Computer Security Symposium 2019
21 - 24 October 2019

制御サーバへの接続性に着目したIoTボットネットの解析

玉井 達也[1,a)]　田辺 瑠偉[2]　伊沢 亮一[3]　吉岡 克成[4]　松本 勉[4]

概要：IoT 機器が急速に普及している一方で，攻撃者はセキュリティに問題のある IoT 機器をマルウェア感染させている．また，感染した機器により構成される IoT ボットネットは，DDoS 攻撃やマイニング，機器の破壊を行うなどインターネット上の脅威となっている．そのような IoT ボットネットの対策を考える上で，IoT マルウェアがダウンロードされるサーバや感染機器を制御するサーバの特徴を把握することは重要である．本研究では，インターネット上に公開した IoT ハニーポットの観測結果を用いて，IoT ボットネットの制御インフラを解析する．実験の結果，観測されたボットネットの大部分において，IoT マルウェアは制御サーバ情報を 1 つしか持たず，制御サーバの生存期間が短命であることから，IoT ボットネットの多くは使い捨てであることがわかった．その一方で，一部の IoT ボットネットが Windows ボットネットで使われていた IP Flux 等の検知回避手法を用いるなど，堅牢なインフラを構成し始めたこともわかった．そこで，IoT ボットネットの特徴とその対策について考察を行った．

キーワード：ボットネット，IoT マルウェア

Analysis of IoT Botnet Focused on the Connectivity to Control Servers

Tatsuya Tamai[1,a)]　Rui Tanabe[2]　Ryoichi Isawa[3]　Katsunari Yoshioka[4]　Tsutomu Matsumoto[4]

Abstract: While IoT devices are rapidly spreading, attackers infect insecure IoT devices with malware. IoT botnets composed of these infected IoT devices have become threats on the Internet conducting various attacks such as record-breaking DDoS attacks by Mirai. For conducting efficient countermeasures, it is important to grasp the characteristics of the malware download servers and Command and Control (C&C) servers. In this paper, we study the control infrastructure of IoT botnet by capturing malware binaries using IoT honeypot and analyzing them with malware sandbox. As a result, we found that most of the analyzed IoT malware binaries contain minimum information to connect their C&C servers whose active period is also very short. Therefore, most of the observed IoT botnets are short-lived and used in disposable manner. However, we note that it is found that a few IoT botnets began to adopt similar techniques used by Windows botnets to construct a robust infrastructure. We then discuss countermeasures.

Keywords: Botnet, IoT malware

1. はじめに

近年，様々な機器をインターネットに接続する事で，多様なサービスを提供するモノのインターネット (Internet of Things) が注目されている．IoT の普及は急速で，2020 年には約 200 億台もの機器がインターネットに接続される

1 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University
2 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
3 国立研究開発法人情報通信研究機構
National Institute of Information and Communications Technology
4 横浜国立大学大学院環境情報研究院/先端科学高等研究院
Graduate School of Environment and Information Sciences, Yokohama National University / Institute of Advanced Sciences, Yokohama National University
a) tamai-tatsuya-hm@ynu.jp

© 2019 Information Processing Society of Japan

と言われている [1].

IoT 機器が増加している一方で，一部の IoT 機器はセキュリティ対策が不十分な状態で販売されている．攻撃者はこれらの機器に共通して問題となっている，容易に推測可能なパスワードで動作する Telnet や遠隔から任意のコードが実行できる脆弱性を突いて攻撃対象機器を自身のコントロール下に置いている．特に，IoT マルウェアに感染した機器によって構成されるボットネットはインターネット上の重大な脅威となっている．例えば，2016 年には DNS サービスサイト Dyn が IoT ボットネットによる 1Tbbps を超える DDoS 攻撃を受けてダウンし，Twitter や Netflix などの有名サービスが一時利用不可能となった [2]．また，DDoS 攻撃以外にも，マイニングスクリプトを実行する IoT マルウェア [3] も登場するなど攻撃は多様化している．

