一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

組込み機器への攻撃を観測するハニーポット IoTPOT の機能拡張

鈴木 将吾† イン ミン パパ† 江澤 優太†
鉄 穎† 中山 颯† 吉岡 克成‡§ 松本 勉‡§
†横浜国立大学 ‡横浜国立大学先端科学高等研究院 §横浜国立大学環境情報研究院
〒240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-1
E-mail: †{suzuki-shogo-mb, yin-pa-dx, ezawa-yuta-xd, nakayama-sou-ch, tie-ying-fc}
‡§{yoshioka, tsutomu}@ynu.ac.jp

あらまし 我々は，これまで組込み機器への攻撃を観測するハニーポットである IoTPOT を提案しているが，IoTPOT がエミュレートするサービスは Telnet に限られていた．本稿では，他の脆弱なサービスのエミュレートを行い，IoTPOT の観測可能性を高める機能拡張を提案する．また，プロキシの利用により，ハニーポットを多数のネットワークに容易に分散配置可能となるようにアーキテクチャの改良を行う．加えて，攻撃元の機器を推定する能動的観測手法の改善を目指す．

キーワード 組込み機器，IoT，ハニーポット，マルウェア動的解析

Improving IoTPOT for Observing Various Attacks Targeting Embedded Devices

Shogo SUZUKI† Yin Minn PA PA† Yuta EZAWA†
Ying Tie† Sou NAKAYAMA† Katsunari YOSHIOKA‡§ and Tsutomu MATSUMOTO‡§
†Yokohama National University ‡Institute of Advanced Sciences Yokohama National University
§Yokohama National University Graduate School of Environment Information Sciences
79-1 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa, 240-8501 Japan
E-mail: †{suzuki-shogo-mb, yin-pa-dx, ezawa-yuta-xd, nakayama-sou-ch, tie-ying-fc}@ynu.jp,
‡§{yoshioka, tsutomu}@ynu.ac.jp

Abstract IoTPOT, which we previously implemented as a honeypot system for embedded devices, can only emulate Telnet service. In this study, we improve IoTPOT by emulating other additional vulnerable services for better observation of attacks targeting embedded devices. In addition, we enhance architecture of IoTPOT by implementing proxy which helps in running distributed IoTPOT in different networks easily. Moreover, we try to upgrade active monitoring functionality of IoTPOT which fingerprints device type of attacking hosts.

Keywords Embedded devices, IoT, Honeypots, Sandbox Analysis

1. はじめに

近年，様々なモノがインターネットに接続されるようになり，この状態は，モノのインターネット(Internet of Things)と称されている．しかし，これらの機器には脆弱性が内在するものも多く，様々なサイバー攻撃を受けることや，攻撃に悪用されることが大きな問題となっている．2012 年には，匿名の研究者によって作成された Carna ボットネット[1]により，1,200 万台以上の組込み機器のパスワードが未設定，または，簡単なパスワードでログイン可能であることが明らかとなった．2014 年 12 月には，Booter と呼ばれる DDoS 代行サービスによってソニーとマイクロソフトのゲームネットワークが攻撃を受け，利用できない状態となったが，これにはルータなど，多数の組込み機器が悪用されたと報告されている[2].

未使用 IP アドレス空間に到達する通信を観測したところ，2014 年以降，当該ポートへ通信を試みるホスト数およびパケット数の両方において，急激な増加が見られた[4]．さらに，観測したホストに対し，80/TCP でスキャンを行ったところ，デジタルビデオレコーダ(以下，DVR)，IP カメラ等，様々な機器のログインインタフェースが確認された．これらの予備調査から，インターネットに接続された組込み機器が攻撃に悪用されていることが推察される．

インターネット上の組込み機器は，グローバル IP アドレスが割り当てられている場合があり，任意の地点から容易にアクセス可能であり，24 時間常時稼働し，アンチウイルスソフトがインストールされていないため，攻撃者の視点から見ると，魅力的なリソースである．このような背景から，我々は，これまでに組込み機器への攻撃を観測するハニーポットである IoTPOT を提案した. IoTPOT は，Telnet サービスを模擬することで，組込み機器への攻撃を観測する．しかし，組込み機器には，Telnet の他に，Web や SSH 等、様々なサービスが実装されており，ルータや DVR のファームウェアに内在する脆弱性も数多く報告されている．そこで本稿では，DVR，ルータの脆弱性および IP カメラのサービスを模擬することで，IoTPOT の観測可能性を高める機能拡張を提案する．また，プロキシの利用

