asec.ahnlab.com /en/85119/

Analysis on the Case of TIDRONE Threat Actor's Attacks on Korean Companies

⋮ 12/12/2024

Malware

- Dec 13 2024

AhnLab SEcurity intelligence Center (ASEC) has recently identified that the TIDRONE threat actor is launching attacks against companies. In the attack cases, Enterprise Resource Planning (ERP) software was exploited to install a backdoor malware called CLNTEND.

TIDRONE is a threat group known for targeting Taiwanese defense companies and drone manufacturers. Trend Micro first reported on TIDRONE in September 2024. [1] TIDRONE, which is known to be associated with a threat group that uses Chinese, targets multiple countries in addition to Taiwan. The group installs a backdoor malware called CXCLNT and CLNTEND by exploiting Enterprise Resource Planning (ERP) software and UltraVNC, a remote desktop software.

ASEC has confirmed that the CLNTEND malware was used in attacks against Korean companies in the first half of 2024. Since July 2024, the group has also been exploiting Korean ERP software. Given that the official websites of these ERP software are not available and they have a limited number of users, it is

likely that the software is developed by small-sized companies and distributed to a few Korean companies.

Figure 1. CLNTEND Installed with ERP

1. Attack Vector

The distribution method of the attack identified in the first half of 2024 has not been confirmed. However, it is known that the attack used DLL side-loading, similar to the report by TrendMicro, with “winword.exe”. From July 2024, there have been two main types of cases where malware was distributed through ERP.

The first type seems to be an ERP related to small-scale development companies in Korea. The developer is assumed to customize and provide the ERP for each client. The legitimate ERPs from this company, which are identified on AhnLab Smart Defense (ASD), are about 20 MB in size. On the other hand, all the malware samples used in attacks are about 4 MB in size.

Figure 2. Cases of attacks exploiting ERP

Although the malware directly distributed by the threat actor was not collected, the “VsGraphicsDesktopEngine.exe” created by this malware is a legitimate program used in another DLL side-loading, which will be covered later. There is a commonality in that TIDRONE’s loader malware is found in the following paths.

%ProgramFiles%\microsoft office\wwlib.dll
%SystemDrive%\3dp\edition\wwlib.dll
%ProgramFiles%\intel\intel(r) serial io\lang\hr-hr\wwlib.dll

The second type is the case where the distribution of actual malware was confirmed. This is another case involving the ERP of a Korean company, and like the first case, there is no official website for this type. Similar to the first case, the threat actor uploaded different versions of the malware to different clients. While one client received a legitimate version of the ERP, the malware was later switched to a dropper that installed both the ERP and CLNTEND.

Module	Behavior	Data
N/A	Downloads executable file	http://exe. .com/ / _ERP.exe Target _ERP[1].exe
N/A	Downloads executable file	http://exe. .com/ _test/ _ERP.exe Target _ERP[1].exe
N/A	Downloads executable file	http://exe. .com/ / _ERP.exe Target _ERP[1].exe
N/A	Downloads executable file	http://exe. .com/ / _ERP.exe Target _erp[1].exe

Figure 3. CLNTEND downloaded from the ERP distribution server

2. Malware Analysis

The malware installed through the above attack consists of a legitimate executable, a DLL responsible for loading, and an encrypted CLNTEND. After distribution, the executable file that was distributed is executed. The legitimate executable loads the malicious DLL that was distributed in the same path through DLL side-loading and ultimately decrypts and executes another file in the memory.

