MRLAB

Ransomware hücumlarına texniki baxış və wannacry analizi 1. hissə

Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti - Malware Research Lab - F. Cəfərov, S. Abasov - 15 Aprel 2022

Son zamanların haqqında ən çox bəhs edilən zərərverici tipləri arasında ransomware-lər geniş yer tutur. İstifadəçilərin kritik məlumatlarından faydalanaraq qazanılan külli miqdarda pullar, böyük kompaniyaların təhklükəsizlik sistemlərindən istifadə etmələrinə baxmayaraq zərər çəkmələri, böyük dövlətlərin məxfi qurumlarının adlarının bi tip kiber əməliyyatlarda hallanması bu tipli zərərvericilərin reklam kompanyasında böyük rol oynadı.

Ransomware nədir?

Ransomware kəliməsi dilimizə fidyə olaraq tərcümə edilir. Adından anlaşılacağı kimi müəyyən bir əməliyyat qarşılığında bir şeyləri qazanmaq məqsədi güdülür. Burada kritik və önəmli olan əməliyyat isə istifadəçiyə aid dəyərli məlumatları istifadəçinin əlindən almaq ve geri qaytarılması üçün istifadəçidən qarşılığında mənfəət əldə etməkdir. Ransomlar tam olaraq bu işi görmək üçün hazırlanan zərərverici proqram təminatlarıdır. Yoluxduqları komputerlərdə mövcud olan kritik (word, excel, powerpoint, pdf, rəsm, musiqi vs) kimi faylları şifrələyərək istifadəçinin bu vacib məlumatlara girişini əngəlləyirlər. Nəticə olaraq kritik məlumatlarına girişi əngəllənən istifadəçi bu məlumatları geri qaytarmaq üçün qarşılığında külli miqdarlarda pul ödəməyə razılaşır (razı salınır). Bəzən fayllar bərpa edilir bəzən isə istifadəçilər yalnız məbləği ödəməklə qalır fayllar bərpa edilmir.

Bəs əməliyyat necə həyata keçirilir?

Bu tipli kiber hücümlar yazılan kodlar ilə yoluxan sistemdə olan faylların ilk öncə axtarışını həyata keçirir. Əgər kritik məlumat daşımaq üçün istifadə edilən fayl formatları aşkarlanar isə həmin fayllar şifrələnir. Daha sonra şifrələnən bu faylların deşifrə edilməsi üçün zərər çəkən şəxsin qarşı tərəf ilə əlaqəyə keçə bilməsi üçün əlaqə məlumatları zərərçəkən şəxs ilə paylaşılır. Zərərçəkən şəxs istənilən fidyəni ödədiktən sonra əgər ransomu proqramlayan şəxs "insaflı" biri olarsa fayllar deşifrə edilir. Bütün bu əməliyyatları daha yaxşı anlamanız üçün bu haqda ən çox verilən sulları cavablamaq daha məqsədə uyğun olacaqdır.

1. **Fayllarımın deşifrə ediləcəyindən necə əmin ola bilərəm və doğru şəxs (ransomu yazan şəxs) ilə əlaqəyə keçdiyimdən necə əmin ola bilərəm?**

Fayllarınız deşifrə edilmədiyi müddətcə bundan əmin ola bilmərsiniz. Çünki bəzən fidyəni qəbul etdikdən sonra faylları deşifrə etmirlər. Bu tamami ilə qarşı tərəfin insafına qalan bir şeydir.

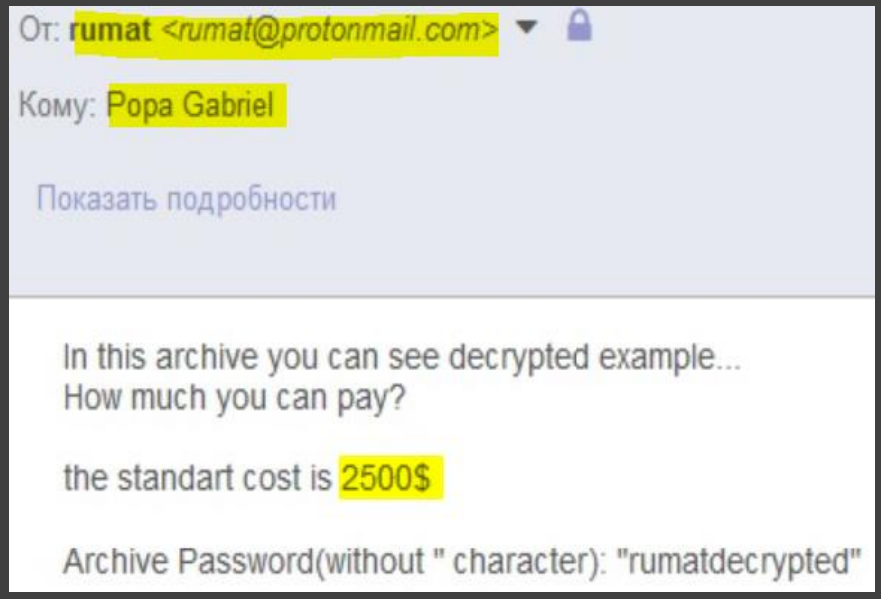
Əlaqəyə keçilən şəxsin doğurdanda sizin fayllarınızı şifrələyən proqramı yazan şəxs olub olmadığı isə dəqiqləşdirmək üçün belə bir yol izlənilir. Siz bu şəxs ilə əlaqəyə keçdiyiniz zaman bu özünün doğru şəxs olduğunu sizə göstərmək üçün sizdən şifrələnən hər hansı bir nümunə faylının ona göndərməyinizi istəyir. Əgər göndərdiyiniz faylı(şifrələnən) deşifrə edib sizə geri qaytarırsa deməli həqiqətən fayllarınızı deşifrə etmək üçün lazım olan açarlar bu şəxsdədir.

