APT37 NEW YEAR ATTACK

https://cyberstruggle.org

NAVY SEALs of Cyber World

EXECUTIVE SUMMARY

This is the analysis report of a sample which is tied to a campaign conducted against *South Korean Unification Ministry - 1 January 2019*. We have identified that aforementioned malware possess information collection capabilities. We also suspect that the malware possesses remote command execution capabilities. Anti analysis techniques are employed. Considering this information, we are confident that the implant functions as a spyware. Although having several distinctive features, tradecraft of this implant is similar to those from "Operation Kimsuky".

GENERAL INFORMATION

Name (UTF-8)	Type	MD5
¦¤Ãª ¢+-Ô¬_.exe (Main Sample)	PE32 executable (GUI) Intel 80386	e9c1dec196441577816d85dc304d702d
Resources/SRV/129 (HncChecker.dll)	PE32 executable (DLL) (GUI) x86-64	8058beb593166f1cc16d6cd3f6784577
Resources/SRV/130 (HncChecker.dll)	PE32 executable (DLL) (GUI) Intel 80386	a65b5e6f104d01916feadd180c8161c2
Resources/SRV/131 (190101-½Å³â»ç_Æò°¡.hwp)	Hangul (Korean) Word Processor File 5.x	07fba69097eff4f0773cff8414f72a80

FILE SECTIONS

NAME	VSIZE	RSIZE	ENTROPY	MD5
.TEXT	32752	32768	6.61	9e1834cb74f3a3d2112b89886d57a298
.RDATA	14328	14336	5.91	8d19678981eac0f477f873dda1a86877
.DATA	14784	5120	3.21	564d9be0c62a0ea837e794ffb8ddedb8
.DATA0	340032	340480	7.95	95b124da70660628261879c6ee701224
.TLS	24	512	0	bf619eac0cdf3f68d496ea9344137e8b
.DATA1	76576	76800	7.62	6c8ff14aea5d965d3dd9a5bbb9a07512
.RELOC	3568	3584	6.25	34f3d1e4a2927676f669b90f2c157561
.RSRC	1353135	1353216	7.05	8a57b5e599a3b5f4121f328b42e9fb16

ACTIVITY SUMMARY

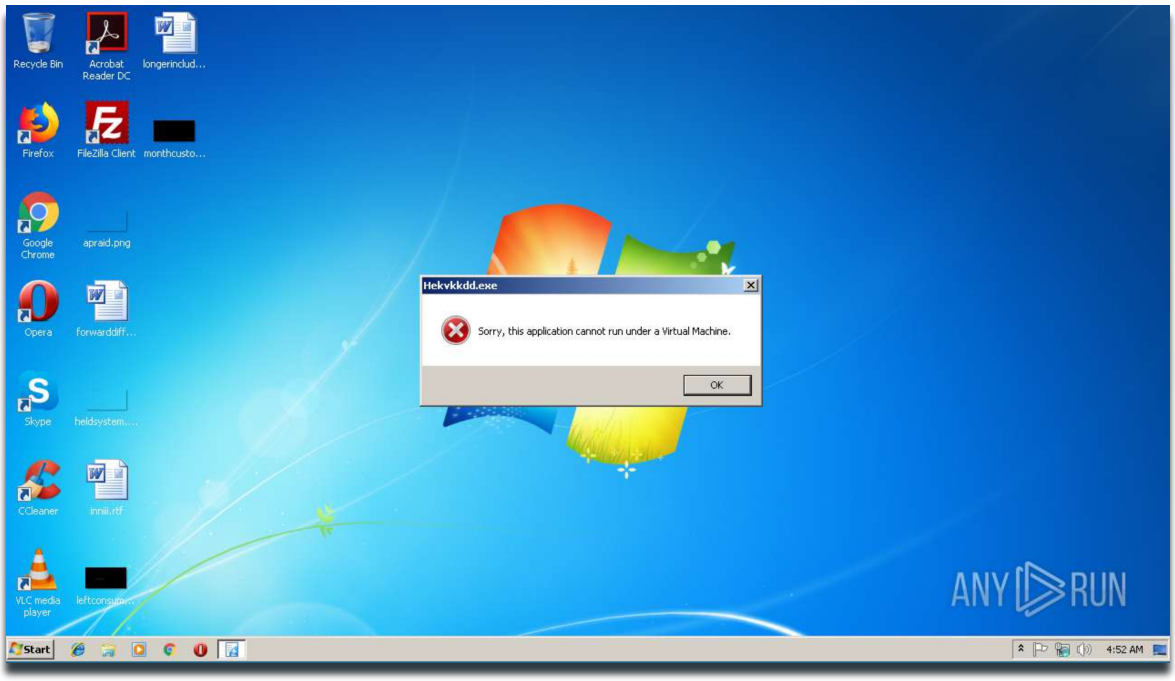
1. Drop HWP document in the same directory
2. Attempt to open HWP document
3. Drop **%TEMP%\[0-9A-F]{4}.dll**
4. Load dropped DLL
5. Invoke EmptySub Method
    - Drop **C:\ProgramData\Hnc\HncChecker.dll**
    - Create **C:\ProgramData\Hnc\serial.info**
    - Create **C:\ProgramData\Hnc\status.dat**
    - Add New Service
        i. **HKLM\System\CurrentControlSet\Services\HncCheck**
    - Log keystrokes
        i. Write into **C:\ProgramData\Hnc\userdata.cab**

