Sebdraven Follow
OSINT, Python,Malware Analysis, Botnet Tracker, SIEM and IPS/IDS and Threats Expert / co-organizer #BotConf / co-creator of #FastIR
Aug 2 · 4 min read

Goblin Panda against the Bears

During my last investigation (here), I've found two RTFs malware documents with the same techniques of exploitation of CVE-2017–11882:

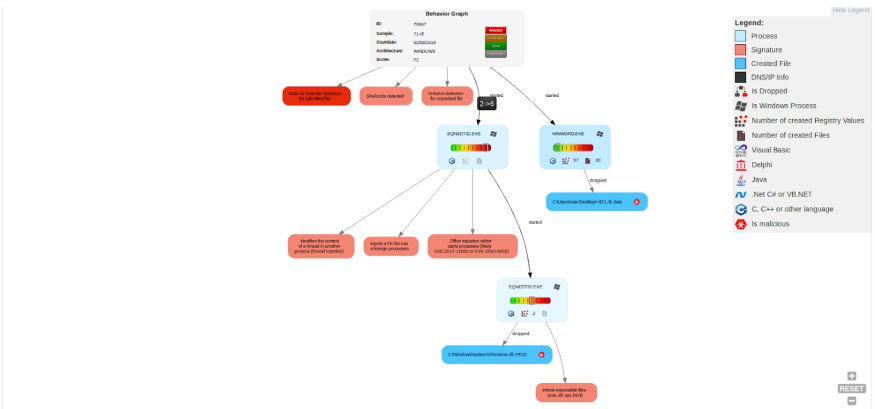
A file 8.t in %TMP% with Package Ole Object

The same loop of decryption

The same runPE after overwriting in memory EQNEDT32.exe

But the payload is really different. It's not a version of PlugX but a version of Sisfider studied by Ncc group.
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8570-rtf-and-the-sisfader-rat/

With the behaviour graph of Joe Sandbox, we can recognize the same interactions with operating system than my last article and the paper of NCC Group.



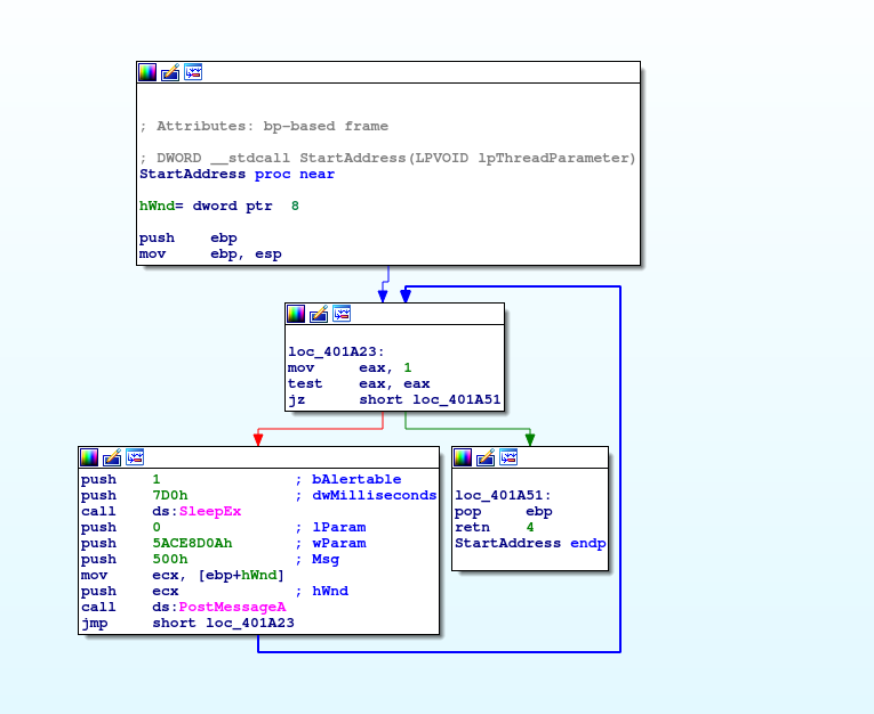
Behaviour of malwares

The difference with the version studied by NCC Group is the Package Ole Object. In the article of NCC Group, the researchers talk about a SCT File and many javascript manipulations for dropping the RAT on the disk and to start it.

