Risen Ransomware / Doxware

Introduction:

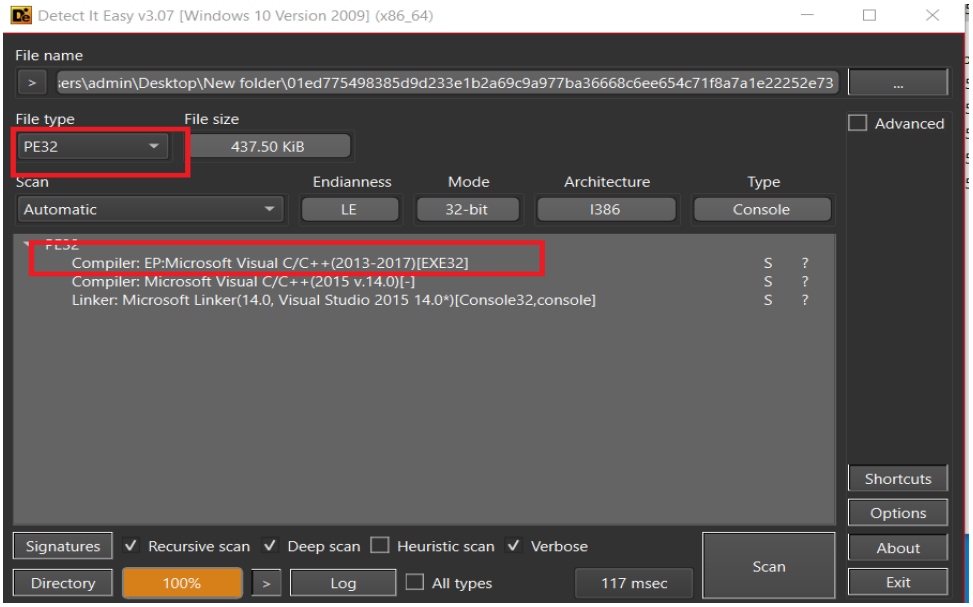
Risen Ransomware / Doxware is new malware, age of this malware is less than 2 months and less known. Regarding this Ransomware / Doxware uses the tactic called **double extortion** and by the way what Is the **Doxware** ?

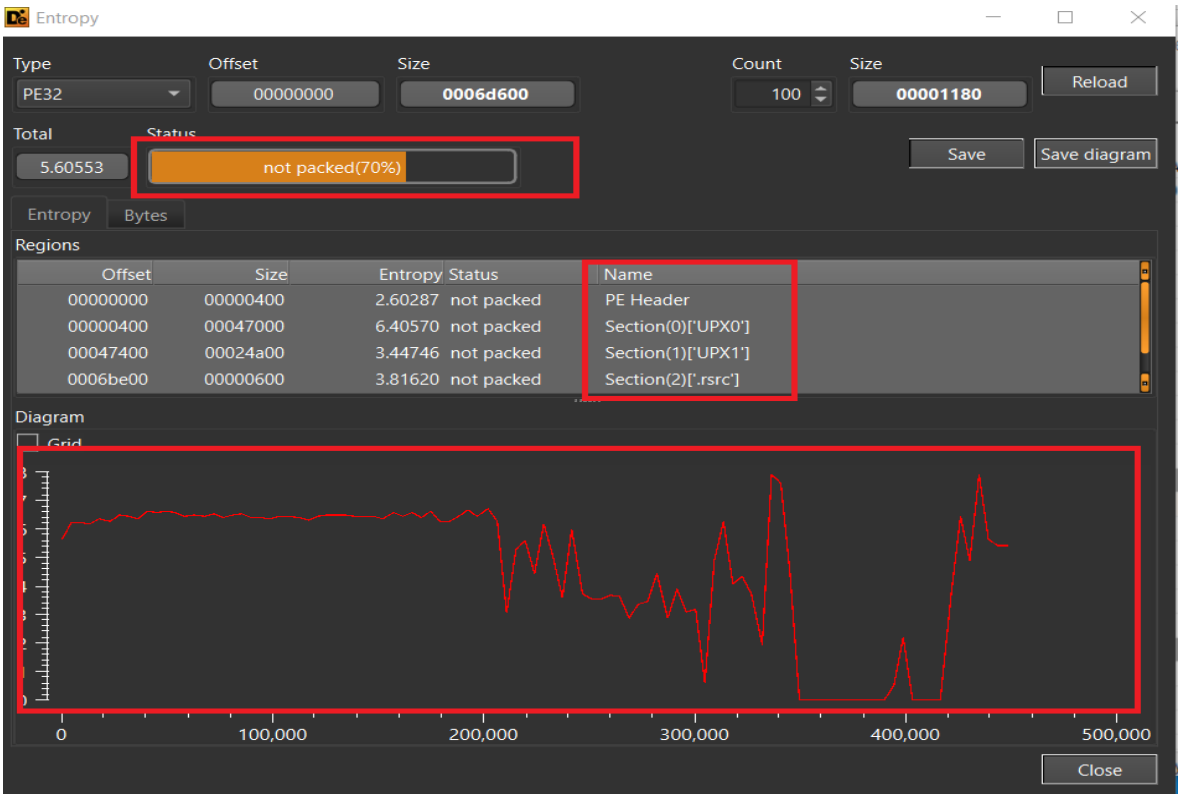
Short story about Doxware:

In 2017 there is gang **The Dark Overlord**, a notorious cybercrime group stole the a lot of intellectual property or data of Larson Studios and one of their major client is **Neflix** . The Dark Overlord Went to studios asked ransom ,if they didn't pay .They will leak their client data supposed to webservices of **Netflix** . Larson Studios Made a signed contract with gang with 50 bitcoins , The Dark Overlord reportedly signed the contract as **Adolf Hitler** but after that studios refused pay to gang because signature of studio is unclear .Later they went netflix and they paid ransom.so doxware is a software that exploits vulnerabilities in a victim's computer system to gain access to sensitive information and threaten to make it public if demands are not met. Most consider it a kind of or evolution of ransomware .Major differences between ransomware and doxware , is ransomware encrypts but doxware encrypt and leaks if they are not paid the ransom and they encrypt few or targeted files which are kind of private chats or identifiable details, because of the risk of public embarrassment or damage to a company's reputation, doxware attackers tend to demand higher ransom compared with typical ransomware developers. So they do threatening by sell/destroy or leak the data is **double extortion** tactic**.**

Hoping we are about clear Doxware ,coming to Risen ransomware , I seen this malware in X post from **AmigoA** and he had good collection of ransomware thanks to him and **Ali** as well. This malware's ancestor is blackhunt ransomware whose code is similar leaked lokibot and conti ransomware .In this article we do find how they are related ofcourse you can say code ,but code functionality and writing of many ransomware are identical ,here we discuss other IOC .so lets go to sample analysis

So regarding the sample, looks straight forward by its metadata I can assume it is dump of Scylla. after checking their sections I doubt that ,we don't have any parent leads for this sample .lets see more about it





