Ransomed by Warlock Dark Army “OFFICIALS”

Published: 2023-02-02 · Archived: 2026-04-05 12:35:00 UTC

Recently we came across a tweet shared by petikvx. The tweet was on a ransomware family that had the group name similar to the WARLOCK DARK ARMY. The similarities with Chaos ransomware seem to end with the attacker group’s name. Upon analyzing the ransomware from the tweet we suspect both to be very different groups just based on their malware’s attributes.

The sample under consideration was compiled using C/C++, in case of Chaos ransomware it is usually .Net. Statically looking at the file we noticed a resource entry under Bitmap with an identifier “14”, while analyzing the file code we noticed that this resource was read and loaded on to the memory. Hence we decided to dump that resource entry.

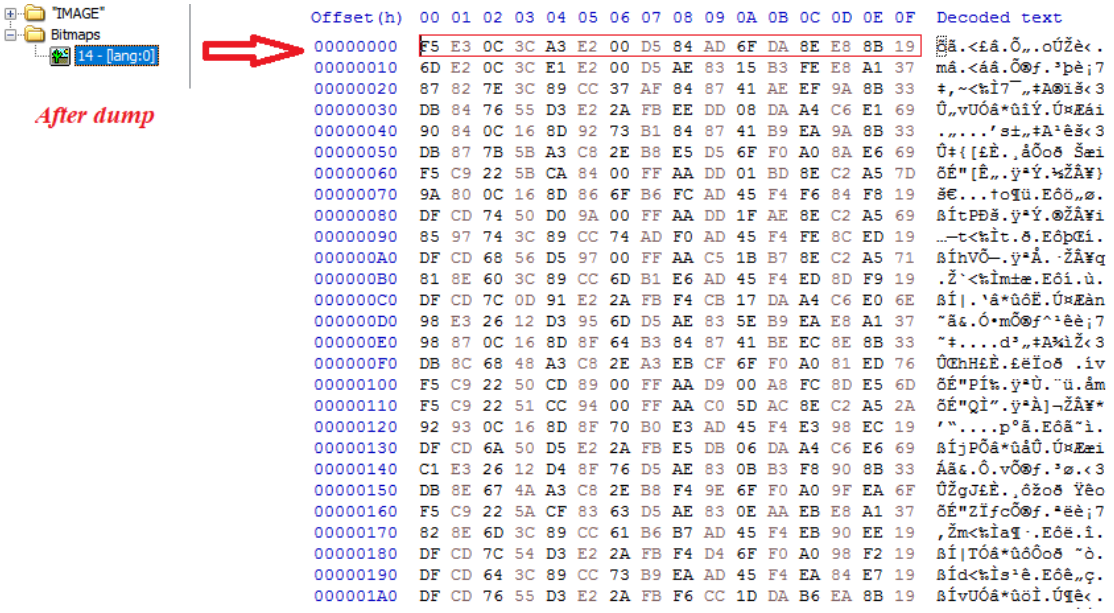


Figure 1: Encrypted blob in resource section

```
push    ebp
mov     ebp, esp
add     esp, 0FFFFFFF0h
push    ebx
push    2               ; lpType
push    14              ; lpName
push    0               ; hModule
call    FindResourceA
or      eax, eax
jnz     short loc_401FA2
jmp     loc_402330
```

Figure 2 : Loading blob into the memory

During our code analysis we found this blob was XOR encrypted. The first 16 bytes of this blob acts as the key for XOR decryption and the rest is the data which plays a key role in this ransomware’s infection/encryption

mechanism. Shown below is the code that does the mentioned activity.

