Chinese Actor APT target Ministry of Justice Vietnamese

medium.com/@Sebdraven/chineses-actor-apt-target-ministry-of-justice-vietnamese-14f13cc1c906

May 10, 2019

Sebdraven

May 11

With the new RTF exploit using 8.t to store theirs payloads, many malicious document have targeted to Vietnam. One document is very interesting because its target specifically the Ministry of Justice.

Analyze

The recipients of the document 41f0757ca4367f22b0aece325208799135c96ebe1dcafcd752d3f3c8dd4a5ccf 8.t are (at the end of the document):

the deputy minister;
- the units under the ministry;
- police of provinces and cities directly under the central government;
- Department of Inspection of Legal Documents of the Ministry of Justice;
- Official Journal, Government Electronic Portal, Ministry of Public Security Portal;
- Archive: VT, C06 (P1).

The document exploits Equation Editor starts application (CVE-2017–11882) to decode the 8.t in memory, after fork to install two files:

C:\Users\admin\AppData\Local\Temp\wsc.dll
4e88f8a3c3be45e0a59a8868f2b2ace51754fcdbfa9ab618e3d9d0e17831990f

and

C:\Users\admin\AppData\Local\Temp\wsc_proxy.exe
1948bb0df11f768d6dd30ae7ecec5550db7c817d09cb31b5e2cee9b86a4047da

The malware is a dll, it seems to be Gh0st RAT.

https://app.any.run/tasks/5715cfe3-2550-4808-aad0-1ea4c4fc7a88

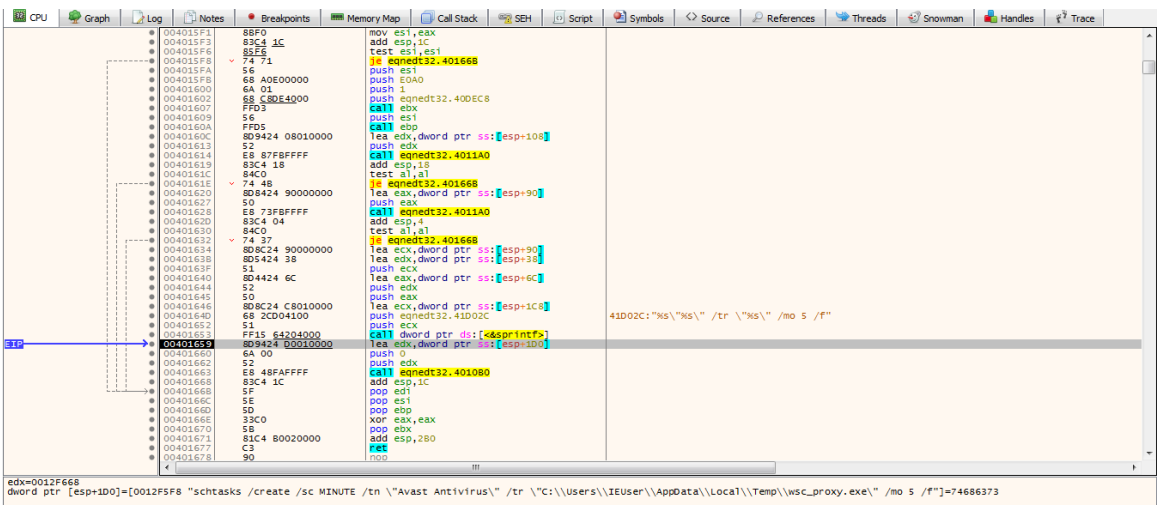
An to start the malware, it uses a side loading technics with a scheduled Task.

The exe call in the entry loads dynamically wsc.dll and call the function _run@4

Decompile: entry - (wsc_proxy.bin)

