Bug in Malware “TSCookie” - Fails to Read Configuration - (Update) - JPCERT/CC Eyes

By 朝長 秀誠 (Shusei Tomonaga)

Published: 2019-05-29 · Archived: 2026-04-06 00:31:49 UTC

May 30, 2019

- BlackTech

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.

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

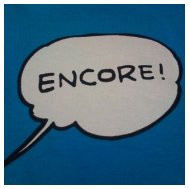
- 96723797870a5531abec4e99fa84548837e9022e9f22074cf99973ab7df2a2e7

Updated malware

- 1ec19677d1e48e4f6ff5f9fe7808b13964059e2ffd48ece19f7305d78e04ec4a
- c2c062ff84a18ad02e92dea0d6e12cafa66ff167ea8d02663fc9aae44de7f4e0

Appendix B: List of C&C servers

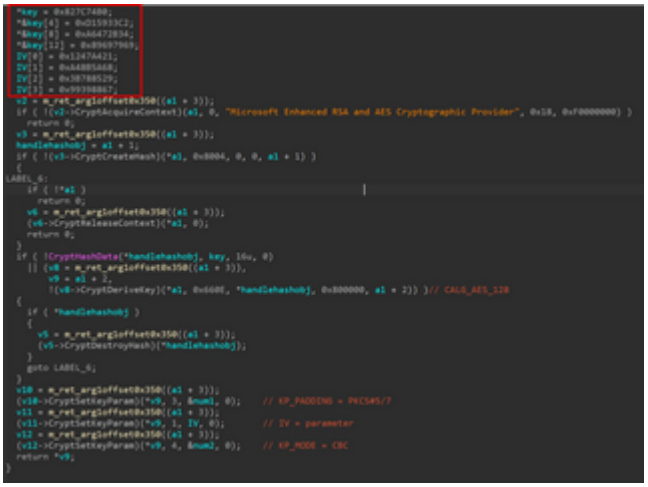
- www.google.com.dns-report.com
- microsoft.com.appstore.dynamicdns.co.uk
- cartview.viamisoftware.com



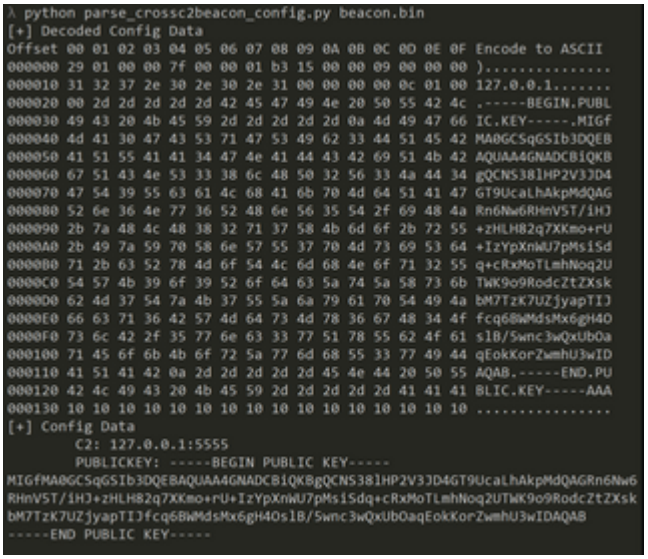
朝長 秀誠 (Shusei Tomonaga)

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.

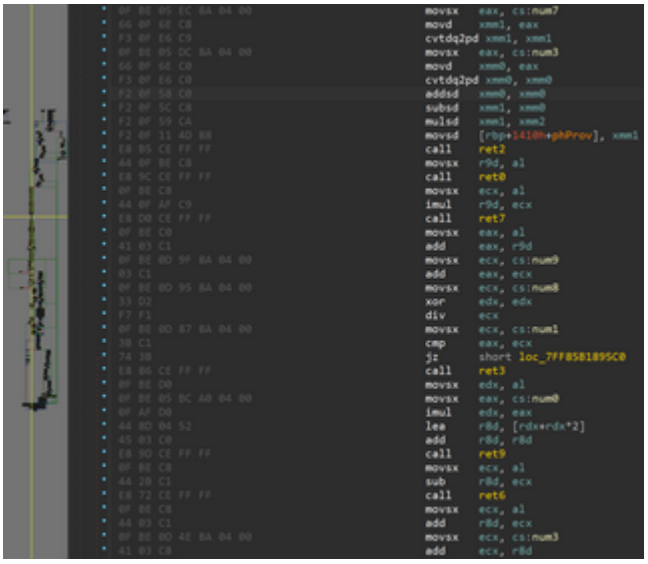
Related articles

- 

  Update on Attacks by Threat Group APT-C-60

- 

  CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks

- 

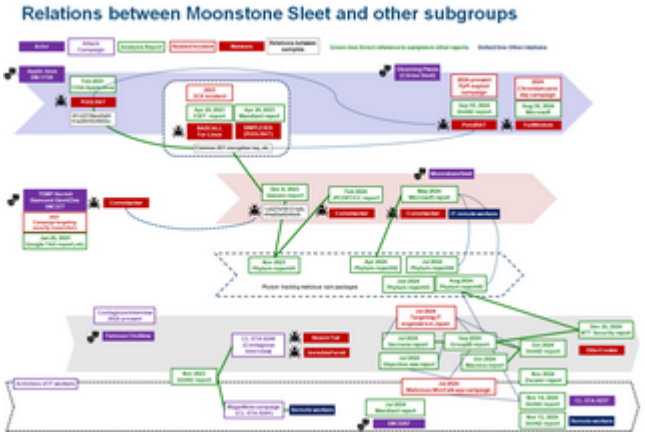
  Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities

- 

```
__int64 __fastcall mal_decode(__int64 encbuf, int bufsize)
{
  __int64 j_1; // rax
  int i; // [rsp+18h] [rbp-Ch]

  if ( encbuf )
  {
    for ( i = 0; ; ++i )
    {
      j_1 = (unsigned int)i;
      if ( i >= bufsize )
        break;
      *(_BYTE *)(encbuf + i) ^= Key1to7[i % 7];
    }
  }
  return j_1;
}
```

  DslogdRAT Malware Installed in Ivanti Connect Secure

- 

  Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup

---

Source: https://blogs.jpcert.or.jp/en/2019/05/tscookie3.html