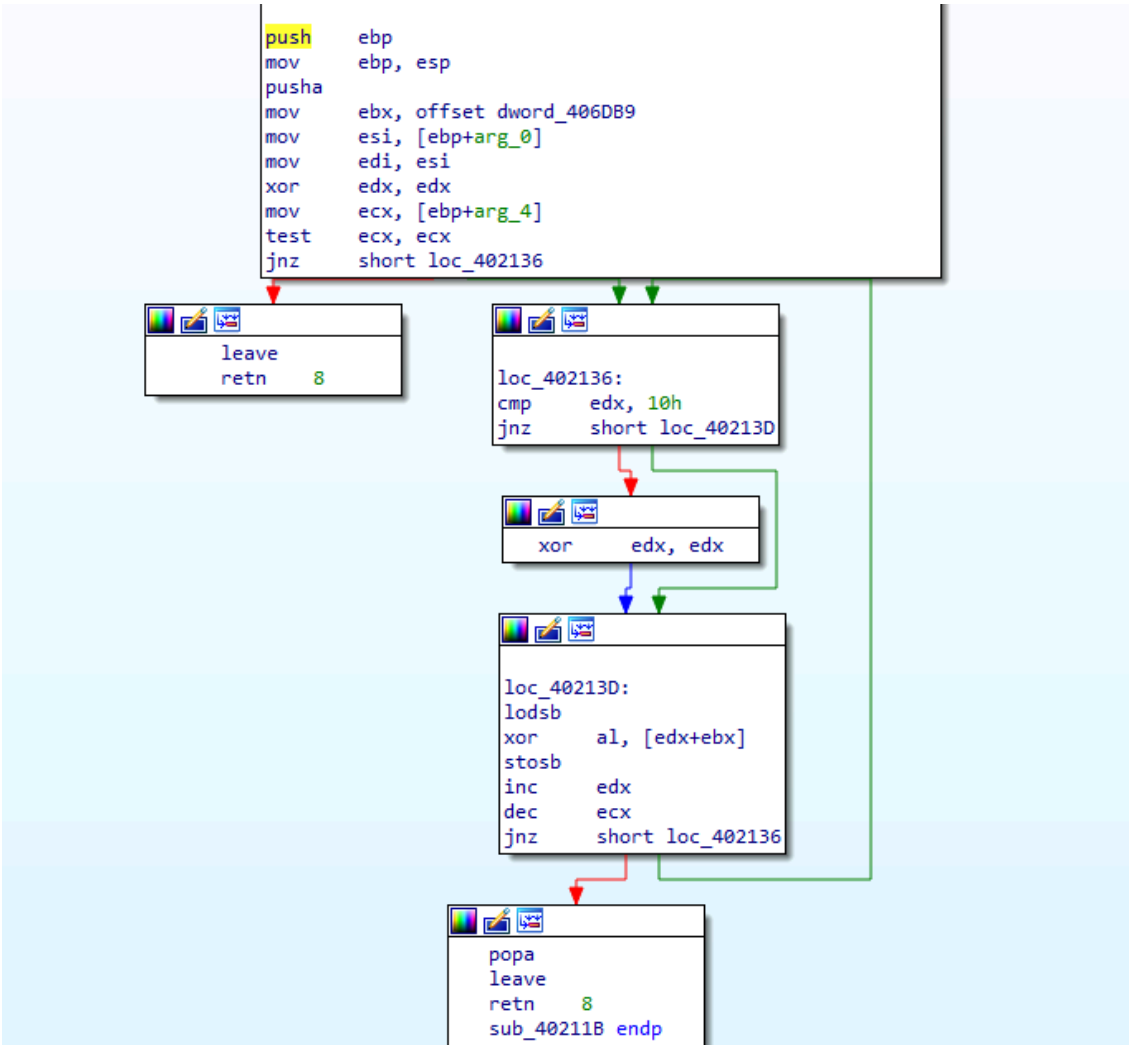


Figure 3 : Xor decryption in memory