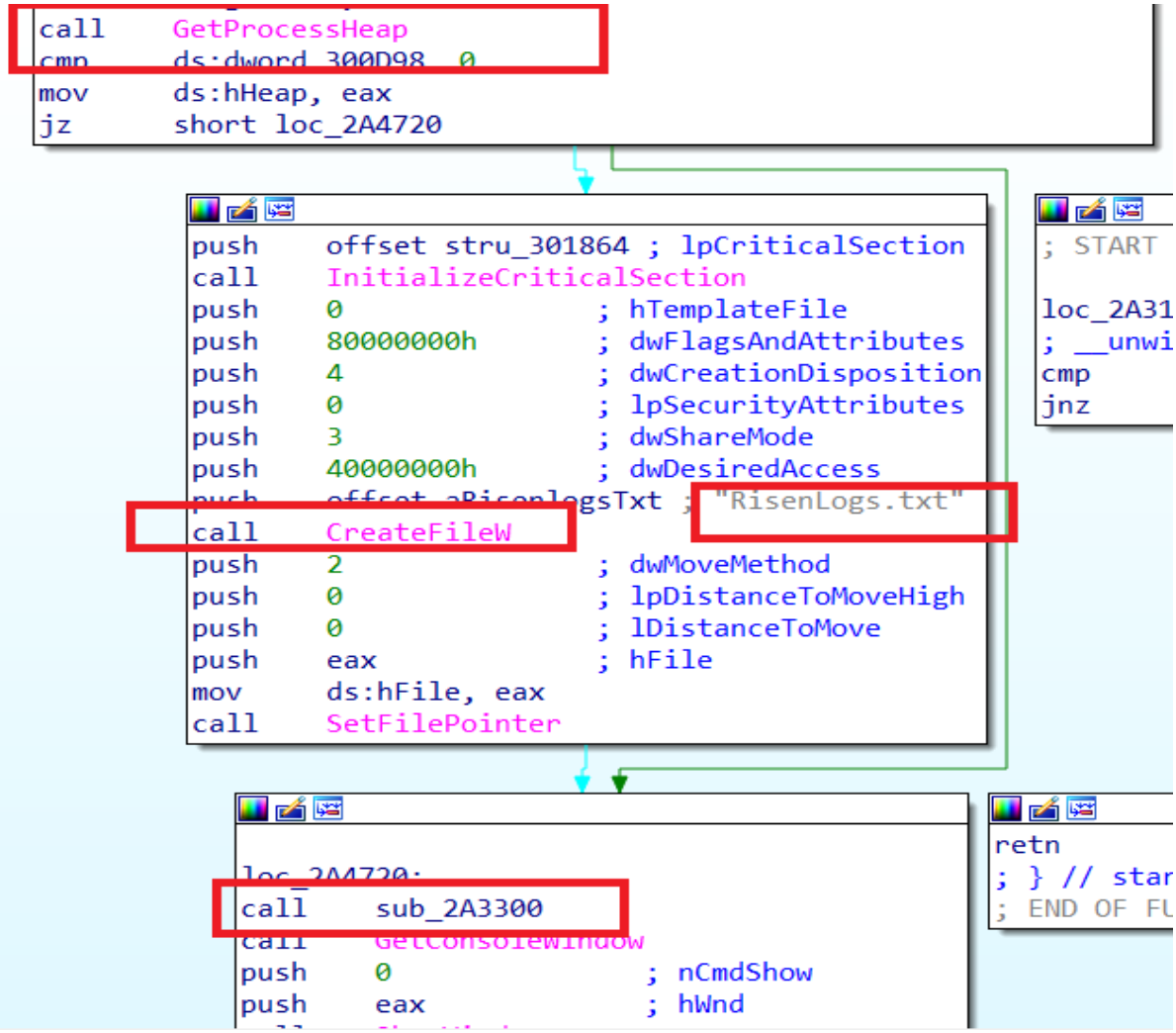
As you see ,it section name are upx0 and upx1 ,usually this naming convention used for upx packer but graph's randomness and above it self shows not packed .To confirm this take help of cff explorer

```
File size      Ratio    Format    Name
--------upx: C:\Users\admin\AppData\Local\Temp\upxD361.tmp: NotPackedException: not packed by UPX
```

Now its confirm it is not packed .

Code flow :

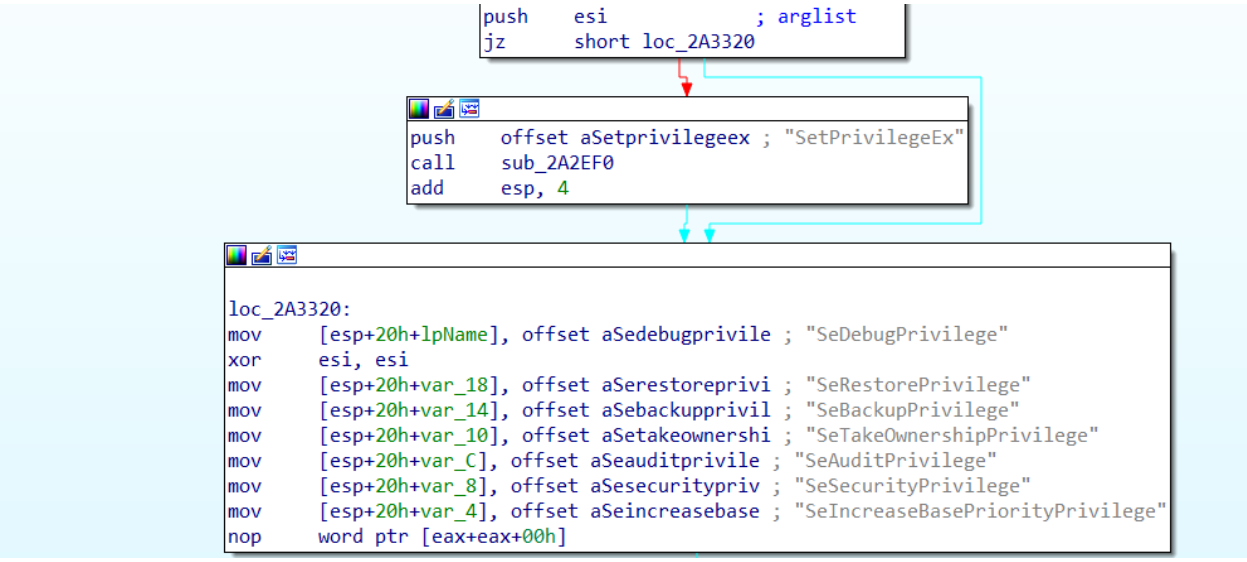
It starts with below code snippet .

