【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】令和6年5月31日(2024.5.31)

【国際公開番号】WO2022/023828
【公表番号】特表2023-534502(P2023-534502A)
【公表日】令和5年8月9日(2023.8.9)
【年通号数】公開公報(特許)2023-149
【出願番号】特願2023-503075(P2023-503075)
【国際特許分類】
Ｇ０６Ｆ 21/56(2013.01)
【ＦＩ】
Ｇ０６Ｆ 21/56
Ｇ０６Ｆ 21/56 ３５０
Ｇ０６Ｆ 21/56 ３６０

【手続補正書】
【提出日】令和6年5月23日(2024.5.23)
【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】
ストレージ装置に接続されたコンピュータシステムを保護する方法であって、
保護されるファイルのセットおよびデコイファイルを、前記ストレージ装置に保管するステップであり、前記デコイファイルに対するいかなる変更も、前記コンピュータシステムに対するサイバー攻撃を示すものである、ステップと、
前記コンピュータシステムで実行されているプロセスから、前記ストレージ装置に保管されているファイルを列挙するためのリクエストを受信するステップと、
前記プロセスを良性または疑わしいものとして分類するために、プロセッサによって、前記プロセスを解析するステップと、
前記プロセスに対して前記保護されるファイルを列挙するステップと、
前記プロセスを疑わしいものとして分類した場合にのみ、前記プロセスに対して前記デコイファイルを列挙するステップと、
を含み、
前記プロセスを解析するステップは、前記プロセスに対して動的解析を実行することを含み、
前記動的解析を実行することは、
前記ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定することを含み、前記スレッドは、スレッドスタックを含むこと、
前記スレッドスタックが、グラフィカルユーザインターフェースの共有ライブラリのメモリアドレスを含むか以下かを判断すること、
前記スレッドスタックが、前記共有ライブラリのメモリアドレスを含まないと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
前記スレッドスタックが、前記共有ライブラリのメモリアドレスを含むと判断した場合に、前記スレッドを良性として分類すること、
を含む、
方法。

【請求項２】
前記サイバー攻撃は、ランサムウェア攻撃を含む、
請求項１に記載の方法。
【請求項３】
前記方法は、
前記プロセスに対して予防措置を開始するステップ、
を含む、請求項１に記載の方法。
【請求項４】
前記予防措置を開始するステップは、
前記プロセスの因果関係チェーンを特定すること、および、
前記因果関係チェーンに対して予防措置を開始すること、
を含む、請求項３に記載の方法。
【請求項５】
前記プロセスを解析するステップは、
前記ストレージ装置上で、前記プロセスを起動した実行可能ファイルを特定すること、および、
前記特定された実行可能ファイルに対して静的解析を実行すること、
を含む、請求項１に記載の方法。
【請求項６】
前記静的解析を実行することは、
前記実行可能ファイルの名前を特定すること、
前記特定された名前をホワイトリスト化名前のリストと比較すること、
前記特定された名前がホワイトリスト化名前のいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記特定された名前がホワイトリスト化名前のいずれかと一致する場合には、前記プロセスを良性として分類すること、
を含む、請求項５に記載の方法。
【請求項７】
前記静的解析を実行することは、
前記実行可能ファイルのパスを特定すること、
前記特定されたパスをホワイトリスト化パスのリストと比較すること、
前記特定されたパスがホワイトリスト化パスのいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記特定されたパスがホワイトリスト化パスのいずれかと一致する場合には、前記プロセスを良性として分類すること、
を含む、請求項５に記載の方法。
【請求項８】
前記静的解析を実行することは、
前記実行可能ファイルの署名を計算すること、
前記計算された署名をホワイトリスト化署名のリストと比較すること、
前記計算された署名がホワイトリスト化署名のいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記計算された署名がホワイトリスト化署名のいずれかと一致する場合には、前記プロセスを良性として分類すること、
を含む、請求項５に記載の方法。
【請求項９】
前記静的解析を実行することは、
前記実行可能ファイルのハッシュ値を計算すること、
前記計算されたハッシュ値をホワイトリスト化ハッシュ値のリストと比較すること、
前記計算されたハッシュ値がホワイトリスト化ハッシュ値のいずれとも一致しない場