ANALYSIS

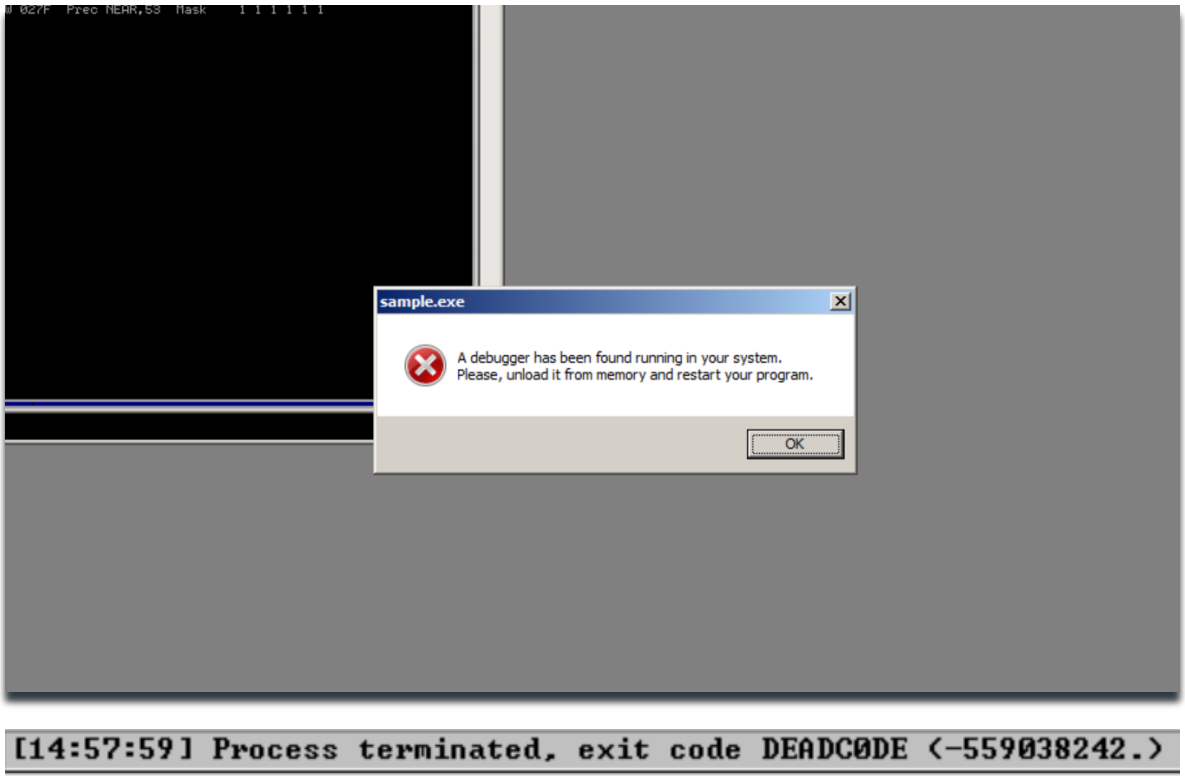
A1 SAMPLE POSSESS ANTI ANALYSIS FEATURES

Source: **Static Features, Signature Match, Dynamic Behaviour**

Sample has unusual section names and sections with high entropy, which usually indicates some form of executable packing and/or encryption. Also, we observed that this sample reacts in the presence of tools and enviroment related to malware analysis. Signature scan and further behavior analysis revealed that this file is protected by a software protection tool called VMProtect.



i- Sample reacting to VM enviroment



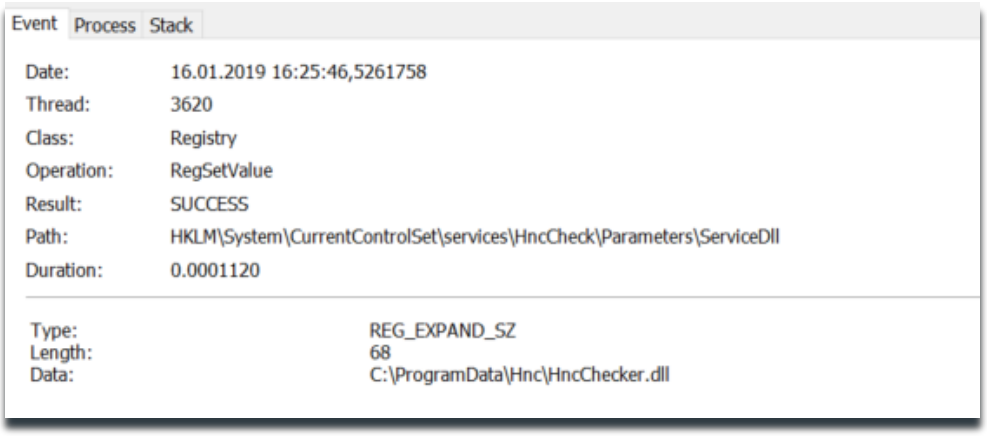
ii- Sample reacting in presence of debugger

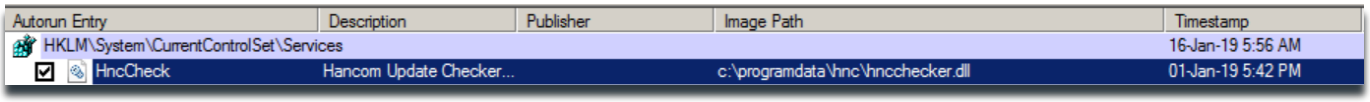
- Sample terminates itself when a debugger is attached to it.
- Sample terminates itself in the presence of a process named “Wireshark.exe”
- Sample terminates itself when it detects a Virtual Machine environment.
- Sample employs executable protection and encryption.

A1 SAMPLE CREATES A NEW SERVICE

Source: **Dynamic Behaviour**

It is observed that sample modifies system registry in an attempt to add itself as a service and ensure persistency.