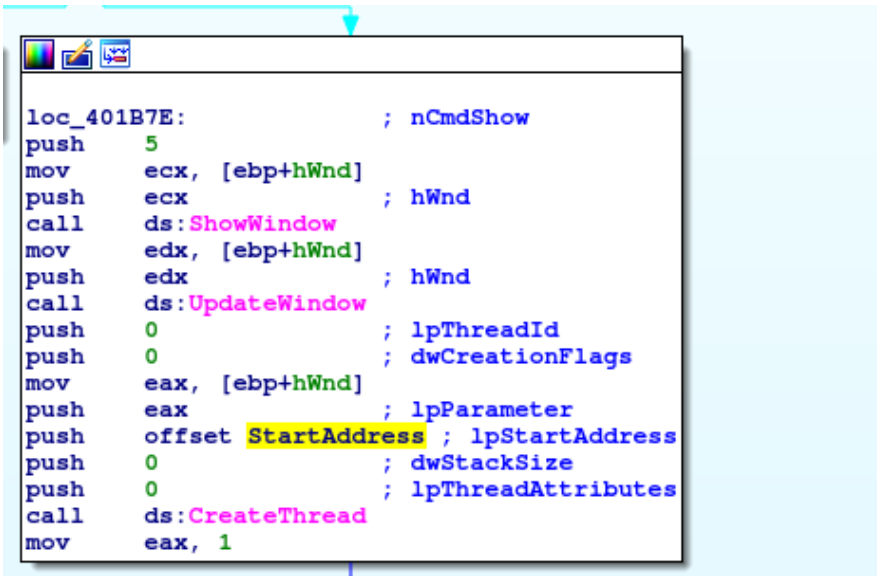
Here, the payload is encrypted in 8.t file

If we analyze EQNEDT32.exe overwritten to recognise the payload, we have the same technics anti emulation with the same value.

In a thread, the process posts in a queue the value 5ACE8D0Ah.



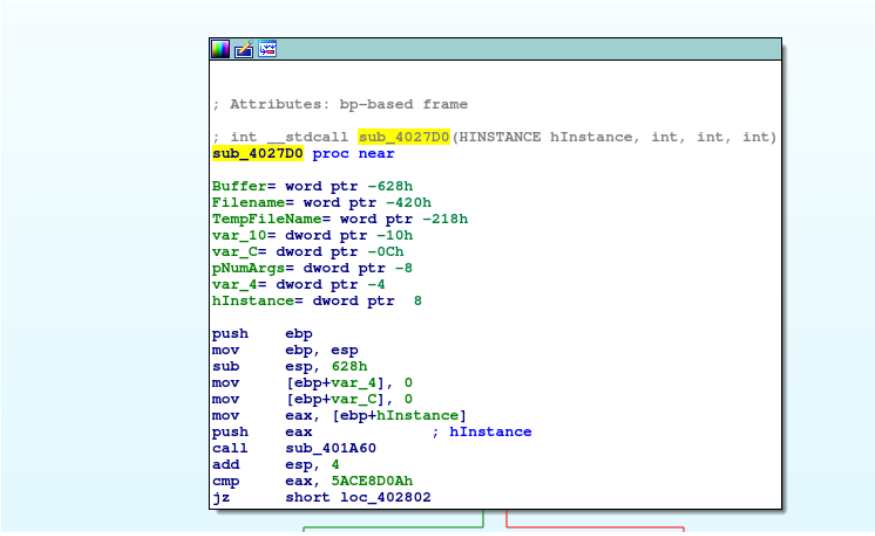
Anti emulation tricks



Anti emulation tricks

The verification is calling GetMessage() and the value is stored in EAX in the function sub_401A60.