NICTER の 2018 年度観測レポート [4] では，インターネット上の機器に対するスキャン活動のうち，Telnet が動作する 23 番ポートや，Mirai 亜種が感染に利用した 52869 番ポートなどの IoT に関連するポートが上位となっており，IoT 機器を狙った攻撃が増加していることがわかる．このため，IoT ボットネットへの早急な対策が求められている．

IoT ボットネットの対策を行なう上で，IoT ボットネットを構成する IoT マルウェアやサーバの情報を把握することは重要である．先行研究において，IoT マルウェアは従来の Windows マルウェアとは異なり，感染機器の再起動などにより感染前の状態に自然に回復することが示されている [5]．一方で，攻撃者が IoT ボットネットをどのように構築して運用しているかを明らかにした研究は少ない．IoT ボットネットを制御するサーバの特徴や運用の実態を把握することは，有効な対策を検討する上で重要でありさらなる調査・研究が望まれている．

本研究では，インターネット上に公開した IoT ハニーポットの観測結果を用いて，IoT ボットネットの制御インフラを分析する．特に，マルウェアバイナリが制御サーバへの接続情報をどの程度保持しているか，また，その制御サーバがどの程度の期間運用されているかなど，制御サーバへの接続性に着目して分析を行う．

分析の結果，観測されたボットネットの大部分において，IoT マルウェアは制御サーバ情報を僅かしか持たず，制御サーバの活動期間が短命であることから，IoT ボットネットの多くは使い捨てであることがわかった．その一方で，Windows ボットネットで使われていた検知回避手法である IP flux を用いる IoT ボットネットが 2 件確認されるなど，堅牢なインフラを構成し始めたこともわかった．そこで，IoT ボットネットの特徴とその対策について考察した．本研究により明らかとなった IoT ボットネットの制御インフラの運用に関する知見を以下にまとめる．

- 多くの IoT マルウェアのバイナリには接続先の制御サーバの情報は 1 つの IP アドレスしか含まておらず，さらに，対応する制御サーバの生存期間が短いことから，多くの IoT ボットネットは使い捨てされている．
- IoT マルウェアの制御サーバの多くはクラウドサービスで運用されており，感染機器をボットネットインフラの一部として利用するような複雑な運用には至っていない．
- IP flux を用いるボットネットが 2 件確認された．IoT ボットネットにおいても Windows ボットネットで用いられていた検知回避手法が用いられ始めている．

本研究の構成は次の通りである．2 章では，背景として，これまでの IoT マルウェアの流行について概説する．3 章では，ボットネットの解析に関する関連研究を説明する．4 章では観測のためのハニーポットについて，5 章ではその観測結果について説明を行なう，6 章では結果に対する考察をし，7 章ではまとめについて述べる

2. 背景

2012 年の Carna[6] と呼ばれるボットネットの登場により，ルータ等の多くの IoT 機器において動作している遠隔操作サービスが，容易に推測可能な ID とパスワードの組で運用されていることが明らかになった．当該マルウェアは，匿名のセキュリティ研究者により作成されたといわれており，約 42 万台もの機器を感染させることで大規模なボットネットを構成した．

その後，Bashlite や Mirai と呼ばれるマルウェアが登場した．これらのマルウェアも Telnet を悪用して多くの機器に感染してボットネットを構成した．2016 年に Bashlite は 400Gbps[7] の，Mirai は 1Tbps の DDoS 攻撃を行い [2]，深刻な被害を引き起こした．さらに，Mirai のソースコードが公開されたことにより，様々な Mirai の亜種が登場した．その中には機器固有の脆弱性を狙うなど [8]，より多様な感染経路をもつ IoT マルウェアも存在する．

また，これまでのワーム型の IoT マルウェアとは異なり，P2P 型の IoT マルウェアである Hajime[9] が報告されている．Hajime はセキュリティ研究者によって作られたといわれており，実際の攻撃には加担した記録はないものの，その規模と感染力から注視すべきボットネットであると指摘されている [10]．一方で，Mac OS X を狙うマルウェアから派生した Tsunami[11] や，DDoS 攻撃以外にもルータに接続したデバイス上でマイニングスクリプトを実行をするマルウェア [3] や機器の破壊を行なうマルウェア [12] が登場するなど，IoT 機器を狙う攻撃が深刻化している．