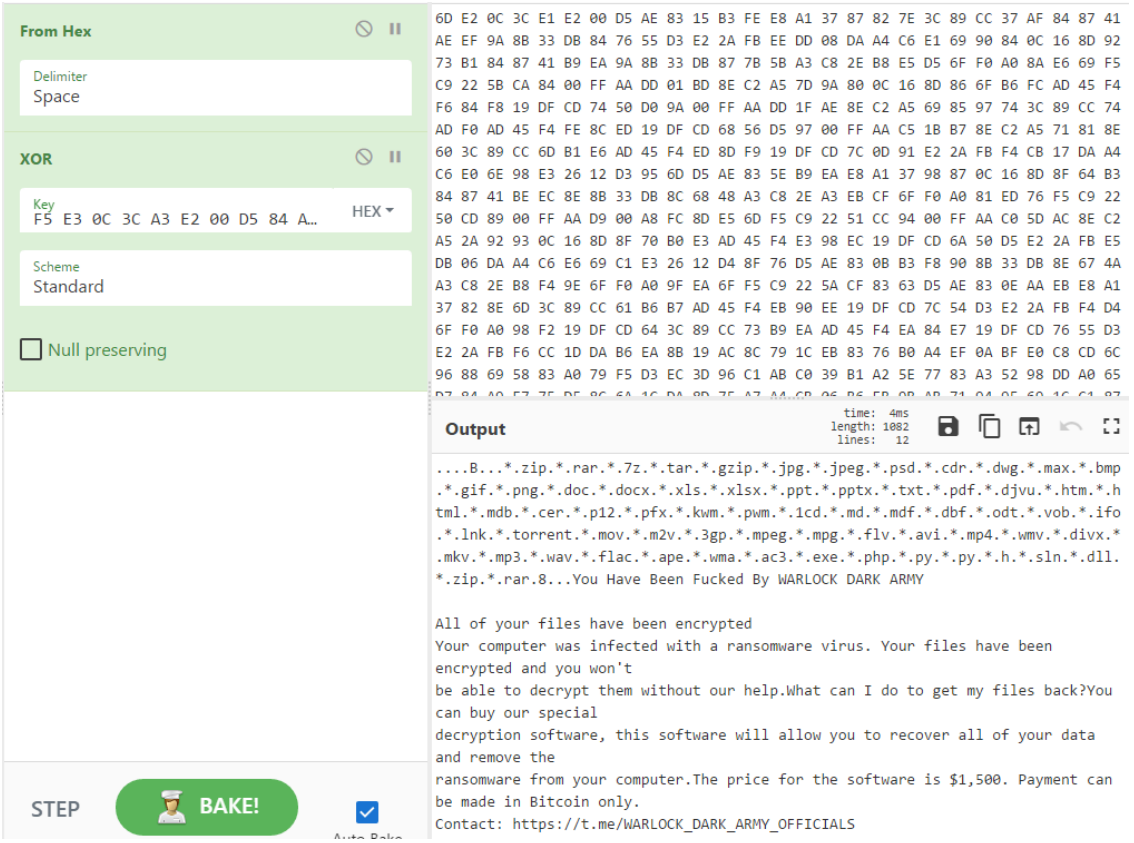
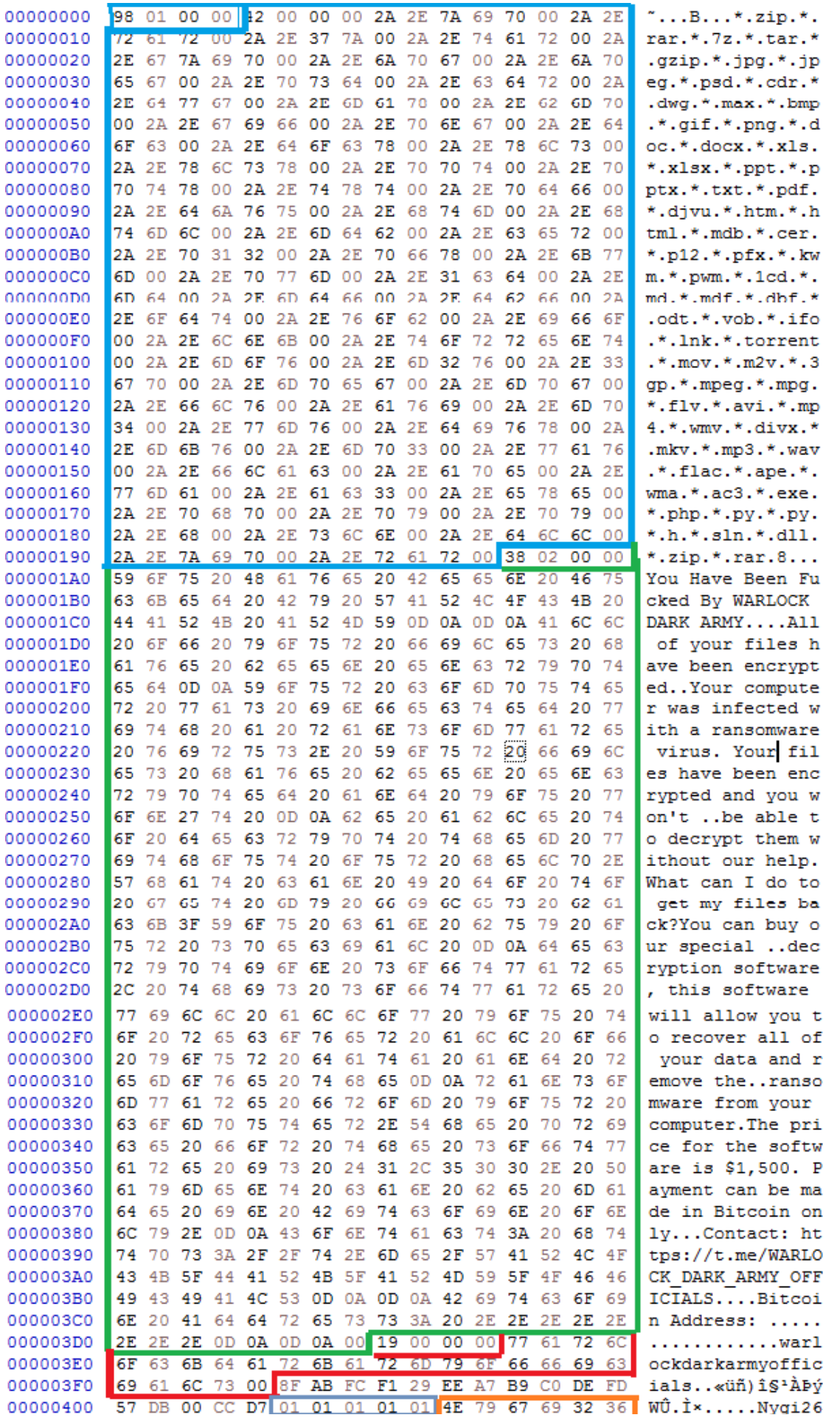


