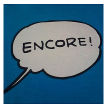
Bug in Malware “TSCookie” - Fails to Read Configuration - (Update)

blogs.jpcert.or.jp/en/2019/05/tscookie3.html



朝長 秀誠 (Shusei Tomonaga)

May 30, 2019

BlackTech

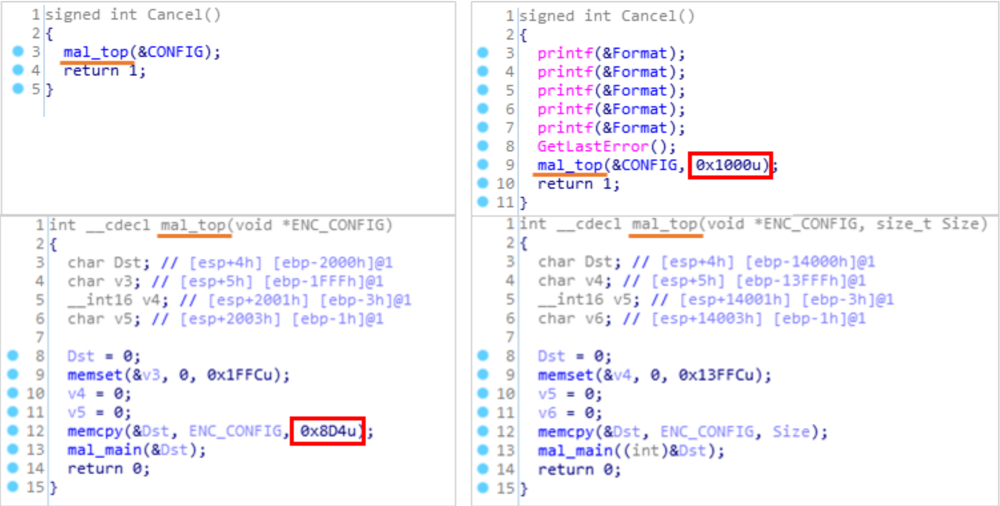
-
- Email

Our past article has presented a bug in malware “TSCookie”, which is reportedly used by BlackTech attack group. This article is to update the features of the malware.

Even after we published the blog article in October 2018, the adversary had continued using the malware as it was. Just in May 2019, we confirmed that the malware had its bug fixed and was used in some attack cases.

Details of the fix

The malware copies its configuration to the memory. In the previous version, the data size to be copied was incorrectly set, which resulted in the configuration not displayed properly (see the article for more details). In the updated version, the data size is set to 0x1000 instead of 0x8D4.



```
signed int Cancel()
{
  mal_top(&CONFIG);
  return 1;
}
```

```
int __cdecl mal_top(void *ENC_CONFIG)
{
  char Dst; // [esp+4h] [ebp-2000h]@1
  char v3; // [esp+5h] [ebp-1FFFh]@1
  __int16 v4; // [esp+2001h] [ebp-3h]@1
  char v5; // [esp+2003h] [ebp-1h]@1

  Dst = 0;
  memset(&v3, 0, 0x1FFCu);
  v4 = 0;
  v5 = 0;
  memcpy(&Dst, ENC_CONFIG, 0x8D4u);
  mal_main(&Dst);
  return 0;
}
```

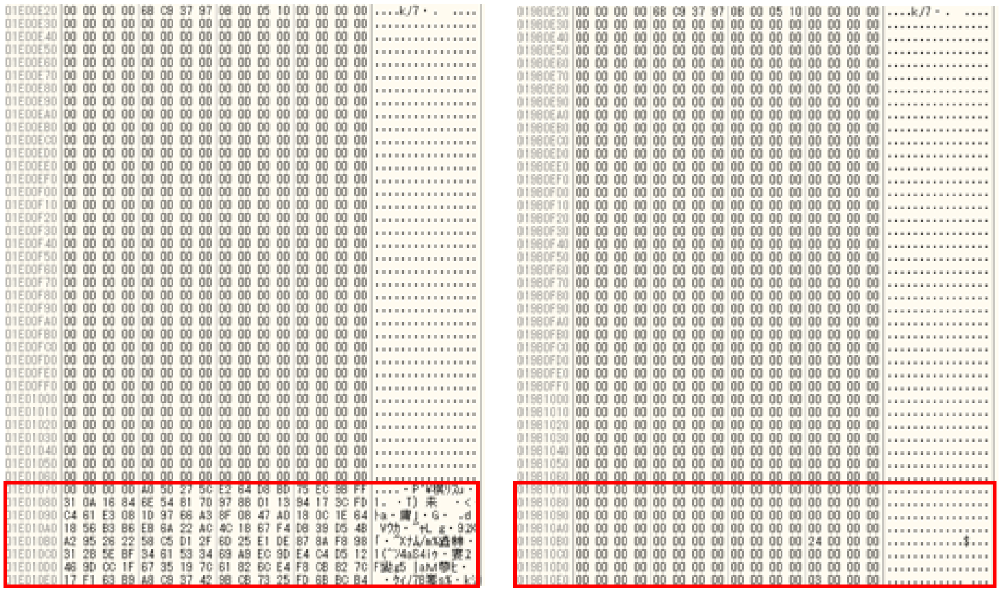
```
signed int Cancel()
{
  printf(&Format);
  printf(&Format);
  printf(&Format);
  printf(&Format);
  printf(&Format);
  GetLastError();
  mal_top(&CONFIG, 0x1000u);
  return 1;
}
```

```
int __cdecl mal_top(void *ENC_CONFIG, size_t Size)
{
  char Dst; // [esp+4h] [ebp-14000h]@1
  char v4; // [esp+5h] [ebp-13FFFh]@1
  __int16 v5; // [esp+14001h] [ebp-3h]@1
  char v6; // [esp+14003h] [ebp-1h]@1

  Dst = 0;
  memset(&v4, 0, 0x13FFCu);
  v5 = 0;
  v6 = 0;
  memcpy(&Dst, ENC_CONFIG, Size);
  mal_main((int)&Dst);
  return 0;
}
```

