(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7393517号
(P7393517)

(45)発行日　令和5年12月6日(2023.12.6)

(24)登録日　令和5年11月28日(2023.11.28)

(51)国際特許分類
Ｇ０６Ｆ　21/54　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/54

請求項の数　20　（全26頁）

(21)出願番号　特願2022-504120(P2022-504120)
(86)(22)出願日　令和2年7月21日(2020.7.21)
(65)公表番号　特表2022-542061(P2022-542061A)
(43)公表日　令和4年9月29日(2022.9.29)
(86)国際出願番号　PCT/US2020/042924
(87)国際公開番号　WO2021/016270
(87)国際公開日　令和3年1月28日(2021.1.28)
審査請求日　令和5年7月6日(2023.7.6)
(31)優先権主張番号　62/877,748
(32)優先日　令和1年7月23日(2019.7.23)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　16/934,997
(32)優先日　令和2年7月21日(2020.7.21)
最終頁に続く

(73)特許権者　517152139
サイバー クルシブル インコーポレイテッド.
ＣＹＢＥＲ ＣＲＵＣＩＢＬＥ ＩＮＣ.
アメリカ合衆国，メリーランド州 ２１１４６，セバーナ パーク，５５０エム リッチー ハイウェイ ナンバー１３５
５５０Ｍ Ｒｉｔｃｈｉｅ Ｈｉｇｈｗａｙ ＃１３５，Ｓｅｖｅｒｎａ Ｐａｒｋ，ＭＤ ２１１４６，Ｕ．Ｓ．Ａ.
(74)代理人　100079108
弁理士　稲葉 良幸
(74)代理人　100109346
弁理士　大貫 敏史
(74)代理人　100117189
最終頁に続く

(54)【発明の名称】　ランサムウェアの検出及び軽減のためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
ランサムウェア攻撃に対して標的システムの計算装置を保護するための方法であって、前記計算装置は、ファイルパスに基づいてファイルにアクセスするために前記計算装置のオペレーティングシステムであって、ファイル名および前記ファイルに関するその他の情報のリストを含むディレクトリを有するストレージにおいて実行されるオペレーティングシステムによって使用されるデータ構造を有するファイルシステムを利用して、前記計算装置に以下のステップ：
ａ．前記計算装置にエージェントをインストールするステップであって、前記エージェントは、各々が前記ディレクトリにトラップファイル名を有する１つ又は複数のトラップファイルへの、前記ストレージ内の１つ又は複数の保存されたファイルパスを指定することを含む１つ又は複数の措置を前記標的システムの代わりに自律的に行うソフトウェア又はハードウェアであり、トラップファイルは、それへのアクセスがランサムウェア攻撃の可能性を示すファイルである、ステップ、
ｂ．前記ランサムウェア攻撃の可能性を検出するために、前記１つ又は複数のトラップファイルへのアクセスをモニタするステップ、
ｃ．トラップファイルへのアクセスの検出時、前記ランサムウェア攻撃の可能性に対する是正措置を行うステップ、
を実行させる、方法。
【請求項２】

前記ファイルシステムの前記データ構造は、木構造である、請求項１に記載の方法。
【請求項３】
トラップファイルのためのファイルパスは、前記木構造の最高点において指定される、請求項２に記載の方法。
【請求項４】
前記トラップファイルへの前記１つ又は複数のファイルパスは、探索木アルゴリズムを使用して指定される、請求項２に記載の方法。
【請求項５】
前記探索木アルゴリズムは、バイナリ探索木アルゴリズムを含む、請求項４に記載の方法。
【請求項６】
前記探索木アルゴリズムは、木走査アルゴリズムを含む、請求項４に記載の方法。
【請求項７】
前記木走査アルゴリズムは、深さ優先走査アルゴリズム、幅優先走査アルゴリズム、モンテカルロ木探索アルゴリズム又はランダムサンプリングアルゴリズムの１つである、請求項６に記載の方法。
【請求項８】
前記深さ優先走査アルゴリズムは、前順アルゴリズム、順序アルゴリズム、逆順アルゴリズム、又は後順アルゴリズムの１つである、請求項７に記載の方法。
【請求項９】
名前を含むトラップファイル属性は、木走査操作中に前記トラップファイルが最初に遭遇されるように設定される、請求項７に記載の方法。
【請求項１０】
前記是正措置は、前記標的システムのユーザに通知することを含む、請求項１に記載の方法。
【請求項１１】
前記是正措置は、解析又は復号のためにトラップファイルを自動でアップロードすることを含む、請求項１に記載の方法。
【請求項１２】
前記是正措置は、前記１つ又は複数のトラップファイルにアクセスするプロセスを識別することを含む、請求項１に記載の方法。
【請求項１３】
前記識別されたプロセスは、隔離されるか、キルされるか又は中断されるかのいずれかである、請求項１２に記載の方法。
【請求項１４】
前記是正措置は、暗号変数を抽出するためにメモリ解析を行うことを含む、請求項１に記載の方法。
【請求項１５】
前記ランサムウェア攻撃の可能性は、前記１つ又は複数のファイルトラップへのアクセスレート、許可レベル、ファイルコンテンツ若しくは属性の変化、暗号活動又はソースプロセスの１つ又は複数に基づいて判定される、請求項１に記載の方法。
【請求項１６】
前記標的システムは、暗号変数活動についてモニタされる、請求項１に記載の方法。
【請求項１７】
潜在的な暗号変数は、捕捉及び記憶される、請求項１に記載の方法。
【請求項１８】
プロセスは、新たなファイルが開かれることを可能にすることなく、進行中のファイル暗号化が完了されることを可能にするようにモニタされる、請求項１に記載の方法。
【請求項１９】
前記ファイルパスは、疑似ランダムファイルパスを含み、及びトラップファイルのコン

テンツは、ステガノグラフィックマテリアルを含む、請求項１に記載の方法。
【請求項２０】
共有資源上のトラップファイルに直接アクセスするクライアントのみが警告される、請求項１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
背景
技術分野
本開示は、概して、サイバーセキュリティ技術に関する。より詳細には、本開示は、ランサムウェアの検出及び軽減のためのシステム及び方法に関する。
【背景技術】
【０００２】
関連技術
サイバーセキュリティの分野では、ランサムウェアは、アクセス権の返還を攻撃者が許可するまで、データ又は機器への被害者によるアクセスを拒否するマルウェアである。典型的には、アクセスは、被害者のデータを攻撃者が暗号化することによって拒否され、被害者が身代金を支払った後に復号機能が与えられる。ランサムウェアに焦点を絞った防御機能及び攻撃者機能は、暗号化能力、拒否される資源の範囲及び支払方法の機能及び複雑さの点で発達している。
【０００３】
暗号化機能に関して、暗号化アルゴリズムは、規格化された暗号化アルゴリズム並びに規制及びセキュリティ保護された政府使用、軍事利用及び商用利用について、現在使用が認められている実装に合わせて品質面で成長している。暗号化アルゴリズムの品質は、意図又は承認された復号器ではない現代の計算ハードウェアを有する当事者が復号不能であることに基づいて評価される。国立標準技術研究所（「ＮＩＳＴ」）によって認証された現行の強い暗号化である２５６ビットＡＥＳ暗号化は、意図しない当事者が復号するには9.63×10^{52}年かかると推定される。
【０００４】
暗号化アルゴリズムの脆弱性は、意図しない当事者によって暴かれることに対する暗号化マテリアル（暗号文）のロバスト性に影響を与える。それらの脆弱性は、暗号自体のロジックの脆弱性及び計算能力の改善によって引き起こされる脆弱性に分類することができる。多くの場合、それぞれの分類は、他方の分類に影響を及ぼす。稚拙な復号を、それでも（例えば）寿命よりも長い時間枠まで短縮し得る発見されるロジックの誤りは、徐々に、計算能力が改善されることによりはるかに短い時間で復号されることになる脅威になる。
【０００５】
ランサムウェアの関連では、一部のランサムウェアマルウェアは、暗号攻撃に脆弱な暗号化アルゴリズムを活用する。かかる形態は、攻撃者に身代金を支払うことなく、セキュリティ研究者がランサムウェアに対する幾らかの初期的な成功を収めることを可能にする１つの方法である。脆弱なランサムウェアは、現在でも使用されている可能性があるが、自らの身代金の支払いを被害者に回避させないようにするための攻撃者の金銭的動機がこの適応的傾向を変えた。現代のランサムウェアマルウェアは、攻撃者によって与えられる復号プログラムなしで暗号化後に復号することに対してロバストな暗号化アルゴリズムを一層活用している。
【０００６】
暗号化操作中、暗号変数は、マテリアルを暗号化及び復号するのに必要な設定及び変数である。これらの変数は、暗号化アルゴリズム又は暗号鍵を超えるものである。これらの変数は、暗号鍵のサイズ、パディングアルゴリズム、ナンス、初期設定ベクトル（ｉｖ）又は暗号化アルゴリズムの改変形態等の要素を含む。それらの暗号変数の作成、拡散及び実装は、いかなる暗号化操作にも必要であり、そのランサムウェアは、確実に暗号化ベー

スの操作である。
【０００７】
暗号化操作は、意図しない受信者による復号を可能にする脆弱性を生じさせない方法で計画され、行われなければならない。ランサムウェアの作者にとって、それは、たとえ使用する暗号化アルゴリズムが強くても、高度なサイバーセキュリティ防衛者がそれらの脆弱性を活用して身代金を支払わずに復号する機会を、不適切に行われる暗号化操作が招き得ることを意味する。
【０００８】
過去、ランサムウェアの作者は、サイバーセキュリティ防衛者がアクセスすることを可能にする方法で暗号変数を作成し、拡散させてきた。かかる暗号変数は、適切なランダム化によって作成されない暗号鍵（例えば、全てゼロの暗号鍵）、暗号変数の不適切な再利用及び暗号化アルゴリズムの不適切な実装等の予測可能な暗号変数を含む。
【０００９】
現代のランサムウェアは、暗号操作に関する知識の増加を示している。暗号変数は、ランダムであり、一意に生成され、確実に拡散され、確実に記憶及び実装される。一部の感染では、過去の操作上の脆弱性に起因する簡単な勝利が依然として存在し得るが、自らの身代金の支払いを強いるように金銭的に動機付けられたランサムウェア攻撃者は、殆どの又は全ての操作上の脆弱性を訂正している。
【００１０】
ランサムウェアの動作範囲に関して、被害者にとって利用不能にされるデータ及び装置が多いほど、ランサムウェアの攻撃者にとって攻撃の金銭的価値が上がる。加えて、装置から装置へのランサムウェアマルウェアの自動拡散は、元の標的と無関係の更なる接続された被害者を招き得る。そのような被害者の例は、ビジネスネットワークを横断する顧客若しくは契約者又は攻撃者の元の標的に接続されるサプライチェーン企業であり得る。
【００１１】
この形態は、被害者が接続するネットワーク資源を含むようにマルウェアの機能面の強化まで拡大した。即ち、被害者が接続するファイルサーバ等のアイテムもときに自動で暗号化することができる。
【００１２】
ランサムウェアの攻撃者は、データ侵害のために通常確保される策略をランサムウェア攻撃と組み合わせ始めた。これは、被害者にとってのコストを最大化すること及びその後の身代金の金額を最大化することの両方に関係する。これは、２つの方法、即ちバックアップを除去すること及び高価値のデータを標的にすることによって行われる。暗号化又は削除によって被害者がバックアップを入手できないことを確実にするために、攻撃者は、現在、被害者のバックアップの自動発見及び手動発見を活用している。かかる形態は、管理者の防御がバックアップを保護しないことを確実にするために、特権を高めること等、他の攻撃活動の導入によって攻撃者がアクセスを得ることを確実にすることも含み得る。
【００１３】
加えて、ランサムウェアを即座に実行することとは対照的に、被害者のネットワーク内で作業する間、攻撃者は、企業又は個人にとって最も価値が高いデータに自らが最初にアクセスすることも確実にする。クライアントにとっての最大コストは、適切なマシン及び許可にネットワーク内で策動することなしに攻撃者が必ずしも即座に入手することができない、サーバ上で見つかる知的財産及び演算データに関係する。
【００１４】
最も価値があるユーザデータ及び企業のデータが暗号化されることを確実にするために、ランサムウェアは、複数のファイルアクセス及び走査アルゴリズムを使用する。ランサムウェアのファイルアクセスアルゴリズムは、バイナリ探索木アルゴリズム等の木走査アルゴリズム及び検出され、停止されることなしに最も多くのデータを暗号化する確率をより高くする方法でそれらの木走査アルゴリズムを実行することの組み合わせで構成される。
【００１５】

