nao-sec.org

By nao_sec

Published: 2019-04-27 · Archived: 2026-04-06 00:07:19 UTC

Amedey is installed by msiexec.exe when you open a malicious excel file. From the document file technique, the threat actor is considered TA505.

First payload is packed. Extract the original PE using the hollows_hunter mode of tknk_scanner.

The dumped PE is compiled with MinGW.

The main function is as follows.

The _Z6aBasici function is as follows.

Some important parameters are encoded. However, the encoding algorithm is very simple.

Finally, we analyze the decoded string and the name of the function in which it was used.

Here is the simple python script.

```
 '''
domain=[0x9F, 0xD4, 0xCA, 0xC5, 0x9C, 0x9E, 0xA7, 0x98, 0xA5, 0x67, 0x96, 0xD1, 0x9D]
AutoRunCmdr=[0x8A, 0xAA, 0xA9, 0x84, 0x74, 0x7D, 0x7D, 0x54, 0x58, 0x81, 0x7E, 0xA5, 0x85, 0xC0, 0x87, 0xA8, 0x9
AV00=[0x79, 0xBB, 0xA3, 0xB7, 0x87, 0x59, 0x8C, 0xA3, 0x9C, 0xAD, 0xAA, 0xC3, 0xA2, 0xC9]#AV00
AV01=[0x79, 0xDB, 0xCB, 0xD6, 0x94]
AV02=[0x83, 0xC6, 0xD5, 0xD4, 0x98, 0xAB, 0xAC, 0x9F, 0xAF, 0x59, 0x7F, 0xC3, 0x92]
AV03=[0x7D, 0xB8, 0xA7, 0xB8]
AV04=[0x88, 0xC6, 0xD0, 0xC8, 0x94, 0x59, 0x8C, 0x99, 0x99, 0xAE, 0xA5, 0xCB, 0xA4, 0xDD]
AV05=[0x7C, 0xD4, 0xC5, 0xD8, 0xA2, 0xAB, 0x59, 0x8B, 0x9B, 0x9B]
AV06=[0x79, 0xBB, 0xA9]
AV07=[0x6B, 0x9B, 0x92, 0xB8, 0xA2, 0xAD, 0x9A, 0xA0, 0x89, 0x9E, 0x96, 0xD7, 0xA2, 0xCD, 0xA8, 0xB2]
AV08=[0x7A, 0xCE, 0xD6, 0xC8, 0x98, 0x9F, 0x9E, 0xA2, 0x9A, 0x9E, 0xA5]
AV09=[0x86, 0xD4, 0xD4, 0xD8, 0xA2, 0xA7]
AV10=[0x8B, 0xD4, 0xD2, 0xCC, 0xA2, 0xAC]
AV11=[0x7B, 0xD4, 0xCF, 0xD3, 0x97, 0xA8]
CMD0=[0x74, 0xC8, 0xA0]
CMD1=[0x74, 0xC9, 0xA0]
DLL=[0x9C, 0xD1, 0xCE]
DropDir=[0x9E, 0x9B, 0x96, 0xC5, 0x67, 0x6B, 0x71, 0x98, 0x9C, 0x9D]
DropName=[0x9B, 0xD2, 0xD7, 0xC5, 0x9F, 0xAB, 0x9C, 0x62, 0x9B, 0xB1, 0x98]
exe=[0x9D, 0xDD, 0xC7]
GetProgDir=[0x88, 0xD7, 0xD1, 0xCB, 0xA5, 0x9A, 0xA6, 0x78, 0x97, 0xAD, 0x94, 0xBE]
OS_AR0=[0xA3, 0xCA, 0xD4, 0xD2, 0x98, 0xA5, 0x6C, 0x66, 0x64, 0x9D, 0x9F, 0xCE]
