

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2017-509996

(P2017-509996A)

(43) 公表日 平成29年4月6日(2017.4.6)

(51) Int.Cl.

G06F 21/55 (2013.01)

F I

G06F 21/55 340

テーマコード (参考)

審査請求 未請求 予備審査請求 未請求 (全 21 頁)

(21) 出願番号 特願2016-558169 (P2016-558169)
 (86) (22) 出願日 平成27年3月3日 (2015.3.3)
 (85) 翻訳文提出日 平成28年9月19日 (2016.9.19)
 (86) 国際出願番号 PCT/US2015/018412
 (87) 国際公開番号 W02015/153037
 (87) 国際公開日 平成27年10月8日 (2015.10.8)
 (31) 優先権主張番号 14/231,409
 (32) 優先日 平成26年3月31日 (2014.3.31)
 (33) 優先権主張国 米国 (US)

(71) 出願人 501113353
 シマンテック コーポレーション
 Symantec Corporation
 アメリカ合衆国、カリフォルニア州 94
 043, マウンテン ビュー, エリス ス
 トリート 350
 (74) 代理人 100147485
 弁理士 杉村 憲司
 (74) 代理人 100134119
 弁理士 奥町 哲行
 (72) 発明者 ペレイラ・シェーン
 アメリカ合衆国 カリフォルニア州 91
 320 ニューベリーパーク ヴィアドロ
 ーレス 5306

最終頁に続く

(54) 【発明の名称】 疑わしいイベントのソースを識別するためのシステム及び方法

(57) 【要約】

疑わしいイベントのソースを識別するためのコンピュータによって実行される方法を記載する。一実施形態では、システムイベントはデータベースに登録することができる。第1のプロセスに関連する疑わしいイベントを検出でき、この第1のプロセスを、複数の潜在的なパペットプロセスのうちの1つであるとして識別することができる。データベース内の登録されたシステムイベントを、第2のプロセスを識別するために照合することができ、第2のプロセスは第1のプロセスを起動することとして検出される。

100

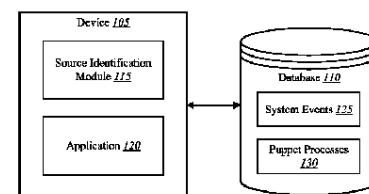


FIG. 1

【特許請求の範囲】

【請求項 1】

疑わしいイベントのソースを識別するためのコンピュータによって実行される方法であって、

データベースにシステムイベントを登録することと、

第 1 のプロセスに関連する疑わしいイベントを検出することと、

複数の潜在的なパペットプロセスのうちの 1 つであるとして前記第 1 のプロセスを識別することと、

前記第 1 のプロセスを起動することとして検出される第 2 のプロセスを識別するために前記データベース内の前記登録されたシステムイベントを照合することと、

を含む、方法。

10

【請求項 2】

前記疑わしいイベントの前記ソースとして前記第 2 のプロセスを識別する通知を生成することを更に含む、請求項 1 に記載の方法。

【請求項 3】

前記第 1 のプロセスを開始する際に前記第 2 のプロセスが終了することを判定することを更に含む、請求項 1 に記載の方法。

【請求項 4】

前記第 1 のプロセスを開始した前記第 2 のプロセスを識別する際、前記第 1 のプロセスをパペットプロセスとして識別することを更に含む、請求項 1 に記載の方法。

20

【請求項 5】

前記第 1 のプロセスが、前記第 2 のプロセスによってコマンドラインインタフェース上に直接供給される命令を介して開始されている、請求項 1 に記載の方法。

【請求項 6】

前記第 1 のプロセスが、少なくとも 1 つのファイルからの命令を介して開始されており、前記少なくとも 1 つのファイルへのパスは前記第 2 のプロセスによってコマンドラインインタフェース上に供給されている、請求項 1 に記載の方法。

【請求項 7】

潜在的なパペットプロセスのリストを維持することと、

検出されたプロセス起動イベントを含む、前記登録されたシステムイベントを介して新しいパペットプロセスを検出することと、

30

前記新しいパペットプロセスを前記潜在的なパペットプロセスのリストに追加することと、を更に含む、請求項 1 に記載の方法。

【請求項 8】

前記潜在的なパペットプロセスのリストが、コマンドラインインタフェースを有する少なくとも 1 つのプロセスを含む、請求項 7 に記載の方法。

【請求項 9】

前記潜在的なパペットプロセスのリストが、`cmd.exe`, `rundll.exe`, `rundll32.exe`, `regsvr32.exe`, `dllhost.exe`, `regedit.exe`, `taskhost.exe`, `cscript`, `wscript`, `vbscript`, `perlscript`, `bash`, `ldconfig`, `terminal.app`, 及び `x-code.app` のうち少なくとも 1 つを含む、請求項 8 に記載の方法。

40

【請求項 10】

前記システムイベントがカーネルモードドライバを介して登録されている、請求項 1 に記載の方法。

【請求項 11】

疑わしいイベントのソースを識別するように構成されたコンピューティングデバイスであって、

プロセッサと、

50

前記プロセッサと電子的に通信しているメモリと、
前記メモリに格納された命令であって、
データベースにシステムイベントを登録することと、
第1のプロセスに関連する疑わしいイベントを検出することと、
複数の潜在的なパペットプロセスのうちの1つであるとして前記第1のプロセスを識別することと、
前記第1のプロセスを起動することとして検出される第2のプロセスを識別するために
前記データベース内の前記登録されたシステムイベントを照合することと、
を前記プロセッサによって実行可能な命令と、を備える、コンピューティングデバイス

10

【請求項12】

前記命令が、
前記疑わしいイベントの前記ソースとして前記第2のプロセスを識別する通知を生成することを、前記プロセッサによって実行可能である、請求項11に記載のコンピューティングデバイス。

【請求項13】

前記命令が、
前記第1のプロセスを開始する際に前記第2のプロセスが終了することを判定することと、
を、前記プロセッサによって実行可能である、請求項11に記載のコンピューティングデバイス。

20

【請求項14】

前記命令が、
前記第1のプロセスを開始した前記第2のプロセスを識別する際、前記第1のプロセスをパペットプロセスとして識別することと、
を、前記プロセッサによって実行可能である、請求項11に記載のコンピューティングデバイス。

【請求項15】

前記第1のプロセスが、前記第2のプロセスによってコマンドラインインタフェース上に直接供給される命令を介して開始されている、請求項11に記載のコンピューティングデバイス。

【請求項16】

前記第1のプロセスが、少なくとも1つのファイルからの命令を介して開始されており、
前記少なくとも1つのファイルへのパスが前記第2のプロセスによってコマンドラインインタフェース上に供給されている、請求項11に記載のコンピューティングデバイス。

30

【請求項17】

前記命令が、
潜在的なパペットプロセスのリストを維持することと、
検出されたプロセス起動イベントを含む、前記登録されたシステムイベントを介して新しいパペットプロセスを検出することと、
前記新しいパペットプロセスを前記潜在的なパペットプロセスのリストに追加することと、
を前記プロセッサによって実行可能である、請求項11に記載のコンピューティングデバイス。

40

【請求項18】

前記潜在的なパペットプロセスのリストが、コマンドラインインタフェースを有する少なくとも1つのプロセスを含む、請求項17に記載のコンピューティングデバイス。

【請求項19】

プロセッサによって疑わしいイベントを識別するためのコンピュータプログラム製品であって、
前記コンピュータプログラム製品は命令を格納する非一時的コンピュータ可読媒体を備え、
前記命令が、
データベースにシステムイベントを登録することと、