ランサムウェアプログラムによるデータの探索及びその後のデータの暗号化は、典型的には、自動化される必要がある。なぜなら、一例では、攻撃者は、自らの暗号化攻撃を多くのマシン及び多くの被害者にわたり、人が手動で管理するには速すぎる速度で実行できなければならないからである。従って、攻撃者は、被害者が大量の価値のあるデータを有する確率に基づいてアルゴリズムを事前設定する必要がある。それらのアルゴリズムは、予測可能であり、数の点で有限である。

【００１６】

最も多くのデータ及び最も価値のあるデータを暗号化することは、価値のあるデータを有する可能性が最も高い、ネットワーク内の位置に暗号化操作の順序がバイアスすることを意味する。例えば、ランサムウェアプログラムは、ユーザとの共有フォルダを有するネットワークサーバを暗号化するように構成することができ、なぜなら、そのサーバは、個人が自分のデスクトップ上に有するよりも業務にとって重要なファイルを有する可能性が最も高く、更に全てのビジネスワークステーションにわたって保存されているファイルの集合体を含むからである。

【００１７】

被害者によって検出され、その後、停止されることなく暗号化することは、被害者にとって価値のあるファイルを最初に暗号化しながら、可能な限り長い時間にわたってユーザ又は管理者によって認識されない暗号化ファイルの優先順位付け等の措置を行うことを意味する。例えば、デスクトップ上のユーザのファイルを暗号化することは、ほぼ確実にサーバよりも少ないファイルを有し、被害者にとっての潜在的価値がより低いことを意味し、暗号化操作がユーザによって直ちに認識される。別の例は、サーバ又はデスクトップの適切な動作に必要なファイルを暗号化することである。オペレーティングシステムのファイルが暗号化されていることを理由にユーザのデスクトップがクラッシュする場合、クラッシュしたシステムが原因でランサムウェアが動作し続けることができないだけでなく、被害者によっても直ちに認識され、その被害者は、更なる暗号化の阻止を試みるために直ちに対策を講じる。

【発明の概要】

【発明が解決しようとする課題】

【００１８】

そのため、ランサムウェア攻撃を検出し、軽減する機能をユーザに与えることが望ましい。従って、本明細書で開示するシステム及び方法は、これら及び他の必要性を解決する。

【課題を解決するための手段】

【００１９】

概要

簡潔には、本発明によれば、ランサムウェア攻撃に対して標的システムの計算装置を保護するためのシステム及び方法は、ファイルを管理するために計算装置のオペレーティングシステムによって使用されるデータ構造を有するファイルシステムを利用する。計算装置におけるソフトウェア又はハードウェアとしてインストールされたエージェントは、標的システムの代わりに１つ又は複数の措置を自律的に行う。エージェントは、ファイリングシステムのデータ構造内に１つ又は複数のトラップファイルを自律的に作成する。トラップファイルは、ファイルであって、それへのアクセスがランサムウェア攻撃の可能性を示す、ファイルである。エージェントは、１つ又は複数のトラップファイルへのアクセスをモニタする。トラップファイルへのアクセスの検出時、ランサムウェア攻撃の可能性に対して標的システムによって是正措置が行われる。

【００２０】

本発明の他の特徴によれば、ファイルシステムのデータ構造は、木構造であり、及びトラップファイルのためのファイルパスは、木構造の最高点において指定される。トラップファイルへのファイルパスは、バイナリ探索木アルゴリズム又は木走査アルゴリズム等の探索木アルゴリズムを使用して指定され得る。木走査アルゴリズムは、深さ優先走査アルゴリズム、幅優先走査アルゴリズム、モンテカルロ木探索アルゴリズム又はランダムサン

プリングアルゴリズムの１つであり得る。深さ優先走査アルゴリズムは、前順アルゴリズム、順序アルゴリズム、逆順アルゴリズム又は後順アルゴリズムの１つであり得る。

【００２１】

本発明の他の詳細によれば、是正措置は、標的システムのユーザに通知すること又はアクセスされたトラップファイルを自動でアップロードすることを含む。是正措置は、識別されたプロセスが隔離されるか、キルされるか又は中断されるかのいずれかであるように、１つ又は複数のトラップファイルにアクセスするプロセスを識別することも含み得る。

【００２２】

図面の簡単な説明

本発明の上記の特徴は、添付図面に関連して解釈される本発明の以下の詳細な説明から明らかになる。

【図面の簡単な説明】

【００２３】

【図１】本開示のシステムを示す図である。

【図２】本開示のソフトウェアエージェント及びハードウェアエージェントのあり得る動作を示す図である。

【図３】本開示のハードウェアエージェントのコンポーネントを示す図である。

【図４】ユーザ装置に対する本開示のハードウェアエージェントの接続の選択肢の一例を示す図である。

【図５】本開示のアーティファクトデータベースに複数のユーザ装置がデータを伝送する一例を示す図である。

【図６】本開示のエージェントによって行われる解析の一例を示す図である。

【図７】ランサムウェア攻撃を検出し、復号器ソリューションを生成／展開するためのステップを示す図である。

【図８】本開示のエージェントに対するユーザライセンスを得るためのステップを示す図である。

【図９】サーバと共にサービス型ソフトウェア（ＳａａＳ）プラットフォームを実装するシステムのブロック図を示す。

【図１０】グループ又はサブグループ内のサービス加入者のための、本発明を実装する図１のシステムのオペレーション層の例示的なブロック図を示す。

【図１１】Admin、マネージャ及び参加者と呼ばれるユーザに指定された役割の階層を示し、Adminユーザ及びマネージャユーザは、読み出し又は書き込み特権を有する一方、参加者ユーザは、読み出し特権のみを有する。

【発明を実施するための形態】

【００２４】

詳細な説明

本発明は、図１～図８に関して以下で詳細に説明する、ランサムウェアの検出及び防御のためのシステム及び方法に関する。

【００２５】

ランサムウェアの挙動検出戦略の一部は、システム上に配置されるモニタされるアーティファクトを使用することである。そのような１つのアーティファクトは、処理ノード若しくはマシン、クライアント、サーバ又は独立型ワークステーションを含む計算装置のオペレーティングシステムによって使用されるファイリングシステム内に配置されるトラップファイルである。トラップファイルへのアクセスは、ランサムウェア攻撃の可能性を示す。ランサムウェア活動及びランサムウェア活動の挙動の両方を非常に高い確率で検出することと、ユーザがアーティファクトに非常に低い確率で遭遇することとを可能にするために、これらのアーティファクトは、位置、コンテンツ及び品質ごとに配置される。

【００２６】

一実施形態では、本発明は、トラップファイルへのアクセスに基づいてランサムウェア攻撃の開始を自動で発見し、攻撃者の暗号化を打ち負かすためのシステム及び方法に関す

る。攻撃者は、攻撃された計算装置が、復号するためにファイルを提出できなくする能力、又はユーザが、感染したシステムと手動で対話することを禁止する能力を得る可能性があるため、別の実施形態では、本発明は、ハードウェアのソリューション及びソフトウェアのソリューションの両方を提供する。

【００２７】

他の実施形態では、本発明は、収集データに対する機械学習技法を使用する暗号解析と組み合わされた、攻撃が起こる直前及び攻撃中に暗号解読技法を使用してユーザの計算装置から収集される標的データの組み合わせを使用し、ランサムウェア攻撃を自動で発見する能力及びランサムウェア攻撃から回復する能力の両方をランサムウェア攻撃の標的に与える。本発明のシステムは、マシン上にインストールされるエージェント及び暗号的にアラインされた解析を行う遠隔サーバを使用する。エージェントは、ソフトウェアベース又はハードウェアベースのモニタリング機能を有し得る。一実施形態では、エージェントは、ランサムウェア攻撃の標的の代わりに様々な措置を自律的に行うソフトウェアコンピュータプログラム又はハードウェアである。

【００２８】

図１は、１０で全体的に示す本開示のシステムを示す図である。システム１０は、ユーザ装置１２、ネットワーク２０、アーティファクトデータベース２２、暗号解析発見サーバ２６及び復号器ビルドサーバ２８を含む。ユーザ装置１２は、パーソナルコンピュータ、デスクトップコンピュータ、タブレットコンピュータ、携帯電話、スマートフォン、ファブレット、埋め込み装置、ウェアラブルデバイス、書換可能ゲートアレイ（「ＦＰＧＡ」）、特定用途向け集積回路（「ＡＳＩＣ」）等の任意の電子装置であり得る。ユーザ装置１２は、ソフトウェアエージェント１４及び／又はハードウェアエージェント１６を含み得る。ユーザ装置１２は、以下でより詳細に論じるエージェントウェブアプリケーション又はエージェントＡＰＩに更に接続することができる。

【００２９】

アーティファクトデータベース２２は、ユーザ装置１２からアーティファクトを受信することができる。一実施形態では、アーティファクトは、ユーザ装置１２上にあるランサムウェアによって生成されるデータ及び／又はテレメトリを含む。暗号解析発見サーバ２６は、ランサムウェアの挙動に焦点を当てた解析を用いてアーティファクトデータベース２２をクエリする１つ又は複数のサーバを含むことができ、暗号的にアラインされた解析を行う解析エンジン２４を実行し得る。復号器ビルドサーバ２８は、ランサムウェアソフトウェアに対処するための復号器ソリューションを生成することができる。これらについては、以下でより詳細に論じる。アーティファクトデータベース２２、暗号解析発見サーバ２６及び復号器ビルドサーバ２８は、単一のハードウェアユニット内又は複数のハードウェアユニット内に実装され得ることに留意されたい。

【００３０】

ユーザ装置１２、アーティファクトデータベース２２、暗号解析発見サーバ２６及び復号器ビルドサーバ２８は、それぞれが互いにデータを送受信することができるようにネットワーク２０に接続され得る。ネットワーク２０は、これのみに限定されないが、旧来の無線アクセスネットワーク（「ＲＡＮ」）、ロングタームエボリューション無線アクセスネットワーク（「ＬＴＥ－ＲＡＮ」）、WiFiネットワーク等の無線ローカルエリアネットワーク（「ＷＬＡＮ」）、イーサネット接続又は通信を支援するために使用される他の任意の種類のネットワークを含む任意の種類の有線ネットワーク又は無線ネットワークであり得る。例えば、ユーザ装置１２は、無線ネットワーク接続（例えば、Bluetooth、WiFi、ＬＴＥ－ＲＡＮ等）によってアーティファクトデータベース２２に接続することができる。暗号解析発見サーバ２６は、解析エンジン２４を実行するために使用される任意の種類のサーバ／データベース／ハードウェアコンポーネントであり得る。代わりに、解析エンジン２４は、クラウド上にあり得る。

