JPCERT Coordination Center official Blog

blogs.jpcert.or.jp/en/2020/11/elf-plead.html

朝長 秀誠 (Shusei Tomonaga)

November 16, 2020

ELF_PLEAD - Linux Malware Used by BlackTech

BlackTech

-
- Email

In a past article, we introduced Linux malware ELF_TSCookie, which is used by an attack group BlackTech. This group also uses other kinds of malware that affects Linux OS. PLEAD module for Windows which we introduced before has its Linux version (ELF_PLEAD) as well. This article describe the details of ELF_PLEAD in comparison to PLEAD module.

Comparison between PLEAD Module and ELF_PLEAD

ELF_PLEAD and PLEAD module share many parts of the code, and most of the functions including communication are similar. Figure 1 shows the comparison of the main functions of PLEAD module and ELF_PLEAD.

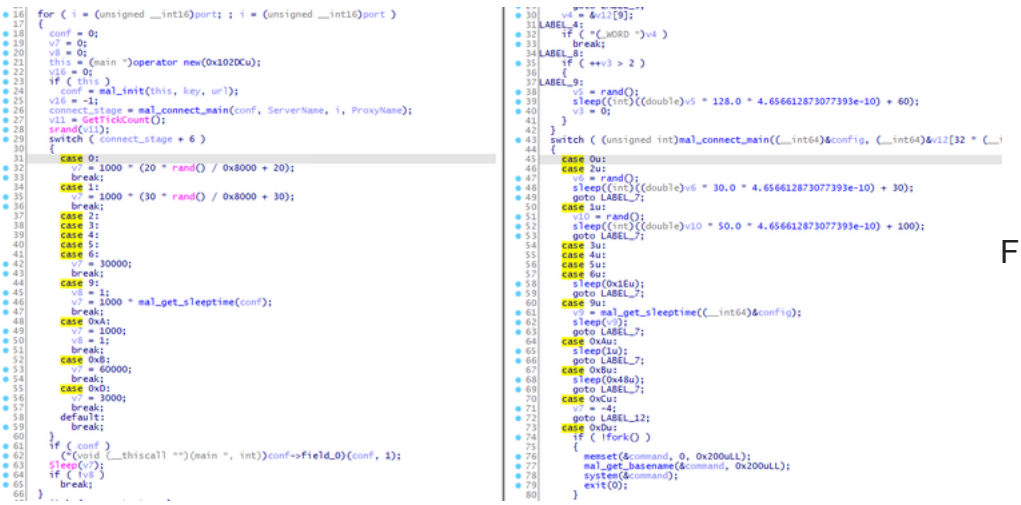


Figure 1: Code comparison of PLEAD module and ELF_PLEAD
(Left: PLEAD module / Right: ELF_PLEAD)

It is clear from the flow of processing that the two types of malware are quite similar. The next sections will describe the features of ELF_PLEAD from the following perspectives:

- Configuration
- Communication protocol
- Commands

Configuration

ELF_PLEAD possesses its configuration with the size of 0x1AA. Figure 2 is an example of configuration. It contains information such as C&C servers and an encryption key. (Please see Appendix A for the details of configuration.)