50

第1のプロセスに関連する疑わしいイベントを検出することと、
複数の潜在的なパペットプロセスのうちの1つであるとして前記第1のプロセスを識別することと、
前記第1のプロセスを起動することとして検出される第2のプロセスを識別するために前記データベース内の前記登録されたシステムイベントを照合することと、
を前記プロセッサによって実行可能な命令と、を備える、コンピュータプログラム製品。

【請求項20】

前記命令が、

前記疑わしいイベントのソースとして前記第2のプロセスを識別する通知を生成することを前記プロセッサによって実行可能である、請求項19に記載のコンピュータプログラム製品。

10

【発明の詳細な説明】

【背景技術】

【0001】

コンピュータシステム及びコンピュータ関連技術の用途は急速に増大し続けている。コンピュータシステムの用途におけるこの増大は、コンピュータ関連技術に対する進歩に影響を与えてきた。実際に、コンピュータシステムは益々、実業界及び個人消費者の活動の重要な部分になってきている。コンピュータシステムは、種々の事業、産業、及び学術的努力を実施するのに使用されることがある。コンピュータの広範囲にわたる使用は、インターネットを含むコンピュータネットワークの使用が増大することによって促進されてきた。

20

【0002】

多くの企業は、ネットワークに接続された様々なコンピュータ間でデータを通信及び共有するために1つ又は2つ以上のコンピュータネットワークを使用している。従業員の生産性及び効率は、しばしば人とコンピュータとの相互作用を必要とする。コンピュータ技術のユーザは、この技術の効率が増大するのを要求し続けている。コンピュータ技術の効率を向上させることは、コンピュータを使用しそれに依存する誰にとっても常に望ましいことである。

【0003】

30

コンピュータ及びモバイルデバイスの広範な使用は、ルートキット、スパイウェア、トロイの木馬などの悪意あるプログラムの存在感の増大をもたらしている。マルウェアプログラムはマルウェア検出においてなされた改善を継続的に適応しており、これはマルウェア検出の改善に適応するマルウェア技法の継続的なサークルを作成する。

【発明の概要】

【課題を解決するための手段】

【0004】

少なくとも1つの実施形態によると、疑わしいイベントのソースを識別するコンピュータ実行方法が記載される。一実施形態では、システムイベントはデータベース内に登録され得る。いくつかの場合では、このシステムイベントはカーネルモードドライバを介して登録される。システムイベントは、コンピュータシステム内で発生する任意の検出可能なイベントを含むことができる。いくつかの場合では、システムイベントは、プロセス起動イベント、ファイルシステムイベントなどを含むことができる。第1のプロセスに関連する疑わしいイベントを検出でき、この第1のプロセスを、複数の潜在的なパペットプロセスのうちの1つであるとして識別することができる。データベース内の登録されたシステムイベントを、第2のプロセスを識別するために照合することができ、第2のプロセスは第1のプロセスを起動するものとして検出される。

40

【0005】

いくつかの実施形態では、通知を生成することができる。通知は、第2のプロセスを疑わしいイベントのソースとして識別することができ、及び／又は第2のプロセスは潜在的

50

な悪意あるプログラムであることを示すことができる。第1のプロセスを起動する際に第2のプロセスが終了することを判定することができる。第1のプロセスを起動する第2のプロセスを識別する際、第1のプロセスを、パペットプロセスとして識別することができる。

【0006】

一実施形態では、第1のプロセスを、第2のプロセスによってコマンドラインインタフェース上に直接供給される命令を介して起動することができる。加えて、又は代替的に、第1のプロセスを、少なくとも1つのファイルからの命令を介して開始することができる。この少なくとも1つのファイルへのパスは第2のプロセスによってコマンドラインインタフェース上に供給されている。潜在的なパペットプロセスのリストは、データベース内などに維持され得る。パペットプロセスは、別の独立したプロセスによって、一式の命令を実行するように構成され得る任意のプロセスとすることができる。新しいパペットプロセスを、登録されたシステムイベントを介して検出することができ、この新しいパペットプロセスを潜在的なパペットプロセスのリストに追加することができる。潜在的なパペットプロセスのリストが、コマンドラインインタフェースを有する少なくとも1つのプロセスを含むことができる。いくつかの場合では、潜在的なパペットプロセスのリストが、cmd.exe、rundll.exe、rundll32.exe、regsvr32.exe、dllhost.exe、regedit.exe、taskhost.exe、cscript、wscript、vbscript、perlscript、bash、ldconfig、terminal.app、及びx-code.appのうち少なくとも1つを含むことができる。

【0007】

疑わしいイベントのソースを識別するように構成されたコンピューティングデバイスについても記載される。このデバイスは、プロセッサと、このプロセッサと電子的に通信しているメモリとを備えることができる。メモリは、データベース内にシステムイベントを登録することと、第1のプロセスに関連する疑わしいイベントを検出することと、複数の潜在的なパペットプロセスのうちの1つであるとして第1のプロセスを識別することと、第1のプロセスを起動する第2のプロセスを識別するためデータベース内に登録されたシステムイベントを照合することと、をプロセッサによって実行可能な命令を格納することができる。

【0008】

疑わしいイベントのソースを識別するためのコンピュータプログラム製品についても記載される。コンピュータプログラム製品は、命令を格納する非一時的コンピュータ可読媒体を備えることができる。命令は、データベース内にシステムイベントを登録することと、第1のプロセスに関連する疑わしいイベントを検出することと、複数の潜在的なパペットプロセスのうちの1つであるとして第1のプロセスを識別することと、第1のプロセスを起動する第2のプロセスを識別するためにデータベース内に登録されたシステムイベントを照合することと、をプロセッサによって実行可能とすることができる。

【0009】

本明細書に記載される一般原理に従い、上記の実施形態のうち任意による特徴を互いに組み合わせて使用することができる。これら及び他の実施形態、特徴、及び利点は、添付の図面及び特許請求の範囲と併せて以下の発明を実施するための形態を読むことによって更に十分に理解されるだろう。

【図面の簡単な説明】

【0010】

添付の図面は、多数の例示的な実施形態を示すものであり、本明細書の一部である。以下の説明と併せて、これらの図面は、本開示の様々な原理を実証及び説明する。

【図1】本発明のシステム及び方法が実装され得る環境の一実施形態を示すブロック図である。

【図2】本発明のシステム及び方法が実装され得る環境の別の実施形態を示すブロック図

10

20

30

40

50

である。

【図3】ソース識別モジュールの一例を示すブロック図である。

【図4】疑わしいイベントのソースを識別するための方法の一実施形態を示すフローチャートである。

【図5】潜在的なパペットプロセスのリストを維持するための方法の一実施形態を示すフローチャートである。

【図6】疑わしいイベントのソースを識別するための方法の一実施形態を示すフローチャートである。

【図7】本発明のシステム及び方法を実装するのに好適なコンピュータシステムを示すブロック図を示す。

10

【0011】

本明細書に記載する実施形態は、様々な修正及び代替的な形態が可能であり、特定の実施形態を例として図面に示しており、本明細書において詳細に記載する。しかしながら、本明細書に記載する例示的な実施形態は、開示される特定の形態に限定されないものとする。むしろ、本開示は、添付の特許請求の範囲内に含まれる全ての修正、等価物、及び代替物を包含するものである。

【発明を実施するための形態】

【0012】

本明細書に記載のシステム及び方法は疑わしいイベントのソースを識別することに関する。より具体的には、本明細書に記載のシステム及び方法は、疑わしいイベントをもたらし潜在的に悪意ある命令を実行するパペットプロセスを検出し、この潜在的に悪意ある命令のソースを識別することに関する。

