KASPERSKY lab

カスペルスキー システムウォッチャーが新たな脅威を防ぐ

現在のコンピューターシステムは、マルチタスクがかつてないほど向上しています。膨大な数のプログラムを同時に実行することができますが、その目的やシステム内での権限はプログラムごとに異なります。

セキュリティ製品の目的は、他のファイルへの感染や、システムレジストリに対する不正な変更など、破壊的な機能を持つプログラムの活動をブロックすることです。こうしたプログラムを特定する「従来」の方法は、以前発見された悪質プログラム固有のコードシグネチャを検知することが基本になっていました。このプロセスはシグネチャベースの検知と呼ばれています。しかし、今やシグネチャベースの方法のみでは、マルウェアに対する効果的な保護が不可能になりました。Kaspersky Lab の内部データによると、1 日当り約 315,000 の新種のマルウェアサンプルが「実環境」で確認されており、その多くにシグネチャが存在しません。

こうしたプログラムへの効果的な対策として、システム内でのアプリケーションのふるまいを分析し、悪意あるソフトウェア特有の活動を検知するという方法があります。しかし、データがプログラムごとに収集されるため断片的な情報しか得られず、コンピューターシステム内で発生しているイベントのすべてを正確に把握することはできません。

成功のカギはシステムイベントの監視

セキュリティ製品の開発は、システムイベントの監視という新たな段階を迎えました。この技術は、システム全体についての情報を可能な限り提供することで、悪意ある活動を最大限抑制し、必要に応じてコンピューターの平常稼働時のパラメータを復元します。

システムイベント監視は、オペレーティングシステムのファイルや設定に対する変更、プログラムの実行、ネットワーク経由のデータ交換など、システム内で発生する重要なイベントをすべて追跡します。イベントは記録、分析され、悪質なソフトウェアであることを示す動作を実行した証拠があれば、その動作をブロックしてロールバックを行い、感染の拡大を防ぎます。

システムイベント監視は応用範囲が幅広く、システム内での破壊活動が疑われるすべてのソフトウェアに対して効果を発揮します。つまり、まだシグネチャが作成されていない新たな攻撃プログラムを、正確に検知することができるのです。

カスペルスキー システムウォッチャー：
さらに高いレベルの保護を実現

Kaspersky Lab のセキュリティ製品は、最先端の高度な技術で脅威に対処してきました。基本的なシステムイベント監視機能は、2009 年から個人向け製品に搭載されています。以来、この機能はさらなる進化を遂げ、カスペルスキー システムウォッチャーとなりました。

システムウォッチャーは、最も関連性の高いシステムイベントデータをスキャンします。追跡の対象となるのは、ファイルの作成や変更、システムサービスの動作、システムレジストリに対する変更、システムコール、ネットワーク上のデータ転送といった情報です。このほか、ファイルやディレクトリへの参照を含むシンボリックリンクの動作、インストールされたオペレーティングシステムのローダーが保存されているマスターブートレコードの変更、OS 再起動の妨害に関する情報も処理されます。

また、TCP（インターネットのトランスポート層の主要プロトコル）で送信されるパケットの中身を分析し、犯罪活動の証拠を探します。データ収集のプロセスは自動で実行されるため、ユーザーが操作する必要はありません。

システムウォッチャーは、Behavior Stream Signatures（BSS）モジュールを使用して、プログラムがマルウェアかどうかを分析結果から独自に判定することができます。さらに、Kaspersky Lab のセキュリティ製品には、BSS モジュールが他のコンポーネント（Web アンチウイルスモジュール、IM アンチウイルス、ホストベースの侵入防止システム、ファイアウォールなど）と継続的に情報を交換する仕組みがあります。これにより、マルウェアやセキュリティポリシー違反を検知する能力が全体的に向上し、こうしたインシデントにつながる一連のイベントを、さらに効果的に特定することができます。

システムウォッチャーは完全に更新することができ、イベントリストやイベント監視メカニズム、ヒューリスティック機能を必要に応じて調整できます。そのため、絶えず変化する脅威やコンピューターシステムの設定に、柔軟かつ迅速に対処することが可能になります。システムウォッチャーの更新は、アンチウイルスデータベースの定期アップデートの一部としてダウンロードされるため、ユーザーが時間を割いて何らかの操作を実行する必要はありません。