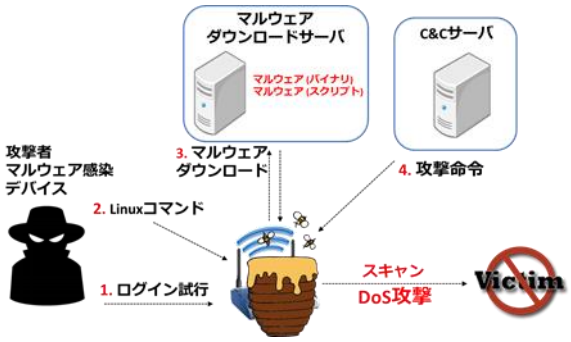

図 1. Telnet を利用した攻撃の一般的な流れ

により，ハニーポットを多数のネットワークに容易に分散配置可能となるようにアーキテクチャの改良を行う．加えて，攻撃元の機器を推定する能動的観測手法の改善を目指す．

提案手法のハニーポットをインターネット上に設置し，検証を行った結果，新たなマルウェアの取得や，脆弱性を攻撃する通信，IP カメラの映像を盗取する攻撃を確認した．

本研究の主要な貢献を次に示す．

1) 組込み機器上で動作する Web サービスや，特定機器の脆弱性を模擬し，これらへの攻撃を観測できるようになった
2) ハニーポットのアーキテクチャを改良し，多数のネットワークに容易に分散配置可能となるようにした
3) ハニーポットによる観測と能動的観測を組み合わせてマルウェアの大量感染が発生しているネットワークを発見した
4) IP カメラの映像を盗聴する攻撃の存在とその実情を観測した
5) 攻撃元機器を推定する能動的観測技術を改善した

本稿の構成は次の通りである．まず 2 章で組込み機器を標的とした攻撃を観測するハニーポットである IoTPOT について説明し，3 章で研究背景について述べ，4 章で組込み機器を標的とした攻撃を観測するハニーポットである IoTPOT の機能拡張を提案する．5 章では検証実験によって観測された攻撃および収集したマルウェア，について説明する．6 章で Telnet に関する分析について説明し，7 章で観測結果に関する考察を示す．8 章で関連研究について述べ，最後に 9 章でまとめと今後の課題を述べる．

2. 組込み機器への攻撃を観測するハニーポット IoTPOT

本章では，組込み機器への攻撃を観測するハニーポット IoTPOT について説明する．本章の構成は，次のとおりである．まず，2.1 節で IoTPOT の概要について説明し，2.2 節でハニーポットのシステム構成について述べる．最期に，2.3 節で，デバイスフィンガープリントについて説明する．

2.1. IoTPOT の概要

我々は，組込み機器の Telnet サービスを模擬するハニーポット IoTPOT をインターネット上に設置し，その通信を観測することで組込み機器を標的とした攻撃を観測する手法を提案し，攻撃の観測・分析を行っている[4,5]．ハニーポットには，初期設定のパスワードや容易に推測可能なパスワードで Telnet が動作する機器を標的とした攻撃が多数到達する．Telnet サービスを模擬することでこれらの攻撃を観測し，攻撃に用いられるマルウェアを収集・分析することで，不正侵入された機器が，どのような攻撃に悪用されるのかを分析することができる．ハニーポットにログインを試みるのは悪意を持ったホストや，攻撃者に操作されているホストに限られるため，ハニーポットで観測されるホストについて分析することで，攻撃に悪用されている機器について分析が可能になる．

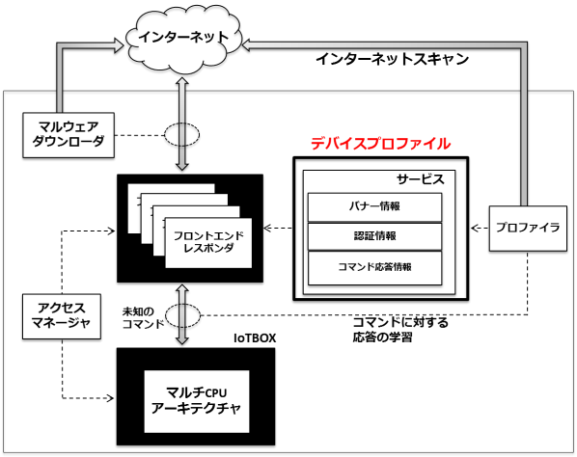

図 2. IoTPOT の全体

ハニーポットによって観測した Telnet による攻撃の一般的な流れを図 1 に示す．まず，攻撃者やマルウェア感染デバイスは，辞書攻撃によるログインを試みる．ログインに成功すると，攻撃者は Linux コマンドを利用し，侵入先の環境整備や調査を行う．最後に，マルウェアをダウンロード・実行し，感染に成功すると C&C サーバから命令を受け，DoS 攻撃や感染拡大を目的としたスキャンを行う．

2.2. システムの構成

IoTPOT の構成とシステムの概要を図 2 に示す．IoTPOT は，「フロントエンド」「IoTBOX」「プロファイラ」「ダウンローダ」「アクセスマネージャ」の 5 つの要素から構成される．なお，図 2 では，実線は通信の流れを，破線はシステム制御を表す．