【００３１】

ユーザ装置１２がデスクトップ／ラップトップ、サーバ、ＩｏＴ／埋め込み装置、モバ

イル装置、計算装置等であるかどうかにかかわらず、ソフトウェア（例えば、ソフトウェアエージェント１４）又はハードウェア（例えば、ハードウェアエージェント１６）として実装されるエージェントは、ユーザ装置１２上の活動に焦点を当てたデータを収集する。本発明の一実施形態のユーザ装置は、ハードドライブ又はディレクトリ内に実装されるファイリングシステムを使用するオペレーティングシステムを実行する計算装置である。ディレクトリは、ファイルに関係するファイル名及びファイルパスを含む他の情報のリストを含む。エージェントは、ソフトウェアアプリケーション又はハードウェアベースのモニタリング機能として存在し得る。

【００３２】

図２は、ソフトウェアエージェント１４及びハードウェアエージェント１６の動作を示す図である。とりわけ、ソフトウェアエージェント１４及びハードウェアエージェント１６は、エージェントを実行すること／動作させること３２、データベース／サーバ（例えば、アーティファクトデータベース２２、暗号解析発見サーバ２６、復号器ビルドサーバ２８及びクラウド）にアクセスすること３４及びアップロード／ダウンロードするためにファイルにアクセスすること３６を含む動作を実行し得る。

【００３３】

図３は、ユーザ装置１２に内部的又は外部的にインストールし及び／又は取り付けることができるハードウェアエージェント１６のコンポーネントを示す図である。とりわけ、図３は、有線又は無線ネットワーク機能コンポーネント４２、システムメモリアクセス機能コンポーネント４４及びアップロード／アップグレードコンポーネント４６を示す。

【００３４】

図４は、ユーザ装置１２（不図示）へのハードウェアエージェント１６の接続の選択肢の一例を示す図である。とりわけ、（フォームファクタ５２を有する）ハードウェアコンポーネント１６は、内部周辺装置５４（例えば、ＰＣＩ－Ｅカード）、外部周辺装置（例えば、ファイアワイヤ）５６又は集積回路５８（例えば、既存のメインボード上に埋め込まれた集積回路）によってユーザ装置１２に接続され得る。他の接続の選択肢が使用され得ることを当業者であれば理解するであろう。

【００３５】

ユーザ装置１２にインストールされたエージェントは、ランサムウェア攻撃を検出するためにファイルのアクセス活動をモニタし、ランサムウェア活動に関与している高い可能性を有するデータのみを提出するのとは対照的に、ランサムウェア活動に関与している未知の可能性を有するデータを提出することへの強いバイアスを用いて、アーティファクトデータベース２２にデータを提出するかどうかを判定するための解析を行う。論理的根拠は、モニタされる装置上でランサムウェア攻撃が生じたら、攻撃の発見及び復号アルゴリズムの発見の両方に必要なアーティファクトが有用であるために既に収集されていなければならないことである。

【００３６】

一実施形態では、遠隔アーティファクトデータベース２２に提出するために、潜在的な暗号変数のフォレンジックエビデンスを求めてエージェントがユーザ装置１２のメモリ及びファイルをリアルタイムでモニタする。かかる暗号変数は、暗号鍵、復号鍵、初期設定ベクトル又はユーザ装置１２上の暗号操作に関連する他のデータ片であり得る暗号変数を含む。エージェントは、オペレーティングシステムの暗号ＡＰＩ呼び出しの使用について、ユーザ装置１２のオペレーティングシステムを更にモニタする。とりわけ、エージェントは、暗号化に関連する機能及び方法をモニタし、それらの使用によって生成される情報がアーティファクトデータベース２２に伝送される。エージェントは、あるプログラムが複数のファイルに書き込むこと又はファイルを再命名するためのプログラムの再三のアクセス等の解析を含めるために、トラップファイルへのアクセスを含むファイルのアクセスイベントもモニタする。プログラムが読み出し及び書き込みのためにファイルにアクセスする順序は、重要であり、データがアーティファクトデータベース２２に送信される間に保存もされる。

【００３７】
図５は、暗号解析発見サーバ２６と通信するアーティファクトデータベース２２に複数のユーザ装置（例えば、デスクトップ、モバイル装置、サーバ及びＩｏＴ装置）がデータを伝送する一例を示す図である。ランサムウェアの攻撃者は、自らの攻撃と干渉する防御製品を攻撃することができ、ユーザ装置への特権アクセスを得て、システム自体を動作不能にし得ることに留意されたい。即ち、ソフトウェアのソリューションは、ランサムウェアの暗号化及びランサムウェアの暗号化ファイルの自動検出、提出及び復号を適切に可能にしない場合がある。
【００３８】
ハードウェアから厳格に行うことができない潜在的なフォレンジックアーティファクトの幾らかの解析及びモニタリングもある。それにより、システム１０は、ハードウェアのみのバージョン（ハードウェアエージェント１６のみを使用する）及びハードウェアとソフトウェアとの混成バージョン（ソフトウェアエージェント１４及びハードウェアエージェント１６の両方を使用する）であり得る。ハードウェアエージェント１６は、１）オペレーティングシステムと独立に動作し、オペレーティングシステムのファイルが暗号化されているかどうかにかかわらず機能することができ、２）システムメモリ及びＣＰＵの動作への可視性を有することができ、３）オンボードのプログラム可能チップ、内部周辺装置（ＰＣＩ－Ｅカード等）又は外部周辺装置として存在することができ、４）有線又は無線ネットワーク通信を行うことができ、５）アーティファクトデータベース２２にアーティファクトを提出することができ、６）潜在的に暗号化されたファイルを解析のために解析エンジン２４に提出することができ、７）復号ソリューションを受信及び実行することができ、８）ソフトウェアエージェント１４を受信及び実行／ロードすることができる。
【００３９】
エージェントは、（ソフトウェアエージェント１４、ハードウェアエージェント１６又はその両方によって）潜在的に有用な情報を遠隔アーティファクトデータベース２２に継続的に提出する。暗号解析発見サーバ２６は、マシン上で示されることになるランサムウェアソフトの挙動に焦点を当てた解析を用いて、アーティファクトデータベース２２を継続的にクエリする。
【００４０】
図６は、エージェントによって行われる解析の一例を示す図である。とりわけ、この解析は、メモリ操作解析６２、ファイル操作解析６４及び暗号ＡＰＩ操作解析６６を含み得る。メモリ操作解析６２は、メモリに対する前処理ロード／アンロード操作及びメモリに対するエントロピ解析を含む。ファイル操作解析６４は、トラップファイルに適用されるものを含む、ファイルのアクセス挙動、ファイルの開け閉じ挙動及びファイルの再命名挙動を含む。暗号ＡＰＩ操作解析６６は、オペレーティングシステムの鍵生成挙動、オペレーティングシステムの鍵使用挙動及びオペレーティングシステムの暗号化機能挙動を含む。これらについては、本開示の全体を通してより詳細に論じる。
【００４１】
疑わしいランサムウェア攻撃の発見中、システム１０は、発見プロセスを行うことができる。例えば、発見プロセスは、例えば、１）プログラムがディレクトリ内の幾つかのファイルに「.encrypted」拡張子を立て続けに追加すること、２）プログラムがメモリ内で認められる大量の暗号変数を短期間で生成すること、及び／又は３）短時間でのファイルの大量の読み出し及び書き込みを伴う、プログラムが暗号に焦点を当てたオペレーティングシステムの機能に短期間で何度もアクセスすることをシステム１０が明らかにすることを含み得る。
【００４２】
加えて、システム１０は、１）正当な操作について予期されるファイル名の変更に統計的確率を適用し、２）アーティファクトデータベース２２内で認められるファイルシステムの変更に関するエントロピ計算を行い、及び／又は３）暗号マテリアルを生成していること又は暗号操作を使用していることが認められるプログラムに関して、統計的確率を適

用するために機械学習解析を適用することができる。

【００４３】

潜在的なランサムウェア攻撃を識別する機械学習又は他の解析の適用の成功時、システム１０は、是正措置を行うことができる。第１の例では、是正措置は、エージェントによって作成されるトラップファイルを含む、選択された事前配置ファイル又はクライアント暗号化ファイルをエージェントウェブアプリケーション又はエージェントＡＰＩによって暗号化ファイルサーバに手動で提出するようにユーザに通知することを含み得る。第２の例では、是正措置は、エージェントが、トラップファイル等の選択された事前配置ファイル又はトラップファイルを含むクライアント暗号化ファイルを暗号化ファイルサーバに自動でアップロードし、そのアップロードをエージェントウェブアプリケーション又はエージェントＡＰＩに登録することを含み得る。

【００４４】

正しく復号されたファイルを可能な限り効率的に識別するために、提出の受信時、システム１０は、解析エンジン２４によって成功の確率を高める方法で暗号変数、暗号操作及びファイル構成の組み合わせを行うことができる。疑わしい暗号活動のアーティファクトと組み合わせて暗号化ファイルからの入力の暗号解析を行うために、様々な解析サーバが並列分散処理モデル内で動作することができ、実装するための正しい暗号変数を決定するために出力が検査される。

【００４５】

例えば、ランサムウェアの改変形態は、ＡＥＳ暗号化アルゴリズムの「ＡＥＳ　ＣＴＲ」の効率的なファイル暗号化の改変形態を使用して、システム上の全てのファイルを暗号化するためのＡＥＳ２５６バイト暗号鍵をランダムに生成することができ、ＰＫＣＳ７パディングを実装する。これら及び他の様々な暗号変数を活用して、アーティファクトデータベース２２は、メモリから認められる又はシステム上の可能性のある暗号活動内で使用されているあり得る全ての鍵又は部分的な鍵マテリアルを含む。直近に生成された鍵から開始して、解析エンジン２４は、ＡＥＳ　ＣＴＲカウンタ値の暗号変数内の特定の提出ファイルの位置を調べ、確度の高い収集された暗号鍵と共に適用するための最も可能性が高いカウンタ暗号変数を決定する。機械学習アルゴリズムが決定した変数から開始して、これらの変数を使用して復号を試みることは、最も高い成功確率を有するが、システム１０は、復号ファイルの出力を調べることにより、暗号変数の成功裏の組み合わせを見つけることができる。

【００４６】

暗号変数の成功裏の組み合わせを発見することは、エージェントウェブアプリケーション及び又はエージェントＡＰＩに登録される。復号に焦点を当てる他の暗号解析サーバは、これを通知され、トラップファイルであり得るその特定のファイルの検査を止める。加えて、システム１０は、ユーザのための復号器ソリューションを生成するタスクを復号器ビルドサーバ２８に課すことができる。システム１０が、暗号化されたトラップファイルを含む、クライアントによって提出される暗号化ファイルを成功裏に復号する暗号変数の組み合わせを見つけ、復号器ソリューションを生成すると、システム１０は、ユーザ装置１２上で実行される復号器ソリューションを自動で展開することができる。

【００４７】

復号器ソリューションは、別個の独立型ソフトウェア、ソフトウェアエージェント１４による動的ロードソフトウェアモジュール又はハードウェアエージェント１６として実行され得る。復号器ビルドサーバ２８は、復号器ソリューションを構築するためのタスクをリスンすることができ、かかるソリューションは、ファイルを復号し、その元の名前に再命名する順序等の変数に加えて、正しい暗号変数が挿入された状態でオーダーメイドされ得る。

【００４８】

復号器ビルドサーバ２８は、復号器ソリューションを生成すると、ファイルサーバにアップロードし、エージェントウェブアプリケーション及び／又はエージェントＡＰＩにそ

の復号器ソリューションを登録する。そこから、エージェントウェブアプリケーション／エージェントＡＰＩによるユーザ構成ごとに、エージェントウェブアプリケーション／エージェントＡＰＩ内で指定されるマシンにダウンロードするために利用可能な復号機能（例えば、復号器ソリューション）があることをユーザに通知することができる。次いで、ユーザは、復号器ソリューションをダウンロードすることができる。利用可能な復号ソリューションがあることと、その復号ソリューションがユーザ装置１２に自動で展開されていることと、その復号ソリューションが現在復号中であることとをユーザが通知されると、ユーザによる遠隔モニタリングのために復号器ソリューションの状態がエージェントウェブアプリケーション／エージェントＡＰＩによって入手可能である。

