

# 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.

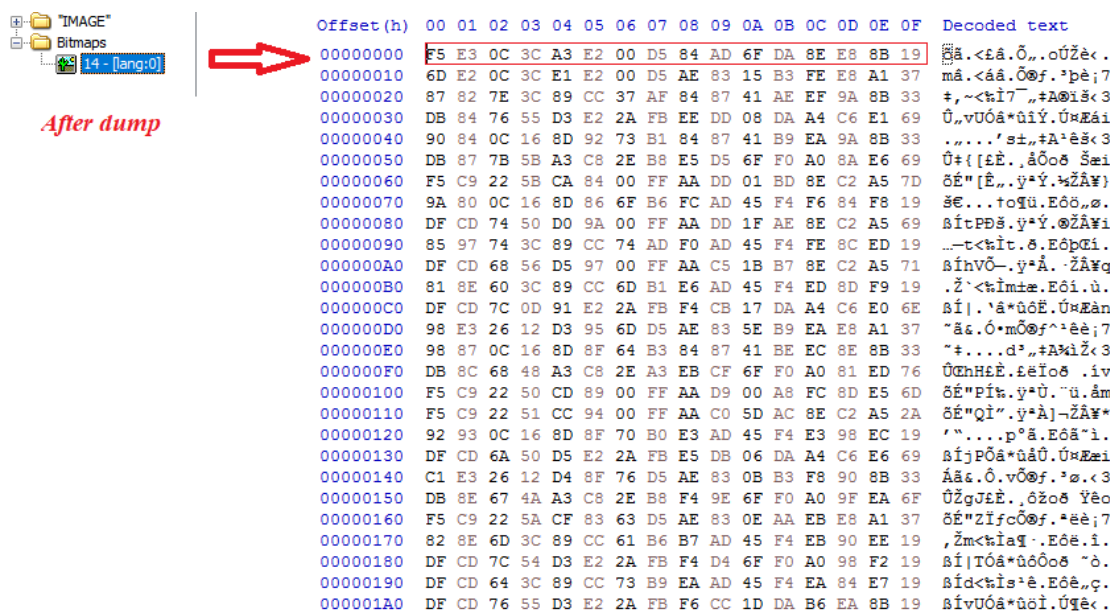


Figure 1: Encrypted blob in resource section

```

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.

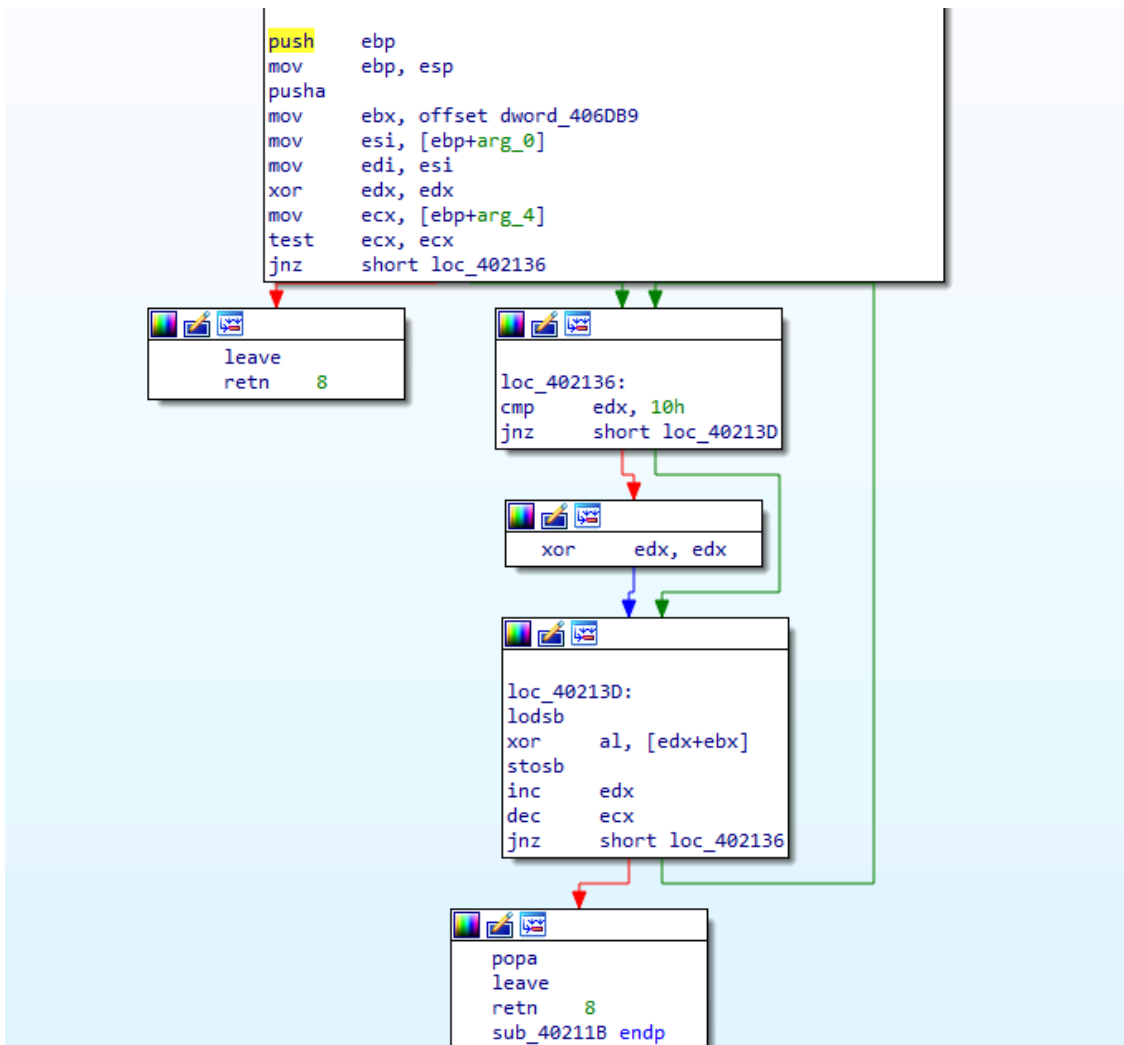


Figure 3 : Xor decryption in memory

The screenshot shows the CyberChef web interface. On the left, the 'From Hex' tool is active with a 'Space' delimiter. Below it, the 'XOR' tool is active with a key of 'F5 E3 0C 3C A3 E2 00 D5 84 A...' and a 'Standard' scheme. A 'Null preserving' checkbox is unchecked. The main area displays a hex dump of the encrypted data. The 'Output' section shows the decrypted text, which is a ransomware message. The message includes a list of file extensions that have been encrypted, a demand for \$1,500 in Bitcoin, and contact information for the ransomware operators.

