Vol.2018-IOT-42 No.8
2018/6/29

ハニーポットを用いた IoT 機器に対する パスワードリスト攻撃の収集と分析

清松天樹[†1]　池部実[†2]　吉田和幸[†3]

概要：Mirai をはじめとした IoT 機器を狙ったマルウェアが次々と出現している．このようなマルウェアは IoT 機器の管理の不十分さ，IoT 機器の脆弱性を狙っており，感染した IoT 機器は踏み台となるため IoT 機器のシステム管理者にとって大きな脅威となっている．我々は，学内 LAN に設置したハニーポットを用いて Telnet サーバ(TCP/23，TCP/2323)へのコネクション接続状況を調査している．これまでの Telnet サービス向けハニーポットでは TCP コネクションを確立した後，接続を切断していた．本研究では Telnet サービスのエミュレートプログラムを開発し，ログイン ID とパスワード収集機能を実装した．Mirai はソースコードが github で公開され，利用しているパスワードリストは既知である．本論文では約 3 か月間収集したパスワードリストや攻撃の送信元とその分析結果について述べる．今回観測したログイン ID とパスワードの組み合わせは 522 種類，観測したパスワードリストは 965 種類であった．最も多く使用されたパスワードリストは Mirai の持つパスワードリストをすべて含み，さらに Mirai の保持していないログイン ID とパスワードの組が存在していた．

キーワード：IoT 機器，Telnet，ハニーポット，パスワードリスト攻撃

Collection and analysis for password list attacks to the IoT devices using honeypot system

TENKI KIYOMATSU[†1]　MINORU IKEBE[†2]
KAZUYUKI YOSHIDA[†3]

Abstract: Malware aiming at IoT devices including Mirai has been appearing one after another. Such malware aims at insufficient management of IoT devices and vulnerability of IoT devices, and infected IoT devices becomes a stepping stone, which is a big threat to system administrator of IoT devices. We are collect the connection status of the Telnet server (TCP / 23, TCP / 2323) using the honeypot built on the campus LAN.The honeypot for the Telnet service has disconnected after establishing a TCP connection. we develop an emulation program for Telnet service and implement function login ID and password. Mirai is published with source code in github, and the password list which Mirai uses is known.
In this paper, we describe the password lists and attacks collected for about 3 months, and their analysis.The number of combinations of login IDs and passwords was 522, and the number of password lists appeared most was 965.password lists included all Mirai's password lists, and there were also several pairs of login IDs and passwords that Mirai did not use.

Keywords: IoT devices, Telnet, honeypot, password list attacks

1. はじめに

IoT(Internet of Things，モノのインターネット)を活用することで業務の効率化や快適な生活を実現できるとして注目されている．IoT 機器とは，自動車や家電をはじめとしてインターネットに接続する様々な機器を意味する．例えば，ネットワークカメラは，高所や水辺など人間が現地で常時観測が困難な場所に設置し，遠隔から映像を確認することで観測場所の状況を把握する．IoT 機器に搭載されている計算資源は端末コスト削減のため，通信の暗号化・復号処理に割り当てる CPU リソースの余力がないことがある．このような IoT 機器を管理者が遠隔から管理するために IoT 機器では通信の暗号化・復号の必要のない Telnet サービスが動作していることがある．Telnet サービスでは ID とパスワードを用いてログインすることで遠隔操作が可能となる．しかし，IoT 機器のパスワードが初期設定のままの場合や，初期設定からパスワードを変更できない場合がある．パスワードが初期設定のままでは攻撃者に容易に侵入されてしまう．

2016 年 10 月に警察庁の発表したインターネット観測結果等(平成 28 年 9 月期)によると，Mirai マルウェアに感染した IoT 機器を発信元とした Telnet サービスを標的とした通信が増加していた[1]．2016 年 9 月 20 日にはジャーナリストであるブライアン・クレブスのウェブサイトへの攻撃や，インターネット関連企業である OVH に対しての大規模な攻撃に Mirai が利用されたと報告されている[2]．この Mirai は Telnet サービスに対してログインを試行する．Mirai はログインに成功すると IoT 機器を遠隔操作し，マルウェ

†1 大分大学院工学研究科工学専攻
Graduate School of Engineering, Oita University
†2 大分大学理工学部共創理工学科知能情報システムコース
Faculty of Science and Technology, Oita University
†3 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

