G-25

IoT デバイスに対するマルウェア解析システムの検討

A Study on analysis system of malware for IoT devices

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

The IoT (Internet of Things) is a concept that connecting various devices to the Internet. With the spread of IoT devices, various cyber attacks have been confilmed. In this paper, we examine the configuration of the system that analyzes the malware sent to the IoT devices and its analysis result.

1. まえがき

近年, IoT の普及によって様々なデバイスがインターネットに接続されるようになった．これに伴い，2016 年に「Mirai」と呼ばれる，IoT デバイスに感染し DDoS 攻撃等を実行させるマルウェアが出現し，多くの IoT デバイスへと感染被害が拡がった[1]．また，2018 年 4 月には「BrickerBot」と呼ばれる，ストレージを破壊することで IoT デバイスを使用不可能な状態にするマルウェアの存在が確認された[2]．Mirai をはじめとする，これまでの DoS 攻撃等を行うことを目的とするマルウェアとは違い，ストレージの破壊が行われるため，再起動等による復旧が不可能となる．このため，マルウェアの実行そのものを阻止する必要があるが，IoT デバイスに対するセキュリティ対策は現状，十分に行われていない．そこで先行研究[3]では,セキュリティ対策を講じるために，まず IoT デバイスに対するサイバー攻撃を分析する必要があると考え，不正アクセスやマルウェアを収集するハニーポットを構築した.本研究では，そのハニーポットで収集したマルウェアを解析するシステムの検討・構築を目的とする．

本稿では，上述したマルウェア解析用システムの構築を行い，マルウェアを解析した結果について示す．

2. ハニーポットとマルウェア解析システムの構成

先行研究で構築したハニーポット(Machine A)と本研究で構築するマルウェア解析システム(Machine B)の構成について Figure 1 に示す．

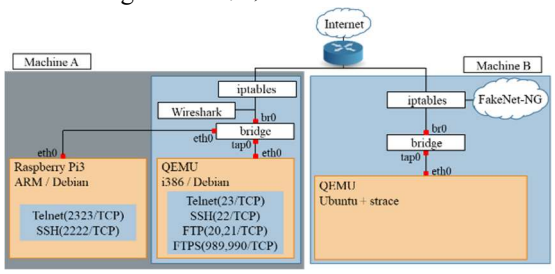

Figure 1. Diagram of Honeypot and analysis system

マルウェア解析システム(Machine B)では，QEMU を用いて IoT デバイスを模した Linux (Ubuntu)デバイスをエミュレートし，ハニーポット(Machine A)で捕獲したマルウェアの解析を行う．なお，エミュレートするデバイスの CPU アーキテクチャについては，解析対象のマルウェアに合わせたものを選択する．マルウェア解析システム(Machine B)を構築するために使用するプログラムを Table 1 に示す．

Table 1. Configuration of Machine B

Categories	Programs to use	Purpose
Access controller	iptables	・To transfer communication generated from malware to Fakenet-NG ・To prohibit communication with the Internet
Internet service simulator	FakeNet-NG	・To emulate the Internet ・To collect communication packet(pcap file)

3. マルウェア解析用システムによる解析

マルウェア解析用システム(Machine B)で使用する解析ソフトウェアとそのソフトウェアを用いて解析する内容について，表層解析と動的解析に分け，Table 2 に示す．なお，マルウェアの実行で発生する各種サーバとの通信に対応するため，FakeNet-NG を用いたインターネットのエミュレートを行った．

なお，Machine B でマルウェアを解析した結果は，マルウェア情報として利用できるようにデータベース化してまとめる．

Table 2. Analysis contents on Machine B

Analysis method	Analysis tools	Analysis contesnts
Surface analysis	PEframe	Information directly written in malware
Dynamic analysis	strace	System calls caused by execution of malware
	pcap file	・C&C server's location ・Communication caused by execution of malware

4. マルウェアの実行結果

本稿では，マルウェア「Linux.Xorddos」(MD5: 24a386648c204b3fff7c2a0007be1a16)の解析を行った．なお，このマルウェアはファイルの作成や，ネットワークを用いた C&C サーバとの通信等の機能を有してい

1：日大理工・院(前)・情報　2：日大理工・教員・情報

る. このマルウェアに対し, 表層解析として PEframe を実行した結果を Figure 2 に示す.

