(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6527590号
(P6527590)
(45)発行日　令和1年6月5日(2019.6.5)　(24)登録日　令和1年5月17日(2019.5.17)

(51)Int.Cl.　F I
*H04L 12/66 (2006.01)*　H04L 12/66 B

請求項の数 18　(全 30 頁)

(21)出願番号　特願2017-543709(P2017-543709)
(86)(22)出願日　平成27年9月10日(2015.9.10)
(65)公表番号　特表2017-538376(P2017-538376A)
(43)公表日　平成29年12月21日(2017.12.21)
(86)国際出願番号　PCT/US2015/049414
(87)国際公開番号　WO2016/069119
(87)国際公開日　平成28年5月6日(2016.5.6)
審査請求日　平成30年9月7日(2018.9.7)
(31)優先権主張番号　62/073,376
(32)優先日　平成26年10月31日(2014.10.31)
(33)優先権主張国　米国(US)

早期審査対象出願

(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　100169904
弁理士　村井　康司
(74)代理人　100181021
弁理士　西尾　剛輝

最終頁に続く

(54)【発明の名称】オフライン・ネットワーク・トラフィックに基づいてカバート・チャネルのネットワーク侵入を検出するためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
オフライン・ネットワーク・トラフィックを処理するように構成された１つまたは複数のサーバであって、前記オフライン・ネットワーク・トラフィックが、対応する複数のカバート・チャネルのシグネチャーに関連する複数のカバート・チャネルの存在を示すことのできる既定のフォーマットを有し、各カバート・チャネルが、検出を回避するために標準ネットワーク・プロトコルから逸脱することによってメッセージを伝達するツールを含む、１つまたは複数のサーバと、
前記オフライン・ネットワーク・トラフィックを解析するように構成された複数のカバート・チャネル・プロセッサであって、１つまたは複数のカバート・チャネルのシグネチャーに基づいて、前記オフライン・ネットワーク・トラフィックが、前記標準ネットワーク・プロトコルから逸脱しているかどうか判定することを前記解析が含む、複数のカバート・チャネル・プロセッサと
を含む、ネットワーク侵入検出のためのシステム。
【請求項２】
前記オフライン・ネットワーク・トラフィックを解析してマルウェアを検出するように構成された複数のマルウェア・プロセッサをさらに含み、マルウェアが、逸脱することなく前記標準ネットワーク・プロトコルを使用する、請求項１に記載のシステム。
【請求項３】
前記オフライン・ネットワーク・トラフィックを解析してステガノグラフィを検出する

ように構成された複数のステガノグラフィ・プロセッサをさらに含む、請求項１に記載のシステム。
【請求項４】
前記オフライン・ネットワーク・トラフィックを解析して潜在的に不要なプログラム（ＰＵＰ）を検出するように構成された複数のＰＵＰプロセッサをさらに含む、請求項１に記載のシステム。
【請求項５】
前記オフライン・ネットワーク・トラフィックが、複数の標準層を有する少なくとも１つの標準ネットワーク・プロトコル・スタックを含む、請求項１に記載のシステム。
【請求項６】
前記カバート・チャネルが、前記標準ネットワーク・プロトコル・スタックの少なくとも１つの標準ネットワーク層で利用される、請求項５に記載のシステム。
【請求項７】
前記少なくとも１つの標準ネットワーク層が、ＨＴＴＰまたはＴＣＰ／ＩＰのうちの１つを含む、請求項６に記載のシステム。
【請求項８】
前記オフライン・ネットワーク・トラフィックが、第１のレベルおよび第２のレベルを含む２つのレベルで解析され、
前記第１のレベルの解析において、カバート・チャネルのシグネチャーに基づいて逸脱が検出され、
前記第２のレベルでは、解析が、標準での暗号解読プロセス、キーイン・プロセス、管理検出プロセス、ヘッダ・チェック・プロセス、またはフィールド・チェック・プロセスのうちの少なくとも１つを含む、請求項１に記載のシステム。
【請求項９】
ネットワーク・データ・トラフィックの前記既定のフォーマットがＰＣＡＰファイルである、請求項１に記載のシステム。
【請求項１０】
オフライン・ネットワーク・トラフィックを処理するステップであって、前記オフライン・ネットワーク・トラフィックが、対応する複数のカバート・チャネルのシグネチャーに関連する複数のカバート・チャネルの存在を示すことのできる既定のフォーマットを有し、各カバート・チャネルが、検出を回避するために標準ネットワーク・プロトコルから逸脱することによってメッセージを伝達するツールを含むステップと、
１つまたは複数のカバート・チャネルのシグネチャーに基づいて、前記オフライン・ネットワーク・トラフィックが、前記標準ネットワーク・プロトコルから逸脱しているかどうか判定するステップと
を含む、ネットワーク侵入検出のための方法。
【請求項１１】
前記オフライン・ネットワーク・トラフィックを解析してマルウェアを検出するステップをさらに含み、マルウェアが、逸脱することなく前記標準ネットワーク・プロトコルを使用する、請求項１０に記載の方法。
【請求項１２】
前記オフライン・ネットワーク・トラフィックを解析してステガノグラフィを検出するステップをさらに含む、請求項１０に記載の方法。
【請求項１３】
前記オフライン・ネットワーク・トラフィックを解析してＰＵＰを検出するステップをさらに含む、請求項１０に記載の方法。
【請求項１４】
前記オフライン・ネットワーク・トラフィックが、複数の標準ネットワーク層を有する少なくとも１つの標準ネットワーク・プロトコル・スタックを含む、請求項１０に記載の方法。

【請求項１５】
前記カバート・チャネルが、前記標準ネットワーク・プロトコル・スタックの少なくとも１つの標準ネットワーク層で利用される、請求項１４に記載の方法。
【請求項１６】
前記少なくとも１つの標準ネットワーク層が、ＨＴＴＰまたはＴＣＰ／ＩＰのうちの１つを含む、請求項１５に記載の方法。
【請求項１７】
前記オフライン・ネットワーク・トラフィックが、第１のレベルおよび第２のレベルを含む２つのレベルで解析され、前記第１のレベルの解析において、カバート・チャネルのシグネチャーに基づいて逸脱が検出され、前記第２のレベルでは、解析が、標準での暗号解読プロセス、キーイン・プロセス、管理検出プロセス、ヘッダ・チェック・プロセス、またはフィールド・チェック・プロセスのうちの少なくとも１つを含む、請求項１０に記載の方法。
【請求項１８】
ネットワーク・データ・トラフィックの前記既定のフォーマットがＰＣＡＰファイルである、請求項１０に記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、アドバンスド・パーシスタント・スレット（ＡＰＴ）を防止するためのシステムおよび方法に関し、より詳細には、オフラインでネットワーク・トラフィックを検出および解析することに関する。
【背景技術】
【０００２】
サイバー攻撃は、不特定の対象に向けた単純な犯罪行為から、高度な攻撃ツールを使用して、標的となる実体に対して長期間にわたっておこなうキャンペーンにまで発展し、また進化してきた。このタイプのサイバー活動は、アドバンスド・パーシスタント・スレット（ＡＰＴ）として知られており、公表できないデータの存在する、あらゆる企業、政府機関、または軍事施設に著しい脅威をもたらす。ＡＰＴ攻撃を解決するコストも、組織にとっては財政的に重荷となる。しかし、攻撃をクリーンアップするのに関連する費用は、貴重な知的財産、機密データ、企業秘密、事業計画、およびサイバー攻撃者たちの標的から情報を抜き取ることに焦点を当てた、彼らが標的とする他のデータの暴露に関連する長期的なコストと比較すると重要なものではない。消費者金融、医療保険の相互運用性と説明責任に関する法律（ＨＩＰＡＡ）、サーベンス・オクスリー法、または軍事データなど、管理規定によって管理されるデータを喪失すると、結果として、かなりの罰金および法的執行措置につながることにもなる。いったんデータ漏洩が公表されると、収入の損失、および顧客信頼度を再確立するためのコストは甚大になる場合がある。
【０００３】
ＡＰＴサイバー攻撃が発覚した後、標的となった実体は、タイミングのよいクリーンアップ、危機分析、法規制の順守について即応する必要がある。これらの実体は、盗まれた知的財産または企業秘密、影響を受けた機器およびアカウント、ならびに攻撃者の属性を可能な限り正確に、素早く識別しなければならない。しかし、世界中の企業、軍事組織、または政府機関から現在公表されている情報によって、ＡＰＴ攻撃についての不穏な傾向が明らかになってきた。企業の盗まれたデータが攻撃者によって売られたり、ばらまかれたりするのを、セキュリティ研究者が目にするまで、通常、サイバー攻撃の発覚は気付かれないままである。この時点で、敵対者は、標的の知的財産、個人情報、および／または機密データの大部分に長期間アクセスしてきた。現在利用可能なサイバー・セキュリティ装置は、うまく仕組まれた攻撃を防げないが、その代わりに、侵入を遅らせ、最終的には

発見できるようにし、発覚した攻撃を調査および除去するのに必要なツールを、攻撃に対処する側へ提供する。攻撃された実体は、攻撃に対して適切に対処できるようになる前に、広範囲にわたる法的な分析、および侵入検出作業を待たなければならないが、攻撃者の行為を推定することだけは受信することがある。

【０００４】

稚拙でサイバー犯罪に焦点を当てたマルウェアとは異なり、ＡＰＴ攻撃は複雑であり、その数が限られている。このＡＰＴ攻撃は、わずかに手直しされるだけで長期間用されることが多い。しかし、その通信メッセージング・システムは複雑であり、サイバー防衛側には、高度な暗号化、プロトコル、およびマルウェア解析の専門知識が必要となる。これにより、規制機関、法執行機関、およびサイバー・セキュリティのサービス・プロバイダは、ＡＰＴ攻撃に対抗するのが困難になる。一方で、ＡＰＴ攻撃者は、その能力速度、検出回避、およびクリーンアップへの反撃技法を向上させている。不完全に実行された侵入応答は、反応する時間を攻撃者に与え、その結果、企業内部の様々な場所で既存の攻撃ツールがさらに高度なバージョンに置き換わることになる。

【０００５】

不要なソフトウェアのバンドリングとは、良心的でない会社が、ユーザを惑わせて、このユーザのプライバシーを損ない、またはユーザのコンピュータの安全性を脆弱にする恐れのある不要なプログラムをインストールさせようとする場合である。会社は、不要なアプリケーションをユーザにインストールさせるよう強制し、ユーザがどのようにしてオプトアウトすればよいのか見つけるのを困難にするラッパー・アプリケーションを有する、必要とされるプログラム・ダウンロードをバンドルすることが多い。ほぼありとあらゆる第三者の無料ダウンロード・サイトが、潜在的に不要なソフトウェアをそのダウンロードにバンドルする。

【０００６】

ウイルス対策会社は、バンドルされたソフトウェアを潜在的に不要なプログラム（ＰＵＰ）と定義し、このプログラムには、押しつけがましい広告を表示し、もしくはユーザのインターネット使用状況を追跡して広告主に情報を売り、ユーザが見るウェブ・ページにそれ自体の広告を挿入し、またはプレミアムのＳＭＳサービスを使用して、ユーザへの課金をせしめるソフトウェアが含まれ得る。望ましくないプログラムは、インストールされている痕跡、およびアンインストールまたはオプトアウトの手順説明を含まないことが多い。望ましくないソフトウェア・バンドルの中には、ユーザの装置にルート証明書をインストールするソフトウェアを含むものがあり、これによって、攻撃者は、ブラウザのセキュリティ警告なしに銀行取引の詳細情報を傍受できるようになる。アメリカ合衆国国土安全保障省は、安全でないルート証明書を除去するよう助言してきたが、それというのも、これによって深刻なサイバー攻撃に対するコンピュータの抵抗力が弱まるからである。

【０００７】

様々な技法を使用して、アドバンスド・パーシスタント・スレット（ＡＰＴ）活動を検出しようと試みる装置が知られている。ネットワーク・セキュリティ装置は、サイバー攻撃ツールの通信を含む特定の攻撃を収集するように調整することができ、現在利用可能である。オープン・ソース・ツールを含め、ネットワーク監視および攻撃発見用の製品およびツールが存在する。侵入検知システムなどのサイバー・セキュリティ防御製品によっては、既知の攻撃に似た挙動またはマルウェアの特徴に基づいて、警告「の事実」を提示するものがある。これらのネットワーク監視装置の多くは、警告に関連するネットワーク・トラフィックを収集する機能、ならびに最新の検出機能を確実にインストールするためのサブスクリプション・サービスも含む。しかし、これらの防御製品は、発見した攻撃ツールのメッセージの内容を抽出することはなく、または悪質なツールのネットワーク活動を処理して、これまでに知られている侵入の詳細を公表することはない。したがって、何か月間または何年間も組織に影響を及ぼし、組織内でうまく動き回った後にＡＰＴ攻撃が発見されると、脅威がさらに大きくなる。

【０００８】

ネットワーク・トラフィックをリアルタイムで、すなわち「オンライン」で解析することが知られている。Ｓｎｏｒｔは、無料でオープン・ソースのネットワーク侵入防止システム（ＮＩＰＳ）およびネットワーク侵入検知システム（ＮＩＤＳ）である。Ｓｎｏｒｔには、インターネット・プロトコル（ＩＰ）ネットワーク上で、リアルタイムのトラフィック解析およびパケット・ロギングを実行する機能がある。Ｓｎｏｒｔは、プロトコル解析、コンテンツ検索、およびマッチングを実行する。Ｓｎｏｒｔは、オペレーティング・システムへの攻撃、フィンガープリンティングの試み、共通ゲートウェイ・インターフェース、バッファ・オーバフロー、サーバ・メッセージ・ブロック・プローブ、およびステルス・ポート・スキャンを検出する。Ｓｎｏｒｔは、パケット検査、プロトコル標準での侵入検出進行および侵入防止、プロトコル異常検出、アプリケーション制御、および痕跡のマッチングを実行する。Ｓｎｏｒｔは、ＨＴＴＰヘッダでの２進コード、ＨＴＴＰ／ＨＴＴＰＳトンネリング、ＵＲＬディレクトリ・トラバーサル、クロスサイト・スクリプティングを含むアプリケーション・レベルの脆弱性を解析し、またＳＱＬインジェクションも解析されることになる。

