ハニーポットを用いた TCP/23 番ポートへの通信の解析

上妻麻美* 橋本涼** 池部実* 吉田和幸***
（大分大学 *工学部知能情報システム工学科 **工学研究科工学専攻 ***学術情報拠点情報基盤センター）

1 はじめに

警察庁の報告によると，インターネットに接続されたディジタルビデオレコーダをはじめとした Linux 機器を標的とした攻撃が観測されている．とくに，TCP/23 番ポート(Telnet)に対するアクセスが増加している[1].攻撃者が侵入に成功した機器は，攻撃者からの命令にもとづいて動作するボットとして機能し,攻撃の踏み台として悪用される.本論文では，Linux 機器を対象とした攻撃の傾向を把握するため,ハニーポットにより TCP/23 宛の通信を収集し，送信元 IP アドレスや通信時刻，他ポートへの通信数などの観点より，TCP/23 番ポートに対する通信の挙動を調査する．

2 ハニーポットによる TCP/23 宛通信の収集

通常,未使用 IP アドレスに対してパケットが送信されることはないが,実際には多くのパケットが観測されている．これらのパケットは不正な活動に起因する.本調査では,未使用 IP アドレスの TCP/23 宛の通信を収集するため,低対話型ハニーポットの Honeyd[2]を用いた．Honeyd はオープンソースの低対話型ハニーポットであり,様々な OS やネットワークサービスを模倣できる．現在，大分大学で稼働している Honeyd では未使用 IP アドレスのうち,ネットワークアドレス長 24 ビットのサブネットを用いている．また，TCP/80，8080 にて Web サーバをエミュレートしている。それ以外のポート番号についてはパケットを受信した記録(アクセス)のみログに書き出している。そのため，現在の Honeyd の設定では TCP/23 宛の通信においては SYN パケットの受信のみ確認できる．

3 ハニーポットのアクセスログ調査

本調査では大分大学に設置している Honeyd で収集したアクセスログのうち， 2016 年 4 月 1 日から 4 月 30 日までの 30 日間のアクセスログデータを分析した．

3．1 アクセス数の調査結果

Honeyd において検知したすべてのコネクション数は 2,655,884 件であった.表 1 にコネクション数の上位 3 つのポート番号を示す．表 1 に示すように，TCP/23 宛のコネクションは全体の約 7 割を占めていた．TCP/80 宛のコネクションの約 32 倍である．TCP/23 宛のコネクションの 1 日当たりの平均コネクション数は約 64,694 件であるが,日によって差があった.最多は,4 月 9 日の 92,246 件,最小は 4 月 30 日の 44,298 件であり，約 5 万の差が確認できた．

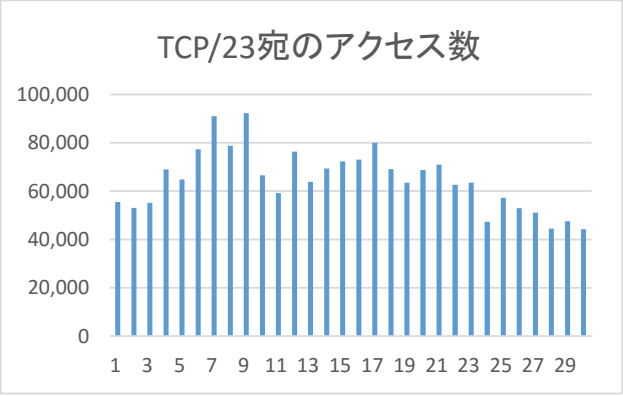

図 1．2016 年 4 月の TCP/23 番ポート宛のアクセス数

表 1．宛先ポート別コネクション数(上位 3 件)

宛先ポート	コネクション数	割合(%)
TCP/23	1,940,825	73.1
UDP/53413	83,188	3.1
TCP/80	59,097	2.2

表 2.他ポートにもアクセスしている IP アドレス(上位 3 件)

国	IP アドレス	コネクション数
オランダ	93.174.X	1,482
フィリピン	124.83.Y	702
中国	183.60.Z	628

表 3.送信元 OS の種類とその割合

OS	コネクション数	割合(%)
Linux	984,857	50.7
Windows	1,467	0.1
Solaris	93	0.0
不明	955,968	49.2

3．2 送信元 IP アドレスの調査結果

TCP/23 宛の通信の送信元 IP アドレスを調査した．TCP/23 のみにアクセスしている送信元のほかに，TCP/23 に加えて，UDP/53413 や TCP/6379 などのルータの脆弱性や NoSQL データベースの脆弱性を狙った送信元を確認した.TCP/23 宛の送信元 89,857 個のうち,上記に示したポートにも通信していた IP アドレスを 29 個確認した.そのうちの上位 3 件の IP アドレスを表 2 に示す．オランダのホスト 93.174.X は，1 日あたり 4 時間活動し，TCP/23，TCP/6379 それぞれに 2 時間ずつアクセスを繰り返していた．

3．3 送信元 OS の調査結果

Honeyd では送信元 OS を判別し，アクセスログに OS の種類を記録する.TCP/23 宛の通信において，送信元 OS を集計した結果,約 50%の送信元 OS が判明した(表 3).判別できた OS は 3 種類あり,大半が Linux であった．警察庁の報告のように，Linux 機器が乗っ取られ，ボットとして攻撃してきていると考えられる．

4 まとめと今後の課題

ハニーポットにて TCP/23 番ポートに対する通信を収集し，分析した.ハニーポットで観測した全体のコネクションにおいて，TCP/23 宛のコネクションは全体の 7 割を占めていた.また,TCP/23 宛のコネクションにおいて判別できる範囲では Linux からのコネクションが大多数を占めていた.今後は Honeyd において，TCP/23 宛のコネクションにおいて TCP スリーウェイハンドシェイクを確立する設定に変更し，分析を進める．さらに，telnet 通信を確立した場合の挙動を分析できるようにハニーポットにおけるエミュレートプログラムの開発を進める．

参考文献

[1] 警察庁,”IoT 機器を標的とした攻撃の観測について”, http://www.npa.go.jp/cyberpolice/topics/?seq=17323, 2015 年 12 月
[2] “Developments of the Honeyd Virtual Honeypot”, http://www.honeyd.org/