20

【0013】

悪意あるソフトウェアの作成者は絶えず、マルウェア検出システムに適合するようにその技法を進化させている。現在のファイルベースのマルウェア検出システムは、ポリモーフィックマルウェアなどの適合可能なマルウェアの検出に関して言えば立ち遅れていることが多い。したがって、マルウェア検出システムは、検出回避、ポリモーフィックマルウェアを識別するために行動学習エンジンを採用することができる。かかる行動エンジンは、純粋に新規の分類されないマルウェアがどのように行動するかに基づいてこのマルウェアを検出することができる。1つ又は2つ以上の行動を観察すると、本明細書に記載するシステム及び方法は、疑わしいイベントをこの疑わしいイベントの最終的な原因であるルートプロセス（例えば、悪意あるプロセス、悪意ある実行ファイルなど）と結びつけることができる。例えば、行動エンジンがRun又はRun Onceレジストリキーに書き込みもうとするのを見ることになっている場合、この行動エンジンはどのプロセスが書き込みコマンドの最終的な原因となるかを確かめることができ、それによって原因となるプロセスを中止する、かつ／又はこのプロセスに関連するファイルを削除するなど、このプロセスに対して措置を講じることができる。

30

【0014】

いくつかの場合では、現在のシステムがマルウェアのイベントを検出するまでに、このマルウェアのイベントのルートプロセスが、マルウェアのイベントへの関与を隠すため、それ自体を中止してしまう。マルウェアの作者は、悪意ある攻撃を実行するようにWindowsの署名されたプロセスを採用することがあるのは、マルウェアの作成者が典型的な行動エンジンが正規のWindowsプロセスに対していかなる救済措置も講じないように構成されていることを理解しているからであり、そうすることによりマシンの不安定にする、かつ／又は重大な機能性を破壊することができるからである。このように、いくつかの場合では、マルウェアの作者は、悪意ある攻撃を実行するために「パペット」プロセスを使用することがある。パペットプロセスは、代理で1つ又は2つ以上の措置を達成するため一次プロセスによって用いられる任意の二次プロセスとすることができる。このプロセスは動作時、いかなる挙動も呈さず、単に終了する。二次プロセスはコマンドラインなどを介して言われることをするので、「パペット」という用語が使われる。例えば

40

50

、マルウェアの作者は、悪意あるプロセス、`cmd.exe`若しくは`rundll32.exe`などのWindowsプロセスを採用するように構成される一次プロセス、二次又はパペットプロセスを作成することができる。いくつかの場合では、この悪意あるプロセスは、コマンドラインインタフェースを有するプロセスを活用することがある。悪意あるプロセスは、1つ又は2つ以上のコマンドライン命令として直接コマンドライン上に悪意ある命令を付与することができる。加えて、又は代替的に、悪意あるプロセスは、コマンドライン上にファイルへのパスが述べられるファイルの中に悪意ある命令を付与することができる。このように、悪意あるプロセスは、この悪意あるプロセスに代わって1つ又は2つ以上の悪意ある命令を実行するようにWindowsプロセスを構成することができる。いったん悪意あるプロセスが悪意ある命令を実行するように二次プロセスを構成すると、二次プロセスを終了させ、そのみが見えるようにすることによってその追跡を隠そうとすることができる。いったん悪意あるプロセスが悪意ある命令を有する二次プロセスを構成すると、悪意あるプロセスは終了し、悪意あるプロセスを終了させたまま、かつ一見どこにも見えないようにしたまま、二次プロセスにこの命令を実行させたままにする。したがって、いくつかの実施形態では、第1のプロセスが第2のプロセスを構成することを判定し、更に二次プロセスから疑わしいイベントを検出すると、この疑わしいイベント及び起動プロセスが悪意あるものであることを示すことができる。いくつかの場合では、第2のプロセスはコマンドラインインタフェースを含むことを判定すると、この疑わしいイベント及び起動プロセスが悪意あるものであることを示すことができる。加えて、又は代替的に、パペットプロセスを起動すると起動プロセスが終了することを判定すると、疑わしいイベント及び起動プロセスが悪意あるものであることを示すことができる。

10

20

【0015】

一実施形態では、本明細書に記載のシステム及び方法は、潜在的なパペットプロセスのリストを（例えば、`exe`名、画像名、プロセス名、プロセス特性、アプリケーションの記述などによって）保管及び維持することができる。このリストは、過去にパペットプロセスとして使用されてきたことが知られたプロセス及び／又はパペットプロセスとして使用可能であることが知られたプロセスを含むことができる。既知のwindowsのパペットプロセスのリストが、1つ又は2つ以上のコマンドラインインタフェースを含むことができる。例えば、リストは、`rundll32.exe`、`regsvr32.exe`、`cscript`、`wscript`、`dllhost.exe`、`taskhost.exe`、`cmd.exe`、`terminal.app`、`x-code.app`、`bash`などを含むことができる。

30

【0016】

一実施例では、パペットプロセスはコマンドライン上に直の悪意ある命令を受信することができる。システム及び方法は、カーネルモードドライバを用いてかかるプロセスが起動するのを追跡することができ、またかかるパペットプロセスの起動の際、パペットプロセスを起動した識別されたプロセスは、パペットプロセスから生じる任意の疑わしいイベントとして識別され、その原因とされ得る。いくつかの場合では、パペットプロセスは、間接的に、コマンドライン上に付与されたファイル（例えば、`.BAT`ファイル、`.CMD`ファイル、`.BTM`ファイル、`.MSC`ファイル、`.JOB`ファイル、`.IDL`ファイル、`.TLB`ファイル、`.EXE`ファイル、`.DLL`ファイル、`.APP`ファイルなど）へのパスを介して命令を受信することができる。このファイルは、更なる命令（例えば、`rundll32.exe`）及び／又は、パペットプロセスとして使用されている`regedit.exe`の場合における`REG`ファイルなどの特別のフォーマットの命令ファイルを含むことがある。いくつかの場合では、パペットプロセスは、命令が検索され得るCOMダイナミックリンクライブラリ（`DLL`）へのパスを配置するために、レジストリ内においてコンポーネントオブジェクトモデル（`COM`）オブジェクトグローバル意識別子（`GUID`）を検索するように命令され得る。かかる悪意あるファイル及び／又は悪意ある命令は、原因となる悪意あるプロセスがそのパッケージをドロップし、パッケージが実行されているまでに既に「デッド（死んでいる）」（すなわち、終了している）

40

50

ので「デッドドロップ」ファイル、及び／又は「デッドドロップ」命令と呼ばれることがある。マルウェアは、デッドドロップファイルを作成し、オペレーティングシステムにパペットプロセスを起動するように命令して、何を実行すべきかについての命令に対するソースとしてそのデッドドロップファイルを使用することができる。したがって、本明細書に記載のシステム及び方法は、デッドドロップファイルを作成したプロセスまでデッドドロップファイルの作成を追跡するためカーネルモードドライバを採用することができる。いくつかの場合では、システム及び方法は全てのプロセス起動を監視することができる。パペットプロセスが起動するのを識別する際、直接的／間接的にこのデッドドロップファイルを受信するコマンドラインを介して、システム及び方法は、デッドドロップファイルの最終的な原因となるプロセス（例えば、悪意あるプロセス、悪意ある実行ファイルなど）を識別し、それに応じて救済措置を講じることができる。

