Lazarus Group Uses the DLL Side-Loading Technique (2) - ASEC

By ATCP

Published: 2024-01-16 · Archived: 2026-04-05 14:51:32 UTC

Through the “Lazarus Group Uses the DLL Side-Loading Technique” **[1]** blog post, AhnLab SEcurity intelligence Center (ASEC) has previously covered how the Lazarus group used the DLL side-loading attack technique using legitimate applications in the initial access stage to achieve the next stage of their attack process. This blog post will cover the added DLL variants and their verification routine for the targets.

The Lazarus group is an APT group that targets South Korean companies, institutions, think tanks, and others. On January 12, 2024, a new legitimate program for DLL side-loading (T1574.002 Hijack Execution Flow: DLL side-loading), a technique commonly used by the Lazarus group to execute malware, was discovered through AhnLab Smart Defense (ASD).

The threat actor typically uses the DLL side-loading technique in the initial access and malware execution stages. This method saves a legitimate application and a malicious DLL in the same folder path so that the malicious DLL is also executed when the application is run. In other words, it is a malware execution technique that allows the malicious DLL to be executed first by changing its name to the filename of the legitimate DLL located in a different path that the legitimate program refers to.

The newly discovered legitimate program is called “wmiapsrv.exe”. The wmiapsrv.exe program is a legitimate MS module that loads **“wbemcomn.dll”**, which is used to load the modified malicious wbemcomn.dll. Additionally,

another modified malicious DLL within the same path called **“netutils.dll”** was discovered. The created wbemcomn.dll and netutils.dll perform as backdoors.

1. wbemcomn.dll

wbemcomn.dll has a verification routine for the targets. The result value of the GetSystemFirmwareTable API call includes unique information from the system, which is used to decrypt the encrypted strings in the resource area of wbemcomn.dll. The file in the path of the decrypted value is then loaded to carry out malicious behaviors. This shows that this is an APT attack attempt that is executed only on specific systems. This is because the file path information cannot be checked when the result of the GetSystemFirmwareTable API call through another system’s information is used for decryption.

```
001AE8A0  1F 34 01 05 52 84 30 02 6C 74 AF 5F AA 06 4B D0  .4..R„0.lt¯_ª.KÐ
001AE8B0  1F D4 78 68 62 80 34 1E 1D BE 1C EB 63 6E B2 CE  .Ôxhb€4..¾.ëcn²Î
001AE8C0  D1 5F 8A AD 52 4F 0A 9D 7A 9E BC 41 21 34 ED EC  Ñ_Š.RO..zž¼A!4íì
001AE8D0  8B 48 E8 24 82 83 22 81 88 5D D1 C0 BA 97 AB D8  ‹Hè$‚ƒ".ˆ]ÑÀº—«Ø
001AE8E0  FF 4B 77 99 92 0C 3B 7C B7 F8 05 CE 22 B2 EC A5  ÿKw™'.;|·ø.Î"²ì¥
001AE8F0  4C 45 2A A6 BA D2 04 02 81 5A D0 FF 23 A4 2A F2  LE*¦ºÒ...ZÐÿ#¤*ò
001AE900  AD 9B DC F9 7D 05 76 E5 AF BC 54 54 F7 E3 64 4B  .›Üù}.vå¯¼TT÷ãdK
001AE910  4E 2F 51 C9 D0 8E 5A 93 89 CF 50 77 F0 20 88 40  N/QÉÐŽZ“‰ÏPwð ˆ@
001AE920  B5 0B E1 3C C3 74 C5 92 6A C0 FF 24 06 C9 BC FD  µ.á<ÃtÅ’jÀÿ$.É¼ý
001AE930  71 9B 70 9E F6 79 55 8C 67 81 6F EE 9E 58 2F 0D  q›pžöyUŒg.oîžX/.
001AE940  38 5B 03 97 65 F4 AB 83 03 DE F4 F0 EE A6 1B 21  8[.—eô«ƒ.Þôðî¦.!
001AE950  06 9C 71 ED 1B 98 41 39 93 A5 5E 40 DD 41 45 BA  .œqí.˜A9“¥^@ÝAE°
001AE960  B1 CE 20 8B 45 12 1C 58 E7 CE 33 5D 76 23 C4 83  ±Î ‹E..XçÎ3]v#Äƒ
001AE970  FC AB 1B 75 E7 81 9F DB 83 30 A6 17 20 22 90 BE  ü«.uç.ŸÛƒ0¦. ".¾
001AE980  BF CB E5 2F 7B E1 C0 B1 F2 06 15 4B 45 49 79 CD  ¿Ëå/{áÀ±ò..KEIyÍ
001AE990  23 25 AC A9 1A 0E BB A7 B6 22 C4 B4 7C 7D 40 F7  #%¬©..»§¶"Ä´|}@÷
001AE9A0  03 86 21 83 BC 89 9B D4 64 37 92 4B 9E 5F 78 45  .†!ƒ¼‰›Ôd7’Kž_xE
001AE9B0  E8 F8 73 41 82 DF C0 D3 C6 96 E7 6F C2 FB 78 6E  èøsA‚ßÀÓÆ–çoÂûxn
001AE9C0  3E 17 5F 7D CF F7 77 06 D3 AA 16 7D 5C A9 C1 F3  >._}Ï÷w.Óª.}\©Áó
001AE9D0  56 EA 24 B9 5B A4 58 1D 8C 52 B1 5E C9 1C 73 1E  Vê$¹[¤X.ŒR±^É.s.
001AE9E0  74 A1 80 11 73 E9 A8 65 0A F3 90 34 3C 06 C9 26  t¡€.sé¨e.ó.4<.É&
001AE9F0  6F 95 E6 67 B4 6D 28 02 95 73 D3 35 CB 75 F3 33  o•æg´m(.•sÓ5Ëuó3
001AEA00  12 F3 79 1D 2D 13 6C 26 34 65 B4 BF B6 6C C0 FA  .óy.-.l&4e´¿¶lÀú
001AEA10  97 5E 58 79 A1 73 C8 F8 9D C5 1C FF 53 24 01 50  —^Xy¡sÈø.Å.ÿS$.P
001AEA20  24 E1 20 3F 5A F6 ED FF AF 1A 09 C7 A5 35 17 3D  $á ?Zöíÿ¯..Ç¥5.=
001AEA30  52 58 F4 0E 2A 1F 3D 67 EC 19 EA E4 53 07 77 68  RXô.*.=gì.êäS.wh
001AEA40  E9 33 0F AD 4F 75 4F E3 AB 8B E9 08 66 B5 B0 5A  é3..OuOã«‹é.fµ°Z
001AEA50  27 10 66 5E 90 39 90 83 9F F5 E6 CA 44 D4 D4 A8  '.f^.9.ƒŸõæÊDÔÔ¨
```