フロントエンドでは，実際に攻撃者からの通信を受信し，プロファイラによって収集されたデバイスプロファイルをもとに，様々な組込み機器のサービスを模擬する．デバイスプロファイルは，バナー情報，認証情報，コマンド応答情報によって構成される．攻撃者から送られてくるコマンドが未知のものであった場合，フロントエンドは，バックエンドの IoTBOX とセッションを確立し，コマンドを IoTBOX へと転送する．IoTBOX は，様々な CPU アーキテクチャの組込み機器 Linux OS が動作するサンドボックス環境であり，実際の組込み機器を用いることも可能である．攻撃者から未知のコマンドがフロントエンドから送られてきた場合，バックエンドである IoTBOX でコマンドを受信し，その応答をフロントエンドへと送信する．攻撃者からのコマンドは，マルウェア感染させるためのものやマシンを乗っ取るためのものなど，深刻な被害を与えるものが多い．そのため，IoTBOX では適宜 OS イメージのクリーンアップを行う必要がある．また， IoTBOX は収集したマルウェアの動的解析環境として，IoTBOX 単体で用いることも可能である．プロファイラは，組込み機器のサービスを模擬するためのデバイスプロファイルを作成する役割を担う．ここでは，フロントエンドと IoTBOX 間における通信の監視や，インターネット上のホストに対しスキャンを行うことでバナー情報の収集を行い，デバイスプロファイルを拡充させる．プロファイラが行うスキャンは大きく 2 つに分けることができる．ひとつは，インターネット上のホストに対しランダムにスキャンを行うスキャンであり，もう一方は IoTPOT で観測されたホストに対するスキャンである．前者は，インターネットに接続されている機器の情報を広く収集することができ，後者は，攻撃に悪用されたている可能性の高い機器の情報を効率よく収集することが可能である．これを，デバイスフィンガープリントとする． ダウンローダは，バイナリファイル等をダウンロードするコマンドやシェルスクリプトを抽出し，抽出した URL からファイルをダウンロードする．フロントエンドと IoTBOX における通信は，iptables[6]や

表 1. 攻撃元の機器推定

機器の種類	ホスト数
DVR	10,734
Router	4,856
IP Camera	1,391
Web Camera	787
Set-Top-Box	430
Modem	411
Network Video Recorder	337
Ethernet Over Coax Adapter	206
CPE	206
Gateway	174

アクセスマネージャによって制御する．

2.3. デバイスフィンガープリント

ハニーポットに攻撃を行なった機器を特定する技術をデバイスフィンガープリントとよぶ．従来手法では，ネットワークスキャンツールである masscan によって 23/TCP，80/TCP のバナーを収集した後，バナー情報に含まれる”DVR”，”IP Camera”といったキーワードによって，攻撃元機器の推定を行っている．本稿では，23/TCP，80/TCP に加えて，21/TCP，443/TCP，8080/TCP のバナー情報も利用し，デバイスフィンガープリントを行った．2015 年 6 月 1 日から 9 月 31 日の期間において，ハニーポットで観測したホストにスキャンを行うことで，攻撃元機器の推定を行った結果を表 1 に示す．表は，機器が推定できたホストの上位 10 種類について，機器の種類とホスト数を表している．この期間に機器推定が可能であったホストは，観測ホスト数 106,570 ホスト中 15,096 ホストと，約 14%程度であった．2015 年 10 月以降，機器推定可能なホストは大きく減少しており，12 月の 1 か月間においては，約 8%であった．この原因の 1 つに，マルウェア Linux.Wifatch[24]の感染拡大が影響していると考えられる．Linux.Wifatch は，Telnet ログイン後にバナー情報を図 3 のように変更した後，当該ポートのサービスを利用不可能にする．2015 年 9 月以前は 23/TCP のみを対象にしていたが，10 月以降は待ち受けポートすべてが利用不可能とするように挙動が変化したため，バナー収集が困難になっている．当該マルウェア感染ホストは，10 月のみで 7,775 ホスト観測され，同時に別のマルウェアにも感染していることが推察されるホストも多数存在する．

3. 背景

2.3 節のデバイスフィンガープリントの分析から，DVR，ルータ，IP カメラが多く悪用されていることがわかる．これらの機器には，脆弱性が報告されているものがある．

特定メーカ製のルータに存在する脆弱性　中国のネットワーク機器メーカ製ルータのバックドアである 53413/UDP において，任意のコードが実行可能な脆弱性が存在することが 2014 年 8 月に報告されている[13].