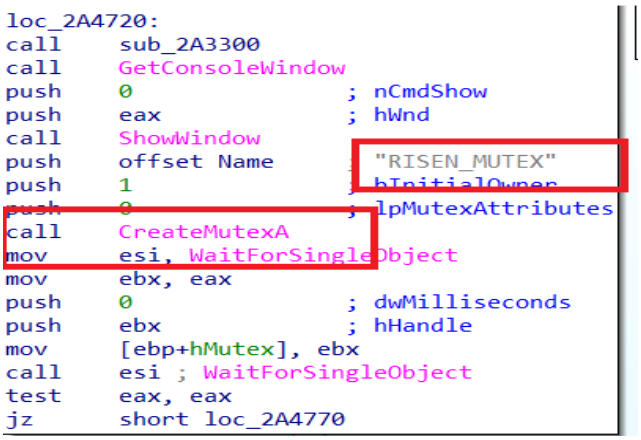


From above we can see api **GetProcessHeap** -this function obtains a handle to the default heap for the calling process. A process can use this handle to allocate memory from the process heap without having to first create a private heap using the HeapCreate function. In reversing perspective ,this api can use to check virtualization , this api pair with **CloseHandle** () and on a real system, CloseHandle () should be faster to execute than GetProcessHeap (). The author checks the time difference between these two APIs for validating the virtualization this sequence used in the locky ransomware

After conditional check it createfile risenlogs.txt ,it contains system is encrypted we can see that last of this section , then after we can a function this try to get admin by access **SeDebugPrivilege** – it is a special privilege that when assigned gives a token high integrity. This is given to users of the Administrator's group by default.if we have this we can bypass andatory Integrity Control (MIC), and ACE checks (both Discretionary Access and Conditional Access)

If you feel bit complicated to understand ,simply it makes you king of system





Then you can see it create mutex ,then sleep for some time in milliseconds and do call operational api call and then starts create registry key

```
call    sub_2A4590
mov     ecx, offset aCRegAddHkeyLoc ; "/c reg add \"HKEY_LOCAL_MACHINESoftware"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_0 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_1 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_2 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_3 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_4 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_5 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_6 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_7 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_0 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_1 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_2 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_3 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_2 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyLoc_8 ; "/c reg add \"HKEY_LOCAL_MACHINE\\Softwa"...
```

But what it is doing we can below

```
:                                       ; DATA XREF: _main+150↑o
 text "UTF-16LE", '/c reg add "HKEY_LOCAL_MACHINESoftware\Policies\Mic'
 text "UTF-16LE", 'rosoft\Windows Defender" /v "DisableAntiSpyware" /t'
 text "UTF-16LE", ' REG_DWORD /d 1 /f',0
 align 8
_0:                                     ; DATA XREF: _main+15A↑o
 text "UTF-16LE", '/c reg add "HKEY_LOCAL_MACHINE\Software\Policies\Mi'
 text "UTF-16LE", 'crosoft\Windows Defender\Real-Time Protection" /v "'
 text "UTF-16LE", 'DisableRealtimeMonitoring" /t REG_DWORD /d 1 /f',0
 align 8
_1:                                     ; DATA XREF: _main+164↑o
 text "UTF-16LE", '/c reg add "HKEY_LOCAL_MACHINE\Software\Policies\Mi'
 text "UTF-16LE", 'crosoft\Windows Defender\Spynet" /v "SubmitSamplesC'
 text "UTF-16LE", 'onsent" /t REG_DWORD /d 2 /f',0
 align 10h
_2:                                     ; DATA XREF: _main+16E↑o
 text "UTF-16LE", '/c reg add "HKEY_LOCAL_MACHINE\Software\Policies\Mi
 text "UTF-16LE", 'crosoft\Windows Defender\Threats" /v "Threats_Threa'
 text "UTF-16LE", 'tSeverityDefaultAction" /t REG_DWORD /d 1 /f',0
 align 4
_3:                                     ; DATA XREF: _main+178↑o
 text "UTF-16LE", '/c reg add "HKEY_LOCAL_MACHINE\Software\Policies\Mi'
 text "UTF-16LE", 'crosoft\Windows Defender\Threats\ThreatSeverityDefa'
 text "UTF-16LE", 'ultAction" /v "Low" /t REG_DWORD /d 6 /f',0
 align 4
_4:                                     ; DATA XREF: _main+182↑o
 text "UTF-16LE", '/c reg add "HKEY_LOCAL_MACHINE\Software\Policies\Mi'
 text "UTF-16LE", 'crosoft\Windows Defender\Threats\ThreatSeverityDefa'
(Synchronized with Pseudocode-A)
```

To disable the av ,then create registry in this hive

```
'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\'
```

This hive had lot capabilities

Exclude credential providers
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**ExcludedCredentialProviders**

Assign a default domain for logon
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**DefaultLogonDomain**

Configure the mode of automatically signing in and locking last interactive user after a restart or cold boot
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**AutomaticRestartSignOnConfig**

Sign-in and lock last interactive user automatically after a restart
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**DisableAutomaticRestartSignOn**

Report when logon server was not available during user logon
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**ReportControllerMissing**

Disable or enable software Secure Attention Sequence
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**SoftwareSASGeneration**

Display information about previous logons during user logon
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**DisplayLastLogonInfo**

Show first sign-in animation
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**EnableFirstLogonAnimation**

Turn off Windows Startup sound
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**DisableStartupSound**

Hide entry points for Fast User Switching

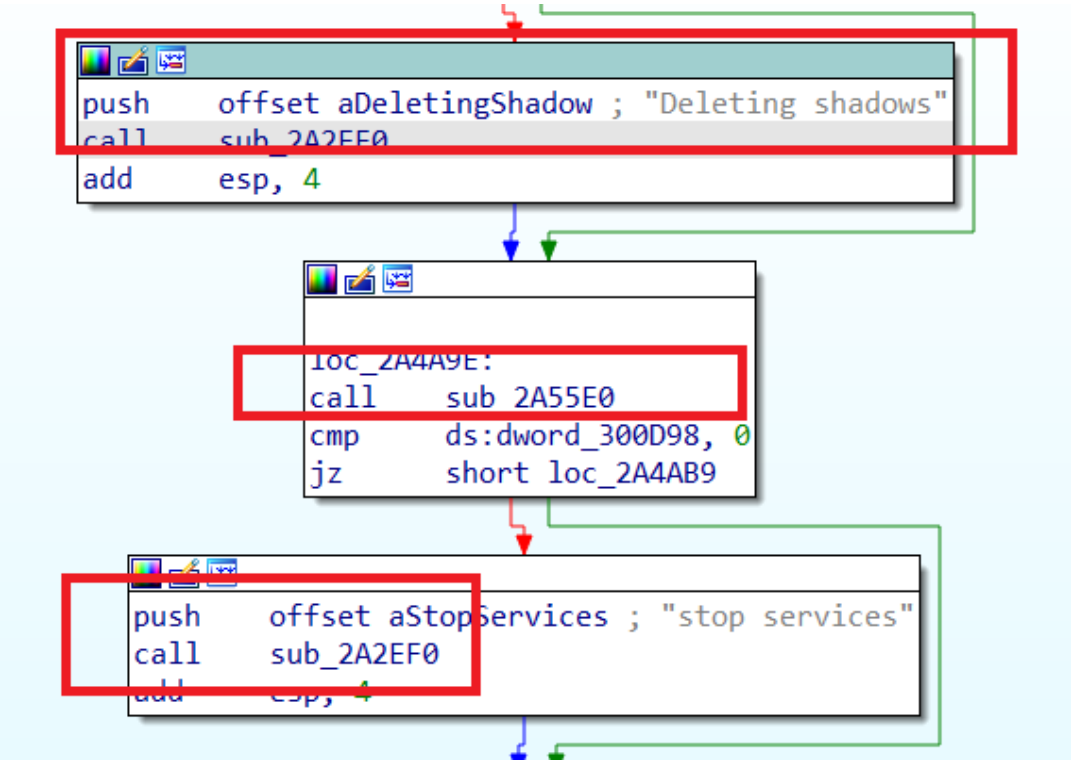
```
mov     edi, RegSetValueExW
lea     eax, [ebp+Data]
push    4               ; cbData
push    eax             ; lpData
push    4               ; dwType
push    0               ; Reserved
push    offset ValueName ; "EnableLUA"
push    [ebp+phkResult] ; hKey
call    edi ; RegSetValueExW
test    eax, eax
jnz     short loc_2A496C
```

