使用することにより、レスポンスラボアナリストが極めて重要な人間の知性と判断を提供できることから、自動化システムとオンホストスキャン技術が補完されます。アナリストは、データベースと自動分析システムを支えるルールを作成、維持するだけでなく、脅威環境を積極的に監視し、マルウェアの特性と動作パターンを研究して、真に悪意のあるプログラムを見分ける最も効果的な方法を見つけます。脅威が確認されると(または既知のファイルのレピュテーションが変更されると)、アップデートされた情報は60秒でセキュリティクラウドに接続されているすべての製品の間でレプリケートされ、最新の保護が保証されます。

ディープガードのアップデート可能な検出ロジックは、インストール済みプログラムの脆弱性を悪用してコンピュータでマルウェアを実行する攻撃に対して特に便利です。このような場合、シグネチャベースまたは動作　ベースのスキャンによって侵入したマルウェア自体が発見およびブロックされます。しかし、さらに早い段階、つまり脆弱性につけ込まれた時点で攻撃を防止するため、レスポンスラボのアナリストは典型的なアクションや動作パターンがないかエクスプロイトメカニズムを調べて、その調査結果をディープガードのスキャンエンジンに組み込みます。スキャンエンジンは脆弱性を悪用しようとする特徴がある不審なアクションを特定してブロックすることで、コンピュータ上にマルウェアがドロップされることを完全に防止できます。

独特な悪用メカニズムと、システムにドロップされるマルウェアの機能と動作を考慮に入れることで、ディープガードはゼロデイ脆弱性を標的にした全く新種のマルウェアに直面したときにも、その場で脅威を効果的に識別してブロックできるのです。

4. ディープガードの仕組み

ディープガードの動作分析は、2つのイベントによってアクティブになります。初めてプログラムが起動するとき、ディープガードはそのプログラムを分析して、実行しても安全かどうか判断します。ディープガードは、プログラムの実行中も引き続き監視を継続します。

4.1 起動前分析

プログラムが初めて実行されるとき、その起動方法（ユーザがファイルのアイコンをクリックする、電子メールの添付ファイルまたはプログラムを起動する等）に関係なく、ディープガードはその実行を一時的に遅らせて以下のチェックを行います。

ファイルレピュテーションチェック
インターネット接続が利用可能な場合、ディープガードはセキュリティクラウド（4ページ）にクエリを送信して、プログラムのレピュテーションに関する最新情報がないかクリーンファイルデータベースをチェックします。このデータベースには、一般的に使用される膨大な数のアプリケーションに関する最新のセキュリティ評価が含まれており、レスポンスラボアナリストによって絶えず維持およびアップデートされています。データベース内でクリーンとして評価されているプログラムは他のチェックを受けずにすぐに起動できますが、既知の悪意のあるファイルはすぐブロックされます。

ユーザにとって、クリーンファイルクラウドルックアップ機能は多くの利点を提供しています。クリーンなファイルデータベースから既知のファイルに関するセキュリティ判定を使用できるため、ユーザは、未知の、または馴染みのないプログラムが正当なものか悪意のあるものかを見分ける必要がなくなります。また、クリーンなファイルに不要なセキュリティ　チェックを行うことも回避できます。同時に、個別に評価する必要があるソフトの数を管理しやすいレベルまで減らすことによって、選択したプログラムのホワイトリストまたはブラックリストに分ける能力がさらに意味のあるものになります。最後に、製品のシグネチャ　データベースが古いか、ほとんどアップデートされていなくても、ディープガードは最新のファイルレピュテーション情報を使用して分析を微調整できます。