3. 関連研究

3.1 Windows ボットネットの対策

ボットネットを検知し，無効化しようとする研究は 2005 年から行われている [13]．特に制御サーバの中でも，攻撃

者が感染した機器へ命令を送るための C&C サーバは，その生存期間がボットネット全体を無効化する手がかりとなることが知られている [14]．そのため，ボットネットを無力化する対策として，C&C サーバへの接続をブラックリストによって防ぐ，あるいはサーバそのものを無力化するといった対策がなされてきた．

その一方で，攻撃者にとっても制御サーバを検知されることは，ボットネットの無力化や自身の特定に繋がってしまう．このため，攻撃者は制御サーバが検知されることを防ぐための様々な検知回避手法をボットネットに用いてきた．攻撃者は, ドメインを大量に生成し制御サーバへ接続する仕組み（DGA）やドメインの解決先の IP アドレスを次々に切り替える IP flux といった手法で制御サーバを検知されないようにしてきた．また，マルウェアの解析を防ぐために，難読化や Evasion といった手法を取ることが知られている．

3.2 IoT ボットネットに関する分析

IoT 機器への攻撃が増加するにつれて，セキュリティ研究者によって，IoT 機器に感染するマルウェアに対しても研究が行われるようになった．

[15] の研究では Mirai マルウェアについてその出現からボットネットがどのように成長していったか，ボットネットの制御の仕組みや攻撃手法に関して詳細に分析が行われている．また，[10] の研究では P2P 型の IoT マルウェアである Hajime について同様の研究が行われている．また，[16] の研究では,Bashlite と Mirai を比較しながら分析し，Mirai では，制御サーバが様々なネットワークに分散し，マルウェアの更新頻度が高いことを明らかにした．このことから [16] の著者らは，IoT マルウェアの管理が容易になっていると分析している．

しかしながら，これまでの IoT ボットネットに関する研究では，制御サーバの生存期間の分析やマルウェア内に含まれる制御サーバへの接続情報の分析は行われておらず，制御サーバのテイクダウンやブロックを行うための検討が十分ではなかった．また，特定のファミリに限らない IoT ボットネット全体の特徴についても分析はなされていない．

そこで本研究では，制御サーバの生存期間やマルウェアの制御サーバへの接続性に着目して，IoT ボットネットの特徴について解析を行なう．

4. 観測機構

本研究では，IoT ボットネットにおける制御サーバの実態を明らかにするために，IoT ハニーポットを用いて観測を行った．IoT ハニーポットは，IoTPOT[17] の構成をもとに設計を行った．IoTPOT では通信の応答部に仮想環境が用いられていたが，本研究では実際の IoT 機器を用いて高対話型のハニーポットを構成した．**図 1** は，解析システムの概要図である．解析システムは、次の 5 つの要素から構成されている．

IoT ハニーポット：IoT ハニーポットでは脆弱性をもつルータや Wi-Fi ストレージ等の実際の IoT 機器を用いた高対話型ハニーポットが動作している．本研究では，10 台のルータと 4 台の Wi-Fi ストレージを用いてハニーポットを構築した．攻撃者によるハニーポットへのログインの試みや侵入後のコマンドシーケンスなどがここで観測される．

IoT マルウェアダウンローダ：IoT マルウェアダウンローダでは、IoT ハニーポットで観測されるコマンドシーケンスから，マルウェアダウンロードコマンドの抽出を行なう．ダウンロードコマンドが確認された場合，直ちに攻撃者のマルウェアダウンロードサーバに接続し，IoT マルウェア検体のダウンロードを試みる．