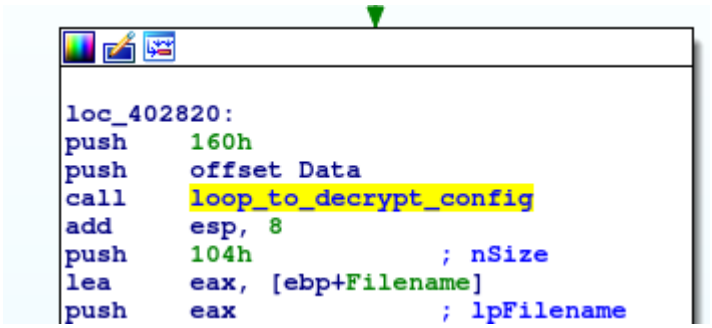
The comparaison is made in the calling function sub_4027D0.



```
; Attributes: bp-based frame

; int __stdcall sub_4027D0(HINSTANCE hInstance, int, int, int)
sub_4027D0 proc near

Buffer= word ptr -628h
Filename= word ptr -420h
TempFileName= word ptr -218h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
pNumArgs= dword ptr -8
var_4= dword ptr -4
hInstance= dword ptr  8

push    ebp
mov     ebp, esp
sub     esp, 628h
mov     [ebp+var_4], 0
mov     [ebp+var_C], 0
mov     eax, [ebp+hInstance]
push    eax             ; hInstance
call    sub_401A60
add     esp, 4
cmp     eax, 5ACE8D0Ah
jz      short loc_402802
```

