G-9

ハニーポットを用いた IoT デバイスに対するサイバー攻撃の分析

Analysis of Cyber attacks on IoT devices using Honeypot

○房安　良和[1]，小寺　建輝[2]，泉　隆[3]（日本大学）
*Yoshikazu Fusayasu[1], Tateki Kodera[2], Takashi Izumi[3](Nihon University)

The IoT (Internet of Things) is a concept that connecting various devices to the Internet. With the spread of IoT devices, it is predicted that the risk of cyber attacks on IoT devices will increase. In this paper, we study the configuration of honeypot observing cyber attacks on IoT devices and its observation result.

1. はじめに

近年，IoT 関連の市場規模が拡大している一方，多くの IoT デバイスがサイバー攻撃の被害に遭っている. 例えば，「Mirai」をはじめとする Linux を搭載した IoT デバイスの Telnet や SSH プロトコルを標的にしたマルウェアの出現，FTP を利用する NAS(Network Attached Storage)への不正アクセス被害等, IoT デバイスの脆弱性に起因するサイバー攻撃の存在が確認されつつあり[1]，IoT デバイスに対するサイバー攻撃は今後も増加・多様化していくと考えられる．この様なサイバー攻撃への対策を講じるためには, IoT デバイスに対する攻撃手法の分析を行う必要がある．以上を踏まえて本研究では，Telnet，SSH，FTP，FTPS のサービスを稼働している IoT デバイスに対するサイバー攻撃の分析を行う，サーバ型ハニーポットの構築を行う.

本稿では, 上述したハニーポットの構築を行い, 観測データを分析した結果について述べる.

2. ハニーポットの構築[2]

ハニーポットは，攻撃者に脆弱なシステムであると見せかけることでサイバー攻撃を観測し，観測データより攻撃者の侵入方法や侵入後の動作を分析するシステムの総称である. 攻撃対象に応じた種類が検討されており, 各攻撃に応じたデータ収集を行うことが可能である.

2.1 ハニーポットの構成

本研究で構築するハニーポット(Figure 1)は，通信パケットによるアクセス解析及びマルウェア捕獲用のマシン A とマルウェア解析用のマシン B に分けて構成する.

本ハニーポットでは, QEMU を用いて様々な CPU アーキテクチャ(マシン A: i386，マシン B: i386，ARM，MIPS，PPC)の Linux(Debian)デバイスを各マシン上でエミュレーションし，IoT デバイスと類似した環境を再現する．マシン A の構成を Table 1，マシン B の構成を Table 2 に示す.

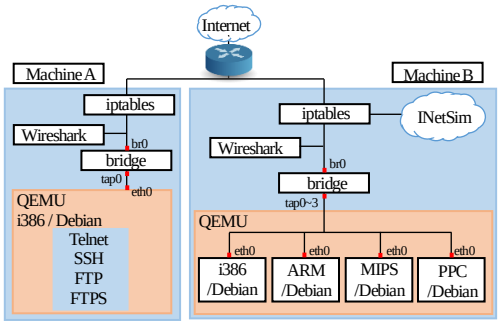

Figure 1. Diagram of honeypot

Table 1. Configuration of Machine A

Categories	Programs to use	Purpose
Access controller	iptables	To restrict a communication from inside to outside (To prevent the occurrence of DoS attack)
Network protocol analyzer	Wireshark	To collect communication packet(pcap file)
Server program	telnetd,sshd,vsftpd	To activate Telnet, SSH, FTP, FTPS server
Shell after login	rbash	To restrict malware removal and execution

Table 2. Configuration of Machine B

Categories	Programs to use	Purpose
Access controller	iptables	・To transfer communication generated from malware to INetSim ・To prohibit communication with the Internet
Internet service simulator	INetSim	To emulate the Internet
Network protocol analyzer	Wireshark	To collect communication packet(pcap file)

2.2 ハニーポットを用いた解析

2.1 節で示したハニーポットにより取得したデータを用いてマシン A で行う解析内容を Table 3，マシン B で行う解析内容を Table 4 に示す．なお，マシン A で捕獲したマルウェアはマシン B の当該 CPU アーキテクチャのデバイスへ送信する.

Table 3. Analysis contents on Machine A

Analysis tools	Analysis contents
login attempt log	User name used
file command	CPU architecture of malware
pcap file	Source IP address , Destination port , Password used , Source area , Number of access/day , Number of unique IP address access/day

Table 4. Analysis contents on Machine B

Analysis method	Analysis tools	Analysis contesnts
Surface analysis	PEframe	Information directly written in malware
	Virus Total	・Whether it is malware ・Malware family
Dynamic analysis	strace	System calls caused by execution of malware
	ltrace	Standard library caused by execution of malware
	pcap file	・C&C server's location ・Communication caused by execution of malware

1：日大理工・学部・情報 2：日大理工・院(前)・情報 3：日大理工・教員・情報

3. 観測結果

2017 年 9 月 1 日から 20 日間，マシン A の稼働を行った．なお，マシン B については未構築であるため稼働させていない．Figure 2 に送信元 IP アドレス数をもとに集計したハニーポットに対するアクセス数を示す．

