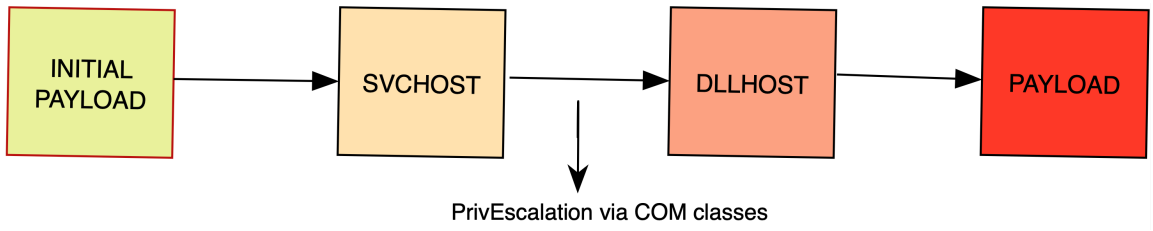
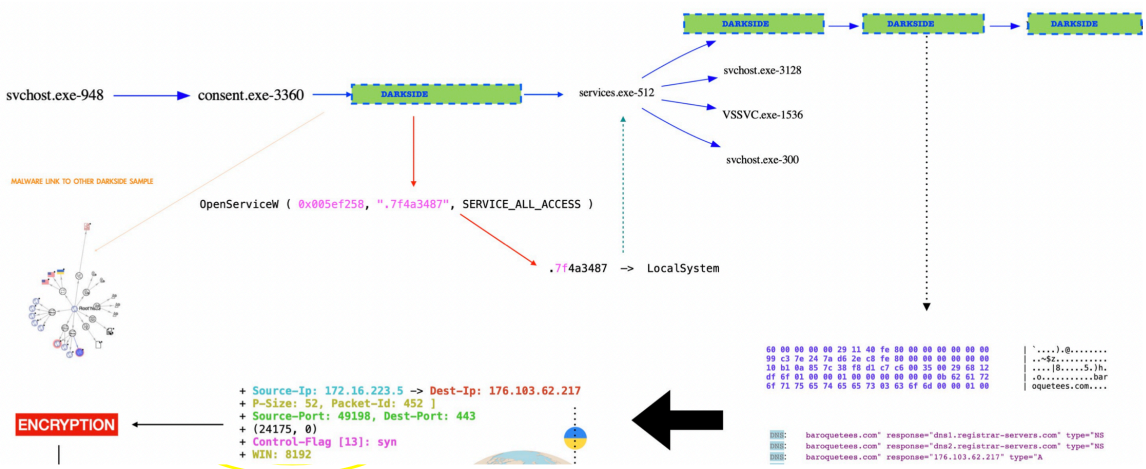
BLACKMATTER

UDURRANI

BlackMatter Ransomware encrypted all your files!
To get your data back and keep your privacy safe,



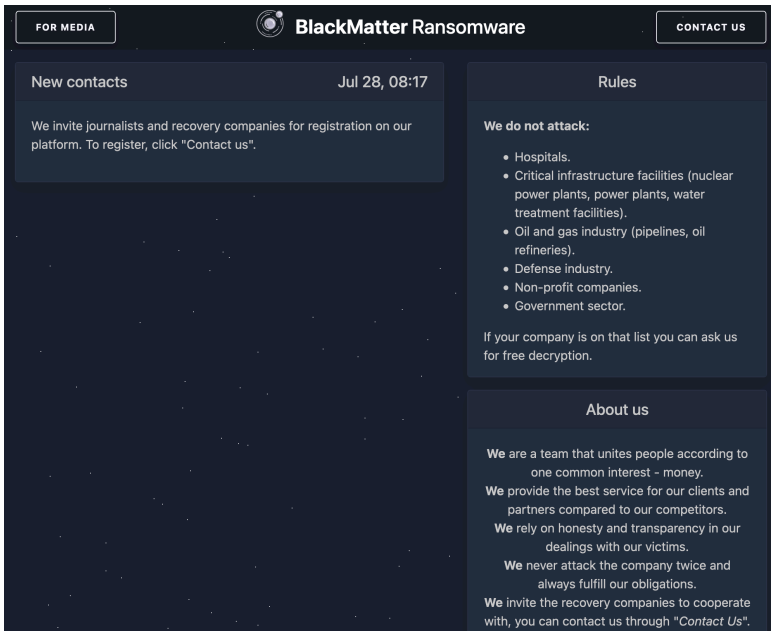
BlackMatter is a successor to **DarkSide** and **Sodinokibi** ransomware. Let's take a quick look at the previous DarkSide ransomware flow.