2. netutils.dll

Unlike wbemcomn.dll, netutils.dll can load specific files without any decryption verification process. The file path and name are shown below.

- PDB information – O:\Develop\Tool_Dev\Loader\7-Zip\Util\7z\Debug\7zDec.pdb
- Loaded file information – C:\ProgramData\Microsoft Editor\editor.dat

```
NumberOfBytesRead = 0;
FileA = CreateFileA("C:\\ProgramData\\Microsoft Editor\\editor.dat", 0x80000000, 0, 0i64, 4u, 0x80u, 0i64);
v1 = FileA;
if ( FileA == (HANDLE)-1i64 )
  return 0i64;
FileSize = GetFileSize(FileA, 0i64);
v4 = operator new(FileSize);
if ( ReadFile(v1, v4, FileSize, &NumberOfBytesRead, 0i64) )
{
  CloseHandle(v1);
  v5 = LocalAlloc(0x40u, FileSize);
  v6 = sub_18000D290(v4, v5, (unsigned int)FileSize);
  v7 = v5;
  if ( v6 && (v8 = sub_18000F9C0(v5), v7 = v5, v8) )
  {
    LocalFree(v5);
    j_j_free(v4);
    return 1i64;
  }
  else
  {
    LocalFree(v7);
    j_j_free(v4);
    return 0i64;
  }
}
else
{
  CloseHandle(v1);
  return 0i64;
}
```

The Lazarus group uses spear phishing, supply chain attacks, and various other attack vectors. This group is very dangerous and is one of the most active attack groups in the world. This type of malware is diagnosed by AhnLab as follows.

[File Detection]

Trojan/Win.LazarLoader.C5572843 (2024.01.12.03)

Trojan/Win.LazarLoader.C5572847 (2024.01.13.00)

[Behavior Detection]

Injection/MDP.Event.M4512

Injection/EDR.Lazarus.M10965

MD5

21def97a3c5b95df1e1aeb6486881656

edca71eda8650a2c591c37c780b6a0c5

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/60792/