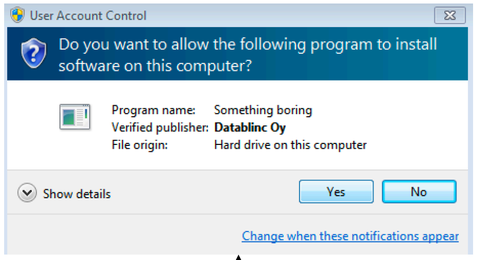
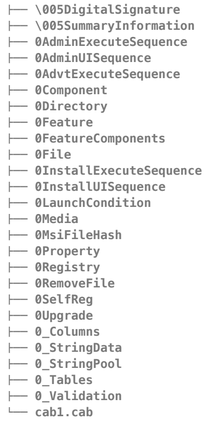
SEKMET RANSOMWARE

The malware comes in as windows update (KB083486A)
Once the msi is launched, it registers a DLL (DLLRegisterServer)



patch_may13869



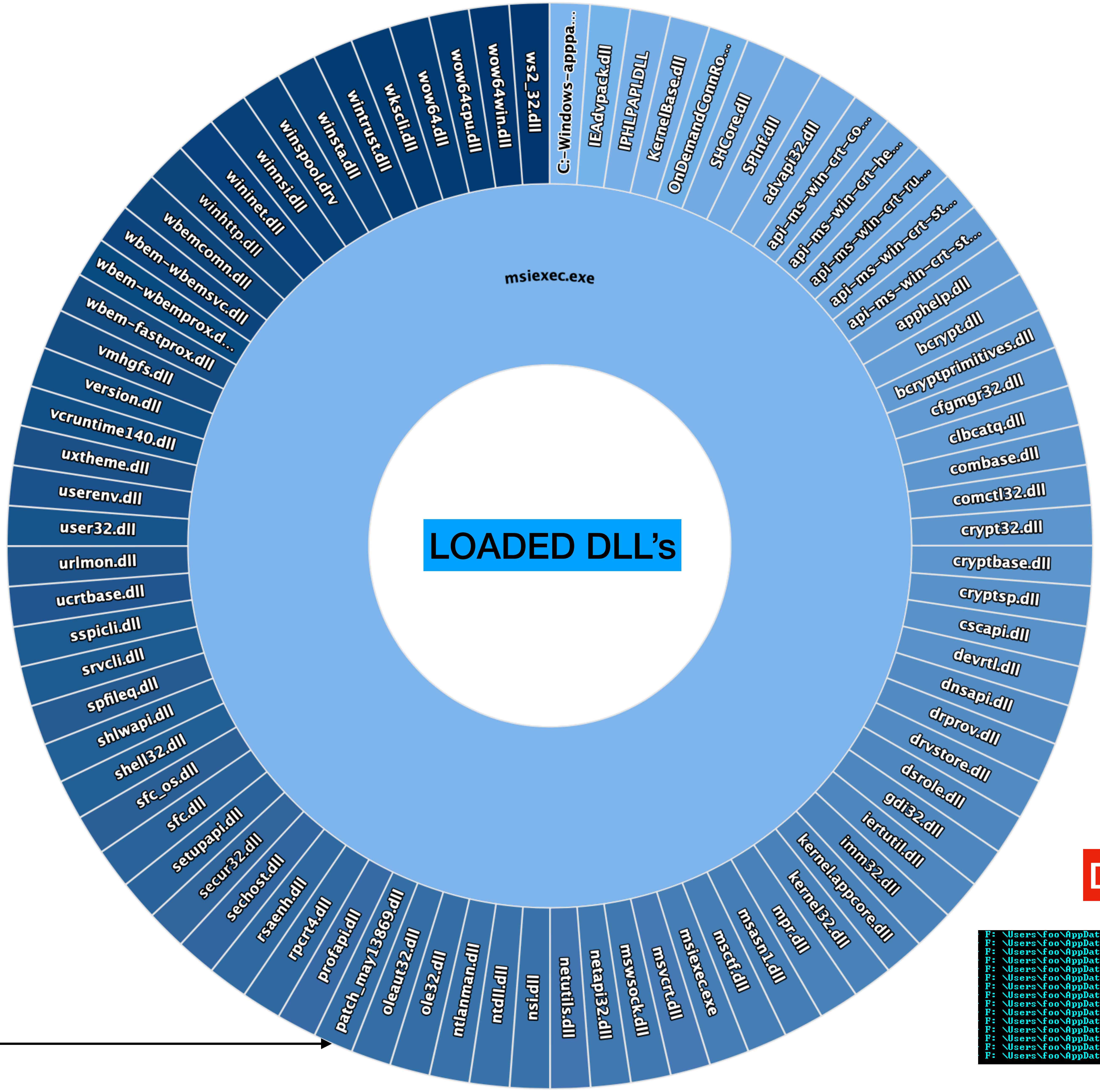
2 svchost.exe-960 → consent.exe-1660

msiexec.exe-3704 → msiexec.exe-3936 ⇄ 185.82.126.85 PORT:80
msiexec.exe-3936 → 185.82.126.87 PORT:80