2. **Şifrələnən faylları özüm deşifrə edə bilərəm?**

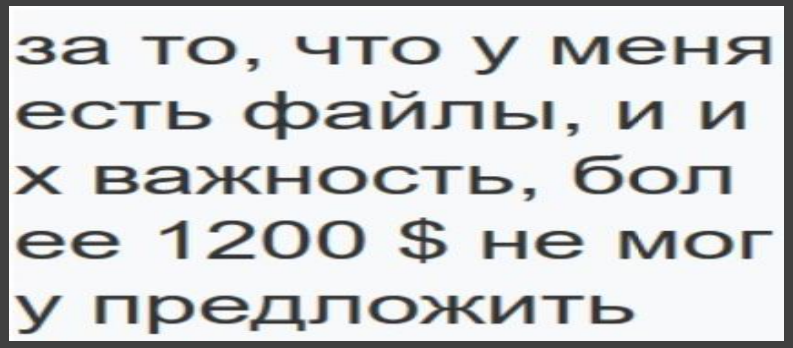
Əgər ransom işini bilən biri tərəfindən hazırlanıb isə xeyr. Bu tipli əməliyyatlarda əksər hallarda daha doğrusu düzgün yazılan ransom assimetrik şifrələmə alqoritmalarından istifadə edir. Yəni məlumatı şifrələyən açar sizdə, deşifrə edən açar isə qarşı tərəfdə olur. Belə olan halda məlumatı deşifrə etmək üçün digər tərəfdə olan açar lazımdır. Tam əksi baş verdiyi halda yəni simmetrik şifrələmə alqoritması istifadə edilib isə ransom içərisindən tərsinə mühəndislik metodları ilə açarı çıxardaraq faylları deşifrə etmək mümkündür. Bəzən təhlükəsizlik(antivirus vs) şifrkətlərinin bunun üçün alətlər paylaşdığını görə bilərsiniz. Bu alətlər məhz bu tipli metodlar ilə əldə edilən açarlar hesabına yaradılır. Birdaha qeyd edək simmetrik alqoritm istifadə edilibdirsə. Digər bir yol isə əgər ransom yazan şəxs yaxalana bilərsə onda olan açarlar üzərindən belə alətlər hazırlamaq mümkündür.

3. **Bəzən 3. tərəflər daha ucuz qiymətə məlumatları deşifrə edə bilir. Əgər açar yalnız zərərlini yazan şəxsdədirsə bu necə mümkündür?**

Bu suala cavab tapa bilmək üçün bir neçə il öncə MRL olaraq kiçik bir əməliyyat keçirmişdik. Beləki ölkəmizdə bir çoxları bunun mümkün olduğunu hətta bəziləri bu yol ilə daha ucuz qiymətə məlumatları deşifrə edə bilmişdilər. Lakin əslində məsələ tamam başqadır. Beləki 3-cü şəxslər sizin adınızdan zərəvericini yazan şəxs ilə əlaqəyə keçərək qiymət endirimi üçün bazarlıq edirlər və əksər hallarda bu effektiv olur. 3-cu tərəf isə qarşı tərəfə daha az pul ödəyərək sizdən isə daha çox(lakin zərərvericini yazan şəxsdən daha az) məbləq alaraq məsələni həll edə bilirlər. Sosial şəbəkələrin birində özünü *rumat* olaraq tanıdan şəxs məlumatları daha ucuz qiymətə deşifrə edə biləcəyini bildirdi. Bizə isə əslində nə baş verdiyini arasdırmaq üçün həmin şəxsə kiçik bir oyun oynadıq. Yuxarıda qeyd etdiyim kimi zərərverici yazan şəxs yoluxmadan sonra istifadəçinin onunla əlaqəyə keçə bilməsi üçün mesaj saxlayır. Bu əksər hallarda şifrələnmiş faylın extensionunda zərərlini yazan şəxsin email ünvanı olur. Bizdə sanki yoluxmuşuq kimi 3-cü tərəf (Popa Gabriel) ilə əlaqə saxladıq. 3-cü tərəf isə zərərvericini yazan şəxsin əlaqə məlumatlarını bilmədiyi üçün bizdən şifrələnmiş bir fayl istədi. Biz isə saxta şifrələnmiş fayl extensionunu öz yaratdığımız email adresini əlavə edərək 3-cu şəxsə göndərərək daha sonra mail üzərindən bizim ilə əlaqəyə keçməsini gözlədik. Uzun sürmədi



