1E-01

IoT 機器への不正な Telnet 接続ログのコマンドに着目した分析

山内 利宏[†‡]　吉元 亮太[†]　吉岡 克成[¶]
岡山大学大学院自然科学研究科[†]　国立研究開発法人科学技術振興機構，さきがけ[‡]
横浜国立大学先端科学高等研究院/大学院環境情報研究院[¶]

１．はじめに

Mirai[1]に代表される IoT 機器を対象としたマルウェアが活動しており，IoT 機器が脅威にさらされている．IoT 機器を対象としたマルウェアは，IoT 機器に不正に侵入し，ボットなどのマルウェアを IoT 機器にダウンロードさせ，感染する．

本稿では，IoT 機器のハニーポットで収集された Telnet ログを分析し，マルウェアによって入力されたコマンドについて解析した結果を報告する．

２．IoT 機器を対象とするマルウェア

IoT 機器を狙った代表的なマルウェアとして，Mirai がある．Mirai は，推測が容易なパスワードを使用する IoT 機器などを対象に，Telnet などを利用して侵入する．Mirai などのマルウェアは，Telnet などで IoT 機器へのログインに成功すると，目的を達成するためにマルウェアなどをダウンロードし，実行する．これにより，IoT 機器をボット化するなどの活動を行う．ボット化した IoT 機器は，感染の拡大化のために，他の IoT 機器に同様の手法で侵入を試みることがある．また，攻撃者は，このようにして作成したボットネットを用いて，DDoS 攻撃を行うことがある．

このため，IoT 機器をよりセキュアにするためには，マルウェアの振る舞いを分析し，対策することが重要である．そこで，本稿では，IoT 機器に Telnet でログインされた際のコマンドの実行ログを取得し，分析した結果を報告する．

３．Telnet ログの分析

3.1　Telnet ログの概要

本研究では，IoT 機器のハニーポットを用いて収集した Telnet ログを評価に用いる．このハニーポットは，Telnet のポートを開放した状態で運用され，外部から接続された際の Telnet コマンドを記録している．分析した Telnet ログは，2017 年 9 月 1 日～7 日の間に収集されたものである．7 日間で収集された約 380 万件のログを分析した．

3.2　実行されたコマンドの解析

実行されることが多いコマンドを解析するため，ログの中でも，コマンドの出現数を調査した．出現数の多いコマンドのうち，上位 20 件を**表 1** に示す．

表 1　出現数の多いコマンド（上位 20 件）

コマンドライン	出現数
/bin/busybox BAT	473,792
sh	173,762
shell	172,186
/bin/busybox ECCHI	169,204
system	111,822
enable	68,004
/bin/busybox kill -9 2232	44,150
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /	42,179
bin/busybox rm /dev/.nippon	38,848
/bin/busybox cat /dev/.nippon	38,840
/bin/busybox echo -e '\\x6b\\x61\\x6d\\x69/dev' > /dev/.nippon	38,303
sh ftp1.sh	36,575
chmod 777 tftp1.sh	34,445
sh tftp1.sh	34,445
sh tftp2.sh	34,445
chmod 777 tftp2.sh	34,411
rm -rf *	33,032
chmod 777 cunty.sh	32,059
sh cunty.sh	32,059
/bin/busybox wget	30,403

表 1 から次のことが分かる．

（１）　busybox によるコマンドの呼び出し

Analysis focusing on commands of telnet logs on IoT devices
Toshihiro Yamauchi†‡, Ryota Yoshimoto†, Katsunari Yoshioka ¶
† Graduate School of Natural Science and Technology, Okayama University
‡ JST, PRESTO
¶ Graduate School of Environment and Information Sciences, Yokohama National University/Institute of Advanced Sciences, Yokohama National University

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.

が多い.
（2） シェルを実行するためのコマンドが多い.
（3） 内部コマンド enable の実行が多い.
（4） ファイルのダウンロード，パーミッション変更，及び削除のコマンドが多い.
（5） シェルスクリプトの実行が多い.

これらのことから，ログイン後，何らかのファイルをダウンロードし，実行して，ファイルを削除していることが推察される.

3.3 実行されたプログラム名の解析

コマンドラインから引数を除き，プログラム名のみでの出現回数の調査も行った．ただし，プログラム名に“busybox”を含むものについては，第 1 引数のコマンド名を含めて出現回数を調査した．出現数の多いプログラム名のうち，上位 15 個を**表 2** に示す.

表 2 出現数の多いコマンド名（上位 15 件）

コマンド名	出現数
/bin/busybox BAT	473,792
echo	399,583
sh	327,915
/bin/busybox cat	311,704
/bin/busybox rm	308,515
/bin/busybox echo	288,706
shell	172,186
/bin/busybox ECCHI	169,204
rm	164,416
chmod	124,659
system	111,822
tftp	80,916
enable	68,004
/bin/busybox kill	66,760
/bin/busybox chmod	61,423

表 2 からも，表 1 と同様に，busybox の利用，ファイルのパーミッション変更や削除，及びシェルの実行に関するコマンドが多いことが分かる.

この調査結果から，busybox を除く Linux のシステム上に存在し，ファイル名をコマンドとして呼び出している上位 6 件を**表 3** に示す.

表 3 から，シェルや，ファイルのパーミッション変更や削除，及びファイル転送のコマンドが多いことが分かる.

表 3 Linux に存在するコマンドの出現数

コマンド	出現数
sh	327,915
rm	164,416
chmod	124,659
tftp	80,916
wget	42,745
ftpget	38,314

3.4 コマンドの実行の順番の解析

コマンドの実行の順序を解析するため，コマンド名を連結し，その出現数の多いものを調査した．調査結果を分析したところ，コマンドの実行の順序として，次の 4 つで始まるものが多かった.

- enable⇒system⇒shell⇒sh
- enable⇒shell⇒sh
- system⇒shell⇒sh
- shell⇒sh

enable は、特権モードのコマンドへのアクセスを許可するためのコマンドであり，system はシステム管理オプションのメニューへ移動するためのコマンドである．shell と sh は Bourne シェルを実行するコマンドである．Linux のシェルへのアクセスを得るために，これらの一連のコマンドを実行していることが分かる[2].

4．おわりに

IoT ハニーポットの telnet ログを分析することにより，マルウェアにより利用されるコマンドやそのコマンドの実行順序などを分析した結果を示した.

今後は，マルウェアに IoT 機器に不正にログインされた場合でも，IoT 機器の悪用を防ぐようなセキュリティ機構の検討を行う.

謝辞：本研究の一部は，JST，さきがけ，JPMJPR1938，および JSPS 科研費 JP19H04111 の助成を受けたものです.

参考文献

[1] Antonakakis, M. et al.：Understanding the mirai botnet：*Proc. 26th USENIX Conference on Security Symposium*, pp.1093-1110 (2017).
[2] Sam Edwards, Ioannis Profetis, Hajime: Analysis of a decentralized internet worm for IoT devices. Tech. Rep. 1, Rapidity Networks. Oct. 2016. URL https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf.

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.