【００４９】

図７は、７０で全体的に示す、ランサムウェア攻撃を検出し、復号器ソリューションを生成／展開するための上記で論じたステップを示す図である。ステップ７２では、システム１０は、復号器ソリューションを生成するタスクを復号器ビルドサーバ２８に課す。ステップ７４では、システム１０は、復号器ソリューションをファイルサーバに保存／アップロードする。ステップ７６では、システム１０は、復号器ソリューションをエージェントウェブアプリケーション及び／又はエージェントＡＰＩに登録する。ステップ７８では、システム１０は、ユーザ装置１２に復号器ソリューションを展開する。ステップ８０では、システム１０は、復号器ソリューションの展開をユーザに通知する。

【００５０】

図８は、９０で全体的に示す、エージェントに対するユーザライセンスを得るためのステップを示す図である。ステップ９２では、ユーザは、エージェントを使用するためのライセンスを購入する。ステップ９４では、ユーザは、エージェントへの指定に利用可能なライセンスのリストを受信する。ステップ９６では、ユーザは、１つ又は複数のエージェントに１つ又は複数のライセンスを指定し、ライセンスの構成を選択する。ステップ９８では、ユーザは、ユーザ装置にエージェントをダウンロードする。本明細書で使用するとき、エージェントは、ユーザ又は組織の代わりに様々な措置を継続的及び自律的に行うソフトウェアプログラム又はハードウェアである。例えば、エージェントは、ノード又はマシン内のオペレーティングシステムによって使用されるファイリングシステム内の位置に様々なトラップファイルを配置することができる。ファイルシステムは、ファイルを管理するために計算装置のオペレーティングシステムによって使用されるデータ構造を有する。エージェントは、ランサムウェア攻撃の場合の是正措置を行う前に、トラップファイルへのアクセスをモニタする。トラップファイルは、それへのアクセスがランサムウェア攻撃の可能性を示すファイルである。

【００５１】

図９は、図１に示す暗号解析発見サーバ２６及び復号器ビルドサーバ２８を含むサーバと共にサービス型ソフトウェア（ＳａａＳ）プラットフォームを実装するシステムのブロック図を示す。このシステムは、Ransomware Rewindと呼ばれるソフトウェアシステムを実行し、Ransomware Rewindは、本願の譲受人であるCyber Crucible Inc.により、ランサムウェア活動を検出することによってランサムマルウェアを防ぐために開発及び実装されている。インストールされると、Ransomware Rewindソフトウェアは、サーバ、クライアント、ユーザ装置又はワークステーションを含むシステムの任意のノード内のエージェントとして実行され得る。実行されると、Ransomware Rewindエージェントは、ノードのファイルシステム内にトラップファイルを作成する。ファイルシステムは、ディスク又はパーティション上のファイル、即ちディスク上でファイルが編成される方法を追跡するためにオペレーティングシステムが使用する方法及びデータ構造である。潜在的なランサムウェア攻撃を検出するためにトラップファイルが作成される。トラップファイルへのアクセスは、ランサムウェア攻撃を示す。Ransomware Rewindエージェントは、トラップファイルアクセスへのアクセスをモニタし、本発明による暗号的にアラインされた解析に基づいて、ランサムウェア攻撃に対する是正措置を行う。

【００５２】

ＳａａＳの一実施形態では、Ransomware Rewindソフトウェアシステムは、Amazonメッセージングサービス（ＳＮＳ／ＳＱＳ）又はＨＴＴＰＳ　ＲＥＳＴ　ＡＰＩによって通信が行われるAmazon Web Serviceを使用して実装される。ＳａａＳは、サブスクリプションベースで加入者１、２及び３に対するライセンシング及びエージェント引き渡しサービスも実装し、中央で又は分散してホストされる。

【００５３】

典型的には、本発明が実装されるネットワークは、１つ又は複数のリンク上で情報をやり取りすることを可能にされる１つ又は複数のプロセッサノード、マシン又はサーバ若しくはサーバ群及び又はノードを含む、複数の私的又は公に接続されるノードを含む。例示的なネットワークは、ＷＡＮ、ＬＡＮ、ＰＡＮ、インターネット１２０及びBluetooth又はエクストラネット等のアドホックネットワークの何れか１つ又は複数を含む。ノードは、ネットワーク内の何れかの場所に位置し、情報を処理し、及び／又は暗号解析等の属性機能を実行する１つ又は複数のプロセッサユニット（ソフトウェア若しくはハードウェア又は仮想ノード）及び／又は装置を含む。上記の解析エンジン又はエージェントを実装するために、任意のノード又はノードを有する任意のコンポーネントをハードウェア又はソフトウェアによって仮想化することができる。様々な種類のノードは、情報を受信する受信機ノード、情報を処理するプロセッサノード及び処理済みの情報を伝送する送信機ノードを含み得る。ノードの例は、サーバノード、クライアントノード、コンピュータノード、プロセッサノード、通信ノード、ワークステーション、ＰＤＡ、モバイル装置、センサ等を含む。

【００５４】

例えば、メモリ解析は、暗号操作を検出し、鍵を抽出するためにシステムのノード又はマシン上のプロセスによって実行され、Ransomware Rewindソフトウェアは、装置の活動をモニタするためにユーザ空間及びカーネル空間の両方のライブラリを使用する。ユーザ装置は、個別に又はグループ若しくはサブグループ単位で動作する装置であり得る。システムのノードは、これのみに限定されないが、クライアントサーバモデル及び階層モデル又は分散モデルを含む任意の適切なネットワークモデルに従って互いに接続され得る。リンクは、２つのノードが互いに情報を通信することができる任意の媒体を含む。例示的なリンクは、これのみに限定されないが、有線リンク、ファイバリンク、ケーブルリンク又は無線リンク（例えば、Bluetooth、ＵＷＢ、ＵＳＢ等）を含む。通信チャネルは、コンテンツを配信するためのリンクと共に使用される任意のチャネルを含み、コンテンツは、ノード、ノード若しくは装置内で実行されるアプリケーション又はエージェントから得られるデータを含み得る。

【００５５】

図１０は、グループ又はサブグループ内のサービス加入者に対して本発明を実装する、図１のシステムのオペレーション層の例示的なブロック図を示す。この実施形態によれば、システムは、バックエンドシステム５３０及びフロントエンドシステム５６０を含む。フロントエンドシステム５６０は、加入しているサービスユーザ及び参加者にユーザインタフェースを提供する。バックエンドシステム５３０は、システム管理、課金等に使用される。フロントエンドシステム５６０は、図１に示すアーティファクトデータベース２２等のバックエンドデータベース５４２Ａ及び５４０Ａにアクセスするアプリケーションセンタ５６２へのユーザアクセスを可能にする。フロントエンドシステム５６０は、ユーザ装置５５０及び５５２によるユーザ及びユーザグループセッションへの対話型アクセスを管理者に与える。ユーザは、インターネット１２０を介して又は有線ネットワーク５２４及び／又は無線ネットワーク５２６によってフロントエンドシステム５６０及びバックエンドシステム５３０とインタフェースする。例示的な実施形態では、ユーザ装置は、複数のアクセス制御レベル下で複数の管理者特権レベルの影響下にあり得る定義済みのアクセス特権に応じて、バックエンドシステム５３０又はフロントエンド５６０にアクセスするために、ネットワークアクセスアプリケーション、例えば、これのみに限定されないが、ブラウザ又は他の任意の適切なアプリケーション若しくはアプレットを実行する。ユーザ

５１０、５５２又は５５０は、システムに入る前に、ログインセッション及び複数レベルの認証を経ることを要求され得る。

【００５６】

図１０に示す例示的な実施形態では、バックエンドシステム５３０は、１つ又は複数のロードバランサ５３４Ａ、５３４Ｂに結合されるファイアウォール５３２を含む。更に、ロードバランサ５３４Ａ～Ｂは、１つ又は複数のウェブサーバ５３６Ａ～Ｂに結合される。ウェブサーバ５３６Ａ～Ｂは、そのそれぞれが１つ又は複数のデータベース５４０、５４２を含み、及び／又はかかるデータベースにアクセスする１つ又は複数のアプリケーションサーバ５３８Ａ～Ｃに結合され、データベース５４０、５４２は、暗号マテリアル及びアーティファクトを記憶する中央データベース又は分散データベースであり得る。

【００５７】

ロードバランサ５３４Ａ～Ｂに結合されるウェブサーバ５３６Ａ～Ｂは、加入者、参加者、ユーザ、マネージャ又は管理者の要求をアプリケーションサーバ５３８Ａ～Ｃの１つ又は複数に転送することにより、最適なオンラインセッション性能をもたらすための負荷平衡機能を実行する。アプリケーションサーバ５３８Ａ～Ｃは、１つ又は複数のデータベース５４０、５４２へのアクセスを管理するデータベース管理システム（ＤＢＭＳ）５４６及び／又はファイルサーバ５４８を含み得る。図１０に示す例示的な実施形態では、アプリケーションサーバ５３８Ａ及び／又は５３８Ｂは、電子インタフェース、アプリケーションマテリアル、参加者プロファイル等を含むアプリケーションを参加者５０６、５１０、５５２に与える。

【００５８】

中央データベース又は分散データベース５４０、５４２は、とりわけ、ユーザ装置に送ることができるアーティファクトデータ及びアプリケーションマテリアルを記憶する。データベース５４０、５４２は、様々な種類の参加者、管理者、マネージャ、ユーザグループ、ユーザプロファイル、課金情報、スケジュール、統計データ、進捗データ、ユーザ属性、参加者属性に関係又は関連する取出し可能情報も記憶する。本発明のシステムを動作させることに関連する所望の目的を達成するために、必要に応じて、上記のデータ、例えば条件、タスク、スケジュール等に関係するデータの何れか又は全てを処理し、関連付けることができる。

【００５９】

１つ又は複数のオペレーティングシステムの制御下にある１つ又は複数のノード内で実行されるRansomware Rewindは、複数の方法を使用してディレクトリ及びドライブ内のトラップファイルへのパスを決定する。Ransomware Rewindは、バイナリ探索木及び木走査等の探索木アルゴリズムを使用して、配置されたトラップファイルのファイルパスを指定する。木走査は、ツリーデータ構造内の各ノードを訪ねるプロセスである。この走査は、ノードが攻撃のためにアクセスされる順序によって分類される。ディレクトリ及びドライブが選択され、それらは、通常のオペレーティングシステムの動作中にユーザ及びプログラムによって使用するためにノードにとってローカルであり得る。ノードが複数のユーザを有する場合、トラップファイルの位置は、管理ユーザ、マネジメントユーザ及びシステムユーザを含む、システム上のあり得る全てのユーザを含む。ファイルシステムがオペレーティングシステム内のマルチツリー階層として組織化されることを所与とし、識別される位置は、ファイルシステム内の最高レベルのツリー点にある。

【００６０】

最高レベルのツリー点をツリーごとに選択した後、「トラップファイル」へのファイルパスを決定する。トラップファイルは、トラップファイルのランサムウェア攻撃者を罠でとらえるために決定されるファイルパスに基づいて記憶される。一実施形態では、トラップファイルのパスを決定するためのアルゴリズムは、深さ優先走査（前順、順序、逆順及び後順）アルゴリズム、幅優先走査アルゴリズム、モンテカルロ木探索アルゴリズム及びランダムサンプリングアルゴリズムの両方を含む木走査アルゴリズムを使用する。アルゴリズムは、ソート方法と組み合わされ、それらの木走査挙動内でのトラップファイルへの