Daha sonra özümüz tərəfindən şifrələnən faylı deşifrə edərək 3-cü tərəfə göndərdik. Qiymət olaraq isə **2500$** istədik. Əlbətdə bizim əslində həm zərərverən həmdə zərərçəkən olduğumuzu bilmədən endirim istədi - **1200$**. Yenidən bizə (zərərçəkən tərəfə) qayıdaraq isə **1500$** istədi.



Bu əməliyyat isə əslində özünü şifrələri sındıraraq faylları deşifrə etdiyini iddia edən şəxslərin əslində hansı metod ilə faylları deşifrə etdiyinin nümunəsidir.

4. **Bu tipli zərərvericilər pul köçürmə əməliyyatları zamanı izlənməkdən yayınmaq üçün nə edir?**

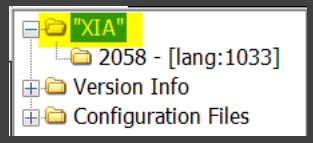
Bu tipli zərərvericilər ödəmə üsulunu normal metodlar ilə deyil kripto valyuta üzərindən həyata keçirirlər. Beləliklə pul köçürmələri izləmək mümkün olmur. Keçirik məsələnin texniki tərəfinə. Bir ransom şifrələmə əməliyyatı zamanı hansı metodlardan istifadə edir hansı yolları izləyir bunlara baxaq. Nümunə üçün WannaCry ransomware -nin əsas icra edilə bilən hissəsinin analizini aparacağıq. Ransomware- lərin bu qədər populyar olmasında bu zərərlinin olduqca böyük payı var. İlk variantı yalnız faylları şifrələyib fidyə istəyən zərərlinin sonrakı variantları daha təhlükəli funksionallıqlara malik idi. Belə ki Amerika Birləşmiş Ştatları NSA (National Security Agency) tərəfindən kiber əməliyyatlar zamanı istifadə edilən exploit (EternalBlue Windows OS) Shadow Brokers adlı hacker qrupu tərəfindən sızdırıldıqdan sonra WannaCry bu exploiti istifadə edərək artıq şəbəkə üzərindən yoluxaraq digər komputerlərdədə şifrələmə əməliyyat həyata keçirir idi. Daha ətraflı https://en.wikipedia.org/wiki/WannaCry_ransomware_attack. Analiz edəcəyimiz nümunə isə EternalBlue exploiti daşımayan sample olacaq. Bu nümunə həmçinin ilk qəbul etdiyimiz zərərli idi.

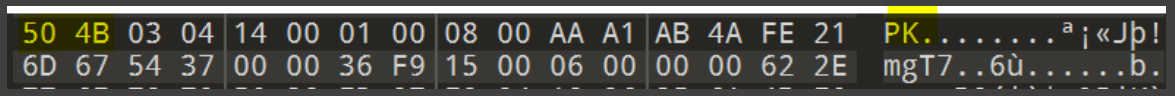
Zərərli dropperin analizi

Nümunə faylımız 32 bitlik **3514368** bayt ölçüsündədir.