DVR 設定ファイルが漏洩する脆弱性　複数メーカの DVR に，認証を要することなく DVR の設定ファイルである「DVR.cfg」がインターネット上から取得可能な脆弱性が報告されている [14]. 本設定ファイルには，DVR のユーザ名/パスワードの他に，PPPoE のアカウント情報，DNS サーバ，FTP サーバ，メールサーバの情報など，機密性の高い情報も含まれる．

インターネット上から閲覧可能な IP カメラ　インターネット上から閲覧可能な IP カメラの情報をまとめた Web サイト[26]が存在する．このサイトでは，国内の飲食店や，幼稚園，個人宅に設置されていると思われる IP カメラの映像が確認できる．

図 3. Linux.Wifatch 感染機器

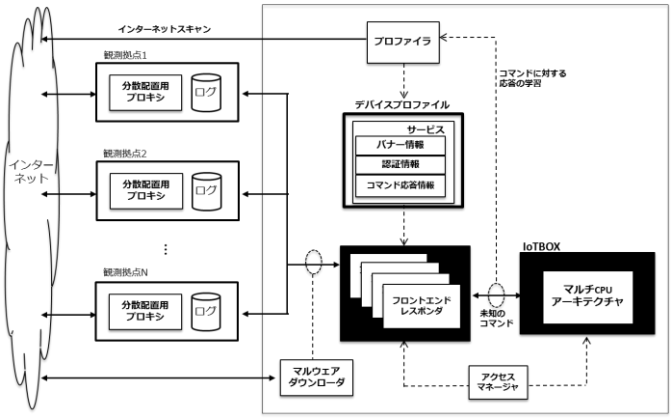

図 4. 提案手法の全体像

4. IoTPOT の機能拡張

本章では，組込み機器への攻撃を観測するハニーポット IoTPOT の機能拡張について提案する．

4.1. 提案手法

本稿では，従来手法の Telnet に加えて，デバイスフィンガープリントの結果，観測ホスト数の多い機器の上位 3 種について，3 章で記述したそれぞれのサービスを模擬することで，Telnet 以外の組込み機器への攻撃を観測するための機能拡張を提案する．また，プロキシを用いることで，ハニーポット分散配置を容易にし，観測可能性を高めるシステム改良も行う．提案手法の構成を図 4 に示す．提案手法の構成は，2.4 節で述べた組込み機器への攻撃を観測するハニーポット IoTPOT の構成から，上記の機能およびプロキシを追加したものである．

4.2. 実装

本稿の検証実験では，各観測点に Ubuntu[7]がインストールされたマシンを設置し，それぞれのマシン上で IoTPOT を実装した．IoTPOT は，フロントエンドとして python スクリプト，プロファイラとしてシェルスクリプトおよびスキャンツールである masscan[8]を利用した．IoTBOX として，プロセッサエミュレータの QEMU[9]により Debian[10]および OpenWrt[11]の異なる 8 種類の CPU アーキテクチャ(MIPS，MIPSEL，PPC，SPARC，ARM，MIPS64，sh4，x86)の Linux OS を模擬するように実装した．アクセスマネージャとして，Linux 標準のコマンドと iptables を用いた．ダウンローダは，python スクリプトによって実装した．なお，通信ログを tcpdump によって取得した pcap ファイル，およびプロファイ

表 2. 実験環境概要

機器の種類		IPカメラ		DVR	ルータ
サービスタイプ		Basic認証+IPカメラ	IPカメラ	設定ファイルを取得可能な脆弱性	53413/UDPの脆弱性
IPアドレス数		100	10	120	87(100)※1
分析対象期間		2016/1/20-29	2016/1/20-29	2016/1/7-1/29	2015/6/24-2016/1/31
観測日数		10日間	10日間	23日間	209日間※2
デバイスプロファイル	バナー情報	1種類	無し	無し	無し
	認証	Basic認証	無し	無し	無し
	コマンド応答情報	IPカメラを使用	IPカメラを使用	自作DVR.cfgを返答	IoTBOXで学習

※1　2015/5/1-10/26 日の期間は 87IP アドレスで観測，2015/10/27 日以降は 100IP アドレスで観測
※2　2015/9/27-10/6，2016/1/24-1/26 の 13 日間はサーバ停止のため分析対象から除外

ラにおけるスキャンの出力を IoTPOT の出力とした．

特定メーカ製のルータに存在する脆弱性　特定メーカ製ルータの脆弱性を模擬するデバイスプロファイルを用意した．バナー情報，認証情報は設定せず，コマンド応答として，コマンドに含まれるマルウェア取得命令を抽出した後，Telnet 同様，既知のコマンドにはフロントエンドが，未知のコマンドに対してはバックエンドに転送することで，当該脆弱性を模擬した．

DVR 設定ファイルが漏洩する脆弱性　DVR のデバイスプロファイルでは，バナー情報，認証情報は設定せず，コマンド応答として，設定ファイル「DVR.cfg」へのリクエストに対し，独自に作成した設定ファイルを返すように実装した．