アクセス順序を明らかにするために自動ファイル及びディレクトリ探索アルゴリズムが使用される。例えば、ファイルのサイズ、ファイル名、ファイルの種類及びファイルの作成日又は最終編集日を全て使用することができる。

【００６１】

例えば、システム全体にわたるトラップファイルへのパスは、木走査アルゴリズム及びアクセスのソート／順序アルゴリズムを使用して決定される。何れのソートアルゴリズム、探索／走査アルゴリズム、ファイルの種類又はファイル属性の優先順位付けアルゴリズムが使用されても、Ransomware Rewindがインストールされたトラップファイルがランサムウェア攻撃に含まれるだけでなく、攻撃のためにアクセスされる最初のトラップファイル又は最初のトラップファイルの１つになる確率が非常に高くなる可能性を最大化するために、トラップファイルの名前及び属性テーブルを作成する。

【００６２】

トラップファイルの命名、トラップファイルのパス、トラップファイルのコンテンツ及びトラップファイルの属性は、疑似ランダムアルゴリズムを使用して調節される。この疑似ランダムアルゴリズムは、何れのソフトウェアインストールが変数を作成したかにかかわらず、トラップファイルに関連する全ての変数が、攻撃者によって自動で検出され、無視されることが不可能であるが、全てのRansomware Rewindソフトウェアによって識別可能であるように設計される。

【００６３】

トラップファイルアーティファクトは、ユーザのビューから隠され、殆どのものは、ユーザが自らのプログラムの通常使用中にかかわらずアクセスしない位置にある。管理者は、特権アカウントアクセスを使用しながら、システム及びサーバの保守活動中にトラップファイルアーティファクトを確認することができる。全てのトラップファイルアーティファクトは、Ransomware Rewindデータベース内にカタログ化され、Ransomware Rewind管理ポータルによる識別のために利用可能である。

【００６４】

Ransomware Rewindがインストールされたシステム上で新たなあり得る装置又はディレクトリが作成されるか又は利用可能になると、防御モニタリングが行われていることを確実にするために、Ransomware Rewindソフトウェアは、必要に応じて、そのドライブ又はディレクトリのための追加のトラップファイルアーティファクトを自動で作成する。ローカルであるか又は遠隔であるかを問わず、且つドライブ名又はマウント点が利用可能資源に関連しているか又はしていないかを問わず、Ransomware Rewindソフトウェアは、インストール及び動作中、システムにとって利用可能にされたファイル資源をモニタする。

【００６５】

集中型の業務拠点内に記憶されるデータ量のため、ネットワーク資源は、多くの場合、攻撃者及び被害者の両方にとってより貴重であるが、業務のために複数の従業員又はプログラムによって使用される各データ片もより重要である可能性が高い。ネットワーク資源のモニタリングは、Ransomware Rewindがインストールされた全てのクライアント及びサーバによって行われる。これは、ネットワーク資源自体を感染させる攻撃者又はネットワークサーバにアクセスする接続クライアントによるネットワーク資源のアクセスがモニタされることを確実にするためである。いかなる個別クライアントも資源上にあること又は資源に接続されることは、考えられないため、共有資源へのアクセスを有する全てのソフトウェアインストールが全て同時にモニタする。

【００６６】

あり得る全てのクライアントが所与の時点において共有資源をモニタしている状態で、共有資源のトラップファイルアーティファクトの対話時、セキュリティマネージャは、接続されている全てのRansomware Rewindソフトウェアインストールからオンラインで警告を受信する。この形態は、場合により、数千件以上のインシデントがセキュリティマネージャに警告されることを招くことになる。攻撃者のアクションによって若しくは別の理

由から共有資源のRansomware Rewindモニタリングが有効にされていない場合、又はトラップファイルにアクセスしているクライアントがRansomware Rewindソフトウェアをインストールしていない場合、複数のクライアントが感染し、共有資源上のトラップファイルアーティファクトにアクセスしようと試みているシナリオにもかかわらず、セキュリティマネージャに最小数の警告が送信されることを確実にするためのアルゴリズムが使用される。

【００６７】

現代のランサムウェアがファイルを暗号化する速度のため、共有ネットワーク資源用の警告報告アルゴリズムは、ミリ秒までの低遅延を有することが好ましい。即ち、例えばトラップファイルをインストールしたクライアント等の現在オフラインのクライアントが、将来のある時点で共有資源に再接続するのを待つか又は他のモニタリングクライアントによって通知されるのを待つ遅延は、存在し得ない。警告報告アルゴリズムは、任意の所与の瞬間において、モニタリングクライアントの何パーセントがローカル及び共有トラップファイルアーティファクトを現在モニタしているかに関係なく機能する。

【００６８】

何れのノードが感染したかをセキュリティマネージャが知るために、且つ感染したノードのみに対する自動又は手動応答を可能にするために、警告報告アルゴリズムは、共有資源のトラップファイルにアクティブに関与している、Ransomware Rewindソフトウェアがインストールされたクライアントのみが警告されるべきであるようにも機能しなければならない。

【００６９】

警告報告アルゴリズムは、共有資源のトラップファイルにアクセスしているクライアントがRansomware Rewindソフトウェアをインストール又は有効化していない場合、アクセスしているクライアントを識別する警告が警告内に含まれるようにも機能しなければならない。

【００７０】

Ransomware Rewindソフトウェアを有する全てのクライアントによって共有資源のトラップファイルのモニタリングが維持されるが、トラップファイルに直接アクセスしており、自動又は手動是正の選択肢を警告及び提供するノードのみが警告していることを確実にするために、アルゴリズムは、共有資源又は遠隔トラップファイルとの対話を示すオペレーティングシステムＡＰＩ、例えばウィンドウズファイルアクセスドライバＡＰＩの活動を使用する。

【００７１】

Ransomware Rewindソフトウェアが有効にされていないクライアントによって現在アクセスされている共有資源のトラップファイルアーティファクトのモニタリングを確実にするか、又はトラップファイルアーティファクトが共有資源サーバ自体からローカルにインストールされている場合、Ransomware Rewindソフトウェアが共有資源サーバ上にインストールされ、共有トラップファイルに遠隔的にアクセスしているクライアントから生成される警告に加え、サーバ上のローカルにアクセスされるトラップファイルに関して警告が生成される。生成される警告に基づき、セキュリティマネージャは、Ransomware Rewindソフトウェアがインストールされていないクライアントがファイルサーバにアクセスしているかどうかを確認する能力を有する。トラップファイルアクセスのソースを詳述するこの情報は、サーバ上のトラップファイルアクセス操作についてのオペレーティングシステムＡＰＩ呼び出しのモニタリングを使用して収集される。

【００７２】

警告は、トラップファイルアーティファクトのアクセス時点において共有資源クライアントの何パーセントがオンラインであるかに関係なく生成される。クライアント及びサーバを有する全てのRansomware Rewindインストールが、全て被害者に警告してはならないか又は全て反応してはならないことを確実にするために、アルゴリズムが使用される。代わりに、そのオペレーティングシステムが攻撃を検出するノード又はワークステーショ

ンのみが警告を送信する。２つのマシンのみが関与する場合、潜在的なトラップファイル活動の最大で２つの警告があり得、それは、即ち、Ransomware Rewindがインストールされた共有資源装置及び共有ネットワーク資源上のトラップファイルに現在アクセスしているクライアントである。

【００７３】

共有資源マシンの場合、トラップファイルは、そのマシンにとってローカルである。サーバ上のRansomware Rewindソフトウェアは、トラップファイルアクセス及び何れの遠隔クライアントがファイルトラップに現在アクセスしているかを報告する。これは、リモートクライアントがRansomware Rewindソフトウェアを現在インストール又は実行していない場合である。

【００７４】

クライアントの場合、何れのトラップファイルがアクセスされているかをクライアントの全てがウィンドウズファイルアクセスドライバＡＰＩによってモニタしている。アクセスを観測可能なあり得る全てのクライアントではなく、トラップファイルに直接アクセスするクライアントのみが潜在的なランサムウェア活動の警告を出す。

【００７５】

サーバのモニタリングとクライアントのモニタリングとの両方を組み合わせることにより、直接暗号化するか又は暗号化した関連クライアント及びサーバのみに関する警告が示されるが、少なくとも１つのマシンがRansomware Rewindをインストールしている場合、少なくとも１つの警告が示される。

【００７６】

一実施形態では、疑似ランダム生成されるトラップファイル内でステガノグラフィが使用される。トラップファイルのコンテンツは、Ransomware Rewindソフトウェアにとって可視的なトラップファイル間で同一であり得ず、システム上の異なるRansomware Rewindインストール間で同一であり得ない。これは、サイバー攻撃中にトラップファイルが盗まれていることが発見される場合に一意性を与え、且つ攻撃者がトラップファイルをとりわけ自動で認識し、トラップファイルの対話（暗号化等）に関して回避するか又は異なって挙動することを防ぐためである。

【００７７】

トラップファイルのコンテンツは、トラップファイルとRansomware Rewindサーバとの間で往復して伝える必要なしに、Ransomware Rewindサーバによって知られる必要もある。なぜなら、たとえ顧客の措置又は攻撃者の窃盗によってトラップファイルが発見されても、改竄を追跡するためだけでなく、トラップファイルが暗号化された場合にRansomware Rewindサーバの復号機能による成功裏の復号を実証するためにも、知られている平文トラップファイルが必要であるためである。

【００７８】

Ransomware Rewindサーバ及び全てのソフトウェアの両方が一意のトラップファイルのコンテンツを追跡することを確実にするために、攻撃者のアクション前にトラップファイルを伝送する必要なしに、Ransomware Rewindサーバ上でファイルコンテンツを再構築することを可能にする、それぞれのための共有及びネゴシエートされたシードを使用可能なアルゴリズムに基づく疑似ランダムトラップファイルコンテンツ生成アルゴリズムが使用される。この自動生成は、真正なテキスト及び画像コンテンツを有するＰＤＦ等の適切なコンテンツを有する正当なファイルをもたらし、かかるファイルは、適切なツール（Adobe PDF Reader等）により、そのアプリケーションによって閲覧される場合に適切にレンダリングされる。

【００７９】

更に、トラップファイルに追加されるのは、データ窃盗の場合に個々のトラップファイルをそのソースまで遡るためのノード、又はクライアント、又はマシン、ファイルの位置及びRansomware Rewindソフトウェアインストールの一意識別子の詳細である。この詳細は、後のフォレンジック解析に有用な環境情報も捕捉する。この詳細は、暗号化され、

利用可能な現代のステガノグラフィ技法の選択を使用してトラップファイル内に符号化される。特定の技法及び暗号鍵がトラップファイルとRansomware Rewindデータベースとの間で共有される。

【００８０】

本発明は、正当なトラップファイルアクセスとランサムウェアとを区別する。正当なファイルアクセスが行われることは、常にあり得る。ランサムウェアではない対話を自動で除外することと、警告中に収集した情報に基づいて自動化の例外又は攻撃の確認をユーザが作成できるようにすることとの両方のためのステップが講じられる。ファイルトラップとの対話に関する観測の組み合わせを使用し、無視、警告又は自動応答するための信頼スコアをもたらす。異なる観測は、攻撃の信頼性が低いことを示す。自動応答のための観測は、以下を含む：

・隠されている、アクセスするために管理者特権を必要とするか、又は通常の業務活動に関連しない位置にあるファイルの読み出し、書き込み又は複製アクセス、

・トラップファイルのコンテンツの変更、

・既知のコンテンツがコンテンツエントロピ面で劇的に増加するトラップファイルのコンテンツの警告。エントロピが高いことは、ランサムウェア内で使用されるようなロバストな暗号化を示す。エントロピの低下は、ランサムウェアプロトコル内で認められることがある、攻撃者によって使用されるランサムウェア追跡識別子と共に暗号化コンテンツをプリペンドするためのファイルコンテンツの変化を示し得る。