合には、前記プロセスを疑わしいものとして分類すること、および、
　前記計算されたハッシュ値がホワイトリスト化ハッシュ値のいずれかと一致する場合には、前記プロセスを良性として分類すること、
を含む、請求項５に記載の方法。
【請求項１０】
前記動的解析を実行することは、
　ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定すること、
　前記スレッドが前記プロセスの中へ注入されたか否かを判断すること、
　前記スレッドが前記プロセスの中へ注入されたと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
　前記スレッドが前記プロセスの中へ注入されなかったと判断した場合に、前記スレッドを良性として分類すること、
を含む、請求項１に記載の方法。
【請求項１１】
前記動的解析を実行することは、
　ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定すること、
　前記スレッドがシェルコードを含むか否かを判断すること、
　前記スレッドがシェルコードを含むと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
　前記スレッドがシェルコードを含まないと判断した場合に、前記スレッドを良性として分類すること、
を含む、請求項１に記載の方法。
【請求項１２】
コンピュータシステムを保護する装置であって、
保護されるファイルのセットおよびデコイファイルを保管するように構成されているストレージ装置であり、前記デコイファイルに対するいかなる変更も、前記コンピュータシステムに対するサイバー攻撃を示すものである、ストレージ装置と、
プロセッサであり、
　前記コンピュータシステムで実行されているプロセスから、前記ストレージ装置に保管されているファイルを列挙するためのリクエストを受信し、
　前記プロセスを良性または疑わしいものとして分類するために、前記プロセスを解析し、
　前記プロセスに対して前記保護されるファイルを列挙し、
　前記プロセスを疑わしいものとして分類したことに応答して、前記プロセスに対して前記デコイファイルを列挙する、
ように構成されている、プロセッサと、
を含み、
前記プロセッサは、前記プロセスに対して動的解析を実行するように構成されており、
前記プロセッサは、
　前記ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定することであり、前記スレッドは、スレッドスタックを含むこと、
　前記スレッドスタックが、グラフィカルユーザインターフェースの共有ライブラリのメモリアドレスを含むか以下かを判断すること、
　前記スレッドスタックが、前記共有ライブラリのメモリアドレスを含まないと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
　前記スレッドスタックが、前記共有ライブラリのメモリアドレスを含むと判断した場合に、前記スレッドを良性として分類すること、
によって、前記動的解析を実行するように構成されている、

装置。
【請求項１３】
前記サイバー攻撃は、ランサムウェア攻撃を含む、
請求項１２に記載の装置。
【請求項１４】
前記プロセッサは、さらに、
前記プロセスに対して予防措置を開始する、
ように構成されている、請求項１２に記載の装置。
【請求項１５】
前記プロセッサは、
前記プロセスの因果関係チェーンを特定すること、および、
前記因果関係チェーンに対して予防措置を開始すること、
によって、前記予防措置を開始する、
ように構成されている、請求項１４に記載の装置。
【請求項１６】
前記プロセッサは、
前記ストレージ装置上で、前記プロセスを起動した実行可能ファイルを特定すること、および、
前記特定された実行可能ファイルに対して静的解析を実行すること、
によって、前記プロセスを解析する、
ように構成されている、請求項１２に記載の装置。
【請求項１７】
前記プロセッサは、
前記実行可能ファイルの名前を特定すること、
前記特定された名前をホワイトリスト化名前のリストと比較すること、
前記特定された名前がホワイトリスト化名前のいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記特定された名前がホワイトリスト化名前のいずれかと一致する場合には、前記プロセスを良性として分類すること、
によって、前記静的解析を実行する、
ように構成されている、請求項１６に記載の装置。
【請求項１８】
前記プロセッサは、
前記実行可能ファイルのパスを特定すること、
前記特定されたパスをホワイトリスト化パスのリストと比較すること、
前記特定されたパスがホワイトリスト化パスのいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記特定されたパスがホワイトリスト化パスのいずれかと一致する場合には、前記プロセスを良性として分類すること、
によって、前記静的解析を実行する、
ように構成されている、請求項１６に記載の装置。
【請求項１９】
前記プロセッサは、
前記実行可能ファイルの署名を計算すること、
前記計算された署名をホワイトリスト化署名のリストと比較すること、
前記計算された署名がホワイトリスト化署名のいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記計算された署名がホワイトリスト化署名のいずれかと一致する場合には、前記プロセスを良性として分類すること、
によって、前記静的解析を実行する、