【０００９】

カバート・チャネルは、サイバー攻撃の被害者にマルウェアを送りつけるための媒体として敵対者によって使用され、たとえばＤＮＳトンネリングとして知られている。ＤＮＳトンネルでは、データは、３２進法および６４進法の符号化を使用して、ＤＮＳクエリおよびＤＮＳ応答内にカプセル化され、ＤＮＳドメイン・ネーム・ルックアップ・システムを使用して、データを双方向に送信する。ボットネットは、ＤＮＳトンネリングを使用して、カバート・チャネルの役割を果たすことができ、検出するのが困難である。カバート・チャネルを識別する唯一の方法は、指令／制御ＤＮＳメッセージを探すことによるものである。攻撃者は、ＤＮＳトンネル・ツールを使用して、カバート・チャネルを作成する。

【００１０】

「Ｓｕｒｉｃａｔａ」は、マルチスレッド・マルウェア・コマンドおよびカバート・チャネルの検出器である。Ｓｕｒｉｃａｔａは、マルウェア・プロセッサまたはマルウェア・エンジンを使用して、ネットワークＩＤＳ、ＩＰＳ、およびセキュリティを監視する。Ｓｕｒｉｃａｔａは、複数のプロセッサ全体にわたって、マルウェアの処理負荷のバランスをとる。Ｓｕｒｉｃａｔａは、ストリームが開始するときに共通プロトコルを認識し、したがって、ルール・ライタが、このプロトコルにルールを書き込めるようになる。Ｓｕｒｉｃａｔａは、ＨＴＴＰ　ＵＲＩからＳＳＬ証明書識別子まで及ぶプロトコル・フィールド上でマッチすることができる。Ｓｕｒｉｃａｔａは、Ｏｆｆ　ｐｏｒｔ　ＨＴＴＰ、ＣｎＣチャネル、ファイル識別、ＭＤ５チェックサム、およびファイル抽出を処理することができる。Ｓｕｒｉｃａｔａは、ネットワークにわたるマルウェア・ファイル・タイプを識別することができる。ファイルは、抽出するためにタグ付けすることができ、キャプチャの状況または流れを記述するメタデータ・ファイルを記憶することができる。ファイルのＭＤ５チェックサムがただちに計算され、その結果、ｍｄ５ハッシュのリストを見つけることができる。

【００１１】

米国特許公報第２００４－０１０７３６１号明細書には、ネットワーク接続上のデータ単位を解析することによって侵入を検出するための、ネットワーク侵入検知システムが開示してある。米国特許第７，３５６，７３６号明細書には、ソフトウェア性能を監視するための、シミュレーションされたコンピュータ・システムが開示してある。米国特許第５，７６５，０３０号明細書には、プログラム実行においてプリフェッチ・キュー・サイズが可変である、プロセッサ・エミュレータ・モジュールが開示してある。米国特許第７，０９３，２３９号明細書では、コンピュータ・システム内の不要なコードを検出するためのコンピュータ免疫システムおよび方法が開示してある。米国特許公報第２０１０－０１００９６３号明細書には、消費電力、計算能力、およびメモリが著しく制限されている、携帯電話、スマートフォン、またはＰＤＡなどのモバイル装置での、攻撃およびマルウェ

アを検出し、防止するためのシステムおよび方法が開示してある。米国特許公報第２００８－００２２４０１号明細書には、マルチコアのネットワーク・セキュリティ処理用の装置および方法が開示してある。米国特許第７，０７６，８０３号明細書には、統合された侵入検出サービスが開示してある。米国特許第６，８５１，０６１号明細書は、ネットワーク・プロトコル・スタック・マルチプレクサを使用する、侵入検出データ収集用のシステムおよび方法である。米国特許公報第２００３－００８４３１９号明細書には、侵入防止システムをネットワーク・スタックに挿入するための、ノード、方法、およびコンピュータ読取り可能な媒体が開示してある。米国特許第６，７７５，７８０号明細書には、エミュレーション中に生成されるシステム・コールのパターンを解析することによって、悪質なソフトウェアを検出することが開示してある。

【００１２】

図１には、複数のマルウェア、カバート・チャネル、ステガノグラフィ、およびＰＵＰのサーバによる脅威の下での、例示的なシステムが示してある。ＡＰＴ攻撃は、通常、予測可能な段階で実行される。攻撃者はまず、ネットワーク上のマシンへのアクセス権を得る。スピア・フィッシングを含む様々な方式で、これを実行することができる。スピア・フィッシングとは、標的となる会社の従業員に不正なｅメールを送りつける戦術である。これらのｅメールは、信頼できる正当な送信元からのように見え、攻撃者が悪質なツールをインストールできるようにする行為を従業員が実行するように欺く。第２に、攻撃者は、進行中の攻撃で後に使用するため、被害者への限定アクセスを可能にするように設計された、小さくて悪質なツールをインストールする。このツールは、ウイルス対策の影響を受けない可能性がある。第３に、攻撃者は、オリジナルの小さくて悪質なツールを使用して、比較的大きくてフル機能の悪質なツールをインストールし、このツールもウイルス対策の影響を受けない可能性がある。このツールは、他のユーザおよび機器にまで拡散すること、および盗んだ機密データを攻撃者に送って戻すことを含め、攻撃者のための様々なタスクを実行することになる。第４に、攻撃者は、ネットワーク全体を通して拡散して、組織に対する長期アクセスを確実なものにし、極めて重要な機密を自在に盗み出し、攻撃ツールをアップグレードして、サイバー・セキュリティのアナリストおよびツールの一歩先を行く。

【００１３】

ＡＰＴ攻撃を通してのあらゆるステップには、攻撃者またはこの攻撃者によって制御されるインフラストラクチャとのネットワーク通信が必要となる。標的への攻撃が段階１から段階４まで継続すると、攻撃それ自体についての情報が多くなるとともに通信が多くなる。攻撃者は、自分たちの攻撃を管理し、個々の被害者のマシンにコマンドを送信し、標的から盗んだデータを受信する手段を必要とする。さらに、攻撃が段階４まで十分に浸透すると、これらの通信は、その安定性および複雑さが増す。段階３および４で使用されるフル機能の悪質なツールは、何ヶ月でも何年でも攻撃の持続時間を継続するように設計されており、また十分に複雑なので、高度なサイバー攻撃キャンペーンを操作している間、単純な検出技法のほとんどを回避することができる。ネットワーク・トラフィックをキャプチャするためのアプリケーション・プログラミング・インターフェース（ＡＰＩ）が存在する。ＵＮＩＸ（登録商標）のようなシステムは、その「ｌｉｂｐｃａｐ」ライブラリでＰＣＡＰを実装する。Ｗｉｎｄｏｗｓシステムは、「ＷｉｎＰｃａｐ」として知られている「ｌｉｂｐｃａｐ」のポートを使用する。ネットワーク・トラフィック監視ソフトウェアは、ｌｉｂｐｃａｐおよび／またはＷｉｎＰｃａｐを使用して、ネットワーク上を流れるパケットをキャプチャしてもよい。ソフトウェアの比較的新しいバージョンでは、ｌｉｂｐｃａｐまたはＷｉｎＰｃａｐは、リンク層でパケットをキャプチャする。ＰＣＡＰＡＰＩはＣで書かれており、Ｊａｖａ（登録商標）、ＮＥＴ言語、スクリプト言語など他の言語はラッパーを使用する。アドバンスド・パーシスタント・スレット（ＡＰＴ）攻撃ツールからキャプチャされたネットワーク通信は、攻撃者と標的の両方に極めて重要な情報を含む。これらカスタマイズされたメッセージは大抵の場合、標的と攻撃者の両方についての情報を常に含んでおり、こうした情報には、被害者のマシン情報、被害者のユー

ザ情報、盗まれた（ひそかに抽出されたともいう）知的財産、攻撃者を特定する情報、標的に対してとった攻撃者の行動、および最初の攻撃の日付など攻撃者のツール情報が含まれる。

【００１４】

ネットワーク・トラフィックを非リアルタイムで、すなわち「オフライン」で解析することが知られている。たとえば、「ＣｈｏｐＳｈｏｐ」は、ＭＩＴＲＥ　Ｃｏｒｐｏｒａｔｉｏｎが開発したフレームワークである。悪質な攻撃から頑強に防御するためのマルウェア・プロセッサが知られている。マルウェア・プロセッサは、検出および解析するための、既に知られているかまたは開発されたマルウェアの痕跡に基づいて動作するように構成される。マルウェアの痕跡は、特定のウイルスを一義的に識別するアルゴリズムまたはハッシュ（一連のテキストから得られる数）である。痕跡は静的でもよく、これは、その最も簡略な形において、マルウェアに固有のコードの断片の計算された数値である。痕跡は動作ベースでもよく、すなわち、マルウェアがＸ、Ｙ、Ｚを実行しようとすると、不審なものとしてそれにフラグを立てる。痕跡は、ウイルスの、ビットの固有ストリング、または２値パターンとすることができる。たとえば、特定のウイルスを検出および識別するのに使用できるという点で、ウイルスの痕跡は指紋のようなものである。アンチウイルス・ソフトウェアは、ウイルスの痕跡を使用して、悪質なコードの存在をスキャンする。ＣｈｏｐＳｈｏｐ　ＡＰＴツールは、マルウェア制御エンドポイント、すなわち図１に示すマルウェア・サーバとの間でやり取りされる実際のコマンドをセキュリティ専門家が理解できるようにする、ネットワーク・ベースのプロトコル・デコーダ向けの、非常に限定された数のマルウェア信号を処理および解析する。サイバー・セキュリティでは、カバート・チャネルも知られている。一例では、カバート・チャネル制御エンドポイント、すなわち図１に示すカバート・チャネル・サーバは、制御エンドポイント間での知的所有権通信チャネルを生成する。本明細書では、カバート・チャネルは、検出を回避するために標準プロトコルから逸脱することによってメッセージを伝達する攻撃ツールである。カバート・チャネルの逸脱は、標準プロトコル・スタックの任意の１つまたは複数の層におけるものとすることができる。マルウェアは、標準プロトコルから逸脱することなく、メッセージを伝達するのに標準プロトコル・スタックを使用する標的に対する攻撃ツールである。

【００１５】

サイバー・セキュリティでは、ステガノグラフィを含む他の攻撃も知られている。悪質なツールは、無害で正当に見えるファイル内部の大量の情報を隠すための数多くの方法、たとえばステガノグラフィとして知られる手法を使用する。このような方法には、データを隠すためのアルゴリズムを使用するものがあり、本発明は、そうしたものをほぼリアルタイムに抽出することができる。ステガノグラフィの技法もあり、これは、隠された情報を抽出する前に、暗号の変数または鍵の、発見または開示を必要とする。

【発明の概要】

【課題を解決するための手段】

【００１６】

本発明は、様々な暗号技法およびフォレンジック技法を利用して、ステガノグラフィを巧みに使う悪質なツールによって使用されている暗号化に攻撃を仕掛け、隠された情報を抽出する。暗号技法およびステガノグラフィ技法によっては、独自のものもあり、復号化に必要な暗号変数を識別するためのカスタム機能必要とすることになる。他の技法は、本発明が利用する標準の復号化スパイ技術に従っており、標準化された暗号攻撃を処理が使用できるようにする。

【００１７】

サイバー・セキュリティでは、ＰＵＰを含む他の攻撃も知られている。ユーザがインストールする誘惑に駆られることのあるブラウザのツール・バーまたはプログラムが知られており、ユーザは、自分たちの日々の活動およびデータの全てを企業に与えることに「同意」した。ユーザは通常、このようなプログラムをインストールすることに同意するはずもなく、または自分たちの日々の活動を提供することに同意し、たとえばそれを潜在的に

不要なプログラム（ＰＵＰ）にしようとは気がつかなかった。ＰＵＰは、何らかのシステム監視ツールによって、ネットワーク層でマシンにインストールされる。ファイアウォールはＰＵＰを検出し、これを管理者に送信する。管理者は、サーバ上でこのプログラムが必要なものか、それとも不要なものか判定する。必要となるプログラムも、ネットワークのオーナによっては不要となる場合もある。発見的解析を実行することも可能であり、これは大抵、管理ツールに焦点を当てたＰＵＰに焦点を当てることになる。発見的解析を使用するほとんどのアンチウイルス・プログラムは、専用の仮想マシン内の疑わしいプログラムまたはスクリプトのプログラミング・コマンドを実行することによってこの機能を実行し、したがって、不審なコードを実在のマシンから分離した状態に保ちながら、不審なファイルが実行されることになる場合に発生するはずの様子を、このアンチウイルス・プログラムが内部でシミュレーションできるようにする。次いで、このアンチウイルス・プログラムは、コマンドが実行されるときにこのコマンドを解析し、複製、ファイルの上書き、不審なファイルの存在を隠す試みなど、既知のウイルス活動について監視する。１つまたは複数のウイルスのような動作が検出される場合、不審なファイルには、ウイルスの可能性があるものとしてフラグが立てられ、ユーザに警告される。発見的解析の別の一般的な方法は、アンチウイルス・プログラムが、不審なプログラムを逆コンパイルし、次いでそれを用いてソース・コードを解析することである。この不審なファイルのソース・コードは、既知のウイルスおよびウイルスのような動作のソース・コードと比較される。ソース・コードのうち一定の割合が、既知のウイルスまたはウイルスのような動作のコードと一致する場合、ファイルにフラグが立ち、ユーザに警告される。

【００１８】

ＰＵＰのもう一方の側面は、テルネット（遠隔コンピュータにアクセスするためのユーザ・コマンドおよび基本となるＴＣＰ／ＩＰプロトコル）、ＲＤＰ（ネットワーク接続を介して別のコンピュータに接続するためのグラフィカル・インターフェースをユーザに提供する独自のプロトコル）、ＦＴＰ（インターネットなどＴＣＰベースのネットワークを介して、あるホストから別のホストまでコンピュータ・ファイルを転送するのに使用される標準のネットワーク・プロトコル）、または他の任意の管理ツールのような管理ツールを含み、これらのツールは、ほとんど全てのネットワークで使用される非常に強力な管理ツールである。これらはまた、ハッカーにも極めて有用である。管理者は、たとえば、中国のＩＰアドレスが使用されているのを目にして、中国には従業員がいないと言及するのは別として、ＰＵＰ（管理ツール）が実際に実行しているものを容易に指摘することができない。システムは、これらのプロトコルも復号化して、これら「潜在的に不要な」管理行為中に実行される活動を明らかにすることになる。