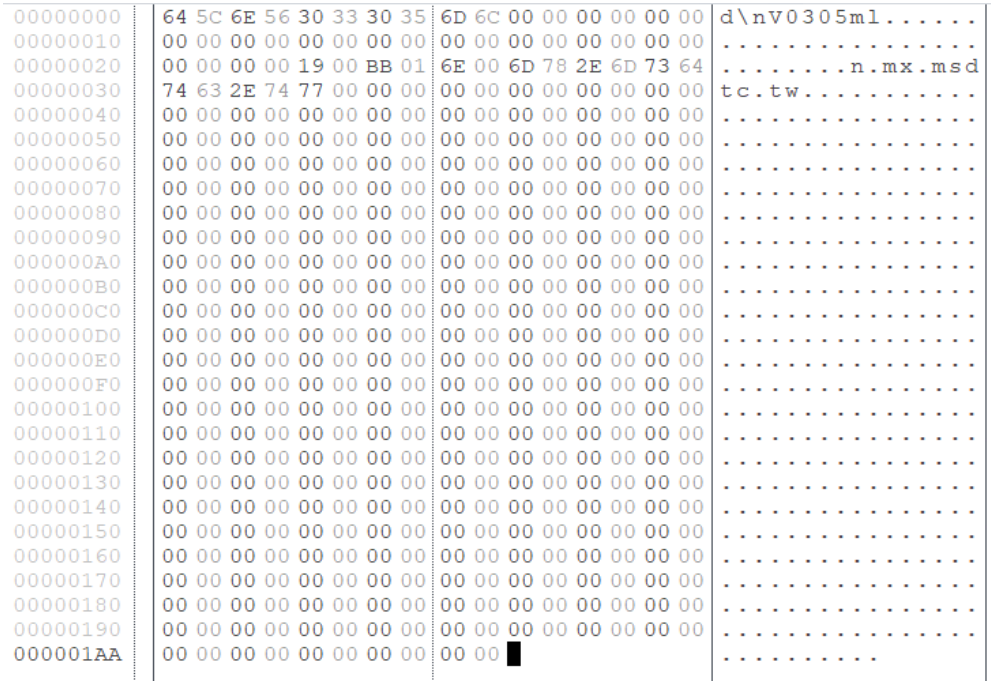


Figure 2: Configuration example

The configuration is RC4-encrypted, and the 32-byte string right before the encrypted configuration is the encryption key itself. Figure 3 is an example of encrypted configuration and its key.

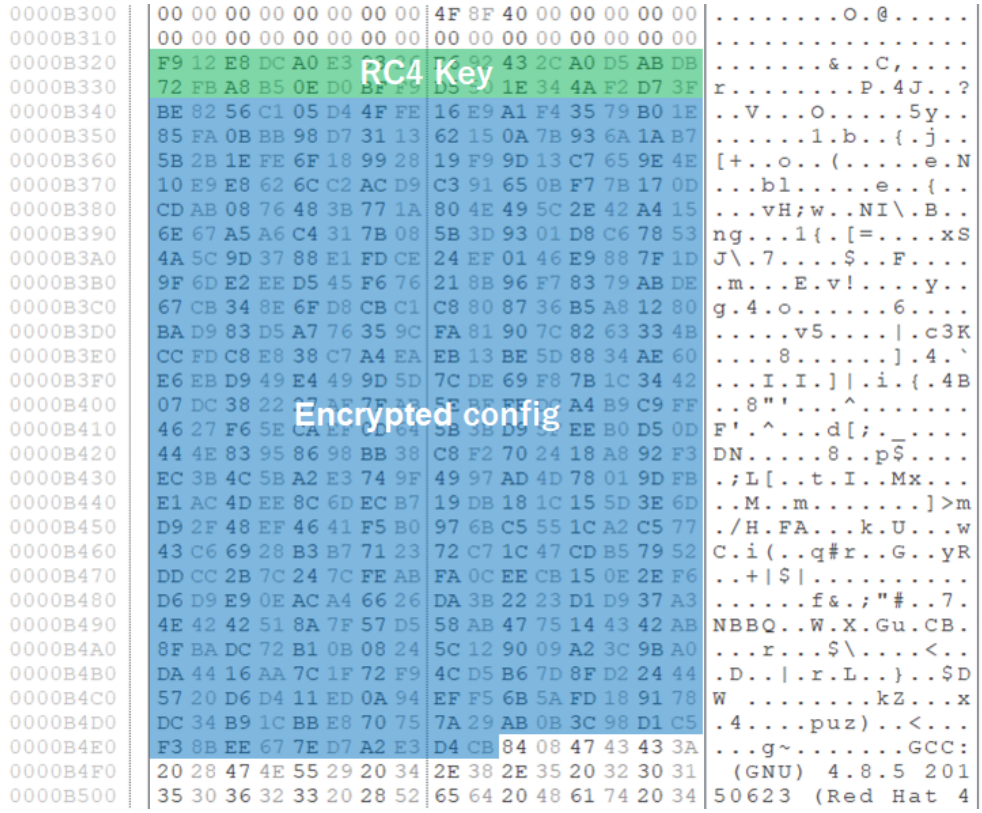


Figure 3: Encrypted configuration and encryption key

Communication protocol

While PLEAD module uses HTTP protocol to communicate with its C&C servers, ELF_PLEAD uses its custom protocol. Besides the difference, the data format and the method for exchanging the encryption key are almost the same. Figure 4 describes the flow of communication that ELF_PLEAD performs.