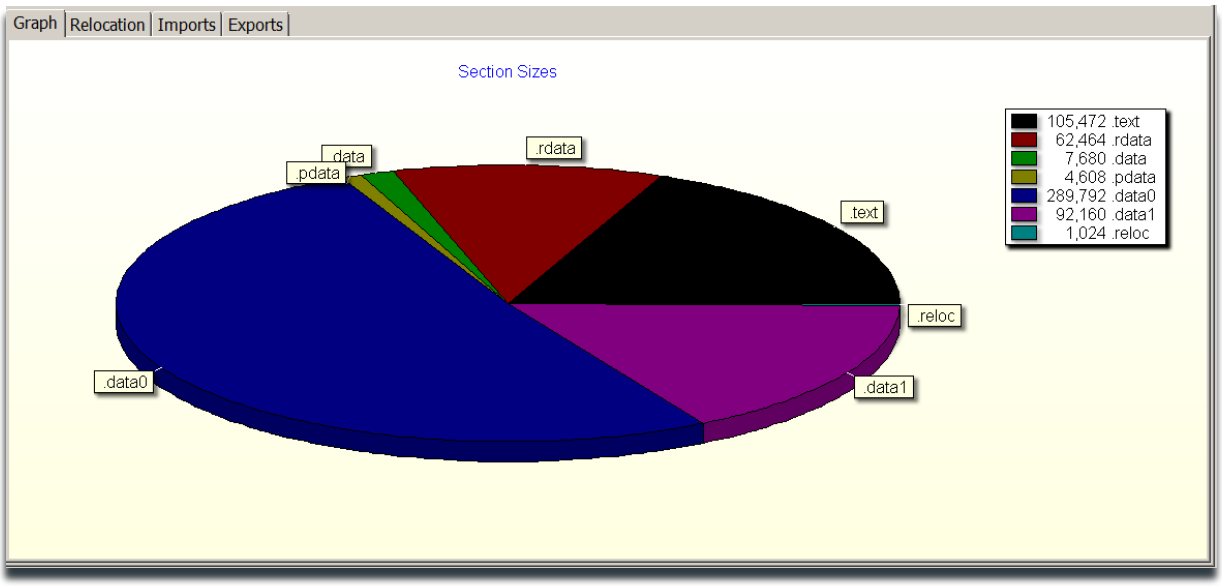
Following registry keys are modified:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\HncCheck
- HKLM\System\CurrentControlSet\services\HncCheck\Parameters\ServiceDll