```
6D E2 0C 3C E1 E2 00 D5 AE 83 15 B3 FE E8 A1 37 87 82 7E 3C 89 CC 37 AF 84 87 41
AE EF 9A 8B 33 DB 84 76 55 D3 E2 2A FB EE DD 08 DA A4 C6 E1 69 90 84 0C 16 8D 92
73 B1 84 87 41 B9 EA 9A 8B 33 DB 87 7B 5B A3 C8 2E B8 E5 D5 6F F0 A0 8A E6 69 F5
C9 22 5B CA 84 00 FF AA DD 01 BD 8E C2 A5 7D 9A 80 0C 16 8D 86 6F B6 FC AD 45 F4
F6 84 F8 19 DF CD 74 50 D0 9A 00 FF AA DD 1F AE 8E C2 A5 69 85 97 74 3C 89 CC 74
AD F0 AD 45 F4 FE 8C ED 19 DF CD 68 56 D5 97 00 FF AA C5 1B B7 8E C2 A5 71 81 8E
60 3C 89 CC 6D B1 E6 AD 45 F4 ED 8D F9 19 DF CD 7C 0D 91 E2 2A FB F4 CB 17 DA A4
C6 E0 6E 98 E3 26 12 D3 95 6D D5 AE 83 5E B9 EA E8 A1 37 98 87 0C 16 8D 8F 64 B3
84 87 41 BE EC 8E 8B 33 DB 8C 68 48 A3 C8 2E A3 EB CF 6F F0 A0 81 ED 76 F5 C9 22
50 CD 89 00 FF AA D9 00 A8 FC 8D E5 6D F5 C9 22 51 CC 94 00 FF AA C0 5D AC 8E C2
A5 2A 92 93 0C 16 8D 8F 70 B0 E3 AD 45 F4 E3 98 EC 19 DF CD 6A 50 D5 E2 2A FB E5
DB 06 DA A4 C6 E6 69 C1 E3 26 12 D4 8F 76 D5 AE 83 0B B3 F8 90 8B 33 DB 8E 67 4A
A3 C8 2E B8 F4 9E 6F F0 A0 9F EA 6F F5 C9 22 5A CF 83 63 D5 AE 83 0E AA EB E8 A1
37 82 8E 6D 3C 89 CC 61 B6 B7 AD 45 F4 EB 90 EE 19 DF CD 7C 54 D3 E2 2A FB F4 D4
6F F0 A0 98 F2 19 DF CD 64 3C 89 CC 73 B9 EA AD 45 F4 EA 84 E7 19 DF CD 76 55 D3
E2 2A FB F6 CC 1D DA B6 EA 8B 19 AC 8C 79 1C EB 83 76 B0 A4 EF 0A BF E0 C8 CD 6C
96 88 69 58 83 A0 79 F5 D3 EC 3D 96 C1 AB C0 39 B1 A2 5E 77 83 A3 52 98 DD A0 65
07 84 A0 E7 7E 0F 8C 6A 1C D8 0D 7E A7 A4 C0 0E 8E F0 00 80 71 84 0F 60 1C C1 87
time: 4ms
length: 1062
lines: 12
```

**Output**

```
...B...*.zip*.rar*.7z*.tar*.gzip*.jpg*.jpeg*.psd*.cdr*.dwg*.max*.bmp
*.gif*.png*.doc*.docx*.xls*.xlsx*.ppt*.pptx*.txt*.pdf*.djvu*.htm*.h
tml*.mdb*.cer*.p12*.pfx*.kwm*.pwm*.1cd*.md*.mdf*.dbf*.odt*.vob*.ifo
*.lnk*.torrent*.mov*.m2v*.3gp*.mpeg*.mpg*.flv*.avi*.mp4*.wmv*.divx*.
mkv*.mp3*.wav*.flac*.ape*.wma*.ac3*.exe*.php*.py*.h*.sln*.dll
*.zip*.rar.8...You Have Been Fucked By WARLOCK DARK ARMY

All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been
encrypted and you won't
be able to decrypt them without our help.What can I do to get my files back?You
can buy our special
decryption software, this software will allow you to recover all of your data
and remove the
ransomware from your computer.The price for the software is $1,500. Payment can
be made in Bitcoin only.
Contact: https://t.me/WARLOCK_DARK_ARMY_OFFICIALS
```

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 12 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 70 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 *.pl2.*.pfx.*.kw
000000C0 6D 00 2A 2E 70 77 6D 00 2A 2E 31 63 64 00 2A 2E m.*.pwm.*.lcd.*.