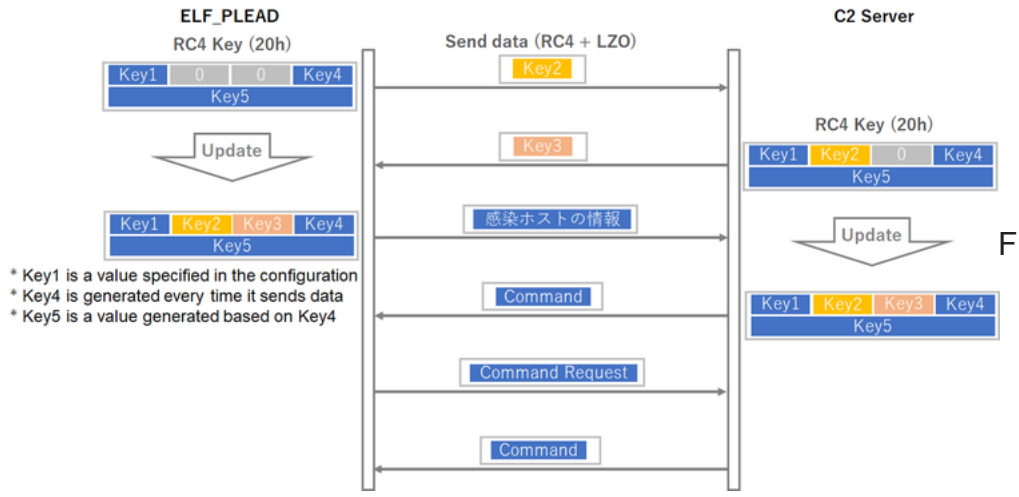


Figure 4: Communication flow of ELF_PLEAD

ELF_PLEAD exchanges a part of RC4 key at the time of first communication. After that, a RC4 key generated by the exchange will be used for the communication that follows. The data sent is RC4-encrypted and then LZO-compressed. (Please see Appendix B for the details of communication protocol.)

Commands

ELF_PLEAD is equipped with 5 command groups as follows. (Please see Appendix C for the details of command functions. The command number may vary in some samples.)

- CFileManager (group number 0): commands for operation on files
- CFileTransfer (group number 1): commands for sending/receiving files
- CRemoteShell (group number 2): commands for remote shell
- CPortForwardManager (group number 3): commands for proxy mode
- No name (group number 0xFF): commands for malware control

```
00008BA0  A8 2D 40 00 00 00 00 00  60 2E 40 00 00 00 00 00  .-@.....`.@.....
00008BB0  31 32 43 46 69 6C 65 4D  61 6E 61 67 65 72 00 00  12CFileManager..
00008BC0  10 B5 60 00 00 00 00 00  B0 8B 40 00 00 00 00 00  ..`.......@.....
00008BD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00008BE0  00 00 00 00 00 00 00 00  C0 8B 40 00 00 00 00 00  ..........@.....
00008BF0  C0 21 40 00 00 00 00 00  D0 21 40 00 00 00 00 00  .!@......!@.....
00008C00  61 62 00 00 00 00 00 00  28 3C 40 00 00 00 00 00  ab......(<@.....
00008C10  68 3C 40 00 00 00 00 00  68 3C 40 00 00 00 00 00  h<@.....h<@.....
00008C20  38 3C 40 00 00 00 00 00  68 3C 40 00 00 00 00 00  8<@.....h<@.....
00008C30  68 3C 40 00 00 00 00 00  48 3C 40 00 00 00 00 00  h<@.....H<@.....
00008C40  58 3C 40 00 00 00 00 00  68 3C 40 00 00 00 00 00  X<@.....h<@.....
00008C50  68 3C 40 00 00 00 00 00  68 3C 40 00 00 00 00 00  h<@.....h<@.....
00008C60  18 3C 40 00 00 00 00 00  00 00 00 00 00 00 00 00  .<@.............
00008C70  31 33 43 46 69 6C 65 54  72 61 6E 73 66 65 72 00  13CFileTransfer.
00008C80  10 B5 60 00 00 00 00 00  70 8C 40 00 00 00 00 00  ..`.....p.@.....
00008C90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00008CA0  00 00 00 00 00 00 00 00  80 8C 40 00 00 00 00 00  ..........@.....
00008CB0  A0 2E 40 00 00 00 00 00  B0 2E 40 00 00 00 00 00  ..@.......@.....
00008CC0  64 65 71 75 65 3A 3A 5F  4D 5F 72 61 6E 67 65 5F  deque::_M_range_
00008CD0  63 68 65 63 6B 00 31 32  43 50 6F 72 74 46 6F 72  check.12CPortFor
00008CE0  77 61 72 64 00 00 00 00  00 00 00 00 00 00 00 00  ward............
00008CF0  10 B5 60 00 00 00 00 00  D6 8C 40 00 00 00 00 00  ..`.......@.....
00008D00  31 39 43 50 6F 72 74 46  6F 72 77 61 72 64 4D 61  19CPortForwardMa
00008D10  6E 61 67 65 72 00 00 00  00 00 00 00 00 00 00 00  nager...........
00008D20  10 B5 60 00 00 00 00 00  00 8D 40 00 00 00 00 00  ..`.......@.....
00008D30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00008D40  00 00 00 00 00 00 00 00  F0 8C 40 00 00 00 00 00  ..........@.....
00008D50  00 4A 40 00 00 00 00 00  60 4B 40 00 00 00 00 00  .J@.....`K@.....
00008D60  00 00 00 00 00 00 00 00  20 8D 40 00 00 00 00 00  ........ .@.....
00008D70  70 4D 40 00 00 00 00 00  B0 4D 40 00 00 00 00 00  pM@......M@.....
```