・サイズ、アクセス日、作成日、許可、所有ユーザ又はファイル名を含むファイル属性の警告、

・適切に署名され、オペレーティングシステムによって検証された実行ファイル、システム特権等の非常に高い許可を有するプログラム、オペレーティングシステムの保護部分へのアクセスをRansomware Rewindが認めたプログラム又は攻撃者によって潜在的に攻撃及びハイジャック（プロセスハロウイング、プロセスインジェクション）されているとRansomware Rewindが認めたプログラム等のプログラム特性のアクセス、

・多くのファイルに同時にアクセスしようと試みているプログラム。

【００８１】

Ransomware Rewindソフトウェアは、所定の方法で常に又は時刻等の設定パラメータに従って自動で反応するか、又は所望の応答に関してユーザに通知し、ユーザを促すように構成可能である。Ransomware Rewindソフトウェアは、マシンが警告しているマシン情報を含む、特定のアーティファクトと対話しているプログラムに関するプロセスのパスの詳細、属性、許可及び関連する解析の詳細を通知中にユーザに与える。Ransomware Rewindソフトウェアは、ユーザによる対話なしの自動化された又はユーザがあり得るランサムウェア活動を確認した後に手動で複数の応答を与えるように構成可能である。

【００８２】

ユーザのエージェントによって生成されている潜在的なセキュリティインシデントに応答するために、ユーザは、ランサム攻撃の可能性に対する是正措置を含む特定の措置を講じるタスクをエージェントに課すことができる。何れのプロセスに措置を講じるかを知るために、タスクは、ＰＩＤ及び／又は実行ファイルのパスを含む。タスクは、特定の時間枠に基づいて又はエージェントの環境のイベントに応答して自動で生じるようにスケジューリングすることができる。これらのタスクの措置は、潜在的なランサムウェア攻撃のフラグが立てられている特定のプロセスをどのように処理又は是正するかをシステムが決めている方法である。潜在的なランサムウェア攻撃を是正するために、エージェントは、プロセス識別子（ＰＩＤ）又は実行ファイルのパスによって所与のプロセスを無視、隔離、（セーフ及びアンセーフ）キル又は（セーフ及びアンセーフ）中断するタスクを課され得る。

【００８３】

隔離すべきプロセスに関してサービスからメッセージが受信されると、そのプロセスのＩＤは、ドライバによってのみ見ることができる内部テーブルに追加され、そのプロセス

のためにハンドルが取得される。隔離プロセスがファイルシステム資源のハンドルの取得中に検査される場合、隔離すべきプロセスＩＤが、ブロックすべき同じプロセスであることを確かめるために、ドライバは、隔離プロセスへの自らのハンドルを使用する。隔離プロセスが除去されると、その古いプロセスＩＤが隔離プロセスのリストから解放され、そのため、隔離するための古い要求の影響を新たなプロセスが受けることはない。

【００８４】

共有資源上のあり得る全てのファイルの自動バックアップ等により、セキュリティマネージャは、Ransomware Rewindソフトウェアがインストールされたトラップファイルアーティファクトへの正当なアクセスを確認することができる。特定のプログラムが特定のマシン上のトラップファイルアーティファクトにアクセスするとき、警告を受信することをセキュリティマネージャが望まない場合があるか、又はセキュリティマネージャは、警告を受信するが、自動応答を行わないことを望む場合がある。警告は、インシデントに現在関連しているプログラムのファイルパス及びシステム位置をセキュリティマネージャに知らせる。セキュリティマネージャは、１回限りの又は永続的なホワイトリストエントリと呼ばれる、将来の警告について警告を無視するか又はそのプログラムを自動是正から除外するための１回限りの又は永続的なタスクを記録することができる。セキュリティマネージャユーザは、クライアント組織内の将来の監査のために記録される。

【００８５】

Ransomware Rewindクライアントのセキュリティマネージャによって行われるようなホワイトリスト化に部分的に応答して、攻撃者は、自らの代わりに信頼されたアプリケーションにタスクを行わせるために正当なビジネスアプリケーションも攻撃する。攻撃者が望む既存の実行アプリケーションに追加機能を加える複数の攻撃が攻撃者及び防衛者に知られており、確立されている。例えば、この無料プログラムは、追加機能を加え、既存の実行プログラムを支配する４種類のソースコードを含み、攻撃者がダウンロードしカスタマイズするために提供されている：https://github.com/3xpl01tc0d3r/ProcessInjection。

【００８６】

Ransomware Rewindの検出及び応答は、攻撃者によってハイジャックされている正当なプログラムがその既知のプログラムをインシデント内で報告する場合に警告する。Ransomware Rewindは、このようなプログラム攻撃をモニタし、トラップファイルアーティファクトにアクセスするこの種の攻撃をプログラムが過去に経験している場合、警告中にそれをセキュリティマネージャに報告する。

【００８７】

セキュリティマネージャがプログラムをホワイトリスト化している場合、たとえプログラムが信頼されていても、警告は、依然としてRansomware Rewindインシデントデータベース内に記録され、セキュリティマネージャが後日確認するために提供される。その場合、セキュリティマネージャは、そのアプリケーションがインシデント時にファイルトラップアーティファクトにアクセスしているべきかどうかに関して、Ransomware Rewindによっても行われるそれらの評価に情報提供することを促進するために自らの業務の知識を使用すべきである。

【００８８】

タスクは、任意の統合アプリケーション、ウェブアプリケーション又はモバイルアプリケーションから作成することができ、エージェントは、新たなタスクのためにＲＥＳＴ　ＡＰＩを用いて周期的に、例えば１分間に１回、構成可能に「チェックイン」する。エージェントは、プロセス情報及び講じる措置を含む任意の未解決タスクに関する情報を受信する。タスクの完了後、エージェントは、ＲＥＳＴ　ＡＰＩを呼び出して特定のタスクの完了を印付けし、疑わしいプロセスに関して得た任意の新たな情報を報告する。タスクは、エージェントに手動で提出することができるか、又は自動でスケジュールすることができる。スケジュールされるタスク応答は、時間及び反復間隔を与えられ得る。所与のユーザ又はグループに関するスケジュールされた間隔中、疑わしいと判定される該当する任意

のホワイトリスト化されていないプロセスがスケジュールに基づいて自動で処理される。この形態は、自動的な措置が、営業時間外、休日中又は誰かが自分の管理パネルに直ちにチェックインし、プロセスに対する措置を講じることを決めることができない可能性がある任意のときに行われることを可能にする。タスクは、セキュリティインシデントへの応答としてウェブアプリケーション又はモバイルアプリケーションからＲＥＳＴ　ＡＰＩに送信される。タスクは、特定の事例において何を行うかをエージェントソフトウェアに知らせる役割を果たす。今後も増えていくが、タスクは、現在、以下の措置、即ち隔離、セーフ中断（フリーズ）、セーフキル、アンセーフ中断（フリーズ）又はアンセーフキルを行うことができる。エージェントは、タスキングのために頻繁に、例えば１分毎にＡＰＩを用いてチェックインする。

【００８９】

ユーザは、選択されたグループに関連するエージェントに、自らの装置に対する潜在的脅威が発生した場合にどのように応答するかを自動で知らせるためにスケジュールを作成することができる。スケジュールを作成する際、ユーザは、柔軟な任意のスケジューリング構成内で開始時点及び終了時点にわたる開始日及び終了日を選択する。繰り返しの選択肢は、毎日、毎週、毎月繰り返すように又は一度も繰り返さないようにその自動化を設定する能力をユーザに与える。この自動化したスケジュールを関連付けるために、ユーザは、自らがメンバであるグループの１つからグループを選択する。ユーザは、プロセスを隔離、セーフ中断、セーフキル、アンセーフ中断及びアンセーフキルするための選択肢を含む、スケジュールに関連付けるタスクを選択することができる。ユーザは、現在のユーザがメンバである任意のグループに関連する既存の全てのスケジュールを含むグリッドを見ることができる。グリッドは、スケジュールに関する有用な情報をユーザに示す。一実施形態では、ユーザは、システムにアクセスして、所与のスケジュールが何れのグループの一部であるかを知ることができる。別の実施形態では、ユーザは、選択された繰り返しパターン、スケジュールが開始し、終了する日付及びスケジュールについて自動化するための選択されたタスクにアクセスすることができる。ユーザは、自動化されたスケジュールを削除するか又はスケジュールを編集する選択肢も有する。疑わしいプロセスにどのように応答するかを自動で決定するために、エージェントは、これらのスケジュールを使用する。

【００９０】

更に別の実施形態では、役割ベースのセキュリティがＳａａＳプラットフォームにわたって適用される。図１１は、Admin、マネージャ及び参加者と呼ばれるユーザに指定された役割の階層を示し、Adminユーザ及びマネージャユーザは、読み出し又は書き込み特権を有する一方、参加者ユーザは、読み出し特権のみを有する。ユーザは、自らのグループ内の他のユーザを管理するために、１つ又は複数のグループ内で役割を指定され得る。グループのメンバであり、十分な特権を有するユーザは、グループのための役割を役割に命名することによって識別することができる。十分な特権を有するユーザは、権利、その役割を選択するか又はそれにアクセスすることができる。例えば、「グループマネージャ」になる役割をユーザに指定することができ、この役割は、そのユーザがグループにユーザを追加すること及びグループからユーザを除去することと、そのグループ内のユーザに役割を指定することとを可能にする。一実施形態では、グループマネージャの役割に属する列挙された全ての許可及び特権を明らかにする「グループマネージャ」チェックボックスを選択するための選択肢をシステムが与える。

【００９１】

グループ又はサブグループ内のユーザに指定される他の役割は、「応答自動化マネージャ」又は「インシデントマネージャ」であり得る。応答自動化マネージャの役割は、役割に指定されたユーザが自動化されたスケジュールを作成すること、スケジュールを編集すること又はスケジュールを削除することを可能にする。インシデントマネージャの役割は、インシデントを無視すること又はキルすること等、インシデントをどのように管理することを望むかをユーザが決定することを可能にする。タスキング並びに自動化された応答

及び是正機能を行う権利は、グループマネージャによって付与される。

【００９２】

グループマネージャは、グループを選択し、カスタム役割を作成することができる。グループマネージャによって許可される場合、そのようなカスタム役割は、グループのために作成を行うアクセス特権を有するユーザによって作成され得る。それらのユーザも、各役割及び自らがメンバであるグループとの各役割の関連付けを見る能力を有する。これらの役割は、特権ユーザが編集又は削除することができるグリッドインタフェース内に表示される。この場合にもやはり、付与された許可を有するユーザのみが役割を編集又は削除することができる。

【００９３】

グループを管理するために、許可を有する特権ユーザは、自らが属するグループに他のユーザを追加することができる。例えば、グループマネージャは、ユーザを追加するためのグループを、そのグループにユーザを追加する許可を被選択グループ内で有する場合に選択することができる。特権を有するユーザは、グループへの追加時に別のユーザを登録することができ、その新たなユーザは、被選択グループに自動で追加される。グループ管理ウェブページがグループのそれぞれ及びそのメンバを表示する。ユーザは、参加している同じグループ内の他のユーザのメンバシップがどのようなものであるかを見ることもできる。更に、グループマネージャは、特定のグループからユーザを除去するか、又はそのグループのために作られた一定の役割をユーザに指定する選択肢を有する。グループ内でユーザが誰でも役割を除去又は指定することがないように、セキュリティチェックが行われる。ユーザは、グループに関連する役割の一覧に対してそのグループを列挙するマップを有する。ユーザは、同じグループに関して複数の役割を指定され得、自らがメンバである任意のグループにわたって複数の役割を指定され得る。役割が削除される場合、その役割が指定されている全てのユーザのマップからその役割が削除される。