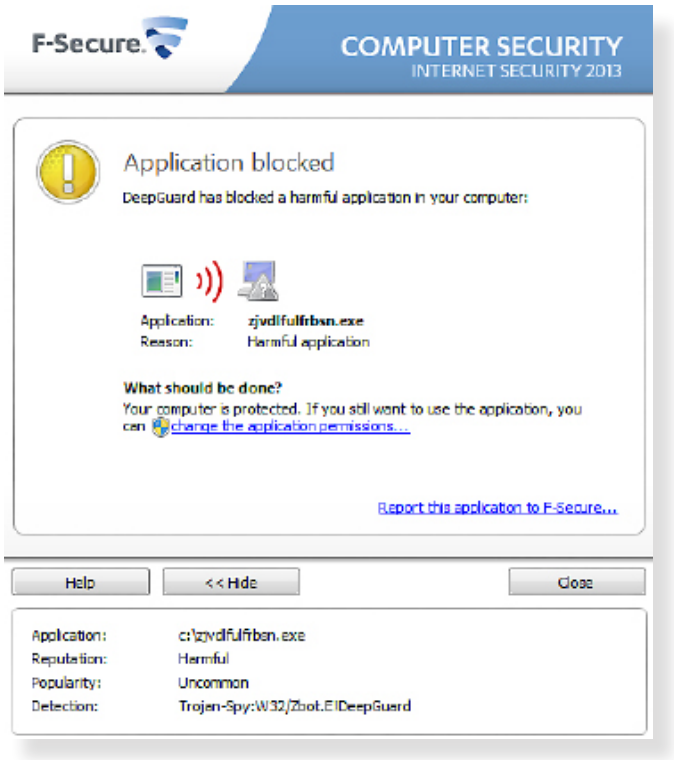


図1：有害なアプリケーションをブロックするディープガード

動作分析
ファイルレピュテーションチェックの間、不審なものとしてフラグが立てられた場合、またはインターネットアクセスが利用できない場合、ディープガードは仮想環境でそのプログラムを実行し、重要なシステムファイルを自己複製、編集、または削除しようとする試みなどの、悪質なアクションがないか動作を観察します。

レスポンスラボ　アナリストは、マルウェアを発見するために必要な最も効果的な動作パターンを確立するために、検出機能を使用してディープガードのスキャンロジックを継続的に調査およびアップデートします。これらの検出機能は、特定のマルウェアファミリ（一般的に同様の機能または動作を共有する）を識別するか、または悪意のある目的を暗示する、プロセスエミュレーション　プログラムから逃れる試みなど、不審なアクションをより全般的に識別できます。このようにしてアナリストはディープガードエンジンを微調整できるため、人による判断と柔軟性の要素が取り入れられることができ、分析がより詳細なものになり、最終的に精度が向上します。

普及率チェック
ディープガードにはファイルの普及率に焦点を当てたモジュールが含まれています。一般的に、クリーンなファイルには数千または数百万のユーザがおり、非常に広く普及しています。対照的に、マルウェアのサンプルは比較的希少です。既知の脅威を監視するエフセキュアの内部システムから生成された統計情報によると、2013年の最初の4カ月に見つかった悪意のあるプログラムのランダムサンプルにおいて、脅威の99.7%は当社のユーザベースにほとんど見られません。珍しいファイルまたは新しいファイルは、自動的に不審ファイルと判断され、その後のプロセス監視段階においてさらに詳細な検査を受けます。

実行時の判定
ディープガードは、エミュレーション中にファイルのレピュテーションおよび動作に基づいて、以下の4つのうち1つの判定を行います。

a) ファイルは悪意のあるものであり、ブロックされる
b) ユーザに起動を許可または拒否するオプションが与えられる
c) ファイルはクリーンであり、実行が許可される
d) ファイルのステータスがクリーンであるかまたは悪意があるかが不明

ファイルの起動がブロックされると、通知メッセージが表示されます（前ページの図1を参照）。メッセージには詳細と、必要に応じてプログラムをホワイトリストに入れるオプションが表示されます。

ファイルのステータスがまだ不明の場合、ディープガードは、そのファイルを実行することを許可しますがその後のプロセス監視ステージ中も監視を継続します。

4.2 アプリケーション実行中

プログラムが起動前の分析に合格して実行された後でも、動作を監視し続けます。これはマルウェアがランタイム チェックを回避する戦術としてよく使用される、実行を遅延する悪質なルーチンに対する予防措置です。ディープガードは、このようにして密かに警戒態勢を維持することで、過剰なプロンプトを表示してユーザエクスペリエンスを明白に邪魔することなく、常に保護を提供できます。

プロセス監視
アプリケーションは、以下を含む（がこれらに限定されない）、数多くのアクションを監視します。

- Windowsレジストリの変更
- 特定の重要なシステムディレクトリ内のファイルの編集
- 別のプロセス空間へのコードの注入
- プロセスを隠したり複製したりする試み

正当なプログラムも、このような操作を実行することがあるため、ディープガードは1回のアクションだけに基づいてプログラムにレッドフラッグを立てずに、不審な操作が複数回行われないか監視します。不審なアクションが重大なしきい値に達すると、ディープガードがそのプロセスの継続をブロックします。

セキュリティクラウドからファイルのレピュテーションや普及率評価情報があれば、それを考慮して、重大なしきい値が決定されます。たとえば、低普及率評価のファイルの場合、ディープガードは、ファイルがブロックされる前に実行される可能性のある不審なアクションの重大なしきい値を下げることによって、それを積極的に扱います。