10

【0017】

図1は、本発明のシステム及び方法が実装され得る環境100の一実施形態を示すブロック図である。いくつかの実施形態では、本明細書に記載のシステム及び方法は、単一のデバイス（例えば、デバイス105）上で実行することができる。例えば、ソース識別モジュール115はデバイス105上に配置され得る。デバイス105の例としては、モバイルデバイス、スマートフォン、パーソナルコンピューティングデバイス、コンピュータ、サーバなどが挙げられる。

【0018】

いくつかの構成では、デバイス105は、ソース識別モジュール115及びアプリケーション120を備えることができる。アプリケーション120により、デバイス105がソース識別モジュール115とインタフェースされるようになる。一実施例では、デバイス105はデータベース110と連結され得る。一実施形態では、データベース110はデバイス105の内部にあってもよい。別の実施形態では、データベース110はデバイス105の外部にあってもよい。いくつかの構成では、データベース110は、システムイベント125とパペットプロセス130とを備えることができる。システムイベント125は、プロセス起動イベント、ファイルシステムイベントなどを含むことができる。いくつかの場合では、パペットプロセス130は、1つ又は2つ以上の潜在的なパペットプロセスのリストを含むことができる。このリストは、パペットプロセスとして使用されてきたことが知られたプロセス及び／又はパペットプロセスとして使用されそうなプロセスを含むことができる。例えば、あるプロセスは、該プロセスの1つ又は2つ以上の特性のため、パペットプロセスとして使用されそうであると考えられ得る。例えば、いくつかの場合では、コマンドラインインタフェースを含むプロセスは、それがないよりも、パペットプロセスとして使用されることが多い。

20

30

【0019】

ソース識別モジュール115は、疑わしいイベントを検出し、特定のプロセスが潜在的なパペットプロセス（例えば、パペットプロセス130）のリストにあるかどうかを判定し、格納されたシステムイベント125を照合し、及び／又は検出された疑わしいイベントに関する通知を生成することにより、疑わしいイベントのソースを識別することができる。以下に、ソース識別モジュール115に関する更なる詳細を説明する。

40

【0020】

図2は、本発明のシステム及び方法が実装され得る環境200の別の実施形態を示すブロック図である。いくつかの実施形態では、デバイス105-aは、ネットワーク205を介してサーバ210と通信でき、及び／又はデータベース110-aにアクセスすることができる。データベース110-aは、図1にあるデータベース110の一例とすることができる。ネットワーク205の例としては、クラウドネットワーク、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）、仮想プライベートネットワーク（VPN）、無線ネットワーク（例えば、802.11を用いる）、セルラネットワーク（例えば、3G及び／又はLTEを用いる）などが挙げられる。いくつかの場合では、ネットワーク205はインターネットを含む。

50

【0021】

いくつかの構成では、デバイス105-aは、図1に示すデバイス105の一例とすることができる。図示するように、デバイス105-aは、ソース識別モジュール115を含まなくてもよい。例えば、デバイス105-aは、デバイス105-aがサーバ210に配置されるソース識別モジュール115とインタフェースできるようにするアプリケーション120を含むことができる。したがって、デバイス105-aは、アプリケーション120、ネットワーク205及びサーバ210を介して、スキャン検出モジュール115の1つ又は2つ以上の機能を実行するように構成され得る。いくつかの実施形態では、デバイス105-aもサーバ210も両方とも、ソース識別モジュール115の機能のうち少なくとも一部がデバイス105-a及びサーバ210において独立してかつ／又は同時に実行されるソース識別モジュール115を含むことができる。

10

【0022】

いくつかの実施形態では、サーバ210は、ソース識別モジュール115を含むことができ、データベース110-aと連結され得る。例えば、ソース識別モジュール115は、データベース110-a内のシステムイベント125及び／又はパペットプロセス130にネットワーク205及びサーバ210を介してアクセスすることができる。データベース110-aはサーバ210の内部にあっても、外部にあってもよい。

【0023】

いくつかの構成では、アプリケーション120により、デバイス105-aがソース識別モジュール115とインタフェースすることができ、プレフィルタウェブページを検索することにより潜在的なスキャンキャンペーンを識別して、このプレフィルタウェブページの中からパターンを検出して、更に潜在的なスキャンをリアルタイムでユーザに通知するためユーザの入力を検出されたパターンと比較することができる。このように、アプリケーション120は、ソース識別モジュール115を介して、潜在的なスキャンキャンペーンを識別し、ユーザにこの潜在的なスキャンキャンペーンを警告することができる。

20

【0024】

図3は、ソース識別モジュール115-aの一例を示すブロック図である。ソース識別モジュール115-aは、図1及び／又は図2に示すソース識別モジュール115の一例であってもよい。図示するように、ソース識別モジュール115-aは、監視モジュール305と、比較モジュール310と、識別モジュール315と、分類モジュール320と、通知モジュール325と、を備えることができる。

30

【0025】

上述したように、悪意あるプロセスは、本来は悪意のない正規のプロセスを標的とすることができる。この悪意あるプロセスに代わって1つ又は2つ以上の行動を実行することができる。いくつかの場合では、悪意あるプロセスは、cmd.exeなどの信頼されたプロセスを標的とし、この信頼されたプロセスをそれに代わって悪意あるタスクを実行するように構成することができる。悪意あるプロセスは、検出を回避すべく悪意あるタスクを実行するように標的となるプロセスを構成することができ、この標的となるプロセスを構成した後、悪意あるプロセスがそれ自体を終了又は中止することを可能にする。このように、悪意あるプロセスは、悪意ある命令を実行中に悪意あるプロセスが行うどんな関与行為も隠そうとして、悪意あるプロセスが従来のマルウェア検出システムの下で検出されないようにすることができる。したがって、悪意あるプロセスは、標的となるプロセスから生じる任意の悪意あるイベントの最終的な原因となる起動プロセス又はソースプロセスと呼ばれることがある。標的となるプロセスは、最終的に全ての文字列を引く悪意あるプロセスであるので、パペットプロセスと呼ばれることがある。このように、起動プロセスが検出されなくなるのを防止するため、ソース識別モジュール115-aは、本明細書に記載のシステム及び方法に応じて疑わしいイベントのソースを識別するように構成され得る。

40

【0026】

一実施形態では、監視モジュール305はデータベース内にシステムイベントを登録す

50

ることができる。いくつかの場合では、このシステムイベントはカーネルモードドライバを介して登録される。監視モジュール305は、第1のプロセスに関連する疑わしいイベントを検出するように構成され得る。比較モジュール310は、第1のプロセス（例えば、乗っ取られたプロセス）が潜在的なパペットプロセスのリストの中からの1つであるかどうかを判定することができる。例えば、パペットプロセスとして使用されてきたことが知られるプロセスのリスト及び／又はパペットプロセスとして使用されそうなプロセスのリストは、第1のプロセスがこのリスト上のプロセスに関連するかどうかを判定するために参照され得る。加えて、又は代替的に、あるプロセスは、そのプロセスの1つ又は2つ以上の特性に基づいて潜在的なパペットプロセスのリストに含まれることがある。いくつかの場合では、潜在的なパペットプロセスのリストはコマンドラインインタフェースを有する少なくとも1つのプロセスを含む。例えば、コマンドラインインタフェースを特徴とするプロセスは、コマンドラインインタフェースを特徴としていないプロセスよりも、パペットプロセスとして悪意ある実体（entity）によって使用される可能性が高いと考えられ得る。したがって、コマンドラインインタフェースを特徴とするプロセスは、潜在的なパペットプロセスのリストに含まれ得る。加えて、又は代替的に、潜在的なパペットプロセスのリストが、以下のcmd.exe、rundll.exe、rundll32.exe、regsvr32.exe、dllhost.exe、regedit.exe、taskhost.exe、cscript、wscript、vbscript、perlscript、bash、ldconfig、terminal.app、及びxcode.appのうち少なくとも1つを含むことができる。