【００１９】

政府機関、企業、および軍事施設のネットワークへのＡＰＴ攻撃と闘う深刻なニーズが認識されてきている。攻撃を理解するのに必要となる高度な技術的解析を実行するには、膨大なリソースが必要となり、これには様々な政府の規制要求事項を考慮に入れなければならない。たとえば、米国でのサイバー・セキュリティ製品の開発者は、武器国際取引に関する規則（ＩＴＡＲ）の下で、国務省および米国国防総省の規制に従わなければならない。

【００２０】

ＡＰＴ攻撃は、攻撃者の活動、影響を受けたユーザおよびマシン、盗まれた知的財産、ならびに攻撃者の属性および動機に関する手がかりを正確に詳述する包括的なレポートを必要とする。さらに、情報技術の担当者は、影響を受ける全ての機器を包括的に把握して、攻撃者が、統合されたクリーンアップ戦略を用いる試みを観察し、それを回避できるようになる可能性を低くする必要がある。したがって、ＡＰＴ攻撃から防御する頑強なシステムが必要となる。

【図面の簡単な説明】

【００２１】

【図１】複数のマルウェア、カバート・チャネル、ステガノグラフィ、およびＰＵＰのサ

ーバによる脅威の下での、例示的なシステムを示す。
【図２】標準プロトコル・スタックに従って構成可能な通信チャネルを介して互いに通信する、２つのネットワーク・ノードを示す。
【図３】複数の標準層を有する、図１の標準プロトコル・スタックを示す。
【図４】サービスとしてのソフトウェア（ＳａａＳ）のプラットフォーム上に本発明を実装する、システムのブロック図を示す。
【図５】図４のＳａａＳで使用されるアプリケーション開発システムの例示的なブロック図を示す。
【図６】図４のＳａａＳで利用される様々なモジュールとのインターフェースのブロック図を示す。
【図７】図６の製品強化モジュールのブロック図を示す。
【図８】図１のシステムの動作層の例示的なブロック図を示す。
【図９】図８のウェブ・サーバによって実装される、マルチプロセッシング・システムのアーキテクチャの図である。
【図１０】図４のＳａａＳへの認証およびプロファイリングを実施する例示的な図を示す。
【図１１】図１のシステムによって処理するための侵入内容の提出を示すブロック図である。
【図１２】図４のＳａａＳによって利用される入れ子型のプロトコル処理のブロック図である。
【図１３】解析装置Ａを示す、検出段階および解析段階を有するＤＮＳカバート・チャネルの一例の流れ図である。
【図１４】解析装置ＡおよびＢを示す、検出段階および解析段階を有するＤＮＳカバート・チャネルの一例の流れ図である。
【図１５】解析装置ＡおよびＢを示し、この解析装置Ｂが４バイトのＸＯＲを使用する、検出段階および解析段階を有するＤＮＳカバート・チャネルの一例の流れ図である。
【図１６ａ】カバート・チャネルのプロセスを示す。
【図１６ｂ】マルウェアのプロセスを示す。
【図１７ａ】カバート・チャネルのプロセスの流れ図である。
【図１７ｂ】マルウェアのプロセスの流れ図である。
【発明を実施するための形態】
【００２２】
簡潔にいえば、本発明によれば、ネットワーク侵入検知のシステムおよび方法は、オフライン・ネットワーク・トラフィックを受信するように構成される。既定のフォーマット、ＰＣＡＰファイルを有するオフライン・ネットワーク・トラフィックは、対応する複数のカバート・チャネルの痕跡に関連した、複数のカバート・チャネルの存在を示すことができる。それぞれのカバート・チャネルは、検出を回避するために標準プロトコルから逸脱することによってメッセージを伝達する攻撃ツールを含む。複数のカバート・チャネル・プロセッサが、オフライン・ネットワーク・トラフィックを解析するように構成される。この解析によって、１つまたは複数のカバート・チャネルの痕跡に基づいて、オフライン・ネットワーク・トラフィックが標準プロトコルから逸脱しているかどうか判定される。カバート・チャネルは、標準プロトコル・スタックの少なくとも１つの標準層において利用され、オフラインのネットワーク・データ・トラフィックは、複数の標準層を有する少なくとも１つの標準プロトコル・スタックを含む。本発明のより詳細な特徴のいくつかによれば、複数のマルウェア・プロセッサが、オフライン・ネットワーク・トラフィックを解析してマルウェアを検出するように構成され、ここで、マルウェアは逸脱することなく標準プロトコルを使用する。また、複数のステガノグラフィ・プロセッサが、オフライン・ネットワーク・トラフィックを解析してステガノグラフィを検出するように構成される。さらに、複数の潜在的に不要なプログラム（ＰＵＰ）プロセッサが、前記オフライン・ネットワーク・トラフィックを解析してＰＵＰを検出するように構成される。さらに、

少なくとも１つの標準層は、ＨＴＴＰまたはＴＣＰ／ＩＰを含む。本発明のより詳細な他の特徴によれば、オフライン・ネットワーク・トラフィックは、２つのレベル、すなわち第１のレベルおよび第２のレベルで解析される。第１のレベルの解析では、カバート・チャネルの痕跡に基づいて逸脱が検出される。第２のレベルでは、解析は、標準での復号化プロセス、キーイン・プロセス、管理検出プロセス、ヘッダ・チェック・プロセス、またはフィールド・チェック・プロセスのうちの少なくとも１つを含む。

【００２３】

例示的な実施形態を以下で詳細に説明する。特定の例示的な実施形態について述べるが、これは、もっぱら説明するためにおこなうものであることを理解されたい。例示的な実施形態を説明し、図示する際には、明確にするために特定の専門用語を使用する。しかし、各実施形態は、このように選択された特定の専門用語に限定されるものではない。各実施形態の精神および範囲から逸脱することなく、他の構成要素および構成を使用してもよいことが、当業者には理解されよう。それぞれ特定の要素は、同様の目的を遂行するのと同様に動作する、全ての技術的均等物を含むことを理解されたい。本明細書に記載の各例および実施形態は、非限定的な例である。

【００２４】

本発明は、カスタム・ネットワーク・メッセージが標的と攻撃者の間で伝送されていることを識別および理解することができ、影響を受けるユーザおよびマシン、標的に送信されるコマンド、盗まれたデータ、ならびに攻撃者についての手がかりを詳細に記載した自動的または半自動的に生成されるレポートに、標的となる組織がアクセスできるようになる。このレポートは、感染した全てのマシンの正確な数量および名前、攻撃者のステージング領域として使用されるマシンの数、攻撃者が現在アクセスしているユーザ・アカウントの正確な数、攻撃者の現在の活動についての情報、およびどのデータが盗まれたのかについての観察、攻撃者のツールがどのようにラベル付けされるのかについての情報、最初に感染した日付、ならびに、企業が発見し、企てをクリーンナップする場合のバックアップ計画として攻撃者がインストールした追加のツールについての情報を提供する。統合されたクリーンアップを組織全体で実行するため、攻撃者がその悪質なツールを移動またはアップグレードする機会を得るよりも恐らく早く、侵入についてのレポートをリーダーおよび侵入対応者に送達することができる。

【００２５】

本発明は、攻撃者のカスタム・ネットワーク・メッセージを理解し、抽出された情報を企業のリーダーに報告するプログラムを用いて、悪質なツールの通信を処理する。以下に述べるように、本発明は、攻撃者の通信ネットワーク内で見つかった有用な被害者情報および攻撃情報を復号化し、抽出し、報告する加入者サービスを提供する。より具体的には、本発明は、ＡＰＴ攻撃に対する弱点を利用する。本発明は、ＡＰＴ攻撃を利用して、影響を受ける機器およびユーザ、攻撃者の識別または目標、盗まれたデータ、および攻撃者の活動に対するほぼリアルタイムの答えまたは手がかりを、標的となる実体に提供する、１組の独自の高度なツールを使用する。

【００２６】

本発明は、ネットワーク暗号（暗号解読）解析、カスタム・ネットワーク・プロトコル（メッセージ）解析、複数の攻撃者ファミリにわたるＡＰＴ攻撃のスパイ技術知識、主要な法執行捜査および国家安全保障活動に精通することを含む、様々なＡＰＴ攻撃ツールの脅威情報追跡、企業ネットワークの処理ソフトウェア技術、クラウド・ソフトウェア技術、およびＡＰＴの悪質なツールを含む徹底的なマルウェア解析を使用する。

【００２７】

一実施形態では、本発明は、検出を回避するために標準プロトコルから逸脱するカバート・チャネルを検出する。カバート・チャネルの逸脱は、標準プロトコル・スタックの任意の１つまたは複数の層におけるものとすることができる。本発明は、非リアルタイムでキャプチャされたネットワーク・トラフィック（オフライン・ネットワーク・トラフィック）を処理することにより、標準プロトコル・スタックの任意の層からカバート・チャネ

ルを識別および抽出するように構成された、カバート・チャネル・プロセッサを備える。別の実施形態では、本発明は、カバート・チャネルに加えて、マルウェアを識別および抽出するように構成されたマルウェア・プロセッサを備える。カバート・チャネルとは対照的に、マルウェアは、逸脱することなく標準プロトコル・スタックを使用する。

【００２８】

本発明は、既定のフォーマットに従ったオフライン・ネットワーク・トラフィック・データを受信するように構成された、１つまたは複数のサーバを備える、ネットワーク侵入検出用のシステムである。対応する複数のカバート・チャネルの痕跡に関連する複数のプロセッサは、通信プロトコルが標準から逸脱していたかどうか判定するように構成される。オフライン・ネットワーク・データ・トラフィックは、標準通信の複数の層を含む標準プロトコル・スタックについての情報を含む。カバート・チャネルは、検出されずに情報を送受信するための認可されていないチャネルを提供するために、プロトコル・スタックの層で利用されるマルウェア／攻撃ツールを含む。プロトコルの逸脱を検出すると、チャネル痕跡上の複数の第２のレベルに従ったある第２のレベルで、オフライン・ネットワーク・トラフィックが処理される。第２のレベルのカバート・チャネルの痕跡は、標準での復号化プロセス、キーイン・プロセス、管理検出プロセス、ヘッダ・チェック・プロセス、またはフィールド・チェック・プロセスを含む。この標準は、たとえば、ＨＴＴＰおよびＴＣＰ／ＩＰを含むことができる。本発明はまた、マルウェアが、検出を回避するための逸脱なしに標準プロトコルを使用しているかどうか判定する。本発明は、攻撃者の活動、影響を受けたユーザおよびマシン、盗まれた知的財産、ならびに攻撃者の属性および動機に関する手がかりを正確に詳述する包括的なレポートを生成する。

【００２９】

したがって、本発明のシステムは、偽陽性を除去して、本格的な処理が第２の段階で必要かどうかについての高信頼度テストを作成するための第１の段階での優先順位付けを含む、２段階の処理を利用する本発明は、テンプレートを調整して、新規の攻撃の痕跡を見つける。このようにして、攻撃者のプロファイル・ツールは自動的に調整可能であり、新規の攻撃の痕跡が見つかると変化する。

【００３０】

図２には２つのネットワーク・ノードＡおよびＢが示してあり、これらは、標準プロトコル・スタックに従って構成可能な通信チャネルを介して互いに通信する。

【００３１】

図示したように、ノードＡおよびノードＢは、様々なネットワーク上でのパケットの伝送用に採用されているものなど、標準プロトコル・スタック上で互いに通信する。標準プロトコル・スタックの例には、ＯＳＩ参照モデルおよびＴＣＰ／ＩＰが含まれる。標準プロトコル・スタックは、アプリケーション層、トランスポート層、ネットワーク層、リンク層、物理層など、様々な標準層１～ｎを含む。

【００３２】

図３には、層１～ｎなど複数の標準層を有する、図１の標準プロトコル・スタックが示してある。アプリケーション層での例示的な標準層は、ＨＴＴＰ、ＦＴＰ、ＴＬＳ／ＳＳＬ、ＳＭＴＰ、ＰＯＰ、およびＩＭＡＰを含む。トランスポート層での例示的な標準層は、ＴＣＰおよびＵＰＤを含む。ネットワーク層での例示的な標準層は、ＩＰ、ＩＣＭＰ、およびＩＧＭＰを含む。リンク層での例示的な標準層は、ＡＲＰ、ＤＳＬ、ＩＳＤＮ、ＯＳＰＦ、およびイーサネット（登録商標）、ならびに他の任意の有線または無線の標準リンク層を含む。

【００３３】

図４には、サービスとしてのソフトウェア（ＳａａＳ）のプラットフォーム上に本発明を実装する、システムのブロック図が示してある。ＳａａＳは、ソフトウェアのライセンシングおよび配信のモデルであり、ここで、ソフトウェアが契約に基づいてライセンスされ、一元的にホスティングされるか、または配布される。ＳａａＳは、健康、金融、サイバー・セキュリティ、工業、輸送、製造、建設のサービスを含むが、それだけに限定され

ない、多種多様なサービスを加入者に提供することができる。ＳａａＳプラットフォームは、１つまたは複数のサーバのアプリケーション／ウェブ・サーバ・クラスタを含み、これが、１つまたは複数のデータベースのデータベース・サーバ・クラスタと通信する。

【００３４】

ＳａａＳプラットフォームを使用して、複数のサービス加入者に提供されるアプリケーション・サービスを実現することができる。たとえば、第１および第２のサービス加入者はそれぞれ、１つまたは複数のファイアウォールのファイアウォール・クラスタを介したインターネット上で、独立したアプリケーション・サービスを、団体または組織内の個々人または参加者に提供することができる。このようなＳａａＳの１つをクラウド上に実装して、医療、健康、金融、マルチメディア、輸送、ロジスティックスなど、様々な産業にサービス提供することができる。

