様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ５ 月 １２ 日現在

機関番号：１４６０２
研究種目：若手研究
研究期間：2018～2022
課題番号：１８Ｋ１８０４５

研究課題名（和文）ネットワークセキュリティを対象とした実ネットワーク指向シミュレータに関する研究

研究課題名（英文）the realistic network oriented simulator for network security

研究代表者
瀧本　栄二（Takimoto, Eiji）

奈良女子大学・情報基盤センター・准教授

研究者番号：９０３９５０５４

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：ネットワークシミュレータ上に，コマンド＆コントロール（C&C）サーバを模倣するノードを作成し，実機上で動作するIoT機器を対象とするマルウェアMiraiおよびその亜種と通信させる機構を作成した．また，ネットワーク構造に依存しない仕組みを取り入れ，かつ通信内容をすべてシミュレータに引き込むことで，外部に影響を与えることなくマルウェアを動作させることを可能にした．これにより，ボット系マルウェアの解析や検証を容易にし，セキュリティ強化やセキュリティ教育への応用が期待できる．

研究成果の学術的意義や社会的意義
情報セキュリティ対策は喫緊の課題である．本研究成果によって，外部に設置されたC&Cサーバとの連携が前提となるボットの動作確認，動作解析を容易にすることができる．これにより，動作解析の結果をセキュリティ対策に組み込むことが想定できる．さらに，実際のマルウェアの振舞いを安全に確認できるため，情報セキュリティ教育への効果も期待できる．

研究成果の概要（英文）：We created a node that imitates a Command & Control (C & C) server on a network simulator, and created a mechanism to communicate with malware Mirai and its variants for IoT devices that run on real devices. We also adopted a mechanism that does not depend on the network structure, and made it possible to operate malware without affecting the outside world by pulling all communication content into the simulator. This makes it easy to analyze and verify bot-based malware, and is expected to be applied to security enhancement and security education.

研究分野：情報学

キーワード：情報セキュリティ　ネットワーク

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

研究開始当初より現在に至るまで，標的型攻撃による機密情報の窃取，ランサムウェアによる金銭的被害と企業活動の妨害等，様々なサイバー攻撃の脅威にさらされている．サイバー攻撃に対する対策の強化が求められる一方，それを担うセキュリティ技術者不足が問題となっていた．セキュリティ技術者にはハードウェア，ソフトウェア，インフラに関する幅広い知識に加え，サイバー攻撃の手口と対策に関する知見と技術が求められるため，その育成が困難である．また，育成に効果的な教材や環境も改善の必要があった．

２．研究の目的

本研究では，異なる２つの目的を設定している．１つはセキュリティ技術者の教育および新たなセキュリティ技術のテストベッド・評価環境を提供することである．セキュリティ技術の習熟には実践的なアプローチが重要であるが，一方でそのためのツールは貧弱である．いくつかの企業では，育成プログラムなどを提供しているが高価であり高専・大学生の教育には不向きである．仮想環境を利用した教育システムもあるが，仮想環境を実現するために高い計算機性能が求められる．そこで，低コストな教育・実践環境の構築を目指す．

もう１つは，ボットに代表される外部通信を前提とするマルウェアの動作を解析し，セキュリティ対策に貢献することである．外部通信を行うマルウェアを解析するためには，実際に外部との通信を許可する必要があり，その過程で他者への感染被害が発生する可能性がある．しかし，完全に閉じた環境では外部との通信ができず，通信内容や挙動の解析が困難となる．また，LAN 内での感染活動を対象とする場合でも，感染先となる端末を用意する必要がありコストがかかる．そこで，低コストで外部・内部通信を再現することを目指す．

３．研究の方法

研究目的を果たす上で，低コストで扱いやすいネットワークシミュレータを用いる．使用したネットワークシミュレータはオープンソースソフトウェアである ns-3 を採用した．また，必要に応じてネットワーク設定を動的に変更する必要や，実際に動作するマルウェアとの通信が必要となるため，タップデバイス機能を用いる．これにより ns-3 のシミュレーションノードと実機上で動作するマルウェアとの通信を可能とする．

上記環境を構築したうえで，マルウェアの通信対象をシミュレーションノードとして実装する．例えば，ボットの制御に用いられる C&C サーバや，DDoS 攻撃において踏み台として利用される DNS サーバである．シミュレーションノードとしてそれらを完全再現する必要はないため，そのエッセンシャルな機能のみを実装し，それらを用いた実環境と連動したシミュレーションを行う．

