

ELF_PLEAD - Linux Malware Used by BlackTech - JPCERT/CC Eyes

By 朝長 秀誠 (Shusei Tomonaga)

Published: 2020-11-15 · Archived: 2026-04-05 21:47:06 UTC

November 16, 2020

- [BlackTech](#)

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.

```
16 for (i = (unsigned __int16)port; i = (unsigned __int16)port)
17 {
18     conf = 0;
19     v7 = 0;
20     v8 = 0;
21     this = (main *)operator new(0x1020Cu);
22     v16 = 0;
23     if (this)
24         conf = mal_init(this, key, url);
25     v18 = -1;
26     connect_stage = mal_connect_main(conf, ServerName, i, ProxyName);
27     v11 = GetTickCount();
28     srand(v11);
29     switch (connect_stage + 6)
30     {
31     case 0:
32         v7 = 1000 * (20 * rand() / 0x8000 + 20);
33         break;
34     case 1:
35         v7 = 1000 * (30 * rand() / 0x8000 + 30);
36         break;
37     case 2:
38         break;
39     case 3:
40         break;
41     case 4:
42         v7 = 30000;
43         break;
44     case 5:
45         v8 = 1;
46         v7 = 1000 * mal_get sleeptime(conf);
47         break;
48     case 0xA:
49         v7 = 1000;
50         v8 = 1;
51         break;
52     case 0xB:
53         v7 = 60000;
54         break;
55     case 0xD:
56         v7 = 3000;
57         break;
58     default:
59         break;
60     }
61     if (conf)
62         (*(void (__thiscall *) (main *, int))conf->field_0)(conf, 1);
63     sleep(v7);
64     if (v8)
65         break;
66 }
```

```
30     v4 = &v12[9];
31 LABEL_4:
32     if (C_WORD "v4")
33         break;
34 LABEL_8:
35     if (++v3 > 2)
36         break;
37 LABEL_9:
38     v5 = rand();
39     sleep((int)((double)v5 * 128.0 * 4.656612873077393e-10) + 60);
40     v3 = 0;
41 }
42 }
43 switch ((unsigned int)mal_connect_main((__int64)&config, (__int64)&v12[32] * (__i
44 {
45     case 0u:
46     case 2u:
47         v6 = rand();
48         sleep((int)((double)v6 * 30.0 * 4.656612873077393e-10) + 30);
49         goto LABEL_7;
50     case 3u:
51         v10 = rand();
52         sleep((int)((double)v10 * 50.0 * 4.656612873077393e-10) + 100);
53         goto LABEL_7;
54     case 3u:
55     case 4u:
56     case 5u:
57         goto LABEL_7;
58     case 6u:
59         sleep(0x1Eu);
60         goto LABEL_7;
61     case 3u:
62         v9 = mal_get sleeptime((__int64)&config);
63         sleep(v9);
64         goto LABEL_7;
65     case 0xAu:
66         sleep(v4u);
67         goto LABEL_7;
68     case 0xBu:
69         sleep(0x4u);
70         goto LABEL_7;
71     case 0xCu:
72         v4 = -4;
73         goto LABEL_12;
74     case 0Du:
75         if (!fork())
76         {
77             memset(&command, 0, 0x200uLL);
78             mal_get_basename(&command, 0x200uLL);
79             system(&command);
80             exit(0);
81         }
```

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.)

00000000	64 5C 6E 56 30 33 30 35	6D 6C 00 00 00 00 00 00	d\nv0305m1.....
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	00 00 00 00 19 00 BB 01	6E 00 6D 78 2E 6D 73 64n.mx.ms d
00000030	74 63 2E 74 77 00 00 00	00 00 00 00 00 00 00 00	tc.tw.....
00000040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000100	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000110	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000120	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000130	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000140	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000150	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000160	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000170	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000180	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000190	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000001AA	00 00 00 00 00 00 00 00	00 00 ■