アをダウンロードさせられる．マルウェアに感染した IoT 機器はボットとして動作し，感染拡大のための Telnet サービス探索活動や先に示したような攻撃の踏み台として利用される．また，Mirai には Telnet サービスを探索する中で，TCP/23 番ポートと TCP/2323 番ポートを 9 対 1 の割合で接続する特徴がある[2]．Mirai は 2016 年 10 月 1 日に，国外の Web サイトでソースコードが公開された．その後，Mirai をベースとしてプログラムを書き換えたと考えられる Mirai ボットの亜種の活動も確認されている[3]．

我々は，これまで学内ネットワーク上にハニーポットを設置し，不正通信の動向や攻撃手法を調査してきた．これまで Web アプリケーションの脆弱性を狙った攻撃を調査するために TCP/80 番ポート，TCP/8080 番ポート宛の HTTP リクエストの収集・分析[4]や，IoT 機器の Telnet サービスへの通信状況調査のために TCP/23，TCP/2323 番ポート宛の通信を観測してきた[5]．本研究では，IoT 機器に対する攻撃の詳細な手法を観測するために，低対話型ハニーポット Honeyd[6]に，Telnet サービスのログイン機能をエミュレートするプログラムを実装した．エミュレートプログラムでは，試行されたログイン ID とパスワードを収集する機能を実装した．今回は，IoT 機器の Telnet サービスを狙った攻撃のうち，マルウェアが次の感染先を探索する際の活動についての状況を把握することを目的として，開発したエミュレートプログラムを組み込んだハニーポットを稼働させ，約 3 ヶ月分の観測結果をもとにデータを分析した結果を報告する．

本論文の構成を以下に示す．第 2 章では本研究で用いた低対話型ハニーポットである Honeyd の特徴について述べ，第 3 章では Telnet サービスに対するパスワードリスト攻撃の観測方法を述べる．第 4 章にて観測データをもとに分析した結果と考察について述べる．最後に 5 章で本研究のまとめと今後の課題について述べる．

2. Honeyd

本研究では低対話型ハニーポットである Honeyd を用いた．Honeyd は 1 台の物理マシンで複数の仮想ホストをエミュレートでき，各仮想ホストでは特定 OS が稼働しているように見せかけられるオープンソースソフトウェアである．

ハニーポットには高対話型と低対話型の 2 種類がある．高対話型ハニーポットは，脆弱性を含む実際の OS やアプリケーションプログラムを用いるため，攻撃者の侵入後の詳細な挙動を観察できるが，攻撃者に攻撃の踏み台とされる可能性があるため慎重な運用が必要である．一方，低対話型ハニーポットは実際の OS やアプリケーションプログラムの機能の一部をエミュレートし攻撃を観察する．攻撃者を観測できるのは機能をエミュレートした範囲に制限される．そのため，実際に攻撃者に侵入され踏み台とされることはなく安全な運用が可能である．しかし，エミュレートした機能の範囲でしか情報を取得できないため，高対話型と比較して得られる情報は限定的である．

Honeyd は低対話型ハニーポットであるため，マルウェアに感染せず危険性が低く高対話型ハニーポットに比べて，安全に運用できる．また，Honeyd は 1 台の物理ホストで複数のホストをエミュレートする機能をもつため，本研究のようにログインおよびパスワード試行を複数の IP アドレスで観測することに適している．

本研究では Telnet サービスのログイン部分をエミュレートするプログラムを実装し，Honeyd に組み込んだ．telnet による TCP/23，TCP/2323 番ポート宛の通信に対してログイン ID とパスワードの入力を促し，Telnet サービスが動作しているように見せかけ，攻撃者のログイン ID とパスワードの入力パターンを観測した．

3. パスワードリスト攻撃の観測方法

3.1 従来の Honeyd サーバの Telnet サービスに対する攻撃の観測方法

先行研究[5]におけるハニーポットで Telnet サービスへの通信状況の観測方法および，Honeyd サーバの設置環境を図 1 に示す．学内ネットワークからサブネット長 24 のサブネットをハニーポット用として割り当て，Honeyd を当該サブネットに設置している．Honeyd でエミュレートしている IP アドレスは， 254 個のうち 251 個である．