5. エクスプロイトのインターセプト

2013年から、ディープガードは2つのエクスプロイトインターセプト手法を採用して、オンホスト動作分析の動的保護も拡張しています。その手法とは、よく標的とされるプログラムのプロセス監視に重点を置く方法と、エクスプロイトに一般的に使用されるドキュメントファイルの種類に特に重点を置く方法です。

5.1 悪用されやすいプログラムを監視

1つ目の方法はJavaランタイム環境（JRE）、Adobe Reader、Microsoft Officeなどの頻繁に利用されるプログラムに焦点を当てたものです。これらのプログラムは特に厳重に監視され、悪意のある動作が検出された場合はより積極的にブロックされます。

もちろん、頻繁に標的になるプログラムがいつも同じである可能性はあまりありません。たとえば、Adobe Readerに換わって、JREが悪用されたソフトのナンバーワンだったのはこの2年間に過ぎません。今後は、別のプログラムがこの迷惑な称号を受ける可能性があります。レスポンスラボアナリストは必要に応じて、ディープガードによって選択された特定のプログラムをアップデートできます。この応答性の高いアプローチを用いることで、ディープガードは脅威環境の変化に対応できるのです。

5.2 ドキュメントエクスプロイトの監視

Microsoft WordまたはAdobe PDFなどは、エクスプロイトによく使用される種類のドキュメントです。したがって、これらの種類のドキュメントを開くために使用されるソフトは、2つ目のエクスプロイトインターセプト手法によって注意深く監視されます。この方法では、悪意のあるドキュメントファイルによって不審な動作が生じていないか、それらのプログラムが詳細にわたりチェックされます。

このエクスプロイトインターセプト形式は、入念に細工されたエクスプロイト入りドキュメントを標的となる被害者または組織に送信するという、最もよくある標的型攻撃形式に対応します。その例としては、2011年のRSAの侵入事件、2013年初頭の「レッドオクトーバー」と呼ばれる事例があります[4]。これらの事例では、仕掛けが施されたExcelおよびWordファイルを使用して、プログラムの既知の脆弱性が悪用されました。

ドキュメントファイルに起因する悪意のあるアクションの検出に重点を置くことにより、ディープガードのこの方法だけで、ファイルの物理的特性や標的とされる特定の脆弱性に関係なく、ドキュメントベースの攻撃に対して幅広くカバーすることができます。

6. 誤検出防止

2011年にベータ検出モジュールがディープガードに追加されたことで、スキャンエンジンのパフォーマンスの精度に目立たないながらも重要な改良がなされました。

ベータ検出機能には、エクスプロイトの試みを識別してブロックするために必要な検出ロジックがすべて含まれていますが、分析されているファイルによって検出が起動される度に、セキュリティクラウドへの通知のみ行うよう、レスポンスアナリストにより設定されています。

このベータテストプロセスを使用することで、レスポンスアナリストは、現実世界に実際にリリースする前に、検出の有効性に関する重要な情報を入手してロジックを微調整し、潜在的な誤検出を防ぐことができます。

図2：Google Earth[7]で見るZeroAccessボットネットの地図

ZEROACCESS

2010年に初めて報告されたZeroAccessルートキットを使用することで、リモート攻撃者がユーザのコンピュータをハイジャックし、クリック詐欺とBitcoinマイニングを実行するボットネットにユーザを追加することができます。2012年現在、ZeroAccessはユーザ環境で最も頻繁に検出されているマルウェアの1つです[5]。

課題

ZeroAccessの伝播戦略は、基本的にボットネットオペレータが、地下フォーラムでリクルートした「アフィリエイトパートナー」[5]に配布をアウトソーシングするという驚くべきものです。アフィリエイトは、エクスプロイトキット経由、ファイル共有サービス上、スパム電子メールの添付ファイル形式、トロイの木馬ダウンローダのペイロードなど、複数の戦略をマルウェアの拡散に使用しています。配布方式の多様化により、ボットネットの地理的範囲を効果的に広げ（上記の図2参照）、ユーザがZeroAccessマルウェアとの遭遇を回避することが難しくなっただけでなく、配布に使用されるチャネルが多岐に渡るため、マルウェアの拡散を抑制する取り組みが複雑になりました。