サンドボックス：サンドボックスは仮想環境と実際の IoT 機器の両方を用いて構成されている．仮想環境は QEMU を使用し，Linux OS（Debian）が動作している．実際の機器はハニーポット部でも用いたルータを利用している．実際の機器を用いたサンドボックスは，仮想環境に比べて，環境の復元に注意が必要である．しかし，先行研究 [18] から，既存の IoT マルウェアは再起動により駆除できることが分かっており，本研究においても機器の再起動により環境の復元を行った．サンドボックスでは，繰り返し接続を試みる宛先や，スキャンポートとは異なる宛先が制御サーバに関連すると考えて解析を行った．

アクセス制御部：アクセス制御部では，インターネットと IoT ハニーポット，IoT マルウェアダウンローダ，サンドボックスの間の通信を制御する．特に，ハニーポットで用いている実際の機器が IoT マルウェアに感染してしまう，動的解析時の通信により攻撃に加担してしまうといったことがないように，通信の制御を適切に行なった．

データベース：観測された攻撃者のサーバ情報やダウンロードしたマルウェアバイナリ，関連する情報はデータベースに保存される．

5. 観測結果

本研究では，観測を 2016/10 から 2017/12 まで（ハニーポット 1 ）と，2018/10 から 2019/5 まで（ハニーポット 2 ）の期間で行った．また，ハニーポット 2 において，通信の制御の見直しを行っている．なお，本研究において P2P 型のマルウェアである Hajime は，制御サーバを持たないことから対象外とした．

5.1 観測した制御サーバ

観測期間における観測によって，6,295 種類の MIPS マルウェア検体を収集し，そのダウンロードサーバ 3,217 件を観測した．さらに，これらの MIPS マルウェアを動的解析することで， 2,869 件の C&C サーバを観測した．ただ

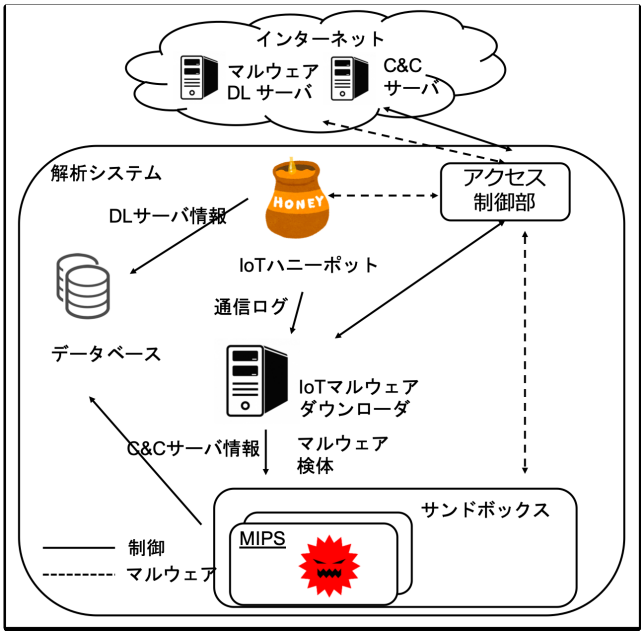

図 1　解析システム構成図
Fig. 1　Structure of Analysis System.

表 1　IoT ハニーポットの観測結果
Table 1　IoT honeypot observation results.

ID	DL	C&C	マルウェア (MIPS)
ハニーポット 1	695	567	1,443
ハニーポット 2	2,523	2,304	4,852
計	3,217	2,869	6,295

し，C&C サーバは [19] の研究の手法を用いて，動的解析時に通信を繰り返し試みる宛先とした．また，基準とする回数は宛先のポートがマルウェアがスキャンを行っているポートと一致する場合は 10 回，一致しない場合は 4 回とした．それぞれのハニーポットにおける収集したデータは**表 1** のようになっている．

また，観測した制御サーバが多く存在した AS について，IP2Location[20] を用いて，その利用目的を調査した (**表 2**, **表 3**)．このうち，利用目的がクラウドサービスとなっていたものを色付けした．多くの制御サーバがクラウドサービスに用いられる AS で動作している．クラウドサービス上で IoT 機器が動作している可能性は低いと考えられ，多くの制御サーバがクラウドサービスを利用して運用されていることが分かった．