Figure 5: Command group names

It is clear that the functions are almost the same as PLEAD module.

In closing

It has been confirmed that BlackTech uses different kinds of malware including TSCookie, PLEAD and KIVARS, which target Linux OS as well as Windows OS. If such malware is found in your Windows environment, it is recommended to check your Linux environment as well.

Shusei Tomonaga
(Translated by Yukako Uchida)

Appendix A: ELF_PLEAD Configuration

Table A: Configuration

Offset	Description	Remarks
0x000	RC4 Key	Used for encrypting communication
0x004	ID	
0x024	Port number 1	
0x026	Port number 2	
0x028	Port number 3	
0x02A	C&C server 1	
0x0AA	C&C server 2	
0x12A	C&C server 3	

Configuration format may vary in some samples.

Appendix B: Contents of data exchanged

Table B-1: Format of sent data

Offset	Length	Contents
0x00	4	RC4 Key (Key4)
0x04	4	Hash value
0x08	4	RC4 key (Key1)
0x0C	2	Length of data sent
0x0E	2	Length of data at offset 0x10 before compression
0x10	-	Encrypted data (RC4 +LZO) (See Table A-2 for details.)

Table B-2: Format of encrypted data

Offset	Length	Contents
0x00	2	0xFF
0x02	4	RC4 key (Key2)
0x06	-	Random data (at least 128 bytes)

Table B-3: Format of received data

Offset	Length	Contents
0x00	4	RC4 key (Key4)
0x04	4	Hash value
0x08	4	RC4 key (Key1)
0x0C	2	Length of data sent
0x0E	2	Length of data at offset 0x10 before compression
0x10	-	Encrypted data (RC4 +LZO) (See Table A-4 for details.)

Table B-4: Format of encrypted data in the received data

Offset	Length	Contents
0x00	2	0x01FF
0x02	4	RC4 key (Key3)

Appendix C: ELF_PLEAD commands

Table C-1: Commands without group name (group number 0xFF)

Value	Contents
4	Send random data
5	Reconnect
6	Restart
7	End
8	End
9	Change socket
11	Change C2 server

Table C-2: Commands for CFileManager (group number 0)

Value	Contents
32	Send list of files
37	Send file size, mode, timestamp

39	Change file name
41	Delete file/directory
43	Upload file
45	Execute file
49	Create directory
51	Move file
53	Delete directory

Table C-3: Commands for CFileTransfer (group number 1)