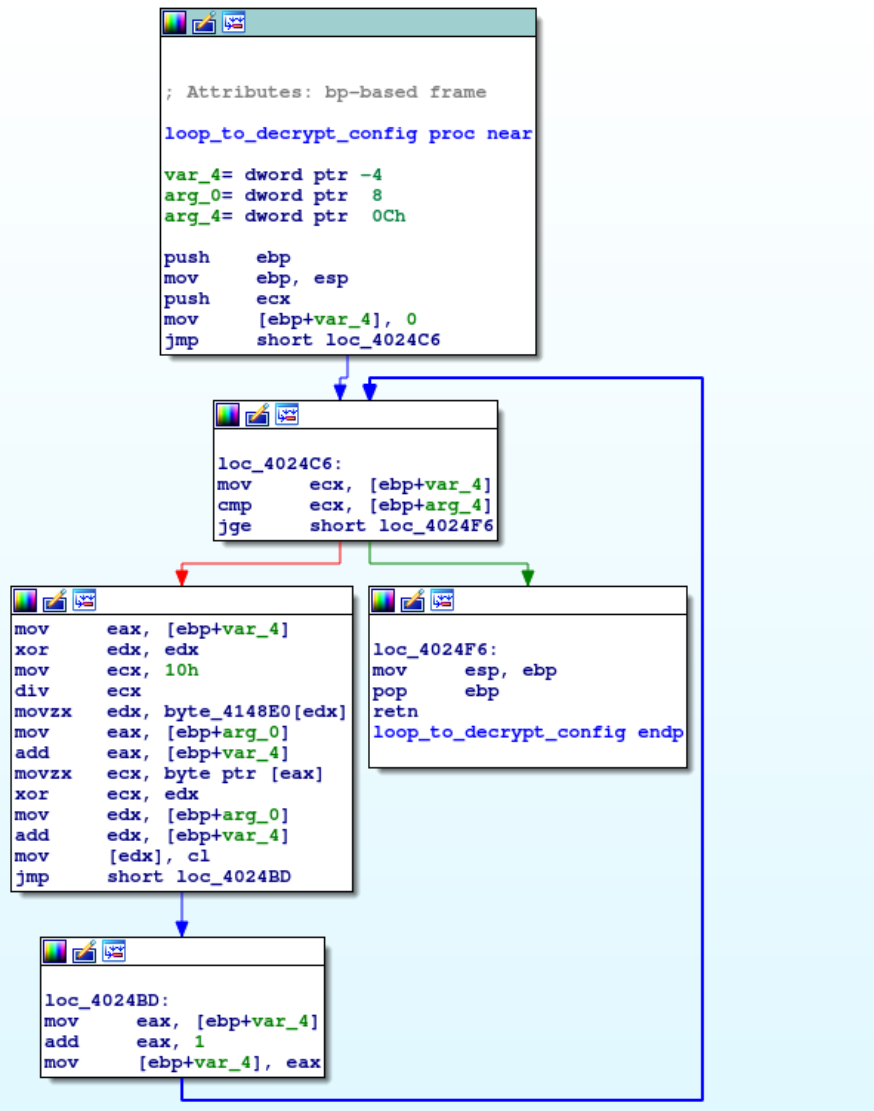
Anti emulation tricks verification

Juste after we found again the loop of decryption for the config.



```
loc_402820:
push    160h
push    offset Data
call    loop_to_decrypt_config
add     esp, 8
push    104h            ; nSize
lea     eax, [ebp+Filename]
push    eax             ; lpFilename
```

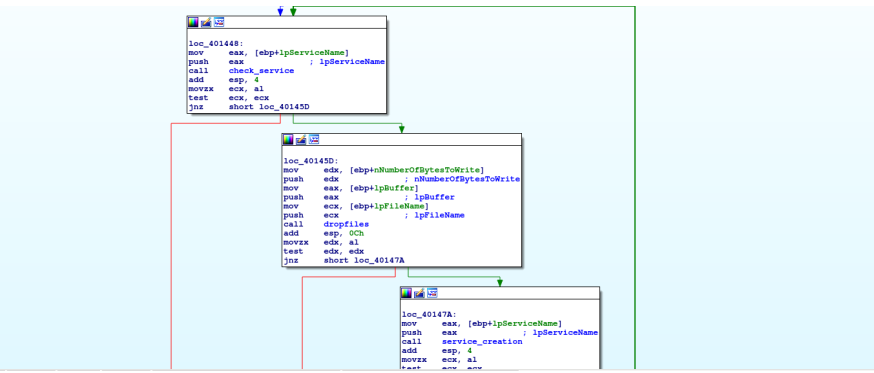
call to loop of decryption



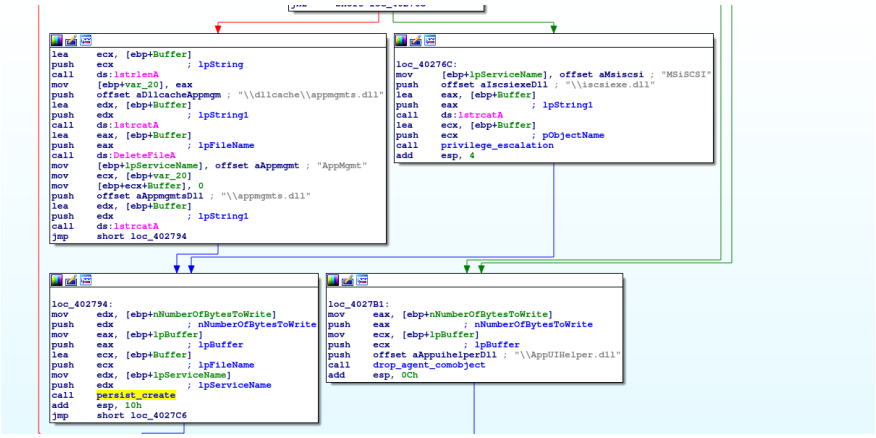
Loop of decrypting config

It's the same algorithm described: a simple XOR loop with rolling key.

The mechanism of persistent is the same with a service creation just after dropping differents files and a privilege escalation.



