様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ８ 日現在

機関番号：１７１０４
研究種目：若手研究(B)
研究期間：2014～2015
課題番号：２６７３００６６

研究課題名（和文）能動型ダークネット観測システムに関する研究

研究課題名（英文）Studies on An Active Darknet Monitoring System

研究代表者
佐藤　彰洋（Satoh, Akihiro）

九州工業大学・情報科学センター・助教

研究者番号：３０６０９３７６

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：本研究では，マルウェアの挙動を迅速に把握するために，能動型ダークネット観測システムの実現に取り組んだ．提案システムは，自動応答生成技術とマルウェア解析技術によって構成される．自動応答生成技術の役割は，マルウェアからのパケットに対して自動で応答を生成することにより，その詳細な情報を取得することである．マルウェア解析技術の役割は，マルウェアの種類の特定とそれが狙う脆弱性に関する情報を取得することである．

研究成果の概要（英文）：We develop an active darknet monitoring system to reveal various types of malware behaviors in detail. The proposed system has two functions: (1) response packet generation and (2) malware classification. The former automatically generates response packets to inspect malware behaviors, and the latter classifies malwares according to their exploit.

研究分野：情報セキュリティ

キーワード：ネットワークセキュリティ　トラヒックモニタリング　機械学習

１．研究開始当初の背景

米 Symantec 社の「インターネットセキュリティ脅威レポート」によると，2011 年に作成されたマルウェアの亜種は 4 億を超える．この様に日々変化を続けるマルウェアを迅速に把握するために，ダークネット観測システムが注目されている．ダークネットとは，インターネット上で到達可能かつ未使用の IP アドレス群である．ダークネットに設置されたセンサ（パケットログ収集機器）で観測されるのは，実在しない機器に対する通信であるため，それらをマルウェアの感染活動などに起因する不正なものと見なすことができる．

既存のダークネット観測システムとして，米 CAIDA の Network Telescope や情報通信研究機構の nicter が挙げられる．nicter は，約 20 万の IP アドレス群から収集した情報を分析することで，インターネットで発生している不正な通信をリアルタイムで可視化する．その運用の結果，W32.Downadup の大規模感染の予兆をつかんだとの報告がされている．

しかしながら，既存のダークネット観測システムは，マルウェアからのパケットは受信するものの自らはパケットを送信しないため，分析に利用できる情報は非常に限定されている．具体的には，送信元 IP アドレスと送信先ポート番号，すなわちマルウェアに感染した機器とそれが狙うサービスのみである．そのため，従来のシステムでは，インターネット上におけるマルウェアの感染活動の活発化については把握できるが，そのマルウェアの種類や対処すべき脆弱性を特定できない．新種のマルウェアへの対策の遅れはその大規模感染を引き起こす要因に成り得るため，この問題の解決は急務である．

２．研究の目的

本研究では，ダークネットに設置されたセンサが自動的に応答を生成することで，マルウェアに関する詳細な情報を取得する仕組みの実現を目指す．ここでは提案システムの核となる(1)自動応答生成技術, (2)マルウェア解析技術について整理する．

自動応答生成技術の基本的なアイディアは，センサがダークネットで観測されたパケットに逐次応答することで，マルウェアの挙動に関する情報を能動的に収集することにある．センサは，ライブネットとダークネットで観測された通信を参照することにより，マルウェアに対する応答パケットを自動で生成する．ここでライブネットとは，実際に機器が接続されている使用中の IP アドレス群を意味する．次に同種のマルウェアがダークネットに出現した場合，センサはそのパケットを送信することでマルウェアからの返答を観測する．この処理を繰り返すことにより，詳細なマルウェアの挙動を取得できる．ここで留意すべき点は，マルウェアからの返答パケットの有無は，自動で生成した応答パケットの是非を判断する上で重要な指標と成り得ることである．

マルウェア解析技術は，前述の能動的に観測された通信と他の比較により，マルウェアの種類とそれが狙う脆弱性に関する情報をネットワーク管理者に通知する．まず，対象の通信と既知のマルウェアの通信を比較することで，マルウェアの種類を特定する．この理由として，同種のマルウェアは通信内容が類似すること，それに反して異種のマルウェアは通信内容が相違することが挙げられる．故に，どのマルウェアにも属さない通信は未知のものと判断できる．次に，対象の通信とライブネットで観測された通信を比較することで，未知のマルウェアが狙う脆弱性を特定するために有用な情報を抽出する．この理由は，ライブネットで観測される通信がマルウェアによるものでないと仮定すると，それらの通信の違いは脆弱性を突く箇所に現れるためである．この情報をネットワーク管理者に通知することで，未知のマルウェアに対する迅速な対処が可能となる．

(1)自動応答生成技術

この機能の役割は，マルウェアからのパケットに対して自動で応答を生成することにより，その詳細な情報を取得することである．具体的なアプローチとして，マルウェアの通信の調査に基づいた応答パケットの系統化と，ライブネットの通信に対する機械学習の適用を検討する．