【００３５】

一般に、本発明が実装されるネットワークは、複数の専用接続または公衆接続されたノードを含み、これは、１つまたは複数のプロセッサ・ノード、またはサーバもしくはサーバおよび／またはノードのクラスタを含み、これらは１つまたは複数のリンクを介して情報を交換できるようになっている。例示的なネットワークは、ＷＡＮ、ＬＡＮ、ＰＡＮ、インターネット１２０、ならびにＢｌｕｅｔｏｏｔｈ（登録商標）またはエクストラネットなどのアドホック・ネットワークのうち、任意の１つまたは複数を含む。インターネット１２０は、一群の相互接続された（公衆および／または専用）ネットワークであり、これらは、１組の標準プロトコルによって互いにリンクされて、地球規模の分散ネットワークを形成する。ノードは、１つまたは複数のプロセッサ・ユニット（ソフトウェアもしくはハードウェア、もしくは仮想ノード）、および／または、情報を処理し、かつ／または分散機能を実行する、ネットワーク内のいずれかに配置された装置を含む。任意のノードまたはノードを有する任意の構成要素は、ハードウェアまたはソフトウェアで仮想化することができる。様々なタイプのノードは、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、および処理された情報を送信する送信機ノードを含むことができる。ノードの例には、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、入口ノード、出口ノード、ユーザ・インターフェース・ノード、アカウンティング・ノード、管理ノード、コンテンツ・デリバリ・ノード、選択ノード、センサ・ノード、有線ノード、無線ノードなどが含まれる。

【００３６】

一実施形態では、本発明のシステムは、ネットワークを介して複数のユーザ装置とインターフェースするように構成された、１つまたは複数のサーバを備える。複数のユーザ装置は、１つまたは複数の第１のユーザ装置、および１つまたは複数の第２のユーザ装置とすることができ、これらは、個別に、またはグループもしくはダブグループで動作する。システムの各ノードは、任意の適切なネットワーク・モデルに従って互いに接続することができ、このモデルには、クライアント・サーバ・モデル、ならびに階層型モデルもしくは分散型モデルが含まれる。リンクは、２つのノードが、互いに情報を伝達することのできる任意の媒体を含む。例示的なリンクには、それだけには限らないが、有線、ファイバ、ケーブル、または無線のリンク（たとえば、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＵＷＢ、ＵＳＢなど）が含まれる。通信チャネルは、コンテンツを配布するためのリンクとともに使用される任意のチャネルを含み、このコンテンツは、ノード、ノードもしくは装置で実行されるアプリケーション、対象物（たとえば、車両、人々）、またはセンサから得られるデータを含むことができる。

【００３７】

図４には、３人のサービス加入者が加入しているクラウド・サービスが示してある。加入者それぞれは、完全処理および侵入レポート生成のために、または送信された悪質なツール・トラフィックについてマルウェア・プロトコル・デコーダが存在するという通知を受信するために、オフライン・ネットワーク・トラフィックをＳａａＳに送信する。登録

後、顧客は、少量のトラフィックを送信して、デコーダをテストすることができるようになる。企業の（フリーではない）ｅメール・アドレスだけを登録することができる。これにより、マーケッティングのリードが可能になり、試験的なトラフィックをセキュリティ・サイトに送信して、悪質なメッセージのデコーダが攻撃者のツールに対して機能するかどうかチェックするという、攻撃者のスパイ技術が防止される。

【００３８】

図５には、ユーザ向けの様々なアプリケーションを開発する、図４のＳａａＳで使用されるアプリケーション開発システム３００の例示的なブロック図が示してある。製品配布は、フル機能のクラウドベースのソリューションと、インターネット・アクセスのないネットワーク用の比較的頑強性に劣る採用可能なソリューションとの両方から構成されることになる。採用可能なバージョンは、機密性の高い組織の詳細について法規制またはプライバシーに関心のあるクライアントに適用可能である。処理するために送信される機密性の高いデータのみが、攻撃者に現在送信されているデータになるので、製品のクライド・インストール・バージョンを使用することが比較的有利である。

【００３９】

アプリケーション開発センタ３０４Ａ、アプリケーション管理センタ３０４Ｂ、および運営センタ３０４Ｃは、インターネット１２０などのネットワークを介して、アプリケーション開発ポータル（ＡＤＰ）３０２に接続される。ＡＤＰ３０２は、ネットワーク１２０を介して、ユーザ装置３０５、３０８、３１６と、アプリケーション開発サポート・センタ３０４Ａ～Ｃと、アプリケーション開発システム（ＡＤＳ）３３０との間にゲートウェイを設ける。ＡＤＳ３３０は、アプリケーション開発者、レビュア、ユーザ、管理者、および他の参加者が互いに通信するのに必要なユーザ・インターフェースを提供し、これにより、たとえばアプリケーション開発のユーザ／参加者は互いに対話できるようになる。このようなアプリケーション開発は、クラウド・システム上で実行してもよい。

【００４０】

開発されたアプリケーションのユーザは、個々のユーザ３０３または３０６（モバイル装置３０５および３０８）、ユーザ３１４（固定したワークステーション３１６）のユーザ・グループ３１０Ａ（またはユーザ・サブグループ）とすることができる。システムのユーザは、アプリケーション開発者３１０Ｂおよび管理者３１０Ｃ、ならびにアプリケーションを開発または使用するために図５のシステムを使用する他の任意の人とすることもできる。このようなユーザは、専門家、開発者、テクニカル・サポート、アカウンティング、エキスパート、またはアプリケーションへの他の任意の参加者とすることができる。ユーザ装置３０５、３０８、３１６でのユーザ３０３、３０６、３１４には、患者、医師、医療従事者、コンサルタント、供給業者、アプリケーション開発者、コンテンツ開発者、金融機関、保険会社などが含まれ得る。あるいは、このユーザは、アプリケーション開発センタ３０４Ａ、アプリケーション管理センタ３０４Ｂ、または運営センタ３０４Ｃに登録された政府側の権限者でもよい。

【００４１】

ＡＤＰ３０２は、アプリケーション・ポータル・データベース３４０へのアクセスを実現し、このデータベースが、それぞれのアプリケーション開発プロセスに登録され、またはそれに関連した全ての参加者／ユーザについてのユーザ情報を記憶する。ＡＤＰ３０２は、参加者が、ユーザＩＤおよびパスワードを用いて、アプリケーション開発サーバ３３０にログオンするための手段を提供する。ユーザＩＤに関連したアクセス権に基づいて、ＡＤＰ３０２は、開発者、管理者、レビュア、医療従事者、教師、学生、または他の任意のタイプのユーザなどとして、この参加者を認証する。最後に、ＡＤＰ３０２は、記憶された情報を、ＡＤＳ３３０とサポート・センタ３０４Ａ～Ｃとの間で同期する。本発明のシステムおよび方法によって作成された環境を介して、たとえば、加入ベース、または他の営利もしくは非営利の仕組みにおいて、一元的または分散してホスティングされる方式でアプリケーションをユーザに提供することができる。

【００４２】

図６には、図４のＳａａＳで利用される様々なモジュールとのインターフェースのブロック図が示してある。本発明は、グラフィック・ユーザ・インターフェース（ＧＵＩ）と、製品機能へのプログラムによるアクセスとの両方を提供する。ＧＵＩは、複数のオペレーティング・システムで利用可能な標準のウェブ技術を活用する。リプレゼンテーショナル・ステート・トランスファ（ＲＥＳＴ）やシンプル・オブジェクト・アクセス・プロトコル（ＳＯＡＰ）のインターフェースなど、標準のウェブ駆動技術を用いて、外部のプログラムによるアクセスがユーザに利用可能となる。標準のウェブ技術を使用することで、広く利用可能なオペレーティング・システム・プラットフォーム、ウェブ・ブラウザ、およびプログラミング言語を使用して、プログラムまたはウェブ・ブラウザを介したシステムとの対話が可能になる。さらに、ウェブ標準技術を使用することで、ユーザは遠隔で製品と対話できるようになる。ユーザは、もっぱらＧＵＩを介して、発明したものと対話してもよいが、製品へのプログラマチック・インターフェースによって、迅速に内容を解析にかけ、タスク状況をチェックし、必要に応じてレポートを受信するための開発者リソースがユーザに提供される。大組織、および他のヘビーユーザは、プログラマチック・インターフェースを活用して、その組織のセキュリティ・フレームワークとのシームレスな統合を可能にしてもよい。

【００４３】

図７には、図６の製品強化モジュールのブロック図が示してある。本発明は、製品強化として分類された複数の機能を介して利用可能な機能に影響を及ぼす能力を、ユーザに与える。本発明の開発者は、製品強化フィードバック・メカニズムを用いてユーザが要求する機能を利用して、要求条件の設定および優先順位付けを支援する。製品強化フィードバックは、公表されているような役割を果たさないか、または現在の機能を強化するものとして分類してもよい。公表されているような役割を果たさないことは、プロセッサにとっての報告された侵入データの誤りもしくは欠落か、または製品機能の別の部分の誤りのいずれかとして分類することができる。現状機能の強化は、完全に新規の侵入メッセージ・プロセッサへの要求、または既存の侵入メッセージ・プロセッサへの拡張からなる。異常終了のタイプまたは強化への要求にかかわらず、本発明により、ユーザは、サポートする内容を提供して、開発者がユーザの要求に迅速に取り組めるようにすることが可能になる。内容の提供には、暗号鍵、マルウェア、マルウェアもしくは侵入のレポート、作成レポート、または処理およびレポート作成の作業を支援できる他の付随情報が含まれ得る。

【００４４】

図８には、図１のシステムの動作層の例示的なブロック図が示してあり、このシステムは、サービス加入者向けに開発したアプリケーションに本発明を実装する。この実施形態によれば、このシステムは、バックエンド・システム５３０、およびフロントエンド・システム５６０を備える。フロントエンド５６０は、開発したアプリケーションにアクセスして、それを使用するためのユーザ・インターフェースを、加入サービスのユーザおよび参加者に提供する。バックエンド・システム５３０は、システム管理、課金、マーケティング、広報などのために使用される。フロントエンド・システム５６０によって、アプリケーション・センタ５６２へのユーザ・アクセスが可能になり、このセンタは、バックエンド・データベース５４２Ａおよび５４０Ａにアクセスする。フロントエンド・システム５６０は、ユーザ装置５５０および５５２を介して、ユーザおよびユーザ・グループのセッションへの対話型アクセスを参加者に提供する。ユーザは、インターネット１２０を介して、または有線ネットワーク５２４および／もしくは無線ネットワーク５２６を介して、フロントエンド・システム５６０およびバックエンド・システム５３０とインターフェースする。バックエンドでは、専用ネットワークまたは公衆ネットワークでもよいネットワークを介して、ユーザ装置５０８がＡＤＰ３０２に接続される。例示的な一実施形態では、ユーザ装置は、定義されたアクセス権に応じて、たとえば、ブラウザまたは他の任意の適切なアプリケーションもしくはアプレットだが、それだけに限定されないネットワーク・アクセス・アプリケーションを実行して、バックエンド・システム５３０またはフロントエンド５６０にアクセスする。このアクセス権は、たとえば様々なＥＡＬレベルに従

って、複数レベルのアクセス制御の下で、複数レベルの管理特権に依存していてもよい。ユーザ５１０、５５２、または５５０には、ログイン・セッションおよび／または複数レベルの認証を経ることを要求してもよい。

【００４５】

図８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つまたは複数の負荷分散装置５３４Ａ、５３４Ｂに結合されたファイアウォール５３２を備える。さらに、負荷分散装置５３４Ａ～Ｂは、１つまたは複数のウェブ・サーバ５３６Ａ～Ｂに結合される。ウェブ・サーバ５３６Ａ～Ｂは、１つまたは複数のアプリケーション・サーバ５３８Ａ～Ｃに結合されており、このアプリケーション・サーバのそれぞれが１つまたは複数のデータベース５４０、５４２を含み、かつ／またはそれにアクセスし、このデータベースは一元的なデータベースまたは分散データベースでもよい。負荷分散装置５３４Ａ～Ｂに結合しているウェブ・サーバ５３６Ａ～Ｂは、負荷分散機能を実行して、加入者、参加者、ユーザ、開発者、または管理者の要求をアプリケーション・サーバ５３８Ａ～Ｃのうちの１つまたは複数に転送することによって実行される最適なオンライン・セッションを実現する。アプリケーション・サーバ５３８Ａ～Ｃは、データベース・マネジメント・システム（ＤＢＭＳ）５４６および／またはファイル・サーバ５４８を備えてもよく、これらが、１つまたは複数のデータベース５４０、５４２へのアクセスを管理する。図７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および／または５３８Ｂが、参加者５０６、５１０、５５２にアプリケーションを提供し、このアプリケーションは、電子インターフェース、アプリケーション内容、参加者プロファイルなどを含む。コンテンツのいくらかは、アプリケーション・サーバ５３８Ａおよび／または５３８Ｂに記憶されたコードを用いて生成され、他のいくらかの情報およびコンテンツは、必要なデータとともに、アプリケーション・サーバ５３８Ｃを介してデータベース５４０、５４２から取り出される。アプリケーション・サーバ５３８Ｂはまた、実行可能ファイルへのアクセス権をユーザ５０６、５１０、５５２に提供してもよく、この実行可能ファイルは、ダウンロードしてユーザ装置５５０、５０８、５５２にインストールして、適切な仮想アプリケーション環境を作成することができるが、これは、特定のアプリケーション、ユーザ、またはユーザ・グループ向けに調整される、商用、ブランディング、またはマーケティングの機能の有無にかかわらない。

【００４６】

一元的または分散型のデータベース５４０、５４２は、とりわけ、参加者に配布可能なコンテンツおよびアプリケーションの内容を記憶する。データベース５４０、５４２はまた、様々なタイプの参加者、開発者、管理者、ユーザ・グループ、医療従事者、教師、学生、アプリケーション開発センタ、アプリケーション管理センタ、管理センタ、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、ソーシャル・ネットワーク・データ、ユーザ属性、参加者属性、開発者属性、マス・コラボレーション・データ、順位付けデータ、コンプライアンス・データ、認可データ、課金ルール、第３者との契約ルール、政府からの要件などに関連し、またはそれらに関連付けられる、取出し可能な情報を記憶する。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、必要に応じて、前述のデータの一部または全部を処理し、関連付けることができる。たとえば、統計データは、条件、ユーザ進捗、スケジュール、などに関連する。