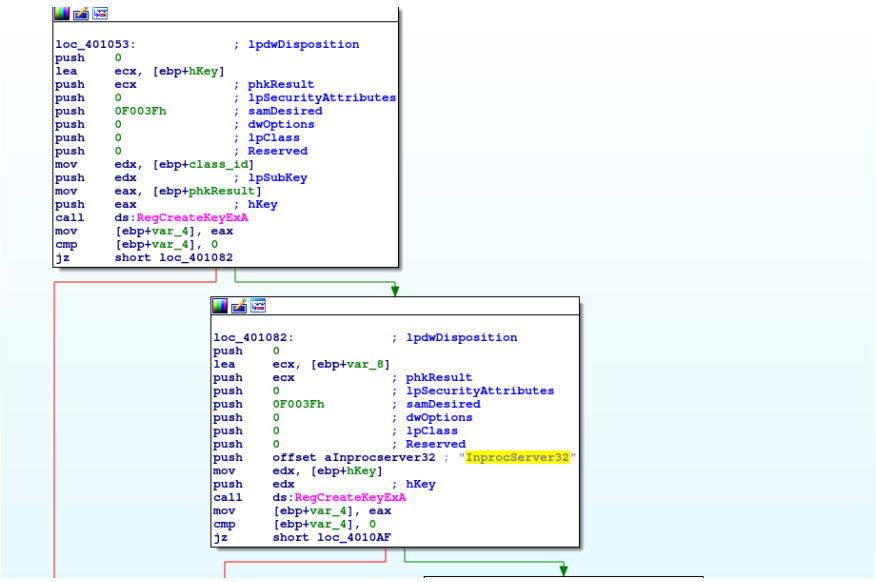
We found the same name of the dll files.



Persistence and loading agent

The malware overwrite the comobject

{9BA05972-F6A8–11CF-A442–00A0C90A8F39} to execute when this com object is called to make a persistence



ComObject Adding

All evidences show is the same payload Sisfader RAT.

Threat Intel

The toolset for exploiting the module of equation is the same using of the compromission for Vietnameses Officials used by Goblin Panda. (APT 1937CN)

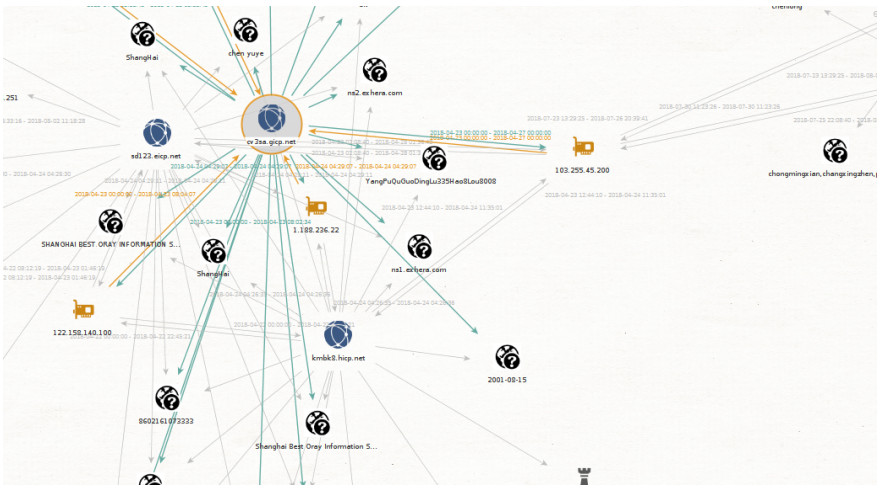
If we check the domain contacted by EQNEDT32.exe is kmbk8.hicp.net. This address is a real good pivot. It makes the link with Goblin Panda and SisFader RAT.

And the infrastructure is very interesting this domains resolved on three IPs:

122.158.140.100, 122.158.140.100 and 103.255.45.200

Theses addresses can permit to found others domains:

Sd123.eicp.net with new IP 180.131.58.9 and cv3sa.gicp.net with new IP 1.188.233.201

