【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成31年1月10日(2019.1.10)

【公表番号】特表2017-539039(P2017-539039A)
【公表日】平成29年12月28日(2017.12.28)
【年通号数】公開・登録公報2017-050
【出願番号】特願2017-546273(P2017-546273)
【国際特許分類】
Ｇ０６Ｆ　21/55　(2013.01)
Ｇ０６Ｆ　21/56　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/55
Ｇ０６Ｆ　21/56　３６０

【手続補正書】
【提出日】平成30年11月21日(2018.11.21)
【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】
悪意のある通信のためのネットワーク接続の確立の試みのクライアント側における検出および防止のためのコンピュータ実施方法であって、
クライアント端末のプロセッサによって実行されるエンドポイントコードによって、前記クライアント端末からサーバへのネットワーク接続の確立のための接続確立プロセスを検出することであり、前記接続確立プロセスが、前記クライアント端末の前記プロセッサによって実行されるアプリケーションによって開始される、接続確立プロセスを検出することと、
前記クライアント端末で管理される開始する前記アプリケーションの少なくとも１つのスタックトレース内の記録を前記アプリケーションのコールスタックから取得することと、
前記開始する前記アプリケーションの前記少なくとも１つのスタックトレース内の前記アプリケーションの記録の解析に基づいて、前記ネットワーク接続を悪意のあるアクティビティに使用するために悪意のある通信を確立する試行を検出することと、
前記解析が前記ネットワーク接続に基づいて前記悪意のある通信を確立する前記試行を検出したとき前記ネットワーク接続の確立をブロックすることとを含む、コンピュータ実施方法。
【請求項２】
前記解析が、前記少なくとも１つのスタックトレースと、接続確立に関連するスレッドデータ、モジュールデータ、およびプロセスデータからなる群の少なくとも１つのメンバとを含むフローデータの解析を含む、請求項１に記載の方法。
【請求項３】
各々のそれぞれのクライアントにおいて、前記少なくとも１つのスタックトレースに関連するデータ、および／またはフローデータを集めることと、
各々のそれぞれのクライアントから中央サーバに前記少なくとも１つのスタックトレースに関連する前記データを送信することと
をさらに含み、

前記解析が前記中央サーバによって実行され、
前記少なくとも１つのスタックトレースに関連するデータが、動的なコードを含む、請求項１に記載の方法。
【請求項４】
前記ネットワーク接続がアクティブ化されていない場合、前記悪意のある通信を確立する前記試行が検出されたときに、前記接続確立プロセスに、前記ネットワーク接続のアクティブ化を許可することをさらに含む、請求項１に記載の方法。
【請求項５】
前記少なくとも１つのスタックトレースが、前記接続確立プロセスの開始のためのインターネットプロトコル群の伝送制御プロトコル（ＴＣＰ）に従って実行される接続確立中に収集される、請求項１に記載の方法。
【請求項６】
前記少なくとも１つのスタックトレースが、前記接続確立プロセスの間に多数のポイントで得られた多数のスタックトレースの少なくとも１つのシーケンスを含み、前記解析が、前記悪意のある通信を確立する前記試行を表すフローデータ解析に前記多数のスタックトレースを突き合わせることを含む、請求項１に記載の方法。
【請求項７】
前記解析が、開始した前記アプリケーションの感染を表す、未知のモジュールおよびブラックリストもしくはホワイトリストに載ったモジュールの少なくとも一方のための前記少なくとも１つのスタックトレースの前記記録を解析することを含む、請求項１に記載の方法。
【請求項８】
前記解析が、前記解析を実行する中央サーバにおいて有効なものとして指定された感染していないアプリケーションによって使用される接続確立フローデータ解析のための前記少なくとも１つのスタックトレースを解析することを含む、請求項１に記載の方法。
【請求項９】
解析することは、前記アプリケーションが、前記悪意のあるアクティビティ／通信を確立する前記試行を開始する注入されたコードに感染していない場合に前記アプリケーションによって生成されると予想される接続確立スタックフローデータ解析との少なくとも１つのスタックトレースの比較を含む、請求項１に記載の方法。
【請求項１０】
悪意のある通信のためのネットワーク接続の確立の試みのクライアント側における検出のためのシステムであって、
少なくとも１つのゲートウェイであり、
クライアント端末からネットワークベースサーバへのネットワーク接続を確立するための接続確立プロセスの間クライアント端末のプロセッサにより実行されるアプリケーションの少なくとも１つのスタックトレースを受信することであって、前記接続確立プロセスは、前記クライアント端末上で実行されるエンドポイントコードによって検出され、前記接続確立プロセスは、前記クライアント端末の前記プロセッサにより実行されるコードによって開始される、受信することと、
前記少なくとも１つのスタックトレースの前記記録を、前記アプリケーションのコールスタックから取得することと、
前記開始したアプリケーションの前記少なくとも１つのスタックトレースの前記アプリケーションの記録の解析に基づいて、前記ネットワーク通信を悪意のあるアクティビティに使用するための前記悪意のある通信の確立の試行の有無を判定することと、
前記ネットワーク接続を使用して前記悪意のある通信を確立する前記試行を表す信号を生成することと
を行うように構成された、少なくとも１つのゲートウェイ
を含む、システム。
【請求項１１】