000000D0 6D 64 00 2A 2E 6D 64 66 00 2A 2E 64 62 66 00 2A md.*.mdf.*.dhf.*
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 *.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 ryped 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 remove 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 67 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..«űñ»İŞ'ÀBý
00000400 57 DB 00 CC D7 01 01 01 01 01 4E 79 67 69 32 36 WŪ.İx*....Nyqi26

```

```

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 RAPPJISH.....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 “KRKKHCRAPPJISH”, 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

Event	Process	Stack	Event	Process	Stack
Date:	12/7/2022 6:54:58.9947990 AM		Date:	12/7/2022 6:54:58.9956338 AM	
Thread:	3940		Thread:	3940	
Class:	Registry		Class:	Registry	
Operation:	RegSetValue		Operation:	RegSetValue	
Result:	SUCCESS		Result:	SUCCESS	
Path:	HKCR\KRXKHCRAPPRJISH\Default		Path:	HKCR\KRXKHCRAPPRJISH\DefaultIcon\Default	
Duration:	0.0004138		Duration:	0.0003383	
Type:	REG_SZ		Type:	REG_SZ	
Length:	18		Length:	114	
Data:	CRYPTED!		Data:	C:\Users\██████████\AppData\Local\Temp\Nygi26XApwVsKic.exe,0	
Event	Process	Stack	Event	Process	Stack
Date:	12/7/2022 6:54:58.9928519 AM		Date:	12//2022 6:54:58.9983984 AM	
Thread:	3940		Thread:	3940	
Class:	Registry		Class:	Registry	
Operation:	RegSetValue		Operation:	RegSetValue	
Result:	SUCCESS		Result:	SUCCESS	
Path:	HKCR\warlockdarkarmyofficials\Default		Path:	HKCR\KRXKHCRAPPRJISH\shell\open\command\Default	
Duration:	0.0010074		Duration:	0.0002721	
Type:	REG_SZ		Type:	REG_SZ	
Length:	37		Length:	110	
Data:	KRXKHCRAPPRJISH		Data:	C:\Users\██████████\AppData\Local\Temp\Nygi26XApwVsKic.exe	

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.

Hex	ASCII
43 3A 5C 55 73 65 72 73 5C 4B 37 55 73 65 72 5C	C:\Users\██████████\
41 70 70 44 61 74 61 5C 4C 6F 63 61 6C 5C 54 65	AppData\Local\Te
6D 70 5C 4E 79 67 69 32 36 58 41 70 77 56 73 4B	mp\Nygi26XApwVsK
69 63 2E 65 78 65 00 00 00 00 00 00 00 00 00 00	ic.exe.....

Figure 8 : Self copy

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

Offset (h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Offset (h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000000	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E
00000010	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000010	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E
00000020	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000020	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E
00000030	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000030	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E
00000040	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000040	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E
00000050	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000050	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E
00000060	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000060	2E 2E 2E 2E 2E 2E 2E 2E 05 C8 D2 67 8C F6 C6 06 05 C8
00000070	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000070	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
00000080	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000080	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
00000090	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000090	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
000000A0	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	000000A0	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
000000B0	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	000000B0	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
000000C0	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	000000C0	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
000000D0	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	000000D0	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
000000E0	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	000000E0	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
000000F0	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	000000F0	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
00000100	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000100	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
00000110	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000110	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8
00000120	2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E	00000120	D2 67 8C F6 C6 06 05 C8 D2 67 8C F6 C6 06 05 C8

Before encryption

After encryption

Figure 9: View of a file before and after encryption

It then sets persistence via the run registry.