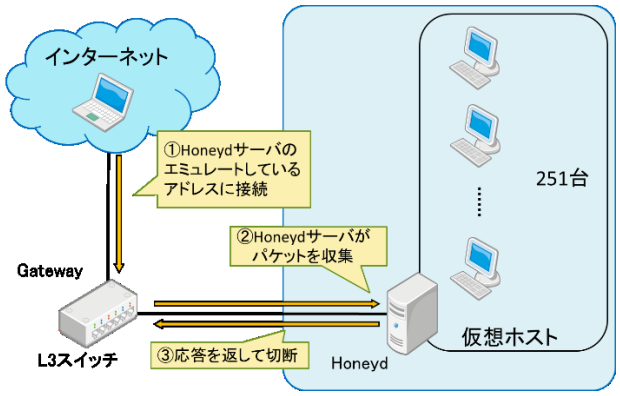

図 1　Honeyd サーバの設置環境

Honeyd サーバがエミュレートしている 251 個の IP アドレスの Telnet サービスに対する通信の観測方法を以下に示す．エミュレートした Telnet サービスは，TCP/23 番ポートおよび TCP/2323 番ポートで接続を待ち受けている．

1. Telnet サービスに対して TCP コネクションの確立要求(TCP SYN)を受信
2. 送信元に対して TCP SYN/ACK を応答し，相手からの TCP ACK を待機
3. 送信元からの TCP ACK を受信し，TCP スリーウェイハンドシェイクが成功し，Telnet サービスへの接続を確立
4. Telnet サービスへの接続直後に Honeyd 側から接続を切断

上記に示した観測方法の中で，以下の 6 項目をアクセスログとして記録した．また実際のアクセスログを図 2 に示す．送信元 OS 判別に p0f[7]を用いている．ただし，p0f では IP パケットから OS を判別できない場合もあるため，アクセスログには送信元 OS の記述がない場合もある．

- 受信時刻(JST)
- 送信元 IP アドレス
- 送信元ポート番号
- 宛先 IP アドレス
- 宛先ポート番号
- 送信元 OS

```
Fri Jun  1 16:06:16 JST 2018 From 219.218.19.249 35072 To 133.37.17.240 23 OS:"Linux 2.6 .1-7"
Fri Jun  1 16:06:17 JST 2018 From 209.97.142.159 37926 To 133.37.17.193 23 OS:"Linux 2.2 20-25"
Fri Jun  1 16:06:17 JST 2018 From 5.250.81.10 58828 To 133.37.17.202 23 OS:""
```

図 2 Honeyd で記録したアクセスログ

図 3 に Honeyd サーバにてエミュレートしている IP アドレス A に対して検証用クライアントから telnet で接続を試みたときの結果を示している．TCP コネクションの確立後，すぐに切断される．

#	コマンドおよび結果
1	$ telnet A
2	Trying A ...
3	Connected to A.
4	Escape character is '^]'.
5	Connection closed by foreign host.

図 3　Honeyd サーバへのログイン試行(1)

従来の Honeyd サーバにて収集したアクセスログにおいてアクセス数や送信元 OS に着目し分析した．分析結果 Telnet サービスへの攻撃が増加していること，判別できた送信元 OS において Linux の比率が高かったことを確認した[6].

3.2 新しい Honeyd サーバの観測方法

そして，本研究では従来収集していたアクセスログに加えて Telnet サーバのログイン機能をエミュレートさせる機能を追加し，送信者が試行したログイン ID とパスワードを収集した．送信者が試行したログイン ID とパスワードの組を既知のパスワードリストと比較し，送信元の特性を調査する．

従来の Honeyd サーバに加えて，Telnet サービスのログイン機能をエミュレートするプログラムを実装した Honeyd サーバ 2(以下，Honeyd サーバ 2)を新たに同じサブネットに設置した．Honeyd サーバ 2 の設置環境を図 4 に示す．従来，ハニーポット用サブネットで使用していた IP アドレス 251 個のうち 10 個を Honeyd サーバ 2 でエミュレートする IP アドレスとして割り当てた．