10

20

【0027】

一実施形態では、分類モジュール325は、潜在的なパペットプロセスのリストを維持することができる。分類モジュール325は、登録されたシステムイベントと関連した新しいパペットプロセスを検出することができる。例えば、ソース識別モジュール115-aによって実行されるアナリシスに基づいて（登録されたシステムイベントの少なくとも一部に基づいてもよく）、プロセスXがパペットプロセスであることが判定され得る。しかし、分類モジュール325は、プロセスXは潜在的なパペットプロセスのリスト上に載っていないことを判定することができる。したがって、プロセスXが潜在的なパペットのリストに含まれないことを判定する際、分類モジュール325はプロセスXを潜在的なパペットプロセスのリストに追加することができる。したがって、分類モジュール325は、第2のプロセスが第1のプロセスを起動し、その第2のプロセスが疑わしいイベントを引き起こす特定の操作を実行するように第1のプロセスを構成することを判定することにより、新しいパペットプロセスを識別することができ、それにより疑わしいイベントの周囲における精密な調査を増強することができる。このように、第2のプロセスが疑わしいイベントを引き起こす第1のプロセスを生成し起動したことを判定するとともに、第2のプロセスを実際に疑わしいイベントの原因となるプロセスとして識別する際、この第1のプロセスを、新しいパペットプロセスとして指定し、潜在的なパペットプロセスのデータベース内に潜在的なパペットプロセスとして追加することができる。

30

【0028】

悪意あるプロセスは、標的となるプロセスの特定の特性により、特有のプロセスを標的とすることができる。例えば、標的となるプロセスは、悪意あるプロセスが中止し又は更にはそれ自体を削除した後でも、悪意あるプロセスに効率的に標的となるプロセスを遠隔制御することが可能となるコマンドラインインタフェースを含むことができる。このように、標的となるプロセスはパペットプロセスと呼ばれることがある。プロセスを起動した起動プロセスを識別する際、識別モジュール315は標的となるプロセスをパペットプロセスとして指定することができる。いくつかの場合では、監視モジュール305は起動プロセスがプロセスを起動する際に終了することを判定することができる。いくつかの場合では、パペットプロセスを開始する際に起動プロセスが終了することを判定することが、疑わしいイベント及び起動プロセスが悪意あるものである可能性の更なる表示かつ増加を付与することができる。

40

50

【0029】

いくつかの場合では、監視モジュール305は、パペットプロセスが起動プロセスによってコマンドラインインタフェース上に直接供給された命令を介して開始されることを判定することができる。加えて、又は代替的に、監視モジュール305は、パペットプロセスがファイルに含まれる命令を介して開始されることを判定することができる。例えば、監視モジュール305は、起動プロセスがパペットプロセスのコマンドラインインタフェース上の1つ又は2つ以上のファイルへのパスを供給する原因となることを判定することができる。したがって、コマンドラインインタフェース上に付与された命令を実行することにより生じる疑わしいイベントを検出する際、識別モジュール315は、疑わしいイベントの最終的な原因となるプロセスとして起動プロセスを識別することができる。

10

【0030】

パペットプロセスを開始するプロセスは、起動プロセス又はソースプロセスとして指定され得る。疑わしいイベントを生成したプロセスが潜在的なパペットプロセスであることを判定する際、識別モジュール315は、パペットプロセスを開始する起動プロセスを識別することができる。いくつかの実施形態では、識別モジュール315は、データベースに格納された登録されたシステムイベント（例えばシステムイベント125）を照合することにより起動プロセスを識別することができる。システムイベントは、プロセス起動イベント、ファイルシステムイベントなどを含むことができる。したがって、データベースに登録されたシステムイベントは、パペットプロセスが特有のプロセスによって起動されることを示すことができる。識別モジュール315は、この識別された特有のプロセスを起動プロセスとして指定することができる。いくつかの実施形態では、このシステムイベントは、起動プロセスがパペットプロセスを開始した後終了することを示すことができる。したがって、起動プロセス及び／又はパペットプロセスの行動、態様、又は特性に関して取得された情報は、疑わしいイベントのソースに関する指示を付与することができる。一実施形態では、通知モジュール320は、疑わしいイベントを検出する、及び／又は起動プロセスを識別する際、通知を生成することができる。この通知は、この起動プロセスを疑わしいイベントのソースとして識別することができる。したがって、上述したように、ソース識別モジュール115は、デッドドロップファイルを作成するプロセスまでこのデッドドロップファイルの作成を追跡するためファイルシステムドライバを使用することができる。ソース識別モジュール115は全てのプロセス起動を監視することができる。したがって、ソース識別モジュール115が、1つ又は2つ以上のファイル（例えば、デッドドロップファイル）を直接的／間接的に指示するコマンドライン命令を介してプロセス起動（例えば、パペットプロセス起動）を検出するとき、ソース識別モジュール115はこの1つ又は2つ以上のファイルの作成者をパペットプロセスがする何かに対し原因となるプロセスとして保持する。

20

30

【0031】

図4は、疑わしいイベントのソースを識別するための方法400の一実施形態を示すフローチャートである。いくつかの構成では、方法400は、図1、図2、及び／又は図3に示すソース識別モジュール115によって実施され得る。いくつかの構成では、方法400は、図1及び／又は図2に示すアプリケーション120によって実施され得る。

40

【0032】

ブロック405では、システムイベントをデータベース内に登録することができる。いくつかの場合では、このシステムイベントを、カーネルモードドライバを介して登録することができる。ブロック410では、第1のプロセスに関連する疑わしいイベントが検出され得る。ブロック415では、第1のプロセスは複数の潜在的なパペットプロセスのうちの1つとして識別され得る。ブロック420では、第1のプロセスが潜在的なパペットプロセスであることを判定する際、第1のプロセスを起動することとして検出される第2のプロセスを識別するためデータベース内の登録されたイベントが照合され得る。

【0033】

図5は、潜在的なパペットプロセスのリストを維持するための方法500の一実施形態

50

を示すフローチャートである。いくつかの構成では、方法500は、図1、図2、及び／又は図3に示すソース識別モジュール115によって実施され得る。いくつかの構成では、方法500は、図1及び／又は図2に示すアプリケーション120によって実施され得る。

【0034】

ブロック505では、潜在的なパペットプロセスのリスト。ブロック510では、新しいパペットプロセスが、登録されたシステムイベントを介して検出され得る。例えば、カーネルモードドライバは、データベース内のシステムイベントを検出しそれを登録するために使用され得る。ブロック515では、新しいパペットプロセスが潜在的なパペットプロセスのリストに追加され得る。

【0035】

図6は、疑わしいイベントのソースを識別するための方法600の一実施形態を示すフローチャートである。いくつかの構成では、方法600は、図1、図2、及び／又は図3に示すソース識別モジュール115によって実施され得る。いくつかの構成では、方法600は、図1及び／又は図2に示すアプリケーション120によって実施され得る。