４．研究成果

（１）DNS を利用した DDoS 攻撃である DNS リフレクタ攻撃をシミュレータで再現するにあたり，その再現方式を検討した．著名な DNS サーバである Bind などは非常に巨大なアプリケーションであり，それらの機能をそのままシミュレータ上に再現することは困難である．そこで，実環境上に踏み台となるサーバを構築し，DNS リフレクタ攻撃を行うノード群と攻撃対象ノードをシミュレータ上に作成し，DDoS 攻撃を模倣した．その結果，実環境とシミュレータ間の結合部分においてオーバヘッドが大きく，期待されるトラフィック量が生成されないことが明らかになった．そこで，DNS リフレクタ攻撃で使用されるパケットフォーマットを認識し期待される大容量パケットを応答として返信するノードを新たに実装した（図１）．実装では，軽量化のため DDoS 攻撃に関連するパケットにのみ，DNS サーバと同等の応答を返すように機能を制限した．また，ns-3 では提供されていない IP スプーフィングと呼ばれる IP アドレス偽装機能も実装し，応

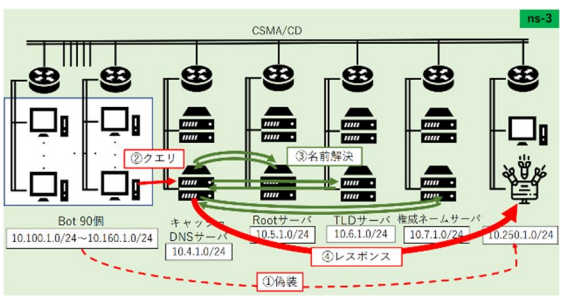

図１　実験シナリオ

答が攻撃対象ノードに返送されるようにした．これにより，実環境と連携した実験では 10Mbps 程度だった攻撃トラフィック量がシミュレータのリンク容量の限界まで上昇することを確認した．また，実験によって得られたパケットデータが正当な DNS パケットとして認識されることをパケット解析ツールを用いて確認した．

（２）IoT マルウェアの多くはボットと呼ばれる種類であり，攻撃者がインターネット上に設置した C&C サーバと通信し，攻撃者からの指令を実行する．その動作解析には C&C サーバが不可欠であるが，実際に C&C サーバと通信を行わせると感染被害等の影響が考えられる．そこで，外部と通信できない閉環境での IoT マルウェア解析を可能とするシステムを作成した．本システムはシミュレータのタップ機能を利用し，IoT マルウェアが動作する実機の通信をすべてシミュレータ内に引き込むことで閉環境を実現する．シミュレータ上には，おとりノードと呼ばれるノードと C&C サーバを模倣する C&C ノードを実装した．実環境上で発生するパケットは IoT マルウェアによるもの以外も多く含まれる．また，C&C サーバの IP アドレスは IoT マルウェア毎に異なる．同様に，IoT マルウェアが指令を受けて攻撃を行う際に指定する IP アドレスは，指令毎に異なる．したがって，IoT マルウェアの通信先となるノードの IP アドレスを予め決めておくことができない．本システムは，引き込んだパケットをすべておとりノードに転送し，おとりノードはそのすべてを受信しつつ，IoT マルウェアによるパケットだけを C&C ノードに転送することで，指定 IP アドレスに関係なく C&C ノードと通信させることを可能としている．C&C ノードは C&C サーバを模倣するが，上述のおとりノードによるパケット転送されたパケットに対する応答は直接 IoT マルウェアに送信する．C&C ノードの動作は解析済みの公開されたものと，本研究で独自に解析したものを利用して実装した．

本システムを利用して，代表的な IoT マルウェアである Mirai とその亜種である Tsunami を用いた動作検証を行った．以下，図示するログはすべて本システムで得られたものを使用している．IoT マルウェアは起動するとハードコーディングされた C&C サーバへの Telnet 通信を試みる（図２）．C&C ノードが応答すると，以降 IoT マルウェアを制御できる状況に置くことができ，IoT マルウェアに攻撃指令を送付して所望の攻撃を行わせることができることを確認した．