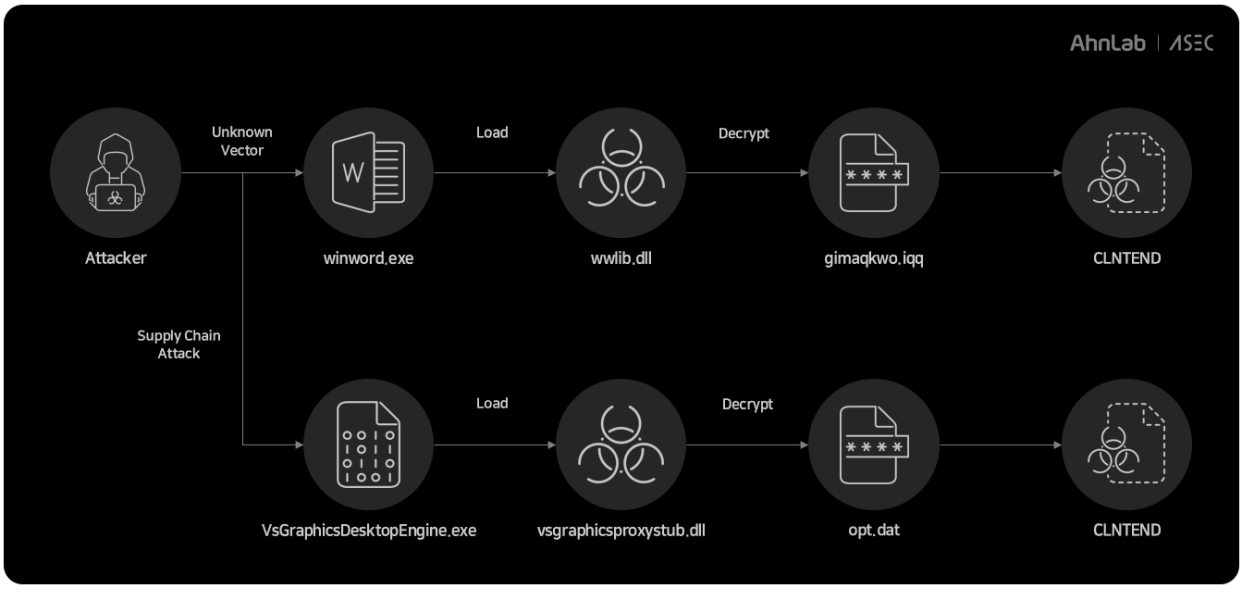


Figure 4. Operation flow chart

The most exploited executable files are Microsoft Word and VsGraphicsDesktopEngine.exe, and recently, rc.exe has been exploited.

Executable File	DLL Name	Data File Name
winword.exe	wwlib.dll	gimaqkwo.iqq
VsGraphicsDesktopEngine.exe	vsgraphicsproxystub.dll	opt.dat
rc.exe	rcdll.dll	wctE5ED.tmp
N/A	jli.dll	cxufejc.abu thaxdle.fxm
N/A	iviewers.dll	opt.dat tmplog

Table 1. DLL Side-Loading

Various loader malware are used in the attack process, and threat actors have created various types of loaders to hinder analysis. The loader covered by Trend Micro uses a technique of overwriting the Fiber structure to hinder analysis. The recent malware also uses obfuscation techniques, and it is characterized by using FlsCallback to decrypt an encrypted data file “wctE5ED.tmp”.