【００４７】

図９は、図８のウェブ・サーバによって実装される、マルチプロセッシング・システムのアーキテクチャの図である。このシステムは、複数のサブシステム、すなわちウェブ・アプリケーション、ジョブ制御装置、およびジョブ実行装置からなる。サブシステムのそれぞれは、水平方向にスケーリングされるように設計され、クラウドベースのサービスとしてのプラットフォームのプロバイダに採用されることになる。全体として、このシステム全体は、単一のマシン上で実行することができる。あるいは、サブシステムの各インスタンスは、別個のマシンに採用される。ウェブ・アプリケーション・サブシステムは、外部システム・インターフェースおよび静的なウェブ・コンテンツをエンドユーザに提供す

る。これはまた、内部の通信インターフェースを使用して、ジョブ制御装置と通信し、それを制御する。アプリケーションを実行するクラスタ化されたウェブ・サーバへのアクセスは、既製の負荷分散ソリューションを用いてバランスをとることになる。ジョブ制御装置サブシステムは、ウェブ・アプリケーションの指示通りに、ジョブのキューを維持する。ジョブは、キューから取り出され、そのジョブ処理のスロットが利用可能になると、ジョブ実行装置のインスタンスに割り当てられる。ジョブのキューが大きくなりすぎると、ジョブ制御装置は、ジョブ実行装置の追加インスタンスを使用可能にするよう、サービスとしてのプラットフォームのプロバイダに要求することができる。逆に、ジョブ実行装置の多くのインスタンスが利用されていない場合、ジョブ制御装置は、これらのインスタンスを使用不能にすることができる。ジョブ実行装置のサブシステムは、ジョブ制御装置から割り当てられたジョブを実行し、その結果を戻す。マルウェア検出論理が、このサブシステムで生じることになる。ジョブ実行装置の単一のインスタンスは、複数の検出ワークフローを通して単一パケットを処理することと、複数のジョブを同時に処理することの両方について、マルチスレッド化されるように設計される。

【００４８】

図１０には、図４のＳａａＳへの認証およびプロファイリングを実施する例示的な図が示してある。一実施形態では、装置７１５－１～７１５－ｎのユーザは、特定のシステム内に登録してもよく、ネットワーク７１０（たとえばインターネット）に接続してもよい。装置７１５－１～７１５－ｎのそれぞれは、コンピュータ、ワークステーション、モバイル装置、ＰＤＡ、ｉＰａｄ（登録商標）、ラップトップ・コンピュータなどでもよい。サーバ７０５は、ソーシャル・ネットワーキング・システム７００において維持してもよく、またサーバ７６０を含んでもよい。サーバ７６０は、サーバ７０５の機能の任意の組合せを含んでもよい。サーバ７６０はまた、ネットワーク７１０を介して、ソーシャル・ネットワーキング・システム７００のその他の部分に接続してもよい。サーバ７６０は、サーバ７０５と同じネットワーク上、またはサーバ７０５とは異なるネットワーク上に配置してもよい。サーバ７６０は、オンライン協働システムを実現するのにソフトウェアが使用した他のインスタンスを実行または操作してもよい。サーバ７６０は、外国または国内の他の団体または実体によって、実行または操作されてもよい。サーバ７６０は、外国または国内の、同じだが別々の場所にある団体または実体によって、実行または操作されてもよい。

【００４９】

サーバ７０５は、ユーザ・プロファイル・データベース７２０、ユーザ・データベース７２５、アプリケーション・データベース７３０、アプリケーション・プロファイル・データベース７３５、ソーシャル・ネットワーク・データベース７４０、認証データベース７４５、アクセス制御データベース７５０、またはその任意の組合せを含む、複数のデータベースに接続してもよく、またはそれを含んでもよい。ユーザ・プロファイル７２０は、任意のユーザについて、コンテンツ、１週間のスケジュール、割当て、リソース、期日、議論、熟考、コンテンツの概要、コンテンツのレビュー、テスト、他の任意のコンテンツもしくはアプリケーションの内容情報、またはその任意の組合せを記憶してもよい。

【００５０】

ユーザ・データベース７２５は、システムを使用するユーザについての任意の情報を記憶してもよい。ユーザ・データベース７２５は、具体的事例、アプリケーション、団体、または会社と密接に関係している、全てのユーザの登録簿を記憶してもよい。一実施形態では、このようなユーザは、ネットワーク・アドレス、たとえばＩＰアドレスに関連付けられており、このアドレスをユーザ・プロファイルに記憶してもよい。ユーザ・データベース７２５は、ユーザの名前、ユーザの特定のデータおよびコンテンツ、場所、アドレスについての情報、ユーザもしくは開発者もしくは管理者が入力するユーザについての情報、ユーザの活動および関心事、ユーザの教育、ユーザの職務経歴、ユーザの写真など、またはその組合せを記憶してもよい。

【００５１】

アプリケーション・データベース７３０は、システム７００が提供することがアプリケーションについての任意の情報を記憶してもよい。アプリケーション・データベース７３０は、コンテンツおよびアプリケーションの名前、識別子、数、説明、医療従事者、スケジュール、登録、過去のコンテンツ、将来のコンテンツ、コンテンツもしくはアプリケーションへの参加を許可されたユーザの数、アプリケーション構造、アプリケーションもしくはコンテンツの前提条件、ユーザ・グループ、またはその任意の組合せを記憶してもよい。

【００５２】

アプリケーション・プロファイル・データベース７３５は、自らの役割によるユーザについての情報を含め、ユーザまたはアプリケーションについての情報を記憶してもよい。たとえば、アプリケーション・プロファイル・データベース７３５は、患者が実行し終えたプログラム、患者が実行し終えた活動、患者が使い終えた健康製品の例、評価、順位付け、またはその任意の組合せについての情報を記憶してもよい。

【００５３】

ソーシャル・ネットワーク・データベース７４０は、このシステムのユーザについてのソーシャル・ネットワーキング情報を記憶してもよい。ソーシャル・ネットワーキング情報には、ユーザがつながっているそのユーザの知り合い、ユーザの交際範囲、ユーザのチャットでのつながり、ユーザのチャット履歴、ユーザのコミュニティ、ユーザに関連するコンテンツおよびアプリケーション、またはその組合せが含まれ得る。本明細書では、ユーザの交際範囲とは、このシステムのユーザに関連する１組の他のユーザを意味する。一実施形態では、ユーザは、その交際範囲を設定してもよい。本明細書では、ユーザのコミュニティには、このユーザがその一部であるとシステムによって識抜されているグループまたは団体が含まれ得る。コミュニティは、知り合いおよび交際範囲とは異なるが、それというのもユーザはコミュニティを直接変えることができないからである。プログラムまたはアプリケーションが終了したら、コミュニティを解散してもよく、または過去のコミュニティを維持してもよい。ソーシャル・ネットワーク・データベース７４０はまた、ソーシャル・ネットワーキング情報に関連する他の任意の情報を記憶してもよい。

【００５４】

認証データベース７４５およびアクセス制御データベース７５０は、このシステムにおける、セキュリティ、アクセス、または認証の情報を記憶してもよい。セキュリティまたは認証の情報には、ユーザのユーザ名、ユーザのパスワード、ユーザの識別情報を検証するのに使用されるセキュリティの質問、セキュリティの質問に対する回答、システムのどの部分にユーザがアクセスできるのか、またはその組合せが含まれ得る。

【００５５】

図１１は、図１のシステムによって処理するための侵入内容の提出を示すブロック図である。本発明により、ユーザは、完全処理および侵入レポート生成のためにオフライン・ネットワーク・トラフィックを送信し、または送信された悪質なツール・トラフィックについてマルウェア・プロトコル・デコーダが存在するという通知を受信することができるようになる。ユーザは、オフライン・ネットワーク・トラフィックを送信して、少なくとも１つの既存の悪質なツール・トラフィック・プロセッサが存在するかどうか検出してもよい。システムによる処理の後、悪質なツールが検出される場合、全ての潜在的なプロセッサを識別し、その悪質なツールに対抗する現在の機能のリストを提供するレポートが生成される。検出機能は、高信頼度のリスト、悪質なツール・トラフィック・プロセッサ全体に組み込まれた高度な初期検出機能、利用可能で高度な検出方法および処理方法の全てを使用することに基づいている。空のレポートは、関連する悪質なツール・トラフィックに対抗する任意の有望な処理機能が、本発明には現在ないことを示す。次いで、ユーザには、このユーザの送信された悪質なツール・トラフィックを認識でき、侵入活動においてそれを処理できるプロセッサの開発要求を、製品強化動作モジュールを介して提出する選択肢がある。そうでなければ、本発明が少なくとも１つの候補プロセッサを戻す場合、ユーザには、処理および侵入の完全なレポートを作成するためにトラフィックを送信する選

択肢がある。

【００５６】

ユーザは、プロセッサ機能レポートで識別されるように、侵入活動レポートの作成、および悪質なツール・トラフィックに対してリストに記載された詳細および活動について、オフライン・ネットワーク・トラフィックを送信してもよい。送信すると、本発明は、適用可能なプロセッサの決定を開始し、レポート生成のためにトラフィックの処理を開始する。この処理はバックグラウンドでただちに実行され、ユーザは、他の活動を実行し、または製品サイトを離れることができるようになる。処理は、復号化、暗号解読、または他の高度なリソースおよび非常に時間のかかる活動を含んでもよく、ユーザがタスク管理インターフェースを介して処理状況をチェックできる非対称処理および報告作業を必要とする。さらに、処理中には様々な高度のチェックが実行されて、適切なレポート詳細が確実に生成され、しかも潜在的な問題がユーザに強調表示される。処理中の高度なチェックはまた、送信されたオフライン・ネットワーク・トラフィックで使用される特定の悪質なツールを自動決定して、複数の潜在的な悪意あるツール・プロセッサが最初に検出されるときに非常に正確なレポート情報が確実に提示されるのに役立つ。

【００５７】

ユーザが送信したオフライン・ネットワーク・トラフィックが首尾よく処理されると、結果として、トラフィックを生成する（１つまたは複数の）悪質なツールについてのプロセッサ機能レポートに公表されている機能に一致する侵入データが作成される。たとえば、プロセッサ機能の公表されているリストが、悪質なツールの機能または収集された疑わしい活動に一致しない場合、開発者が新規のマルウェア・プロセッサを作製し、または既存のマルウェア・プロセッサを改良できるよう、ユーザは、製品強化動作モジュールを介して要求を提出してもよい。

【００５８】

悪質なツール・メッセージ処理は、機能しているように見えることがあるが、有用な侵入活動レポートを首尾よく作成してはいない。これが生じる症状は、レポートに入力される無意味なデータ、またはデータが欠落したレポートである。この挙動は様々な問題に起因する場合があり、こうした問題には、様々な中間処理検証チェックにもかかわらず生じる、選択されたプロセッサの誤識別、本発明が処理モジュールをそのために作製した悪質なツールの新規の変形形態もしくはカスタマイゼーション、またはプロセッサ内でのソフトウェア誤りが含まれる。ユーザは、製品強化動作モジュールを介して要求を送信して、処理機能不良の原因を調査してもよい。

【００５９】

悪質なツールによっては、高度な暗号解読処理を必要とする場合がある。この場合、本発明は、暗号攻撃、鍵発見、および同じ悪質なツールの他のサンプルで観察される暗号鍵の使用を含め、様々な技術を使用して暗号解読を試みようとする。自動化されてほぼすぐ使える暗号解読技法が機能しないか、または利用可能でない場合、それよりも期間の長い暗号解読技法を要求してもよいことがユーザに通知される。その時点で、ユーザはまた、追加の悪質なツール・トラフィック、任意の侵入解析ノート、他の方法で得られた暗号鍵、または悪質なツールへの感染を促されて、他の方法では場合によっては不可能な、またはリソースおよび時間をかなり要する暗号解読処理が可能になる。本発明は、付随情報から暗号解読するのに必要となる暗号鍵を抽出しようと試みる、様々な自動処理を有する。鍵抽出のための付随情報のこの処理は完全自動でもよく、それにより、悪質なツール・トラフィックが、暗号解読用のプロセッサに再注入されることになる。鍵抽出の自動処理が異常終了する場合、本発明は任意選択として、相対的に期間の長い様々な解析技法を利用して、鍵抽出など暗号解読を可能にする手法または技法を試みることができる。可能なら、全てのステップおよび推定完了時間が、タスク管理インターフェースを介してユーザに伝達される。

【００６０】

図１２は、図４のＳａａＳによって利用される入れ子型のプロトコル処理のブロック図

である。侵入を発見すると、複数の理由により、集中して処理する期間が必要となるが、それというのも、顧客は、悪質な通信を復号化し、それに続いて作業期間を最小限に抑えたいと望むからである。クラウド・インフラストラクチャを活用して、修正を処理するためのアップグレードの迅速な導入、攻撃の合間に攻撃者が既存の悪質なＡＰＴツールを修正するときの適合処理、およびコスト上限内の処理要求を満たすための自動処理インフラストラクチャのスケーリングを可能にする。本発明は、既に収集されたサイバー攻撃ツールのメッセージを処理するという位置付けである。したがって、あるタイプのリアルタイム・ネットワーク収集装置および処理装置とは異なり、サーバが、適時にデータを処理するのに十分な速さではないという危険性はほとんどない。キュー管理システムを実装して、確実に全ての顧客が適時にレポートを受信できるようにする。

【００６１】

ＡＰＴネットワーク通信は、複数の符号化、難読化、データ隠蔽、および暗号化の技法をしばしば使用し、これらは、多段の識別および処理を必要とする。攻撃についての詳細情報を正確に報告するために、マルウェアが使用するネットワーク通信プロトコルを処理して、使用可能なフォーマットにしなければならない。本発明は、再使用可能な処理ブロックを利用して、入れ子型のプロトコル処理、復号化、および報告するのに適したフォーマットにデータを変換するために必要な暗号解読を実行する。プロトコル・プロセッサはまた、適切なメタデータを抽出して、報告で使用される鍵となる情報を提供する。