EnableLUA specifies whether Windows User Account Controls (UAC) notifies the user when programs try to make changes to the computer.after that it uses uac change group policy and the malware sets the `EnableLinkedConnections` registry key, allowing any user to see network drives that were mapped for other users. This gives ransomware the ability to gain access to sensitive network resources The malware invokes the `RefreshPolicyEx` API function to enforce the modifications made.

```
push    eax
lea     eax, [ebp+var_D18]
push    offset aCSchtasksExeCr ; "/c SCHTASKS.exe /Create /RU \"NT AUTHOR"...
push    eax             ; LPWSTR
```

```
'/c SCHTASKS.exe /Create /RU "NT AUTHORITY\SYSTEM" /'
'sc onstart /TN "SystemDefense" /TR "%s" /F',0
```

It try to to create a scheduled task from a Windows service.

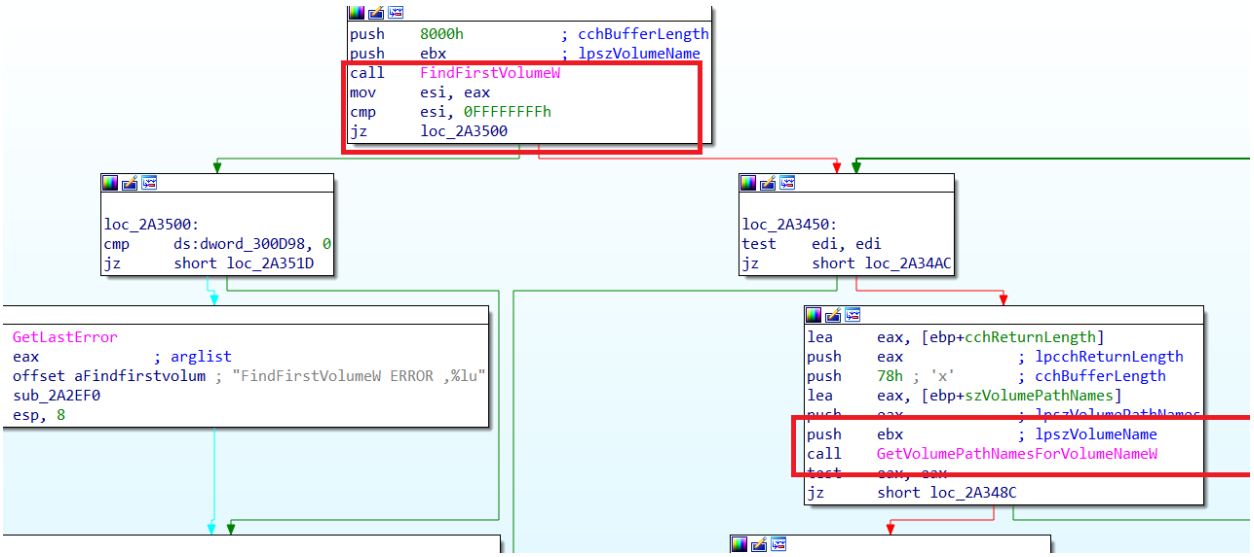


Next it delete shadow copies of system ,mandatory for ransomware ,then it kills few service and process

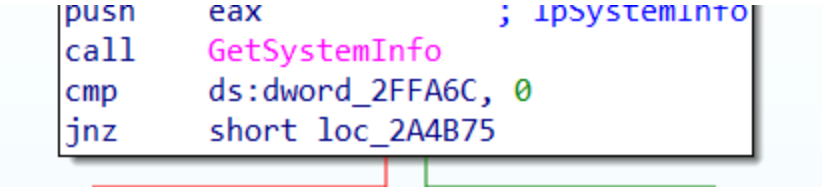
```
loc_2A4AB9:
call    sub_2A5360
push    offset aHttpS2wk77h653 ; "http://s2wk77h653qn54csf4gp52orhem4y72d"...
push    offset aHttpS2wk77h653 ; "http://s2wk77h653qn54csf4gp52orhem4y72d"...
push    offset Buffer
push    offset aDectokyoCockLi ; "dectokyo@cock.li"
push    offset aDectokyoOnionm ; "dectokyo@onionmail.org , TELEGRAM:@toky"...
push    offset aDoctypeHtmlHtm ; "<doctype html><html><head><hta:applicat"...
push    offset dword_2F6DC0
call    sub_2A3000
push    offset aHttpS2wk77h653 ; "http://s2wk77h653qn54csf4gp52orhem4y72d"...
push    offset Buffer
push    offset aDectokyoCockLi ; "dectokyo@cock.li"
push    offset aDectokyoOnionm ; "dectokyo@onionmail.org , TELEGRAM:@toky"...
push    offset aRisennoteReadT ; "RisenNote :\n\n\nRead this text file ca"...
push    offset dword_2FFDF8
call    sub_2A3000
add     esp, 34h
call    sub_2A3390
cmp     eax, 1
jnz     short loc_2A4B2C
```