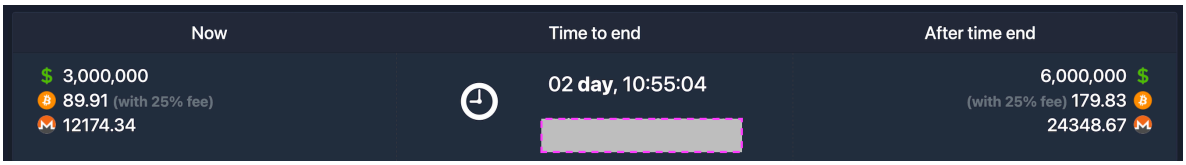
A quick look at **Sodinokibi** Ransomware and its obfuscation:

https://udurrani.com/0fff/ransomware_using_net_assemblies/

BlackMatter operates in a similar fashion to its predecessor DarkSide. It tries to gain the right privileges to conduct all the activities. The group has adapted new techniques and developed features to exfiltrate/push files before the actual encryption starts. The group maintains its presence on the dark web.

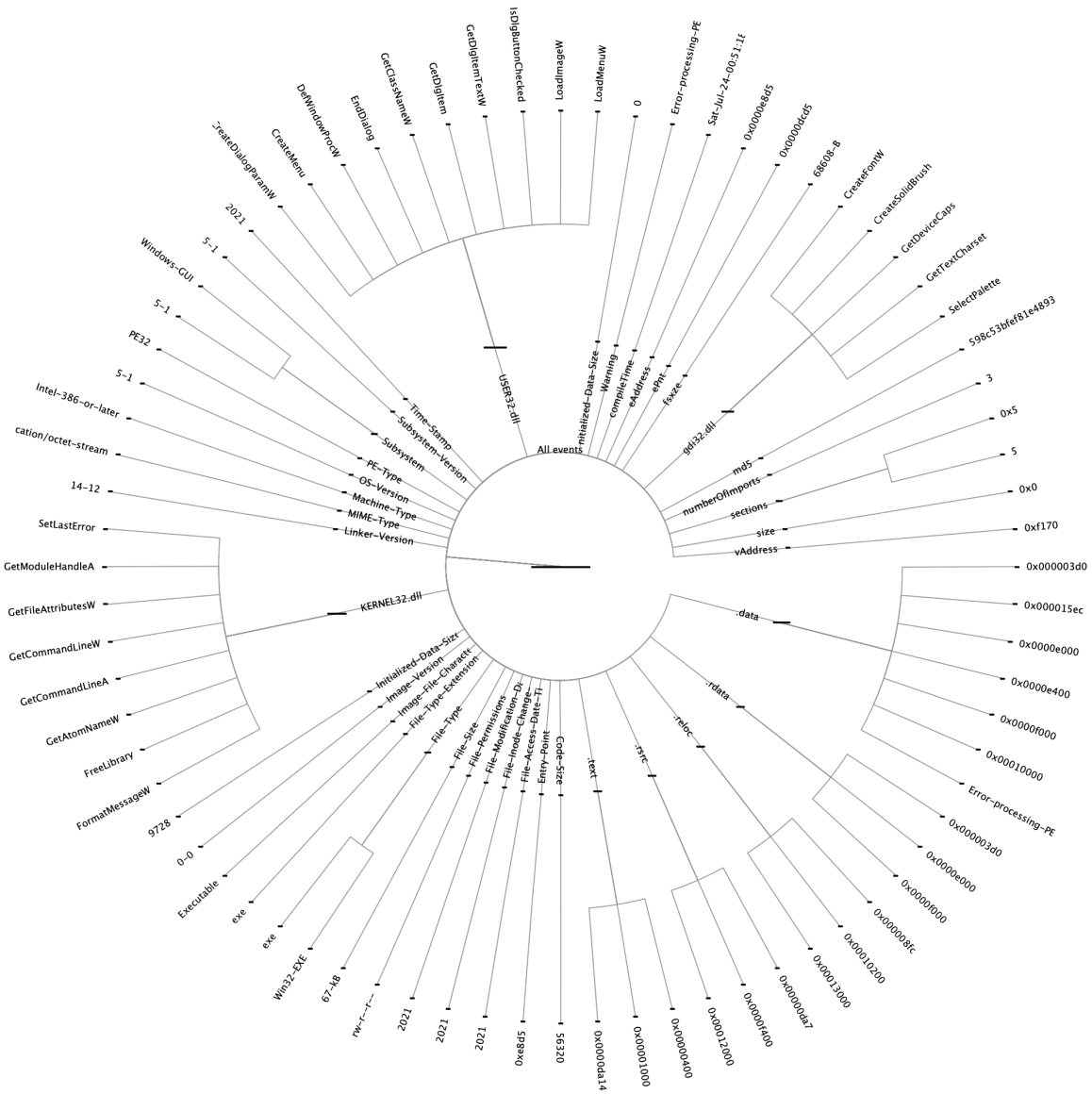


Depending on the company, the initial price is pretty high.

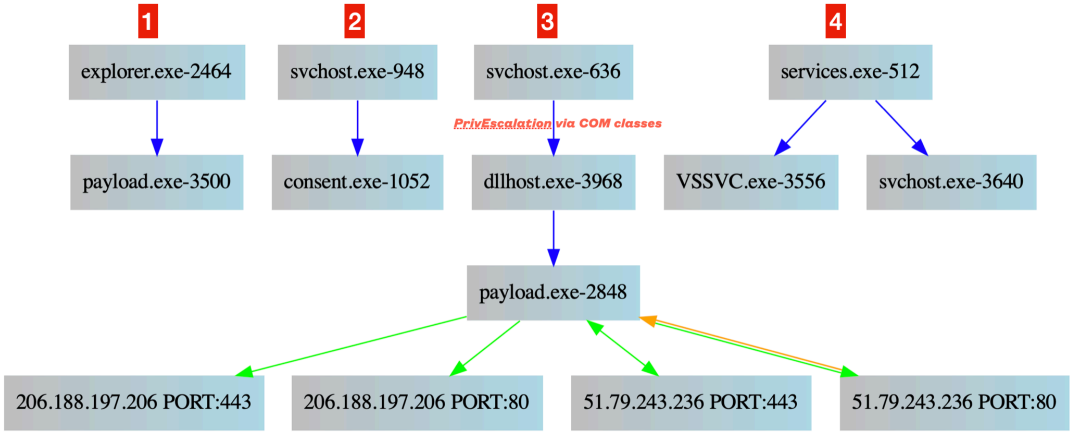


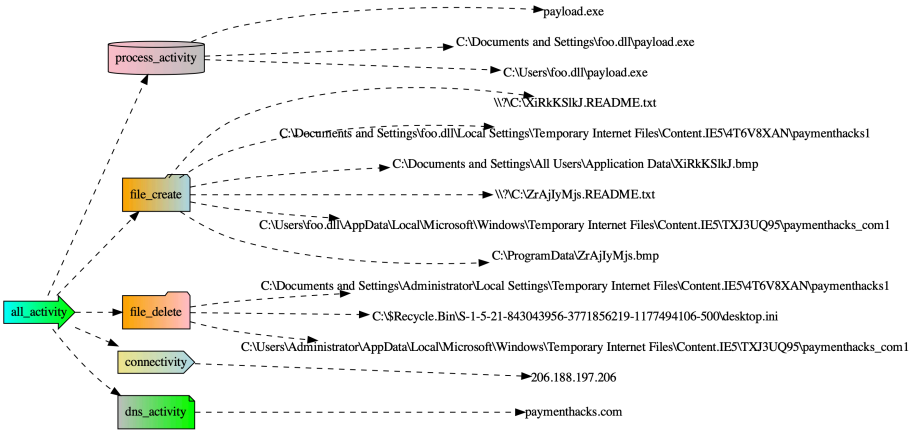
The threat group creates a unique payload for each victim (company). The payload eventually creates a special URL that can be mapped to the victim. This way the victim can easily communicate to the threat actor.