【００６２】

本発明は、物理層からアプリケーション層までの後続の処理および報告のために、通信データおよび抽出データの再構成に必要な全てのプロトコル層を処理する。これには、適切な場合、デフラグメンテーションおよびセッション化などの態様が含まれる。プロトコル・プロセッサは、層を認識しており、マルウェアが生成する全ての関連情報を検出および抽出するのに必要な、全てのプロトコル・フィールドにアクセスすることになる。本発明は、知的所有権および非標準のプロトコルを扱う。本発明はまた、インターネット技術タスクフォース（ＩＥＴＦ）、コメント要求（ＲＦＣ）仕様などの既存の業界標準を侵害する方式で既存のプロトコルが使用されるときに、オフライン・ネットワーク・トラフィックを処理する。

【００６３】

処理されているプロトコルが、符号化スキームを使用してデータを送信または難読化するとき、本発明は、適切な復号化スキームを利用して、データを後続の処理または報告に適したものにする。たとえば、本発明は、Ｂａｓｅ６４符号化、ユーユー符号化、および同様の標準符号化スキームを復号化する。本発明は、非標準のアルファベットを用いるＢａｓｅ６４符号化、またはビット逆転とそれに続くＢａｓｅ６４符号化のように、データを難読化しようとする非標準符号化スキームをも扱う。

【００６４】

図１３は、解析装置Ａを示す、検出段階および解析段階を有するＤＮＳカバート・チャネルの一例の流れ図である。

【００６５】

組織のセキュリティ監視ソフトウェアが、そのネットワーク・セキュリティ監視インフラストラクチャによる通知を介して、カバート・チャネルを発見する。組織のセキュリティ・チームが、このセキュリティ通知に関連するトラフィックの収集をただちに開始して、詳細な自動侵入解析について本発明に送信する。組織は、可能性のあるプロセッサを識別するためにオフライン・ネットワーク・トラフィックを送信し、これによって、侵入活動レポートを生成することができるようになる。可能性のあるマルウェア・プロセッサを識別するためだけのトラフィックを最初に送信するので、本発明は、侵入活動生成のための可能性のある２つの完全処理モジュールを報告する。すなわち、一方は、ドメイン・ネーム・システム（ＤＮＳ）プロトコルを使用する悪質なツール・プロトコルであり、もう一方は、ＤＮＳ上で動作するカバート・チャネルである。有望なプロセッサが存在するということを確信して、組織のセキュリティ・チームは、完全処理のためにオフライン・ネ

ットワーク・トラフィックを送信することを選択する。

【００６６】

本発明は、２つの潜在的なプロセッサを識別し、互いに復号および暗号解読を試みる。両方の候補プロトコルがＤＮＳパケットから構成されているにもかかわらず、ＤＮＳパケットのコンテンツは、ＤＮＳを使用する悪質なプロトコルに応じて異なるものになる。本発明のプリプロセッサは、ＤＮＳトラフィックを認識し、基本となるネットワーク層フラグメンテーション、またはトランスポート層セッション化にかかわらず、ＤＮＳラフィックが確実正確に処理されるように、必要に応じて最良の第三者開発およびカスタム開発されたＤＮＳ処理技法を使用する。ＤＮＳトラフィックが解析され、次いで、プロセッサＡおよびプロセッサＢに送られて、さらに検証および侵入活動処理が実行される。

【００６７】

プロセッサＡは、ＤＮＳメッセージを検査し、ＤＮＳクエリ・ホストネームの最下位レベル領域（ＬＬＤ）部分のＤＮＳクエリでの、Ｂａｓｅ３２符号化されたコマンドを検索する。プロセッサＡ用のＢａｓｅ３２デコーダは、ホストネームのＬＬＤ部分を復号化しようと試み、不適切な文字が生じることによって異常終了する。プロセッサＡは、この異常終了を制御装置に報告する。ネットワーク収集が破損しているか、プロセッサＡに関連するマルウェアが、そのプロトコルを変更したか、またはこれは、プロセッサＡによって処理されるプロトコルに関連していない異なるマルウェアである。

【００６８】

プロセッサＢは、ＤＮＳメッセージを検査し、既知のＤＮＳトンネリング・プロトコルに関連するトラフィックを検索する。このプロトコルは、アドバンスド・パーシスタント・スレット（ＡＰＴ）攻撃者によって使用されてきたものである。このプロトコルは、ＧＺＩＰ圧縮されたオフライン・ネットワーク・トラフィックのＢａｓｅ３２、Ｂａｓｅ６４、またはＢａｓｅ１２８符号化のいずれかを使用する。プロセッサＡのように、被害者からＡＰＴ攻撃者への情報は、ＤＮＳクエリ・ホストネームの最下位レベル領域（ＬＬＤ）での符号化された情報からなる。プロセッサＢは、被害者と攻撃者の間で送られるときにＭＤ５ハッシュ化されたパスワード、ならびにＤＮＳカバート・チャネル・ツールのバージョンを識別および抽出する。このツールのバージョンは「０．７．０」である。

【００６９】

侵入活動の抽出を継続するには、ツールのバージョンもＡＰＴ攻撃者のパスワードも必要ではないが、両方とも、攻撃者の可能性のある属性に対する潜在的な手がかり、または他の攻撃を追跡して法執行を支援することになる情報を提供する。この場合、ツールのバージョンは、プロセッサＢが識別および抽出するにはどうでもよいものである。ハッシュ化されたパスワードを暴露するには、追加処理が必要となる。プロセッサＢは、ＭＤ５ハッシュを適切なパスワード・デコーダ・モジュールに伝達し、これが、様々な力ずく、辞書、およびハッシュ事前計算（レインボー・テーブル）技法を使用して、攻撃者が使用するパスワードをプロセッサＢに戻して報告する。この場合、パスワードは「メドベージ」であり、これはロシア語で「熊」であり、ことによると、ＡＰＴ攻撃者は、この場合ロシア出身であることを示す。

【００７０】

プロセッサＢは、パスワードおよびバージョン番号の抽出と並行して、侵入活動の抽出を継続する。Ｂａｓｅ３２およびＢａｓｅ６４のデコーダは両方とも、不適切な文字が存在することに起因する異常終了を報告するが、Ｂａｓｅ１２８デコーダは正常終了を報告する。次いで、プロセッサＢは、ＧＺＩＰ圧縮のトラフィックを検査し、正常終了する。プロセッサＢは、非圧縮データを解析し、カバート・チャネル・トラフィックの保守および管理用のヘッダ情報からなる、既知のＤＮＳトンネリング・プロトコルとして、このプロトコルを認識する。プロセッサＢは、攻撃者へ向かうアップストリームおよび被害者へ向かうダウンストリームの双方向で収集されたトラフィックを、デフラグおよび再構築する。このプロセッサは、攻撃者が、そのトラフィックを復号化および解析するため、標的に対する搾取行為を維持できるようにする、同じトラフィック管理技法を使用することが

できる。プロセッサＢは、数多くのＤＮＳパケットにわたって観察される、フラグメント化されたカバート・チャネル・メッセージを再構築し、次いで、明らかにされて再構築されたトラフィックを解析し、これは、基本となる通信がＩＰパケットであることを示す。抽出されたＩＰパケットは、適切なメタデータでマーキングされて、このパケットを元のＤＮＳカバート・チャネル通信に関連付け、組織に戻すためＰＣＡＰフォーマットで保存される。

【００７１】

次いで、抽出されたパケットは、顧客のオフライン・ネットワーク・トラフィック送信がとるはずの同じ処理および報告の流れで、可能性のある悪質なトラフィック処理のために全てのモジュールによって処理するよう、制御装置に再注入される。この目的は、可能性のある悪質なツール・トラフィック、およびＩＰアドレスやポートなどのトラフィック・インジケータについて、これまで隠されていたネットワーク通信を検査することであり、このＩＰアドレスやポートは、プロセッサＢからのカバート・チャネル上で実行される報告と組み合わせると特に価値がある。元のトラフィックだけが組織の１つのＤＮＳサーバのＩＰから来ると思われるにもかかわらず、抽出されたパケット上で実行される、この第２ラウンドの処理の結果、被害者のネットワークでのＡＰＴ攻撃者と１２のＩＰアドレスとの間の侵入活動が発見されることになる。

【００７２】

処理の全ての段階全体を通して、侵入に関連するトラフィックから抽出できる全ての情報が、ＸＭＬなどの構造化メタデータ・フォーマットでレポートに書き込まれる。ＩＰアドレス、ＴＣＰおよびＵＤＰのポート、あらゆる固有のマルウェア識別子、ならびに全てのマルウェア・コマンドおよび応答のコードが、人間の読めるフォーマットに変換される。抽出されたＩＰアドレス、関連するＤＮＳホストネーム、パスワード、および注入識別値を含め、ＤＮＳカバート・チャネル内で使用される全てのメタデータが、保存され、報告される。これは、被害者および行為者の侵入データについても処理された、カプセル化カバート・チャネルの下で隠された通信チャネル用に保存されたメタデータに加えられる。

【００７３】

完了すると、機械読取り可能なレポートとして、または本発明のグラフィカル・ユーザ・インターフェース（ＧＵＩ）を介して目に見えるものとして、レポートが組織に利用可能となる。組織は、まずＧＵＩを介してこのレポートを確認し、そのネットワーク内の被害者の１２のＩＰアドレスを記録する。組織は、その情報を組織のマシンの機能と関係付け、次いで、抽出され、これまで隠されていたネットワーク通信を検査して、ＡＰＴ連邦政府の契約のために解析されるデータ、およびこの契約において使用するための企業が開発した知的所有権下にあるアルゴリズムを、攻撃者がひそかに抽出したことが分かる。ＧＵＩレポートの最初の確認の後、組織は、その企業セキュリティ事故報告の枠組みで受け入れるために、プログラムによるレポートをダウンロードし、関連のある侵入トラフィックをさらに送信して報告を拡充する。

【００７４】

図１４は、解析装置ＡおよびＢを示す、検出段階および解析段階を有するＤＮＳカバート・チャネルの一例の流れ図である。組織は、その侵入検知システムを介して悪質だと識別されてきたオフライン・ネットワーク・トラフィックを送信する。組織のセキュリティ・チームは、詳細な自動侵入解析に供するために、侵入検知システムの警告に関連するトラフィックの収集をただちに開始する。組織は、可能性のあるプロセッサを識別するためにオフライン・ネットワーク・トラフィックを送信し、これによって、侵入活動レポートを生成することができるようになる。可能性のあるマルウェア・プロセッサを識別するためだけのトラフィックを最初に送信するので、本発明は、侵入活動生成のための可能性のある２つの完全処理モジュールを報告する。有望なプロセッサが存在するということを確信して、組織のセキュリティ・チームは、完全処理のためにオフライン・ネットワーク・トラフィックを送信することを選択する。

【００７５】
本発明は、潜在的な２つのプロセッサを識別し、互いに復号および暗号解読を試みる。両方の候補マルウェア・プロトコルが、同じキーワード「ＢＡＮＡＮＡ」から始まるＴＣＰから構成されているにもかかわらず、この２つのプロトコルは、劇的に異なるコンテンツを継続する。両方のプロセッサは、さらなる処理が生じる前に発生するＴＣＰセッション化を利用するので、送信されたＰＣＡＰファイルが処理されて、ＩＰパケットからＴＣＰセッションを作成する。プロセッサＡとＢは両方とも、最初の「ＢＡＮＡＮＡ」チェックに一致し、したがって、ＴＣＰセッションが両方のプロセッサに送られて、さらに解析される。

【００７６】
プロセッサＡは、標準のＢａｓｅ３２符号化スキームで符号化された、ＧＺＩＰ圧縮されたデータに従う。プロセッサＡ用のＢａｓｅ３２デコーダは、ＧＺＩＰ圧縮されたデータを公表しない。データは誤ったフォーマットにあり、したがって、プロセッサＡが、誤り状況を制御装置に戻す。ネットワーク収集が破損しているか、プロセッサＡに関連するマルウェアが、そのプロトコルを変更したか、またはこれは、プロセッサＡによって処理されるプロトコルに関連していない異なるマルウェアである。

【００７７】
本発明のプロセッサＢはまた、キーワード「ＢＡＮＡＮＡ」から始まるＴＣＰデータをチェックするが、以下のデータがＬＺ４圧縮されることを見込む。ＬＺ４復元が試みられ、復元された悪質なトラックを首尾よく戻す。追加のチェックが実行されて、復元されたデータが文字列「ＦＩＮＩＳＨＥＤ」で終了し、正常に戻ることを確認する。この復元されたデータは、マルウェア用のコマンド符号語、３つのコロン、マルウェアの一意な識別子、３つのコロン、次いでコマンドの内容または被害者からのコマンドの結果、および最後には文字列「ＦＩＮＩＳＨＥＤ」から構成される。この場合、被害者に送信されたことが観察されるコマンドは、Ｅｘｃｅｌスプレッドシート用であり、これからのオフライン・ネットワーク・トラフィックが、ファイル・アップロードのコマンド応答としてマルウェア・コードでラベル付けされる。本発明のプロセッサＢは、有望なファイル・コンテンツを自動的に抽出し、どのタイプのファイルがＥｘｃｅｌファイルのヘッダの検査を介してサイバー攻撃者に伝送されたのかを検証し、侵入活動レポートの送達中にクライアントに送達するためのファイルを保存する。

【００７８】
この処理中、侵入に関連するトラフィックから抽出できる全ての情報が、ＸＭＬなどの構造化メタデータ・フォーマットでレポートに書き込まれる。ＩＰアドレス、ＴＣＰポート、あらゆる固有のマルウェア識別子、および全てのマルウェア・コマンドおよび応答のコードが、人間の読めるフォーマットに変換される。攻撃者が制御する被害マシンが攻撃者のサーバにアップロードするファイル名など、被害者に送信された全てのコマンド・コンテンツがリストに記載される。全てのコマンド応答もリストに記載される。ファイルが攻撃者にアップロードされる場合、キャプチャされた添付ファイルへのリンクが、実ファイル名（自動解析がファイル名を識別できるとき）か、独自のファイル名（元のファイル名を確認できないとき）のいずれかでリストに記載される。この場合、本発明のプロセッサＢはファイル名を関連付けることができ、したがって、レポートは、顧客のマシン上でファイルに名前が付けられるときに、そのファイルへのリンクを含む。