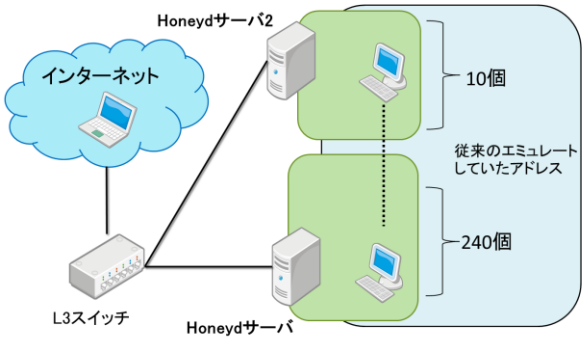

図 4　Honeyd サーバ 2 の設置環境

Honeyd サーバ 2 でエミュレートしている 10 個の IP アドレスに対する Telnet サービスへのアクセスの流れを以下に示す．Honeyd2 でエミュレートした Telnet サービスは，従来と同様に TCP/23 番ポートおよび TCP/2323 番ポートで接続を待ち受けている．下記に示した観測方法の中で，受信時刻，送信元 IP アドレス，試行したログイン ID とパスワードをログとして保存する．

1. Telnet サービスに対して TCP コネクションの確立要求(TCP SYN)を受信
2. 送信元に対して TCP SYN/ACK を応答し，相手からの TCP ACK を待機
3. 送信元からの TCP ACK を受信し，TCP スリーウェイハンドシェイクが成功し，Telnet サービスへの接続を確立
4. 従来の Honeyd サーバと同様のアクセスログを記録
5. 送信元に Telnet サービスへの ID の入力を促す
6. ID が入力されると，パスワードの入力を促す
7. パスワードが入力されると，認証失敗と応答
8. 再度，ID とパスワードの入力を促す．
9. ID とパスワードの試行を 3 回繰り返すと，通信切断

図 5 は Honeyd サーバ 2 にてエミュレートしている IP アドレス B に対して検証用クライアントから telnet で接続を試みたときの結果を示している．Honeyd2 サーバでは TCP コネクションの確立後ログイン ID の入力を待つ(図 5:7 行目)．ここではログイン ID として test として入力した．その後 Honeyd2 サーバはパスワードの入力を待つ(図 5:8 行目)．パスワードはエコーバックされないため表示されていないが test と入力している．パスワードの入力を受けた Honeyd サーバ 2 はログインを拒否し，新しい ID とパスワードの入力を受け付ける．これを後 2 回繰り返して，ログ

イン ID とパスワードの取得し, コネクションを切断した.

#	コマンドおよび結果
1	$ telnet B
2	Trying B ...
3	Connected to B.
4	Escape character is '^]'.
5	Red Hat Enverprise Linux Server release 5.4 (Tikanga)
6	Kernel 2.6.18-164.el5 on an x86_64
7	Username: test
8	Password:
9	% Access denied
10	
11	Username: test1
12	Password:
13	% Access denied
14	
15	Username: test2
16	Password:
17	% Access denied
18	Connection closed by foreign host.

図 5　Honeyd サーバ 2 へログイン試行(2)

4. 観測データの解析結果と考察

3.2 説で示した収集方法により集めたアクセスログ, およびパスワードログのうち，2018 年 2 月 22 日から 2018 年 6 月 1 日までの 99 日分のデータを分析した．データ分析に用いた期間中において，TCP/23 番ポートおよび TCP/2323 番ポート宛のコネクション確立数は 1,151,553 件，Telnet サービスに対するログイン試行回数は 326,594 件，Telnet サービスに対するログインを試行した送信元 IP アドレス数は 5,094 であった.

4.1 ログイン試行回数分析

1 日あたりの TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクション確立数を示したグラフを図 6 に示す．図 6 のグラフより TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクションの確立数は 2018 年 5 月 9 日をピークとして約 9 万件があり，その他の日は平均 1 万件程度であった.

1 日あたりのログイン試行回数を図 7 に示す．図 6 に示したように TCP/23 番ポートおよび TCP/2323 番ポート宛の TCP コネクション確立数は常時 1 万件程度にも関わらず，2018 年 3 月 26 日を境にログイン試行の回数が急激に減少した．この現象は利用している IP アドレスがハニーポットとばれてしまったことなど理由はいくつか考えられるが現在のところこの症状の原因は判明していない.