インターネット上から閲覧可能な IP カメラ　IP カメラの模擬では，2 つのデバイスプロファイルによりサービスを実装した. 一つ目は，Basic 認証後に動画を閲覧可能なカメラを想定し，二つ目は，認証無しで動画を閲覧可能なカメラを想定した．認証では，”admin/admin”，”admin/12345”，”root/root”，”root/12345”，”admin/password”の 5 つの組でログイン可能とした．コマンド応答情報に関しては，Telnet 同様，既知のコマンドにはフロントエンドが，未知のコマンドに対してはバックエンドが応答を返す．バックエンドには，Panasonic 製 IP カメラ「BB-SP104W」[12]を利用し，映像内にユーザ名/パスワードが映るようにカメラを設置した．

5. 検証実験

本章では，4 章で説明した IoTPOT の機能拡張に関して，その効果を検証する実験の方法と結果について述べる．

5.1. 実験方法

提案手法により，組込み機器への攻撃の観測を行う．検証実験で用いたハニーポットの設定を表 2 に示す．3 種類の機器について，表 2 にある IP アドレス数，観測期間およびデバイスプロファイルにより，各サービスを模擬し，攻撃の観測を行った．IP カメラの Basic 認証では，IP カメラ「BB-SP104W」のバナーを利用した. DVR の設定ファイルには，実験用の認証情報を記載した．

5.2. 実験結果

特定メーカ製ルータに存在する脆弱性　特定メーカ製のルータのバックドアである 53413/UDP 通信に対して, ハニーポットでは大きく分けて 2 種類の通信が観測された．一つ目は，Linux コマンド「wget」,「tftp」を用いて，マルウェアダウンロード用のスクリプトを実行する通信で，2015 年 8 月 27 日以降観測している．スクリプトが実行されると，様々なアーキテクチャに対応したマルウェア群がダウンロード・実行される．外部からマルウェアのダウンロードを試みたホストは観測期間中で 1,215 ホストあり，ダウンロード試行回数は 74,619 回，収集できた検体は 55 検体，10 種類の CPU アーキテクチャで動作するマルウェアが確認された．なお，観測によって収集した検体のうち, 30 種類は Telnet ハニーポットによって収集した検体と重複していた．二つ目は，18 バイトのペイロードを含むパケットであり，本パケットを送信するホストは，観測期間中に 899 ホスト観測された．収集検体を動的解析した結果，2 検体において C&C サーバから命令を受信後，当該ペイロードを含む 53413/UDP 宛スキャンが発生した．ハニーポットと動的解析で観測した 53413/UDP 宛スキャンパケットには，IP ヘッダと UDP ヘッダの Length フィールドに，実際のパケット長とは異なる値が代入されているという特徴が見られた．以上の観測結果から，18 バイトの 53413/UCP スキャンを行うホストの実態は，本脆弱性によりマルウェア感染し，攻撃者に操作されている組込み機器であると推測される．

DVR 設定ファイルが漏洩する脆弱性　分析対象期間に，22 ホストから累計 906 回の DVR 設定ファイル DVR.cfg の取得を試みる通信を観測した．また，リクエストに対し，ユーザ名/パスワードを記載した自作 DVR.cfg ファイルを返答した結果，Basic 認証の際に，設定ファイルに記載されたユーザ名/パスワードを入力したホストを確認した．

IP カメラ　分析対象期間において, IP カメラに不正にアクセスし，映像を閲覧したホストが 18 ホスト存在し，累計 68 回の接続を観測した．これらのホストの平均接続時間は約 19 秒であり，最大で 116 秒間接続があった．特徴的なホストとして，4 日間連続で同一の IP カメラにアクセスし，映像を閲覧するホストを確認した．また，映像内にユーザ名/パスワードが映り込むように, カメラを設置した結果，撮影されたユーザ名/パスワードを Basic 認証で入力したホストを確認した．このことから，映像を目視確認している攻撃者が存在することがわかった．

6. Telnet に関する攻撃の分析

本章では，既存手法によって観測された結果について説明する．Telnet サービスの模擬では, スキャンによって収集した異なる 50 種類のバナーを用意し，認証では，任意のユーザ名/パスワードの組でログインできるように設定した．使用 IP アドレス数状況は，表 2 のルータと同じであり，分析対象期間は，2015 年 5 月 1 日から 2016 年 1 月 31 日までの 263 日間とした．

6.1. 観測結果

分析対象期間において， Telnet で通信を行ったホストは, 267,925 ホストであった．そのうち，Telnet でのログインに成功したホストは 199,386 ホストであり，外部からマルウェアのダウンロードを試みたホストは 145,814 ホスト, ダウンロード試行回数は 5,234,103 回であった． 収集した検体は，1027 検体におよび，11 種類の CPU アーキテクチャで動作するマルウェアが確認された．収集した検体のうち, マルウェア検査サービス VirusTotal[25]のデータベースに登録済みであった検体が 331 検体あり，未登録であった検体は 696 検体であった(2016 年 1 月 31 日時点)．登録済みであった 331 検体のうち，VirusTotal の 57 種すべてのアンチウイルスソフトで悪性であると判定できなかった検体が 301 検体あった(2106 年 1 月 31 日時点).