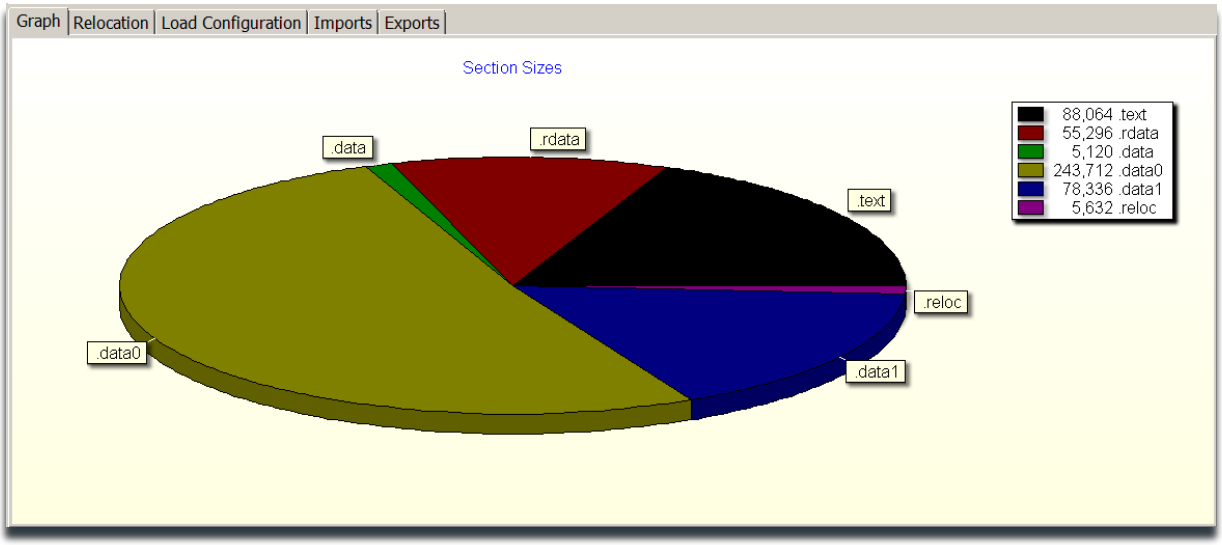
A1 SAMPLE DROPS 2ND STAGE MALWARE

Source: **Static Features, Dynamic Behaviour**

Sample contains two DLL files in its resources which is assessed to be the second stage payload. Two DLL files are essentially the same payload compiled for different architectures x86 and x86-64. It is observed that malware first determines architecture of infected system and then drops the according DLL file.