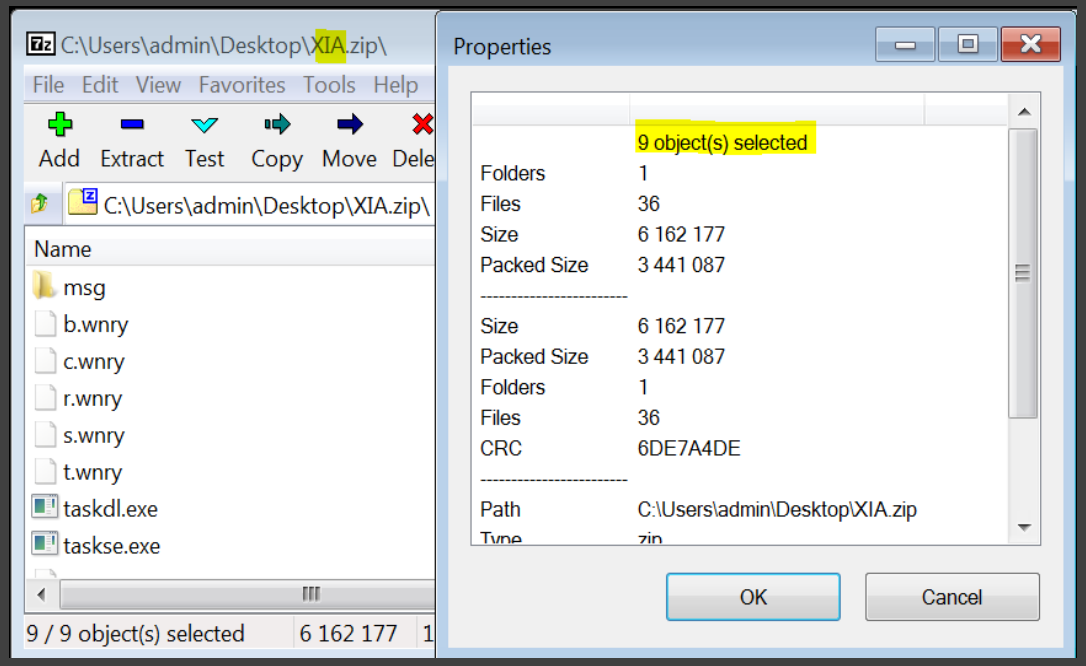
MD5: 84c82835a5d21bbcf75a61706d8ab549
SHA-1: 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467

Burada diqqəti çəkən ilk məqam PE bölmələrində (sections) idi. .rsrc bölməsi fayla aid resursların saxlanıldığı bölmədir. Anomaliya bölmənin həcminin olduqca böyük olmasında idi. Resurs bölməsində keçid edərək hansı datanın bu qədər yer tutduğunu aydınlaşdırmağa çalışdım. Burada saxlanılan məlumat headeri bizə ZIP olduğunu deyirdi.





Məlumatı xam şəkildə dump edərək içərisində nə olduğuna baxmaq istədikdə isə zip faylın şifrə ilə qorunduğunu gördüm.



Bundan sonra isə faylın import tablosuna baxmaq qərarına gəldim. Burada da maraqlı kitabxana funksiyaları istifadə edilir. Məsələn **advapi32.dll** kitabxanası import edilmiş idi və windows servislər ilə işləmək üçün funksiyalar çağrılırdı. Digər tərəfdən kernel32 içərisində PE resursları ilə işləmək üçün funksiyalar import edilmiş idi. Bu funskiyalar ehtimal ki, həmin resursu extract etmək üçün istifadə edilirdi.

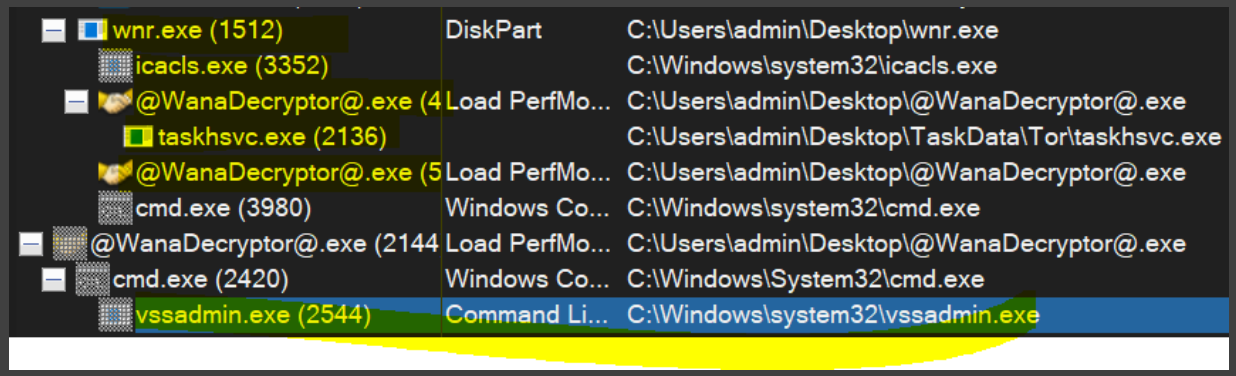
8000	CreateServiceA
8004	OpenServiceA
8008	StartServiceA
800C	CloseServiceHandle
8010	CryptReleaseContext
8014	RegCreateKeyW
8018	RegSetValueExA