Fig 1: Updates in TSCookie (Left: Code with the bug / Right: Updated code)

This update enables TSCookie to decode the configuration correctly. Fig 2 is the comparison of decoded configuration. This update has also fixed the issue where the malware fails to reconnect to a C&C server for a few days.



```
01E00E20 00 00 00 00 6B C9 37 97 0B 00 05 10 00 00 00 00 ....k/7・.  ....
01E00E30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00E40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00E50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00E60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00E70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00E80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00E90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00EA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00EB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00EC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00ED0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00EE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00EF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E00FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01E01070 00 00 00 00 A0 5D 27 5C E2 64 D8 BD 75 EC 98 FF ....・P'¥蜷ｿu・
01E01080 31 0A 16 84 6E 54 81 70 97 88 01 13 94 17 3C FD 1.  ・T) 宗   ・<・
01E01090 C4 61 E3 08 1D 97 68 A3 8F 08 47 A0 18 0C 1E 64 ﾄa・闇｣・G・  .d
01E010A0 18 56 B3 B6 EB 6A 22 AC 4C 18 67 F4 D8 39 D5 4B  Vｳｶ・ "ｬL g・9ﾕK
01E010B0 A2 95 26 22 58 C5 D1 2F 6D 25 E1 DE 87 8A F8 98 ｢・&"Xﾅﾑ/m%矧奄・
01E010C0 31 28 5E BF 34 61 53 34 69 A9 EC 9D E4 C4 D5 12 1(^ｿ4aS4iｩ・揺ﾕ2
01E010D0 46 9D 0C 1F 67 35 19 7C 61 82 6C E4 F8 C8 82 7C F撒g5 |aM螺・|
01E010E0 17 F1 63 B9 A8 C9 37 42 98 C8 73 25 FD 6B BC B4  ・ｼｸｼ/7B蘇s%・k・
```

```
01980E20 00 00 00 00 6B C9 37 97 0B 00 05 10 00 00 00 00 ....k/7・.  ....
01980E30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980E40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980E50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980E60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980E70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980E80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980E90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980EA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980EB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980EC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980ED0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980EE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980EF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01980FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
01981090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
019810A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
019810B0 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 ............$...
019810C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
019810D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
019810E0 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 ............ ...
```

Fig 2: Decoded configurations of TSCookie (Left: Sample with the bug / Right: Updated sample)

In closing

As we pointed out before, it is likely that adversaries also follow publications and blogs from security vendors, etc. We assume that the adversary recognised the bug on our blog and fixed the issue accordingly. If we see any updates on the malware, we will introduce them here.
Hash values of the samples described in the article are listed in Appendix A, along with C&C servers in Appendix B. Please make sure that none of your devices is accessing these hosts.

Thank you for reading.

Shusei Tomonaga
(Translated by Yukako Uchida)

Appendix A: Hash value of the samples

Malware with the bug

96723797870a5531abec4e99fa84548837e9022e9f22074cf99973ab7df2a2e7

Updated malware

- 1ec19677d1e48e4f6ff5f9fe7808b13964059e2ffd48ece19f7305d78e04ec4a
- c2c062ff84a18ad02e92dea0d6e12cafa66ff167ea8d02663fc9aae44de7f4e0

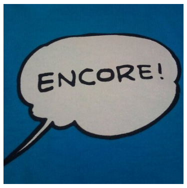
Appendix B: List of C&C servers

- www.google.com.dns-report.com

- microsoft.com.appstore.dynamicdns.co.uk
- cartview.viamisoftware.com

-
- 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.

Back
Top
Next