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.

```

0000B300 | 00 00 00 00 00 00 00 00 | 4F 8F 40 00 00 00 00 00 | .....O.@.....
0000B310 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....
0000B320 | F9 12 E8 DC A0 E3 C3 62 | 7C 60 43 2C A0 D5 AB DB | .....&..C.....
0000B330 | 72 FB A8 B5 0E D0 E1 F4 | D5 50 1E 34 4A F2 D7 3F | r.....P.4J.?.
0000B340 | BE 82 56 C1 05 D4 4F FE | 16 E9 A1 F4 35 79 B0 1E | ..V...O.....5y..
0000B350 | 85 FA 0B BB 98 D7 31 13 | 62 15 0A 7B 93 6A 1A B7 | [.....l.b...{.j..
0000B360 | 5B 2B 1E FE 6F 18 99 28 | 19 F9 9D 13 C7 65 9E 4E | [+...o..(.....e.N
0000B370 | 10 E9 E8 62 6C C2 AC D9 | C3 91 65 0B F7 7B 17 0D | ...bl.....e...{..
0000B380 | CD AB 08 76 48 3B 77 1A | 80 4E 49 5C 2E 42 A4 15 | ...vH;w..NI\..B..
0000B390 | 6E 67 A5 A6 C4 31 7B 08 | 5B 3D 93 01 D8 C6 78 53 | ng...l{.[=...xS
0000B3A0 | 4A 5C 9D 37 88 E1 FD CE | 24 EF 01 46 E9 88 7F 1D | J\..7....$.F....
0000B3B0 | 9F 6D E2 EE D5 45 F6 76 | 21 8B 96 F7 83 79 AB DE | .m...E.v!...y..
0000B3C0 | 67 CB 34 8E 6F D8 CB C1 | C8 80 87 36 B5 A8 12 80 | g..4.o.....6....
0000B3D0 | BA D9 83 D5 A7 76 35 9C | FA 81 90 7C 82 63 33 4B | .....v5....|.c3K
0000B3E0 | CC FD C8 E8 38 C7 A4 EA | EB 13 BE 5D 88 34 AE 60 | ....8.....].4.`
0000B3F0 | E6 EB D9 49 E4 49 9D 5D | 7C DE 69 F8 7B 1C 34 42 | ...I.I.]|.i.{.4B
0000B400 | 07 DC 38 22 03 0F 7F 35 | 5E 5E 5E 5E A4 B9 C9 FF | ..8"'.^.....
0000B410 | 46 27 F6 5E CA EF CD 64 | 5B 3B D9 50 EE B0 D5 0D | F'.^...d[;.....
0000B420 | 44 4E 83 95 86 98 BB 38 | C8 F2 70 24 18 A8 92 F3 | DN.....8...p$.
0000B430 | EC 3B 4C 5B A2 E3 74 9F | 49 97 AD 4D 78 01 9D FB | .;L[.t.I..Mx...
0000B440 | E1 AC 4D EE 8C 6D EC B7 | 19 DB 18 1C 15 5D 3E 6D | ..M..m.....]>m
0000B450 | D9 2F 48 EF 46 41 F5 B0 | 97 6B C5 55 1C A2 C5 77 | ./H.FA...k.U...w
0000B460 | 43 C6 69 28 B3 B7 71 23 | 72 C7 1C 47 CD B5 79 52 | C.i(..q#r..G..yR
0000B470 | DD CC 2B 7C 24 7C FE AB | FA 0C EE CB 15 0E 2E F6 | ..+|$.|.....
0000B480 | D6 D9 E9 0E AC A4 66 26 | DA 3B 22 23 D1 D9 37 A3 | .....f&.;"#.7.
0000B490 | 4E 42 42 51 8A 7F 57 D5 | 58 AB 47 75 14 43 42 AB | NBBQ..W.X.Gu.CB.
0000B4A0 | 8F BA DC 72 B1 0B 08 24 | 5C 12 90 09 A2 3C 9B A0 | ...r...$.|...<..
0000B4B0 | DA 44 16 AA 7C 1F 72 F9 | 4C D5 B6 7D 8F D2 24 44 | .D..|.r.L..}..$D
0000B4C0 | 57 20 D6 D4 11 ED 0A 94 | EF F5 6B 5A FD 18 91 78 | W .....kZ...x
0000B4D0 | DC 34 B9 1C BB E8 70 75 | 7A 29 AB 0B 3C 98 D1 C5 | .4....puz)..<CC.
0000B4E0 | F3 8B EE 67 7E D7 A2 E3 | D4 CB 84 08 47 43 43 3A | ..g~.....<G.CC:
0000B4F0 | 20 28 47 4E 55 29 20 34 | 2E 38 2E 35 20 32 30 31 | (GNU) 4.8.5 201
0000B500 | 35 30 36 32 33 20 28 52 | 65 64 20 48 61 74 20 34 | 50623 (Red Hat 4

```

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.