【００９４】

プログラムの暗号化を阻止することを含む、ファイルの暗号化に干渉することは、典型的には、破損ファイルの原因となる。ランサムウェアを含む現代のプログラムによく見られるプログラムが複数のファイルを同時に暗号化する場合、暗号化途中の全てのファイルが破損する。ランサムウェアのサンプルは、暗号化するために一度に５０個ものファイルを開くことが認められており、ランサムウェアを暗号化の途中で中止することは、この例では、５０個の破損ファイルを生じさせることを意味する。

【００９５】

Ransomware Rewindソフトウェアは、オペレーティングシステムのセキュリティトークンを調節することにより、実行中のプロセスが書き込むための追加のファイルにアクセスする許可を自動で又はユーザ介入によって除去する。プロセスのためのオペレーティングシステムのセキュリティトークンは、オペレーティングシステムがプロセスの措置を許可するか又は許可しないための手段である。オペレーティングシステムは、オペレーティングシステムＡＰＩ呼び出しを行う前にプロセスのセキュリティトークンを確認するため、この隔離応答は、ほぼ瞬時であり、そのうちのファイルアクセス操作は、オペレーティングシステムの許可のコンテキスト内で機能する。

【００９６】

プロセスに対するRansomware Rewindソフトウェアによる中断応答は、プロセスを中断するために、プロセスに関する全ての操作及びメモリをフリーズするオペレーティングシステムのメモリ及びプロセス管理カーネルＡＰＩ呼び出しを活用する。このようにプロセスを中断することは、プロセスが行っている全ての活動を停止するが、Ransomware Rewindの応答時にプロセスがあった状態を維持する。

【００９７】

Ransomware Rewindソフトウェアによる中断が生じると、全てのプロセス機能の列挙、メモリ状態の捕捉、悪意ある活動の挙動上のインジケータ又は侵害インジケータ（ＩＯＣ）に関するプロセスの調査並びに暗号化の挙動及び暗号変数を探すためのメモリ上の暗

号挙動解析の実行を含むように、新規及び非新規のフォレンジックメモリ及びプロセス解析が中断プロセスに対して実行される。

【００９８】

必要に応じて、ユーザは、中断したプロセスの動作を、Ransomware Rewindソフトウェアにより、同じオペレーティングシステムの中断／中断解除ＡＰＩ呼び出しによって再開することができる。これは、システム及びネットワークが保護され、インシデント応答又はフォレンジック活動中に更なる悪意ある挙動又は解析が望まれた後に望まれ得る。これは、正当なプロセスが警告される場合にも有用であり得る。

【００９９】

ユーザは、Ransomware Rewindソフトウェアによってプロセスを自動で又はユーザコマンドによってキルすることもできる。これは、オペレーティングシステムのプロセス実行及び終了ＡＰＩ呼び出しを使用する。

【０１００】

Ransomware Rewindソフトウェアは、隔離、中断又はキルの実行を可能にする。「セーフ中断」及び「セーフキル」機能は、暗号化途中のファイルのファイル破損をなくすために、隔離、中断又はキル及び１つの追加機能を組み合わせる。攻撃者は、ファイルを暗号化する前にバックアップを概して削除又は暗号化し、及びバックアップは、典型的には、不完全であるため、復号を可能にするためにファイルを不要に破損させることは、回避すべきである。Ransomware Rewindソフトウェアは、隔離又は隔離を活用する任意の組み合わせコマンドの実行時、オペレーティングシステムのファイルアクセスＡＰＩを使用して現在書き込まれているファイルをモニタする。そのプロセスのための全てのファイルが完全に暗号化された後、ユーザデータの暗号化が阻止されない場合のシナリオでは、Ransomware Rewindがセキュリティマネージャに状態を報告し、必要に応じてプログラムを自動で中断又はキルし続ける。隔離を使用し、進行中の任意の暗号化の完了を必要に応じて待ち、任意の暗号化ファイルの復号が可能である。

【０１０１】

Ransomware Rewindソフトウェアによってアンセーフ中断又はキルが可能であり、これらの操作では、プロセスを中断又はキルする前に隔離することも、又は既存のファイル暗号化活動が行われるのを待つことも遂行されない。

【０１０２】

管理ウェブページによる本発明の実装は、Ransomware Rewindソフトウェアシステムによって以下を生成する：

・エージェント管理ページ

〇このページは、現在のユーザがその一部であるグループＩｄに関連する全てのエージェントを列挙するグリッドを含む。グリッド上のカラムは、各エージェントに関する情報を示す。グリッド上では、低～極限の一様でないエージェントのスキャン速度を変更する選択肢があり、カーネルを真又は偽としてモニタするためのエージェントを設定する選択肢がある。存在する場合、トラップファイルのパスを示すエージェントグリッドのサブグリッドがある。更に、このページ上には、エージェントをダウンロードする選択肢をユーザに与えるダウンローダボタンがある。

・復号器管理ページ

〇このページは、現在のユーザがその一部であるグループごとに購入されている復号器をユーザが見ることを可能にする。復号器ごとの情報がページのグリッド上に表示され、ユーザは、各復号器をダウンロードする選択肢も有する。

・暗号化ファイル提出／ソリューションダウンロードページ

〇暗号化ファイル提出ページは、暗号化ファイルを提出し、そのファイルを復号するエージェントを選択する機能をユーザに与える。

〇ユーザは、このアップロード済みファイルのためのソリューションをソリューションダウンロードページ内で見ることができる。アップロードファイルのためのソリューションを示すグリッドがこのページ上にある。ユーザは、暗号化ファイルをダウンロードし、

復号サンプルをダウンロードするか、又はアップロードファイルのためのソリューションをダウンロードすることができる。

・セキュリティインシデントページ

〇このページは、現在のユーザがメンバである任意のグループＩｄに関連する、特定のインシデントの状態を含む任意のセキュリティインシデントのグリッドをユーザが見ることを可能にする。

〇ユーザは、グリッドの詳細におけるインシデントに関する更なる情報を見ることもできる。ユーザは、インシデントを却下、隔離、中断又はキルすること等のタスクをインシデントに指定する選択肢も有する。ユーザは、必要に応じてインシデントを無視する選択肢も有する。

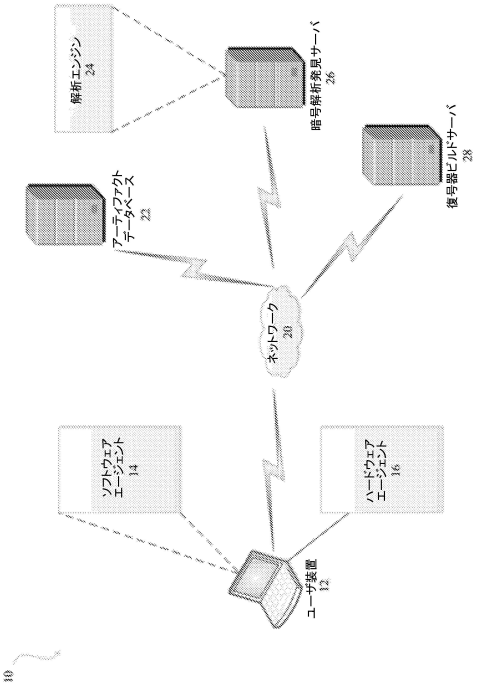
〇インシデントの管理については、タスキング及び自動応答及び是正の節を更に参照されたい。

【０１０３】

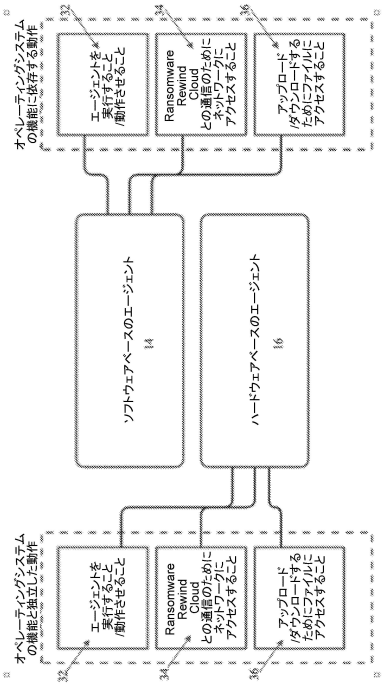
このように本システム及び方法を詳細に記載してきたが、上記の説明は、その趣旨及び範囲を限定することを意図しないことを理解すべきである。本明細書に記載した本開示の実施形態は、例示に過ぎず、当業者は、本開示の趣旨及び範囲から逸脱することなく任意の改変形態及び修正形態がなされ得ることを理解するであろう。上記で論じたものを含むそのような全ての改変形態及び修正形態は、本開示の範囲に含まれることを意図する。

【図面】

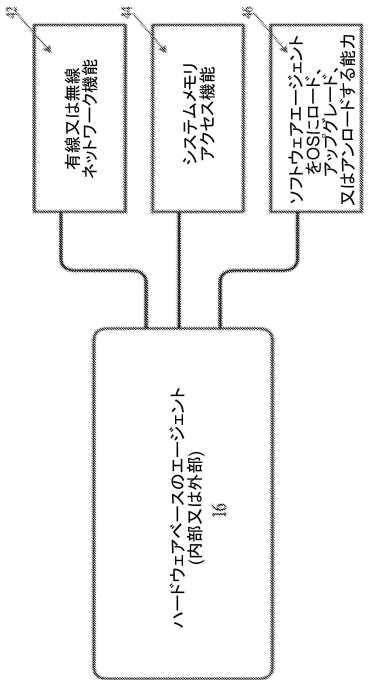
【図１】


解析エンジン
24
暗号解析発見サーバ
26
アーティファクト
データベース
23
復号器ビルドサーバ
28
ネットワーク
20
ソフトウェア
エージェント
14
ハードウェア
エージェント
16
ユーザ装置
12
10

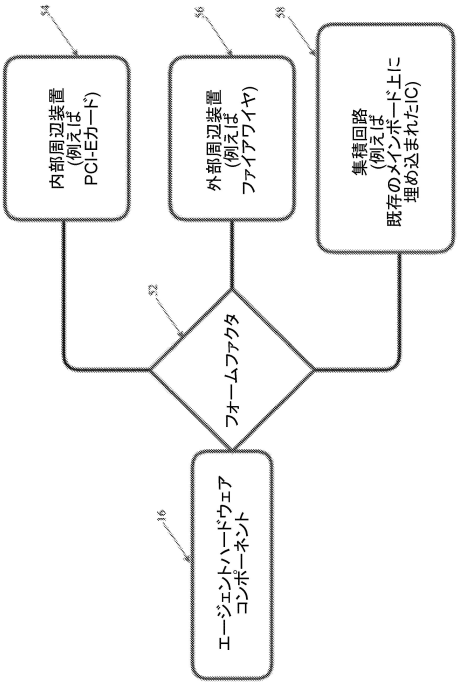
【図２】


オペレーティングシステム
の機能に依存する動作
32
エージェントを
実行すること
/動作させること
34
Ransomware
Rewind
Cloud
との通信のために
ネットワークに
アクセスすること
36
アップロードする
ためにファイルに
アクセスすること
ソフトウェアベースのエージェント
14
ハードウェアベースのエージェント
16
オペレーティングシステム
の機能と独立した動作
32
エージェントを
実行すること
/動作させること
34
Ransomware
Rewind
Cloud
との通信のために
ネットワークに
アクセスすること
36
アップロード
/ダウンロードする
ためにファイルに
アクセスすること

