【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1年10月31日(2019.10.31)

【公表番号】特表2018-536932(P2018-536932A)
【公表日】平成30年12月13日(2018.12.13)
【年通号数】公開・登録公報2018-048
【出願番号】特願2018-521349(P2018-521349)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
Ｇ０６Ｆ　21/53　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56　　３６０
Ｇ０６Ｆ　21/53

【手続補正書】
【提出日】令和1年9月18日(2019.9.18)
【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】
アプリケーションによる悪意のある活動をトリガするためにハニーポットシステムにおいて実施される方法であって、
コンピューティングデバイス上のリソースにアクセスするための前記アプリケーションのパーミッションに基づいて、前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを、前記コンピューティングデバイスのプロセッサを介して決定するステップであって、前記リソースが1つまたは複数のデバイス構成要素およびデータの一方または両方を備える、ステップと、
前記アプリケーションが潜在的に悪意があるという決定に応答して、前記アプリケーションをターゲットアプリケーションとして指定するステップと、
前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションの前記パーミッションに基づいて前記ターゲットアプリケーションのトリガ条件を、前記プロセッサを介して予測するステップであって、前記トリガ条件が、前記ターゲットアプリケーションに悪意のある活動を提示させる、ステップと、
前記予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを前記プロセッサを介して供給するステップと、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップと、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意のあるアプリケーションであるかどうかを、前記プロセッサを介して決定するステップと
を備える、方法。
【請求項２】
前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップが、同じトリガ条件を有し得るアプリケーションのグループを監視するステップを備える、請求項1に記載の方法。
【請求項３】

前記コンピューティングデバイス上で現在実行中の前記アプリケーションが潜在的に悪意があるかどうかを、前記プロセッサを介して決定するステップが、
前記コンピューティングデバイスのリソースにアクセスすることに対応する、前記アプリケーションのパーミッション、および前記アプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを、前記プロセッサを介して解析するステップ
を備える、請求項1に記載の方法。
【請求項４】
前記1つまたは複数のリソースが、1つまたは複数のデバイス構成要素およびデータのうちの一方または両方を備える、請求項1に記載の方法。
【請求項５】
前記1または複数のデバイス構成要素が、インストール済みアプリケーション、オペレーティングシステム、ネットワークインターフェース、処理ユニット、データ記憶ユニット、結合されたデバイス、出力ユニット、入力ユニット、およびセンサからなるグループの少なくとも1つのメンバーを備える、請求項4に記載の方法。
【請求項６】
前記データが、連絡先リスト、記憶されたファイル、個人情報、ネットワーキング状態データ、加入情報、ロケーション情報、システム情報、既知の脆弱性情報、およびセンサデータからなるグループの少なくとも1つのメンバーを備える、請求項4に記載の方法。
【請求項７】
前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションの前記トリガ条件を、前記プロセッサを介して予測するステップが、
前記ターゲットアプリケーションのパーミッション、前記ターゲットアプリケーションにとって以前にアクセス可能であった任意のリソース、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データのうちの少なくとも1つを、前記プロセッサを介して評価するステップ
を備える、請求項1に記載の方法。
【請求項８】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを、前記プロセッサを介して供給するステップが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記ターゲットアプリケーションにとって以前に認識可能であったリソースを、前記プロセッサを介して調整するステップ、および
前記ターゲットアプリケーションにとって以前に認識可能でなかったリソースを、前記ターゲットアプリケーションにとって前記リソースが認識可能になるように、前記プロセッサを介して構成するステップ
のうちの少なくとも1つを備える、請求項1に記載の方法。
【請求項９】
前記予測されたトリガ条件に少なくとも部分的に基づいて、前記1つまたは複数のリソースを前記プロセッサを介して供給するステップが、
前記予測されたトリガ条件に少なくとも部分的に基づいて、仮想リソースを、前記プロセッサを介して作成するステップを備え、前記仮想リソースが、前記コンピューティングデバイス内に実際には存在しないかまたは前記コンピューティングデバイスによってサポートされない、エミュレートされたデバイス構成要素またはデータを表す、
請求項1に記載の方法。
【請求項１０】
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を、前記プロセッサを介して監視するステップが、
前記ターゲットアプリケーションによって行われるアプリケーションプログラミングインターフェース(API)呼出しを、前記プロセッサを介して検出するステップ

を備える、請求項1に記載の方法。
【請求項１１】
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意のあるアプリケーションであるかどうかを前記プロセッサを介して決定するステップが、
前記監視された活動、および前記ターゲットアプリケーションの以前の活動を示す記憶された活動データを、前記プロセッサを介して評価するステップ
を備える、請求項1に記載の方法。
【請求項１２】
前記ターゲットアプリケーションが悪意のあるアプリケーションであるという決定に応答して供給されたリソースに関する情報を含む、前記ターゲットアプリケーションに対して記憶された活動データを、前記プロセッサを介して更新するステップをさらに備える、請求項1に記載の方法。
【請求項１３】
前記ターゲットアプリケーションが悪意のあるアプリケーションであるという決定に応答して、前記ターゲットアプリケーションに対する前記トリガ条件を示す報告メッセージを送信するステップをさらに備える、請求項1に記載の方法。
【請求項１４】
コンピューティングデバイスであって、
コンピューティングデバイス上のリソースにアクセスするためのアプリケーションのパーミッションに基づいて、前記コンピューティングデバイス上で現在実行中のアプリケーションが潜在的に悪意があるかどうかを決定するための手段であって、前記リソースが1つまたは複数のデバイス構成要素およびデータの一方または両方を備える、手段と、
前記アプリケーションが潜在的に悪意があるという決定に応答して、前記アプリケーションをターゲットアプリケーションとして指定するための手段と、
前記ターゲットアプリケーションが潜在的に悪意があるという決定に応答して、前記ターゲットアプリケーションの前記パーミッションに基づいて前記ターゲットアプリケーションのトリガ条件を予測するための手段であって、前記トリガ条件が、前記ターゲットアプリケーションに悪意のある活動を提示させる、手段と、
前記予測されたトリガ条件に少なくとも部分的に基づいて、1つまたは複数のリソースを供給するための手段と、
前記供給された1つまたは複数のリソースに対応する、前記ターゲットアプリケーションの活動を監視するための手段と、
前記監視された活動に少なくとも部分的に基づいて、前記ターゲットアプリケーションが悪意があるかどうかを決定するための手段と
を備える、コンピューティングデバイス。
【請求項１５】
プロセッサによって実行されると、前記プロセッサに請求項1～13のいずれか一項に記載の方法を実行させる命令を備えるコンピュータプログラム。