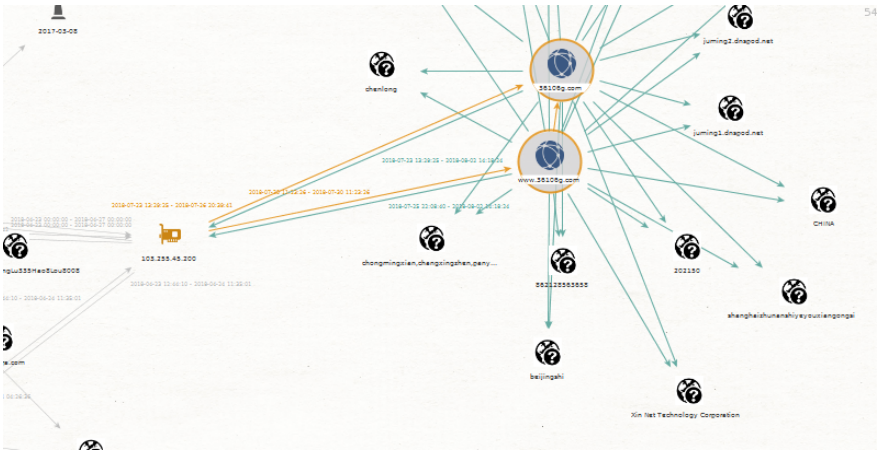


Infrastructure

The Ip Address 103.255.45.200 has two domains:

www.36106g.com

36106g.com

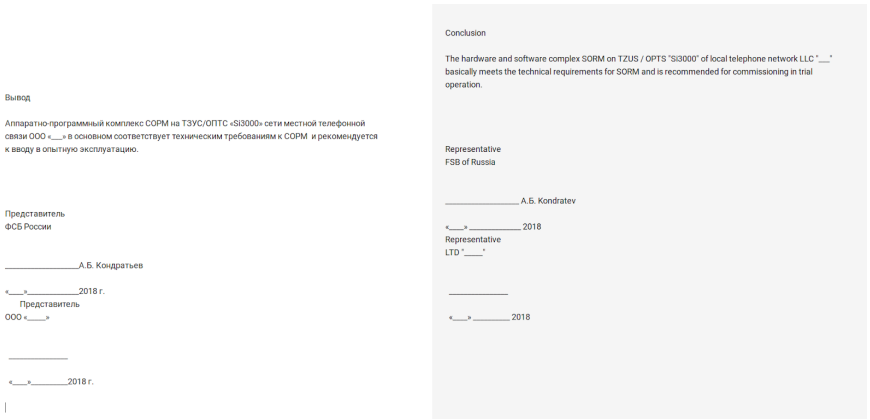


Infrastructure

All infrastructure is based at Shanghai.

The victims are different than the Vietnameses campaign.

They targeted Telecom Firms pretending to be the Intelligence Service of Russia (FSB)



Вывод

Аппаратно-программный комплекс СОРМ на ТЗУС/ОПТС «SI3000» сети местной телефонной связи ООО «___» в основном соответствует техническим требованиям к СОРМ и рекомендуется к вводу в опытную эксплуатацию.

Представитель
ФСБ России

_____А.Б. Кондратьев

«____»_____2018 г.

Представитель
ООО «_____»

_____

«____»_____2018 г.

Conclusion

The hardware and software complex SORM on TZUS / OPTS "SI3000" of local telephone network LLC "___" basically meets the technical requirements for SORM and is recommended for commissioning in trial operation.

Representative
FSB of Russia

_____ A.B. Kondratev

«____» _____ 2018

Representative
LTD "____"

_____

«____» _____ 2018

RTFs content

So Gobelin Panda targets like the report of CrowdStrike https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf he telecom industries in Russia.

Conclusion

Goblin Panda used Sisfader RAT to target the Telecom Firms russian with the same exploitation techniques for Vietnameses Officials. They updated theirs technics than the report of NCC group.

IOCs:

Rtfs:

722e5d3dcc8945f69135dc381a15b5cad9723cd11f7ea20991a3ab867d9428c7

71c94bb0944eb59cb79726b20177fb2cd84bf9b4d33b0efbe9aed58bb2b43e9c

Domains IP:

1.188.233.201 cv3sa.gicp.net

1.188.236.22 cv3sa.gicp.net

1.188.236.22 kmbk8.hicp.net

1.188.236.22 sd123.eicp.net

103.255.45.200 36106g.com

103.255.45.200 cv3sa.gicp.net

103.255.45.200 kmbk8.hicp.net

103.255.45.200 sd123.eicp.net

103.255.45.200 www.36106g.com

122.158.140.100 cv3sa.gicp.net

122.158.140.100 kmbk8.hicp.net

122.158.140.100 sd123.eicp.net