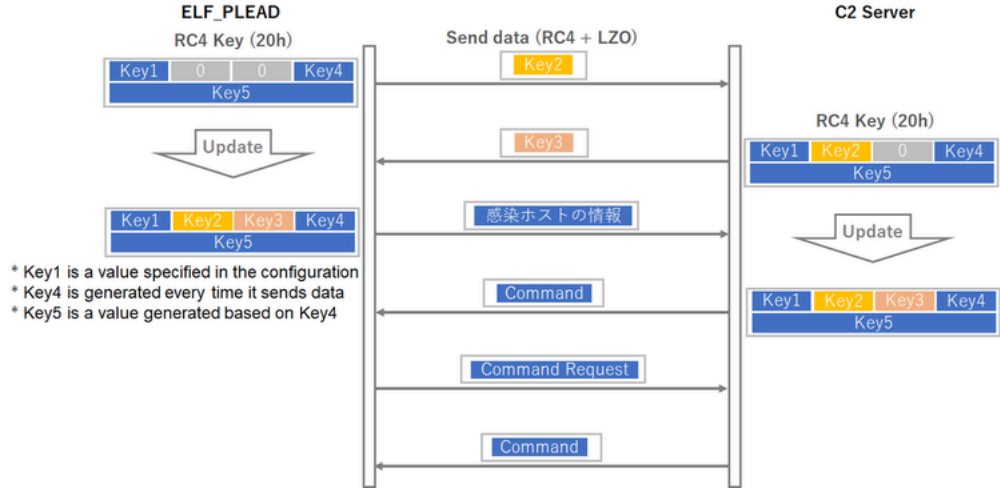


Figure 4: Communication flow of ELF_PLEAD

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)

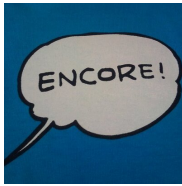
Value	Contents
96	Set up proxy
100	Connect proxy
102	Send proxy data
104	-
106	-
108	End proxy

Appendix D: C&C server

- mx.msdtc.tw

Appendix E: Malware hash value

- 5b5f8c4611510c11d413cb2bef70867e584f003210968f97e0c54e6d37ba8d8d
- ca0e83440b77eca4d2eda6efd9530b49ffb477f87f36637b5e43f2e428898766



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.

Related articles

```
*key = 0x42714862;
*key[4] = 0x015813C2;
*key[8] = 0x66d72834;
*key[12] = 0x80807969;
Dv[4] = 0x1456421;
Zv[1] = 0x48803A68;
Zv[2] = 0x30788529;
Zv[3] = 0x00000007;
v4 = m_ret_argOffset0x350(a1 + 1);
if ( !((v3->CryptAcquireContext)(a1, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 0x1, 0xF0000000) )
return 0;
v5 = m_ret_argOffset0x350(a1 + 3);
handlehash0 = a1 + 1;
if ( !((v3->CryptCreateHash)(*a1, 0x0004, 0, 0, a1 + 1) )
LABEL_0:
if ( *a1 )
return 0;
v6 = m_ret_argOffset0x350(a1 + 3);
(v6->CryptInitialize)(*a1, 0);
return 0;
}
if ( !CryptHashData(*handlehash0, key, 16u, 0)
|| (v6 = m_ret_argOffset0x350(a1 + 3);
v6 = a1 + 1;
!(v6->CryptDeriveKey)(*a1, 0x0004, *handlehash0, 0x000000, a1 + 2)) // CALD_AES_128
{
if ( *handlehash0 )
{
v5 = m_ret_argOffset0x350(a1 + 3);
(v5->CryptDestroyHash)(*handlehash0);
}
goto LABEL_0;
}
v10 = m_ret_argOffset0x350(a1 + 3);
(v10->CryptSetKeyParam)(*v9, 3, 0x0001, 0);
v11 = m_ret_argOffset0x350(a1 + 3);
(v11->CryptSetKeyParam)(*v9, 1, 0v, 0); // DV = parameter
v12 = m_ret_argOffset0x350(a1 + 3);
(v12->CryptSetKeyParam)(*v9, 4, 0x0002, 0); // 0x_0000 = CBC
return *v9;
}
```