3 services.exe-520 → VSSVC.exe-3520
services.exe-520 → svchost.exe-3532

1 explorer.exe-2888 → msiexec.exe-388 ⇄ 2.21.231.241 PORT:80
msiexec.exe-388 ⇄ 151.139.128.14 PORT:80
msiexec.exe-388 ⇄ 23.208.213.45 PORT:80

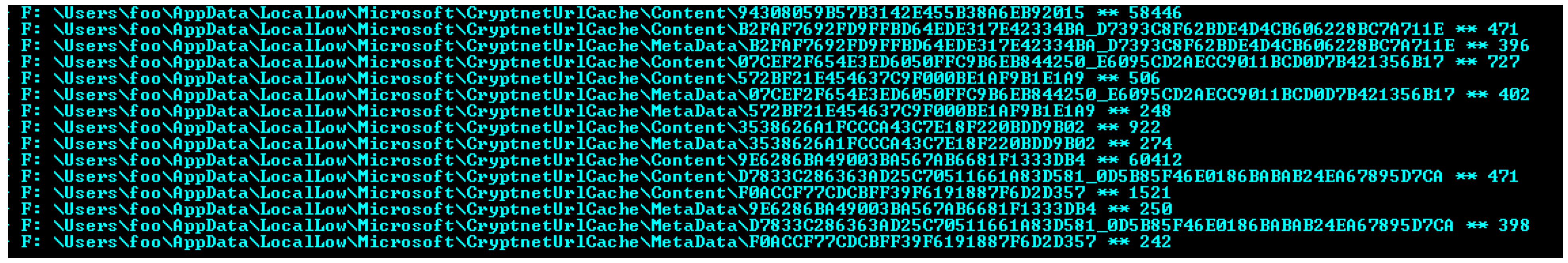
```
(LAYER: 4)
s_port: 53 |d_port: 50210 |len=50210
    9E 10 81 80 00 01 00 01 00 00 00 00 04 6F 63 73          ...?.........ocs
    70 08 63 6F 6D 6F 64 6F 63 61 03 63 6F 6D 00 00          p.comodoca.com..
    01 00 01 C0 0C 00 01 00 01 00 00 00 05 00 04 97          ................
    8B 80 0E                                                 .?.

============================ (UDURRANI) ==============================
(INIT) SYN PACKET SENT FROM 172.16.223.241     TO IP ADDRESS 151.139.128.14
     PORT INFORMATION (53947, 80)
     SEQUENCE INFORMATION (3646102650, 0)
     |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (66)

============================ (UDURRANI) ==============================
(DATA PUSH!) IS COMING FROM 172.16.223.241     TO IP ADDRESS 151.139.128.14
     PORT INFORMATION (53947, 80)
     SEQUENCE INFORMATION (3646102651, 2846469139)

     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (285)
    47 45 54 20 2F 4D 46 45 77 54 7A 42 4E 4D 45 73          GET /MFEwTzBNMEs
    77 53 54 41 4A 42 67 55 72 44 67 4D 43 47 67 55          wSTAJBgUrDgMCGgU
    41 42 42 52 54 74 55 39 75 46 71 67 56 47 48 68          ABBRTtU9uFqgVGHh
    4A 77 58 5A 79 57 43 4E 58 6D 56 52 35 6E 67 51          JwXZyWCNXmVR5ngQ
    55 6F 42 45 4B 49 7A 36 57 38 51 66 73 34 71 38          UoBEKIz6W8Qfs4q8
    70 37 34 4B 6C 66 39 41 77 70 4C 51 43 45 44 6C          p74Klf9AwpLQCEDl
    79 52 44 72 35 49 72 64 52 31 39 4E 73 45 4E 30          yRDr5IrdR19NsEN0
    78 4E 5A 55 25 33 44 20 48 54 54 50 2F 31 2E 31          xNZU%3D HTTP/1.1
    0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65          ..Connection: Ke
    65 70 2D 41 6C 69 76 65 0D 0A 41 63 63 65 70 74          ep-Alive..Accept
    3A 20 2A 2F 2A 0D 0A 55 73 65 72 2D 41 67 65 6E          : */*..User-Agen
    74 3A 20 4D 69 63 72 6F 73 6F 66 74 2D 43 72 79          t: Microsoft-Cry
    70 74 6F 41 50 49 2F 36 2E 31 0D 0A 48 6F 73 74          ptoAPI/6.1..Host
    3A 20 6F 63 73 70 2E 63 6F 6D 6F 64 6F 63 61 2E          : ocsp.comodoca.