【0036】

ブロック605では、実行している第1のプロセスが検出され得る。上述したように、1つ又は2つ以上のシステムイベントがデータベースに登録され、格納され得る。したがって、第1のプロセス及び他のプロセスの操作は、かかるデータベースに格納され得る。ブロック610では、第2のプロセスを開始する第1のプロセスが検出され得る。ブロック615では、疑わしいイベントを生成する第2のプロセスが検出され得る。ブロック620では、第1のプロセスに関する情報が取得され得る。例えば、登録されたシステムイベントは、第2のプロセスを開始する第1のプロセスに関するデータを含むことができる。いくつかの場合では、登録されたシステムイベントは、第1のプロセスが第2のプロセスを開始した後終了することを示すことができる。ブロック625では、第2のプロセスが潜在的なパペットプロセスのリストと比較され得る。かかるプロセスの例としては、cmd.exe, rundll32.exeなどのコマンドラインインタフェースから開始されるプロセスが含まれ得る。ブロック630では、一致が見つかった場合、第2のプロセスはパペットプロセスとして指定され得る。ブロック635では、一致がなかった場合、その後、第1のプロセスが第2のプロセスを開始したことを判定する際、第2のプロセスがリストに追加され得る。例えば、第1のプロセスが第2のプロセスを開始したこと、更に第2のプロセスが疑わしいイベントを生成したことを判定する際、その後、第1のプロセスは潜在的なパペットプロセスのリストに追加され得る。ブロック640では、第1のプロセスが疑わしいイベントのソースとして識別され得る。上述したように、いくつかの場合では、第1のプロセスは、カーネルモードドライバを介して登録されるシステムイベントを介して識別され得る。いくつかの実施形態では、第1のプロセスを疑わしいイベントのソースとして識別する際、通知が生成され得る。いくつかの場合では、この通知は、この起動プロセスを疑わしいイベントのソースとして識別することができる。加えて、又は代替的に、この通知は起動プロセスを潜在的な悪意あるプロセスとして識別することができる。

【0037】

図7は、本発明のシステム及び方法を実行するのに好適なコンピュータシステム700のブロック図を示す。コンピュータシステム700は、中央処理装置710、システムメモリ715（一般的にはRAMであるが、ROM、フラッシュRAMなども含んでもよい）、入出力コントローラ720、音声出力インタフェース730を介するスピーカシステム725などの外部音声デバイス、ディスプレイアダプタ740を介するディスプレイ画面735などの外部デバイス、キーボード745（キーボードコントローラ750とインタフェース接続される）（若しくは他の入力デバイス）、複数のUSBデバイス765（USBコントローラ770とインタフェース接続される）、及び記憶装置インタフェース780など、コンピュータシステム700の主要なサブシステムを相互接続するバス70

10

20

30

40

50

5を含む。また、シリアルポート760を通してバス705に接続されるマウス755（若しくは他のポイントアンドクリックデバイス）、及びネットワークインタフェース785（バス705に直接連結される）も含まれる。

【0038】

バス705によって、中央処理装置710と、上述したような、読出し専用メモリ（ROM）又はフラッシュメモリ（どちらも図示なし）及びランダムアクセスメモリ（RAM）（図示なし）を含んでもよい、システムメモリ715との間のデータ通信が可能になる。RAMは、概して、オペレーティングシステム及びアプリケーションプログラムがロードされるメインメモリである。ROM又はフラッシュメモリは、他のコードの中でも、周辺構成要素又はデバイスとの相互作用などの基本的なハードウェア動作を制御する、ベーシック入出力システム（BIOS）を含むことができる。例えば、本発明のシステム及び方法を実行するソース識別モジュール115-bは、システムメモリ715に格納されてもよい。コンピュータシステム700に常駐するアプリケーション（例えば、アプリケーション120）は、一般的に、ハードディスクドライブ（例えば、固定ディスク775）又は他の記憶媒体などの非一時的コンピュータ可読媒体に記憶され、それを介してアクセスされる。それに加えて、アプリケーションは、インタフェース785を介してアクセスされるとアプリケーション及びデータ通信技術にしたがって変調される、電子信号の形態であることができる。

【0039】

ストレージインタフェース780は、コンピュータシステム700の他のストレージインタフェースと同様に、固定ディスクドライブ775など、情報の記憶及び／又は検索用の標準的なコンピュータ可読媒体に接続することができる。固定ディスクドライブ775は、コンピュータシステム700の一部であってもよく、又は独立したものであって、他のインタフェースシステムを通してアクセスされてもよい。ネットワークインタフェース785は、POP（ポイントオブプレゼンス）を介したインターネットに対する直接ネットワークリンクを介して、リモートサーバに対する直接接続を提供してもよい。ネットワークインタフェース785は、デジタル携帯電話接続、セルラーデジタルパケットデータ（CDPD）接続、デジタル衛星データ接続などを含む無線技術を用いて、かかる接続を提供してもよい。

【0040】

他の多くのデバイス又はサブシステム（図示なし）は、同様の方法で接続されてもよい（例えば、文書スキャナ、デジタルカメラなど）。逆に、図7に示される全てのデバイスが、本発明のシステム及び方法を実践するために必ずしも存在しなくてもよい。デバイス及びサブシステムは、図7に示されるものとは異なる形で相互接続することができる。図7に示されるものなどのコンピュータシステムの動作は、当該技術分野において容易に知られており、本出願では詳細に考察しない。本開示を実装するコードは、システムメモリ715又は固定ディスク775の1つ以上など、非一時的コンピュータ可読媒体に格納することができる。コンピュータシステム700上に提供されるオペレーティングシステムは、iOS（登録商標）、MS-DOS（登録商標）、MS-WINDOWS（登録商標）、OS/2（登録商標）、UNIX（登録商標）、LINUX（登録商標）、又は別の既知のオペレーティングシステムであってもよい。

【0041】

更に、本明細書に記載する信号に関して、当業者であれば、信号を第1のブロックから第2のブロックに直接伝送できること、又は信号をブロック間で修正（例えば、増幅、減衰、遅延、ラッチ、バッファ、反転、フィルタリング、又は別の方法で修正）できることを認識するであろう。上述の実施形態の信号は、あるブロックから次のブロックに伝送されるものと特徴付けられるが、本発明のシステム及び方法の他の実施形態は、信号の情報及び／又は機能面がブロック間で伝送される限り、かかる直接伝送される信号の代わりに修正済みの信号を含んでもよい。ある程度、第2のブロックにおける信号入力、関係する回路の物理的制約（例えば、いくらかの減衰及び遅延が必然的に存在する）により、第

10

20

30

40

50

1のブロックからの第1の信号出力から得られた第2の信号として概念化することができる。したがって、本明細書で使用する時、第1の信号から得られた第2の信号は、回路制約によるものであるか、あるいは第1の信号の情報及び／又は最終機能面を変更しない他の回路素子を通することによるものであるか否かにかかわらず、第1の信号又は第1の信号に対する何らかの修正を含む。

【0042】

上述の開示は、特定のブロック図、フローチャート、及び例を使用して様々な実施形態を説明しているが、本明細書に記載及び／又は例証されるブロック図の構成要素、フローチャートのステップ、動作、及び／又は構成要素はそれぞれ、個別にかつ／又は集合的に、広範なハードウェア、ソフトウェア、又はファームウェア（若しくはそれらの任意の組み合わせの）構成を使用して実行されてもよい。それに加えて、他の多くのアーキテクチャが同じ機能性を達成するように実装可能であるので、他の構成要素内に含有される構成要素のあらゆる開示は、本質的に例示と見なされるべきである。

10

【0043】

本明細書に記載及び／又は例証されるプロセスパラメータ、及びステップの順序は、単なる例として与えられるものであり、所望に応じて変更することができる。例えば、本明細書に例証及び／又は記載されるステップは特定の順序で図示若しくは検討されることがあるが、これらのステップは必ずしも例証又は検討される順序で行われなくてもよい。本明細書に記載及び／又は例証される様々な例示的な方法はまた、本明細書に記載若しくは例証されるステップの1つ以上を省略してもよく、又は開示されるステップに加えて追加のステップを含んでもよい。