また、ZeroAccess開発者は長年にわたってルートキットを積極的に変更して分析と検出を混乱させ、アンチエミュレーションとアンチデバッギング、暗号化などの機能を組み込んできました[6]。また、ボットネットオペレータと感染したコンピュータ間の通信をブロックできないように、高度なピア ツー ピア（P2P）コマンドと制御構造も導入されました。ZeroAccessの継続的な開発は否応なしに、マルウェアのエンジニアとアンチウイルス研究者の軍拡競争のようなものになっています。

ZeroAccessの防御を破る

ディープガードは、ファイルレピュテーションチェック、シグネチャスキャンなどセキュリティ製品の他のコンポーネントと連携して、ZeroAccessマルウェアが使用するさまざまな攻撃に対処します。ディープガードのエクスプロイトインターセプトモジュールは、エクスプロイトベースの侵入を検出して防止するため、コンピュータにZeroAccessをドロップする攻撃を阻止するうえで特に有効です。

ZeroAccessファイルが侵入してしまった場合（さらに初めて見つかった場合）、ディープガードの動作分析機能の出番です。マルウェアは技術的に洗練されているものの、どうしても無防備で脆弱性を伴う基本的な側面が1つあります。それは、マルウェアがコンピュータ上で実行する、悪質なアクションです。ディープガードは、ZeroAccessのルーチンに関する広範な研究結果に基づく検出ロジックを使用して、皮肉にも、マルウェアが自らを検出されないようとする試みを見分けることで、マルウェアを認識してブロックすることができます。

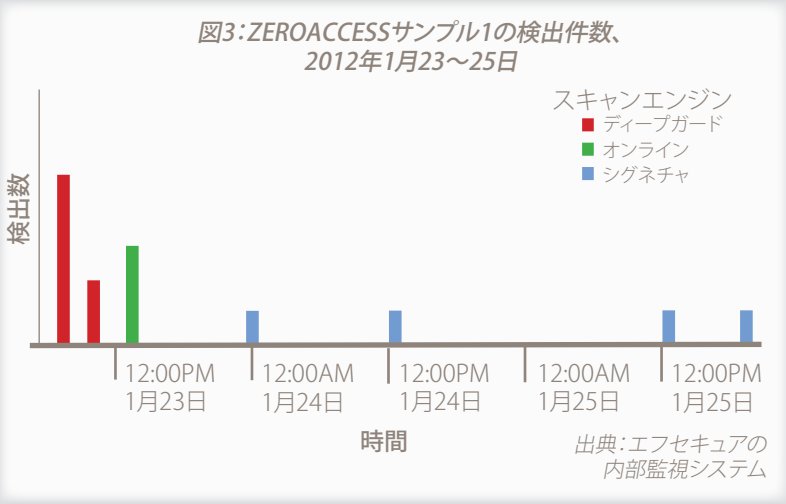


図3：ZEROACCESSサンプル1の検出件数、2012年1月23～25日

出典：エフセキュアの内部監視システム

セキュリティクラウドへの接続（4ページ参照）が利用可能な場合、ディープガードは、エフセキュアのクラウドベースインフラストラクチャ内にある各種データベースおよび自動分析システムに目に付くファイルの詳細を報告します。この情報は最終的に、特定の亜種を識別するシグネチャ検出の作成に使用されます。これ以降、その亜種はファイルレピュテーションチェックまたはシグネチャスキャンによって認識されるようになります。

ZeroAccess亜種のケースで、ディープガードのプロアクティブな保護が実際に機能している様子を確認することができます。2013年1月22日の深夜にユーザ環境で発生した亜種を、サンプル1と呼びます。図3（上記）は、亜種が最初に発生したコンピュータによって報告された検出統計情報ですが、これからわかるように、ディープガードは製品において感染の試みを認識してブロックした最初のスキャンエンジンでした。その後まもなく、この特定のサンプルに関連した詳細情報でセキュリティクラウドがアップデートされ、続いて感染の試みを数件ブロックしました。それから24時間以内に、シグネチャ検出のアップデートがリリースされ、エフセキュア セキュリティ製品がシグネチャスキャンエンジンを使用してサンプル1を識別およびブロックしました。

簡単に言えば、ディープガードは動作ベースのプロアクティブな分析を行い、それまで検出されたことのない脅威を認識してブロックしたのです。ディープガードが、悪意のあるファイルを識別するために必要な情報をエフセキュアのクラウドベースシステムに伝達すると、クラウドベースシステムは、保護された他のすべてのシステムに迅速に伝達し、それらシステムがまだ遭遇していなかった脅威に対する「免疫」を効果的に与えました。既知の脅威となったそのファイルは、それ以降シグネチャ検出によって識別されるため、ディープガードはそれ以上のセキュリティ チェックを行う必要なく、このファイルをブロックできるようになりました。