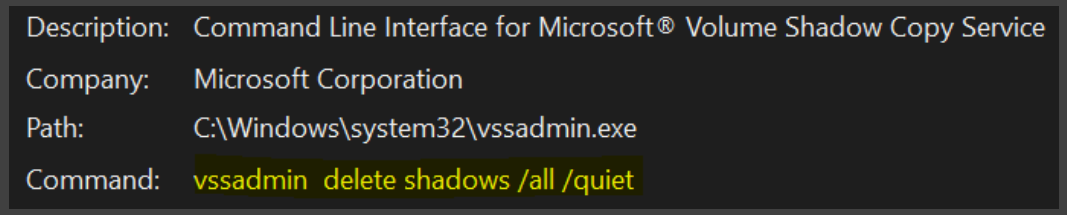
806C	SizeofResource
8070	LockResource
8074	LoadResource

Başqa diqqətə çarpan bir informasiya olmadığı üçün proqramı icra edib nələr etdiyini görmək istədim. Bundan öncə isə daha effektiv analiz üçün saxta (honeypot) qovluq yaradaraq içərisində bir neçə fayl yaratdım. Lazım olan proqram təminatlarını hazırladıqdan sonra proqramı işhə saldım. Bir neçə dəqiqədən keçdikdən sonra sistemdə olan bütün məlumatlarım, şəkillərim, sənədlərim şifrələnmiş idi. Ekranda isə aşağıdaki pəncərə.

Şəkil 1 WannaCry əsas pəncərə

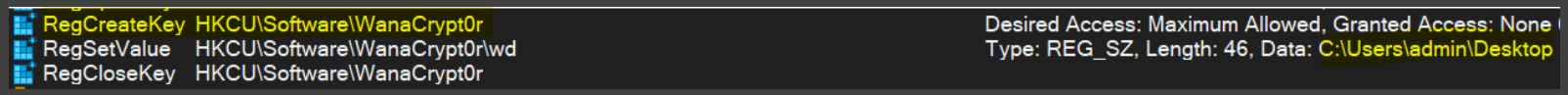
Topladığım logların analizinə başladım. Process tree də olduqca maraqlı informasiyalar var idi.





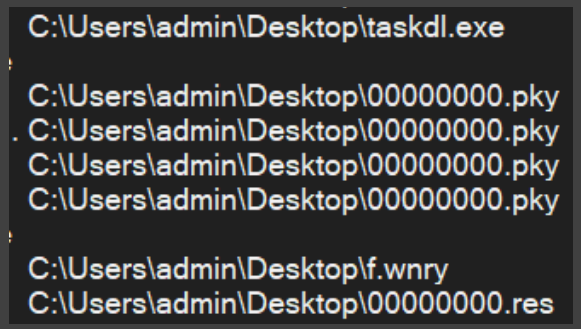
Şəkil 2 vsadmin ilə backup kopyalarının silinməsi

WannCry sistemde olan shadow kopyaları vsadmin aləti köməkliyi ilə silir. https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service
Bundan əlavə olaraq "**cmd.exe /c reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "swjwogwnbof758" /t REG_SZ /d "\"C:\Users\admin\Desktop\tasksche.exe\"" /f**" əmri ilə növbəti sistem işə salınmasında zərərlinin avtomatik işə düşməsi üçün yeni registry key yaradır. Zərərli registry içərisində WannaCrypt0r adında yeni key yaradır və içərisində işə salındığı cari qovluğun pathını yazır.