【００７９】
完了すると、機械読取り可能なレポートとして、または本発明のグラフィカル・ユーザ・インターフェース（ＧＵＩ）を介して目に見えるものとして、送信する組織にレポートが利用可能となる。組織は、まずＧＵＩを介してこのレポートを確認し、レポート検索機能を使用して、会社の極秘プロジェクトに関係付けられた文字列、および会社のクレジット・カード処理に関連付けられたデータを検索して、いずれのデータが攻撃者の手に落ちたのか確認する。さらに、顧客の情報セキュリティ担当者は、生成された侵入活動レポートを使用して、識別された７つのマシン上に、７つのマルウェアが存在することを迅速に

識別する。ＧＵＩレポートの最初の確認の後、組織は、その企業セキュリティ事故報告の枠組みで受け入れるために、プログラムによるレポートをダウンロードし、関連のある侵入トラフィックをさらに送信して報告を拡充する。

【００８０】

図１５は、解析装置ＡおよびＢを示し、この解析装置Ｂが４バイトのＸＯＲを使用する、検出段階および解析段階を有するＤＮＳカバート・チャネルの一例の流れ図である。組織は、その侵入検知システムを介して悪質だと識別されてきたトラフィックを送信する。組織のセキュリティ・チームは、実現可能で詳細な自動侵入解析に供するために、侵入検知システムの警告に関連するトラフィックの収集をただちに開始する。組織は、可能性のあるプロセッサを識別するためにオフライン・ネットワーク・トラフィックを送信し、これによって、侵入活動レポートを生成することができるようになる。本発明は、侵入活動生成のための可能性のある２つの完全処理モジュールを報告し、組織のセキュリティ・チームは、完全処理のためにオフライン・ネットワーク・トラフィックを送信することを選択する。

【００８１】

本発明は、可能性のある２つのプロセッサを識別し、互いにデータの復号を試みる。両方のプロセッサが、本質的にいくらかランダムなデータを受信することを予測しているので、いずれのプロセッサを実行すべきかを識別するための既知のパターンはデータ内に存在しない。本発明は、復元を試みることによってＺＩＰの変形形態が使用されるかどうか迅速に検証することができ、その結果、最初にそのプロセッサを実行することを選択する。プロセッサＡは、再構築されたＴＣＰストリームを、わずかに修正されたＺＩＰアーカイブとして処理しようと試みる。この変形形態を生成するマルウェアは、ＺＩＰファイルの最初の４バイト（「マジック・バイト」と呼ばれている）を取り除いて、検出を回避するが、ＺＩＰファイル・セントラル・ディレクトリをファイルの末尾に残す。プロセッサＡは、本発明のエントロピー・チェック・モジュールを使用して、オフライン・ネットワーク・トラフィックのコンテンツが、セントラル・ディレクトリまでのＺＩＰファイル・データである可能性が高いことを識別する。プロセッサＡは、セントラル・ディレクトリを分析し、ＺＩＰアーカイブに共通のマジック・バイトを、再構築されたＴＣＰストリームの先頭に追加し、次いで、想定したＺＩＰファイルを復元しようと試みる。復元ルーチンは、データを復元することができず、異常終了した復号を示す誤りコードを戻す。

【００８２】

プロセッサＢは、攻撃ツール・プロトコルに関連しており、これが、全ての伝送済みデータに４バイトＸＯＲを使用する。このツールを用いてこれまでに発見された攻撃では、ＡＰＴ行為者が、攻撃ごとにＸＯＲ鍵の暗号化変数を変更することが示されてきたが、被害者および攻撃インフラストラクチャとの間の、基本となる暗号化されたコマンドおよび応答は常に同じである。本発明のプロセッサＢは、ＴＣＰセッションを開始することになる７つのコマンドの、可能性のある２５６全ての暗号文を事前計算している。プロセッサＢは、ＨＴＴＰ　ＰＯＳＴコンテンツの第１の部分を、可能性のある全ての暗号文サンプルに照らしてチェックする。プロセッサＢの比較は正常終了し、暗号文に関連する４バイト鍵を、０ｘＤＥ　０ｘＡＤ　０ｘＢＥ　０ｘＥＦとして識別する。プロセッサＢは、侵入オフライン・ネットワーク・トラフィックを暗号解読モジュールに伝達し、この暗号解読モジュールが、鍵０ｘＤＥ　０ｘＡＤ　０ｘＢＥ　０ｘＥＦを使用して、全てのＨＴＴＰ　ＰＯＳＴコンテンツを暗号解読する。暗号解読モジュールは、暗号解読されたトラフィックをプロセッサＢに戻し、侵入活動通信からここで明らかとなったコマンドおよび応答が、解析および報告に利用可能となる。プロセッサＢは、被害者のネットワークとの間で双方向に侵入活動を処理するステップと、結果を侵入レポートに書き込むステップとを開始する。

【００８３】

完了すると、機械読取り可能なレポートとして、または本発明のグラフィカル・ユーザ・インターフェース（ＧＵＩ）を介して目に見えるものとして、組織にレポートが利用可

能となる。組織は、まずＧＵＩを介してレポートを確認し、復号化されたＰＤＦファイルを見て、どのデータが攻撃者の手に落ちたか発見する。さらに、組織の情報セキュリティ担当者は、本発明の生成された侵入活動レポートを使用して、識別された７つのマシン上に、７つのマルウェアが存在することを迅速に識別する。ファイル・サーバの接続がこの７つのマシンに対して確立されているので、侵入活動報告によって、攻撃者がネットワーク上の全ての内部値付け記録および未提出の暫定特許文書をひそかに抽出したことが明らかになった。ＧＵＩレポートの最初の確認の後、組織は、その企業セキュリティ事故報告の枠組みで受け入れるために、プログラムによるレポートをダウンロードし、関連のある侵入トラフィックをさらに送信して報告を拡充する。

【００８４】

図１６ａには、標準プロトコル・スタック内でのカバート・チャネルのプロセスが示してある。このスタックは、様々な標準層１～ｎを含む。プロトコル・スタックの各層は、それ自体のカバート・チャネルの痕跡１～ｎを有する。ＡＰＴツールは、プロトコル・スタックの各層のうち任意の層で利用でき、標準プロトコルを乱用して検出を回避できるカバート・チャネルを使用する場合がある。本発明は、プロトコル処理の一部としてカバート・チャネルが送信される層から、カバート・チャネルを抽出する。本発明のカバート・チャネル・プロセッサは、プロトコル・スタックの任意の部分で、カバート・チャネル情報を識別および抽出することができる。たとえば、悪質なソフトウェアが、ＩＰヘッダ、インターネット制御メッセージ・プロトコル（ＩＣＭＰ）メッセージ、またはドメイン・ネーム・システム（ＤＮＳ）メッセージ内のカバート・チャネル内に、その抽出データを隠す場合、処理アルゴリズムは、入力データをＰＣＡＰフォーマットで受信し、それに応じてカバート・チャネルからデータを抽出する。

【００８５】

図１６ｂには、標準プロトコル・スタック内でのマルウェアのプロセスが示してある。このスタックは、様々な標準層１～ｎを含む。プロトコル・スタックの各層は、それ自体のマルウェアの痕跡１～ｎを有する。

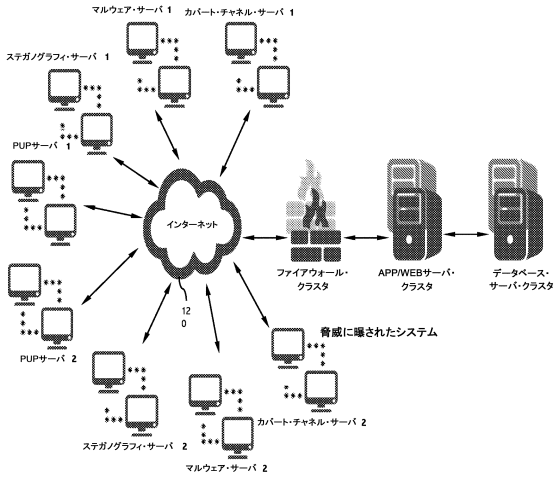
【００８６】

図１７ａは、カバート・チャネルのプロセスの流れ図である。カバート・チャネルの逸脱は、標準プロトコル・スタックの任意の１つまたは複数の層におけるものとすることができる。オフライン・ネットワーク・トラフィックは、図４のＳａａＳに送信される。オフライン・ネットワーク・トラフィックが処理される。カバート・チャネルの検出は、標準プロトコルの逸脱に基づく。プロセスが完了すると、レポートが生成される。

【００８７】

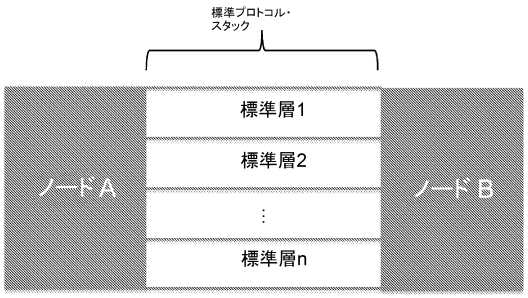
図１７ｂは、マルウェアのプロセスの流れ図である。標的に対するマルウェア攻撃ツールは、標準プロトコルから逸脱することなく、メッセージを伝達するのに標準プロトコル・スタックを使用する。オフライン・ネットワーク・トラフィックは、図４のＳａａＳに送信される。オフライン・ネットワーク・トラフィックが処理される。マルウェアの検出は、標準プロトコルの逸脱とは無関係である。プロセスが完了すると、レポートが生成される。

【図１】

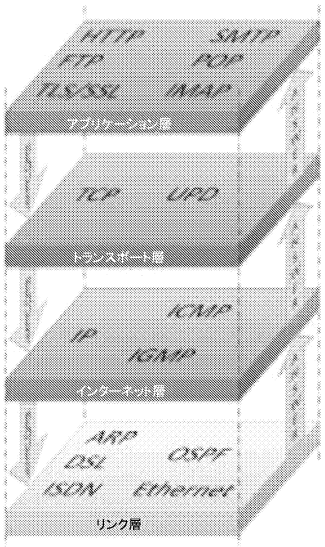



先行技術

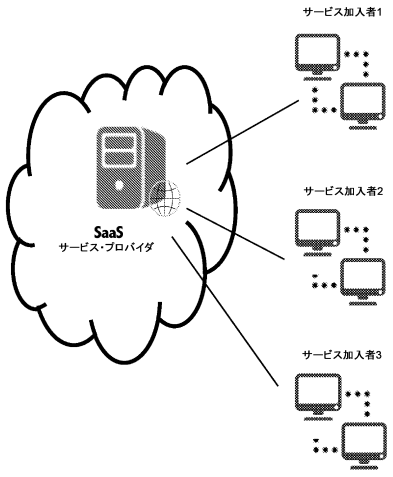
【図２】



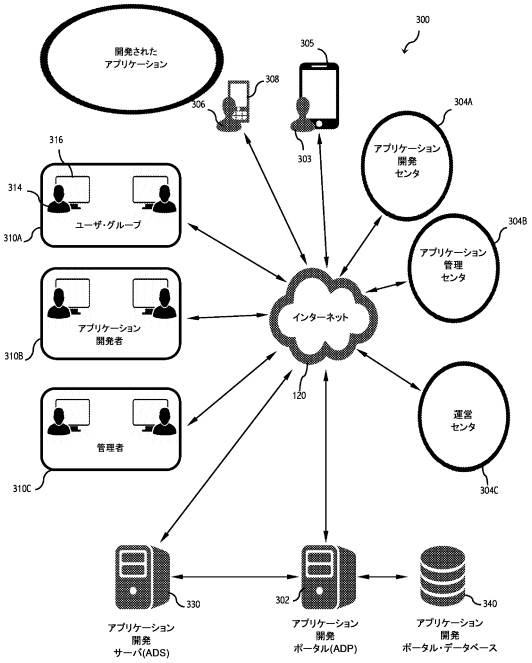

【図３】



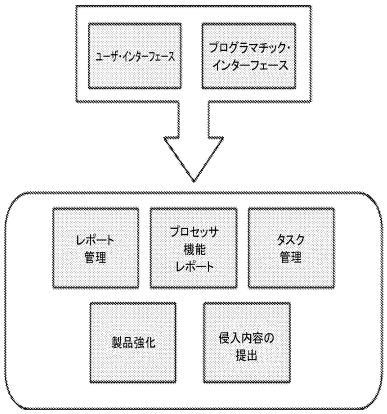

【図４】



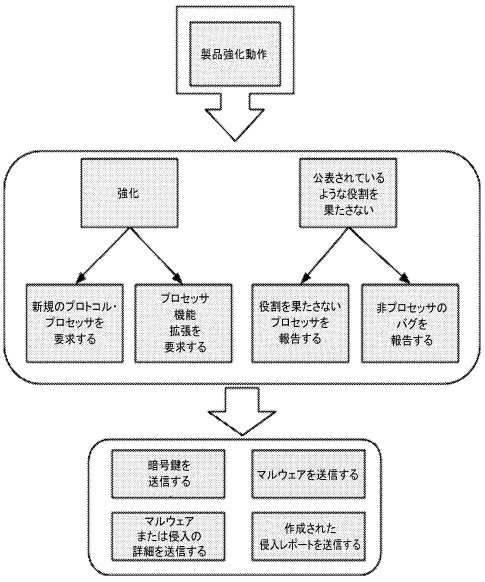
【図５】


300
開発された
アプリケーション
305
308
306
303
304A
アプリケーション
開発
センタ
316
314
ユーザ・グループ
310A
304B
アプリケーション
管理
センタ
アプリケーション
開発者
310B
インターネット
120
運営
センタ
304C
管理者
310C
330
302
340
アプリケーション
開発
サーバ(ADS)
アプリケーション
開発
ポータル(ADP)
アプリケーション
開発
ポータル・データベース