iii- First DLL

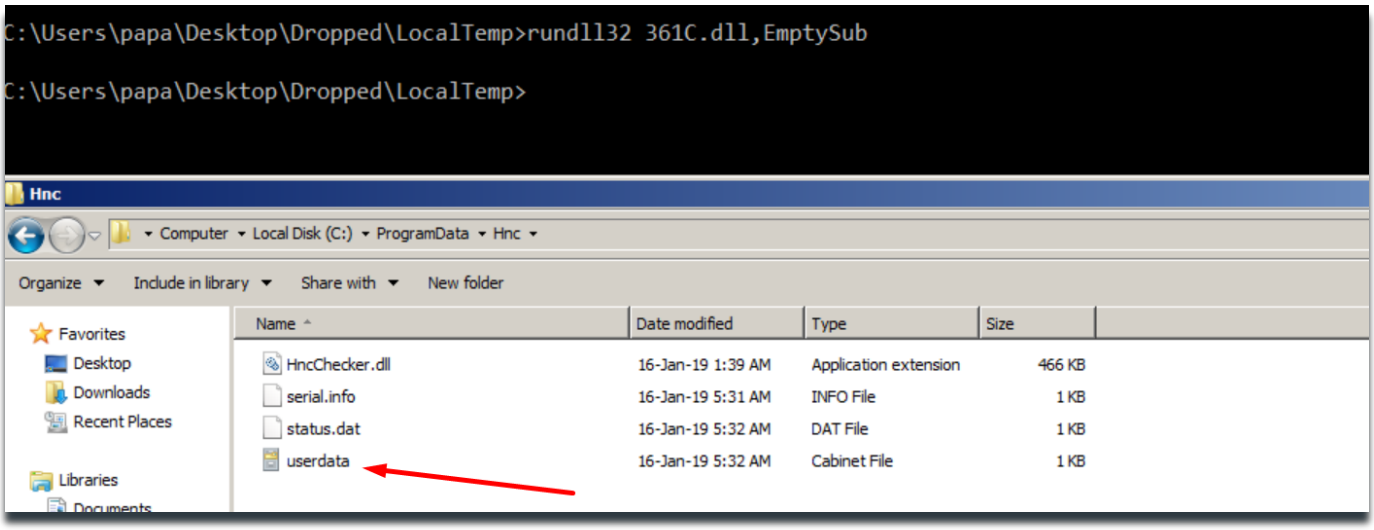


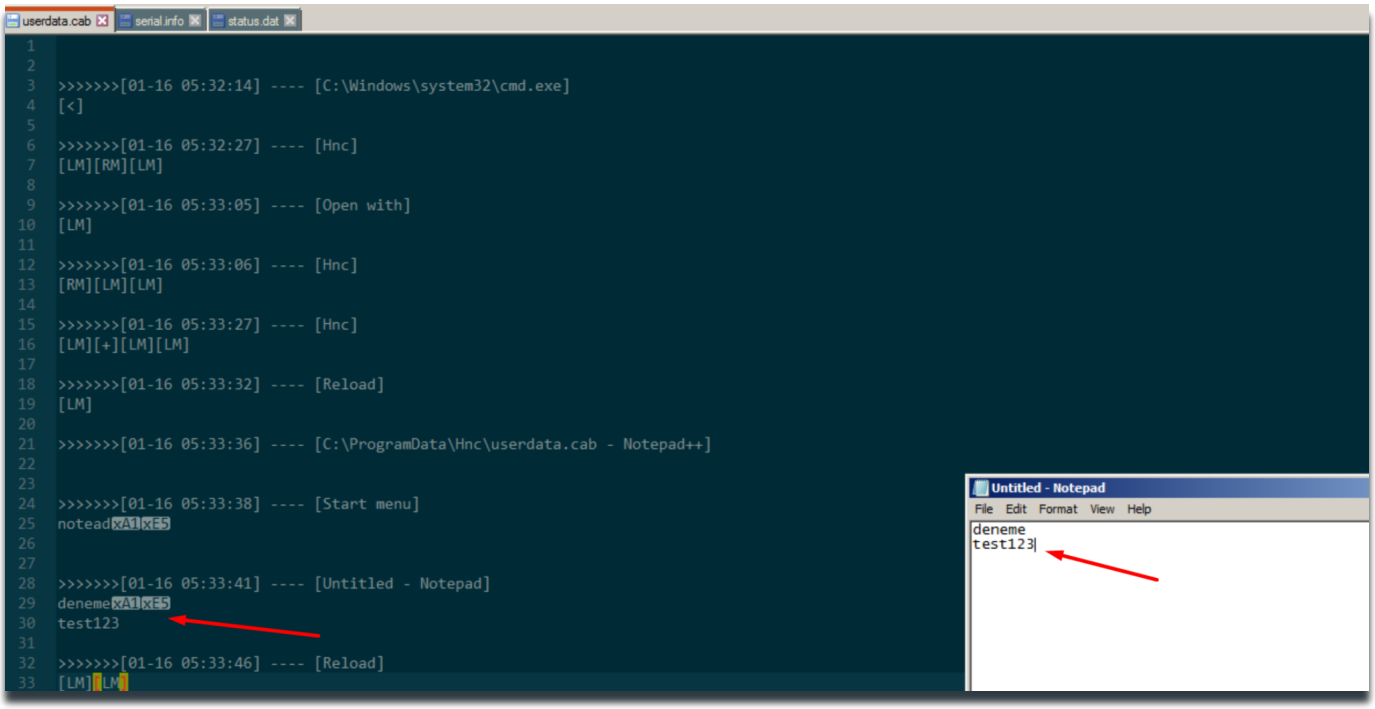
iv- Second DLL

A1 SAMPLE IS LOGGING KEYSTROKES

Source: **Dynamic Behaviour**

When **EmptySub** method of dropped **HncChecker.dll** module is invoked the malware starts to capture keystrokes and writes to local file **C:\ProgramData\Hnc\userdata.cab** it has created. Although it is not observed we suspect that this malware also contains other collection capabilities.





v- Malware logging keystrokes in local file

F2 SAMPLE IS COMMUNICATING THROUGH ONLINE SERVICES

Source: **Strings**

We have encountered strings indicating HTTP requests to API of an online E-mail service. This could mean that malware is communicating with its command and control servers through this E-mail service. We also suspect that malware could be using this service for file transfer. However, we have not yet observed this behavior in dynamic analysis environment.

```
/accounts/srp.do?slevel=1&rid=
&srplm1=
url=http%3A%2F%2Fmail2.daum.net%2Fhanmailex%2FTop.daum&relative=&weblogin=1&service=&fuid=
&slevel=1&finaldest=&reloginSeq=0&id=
```

```
document.location.replace("http://mail2.daum.net/hanmailex/Top.daum");
composerId=
&attachIndex=
&filename=
```

```
MailListing : InternetConnect failed
MailListing : HttpOpenRequest failed
GET
 HTTP/1.1
User-Agent:
Accept:
MailListing : HttpSendRequest failed
MailInboxList : InternetQueryDataAvailable error
MailInboxList : InternetReadFile failed
"id":"INBOX"
"mailsTotal":
/v2/mails?offset=0&limit=30&folderId=INBOX&labelIds=
```