5.2　制御サーバにおけるドメインの利用状況

次に，制御サーバの特徴を追跡するために，これらのサーバにおけるドメインの利用状況を調査した．特に，同じドメインが異なる観測 IP アドレスに解決される場合に着目して，攻撃者がドメインを用いて複数の IP アドレスを管理する場合を調査した．このような場合には，攻撃者は制御サーバの IP アドレスが切り替わった後も，マルウェア感染させた IoT 機器を継続してコントロールすることができる．

観測した IP アドレスに解決されるドメインの調査を DNSDB[21] を用いて行った．ただし，観測した IP アドレスに解決されるドメインの中には，例えば********.[プロバイダ名]dns.com.** のようにプロバイダによって設定されるものや正規のユーザが設定したものも含まれてしまう．そこで，VirusTotal[22] を用いて得られたドメインを調査し，悪性と判断されたドメインを分析対象とした．

調査した結果，攻撃者が複数の IP アドレスを管理するドメインを計 53 件観測した．例えば **bot.sunless.network** というドメインでは 2018/12/20/から 2019/5/14 まで，解決先の制御サーバの IP アドレスが複数の AS の IP アドレ

表 2　ダウンロードサーバの AS 情報
Table 2　AS Information of Malware Download Server.

	ハニーポット 1		ハニーポット 2	
	ASN	IP 数	ASN	IP 数
1	20473	91	14061	1,334
2	31034	87	60144	77
3	14061	83	51659	75
4	23033	69	20473	73
5	36352	30	54290	69
6	12876	30	53667	56
7	43350	27	31034	56
8	60781	21	16276	52
9	16276	16	15169	34
10	4766	8	57673	32

表 3　C&C サーバの AS 情報
Table 3　AS Information of C&C Server.

	ハニーポット 1		ハニーポット 2	
	ASN	IP 数	ASN	IP 数
1	31034	78	14061	1216
2	20473	68	60144	76
3	14061	55	20473	65
4	23033	50	16276	62
5	36352	21	51659	61
6	60781	17	54290	56
7	43350	16	31034	52
8	25369	12	53667	39
9	12876	11	15169	28
10	44812	11	57673	28

表 4　制御サーバにおけるドメインの利用状況
Table 4　Domain usage on the control server

	ハニーポット 1		ハニーポット 2	
	DL	C&C	DL	C&C
対象 IP 数	695	567	2,523	2,304
複数の観測 IP に解決される悪性ドメイン数	12	14	36	24
関連する IP 数	23	23	100	76