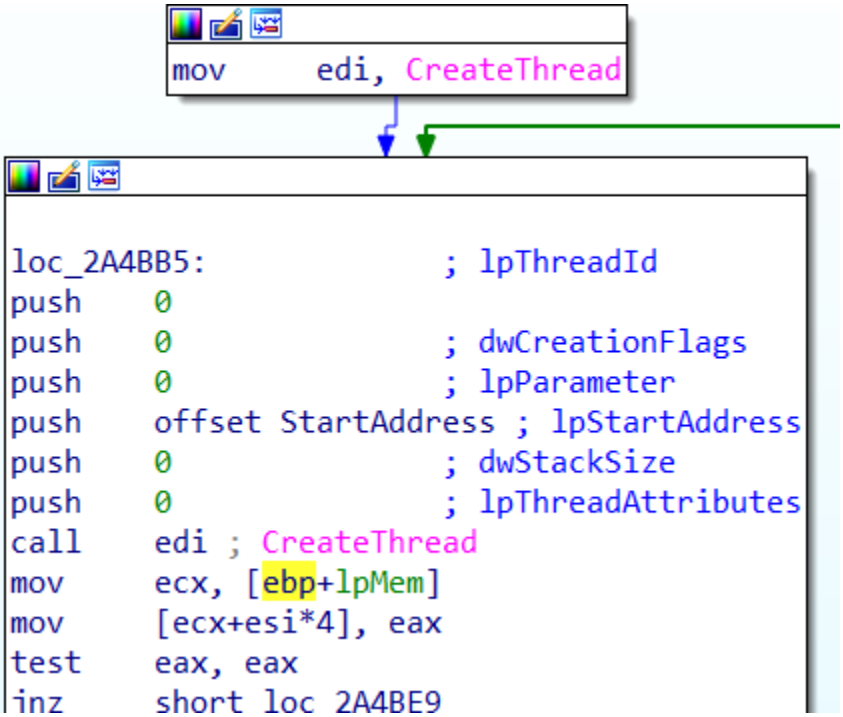
```
'http://s2wk77h653qn54csf4gp52orhem4y72dgxsquxulf255'
'pcymazeepbyd.onion/',0
```

Then make setup for final stage

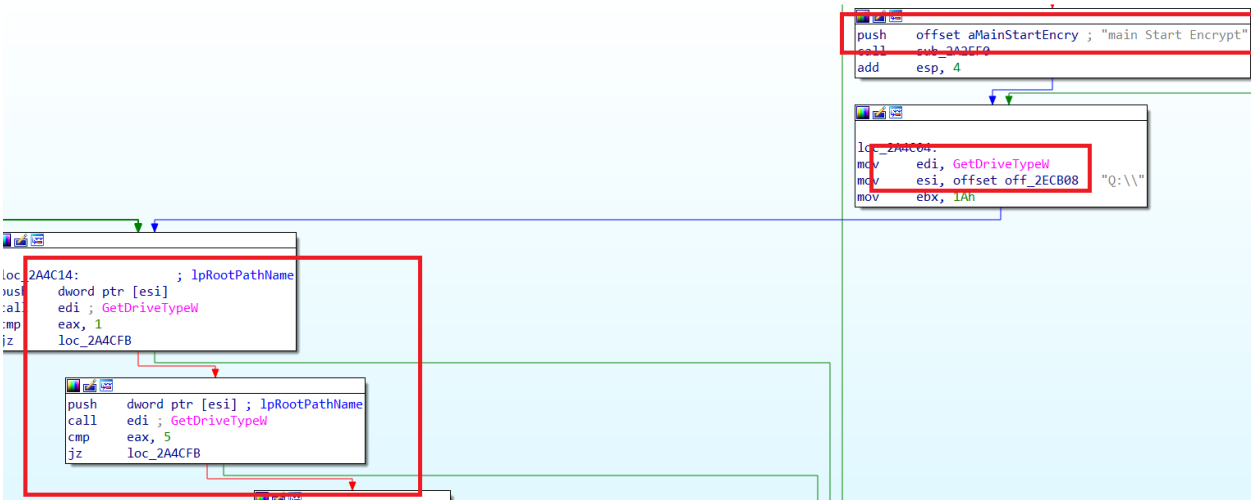


Finding drives and make to encrypt





Next , creating thread



Encryption starts

```
push    offset aEncryptComplet ; "Encrypt Complete , Delete Journals"
call    sub_2A2EF0
add     esp, 4
```

```
loc_2A4E10:
mov     ecx, off_2DD248[esi] ; "/c wevtutil.exe cl Setup"
call    sub_2A3120
add     esi, 4
```

Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.

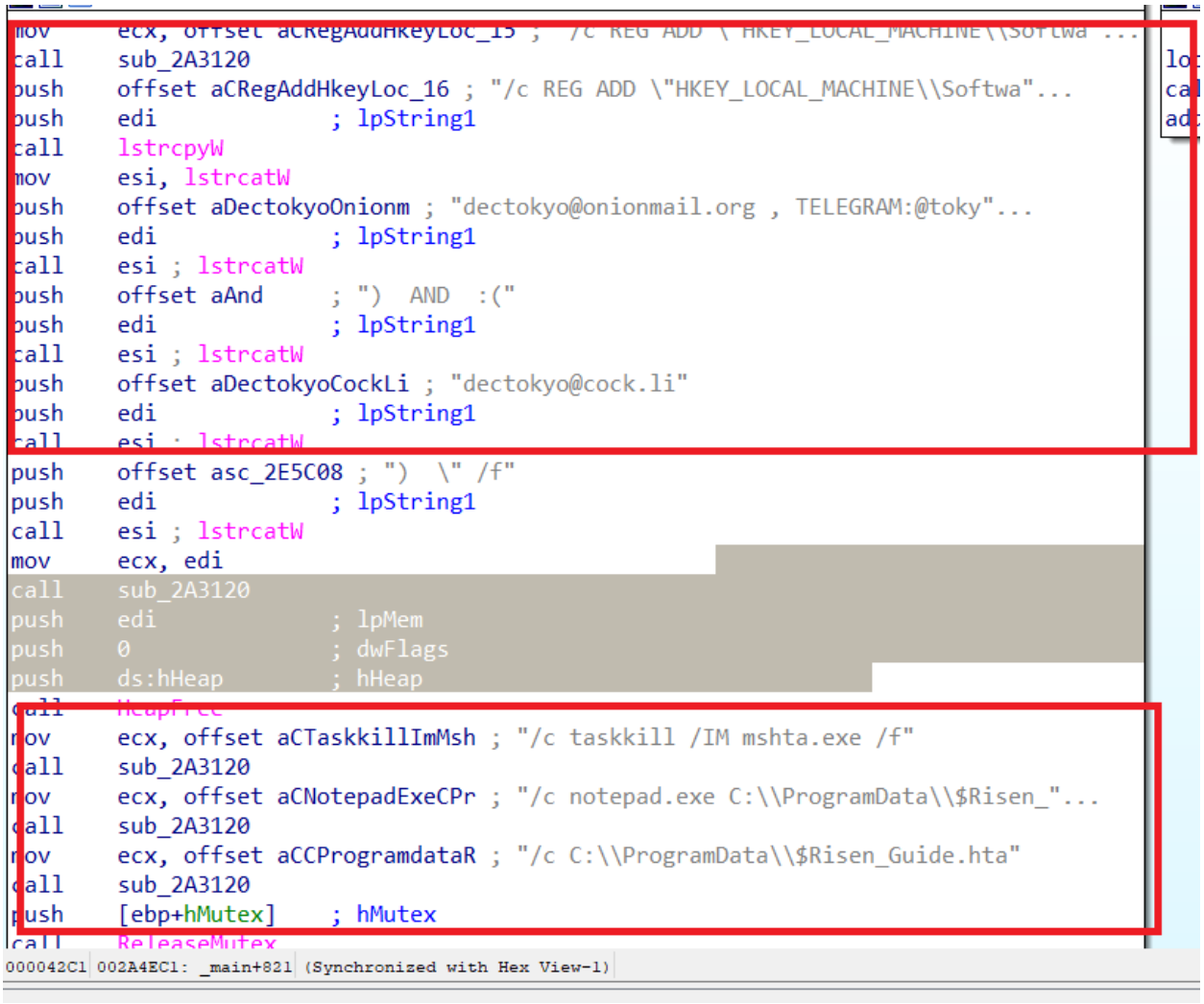
```
, '/c vssadmin.exe Delete Shadows /all /quiet',0
```