Figure 4: Decrypting with the XOR key using CyberChef

We used CyberChef to decrypt the data from the resource blob. Shown below is the decrypted content of the blob.



```
00000000  98 01 00 00 42 00 00 00 2A 2E 7A 69 70 00 2A 2E  ˜...B...*.zip.*.
00000010  72 61 72 00 2A 2E 37 7A 00 2A 2E 74 61 72 00 2A  rar.*.7z.*.tar.*
00000020  2E 67 7A 69 70 00 2A 2E 6A 70 67 00 2A 2E 6A 70  .gzip.*.jpg.*.jp
00000030  65 67 00 2A 2E 70 73 64 00 2A 2E 63 64 72 00 2A  eg.*.psd.*.cdr.*
00000040  2E 64 77 67 00 2A 2E 6D 61 78 00 2A 2E 62 6D 70  .dwg.*.max.*.bmp
00000050  00 2A 2E 67 69 66 00 2A 2E 70 6E 67 00 2A 2E 64  .*.gif.*.png.*.d
00000060  6F 63 00 2A 2E 64 6F 63 78 00 2A 2E 78 6C 73 00  oc.*.docx.*.xls.
00000070  2A 2E 78 6C 73 78 00 2A 2E 70 70 74 00 2A 2E 70  *.xlsx.*.ppt.*.p
00000080  70 74 78 00 2A 2E 74 78 74 00 2A 2E 70 64 66 00  ptx.*.txt.*.pdf.
00000090  2A 2E 64 6A 76 75 00 2A 2E 68 74 6D 00 2A 2E 68  *.djvu.*.htm.*.h
000000A0  74 6D 6C 00 2A 2E 6D 64 62 00 2A 2E 63 65 72 00  tml.*.mdb.*.cer.
000000B0  2A 2E 70 31 32 00 2A 2E 70 66 78 00 2A 2E 6B 77  *.p12.*.pfx.*.kw
000000C0  6D 00 2A 2E 70 77 6D 00 2A 2E 31 63 64 00 2A 2E  m.*.pwm.*.1cd.*.
000000D0  6D 64 00 2A 2E 6D 64 66 00 2A 2E 64 62 66 00 2A  md.*.mdf.*.dbf.*
000000E0  2E 6F 64 74 00 2A 2E 76 6F 62 00 2A 2E 69 66 6F  .odt.*.vob.*.ifo
000000F0  00 2A 2E 6C 6E 6B 00 2A 2E 74 6F 72 72 65 6E 74  .*.lnk.*.torrent
00000100  00 2A 2E 6D 6F 76 00 2A 2E 6D 32 76 00 2A 2E 33  .*.mov.*.m2v.*.3
00000110  67 70 00 2A 2E 6D 70 65 67 00 2A 2E 6D 70 67 00  gp.*.mpeg.*.mpg.
00000120  2A 2E 66 6C 76 00 2A 2E 61 76 69 00 2A 2E 6D 70  *.flv.*.avi.*.mp
00000130  34 00 2A 2E 77 6D 76 00 2A 2E 64 69 76 78 00 2A  4.*.wmv.*.divx.*
00000140  2E 6D 6B 76 00 2A 2E 6D 70 33 00 2A 2E 77 61 76  .mkv.*.mp3.*.wav
00000150  00 2A 2E 66 6C 61 63 00 2A 2E 61 70 65 00 2A 2E  .*.flac.*.ape.*.
00000160  77 6D 61 00 2A 2E 61 63 33 00 2A 2E 65 78 65 00  wma.*.ac3.*.exe.
00000170  2A 2E 70 68 70 00 2A 2E 70 79 00 2A 2E 70 79 00  *.php.*.py.*.py.
00000180  2A 2E 68 00 2A 2E 73 6C 6E 00 2A 2E 64 6C 6C 00  *.h.*.sln.*.dll.
00000190  2A 2E 7A 69 70 00 2A 2E 72 61 72 00 38 02 00 00  *.zip.*.rar.8...
000001A0  59 6F 75 20 48 61 76 65 20 42 65 65 6E 20 46 75  You Have Been Fu
000001B0  63 6B 65 64 20 42 79 20 57 41 52 4C 4F 43 4B 20  cked By WARLOCK
000001C0  44 41 52 4B 20 41 52 4D 59 0D 0A 0D 0A 41 6C 6C  DARK ARMY....All
000001D0  20 6F 66 20 79 6F 75 72 20 66 69 6C 65 73 20 68   of your files h
000001E0  61 76 65 20 62 65 65 6E 20 65 6E 63 72 79 70 74  ave been encrypt
000001F0  65 64 0D 0A 59 6F 75 72 20 63 6F 6D 70 75 74 65  ed..Your compute
00000200  72 20 77 61 73 20 69 6E 66 65 63 74 65 64 20 77  r was infected w
