Analysis of Commands of Telnet Logs Illegally Connected to IoT Devices

Toshihiro Yamauchi, Ryota Yoshimoto, Takahiro Baba (Okayama University),
Katsunari Yoshioka (Yokohama National University)

1. Introduction

- *MIRAI* is an active malware that targets and poses constant threats to IoT devices.
- The purpose of this study is to propose security functions at the operating system level to prevent the infectious activities of IoT malware and their malicious behavior.
- We analyzed the behavior of IoT malware after it entered an IoT device via Telnet.

2. Analysis of Telnet Logs

Approximately 3.8 million Telnet logs from September 1 to 7, 2017 were analyzed.

TABLE I COMMANDS WITH THE HIGHEST NUMBER OF OCCURRENCES (TOP 30) (Excerpt)

Command line	Appearances
/bin/busybox BAT	473,792
sh	173,762
shell	172,186
/bin/busybox ECCHI	169,204
system	111,822
enable	68,004
bin/busybox rm /dev/.nippon	38,848
sh ftp1.sh	36,575
chmod 777 tftp1.sh	34,445
/bin/busybox wget	30,403

(1) Several commands were executed by busybox.
(2) There were many commands to execute the shell.
(3) The internal command "enable" was executed several times.
(4) There were many commands that download, change permissions, or delete files.
(5) Shell scripts were executed many times.

Order of Executing Commands

Commands were often executed in the following order.

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

- "enable" is a command to allow access to privileged-mode commands.
- "system" is a command to navigate to a menu of system-management options.
- "shell" and "sh" are commands that execute Bourne shell.

When these commands are executed in the above order, a Linux shell can be accessed.

TABLE II NAMES OF COMMANDS WITH THE HIGHEST NUMBER OF OCCURRENCES (TOP 30). (Excerpt)

Command name	Appearances
/bin/busybox BAT	473,792
sh	327,915
/bin/busybox rm	308,515
shell	172,186
/bin/busybox ECCHI	169,204
rm	164,416
chmod	124,659
tftp	80,916

- Only names of commands excepting arguments from the command line were investigated.
- The number of appearances that include "busybox" in the first argument and the second argument were investigated.
- From Table 1 and Table 2, we can see that there are many commands related to using busybox, changing or deleting file permissions, and executing shells.

TABLE III THE NUMBERS OF APPEARANCES OF COMMANDS EXIST IN Linux. (Excerpt)

Command	Appearances
sh	327,915
rm	164,416
chmod	124,659
tftp	80,916
wget	42,745
ftpget	38,314
cat	12,679
/bin/echo	5,805
/usr/bin/printf	5,805
ping	400

- From Table 3, we can see that there are many commands for executing shells, changing or deleting file permissions, and transferring files.

3. Conclusions

- After IoT malware intrudes IoT devices, it often operates files, downloads malware, and executes it.
- Thus, to prevent malicious activities in IoT devices, we should focus on preventing such malicious commends' execution