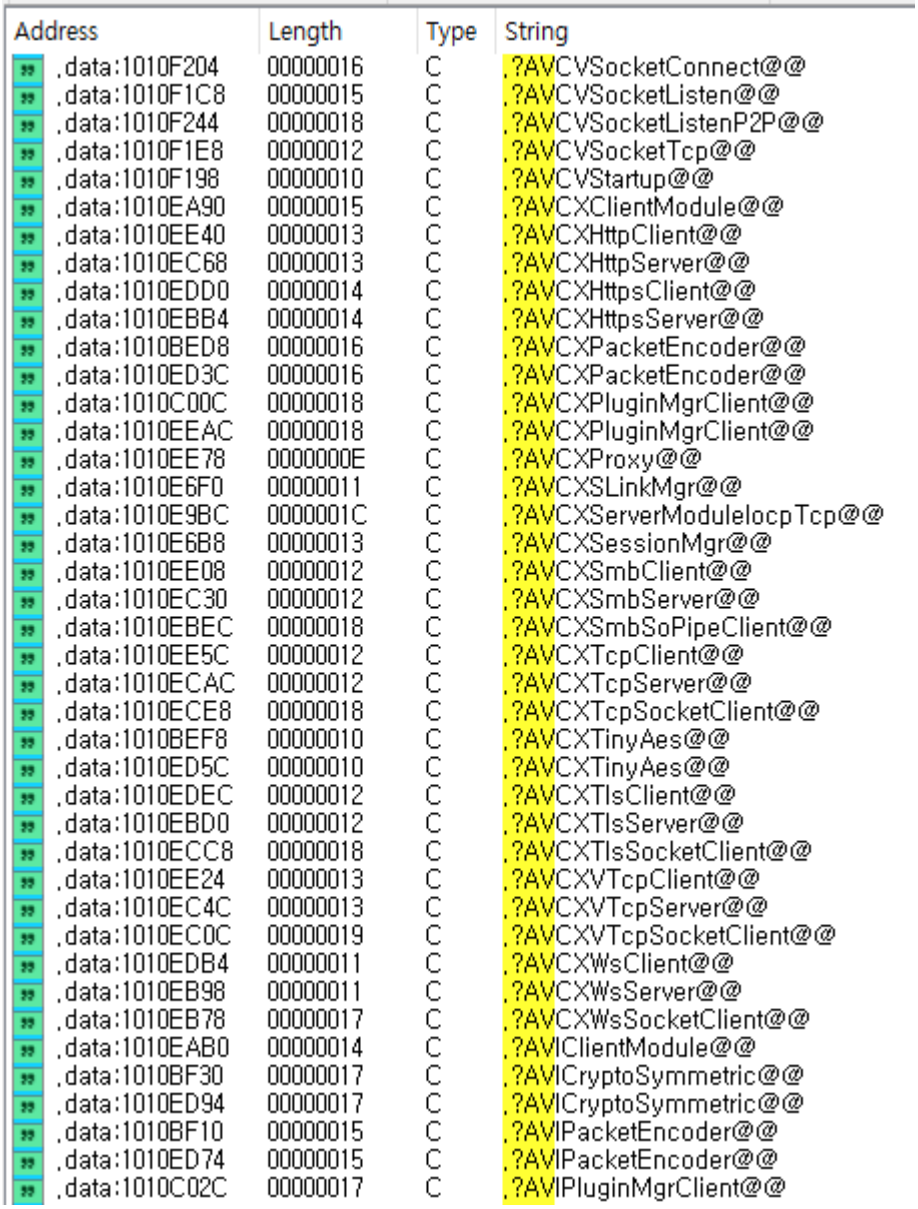
```
BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason,
{
  BOOL v3; // ebx
  DWORD cbNeeded; // [esp+0h] [ebp-94h] BYREF
  DWORD idProcess[35]; // [esp+4h] [ebp-90h] BYREF

  if ( fdwReason != 1 )
    return 1;
  memset(idProcess, 0, sizeof(idProcess));
  cbNeeded = 0;
  K32EnumProcesses(idProcess, 0x8Cu, &cbNeeded);
  v3 = cbNeeded == 140;
  if ( cbNeeded == 140 )
    dwFlsIndex = FlsAlloc(Callback);
```

```
lstrcatA(Filename, (LPCSTR)v0);
v11 = fn_readEncData(Filename);
FlsSetValue(dwFlsIndex + v11, Filename);
FlsFree(dwFlsIndex);
hThread = (int)CreateThread(0, 0, lpStartAddress, 0, 0, 0);
WaitForSingleObject((HANDLE)hThread, 0xFFFFFFFF);
ExitProcess(0);
```

```
void __stdcall Callback(PVOID lpFlsData)
{
  VirtualProtect(lpStartAddress, dwSize, 0x40u, &flOldProtect);
  v1 = dwSize;
  v2 = 0;
  for ( i = lpStartAddress; v2 < v1; *v4 = v5 )
  {
    v4 = (char *)i + v2;
    v5 = v2 ^ *((_BYTE *)i + v2) ^ ((*((_BYTE *)&dwSize + (v2 & 3)) ^ (v2 + 62)) + 79);
    ++v2;
  }
```

Figure 5. Decryption routine using FlsCallback

CLNTEND is a RAT malware. According to the report by Trend Micro, it has been used in attacks along with CXCLNT. CLNTEND is known for supporting various communication protocols such as TCP (Raw Socket, Web Socket), TLS, HTTP, HTTPS, and SMB, unlike CXCLNT.