20

【0044】

更に、様々な実施形態を、完全に機能的なコンピューティングシステムの文脈において本明細書に記載及び／又は例証してきたが、これらの例示的な実施形態の1つ以上は、実際に配布を実施するために使用されるコンピュータ可読媒体の特定のタイプにかかわらず、様々な形態のプログラム製品として配布されてもよい。本明細書で開示される実施形態はまた、特定のタスクを実行するソフトウェアモジュールを使用して実行されてもよい。これらのソフトウェアモジュールは、スクリプト、バッチ、又はコンピュータ可読記憶媒体上若しくはコンピューティングシステム内に格納してもよい他の実行可能ファイルを含んでもよい。いくつかの実施形態では、これらのソフトウェアモジュールは、本明細書で

30

【0045】

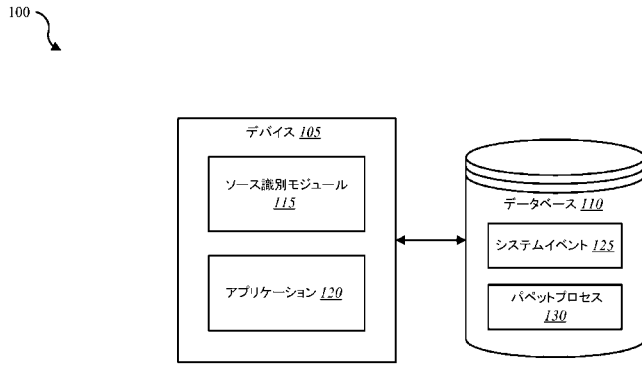
上記の記載は、説明を目的として特定の実施形態を参照して記載してきた。しかしながら、上述の例示的考察は、包括的であること、又は本発明を開示される正確な形態に限定することを意図するものではない。上述の教示を考慮して、多くの修正及び変形が可能である。実施形態は、本発明のシステム及び方法並びにそれらの実際の適用の原理を最も良く説明するために選択し記載したものであり、それによって他の当業者が、企図される特定の用途に好適であり得る様々な修正を用いて、本発明のシステム及び方法並びに様々な実施形態を最大限に利用することが可能になる。

40

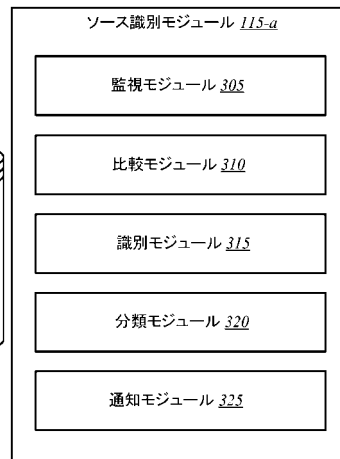
【0046】

別途記載のない限り、「a」又は「an」という用語は、本明細書及び特許請求の範囲で使用する時、「～の少なくとも1つ」を意味すると解釈されるものとする。それに加えて、使用しやすくするため、「含む」及び「有する」という語は、本明細書及び特許請求の範囲で使用する時、「備える」という語と交換可能であり、同じ意味を有する。それに加えて、「～に基づく」という用語は、本明細書及び特許請求の範囲で使用する時、「～の少なくとも1つに基づく」という用語と解釈されるものとする。