PE VIEW:


All events
USER32.dll
IsDlgButtonChecked
LoadImageW
LoadMenuW
GetDlgItemTextW
GetDlgItem
GetClassNameW
EndDialog
DefWindowProcW
CreateMenu
CreateDialogParamW
Time-Stamp
Subsystem-Version
Subsystem
PE-Type
OS-Version
Machine-Type
MIME-Type
Linker-Version
2021
5-1
Windows-GUI
5-1
PE32
5-1
Intel-386-or-later
cation/octet-stream
14-12
KERNEL32.dll
SetLastError
GetModuleHandleA
GetFileAttributesW
GetCommandLineW
GetCommandLineA
GetAtomNameW
FreeLibrary
FormatMessageW
9728
0-0
Executable
exe
exe
Win32-EXE
67-kB
rw-r--r--
2021
2021
2021
5f68x0
56320
Code-size
Entry-Point
File-Access-Date-Ti
File-Modification-Da
File-Permissions
File-Size
File-Type
File-Type-Extension
Image-File-Characte
Image-Version
Initialized-Data-Size
.text
0x00004a14
0x00001000
0x00000400
.rsrc
0x00012000
0x0000f400
.reloc
0x000004a7
.rdata
0x00013000
0x00010200
0x000008fc
0x0000f000
0x0000e000
0x000003d0
Error-processing-PE
0x00010000
0x0000f000
0x0000e400
0x0000e000
0x000015ec
0x000003d0
.data
vAddress
size
sections
numberOfImports
md5
gdi32.dll
fsxze
eAddress
compileTime
Warning
Initialized-Data-Size
0
LoadMenuW
LoadImageW
IsDlgButtonChecked
GetDlgItemTextW
GetDlgItem
GetClassNameW
EndDialog
DefWindowProcW
CreateMenu
CreateDialogParamW
Error-processing-PE
Sat-Jul-24-00:51:1
0x0000e8d5
0x0000dcd5
68608-B
CreateFontW
CreateSolidBrush
GetDeviceCaps
GetTextCharset
SelectPalette
598c53bfef81e4893
3
0x5
5
0x0
0xf170

THE FLOW:

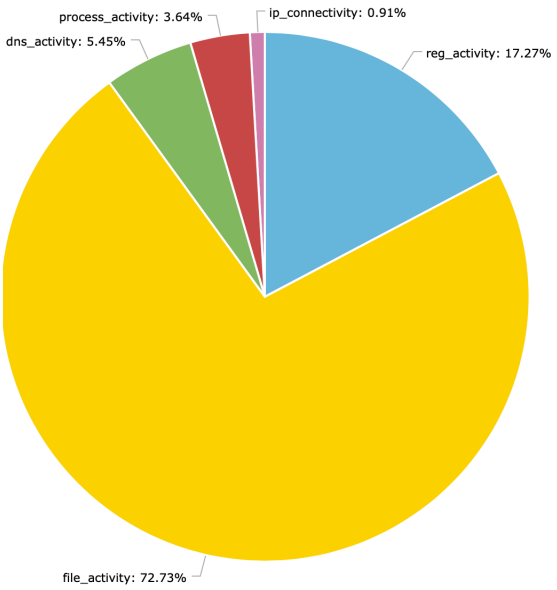





```
DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}

C:\Windows\SysWOW64\dllhost.exe -> payload.exe

C:\Windows\system32\vssvc.exe
C:\Windows\System32\svchost.exe -k swprv
```