```

```
OS_AR1=[0x7F, 0xCA, 0xD6, 0xB2, 0x94, 0xAD, 0xA2, 0xAA, 0x9B, 0x8C, 0xAC, 0xD5, 0xA4, 0xC9, 0xA1, 0x82, 0xA5, 0x
Param0=[0xA1, 0xC9, 0x9F]
Param1=[0x5E, 0xDB, 0xD5, 0xA1]
Param2=[0x5E, 0xC6, 0xD4, 0xA1]
Param3=[0x5E, 0xC7, 0xCB, 0xA1]
Param4=[0x5E, 0xD1, 0xD8, 0xA1]
Param5=[0x5E, 0xD4, 0xD5, 0xA1]
Param6=[0x5E, 0xC6, 0xD8, 0xA1]
Param7=[0x5E, 0xD5, 0xC5, 0xA1]
Param8=[0x5E, 0xDA, 0xD0, 0xA1]
Post0=[0x45, 0x6F]
Post1=[0x58, 0xAD, 0xB6, 0xB8, 0x83, 0x68, 0x6A, 0x62, 0x67]
Post2=[0x79, 0xC8, 0xC5, 0xC9, 0xA3, 0xAD, 0x73, 0x54, 0x60, 0x68, 0x5D]
Post3=[0x7B, 0xD4, 0xD0, 0xD8, 0x98, 0xA7, 0xAD, 0x61, 0x8A, 0xB2, 0xA3, 0xC7, 0x6A, 0x84, 0x95, 0xA9, 0xA7, 0xA
Post4=[0x80, 0xD4, 0xD5, 0xD8, 0x6D, 0x59]
Post5=[0x7B, 0xD4, 0xD0, 0xD8, 0x98, 0xA7, 0xAD, 0x61, 0x82, 0x9E, 0xA1, 0xC9, 0xA4, 0xCC, 0x6E, 0x59]
Post6=[0x88, 0xB4, 0xB5, 0xB8, 0x53, 0x68]
RunAs=[0xAA, 0xDA, 0xD0, 0xC5, 0xA6]
RunDll_0=[0xAA, 0xDA, 0xD0, 0xC8, 0x9F, 0xA5, 0x6C, 0x66, 0x64, 0x9E, 0xAB, 0xC7, 0x50]
Script=[0xA8, 0xD5, 0xCD, 0x93, 0x9C, 0xA7, 0x9D, 0x99, 0xAE, 0x67, 0xA3, 0xCA, 0xA0]
Shell=[0x8B, 0xAD, 0xA7, 0xB0, 0x7F, 0x6C, 0x6B, 0x62, 0x7A, 0x85, 0x7F]
TimeOut=[0x60, 0xEA, 0x00, 0x00, 0x44]
URLMon_0=[0xAD, 0xD7, 0xCE, 0xD1, 0xA2, 0xA7]
URLMon_1=[0x8D, 0xB7, 0xAE, 0xA8, 0xA2, 0xB0, 0xA7, 0xA0, 0xA5, 0x9A, 0x97, 0xB6, 0x9F, 0xAA, 0x9D, 0xA5, 0x9C,
Vers=[0x69, 0x93, 0x94, 0x96]
ZoneIdent =[0x72, 0xBF, 0xD1, 0xD2, 0x98, 0x67, 0x82, 0x98, 0x9B, 0xA7, 0xA7, 0xCB, 0x96, 0xCD, 0x99, 0xAB]
'''

encoded_str=[0x9F, 0xD4, 0xCA, 0xC5, 0x9C, 0x9E, 0xA7, 0x98, 0xA5, 0x67, 0x96, 0xD1, 0x9D]

Key="8ebd3994693b0d4976021758c2d7bff793b0d4976021758c2d7bff7"
c=0

while(1):
    length = len(encoded_str)
    if length <= c:
        break
    length = len(Key);
    print(chr(encoded_str[c] - ord(Key[c % length])), end='')
    #print(encoded_str[c] - ord(Key[c % length]), end='')
    c += 1
```

Source: https://nao-sec.org/2019/04/Analyzing-amadey.html