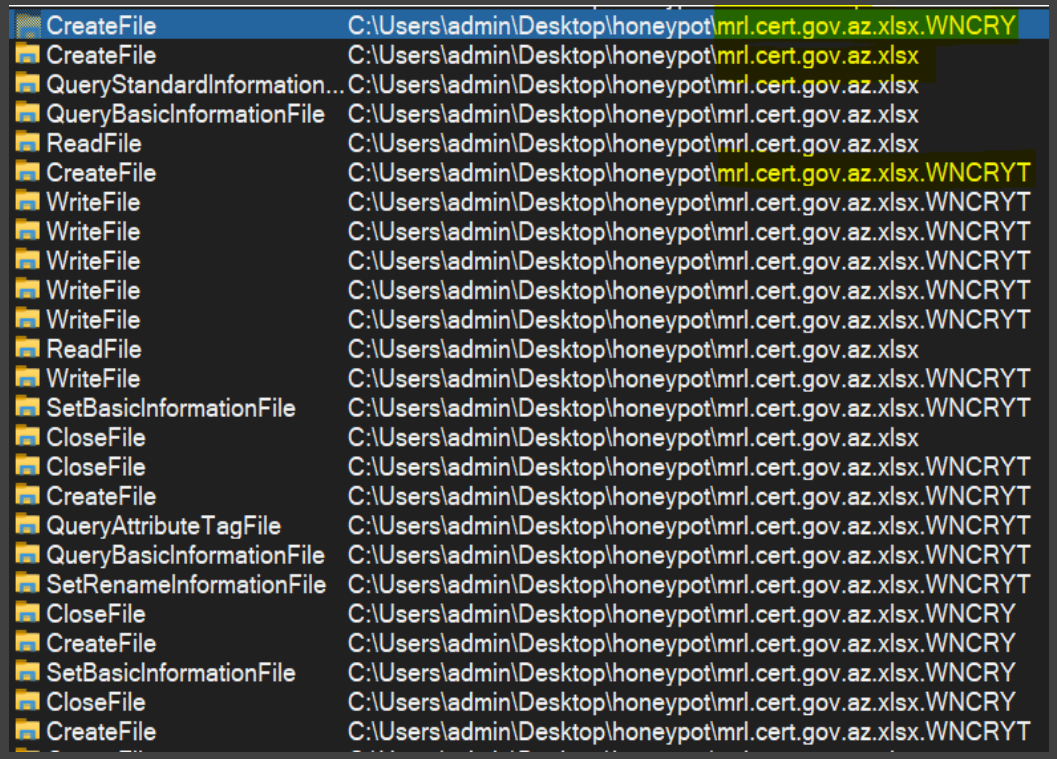


Şəkil 3 WannaCrypt0r keyinin yaradılması

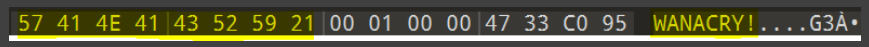
Bundan sonra özünə aid resursdan export etdiyi fayllarıda cari qovluğa yazır və **attrib +h** əmri ilə bu faylları gizlədir.



Honeypot olaraq yaratdığım qovluq üzərində hansı əməliyyatları həyata keçirdiyini görmək üçün bu qovluğa göz gəzdirdim. Bu zərərlinin şifrələmə üçün hansı yollardan keçdiyi haqqında bizə təxmini məlumat verir.



WannaCry burada ilk olaraq hədəf.**WNRCRY** faylının mövcud olub- olmadığını yoxlayır. Daha sonra hədəf faylı oxumaq üçün açır. Hədəf haqqında məlumat toplamaq üçün sorğu göndərir.
Bundan sonra fayldan offset 0 dan başlayaraq 8 baytlıq məlumat oxuyur. Oxuduqdan sonra həmin qovluqda hədəf.**WNCRYT** və offset 0 dan başlayaraq 8 bayt məlumat yazır. Bu məlumat wannacry header imzası idi.



Bundan əlavə olaraq daha 4 + 256 + 4 + 8 baytlıq məlumat yazdıqdan sonra hədəf faylı tam olaraq oxuyur və ehtimal ki, şifrələyərək yaratdığı .WNCRYT faylına yazır. Ardınca isə yenidən hədəf faylı write modu ilə açaraq içərisinə məlumat yazır. Bu yazılan məlumat çox böyük ehtimal zərərçəkən tərəfin şifrələnmiş faylları sonradan recover software ilə geri qaytarmaması üçün nəzərdə tutulub. Zərərçəkən tərəfə sistemində nəyin baş verdiyini anlaması üçün @Please_Read_Me@.txt adında mətn faylında mesaj saxlayır. İcra olunduğu qovluqda @WanaDecryptor@.exe adında exe yaradan zərərli şifrələnmiş məlumatların olduğu qovluqlara bu exenin (.lnk)

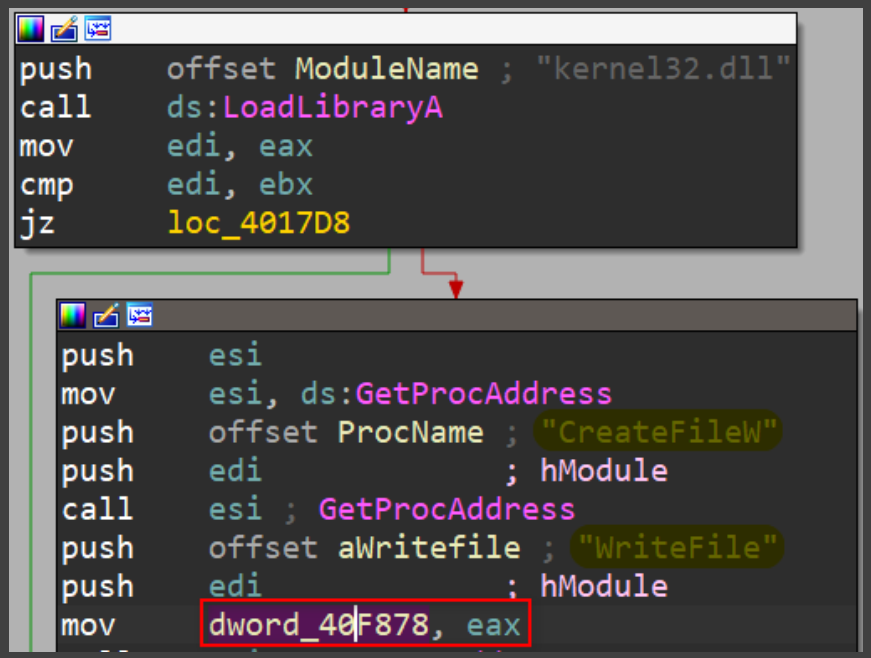
uzantısında bir ədəd shortcut faylı yaradır. @WanaDecryptor@.exe faylı isə istifadəçidən fidyə istəyən zərərli proqramdır. Son olaraq isə zərərli original hədəf faylı sistemdən silir. Bu əməliyyat sistemdə olan bütün fayllara (lazım olan formatlar) icra edilir. Zərərli haqqında ilkin məlumatlar topladıqdan sonra daha ətraflı analiz üçün zərərlinin kodlarına baxdım. Zərərli ilk olaraq cari modulun adını götürərək bunu strchr funksiyası parametr olaraq göndərir ilə "\\" xarakterini axtarır və bölərək icra edildiyi qovluğu **SetCurrentDirectory** funksiyası defolt qovluq olaraq set edir. Bundan sonra isə registry üzərindən **WannaCrypt0r** açarını yaradır.

```
lea     eax, [ebp+Destination]
push    offset Source   ; "WanaCrypt0r"
push    eax             ; Destination
```