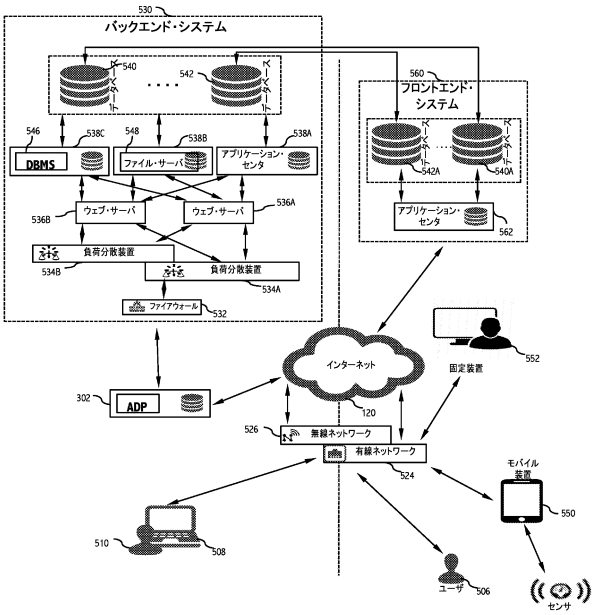
【図６】


ユーザ・インターフェース
プログラマチック・
インターフェース
レポート
管理
プロセッサ
機能
レポート
タスク
管理
製品強化
侵入内容の
提出

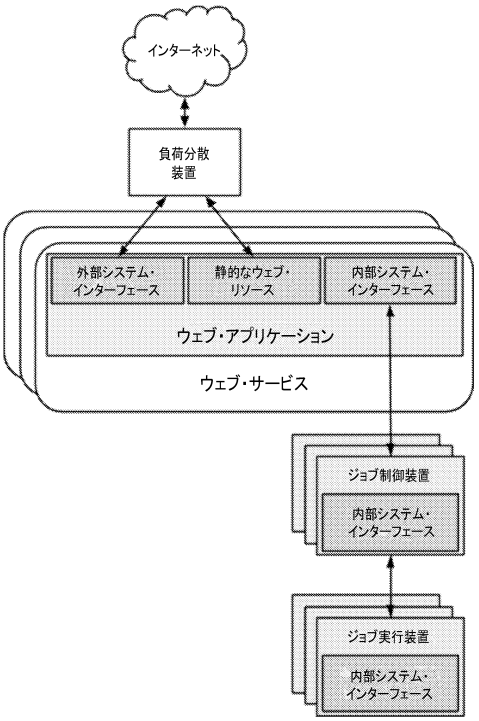
【図７】


製品強化動作
強化
公表されている
ような役割を
果たさない
新規のプロトコル・
プロセッサを
要求する
プロセッサ
機能
拡張を
要求する
役割を果たさない
プロセッサを
報告する
非プロセッサの
バグを
報告する
暗号鍵を
送信する
マルウェアを送信する
マルウェア
または侵入の
詳細を送信する
作成された
侵入レポートを送信する

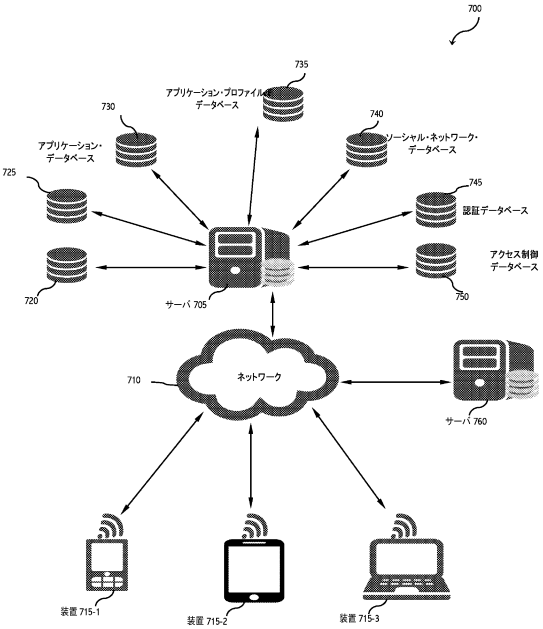
【図８】


530
バックエンド・システム
540
542
560
フロントエンド・
システム
546
538C
548
538B
538A
DBMS
ファイル・サーバ
アプリケーション・
センタ
542A
540A
536B
ウェブ・サーバ
ウェブ・サーバ
536A
アプリケーション・
センタ
562
負荷分散装置
534B
負荷分散装置
534A
ファイアウォール
532
552
固定装置
インターネット
302
ADP
120
526
無線ネットワーク
有線ネットワーク
524
モバイル
装置
550
510
508
ユーザ
506
センサ

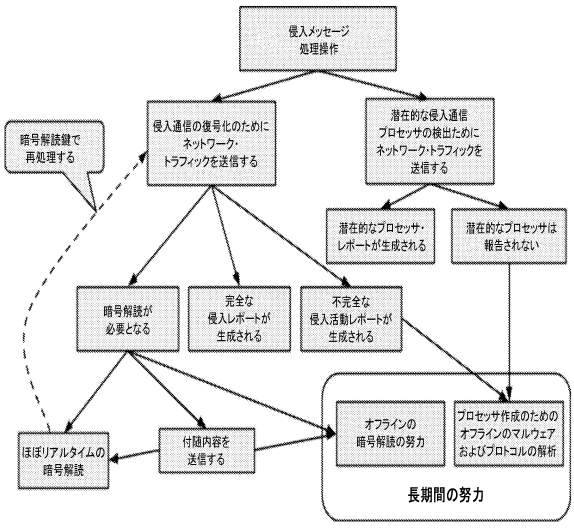
【図９】



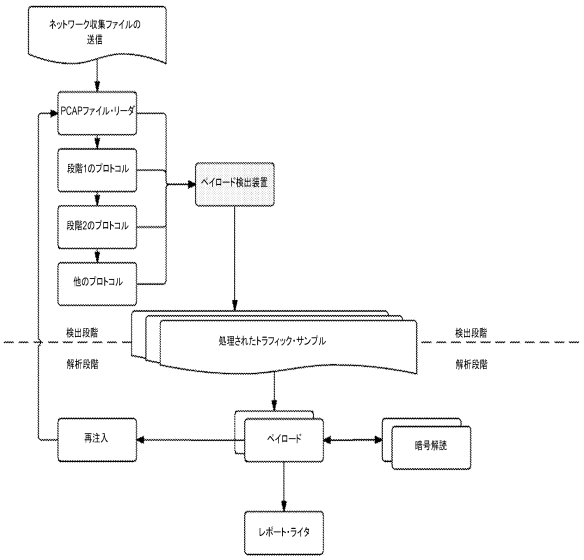

【図１０】



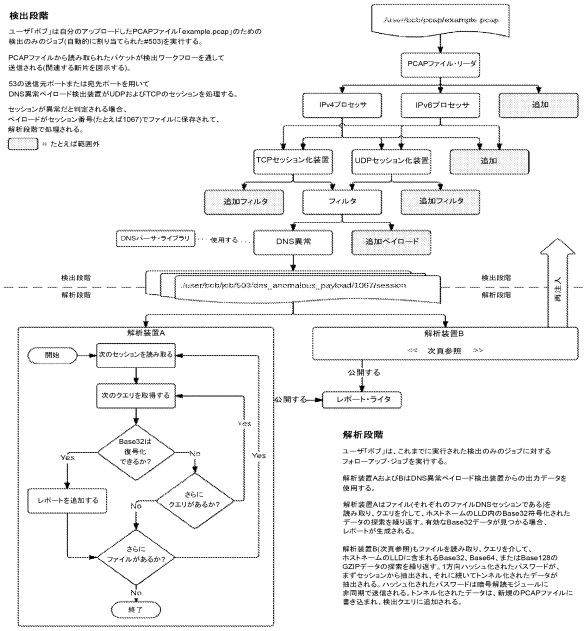

【図１１】



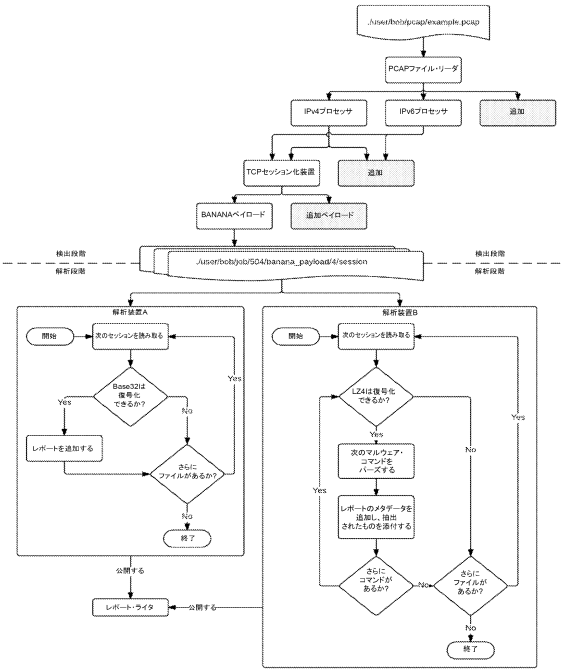

【図１２】



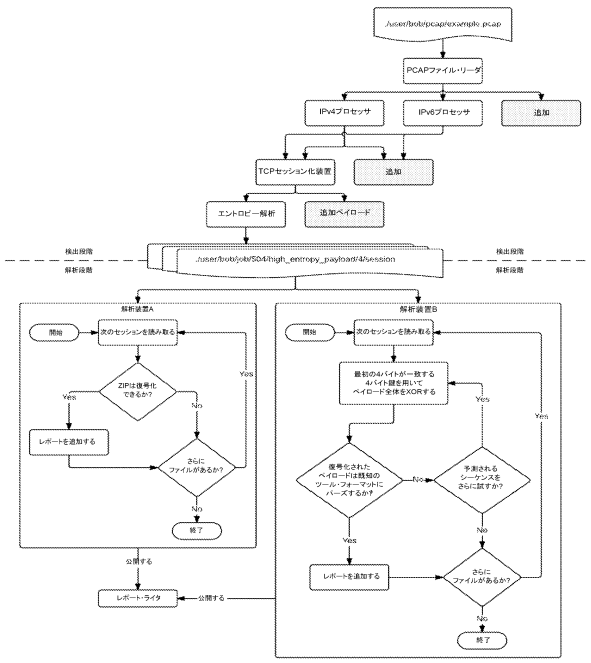
【図１３】



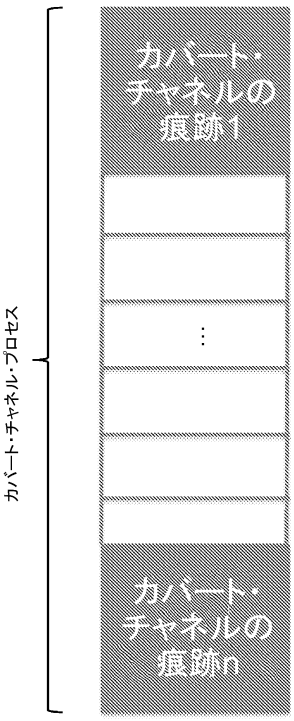

【図１４】



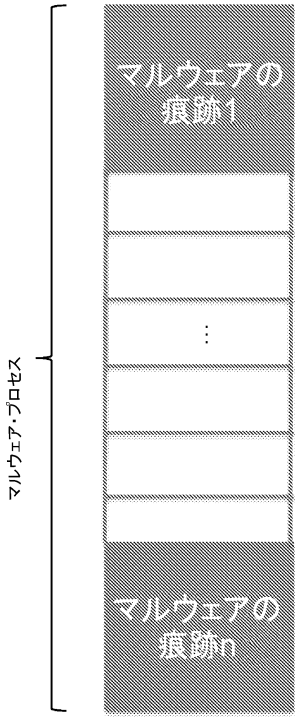

【図１５】



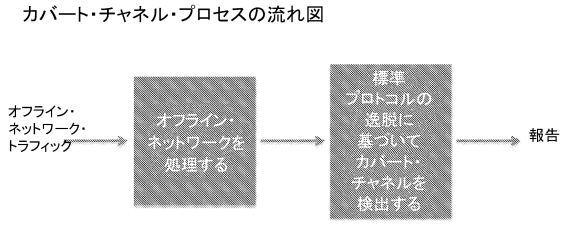

【図１６ａ】



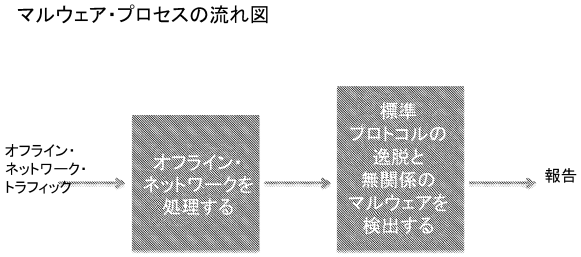
【図１６ｂ】




【図１７ａ】




【図１７ｂ】



フロントページの続き

(72)発明者　デニス　アンダーウッド
アメリカ合衆国, メリーランド州　２１０６１, グレン　バーニー, フォックスファーム　レーン　７８６３
(72)発明者　イーサン　ストライカー
アメリカ合衆国, メリーランド州　２１０４６, コロンビア, キンドラー　ロード　７３７５
(72)発明者　ジョナサン　ピーターソン
アメリカ合衆国, メリーランド州　２１１１３, オデントン, バレッド　オウル　ウェイ　２６３９

審査官　宮島　郁美

(56)参考文献　特開２００３－２４１９８９（ＪＰ, Ａ）
特開２０１４－１３０６１４（ＪＰ, Ａ）
特開２０１３－１６８１４１（ＪＰ, Ａ）
特開２００９－２３８１５３（ＪＰ, Ａ）
特開２００６－３２４８１７（ＪＰ, Ａ）
特開２００７－２４２００２（ＪＰ, Ａ）
米国特許出願公開第２００９／０２８２４８３（ＵＳ, Ａ１）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２６, １２／５０－１２／９５５
Ｇ０６Ｆ２１／００