Time	Source	Destination	Protc	Leng	Info
58.4015…	10.1.1.1	148.155.167.1…	TCP	76	41140 → 23 [SYN] Seq=0 Win=64
58.4997…	148.155.167.122	10.1.1.1	TCP	72	23 → 41140 [SYN, ACK] Seq=0 A
58.4998…	10.1.1.1	148.155.167.1…	TCP	68	41140 → 23 [ACK] Seq=1 Ack=1
58.5023…	10.1.1.1	148.155.167.1…	TCP	68	41140 → 23 [FIN, ACK] Seq=1 A
58.6061…	148.155.167.122	10.1.1.1	TCP	68	23 → 41140 [ACK] Seq=1 Ack=2
58.6084…	148.155.167.122	10.1.1.1	TE…	71	Telnet Data ...
58.6085…	10.1.1.1	148.155.167.1…	TCP	56	41140 → 23 [RST] Seq=2 Win=0
59.5726…	10.1.1.1	148.155.167.1…	TCP	76	41144 → 23 [SYN] Seq=0 Win=64
59.6030…	148.155.167.122	10.1.1.1	TCP	72	23 → 41144 [SYN, ACK] Seq=0 A
59.6030…	10.1.1.1	148.155.167.1…	TCP	68	41144 → 23 [ACK] Seq=1 Ack=1
59.6070…	148.155.167.122	10.1.1.1	TE…	71	Telnet Data ...
59.6071…	10.1.1.1	148.155.167.1…	TCP	68	41144 → 23 [ACK] Seq=1 Ack=4
59.6172…	10.1.1.1	148.155.167.1…	TE…	71	Telnet Data ...
59.7113…	148.155.167.122	10.1.1.1	TE…	77	Telnet Data ...

図２ C&C サーバと IoT マルウェアによる telnet 通信ログ

本研究の結果，無償のネットワークシミュレーションを利用することで，サイバー攻撃を再現できることを確認した．シミュレータでは各種実験をシナリオとして記述するため，同等の実験環境を即座に再現することがでる．このような安価・手軽なサイバー攻撃の再現はセキュリティに関する教育・実践に大きく貢献すると考えている．また，図２のようにログがパケット解析ソフトを用いて解析できる形で提供されるため，マルウェアの通信解析等にも有効であり，研究目的にそった成果が得られた．ただし，サイバー攻撃，マルウェアは常に進化しており，実用性という面ではさらなる作りこみに加え最新の状況に迅速に対応する必要があり，そのための開発容易性などが課題として残った．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Keigo Taga, Junjun Zheng, Koichi Mouri, Shoichi Saito, Eiji Takimoto	４．巻 E105-D
２．論文標題 Firewall Traversal Method by Pseudo-TCP Encapsulation	５．発行年 2022年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 105-115
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021EDP7050	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 多可 啓悟, 毛利 公一, 鄭 俊俊, 齋藤 彰一, 瀧本 栄二
２．発表標題 エンドノードでの擬似TCPヘッダ挿入によるファイアウォールトラバーサル手法の実装と評価
３．学会等名 信学技報
４．発表年 2019年

１．発表者名 申 河英, 鄭 俊俊, 齋藤 彰一, 毛利 公一, 瀧本 栄二
２．発表標題 ns-3とDNSサーバによるDNSリフレクタ攻撃エミュレーション
３．学会等名 第18回科学技術フォーラム(FIT2019)
４．発表年 2019年

１．発表者名 小西崇之, 瀧本栄二
２．発表標題 DDoS攻撃対策のためのISP間連携フレームワークの構築
３．学会等名 第18回科学技術フォーラム(FIT2019)
４．発表年 2019年

１．発表者名
小西崇之，瀧本栄二

２．発表標題
DDoS攻撃対策のためのISP間連携フレームワーク

３．学会等名
コンピュータセキュリティシンポジウム2019

４．発表年
2019年

１．発表者名
瀧本栄二

２．発表標題
ネットワークセキュリティシミュレータに関する検討

３．学会等名
信学技報

４．発表年
2018年

１．発表者名
多可啓悟，鄭俊俊，毛利公一，齋藤彰一，瀧本栄二

２．発表標題
QUICへの擬似TCPヘッダ挿入によるファイアウォールトラバーサル手法

３．学会等名
信学技報

４．発表年
2018年

１．発表者名
Keigo Taga, Junjun Zheng, Koichi Mouri, Shoichi Saito, Eiji Takimoto

２．発表標題
Firewall Traversal Method by Inserting Pseudo TCP Header into QUIC

３．学会等名
International MultiConference of Engineers and Computer Scientists 2019 (IMECS 2019)（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関