図 1：システムウォッチャーは［設定］メニューから設定できます。

脅威の検知

内蔵の BSS モジュールは、プログラムが悪質なものかどうかを判定します。このモジュールは、各プログラムの実際のふるまいと、典型的なマルウェアのふるまいを比較して、プログラムのふるまいを分析し、リアルタイムで判定を下します。また、Kaspersky Lab のセキュリティ製品にはヒューリスティック BSS ベース検知という機能もあり、必ずしもマルウェアのふるまいとは言えないものの、マルウェアに近い動作をするプログラムを検知することができます。システムウォッチャーは標準の検知機能を使用するだけでなく、悪質性が疑われる動作も特定できます。たとえば、エクスプロイト攻撃の結果、信頼できるアプリケーションが危険なコードを実行した場合、その動作を検知し、不審な活動をブロックするよう提案します。

この機能は、完全な自動モードか対話モードのいずれかを選択できます。対話モードでは、さまざまなアクションから選ぶことができます。

クリプトマルウェア対策サブシステム

ユーザーのデータを暗号化して復号鍵と引き替えに金銭を要求するクリプトマルウェアは、拡散が進んでおり、対策が急務となっていましたが、そのための技術がシステムウォッチャーに導入されました。この機能は、ユーザーのデータファイルが不審なプログラムによって開かれると、保護されたバックアップコピーをローカルに作成し、暗号化攻撃の影響を無効化します。バックアップコピーのデータを使用できるため、攻撃を受けたデータを復号化する必要はありません。

デスクトップロッカーからの保護

デスクトップロッカーもランサムウェアの一種で、閉じることができないとされるバナーを表示してコンピューター機能へのアクセスをブロックし、金銭を要求するプログラムです。システムウォッチャーはこの種のマルウェアを防ぐ機能を内蔵しています。システムウォッチャーの設定メニュー内の項目で、この機能を有効にすることや、デスクトップロッカーを手動で閉じるためのキーの組み合わせを設定することができます。このキーの組み合わせを押すことで、閉じることのできないバナーを排除し、原因のマルウェアを削除できます。この機能は既定で有効になっています。

ぜい弱性攻撃ブロックサブシステム

システムウォッチャーには、ぜい弱性攻撃ブロック（AEP）というモジュールもあります。これはソフトウェアのぜい弱性を狙うマルウェアに対処するモジュールで、ゼロデイぜい弱性にも対応します。さまざまなアプリケーションを制御でき、頻繁に狙われるアプリケーションには特に有効で、不審なコードが実行されると追加のチェックを開始します。このようにして収集された情報が、エクスプロイトの活動を検知してブロックするときに役立ちます。さらに、ぜい弱性攻撃ブロックは、アドレス空間配置のランダム化強制（Forced Address Space Layout Randomization）技術を使用します。これは、メモリ内にあるエクスプロイトの悪質コードの場所を、エクスプロイトに特定されにくくすることで、ぜい弱性の悪用を防ぐ技術です。この技術の詳細については、AEP のホワイトペーパーをご覧ください。

Java アプリケーションの制御モジュール

Java プラットフォームのぜい弱性からの保護は、すべての Java プログラムが実行される Java 仮想マシン（JVM）環境の普及率と不透明性から、常に重大なセキュリティ問題とされてきました。Java 経由の攻撃を検知するために、システムウォッチャーに搭載の Java2SW という特別なモジュールが、Java プラットフォームに直接アクセスし、各 JVM にさらなるセキュリティ要素を追加します。Java2SW は内部からコードを分析し、検知した不正な活動を停止させます。

システム内の不要な変更のロールバック

システムウォッチャーは感染を検知すると、ロールバック（コンピューターシステムを以前の安全なパラメータに戻す操作）を開始します。ロールバックシステムは、作成、変更された実行ファイル、MBR の変更、Windows の重要なファイルやレジストリキーに対応します。カスペルスキー製品の最新バージョンでは、ロールバックの機能を更新することができます。

搭載製品

システムウォッチャー技術は、個人向け製品と法人向け製品に搭載されています。

個人向け製品

- カスペルスキー インターネット セキュリティ
- カスペルスキー アンチウイルス

法人向け製品

- Kaspersky Endpoint Security for Business
- カスペルスキー スモール オフィス セキュリティ

結論

システムウォッチャーを使ったコンピューターシステムの監視と実行は、保護における新たなアプローチです。重要なシステムアクティビティがすべて監視され、監視データに基づいて悪意あるプログラムが検知されます。

このアプローチでは、コードのシグネチャが利用可能かどうかにかかわらず、あらゆるプログラムの破壊活動をブロックすることができます。破壊的なふるまいは、悪意あるプログラムを判定する上で最も確実な特性であることから、高い検知率を実現しつつ、誤検知を抑えることが可能になります。

また、コンピューターシステムに対する継続的かつ詳細な監視によって、マルウェアの活動を非常に正確にロールバックすることができます。さらに、コンピューター全体のセキュリティレベル評価も信頼性が高く、セキュリティの観点から異常と見られる状態やプロセスを、より正確に診断できます。