ように構成されている、請求項１６に記載の装置。
【請求項２０】
前記プロセッサは、
前記実行可能ファイルのハッシュ値を計算すること、
前記計算されたハッシュ値をホワイトリスト化ハッシュ値のリストと比較すること、
前記計算されたハッシュ値がホワイトリスト化ハッシュ値のいずれとも一致しない場合には、前記プロセスを疑わしいものとして分類すること、および、
前記計算されたハッシュ値がホワイトリスト化ハッシュ値のいずれかと一致する場合には、前記プロセスを良性として分類すること、
によって、前記静的解析を実行する、
ように構成されている、請求項１６に記載の装置。
【請求項２１】
前記プロセッサは、
ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定すること、
前記スレッドが前記プロセスの中へ注入されたか否かを判断すること、
前記スレッドが前記プロセスの中へ注入されたと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
前記スレッドが前記プロセスの中へ注入されなかったと判断した場合に、前記スレッドを良性として分類すること、
によって、前記動的解析を実行する、
ように構成されている、請求項１２に記載の装置。
【請求項２２】
前記プロセッサは、
ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定すること、
前記スレッドがシェルコードを含むか否かを判断すること、
前記スレッドがシェルコードを含むと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
前記スレッドがシェルコードを含まないと判断した場合に、前記スレッドを良性として分類すること、
によって、前記動的解析を実行する、
ように構成されている、請求項１２に記載の装置。
【請求項２３】
コンピュータシステムを保護するためのコンピュータプログラムであって、前記コンピュータプログラムは、プログラム命令を含み、非一時的なコンピュータ可読記憶媒体に保管されており、コンピュータによって命令が読み込まれると、前記コンピュータに、
前記コンピュータシステムに接続されているストレージ装置に、保護されるファイルのセットおよびデコイファイルを保管し、前記デコイファイルに対するいかなる変更も、前記コンピュータシステムに対するサイバー攻撃を示すものであり、
前記コンピュータシステムで実行されているプロセスから、前記ストレージ装置に保管されているファイルを列挙するためのリクエストを受信し、
前記プロセスを良性または疑わしいものとして分類するために、前記プロセスを解析し、
前記プロセスに対して前記保護されるファイルを列挙し、
前記プロセスを疑わしいものとして分類したことに応答して、前記プロセスに対して前記デコイファイルを列挙する、
ようにさせ、
前記プログラム命令は、前記プロセスに対して動的解析を実行することによって前記プロセスを解析するように構成されており、

前記プログラム命令は、
前記ファイルを列挙するための前記リクエストを伝達した前記プロセスにおけるスレッドを特定することであり、前記スレッドは、スレッドスタックを含むこと、
前記スレッドスタックが、グラフィカルユーザインターフェースの共有ライブラリのメモリアドレスを含むか以下かを判断すること、
前記スレッドスタックが、前記共有ライブラリのメモリアドレスを含まないと判断した場合に、前記プロセスを疑わしいものとして分類すること、および、
前記スレッドスタックが、前記共有ライブラリのメモリアドレスを含むと判断した場合に、前記スレッドを良性として分類すること、
によって、前記動的解析を実行するように構成されている、
コンピュータプログラム。