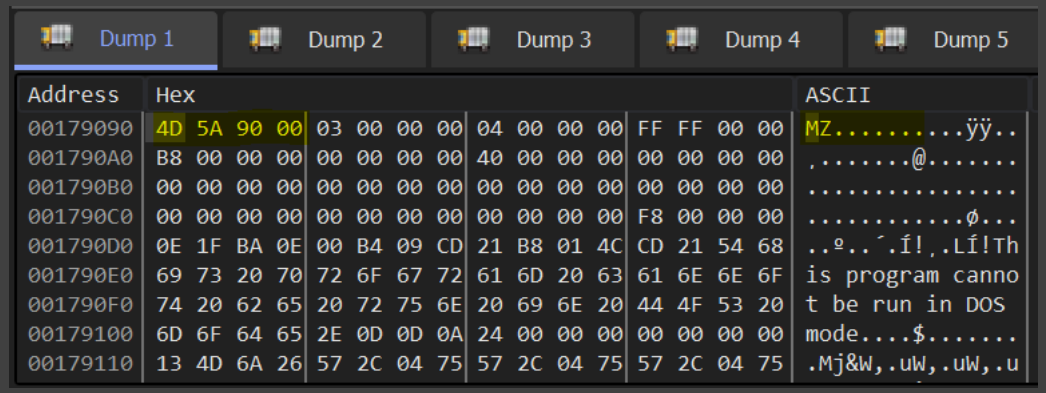
Registry açar yaradıldıqdan zərərlinin resurs bölməsində olan "**XIA**" tipində resurs extract edilir. Disasm zamanı unzip üçün şifrənidə əldə etdim. "WNcry@2ol7". ZIP resursunu yenidən manual extract edib içərisində nələr olduğuna baxdım.
b.wnry - BMP rəsm faylıdır. Bu fayl şifrələmə əməliyyatından sonra ekran görüntüsünü bu rəsm ilə dəyişir

c.wnry	**İçərisində Tor şəbəkəsinə aid onion adreslər saxlayır**
msg	Qovluq içərisində istifadəçilərə şifrələnmə haqqında məlumat vermək üçün müxtəlif dillərdə olan tərcümə faylları saxlayır
r.wnry	Həmçinin istifadəçilərə məlumat vermək üçün mətn faylı
s.wnry	PK formatında olan zip faylı içərisində tor browser fayllarını saxlayır
t.wnry	WannaCry imzasını daşıyan şifrələnmiş fayl ?
taskdl.exe	Naməlum
taskse.exe	Naməlum
u.wnry	Naməlum PE32 faylı