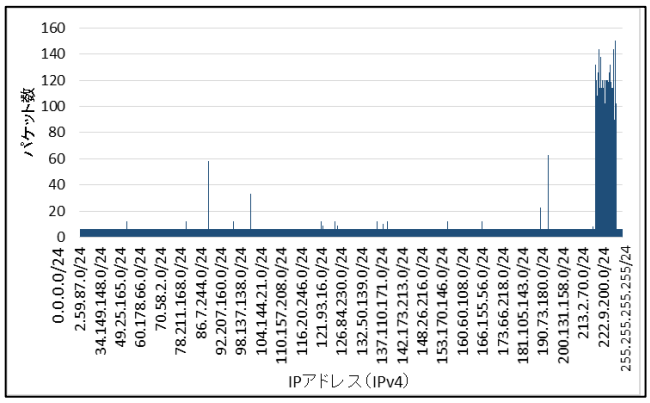

図 5. 23/TCP スキャンの宛先アドレス

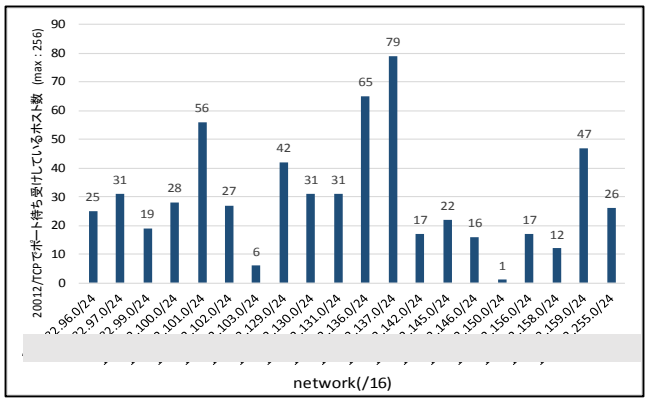

図 6. 20012/TCP でポート待ち受けしていたホスト数

6.2. ルータを標的としたワーム Moose

Moose は，容易に推測可能なユーザ名/パスワードで，Telnet によりログイン可能な機器を標的に感染拡大するワームであり[22]，ハニーポットにおいても継続的に検体が収集されている．収集検体を動的解析したところ，23/TCP，20012/TCP によるネットワークスキャン，20012/TCP におけるポート待ち受け， SNS のひとつであるインスタグラムにて「いいね」を増やすといった挙動が観測された．24 時間の動的解析で発生した 20012/TCP 宛のスキャンを，/24 のネットワークごとに集計したグラフを図 5 に示す．図から，Moose のスキャンにおける宛先 IP アドレスの選定には大きく偏りがあり，特に 222.9.0.0/16 周辺はパケット数が多く観測された．当該ネットワークは，動的解析環境のグローバル IP アドレス周辺であることから，Moose は，感染環境の周辺ネットワークに対して重点的に感染拡大を試みることが推測される. 次に, ハニーポットに 20012/TCP で通信したホストの周辺 IP アドレスに対し，スキャンを行うことで 20012/TCP でポート待ち受けしているホストの調査を行った．特定の/16 ネットワークにおける 2015 年 9 月 9 日時点の調査結果を図 6 に示す. 図より, 当該ネットワークでは多くのホストが 20012/TCP でポート待ち受けをしており，多いところでは約 31%(79/255)にもおよぶことがわかる．さらに，これらの多くが 23/TCP でもポート待ち受けしていることから，本ネットワークのあるホストが Moose に感染し，その後，周辺アドレスへの感染拡大により，局所的に Moose が大流行していることが推測される．調査の結果，このような/16 ネットワークを他に 3 つ確認しており，これらはすべて同一の国，ISP， AS に属していた．また，これらのホストの Telnet バナーに「Residential Gateway」という文字列が含まれることから，ISP 等によって配布された脆弱な機器が原因となり，Moose が大流行していることが疑われる．

7. 考察

本章では，5 章の検証実験結果およびハニーポットの分散配置を容易にするアーキテクチャの改良に関する考察を記述する．

7.1. Telnet 以外の組込み機器への攻撃

特定メーカ製のルータに存在する脆弱性　当該脆弱性に関しては，2014 年 8 月 27 日に[13]で脆弱性が報告され，製品ベンダがファームウェアのアップデートをすることで, 2014 年 9 月 5 日までに解決されたと報告されている[23]．本稿の観測では，脆弱性の修正から約 1 年後に攻撃の増加を観測し，また，脆弱性修正以降も攻撃が継続していることから，問題が修正されずに運用されている機器が多数存在することが推察される．