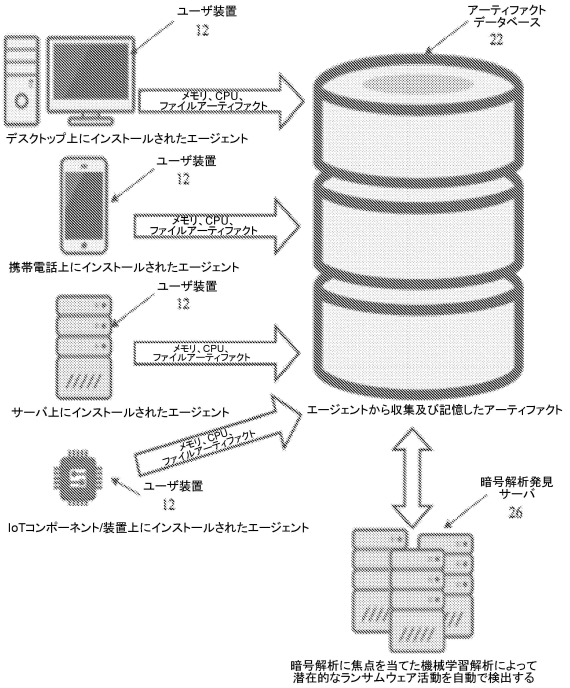
【図３】


42
有線又は無線
ネットワーク機能
44
システムメモリ
アクセス機能
46
ソフトウェアエージェント
をOSにロード、
アップグレード、
又はアンロードする能力
ハードウェアベースのエージェント
(内部又は外部)
16

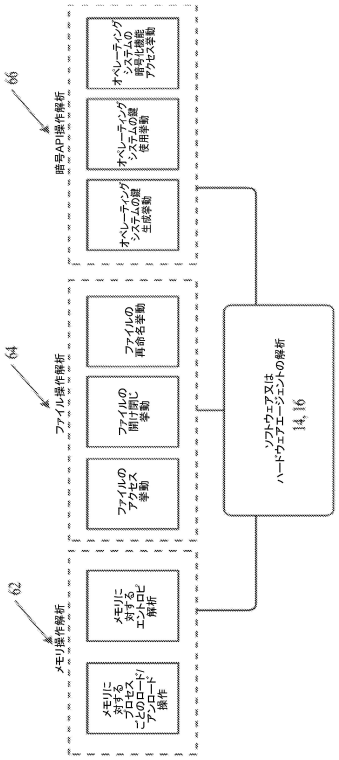
【図４】


54
内部周辺装置
(例えば
PCI-Eカード)
56
外部周辺装置
(例えば
ファイアワイヤ)
58
集積回路
(例えば
既存のメインボード上に
埋め込まれたIC)
52
フォームファクタ
16
エージェントハードウェア
コンポーネント

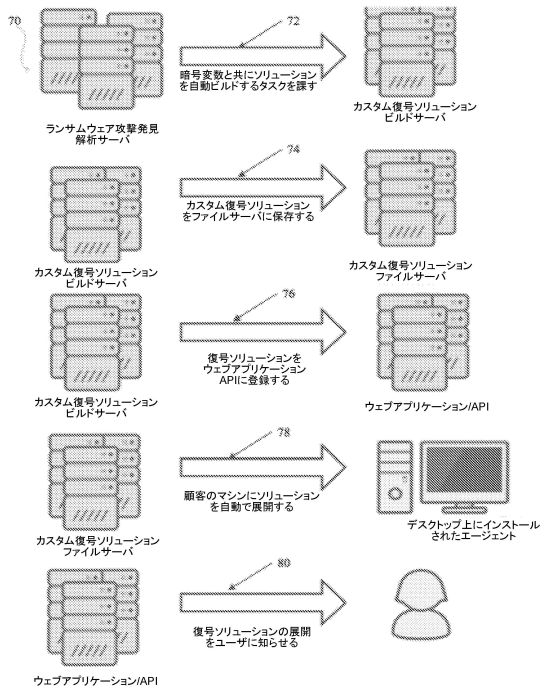
【図５】


ユーザ装置
12
アーティファクト
データベース
22
メモリ、CPU、
ファイルアーティファクト
デスクトップ上にインストールされたエージェント
ユーザ装置
12
メモリ、CPU、
ファイルアーティファクト
携帯電話上にインストールされたエージェント
ユーザ装置
12
メモリ、CPU、
ファイルアーティファクト
サーバ上にインストールされたエージェント
エージェントから収集及び記憶したアーティファクト
メモリ、CPU、
ファイルアーティファクト
ユーザ装置
12
IoTコンポーネント/装置上にインストールされたエージェント
暗号解析発見
サーバ
26
暗号解析に焦点を当てた機械学習解析によって
潜在的なランサムウェア活動を自動で検出する

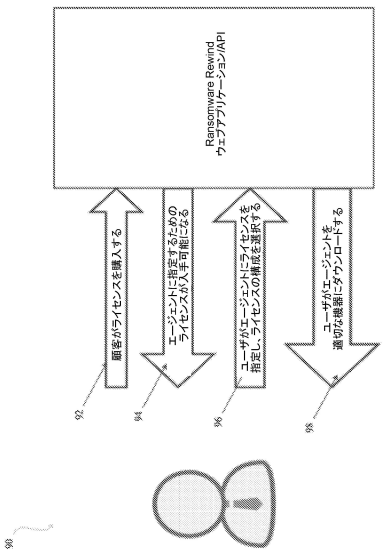
【図６】


66
暗号API操作解析
オペレーティングシステムの鍵生成挙動
オペレーティングシステムの鍵使用挙動
オペレーティングシステムの鍵保存挙動
64
ファイル操作解析
ファイルの再命名挙動
ファイルの削除挙動
ファイルのアクセス挙動
62
メモリ操作解析
メモリに対するエントロピー解析
メモリに対するプロセスごとのロード/アンロード操作
ソフトウェア又はハードウェアエージェントの解析
14, 16

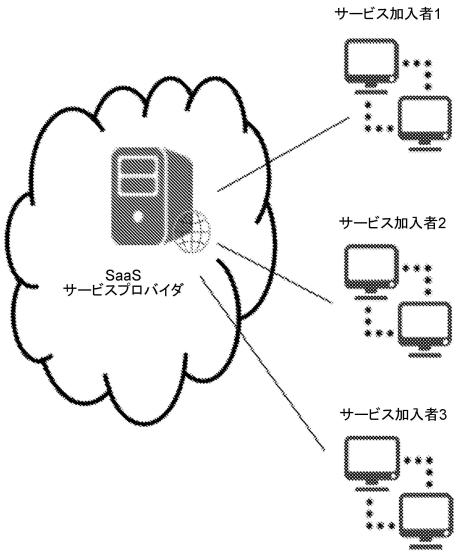
【図７】


70
ランサムウェア攻撃発見
解析サーバ
72
暗号変数と共にソリューション
を自動ビルドするタスクを課す
カスタム復号ソリューション
ビルドサーバ
74
カスタム復号ソリューション
をファイルサーバに保存する
カスタム復号ソリューション
ビルドサーバ
カスタム復号ソリューション
ファイルサーバ
76
復号ソリューションを
ウェブアプリケーション
APIに登録する
カスタム復号ソリューション
ビルドサーバ
ウェブアプリケーション/API
78
顧客のマシンにソリューション
を自動で展開する
カスタム復号ソリューション
ファイルサーバ
デスクトップ上にインストール
されたエージェント
80
復号ソリューションの展開
をユーザに知らせる
ウェブアプリケーション/API

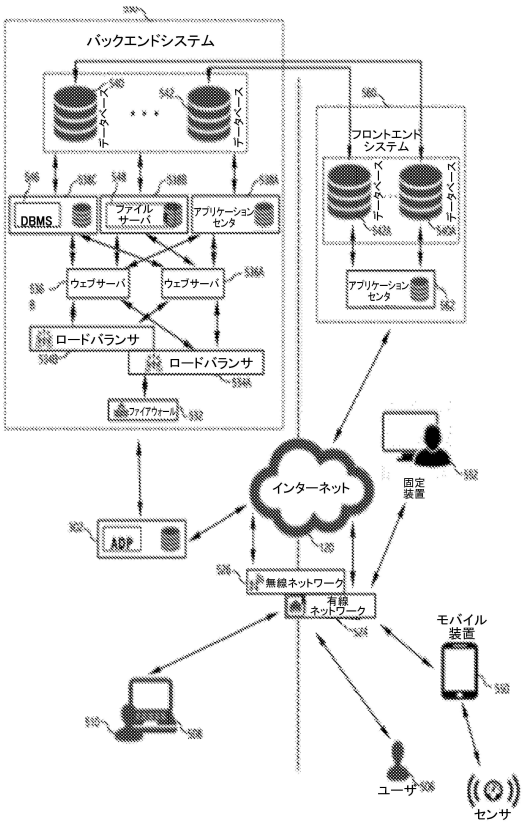
【図８】


Ransomware Rewind
ウェブアプリケーション/API
顧客がライセンスを購入する
エージェントに指定するためのライセンスが入手可能になる
ユーザがエージェントにライセンスを指定し、ライセンスの構成を選択する
ユーザがエージェントを適切な場所にダウンロードする
92
94
96
98
90

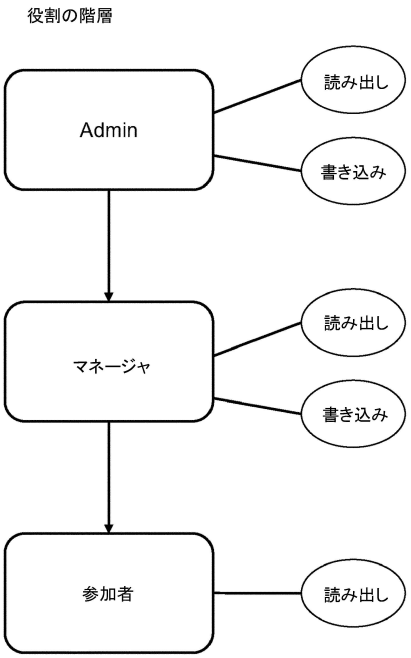
【図９】


サービス加入者1
サービス加入者2
サービス加入者3
SaaS
サービスプロバイダ

【図１０】


バックエンドシステム
フロントエンド
システム
DBMS
ファイル
サーバ
アプリケーション
センタ
ウェブサーバ
ロードバランサ
ファイアウォール
インターネット
固定
装置
ADP
無線ネットワーク
有線
ネットワーク
モバイル
装置
ユーザ
センサ

【図１１】


役割の階層
Admin
読み出し
書き込み
マネージャ
読み出し
書き込み
参加者
読み出し

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
早期審査対象出願
弁理士　江口 昭彦
(74)代理人　100134120
弁理士　内藤 和彦
(72)発明者　アンダーウッド，デニス
アメリカ合衆国，ペンシルベニア州 １５１３９ オークモント ペンシルベニア アベニュー ７０１
(72)発明者　ネーマン，カイル
アメリカ合衆国，メリーランド州 ２１６４１ ヒルズボロ ヒルズボロ ロード ２２１２５
(72)発明者　グリーンバーグ，ノア
アメリカ合衆国，ペンシルベニア州 １５３６７ ヴェニシア ウォルナット ドライブ ２２２
(72)発明者　ワイデマン，マーク
アメリカ合衆国，ペンシルベニア州 １５０４４ ギブソニア ヒルクレスト ドライブ １１７
審査官　岸野 徹
(56)参考文献　米国特許出願公開第２０１９／０１５８５１２（ＵＳ，Ａ１）
米国特許出願公開第２０１９／００６５７４５（ＵＳ，Ａ１）
米国特許出願公開第２０１７／００１２９７８（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５４