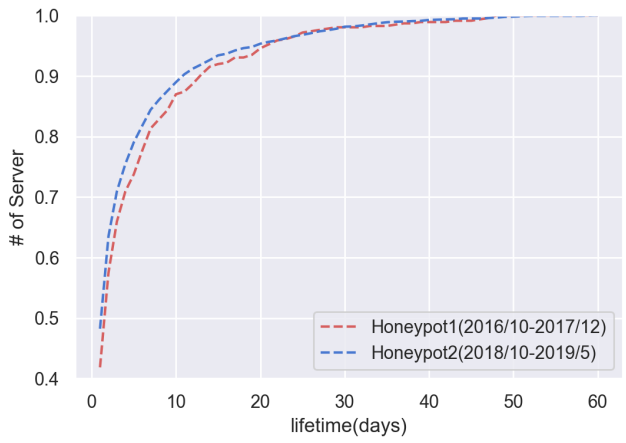

図 2　ダウンロードサーバの生存期間
Fig. 2　Lifetime of Download Server

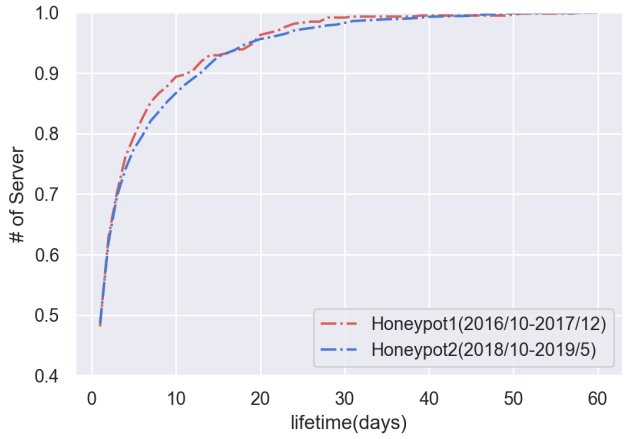

図 3　C&C サーバの生存期間
Fig. 3　Lifetime of C&C Server

スへ順に切り替わっていた．しかしながら，全体のうち複数の IP アドレスに結びつく悪性ドメインは非常に少なく，DNS を利用して柔軟に制御サーバへの接続を確保するようなボットネット運用はほとんど見られなかった (**表 4**).

5.3　制御サーバの生存期間

さらに，制御サーバの生存期間を調査した．生存期間は IP アドレス毎に最初の観測日と最後の観測日の差分を計算した．ただし，前節で同じドメインに結びついた IP アドレスについては，同じ制御サーバとして計算を行った．また，一度のみ観測した制御サーバの生存期間を 0 日とした (**図 2**，**図 3**)．いずれのハニーポットの観測においても，5 日以内に 7 割，2 週間以内に 9 割近くの制御サーバが活動しなくなった．その一方で，一部の C&C サーバが 150 日近く活動し続ける様子も観測された．

5.4　マルウェアの C&C サーバへの接続性

マルウェア内の制御サーバ情報について調査を行った．攻撃者はマルウェアに制御サーバの情報を IP アドレスのリストやドメインでハードコードする．攻撃者は制御サーバを別の IP アドレスに変更したり，ブラックリスト等で一部のサーバに接続ができなくなっても，継続して感染機器をコントロールすることができる．

動的解析によって C&C サーバが抽出できた 5,289 検体のうち，1 つの C&C サーバに接続できない場合に別の C&C サーバへの接続を試みる検体，すなわち複数の C&C サーバ IP アドレスをリストとしてもつ検体は 280 検体であった．また，ドメインによって制御サーバへ接続する検体は 480 検体であった．

さらに，ハニーポット 1 において収集した 1,443 個の検体について制御サーバへの接続機能を静的解析したところ，これらの検体には制御サーバ接続情報として 1 つの IP アドレスのみが含まれていた．このように制御サーバへの接続情報は必要最小限しか保持しないマルウェアが多数であることからほとんどの IoT ボットネットの C&C サーバへの接続は脆弱であると考えられる．

5.5　検知対策

本節では，本研究において観測した攻撃者の検知対策についてまとめる．5.2 節において，ハニーポット 2 で観測した IP アドレスに解決されるドメインを調査した際，複数 IP に結びつくドメインが 53 件と少なかった一方で，非常に多くの IP が紐づく特異なドメインが存在した．このドメインについて調査したところ，このドメインは数秒から数十秒程度で解決先が切り替わりながら，多くの IP アドレスに解決されていることが分かった．このような特徴が現れるのは，従来の Windows ボットネットで用いられていた検知回避手法である IP flux が用いられているからであると考えられる．全体の傾向としては複数 IP に結びつくものは少なく，IoT ボットネットの運用において冗長化，耐性は見られなかった一方で，特異な事例としてこのような IP Flux の運用も観測された．

また，動的解析時に，実行名をハニーポットでの観測時と同じ引数にしたときにのみ C&C サーバへの通信を試みる検体を確認した．検体を実行する際に，Windows マルウェアでも用いられていた，hash 値等の実行名で実行した際に挙動を変えるという解析対策が用いられていると考えられる．公開された Mirai のソースコードにおいても，引数によって挙動を変える仕組みが存在しており，一部の攻撃者はこのような動的解析対策も行っていることが明らかになった．