Value	Contents
64	Send file/directory information
67	Create directory
70	Download file
71	Send file information
75	Upload file

Table C-4: Commands for CRemoteShell (group number 2)

Value	Contents
80	Launch remote shell

Table C-5: Commands for CPortForwardManager (group number 3)

Value	Contents
96	Set up proxy
100	Connect proxy
102	Send proxy data
104	-
106	-
108	End proxy

Appendix D: C&C server

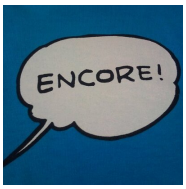
mx.msdtc.tw

Appendix E: Malware hash value

- 5b5f8c4611510c11d413cb2bef70867e584f003210968f97e0c54e6d37ba8d8d
- ca0e83440b77eca4d2eda6efd9530b49ffb477f87f36637b5e43f2e428898766

-
- Email

Author



朝長 秀誠 (Shusei Tomonaga)

Since December 2012, he has been engaged in malware analysis and forensics investigation, and is especially involved in analyzing incidents of targeted attacks. Prior to joining JPCERT/CC, he was engaged in security monitoring and analysis operations at a foreign-affiliated IT vendor. He presented at CODE BLUE, BsidesLV, BlackHat USA Arsenal, Botconf, PacSec and FIRST Conference. JSAC organizer.

Was this page helpful?

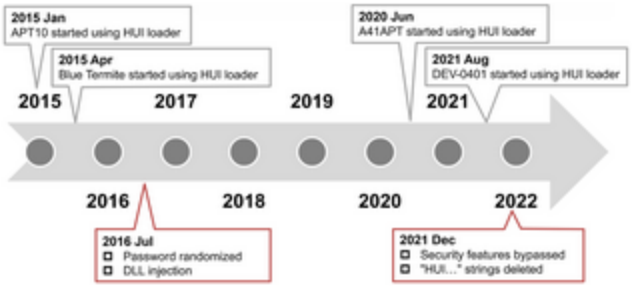
0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

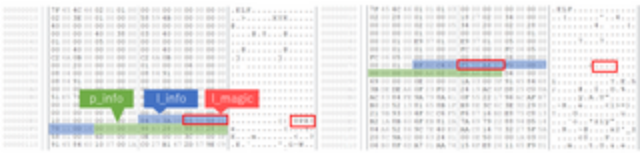
This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

Related articles

- 

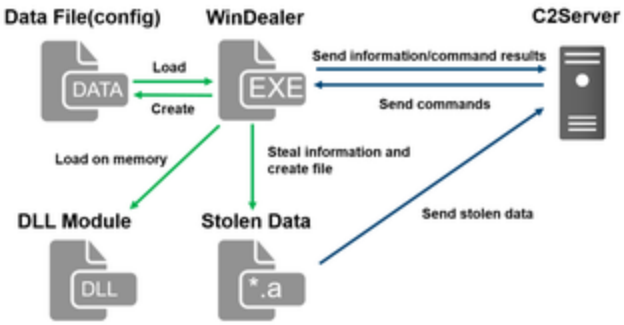
Analysis of HUI Loader

- 

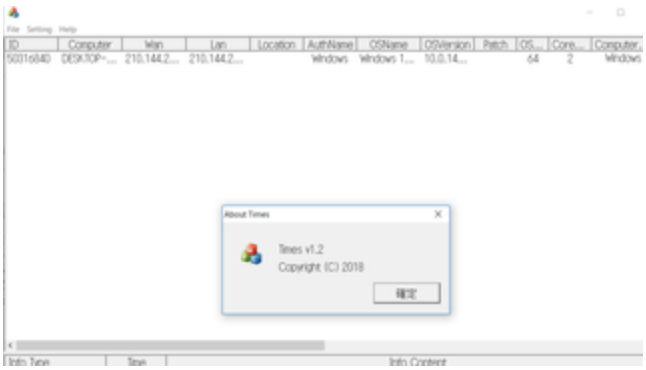
Anti-UPX Unpacking Technique

- 

FAQ: Malware that Targets Mobile Devices and How to Protect Them

- 

Malware WinDealer used by LuoYu Attack Group

- 
Malware Gh0stTimes Used by BlackTech

Back
Top
Next