DVR 設定ファイルが漏洩する脆弱性　認証不要で DVR 設定ファイルが漏洩する脆弱性に関しては，現在までに脆弱性の修正が行われたという情報は確認できていない．また，被害を受ける機器がどの程度運用されているのかも定かではない．設定ファイルには，DVR のユーザ名/パスワードの他に，PPPoE のアカウント情報，DNS サーバ，FTP サーバ，メールサーバ等，機密性の高い情報も含まれており，より深刻な被害に繋がる可能性がある．

インターネット上から閲覧可能な IP カメラ　検証実験の結果から，IP カメラの映像を盗聴するホストの存在が確認できた．また，映像内のユーザ名/パスワードを Basic 認証で使用した攻撃者は，マルウェアによる不正アクセスではなく，実際の人間によるものであることが推測される．また，本研究においても，攻撃者を惹きつけるため，[26]のサイトに IP カメラの登録を試みたが，Web サイトからエラーが返され，登録は成功しなかった．

7.2. 組込み機器を標的とした攻撃への対策

組込み機器の特性上，通常の PC のように，OS を再インストールすることや，ストレージを取り替えるといったことが難しく，また組込み機器用アンチウイルスソフトも普及していないため，一度マルウェア感染してしまうと復旧が困難な場合が多く，事前対策が重要になる．Telnet による不正侵入に対しては，SSH プロトコルを使用する，強固なユーザ名/パスワードに変更する，ISP が 23/TCP の通信を遮断することで大半を防ぐことができると推測される．既に機器がマルウェアに感染してしまった場合，マルウェアによっては Telnet や SSH といった遠隔操作用のデーモンプログラムを停止させてしまい，リモートからの復旧が困難になる場合も少なくない．今後，組込み機器への攻撃が多彩化する可能性があるため，継続して 23/TCP への攻撃の動向を注意深く観測する必要がある．

7.3. ハニーポットの分散配置

従来の提案手法では, 各観測地点にそれぞれハニーポットを構築する必要があった．IoTPOT の構築には，システムを効果的に運用するための技術的知識や，十分なサーバ資源，安全性を確保するための設定等，非常にコストを要した．提案手法では，各観測点にプロキシを配置し，攻撃者からの通信をすべて中央観測拠点の IoTPOT に転送することで，ハニーポットを多数のネットワークに容易に分散配置可能となり，観測可能性の向上が期待できる．

8. 関連研究

リモートエクスプロイトにより感染を拡大させるマルウェアの観測や検体収集を目的としたサーバ型のハニーポットを用いた研究は活発に行われている[15,16,17].

23/TCP でポート待ち受けを行うハニーポットには Honeyd [18], Telnet password ハニーポット [19]がある．Honeyd は，低対話型のハニーポットで，Telnet オプションや攻撃者からのコマンドに対する

応答を高い精度で模擬することができない．Telnet password ハニーポットは，Telnet の認証におけるパスワードを収集することに特化しており，ログイン成功後については，実装がなされていない．

岸本らの提案した IPv6 のハニーポット[20]では，宛先 IP アドレスにおけるベンダ情報を含む NS メッセージに着目することで，IPv6 アドレスを適切な高対話型ハニーポットへ動的に割り当てる．SGNET [21] は，IoTPOT 同様，分散配置されたフロントエンドとバックエンドのハニーポットによって構成される．分散配置されたフロントエンドに到達した攻撃が未知のものであった場合，バックエンドのシステムに通信を転送し，それに対する応答を学習することで模擬可能な攻撃を拡充させる．IoTPOT と上述した SGNET および IPv6 のハニーポットでは，ハニーポットの構成に類似点が見られる．学習したコマンドに対してはフロントエンドで応答を返し，未知の攻撃はバックエンドのシステムに転送する点が SGNET と類似し，異なるホストの様々な機器の模擬を実現する点において IPv6 honeypot と類似する．これらの既存研究と提案手法における最も大きな違いは，ハニーポットに攻撃してきたホストに対しスキャンを行うことにより，攻撃ホストのデバイスプロファイルを自動収集する点である．本機能により，提案手法は，実際にマルウェアに感染し，悪用されている組込み機器に関する情報を収集し，これらの脆弱な組込み機器をハニーポットで模擬することが可能となる．