Address	Length	Type	String
.data:1010F204	00000016	C	.?AVCVSocketConnect@@
.data:1010F1C8	00000015	C	.?AVCVSocketListen@@
.data:1010F244	00000018	C	.?AVCVSocketListenP2P@@
.data:1010F1E8	00000012	C	.?AVCVSocketTcp@@
.data:1010F198	00000010	C	.?AVCVStartup@@
.data:1010EA90	00000015	C	.?AVCXClientModule@@
.data:1010EE40	00000013	C	.?AVCXHttpClient@@
.data:1010EC68	00000013	C	.?AVCXHttpServer@@
.data:1010EDD0	00000014	C	.?AVCXHttpsClient@@
.data:1010EBB4	00000014	C	.?AVCXHttpsServer@@
.data:1010BED8	00000016	C	.?AVCXPacketEncoder@@
.data:1010ED3C	00000016	C	.?AVCXPacketEncoder@@
.data:1010C00C	00000018	C	.?AVCXPluginMgrClient@@
.data:1010EEAC	00000018	C	.?AVCXPluginMgrClient@@
.data:1010EE78	0000000E	C	.?AVCXProxy@@
.data:1010E6F0	00000011	C	.?AVCXSLinkMgr@@
.data:1010E9BC	0000001C	C	.?AVCXServerModulelocpTcp@@
.data:1010E6B8	00000013	C	.?AVCXSessionMgr@@
.data:1010EE08	00000012	C	.?AVCXSmbClient@@
.data:1010EC30	00000012	C	.?AVCXSmbServer@@
.data:1010EBEC	00000018	C	.?AVCXSmbSoPipeClient@@
.data:1010EE5C	00000012	C	.?AVCXTcpClient@@
.data:1010ECAC	00000012	C	.?AVCXTcpServer@@
.data:1010ECE8	00000018	C	.?AVCXTcpSocketClient@@
.data:1010BEF8	00000010	C	.?AVCXTinyAes@@
.data:1010ED5C	00000010	C	.?AVCXTinyAes@@
.data:1010EDEC	00000012	C	.?AVCXTlsClient@@
.data:1010EBD0	00000012	C	.?AVCXTlsServer@@
.data:1010ECC8	00000018	C	.?AVCXTlsSocketClient@@
.data:1010EE24	00000013	C	.?AVCXVTcpClient@@
.data:1010EC4C	00000013	C	.?AVCXVTcpServer@@
.data:1010EC0C	00000019	C	.?AVCXVTcpSocketClient@@
.data:1010EDB4	00000011	C	.?AVCXWsClient@@
.data:1010EB98	00000011	C	.?AVCXWsServer@@
.data:1010EB78	00000017	C	.?AVCXWsSocketClient@@
.data:1010EAB0	00000014	C	.?AVIClientModule@@
.data:1010BF30	00000017	C	.?AVICryptoSymmetric@@
.data:1010ED94	00000017	C	.?AVICryptoSymmetric@@
.data:1010BF10	00000015	C	.?AVIPacketEncoder@@
.data:1010ED74	00000015	C	.?AVIPacketEncoder@@
.data:1010C02C	00000017	C	.?AVIPluginMgrClient@@

Figure 6. Class names of CLNTEND

Threat actors also distributed Loader, encrypted data, and Launcher malware. It is responsible for executing files in a specific path. However, the hard-coded path names allow the installation path and file name of the malware to be estimated.

Type	Execution Path
Type A	C:\AMD\Chipset_SoftWare\VsGraphicsDesktopEnginese.exe
Type B	C:\NVIDIA\DisplayDriver\rc.exe C:\NVIDIA\nForceWin7Vista64Int\rc.exe C:\NVIDIA\GLCache\rc.exe C:\AMD\Chipset_Software\rc.exe
Type C	C:\ProgramData\Microsoft OneDrive\setup\nir.exe” exec hide cdb.exe -pd -cf “C:\ProgramData\Microsoft OneDrive\setup\dbglog.dat” dllhost
Type D	C:/******/*****/Application/de/oleview.exe

Table 2. Execution paths of Launcher

3. Conclusion

The activities of the TIDRONE threat actor, known for attacking defense companies in Taiwan, are continuously being identified in South Korea. The recently identified attack cases involve the exploitation of ERPs that are suspected to have been created by small-scale development companies.

Users must control access from threat actors by using security products. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection
– Trojan/Win.Loader.R679179 (2024.11.11.00)
– Trojan/Win.Loader.R679207 (2024.11.11.00)
– Trojan/Win.Loader.R681991 (2024.11.16.03)
– Trojan/Win.Agent.C5628462 (2024.05.31.02)
– Trojan/Win.Loader.C5666988 (2024.09.08.03)
– Trojan/Win.Launcher.C5666991 (2024.09.08.03)
– Trojan/Win.Loader.C5666994 (2024.09.10.00)
– Dropper/Win.Agent.C5692128 (2024.11.10.03)
– Trojan/Win.Launcher.C5692134 (2024.11.11.00)
– Trojan/Win.Loader.C5692141 (2024.11.11.00)
– Data/BIN.EncPe (2024.11.11.03)
– Data/BIN.Shellcode (2024.05.29.02)

MD5

11529c342d150647a020145da873ea98

127c722bf973d850ee085ab863257692

26ff6fac8ac83ece36b95442f5bb81ce

30c0796aa5d7ba9ea3790a0210ec9840

314f239e2ba3fbf6b9e6b4f13ee043e7

Additional IOCs are available on AhnLab TIP.

FQDN

ac[.]metyp9[.]com

server[.]microsoftsvc[.]com

Additional IOCs are available on AhnLab TIP.