(2)マルウェア解析技術

この機能の役割は，マルウェアの種類の特定とそれが狙う脆弱性に関する情報を抽出することである．具体的なアプローチとして，ペイロードのハッシュ値を比較する方法，通信の特徴（パケットの数やサイズ，通信方向など）を比較する方法について検討する．加えて，ライブネットの通信と比較することで，それが狙う脆弱性に関する情報を抽出できるか否かについても検討する．

３．研究の方法

本研究では，ダークネットに設置されたセンサが自動的に応答を生成することで，マルウェアに関する詳細な情報を取得する仕組みを実現するために，(1)自動応答生成技術，(2)マルウェア解析技術の，2 つのサブテーマの達成に取り組む．初年度は主に，2 つのサブテーマに共通するダークネットの観測のための環境構築と，そこで観測された通信の解析を行う．次年度以降は，通信の解析結果に基づいて 2 つのサブテーマの提案方式を検討し，既存システムとの比較により各方式の効果を示す．加えて，それら 2 つの技術を統合したシステム全体の有効性・実用性につい

ても検証する．

４．研究成果

(1)ダークネットで観測された通信の分析

自動応答生成技術とマルウェア解析技術の実現のために，ダークネットにおいて観測されるマルウェアの通信に対して手動で生成した応答を返すことで得られる結果について調査した．その手順は次の通りであり，適時②から④を繰り返す．

① ダークネットの観測により，マルウェアが狙う宛先ポート番号を特定する

② ライブネットの通信を参照することで，分析者が手動で応答パケットを生成する

③ 次に同マルウェアの通信が出現した時，事前に生成した応答パケットを送信する

④ マルウェアからの返答パケットを調査する

ここで，応答パケットを生成するにあたり，アプリケーションヘッダの各項目が取る値を様々に変えること，ペイロードをランダム値に置き換えること，ペイロード自体を削除することなどを試みた．また，マルウェアからの返答パケットの有無は，手動で生成した応答パケットの是非を判断する上で有効な指標となり得るかについて検討した．その結果，SSH 総当り攻撃やドライブバイダウンロード攻撃などにおいて，その通信を系統化することに成功した．特に，ここで得られた知見に基づくことで，高い精度での通信の分類と検出が可能であることを示した．

(2)自動応答生成技術

自動応答生成技術を実現するための仕組みを提案し，既存のダークネット観測システムとの比較により効果を検証した．この機能の役割は，マルウェアからのパケットに対して自動で応答を生成することにより，その詳細な情報を取得することである．その実現のためのアプローチとして，前述の調査結果に基づいた応答パケットの系統化と，ライブネットとダークネットの通信に対する機械学習の適用である．具体的には，系統化のためにオントロジーや知識処理，機械学習としてリーベンシュタイン距離によるクラスタリング，共起分析やアソシエーション分析を用いた．ここで作成したプロトタイプシステムについては，今後も継続した運用と改善を行う予定である．

(3)マルウェア解析技術

マルウェア解析技術を実現するための仕組みを提案し，既存のダークネット観測システムとの比較により効果を検証した．この機能の役割は，未知のマルウェアを検出することと，それが狙う脆弱性の特定することである．未知のマルウェアの検出を実現のためのアプローチとして，ペイロードのハッシュ値を比較する方法，通信の特徴（パケットの数やサイズ，通信方向など）を比較する方法などについて検討した．これは，未知のマルウェアは既知のものと比較して通信の内容が異なることが想定されるためである．加えて，ライブネットで観測された通信と比較することで，それが狙う脆弱性を特定できるか否かについても検討した．特にドライブバイダウンロード攻撃においては，通信の特徴を比較することで，脆弱性の種類ごとに分類することに成功した．この成果については，現在論文誌に投稿中である．

５．主な発表論文等

〔雑誌論文〕（計 3 件）

① Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, A Flow-based Detection Method for Stealthy Dictionary Attacks against Secure Shell, Journal of Information Security and Applications, Vol.21, pp.31-41, 2015. 査読有

② Akihiro Satoh, Yutaka Nakamura, Takeshi Ikenaga, A New Approach to Identify User Authentication Methods toward SSH Dictionary Attack Detection, IEICE Transactions on Information and Systems, Vol.E98-D, No.4, pp.760-768, 2015. 査読有

③ Yasutaka Shindo, Akihiro Satoh, Yutaka Nakamura, Katsuyoshi Iida, Lightweight Approach to Detect Drive-by Download Attacks Based on File Type Transition, Proceedings of the 2014 CoNEXT on Student Workshop, pp.28-30, 2014. 査読有

〔学会発表〕（計 1 件）

① 進藤康孝, 佐藤彰洋, 中村豊, 飯田勝吉, マルウェア感染ステップのファイルタイプ遷移に基づいた Drive-by Download 攻撃検知手法, コンピュータセキュリティシンポジウム，北海道，2014 年 10 月 15 日

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕

６．研究組織

(1)研究代表者

佐藤彰洋（　Akihiro Satoh　）
九州工業大学・情報科学センター・助教
研究者番号：30609376

(2)研究分担者

無し

(3)連携研究者

無し