Update on Attacks by Threat Group APT-C-60

```
python parse_cross2beacon_config.py beacon.bin
[+] Decoded Config Data
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Encode to ASCII
000000 29 01 00 00 7f 00 00 01 b3 15 00 00 09 00 00 00 ).....
000010 31 32 37 2e 30 2e 30 2e 31 00 00 00 00 0c 01 00 127.0.0.1.....
000020 00 2d 2d 2d 2d 2d 42 45 47 49 4e 20 50 55 42 4c ,----BEGIN,PUBL
000030 49 43 20 4b 45 59 2d 2d 2d 2d 2d 2d 0a 4d 49 47 66 IC.KEY----.MIGF
000040 4d 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 MA8GCSqGS1b3QDEB
000050 41 51 55 41 41 34 47 4e 41 44 43 42 69 51 4b 42 AQUAAAGNADCB1QKB
000060 67 51 43 4e 53 33 38 6c 48 50 32 56 33 4a 44 34 gQCNS3B1HP2V33D4
000070 47 54 39 55 63 61 4c 68 41 6b 70 4d 64 51 41 47 GT9UcaLhAkpM4QAG
000080 52 6e 36 4e 77 36 52 48 6e 56 35 54 2f 69 48 4a Rn6Nw6RHnVST/1HJ
000090 2b 7a 48 4c 48 38 32 71 37 58 4b 6d 6f 2b 72 55 +zHLH82q7XKmo+rU
0000A0 2b 49 7a 59 70 58 6e 57 55 37 70 4d 73 69 53 64 +IzYpXnwU7pMs1Sd
0000B0 71 2b 63 52 78 4d 6f 54 4c 6d 68 4e 6f 71 32 55 q+cRxoTLmhNoq2U
0000C0 54 57 4b 39 6f 39 52 6f 64 63 5a 7a 5a 58 73 6b TwK9o9RodcZtZxsk
0000D0 62 4d 37 54 7a 4b 37 55 5a 6a 79 61 70 54 49 4a bM7Tzk7UZjyapTIJ
0000E0 66 63 71 36 42 57 4d 64 73 4d 78 36 67 48 34 4f fcq6BwMdsMx6gh40
0000F0 73 6c 42 2f 35 77 6e 63 33 77 51 78 55 62 4f 61 s1B/Swnc3wXuU0a
000100 71 45 6f 6b 4b 6f 72 5a 77 6d 68 55 33 77 49 44 qEokKorZwmHU3wID
000110 41 51 41 42 0a 2d 2d 2d 2d 2d 45 4e 44 20 50 55 AQAB.----END.PU
000120 42 4c 49 43 20 4b 45 59 2d 2d 2d 2d 2d 41 41 41 BLIC.KEY----AAA
000130 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 .....
[+] Config Data
C2: 127.0.0.1:5555
PUBLICKEY: ----BEGIN PUBLIC KEY----
MIGFMA8GCSqGS1b3QDEBAQUAAAGNADCB1QKBgQCNS3B1HP2V33D4GT9UcaLhAkpM4QAGRn6Nw6
RHnVST/1HJ+zHLH82q7XKmo+rU+IzYpXnwU7pMs1Sdq+cRxoTLmhNoq2UTwK9o9RodcZtZxsk
bM7Tzk7UZjyapTIJfcq6BwMdsMx6gh40s1B/Swnc3wXuU0aqEokKorZwmHU3wIDAQAB
----END PUBLIC KEY----
```

CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks

