【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28年10月6日(2016.10.6)

【公開番号】特開2016-146192(P2016-146192A)
【公開日】平成28年8月12日(2016.8.12)
【年通号数】公開・登録公報2016-048
【出願番号】特願2016-45104(P2016-45104)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56　　３１０

【手続補正書】
【提出日】平成28年8月19日(2016.8.19)
【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】
ファイアウォールを実行するように構成された第１プロセッサを有する第１の装置と、
仮想マシンを実行するように構成された第２プロセッサを有する第２の装置と、
前記第１の装置の前記第１プロセッサを用いる前記ファイアウォールの実行は、
ネットワークトラフィックフローに関連するアプリケーションの種類を特定することと、
少なくとも前記特定されたアプリケーションに基づき前記ネットワークトラフィックフローをデコードし、前記ネットワークトラフィックフローのデコードによって、前記ネットワークトラフィックフローに関連する１以上のパケットを正しい順序に組み立てるデコーダを選択することと、
前記ネットワークトラフィックフローの少なくとも一部から、マルウェア候補サンプルを生成するために前記ファイアウォールを使用することと、
既存のシグネチャーに一致しない前記マルウェア候補サンプルを決定することと、
前記マルウェア候補サンプルを前記ファイアウォールから前記仮想マシンに送信することと、を含み、
前記第２の装置の前記第２プロセッサを用いる前記仮想マシンの実行は、
マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることと、
前記マルウェア候補サンプルがマルウェアであると判定された場合に、前記仮想マシンを使用してシグネチャーを自動的に生成することと、
少なくとも一部の前記シグネチャーに基づくネットワークアクセスのためのセキュリティポリシーを強制するように構成されている前記ファイアウォールに、前記シグネチャーを前記仮想マシンから送信することと、を含む
システム。
【請求項２】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、セキュリティアプリケーションの設定と、プラットフォームの設定との少なくとも一部のプログラムの変更を特定することを含む

請求項１に記載のシステム。
【請求項３】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、HTTPトラフィック用の非標準的なHTTPポートに接続すること、架空ドメインにアクセスすること、非標準的な実行ファイル拡張子を有する実行ファイルをダウンロードすること、ｅメールサーバ用のDNSクエリを実行すること、一般的な長さよりも短い長さのHTTPヘッダを用いて通信を行うこと、HTTPトラフィックにおいてポスト法で通信を行うこと、IRCトラフィック用の非標準的なIRCポートに接続すること、侵入防止システム回避手法を用いて通信を行うこと、及び、HTTPポートを介して分類されていないトラフィックの通信を行うことの１つ以上を特定することを含む
請求項１に記載のシステム。
【請求項４】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、アクセスされたドメインが閾値を超える長さのドメイン名を持つこと、アクセスされたドメインがダイナミックDNSドメインであるか否か、アクセスされたドメインがファストフラックスドメインであるか否か、及びアクセスされたドメインが最近作成されたドメインであるか否かのうちの１つ以上を特定することを含む
請求項１に記載のシステム。
【請求項５】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、悪質なドメインの特定を含み、
前記監視対象のアクセスされたドメインは、アクセスされたドメインが閾値を超える長さのドメイン名を持つこと、アクセスされたドメインがファストフラックスドメインであるか否か、及びアクセスされたドメインが最近作成されたドメインであるか否かのうちの１つ以上に基づき、潜在的に悪質なドメインであることを示す
請求項１に記載のシステム。
【請求項６】
前記第１の装置の前記第１プロセッサを用いる前記ファイアウォールを実行することは、さらに、マルウェア候補に関するログ情報を前記仮想マシンに送信することを含み、
前記ログ情報は、セッション情報、アプリケーション識別情報、ＵＲＬカテゴリー情報、及び、脆弱性警告情報の１つ以上を含む
請求項１に記載のシステム。
【請求項７】
前記シグネチャーは、マルウェアファイルを識別するためのＭＤ５ハッシュ型シグネチャー、マルウェアファイルを識別するためのファイルの種類に基づくファイルのヘッダ情報からのダイジェスト、及びヒューリスティック型ファイルシグネチャーの１つ以上によって構成される
請求項１に記載のシステム。
【請求項８】
前記シグネチャーは、ＤＮＳ型シグネチャー、ＵＲＬ型シグネチャー、ＩＰ型シグネチャー、プロトコル型シグネチャー、及びポート型シグネチャーの１つ以上によって構成される
請求項１に記載のシステム。
【請求項９】
前記ネットワークトラフィックフローは、ＰＤＦファイルを含み、
前記シグネチャーは、前記ＰＤＦファイルに含まれるスクリプトの少なくとも一部に基づき生成される
請求項１に記載のシステム。

【請求項１０】
前記ネットワークトラフィックフローは、ＰＤＦファイルを含み、
前記シグネチャーは、前記ＰＤＦファイルに含まれるクロスリファレンステーブルの少なくとも一部に基づき生成される
請求項１に記載のシステム。
【請求項１１】
前記ネットワークトラフィックフローの少なくとも一部から、前記マルウェア候補サンプルを生成するために前記ファイアウォールを使用することは、前記ネットワークトラフィックフローの復号を含む
請求項１に記載のシステム。
【請求項１２】
前記第２の装置の前記第２プロセッサを用いる前記仮想マシンを実行することは、さらに、前記シグネチャーを、前記仮想マシンから、前記第１の装置以外の１以上のセキュリティ装置に送信することを含む
請求項１に記載のシステム。
【請求項１３】
ネットワークトラフィックフローに関連するアプリケーションの種類を特定することと、
少なくとも前記特定されたアプリケーションに基づき前記ネットワークトラフィックフローをデコードし、前記ネットワークトラフィックフローのデコードによって、前記ネットワークトラフィックフローに関連する１以上のパケットを正しい順序に組み立てるデコーダを選択することと、
前記ネットワークトラフィックフローの少なくとも一部から、マルウェア候補サンプルを生成するために、第１の装置の実行によってファイアウォールを使用することと、
既存のシグネチャーに一致しない前記マルウェア候補サンプルを決定するために、前記ファイアウォールを使用することと、
前記マルウェア候補サンプルを前記ファイアウォールから、第２の装置によって実行される仮想マシンに送信することと、
マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることと、
前記マルウェア候補サンプルがマルウェアであると判定された場合に、前記仮想マシンを使用してシグネチャーを自動的に生成することと、
少なくとも一部の前記シグネチャーに基づくネットワークアクセスのためのセキュリティポリシーを強制するように構成されている前記ファイアウォールに、前記シグネチャーを前記仮想マシンから送信することと、
を含む方法。
【請求項１４】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、セキュリティアプリケーションの設定と、プラットフォームの設定との少なくとも一部のプログラムの変更を特定することを含む
請求項１３に記載の方法。
【請求項１５】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、HTTPトラフィック用の非標準的なHTTPポートに接続すること、架空ドメインにアクセスすること、非標準的な実行ファイル拡張子を有する実行ファイルをダウンロードすること、ｅメールサーバ用のDNSクエリを実行すること、一般的な長さよりも短い長さのHTTPヘッダを用いて通信を行うこと、HTTPトラフィックにおいてポスト法で通信を行うこと、IRCトラフィック用の非標準的なIRCポートに接続すること、侵入防止システム回避手法を用いて通信を行うこと、及び、HTTP

ポートを介して分類されていないトラフィックの通信を行うことの１つ以上を特定することを含む
請求項１３に記載の方法。
【請求項１６】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、アクセスされたドメインが閾値を超える長さのドメイン名を持つこと、アクセスされたドメインがダイナミックDNSドメインであるか否か、アクセスされたドメインがファストフラックスドメインであるか否か、及びアクセスされたドメインが最近作成されたドメインであるか否かのうちの１つ以上を特定することを含む
請求項１３に記載の方法。
【請求項１７】
前記マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることは、悪質なドメインの特定を含み、
前記監視対象のアクセスされたドメインは、アクセスされたドメインが閾値を超える長さのドメイン名を持つこと、アクセスされたドメインがファストフラックスドメインであるか否か、及びアクセスされたドメインが最近作成されたドメインであるか否かのうちの１つ以上に基づき、潜在的に悪質なドメインであることを示す
請求項１３に記載の方法。
【請求項１８】
さらに、マルウェア候補に関するログ情報を前記仮想マシンに送信することを含み、
前記ログ情報は、セッション情報、アプリケーション識別情報、ＵＲＬカテゴリー情報、及び、脆弱性警告情報の１つ以上を含む
請求項１３に記載の方法。
【請求項１９】
前記シグネチャーは、マルウェアファイルを識別するためのＭＤ５ハッシュ型シグネチャー、マルウェアファイルを識別するためのファイルの種類に基づくファイルのヘッダ情報からのダイジェスト、及びヒューリスティック型ファイルシグネチャーの１つ以上によって構成される
請求項１３に記載の方法。
【請求項２０】
ネットワークトラフィックフローに関連するアプリケーションの種類を特定することと、
少なくとも前記特定されたアプリケーションに基づき前記ネットワークトラフィックフローをデコードし、前記ネットワークトラフィックフローのデコードによって、前記ネットワークトラフィックフローに関連する１以上のパケットを正しい順序に組み立てるデコーダを選択することと、
前記ネットワークトラフィックフローの少なくとも一部から、マルウェア候補サンプルを生成するために、第１の装置の実行によってファイアウォールを使用することと、
既存のシグネチャーに一致しない前記マルウェア候補サンプルを決定するために、前記ファイアウォールを使用することと、
前記マルウェア候補サンプルを前記ファイアウォールから、第２の装置によって実行される仮想マシンに送信することと、
マルウェアの特定のためのエミュレーションの際に前記マルウェア候補サンプルの挙動を監視するために、前記仮想マシンを用いることと、
前記マルウェア候補サンプルがマルウェアであると判定された場合に、前記仮想マシンを使用してシグネチャーを自動的に生成することと、
少なくとも一部の前記シグネチャーに基づくネットワークアクセスのためのセキュリティポリシーを強制するように構成されている前記ファイアウォールに、前記シグネチャーを前記仮想マシンから送信することと、

を前記第１及び第２の装置に実行させるためのプログラム。