    63 6F 6D 0D 0A 0D 0A                                     com....

01 F6 30 81 DF 02 01 01 30 0D 06 09 2A 86 48 86          ..0.....0...*.H.
F7 0D 01 01 05 05 00 30 7B 31 0B 30 09 06 03 55          .......0{1.0...U
04 06 13 02 47 42 31 1B 30 19 06 03 55 04 08 0C          ....GB1.0...U...
12 47 72 65 61 74 65 72 20 4D 61 6E 63 68 65 73          .Greater Manches
74 65 72 31 10 30 0E 06 03 55 04 07 0C 07 53 61          ter1.0...U....Sa
6C 66 6F 72 64 31 1A 30 18 06 03 55 04 0A 0C 11          lford1.0...U....
43 6F 6D 6F 64 6F 20 43 41 20 4C 69 6D 69 74 65          Comodo CA Limite
64 31 21 30 1F 06 03 55 04 03 0C 18 41 41 41 20          d1!0...U....AAA
43 65 72 74 69 66 69 63 61 74 65 20 53 65 72 76          Certificate Serv
69 63 65 73 17 0D 32 30 30 39 32 30 32 33 31 32          ices..2009202312
31 37 5A 17 0D 32 30 30 39 32 37 32 33 31 32 31          17Z..20092723121
37 5A A0 30 30 2E 30 1F 06 03 55 1D 23 04 18 30          7Z.00.0...U.#..0
16 80 14 A0 11 0A 23 3E 96 F1 07 EC E2 AF 29 EF          .?....#>......).
82 A5 7F D0 30 A4 B4 30 0B 06 03 55 1D 14 04 04          ...0..0...U....
02 02 13 2D 30 0D 06 09 2A 86 48 86 F7 0D 01 01          ...-0...*.H.....
05 05 00 03 82 01 01 00 65 10 3D 53 D4 DB 0B 60          ........e.=S..`
DF 51 B2 74 80 CC 85 D9 7B 97 2B EC AF 77 40 D1          .Q.t?...{.+..w@.
50 7C A1 8F 6B 37 75 78 2A F9 42 9C 47 F6 D1 E4          P|..k7ux*.B.G...
01 B5 AA 1F E7 DB 92 C4 95 EB D9 A8 31 59 6E FA          ............1Yn.
BF 8B 7B 7D 92 9C 47 CF 0B AF F9 F5 1F C4 5A 39          ..{}..G.......Z9
E4 F1 B6 C4 6D 17 22 A8 EE C7 D4 FA DA 44 B3 8E          ....m."......D..

(LAYER: 4)
s_port: 53 |d_port: 62374 |len=62374
    DF EF 81 80 00 01 00 01 00 00 00 00 04 6F 63 73          ...?.........ocs
    70 09 75 73 65 72 74 72 75 73 74 03 63 6F 6D 00          p.usertrust.com.
    00 01 00 01 C0 0C 00 01 00 01 00 00 00 05 00 04          ................
    97 8B 80 0E                                              ..?.

============================ (UDURRANI) ==============================
(INIT) SYN PACKET SENT FROM 172.16.223.241     TO IP ADDRESS 151.139.128.14
     PORT INFORMATION (53949, 80)
     SEQUENCE INFORMATION (3444352876, 0)
     |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
     (66)
```