前記少なくとも１つのゲートウェイが、ネットワークを通じて前記クライアント端末と通信するリモートサーバに常駐する、請求項１０に記載のシステム。
【請求項１２】
前記少なくとも１つのゲートウェイが、前記クライアント端末に常駐するソフトウェアモジュールである、請求項１０に記載のシステム。
【請求項１３】
前記クライアント端末へのインストールのためのエンドポイントモジュールであり、
前記アプリケーションによる前記ネットワーク接続の確立の開始を検出し、
前記少なくとも１つのスタックトレースおよび／またはフローデータを前記ゲートウェイに送信し、
前記ゲートウェイからの前記信号を受信し、
前記受信した信号に基づいて前記ネットワーク接続のアクティブ化を防止するために前記接続確立プロセスをブロックする
ように構成された、エンドポイントモジュール
をさらに含む、請求項１０に記載のシステム。
【請求項１４】
前記少なくとも１つのゲートウェイと通信する管理サーバであり、各クライアントに関連する各ネットワーク接続要求に対して前記少なくとも１つのゲートウェイによって生成された前記信号を収集するように構成された、管理サーバ
をさらに含む、請求項１０に記載のシステム。
【請求項１５】
前記管理サーバは、前記生成された信号を再調査すること、前記生成された信号を管理すること、前記少なくとも１つのゲートウェイの構成を一元的に制御すること、前記少なくとも１つのゲートウェイと通信する少なくとも１つのクライアント端末の構成を一元的に制御すること、前記少なくとも１つのゲートウェイの状態をモニタすること、および前記少なくとも１つのゲートウェイと通信する少なくとも１つのクライアント端末の状態をモニタすることからなる群の少なくとも１つのメンバをユーザが実行できるようにするように構成されたユーザインタフェースをさらに含む、請求項１４に記載のシステム。
【請求項１６】
前記接続確立プロセスが、前記ネットワーク接続のためのローカルエンドポイントを表すアプリケーションプログラミングインタフェースによって管理される、請求項１０に記載のシステム。
【請求項１７】
他のクライアント端末からの類似したスタックフローデータ解析を識別するために、前記悪意のある通信のための前記ネットワーク接続の確立の前記識別された試みに関連づけられるスタックフローデータ解析で前記少なくとも１つのゲートウェイを更新することをさらに含む、請求項１０に記載のシステム。
【請求項１８】
前記少なくとも１つのゲートウェイが、
前記ネットワーク接続がアクティブであるとき前記アプリケーションの少なくとも１つのスタックトレースを受信し、
接続確立後の前記アクティブなネットワーク接続を使用する悪意のあるアクティビティをモニタするために前記少なくとも１つのスタックトレース内の記録を解析する
ようにさらに構成される、請求項１０に記載のシステム。
【請求項１９】
前記少なくとも１つのゲートウェイが、
複数のクライアントの各々から複数の少なくとも１つのフローデータを受信し、
組織的攻撃を検出するために前記複数の少なくとも１つのフローデータを解析する
ようにさらに構成される、請求項１０に記載のシステム。
【請求項２０】

悪意のあるアクティビティのためのネットワーク接続の確立の試みのクライアント側における検出の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が、

少なくとも１つの非一時的コンピュータ可読記憶媒体と、前記少なくとも１つの記憶媒体のうちの少なくとも１つに格納されたプログラム命令と

を含み、前記プログラム命令が、

クライアント端末からサーバへのネットワーク接続の確立のための接続確立プロセスの、前記クライアント端末のプロセッサにより実行されるエンドポイントコードによる検出の指示を受信するためのプログラム命令であり、前記接続確立プロセスが、前記クライアント端末の前記プロセッサにより実行されるアプリケーションによって開始される、受信するためのプログラム命令と、

前記クライアント端末で管理される開始する前記アプリケーションの少なくとも１つのスタックトレース内の記録を、前記アプリケーションのコールスタックから取得するためのプログラム命令と、

前記開始する前記アプリケーションの前記少なくとも１つのスタックトレースの前記アプリケーションの前記記録の解析に基づいて、前記ネットワーク接続が悪意のあるアクティビティで使用される悪意のある通信を確立する試行を検出するためのプログラム命令と、

前記解析が、前記ネットワーク接続に基づいて前記悪意のある通信を確立する前記試行を検出したとき前記ネットワーク接続の確立をブロックするためのプログラム命令と

を含む、コンピュータプログラム製品。