Retrieved shadows deleted by now

```
mov     ecx, offset aCSchtasksExeDe ; "/c SCHTASKS.exe /Delete /TN \"SystemDef"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_6 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
mov     ecx, offset aCRegAddHkeyCur_7 ; "/c reg add \"HKEY_CURRENT_USER\\SOFTWAR"...
call    sub_2A3120
push    1               ; fWinIni
push    offset pvParam  ; "C:\\ProgramData\\RisenBackGround.JPG"
push    0               ; uiParam
push    14h             ; uiAction
call    SystemParametersInfoW
mov     esi, HeapAlloc
nop     dword ptr [eax]
```

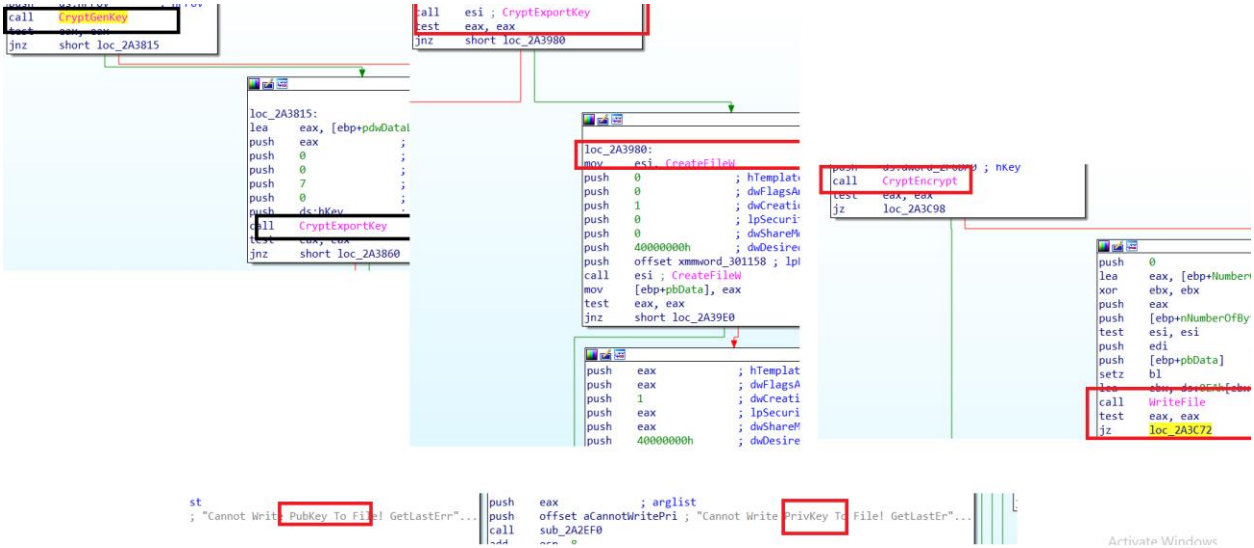
```
        ; DATA XREF: _main+7A2↑o
'/c reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Wi'
'ndows\CurrentVersion\Policies\System" /v "DisableTa'
'skMgr" /t REG_DWORD /d 0 /f',0

        ; DATA XREF: _main+7AC↑o
'/c reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Wi'
'ndows\CurrentVersion\Policies\Explorer" /v "NoRun" '
'/t REG_DWORD /d 0 /f',0

        ; DATA XREF: _main+7E5↑o
'/c REG ADD "HKEY_LOCAL_MACHINE\Software\Microsoft\W'
'indows\CurrentVersion\Policies\System" /v "legalnot'
'icecaption" /t REG_SZ /d "WELCOME   " /f',0

        ; DATA XREF: _main+7EF↑o
'/c REG ADD "HKEY_LOCAL_MACHINE\Software\Microsoft\W'
'indows\CurrentVersion\Policies\System" /v "legalnot'
'icetext" /t REG_SZ /d " We have penetrated your who'
'le network due some critical security issues.  We h'
'ave encrypted all files on each host in the network'
' , We have also Took your critical data AND in case'
' of NO corporation until the end of the deadline we'
' WILL leak or sell your data, the only way to stop '
```