9. まとめと今後の課題

本稿では，組込み機器への攻撃を観測するハニーポットである IoTPOT の機能拡張を提案し，検証実験により，Telnet に加えて，DVR 設定ファイルが漏洩する脆弱性，特定メーカ製ルータに存在する脆弱性および IP カメラに対する攻撃が存在することを確認した．また，本分析結果は，攻撃に悪用されている機器の特定や，組込み機器を悪用しての攻撃の観測にも活用可能であることから，マルウェア感染状況の把握や対策技術への応用に期待できる．また，IoTPOT を用いて組込み機器への攻撃の動向を継続監視・分析することは，組込み機器への攻撃の対策を検討するうえで有効であるといえる．

今後の課題としては，提案手法による組込み機器への攻撃の観測・分析を継続するとともに，観測した攻撃に対する対策手法の検討や，既にマルウェア感染してしまったデバイスの復旧・復元について調査を行いたい．

謝辞

本研究の一部は，総務省情報通信分野における研究開発委託／国際連携によるサイバー攻撃の予知技術の研究開発により行われた．また本研究の一部は，文部科学省国立大学改革強化推進事業の支援を受けて行われた．

文　献

[1] Internet Census 2012. [Last visited: 2015/05/24]. http://internetcensus2012.bitbucket.org/paper.html.

[2] Lizard Stresser Runs on Hacked Home Routers — Krebs on Security. [Last visited: 2015/05/24]. http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.

[3] RFC 854 - Telnet Protocol Specification. [Last visited: 2015/05/24]. https://tools.ietf.org/html/rfc854.

[4] Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow “IoTPOT: Analysing the Rise of IoT Compromises”, 9th Usenix Workshop on Offensive Technologies (WOOT’ 2015), Washington D.C, United States, 2015 August.

[5] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow “IoTPOT: A Novel Honeypot for Revealing Current IoT Threats”, Journal of Information Processing, Japan, Vol.24, No.3. March 2016.

[6] netfilter/iptables project homepage - The netfilter.org project. [Last visited: 2015/11/03]. http://www.netfilter.org/.

[7] Ubuntu. [Last visited: 2016/01/28]. http://www.ubuntu.com/

[8] robertdavidgraham/masscan · GitHub. [Last visited: 2015/05/24]. https://github.com/robertdavidgraham/masscan.

[9] QEMU. [Last visited: 2015/09/30] http://wiki.qemu.org/Main_Page.

[10] Index of /~aurel32/qemu/mipsel. [Last visited: 2015/11/04]. https://people.debian.org/~aurel32/qemu/mipsel/.

[11] OpenWrt. [Last visited: 2015/09/30]. https://openwrt.org/.

[12] BB-SP104W, Panasonic. [Last visited: 2016/01/28] http://panasonic.biz/netsys/netwkcam/lineup/sp104w.html

[13] トレンドマイクロセキュリティブログ, UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認. [Last visited: 2016/01/28] http://blog.trendmicro.co.jp/archives/9725

[14] RAID7, Multiple DVR Manufacturers Configuration Disclosure. [Last visited: 2016/01/28] https://www.rapid7.com/db/modules/auxiliary/scanner/misc/dvr_config_disclosure

[15] dionaea — catches bugs. [Last visited: 2015/05/24]. http://dionaea.carnivore.it/.

[16] Nepenthes - finest collection. [Last visited: 2015/05/24]. http://nepenthes.carnivore.it/.

[17] desaster/kippo · GitHub. [Last visited: 2015/05/24]. https://github.com/desaster/kippo.

[18] Developments of the Honeyd Virtual Honeypot. [Last visited: 2015/05/24]. http://www.honeyd.org/.

[19] zx2c4/telnet-password-honeypot · GitHub. [Last visited: 2015/05/24]. https://github.com/zx2c4/telnet-password-honeypot.

[20] K. Kishimoto, K. Ohira, Y. Yamaguchi, H. Yamaki, and H. Takakura, “An adaptive honeypot system to capture ipv6 address scans,” in *Cyber Security (CyberSecurity), 2012 International Conference on*, 2012, pp. 165–172.

[21] C. Leita and M. Dacier, “SGNET: a worldwide deployable framework to support the analysis of malware threat models,” in *Dependable Computing Conference, 2008. EDCC 2008. Seventh European*, 2008, pp. 99–109.E

[22] welivesecurity, Dissecting Linux/Moose. [Last visited: 2016/01/28] http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf

[23] トレンドマイクロセキュリティブログ, Netis 製ルータに存在する不具合を修正する更新プログラムを検証. [Last visited: 2016/01/28] http://blog.trendmicro.co.jp/archives/10050

[24] Symantec Official Blog, Is there an Internet-of-Things vigilante out there? [Last visited: 2016/01/28] http://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there

[25] VirusTotal - Free Online Virus, Malware and URL Scanner. [Last visited: 2016/01/28]. https://www.virustotal.com/.

[26] Insecam.com, Network live IP video cameras directory. [Last visited: 2016/01/28]. http://www.insecam.org/