6.　考察

6.1　攻撃者によるボットネットの使い捨て

観測結果から，攻撃者の制御サーバの大半は生存期間が短いにも関わらず，複数の IP アドレスがドメインやマルウェア検体内のリストによって紐づくことは少ないことが

分かった．そのため，マルウェアに感染した IoT 機器は，短期間で制御サーバとの通信を行えなくなり，攻撃者は機器のコントロールを失うことになると考えられる．

このことから，マルウェア感染によって構成される IoT ボットネットの大半は攻撃者に使い捨てられていると考えられる．すなわち，攻撃者は，新たに制御サーバを用意し，機器を感染させボットネットを構成するということを短期間に繰り返していると考えられる．

次に，攻撃者がボットネットを使い捨てる要因について考察する．このような使い捨ての要因には IoT 機器の性質や IoT セキュリティが不十分である現状が関係すると考えられる．

要因の 1 つとして，容易にマルウェア感染が可能な，セキュリティに問題のある IoT 機器が多く存在していることが挙げられる．攻撃者がマルウェアに感染させ，コントロール下においた機器を簡単に手放すことは，再度感染させることができる機器が十分に存在していなければできない．特に，安価な IoT 機器ではファームウェアの更新が十分でない場合が多いことは，マルウェアの感染をさらに容易にさせていると考えられる．

一方で，感染させた機器をコントロールし続けることが難しいことも，攻撃者がボットネットを使い捨てる一因となっていると考えられる．先行研究において，IoT マルウェアは，感染機器の再起動によって，感染前の状態に自然回復する確率が高いことが明らかにされている [5]．Hajime マルウェアの一部は永続感染する [23] ことが報告されているが，永続感染の仕組みから永続感染可能な機器は一部に限定されている．本研究においても，動的解析の環境は再起動によって復元することができた．

さらに，[24] などで指摘されているように，IoT ボットネットを作成するためのツールが，ダークマーケットで販売されるなど容易に入手可能となっていることも要因と考えられる．ツールが簡単に入手できることは，スクリプトキディと呼ばれる興味本位で攻撃を行なう攻撃者を増加させる．

一方で，一部のボットネットの制御サーバはドメインを用いていたり，1 つの IP アドレスで長期間活動を続けるなど，堅牢なボットネットも存在している．そのため，IoT ボットネットの対策は，このような 2 つの性質があることに注意しながら行う必要がある．

6.2 IoT ボットネット対策

次に，このような IoT ボットネットの特徴を踏まえた上でその対策について考察する．まず第一に，[15] で議論されていたように，機器側において不要な telnet サービスを閉じるなどして，マルウェアの侵入経路をなくすことはボットネットの特徴に関わらず重要であるといえる．

一方で，機器が感染しないように，制御サーバへのアクセスを IP アドレスやドメインをブラックリストによって制限することは，寿命の短い使い捨てのボットネットに対しては有効でないと考えられる．

また，制御サーバを停止させることでボットネットを無力化する対策も存在する．この対策についても新たなボットネットが容易に作成できる場合には有効な対策ではないと考えられる．

対策の難しい，使い捨てボットネットが存在するのは，容易に感染可能な機器が多く存在することが一因である．そのため，機器側での対策によって，このような状況を解消することが重要であるといえる．

7. まとめ

本研究では，インターネット上に公開した IoT ハニーポットを用いて IoT ボットネットの観測を行い，6,295 種類の MIPS マルウェア検体を収集し，3,217 件のダウンロードサーバと 2,869 件の C&C サーバを観測した．

さらに，制御サーバへの接続性に着目して，その特徴について分析を行った．分析の結果，IoT マルウェアの制御サーバの多くはクラウドサービスで運用されていた．このことから，P2P 型のボットネットを除き，攻撃者は感染させた IoT 機器をボットネットの制御インフラの一部としては利用していないことがわかった．また，制御サーバの多くは短い期間しか稼働していないにも関わらず，マルウェアバイナリには制御サーバへの接続情報が 1 つの IP アドレスしか含まれないことから，多くの IoT ボットネットは攻撃者に使い捨てられていると予想される．加えて，一部の IoT ボットネットにおいて，Windows ボットネットで用いられていた IPflux 等の検知回避手法が用いられ始めていることを明らかにした．

さらに，このような IoT ボットネットの特徴について要因とその対策の考察を行った．制御サーバに対する対策は使い捨てのボットネットが存在することを踏まえて行なうことが重要であるといえる．

参考文献

[1] Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 (参照:2019.08.21).