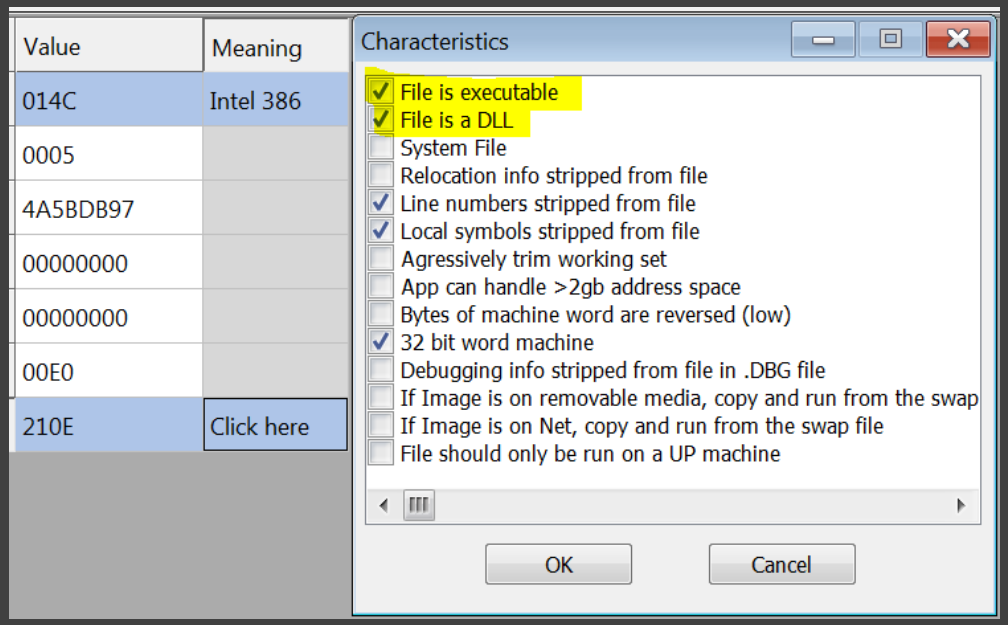
Daha sonra zərərli ard-arda **attrib + H** və **icacls . /grant Everyone:F /T /C /Q** əmrlərini icra edir. Bünün üçün **CreateProcess** funksiyasından istifadə edir. Zərərli statik analizdən yayınmaq üçün növbəti funksiyada kiçik bir fənd (obfuskasiya) işlədir. Kritik funksiyaları birbaşa çağırmaq əvəzinə həmin funksiya adreslərini bir structura yazır və funksiya çağrılan zaman bir başa deyil məhz bu struktur üzərində olan eslərdən istifadə edərək funksiyaları çağırır. Bu metodun dinamik analiz zamanı heç bir effekti olmasada statik naliz zamanı funksiya ref -lərini gizlətmək üçün effektiv metoddur. Bundan əlavə olaraq şifrələmə əməliyyatları zamanı istifadə ediləcək crypto (**advapi32.dll**) funksiyaları üzərində də eyni əməliyyatı həyata keçirir.



Bundan sonra zərərli **t.wnry** faylını oxuyur.
Yuxarıda qeyd etdiyim kimi bu fayl özü tərəfindən şifrələnmiş məlumat daşıyır.
Kodları trace etdiyim zaman zərərli bu şifrələnmiş məlumatı decrypt edərək yeni yaradılan yaddaş bölgəsində PE32 formatında məlumat generasiya edir.



Məlumatın bir hissəsini dump edərək PE editorda baxdığım zaman 32 bitlik DLL olduğunu aşkarladım.



Bu məlumatları şifrələyən əsas DLL faylıdır. Açığı dropperi ilk analiz zamanı şifrələmə ilə bağlı heçnə gözə dəymirdi. Diqqətimi cəlb etmiş idi. Full dump etdikdən sonra isə səbəbi məlum oldu. Dropper şifrələmə əməliyyatını özü deyil məhz **t.wnry** içərisindən əldə etdiyi bu dll kitabxanası ilə edir. Kitabxana faylı 1 ədəd **TaskStart** adından funksiyanı export edib.

00000001	00005AE0	0000	0000BBFD	TaskStart

Import tablosuna baxdığım zaman olduqca maraqlı funksiyalar var idi. Bu funksiyalar şifrələmənin doğurdan da bu dll faylı üzərindən aparıldığı haqqında bəzi işarələr verirdi.

0000B362	0000B362	00CE	FindClose
0000B36E	0000B36E	00DD	FindNextFileW
0000B37E	0000B37E	00D5	FindFirstFileW

0000B6D2	0000B6D2	0096	CryptGenRandom
0000B6BE	0000B6BE	009A	CryptGetKeyParam

Bundan sonra zərərli yaddaşa yüklənmiş DLL faylını parse edərək export tablosuna keçir. Burada **stricmp** funksiyasının köməkliyi ilə **TaskStart** funksiyasının adresini(rva) öyrənərək bu adresi geri qaytarır. Daha sonra call eax instruction ilə **TaskStart** funksiyası çağrılır və şifrələmə əməliyyatı başlayır.

```
esi=BBC0
dword ptr ds:[eax]=[10000170]=BBC0
```

```
1: [esp] 0040F4E8 "TaskStart"
2: [esp+4] 1000BBFD "TaskStart"
```

```
EAX   10005AE0
```

```
call eax
```

Məqalənin ilk hissəsində olduqca kompleks zərərlinin dropperini analiz etdik.
2. hissədə zərərvericinin şifrələmə mexanizmi haqqında məlumat veriləcək.

İstinadlar

https://en.wikipedia.org/wiki/Ransomware
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
https://www.kaspersky.com/resource-center/threats/ransomware-wannacry