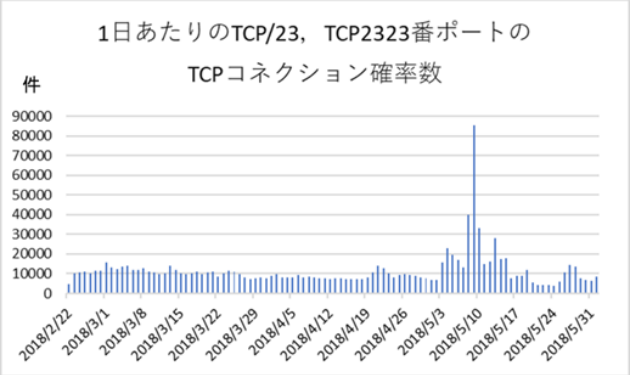

図 6　1 日あたりの TCP/23 番ポートおよび
TCP/2323 番ポート宛の TCP コネクションの確立数

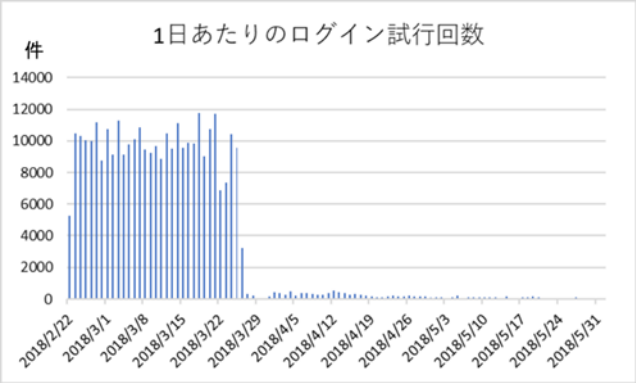

図 6　1 日あたりの Telnet サービスへのログイン試行回数

4.2 試行されたログイン ID とパスワードの分析

調査期間中に試行されたログイン ID とパスワードを送信元 IP アドレスごとに集計した．送信元 IP アドレスごとにログイン ID とパスワードの組を集計した結果から重複を排除した結果をパスワードリストと呼ぶ．集計結果よりパスワードリストは 965 種類であった．965 種類のパスワードリストのうち，上位 5 個のパスワードリストを使用した送信元 IP アドレス数を表 1 に示す．また 1 つの送信元 IP アドレスでのみ使用されたパスワードリストを 827 個存在した．Telnet サービスにログインを試行した送信元 IP アドレス数は 5,094 であるため，表 1 よりパスワードリスト A が 58.9%を占めていた.

一番多く観測したパスワードリスト A を表 2 に示す．表 2 中のログイン ID とパスワードのうち，Mirai で使用されるログイン ID とパスワードを網掛けして表している.

表 1　同一パスワードリストを用いた送信元数

パスワードリスト	送信元 IP アドレス数
A	3001
B	522
C	49
D	45
E	22

表 2 から今回多く観測されたパスワードリスト A は Mirai の持つパスワードリストをすべて含み，さらに Mirai の保持していないログイン ID とパスワードの組が存在していたことから Mirai の保持するパスワードリストを拡張した亜種が活発に活動していると推測される．

表 3 にログイン試行に用いられたログイン ID とパスワードの組のうち，上位 10 件を示す．最も多かったログイン ID とパスワードの組は文字化けしていたため 16 進数で表示している．表 3 から文字化けしていた最多の組以外はパスワードリスト A に含まれていた．多く試行されたパスワードは 1234 と数字が並んでいた．表 3 中の 2 番目と 6 番目の組はワイヤレスルータのデフォルトパスワード，4 番目の組は防犯カメラのデフォルトのパスワードであった．このように攻撃者側は製品のデフォルトのパスワードや，安易なパスワードを狙っていた．

表 3　試行回数上位の ID とパスワードの組

	試行回数	ID	パスワード
1	7549	(0x0603)	(0x0E09)
2	7121	root	aquario
3	7116	admin	1234
4	3608	root	xc3511
5	3597	admin	123456
6	3591	root	5up
7	3586	root	GM8182
8	3585	root	juantech
9	3584	support	support
10	3582	root	123123

5. まとめと今後の課題

5.1 まとめ

本研究では Honeyd を用いて, Telnet サービスのログイン機能をエミュレートし，Telnet サービスへのログイン試行に用いられるログイン ID とパスワードの組を 99 日分取得し分析した．その結果 2018 年 3 月 26 日以降にログイン試行数が急激に減少したこと，また Mirai の持つパスワードリストを拡張したパスワードリストを用いるマルウェアが活発に活動していること，安易なパスワードや製品のデフォルトのパスワードが狙われやすいことを確認した．