Previously created ones used for this



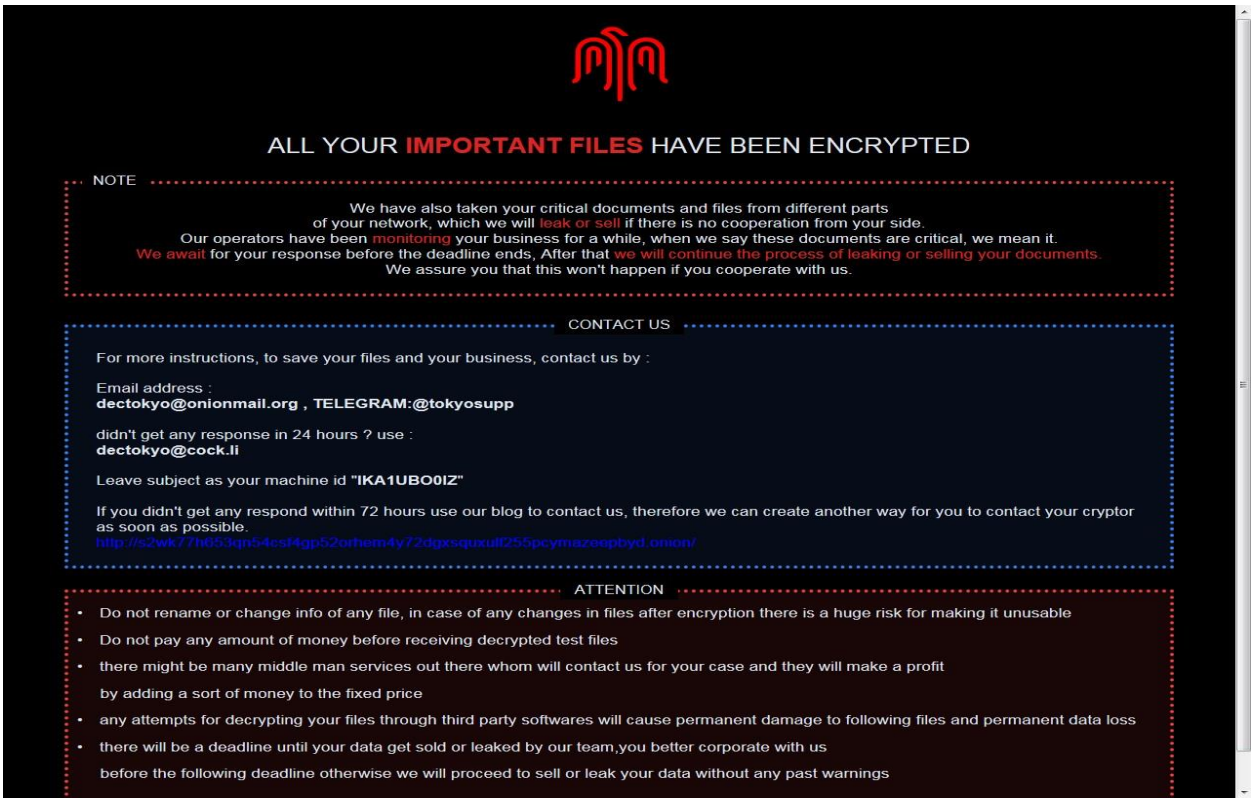
Setup for final act

In depth encryption inspection do on debugging part in coming blogs we lightly touch here

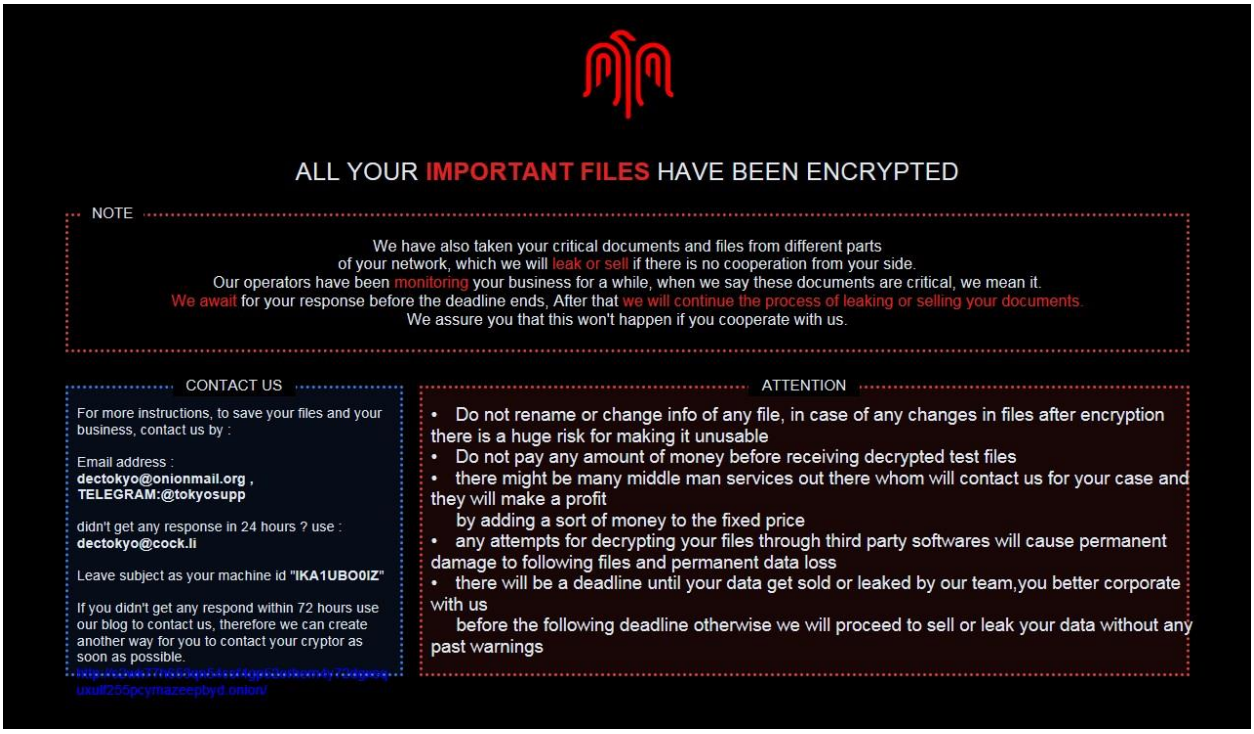


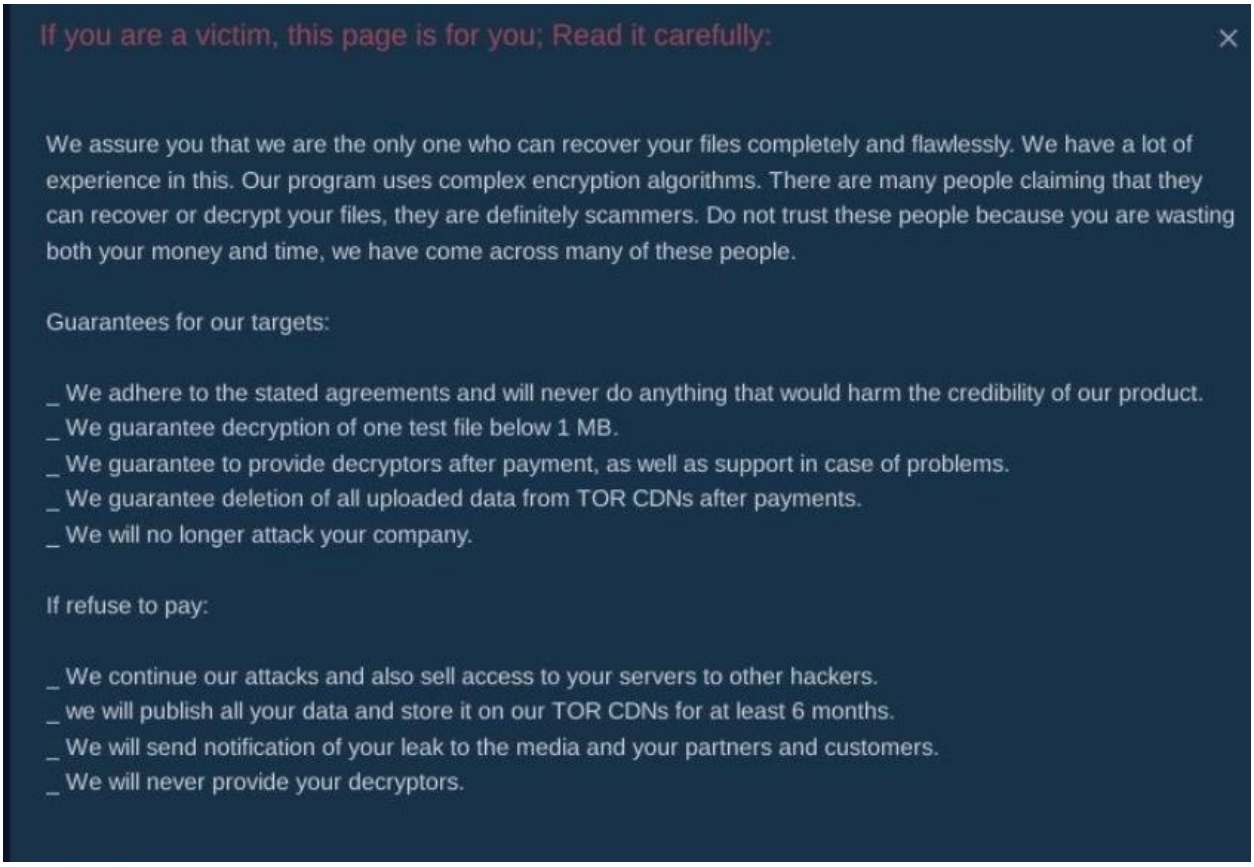
Create crypto key ,create file ,then encypt and write data ,below you can see public and private it shows it use asymmetric algorithm. It is easy to show this process in the **.net file** and .ini, dll .hrmlogs exe lnk files are excluded in the encryption .