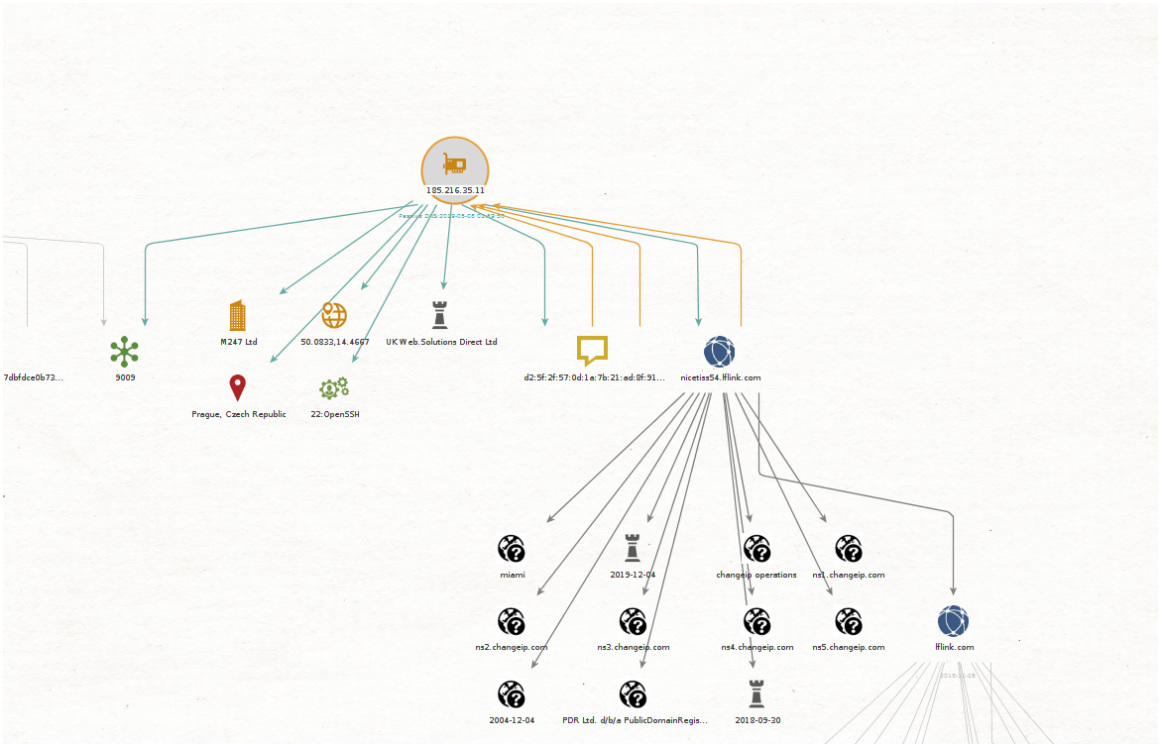
```
1
2  void entry(void)
3
4  {
5    code *pcVar1;
6    HMODULE hModule;
7    FARPROC pVar2;
8    LPWSTR pWVar3;
9    UINT uExitCode;
10
11   hModule = GetModuleHandleW(L"kernel32.dll");
12   pVar2 = GetProcAddress(hModule,"SetDefaultDllDirectories");
13   SetDllDirectoryW(L"");
14   if (pVar2 != (FARPROC)0x0) {
15     (*pVar2)(0x1000);
16   }
17   hModule = LoadLibraryW(L"wsc.dll");
18   if (hModule == (HMODULE)0x0) {
19     uExitCode = GetLastError();
20   }
21   else {
22     pVar2 = GetProcAddress(hModule,"_run@4");
23     if (pVar2 == (FARPROC)0x0) {
24       uExitCode = GetLastError();
25       FreeLibrary(hModule);
26     }
27     else {
28       pWVar3 = GetCommandLineW();
29       uExitCode = (*pVar2)(pWVar3);
30       FreeLibrary(hModule);
31     }
32   }
33   ExitProcess(uExitCode);
34   pcVar1 = (code *)swi(3);
35   (*pcVar1)();
36   return;
37 }
38
```

Side Loading



Scheduled Task

The RAT tries to connect to nicetiss54.lflink.coml185.216.35.11.



Threat Intelligence Consideration

We have the same TTps and victimology like Goblin Panda:

- Officials Vietnameses
- Side Loading
- 8.t RTF kit exploit
- a dynamic dns name

But the payload has changed and the launch of the backdoor has changed.

It’s used a scheduled task.

Usually this group uses NewCoreRat.

IOCs

Main object-
“41f0757ca4367f22b0aece325208799135c96ebe1dcafcd752d3f3c8dd4a5ccf”
sha256 41f0757ca4367f22b0aece325208799135c96ebe1dcafcd752d3f3c8dd4a5ccf
sha1 6e670a837970a1fb4161d77d5f720d318d7e4dbc
md5 f34514118eb4689560cd6c0c654f26d9

Dropped executable file

sha256 C:\Users\admin\AppData\Local\Temp\wsc.dll
4e88f8a3c3be45e0a59a8868f2b2ace51754fcdbfa9ab618e3d9d0e17831990f

sha256 C:\Users\admin\AppData\Local\Temp\wsc_proxy.exe
1948bb0df11f768d6dd30ae7ecec5550db7c817d09cb31b5e2cee9b86a4047da

DNS requests
domain nicetiss54.lflink.com

Connections
ip 185.216.35.11