7. まとめ

エフセキュアのセキュリティ製品は、現実世界の脅威から生み出される問題に対処する複数のコンポーネントで構成された複数層のアプローチを使用しています。ディープガードによって実行される動作分析およびプロセス監視は、現在普及している最も高度なマルウェアを識別、ブロックする上で不可欠な機能です。

ディープガードは、特定の既知の脅威を静的に識別するのではなく、悪意のあるアプリケーションの動作に着目することで、新種の脅威に対して即時のプロアクティブなホスト保護を提供します。この着目点の変化によって、ディープガードはマルウェアの動作のみに基づいて未知のマルウェアでも識別およびブロックできるため、セキュリティ研究者が特定の脅威の検出を分析および発行できるようになるまでの間もしっかりと保護します。

また、ディープガードはエフセキュアのセキュリティクラウドに対するクラウドルックアップ機能を備えているため、それまでに遭遇したオブジェクトに利用できる最新のファイルレピュテーション情報を使用してセキュリティ評価を微調整することができます。これにより、誤検出のリスクだけでなく、ユーザエクスペリエンスに悪影響を及ぼす可能性のある冗長分析のリスクが減少します。

ディープガードのオンホスト動作分析は、人気の高いプログラムの脆弱性を悪用してコンピュータにマルウェアをインストールしようとする攻撃を阻止することもできます。ディープガードは、エクスプロイト攻撃の特徴的なルーチンを識別してブロックすることで悪用を阻止し、さらには感染を防止します。エクスプロイトのインターセプトは、コンピュータ上に脆弱なプログラムがある場合でさえ、ユーザを被害から守ることができます。

ディープガードは、高度なスキャンエンジン技術と、エフセキュアのレスポンスラボアナリストの技術的な専門知識を合わせて、正確で詳細なオンホスト動作ベースおよびレピュテーションベースの分析を実行し、最終的にユーザのセキュリティを大幅に向上します。

AV-Test Award受賞の決め手となったディープガード

ディープガードの動作分析とプロセス監視の有効性は、独立ベンチマーク測定機関であるAV-Testによって行われた製品テストで証明されました。このテストにおいてエフセキュアのインターネット　セキュリティ2013製品は、実際の多くのマルウェアサンプルとユーザシナリオを使用して検証されました。

非常に接戦となった中、ディープガードの動作ベースおよびレピュテーションベースの分析は、テスト対象の全製品のうち、最も多くのマルウェアを識別およびブロックすることでその重要性を証明しました。

エフセキュアのインターネット　セキュリティ2013は、製品パフォーマンスの結果から、「AV-TEST Best Production Award 2012」を受賞しました[3]。

8. 入手方法

ディープガードは、アンチウイルス、クライアント　セキュリティ、インターネット セキュリティ、プロテクション サービスビジネス（PSB）など、さまざまなエフセキュア　セキュリティ製品の重要なコンポーネントです。

これらの製品において、ディープガードはデフォルト設定で有効になっていますが、個別にオフにすることもできます。

参考文献

1. 連邦捜査局、Robert S. Mueller, III、*上院国土安全保障・政府問題委員会における証言*、ワシントン D.C.、2012年9月19日
   http://www.fbi.gov/news/testimony/homeland-threats-and-agency-responses
2. *エフセキュアブログ*、*Karmina Aquino*、*Exploit Kit Distribution in the Wild（ユーザ環境でのエクスプロイト キット配布）*、2013年3月12日
   http://www.f-secure.com/weblog/archives/00002522.html
3. AV-TEST、*AV-Test Award 2012*、2013年1月28日
   http://www.av-test.org/en/test-procedures/award/2012/
4. エフセキュアブログ、*Every Month is Red October（毎月がレッドオクトーバー）*、2013年1月15日
   http://www.f-secure.com/weblog/archives/00002486.html
5. エフセキュアラボ、*2012年下半期脅威レポート*、2013年2月5日
   http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2012.pdf
6. SophosLabs、イギリス、James Wyke、*ZeroAccessルートキット*
   http://nakedsecurity.sophos.com/zeroaccess4/
7. エフセキュアブログ、ショーン サリバン、*The United States of ZeroAccess（ZeroAccess合衆国）*、2012年9月20日
   http://www.f-secure.com/weblog/archives/00002430.html