Few IOC :



Ransome note (pic taken from amigo site)


ALL YOUR IMPORTANT FILES HAVE BEEN ENCRYPTED
NOTE
We have also taken your critical documents and files from different parts
of your network, which we will leak or sell if there is no cooperation from your side.
Our operators have been monitoring your business for a while, when we say these documents are critical, we mean it.
We await for your response before the deadline ends, After that we will continue the process of leaking or selling your documents.
We assure you that this won't happen if you cooperate with us.
CONTACT US
For more instructions, to save your files and your business, contact us by :
Email address :
dectokyo@onionmail.org ,
TELEGRAM:@tokyosupp
didn't get any response in 24 hours ? use :
dectokyo@cock.li
Leave subject as your machine id "IKA1UBO0IZ"
If you didn't get any respond within 72 hours use our blog to contact us, therefore we can create another way for you to contact your cryptor as soon as possible.
uxulf255pcymazeepbyd.onion/
ATTENTION
• Do not rename or change info of any file, in case of any changes in files after encryption there is a huge risk for making it unusable
• Do not pay any amount of money before receiving decrypted test files
• there might be many middle man services out there whom will contact us for your case and they will make a profit
by adding a sort of money to the fixed price
• any attempts for decrypting your files through third party softwares will cause permanent damage to following files and permanent data loss
• there will be a deadline until your data get sold or leaked by our team,you better corporate with us
before the following deadline otherwise we will proceed to sell or leak your data without any past warnings


If you are a victim, this page is for you; Read it carefully:
We assure you that we are the only one who can recover your files completely and flawlessly. We have a lot of experience in this. Our program uses complex encryption algorithms. There are many people claiming that they can recover or decrypt your files, they are definitely scammers. Do not trust these people because you are wasting both your money and time, we have come across many of these people.
Guarantees for our targets:
_ We adhere to the stated agreements and will never do anything that would harm the credibility of our product.
_ We guarantee decryption of one test file below 1 MB.
_ We guarantee to provide decryptors after payment, as well as support in case of problems.
_ We guarantee deletion of all uploaded data from TOR CDNs after payments.
_ We will no longer attack your company.
If refuse to pay:
_ We continue our attacks and also sell access to your servers to other hackers.
_ we will publish all your data and store it on our TOR CDNs for at least 6 months.
_ We will send notification of your leak to the media and your partners and customers.
_ We will never provide your decryptors.

Their logo

The extension is added to encrypted files: .<random _ID >

In fact, a compound extension using a template is used:

.[ransom_email, TELEGRAM:ID].random_ID

An example of such an extension:

.[dectokyo@onionmail.org, TELEGRAM:@tokyosupp].IKA1UBO0IZ

$Risen_Note.txt - name of the file with the ransom demand;

$Risen_Guide.hta - name of the file with the ransom demand;

Risen_ID.txt - file with the victim's ID;

$Risen[IKA1UBO0IZ].Private, $Risen[GL6MNBAZEJ].Private - examples of special files;

$Risen[IKA1UBO0IZ].Public, $Risen[GL6MNBAZEJ].Public - examples of special files;

RisenBackGround.JPG - the original image of the ransomware, replacing the Desktop wallpaper;

Risen.exe is the name of the malicious file;

Risen.pdb - project file. **Locations:** \Desktop\ -> \User_folders\ -> \%TEMP%\ -

E:\repos\Risen\Release\Risen.pdb **Registry entries associated with this Ransomware:** See analysis results below. **Mutexes:** See analysis results below.

Network connections and connections: Tor-URL: hxxx://s2wk77h653qn54csf4gp52orhem4y72dgxsquxulf255pcymazeepbyd.onion

Ransom notes are called:

$Risen_Note.txt

$Risen_Guide.hta

```
RisenNote :


Read this text file carefully.

We have penetrated your whole network due some critical security issues.

We have encrypted all of your files on each host in the network within strong algorithm.

We have also Took your critical data such as docs, images, engineering data, accounting data, customers and ...
        And trust me, we exactly know what should we collect in case of NO corporation until the end of the deadline we WILL leak or sell your data,
        the only way to stop this process is successful corporation.

We have monitored your Backup plans for a whileand they are completely out of access(encrypted)

The only situation for recovering your files is our decryptor,
        there are many middle man services out there whom will contact us for your caseand add an amount of money on the FIXED price that we gave to them,
        so be aware of them.

Remember, you can send Upto 3 test files for decrypting, before making payment,
        we highly recommend to get test files to prevent possible scams.

In order to contact us you can either use following email :

Email address : dectokyo@onionmail.org , TELEGRAM:@tokyosupp

Or If you weren't able to contact us whitin 24 hours please Email : dectokyo@cock.li

Leave subject as your machine id : IKA1UBO0IZ

If you didn't get any respond within 72 hours use our blog to contact us,
therefore we can create another way for you to contact your cryptor as soon as possible.
 BLOG : http://s2wk77h653qn54csf4gp52orhem4y72dgxsquxulf255pcymazeepbyd.onion/
```

Conclusion :

Hope you get an idea how ransomware works ,they is unexplored area like weird resource section ,which contains hashes ,looks this had scope of using to hashbd to obfuscate api hashing ,still it is new one ,that is out of scope for this article.In upcoming we do try api hashing .Apart from code ,contacted domains ,ip and url are related to blackhunt malware .As per one report might be c2 operator are might same or helping hands .Thank you