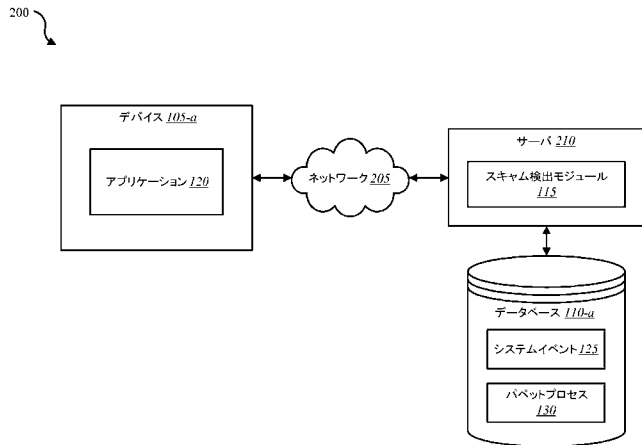
【図 1】



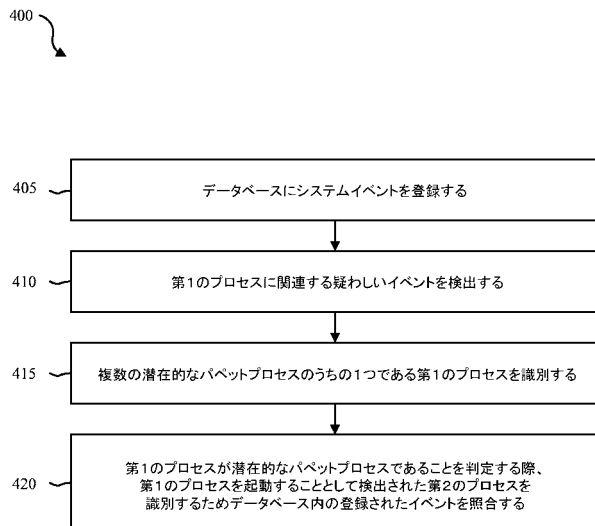
【図 3】



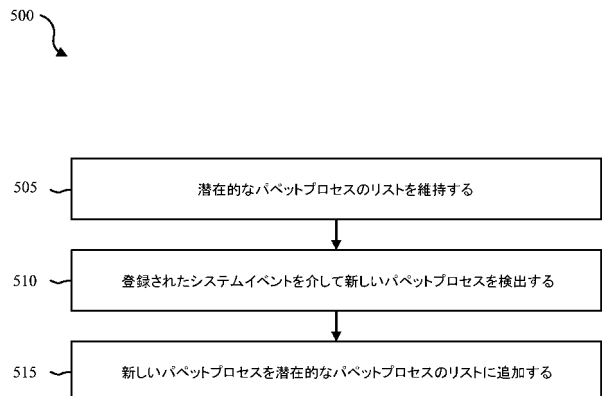
【図 2】



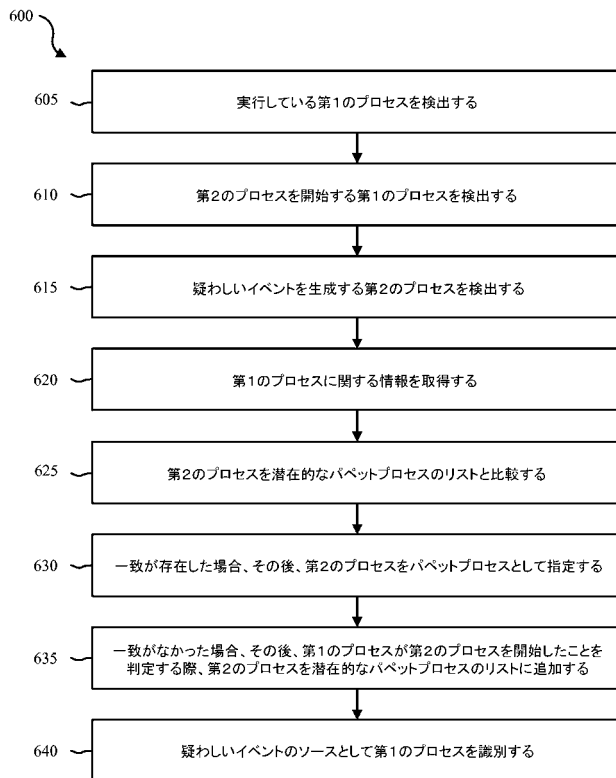
【図 4】



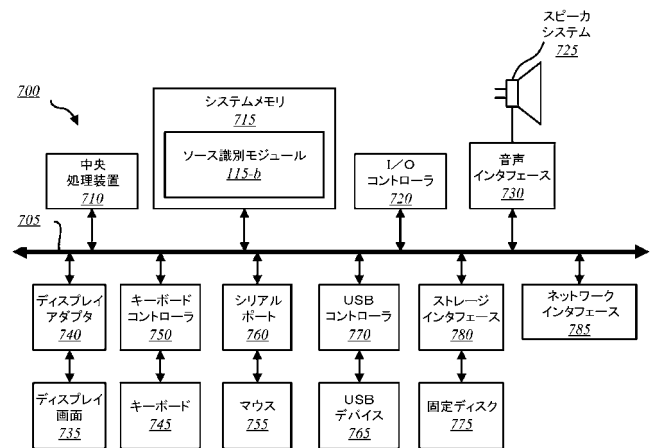
【図 5】



【図 6】



【図 7】



【手続補正書】

【提出日】平成28年10月4日(2016.10.4)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

疑わしいイベントのソースを識別するためのコンピュータによって実行される方法であって、

データベースにシステムイベントを登録することと、

第1のプロセスに関連する疑わしいイベントを検出することと、

複数の潜在的なパペットプロセスのうちの1つであるとして前記第1のプロセスを識別することと、

前記第1のプロセスを起動することとして検出される第2のプロセスを識別するために前記データベース内の前記登録されたシステムイベントを照合することと、

を含む、方法。

【請求項 2】

前記疑わしいイベントの前記ソースとして前記第2のプロセスを識別する通知を生成することを更に含む、請求項 1 に記載の方法。

【請求項 3】

前記第1のプロセスを開始する際に前記第2のプロセスが終了することを判定することを更に含む、請求項 1 に記載の方法。

【請求項 4】

前記第 1 のプロセスを開始した前記第 2 のプロセスを識別する際、前記第 1 のプロセスをパベットプロセスとして識別することを更に含む、請求項 1 に記載の方法。

【請求項 5】

前記第 1 のプロセスが、前記第 2 のプロセスによってコマンドラインインタフェース上に直接供給される命令を介して開始されている、請求項 1 に記載の方法。

【請求項 6】

前記第 1 のプロセスが、少なくとも 1 つのファイルからの命令を介して開始されており、前記少なくとも 1 つのファイルへのパスは前記第 2 のプロセスによってコマンドラインインタフェース上に供給されている、請求項 1 に記載の方法。

【請求項 7】

潜在的なパベットプロセスのリストを維持することと、

検出されたプロセス起動イベントを含む、前記登録されたシステムイベントを介して新しいパベットプロセスを検出することと、

前記新しいパベットプロセスを前記潜在的なパベットプロセスのリストに追加することと、を更に含む、請求項 1 に記載の方法。

【請求項 8】

前記潜在的なパベットプロセスのリストが、コマンドラインインタフェースを有する少なくとも 1 つのプロセスを含む、請求項 7 に記載の方法。

【請求項 9】

前記潜在的なパベットプロセスのリストが、`cmd.exe`, `rundll.exe`, `rundll32.exe`, `regsvr32.exe`, `dllhost.exe`, `regedit.exe`, `taskhost.exe`, `cscript`, `wscript`, `vbscript`, `perlscript`, `bash`, `ldconfig`, `terminal.app`, 及び `x-code.app` のうち少なくとも 1 つを含む、請求項 8 に記載の方法。

【請求項 10】

前記システムイベントがカーネルモードドライバを介して登録されている、請求項 1 に記載の方法。

【請求項 11】

疑わしいイベントのソースを識別するように構成されたコンピューティングデバイスであって、

プロセッサと、

前記プロセッサと電子的に通信しているメモリと、

前記メモリに格納された命令であって、

データベースにシステムイベントを登録することと、

第 1 のプロセスに関連する疑わしいイベントを検出することと、

複数の潜在的なパベットプロセスのうちの 1 つであるとして前記第 1 のプロセスを識別することと、

前記第 1 のプロセスを起動することとして検出される第 2 のプロセスを識別するために前記データベース内の前記登録されたシステムイベントを照合することと、

を前記プロセッサによって実行可能な命令と、を備える、コンピューティングデバイス。

【請求項 12】

前記命令が、

前記疑わしいイベントの前記ソースとして前記第 2 のプロセスを識別する通知を生成することを、前記プロセッサによって実行可能である、請求項 11 に記載のコンピューティングデバイス。

【請求項 13】

前記命令が、

前記第 1 のプロセスを開始する際に前記第 2 のプロセスが終了することを判定すること

を、前記プロセッサによって実行可能である、請求項 1 1 に記載のコンピューティングデバイス。

【請求項 1 4】

前記命令が、

前記第 1 のプロセスを開始した前記第 2 のプロセスを識別する際、前記第 1 のプロセスをパペットプロセスとして識別することを、前記プロセッサによって実行可能である、請求項 1 1 に記載のコンピューティングデバイス。

【請求項 1 5】

プロセッサによって疑わしいイベントを識別するためのコンピュータプログラム製品であって、前記コンピュータプログラム製品は命令を格納する非一時的コンピュータ可読媒体を備え、前記命令が、

データベースにシステムイベントを登録することと、

第 1 のプロセスに関連する疑わしいイベントを検出することと、

複数の潜在的なパペットプロセスのうちの 1 つであるとして前記第 1 のプロセスを識別することと、

前記第 1 のプロセスを起動することとして検出される第 2 のプロセスを識別するために前記データベース内の前記登録されたシステムイベントを照合することと、

を前記プロセッサによって実行可能な命令と、を備える、コンピュータプログラム製品

。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/018412

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/55
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/068774 A1 (NIE WANQUAN [CN]) 6 March 2014 (2014-03-06) paragraph [0013] - paragraph [0035]; figures 2, 3 -----	1-4, 7, 10-14, 17, 19, 20
A	US 8 205 257 B1 (SATISH SOURABH [US] ET AL) 19 June 2012 (2012-06-19) abstract -----	1-20
A	US 2012/311708 A1 (AGARWAL ROMANCH [IN] ET AL) 6 December 2012 (2012-12-06) paragraph [0005] - paragraph [0007] -----	1-20
A	US 8 646 084 B1 (PAVLYUSHCHIK MIKHAIL A [RU] ET AL) 4 February 2014 (2014-02-04) column 2; figure 3 -----	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

8 May 2015

Date of mailing of the international search report

18/05/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel: (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Jascau, Adrian

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2015/018412

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2014068774	A1	06-03-2014	CN 103632088 A TW 201409272 A US 2014068774 A1	12-03-2014 01-03-2014 06-03-2014
US 8205257	B1	19-06-2012	NONE	
US 2012311708	A1	06-12-2012	CN 103782303 A EP 2715596 A2 JP 2014515538 A KR 20140033145 A US 2012311708 A1 WO 2012167056 A2	07-05-2014 09-04-2014 30-06-2014 17-03-2014 06-12-2012 06-12-2012
US 8646084	B1	04-02-2014	RU 2012141466 A US 8646084 B1	10-04-2014 04-02-2014

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US