[2] Dyn, Dyn Analysis Summary Of Friday October 21 Attack, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (参照:2019.08.21).

[3] SpiderLabs blog, Mass MikroTik Router Infection First we cryptojack Brazil, then we take the World?, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/mass-mikrotik-router-infection-first-we-cryptojack-brazil-then-we-take-the-world/^^c2^^a0 (参照:2019.08.21).

[4] 国立研究開発法人情報通信研究機構, NICTER 観測

レポート 2018, https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf (参照:2019.08.21).
[5] etin, Orun, et al., Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai, NDSS. 2019.
[6] C. Botnet, Internet census 2012 port scanning using insecure embedded devices, http://internetcensus2012.git-hub.io/InternetCensus2012/paper.html (参照:2019.08.21).
[7] Tom Spring, LizardStresser IoT Botnet Part of 400Gbps DDoS Attacks, https://threatpost.com/lizardstresser-iot-botnet-part-of-400gbps-ddos-attacks/119006/ (参照:2019.08.21).
[8] TrendMicro, Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers (参照:2019.08.21).
[9] Sam Edwards and Ioannis Profetis, Hajime: Analysis of a decentralized internet worm for IoT devices, https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf
[10] Herwig, Stephen, et al, "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet.", NDSS. 2019.
[11] Barnett Ryan and Zioni Moshe, NEW TSUNAMI/KAITEN VARIANT: PROPAGATION STATUS, https://www.theregister.co.uk/2011/10/26/tsunami_mac_backdoor/ (参照:2019.08.21).
[12] DAN GOODIN, Rash of in-the-wild attacks permanently destroys poorly secured IoT devices, https://arstechnica.com/information-technology/2017/04/rash-of-in-the-wild-attacks-permanently-destroys-poorly-secured-iot-devices/ (参照:2019.08.21).
[13] Cooke, Evan, Farnam Jahanian, and Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets.", SRUTI 5 (2005): 6-6.
[14] Gan, Carlos, Orcun Cetin, and Michel van Eeten., "An empirical analysis of ZeuS C&C lifetime." , Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015.
[15] Antonakakis, Manos, et al. , "Understanding the mirai botnet.", 26th USENIX Security Symposium (USENIX Security 17). 2017.
[16] Marzano, Artur, et al., "The Evolution of Bashlite and Mirai IoT Botnets.", 2018 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2018.
[17] Pa, Yin Minn Pa, et al., "IoTPOT: analysing the rise of IoT compromises." 9th USENIX Workshop on Offensive Technologies (WOOT, 15). 2015.
[18] 原悟史, et al., "感染持続型 IoT マルウェアの実態調査と実機による概念実証.", 電子情報通信学会論文誌 B 102.8 (2019): 524-535.
[19] 鉄穎, et al. , "IoT マルウェアによる DDoS 攻撃の動的解析による観測と分析.", 情報処理学会論文誌 59.5 (2018): 1321-1333.
[20] IP2location, https://www.ip2location.com/ (参照:2019.08.21).
[21] Farsight Security, DNSDB, https://www.dnsdb.info/ (参照:2019.08.21).
[22] Virustotal, https://www.virustotal.com/ (参照:2019.08.21).
[23] 横浜国立大学 情報・物理セキュリティ研究拠点, 電源を切っても消えない持続感染型 IoT マルウェアについて, http://ipsr.ynu.ac.jp/iotmalware/index.html (参照:2019.08.21).
[24] IIJ Security Diary, 2018 年の IoT ボット観測状況と最近の動向, https://sect.iij.ad.jp/d/2019/01/288147.html (参照:2019.08.21).