00000210  69 74 68 20 61 20 72 61 6E 73 6F 6D 77 61 72 65  ith a ransomware
00000220  20 76 69 72 75 73 2E 20 59 6F 75 72 20 66 69 6C   virus. Your fil
00000230  65 73 20 68 61 76 65 20 62 65 65 6E 20 65 6E 63  es have been enc
00000240  72 79 70 74 65 64 20 61 6E 64 20 79 6F 75 20 77  rypted and you w
00000250  6F 6E 27 74 20 0D 0A 62 65 20 61 62 6C 65 20 74  on't ..be able t
00000260  6F 20 64 65 63 72 79 70 74 20 74 68 65 6D 20 77  o decrypt them w
00000270  69 74 68 6F 75 74 20 6F 75 72 20 68 65 6C 70 2E  ithout our help.
00000280  57 68 61 74 20 63 61 6E 20 49 20 64 6F 20 74 6F  What can I do to
00000290  20 67 65 74 20 6D 79 20 66 69 6C 65 73 20 62 61   get my files ba
000002A0  63 6B 3F 59 6F 75 20 63 61 6E 20 62 75 79 20 6F  ck?You can buy o
000002B0  75 72 20 73 70 65 63 69 61 6C 20 0D 0A 64 65 63  ur special ..dec
000002C0  72 79 70 74 69 6F 6E 20 73 6F 66 74 77 61 72 65  ryption software
000002D0  2C 20 74 68 69 73 20 73 6F 66 74 77 61 72 65 20  , this software
000002E0  77 69 6C 6C 20 61 6C 6C 6F 77 20 79 6F 75 20 74  will allow you t
000002F0  6F 20 72 65 63 6F 76 65 72 20 61 6C 6C 20 6F 66  o recover all of
00000300  20 79 6F 75 72 20 64 61 74 61 20 61 6E 64 20 72   your data and r
00000310  65 6D 6F 76 65 20 74 68 65 0D 0A 72 61 6E 73 6F  emove the..ranso
00000320  6D 77 61 72 65 20 66 72 6F 6D 20 79 6F 75 72 20  mware from your
00000330  63 6F 6D 70 75 74 65 72 2E 54 68 65 20 70 72 69  computer.The pri
00000340  63 65 20 66 6F 72 20 74 68 65 20 73 6F 66 74 77  ce for the softw
00000350  61 72 65 20 69 73 20 24 31 2C 35 30 30 2E 20 50  are is $1,500. P
00000360  61 79 6D 65 6E 74 20 63 61 6E 20 62 65 20 6D 61  ayment can be ma
00000370  64 65 20 69 6E 20 42 69 74 63 6F 69 6E 20 6F 6E  de in Bitcoin on
00000380  6C 79 2E 0D 0A 43 6F 6E 74 61 63 74 3A 20 68 74  ly...Contact: ht
00000390  74 70 73 3A 2F 2F 74 2E 6D 65 2F 57 41 52 4C 4F  tps://t.me/WARLO
000003A0  43 4B 5F 44 41 52 4B 5F 41 52 4D 59 5F 4F 46 46  CK_DARK_ARMY_OFF
000003B0  49 43 49 41 4C 53 0D 0A 0D 0A 42 69 74 63 6F 69  ICIALS....Bitcoi
000003C0  6E 20 41 64 64 72 65 73 73 3A 20 2E 2E 2E 2E 2E  n Address: .....
000003D0  2E 2E 2E 0D 0A 0D 0A 00 19 00 00 00 77 61 72 6C  ............warl
000003E0  6F 63 6B 64 61 72 6B 61 72 6D 79 6F 66 66 69 63  ockdarkarmyoffic
000003F0  69 61 6C 73 00 8F AB FC F1 29 EE A7 B9 C0 DE FD  ials..«üñ)î§¹ÀÞý
00000400  57 DB 00 CC D7 01 01 01 01 01 4E 79 67 69 32 36  WÛ.Ì×.....Nygi26
```

```
00000410  58 41 70 77 56 73 4B 69 63 00 4B 52 4B 4B 48 43  XApwVsKic.KRKKHC
00000420  52 41 50 50 52 4A 49 53 48 00 05 00 00 00 30 00  RAPPRJISH.....0.
00000430  00 00 66 00 00 00 17 E2 13 00                    ..f....â..
```