Thread:	77564
Class:	Registry
Operation:	RegSetValue
Result:	SUCCESS
Path:	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Alcmeter
Duration:	0.0006900

---

Type:	REG_SZ
Length:	110
Data:	C:\Users\██████████\AppData\Local\Temp\Nygi26XApwVsKic.exe

```

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

```

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:

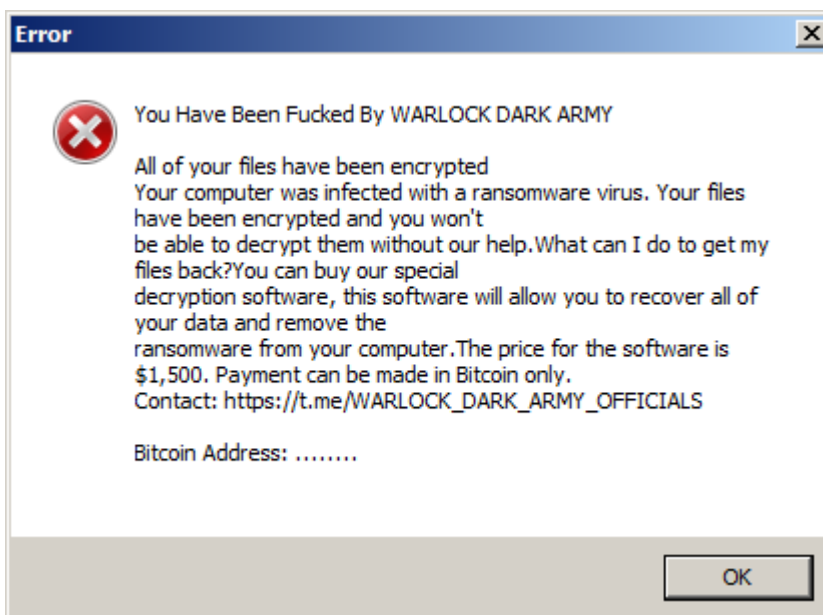


Figure 12 : Ransom note

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.

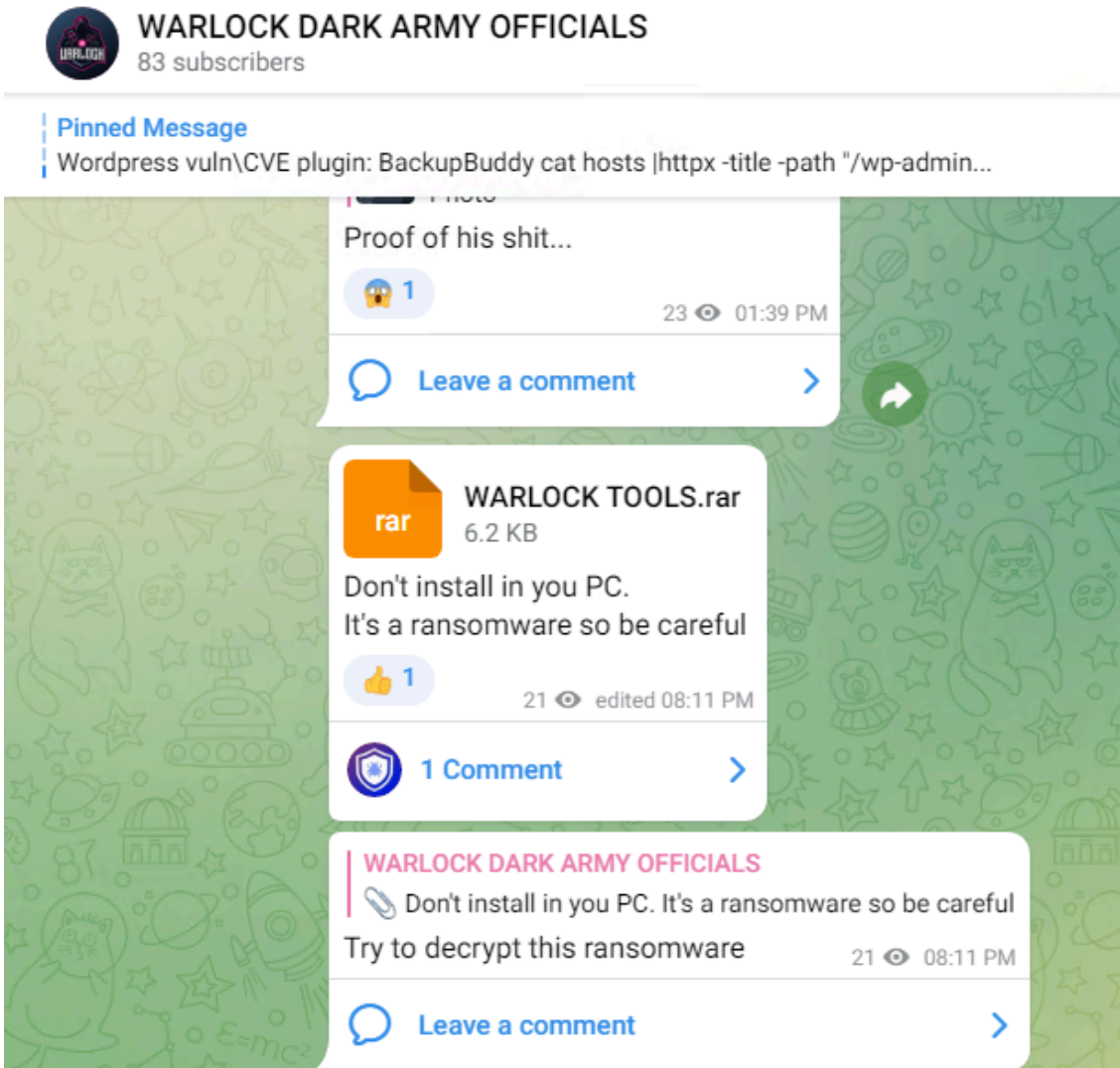


Figure 13 : Telegram channel

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.