Figure 2. Surface analysis result in PEframe

Figure2 より，マルウェアの実行対象とする CPU アーキテクチャが i386(Intel 80386)であること，ファイル名，サイズ，ハッシュ値，マルウェア内に記述されているファイル名等について確認することができた．ただし，Figure2 のみではマルウェアがどのような動作を行うものであるか判断することが困難であるため，動的解析等の他手法と組み合わせることが必要である．

4.2 動的解析の実行結果

QEMU 上の仮想マシンでマルウェアに対して strace を用いて動的解析を行ったところプロセス ID 別に 14 個のログファイルが生成された. strace で生成された全ログファイルのうち，ファイルの作成に関するログの一部を Figure 3 に，デバイス情報を取得していたログの一部を Figure 4 に示す．さらに，Fakenet-NG のログから，マルウェアの実行によって発生した通信について Figure 5 に示す.

```
open("/etc/init.d/.777", 1535528111", O_WRONLY|O_CREAT, 0777)
symlink("/etc/init.d/.777", 1535528111", "/etc/rc1.d/S90.777", 1535528111")
symlink("/etc/init.d/.777", 1535528111", "/etc/rc2.d/S90.777", 1535528111")
symlink("/etc/init.d/.777", 1535528111", "/etc/rc3.d/S90.777", 1535528111")
symlink("/etc/init.d/.777", 1535528111", "/etc/rc4.d/S90.777", 1535528111")
symlink("/etc/init.d/.777", 1535528111", "/etc/rc5.d/S90.777", 1535528111")
```

Figure 3. Dynamic analysis result in strace

(Register for auto start)

```
uname({sys="Linux", node="rootuser", ...})
open("/sys/devices/system/cpu/online", O_RDONLY|O_CLOEXEC)
open("/proc/meminfo", O_RDONLY) = 1
send(1, "¥1¥0¥0¥0Linux3.2.0-126-generic-pae-c"..., 228, 0)
```

Figure 4. Dynamic analysis result in strace

(Send device information)

```
[ Diverter] Received nonlocal IPv4 datagram destined for 8.8.8.8
[ DNS Server] Received A request for domain '
[ DNS Server] Responding with '192.0.2.123'
[ Diverter] Received nonlocal IPv4 datagram destined for 192.0.2.123
[ IRCServer] Client connected
[ IRCServer] Client issued an unknown command linux3.2.0-126-generic-pae-ccs4*2711MHZ100OMB(null)
```

Figure 5. Dynamic analysis result in Fakenet-NG

(Send and receive information on emulation server)

Figure 3 では，open によって自動起動を設定するためのディレクトリ「/etc/init.d」にファイル名「.777」を作成し，symlink によって起動時の動作モードへの設定を行っている．これにより，次回以降の起動時にもマルウェアが実行されることになる．

Figure 4 では，uname によってデバイスの OS 名等の情報を, open によって,「/sys/devices/system/cpu/online」から稼働中の CPU 数を，「/proc/meminfo」からメモリ情報についての取得を行っている．また，send によって，マルウェアに感染したデバイスの制御を行う C&C サーバへデバイス情報を送信していることが確認できる．

Figure 5 から DNS サーバへ C&C サーバの IP アドレスを問い合わせしていることが確認できる．また，IRC プロトコルを用いた C&C サーバとの接続確立と Figure 4 で送信されていた感染デバイス情報が受信されていることがわかる．

このように，マルウェア実行・感染後に次回起動時以降での自動起動を行う設定や，C&C サーバにデバイス情報の送信を行っていたことが確認できた．しかし，C&C サーバ側から感染デバイスへコマンドの送付等を行う場合については，使用するコマンドが不明であることから解析できていないため，今後はシンボリック実行等を併用し動的解析では実行されなかったマルウェアの機能について解析する必要がある．

5. まとめ

本稿では，マルウェア解析用ハニーポットの構成についての検討及びマルウェアの解析を行い，C&C サーバからのコマンド送付の通信を伴わない場合の挙動について確認することができた．

今後は，マルウェア解析用のハニーポット上で C&C サーバからのコマンド送付を伴うマルウェアや解析妨害機能を含むマルウェアの解析を行うため，シンボリック実行等の手法の導入について検討を行う．

6. 参考文献

[1]WIRED:「The Reaper IoT Botnet Has Already Infected a Million」,
https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/,2018-09
[2]radware:「Bricker PDoS Attack: Back With A Vengence」,
https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/, 2018-09
[3]房安良和・小寺建輝・泉隆:「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」,
平成 30 年電気学会全国大会,3-089,2018-03