Figure 5: Decrypted resource

At first glance it is evident that this data blob contains information that is used during the ransomware encryption process, like list of extensions to look for and the ransom note etc. Here the first DWORD which is highlighted in BLUE denotes the size of the data block that follows, which are relevant extensions to look for encryption. The DWORD is little endian, denoting that this block is 0x198 bytes.

At the end of this block of data is another DWORD, highlighted green, which has the size of the next block of data holding the ransom note or the content of the readme text (0x238 is the number in little endian). The next DWORD highlighted red represents the extension of the files after encryption, which is ".warlockdarkarmyofficials".

After 0x10 bytes there is a value 01. If 01 is present then the below HKCR entries are written to the Windows Registry. The ransomware sets an entry under HKCR with the key name "KRKKHCRAPPRJISH", highlighted orange. There are Shell->open->command entries under this key which defaults to the malware's self-copy location. Mostly done to set default icons for specific file types.

```
call    CloseHandle
cmp     byte_407529, 1
jnz     short loc_4022D3

push    offset str_ptr_TempPath_str_Nygi26XApwVsKic_exe ; lpString
push    offset ValueName ; "Alcmeter"
push    offset SubKey    ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe"...
push    80000002h        ; hKey
call    mw_set_persistence_hkcr
```

Figure 6 : Compare DWord to set persistence

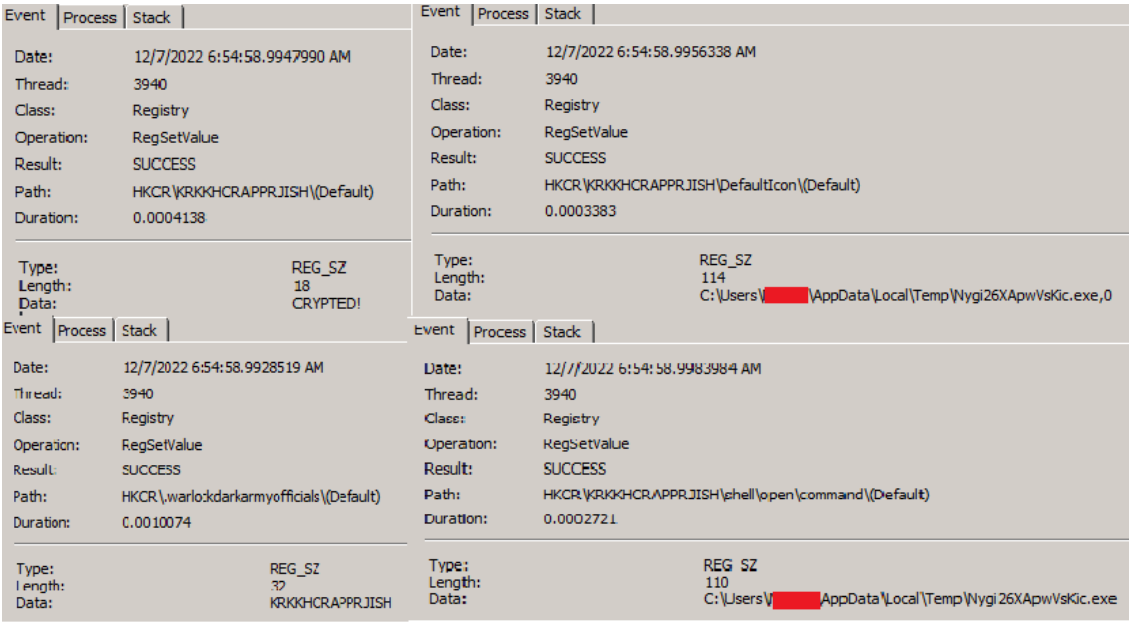


Figure 7: HKCR Shell->open->command entries

The DWORD highlighted in purple denotes the number of bytes to skip when the malware starts to encrypt a file, 0x66 bytes in this case.

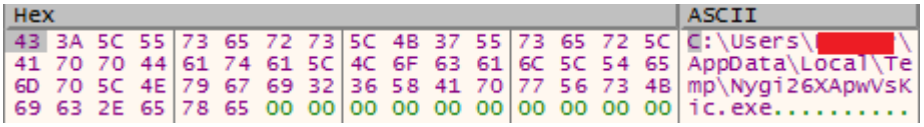


Figure 8 : Self copy

After execution it copies itself with the filename of “Nygi26XApwVsKic” to the temp folder.

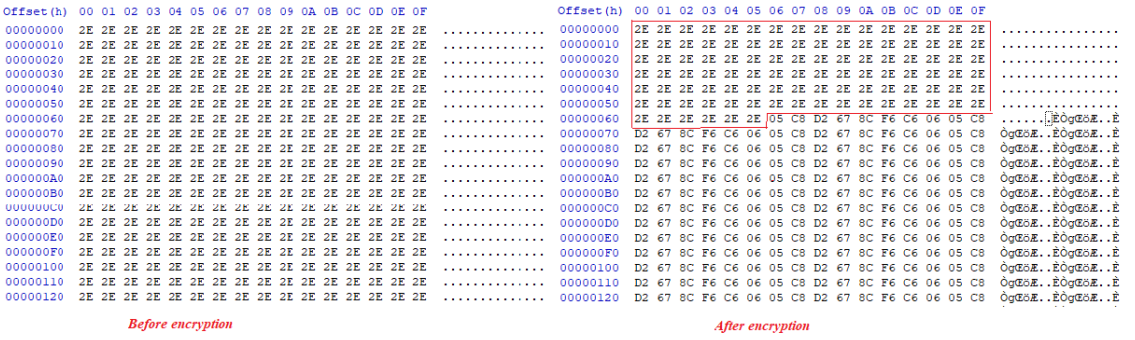


Figure 9: View of a file before and after encryption

It then sets persistence via the run registry.