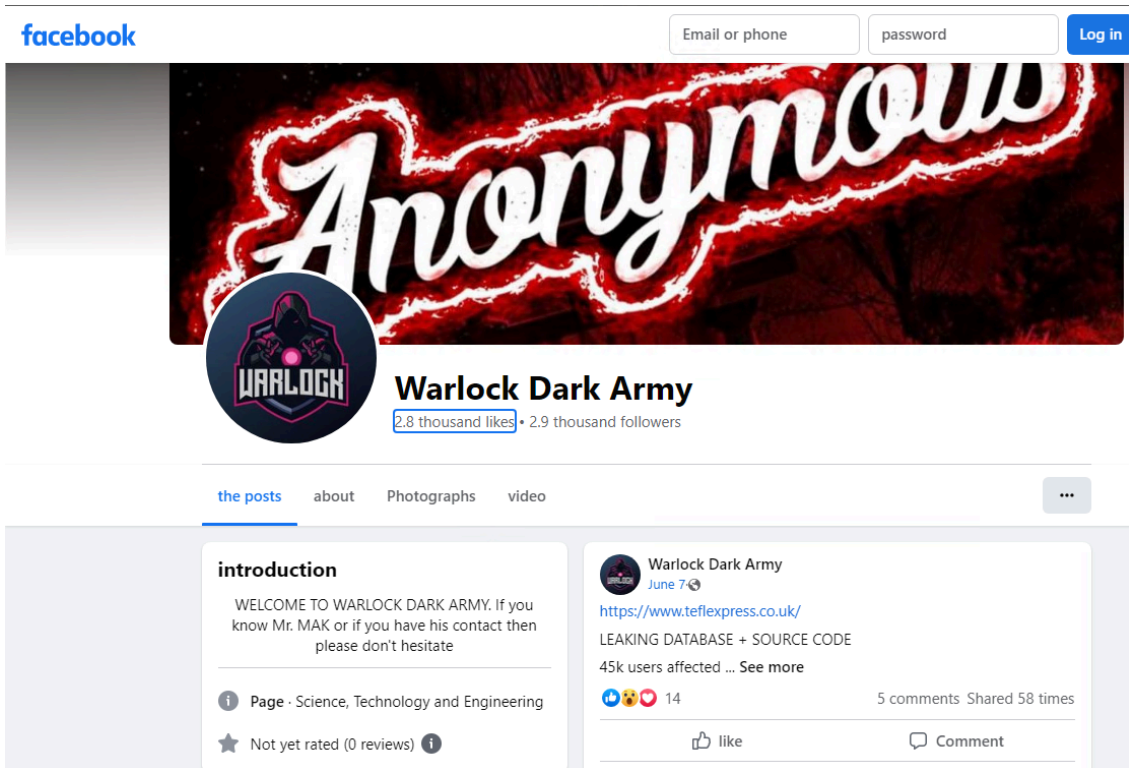


Figure 14: Facebook page of Warlock Dark Army

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/>