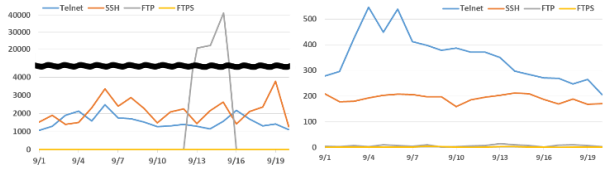

Figure 2. Number of accesses to honeypot (Left:Number of accesses/day, Right:Number of unique IP address accesses/day)

Figure 2(Left)より, Telnet や SSH に比べて, FTP や FTPS に対するアクセス数は極端に少ない結果となった．しかし，FTP に関しては，アクセス数が他サービスに比べ極端に多い日が存在した．例えば，9 月 14 日には，FTP に対して 19,279 件のアクセスが記録された．9 月 14 日の pcap ファイルを確認した結果，4 時間半に渡り平均 70 パケット/分で大量の SYN パケットが同一 IP アドレスから送信されていた．このことから，DoS 攻撃によるものであると推測される．

Figure 2(Right)より，SSH に比べ Telnet に対する 1 日当たりの IP アドレスのユニーク数が多い結果となっているが，Mirai 等のマルウェアに感染した IoT デバイスから，他の IoT デバイスへ感染拡大を狙う動きによるものであると推測される．また，Mirai の亜種等の出現[3]により，SSH に対する感染拡大の動きによって Telnet に次いで SSH に対してのアクセス数も増加していると考えられる．

ここで，Table 5 に Telnet へのアクセス数上位 5 ヵ国とログイン失敗時に使用されたユーザ名上位 2 種を，Table 6 に SSH へのアクセス数上位 5 ヵ国とログイン失敗時に使用されたユーザ名上位 5 種を示す．なお，FTP 並びに FTPS についてはアクセス数が少なく，十分なデータが取得できなかったため，ここでは省略する．

Table 5. Analysis result of Telnet access (Left: Top 5 countries of access to honeypot, Right: Top 2 types of User name used when login failed)

Country name	Number of access
India	1,305
Brazil	1,245
China	1,109
United States	598
Mexico	460

Username	Number of used
root	7,185
UNKNOWN	5,359

Table 6. Analysis result of SSH access (Left: Top 5 countries of access to honeypot, Right: Top 5 types of User name used when login failed)

Country name	Number of access
Vietnam	892
China	887
United States	402
Netherland	380
France	163

Username	Number of used
root	33,542
Admin	3,120
user	1552
pi	574
test	572

Table 5，6(Left)より，Telnet と SSH におけるアクセス元の国には，一部上位の国に違いが見られた．これは，それぞれの国で流通しているデバイスで使用されているプロトコルの違いによるものであると推測する．一方，アメリカや中国は，Telnet と SSH 共にアクセス数で上位となった．経済規模の大きいアメリカや中国では，多くの IoT デバイスが流通しており，Mirai 等に感染している IoT デバイスも多いことが原因であると考えられる．

Table 5(Right)より，Telnet のログイン試行で用いられたユーザ名は root と UNKNOWN の 2 種のみであった．これは，root 以外のユーザ名を用いた場合，Telnet へのログイン履歴には UNKNOWN と残ってしまったためである．この様に表示された原因は不明であるが Telnet へのログイン施行で用いられるユーザ名の傾向分析を行うために，原因の特定と対策を行っていく必要がある．Table 6(Right)より，SSH では Raspberry Pi で使用されるユーザ名 pi や Table 6 に示した以外にも ubnt(UBIQUITI 社のルータ等), cisco(cisco 製のルータ等)等がユーザ名として使用されていた．これは，SSH を稼働している IoT デバイスを標的としたログイン試行であることが考えられる．

また，マシン A でダウンロードされたマルウェアは 6 種類，計 10 個であった．これらのマルウェアに，1 章で述べた Mirai は含まれていなかったが, バックドアの作成や DDoS 攻撃を行うもの，実行中のマルウェアを偽装・隠蔽する目的のものが確認できた．しかし, マルウェアのダウンロードに使用されたプロトコルの判断が出来なかったため，今後はディレクトリをプロトコル毎に別けることで上述の問題を改善する．さらに, 攻撃者の侵入後，マルウェアのダウンロードを行う前に通信を終了されているログが目立ち，十分な数のマルウェアを捕獲することが出来なかった．これは, 攻撃者にハニーポットとして検知されていることが原因であると考えられ，今後はそれに対する改善方法について検討する必要がある．

4. まとめ

本稿では，アクセス解析及びマルウェア捕獲用ハニーポットの構築を行い，観測データの分析を行った．

今後はマルウェア解析用ハニーポットを構築し，マルウェア捕獲用ハニーポットと併せて運用することで IoT デバイスに対するサイバー攻撃の分析を進めていく．

5. 参考文献

[1]trendmicro:「家庭用ルータや IoT 機器を「ゾンビ化」する攻撃，その影響を解説」, http://blog.trendmicro.co.jp/archives/14185,2017-09

[2]八木毅,青木一史,秋山満昭,幾世知範,高田雄太,千葉大紀:「実践サイバーセキュリティモニタリング」,コロナ社,2016-04-18

[3] trendmicro:「Mirai 亜種出現で挙動が変化|JPCERT/CC 2016 年 10 月-12 月観測レポート」, https://www.trendmicro.com/jp/iot-security/news/20072,2017-09