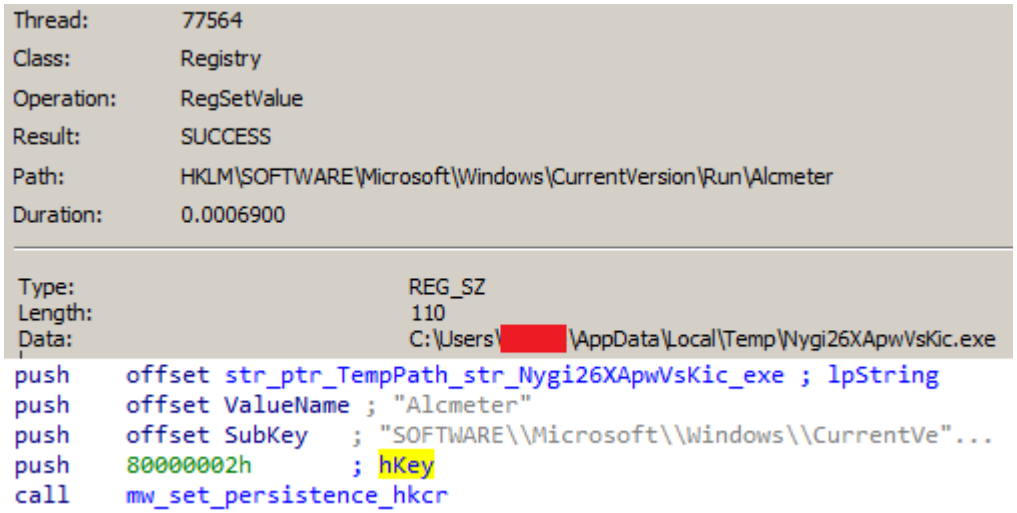


Figure 10 : Run registry

The algorithm used in this malware is **“Tiny encryption algorithm”**. This is one key difference between Chaos and this ransomware, Chaos uses AES.

```
uint uVar1;
uint uVar2;
int iVar3;

uVar1 = *param_1;
uVar2 = param_1[1];
iVar3 = 0;
uVar1 = uVar1 >> 0x18 | (uVar1 & 0xff0000) >> 8 | (uVar1 & 0xff00) << 8 | uVar1 << 0x18;
uVar2 = uVar2 >> 0x18 | (uVar2 & 0xff0000) >> 8 | (uVar2 & 0xff00) << 8 | uVar2 << 0x18;
do {
  uVar1 = uVar1 + (uVar2 * 0x10 + _DAT_00406585 ^ iVar3 + -0x61c88647 + uVar2 ^
                   (uVar2 >> 5) + _DAT_00406589);
  uVar2 = uVar2 + (uVar1 * 0x10 + _DAT_0040658d ^ iVar3 + -0x61c88647 + uVar1 ^
                   (uVar1 >> 5) + _DAT_00406591);
  iVar3 = iVar3 + 0x3c6ef372;
  uVar1 = uVar1 + (uVar2 * 0x10 + _DAT_00406585 ^ iVar3 + uVar2 ^ (uVar2 >> 5) + _DAT_00406589);
  uVar2 = uVar2 + (uVar1 * 0x10 + _DAT_0040658d ^ iVar3 + uVar1 ^ (uVar1 >> 5) + _DAT_00406591);
} while (iVar3 != DAT_004065a5 * -0x61c88647);
*param_2 = uVar1 >> 0x18 | (uVar1 & 0xff0000) >> 8 | (uVar1 & 0xff00) << 8 | uVar1 * 0x1000000;
param_2[1] = uVar2 >> 0x18 | (uVar2 & 0xff0000) >> 8 | (uVar2 & 0xff00) << 8 | uVar2 * 0x1000000;
return;
```

Figure 11 : Encryption code

After the encryption of all the files, it leaves a ransom message as shown below:

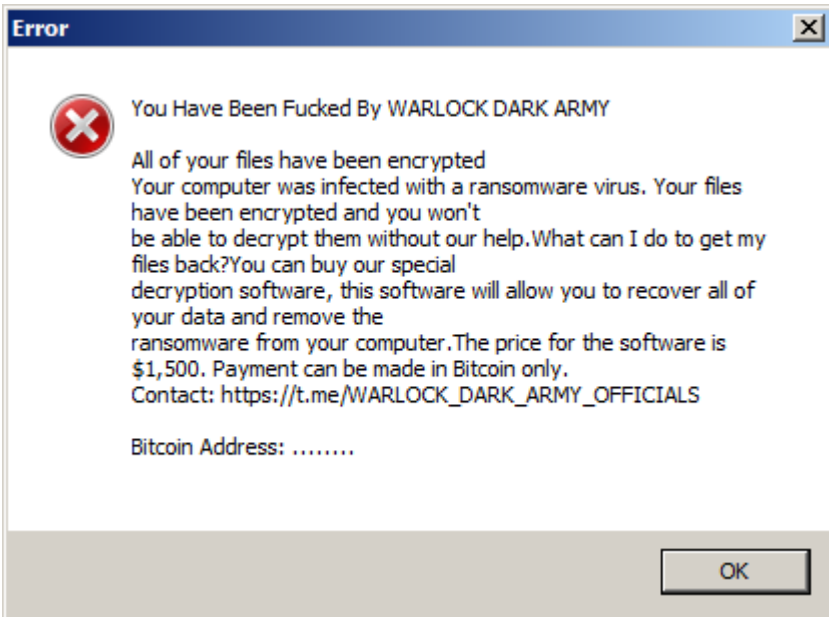


Figure 12 : Ransom note

In the above message the actors have not mentioned any cryptocurrency wallet's address for making the ransom payment, they have however mentioned a Telegram channel for the payment and decryption, it goes without saying that one should not attempt to pay up the ransom to get the files back.