0x1943601152

Malicious DLL

Dropped files

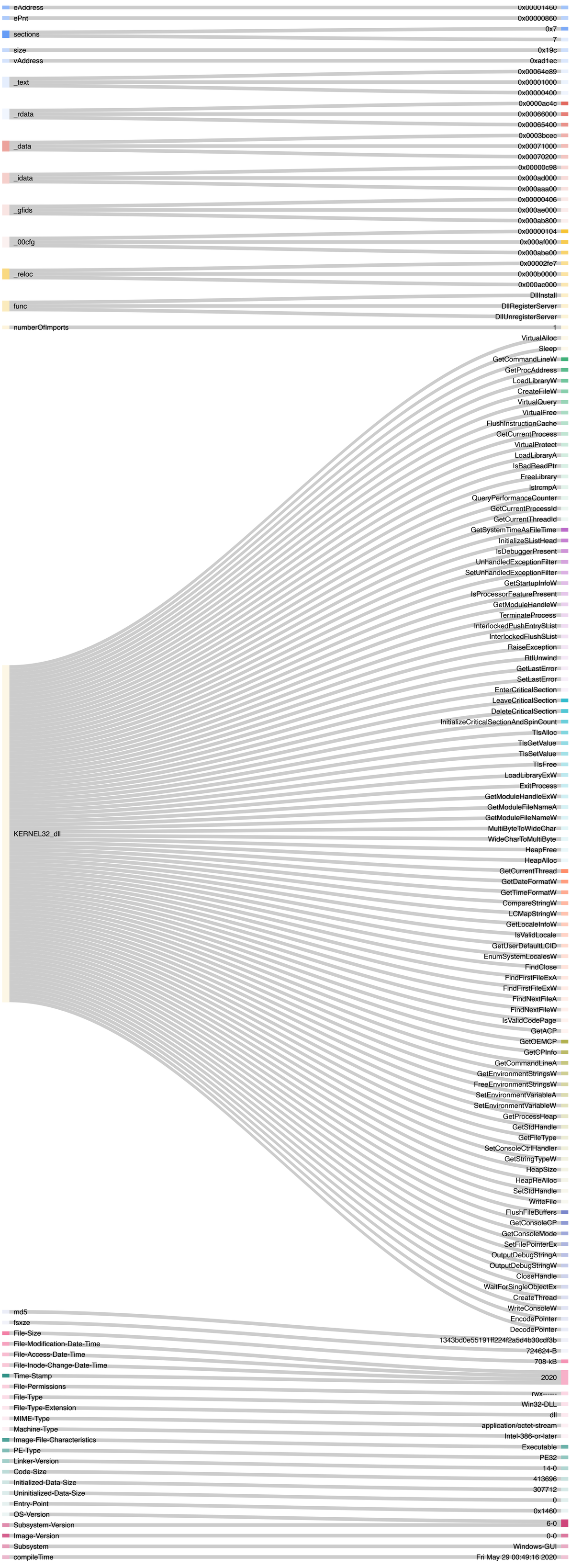


```
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A6EB92015 ** 58446
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E ** 471
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E ** 396
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\07CEF2F654E3ED6050FFC9B6EB844250_E6095CD2AECC9011BCD0D7B421356B17 ** 727
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\572BF21E454637C9F000BE1AF9B1E1A9 ** 506
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\07CEF2F654E3ED6050FFC9B6EB844250_E6095CD2AECC9011BCD0D7B421356B17 ** 402
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\572BF21E454637C9F000BE1AF9B1E1A9 ** 248
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3538626A1FCCCA43C7E18F220BDD9B02 ** 922
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3538626A1FCCCA43C7E18F220BDD9B02 ** 274
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9E6286BA49003BA567AB6681F1333DB4 ** 60412
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D7833C286363AD25C70511661A83D581_0D5B85F46E0186BABAB24EA67895D7CA ** 471
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0ACCF77CDCBFF39F6191887F6D2D357 ** 1521
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9E6286BA49003BA567AB6681F1333DB4 ** 250
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D7833C286363AD25C70511661A83D581_0D5B85F46E0186BABAB24EA67895D7CA ** 398
F: \Users\foo\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0ACCF77CDCBFF39F6191887F6D2D357 ** 242
```

RANSOM NOTE

```
--------------
| Attention! |
--------------

Your company network has been hacked and breached. We downloaded confidential and private data.
In case of not contacting us in 3 business days this data will be published on a special website available for public view.

Also we had executed a special software that turned files, databases and other important data in your network into an encrypted state using RSA-2048 a
A special key is required to decrypt and restore these files. Only we have this key and only we can give it to you with a reliable decryption software.

--------------------------------------
| How to contact us and be safe again |
--------------------------------------

The only method to restore your files and be safe from data leakage is to purchase a private key which is unique for you and securely stored on our se
After the payment we provide you with decryption software that will decrypt all your files, also we remove the downloaded data from your network and n

There are 2 ways to directly contact us:

1) Using hidden TOR network:

   a) Download a special TOR browser: https://www.torproject.org/
   b) Install the TOR browser
   c) Open our website in the TOR browser: http://o3n4bhhtybbtwqqs.onion/4E5FFEBF9BB36C58
   d) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

   a) Open our website: https://sekhmet.top/4E5FFEBF9BB36C58
```

DLL STATIC VIEW



LOADED DLL, B_ADDRESS, SIZE