ON THE WIRE:

```
60 09 00 00 00 3a 11 40 fe 80 00 00 00 00 00 00        | `....:.@........
10 f2 f0 0b 02 30 7e 18 fe 80 00 00 00 00 00 00        | .....0~.........
99 c3 7e 24 7a d6 2e c8 00 35 eb 0b 00 3a 40 1a        | ..~$z....5...:@.
b1 cc 81 80 00 01 00 01 00 00 00 00 0c 70 61 79        | .............pay
6d 65 6e 74 68 61 63 6b 73 03 63 6f 6d 00 00 01        | menthacks.com...
00 01 c0 0c 00 01 00 01 00 00 08 ca 00 04 ce bc        | ................
c5 ce
```

```
+ Source-Ip: 172.16.223.5 -> Dest-Ip: 206.188.197.206
+ P-Size: 48, Packet-Id: 9445 ]
+ Source-Port: 50693, Dest-Port: 80
+ (35839, 0)
+ Control-Flag [13]: syn
+ WIN: 8192
```

```
45 00 00 30 24 e5 40 00 80 06 b6 41 ac 10 df 05        | E..0$.@....A....
ce bc c5 ce c6 05 00 50 8b ba f7 e9 00 00 00 00        | .......P........
70 02 20 00 f9 83 00 00 02 04 05 b4 01 01 04 02        | p. .............
```

```
60 09 00 00 00 37 11 40 fe 80 00 00 00 00 00 00        | `....7.@........
10 f2 f0 0b 02 30 7e 18 fe 80 00 00 00 00 00 00        | .....0~.........
99 c3 7e 24 7a d6 2e c8 00 35 d7 e8 00 37 40 17        | ..~$z....5...7@.
65 19 81 80 00 01 00 01 00 00 00 00 09 6d 6f 6a        | e............moj
6f 62 69 64 65 6e 03 63 6f 6d 00 00 01 00 01 c0        | obiden.com......
0c 00 01 00 01 00 00 08 ca 00 04 33 4f f3 ec          | ...........3O..
```

```
+ Source-Ip: 172.16.223.5 -> Dest-Ip: 51.79.243.236
+ P-Size: 427, Packet-Id: 9466 ]
+ Source-Port: 50698, Dest-Port: 80
+ (45055, 10747)
+ Control-Flag [13]: psh ack
+ WIN: 16698
```

```
45 00 01 ab 24 fa 40 00 80 06 22 01 ac 10 df 05        | E...$.@...".....
33 4f f3 ec c6 0a 00 50 af c9 f4 32 29 ca ba eb        | 3O.....P...2)...
50 18 41 3a b8 b7 00 00 50 4f 53 54 20 2f 3f 4e        | P.A:....POST /?N
36 4f 37 41 52 48 4d 6a 3d 39 53 33 57 78 75 30        | 6O7ARHMj=9S3Wxu0
4e 6d 71 4c 4f 6f 55 68 26 44 78 69 78 58 55 45        | NmqLOoUh&DxixXUE
46 71 3d 74 45 47 42 62 6e 72 33 65 75 30 47 6d        | Fq=tEGBbnr3eu0Gm
49 33 58 26 4d 32 56 43 69 4b 3d 64 61 67 4f 71        | I3X&M2VCiK=dagOq
53 4e 61 58 5a 4c 54 46 6f 65 56 75 45 4a 26 77        | SNaXZLTFoeVuEJ&w
52 66 57 54 6a 36 74 78 3d 48 52 42 68 72 6b 31        | RfWTj6tx=HRBhrk1
43 42 63 76 63 69 32 43 74 41 79 79 26 53 76 41        | CBcvci2CtAyy&SvA
49 64 4d 52 67 3d 4a 53 49 74 73 71 26 46 61 4f        | IdMRg=JSItsq&FaO
63 74 3d 4d 36 73 54 71 5a 67 72 48 4f 64 6e 38        | ct=M6sTqZgrHOdn8
39 58 26 6c 61 31 72 4d 6b 66 3d 7a 62 71 37 69        | 9X&la1rMkf=zbq7i
36 71 4c 6b 77 71 48 62 69 43 61 46 45 20 48 54        | 6qLkwqHbiCaFE HT
54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20        | TP/1.1..Accept:
2a 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a        | */*..Connection:
20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 63 63        |  keep-alive..Acc
65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a        | ept-Encoding: gz
69 70 2c 20 64 65 66 6c 61 74 65 2c 20 62 72 0d        | ip, deflate, br.
0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74        | .Content-Type: t
65 78 74 2f 70 6c 61 69 6e 0d 0a 55 73 65 72 2d        | ext/plain..User-
```