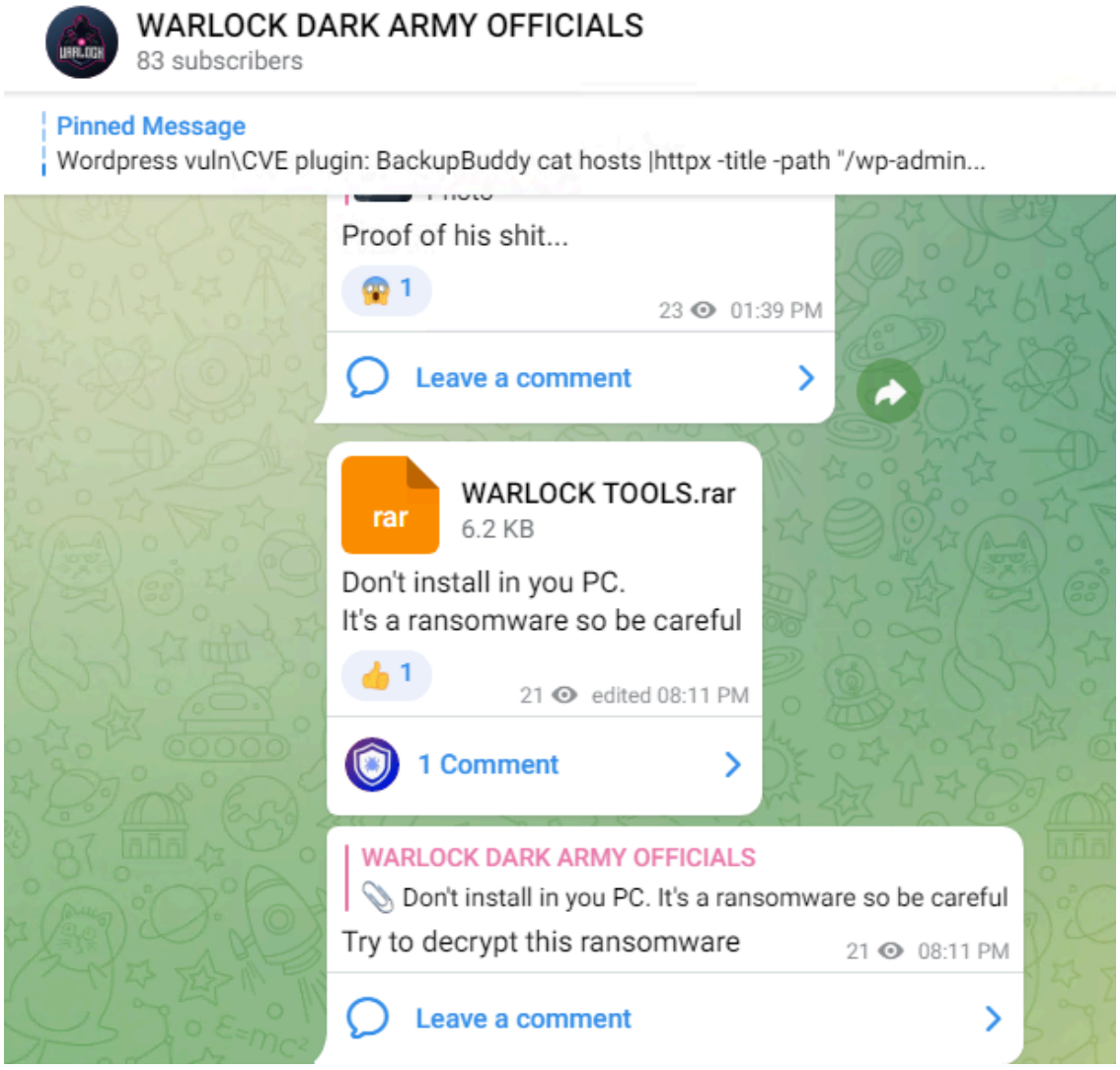


Figure 13 : Telegram channel

This Telegram channel also acts as a marketplace for malware distribution, apart from being used as the payment channel.

This group had their social media pages in Facebook and Instagram as well, but were taken down. Shown below is the Facebook page of Warlock Dark Army, one can note the identical profile pictures though (Ref. Telegram group profile pic and Facebook profile pic). The similarities are only in the naming and the images, but based on the TTPs we can say that both are unrelated.

Figure 14: Facebook page of Warlock Dark Army

We at K7 labs provide detection against such threats. Users are advised to use a reliable security product such as **“K7 Total Security”** and keep it up-to-date so as to safeguard their devices.

IOCs

Hash : f0979d897155f51fd96a63c61e05d85c

Detection name : Ransomware (005451b81)

Source: https://labs.k7computing.com/index.php/ransomed-by-warlock-dark-army-officials/