5.2 今後の課題

●ログイン試行の減少の原因の調査

2018 年 3 月 26 日以降, TCP/23 および TCP/2323 宛の TCP コネクション数は変化していないにも関わらず，Telnet サービスへのログイン試行が急激に減少していた．現時点でこの原因は特定できていない．しかし，IoT 機器への攻撃を調査するためには，ログイン試行される必要がある．Honeyd サーバ 2 宛のパケットを解析し, ログイン試行が減少している原因を調査する．

●ログイン試行した送信元からの他ポートに対する攻撃の調査

本研究ではハニーポットで取得したログイン ID とパスワードの組について分析した．この他にもハニーポットにて TCP/23，TCP/2323 以外のポートに対するアクセスや，送信元 OS や送信元ポート番号などを収集している．これらの情報と Telnet サービスへログイン試行した IP アドレスの情報を組み合わせて分析することにより，IoT 機器を狙ったマルウェアによる，Telnet サービス以外の攻撃についても調査することができると考えている．

●IoT 機器を狙ったより詳細な攻撃の把握

今回は IoT 機器の Telnet サービスを狙った攻撃のうち，マルウェアが次の感染先を探索する際の活動についての状況把握を目的として調査した．今後はマルウェアからのログイン試行に対して, ログインを成功させる機能を追加し，ログイン成功後のマルウェアの挙動についても観測することを検討している．

参考文献

[1] 警察庁, “インターネット観測結果等(平成 28 年 9 月期)”, https://www.npa.go.jp/cyberpolice/important/2016/19361.html (参照 2018-5-30)
[2] IT メディア編集部, “ITmedia IoT マルウェア「Mira」とは何か”, http://techfactory.itmedia.co.jp/tf/articles/1704/13/news010.html (参照 2018-5-30)
[3] “ITmedia NEWS IoT マルウェア「Mirai」の亜種が急拡大、日本でも感染か？”, http://www.itmedia.co.jp/news/articles/1711/28/news061.html (参照 2018-05-30).
[4] 池部実, 宮崎桐果, 吉田和幸, “ハニーポットによる大分大学におけるダークネット宛通信の分析”, 情報処理学会研究報告インターネットと運用技術研究会(IOT), Vol.2015-IOT-29, pp.1-8, 2018 年 1 月
[5] 上妻麻美, 橋本涼, 池部実, 吉田和幸, “ハニーポットを用いた TCP/23 番ポートへの通信の解析”, 第 69 回電気・情報関係学会九州支部連合大会, p.272, 2016 年 9 月
[6] “Honeyd”. http://www.Honeyd.org/ (参照 2018-5-30)
[7] “p0f”. http://lcamtuf.coredump.cx/p0f3/ (参照 2018-6-4)

表２　パスワードリストA

ログイン ID	パスワード	ログイン ID	パスワード	ログイン ID	パスワード
666666	666666	guest	guest	root	ikwb
888888	888888	mother	fucker	root	ivdev
Admin	5up	root	0	root	juantech
Administrator	admin	root	1001chin	root	jvbzd
admin	1111	root	1111	root	klv123
admin	1111111	root	123123	root	klv1234
admin	1234	root	1234	root	oelinux123
admin	12345	root	12345	root	oelinux1234
admin	123456	root	123456	root	pass
admin	1234567890	root	1234567890	root	password
admin	1988	root	1234qwer	root	qazxsw
admin	54321	root	54321	root	realtek
admin	7ujMko0admin	root	5up	root	root
admin	Win1doW$	root	666666	root	system
admin	admin	root	7ujMko0admin	root	ttnet
admin	admin1234	root	7ujMko0vizxv	root	user
admin	cat1029	root	888888	root	vizxv
admin	ipcam_rt5350	root	GM8182	root	xc3511
admin	meinsm	root	Win1doW$	root	xmhdipc
admin	pass	root	Zte521	root	zlxx.
admin	password	root	admin	root	zsun1188
admin	smcadmin	root	alpine	service	service
admin	vertex25ektks123	root	anko	supervisor	supervisor
admin	zhongxing	root	aquario	supervisor	zyad1234
admin1	password	root	default	support	support
administrator	1234	root	dreambox	tech	tech
default	antslq	root	founder88	ubnt	ubnt
guest	12345	root	hi3518	user	user
guest	friend	root	hunt5759		