vi- Strings indicating HTTP requests to online e-mail service

F2 SAMPLE HAS REMOTE COMMAND EXECUTION CAPABILITIES

Source: **Strings**

We have encountered strings indicating remote command execution capabilities. However, we have not yet observed this behavior in dynamic analysis environment.

```
Cmd[%d] : %s
```

```
Executing cmd...
```

vii- Strings indicating remote command execution capabilities

F2 SAMPLE HAS FILE TRANSFER CAPABILITIES

Source: **Strings**

We have encountered strings indicating file transfer capabilities. However, we have not yet observed this behavior in dynamic analysis environment.

```
"uploadUrl":"https://
 getting the attachFile handle error in uploading step-1
file buffer malloc error in uploading step-1
----------------------------7e222d1d50232
Content-Disposition: form-data; name="type"
attach
----------------------------7e222d1d50232
Content-Disposition: form-data; name="file"; filename="
Content-Type: text/plain
----------------------------7e222d1d50232--
uploading step-1 : InternetConnect failed
 uploading step-1 : HttpOpenRequest failed
 uploading step-1 : HttpSendRequest failed
Uploading : InternetQueryDataAvailable error
Uploading : InternetReadFile failed
```

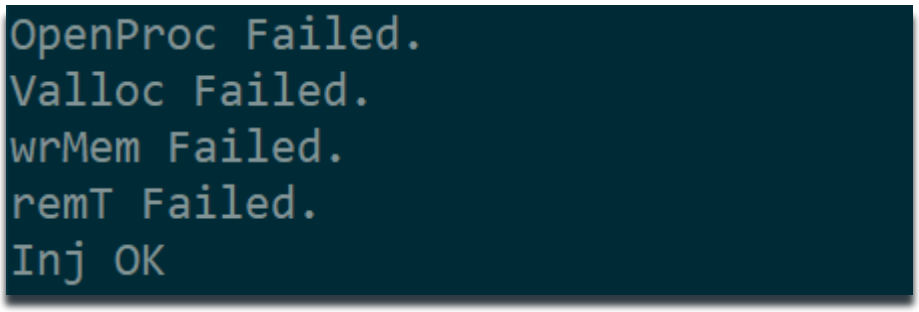
```
Cannot open file downloaded. err = %d
ExeDownCmd : Invalid Size!! %d
File Corrupted!!! %X, %s
Target : %s
```

viii- Strings indicating file transfer capabilities

F3 SAMPLE HAS PROCESS INJECTION CAPABILITIES

Source: **Strings**

We have encountered strings indicating process injection capabilities. We suspect that this malware can inject any executable into a process, on attacker's request. However, we have not yet observed this behavior in dynamic analysis environment.



ix- Strings indicating process injection capabilities

ADVERSARY TACTICS

Several tactics used by this sample is mapped accordingly with MITRE's Adversarial Tactics, Techniques & Common Knowledge.

Initial Access	Execution	Persistence	Defense Evasion	Collection	Command and Control
Spearphishing Attachment (T1193)	Execution through Module Load (T1129)	New Service (T1050)	Obfuscated Files or Information (T1027)	Input Capture (T1119)	Web Service (T1102)
	Command-Line Interface (T1059)		Process Injection (T1055)	Automated Collection (T1056)	
			Software Packing (T1045)		

DELTA GROUP

Cyber Struggle

MULTIDISCIPLINARY WARRIOR BOOTCAMP

HEADQUARTER

DAP Yapi Z Office Plaza
Floor 3, No 299

Kagithane / Istanbul
Turkey

+90-850-885-2121
info@cyberstruggle.org
www.cyberstruggle.org

RESEARCH DEVELOPMENT

ISTANBUL TECHNICAL UNIVERSITY
ARI Teknopark No:1101

Sarıyer / Istanbul
Turkey

+90-850-885-2121
info@cyberstruggle.org
www.cyberstruggle.org